Erka Koivunen

EFFECTIVE INFORMATION SHARING FOR INCIDENT RESPONSE COORDINATION

Reporting Network and Information Security Incidents and Requesting Assistance

Faculty of Electronics, Communications and Automation

Thesis submitted for examination for the degree of Master of Science in Technology in Espoo, 30 May 2010.

Instructor:

Timo Lehtimäki, M.Sc. (Tech.)

Supervisor:

Prof. Tuomas Aura

Aalto University
School of Science
and Technology

AALTO UNIVERSITY
SCHOOL OF SCIENCE AND TECHNOLOGY

MASTER'S THESIS
ABSTRACT

Author: Erka Koivunen

Thesis Title: Effective Information Sharing for Incident Response Coordination: Reporting Network and Information Security Incidents and Requesting Assistance

Date: 2010-05-30 Language: English Number of Pages: 87 + 35

Faculty of Electronics, Communications and Automation

Department of Computer Science and Engineering

Data Communications Software

Supervisor: Prof. Tuomas Aura

Instructor: Timo Lehtimäki, M.Sc. (Tech).

One often neglected aspect of network and information security incident response is the art of requesting assistance. There is a delicate balance to be struck between clarity and completeness of incident reports as well as choosing the best possible set of addressees in order to get the desired response to the assistance requests.

Designated points-of-contact, such as internet service providers' abuse helpdesks, as well as coordinative bodies, such as computer security incident response teams (CSIRTs), receive a constant flow of incident reports. These reports exhibit varied levels of technical clarity and operational relevance – ranging from unintelligible to actionable. The CSIRTs with a national responsibility typically handle the widest variety of incident types. Therefore, they must adopt a relatively agnostic approach to identifying from whom to request assistance.

Regrettably, there are no universally agreed standards for formatting the incident reports or easily communicable specifications on what information is required in the reports to ensure a successful resolution of the incident. To make matters worse, it is often difficult to anticipate, which parties will be involved in the eventual investigation and resolution of the incident and what kind of roles they will assume. Lack of trust between the parties may bring the investigation to a halt if the processes and underlying assumptions for information sharing are not well understood. Competing priorities, legal obscurities and mandate conflicts create the possibility for misunderstandings that can further complicate cooperation.

This study presents a collection of carefully analysed real-life incidents as seen from the national CSIRT's viewpoint. The focus is in the information flow. In an effort to add perspective, the way things are handled in practice is then contrasted with standards and other normative literature governing incident response. Areas of development in both the standardisation regime and incident response practices are identified.

The results of this study are being used in the development of incident response practices and automated tools such as Abuse Helper at CERT-FI. Other CSIRTs are encouraged to utilise the study findings as well. The results can be used as a background material for standardisation. Some of the transcribed case studies have been submitted for consideration in the preparations of the ITU-T CYBEX Framework.

Keywords: Information Security, Network Security, NIS, Incident, Information Sharing, CERT, CSIRT, Abuse, RFC, Request for Comments, IODEF, CYBEX.

AALTO-YLIOPISTO
TEKNILLINEN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Erka Koivunen

Työn nimi: Tehokas tietojen vaihto tietoturvaloukkausten selvittämisen tukena. Tietoturvaloukkausten raportointi ja toimenpidepyynnöt

Päivämäärä: 30.5.2010 Kieli: Englanti Sivumäärä: 87 + 35

Elektroniikan, tietoliikenteen ja automaation tiedekunta

Tietotekniikan laitos

Tietoliikenneohjelmistot

Valvoja: Prof. Tuomas Aura

Ohjaaja: DI Timo Lehtimäki

Tietoturvaloukkausten käsittelystä puhuttaessa usein aliarvioidaan, miten haastavaa ulkopuolisen avun pyytäminen saattaa olla. Tietoturvaloukkauksista raportoitaessa on pyrittävä tasapainoilemaan välitettävän viestin selkeyden ja teknisen tietosisällön kattavuuden välillä. Tarkoituksenmukaisen vasteen saamiseksi on myös kiinnitettävä huomiota, kenelle raportit osoitetaan.

Tietoturvaloukkausraporttien vastaanottoon ja käsittelyyn osoitetut yhteyspisteet, kuten teleyritysten väärinkäytösten selvittämiseen erikoistunut asiakastuki sekä tietoturvaloukkaustapauksia koordinoivat tahot, kuten CSIRT-toimijat vastaanottavat jatkuvana virtana tapausraportteja. Raporttien tekninen taso ja operatiivinen arvo on kirjavaa. Osa johtaa suoraan toimenpiteisiin, osaa ei edes kyetä tulkitsemaan. Koska kansallisten CSIRT-toimijoiden vastuualue on kattavin, niiden tulee omaksua varsin ennakkoluuloton asenne yhteistyökumppanien valintaan.

Valitettavasti alalla ei ole yleisesti hyväksyttyjä standardeja tietoturvaloukkausilmoitusten raportointiin saati sitten helposti tulkittavia kuvauksia siitä, mitä tietoja tietoturvaloukkauksen onnistuneen käsittelyn varmistamiseksi tarvittaisiin. Asiaa ei ainakaan helpota se, että usein on vaikeaa nähdä ennalta, mitä kaikkia osapuolia tietoturvaloukkauksen selvittämiseksi tullaan tarvitsemaan ja missä roolissa osapuolet toimivat. Osapuolten välisen luottamuksen puute voi jopa estää tapauksen selvittämisen, mikäli prosessin eteneminen ja tietojen jakamista koskevia periaatteita tulkitaan eri tavoin. Priorisointiongelmat, kiistanalaiset lakitulkinnat ja toimivaltaan liittyvät konfliktit voivat johtaa väärinkäsityksiin ja vaikeuttavat yhteistyötä.

Tässä tutkielmassa esitellään joukko perusteellisesti analysoituja todellisia tietoturvaloukkaustapauksia ja arvioidaan, kuinka niiden raportoinnissa onnistuttiin kansallisen CSIRT-toimijan näkökulmasta. Arvioinnin syvyyttä lisätään vertaamalla näitä käytännön tapauksia alaa koskeviin standardeihin ja muihin ohjausasiakirjoihin. Työssä tunnistetaan kehittämistarpeita sekä tietoturvastandardien että käytännön tietoturvatyön osalta.

Tutkielman tuloksia tullaan hyödyntämään CERT-FI:n toiminnan kehittämisessä. Muita CERT-toimijoita rohkaistaan tutustumaan tutkimuksen löydöksiin. Tutkielmaa voi hyödyntää myös standardoinnin taustamateriaalina. Osa tapauskuvauksista toimitettiin ITU-T:n CYBEX-työryhmän arvioitavaksi tutkielman ollessa vasta valmisteltavana.

Avainsanat: Tietoturvallisuus, tietoturvaloukkaukset, NIS, tiedonvaihto, CERT, CSIRT, Abuse, RFC, Request for Comments, IODEF, CYBEX

Preface

Many people – not least I myself – were positively surprised to learn about my graduation after me having spent 17 years of cosy life as an undergraduate student at TKK.

This thesis has been "in the works" already since the year 2000. At the time, while serving as a conscript in the military, I made a decision to seek a career in information security. Incident response in particular seemed interesting, as I felt fascinated to see how the technical constructs break and policy statements are violated. Since then, many ideas for topics have come and gone but they all seem to have revolved around the notion of something bad taking place in the context of information security. Incidents, that is.

Now, after ten years, the career has become a reality. Somehow, still I felt incomplete without putting a finishing touch to my studies. Although I only submitted this thesis right at the last possible moment, it represents what I have wanted to say all this time.

I wish to express my gratitude to my supervisor Prof. Tuomas Aura and my instructor Mr. Timo Lehtimäki. Their encouragement was sincere throughout the duration of the work. It helped overcome all the obstacles encountered.

During the course of writing the thesis following people volunteered to give helpful advice and took time from their busy schedules to comment draft versions: Damir Rajnovic of Cisco Systems, Thomas Millar of US-CERT, Marco Thorbruegge of ENISA, Eneken Tikk of CCD COE, Mikko Hyppönen of F-Secure, and several people from CERT-FI: Harri Bryk, Juhani Eronen, Sauli Pahlman, and Antti Kiuru. I was not able to incorporate all the excellent advice in this study but they will not be forgotten. William Martin of Aalto University helped eliminate the worst cases of "Finglish" in my text.

Our as-of-yet-unnamed son was born during the final stages of writing this study report. Words cannot express how obligated I feel to finish this project so that I can devote the rest of my life to him.

Hanna. Without your endurance and continued support, I would have never finished this project. This was an exceptionally rough spring for both of us. Next year we will calmly look back to this all and give it a good laugh, won't we. I love you!

Helsinki, 30 May 2010

Erka Koivunen

Table of Contents

Glossary

API	*Application Programming Interface*, a structured way for a software program to exchange information and interface with other software
ASN	*Autonomous System Number*, a numerical identifier for a group of IP networks (Autonomous Systems) with a single and clearly defined external routing policy
Botnet	Centrally controlled network of hijacked computers (called *bots* or *zombies*). The term is derivative of expression *Robot Network*
CERT®	*Computer Emergency Response Team*, a registered trademark of Carnegie Mellon University. [16] See also: CSIRT
CERT/CC	*CERT® Coordination Center* (USA), www.cert.org
CERT-FI	Computer Emergency Response Team of Finnish Communications Regulatory Authority (Finland), www.cert.fi
CIIP	*Critical Information Infrastructure Protection*
CPNI	*Centre for Protecting National Infrastructure* (United Kingdom), www.cpni.gov.uk
CSIRT	*Computer Security Incident Response Team*, an alternative way of referencing to a CERT
DDoS	*Distributed Denial of Service* attack, a DoS condition induced by employing a number of attack sources in a distributed fashion
DoS	*Denial of Service* condition, a resource exhaustion situation where an ICT system becomes unresponsive as a consequence of e.g. an external attack
DNS	*Domain Name System*, a highly distributed hierarchical database to translate domain names to IP addresses expressed in numerical form and vice versa. DNS is an infrastructure service vital to functioning of the internet
EGC	*European Government CERTs Group*, www.egc-group.org

ENISA	*European Network and Information Security Agency*, www.enisa.eu
FIRST	*Forum of Incident Response and Security Teams*, www.first.org
GPG	See PGP
ICT	*Information and Communications Technology*
IDS	*Intrusion Detection System*, a system for detecting attack attempts by comparing the object's observed behaviour against known attack methods
IEC	*International Electrotechnical Commission*, www.iec.ch
IEEE	*Institute of Electrical and Electronics Engineers*, www.ieee.org
IETF	*Internet Engineering Task Force*, www.ietf.org
ISO	*International Organization for Standardization*, www.iso.org
ISP	*Internet Service Provider*
ITU	*International Telecommunications Union*, www.itu.int
ITU-T	ITU's standardisation sector
Malware	Piece of computer software or a run-time script crafted for malicious purposes. The term is derivative of an expression *malicious software*
NIS	*Network and Information Security*
PGP	*Pretty Good Privacy*, a commercial encryption tool. Open source version is called GNU Privacy Guard, GPG
Phishing	Criminal act of luring the end-users voluntarily surrender sensitive information by faking a trusted entity such as bank's web site
RFC	*Request for Comments*, a form of documenting and standardising Internet-related technologies and good practices
RIR	*Regional Internet Registry*, organisations responsible of allocating IP addresses and AS numbers

WHOIS	Network protocol commonly used to query for ownership information and technical parameters about registered network objects such as internet domain names, IP subnets and autonomous systems
XML	*Extensible Markup Language*, a standard for representing information in a structured fashion

1 Introduction

Thousands of people fall victim to information security breaches every day. The home computers of private individuals become infected with mass-spreading malware and business servers are compromised by attacks conducted by criminals on the other side of the world. The attacks deprive people of their right to confidentiality, integrity, and availability of information processing services.

Network and information security incidents pose a genuine threat to an information system's ability to function in the manner originally intended. Moreover, systems grow ever more complex and increasingly networked, adding to their interdependence. An incident's impact may be extended far beyond the primary attack target in ways difficult to anticipate. [33]

If left unresolved, these incidents have a potential to undermine the trust to the information society. It has also been debated whether the first acts of cyber warfare have already been witnessed [76],[98],[99].

1.1 Need for incident reporting

In an ideal situation, attack attempts are successfully repelled by the security controls employed by the asset owner to protect the intended target or some other entity on the attack path. Merely applying preventive measures to protect information security is not sufficient, however. The architectural characteristics of the internet make it virtually impossible to completely prevent attacks from taking place. In their essay, Böhme and Moore [15] suggest that there is sound economic sense in shifting some of the focus from preventive security controls to the incident response, given that lessons are learnt from past incidents.

> *"If instead we allow for repeated defensive investments, an uncertain defender will initially protect fewer assets and wait for the attacker to 'identify' the weakest links to be fixed in later rounds. Hence, it can be quite rational to underinvest in security until threats are realized."* [15]

According to Böhme and Moore, an effective incident response aims to frustrate the criminal utilisation of the information and communications technology (ICT), thus helping to prevent further incidents.

> *"There is substantial evidence that attackers concentrate their efforts at the most irresponsible ISPs, moving on to others once the ISP cleans up its act or is shut down."*

It would be fair to assume that this holds true to not only internet service providers (ISP) but also everyone present in the internet: corporations, governments, private citizens, content providers, and even nations.

While it is advisable to continue investing in preventive measures such as traffic filtering, software updates and awareness building, experience has shown that there is an ever-greater demand for efficient after-the-fact handling of computer security incidents. For incidents are increasing in numbers and have potential to incur ever more dire consequences for the law-abiding citizens. Security vulnerabilities and configuration weak-

nesses will prevail and flawed human judgement continues to create plenty of opportunities for successful attacks also in the future. Learning as much as possible about the incidents and being able to investigate them efficiently is crucial to the survival of the information society.

It would seem obvious that there would be a positive attitude towards resolving incidents as quickly and effectively as possible. One would expect that historical incidents would be carefully studied to identify good practice in areas of prevention, detection, and mitigation. [56],[54] Furthermore, in the light of publicised incidents one would expect that the systems designers and service providers would make it their priority to build the systems resilient enough to withstand external failures and to endure direct attacks. [24] This is not necessarily the case, however.

Detection capabilities would need to be enhanced in a way that would enable incident responders to discover security breaches or attempted attacks as early as possible. Currently, many attack victims are caught by surprise. In addition, knowledge about past incidents along with the observed effects of associated security controls would need to be analysed more carefully. For the organisations to be able to step up the preventive measures to protect against future attacks, more and better quality information about recent attacks would be needed. The problem, however, is that the information does not necessarily reach those who would need it. The process, as depicted in Figure 1, cannot tolerate discontinuations in information flow.

Figure 1 – Effective incident response can help enhance preventive security controls in the future.

Information about attempted attacks may shed some light on the attack methods employed, help bring to light other attack targets and collateral victims and possibly even identify the attackers. Successful attacks, on the other hand, would require concrete responses to limit further damage and to recover from that already caused. Information sharing is a prerequisite for an effective response in situations where actions would need to be taken by two or more actors together. Due to the highly distributed nature of virtually all practical information systems, these situations arise constantly.

This calls for agile approaches to troubleshooting network and information security incidents such as those practiced by, for instance, ISPs, computer security incident response teams (CSIRTs), anti-virus companies, and internet security researchers.

1.2 Information sharing challenge

Professionals in the fields of incident handling and incident coordination have learnt to appreciate the difficulty of reporting incidents in a meaningful and efficient way. Common difficulties stem from incomplete (or altogether missing!) information or a failure to share the information with relevant parties in due time. All too often, important information crucial to solving the incident either is not collected at all, never reaches the people in position to take action or is not used to draw conclusions that would help build better systems or processes in the future.

The information about incidents is technical by nature and its collection on a system level is largely dictated by the needs of systems engineering and technical troubleshooting. While the act of turning on the event logging in the ICT systems is technically easy, spotting which portions of the information gathered are relevant to further analysis poses problems. The difficulties in incident response lie mostly in inter-organisational cooperation and poor communication.

Too few organisations have meaningful incident response strategies. The management may need convincing as to why it would be in the interest of the organisation to maintain a dedicated function to receive trouble reports from outsiders. Organisations have reservations in seeking outside advice or extending investigations to involve external parties. Conveying the information in a trustworthy fashion requires the creation of a pre-existing infrastructure and establishment of a network of trusted contacts. Unprepared organisations would have a hard time determining, which people in their own staff or contractors' workforce would be in a position to resolve an incident and what information they would need to succeed in the task.

1.3 Research problem

Enhancing the incident response process requires ensuring that the correct amount of technically valid and actionable information is being collected and effectively shared among the incident handlers. Only once we understand what information is needed in different parts of the process, we are able to discuss how the actual exchange can be realised by technical – and ultimately – by automated means.

Our challenge is, then, to identify effective ways to bring information about the incidents to the potential victims or to those with the means to protect them. As it turns out, there are plenty of process inefficiencies to be solved.

Figure 2 – Components of information exchange during the incident response.

In our work, we focus on four phases of the incident response process as highlighted in green in Figure 2. We then present ourselves a following set of questions corresponding to each of the phases.

- How to distinguish which anomalies in local ICT systems are indicative of computer breaches taking place somewhere else?
- How to identify authoritative points of contacts to approach and to exchange the collected evidence with?
- What data formats and structures should one use during the exchange?
- How to validate that the report contains accurate and actionable information and that the reporting party is who he claims to be?

It is our belief that answers to the abovementioned questions can yield important clues that help us solve process deficiencies identified.

1.4 Definitions

1.4.1 Network and information security - NIS

The term *ubiquitous computing* usually refers to the pervasive and invisible nature of modern day networked computing. All kinds of constructs from a seemingly simple coffee maker to multi-billion euro nuclear power plants contain microprocessors, communications links, and interfaces that connect their internal computing capabilities to the outside world. Under hostile circumstances, however, ubiquitousness can spell out largely unpredictable and surprisingly widespread adverse effects should critical information systems fail.

To underline the interconnectedness of network security and information security, the European Network and Information Security Agency (ENISA)[1] insist on using the term *Network and Information Security,* or *NIS,* in their publications. Unfortunately, the use of the term outside official European Union publications has so far been rather limited. EU directives since 2001 use the term in a fashion that suggests it is assumed well introduced [109]. ENISA itself defines the term in relation to the network-connected object's ability to resist attacks.

> *"The ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems."* [36]

The abbreviation NIS is used throughout this study as convenient shorthand when referring to the broader meaning of security in our society that is heavily dependent on ICT.

1.4.2 Events, attacks and incidents

Howard and Longstaff [51] define an *incident* in the context of network and information security as

> *"a group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing."*

Additionally, they define an attack as a series of events

> *"intended to result in something that is not authorized to happen."*

To complete the definition chain, Institute of Electrical and Electronics Engineers (IEEE) defines an *event* as

> *"an action directed at a target which is intended to result in a change of state (status) of the target."* [80]

It can be argued that this triplet describes incidents to be a consequence of some action taken with malicious intent. On the other hand, Request for Comment (RFC) documents 2828 [93] and 2350 [10] (respectively) define the terms *security incident* and *computer security incident* as follows:

---

[1] http://www.enisa.eu

> *"A security event that involves a security violation."*

and

> *"any adverse event which compromises some aspect of computer or network security."*

International standardisation body ISO/IEC [54] defines an *information security incident* as

> *"a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security."*

These definitions omit the requirement of intent. Instead, they focus on the adverse effects to the observed object. The definitions stem from the notion of incidents being a departure from the norm – a behaviour different from the expected and harmful by nature in an otherwise controlled environment. Or, to put it in the terms more familiar to the security professionals, incidents are violations of security policies.

Importantly, according to RFC 2350, even failed attacks should be considered as incidents

> *"Attacks, even if they failed because of proper protection, can be regarded as Incidents."* [10]

To summarise, incidents in the NIS sense are situations where effects harmful to security have manifested or have had potential to manifest in the networks or networked information systems.

Some incidents may turn out to be caused by administrative errors, end-user lapses, unfavourable circumstances, or just bad luck. Worryingly often, however, they are caused by irresponsible or downright hostile actions taken by outside parties to spread damage or to gain unfair advantage over others.

1.4.3 CSIRTs and CERTs

The need to handle voluminous number of NIS incidents has lead some organisations to establish specialised teams dedicated to incident response. These teams are often called CERTs or CSIRTs, but other terms such as abuse helpdesks and security teams are also used. Acronyms *CERT* and *CSIRT* stand for "computer emergency response team" and "computer security incident response team," respectively.

The reader should be advised that the expressions CERT and Computer Emergency Response Team are registered trademarks of Carnegie Mellon University of Pittsburgh, PA in the United States of America. The university hosts the world's first CERT organisation, namely *CERT Coordination Center* or *CERT/CC* for short. For the purpose of this study, however, the terms CERT and CSIRT are used interchangeably and they both refer to incident response teams without indicating any distinction between the terms or without underlining any organisational affiliation.

According to the frequently asked questions portion of the CERT Coordination Center's web pages

> *"A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity."* [17]

On the other hand, a report prepared by the European Network and Information Security Agency defines CSIRT as follows:

> *"A CSIRT is a team that responds to computer security incidents by providing all necessary services to solve the problem(s) or to support the resolution of them."* [8]

Throughout this document, it is assumed that incidents are being handled by incident response teams of some kind. These teams can be either formally established CERTs or informal collections of individuals in relevant positions within their respective organisations working together to solve an incident. Being able to contribute to the handling of an incident is considered more important than the actual organisational form or status of the contributing party.

1.5 Structure of the study

An effort has been made to organise this thesis in a way that highlights the gap between theoretical ideals, such as standards, and the practical state of affairs in NIS incident reporting.

The first chapter is a short introductory text describing the study topic. Terminology central to understanding the study is presented. Chapter 2 presents the methods used during the research and explains the underlying assumptions that the reader should be aware of.

Beginning from Chapter 3, we begin our dive into the actual substance of the study. Normative literature and best practices governing the discovery of incidents, identifying points of contacts, data exchange formats and ways to establish the authenticity of both the report and the reporter are presented. Even the title of this chapter hints that these are idealised models. In the last two subsections, we take a brief tour to familiarise ourselves with the current advances in the field.

In a deliberate effort to contrast the reality with the somewhat rosy worldview of information security standards, we then walk through a set of real-life incidents in Chapter 4. Even though presenting the practice of incident response ended up filling a major portion of the study, the sacrifice was deemed necessary. Normally, the details of the information exchange taking place during the incident response are visible only to the "insiders" participating in the response process. Careful transcription of practical incidents opens these details to the "outsiders," too. Already during the preparation of the study report, the incident descriptions were being used as background material to benefit standardisation efforts at United Nations telecommunications body ITU-T. During the research, it became obvious that the post-mortem transcriptions of the incidents revealed new information even to the incident handlers themselves. Some surprises were positive, some revealed systematic omissions and even failures that would need to be addressed in the future.

Chapter 5 is dedicated to discussion of the merits and shortcomings of both the idealised models and the observed real-life practices. For the impatient reader in search of concrete recommendations, this would be the most important chapter.

Chapter 6 summarises the whole study and lists the key findings. Moreover, areas for future study are suggested.

The appendices contain additional material not essential to understanding the report's conclusions. Appendix II would be recommended reading for a reader not familiar with the investigative tools used by CERTs to collect information about incidents. The chapter walks us through a series of rudimentary tools using information about Aalto University systems as examples.

2 Methodology

This study is a culmination of the author's ten-year-long professional experience in the field of NIS incident response. The report was commissioned by the Finnish Communications Regulatory Authority, which hosts the Finnish national incident response team, *CERT-FI*. The author has been the head of CERT-FI since November 2005.

Consequently, the focus of the study is on incidents with relevance to CERTs with a national responsibility. Examination of how individual end-users and plaintiffs are involved is thus limited to the portions interfacing the handling of an incident by the CERTs and the network owners.

Throughout the document, the incident handling conventions followed reflect those adopted by CERT-FI and may differ from the operating procedures used by other incident responders. The study is not to be interpreted as an effort to endorse CERT-FI procedures over others. An earlier study conducted by Bryk [13],[12] has already established that all national CERTs are unique and eventually evolve to reflect the legal, economical and policy realities of each nation, economy and governing culture.

2.1 Data sources

Data sources used in this study can be grouped in three categories: written documents found in public sources, oral and anecdotal material, and non-public references.

2.1.1 Public documents

Standards and practices in the field of incident response and associated information exchange are still evolving, which helps explain the report's bias towards referencing RFC documents over other standards literature. Opinions have been voiced that RFCs should not be treated as standards in the traditional sense. RFCs, however, appeared to be the most easily available references in the field.

Upon assessing the authority of a given RFC, some consideration was given to the number of external referrals to the documents. In this sense, RFCs 2350 (expectations to incident response) and 5070 (IODEF) appeared to be actively enforced norms while some other RFCs seemed to have gained less support in practical incident response.

2.1.2 Non-public documents

This report is to be treated as a public document. Use of non-public sources has been limited in a way not to affect the document's status.

Understanding that non-public sources can be difficult or downright impossible for the reader to cross-check, an effort has been made to also find unclassified versions of the non-public documents.

The real-life incidents covered in Chapter 4 were selected from the CERT-FI incident archives. Information provided by CERT-FI was – where possible – augmented by information found from public sources. Upon selecting the incidents, precedence was

given to incidents where public material could be found. It should be acknowledged that it is not common for the incident reporters to make their findings public.

It is understandable that this lack of openness has the potential to distort the image of typical incidents reported to CERT-FI. The reader is cautioned against assuming that the selection of incidents would represent a full and balanced range of incidents handled by CERT-FI or any other national CERT.

The material in the CERT-FI archives is assumed sensitive and is largely left unpublished. Citations to non-public material are chosen in a way to avoid publishing potentially non-public portions. If only single characters or words are being edited for publishing, and the text is otherwise relevant to the study, the redacted portions are marked with a black bar similar to this: [redacted]. The length of the bar does not necessarily reflect the length of the removed text. This is not to be confused with citations truncated for brevity. Removed portions are marked with two dots surrounded by square brackets: *[..]*.

It is debatable, whether portions of the incident material published by third parties could after all be interpreted as containing personally identifiable information or corporate secrets. However, since the material had already been made available from public sources, a decision was made for the benefit of this study to treat the material as public.

No effort was made to obtain material from other incident handlers' archives. This is only partly justified by logistical convenience. It is a shared opinion among CERTs that information related to incidents is requested and shared for the sole purpose of incident handling, not for making the material public. It was decided that no enquiries of this nature would be sent, as they would have the potential of endangering CERT-FI's reputation as a trustworthy reporting partner.

2.1.3 Oral and anecdotal sources

No actual interviews were conducted for the purpose of the study. Written material was given precedence and public documents were preferred over non-public ones. Some statements and conclusions in this study, however, are based on information obtained from authoritative people with whom the author has been in touch. These anecdotal sources have been documented with the permission of the source. Unless a source is specifically stated, the conclusions and opinions are drawn from the author's own professional experience.

2.2 Visualisation of information and process flow

An experiment was made to visualise the information and process flows using a tool called *GraphingWiki* [34] developed by Juhani Eronen[2]. The decision to select GraphingWiki over some of the more obvious choices, such as message sequence charts or UML flowcharts, was due to the fact that, at the time of writing the report, CERT-FI was investigating the use of wikis to aid in the analysis of complicated incidents and tracking the status of a large number of incidents.

---

[2] https://portal.huttu.net/gwiki/

The incident data and relations between the subjects were typed manually into the wiki for visualisation purposes. For the method to qualify for day-to-day operational use, the process would need to be automated. The material in the CERT-FI incident archives, however, is currently organised in a way that does not support automated visualisation of information or process flow. This was, in fact, an important finding in its own right.

Some development ideas for the GraphingWiki were identified and presented to its creator for future consideration. Especially the sorting and colouring capabilities were not readily supportive of presenting sequential flows or identifying actors in different roles.

2.3 Limits to the scope of the study

This study is not proposing any new standards or techniques. Rather, it is a study into the current state of affairs. The study is not intended as an exhaustive review of information security standards, either. The standards identified are chosen here to illustrate their applicability to practical incident response.

Legal considerations are excluded from the scope of this study. The study recognises that there are mandate differences between various CERTs but no effort to examine the causes and consequences is made. Legal issues related to the sharing of personally identifiable information as well as information protected by the laws governing communications secrecy are not covered, either. It is strongly encouraged that each incident handling party seeks competent advice before committing to data gathering and information exchange.

Furthermore, procedures and tools employed to protect the classified governmental or confidential business data and ICT systems are out of the scope of this study as each party is assumed to take such considerations into account before releasing incident data.

3 The Ideal: Data Formats and Standards

As indicated previously, some aspects of the topic of incident reporting have already been covered in earlier research and practical solutions have been developed within the community. This chapter discusses these earlier attempts and briefly touches upon some current efforts.

3.1 Correlating local anomalies and remote effects

Network and information security incidents come in many forms and wear several disguises. While the internals of intrusion detection and intrusion prevention technologies [91],[94] are beyond the scope of this study, readers are advised to familiarise themselves with some basic concepts in order to fully appreciate the complexity involved. Furthermore, for the purpose of this study, the interest lies in incidents with relevance solely to ICT systems. Hence, non-ICT information security breaches, such as dumpster-diving, corporate espionage performed by organisational insiders or dissemination of inappropriate digital content, would not be counted as NIS incidents.

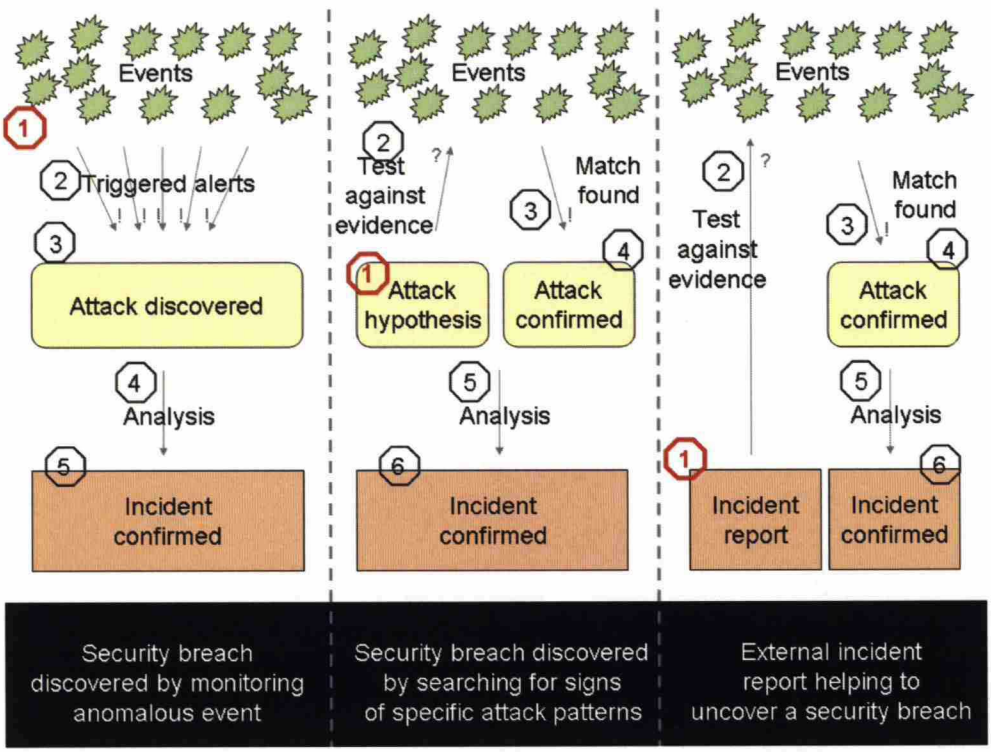

Figure 3 – Three routes via which security breaches in a networked system can be brought to the attention of the affected organisation. Incident response process entry points are highlighted in red. The three use cases from left to right correspond to chapters 3.1.1 – 3.1.3.

In Section 1.4.2, we were presented with the event – attack – incident chain. In a way, each of these concepts represents a different level of abstraction and has its own relation to a security breach in an ICT system. The response to an incident in the NIS sense may be initiated after observing an anomalous event, by searching for patterns associated with known attack methods, or after learning about plausible incident scenarios and

checking their validity against evidence. These approaches have been summarised in Figure 3 above and will be explained in the following three sections.

3.1.1 Anomalous events as triggers

A fundamental requirement for detecting NIS incidents by means of event monitoring is to have a working event logging mechanism in place. Unless the ICT system is capable of expressing what state of operation it is in at any given time or what kind of response it performed to a given input, little can be done in terms of monitoring the system for security breaches.

While this ideal is often neglected in practice, it has been recognised as an essential feature of a secure information system already over 20 years ago in the document called *Orange Book* [72]. Nowadays, a similar requirement can be found practically in all normative documents, ranging from functional auditing requirements described in Common Criteria [27] to control objectives under section 10.10 of ISO/IEC information security standards [55],[56] and to section 15 of the Finnish Act on the Protection of Privacy in Electronic Communications [41].

Monitoring anomalous system events can serve the systems administrators in both uncovering configuration errors and failing systems as well as in helping to detect attempted or successful breaches of security. While failed login attempts, refused communication attempts in a firewall and abnormal requests to web server resources may turn out to have innocuous explanations, they may also be signs of computer break-ins. As ISO/IEC 27002:2005 puts it:

> *"Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified."* [56]

Thus, anomalous events may warrant a security investigation, which in turn may lead to revealing an attack and – if the attacks turn out be orchestrated by nature – expose an incident.

Managing the creation and security of log files and fine-tuning system logging levels can be a daunting task and would deserve more in-depth treatment than is possible here. Examples of methods for managing log files for distributed systems are the *Syslog* protocol [44],[67] and various *Security Information and Event Management (SIEM)* tools [95].

Syslog has its origins in the *Berkeley Unix* operating system but it has since been adopted in several other platforms. *Syslog* has been recognised since 2001 in the RFC series of documents maintained by the Internet Engineering Task Force (IETF). At first, it was categorised as an *informational* RFC 3164. [67] A more recent revised version, RFC 5424, [44] has now been accepted in the standards track, currently as a *proposed standard.*

While *Syslog* aims to solve the distributed log collection challenge by defining a structured data format, the *SIEM* tools rather adopt an agnostic approach to event log data by accepting several different log formats. For instance, an open source tool called *OSSIM* currently incorporates 2,395 plug-ins to support legacy systems, most of which have no

native way to correlate logs. It is also possible to create new plug-ins to add support to previously undefined data sources[3].

3.1.2 Attacks as wake-up calls

Attacks have the ability to manifest themselves through complex and subtle symptoms. Even when not directly observable by monitoring the event flow, some attacks can still be detectable through various side channels. For example, a networked ICT system that all of the sudden slows down or becomes unresponsive may be experiencing a denial of service condition caused by an external attack. Unexpected error messages or out-of-normal output may indicate integrity problems resulting from unauthorized access or hostile input manipulation. Symptoms as diverse as lost business, bad press, and users being active at unusual hours could raise alarm about a leaked corporate secrets or stolen user credentials.

In many incidents, the initial discovery can be attributed to observant end-users and administrators familiar with the system having an intangible feeling of "things not being as they should." While these weak signals contain little information that would help put a finger on the problem, they may be the result of complex holistic analysis of a subconscious sort – something automated anomaly detection systems still cannot fully replicate.

Such a hypothesis naturally has to be first verified against technical facts by applying the systems engineering approach. Figuring out which parts of the system the observed symptoms may be coming from and what kind of an event trail it could produce requires intimate knowledge of the ICT system at hand.

Early-warning systems, such as the proposed *National and European Information Sharing and Alerting System (NEISAS)*[4] and *Network Security Information Exchanges (NSIE)* proposed by ENISA [37], may help to bring knowledge about attack techniques identified elsewhere to the service of local attack detection and log correlation. Application of intrusion detection systems (IDS) such as *Snort* [88],[57] and SIEMs help automate the detection once there is solid information about what signs of intrusions to look for.

3.1.3 Correlating attacks to incidents

Verified attacks and attack signatures are valuable information for those responsible for defending the information systems. As the *Honeynet Project* puts it:

> *"The primary purpose of a honeynet is to gather information on threats. [..] Security responders can use honeynets for incident response, collecting information on [..] compromised systems."* [50]

Traditionally, production of attack signatures has been dominated by vendors of anti-virus products. By collecting and analysing samples of software seen experiencing malicious behaviour, the anti-virus vendors have been able to build libraries of existing malware for their own use. The identities of these malware are then reduced to signatures, also called fingerprints, which capture the essential characteristics of the mali-

---

[3] http://www.alienvault.com/community.php?section=Plugins
[4] http://www.neisas.eu/

cious software. These signatures can then be disseminated to the users of these products in the hope of being able to identify malicious software instances before they have a chance to infect the customer computers.

Another family of NIS security products with a long tradition in attack signature sharing is intrusion detection systems, a prime example of which is the *Emerging Threats* project[5], home of the Snort signatures. Other veterans in attack information collection and sharing include the Honeynet Project[6], the *SANS DShield*[7], *Shadowserver Foundation*[8], and *Team Cymru*[9]. These operators accept voluntary incident reports and log file submissions, and use them to create an aggregated view of current attack trends.

Lately, there has been increased interest in sharing information about observed attacks with the owners of the affected networks so that they can in turn take concrete action to protect their ICT assets. This is valuable information as the attacks have been detected by systems external to those contributing to the attack. Combining such information may reveal attack patterns, indicate the target, and help identify other victims – in short, to characterise an incident. Monitoring command and control servers may reveal corporate computers turned into botnet zombies. Collecting large quantities of spam e-mails often reveals not only the spam sources but also web sites used for phishing, spreading malware or illicit advertising.

Most of the parties listed above make the information available to the network owners. The methods of sharing differ, though. For example, while DShield makes data publicly available[10], others may release the information by specific request. Companies such as *RSA*[11] and *Symantec*[12] release the information to paying subscribers only. The non-profit *Shadowserver Foundation* describes their service on their web pages[13] in the following manner:

> *"The Shadowserver Foundation filters data received from its worldwide sensor and monitoring networks and employs an analysis engine to classify the attacks. It then sorts this data according to ASN, netblock, and even Geolocation. Detected malicious activity on a subscriber's network is flagged accordingly and is included in daily summarization reports detailing the previous 24 hours of activity. Reports are only sent upon detection of malicious activity. These customized reports are made freely available to the responsible network operators as a subscription service."*

As shown in the discussion above, acquiring information about the incidents of distributed nature is not trivial. There is, however, widespread acceptance of the importance of making the information available to those with the means to secure the ICT assets. The next section discusses the difficulties in finding the asset owners.

---

[5] http://www.emergingthreats.net/
[6] http://www.honeynet.org/
[7] http://www.dshield.org/howto.html
[8] http://www.shadowserver.org/
[9] http://www.team-cymru.com/
[10] For instance, the current DShield report for autonomous system number 719 operated by Finnish telecommunications provider Elisa Oyj can be downloaded here: http://www.dshield.org/asdetailsascii.html?as=719
[11] http://www.rsa.com/node.aspx?id=3071
[12] http://deepsight.symantec.com/
[13] http://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork

3.2 Identifying points of contacts

We must accept that victims of incidents are not necessarily the ones to detect incidents taking place. Many times, the discovery is made by an outside party with possibly no practical relation to the victim. In such a case, clearly, the need to submit a report has arisen. To whom should it be addressed, then? It is not always clear who to contact, as illustrated by the following anecdote.

> *"Our hosts [during a visit to a large software company] were telling us that they only receive vulnerability reports via their customer support channels. When asked, whether our hosts had established a publicly accessible contact point for reporting security problems, they seemed astounded. They had never realised that someone from 'the outside' could be in a position to learn about security problems in their products!"* [105]

3.2.1 Internet standards

Some of the earlier attempts to solve the problem of identifying points of contacts for incident response in the internet are documented in RFCs. The RFCs of particular interest to identifying points of contacts for incident response are listed in Table 1.

Table 1 – List of RFCs with relevance to identifying organisational points of contacts for incident reports and response.

RFC name and relevant sections	RFC id	Sub-Series id	RFC status	Year
Recommended Internet Service Provider Security Services and Procedures • *2.1 Contact Information (ref. RFC 2142)* • *2.5 Incident Response and Computer Security Incident Response Teams (CSIRTs) (ref. RFC 2350)*	RFC 3013 [59]	BCP 46	Best Current Practice	2000
Internet Security Glossary	RFC 2828 [92]	FYI 36	Informational	2000
Expectations for Computer Security Incident Response • *2.1 Publishing CSIRT Policies and Procedures* • *2.2 Relationships between different CSIRTs* • *3 Information, Policies and Procedures*	RFC 2350 [10]	BCP 21	Best Current Practice	1998
Mailbox Names for Common Services, Roles and Functions • *4 Network Operations Mailbox Names* • *5 Support Mailbox Names for Specific Internet Services*	RFC 2142 [30]	N/A	Proposed Standard	1997
Site Security Handbook • *5 Security Incident Handling*	RFC 2196 [43]	FYI 8	Informational	1997
Guidelines for the Secure Operation of the Internet	RFC 1281 [77]		Informational	1991

Request for Comments – or RFCs for short – can be considered the internet community's answer to requirements for documentation, self-regulation and standardisation in a rapidly evolving environment. [7],[87] The list is sorted [86] by the RFC status (or "maturity level") in accordance with the RFC categorisation scheme described in RFC 2026 [7].

The United States National Institute of Standards (NIST) has published an incident-handling manual [45] whose Section 3.6 recommends that:

> *"Organizations should publish a phone number and e-mail address that outside parties can use to report such incidents."*

Based on the documents listed above, two conclusion can be drawn immediately. First, organisations administering internet-facing ICT infrastructure need to prepare themselves for handling information security incidents. Second, in order to facilitate this they must be approachable via publicly announced points of contacts. These observations have been addressed on several fronts.

3.2.2 Approaches taken by internet registries

Regional internet registries (RIRs) oversee the allocation of IP addresses and AS numbers. There are five RIRs, each responsible for a certain region of the world, namely RIPE NCC, ARIN, LACNIC, APNIC, and AfriNIC. Currently, the RIRs are in process of creating public registries of incident response contacts within their allocated IP networks.

- RIPE NCC has introduced an optional "IRT Object" [28] to denote "*which CSIRT is responsible for handling computer and network incidents*" [83] for a delegated IP address range (specifically: *inetnum* and *inet6num* objects).
- ARIN in North America has an optional Abuse POC record associated with IP address ranges, Autonomous System Numbers (*aut-num* objects) or organisation objects. [2]
- LACNIC of South America currently has incorporated a voluntary security contact (abuse-c) for IP address ranges and Autonomous Systems. [64],[63]
- APNIC in Asia is currently considering introducing a mandatory IRT reference for IP address ranges and Autonomous System Numbers. [63] If adopted, APNICs registry would have the strictest requirements in this sense.
- AfriNIC currently has no such mechanism; however, successful adoption of one in Asia may be followed with a similar proposal in Africa. [63]

A similar idea was adopted by Finland in 2005 when a regulation issued by Finnish Communications Regulatory Authority (FICORA) came into force. It requires the Finnish network owners to document their abuse handling contacts in WHOIS. [40]

3.2.3 Role of CSIRTs

A study conducted by the Finnish Communications Regulatory Authority (FICORA) echoes the finding of chapter 3.2.1. FICORA charted the services, organisation and mandate among 11 European national and governmental CERTs. [13],[111],[112] One of the major findings of the study is summarised as follows:

> *"The CSIRT needs to have a clearly defined point of contact that interfaces the team with the outside world."* [12]

The European Commission has identified national CSIRTs as key players in incident response coordination and has set a goal to establish CSIRTs in every European Union member state. [26] Adding to this sentiment, the European Network and Information Security Agency states the following on its web page:

> *"Not every country connected to the internet disposes of CERT capabilities. And the level of maturity among those who do vary dramatically. It is ENISAs mission to as much as we can clear out the 'white spots' on the CERT worldmap and to minimise the gaps by facilitating setting-up, training and exercising of CERTs."* [35]

CSIRTs themselves have long ago recognised the need for identifying and maintaining a list of authoritative peer contacts. Several initiatives have been introduced by organisations such as ENISA [38], CERT/CC [18], Forum of Incident Response and Security Teams (FIRST) [42],[124], Trusted Introducer (TI) [100],[127], the European Government CERTs Group (EGC) [123] and Asia Pacific Computer Emergency Response Team (APCERT) [4].

3.2.4 CIIP initiatives

Outside the standardisation and regulatory realms, the G8 countries have facilitated an *International CIIP Directory* [125], a collection of government-appointed contact points in the field of critical information infrastructure protection. The directory has since evolved and nowadays includes official contact information on 16 different topics from nearly 30 countries. The directory is compiled by the British *Centre for the Protection of National Infrastructure* (CPNI) and promoted by the *Meridian process*[14]. The document is not available to the public.

On the other hand, another somewhat similarly titled publication, the *CIIP Handbook* [11] compiled by ETH of Switzerland, is publicly available. The handbook aims to identify key policies and organisations involved in protecting the critical information infrastructure in each of the 25 countries covered. The handbook is compiled from a combination of public documents and expert interviews.

3.3 Data exchange formats

Due to the RFC mechanism having origins in protocol standardisation, one would expect that RFCs on data exchange formats would exist in the field of NIS incident exchange. Table 2 below presents a handful of RFCs with references to incident data exchange.

Table 2 – List of RFCs with relevance to negotiating data exchange formats.

RFC name and relevant sections	RFC id	Sub-Series id	RFC status	Year
The Incident Object Description Exchange Format	RFC 5070 [31]	N/A	Proposed Standard	2007
TERENA's Incident Object Description and Exchange Format Requirements	RFC 3067 [3]	[missing]	Informational	2001
Internet Security Glossary	RFC 2828 [92]	FYI 36	Informational	2000
Expectations for Computer Security Incident Response • *3.6 Incident Reporting Forms*	RFC 2350 [10]	BCP 21	Best Current Practice	1998
Site Security Handbook • *5.4.1 Types of Notification and Exchange of Infor-*	RFC 2196 [43]	FYI 8	Informational	1997

[14] http://www.meridianprocess.org

RFC name and relevant sections	RFC id	Sub-Series id	RFC status	Year
mation				

Somewhat surprisingly, RFCs prior to the 21st century were rather vague on the data formats. This suggests that automating the processing of incident reporting is a relatively new idea. Up until recent years, it was expected that communications would take place between human handlers.

A machine-readable data format was not formulated until the *Trans-European Research and Education Networking Association* (TERENA) proposed an XML-based scheme called IODEF. According to Cover:

> *"The Incident Object Description and Exchange Format (IODEF) is a format for Computer Security Incident Response Teams (CSIRTs) to exchange operational and statistical incident information among themselves, their constituency, and their collaborators. It can also provide the basis for the development of interoperable tools and procedures for incident reporting."* [29]

In the world of RFCs, IODEF remains the only serious proposal on solving the problem of automating the exchange of incident-related information. However, even RFC 5070 warns against expecting that merely agreeing on data formats would be sufficient to eliminate the need for human intervention:

> *"The domain of security analysis is not fully standardized and must rely on free-form textual descriptions. The IODEF attempts to strike a balance between supporting this free-form content, while still allowing automated processing of incident information."* [31]

In a presentation [32] during the FIRST Conference 2009 in Kyoto, Till Dörges brought together a comprehensive listing of data expression and exchange standards in the technical information security field. The standards and data formats identified are in Table 3.

Table 3 – List of standards and data formats identified by Dörges [32]. Table in Appendix I lists pointers for more information.

Document Name	Short name	Year
Common Attack Pattern Enumeration and Classification	CAPEC	2008
Common Configuration Enumeration	CCE	2009
Common Information Model	CIM	2009
Common Model of System Information	CMSI	2005
Common Platform Enumeration	CPE	2009
Common Result Format	CRF	2007
Default Password Enumeration	DPE	2008
Open Vulnerability & Assessment Language	OVAL	2008
Extensible Configuration Checklist Description Format	XCCDF	2008
Common Vulnerabilities and Exposures	CVE	2009
Common Vulnerability Scoring System	CVSS	2007
Vulnerability and Exploit Description and Exchange Format	VEDEF	2005
Vulnerability and Exposure Markup Language	VuXML	2005
OASIS Application Vulnerability Description Language TC	AVDL	2004

Document Name	Short name	Year
Common Announcement Interchange Format	CAIF	2005
Deutsches Advisory Format	DAF	2004
European Information Security Promotion Programme (EISPP) advisory format		2004
Common Weakness Enumeration	CWE	2009
Common Malware Enumeration	CME	2005
Malware Attribute Enumeration and Characterization	MAEC	
Intrusion Detection Msg. Exchange Format	IDMEF	2007
Intrusion Detection Exchange Protocol	IDXP	2007
Incident Object Description Exchange Format [31]	IODEF	2007
Abuse Reporting Format [92]	ARF	2009
Common Event Expression	CEE	2008
Security Content Automation Protocol	SCAP	2009

To summarise this breathtaking list of standards and data format definitions, Dörges presents the following conclusion:

> *"Investigated > 30 standards*
>
> - *13 languages*
> - *8 enumerations*
> - *5 other*
>
> *9 unused (dead or never alive)*
>
> *6 unclear*
>
> *17 actively used or developed."* [32]

According to Dörges, the entries listed in Table 3 above can be categorised as follows: advisory formats (3 entries), asset descriptors (9), incident handling (2), intrusion detection (2), malware (2), threat assessment (1) and vulnerability characterisation (5). Two standards were left without being assigned a category.

According to Dörges' assessment, the key standards in Table 3 associated with incident handling would be IODEF, ARF, and – to a certain extent – CEE. The widespread adoption of the two latter initiatives remains to be seen.

3.4 Report validity

In the light of previous sections, it would seem obvious that an organisation should develop a rather agnostic approach to choosing the sources from which it accepts incident reports. One never knows in advance, which party may be in the possession of information of relevance to the organisation. Merely having an "open door policy" to reporting incidents is not sufficient, however.

There must be a means to validate the report. If this is not possible, there must be a way to authenticate the reporter. In addition, the reporter needs to be able to validate that the information has been sent to the correct place.

3.4.1 Validating the report

In order to validate the accuracy of the report, the recipient should be provided either with enough information to reconstruct the incident or pointers to additional information obtainable by the recipient.

IODEF provides a method of submitting incident descriptions, impact assessments and even event logs. These are optional, however.

> *"The EventData class can be thought of as a container for the properties of an event in an incident. These properties include: the hosts involved, impact of the incident activity on the hosts, forensic logs, etc."* [31]

With regard to representing dates and timestamps, IODEF refers to RFC 3339 [62], which is an internet adaptation of ISO 8601.

Anti-virus vendors have agreed on an industry-wide convention that malware samples should be packaged inside a password-protected zip archive and use the word "infected" as password.[15] Due to CSIRTs having close relationship with anti-virus research community, they have too adopted the convention.

However, sometimes it is not possible to provide proof along with the report. For instance, when reporting about stolen passwords or other personal information, it is customary to leave out the actual passwords and other personally identifiable information and merely describe what kind of information was stolen. Incidents involving large amounts of data in the form of e.g. log files or large artefacts pose a challenge, too. The recipients are usually spared such details in an effort to prevent the reports from filling up their mailboxes.

If incident details are left out, that leaves the receiving party with a dilemma. The options are to trust the reporter and risk falling into hoax or to simply discard the report unless additional proof is presented. The decision is made easier if the reporter has previously proven to be trustworthy. In that case, the recipient may decide to extend the trust to this new piece of information. This kind of trust is easy to exploit for nefarious purposes, however, if the report's contents cannot be verifiably linked to the trusted reporter.

3.4.2 Authenticating the reporter

One method of establishing the report's authenticity would be digitally signing the message with a method that lets the recipient validate that the report actually came from a known – possibly trusted – party. RFC 2350 [10] suggests that each incident response operator employ at least encryption tool called PGP, which supports public-key encryption and message authentication. Most CERTs follow this advice rather well. For instance, FIRST requires that a team aspiring to become a member to support the use of PGP:

> *"To be a member in FIRST, a CSIRT must maintain and use PGP encryption. Encryption keys must be distributed to all parties that will use it."* [89]

---

[15] E.g. https://analysis.f-secure.com/portal/infoPage.html, http://vil.nai.com/vil/submit-sample.aspx, http://social.answers.microsoft.com/Forums/en-US/msescan/thread/08ec359b-0519-4850-8373-561445a05f99

The Trusted Introducer program[16] refrains from requiring the use of PGP but rather finds that the tool has been recognised as a *de-facto* standard:

> *"For all practical considerations PGP/GPG is the established standard for providing confidential and authentic communication within the CSIRT community."* [90]

The EGC[17] and APCERT[18] follow similar conduct in recommending the use of PGP in both encrypting sensitive e-mail communication and signing content.

Other authentication methods could include alternative messaging encryption techniques (for instance, S/MIME), extranet websites attributable to the reporter, and out-of-band communications channels.

Government-attributed organisations traditionally have specific requirements for the handling of classified information and information exchange. They are, however, out of the scope of this study.

3.4.3 Following up the reports

After the report has been submitted, the reporter has three possible approaches to choose from to track the progress of the incident resolution. The reporter choosing the *opportunistic approach* would regard the case resolved and move on to conduct other business as soon as the report has been sent. Adopting the *iterative approach* would require the reporter to prepare itself for an ensuing dialogue with the recipient. In the iterative approach, the initial contact only serves as a trigger after which additional material can be requested and exchanged. Finally, the reporter can choose the *active approach.* An active reporter continues monitoring the situation and holds the case open until the problem has verifiably been resolved.

Popular incident handling systems such as OTRS[19], RTIR[20] and RT[21] issue unique identifiers to incident-related e-mail correspondence. If an external partner later decides to request or submit additional incident-related information, he can refer to the previously created trouble ticket simply by mentioning the identifier. IODEF supports using such identifiers and acknowledges that there needs to be a link between the identifiers assigned by each corresponding party.

> *"The AlternativeID class lists the incident tracking numbers used by CSIRTs, other than the one generating the document, to refer to the identical activity described the IODEF document. A tracking number listed as an AlternativeID references the same incident detected by another CSIRT."* [31]

Opportunistic reporters submit the material in blind and generally expect neither acknowledgements nor additional information in return. An opportunistic report can be submitted via e-mail without ever expecting a response. The report may also be surren-

---

[16] http://www.trusted-introducer.org/
[17] http://www.egc-group.org/contact.html
[18] http://www.apcert.org/application/docs/Application_GM.doc
[19] http://otrs.org
[20] http://www.bestpractical.com/rtir/
[21] http://www.bestpractical.com/rt/

dered to a third party for post-processing or can be posted on a web page in the hope of someone else taking concrete action.

Iterative reporters accept the fact that some of the recipients are interested in learning additional details while some may never return a call. During the dialogue, the iterative reporters have a chance to acquire information in return, thus helping the reporter build better picture of the incident they helped uncover. Dialogue is also a convenient way to avoid sending excessive amounts of data blindly to potentially uninterested or wrong recipients.

Active reporters assume ownership of the incident for as long as they can find responsible handlers to take over. Active reporters want to be able to verify themselves that the incident has been resolved instead of blindly trusting the recipients of their reports. They may follow the progress of incident response by e.g. monitoring reported phishing sites until the offending content has been removed. Should the case exhibit signs of stalling, an active reporter can take corrective measures to escalate it or otherwise circumvent obstacles.

3.5 Work in progress

At the time of writing this study report, progress is being made on several fronts. A common feature to all of these initiatives is that existing data expression and exchange formats are being reused and put into new service. The outcomes of these initiatives will be varied, ranging from normative and all-encompassing frameworks to concrete software-based products.

3.5.1 CYBEX framework of ITU-T

The first initiative is a standardisation effort of the United Nation's telecommunication standardisation organisation ITU-T. A working group is currently drafting a set of standards and recommendations under the title "*Cybersecurity information exchange framework,*" or CYBEX for short. According to the draft documents, the framework aims to, among other things, devise a standard for identifying public points of contacts for reporting information security incidents for various internet resources, and promote the use of standardised data formats for expressing the incident details. [85],[81]

Based on the initial documents seen by the author of this study, CYBEX aims to bring together a number of existing data formatting and exchange standards ranging from those used to describe and exchange information regarding software vulnerabilities, NIS events and incidents, forensic evidence, organisational identities and information requests.

Figure 4 below, taken from the CYBEX documentation, makes an effort to describe the dependencies and relationships between different entities that the document refers to as "structured information exchange capabilities." Except for CWSS, the entities in the picture have already been listed in Table 3 earlier. The exact purpose of the dotted line in the picture is not clear from the CYBEX documentation. According to the documentation, IODEF, CEE, and CAPEC are included *"for the purpose of exchanging event, incident or heuristic information."* [85]

The incident transcriptions in the Chapter 4 of this study have been submitted as background material for the ad-hoc working group within FIRST lead by Damir Rajnovic. The outcome of the CYBEX framework and its eventual acceptance in practical settings remains to be seen.

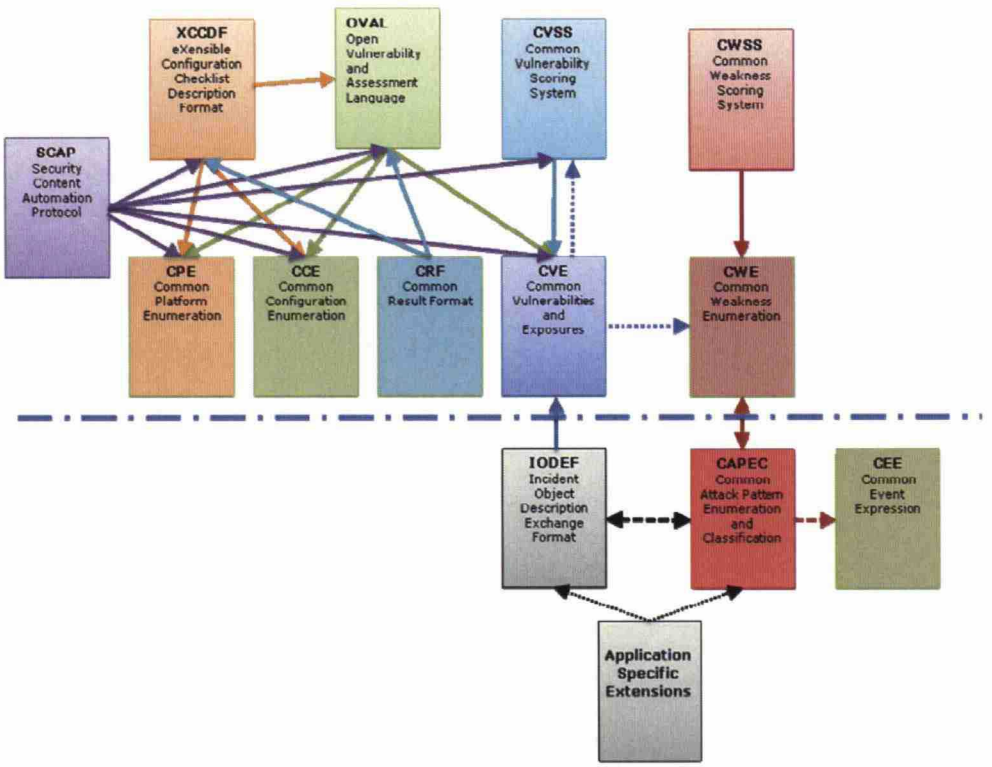

Figure 4 – Relationships and dependencies among structured information exchange capabilities as identified by the CYBEX draft document. Picture taken from ITU-T Study Group 17 report TD 0503 Rev.1. [85]

3.5.2 Abuse Helper

Another development is an open source software project entitled Abuse Helper. [1] This project, lead by CERT Estonia, aims to build a tool for national CERTs and network owners to effectively exchange and process NIS incident reports represented in standardised format. The tool is inspired by service of CERT-FI called Autoreporter, [46],[47] which was introduced into operational use in late 2005.

Once completed, the tool is supposed to help in retrieving incident-related information from a diverse set of reporting sources. According to the project's wiki pages:

> *"With Abuse Helper you can:*
>
> - *Retrieve Internet Abuse Handling related information via several sources which are*
>   - *near-real-time (such as IRC)*
>   - *periodic (such as Email reports), or*
>   - *request/response (such as HTTP)."* [1]

Once collected, the information can be regrouped in various ways to accommodate the statistical analysis and further dissemination of takedown requests. Finally, the reports can be sent out using the format, transport and schedule most convenient for the recipient.

Abuse Helper employs several incident description formats, including the *Incident Object Description and Exchange Format.* [31],[3] IODEF was listed in Table 3 on page 18.

3.5.3 Two new internet-drafts in RFC series

The third area of progress is the RFC series within Internet Engineering Task Force. At the time of writing this report, two RFCs are being drafted for the consideration of IETF. Table 4 shows summarised information about these two documents. According to the RFC process described in Section 2.2 of RFC 2026 [7] the drafts will expire in six months unless a new version is submitted or the paper is accepted for a standardisation path.

Table 4 – List of active internet-drafts with relevance to the study topic.

Document name and relevant sections	Internet-Draft id	Intended RFC status	Commenting period	version
Recommendations for the Remediation of Bots in ISP Networks	draft-oreirdan-mody-bot-remediation [66]	Informational	2010-02-12 – 2010-08-16	07
An Extensible Format for Email Feedback Reports	draft-ietf-marf-base [92]	Internet-draft	2010-04-30 – 2010-11-01	04

An internet-draft with the title "*Recommendations for the Remediation of Bots in ISP Networks*" has already undergone seven revisions, the latest being from February 2010. [66] The document was originally submitted in July 2009 by Comcast, which is a large US based telecommunications company. The document promises to provide:

> *"[..] recommendations on how Internet Service Providers can manage the effects of computers used by their subscribers, which have been infected with malicious bots, via various remediation techniques."*

Another internet-draft with the title *"An Extensible Format for Email Feedback Reports"* is currently in its second revision. [92] The initial version of this document was submitted in January 2010 by an IETF working group called the "*MARF Working Group.*" [22] MARF is shorthand for *Messaging Abuse Reporting Format.* The reader is reminded that Abuse Reporting Format (ARF) has been identified earlier in Table 3. According to the document abstract:

> *"This document defines an extensible format and MIME type that may be used by network operators to report feedback about received email to other parties. This format is intended as a machine-readable replacement for various existing report formats currently used in Internet email."*

[22] http://datatracker.ietf.org/wg/marf/charter/

3.5.4 Palantir framework for collaborative incident response

An interesting related paper by Khurana et al. describes a tool called "*Palantir*" that aims to provide a collaborative environment for inter-organisational incident response and investigations. According to the 2009 paper, they claim the system to be the first of its kind.

An important thing to notice in relation to this study is that *Palantir* assumes the existence of a central trusted entity in possession of the framework system.

> *"While the proposed response and investigation system is distributed in nature, it is centrally managed by a trusted entity, which we call an Independent Center for Incident Management (ICIM)."* [58]

In contrast to this requirement, our study is built on the notion of independent and autonomous incident response teams seeking to share incident-related information efficiently on a global scale. Due to political and business reasons, introduction of a single trusted entity would be impossible. However, the *Palantir* framework may be useful when used in settings where the subjects either trust each other or reach an agreement on which entity should be the trusted third party.

3.6 Other related work

Possibly of relevance for the purpose of this study is the earlier work by CERT/CC and Japanese national CERT on automating the handling of software vulnerabilities. The *Vulnerability Response Decision Assistance* (VRDA) concept focuses not only on the exchange of the vulnerability descriptions, but also aims to bring automation to the decision-making related to vulnerability response. [14]

4 The Practice: Examples of Real-Life Incidents

In the previous section we familiarised ourselves with the existing normative efforts aimed at helping solve network and information security incidents in the public communications networks. In this section we are introduced to a collection of incident transcripts taken from the CERT-FI archives in the hope of exposing ourselves to the real-life challenges that may hinder the effectiveness of the incident handling and coordination efforts.

The case descriptions are – when necessary – anonymised to protect the identities of the affected parties. This holds especially true for private persons. Company names and network addresses related to incidents are only removed if they are not easily obtainable from public sources. Citations and code examples may be truncated for brevity. Each case is explained and a set of attributes to identify the actors and shared information is presented.

The reader should be advised that "incident ticket" identifiers written in brackets, for example, *[FICORA #309474]* or *[CERT-FI: 36789]*, are referring to notes archived in the CERT-FI incident handling system. Tickets numbered using five digits indicate incidents from a period between 2004 and 2007. Six-digit entries are more recent. Other identification tags used by other handlers are indicated within the text where applicable.

4.1 Compromised web servers

Web servers are a sought-after target for network attackers for a number of reasons. Their weaknesses are easy to examine since they are always online and are generally accessible from the whole world. Popular web servers typically have high-bandwidth network links, which makes them ideal for spreading malware to a large number of victims, sending loads of spam e-mails, or launching devastating denial-of-service attacks. They also have a static IP addresses, which makes them rather stable platforms for sustained presence in the network.

The contents of web sites are seldom integrity-checked by their legitimate owners. The traffic patterns are barely ever monitored using anomaly detection. Lack of supervision by the rightful owners helps the attacker stay undetected for long periods of time. Basically anybody can set up a web server. No technical qualification is required, and as web hosting is cheap, servers can be set up by those with less than solid financial standing. Many web servers are introduced online without applying even basic protections, are administered with minimal effort, are being run on substandard software foundation, and may eventually be abandoned while still online. The web server's true owner or technical administrator can be next to impossible to identify by an outsider let alone to reach in due time for reporting about the ongoing misuse. This makes such servers ideal platforms for the attacker to run sustained malicious operations such as collection of personal information via phishing sites or advertising of illegal goods or services.

4.1.1 Finnish web server hosting a phishing site: resolved, apparently

In our first case, a web server in Finland has been broken into and a lookalike page portraying to be the bank *Wachovia* has been inserted onto the server. The compromised

server belongs to a small Finnish non-profit organisation. The fake bank site was then used to pilfer personal information from the bank's customers. The case has identification *[FICORA #309474]* [121] in the CERT-FI incident handling system. Over a hundred similar cases were registered with CERT-FI in 2009.

The information flow related to the case is depicted in Figure 5. The information flow has been reconstructed using the parts of the correspondence seen by CERT-FI. In the following passage, we walk through the picture from top to bottom using the message log and other evidence archived in *[FICORA #309474]* [120] as our guide.

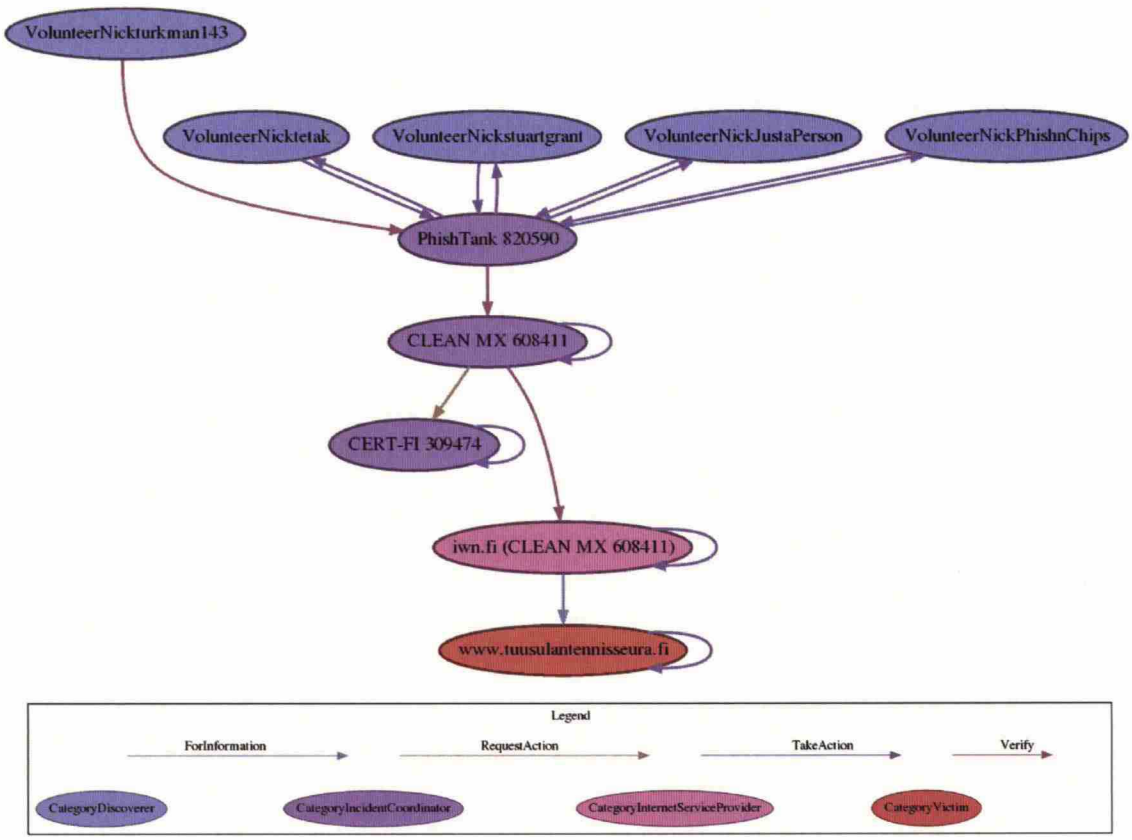

Figure 5 – A GraphingWiki representation of actions taken by various bodies in discovering and helping to remove a phishing site on a Finnish web server.

While not evident from the material collected by CERT-FI, the unsuspecting *Wachovia* customers most probably were approached by more or less convincing-looking spam e-mails claiming to be coming from the bank and urging the recipients to visit the fraudulent site. As seen in Figure 6 below, the visitors were encouraged to type in their personal information.

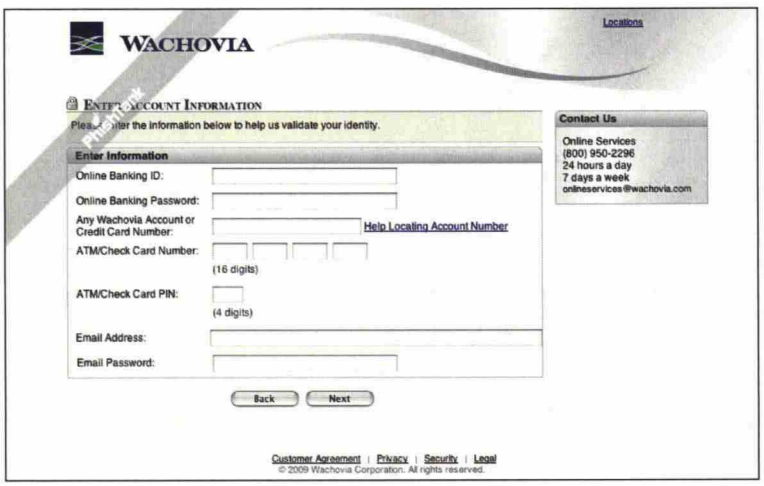

Figure 6 – Screenshot of a phishing site discovered on a Finnish web server. The phishing operation in question was targeting Wachovia customers. Picture courtesy of OpenDNS, LLC, the operator of "PhishThank.com" service. [74]

4.1.1.1 Initial discovery

The phish site was originally discovered by a contributor to a service called *PhishTank*. The contributor is identified by his nickname "*turkman143*." According to the PhishTank web site[23], they are a clearing-house for volunteers to report phishing sites into a public database. The service is operated by *OpenDNS*, which is a Californian company specialised in internet infrastructure and security services.

New reports arriving to PhishTank are subjected to a peer review in an apparent effort to minimise the number of false positives and to make it harder to abuse the reporting system with unsubstantiated and outright falsified claims. This particular report with id 820590 was deemed valid by four other people. [74] The CERT-FI archives contain no indication of other discoveries except the report by PhishTank concerning this particular phishing site.

4.1.1.2 Evidence collection

Following the information flow graph in Figure 5, it appears that PhishTank is the first operative that systematically collects evidence about the incident. A set of basic information about each case is made publicly available. As can be seen in Figure 7, the following information is displayed:

- *ID*: A unique reference number is being issued to distinguish the case from other reports in the database. In this case, the id is *820590*.
- *Timestamp*: The exact submission date and time as observed by PhishTank is recorded. The timestamp is "*Sep 19th 2009 4:41 PM*," time zone apparently being UTC.

[23] http://www.phishtank.com/

- *URL*: This is the original URL (including the host name) where the phishing site was observed. In the context of this case, the URL is *"http://www.tuusulantennisseura.fi/assets/export/lbg.php,"* which would indicate a system with ties to Finland (this is indeed the case, as the web site belongs to a tennis club in Southern Finland).
- *Network information*: WHOIS output of the domain name is displayed. IP netblock and the AS number and name associated with the web server is recorded. In particular, the network block is identified as *"212.94.64.0/19 (AS5515 TS-FINLAND-DATANET-OLD TS Finland DataNet)."*
- *Reporters:* Identities (nicknames, not real names) of the discoverer and verifiers are displayed. In addition to recognising "turkman143" as the discoverer, four verifiers *"stuartgrant,"* *"tetak,"* *"PhishnChips"* and *"JustaPerson"* are also mentioned as contributors.
- *Confidence:* Subjective estimate of the observed site's "phishiness" is provided. In this particular case, there is 100 % confidence as five out of five volunteers agreed with the claim. To back up the claim, a screenshot of the phishing site found on the compromised server is archived.
- *Takedown status:* Lastly, the report indicates whether the site has been taken offline or not. [74]

Apart from collecting and making the information available, PhishTank refrains from processing the incident further. Luckily, the story does not end here, though.

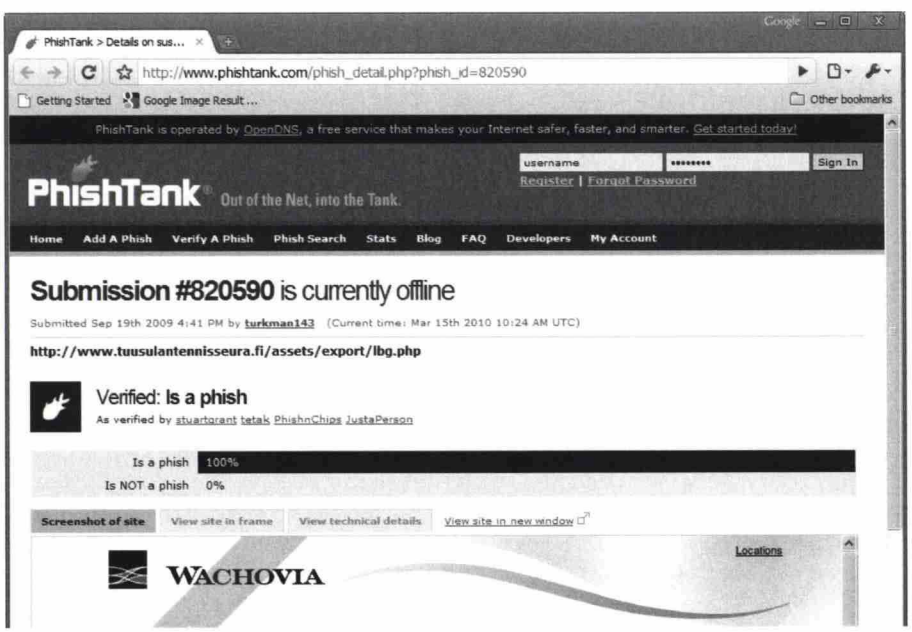

Figure 7 – Screenshot of PhishTank report with the submission id 820590.

The next handler in line is the German company *NETpilot GmbH*, which runs a service called *CLEAN MX*[24]. CLEAN MX uses a public API[25] through which it queries for new submissions from the PhishTank database. After downloading the information, CLEAN MX issued the report with an id of 608411 and performed a series of tests to determine its accuracy. The data is enriched with DNS and WHOIS queries to determine where the server is and who is responsible for it. The status of the server and the offending content found is being monitored by periodic download tests.

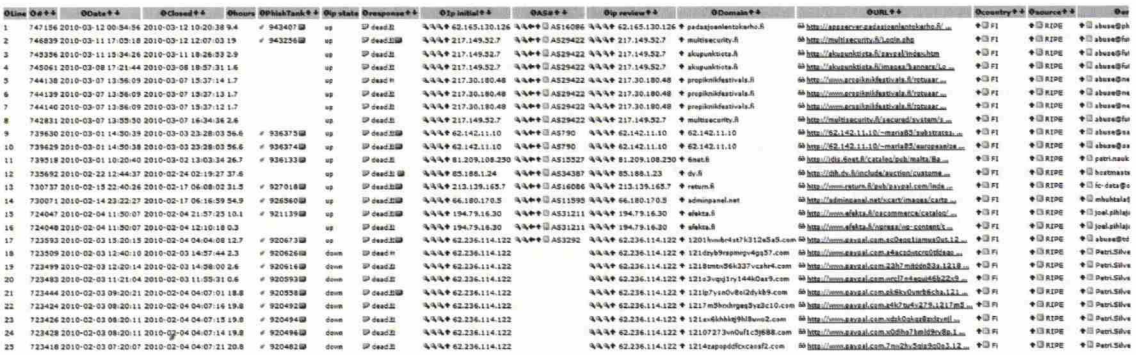

Figure 8 – Partial view of a country report for Finland listing phishing sites as tracked by CLEAN MX.[26] The screenshot represents the situation on 13 March 2010.

For each report, the following information is made publicly available by CLEAN MX:

- *ID*: A reference to the PhishTank report is provided (here: #608411), thus creating a link between the two id numbers.
- *Timestamp*: Date and timestamps indicating the moment the incident was added to the CLEAN MX database (2009-09-19 18:41:37) and the moment the phishing site was taken offline (2009-09-20 21:04:12). Additionally, a delta value indicating the site's persistence was calculated (26.4 hours).
- *Online status*: Results of various connectivity tests used to determine whether the server and the phishing site were still online are displayed. The server's HTTP response is logged and displayed as seen in Figure 9. In this instance, the takedown was verified on the evening of 20 September 2009.
- *Network information*: DNS name resolution was performed and the IP address associated with the hostname is shown. A collection of links to other public services offering more information about the address is provided: Cisco System's IronPort SenderBase[27] report [25], BFK's Passive DNS replication[28] lookup [6], and RIPE database[29] search results [84]. A link to examine other entries for the same IP address in the CLEAN MX database is also provided, as is the associated Autonomous System along with historical data related to the AS number. Links to external databases include International Se-

[24] http://www.clean-mx.de/
[25] http://www.phishtank.com/developer_info.php
[26] http://support.clean-mx.de/clean-mx/phishing.php?country=FI&response=
[27] http://www.senderbase.org/about
[28] http://www.bfk.de/bfk_dnslogger_en.html
[29] http://www.db.ripe.net/whois

cure Systems Lab's FIRE database (Finding rogue networks) [52] and the Google SafeBrowsing [79] diagnostics page. A top-level internet domain (TLD) associated with the hostname and a link to past incidents associated with the domain are shown. The domain name servers are identified from DNS Start of Authority (SOA) records. In addition, the IP netblock object (inetnum) and owner of the network are obtained from WHOIS and presented. The country code and regional IP registrar (RIR) associated with the IP address are identified and links to past incidents are displayed. For instance, historical incidents with relation to Finnish networks can be found using a suitable query [73] as seen in Figure 8 on page 30.

- An educated guess about the abuse handling contact closest to the observed server is made. Historical incidents belonging to this contact are displayed.
- The service incorporates a special "safe viewer" as a way for the observer to view the web server contents without actually having to visit the site using one's own web browser. [73]

Admittedly, this is a rather complete dossier of evidence. It contains enough information to determine whether the suspected phishing site actually exists and who would be responsible for the server that is hosting the harmful content. Interestingly, though, not even CLEAN MX retains a forensic copy of the offending content found on the server.

```
DEBUG output created by Wget 1.10.2 on linux-gnu.

--21:04:12--  http://www.tuusulantennisseura.fi/assets/export/lbg.php
          => 'output.608411.html'
Auflösen des Hostnamen »www.tuusulantennisseura.fi«.... 212.94.64.154
Caching www.tuusulantennisseura.fi => 212.94.64.154
Verbindungsaufbau zu www.tuusulantennisseura.fi|212.94.64.154|:80... verbunden.
Created socket 9.
Releasing 0x080997a8 (new refcount 1).

---request begin---
GET /assets/export/lbg.php HTTP/1.0
Pragma: no-cache
User-Agent: Mozilla/5.0 (compatible; en-US)
Accept: */*
Host: www.tuusulantennisseura.fi
Connection: Keep-Alive

---request end---
HTTP Anforderung gesendet, warte auf Antwort...
---response begin---
HTTP/1.1 403 Forbidden
Date: Sun, 20 Sep 2009 19:04:13 GMT
Server: Apache/1.3.41 (Unix) mod_ssl/2.8.31 OpenSSL/0.9.8k
Connection: close
Content-Type: text/html; charset=iso-8859-1

---response end---
```

Figure 9 – Output of *wget* tool indicating that the phishing site was taken offline. The return code 403 in the HTTP response part is a sign of access to the the material having been blocked by applying restrictions to the folder permissions on the server.

A couple of words on the timestamps is in place. On the CLEAN MX web page (see Figure 8), the date is expressed without the time zone information. For instance, the announced date of discovery is "*2009-09-19 18:41:37*." Other circumstancial evidence suggests that the times are expressed using the German time zone, which has the offset

UTC+1. This is not correct, though. Upon examining the calendar, one would discover that in September 2009 Germany was observing the daylight saving time. The Central European summer time – the CEST – has the offset UTC+2. Timestamp offsets can potentially be a source of great confusion. It has become customary in the global incident response to either specifically state the time zone offset or express the times in UTC. The discovery date should then be expressed either as "*2009-09-19 18:41:37 UTC+2*" or "*2009-09-19 16:41:37*." [61]

Adding to the cacophony is the *wget* output displayed in Figure 9. The reader should be advised that the expression "*Date: Sun, 20 Sep 2009 19:04:13 GMT*" in the output is announced by the remote server and cannot be fully trusted. It is often the case with unattended and poorly maintained servers that their local system time is wrong. The other timestamp ("*--21:04:12--*") is produced by *CLEAN MX*. We must assume it is trustworthy. Once again, though, one has to guess the timezone. Comparing the timestamps, both appear to indicate the same time, only in different formats.

4.1.1.3 Incident coordination

In addition to merely collecting information, CLEAN MX makes a genuine effort to notify the responsible owners of the compromised systems. As mentioned earlier, identifying the owner is easier said than done, at least when using automated means. As usual with cases of a similar nature, the owner of the compromised server is among the last ones to learn about the issue.

Instead of directly contacting the server owner, CLEAN MX proceeded to notify both the ISP (in this case a company in Kuopio, Finland) and CERT-FI about the phishing site and a potential computer break-in. [73] The report is sent via e-mail (see Figure 10 below) but all information can be found on CLEAN MX web pages.

```
+-------------------------------------------------------------------------
|date                      |id     |ip            |Url
+-------------------------------------------------------------------------
|2009-09-19 18:41:37 CEST |608411 |212.94.64.154 |http://www.tuusulantennisseura.fi/asse
ts/export/lbg.php
+-------------------------------------------------------------------------
```

Figure 10 – CLEAN MX's simple report about a phishing site on Finnish web server.

CLEAN MX's report [73] comes in three different formats: simple human-readable e-mail message, a web page with clickable links that the reader can "drill into" for additional information and a structured XML document.

The e-mail report contains bare necessities such as timestamp of the discovery, IP address of the server hosting the reported phishing content and full URL for the offending site. The report also includes some URLs to sites with more information about the incident.

The information on the web page has already been covered thoroughly in Section 4.1.1.2 and an example can be seen in Figure 8.

The essential parts of the same report in XML format are shown in Figure 11 below.

```
<?xml version="1.0" encoding="iso-8859-15"?>
<output>
 [..]
<entries>
<entry>
  <line>1</line>
  <id>608411</id>
  <first>1253378497</first>
  <last>1253473452</last>
  <phishtank>820590</phishtank>
  <url><![CDATA[http://www.tuusulantennisseura.fi/assets/export/lbg.php]]></url>
  <recent>up</recent>
  <response>dead</response>
  <ip>212.94.64.154</ip>
  <review>212.94.64.154</review>
  <domain>tuusulantennisseura.fi</domain>
  <country>FI</country>
  <source>RIPE</source>
  <email>abuse@iwn.fi</email>
  <inetnum>212.94.64.0 - 212.94.68.255</inetnum>
  <netname>IWN-LAN1</netname>
  <descr><![CDATA[Oy IW-Net Ltd - Image WorldNiiralankatu 1670600 Kuopio]]></descr>
  <ns1>ns.iwn.fi</ns1>
  <ns2>ns2.iwn.fi</ns2>
  <ns3>ns3.iwn.fi</ns3>
  <ns4></ns4>
  <ns5></ns5>
</entry>
</entries>
</output>
```

Figure 11 – XML output of CLEAN MXs report. A simple human-readable version of the same incident report is seen in Figure 10 above.

As the volume of reports from CLEAN MX can be characterised to be moderate, the CERT-FI handlers have so far been content with the e-mail format. 311 reports from CLEAN MX were received in 2009, 81 of them related to phishing. In case additional information not evident in the e-mail report is needed, CERT-FI may visit the web page using the link provided in the e-mail report. CERT-FI currently has no system in place to automatically parse reports in XML format.

Upon receiving the report, CERT-FI was satisfied to see that the hosting provider closest to the web site owner had already been informed. Apart from verifying that the phishing site was actually taken offline, CERT-FI did nothing.

4.1.1.4 Incident Resolution

The phishing site was removed shortly after the initial notification from CLEAN MX. It is assumed that the ISP corrected the problem on behalf of the customer, as it seems the web site was hosted on the ISP's shared web platform. This is speculation, however, as no further evidence apart from the *wget* output (see Figure 9 on page 31) is available to determine how the site was taken offline. No communication between CERT-FI and the parties hosting the web server ever took place.

It is possible be that the internet service provider contacted the web server owner using contact information found in the customer database and the server owner then corrected the problem. It is also possible that the server owner found out about the compromise from other sources or independently.

4.1.1.5 Unresolved issues

Based on the material presented above it seems evident that the web server indeed was compromised and unauthorized content in the form of a phishing page was uploaded onto the server. Remembering that phishing sites are being used to conduct further attacks against the banks and their customers, we can conclude that this case easily fulfils the criteria for an attack and information security incident as presented on page 4. While we admittedly learnt a staggering number of technical facts about the compromise during the incident response, we are still left with three unanswered questions.

To start with, the timestamp of the original break-in and attack vectors employed are not known. Arguably, these would be crucial pieces of information if we were to conduct further forensic analysis to learn about the root cause that made the break-in possible in the first place. Without knowing how the break-in was technically possible, the task of warning and advising other server owners becomes difficult or even impossible. Disseminating ambiguous advisories would yield few good results.

Second, we have no knowledge whatsoever of those unsuspecting Wachovia customers who may have fallen victims to the fraud and as a consequence have submitted their personal information to the hands of the criminals. Furthermore, there is no information indicating where the phished information might have been sent. During the course of the incident handling, no effort was made to warn either the customers or the bank. Based on previous incidents of the same sort, the observed modus operandi is to use the phishing site merely as a front and immediately forward the collected material to a collection site somewhere else – usually in some other country with a completely different time zone. While the bank and its customers probably benefitted to some extent from having this particular phishing site taken offline, it can be argued that the incident response process almost completely missed the mark of uncovering the phishing operation. It appears there is no linkage between the original phishing e-mails, their timestamps, where they came from and who authored them. Most probably, other servers have been broken into as well and turned into phishing platforms. There is, however, not enough information to correlate these break-ins with the one examined here. In fact, there is nothing to indicate that other break-ins even took place.

Lastly, the exact time of the takedown is not known. Combined with the time of the incident initiation, this would be valuable information for process development purposes. For instance, Moore and Clayton [69] have examined the lifetimes (i.e. time between from the initial break-in to the site being taken offline) of phishing sites in various parts of the world. Based on the observations they have made conclusions about the effects of incentives on the effectiveness of incident response in the context of notice and takedown procedure. This particular incident would not necessarily qualify for such statistical analysis as the site lifetime is not exactly known. Collecting such information would require combining incident-related information from several sources.

As we already discovered, a service called PhishTank played an important role in the incident discovery. Starting on page 28, we sketched a list of the information PhishTank makes available for the incident response coordination. That includes a URL, timestamp, netblock domain name and screenshot of the phishing site. Although admittedly useful material, a couple of noteworthy omissions stand out still.

Perhaps the most important information missing from material shared by PhishTank is the actual IP address resolved by querying the hostname from the DNS server at the time of initial discovery. While it is important to know the hostname, almost equally important are the IP addresses to which it was resolving in the DNS during the time of discovery. That is because information found in the DNS should be considered volatile and containing no historical data. [19] That means that forward-lookup records in the DNS can chance at any time, thus possibly leading the incident coordinators to direct their investigations into different – quite possibly wrong – systems. However, in this instance, the hostname resolved to a single and relatively static IP address, thus eliminating the possibility for ambiguity. Furthermore – again, applicable to this case only – the criminals behind the phishing operation had no control over the DNS records related to this domain and hostname.

Accurate and non-ambiguous IP address information is particularly important when investigating incidents where a technique called fast-flux is being employed. Fast-fluxed hostnames resolve to a number of IP addresses in a round-robin manner and the list of IP addresses is rapidly changing in a shameless effort to shake off potential investigators.

The second piece of information missing from the material available from PhishTank is the actual contents of the phishing site. A copy of the HTML source code and binary content may have forensic value and may help determine how the illegally inserted contents evolve over time. It is also a common practice for the criminals to manipulate the compromised server in a way that different contents are displayed based on who is viewing the page. For instance, the phishing site might be shown only to visitors coming from certain countries or using specific language locale on their web browsers. Specifics such as this may not be obvious by merely looking at a bitmap picture as provided by PhishTank. As was seen from page 30 onwards, information collected by CLEAN MX effectively removed all ambiguity left by the PhishTank report.

4.1.1.6 Summary of information collected and actions taken

In Table 5 below, the cells marked in white indicate that information is not collected or recorded. Red cells with a question mark indicate the answer is not known. Cells in amber contain speculative information by the author. Green cells indicate that the author has been able to verify the material either from the CERT-FI archives or from other sources.

Table 5 – Summary of information collected during the incident *[FICORA #309474]*.

	Incident Repository	Incident Repository	National CERT	ISP	Victim	Victim
	PhishTank	CLEAN MX	CERT-FI	IWN	www.tuusulan tennisseura.fi	Wachovia Bank
Report received from	individual	PhishTank	CLEAN MX	CLEAN MX	IWN	?
Incident ID	#820590	#608411	[FICORA #309474]	?	?	?
Associated IDs	-	PhishTank #820590	CLEAN MX #608411, PhishTank #820590	CLEAN MX #608411, PhishTank #820590	?	?
Next-in-line incident handling contacts	-	ISP's abuse team, national CERT	ISP's abuse team	customer (web server owner)	?	?
Recorded incident status	resolved, site taken offline	resolved, site taken offline	resolved, site taken offline	?	?	?
Date discovered (in UTC)	2009-09-19 16:41	2009-09-19 16:41	2009-09-20 07:59	2009-09-20 07:59	?	?
Resolved (in UTC)	-	2009-09-20 19:04	between 2009-09-21 and 2009-09-23	?	?	?
Persistence	-	26.4 h (> 1 day)	-	?	?	?
Network info resolved	URL	URL, hostname, domain whois, IP address (PTR), IP netblock, ASN, IP whois, AS name, peer ASNs, country code, RIR	as indicated in the report received	as indicated in the report received	?	?
Evidence inherited from	reports from volunteers	PhishTank	CLEAN MX and PhishTank	CLEAN MX and PhishTank	?	?
Evidence secured	discoverer identity, screenshot	wget connection log, links to other public reports by 3rd parties	quick connectivity test	?	?	?
Actions taken	receive, verify, share, archive	receive, verify, analyse, share, request assistance, archive	receive, verify, archive	receive, verify, issue take-down?	?	?

Once a web server has successfully been compromised, the attacker can turn it into a malware distribution point with the same ease as into a phishing site. The next two incident transcriptions describe such cases and only highlight parts where the process differs from the incident just described.

4.1.2 Finnish web server hosting malware: escalation needed

This incident has been issued with an id *[FICORA #308909]* [120]. Figure 12 summarises the information flow. Compared to Figure 5 on page 27, this time the role of CERT-FI is visibly pronounced.

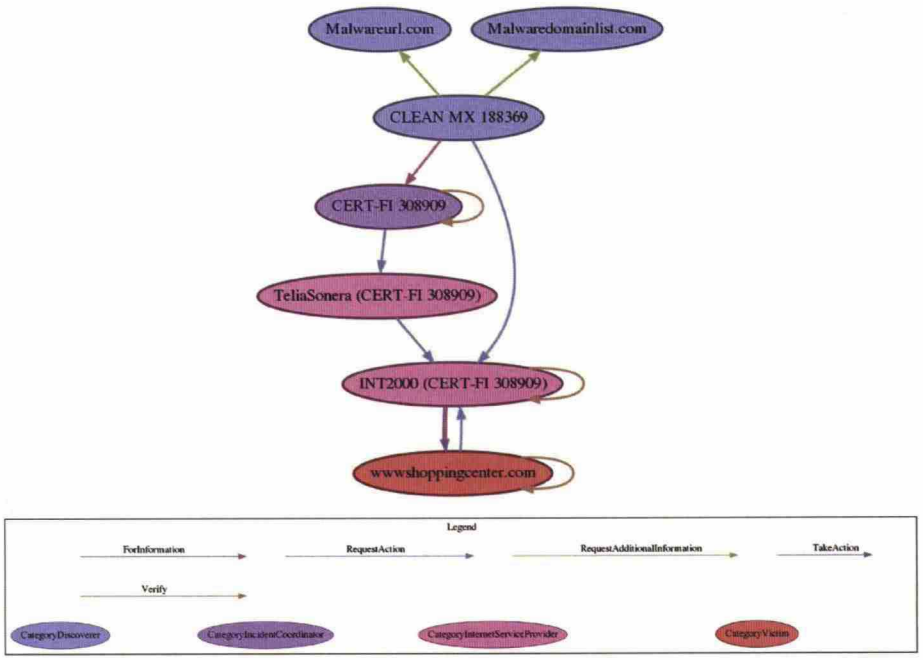

Figure 12 – Information flow related to incident *[FICORA #308909]*.

4.1.2.1 Initial discovery

CERT-FI learnt about the incident from a CLEAN MX report similar to the one discussed in the previous section.

```
+-------------------------------------------------------------------------------------------
|date |id |virusname |ip |domain |Url|
+-------------------------------------------------------------------------------------------
|2009-09-13 20:14:42 CEST |188369 |HTML/Crypted.Gen |212.182.218.2 |wwwshoppingcenter.co
m |http://wwwshoppingcenter.com/
+-------------------------------------------------------------------------------------------
```

Figure 13 – CLEAN MX report about malware on a Finnish web server. Some overly long lines in the report have been truncated for clarity.

4.1.2.2 Evidence collection

The gist of the report shown in Figure 13 was that a web server in Finland had been observed spreading software of a malicious nature. According to the report, the actual malware was a *javascript* code embedded in the HTML source code on the server. At the time of the report the malware was only recognised by some anti-virus programs as shown in Figure 14. [102]

File **188369** received on **2009.09.13 18:53:27 (UTC)**
Current status: **finished**
Result: **6/41 (14.63%)**

Compact Print results

Antivirus	Version	Last Update	Result
a-squared	4.5.0.24	2009.09.13	-
AhnLab-V3	5.0.0.2	2009.09.13	-
AntiVir	7.9.1.14	2009.09.11	HTML/Crypted.Gen
Antiy-AVL	2.0.3.7	2009.09.11	-
Authentium	5.1.2.4	2009.09.13	-
Avast	4.8.1351.0	2009.09.12	HTML:IFrame-EJ
AVG	8.5.0.412	2009.09.13	-
BitDefender	7.2	2009.09.13	Trojan.Script.191677
CAT-QuickHeal	10.00	2009.09.12	-
ClamAV	0.94.1	2009.09.13	-
Comodo	2307	2009.09.13	-
DrWeb	5.0.0.12182	2009.09.13	-
eSafe	7.0.17.0	2009.09.13	-
eTrust-Vet	31.6.6733	2009.09.11	HTML/Iframe.C!exploit
F-Prot	4.5.1.85	2009.09.13	-
F-Secure	8.0.14470.0	2009.09.13	-

Figure 14 – A picture showing a part of the *Virustotal* report indicated in the *CLEAN MX* report. At the time of the incident, the malware was only recognised by some anti-virus programs. [102]

Upon receiving the report, the CERT-FI handler did a simple connection test to determine that the malicious code was still online.

4.1.2.3 Incident coordination

In a routine already familiar from the previous section, the CLEAN MX reporting system had issued a takedown request to the hosting provider and had merely sent a reference copy to CERT-FI.

In contrast to the previous case, this time the handler on duty at CERT-FI determined that concrete actions were needed. The CERT-FI duty officer had determined that the web server was running a poorly configured *Joomla*[30] installation containing known vulnerabilities. It was seen highly probable that the server was compromised and it was bound to contain other malicious files and unauthorized content as well. This needed to be communicated to the party responsible for the server's security. A separate takedown request shown in Figure 15 was sent by CERT-FI. However, instead of sending the request to the hosting provider, it was addressed to the telecommunications operator providing the network uplink to the hosting provider.

---

[30] http://www.joomla.org/

```
We received a report indicating a customer to Sonera's networks. On the server there is
at least a seemingly poorly configured Joomla to be found, the service seems worth
checking out.

https:///wwwshoppingcenter.com/ -->
ICENSE.php * Joomla! is free software. This version may have been
modified pursuant * to the GNU General Public License, and as
distributed it includes or * is derivative of works licensed under the
GNU General Public License or * other free or open source software
licenses. * See COPYRIGHT.php for copyright notices and details. */ //
Set flag that this is a parent file define( '_JEXEC', 1 );
define('JPATH_BASE', dirname(__FILE__) ); define( 'DS',
DIRECTORY_SEPARATOR ); require_once ( JPATH_BASE
[..]
```

Figure 15 – Part of an incident report sent by CERT-FI. The translation from Finnish of the short covering note on the top of the message is by the author.

4.1.2.4 Incident resolution

After a while, the malware was removed. No further correspondence after the takedown request was ever recorded and no information about the actions taken by the hosting provider was received. This being a routine case, CERT-FI merely closed the "ticket" and moved on. A reference copy of the malware script was not retained by CERT-FI.

4.1.2.5 Unresolved issues

The rationale behind the duty officer's decision to escalate the handling to the upstream network provider instead of the hosting provider has not been properly recorded. Speculation permitting, the decision to escalate may have been motivated by one or more of following reasons:

- The handler may have decided to use the escalation as a means to emphasise the urgency of the incident and put indirect pressure on the hosting provider to better its security posture.
- The handler may have determined that the hosting provider has had a bad history in handling similar incidents in the past and decided to bring the problems to the upstream network provider for consideration.

The escalation may also have been an oversight since CERT-FI only maintains a list of authoritative incident handling contacts for autonomous systems (see Figure 18). This contact list contained the upstream network provider but not the hosting company.

Whatever the reason, the malware was removed shortly after the upstream provider had been informed.

Table 6 summarises the information collected during the incident handling.

Table 6 – Summary of information collected during the handling of incident *[FICORA #308909]*.

	Incident reporting clearing-house	Incident reporting clearing-house	National CERT	ISP	ISP	Victim
	Malwaredo-mainlist.com and Mal-wareurl.com	CLEAN MX	CERT-FI	TeliaSonera	INT2000	wwwshop-pingcen-ter.com
Report received from	?	Malwaredo-mainlist.com or Mal-wareurl.com	CLEAN MX	CERT-FI	CLEAN MX	?
Incident ID	-	#188369	[FICORA #308909]	?	?	?
Associated IDs	-	-	CLEAN MX #188369	[FICORA #308909], CLEAN MX #188369	CLEAN MX #188369	?
Next-in-line incident handling contacts	-	INT2000, CERT-FI	TeliaSonera (upstream ISP)	INT2000 (downstream ISP)	customer (web server owner)	?
Recorded incident status	-	resolved, site taken offline	resolved, site taken offline	?	?	?
Date discovered (in UTC)	?	2009-09-13 20:14	2009-09-19 16:55	2009-09-23 07:35	2009-09-19 16:55	?
Resolved (in UTC)	-	2009-09-28 22:01	2009-09-25 15:35	?	?	?
Persistence	-	361.8 h (> 15 days)	-	?	?	?
Network information resolved	URL, host-name, domain whois, IP address (PTR), ASN, AS name, coun-trycode	URL, host-name, domain whois, IP address (PTR), IP whois, ASN, AS name, peer-ASNs, countrycode, RIR	as indicated in the report received	?	?	?
Evidence inherited from	Various, in-cluding Virus-total, Anubis, Wepawet, ThreatExpert, Google Diag-nostic Page, WOT Score Card..	Malwaredo-main.com and Mal-wareurl.com	CLEAN MX	CERT-FI and CLEAN MX	CLEAN MX	?
Evidence secured	Malware identi-fier (MD5, name), links to public reports by analysis	connection log, links to other public reports by 3rd parties	connectivity test, web server vulner-ability analysis	?	?	?
Actions taken	receive, verify, share	receive, verify, analyse, share, request assis-tance, archive	receive, verify, analyse, send takedown request, ar-chive	receive, verify, send takedown request	receive, verify, issue take-down?	?

4.1.3 Six Finnish web servers hosting malware: a chain of trust

The following incident was reported to CERT-FI by an incident clearing-house that has expressed a wish to remain unidentified. The incident has been issued id of *[FICORA #295909]* [118] by CERT-FI.

In addition to preferring to stay unnamed, this particular clearing-house refuses to identify individual report sources. The decision to omit source information is in part justified by an effort to protect the monitoring capabilities from being discovered by the attacking party. If the attackers would have the knowledge of the location and exact characteristics of the monitoring systems, they would simply adjust the attacks in way to evade detections. Additionally, some sources have presumably determined that being identified would not serve them in their main line of business as it may be completely removed from NIS.

Despite this pronounced secrecy, a history of accurate reports and successful takedowns has helped to develop mutual trust between CERT-FI and the reporting party. The reports only contain the bare minimum information necessary for the network administrators to identify the individual users or ICT systems indicated in the reports. Once received by CERT-FI, the reports are sent to the network administrators for actions. At this point, the reports assume new identities. As far as the ultimate recipient can see, the reporter is CERT-FI.

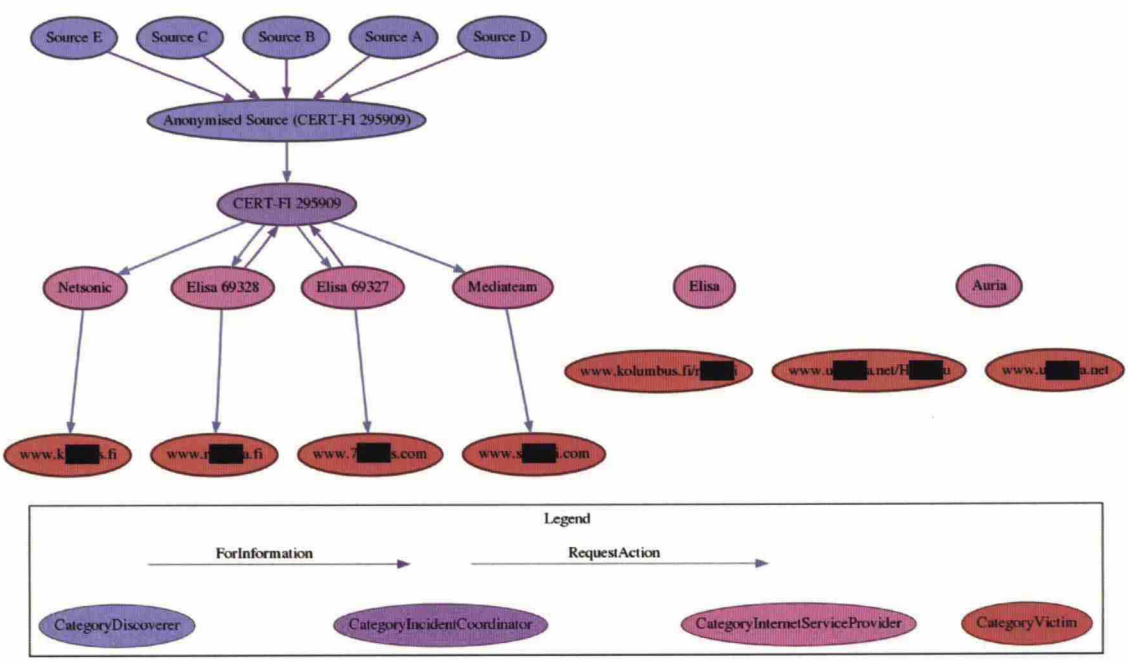

Figure 16 – Information flow in incident *[FICORA #295909]*. The black boxes have been introduced to protect the victims' identities.

The Figure 16 above makes an effort to illustrate the information flow during the incident handling. Without knowing, exactly how many original sources contributed to the discovery there are five sources labelled from A to E in the picture. The sources have surrendered their log material to the clearing-house for correlation purposes on the con-

dition of anonymity. After having processed the data, the clearing-house determined seven instances of relevance to Finland and reported them to CERT-FI.

4.1.3.1 Initial discovery

The original incident report received by CERT-FI is shown in Figure 17. Some portions of the report have been edited to protect the victims' identities and brands.

```
3336  | 193.229.[redacted] | 2009-08-16 12:54:12 http://www.r[redacted]a.fi/              | ELISA-AS
3336  | 193.229.[redacted] | 2009-08-16 13:55:16 http://www.kolumbus.fi/r[redacted]i/     | ELISA-AS
3336  | 193.229.[redacted] | 2009-08-16 12:56:43 http://www.7[redacted]s.com/             | ELISA-AS
16044 | 62.73.[redacted]   | 2009-08-16 13:13:22 http://www.u[redacted]a.net/H[redacted]u/ | AURIA
16044 | 62.73.[redacted]   | 2009-08-16 13:34:16 http://www.u[redacted]a.net/             | AURIA
16023 | 81.17.[redacted]   | 2009-08-16 13:38:18 http://www.k[redacted]s.fi/index.php     | NETSONIC
39324 | 81.22.[redacted]   | 2009-08-16 13:30:13 http://www.s[redacted]i.com/             | MEDIAM-AS
```

Figure 17 – Automated bulk report received by CERT-FI indicates seven URLs seen distributing malicious software on six web servers. The incident id is *[FICORA #295909]*. The IP addresses and portions of URLs are masked to protect the victims' identities.

The report has been formatted in a way that enables both manual and automated processing. The representation is rather condensed, listing one incident per line. The outermost columns (separated by a vertical line) contain an AS number and the name of the corresponding autonomous system. These effectively tell which organisation – usually an ISP – owns the part of the network to which the web server is connected. In this case, the compromised servers were in four different networks belonging to Elisa, Auria, Netsonic, and Mediateam. Of these, Elisa and Auria are network providers. Netsonic and Mediateam can be best described as hosting providers as they provide web server hosting rather than backbone networks or subscriber lines. The second column from the left indicates the unicast IP address associated with the incident. The third column contains the date and timestamp of the discovery along with additional information, in this case the URL containing the malware[31].

Reports using this format are produced by using an IP to AS mapping tool provided by Team Cymru. Appendix II contains examples that illustrate how this important tool can be used to find appropriate network owner contacts to submit reports to. Most CERTs and ISPs have developed methods for automating the parsing of reports sent in the so-called "Cymru format." The data format has been proven powerful as it is relatively easy to read by both humans and parsing scripts. The format represents essential incident data in relation to the parties responsible for the networks. CERT-FI routinely combs through similar listings in search of AS numbers belonging to Finnish organisations.

4.1.3.2 Evidence collection

Before blindly forwarding the reports, CERT-FI ran a set of simple tests to establish whether the reports indicated genuine incidents, and to determine relevant network owners along with their incident reporting points of contact. The set of masked results is shown in Figure 18.

---

[31] To be exact, this report type indicates URLs containing links to the actual malware and necessary script routines used to initiate automatic download of the malware.

```
Testing for the existence of malware
http://www.s[redacted]i.com/ Tue, 18 Aug 2009 05:05:13 +0000
200
Found AS contacts for AS 39324: [redacted]

Testing for the existence of malware
http://www.kolumbus.fi/r[redacted]i/ Tue, 18 Aug 2009 05:05:13 +0000
200
Found AS contacts for AS 3336: abuse@elisa.fi

Testing for the existence of malware
http://www.7[redacted]s.com/ Tue, 18 Aug 2009 05:05:14 +0000
200
Found AS contacts for AS 3336: abuse@elisa.fi
Testing for the existence of malware
http://www.r[redacted]a.fi Tue, 18 Aug 2009 05:05:14 +0000
200
Found AS contacts for AS 3336: abuse@elisa.fi

Testing for the existence of malware
http://www.u[redacted]a.net/H[redacted]u/ - malware taken offline Tue, 18 Aug 2009
05:05:14 +0000
403
http://www.u[redacted]a.net/ - malware taken offline Tue, 18 Aug 2009 05:05:14 +0000
403
Testing for the existence of malware

http://www.k[redacted]s.fi/index.php Tue, 18 Aug 2009 05:05:14 +0000
200
Found AS contacts for AS 16023: [redacted]
```

Figure 18 – A portion of case log archived under *[FICORA #295909]*. This the output of an automated tool used by CERT-FI to test the existence of the reported malware and to find an authoritative reporting point to send a takedown request to. The URLs are masked to protect the victims' identities. Also, the reporting points not found in public registries are masked away.

From the lines containing the text *"Found AS contacts for"* in Figure 18 above, one can see that CERT-FI has accumulated an in-house registry of incident handling contacts for the Finnish networks. The contact details have been removed unless they have otherwise been made public by the use of the IRT object in the WHOIS as described in Section 3.2. Numbers 200 and 403 indicate web server response codes. For the purposes of this study, it suffices to know that the response code 200 stands for success and 403 means that the file does not exist. Of the seven URLs listed in Figure 17, two belonging to Auria appear to have already been taken offline.

The remaining five URLs were quickly downloaded using *wget* tool to establish that the harmful content is still present. One of the URLs in Elisa's networks neither contained malware nor pointers to malware. Those may have been removed before CERT-FI had a chance to investigate. [106]

The remaining four sites contained pointers to malware. For instance, the HTML source code at www.7[redacted]s.com contained a hidden *iframe* object pointing to a Russian web server. Portions of the source code are displayed in Figure 19 below. The injected *iframe* portion is highlighted in red font.

```
[..]
<body link="#111111" vlink="#111111" alink="#111111" topmargin="0" leftmargin="0"
 text="#111111" bgcolor="#111111" onload="dynAnimation()"><iframe
 src="http://3a1.ru:8080/index.php" width=193 height=178 style="visibility:
 hidden"></iframe>
[..]
```

Figure 19 – The front page of www.7[redacted]s.com contained a hidden *iframe* object. It had most probably been inserted on the server as a result of a successful break-in.

4.1.3.3 Incident coordination

CERT-FI eventually sent four takedown requests similar to the one seen in Figure 20 below. Two of the requests were sent to an ISP, whose abuse department sent an automatic response indicating the trouble ticket identifier assigned to the report in their handling system. The two reports sent to hosting providers were never acknowledged.

```
************************************************** CERT-FI *****

Case reference: [FICORA #295909]

*********************************************************************
Malware in your network

CERT-FI has received information about a malware hosting website in
your network. Please review the information below and take appropriate
action to remove the site from your network. If you are not the
contact responsible for this domain, please forward this message to
whom it may concern.

Please also fix the security problem which made it possible for the
abusers to upload the content to the server. The security problem may
be due to leaked login credentials, a vulnerability or a
misconfiguration. Additionally, it is possible that the server is now
backdoored. Thus just simply removing the offending content is not
enough to prevent this from happening again in the future.

- CERT-FI case: 295909
- Site: http://www.s[redacted]i.com/
Tue, 18 Aug 2009 05:05:13 +0000
- Hostname: srv-g[redacted].esp.mediateam.fi
- Hostname: www.s[redacted]i.com
- Hostname: [redacted].serv.kotisivut.com
```

Figure 20 – A copy of a takedown request sent by CERT-FI in response to incident *[FICORA #295909]*. The original request was in Finnish but for the purposes of this study the message body is replaced with identical English translation used by CERT-FI *abuse.py* tool.

4.1.3.4 Incident resolution

According to the CERT-FI archives, the incident was marked as resolved shortly after the reports were sent out. The state of the offending sites was not polled afterwards.

4.1.3.5 Unresolved issues

CERT-FI never learnt when and how the web server owners or Auria and Elisa came to discover and fix the security problem. The malware had already been removed at the time CERT-FI had a chance to take a look at the report.

Furthermore, there is no knowledge about the concrete actions taken by Elisa, Netsonic and Mediateam. All but one of the web server owners remained unidentified and CERT-

FI made no effort to contact them. Kolumbus.fi is a shared web server of the ISP Elisa, which made it easy to identify the server owner.

Since no forensics reports were received, no factual information about the duration of the security problem exists.

CERT-FI obtained no copies of the malware encountered on the servers.

Table 7 provides a brief summary of information obtained.

Table 7 – Summary of information collected during the handling of incident *[FICORA #295909]*.

	Discoverers	Incident reporting clearing-house	National CERT	ISP	ISP	ISP
	Anonymous discoverers	Incident Repository (identity withheld)	CERT-FI	Elisa	Netsonic, Mediateam	Auria, Elisa
Report received from	-	Anonymous Discoverers	Incident Repository	CERT-FI	CERT-FI	?
Incident ID	-	-	[FICORA #295909]	#69327, #69328,	?	?
Associated IDs	-	-	-	[FICORA #295909]	[FICORA #295909]	?
Next-in-line incident handling contacts	Incident Repository	CERT-FI	Elisa, Netsonic, Mediateam, Auria	customer	customer	?
Recorded incident status	-	-	resolved, site assumed taken offline	?	?	?
Date discovered (in UTC)	2009-08-16 12:54	2009-08-16 12:54	2009-08-17 09:31	2009-08-18 05:11	2009-08-18 05:11	?
Resolved (in UTC)	-	-	2009-08-21 05:25	?	?	before 2009-09-18 05:05
Persistence	-	-	-	?	?	?
Network info resolved	URL	URL, IP, ASN, AS name	Multiresolver tests[32]	?	?	?
Evidence inherited from	-	Anonymous Discoverers	Incident Repository	CERT-FI	CERT-FI	?
Evidence secured	-	malware sample	connectivity test	?	?	?
Actions taken	discover, share	receive, share, archive	receive, verify, analyse, send takedown request, archive	issue takedown	issue takedown	?

4.1.4 Foreign web server suspected of spreading malware

Here, we examine a case where a web server in the United States had been determined to be disseminating a piece of software with the characteristics of malicious nature. The incident has been issued a tracking code *[FICORA #307761]* in the CERT-FI incident handling system [119]. Figure 21 gives an overview of the incident coordination.

[32] For details, see Appendix III: Multiresolver output of [FICORA #295909].

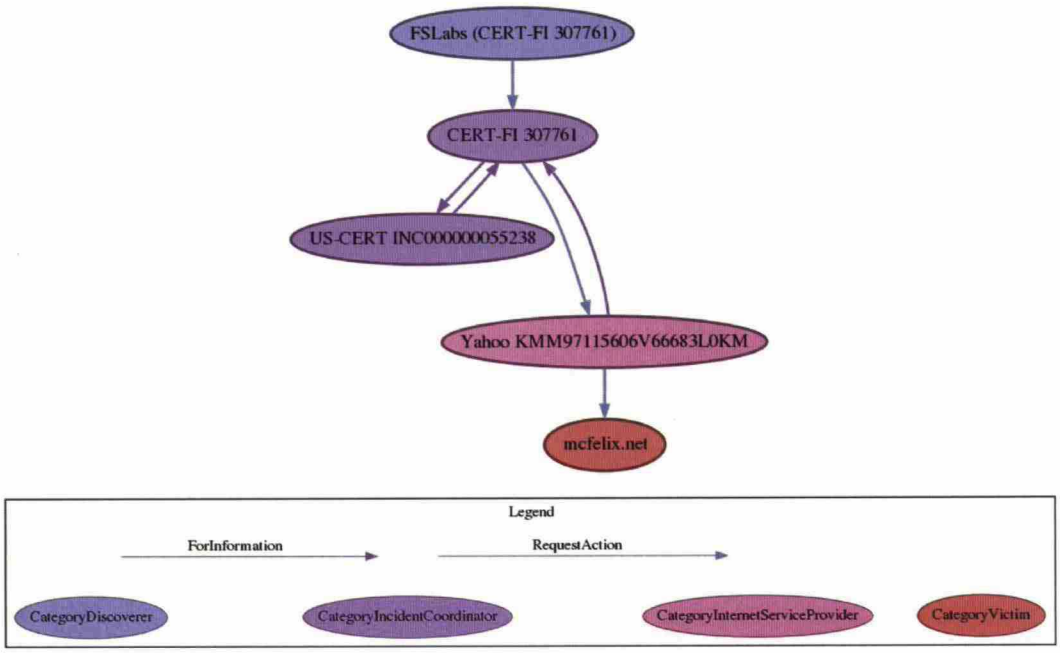

Figure 21 – Chart depicting the information flow and actions being taken by various actors during the incident investigation in *[FICORA #307761]*.

4.1.4.1 Initial discovery

The existence of the said site had been brought to the attention of CERT-FI by malware analysts at F-Secure, an internet security company. As part of their routine job, they have been reverse-engineering samples of suspicious software. Among other things, the analysts had been able to extract web site addresses pointing to web sites used to distribute updates to the original malware.

4.1.4.2 Evidence collection

After having received the report, the analyst at CERT-FI performed routine tests to establish the credibility of the claim. Quick tests were performed using an in-house scripting tool called *abuse.py*. The first item to test was to see whether the contents were still online as seen in Figure 22 below.

```
Testing for the existence of malware
http://mcfelix.net/images/especta8.gif Thu, 17 Sep 2009 05:45:59 +0000
200
http://mcfelix.net/imagenes/poster-blau2.jpg Thu, 17 Sep 2009 05:46:01 +0000
200
http://mcfelix.net/imagenes/fiat3.jpg Thu, 17 Sep 2009 05:46:03 +0000
200
```

Figure 22 – Results of the simple test tool used in examining the existence of the suspected malware.

The three URLs pointed to files that at first appear to be bitmap files. On a closer examination, however, the files turned out to be binary files containing an update (the so-called secondary stages) to a previously detected malware.

The extracted data clearly indicated that a security incident of some kind was taking place. It would have been a waste of analytical resources, and outright irresponsible, to have turned a blind eye towards the problematic server and let it stay online infecting innocent bystanders. As a result, it has developed a routine practice for analysts at F-Secure to pass this kind of information to CERT-FI for coordination, an arrangement that has had apparent benefit for CERT-FI as well.

4.1.4.3 Incident coordination

Shortly afterwards, CERT-FI received three simplistic e-mails from F-Secure with non-descript topics and URLs pointing to malware-distributing sites in the body of the message. The routine of sharing the data and the reporting format had been agreed beforehand between CERT-FI and F-Secure.

After having established that there was a valid case and that CERT-FI was in a position to help resolve it, the case officer proceeded to request assistance in taking down the malware distribution site. It was quickly determined that the web server was outside Finland, namely in the United States.

The domain name holder was not previously known to CERT-FI and publicly available contact details were too ambiguous for the purpose of submitting reports.

Instead of contacting the server owner, CERT-FI proceeded by referring the case to a party with incident handling capabilities closest to the victim, in this case Yahoo. In this instance, closest meant proximity in the network topology sense, as demonstrated in Appendix II. Following the good practices of responsible internet service providers, Yahoo had made incident response contacts easily obtainable. A takedown request, shown in Figure 23, was submitted to Yahoo.

```
************************************************** CERT-FI *****

Incident ID: [FICORA #307761]

*****************************************************************
Malware in your network

CERT-FI has received information about a malware hosting website in your network. Please
review the information below and take appropriate action to remove the site from your
network. If you are not the contact responsible for this domain, please forward this
message to whom it may concern.

Please also fix the security problem which made it possible for the abusers to upload
the content to the server. The security problem may be due to leaked login credentials,
vulnerability or a misconfiguration. Additionally, it is possible that the server is now
backdoored. Thus just simply removing the offending content is not enough to prevent
this from happening again in the future.

- CERT-FI case: 307761
- Site: http://mcfelix.net/imagenes/fiat3.jpg
- Malicious Content: Trojan-Spy:W32/Zbot.OYK
Thu, 17 Sep 2009 05:46:03 +0000
- Site: http://mcfelix.net/imagenes/poster-blau2.jpg
- Malicious Content: Trojan-Spy:W32/Zbot.OYI
Thu, 17 Sep 2009 05:46:01 +0000
- Site: http://mcfelix.net/images/especta8.gif
- Malicious Content: Trojan-Spy:W32/Zbot.OYH
Thu, 17 Sep 2009 05:45:59 +0000
- Hostname: mcfelix.net
- Hostname: p8p.geo.vip.mud.yahoo.com
- Host ip: 68.142.212.70
- Host country: US
```

```
- ASN: 14780 INKTOMI-LAWSON - Inktomi Corporation

In addition to your own actions, please forward this information to your resident law
enforcement agents (FBI/USSS) for law enforcement action.
```

Figure 23 – Incident report sent by CERT-FI to the ISP and the US-CERT. Refer to Figure 21 on page 46.

An informational copy of the report was sent to the United States computer emergency response team, *US-CERT*. In this example, US-CERT did not necessarily take any action beyond returning a trouble ticket number to assist in further correspondence.

It is not known, what actions Yahoo performed. It, however, sent an acknowledgement message indicating that the report had been received and that Yahoo will – in their own words – "*investigate the site and take the appropriate action.*"

Ultimately, it is the server owner's responsibility to investigate the issue and to fix the problem. In this case, the web server hosting the web site mcfelix.net was owned by Yahoo.

4.1.4.4 Incident resolution

CERT-FI was satisfied with the response received and never even bothered to verify that the files had been taken offline. The trouble ticket was closed first thing on Monday morning.

4.1.4.5 Unresolved issues

No information was ever received regarding what had taken place on the web server. It is assumed that the malware was put online following a system compromise instead of the server deliberately been spreading malicious software. There is not enough information to determine how long the malware was online, how many people downloaded it, and who they were.

It is a recommended practice to report break-ins to law enforcement for further criminal investigation. There is nothing to suggest that law enforcement was ever involved, however.

Table 8 displays a summary of the collected information.

Table 8 – Summary of information collected during the handling of incident *[FICORA #307761]*.

	Discoverer	National CERT	National CERT	ISP	Victim
	F-Secure	CERT-FI	US-CERT	Yahoo	mcfelix.net
Report received from	sample submission	F-Secure	CERT-FI	CERT-FI	?
Incident ID	-	[FICORA #307761]	US-CERT INC00 0000055238	Yahoo KMM97115606V 66683L0KM	?
Associated IDs	-	US-CERT INC00 0000055238, Yahoo KMM97115606V 66683L0KM	[FICORA #307761]	[FICORA #307761]	Yahoo KMM97115606V 66683L0KM
Next-in-line incident handling contacts	CERT-FI	Yahoo	?	?	?

	Discoverer	National CERT	National CERT	ISP	Victim
	F-Secure	CERT-FI	US-CERT	Yahoo	mcfelix.net
Recorded incident status	?	resolved	resolved	resolved	resolved
Date discovered (in UTC)	?	2009-09-16 20:57	2009-09-17 05:50	2009-09-17 05:50	?
Resolved (in UTC)	?	2009-09-21 05:48	?	?	?
Persistence	?	-	?	?	?
Network info resolved	hostname	IP, ASN, connection test	?	?	?
Evidence inherited from	?	F-Secure	CERT-FI	CERT-FI	?
Evidence secured	malware sample	-	?	?	?
Actions taken	receive, analyse, report	receive, analyse, report, archive	receive, acknowledge, archive	receive, acknowledge, investigate	?

4.2 Data Breaches

4.2.1 Case "78kfinnpwhashes.zip" – list of passwords posted on internet

On October 2007, a zipped archive containing over 78,000 user names and passwords began circulating on the internet. The title of this section reflects the name of the file, "*78kfinnpwhashes.zip*." Once discovered, it soon became evident that the passwords were genuine and stolen from several Finnish web sites. Therefore, an exceptionally large number of user accounts and web sites were left without proper defence against abuse.

In addition to the exceptional breadth of the security breach, this case was also special in the sense that the person behind the computer break-ins and publication of the passwords was later identified, arrested and tried in court. The criminal investigation and judicial proceedings [78] helped bring to light information that was not readily available at the time of incident handling.

For the purposes of this study, we are forced to limit ourselves to merely examining the flow and accumulation of information rather than attempting to describe the incident in detail. Uncovering the circumstances that made the breach possible and evaluating how the incident affected the users and businesses would deserve a study of its own. Trial documents [78], public announcements by the police [70],[71] and CERT-FI [21],[22],[23], news articles[33], blog commentaries[34] and forum chatter[35] can now be combined with material found in the CERT-FI archives to help us understand how the incident response portion of the case advanced. The incident notes have been archived under *[CERT-FI: 36789]*. [116]

---

[33] E.g. http://www.hs.fi/english/article/Leaked+list+of+passwords+already+put+to+nefarious+use+/1135231072527, http://arstechnica.com/security/news/2007/10/hackers-target-finnish-forum-crack-logins-for-almost-80000-users.ars and http://www.nelonen.fi/uutisvideot/default.asp?video=769&c=1&newpage=0

[34] http://www.f-secure.com/weblog/archives/00001293.html and http://www.omasana.fi/jouko-pynnonen/19698

[35] http://murobbs.plaza.fi/yleista-keskustelua/507132-78000-suomalaisen-salasanat-julki-tarkastakaa-ja-reagoikaa.html

4.2.1.1 Initial security breaches

According to court documents [78], the initial events took place in September 2007 when the offender took steps to break into several web sites. One by one, he accessed the user databases and retrieved a copy of them for his own use. The databases contained user names, e-mail addresses and passwords. Some passwords were in hashed form, a clear indication of the material being acquired by having unrestricted access to the user database.

A compilation of stolen passwords was then created and the file was posted online on 12 October. [97] A covering note prefixing the actual list urged people to take the passwords and use them, for instance, for reading people's e-mails and modifying their web pages. As the existence of the password list became more widely known, several individuals followed the advice and posted evidence describing their exploits to encourage others. Collaborative efforts to crack the hashed passwords in the file were launched almost immediately [108].

4.2.1.2 Incident discovery

According to the incident archives [116], CERT-FI only learnt about the incident on Saturday 13 October when private citizens started hinting about the password list. Also news media journalists were quick to discover an exceptional story and contacted CERT-FI. According to the reports received from the owners of the affected web sites, most of them were taken by surprise. Most had found out about the security breach either in the news or from their end-users.

Further correspondence, however, revealed that some administrators had seen symptoms that turned out be indications of a break-in being prepared. On Sunday 14 October, one administrator wrote to CERT-FI that two administrator accounts had been breached already over two weeks ago in late September. The following citations are taken from the incident ticket, translated from Finnish by the author.

> *"Between 29 and 30 October [the reporter actually meant September], two user accounts were used by an unauthorised party. The accounts in question belonged to so-called moderators. [..] The incident struck us as odd, as this was the first time ever [..] that moderator accounts were leaked."*

Later during the same day, the same person added:

> *"This [referring to logs provided] reminds me of a couple of details that I already had forgotten. Some of the compromised accounts were taken over by first breaking into the users' mailboxes. In our service, one can use e-mail to reset one's password [..]"*

The administrator returned the next day after having carefully analysed the anomalies found on the system logs. The redacted portion refers to a user account name possibly related to the attacker.

> *"So it seems that the password list was in limited circulation already on 26 September and ended up with* [redacted]*, who then started systematically going through the accounts found on the list."*

These findings helped establish the timeline of the break-ins and indicate the identity of the person behind the attack. The attack methods employed were beginning to unravel, too. Still there was no foolproof way to confirm from which services the password information was stolen. A method of trial and error produced good results, however. In the words of another administrator in a correspondence on 14 October:

> *"We have been comparing the password list against our user database. We have also received reports from various people indicating that the list contains a significant number of our users. The list appears to contain a large portion of our users, if not all."*

After the initial distribution site went offline, CERT-FI began receiving requests to share a copy of the password file. After legal consultation, it was decided that those administrators responsible of considerable number of end-users could be provided with a copy of the list for verification purposes. [108] A copy of the list was sent to a small number of administrators. Most certainly a larger number of administrators and bystanders simply downloaded their copy from one of the several mirrors that began popping up all over the internet.

Upon comparing the publicised password list to their local user databases, some administrators noted that the password list not only contained perfect matches but also listed the usernames in the exact same order as found in their systems. Since some of the sites had made their member list public, a couple of end-users were able to reach the same conclusion. One by one, the list of sites from where the passwords had been stolen began to emerge.

Some administrators were even able to determine the time of the break-in by comparing the published user list with the recent additions to the database and using a simple deductive reasoning. Usernames present in the local user database but missing in the *"78kfinnpwhashes.zip"* must have been created after the break-in took place. Using a simple comparison using the *diff* tool[36] and looking up the creation times of the last user id present in both files and the first username missing from the public list, one comes up with a time span during which the break-in took place. By comparing this information with the log files obtained from the web servers helped in part to identify the attacker.

By the end of Friday 19 October, the administrators had gathered enough evidence to suggest that the password databases were primarily stolen using a method called *SQL Injection*. This is an attack type where flaws in the web application's input validation routines are being exploited to inject unrestricted commands for the backend database to process. The discovery helped the administrators to interpret the log files to find the original break-ins. This portion of the investigation was performed under the guidance of the police rather than CERT-FI. Instead, following a recommendation by the police, CERT-FI refrained from publicly mentioning the SQL Injection attack vector until 9 November [22],[23]. This was determined a necessary measure by the police interrogators.

Although not known at the time, the court documents later indicated the attacker had performed a series of *SQL Injection* attacks with varying rates of success while preparing for the data breach. [78] Based on the information available to CERT-FI, the log files were seldomly analysed for signs of SQL Injection until specific suspicions arose.

---

[36] http://www.gnu.org/software/diffutils/

4.2.1.3 Incident coordination

Immediately after having learnt about the incident, CERT-FI took steps to determine that the password file contained genuine credentials. At first, it was still unclear from where the passwords were stolen. It was clear, however, that the material was taken from several different servers and, after taking a quick look at the usernames, it became obvious that the users were mostly Finnish-speaking people.

While this puzzle was still being sorted out, it was determined that the file was hosted on a server in the United States. A takedown request, shown in Figure 24 below, was sent to the ISP's security team – in this case Dreamhost – and US-CERT.

```
US-CERT: Please notify your FBI/USSS officers immediately on this.
         Please take all other appropriate action.

Dreamhost: We request that

-the abovementioned file is taken offline immediately
-please keep a freezed copy of all content, files and account information related to
abovementioned site
```

Figure 24 – A takedown request sent to the hosting provider informing about the password file.

It turned out that determining where the password lists had been stolen from was less than straightforward. A combination of public advisories, enquiries directed to Finnish security experts and educated guesses was used. Reading the chatter in the public forums also helped in providing good leads to follow. This method quickly produced a list of twenty servers, whose administrators were then approached with a request for information. Public advisories were sent out to inform both the end-users and the system administrators about the situation. People with information to share were encouraged to contact CERT-FI.

Since the incident clearly involved a series of criminal acts, whose investigation is outside the mandate of CERTs, police was notified. The incident involved a large number of personal information, which made it necessary to inform the data protection ombudsman of Finland[37] also.

Throughout the weekend and during the next week, new information kept coming in. Several server administrators were able to confirm that their systems had been broken into. With a little help, most of them were able to determine how the compromise was possible and when it took place. Additionally, some administrators were able to determine that their systems had not been broken into, thus refuting the rumours. A fair amount of end-users contacted for advice but instead of engaging in time-consuming dialogue with individual users, time was devoted to crafting advisories and responding to media enquiries.

CERT-FI never approached the end-users personally nor was any effort made to identify the users. Instead, the server administrators – essentially, the service providers – were encouraged to inform their users by the means they found most suitable for the situation.

---

[37] http://www.tietosuoja.fi

Some individuals reported that their e-mail accounts or their profiles on the social media sites had been accessed and modified in an unauthorised manner. These reports were acknowledged with instructions to contact the service provider and the police. Active incident coordination was never initiated to resolve these sidelines.

The password file was taken quickly offline by Dreamhost but several copies had already been published. CERT-FI gave out recommendations to take the files offline, but never actively pursued further takedowns.

Less than week after the first incident reports were received, police performed a successful arrest and got a preliminary confession from the suspect. By that time, the work of CERT-FI was already largely completed.

4.2.1.4 Criminal investigation and court proceedings

It is relatively uncommon for the NIS incidents to lead to a criminal investigation. Even less common it is for the police to find a suspect. This time, however, the victims were mostly Finnish and the perpetrator turned out to be a Finnish national. With few cross-border assistance requests necessary, the police was able to execute with a pace. The police was informed on Saturday 13 October, the launch of an investigation was publicly announced on Monday 15 October and the arrest was made public on Thursday 18 October.

After a longish quiet period, the case finally proceeded to court with an indictment on 8 June 2009 and the sentencing on 18 September 2009 [78]. Since there were no appeals, the sentence became legally valid on October 2009, quite exactly two years after the incident was for the first time brought to public attention.

4.2.1.5 The incident time versus judicial time

Upon comparing the incident response and judicial process, one immediately observes the scale difference in the incident timeline. As seen, it may take years for the justice system to complete its work and long delays may be introduced.

In contrast, the incident response process is launched immediately after the first indications of the security breach have surfaced and the success or failure of the incident resolution may depend on delays counted in days, if not hours. As in this case, there is often an active opponent trying to outmanoeuvre the defenders of the ICT systems. Also true with this case was the fact that the incident sometimes has the potential to balloon out of control unless concrete counter-measures can be deployed in a uniform fashion even in systems of distributed nature.

In the case described here, the embarrassing and harmful publication of passwords could have been avoided if the offender had been identified and captured earlier. After the publication took place, the most effective counter-measures included forced password changes and emergency shutdowns of the services. These were performed within day or two after the incident discovery and effectively helped reduce the damage. Immediate actions were also taken to secure the evidence for the purposes of criminal investigation and technical root-cause analysis.

Judging by the actions taken by CERT, the acute phase of the incident response took place during the five-day period between Saturday and Wednesday. Police investigation

led to arrest exceptionally fast but interrogations and finalising the investigations still required many months to complete. It is common for the court proceedings to take place only long after the incident. The incident has been summarised in Table 9.

Table 9 – Summary of information collected during the handling of incident *[CERT-FI: 36789].*

	National CERT	National CERT	ISP	ISPs	Victims	Collateral victims	Law enforcement	Law enforcement	Judicial system
	CERT-FI	US-CERT	Dreamhost	Finnish network and hosting providers	Web server owners (10)	Individuals (thousands)	National bureau of investigations (NBI)	FBI	Prosecutor, district court
Report received from	Individuals, ISPs, victims	CERT-FI	CERT-FI	CERT-FI, individuals	CERT-FI, individuals	CERT-FI, web server owners, media	CERT-FI, victims	NBI	law enforcement
Incident ID	[CERT-FI: 36789]	US#067747	?	?	-	-	2400/R/431/07	?	criminal case: R 09/1978, sentence: R 09/446
Associated IDs	US-CERT: US#067747, police: 2400/R/431/07, criminal case: R 09/1978, sentence: R 09/446	[CERT-FI: 36789]	[CERT-FI: 36789], police: 2400/R/431/07	[CERT-FI: 36789]	[CERT-FI: 36789], police: 2400/R/431/07	-	[CERT-FI: 36789]	police: 2400/R/431/07, [CERT-FI: 36789]	police: 2400/R/431/07
Next-in-line incident handling contacts	hosting providers, server owners, ISPs, law enforcement, data protection officials, individual citizens (through advisories)	?	-	web server owners	end-users, law enforcement	?	judicial system	?	-
Recorded incident status	resolved	resolved	resolved	resolved	resolved	?	resolved	?	resolved
Date discovered (in UTC)	2007-10-13 13:47	2007-10-13	2007-10-13 16:40	2007-10-13 15:53	between 2007-10-13 and 007-10-14	2007-10-13	2007-10-13 15:54	2007-10-14	2009-06-08
Resolved (in UTC)	2007-10-21	?	2007-10-14 05:48	?	?	?	2009-06-08	?	2009-09-18
Persistence	-	?	?	?	?	?	?	?	?
Network info resolved	URLs, IP, ASN, AS name, DNS, WHOIS	?	?	?	?	?	?	?	?
Evidence inherited from	individual reporters, victims	CERT-FI	CERT-FI	CERT-FI	CERT-FI	CERT-FI, service providers	plaintiffs, CERT-FI, individual citizens	CERT-FI, NBI	police, plaintiffs, data protection ombudsman
Evidence secured	offline copy of password list	?	?	?	server logs, user databases	?	password list, victims' log files, surveillance material, interrogations	?	court proceedins
Actions taken	receive, request takedown, investigate, report, produce advisories	?	issue takedown	?	investigate, inform customers, repair, witness in court	?	order takedown, investigate, preserve evidence, arrest, submit for prosecution, a, witness in court	order takedown	issue sentence

4.3 Case Allaple – an eternal DDoS

The websites of three Estonian companies began experiencing symptoms of denial of service attacks in the summer of 2006. One of the targets was a subsidiary to a company based in Finland, which automatically made the incident interesting to CERT-FI. At that time, the targeted website got its internet connection from a Norwegian telecommunications operator, although the servers were later migrated to a network in Finland. There were affected parties in Estonia, Finland, and Norway. The attack traffic kept pouring in from all over the world and gained in strength day by day.

To track the incident's progress and record the correspondence involved, CERT-FI established an incident ticket *[CERT-FI: 19608]* [113]. Additional incident-related material is archived under *[CERT-FI: 25462]*[114] and *[CERT-FI: 25902]*[115]. Having already lasted for several months, the incident was later publicly covered in two quarterly reports.[38]

4.3.1 Persistent threat

A particular feature of this incident is its remarkable persistence. At the time of writing this report, the attack has continued uninterrupted. During the investigation, the everlasting nature of the attack became slowly evident.

After some initial confusion in 2006, samples of the malware binaries attributed to the attack were successfully extracted for analysis. Upon examination, it was soon established that no control structure capable of issuing commands to the infected computers was present, a feature rarely seen in modern malware. Omission of control channels meant that the attack would be sustained for as long as there were infected computers in the networks to carry the attack. One of the first official analyses requested by the police and prepared by CERT-FI is dated in November 2006:

> *"The malware has been created to cause an 'eternal' DDOS at the selected target sites. Since there is no Command and Control channels [sic] present, there is no single point in the mechanism that could be intercepted and the activity stopped. The malware will spread autonomously as long as there are Radmin installations with weak passwords and it will DDOS the sites as long as well."* [126]

The spreading mechanism required no human intervention, either. During the time, the malware was called *"Rahack"* since it spread from host to host by brute forcing weak passwords through the Famatech's Radmin software. The author later augmented the spreading mechanism to include other, more efficient methods, such as exploiting software vulnerabilities. The malware was then renamed *"Allaple"* as it is widely known now. The first mention[39] of Allaple in the F-Secure virus database is dated 7 December 2006.

---

[38] http://www.cert.fi/attachments/tietoturvakatsaukset/5ou4t0B1X/CERT-FI_situation_report_1-2007.pdf and http://www.cert.fi/attachments/tietoturvakatsaukset/5q88Lrkr6/CERT-FI_Information_Security_Review_2_2007.pdf

[39] http://www.f-secure.com/v-descs/allaple_a.shtml

4.3.2 Filtering – a game of cat and mouse

At the height of the attack, the traffic volume exceeded not only the capability of the targeted websites but also threatened to collapse the ISP networks. A packet-filtering device was introduced to the network and, for a long time, it had to discard over 99 % of the offered incoming traffic deemed as generated by the attack. The filter had to be reconfigured each time a new variant of the malware was introduced in the wild; otherwise the servers would have been immediately rendered unresponsive under the flood of traffic. [107]

4.3.3 The attacker makes a mistake, helps produce IDS signature

After having analysed tens of different variants, the reverse-engineering analyst at CERT-FI made an important discovery that greatly helped in recognising the attack traffic from legitimate visitors to the web site. In March 2007, it was discovered that the author had made small mistakes in writing the portions of the code involved in handling the network protocols. These mistakes remained consistent between different variants, which made them ideal for signatures to identify the attack traffic.

While this was clearly an important piece of information to be shared with the network administrators all over the world, there were also a number of compelling reasons to treat the information as sensitive. The first argument against releasing the information was to do with pure tactics: if the attacker were to learn how the signatures were created, he could easily fix the mistakes and release an updated and harder-to-detect version of the malware. Second, law enforcement involvement was picking up speed and this was regarded as a potential forensic clue in case the author of the malware was to ever get caught. The third argument against sharing was that the filtering device in front of the attack target seemed to endure, hence giving the defenders some time to simply wait and see.

However, the number of infections in the global networks kept on growing. It was understood that time was getting short for merely relying on passive filtering methods. Unless the number of attacking hosts was not reduced, the attack volume could grow in an uncontrollable fashion. In order to initiate a worldwide takedown of infected hosts, some information would need to be shared.

After some hesitation, it was decided to share some of the signature-related information publicly in an effort to provide the network administrators with the tools necessary to identifying infected sources within their local networks.

The other option would have been to pump out takedown requests to those administrators whose networks were seen participating in the attacks. This would have required a massive number of e-mails to be sent and would have created a huge amount of questions and requests for more information or even angry letters denouncing the e-mails as spam messages. That would have effectively halted CERT-FI's normal operations. It was clear that the only workable solution would be to go public.

In 2007, however, the name and good reputation of CERT-FI was not known well enough to guarantee wide enough circulation of information. Using the *SANS Internet*

Storm Center[40] as a multiplier appeared to be the fastest way to get the word out. On 14 March 2007, the following message [53] was posted on the internet.

```
In case you are in the correct position, and you feel you would
want to help in this pesky problem, here are a few tricks you can
use to identify Allaple variants on the loose in your networks:

1) ICMP packets with the string "Babcdefghijklmnopqrstuvwabcdefghi",
sans quotes, in the payload.
2) Echo requests to entire networks including host octets of 255 and 0.

We have reason to believe that there will be more variants,
it's just a matter of time when a new one pops out into the open.
```

Figure 25 – A public letter [53] to the readers of Internet Storm Center describing the unique traffic signatures generated by the Allaple worm. Sharing this information was crucial in enabling a large number of network administrators to identify infected hosts in their network segments.

CERT-FI was in possession of more information than visible in the message in Figure 25 above, though. It was decided that a more detailed version of the message would be shared to a limited list of recipients, mostly other CERTs and security software vendors. An inadvertent information leak, however, took place, thus threatening to torpedo the effort of covertly disseminating an attack signature. A copy of the message sent to the Snort signatures project was accidentally released to public dissemination, thus revealing the extra information and indicating that the author's actions were being closely monitored. A portion of the text that was not meant for public dissemination is displayed in Figure 26 below and it is still available on the internet [57].

```
In case you are in the correct position, and you feel you could want to help in this
pesky problem, here are a few tricks you can use to identify Allaple variants on the
loose in your networks:

1) ICMP packets with the string "Babcdefghijklmnopqrstuvwabcdefghi", sans quotes, in the
payload.

2) HTTP GET requests to www.if.ee. Due to a mishap in the code, the GET request is
unique. The request looks something like this: "GET / HTTP/1.1\r\n". There are two
whitespaces trailing after the first slash. While the RFC says this is ok, we have not
been able to reproduce this behaviour with any real client. Thus, every client showing
this behaviour should be blackholed to the abyss.

3) TCP SYN packets to www.if.ee, port 97. There is no real service in this port. We do
know why it is targeted, but I can't discuss the reasons why. All I can state is that
it's an error on the attackers side :-)

We have no reason to believe that there would be no more variants, it's just a matter of
time when a new one pops out in the open.
```

Figure 26 – Due to a communications mishap, a more detailed version of the letter was accidentally released along with Snort ruleset #2003484.[57] The portions of the text not originally intended for public release are higlighted in red.

Luckily, the malware author either did not find the message in time or was otherwise not anymore in a position to change the attack type. The behaviour described in Figure 26 above is still valid and can be used to accurately identify the Allaple-generated traffic.

---

[40] http://isc.sans.org

At the same time, major anti-virus vendors had created fingerprints to identify the worm. [101] After monitoring the situation for a while, also Microsoft added the signature to its *Malicious Software Removal Tool* (MSRT) on 7 June 2007.[41] It should be noted that a detection signature is added to the MSRT only if the number of infections and the rate of spreading are exceptionally high.

4.3.4 Justice being served

From the early stages on, the plaintiffs were encouraged to file a criminal complaint and to pursue the attacker by legal means. The criminal investigations were carried on in Finland and Estonia independently from the incident response. In cases where a permission to share the information with the law enforcement authorities was granted, CERT-FI surrendered its findings to the police. [126],[117]

The investigations led to one person being arrested in 2008. To the relief of many, this brought the introduction of new malware variants to a complete halt. No new Allaple variants have been released for two years already.

The litigation took place in March 2010. The district court in Tallinn sentenced an Estonian male in his 40s to prison for writing and disseminating the Allaple malware. [48] Based on news sources the person got into dispute with his insurance company in 2006 and decided to craft his revenge.[42]

---

[41] http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Win32%2fAllaple

[42] E.g. http://www.f-secure.com/weblog/archives/00001907.html, http://uudised.err.ee/index.php?06196827 and http://www.postimees.ee/?id=235174

5 Merits and Shortcomings of Current Incident Reporting Approaches

In the previous two chapters we first examined existing normative approaches to reporting NIS incidents and then familiarised ourselves with the current state of play through a selection of transcripts of real-life incidents. We are now qualified to assess the strengths and weaknesses of both these domains.

To begin with, we will discuss the four themes introduced in Sections 3.1 to 3.4, namely incident discovery, identifying points of contacts, report formatting, and assessing the validity of the data exchanged. To complement the discussion, we then devote some time to considering the incident management lifecycle from the viewpoint of learning from the past incidents and devising ways to make incident handling more efficient through information exchange.

5.1 Incident discovery

Remembering Figure 3 on page 11, we suggested that incident investigation can be triggered by anomalies detected by local event monitoring or indirect information acquired from external sources. A striking commonality in the incidents described in Chapter 4 is that none of the targets of the security breaches seemed to have discovered the incidents on their own. Clues from external reporters in one form or another were required either to set the wheels of incident response in motion or at least to complement the victim's limited view of the incident's true scope. While arguably the choice of incidents in Chapter 4 was somewhat arbitrary, it certainly painted a picture of a phenomenon bigger than a single observer acting on his own can ever fathom.

Naturally, an ICT system can only log events that take place within its own domain of control. File system events are local to the computer attached to the data storage. Logon events are limited to systems using the given user database and firewalls only register communications whose paths cross its network interfaces. Local event logging completely misses incidents that take place in remote systems, thus giving no early warning about impending attacks that may exploit similar vulnerabilities existing in the local systems. Local event logging also loses track of incidents once the focus of the attacker's actions has shifted to other systems. This is especially true in cases where information stolen from one system is being spread or exploited in other systems. Even cloud computing does not completely tear down the barriers to event monitoring.

In a truly ideal world, the observer would be in possession of all information relevant to the discovery, subsequent investigation and resolution of an incident. Already in networks much smaller than the internet, the task of logging all events, correctly interpreting anomalies and anticipating attacks becomes a virtual impossibility. This has not hindered standards literature from insisting that each organisation should build internal monitoring systems capable of detecting incidents. While important, local monitoring is not sufficient.

There simply exists no *Panopticon* [5],[60],[49] of internet security incidents to whom to turn and request external monitoring. Instead of having produced the much-feared *"Big Brother"* in the Orwellian sense [75], internet has more likely been evolving in the direc-

tion of Mika Mannermaa's depiction of *"Some Brother Society"* [68]. Instead of a single omnipotent entity monitoring and controlling everything, we have a huge number of independent observers sharing their findings with each other to form composite – yet still limited – windows to the reality.

Contrasting with the discussion on local event monitoring in Section 3.1.1, the use cases involving external observers introduced in Sections 3.1.2 and 3.1.3 were lacking references to the standards. It is as though the notion of an external entity being able to detect incidents would be foreign to standardisation and normative literature. In the absence of support from standards, the idea will be missed by majority of the organisations, too. They continue to see NIS incident reporting and information exchange an extra burden with unquantifiable benefits.

In some ways, it is frustrating to read the incident transcripts in Section 4.2. In these incidents, a number of people had fallen victim to identity theft without possibly ever knowing about it.

Meanwhile, pragmatic approaches manifested e.g. by the continued work of ShadowServer Foundation and development of reporting tools such as Abuse Helper aim to bridge the gap between accidental observers and victims. As it turns out, a seemingly accidental chain of voluntary incident reporters can after all be herded to better the chances of matching the incident-related data with the victims.

Roughly speaking, victims of many common internet threats are nowadays among the last ones to learn about the network and information security incidents affecting them. Changing this would require a change of heart in both NIS standardisation and security objectives of business organisations.

Even the best of parents do not have eyes in their backs. Hence the proverb: it takes a village to raise a child. Translated in the world of NIS incidents, it would take collaboration of *Some Brothers* to spot all incidents.

5.2 Identifying points of contact

In Section 3.2, we interpreted the RFCs listed in Table 1 to suggest that organisations with internet-facing ICT infrastructure would need to develop incident-handling capabilities and be approachable via publicly announced points of contacts. While this may sound self-evident, practice has shown that finding a competent party to report incidents to can at times be complicated or even next to impossible. Section 4 portrayed case studies underlining this. In Section 3.1.3, incident reporting clearing-houses were seen as means to help match victims with information of relevance to the incident.

The case transcripts in Sections 4.1.1 and 4.1.2 featured a German clearing-house actively reaching out to the responsible network administrators. Obviously, for such an approach to be successful on the scale of the whole internet, the recipients' security contacts have to be made publicly available.

As discussed in Section 3.2 earlier, the regional internet registries (RIR) have gradually extended support for identifying incident response contacts. These IRT objects, however, only apply to IP address blocks and autonomous systems and their use is currently not mandatory.

Even worse, the top-level domain (TLD) registries do not require the incident response contacts for the domain names to be documented in WHOIS.

Lastly, RFC 2142 [30] recommends that every internet domain should be reachable via e-mail addresses formed in a standardised manner, security contacts included. Alas, this advice is rarely followed in practice.

An exception to the norm is the approach taken in Finland. The requirement to maintain and publish security contacts for both internet domains [39] and network blocks [40] has been expressly stated in the Finnish telecommunications regulation. Major telecommunications service providers actively participated in the formation of the regulatory text, which has lead to relatively widespread adoption.

In the absence of universally adopted conventions, however, figuring out the security contacts can be next to impossible. Without knowing the security contacts, the sender has two options; either to guess the recipient addresses and blindly send the reports, or to send the reports to addresses found in the WHOIS. The latter is familiar to those poor individuals whose e-mail address has been listed in WHOIS as technical or administrative contacts. Their fate is to end up receiving huge number of e-mails, some possibly security-related but mostly spam.

In response to this problem, RIPE Labs has developed a tool called *Abuse Finder*. [82] The tool combs through the WHOIS database and automatically guesses the incident response contact for a given address. The usability of the tools, however, remains to be seen.

In the meanwhile, CSIRTs have accepted that finding the ultimate contact to send the reports to is not always possible. Instead, as seen in Chapter 4, they are content with identifying the next-in-line incident handlers. The method involves advancing the steps described below until a satisfactory combination of reporting points has been found:

1. *Names*: identify hostnames, names of organisations and popular brands involved in the incident

   → if security contacts for those entities can be found and can be expected to take action based on the information, send report

2. *IP*: identify IP addresses involved in the incident; resolve hostnames to numeric if necessary

   → if security contacts can be found and are known to be capable enough to handle the incident, send report

3. *AS*: associate the IP addresses with the corresponding autonomous systems

   → report the incident to the security contact of the autonomous system and request assistance in finding the ultimate contact

4. *CC*: determine in which country the autonomous system or the brand names are associated

   → identify the national CSIRT or other "CSIRT of last resort2 in that country and request assistance in finding the ultimate contact

5. *Upstream*: determine the network service providers responsible for the upstream communications link

→ report the incident to the security contact of the upstream provider and request assistance in finding the ultimate contact if appropriate

6. *Region*: chart the geographic region neighbouring the country; observe geopolitical and cultural nuances

   → identify national CSIRTs or other trusted resources familiar with the culture and language and request assistance in finding the ultimate contact if appropriate

7. *Publicise*: if no contacts can be found or no response have been received, widen the circulation or make the incident public in the hope of limiting collateral damage. If the primary victim cannot be helped, at least let secondary targets know about the incident

8. *Drop case*: if all options have already been exhausted, drop the case.

A combination of information obtained from public records such as WHOIS and from private databases is used to determine the actual recipients for the report. Some possible scenarios have been presented as examples in Appendix II.

The further we advance along the algorithm described above, the more intermediaries are involved. This increases the risk of information loss while data crosses interfaces. Introducing new intermediate operators also lowers the initiator's and the target's ability to control the process. The more handlers there are in the process, the greater the expected latency. This holds especially true when human intervention is needed.

To conclude the discussion above, at least some level of deliberation by humans will be required when identifying points of contact. This will not change in the foreseeable future unless a concrete change in security priorities permeates the standardisation organisations and nations connected to the internet. The effect of e.g. the European Union initiative on enhancing the role of national CSIRTs remains to be seen. Similarly, the CYBEX framework drafted by ITU-T has potential in bringing the issue of identifying contacts for incident reporting to the attention of standardisation bodies.

5.3 Data exchange formats

In Section 3.3, we gave voice to an assumption that prior to the 21st century there seemed to have been no need for automated incident data exchange. Data format issues may have been unimportant due to the relatively low number of incident reports. For most organisations at the time, the internet was regarded more like an auxiliary service than a critical platform to run serious business on.

The number of users and organisations present in the internet has since risen remarkably. Incident-handling clearing-houses similar to the ones seen in Chapter 4 have been forced to come up with efficient ways to report large amounts of incident data to an unbounded set of recipients.

Earlier, when discussing the standards listed in Table 3 on page 18, we learnt that three standards exist for handling incidents: IODEF, ARF, and CEE. Of these, however, only IODEF is of interest to this study. CEE defines a taxonomy of expressing events in logs, and ARF is limited to registering complaints regarding unsolicited bulk e-mail. Both are

relatively new and their adoption remains to be seen. IODEF on the other hand appears to be mature and already has applications in practical settings.

IODEF enjoys all the benefits and power of XML data formats. The data can be parsed using standard libraries without having to write dedicated software to interpret the incoming data. Human-readable presentation of the data can be treated separate from the actual data contents. The data can be exchanged on practically any type of transport such as e-mail or http. The schema can also be tailored to suit the needs of the application without having to invent altogether new data formats.

While the majority of incidents handled by CERT-FI are still being handled using human-readable data formats, new tools are built to support IODEF from the beginning. Autoreporter [20],[46],[47] supports IODEF as an alternative form of representing the data.[43] Abuse Helper [1], whose development is still under way, sees IODEF as a key component in interorganisational data exchange. If this is in any way a sign of a trend, it can be concluded that the perseverance of TERENA in advancing the adoption of IODEF as an internet standard is finally showing early signs of paying off. The format was first introduced in the RFC series in 2001 and has since been escalated to RFC 5070 with the status of *proposed standard* in 2007.

A separate, yet disturbingly recurrent problem worth bringing up here is the difficulty of interpreting timestamps. IODEF encourages the use of ISO timestamps as defined in RFC 3339. [31],[62] This advice is well-founded as automating the incident handling absolutely requires universally agreed formats for representing dates and times associated with the detection of events and actions taken during the response.

Time zones pose a chronic problem in global information exchange. It is common for the event logs to register timestamps in a local time zone. Irritatingly often, the time zone offset declaration is missing or has been expressed using ambiguous notation. For example, a commonly used expression "PST" can stand for – according to *wikipedia* – three different time zones, namely "Pacific Standard Time," "Pakistan Standard Time," or "Philippine Standard Time." Their corresponding offsets from the normalised UTC time are -8, +5 and +8, respectively. Adding to the confusion is the politically motivated routine of constantly switching back and forth between "daylight saving time" and "normal" time. The switch takes place on different days in various parts of the world. Agreeing on timestamp formatting is obviously something the ICT industry should get to grips with. Tried and tested standards exist already. Alas, they are not always followed in practice.

A non-standard but widely used data format worth mentioning here is the *IP2ASN* [96] (as in "IP to ASN") format developed by Team Cymru. Example of IP2ASN output is displayed in Figure 17 on page 42. IP2ASN is also featured in Appendix II. The format has found loyal user base in the security investigators of major internet operators and CSIRTs. This is probably due to the fact that data is represented in relation to the incident's occurrence in the network. For instance, the network owners can conveniently search for incidents in networks they are responsible for and national CSIRTs can easily pinpoint incidents having ties to their own countries. The information is fitted into a single line of text per host, producing condensed output. Reports involving large num-

---

[43] See Appendix IV for more information.

ber of hosts fit into economical space. The data format is relatively easy to interpret by human handlers while at the same time bulk operations can be effectively performed using basic command line tools such as *grep*, *awk* and *sort*.

The IP2ASN format is not without its problems, however. The incident report in Appendix IV exhibits several of them. Due to the condensed nature of the data format, additional information to describe the surrounding conditions may be needed. The data format is best suited for expressing incidents involving large numbers of internet hosts. The sample incident report only indicates two internet addresses. The resulting report can hardly be claimed condensed if mere two lines of substance are first preceded by 78 lines of explanatory notes! The mix of freeform text and IP2ASN substance can be challenging for the parsers if scripts are used to automate the handling of reports. Unlike with XML-based formats, a parser has to be built for each application from the scratch. In the sample report in Appendix IV, the two lines of substance have been split in the process of signing the message body with PGP. Split lines are difficult to parse with command line tools and are a nuisance when read by humans.

The IP2ASN data format is at its best when used to report large numbers of IP addresses associated with a single incident. For instance, CERT-FI routinely parses through thousands of lines of IP2ASN reports looking for lines associated with Finland. Instead of having to read the list manually, its contents are simply fed into a parsing script to produce a report of incidents of interest to Finland.

Less popular data formats featured in this study include *abuse.py* tool of CERT-FI in Figure 20 on page 44 and those employed by CLEAN MX in e.g. Section 4.1.1. To the knowledge of the author of this study, they are not in widespread use. The *abuse.py* format has been mimicks one by CERT.br of Brazil. The format was determined to be conveniently condensed yet easy to grasp by human eye.

In Section 3.5.2, a project to build a tool called *Abuse Helper* was mentioned. While determined to support IODEF, the project crew has acknowledged that in order for the tool to be useful in practical settings, it has to provide support for existing data formats, too. This would include even the proprietary and obscure ones. What is remarkable about Abuse Helper is that the developer team has tasked itself with approaching the major incident-reporting clearing houses to agree on the best ways to extract data from their repositories. As of writing this study report, the project has identified 11 different clearing houses capable of producing steady streams of incident reporting feeds worth automating and listed 25 additional sources for reporting what they call "malicious IP addresses." [110]

5.4 Assessing the Validity of Incident Reports

So far in our incident handling lifecycle, the incident has been discovered, a decision to inform the affected parties has been made, points of contacts for reporting have been identified, and a written report has been formulated and submitted to the recipients for evaluation. After all this trouble, one would hope that action would follow based on the report. There is still one hurdle to be cleared: the recipient needs to be satisfied that the report description is genuine and that concrete actions would be needed to correct the situation. For the recipient, the report simply represents a claim that something has taken place. If the claim is left unsubstantiated, the report will be discarded.

In Section 3.4.1 we were introduced ways to provide the recipient with technical facts that would help prove the report's correctness. Concepts such as reconstruction and providing pointers to additional information were mentioned. Let us reflect on those concepts by recalling the measures taken by the clearing-house in Sections 4.1.1 and 4.1.2. A German company CLEAN MX had taken the task upon itself of providing ICT system owners with comprehensive dossiers about incidents taking place in their networks.

CLEAN MX appears appreciative of the fact that sending large number of e-mails all over the world would bring practical challenges in getting the message through. Without a doubt, the reporter will be previously unknown to most recipients. Faced with an unpleasant surprise, the recipient may be hesitant in taking actions based on the reports. Having recognised this as a potential problem, CLEAN MX goes to great lengths to ensure a fair amount of evidence will be made available to the recipient for consideration. Figure 8 on page 30 illustrates the richness of evidence collected.

Providing evidence to support the claim through incident reconstruction may seem like a good idea but it is not without its dangers, either. To illustrate a case gone wrong, we can examine a serious incident that took place shortly after Christmas in 2005. A short anonymous message, displayed in Figure 27, containing a URL and a vague warning was posted to the *Bugtraq* mailing list. The posting contained a link that – when followed – infected any Windows-based operating systems with a malware. The malware exploited vulnerability in the Microsoft Windows operating system that practically nobody in the world had immunity over. [65],[103] While the reporter was impossible to identify, the report's validity was relatively easy to verify by merely clicking the link on a system running Microsoft Windows. The downside to this was, naturally, that after clicking the link, users' computers were compromised and needed repair.

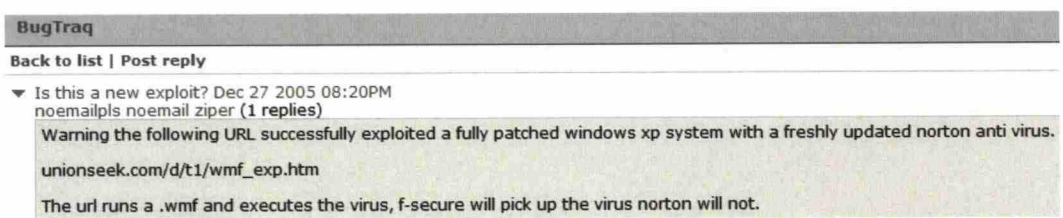

Figure 27 – An anonymous posting[44] to the *Bugtraq* mailing list that launched a race to exploit a Windows vulnerability before it was finally fixed by Microsoft on 5 January 2006[45].

Naturally, rogue incident reports such as the one displayed above should not be encouraged. They are to be expected, though. Incident response teams routinely get e-mails containing malware attachments and links to infection sources with simplistic covering notes along the lines of "Look at this!" This makes it necessary for incident reporting contact points to employ effective controls against ICT systems compromise and means to acquire and preserve evidential information in an effective manner.

We now must continue the discussion on the topic of timestamps already started in the previous section. According to solid ICT operations practices the system clocks should be synchronised in a way to enable meaningful log correlation. [56] As was already dis-

---

[44] http://www.securityfocus.com/archive/1/420288/30/0/threaded
[45] http://www.microsoft.com/technet/security/Bulletin/MS06-001.mspx

cussed on page 31, however, compromised computers commonly suffer from incorrectly set system time, thus potentially rendering the timestamps unusable. Logs obtained from compromised systems should always be treated with caution. System clocks of compromised computers have at times been off by several years even. If a constant offset from the correct time can be determined, this has to be affixed with the logs. According to the experience of CERT-FI, timestamp offsets and system clock accuracy have to be double-checked each time with the reporters.

In addition to presenting compelling evidence to the recipient, CLEAN MX also has another trick to ensure the reports get the attention they deserve. In Sections 4.1.1, and 4.1.2, it was seen that an informational copy was sent to a fallback contact, in this case the national CERT. The rationale is that bringing issues to the attention of impartial coordinators or supervising authorities may help create the positive pressure needed to resolve the problem. The additional recipients would similarly need to establish the report's validity before taking any coordinative actions or exerting any pressure.

In Section 3.4.2 we discussed ways to identify the reporter. Internet standards and CSIRT manuals suggest using PGP signatures for ensuring the message contents have not been tampered with and the message originated from the genuine reporter. Unfortunately, users of PGP are faced with the cruel fact that PGP is virtually unheard-of in circles outside the internet security professionals. To make matters worse, different versions of PGP and its open source counterpart are not entirely compatible with each other. In theory, a message with a broken digital signature should set off alarms and the message should be treated with a healthy dose of suspicion. However, more often than not the e-mail messages are rendered unverifiable by mere character encoding incompatibilities between the sender and the recipient.

It should also be noted that just using PGP or any other kind of message authentication and encryption product is not enough to establish trust between the corresponding parties. The trust building schemes between CSIRTs involve a fair amount of physical meetings, peer audits and introduction of rudimentary rules for information exchange. [37] The groups of trusting CSIRTs make a point in only introducing new members after they have been "sponsored" by trusted persons or organisations. The use of tools such as PGP merely enforces the previously established trust.

Parallel to the system of establishing the reporter's identity is the complementary system of hiding source identities. In Section 4.1.3, we were introduced an anonymising incident-reporting clearing-house. These types of clearing-houses act as a trusted intermediary by hiding the original sources of incident reports. The ultimate recipient can only determine that the report came from a clearing-house and has to trust that the clearing-house exercises quality control over the material obtained from the anonymised sources.

According to the experience of CERT-FI, there is demand for both source and recipient anonymisation. Although not necessarily displayed in case transcripts, it is a common routine for CERT-FI to receive incoming reports on the condition of withholding the reporter's true identity during the subsequent incident coordination. Additionally, CERT-FI routinely protects its clandestine incident response contacts by refusing to surrender the contact details but instead offering to proxy messages.

In many of the incident summary tables in Chapter 4, there are question marks representing the unknowns in the incident coordination and information exchange. Remarkably often the reporter has no knowledge of the incident resolution. Even the trouble

ticket numbers are not necessarily communicated back to the reporter to enable further inquiries.

In Section 3.4.3, we devised three different approaches a reporter can take. These were dubbed opportunistic, iterative and active. Based on the examples covered in Chapter 4, PhishTank can be characterised an opportunistic reporter while CLEAN MX would fit into the active reporter profile. CERT-FI, on the other hand, fluctuated, assuming any of the three approaches depending on case. It is not clear, though, whether CERT-FI's choice of reporting strategy was based on careful deliberation during the incident progression or whether it involved an element of randomness. From the discussions under the topic of unresolved issues in Chapter 4, one can easily verify that important incident details are routinely left unrecorded. One would expect that employing approaches other than the opportunistic one would yield more data for analysis.

5.5 Learning from past incidents

Security controls can be grouped into reactive, proactive, and management measures. [104],[9] Throughout this study, we have been focusing on network and information security through examining reactive measures. This is only natural as, due to causality, incident response first requires a stimulus in form of an attack or a security threat before a response can be initiated.

Efficient incident response helps enhance security in two acts: first, by helping limit damages immediately at the time of an incident and, second, by producing valuable information about the efficiency of pre-existing security controls to be used in future security planning. According to ISO/IEC 27002:

> *"The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, or to be taken into account in the security policy review process [..]."* [56]

Böhme and Moore go even further in suggesting that organisations should adopt a rather conservative approach in investing preventive security measures until observed incidents eventually pinpoint which security investments would bring the greatest returns. [15] Considering this rather radical idea helps highlight the importance of getting constant feedback in the form of lessons learnt from observed security failures.

In Chapter 4, we made an attempt to summarise each case study by compiling tables populated with information accumulated during the incident response. The tables were distinctly "red" in colour, meaning that not enough information was obtained at the time of performing the response. This is a telling feature of incident response – an observer has a limited view on the incident's impact, actions taken by others, and the effectiveness of the response. More information should be collected for the benefit of after-the-fact analysis.

5.6 Enhancing the information exchange

Earlier, we have identified three different incident reporting approaches; opportunistic, iterative and active. Based on the ideas presented in previous section, a conclusion can be made that only iterative or active approaches are able to produce information neces-

sary for the evaluation of the effectiveness of the security controls. Similarly, in their study, Moore and Clayton [69] suggest that the more active approach the reporter chooses, the better results will be yielded in terms of successful takedowns.

Judging by this, the active approach to incident reporting seems to bring the most benefits and should be recommended for result-oriented organisations.

Intuitively, of the three approaches available to incident reporting, the active one ties the most time and effort as the progress of the incident response actions taken by others is monitored all the way through to the final resolution. In order to be a viable solution, the active reporting strategy must be matched with sufficient resourcing. In order to utilise the increased information obtained, efficient documentation procedures must be put in place.

Throughout the Chapter 4, we witnessed several examples of how CERT-FI performed during the response process. We saw successes and failures during the acts of receiving incident reports, performing situation analysis and choosing the most appropriate response strategies.

For instance, we noticed that CERT-FI does not systematically record the incident's persistence, i.e., time between the first occurrence and successful resolution. Currently, there is not enough information in the CERT-FI incident archive to calculate temporal metrics other than the time between the creation and resolution of the incident ticket. In order to obtain more accurate information, CERT-FI would need to get copies of forensic data and actively monitor the progress of takedowns. With the incident volumes steadily growing[46], there is no other choice to enhancing the information exchange but making it more efficient through increased automation. Consequently, CERT-FI has vested interest in the widespread adoption of tools similar to Abuse Helper among CSIRTs all over the world.

Lastly, let us focus on another process challenge earlier identified by CERT-FI and displayed by comparing the three process flows, seen in Figure 28 below, which originally appeared on pages 27, 37 and 41.

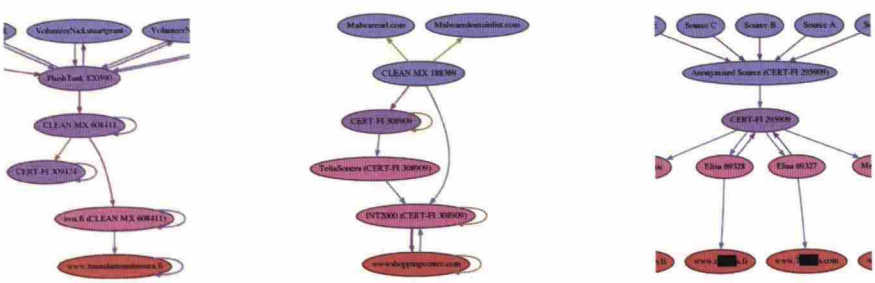

Figure 28 – Choosing the most appropriate incident coordinator role for CERT-FI. From left to right: inaction, escalation, anonymisation. The pictures have been cropped for brevity.

In each of these cases, the duty officer has somehow decided between whether to actively engage in incident coordination or whether to refrain from taking action. However, none of the incident tickets contains documented evidence to support or dispute

[46] http://www.cert.fi/en/reports/statistics.html

the duty officer's decision. The decision seems to have been taken intuitively without subjecting the incident to explicit tests to determine which course of action to take. Although not necessarily displayed in the examples in this study, the decision to choose inaction has sometimes in the past been made based on incomplete information or otherwise erroneously.

As a response to this problem, this study presents a series of tests to determine the role of CERT-FI and the level of action that the handling of an incident would require. The test is portrayed in Table 10 below. The sample table is populated with relevant information acquired from the incident transcribed in section 4.1.4 starting on page 45. It should be noted that due to time restraints, the model has never been tried in practice. This will be taken into future consideration at CERT-FI, however.

Table 10 – A series of tests used to help determine CERT-FI's role in the incident coordination and to choose the most appropriate incident reporting approach. The test has be prepopulated with information obtained from [FICORA #307761] examined in Section 4.1.4.

Attributes for Incident [FICORA #307761]	
Reporter's Identity Established?	[ ] Reporting party unknown [ ] Reporter's personal Identity not known [X] Organisational affiliation known: F-Secure Lab (weak authentication) [ ] Own investigation
Reporter Trusted?	[ ] Not trusted [ ] Personal trust established [X] Organisational trust established: previously agreed arrangement [ ] Implicit trust (no need to verify report's accuracy)
Claim Provable?	[ ] Claim not provable, no evidence presented [ ] Claim plausible, limited evidence presented [X] Claim demonstrated, conditions apply: sample successfully downloaded [ ] Claim fully demonstrated
Target's Nationality	[ ] Not known [X] Foreign, non-EU: the US [ ] Foreign, EU [ ] Finnish, non-CNI [ ] Finnish, part of CNI
Incident Categorisation	[X] Malware [X] Computer break-in or misuse [ ] Denial of service [ ] Social engineering, e.g. phishing [ ] Spam [ ] Vulnerability [ ] Other (please specify)
Poses a Threat to Finnish Interests?	[ ] Not known [ ] None [X] Indirect [ ] Direct and imminent
Information Actionable?	[ ] Not known [ ] Not [X] By an external: ISP and US-CERT [ ] By CERT-FI
Action Required by CERT-FI?	[ ] Not known (in case threat is direct and imminent, must act) [ ] Not [X] Likely: Incident probably not known by the target [ ] Highly recommended [ ] Must act (legal obligation)
Type of Action Required	[X] Request assistance: ISP X and Victim [X] Inform: US-CERT [ ] Assign authority orders
Permission to Act?	[ ] Not known [ ] Not [ ] Restrictions apply [X] Implicit permission: previously agreed arrangement (TLP: WHITE) [ ] Explicit permission [ ] Legal mandate or obligation to act

6 Conclusion

This study is an effort to combine a review of normative literature with a collection of case studies to produce an informed opinion of the state of play in the field of network and information security incident reporting. Information security standards and authoritative publications were contrasted with transcripts of real-life incidents. This was done with the idea to find how far apart the two worlds are from each other.

6.1 Key findings

In the introduction in Chapter 1, we anticipated that the difficulties in incident response lie in inter-organisational cooperation and poor communication. The incident examples clearly confirmed this assertion. A lack of support in standards to address this apparent omission makes our discovery ever more urgent. Following this, four key findings can be extracted in this study.

6.1.1 Incidents can be detected by outside parties

The case studies in this study report helped underline the fact that there is a discontinuation in the way incidents are being discovered and who they target. The victims are often among the last ones to learn about the incident, while at the same time perfect strangers can detect them without an effort.

This underlines the importance of an agnostic approach to the sources of incident reports. By refusing to accept reports from outsiders, the organisation risks missing important information about its own security weaknesses.

6.1.2 Finding correct incident reporting contacts is challenging

Internet registries have only recently discovered that they could have a role to play in helping people determine who is responsible for handling information security breaches in various parts of the internet. It is rather remarkable that this has not happened earlier, as the delay has helped produce black spots in the internet where malicious activities go often unnoticed for long periods of time.

In the meanwhile, the incident discoverers have teamed up to form incident-reporting clearing-houses. Some of the clearing-houses have created automated methods to inform the affected parties about incidents, which has spelled increase in the incident reports received by those whose security contacts can be identified. Some of the clearing-houses choose to make their findings public in frustration or surrender the material to other incident aggregators in order to be delivered to competent network owners.

Incident-reporting clearing-houses are invaluable as they perform the task that otherwise would belong to nobody. That is, they help the incident discoverers reach the victims affected by the incidents.

6.1.3 Incident reporting not fully understood in standards literature

Earlier efforts to standardise information security processes in the internet have succeeded in producing a couple of well-meaning RFC documents emphasising the importance of maintaining incident response capability within the organisations. Incident reporting is a policy issue and the RFCs are better suited for protocol documentation, which has caused these RFCs to somewhat miss their mark.

The study found ISO/IEC 27002 and IETF RFC 5070 to be the prime examples of standards with a say in incident response and reporting. The ISO standard describes the management system level requirements and justification for incident response and the RFC provides a way to automate the processing and exchange of incident-related data.

The standards literature has yet, however, to discover the importance of complementing local event monitoring with reports received from external sources. The notion of having to base security procedures partly on data from unknown sources fits rather poorly with the well-defined and controllable world of standardisation.

6.1.4 Automation not fully exploited in incident reporting

The everyday business of incident reporting and requesting takedowns of malicious content still largely relies on human-to-human e-mail correspondence. The current automated tools do not quite hit the target by being content with producing and sending large amounts of human-readable reports in an automated fashion or by automating the parsing of incoming human-readable material. There are existing standards capable of automating the whole exchange of incident-related material, but they are heavily underused, as they have not yet been translated into products.

Due to the incident response being a holistic process, the need for human correspondence never totally ceases. However, the aim should be in computer-aided human communications and seeking ways to support iterative information exchange and ad-hoc communications paths.

6.2 Open issues for further studies

This study demonstrated that the incident transcripts can be used to identify process deficiencies and certainly contain valuable information worth analysing in more detail. Creating visualisation techniques for expressing the flow of incident-related information and highlighting critical decision points has potential for moving the incident analysis on a higher level of abstraction.

The interplay between the incident-reporting clearing-houses, CSIRTs and network owners was described briefly. It would be interesting to learn how *Abuse Helper*, once completed, enhances the information flow and how the actors' roles change as a result.

The related effectiveness of the three incident-reporting approaches identified in Section 3.4.3 would need to be examined in detail. Additionally, the test described in Table 10 for choosing the most appropriate incident coordination strategy would deserve a test drive.

In Appendix II, a walk-through of rudimentary tools to preserve information about the volatile network configuration was presented. An in-depth study on the advanced usage

scenarios of similar tools would provide CSIRTs around the world with a reference manual into investigative use of internet.

This study steered away from the legal considerations that must necessarily be taken into account when dealing with cross-border information exchange and investigating criminal acts taking place in the internet. The study would need to be interdisciplinary for the purpose of bridging the legal and technical worldviews.

Lastly, there still is a genuine need for standardising network and information security incident response. In order to choose the best possible strategy and standardisation body, more information than presented here would be needed. In particular, the development of the ITU-T CYBEX framework calls for additional research to identify demands and practical limitations in the information exchange.

References

List of References

[1] AbuseHelper project pages on Google Code [referenced 2010-05-27]

URL: http://code.google.com/p/abusehelper/

URL: http://code.google.com/p/abusehelper/wiki/README

[2] American Registry for Internet Numbers ARIN, Introduction to ARIN's database [referenced 2010-05-02]

URL: https://www.arin.net/knowledge/database.html#abusepoc

[3] Arvidsson, J., Cormack, A., Demchenko, Y., Meijer, J., '*RFC 3067: TERENA's Incident Object Description and Exchange Format Requirements*', Internet Engineering Task Force, 2/2001

[4] Asia Pacific Computer Emergency Response Team (APCERT), Member Teams [referenced 2010-05-02]

URL: http://www.apcert.org/about/structure/members.html

[5] Bentham, J., Bowring, J., *'The works of Jeremy Bentham – Volume 4 of The Works of Jeremy Bentham: Published Under the Superintendence of His Executor John Bowring*', William Tait, London 1843, 594 p., digitized by Google, Inc. 2008 [referenced 2010-04-28]

[6] BFK edv-consulting GmbH, Passive DNS replication report for '212.94.64.154' [referenced 2010-03-21]

URL: http://www.bfk.de/bfk_dnslogger.html?query=212.94.64.154#result

[7] Bradner, S., '*RFC 2026 (BCP 9): The Internet Standards Process -- Revision 3*', Internet Engineering Task Force, October 1996

[8] Bronk, H., Thorbruegge, M., Hakkaja, M., '*A basic collection of good practices for running a CSIRT*', ENISA Deliverable WP2007/2.4.9/1 (CERT-D3.1: Collecting good practices for quality assurance for CERTs), 12/2007, 86 p.

URL: http://www.enisa.europa.eu/act/cert/support/guide2/files/a-collection-of-good-practice-for-cert-quality-assurance

[9] Bronk, H., Thorbruegge, M., Hakkaja, M., '*A step-by-step approach on how to set up a CSIRT: Including examples and checklist in form of a project plan*', ENISA Deliverable WP2006/5.1(CERT-D1/D2), 12/2006, 85 p.

URL: http://www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide

[10] Brownlee, N., Guttman, E., '*RFC 2350 (BCP 21): Expectations for Computer Security Incident Response*', Internet Engineering Task Force, June 1998

[11] Brunner, E., Suter, M., '*International CIIP Handbook 2008/2009, An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*', Center for Security Studies, ETH Zurich, September 2008, 648 p.

[12] Bryk, H., '*National and Government CSIRTs in Europe, Study Conducted by CERT-FI*', October 2009

URL: http://www.cert.fi/en/reports/2009/certfistudyonnationalandgovernmentalcsirtsineurope.html

[13] Bryk, H., '*A study among certain European computer security incident response teams and application of good practices in Finnish Communication Regulatory Authority*', Helsinki University of Technology, Espoo, Finland, December 2008, 84 p. [in Finnish, contains English abstract]

[14] Burch, H., Manion, A., Ito, Y., '*Vulnerability Response Decision Assistance*', Software Engineering Institute, Carnegie Mellon University, July 2008

[15] Böhme, R., Moore, T., '*The Iterated Weakest Link: A Model of Adaptive Security Investment*', Workshop on the Economics of Information Security (WEIS), 2009

URL: http://weis09.infosecon.net/files/152/paper152.pdf

[16] CERT Coordination Center, Authorized Users of "CERT" [referenced 2010-02-28]

URL: http://www.cert.org/csirts/cert_authorized.html

[17] CERT Coordination Center, CSIRT FAQ [referenced 2010-04-15]

URL: http://www.cert.org/csirts/csirt_faq.html

[18] CERT Coordination Center, CSIRTs with National Responsibility [referenced 2010-03-21]

URL: http://www.cert.org/csirts/national/

[19] CERT Coordination Center, '*Finding Site Contacts*' (historic document), 5/1999 [referenced 2010-03-07]

URL: http://www.cert.org/tech_tips/finding_site_contacts.html

[20] CERT-FI, Autoreporter Statistics Page [referenced 2010-02-28]

URL: http://www.cert.fi/en/reports/statistics/autoreporter.html

[21] CERT-FI, CERT-FI Annual Report 2007

URL: http://www.cert.fi/attachments/tietoturvakatsaukset/5v5bo4KzA/CERT-FI_annual_report_2007.pdf

[22] CERT-FI, A chronological listing of advisories and alerts with association to [CERT-FI: 36789] [116], publicised between 13 – 19 October 2007 [in Finnish]

URL: http://www.cert.fi/tietoturvanyt/2007/10/P_5.html,
http://www.cert.fi/varoitukset/2007/varoitus-2007-7.html,
http://www.cert.fi/tietoturvanyt/2007/10/P_6.html,
http://www.cert.fi/tietoturvanyt/2007/10/P_7.html,
http://www.cert.fi/tietoturvanyt/2007/10/P_8.html,
http://www.cert.fi/tietoturvanyt/2007/10/P_9.html,
http://www.cert.fi/tietoturvanyt/2007/10/P_12.html,
http://www.cert.fi/tietoturvanyt/2007/10/P_13.html,
http://www.cert.fi/tietoturvanyt/2007/10/P_16.html,

http://www.cert.fi/tietoturvanyt/2007/10/P_19.html,
http://www.cert.fi/tietoturvanyt/2007/10/P_20.html

[23] CERT-FI, '*SQL injection -hyökkäysten havaitseminen*', Tietoturva nyt! blog entry, November 2007 [in Finnish]

URL: http://www.cert.fi/tietoturvanyt/2007/10/P_14.html

[24] CERT-FI, '*Vulnerability coordination policy*', January 2010 [referenced 2010-05-01]

URL: http://www.cert.fi/en/activities/Vulncoord/vulncoord-policy.html

[25] Cisco Systems, Inc., Cisco IronPort SenderBase report of '212.94.64.154' [referenced 2010-03-21]

URL: http://www.senderbase.org/senderbase_queries/detailip?search_string=212.94.64.154

[26] Commission to the European Communities, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - '*Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*', COM(2009) 149 final, Brussels March 2009, 11 p.

[27] Common Criteria for Information Technology Security Evaluation, '*Part 2: Security functional components*', Version 3.1, Revision 3, Final (CCMB-2009-07-002), July 2009

[28] Cormack, A., Stikvoort, D., Woeber, W., Robachevsky, A., '*IRT Object in the RIPE Database*', ripe-254, July 2002 [referenced 2010-03-01]

URL: http://www.ripe.net/docs/ripe-254.html

[29] Cover, R. (editor), '*Incident Object Description and Exchange Format (IODEF)*', Cover Pages [referenced 2010-02-28]

URL: http://xml.coverpages.org/iodef.html

[30] Crocker, S., '*RFC 2142: Mailbox Names for Common Services, Roles and Functions*', Internet Engineering Task Force, May 1997

[31] Danyliw, R., Meijer, J., Demchenko, Y., '*RFC 5070: The Incident Object Description Exchange Format*', Internet Engineering Task Force, February 2007

[32] Dörges, T., '*Information Security Exchange Formats and Standards*', Slides for the presentation held during FIRST 2009 Conference in Kyoto, July 2009

[33] Eronen, J., '*A collaborative method for assessing the dependencies of critical information infrastructures*', University of Oulu, Oulu, Finland, 2006, 79 p.

[34] Eronen J., Röning J. '*Graphingwiki - a Semantic Wiki extension for visualising and inferring protocol dependency*'. Paper presented in the First Workshop on Semantic Wikis "SemWiki2006 - From Wiki to Semantics," co-located with the 3rd Annual European Semantic Web Conference (ESWC), Budva, Montenegro, 11th - 14th June, 2006, 15 p.

URL: https://www.ee.oulu.fi/research/ouspg/PROTOS_SemWiki2006

[35] European Network and Information Security Agency (ENISA), ENISA's work in the field of CERTs / CSIRTs, ENISA's homepage [referenced 2010-03-03]

URL: http://www.enisa.europa.eu/act/cert

[36] European Network and Information Security Agency (ENISA), Glossary for the most important telecommunications' resilience terms [referenced 2010-04-26]

URL: http://www.enisa.europa.eu/act/res/files/glossary

[37] European Network and Information Security Agency (ENISA), '*Good Practice Guide: Network Security Information Exchanges*', June 2009, 49 p.

[38] European Network and Information Security Agency (ENISA), Inventory of CERT activities in Europe, version 1.9, November 2009 [referenced 2010-03-01]

URL: http://www.enisa.europa.eu/act/cert/background/inv/files/inventory-of-cert-activities-in-europe

[39] Finnish Communications Regulatory Authority, '*Regulation 11 A/2008 M: On information security and functionality of e-mail services*', Helsinki September 2008 [unofficial English translation]

[40] Finnish Communications Regulatory Authority, '*Regulation 13 A/2008 M: On information security and functionality of Internet access services*', Helsinki September 2008 [unofficial English translation]

[41] Finnish Parliament, 'Act on the Protection of Privacy in Electronic Communications 516/2004', 2004 [unofficial English translation]

[42] Forum of Incident Response and Security Teams (FIRST), Alphabetical list of FIRST Members [referenced 2010-03-21]

URL: http://www.first.org/members/teams/

[43] Fraser, B., '*RFC 2196: Site Security Handbook*', Internet Engineering Task Force, September 1997

[44] Gerhards, R., '*RFC 5424: The Syslog Protocol*', Internet Engineering Task Force, March 2009

[45] Grance, T., Kent, K., Kim, B., '*Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology*', NIST Special Publication 800-61, January 2004, 148 p.

[46] Grenman, T., '*Autoreporter – Keeping the Finnish Network Space Secure*', CERT-FI, June 2009 [referenced 2010-05-02]

URL: http://www.cert.fi/attachments/5hy9xPcNt/Autoreporter.pdf

URL: http://www.cert.org/csirts/national/contest_2009.html

[47] Grenman, T., '*Autoreporter – Keeping the Finnish Network Space Secure*', ENISA Quarterly Report Vol. 5, No. 1, Jan-Apr 2009, pp. 12 – 13 [referenced 2010-02-28]

[48] Harju Maakohus (Harju District Court), Court decision in criminal case 1-09-3476 (07221000080), judge Julia Vernikova, Tallinn, March 2010 [in Estonian]

[49] Heinonen, R., Hannula, I., '*Valvonta tietoyhteiskunnassa*', Edita, Helsinki 1999, 181 p. [in Finnish]

[50] Honeynet Project, '*Know Your Enemy: Honeynets. What a honeynet is, its value, overview of how it works, and risk/issues involved*', May 2006 [referenced 2010-03-28]

URL: http://old.honeynet.org/papers/honeynet/

[51] Howard, J., D., Longstaff, T., A., '*A Common Language for Computer Security Incidents*', Sandia National Laboratories, 1998, 26 p.

[52] International Secure Systems Lab, FIRE (FInding RoguE Networks) report on 'AS5515' [referenced 2010-03-21]

URL: http://maliciousnetworks.org/chart.php?as=AS5515

[53] Internet Storm Center, '*Allaple worm*', a diary article #2451, March 2007

URL: http://isc.sans.org/diary.html?storyid=2451

[54] ISO/IEC TR 18044:2004(E), '*Information technology — Security techniques — Information security incident management*', Technical report, First edition, October 2004

[55] ISO/IEC 27001:2005(E), '*Information technology. Security techniques. Information security management systems. Requirements', International standard, First edition, October 2005*

[56] ISO/IEC 27002:2005(E), '*Information technology — Security techniques — Code of practice for information security management*', International standard, First edition, June 2005

[57] Jonkman, M., '*ET WORM Allaple Unique HTTP Request - Possibly part of DDOS*', Emerging Threats attack signature #2003484, revisions 1 – 8, March 2007 – September 2008

URL: http://doc.emergingthreats.net/bin/view/Main/2003484

[58] Khurana, H., Basney, J., Bakht, M., Freemon, M., Welch, V., Butler R., '*Palantir: A Framework for Collaborative Incident Response and Investigation*', pp. 38-51 of the Proceedings of the 8th Symposium on Identity and Trust on the Internet, Gaithersburg, Maryland, 2009

[59] Killalea, T., '*RFC 3013 (BCP 46): Recommended Internet Service Provider Security Services and Procedures*', Internet Engineering Task Force, October 2000

[60] Kimble, C., '*Control and Surveillance*', Chapter 7 of the course material of an undergraduate level course "CIS (Computers In Society)" taught between 1995 and 1999 [referenced 2010-04-28]

URL: http://www.chris-kimble.com/Courses/cis/cis7.html

[61] Klensin, J., '*RFC 4084 (BCP 104): Terminology for Describing Internet Connectivity*', Internet Engineering Task Force, May 2005

[62] Klyne, G., Newman, C., '*RFC 3339: Date and Time on the Internet: Timestamps*', Internet Engineering Task Force, July 2002

[63] Knecht, T., '*prop-079: Abuse contact information, version 3*', March 2010 [referenced 2010-03-21]

URL: http://www.apnic.net/policy/proposals/prop-079

URL: http://meetings.apnic.net/__data/assets/pdf_file/0006/18429/crocker-prop-079.pdf

[64] Latin American and Caribbean Internet Addresses Registry LACNIC, '*LACNIC Policy Manual (v1.3 - 07/11/2009)*', 3. Allocation of Autonomous System Numbers (ASN) [referenced 2010-03-03]

URL: http://lacnic.net/en/politicas/manual4.html

[65] Lindholm, J., '*Mikko Hyppösen paha päivä*', Suomen kuvalehti 41/2006, November 2006 [in Finnish only]

[66] Livingood, J., Mody, N., O'Reirdan, M., *'Internet-Draft: Recommendations for the Remediation of Bots in ISP Networks*', version 7, Internet Engineering Task Force, February 2009 (expires August 2010) [referenced 2010-03-31]

URL: https://datatracker.ietf.org/doc/draft-oreirdan-mody-bot-remediation/

[67] Lonvick, C., '*RFC 3164: The BSD syslog Protocol*', Internet Engineering Task Force, August 2001

[68] Mannermaa, M., '*JOKUVELI. Elämä ja vaikuttaminen ubiikkiyhteiskunnassa*', WsoyPro, Juva, 2008, 244 p. [in Finnish only]

[69] Moore, T., Clayton, R., '*The Impact of Incentives on Notice and Take-down*', Proceedings of the Seventh Workshop on the Economics of Information Security (WEIS 2008), June 2008

[70] National Bureau of Investigation press statement, '*Salasanamurtojen tutkinta käynnistynyt*', 15 October 2007 [in Finnish only]

URL: http://www.poliisi.fi/poliisi/krp/home.nsf/headlinesfin/F92F546EE8744753C22573750049CCE5?opendocument

[71] National Bureau of Investigation press statement, '*Salasanamurtojutussa pidätys*', 18 October 2007 [in Finnish only]

URL: http://www.poliisi.fi/poliisi/krp/home.nsf/headlinesfin/A4896071018FB264C22573780046EFD4?opendocument

[72] National Computer Security Center, '*Department of Defense Trusted Computer Security Evaluation Criteria (DoD 5200.28-STD)*', December 1985

[73] NETpilot GmbH, CLEAN MX realtime database, Evidence collected for incident #608411 [referenced 2010-03-14]

URL: http://support.clean-mx.com/clean-mx/phishing.php?domain=tuusulantennisseura.fi&response=

URL: http://support.clean-mx.com/clean-mx/evidence/error.608411.txt

[74] OpenDNS, LLC., PhishTank Submission #820590, Submitted Sep 19th 2009 4:41 PM [referenced 2010-02-14]

URL: http://www.phishtank.com/phish_detail.php?phish_id=820590

[75] Orwell, G., '*Nineteen Eighty-Four*', Secker and Warburg, London, June 1949, 326 p.

[76] Palojärvi, P., '*A battle in bits anf bytes: Computer network attacks and the law of armed conflict*', Erik Castrén Institute Research Reports 27/2009, Hakapaino Oy, Helsinki 2009, 186 p.

[77] Pethia, R., Crocker, S., Fraser, B., '*RFC 1281: Guidelines for the Secure Operation of the Internet*', Internet Engineering Task Force, 10/1991

[78] Porvoo magistrate's court, Decision 09/863 in criminal case R 09/446, September 2009 [only available in Finnish: Porvoon käräjäoikeus, tuomio 09/863 asiassa R 09/446, 18.9.2009]

[79] Provos, N., 'Safe Browsing Diagnostic To The Rescue', Google Online Security Blog 2008 [referenced 2009-10-31]

URL associated with Section 4.1.1.2:
http://safebrowsing.clients.google.com/safebrowsing/diagnostic?site=AS:5515

[80] Radatz, J. (editor), '*The IEEE Standard Dictionary of Electrical and Electronics Terms*', Sixth Edition, Institute of Electrical and Electronics Engineers, Inc., New York, NY, 1996

[81] Rajnovic, D., Forum of Information Response and Security Teams (FIRST) web page for ITU-T/CYBEX Framework [referenced 2010-02-28]

URL: http://first.org/global/standardisation/cybex/index.html

[82] RIPE Labs, '*Find Abuse Handler Details Using the Abuse Finder*', an article posted on the Tools section of RIPE Labs by Paul P., April 2010 [referenced 2010-04-29]

URL: http://labs.ripe.net/content/abuse-finder

[83] RIPE NCC, '*RIPE Database Query Reference Manual*' [referenced 2010-03-03]

URL: http://www.ripe.net/db/support/query-reference-manual.pdf

[84] RIPE NCC, RIPE Database Search for '212.94.64.154' [referenced 2010-03-21]

URL: http://www.db.ripe.net/whois?form_type=simple&full_query_string=&searchtext=212.94.64.154&submit.x=0&submit.y=0&submit=Search

[85] Rutkowski T. (Q.4/17 Rapporteur), '*Proposed initial draft text for Rec. ITU-T X.cybex, Cybersecurity information exchange framework*', Study Group 17, TD 0503 Rev.1, 16-25 September 2009

[86] RFC Editor, Official Internet Protocol Standards [referenced 2010-02-28]

URL: http://www.rfc-editor.org/rfcxx00.html

[87] RFC Editor, RFC Tutorial Slides, IETF 76, Hiroshima, Japan, 8 November 2009 [referenced 2010-02-28]

URL: ftp://ftp.rfc-editor.org/in-notes/rfc-editor/tutorial.latest.pdf

[88] Roesch, M., '*Snort - Lightweight Intrusion Detection for Networks*', Proceedings of LISA '99: 13 Systems Administration Conference, Seattle, Washington, USA, November 1999, pp. 229–238

[89] Ruefle, R. Rajnovic, D., '*FIRST Site Visit Requirements and Assessment*', version 1.0, 4/2006, 22 p. [referenced 2010-04-17]

URL: http://www.first.org/membership/site-visit-V1.0.pdf

[90] S-Cure, '*Trusted Introducer for CSIRTs in Europe, Appendix B: Information Template for "accredited" CSIRTs*', version 4.0, 5/2009 [referenced 2010-04-17]

URL: http://www.trusted-introducer.org/ti_process/Invitation-Package-Appendices.pdf

[91] SANS Institute, '*Intrusion Detection FAQ*' [referenced 2010-03-07]

URL: http://www.sans.org/security-resources/idfaq/

[92] Shafranovich, Y., Levine, J., Kucherawy, M., '*Internet-Draft: An Extensible Format for Email Feedback Reports*', version 4, MARF Working Group, April 2010 (Expires November 2010) [referenced 2010-05-03]

URL: https://datatracker.ietf.org/doc/draft-ietf-marf-base/

[93] Shirey, R., '*RFC 2828: Internet Security Glossary*', Internet Engineering Task Force, 5/2000

[94] Sundaram, A., An Introduction to Intrusion Detection, 1996 [referenced 2010-03-07]

URL: http://www.acm.org/crossroads/xrds2-4/intrus.html

[95] Swift, D., '*A Practical Application of SIM/SEM/SIEM Automating Threat Identification*', SANS Institute InfoSec Reading Room, December 2006, 38 p.

[96] Team Cymru, Inc., '*IP to ASN Mapping*' [referenced 2010-03-21]

URL: http://www.team-cymru.org/Services/ip-to-asn.html#whois

[97] The Pirate Bay, '*78 000 passwords (from finnish sites) by. tmpb & zeropoint*', a torrent file to '78kfinnpwhashes.zip' [referenced 2010-03-21]

URL: http://thepiratebay.org/torrent/3838998/78_000_passwords_%28from_finnish_sites%29_by._tmpb__amp__zeropoint

[98] Tikk, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm, A., Vihul, L., '*Cyber Attacks Against Georgia: Legal Lessons Identified*', NATO Unclassified, Version 1.0, Cooperative Cyber Defence Centre of Excellence, Tallinn November 2008

URL: http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

[99] Tikk, E., Kaska, K., Vihul, L., '*International Cyber Incidents: Legal Considerations*', Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn 2010

[100] Trusted Introducer (TI), Team Info, Listed Teams by Name [referenced 2010-03-01]

URL: https://www.trusted-introducer.org/teams/alpha_LICSA.html

[101] Virus Bulletin, '*Prevalence Table – May 2007*', on page 3 of July 2007 issue

[102] Virustotal.com, '*File 188369 received on 2009.09.13 18:53:27 (UTC)*', MD5: f4d12f2e6ed87a7ae818a9e359342821, Heuristic.BehavesLike.JS.CodeUnfolding.B, Trojan.Script.191677 HTML/Crypted.Gen. An automated analysis of a malware sample involved with incident [FICORA #308909]

URL:
http://www.virustotal.com/analisis/32b9ea3acdbd54180f429c35d01523e73778cb9acf48a65d698cbcb94f83bba1-1252868007

[103] Voorhees, J., '*The December Storm of WMF: Preparation, Identification, and Containment of Exploits*', SANS Institute, October 2006, 74 p.

URL: http://www.sans.org/reading_room/whitepapers/honors/december-storm-wmf-preparation-identification-containment-exploits_1666

[104] West-Brown, M. J., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., Zajicek, M., 'Handbook for Computer Security Incident Response Teams (CSIRTs)', 2nd Edition, 4/2003, 200 p.

URL: http://www.cert.org/archive/pdf/csirt-handbook.pdf

List of Interviews and Anecdotal References

[105] Eronen, J., Information Security Adviser, CERT-FI, A remark made during oral reporting on November 2007 of a visit to various international vulnerability handling partners, Finnish Communications Regulatory Authority, Itämerenkatu 3 A, Helsinki.

[106] Kiuru, A., Information Security Adviser, CERT-FI, IRC correspondence on 28 April 2010

[107] Lehmuskallio, A., Security Manager, TeliaSonera Finland Oyj, Interview conducted on 23 March 2007 during Teleware Technical Security Forum, Laajalahdentie 23, Helsinki

[108] Pahlman S., Information Security Adviser, CERT-FI, E-mail correspondence on 28 April 2010, '*Kommentteja DI-työstä*'

[109] Thorbruegge, M., Senior Expert for Computer Security and Incident Response, European Network and Information Security Agency (ENISA), E-mail correspondence between 23 and 26 April 2010: '*Is there a definition for the term 'NIS' somewhere?*'

List of Non-Public References

[110] AbuseHelper, Project documentation found on the developer extranet [referenced 2010-05-04]

[111] Bryk, H., '*Survey on certain European CSIRT teams' administration, operations, co-operation and communications, Part 1: Summary*', Finnish Communications Regulatory Authority 838/69/2009, Helsinki March 2009, 18 p.

[112] Bryk, H., '*Survey on certain European CSIRT teams' administration, operations, co-operation and communications, Part 2: Team reports*', Finnish Communications Regulatory Authority 838/69/2009, Helsinki January 2009, 70 p.

[113] CERT-FI Incident Ticket [CERT-FI: 19608], Incident Category: Denial of Service, 30 June 2006 – 29 June 2007

[114] CERT-FI Incident Ticket [CERT-FI: 25462], Incident Category: Denial of Service, 26 October 2006

[115] CERT-FI Incident Ticket [CERT-FI: 25902], Incident Category: Denial of Service, 17 – 24 October 2006

[116] CERT-FI Incident Ticket [CERT-FI: 36789], Incident Category: Computer Break-in, 13 October – 17 December 2007

[117] CERT-FI Incident Ticket [CERT-FI: 46580], Incident Category: Malware, 12 December 2007 – 2 January 2008

[118] CERT-FI Incident Ticket [FICORA #295909], Incident Category: Malware, 17 – 21 August 2009

[119] CERT-FI Incident Ticket [FICORA #307761], Incident Category: Malware, 16 – 21 September 2009

[120] CERT-FI Incident Ticket [FICORA #308909], Incident Category: Social Engineering, 20 – 25 September 2009

[121] CERT-FI Incident Ticket [FICORA #309474], Incident Category: Social Engineering, 20 September 2009

[122] CERT-FI Incident Ticket [FICORA #378078], Incident Category: Handled by Autoreporter, 28 April 2010

[123] EGC Emergency Contact Information

[124] Forum of Incident Response and Security Teams FIRST (members section) [referenced 2010-03-31]

[125] Centre for the Protection of National Infrastructure (CPNI), *'International CIIP Directory, Issue 21*', September 2009, 215 p.

[126] Koivunen, T., '*Analysis on W32/Rachack malware*', November 2006

[127] Trusted Introducer list of "Accredited" Teams (members section) [referenced 2010-03-31]

List of Figures

List of Tables

Appendices

Appendix I Pointers to standards listed in Table 3 on page 18

Name	Short name	URL
Common Attack Pattern Enumeration and Classification	CAPEC	http://capec.mitre.org/
Common Configuration Enumeration	CCE	http://cce.mitre.org/
Common Information Model	CIM	http://www.dmtf.org/standards/cim/
Common Model of System Information	CMSI	http://www.cert-verbund.de/cmsi/
Common Platform Enumeration	CPE	http://cpe.mitre.org/
Common Result Format	CRF	http://makingsecuritymeasurable.mitre.org/crf/
Default Password Enumeration	DPE	http://www.security-database.com/dpe.php
Open Vulnerability & Assessment Language	OVAL	http://oval.mitre.org/
Extensible Configuration Checklist Description Format	XCCDF	http://scap.nist.gov/specifications/xccdf/
Common Vulnerabilities and Exposures	CVE	http://cve.mitre.org/
Common Vulnerability Scoring System	CVSS	http://www.first.org/cvss/
Vulnerability and Exploit Description and Exchange Format	VEDEF	N/A
Vulnerability and Exposure Markup Language	VuXML	http://www.vuxml.org/
OASIS Application Vulnerability Description Language TC	AVDL	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=avdl
Common Announcement Interchange Format	CAIF	http://www.caif.info/
Deutsches Advisory Format	DAF	http://www.cert-verbund.de/daf/index.html
European Information Security Promotion Programme (EISPP) advisory format		http://www.eispp.org/
Common Weakness Enumeration	CWE	http://cwe.mitre.org/
Common Malware Enumeration	CME	http://cme.mitre.org/
Malware Attribute Enumeration and Characterization	MAEC	https://buildsecurityin.us-cert.gov/swa/malact.html
Intrusion Detection Msg. Exchange Format	IDMEF	http://tools.ietf.org/html/rfc4765
Intrusion Detection Exchange Protocol	IDXP	http://tools.ietf.org/html/rfc4767
Incident Object Description Exchange Format [31]	IODEF, RFC 5070	http://www.ietf.org/rfc/rfc5070.txt
Abuse Reporting Format [92]	ARF	http://www.shaftek.org/publications/drafts/abuse-report/
Common Event Expression	CEE	http://cee.mitre.org/
Security Content Automation Protocol	SCAP	http://scap.nist.gov/

Appendix II Example of Using Public WHOIS Records to Identify Point of Contact Responsible for Security on an Internet Address

Below is a collection of information obtained from public records while trying to determine to whom the NIS incident report should be sent. Following an imaginary incident involving the web site of Aalto University, we start our search from 'www.aalto.fi'.

The reader should be advised that WHOIS output is coloured for readability. Text in blue are commands and the portions of the output most relevant are coloured in red. Portions that are deemed uninteresting in the purpose of finding the contacts in this instance are typed in grey.

In this example, we find out that according to the WHOIS records, the responsible organisation for the Aalto University's web site is *Teknillinen korkeakoulu*, or *Helsinki University of Technology*, which turns out to be its name in English. The DNS forward and reverse lookups reveal the same mismatch – in this case the mismatch is not indicative of malicious activity but rather a consequence of recent creation of Aalto University.

While performing a query against RIPE WHOIS service we find the IRT object described in Section 3.2. Under typical circumstances, the best bet would be to send the incident reports and takedown requests to the e-mail address found in the "abuse-mailbox" field. Additional information about the network in question can be obtained by examining the WHOIS entry for AS number 15496.

Should this approach fail to produce results, one still has options left. The upstream provider for the said network is FUNET, the Finnish University Network. As it happens, FUNET runs a CERT of its own and it can be reached via the e-mail address specified in the abuse-mailbox field of AS1741.

In case both the Aalto University and FUNET contacts fail to respond, there still is an option to escalate the incident to the national CERT level. Determining the national CERT for a given country is anything but straightforward. Good leads can be found from CERT/CC's list of CSIRTs with National Responsibility. [18] Additional information can be found from ENISA's web page [38] and member listings of collectives such as FIRST[47], Trusted Introducer[48], APCERT[49] and EGC [50].

In case additional information is needed, one can further analyse name server and routing information by using publicly available tools provided by Team Cymru, Inc., BFK edv-consulting GmbH, Robtex.com, DNSstuff, LLC and the Honeynor Project. The web server info and the site's contents can be obtained safely using a command line HTTP client called *wget*. In this example, the wget is instructed to impersonate Internet Explorer 8 on a Windows workstation. Usually impersonation of this sort is needed if there is reason to believe the web server would serve malicious content only to certain

---

[47] http://www.first.org
[48] http://www.trusted-introducer.org/
[49] http://www.apcert.org
[50] http://www.egc-group.org

kinds of victims. Usual targets are expected to use Windows platforms or arrive to the site following results from search engines such as Google.

Output of name server forward lookup for hostname 'www.aalto.fi'

```
> dig www.aalto.fi

; <<>> DiG 9.5.1-P2.1 <<>> www.aalto.fi
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11770
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4

;; QUESTION SECTION:
;www.aalto.fi.                  IN      A

;; ANSWER SECTION:
www.aalto.fi.           3600    IN      A       130.233.224.254

;; AUTHORITY SECTION:
aalto.fi.               3600    IN      NS      ns1.hut.fi.
aalto.fi.               3600    IN      NS      ns2.hut.fi.
aalto.fi.               3600    IN      NS      ns-secondary.funet.fi.

;; ADDITIONAL SECTION:
ns1.hut.fi.             3600    IN      A       130.233.224.1
ns2.hut.fi.             3600    IN      A       130.233.224.13
ns-secondary.funet.fi.  12717   IN      A       128.214.248.132
ns-secondary.funet.fi.  13004   IN      AAAA    2001:708:10:55::53

;; Query time: 1 msec
;; SERVER: 130.233.224.1#53(130.233.224.1)
;; WHEN: Sat Mar 20 12:28:15 2010
;; MSG SIZE  rcvd: 195
```

Output of name server reverse lookup for IP '130.233.224.254'

```
> dig -x 130.233.224.254

; <<>> DiG 9.5.1-P2.1 <<>> -x 130.233.224.254
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62613
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4

;; QUESTION SECTION:
;254.224.233.130.in-addr.arpa.  IN      PTR

;; ANSWER SECTION:
254.224.233.130.in-addr.arpa. 3600 IN   PTR     www.hut.fi.

;; AUTHORITY SECTION:
233.130.in-addr.arpa.   3600    IN      NS      ns1.hut.fi.
233.130.in-addr.arpa.   3600    IN      NS      ns2.hut.fi.
233.130.in-addr.arpa.   3600    IN      NS      ns-secondary.funet.fi.

;; ADDITIONAL SECTION:
ns1.hut.fi.             3600    IN      A       130.233.224.1
ns2.hut.fi.             3600    IN      A       130.233.224.13
ns-secondary.funet.fi.  32      IN      A       128.214.248.132
ns-secondary.funet.fi.  202     IN      AAAA    2001:708:10:55::53

;; Query time: 0 msec
;; SERVER: 130.233.224.1#53(130.233.224.1)
```

```
;; WHEN: Sun Mar 21 00:01:55 2010
;; MSG SIZE  rcvd: 215
```

Note about name server lookups

Performing name server lookups might seem like a harmless thing to do, and usually they are.

However, a word of caution is in place when investigating incidents of targeted nature, for instance espionage attempts. In theory, the attacker could set up a special domain or IP range and take on operating authoritative name servers for those objects. If the attack would remain truly targeted and not detected, only a handful of name server queries should reach those name servers and they should originate from the victim's infected computer. Queries performed from an altogether different network could set the alarms off on the attacker's side, thus hinting that the attack has been discovered.

Output of WHOIS lookup for second level domain name 'aalto.fi'

Whois is a service operated by the domain name and network registries. Whois returns information related to the registered status of the queried object.

```
> whois aalto.fi

domain:   aalto.fi
descr:    Teknillinen korkeakoulu
descr:    02459026
address:  Kirjaamo / Tietohallinto / Pirjo Ruuskanen
address:  PL 1000
address:  02015
address:  TKK
phone:    09-4511
status:   Granted
created:  27.3.2009
expires:  27.3.2012
nserver: ns1.hut.fi [OK]
nserver: ns2.hut.fi [OK]
nserver: ns-secondary.funet.fi [OK]

More information is available at https://domain.ficora.fi/
Copyright (c) Finnish Communications Regulatory Authority
```

Output of WHOIS lookup for IP address '130.233.224.254'

```
> whois 130.233.224.254

OrgName:    RIPE Network Coordination Centre
OrgID:      RIPE
Address:    P.O. Box 10096
City:       Amsterdam
StateProv:
PostalCode: 1001EB
Country:    NL

ReferralServer: whois://whois.ripe.net:43

NetRange:   130.225.0.0 - 130.244.255.255
CIDR:       130.225.0.0/16, 130.226.0.0/15, 130.228.0.0/14, 130.232.0.0/13, 130.240
.0.0/14, 130.244.0.0/16
NetName:    RIPE-ERX-130-225-0-0
NetHandle:  NET-130-225-0-0-1
Parent:     NET-130-0-0-0-0
```

```
NetType:        Early Registrations, Transferred to RIPE NCC
Comment:        These addresses have been further assigned to users in
Comment:        the RIPE NCC region.  Contact information can be found in
Comment:        the RIPE database at http://www.ripe.net/whois
RegDate:        2003-11-12
Updated:        2003-11-12

# ARIN WHOIS database, last updated 2010-03-19 20:00
# Enter ? for additional hints on searching ARIN's WHOIS database.
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at https://www.arin.net/whois_tou.html


Found a referral to whois.ripe.net:43.

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '130.233.0.0 - 130.233.255.255'

inetnum:        130.233.0.0 - 130.233.255.255
netname:        HUTNET
descr:          Helsinki University of Technology
country:        FI
admin-c:        JM5323-RIPE
tech-c:         KL66
remarks:        rev-srv:        ns1.hut.fi
remarks:        rev-srv:        ns2.hut.fi
remarks:        rev-srv:        ns-secondary.funet.fi
status:         ASSIGNED PA
mnt-by:         HUTFI-MNT
source:         RIPE # Filtered
remarks:        rev-srv attribute deprecated by RIPE NCC on 02/09/2009

person:         Juhani Markula
address:        Helsinki University of Technology
address:        Information Resources Management
address:        P.O.B. 1100
address:        FIN-02015 TKK
address:        FINLAND
address:        street address Otakaari 1, Espoo
phone:          +358 9 4511
fax-no:         +358 9 464 788
abuse-mailbox:  abuse@tkk.fi
nic-hdl:        JM5323-RIPE
mnt-by:         HUTFI-MNT
source:         RIPE # Filtered

person:         Kimmo Laaksonen
address:        Helsinki University of Technology
address:        Computing Centre
address:        P.O.B. 1100
address:        FIN-02015 TKK
address:        Finland
address:        street address Otakaari 1, Espoo
phone:          +358 9 4511
fax-no:         +358 9 464 788
abuse-mailbox:  abuse@tkk.fi
```

```
nic-hdl:        KL66
mnt-by:         HUTFI-MNT
source:         RIPE # Filtered

% Information related to '130.233.0.0/16AS15496'

route:          130.233.0.0/16
descr:          Helsinki University of Technology
descr:          FINLAND
origin:         AS15496
mnt-by:         HUTFI-MNT
source:         RIPE # Filtered
```

Output of tool to map IP address to AS number

The IP2ASN mapping tool is provided by Team Cymru, Inc. returns information about the autonomous system under which the IP address belongs to. [96]

```
> whois -h whois.cymru.com " -v 130.233.224.254"
AS      | IP               | BGP Prefix          | CC | Registry | Allocated  | AS
Name
15496   | 130.233.224.254  | 130.233.0.0/16      | EU | ripencc  | 1988-10-21 | Hel
sinki University of Technology
```

Output of IP to AS mapping tool indicating the associated upstream network

A variation of the IP2ASN tool is used to extract the AS number of the upstream network provider.

```
> whois -h peer-whois.cymru.com " -v 130.233.224.254"
PEER_AS | IP               | BGP Prefix          | CC | Registry | Allocated  | AS
Name
1741    | 130.233.224.254  | 130.233.0.0/16      | EU | ripencc  | 1988-10-21 | FUN
ETAS FUNET autonomous system
```

Output of WHOIS lookup for Autonomous System the IP address belongs to

```
> whois AS15496
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to 'AS15360 - AS16383'

as-block:       AS15360 - AS16383
descr:          RIPE NCC ASN block
remarks:        These AS Numbers are further assigned to network
remarks:        operators in the RIPE NCC service region. AS
remarks:        assignment policy is documented in:
remarks:        <http://www.ripe.net/ripe/docs/asn-assignment.html>
remarks:        RIPE NCC members can request AS Numbers using the
remarks:        form available in the LIR Portal or at:
remarks:        <http://www.ripe.net/ripe/docs/asnrequestform.html>
org:            ORG-NCC1-RIPE
admin-c:        CREW-RIPE
tech-c:         RD132-RIPE
```

```
mnt-by:         RIPE-DBM-MNT
mnt-lower:      RIPE-NCC-HM-MNT
source:         RIPE # Filtered

organisation:   ORG-NCC1-RIPE
org-name:       RIPE NCC
org-type:       RIR
address:        RIPE Network Coordination Centre
address:        P.O. Box 10096
address:        1001 EB Amsterdam
address:        The Netherlands
phone:          +31 20 535 4444
fax-no:         +31 20 535 4445
admin-c:        CREW-RIPE
tech-c:         CREW-RIPE
mnt-ref:        RIPE-NCC-RIS-MNT
mnt-ref:        RIPE-NCC-HM-MNT
mnt-by:         RIPE-NCC-HM-MNT
source:         RIPE # Filtered

role:           RIPE NCC Registration Services Department
address:        RIPE Network Coordination Centre
address:        P.O. Box 10096
address:        1001 EB Amsterdam
address:        the Netherlands
phone:          +31 20 535 4444
fax-no:         +31 20 535 4445
org:            ORG-NCC1-RIPE
admin-c:        AdlH1-RIPE
admin-c:        ACM2-RIPE
tech-c:         TIM4-RIPE
tech-c:         KL1200-RIPE
tech-c:         IW112-RIPE
tech-c:         PINK1-RIPE
tech-c:         XAV
tech-c:         AKA
tech-c:         SD1131-RIPE
tech-c:         SLON-RIPE
tech-c:         ALEX
tech-c:         DIRK1-RIPE
tech-c:         NATH
tech-c:         ARNE
tech-c:         SHAR1-RIPE
tech-c:         DEV82-RIPE
tech-c:         MdB176-RIPE
tech-c:         MSCH2-RIPE
tech-c:         TA2370-RIPE
tech-c:         GAV
nic-hdl:        CREW-RIPE
abuse-mailbox:  abuse@ripe.net
mnt-by:         RIPE-NCC-HM-MNT
source:         RIPE # Filtered

role:           RIPE DBM
remarks:        ************************************************
remarks:        Information about the RIPE Database can be found at:
remarks:        http://www.ripe.net/db/index.html
remarks:        ************************************************
nic-hdl:        RD132-RIPE
org:            ORG-NCC1-RIPE
address:        RIPE Network Coordination Centre
address:        P.O. Box 10096
address:        1001 EB Amsterdam
address:        The Netherlands
phone:          +31 20 535 4444
```

```
fax-no:         +31 20 535 4445
abuse-mailbox:  abuse@ripe.net
admin-c:        DW-RIPE
tech-c:         DW-RIPE
tech-c:         INTY1-RIPE
tech-c:         HAJ-RIPE
tech-c:         LMC-RIPE
tech-c:         GRUM-RIPE
tech-c:         PP-RIPE
tech-c:         RIPE124-RIPE # Nagios stuff
tech-c:         DUMY-RIPE    # placeholder object for dummification
mnt-by:         RIPE-DBM-MNT
source:         RIPE # Filtered

% Information related to 'AS15496'

aut-num:        AS15496
as-name:        UNSPECIFIED
descr:          Helsinki University of Technology
descr:          Computing Centre
descr:          P.O.B. 1100
descr:          FIN-02015 TKK
descr:          Finland
import:         from AS1741
                action pref=90;
                accept ANY
import:         from AS1741
                action pref=100;
                accept AS-FUNET
export:         to AS1741
                announce AS15496
admin-c:        JM5323-RIPE
tech-c:         KL66
mnt-by:         HUTFI-MNT
source:         RIPE # Filtered

person:         Juhani Markula
address:        Helsinki University of Technology
address:        Information Resources Management
address:        P.O.B. 1100
address:        FIN-02015 TKK
address:        FINLAND
address:        street address Otakaari 1, Espoo
phone:          +358 9 4511
fax-no:         +358 9 464 788
abuse-mailbox:  abuse@tkk.fi
nic-hdl:        JM5323-RIPE
mnt-by:         HUTFI-MNT
source:         RIPE # Filtered

person:         Kimmo Laaksonen
address:        Helsinki University of Technology
address:        Computing Centre
address:        P.O.B. 1100
address:        FIN-02015 TKK
address:        Finland
address:        street address Otakaari 1, Espoo
phone:          +358 9 4511
fax-no:         +358 9 464 788
abuse-mailbox:  abuse@tkk.fi
nic-hdl:        KL66
mnt-by:         HUTFI-MNT
source:         RIPE # Filtered
```

Output of WHOIS lookup for upstream AS

```
> whois AS1741

OrgName:     RIPE Network Coordination Centre
OrgID:       RIPE
Address:     P.O. Box 10096
City:        Amsterdam
StateProv:
PostalCode:  1001EB
Country:     NL

ReferralServer: whois://whois.ripe.net:43

ASNumber:    1741
ASName:      RIPE-ASNBLOCK-1741
ASHandle:    AS1741
Comment:     These addresses have been further assigned to users in
Comment:     the RIPE NCC region. Contact information can be found in
Comment:     the RIPE database at http://www.ripe.net/whois
RegDate:     2002-10-15
Updated:     2003-04-25

# ARIN WHOIS database, last updated 2010-03-19 20:00
# Enter ? for additional hints on searching ARIN's WHOIS database.
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at https://www.arin.net/whois_tou.html


Found a referral to whois.ripe.net:43.

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to 'AS1741 - AS1741'

as-block:       AS1741 - AS1741
descr:          RIPE NCC ASN block
remarks:        These AS Numbers are further assigned to network
remarks:        operators in the RIPE NCC service region. AS
remarks:        assignment policy is documented in:
remarks:        <http://www.ripe.net/ripe/docs/asn-assignment.html>
remarks:        RIPE NCC members can request AS Numbers using the
remarks:        form available in the LIR Portal or at:
remarks:        <http://www.ripe.net/ripe/docs/asnrequestform.html>
org:            ORG-NCC1-RIPE
admin-c:        CREW-RIPE
tech-c:         RD132-RIPE
mnt-by:         RIPE-DBM-MNT
mnt-lower:      RIPE-NCC-HM-MNT
source:         RIPE # Filtered

organisation:   ORG-NCC1-RIPE
org-name:       RIPE NCC
org-type:       RIR
address:        RIPE Network Coordination Centre
address:        P.O. Box 10096
address:        1001 EB Amsterdam
```

```
address:        The Netherlands
phone:          +31 20 535 4444
fax-no:         +31 20 535 4445
admin-c:        CREW-RIPE
tech-c:         CREW-RIPE
mnt-ref:        RIPE-NCC-RIS-MNT
mnt-ref:        RIPE-NCC-HM-MNT
mnt-by:         RIPE-NCC-HM-MNT
source:         RIPE # Filtered

role:           RIPE NCC Registration Services Department
address:        RIPE Network Coordination Centre
address:        P.O. Box 10096
address:        1001 EB Amsterdam
address:        the Netherlands
phone:          +31 20 535 4444
fax-no:         +31 20 535 4445
org:            ORG-NCC1-RIPE
admin-c:        AdlH1-RIPE
admin-c:        ACM2-RIPE
tech-c:         TIM4-RIPE
tech-c:         KL1200-RIPE
tech-c:         IW112-RIPE
tech-c:         PINK1-RIPE
tech-c:         XAV
tech-c:         AKA
tech-c:         SD1131-RIPE
tech-c:         SLON-RIPE
tech-c:         ALEX
tech-c:         DIRK1-RIPE
tech-c:         NATH
tech-c:         ARNE
tech-c:         SHAR1-RIPE
tech-c:         DEV82-RIPE
tech-c:         MdB176-RIPE
tech-c:         MSCH2-RIPE
tech-c:         TA2370-RIPE
tech-c:         GAV
nic-hdl:        CREW-RIPE
abuse-mailbox:  abuse@ripe.net
mnt-by:         RIPE-NCC-HM-MNT
source:         RIPE # Filtered

role:           RIPE DBM
remarks:        ************************************************
remarks:        Information about the RIPE Database can be found at:
remarks:        http://www.ripe.net/db/index.html
remarks:        ************************************************
nic-hdl:        RD132-RIPE
org:            ORG-NCC1-RIPE
address:        RIPE Network Coordination Centre
address:        P.O. Box 10096
address:        1001 EB Amsterdam
address:        The Netherlands
phone:          +31 20 535 4444
fax-no:         +31 20 535 4445
abuse-mailbox:  abuse@ripe.net
admin-c:        DW-RIPE
tech-c:         DW-RIPE
tech-c:         INTY1-RIPE
tech-c:         HAJ-RIPE
tech-c:         LMC-RIPE
tech-c:         GRUM-RIPE
tech-c:         PP-RIPE
tech-c:         RIPE124-RIPE # Nagios stuff
```

```
tech-c:         DUMY-RIPE    # placeholder object for dummification
mnt-by:         RIPE-DBM-MNT
source:         RIPE # Filtered

% Information related to 'AS1741'

aut-num:        AS1741
as-name:        FUNETAS
descr:          FUNET autonomous system
import:         from AS375 action pref=167; accept AS375
import:         from AS565 action pref=500; accept AS565
import:         from AS719 accept AS-KOLUMBUS
import:         from AS1342 accept AS-ICLFI
import:         from AS1739 action pref=500; accept AS1739
import:         from AS1759 accept AS-TSF-customers
import:         from AS2603 accept ANY
import:         from AS2686 accept AS-IGNEMEA
import:         from AS3292 accept AS-TDCNETFI
import:         from AS5400 accept AS-BT-EU
import:         from AS6667 accept AS-EUNETIP
import:         from AS8434 accept AS8434:AS-CUSTOMERS
import:         from AS8674 accept AS-NETNOD-ANYCAST
import:         from AS9002 accept AS-RETN
import:         from AS12552 accept AS-IPO
import:         from AS12659 accept AS-BBNWKS
import:         from AS15496 action pref=500; accept AS15496
import:         from AS16086 accept AS16086:AS-CUST
import:         from AS20542 accept AS-WELHO
import:         from AS20569 accept AS-AINAIP
import:         from AS1248 accept AS-NOK
import:         from AS24751 accept AS-MULTIFI
import:         from AS25152 accept RS-KROOT-FICIX
import:         from AS26415 accept AS-GTLD
import:         from AS29154 accept AS-ACADEMICAFI
import:         from AS29422 accept AS-NBLNETFI
import:         from AS30754 action pref=167; accept AS30754
import:         from AS30798 accept AS-TNNET
import:         from AS33935 accept AS-24ONLINE
import:         from AS34188 accept AS34188
import:         from AS39098 action pref=500; accept AS39098
import:         from AS39857 action pref=500; accept AS39857
import:         from AS47605 accept AS-set-FNE
import:         from AS39662 accept AS39662
import:         from AS29243 accept AS-MMD
export:         to AS375 announce AS-FUNET
export:         to AS565 announce {0.0.0.0/0}
export:         to AS719 announce AS-FUNET
export:         to AS1342 announce AS-FUNET
export:         to AS1739 announce {0.0.0.0/0}
export:         to AS1759 announce AS-FUNET
export:         to AS2603 announce AS-FUNET
export:         to AS2686 announce AS-FUNET
export:         to AS3292 announce AS-FUNET
export:         to AS5400 announce AS-FUNET
export:         to AS6667 announce AS-FUNET
export:         to AS8434 announce AS-FUNET
export:         to AS8674 announce AS-FUNET
export:         to AS9002 announce AS-FUNET
export:         to AS12552 announce AS-FUNET
export:         to AS12659 announce AS-FUNET
export:         to AS15496 announce {0.0.0.0/0}
export:         to AS16086 announce AS-FUNET
export:         to AS20542 announce AS-FUNET
export:         to AS20569 announce AS-FUNET
export:         to AS1248 announce AS-FUNET
```

```
export:         to AS24751 announce AS-FUNET
export:         to AS25152 announce AS-FUNET
export:         to AS26415 announce AS-FUNET
export:         to AS29154 announce AS-FUNET
export:         to AS29422 announce AS-FUNET
export:         to AS30754 announce ANY
export:         to AS30798 announce AS-FUNET
export:         to AS33935 announce AS-FUNET
export:         to AS34188 announce AS-FUNET
export:         to AS39098 announce {0.0.0.0/0}
export:         to AS39857 announce {0.0.0.0/0}
export:         to AS47605 announce AS-FUNET
export:         to AS39662 announce ANY
export:         to AS29243 announce AS-FUNET
default:        to AS2603 action pref=500; networks ANY
mp-import:      afi ipv6 from AS1248 accept AS-NOK
mp-import:      afi ipv6 from AS1759 accept AS-TSF-Customers
mp-import:      afi ipv6 from AS2603 accept ANY
mp-import:      afi ipv6 from AS3292 accept AS-TDCNET-IPV6
mp-import:      afi ipv6 from AS6667 accept AS-EUNETIP-V6
mp-import:      afi ipv6 from AS9002 accept AS-RETN6
mp-import:      afi ipv6 from AS12552 accept AS-IPO6
mp-import:      afi ipv6 from AS16086 accept AS16086:AS-CUST
mp-import:      afi ipv6 from AS20569 accept AS-AINAIP
mp-import:      afi ipv6 from AS30798 accept AS-TNNET
mp-import:      afi ipv6 from AS29422 accept AS-NBLNETFI
mp-import:      afi ipv6 from AS719 accept AS-KOLUMBUS
mp-import:      afi ipv6 from AS39662 accept AS39662
mp-import:      afi ipv6 from AS29243 accept AS-MMD
mp-export:      afi ipv6 to AS1248 announce AS-FUNET
mp-export:      afi ipv6 to AS1759 announce AS-FUNET
mp-export:      afi ipv6 to AS2603 announce AS-FUNET
mp-export:      afi ipv6 to AS3292 announce AS-FUNET
mp-export:      afi ipv6 to AS6667 announce AS-FUNET
mp-export:      afi ipv6 to AS9002 announce AS-FUNET
mp-export:      afi ipv6 to AS12552 announce AS-FUNET
mp-export:      afi ipv6 to AS16086 announce AS-FUNET
mp-export:      afi ipv6 to AS20569 announce AS-FUNET
mp-export:      afi ipv6 to AS29422 announce AS-FUNET
mp-export:      afi ipv6 to AS30798 announce AS-FUNET
mp-export:      afi ipv6 to AS719 announce AS-FUNET
mp-export:      afi ipv6 to AS39662 announce ANY
mp-export:      afi ipv6 to AS29243 announce AS-FUNET
admin-c:        FA1183-RIPE
tech-c:         FH437-RIPE
mnt-by:         AS1741-MNT
source:         RIPE # Filtered

role:           FUNET Admin
address:        CSC - IT Center for Sciece
address:        POBox 405, FIN-02101 Espoo
address:        Finland
org:            ORG-FF1-RIPE
phone:          +358 9 457 2704
fax-no:         +358 9 457 2302
admin-c:        JK3657-RIPE
tech-c:         JK3657-RIPE
nic-hdl:        FA1183-RIPE
abuse-mailbox:  abuse@funet.fi
mnt-by:         AS1741-MNT
source:         RIPE # Filtered

role:           FUNET Hostmaster
address:        CSC - IT Center for Science
address:        PO Box 405, FIN-02101 Espoo
```

```
address:        Finland
org:            ORG-FF1-RIPE
phone:          +358 9 457 2704
fax-no:         +358 9 457 2302
admin-c:        JK3657-RIPE
admin-c:        LP2013-RIPE
tech-c:         JM2197-RIPE
tech-c:         TP1041-RIPE
tech-c:         KH622-RIPE
tech-c:         MASA3-RIPE
tech-c:         AR414-RIPE
tech-c:         JO2633-RIPE
nic-hdl:        FH437-RIPE
mnt-by:         AS1741-MNT
abuse-mailbox:  abuse@funet.fi
source:         RIPE # Filtered
```

Output of BFK's passive DNS replication tool for query 'www.aalto.fi'

```
The server returned the following data:
www.aalto.fi          A        130.233.224.254

The server state is: 201 Okay
```

Output of BFK's passive DNS replication tool for query '130.233.224.254'

This tool has a web-based user interface via which a following query was performed:

URL: http://www.bfk.de/bfk_dnslogger_en.html?query=130.233.224.254#result

```
The server returned the following data:
sahkotekniikka.tkk.fi            CNAME      www.hut.fi
liikunta.tkk.fi       CNAME      www.hut.fi
tuta.tkk.fi           CNAME      www.hut.fi
kva.tkk.fi            CNAME      www.hut.fi
engineering.tkk.fi    CNAME      www.hut.fi
civil.tkk.fi          CNAME      www.hut.fi
wwwlogin.tkk.fi       CNAME      www.hut.fi
information.tkk.fi    CNAME      www.hut.fi
ics.tkk.fi            A          130.233.224.254
electronics.tkk.fi    CNAME      www.hut.fi
comnet.tkk.fi         A          130.233.224.254
urapalvelut.tkk.fi    CNAME      www.hut.fi
www.tkk.fi            CNAME      www.hut.fi
www.aalto.fi          A          130.233.224.254
www.hut.fi            A          130.233.224.254

The server state is: 201 Okay
```

Testing whether the network is registered to Finland using a tool provided by the Honeynor Project

Honeynor is a Norwegian branch of the Honeynet project. As a service to the public, they have created a simple tool called *CC2ASN* that lists all autonomous systems associated with a given country. While not producing foolproof results, the tool is a convenient aid for the national CERTs in finding which networks belong to the CERTs constituency.

More information about the tool can be found here:

URL: http://www.honeynor.no/2009/06/19/country-lookup/

```
> whois -h atari.honeynor.no fi | grep AS15496
AS15496
```

The ouput confirms that, according to BGP route announcements, AS15496 is a Finnish network.

Output of an ICMP traceroute to the target host

Tracerouting the target is an active measure since actual ICMP ECHO packets ('ping packets') are being sent to the target host. Theoretically, the controller of the target system could be monitoring incoming packets in an effort to determine whether the attack has been identified and has proceeded into an investigation.

```
> traceroute www.aalto.fi

Tracing route to www.aalto.fi [130.233.224.254]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2    39 ms   106 ms    19 ms  212.90.64.1
  3    37 ms   194 ms    26 ms  212.90.64.177
  4    14 ms    29 ms    24 ms  csc.ficix2-ge.ficix.fi [193.110.224.14]
  5    29 ms   140 ms    27 ms  csc4-g3100-helsinki0.funet.fi [193.166.187.181]
  6    12 ms    17 ms    28 ms  gw-2-funet-ge-1.hut.fi [130.233.231.226]
  7    27 ms    13 ms    31 ms  www.hut.fi [130.233.224.254]

Trace complete.
```

Output of a TCP traceroute to the target host

Tcptraceroute is an active measure, too. It differs from the "ordinary" traceroute tool in using TCP packets instead of ICMP ECHO packets. Targets hiding behind firewalls and network address translation (NAT) gateways may produce different results when probed with *tcptraceroute* than with *traceroute*. This is especially true in cases where ping packets are being filtered out before reaching their final destination.

More information about *tcptraceroute* can be found here:

URL: http://michael.toren.net/code/tcptraceroute/

```
> tcptraceroute www.aalto.fi

Tracing route to 130.233.224.254 [www.hut.fi] on port 80
Over a maximum of 30 hops.
1       18 ms   39 ms   37 ms   0.0.0.0
2       27 ms   43 ms   21 ms   212.90.64.1
3       39 ms   65 ms   27 ms   212.90.64.177
4       36 ms   15 ms   29 ms   193.110.224.14  [csc.ficix2-ge.ficix.fi]
5       15 ms   28 ms   36 ms   193.166.187.181 [csc4-g3100-helsinki0.funet.fi]
6       21 ms   36 ms   18 ms   130.233.231.226 [gw-2-funet-ge-1.hut.fi]
7       Destination Reached in 21 ms. Connection established to 130.233.224.254
Trace Complete.
```

In this case, *traceroute* and *tcptraceroute* produce identical results. The TCP port 80 was a natural selection as the remote host was assumed to be a web server. The name of the localhost has been removed form the output.

Additional clues can be found by paying attention to the network latency indicated in milliseconds. Exceptionally long latency may indicate a redirected connection – some-

times the actual host may be even on a totally different continent than the registered IP address would indicate.

A hint: a powerful Python-based tool called *Scapy* employs among other things a visual tcptraceroute that not only performs the connection test but also draws a network topology map indicating the route from the querying host to the final destination.

Information obtained by connecting to the target host

Wget is a small command-line tool for connecting to web servers in the HTTP protocol. Using wget does basically the same as pointing a web browser to the target host. For the purpose of CERT investigations, the HTTP headers normally not shown when using a browser may provide additional information of interest to understanding which kind of system the remote hosts is running on.

Connecting to the remote system using a web browser, wget or any other active tool naturally leaves a visible trace on the remote system. The owner of the target system can monitor the connection attempts by using, for example, firewall, IDS, and HTTPD logs.

In the example below, *wget* is instructed to craft a false user agent string in an effort to make the connection look like it was coming from Microsoft Internet Explorer version 8. This would be a useful feature when testing whether the server would return JavaScript content tailored for certain web browsers. It is a standard practice for the criminals to exploit web browser vulnerabilities to infect unsuspecting web site visitors. The *referer* argument in the *wget* query is crafted in a way to make it look like the browser was following a link from Google's result. It is another standard practice for the criminals to instruct the compromised web servers to only infect visitors following a specially crafted search engine hit.

```
> wget -S -U "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET
CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648; .N
ET CLR 3.0.4506.2152; .NET CLR 3.5.30729)" --referer="http://www.google.com/search?
hl=en&rls=com.microsoft%3Aen-GB&q=searchstring&aq=f&aqi=&aql=&oq=&gs_rfai=" http://
www.aalto.fi
--2010-03-20 23:00:24--  http://www.aalto.fi/
Resolving www.aalto.fi... 130.233.224.254
Connecting to www.aalto.fi|130.233.224.254|:80... connected.
HTTP request sent, awaiting response...
  HTTP/1.0 301 Moved Permanently
  Date: Sat, 20 Mar 2010 20:57:03 GMT
  Server: Apache/2.2.3 (Red Hat)
  Location: http://www.aalto.fi/fi/
  Cache-Control: max-age=3600
  Expires: Sat, 20 Mar 2010 21:57:03 GMT
  Content-Length: 309
  Content-Type: text/html; charset=iso-8859-1
  Age: 201
  X-Cache: HIT from buster.hut.fi
  X-Cache-Lookup: HIT from buster.hut.fi:80
  Via: 1.0 buster.hut.fi:80 (squid/2.6.STABLE6)
  Connection: keep-alive
Location: http://www.aalto.fi/fi/ [following]
--2010-03-20 23:00:24--  http://www.aalto.fi/fi/
Reusing existing connection to www.aalto.fi:80.
HTTP request sent, awaiting response...
  HTTP/1.0 200 OK
  Date: Sat, 20 Mar 2010 20:51:21 GMT
  Server: Apache/2.2.3 (Red Hat)
  X-Powered-By: Midgard/8.09.7
```

```
  X-MidCOM-meta-cache: HIT R-76c6a8f676e2f24dbe590579efac9c83
  X-MidCOM-meta-cache: HIT C-e2febc8ee44cf61c2b4d197bc400736a
  X-MidCOM-data-cache: HIT C-e2febc8ee44cf61c2b4d197bc400736a
  ETag: e2febc8ee44cf61c2b4d197bc400736a
  Accept-Ranges: none
  Last-Modified: Fri, 19 Mar 2010 15:09:19 GMT
  Cache-Control: public max-age=3600
  Pragma: public
  Expires: Sat, 20 Mar 2010 21:12:09 GMT
  Content-Type: text/html; charset=utf-8
  Age: 543
  X-Cache: HIT from belly.hut.fi
  X-Cache-Lookup: HIT from belly.hut.fi:80
  Via: 1.0 belly.hut.fi:80 (squid/2.6.STABLE6)
  Connection: close
Length: unspecified [text/html]
Saving to: `index.html'

    [ <=>                                                 ] 16,603      --.-K/s   in 0s

2010-03-20 23:00:25 (45.8 MB/s) - `index.html' saved [16603]
```

Output of visual analysis tools

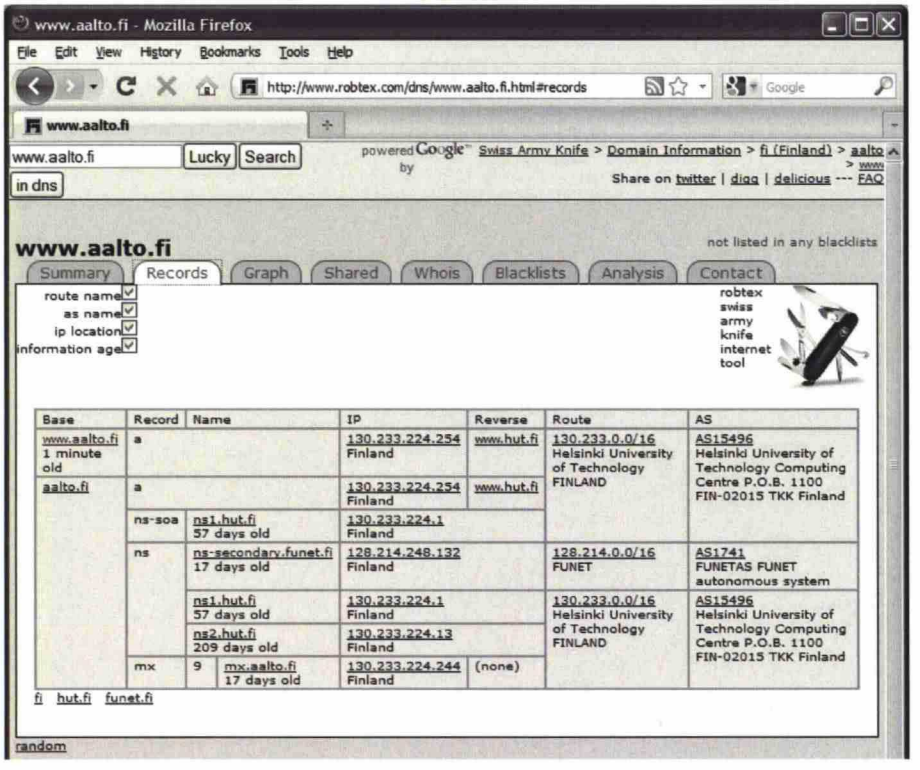

Figure 29 – DNS and AS report of 'www.aalto.fi'. Screenshot taken from Robtex.com on 2010-03-20.

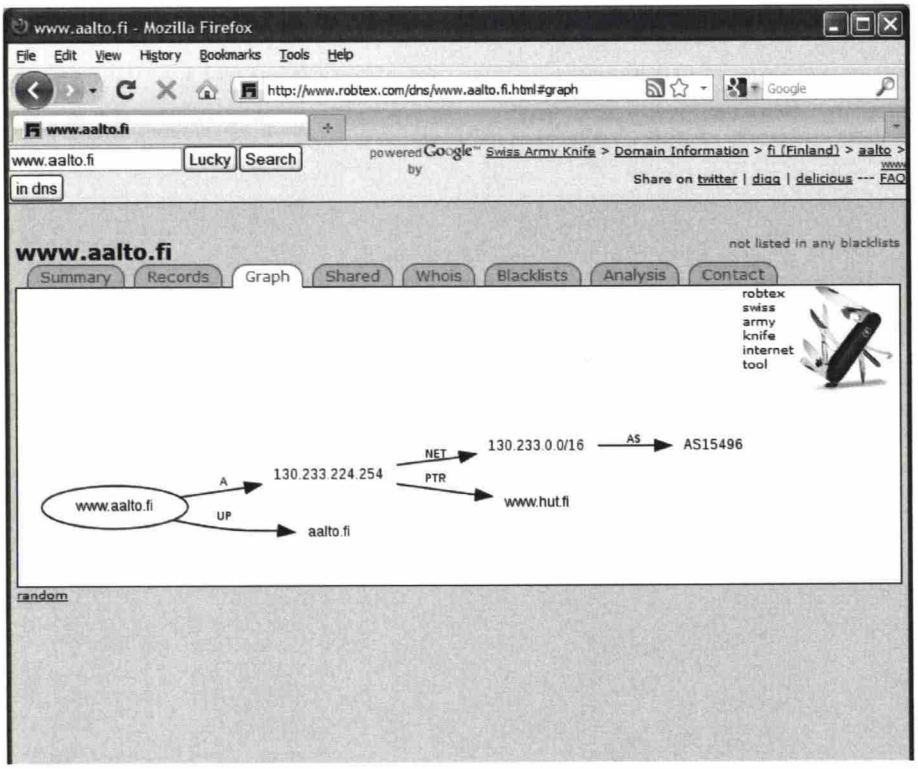

Figure 30 – Graph of IP routing for 'www.aalto.fi'. Screenshot taken from Robtex.com on 2010-03-20.

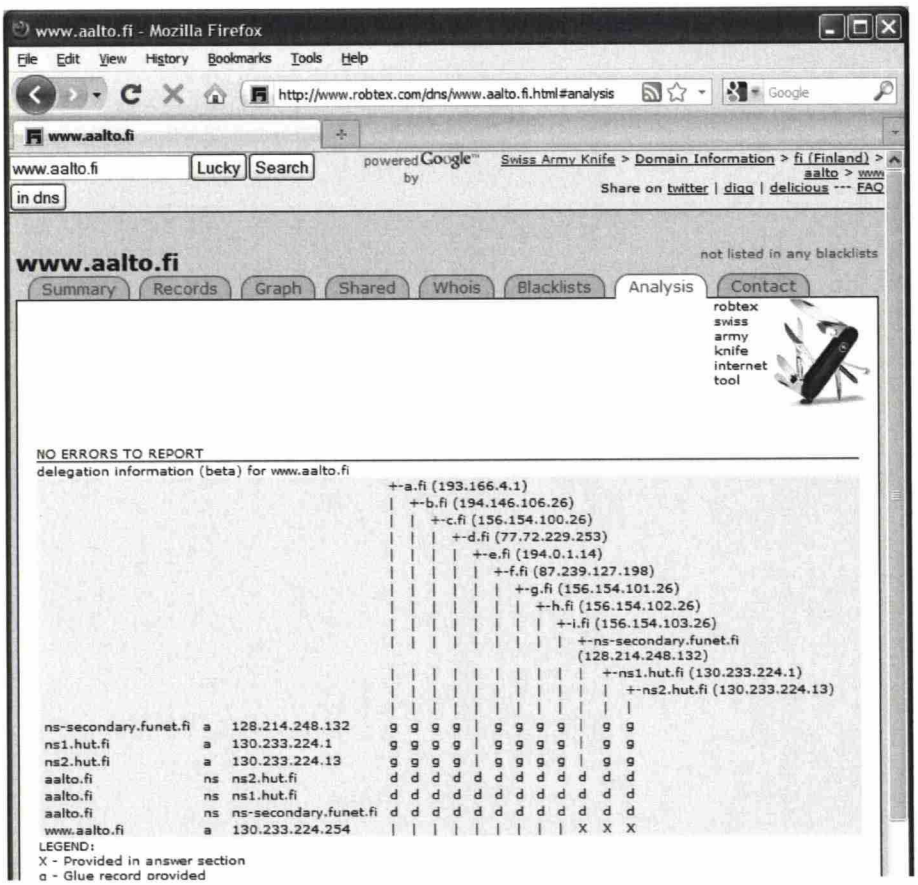

Figure 31 – DNS analysis of 'www.aalto.fi'. Screenshot taken from Robtex.com on 2010-03-20.

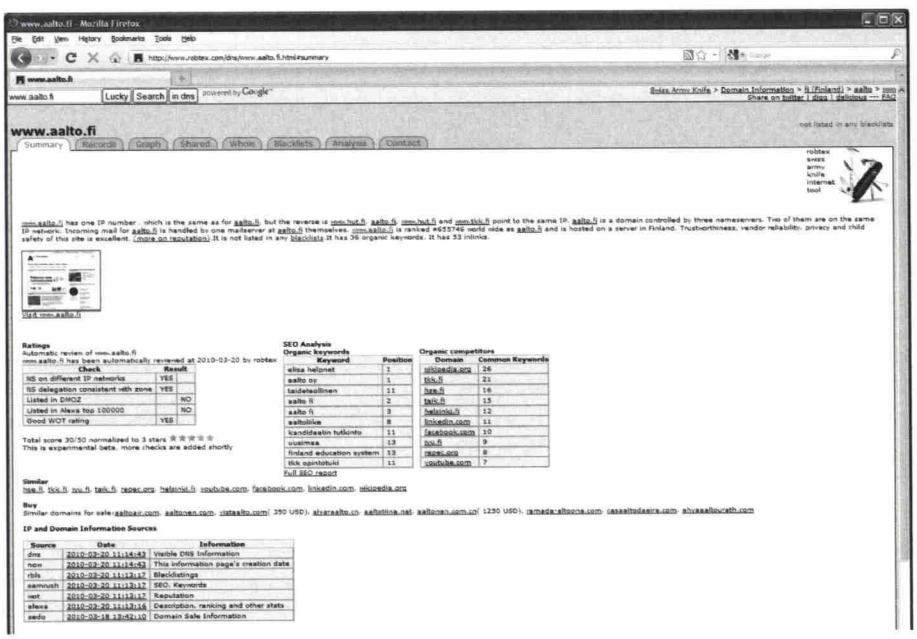

Figure 32 – A summary report of network information related to 'www.aalto.fi' as seen by Robtex.com.

CERT® Coordination Center's map of CSIRTs with National Responsibility

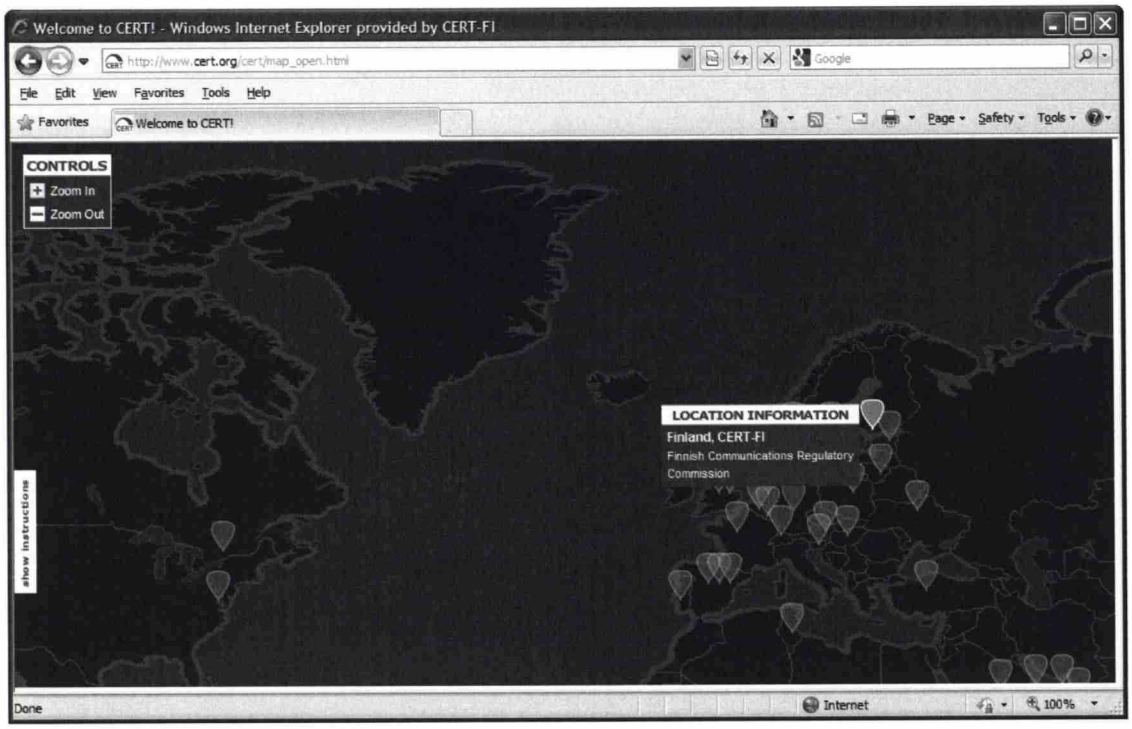

Figure 33 – CERT® Coordination Center of Pittsburgh, PA, US maintains an unofficial registry CSIRTs with National Responsibility. The information is browsable via interactive world map. The registry indicates that the national CERT or "CERT of last resort" for Finland is CERT-FI.

Appendix III Multiresolver output of [FICORA #295909]

Sites: www.u[redacted]a.net
www.7[redacted]s.com
www.kolumbus.fi
www.s[redacted]i.com
www.r[redacted]a.fi
www.k[redacted]s.fi
IP;ASN;CC;ABUSE;REGISTRY;ALLOCATED;ROUTE;PTR;DNAME;CNAME;NS;MX;SOA;EPOCH;ORR
62.65.30.9;3292;SE;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;2000-07-06;62.65.0.0/19;ns-no.sn.net;ns-no.sn.net;UNRESOLVED;ns1.songnet.fi,ns2.songnet.fi,ns3.songnet.fi;UNRESOLVED;ns1.songnet.fi hostmaster.songnet.fi 2009081700 serial 28800 refresh 7200 retry 1209600 expire 86400 minimum;1250571913;NO
194.100.0.100;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1994-10-07;194.100.0.0/16;ns1.songnet.fi;ns1.songnet.fi;UNRESOLVED;ns2.songnet.fi,ns3.songnet.fi,ns1.songnet.fi;mx1.song.fi:0,mx2.song.fi:0;ns1.songnet.fi hostmaster.songnet.fi 2009081700 serial 28800 refresh 7200 retry 1209600 expire 86400 minimum;1250571912;NO
62.248.254.2;3336;FI;abuse@elisa.fi;ripencc;2000-12-21;62.248.128.0/17;ns-se.elisa.net;ns-se.elisa.net;UNRESOLVED;ns-se.elisa.net,ns-fi.elisa.net;UNRESOLVED;ns-fi.elisa.net hostmaster.elisa.fi 2009061700 serial 86400 refresh 7200 retry 3600000 expire 172800 minimum;1250571911;NO
193.229.5.160;3336;FI;abuse@elisa.fi;ripencc;1995-12-15;193.229.0.0/16;mx.kolumbus.fi;mx.kolumbus.fi;UNRESOLVED;ns-se.elisa.net,ns-fi.elisa.net;UNRESOLVED;ns-fi.elisa.net hostmaster.elisa.fi 2009081000 serial 86400 refresh 7200 retry 3600000 expire 172800 minimum;1250571911;NO
213.50.29.189;3292;SE;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1999-09-17;213.50.0.0/16;ns-se.sn.net;ns-se.sn.net;UNRESOLVED;ns1.songnet.fi,ns2.songnet.fi,ns3.songnet.fi;UNRESOLVED;ns1.songnet.fi hostmaster.songnet.fi 2009081700 serial 28800 refresh 7200 retry 1209600 expire 86400 minimum;1250571913;NO
193.229.9.133;3336;FI;abuse@elisa.fi;ripencc;1995-12-15;193.229.0.0/16;kotiweb.kolumbus.fi;www.7[redacted]s.com;UNRESOLVED;ns-fi.elisa.net,ns-se.elisa.net;UNRESOLVED;ns-fi.elisa.net hostmaster.elisa.fi 2007070401 serial 28000 refresh 7200 retry 604800 expire 86400 minimum;1250571912;YES
193.229.9.133;3336;FI;abuse@elisa.fi;ripencc;1995-12-15;193.229.0.0/16;kotiweb.kolumbus.fi;kotiweb.kolumbus.fi;UNRESOLVED;ns-fi.elisa.net,ns-se.elisa.net;mail.kolumbus.fi:10;ns-fi.elisa.net hostmaster.elisa.fi 2009081000 serial 86400 refresh 7200 retry 3600000 expire 172800 minimum;1250571912;NO
62.73.58.134;16044;FI;abuse@teliasonera.com;ripencc;2002-10-11;62.73.32.0/19;ns2.daous.com;ns2.daous.com;UNRESOLVED;ns2.daous.com,ns.daous.com;UNRESOLVED;ns.daous.com postmaster.daous.com 2006121732 serial 28800 refresh 7200 retry 604800 expire 600 minimum;1250571911;NO
81.17.195.50;16023;FI;abuse@netsonic.fi;ripencc;2002-01-11;81.17.192.0/20;a-serv.kotisivut.com;a.ns.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com,b.ns.kotisivut.com,c.ns.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com hostmaster.kotisivut.com 2009081302 serial 1800 refresh 600 retry 86400 expire 1800 minimum;1250571911;NO
81.22.246.8;39324;FI;NO_CONTACT;ripencc;2006-01-30;81.22.240.0/20;srv-g8.esp.mediateam.fi;n.serv.kotisivut.com;UNRESOLVED;b.ns.kotisivut.com,c.ns.kotisivut.com,a.ns.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com hostmaster.kotisivut.com 2009081302 serial 1800 refresh 600 retry 86400 expire 1800 minimum;1250571912;NO
81.22.246.8;39324;FI;NO_CONTACT;ripencc;2006-01-30;81.22.240.0/20;srv-g8.esp.mediateam.fi;www.s[redacted]i.com;n.serv.kotisivut.com;a.ns.kotisivut.com,b.ns.kotisivut.com,c.ns.kotisivut.com;UNRESOLVED;UNRESOLVED;1250571912;YES
81.22.246.8;39324;FI;NO_CONTACT;ripencc;2006-01-30;81.22.240.0/20;srv-g8.esp.mediateam.fi;srv-g8.esp.mediateam.fi;UNRESOLVED;a.ns.kotisivut.com,b.ns.kotisivut.com,c.ns.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com hostmaster.kotisivut.com 2008091001 serial 28800 refresh 3600 retry 604800 expire 86400 minimum;1250571912;NO
80.64.1.100;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;2001-05-08;80.64.0.0/20;ns3.songnet.fi;ns3.songnet.fi;UNRESOLVED;ns3.songnet.fi,ns1.songnet.fi,ns2.songnet.fi;mx1.song.fi:0,mx2.song.fi:0;ns1.songnet.fi hostmaster.songnet.fi 2009081700 serial 28800 refresh 7200 retry 1209600 expire 86400 minimum;1250571912;NO
81.17.195.36;16023;FI;abuse@netsonic.fi;ripencc;2002-01-11;81.17.192.0/20;host36.webtoyou.fi;www.k[redacted]s.fi;k.serv.kotisivut.com,k[redacted]s.fi.kotisivut.com;c.ns.kotisivut.com,a.ns.kotisivut.com,b.ns.kotisivut.com;UNRESOLVED;UNRESOLVED;1250571912;YES
81.17.195.36;16023;FI;abuse@netsonic.fi;ripencc;2002-01-11;81.17.192.0/20;host36.webtoyou.fi;k.serv.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com,b.ns.kotisivut.com,c.ns.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com hostmaster.kotisivut.com 2009081302 serial 1800 refresh 600 retry 86400 expire 1800 minimum;1250571912;NO
81.17.195.36;16023;FI;abuse@netsonic.fi;ripencc;2002-01-11;81.17.192.0/20;host36.webtoyou.fi;host36.webtoyou.fi;UNRESOLVED;named.kotisivut.com,named3.kotisivut.com;UNRESOLVED;named.kotisivut.com hostmaster.kotisivut.com 2008102703 serial 1800 refresh 600 retry 86400 expire 1800 minimum;1250571912;NO
81.17.195.36;16023;FI;abuse@netsonic.fi;ripencc;2002-01-11;81.17.192.0/20;host36.webtoyou.fi;k[redacted]s.fi.kotisivut.com;k.serv.kotisivut.com;c.ns.kotisivut.com,a.ns.kotisivut.com,b.ns.kotisivut.com;UNRESOLVED;UNRESOLVED;1250571912;NO
194.100.97.29;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-04;194.100.0.0/16;ns.daous.com;ns.daous.com;UNRESOLVED;ns.daous.com,ns2.daous.com;UNRESOLVED;ns.daous.com postmaster.daous.com 2006121732 serial 28800 refresh 7200 retry 604800 expire 600 minimum;1250571911;NO
194.100.94.103;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-04;194.100.0.0/16;UNRESOLVED;named3.kotisivut.com;UNRESOLVED;c.ns.kotisivut.com,a.ns.kotisivut.com,b.ns.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com hostmaster.kotisivut.com 2009081302 serial 1800 refresh 600 retry 86400 expire 1800 minimum;1250571912;NO
194.100.97.66;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-04;194.100.0.0/16;ns6.masterplanet.fi;ns2.kampusdata.fi;UNRESOLVED;ns2.kampusdata.fi,ns1.kampusdata.fi;UNRESOLVED;ns1.kampusdata.fi hostmaster.wiofso.com 64 serial 28800 refresh 7200 retry 604800 expire 86400 minimum;1250571912;NO
194.100.97.66;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-04;194.100.0.0/16;ns6.masterplanet.fi;ns6.masterplanet.fi;UNRESOLVED;ns7.masterplanet.fi,ns1.kampusdata.fi,ns6.masterplanet.fi;UNRESOLVED;ns6.masterplanet.fi hostmaster.masterplanet.fi 2008012225 serial 7200 refresh 7200 retry 604800 expire 7200 minimum;1250571912;NO
194.100.97.2;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-04;194.100.0.0/16;mailhost.masterplanet.fi;mailhost.masterplanet.fi;UNRESOLVED;ns7.masterplanet.fi,ns1.kampusdata.fi,ns6.masterplanet.fi;UNRESOLVED;ns6.masterplanet.fi hostmaster.masterplanet.fi 2008012225 serial 7200 refresh 7200 retry 604800 expire 7200 minimum;1250571912;NO
194.100.97.2;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-04;194.100.0.0/16;mailhost.masterplanet.fi;ns7.masterplanet.fi;UNRESOLVED;ns7.masterplanet.fi,ns1.kampusdata.fi,ns6.masterplanet.fi;UNRESOLVED;ns6.masterplanet.fi hostmaster.masterplanet.fi 2008012225 serial 7200 refresh 7200 retry 604800 expire 7200 minimum;1250571912;NO
194.100.94.100;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-04;194.100.0.0/16;server.webtoyou.fi;b.ns.kotisivut.com;UNRESOLVED;b.ns.kotisivut.com,c.ns.kotisivut.com,a.ns.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com hostmaster.kotisivut.com 2009081302 serial 1800 refresh 600 retry 86400 expire 1800 minimum;1250571912;NO
194.100.94.100;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-04;194.100.0.0/16;server.webtoyou.fi;server.webtoyou.fi;UNRESOLVED;named.kotisivut.com,named3.kotisivut.com;UNRESOLVED;named.kotisivut.com hostmaster.kotisivut.com 2008102703 serial 1800 refresh 600 retry 86400 expire 1800 minimum;1250571912;NO
195.197.208.150;790;FI;NO_CONTACT;ripencc;1997-09-03;195.197.0.0/16;c.ns.kotisivut.com;c.ns.kotisivut.com;UNRESOLVED;b.ns.kotisivut.com,c.ns.kotisivut.com,a.ns.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com hostmaster.kotisivut.com 2009081302 serial 1800 refresh 600 retry 86400 expire 1800 minimum;1250571911;NO
81.17.195.51;16023;FI;abuse@netsonic.fi;ripencc;2002-01-11;81.17.192.0/20;alpha.kotisivut.com;alpha.kotisivut.com;UNRESOLVED;c.ns.kotisivut.com,a.ns.kotisivut.com,b.ns.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com hostmaster.kotisivut.com 2009081302 serial 1800 refresh 600 retry 86400 expire 1800 minimum;1250571912;NO
81.17.195.51;16023;FI;abuse@netsonic.fi;ripencc;2002-01-11;81.17.192.0/20;alpha.kotisivut.com;a-serv.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com,b.ns.kotisivut.com,c.ns.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com hostmaster.kotisivut.com 2009081302 serial 1800 refresh 600 retry 86400 expire 1800 minimum;1250571912;NO
212.182.218.28;1759;FI;NO_CONTACT;ripencc;2001-02-15;212.182.192.0/18;mx6.nuoli.com;mx6.nuoli.com;UNRESOLVED;ns.daous.com,ns2.daous.com;UNRESOLVED;ns.daous.com postmaster.daous.com 2005021125 serial 28800 refresh 7200 retry 604800 expire 600 minimum;1250571911;NO

```
80.66.162.69;20774;FI;NO_CONTACT;ripencc;2001-05-17;80.66.160.0/20;ns1.kampusdata.fi;ns1.kampusdata.fi;UNRESOLVED;ns1.kampusd
ata.fi,ns2.kampusdata.fi;UNRESOLVED;ns1.kampusdata.fi hostmaster.wiofso.com 64 serial 28800 refresh 7200 retry 604800 expire
86400 minimum;1250571912;NO
193.229.9.132;3336;FI;abuse@elisa.fi;ripencc;1995-12-15;193.229.0.0/16;www.kolumbus.fi;www.kolumbus.fi;UNRESOLVED;ns-se.elisa
.net,ns-fi.elisa.net;mx.kolumbus.fi:0;ns-fi.elisa.net hostmaster.elisa.fi 2009081000 serial 86400 refresh 7200 retry 3600000
expire 172800 minimum;1250571909;YES
193.229.0.49;3336;FI;abuse@elisa.fi;ripencc;1995-12-15;193.229.0.0/16;ns-fi.elisa.net;ns-fi.elisa.net;UNRESOLVED;ns-fi.elisa.
net,ns-se.elisa.net;UNRESOLVED;ns-fi.elisa.net hostmaster.elisa.fi 2009061700 serial 86400 refresh 7200 retry 3600000 expire
172800 minimum;1250571911;NO
193.229.0.46;3336;FI;abuse@elisa.fi;ripencc;1995-12-15;193.229.0.0/16;mail.kolumbus.fi;mail.kolumbus.fi;UNRESOLVED;ns-fi.elis
a.net,ns-se.elisa.net;mail.kolumbus.fi:0;ns-fi.elisa.net hostmaster.elisa.fi 2009081000 serial 86400 refresh 7200 retry 36000
00 expire 172800 minimum;1250571911;NO
195.10.132.100;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-22;195.10.128.0/18;ns2.songnet.fi;ns2.
songnet.fi;UNRESOLVED;ns1.songnet.fi,ns2.songnet.fi,ns3.songnet.fi;mx1.song.fi:0,mx2.song.fi:0;ns1.songnet.fi hostmaster.song
net.fi 2009081700 serial 28800 refresh 7200 retry 1209600 expire 86400 minimum;1250571912;NO
193.229.9.131;3336;FI;abuse@elisa.fi;ripencc;1995-12-15;193.229.0.0/16;vweb1.kolumbus.fi;www.r[redacted]a.fi;vweb1.kolumbus.fi
;ns-fi.elisa.net,ns-se.elisa.net;mail.kolumbus.fi:10;UNRESOLVED;1250571911;YES
193.229.9.131;3336;FI;abuse@elisa.fi;ripencc;1995-12-15;193.229.0.0/16;vweb1.kolumbus.fi;vweb1.kolumbus.fi;UNRESOLVED;ns-se.e
lisa.net,ns-fi.elisa.net;mail.kolumbus.fi:10;ns-fi.elisa.net hostmaster.elisa.fi 2009081000 serial 86400 refresh 7200 retry 3
600000 expire 172800 minimum;1250571911;NO
194.100.2.104;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1994-10-07;194.100.0.0/16;mx1.tdc.fi;mx1.tdc.fi
;UNRESOLVED;ns-fi.sn.net,ns-no.sn.net,ns-se.sn.net;UNRESOLVED;ns-fi.sn.net hostmaster.song.fi 2009081701 serial 28800 refresh
 7200 retry 1209600 expire 86400 minimum;1250571912;NO
194.100.2.104;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1994-10-07;194.100.0.0/16;mx1.tdc.fi;mx1.song.f
i;UNRESOLVED;ns3.songnet.fi,ns1.songnet.fi,ns2.songnet.fi;UNRESOLVED;ns1.songnet.fi hostmaster.songnet.fi 2009081601 serial 2
8800 refresh 7200 retry 1209600 expire 21600 minimum;1250571912;NO
62.73.58.160;16044;FI;abuse@teliasonera.com;ripencc;2002-10-11;62.73.32.0/19;personal.int2000.net;personal.int2000.net;UNRESO
LVED;ns.daous.com,ns2.daous.com;UNRESOLVED;ns.daous.com postmaster.daous.com 2005031078 serial 28800 refresh 7200 retry 60480
0 expire 600 minimum;1250571912;NO
62.73.58.160;16044;FI;abuse@teliasonera.com;ripencc;2002-10-11;62.73.32.0/19;personal.int2000.net;u[redacted]a.net;UNRESOLVED;
ns.daous.com,ns2.daous.com;mx6.nuoli.com:10;ns.daous.com postmaster.daous.com 2005022510 serial 28800 refresh 7200 retry 6048
00 expire 600 minimum;1250571912;NO
62.73.58.160;16044;FI;abuse@teliasonera.com;ripencc;2002-10-11;62.73.32.0/19;personal.int2000.net;www.u[redacted]a.net;u[redacted]
[redacted]a.net;ns2.daous.com,ns.daous.com;mx6.nuoli.com:10;ns.daous.com postmaster.daous.com 2005022510 serial 28800 refresh 7200 r
etry 604800 expire 600 minimum;1250571912;YES
195.10.132.70;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-22;195.10.128.0/18;mx2.tdc.fi;mx2.song.
fi;UNRESOLVED;ns2.songnet.fi,ns3.songnet.fi,ns1.songnet.fi;UNRESOLVED;ns1.songnet.fi hostmaster.songnet.fi 2009081601 serial
28800 refresh 7200 retry 1209600 expire 21600 minimum;1250571912;NO
195.10.132.70;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-22;195.10.128.0/18;mx2.tdc.fi;mx2.tdc.f
i;UNRESOLVED;ns-se.sn.net,ns-fi.sn.net,ns-no.sn.net;UNRESOLVED;ns-fi.sn.net hostmaster.song.fi 2009081701 serial 28800 refres
h 7200 retry 1209600 expire 86400 minimum;1250571912;NO
195.10.143.2;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-22;195.10.128.0/18;ns-fi.sn.net;ns-fi.sn
.net;UNRESOLVED;ns1.songnet.fi,ns2.songnet.fi,ns3.songnet.fi;UNRESOLVED;ns1.songnet.fi hostmaster.songnet.fi 2009081700 seria
l 28800 refresh 7200 retry 1209600 expire 86400 minimum;1250571913;NO
194.100.94.101;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-04;194.100.0.0/16;joshua.w2u.org;named
.kotisivut.com;UNRESOLVED;c.ns.kotisivut.com,a.ns.kotisivut.com,b.ns.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com hostmaster.k
otisivut.com 2009081302 serial 1800 refresh 600 retry 86400 expire 1800 minimum;1250571912;NO
194.100.94.101;3292;FI;abuse@tele.dk,abuse@post.tele.dk,csirt@csirt.dk;ripencc;1996-10-04;194.100.0.0/16;joshua.w2u.org;joshu
a.w2u.org;UNRESOLVED;a.ns.kotisivut.com,b.ns.kotisivut.com,c.ns.kotisivut.com;UNRESOLVED;a.ns.kotisivut.com hostmaster.kotisi
vut.com 2007040101 serial 28800 refresh 3600 retry 604800 expire 86400 minimum;1250571912;NO
UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;29.0-25.97.100.194.in-addr.arpa;UNRES
OLVED;UNRESOLVED;UNRESOLVED;ns6.masterplanet.fi hostmaster.masterplanet.fi 2007012742 serial 28800 refresh 14400 retry 360000
0 expire 86400 minimum;1250571913;NO
UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;28.0-63.218.182.212.in-addr.arpa;UNRE
SOLVED;UNRESOLVED;UNRESOLVED;ns.daous.com postmaster.daous.com 2006110216 serial 28800 refresh 7200 retry 604800 expire 600 m
inimum;1250571913;NO
UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;134.128-255.58.73.62.in-addr.arpa;UNR
ESOLVED;UNRESOLVED;UNRESOLVED;ns.daous.com postmaster.daous.com 2005101028 serial 28800 refresh 7200 retry 604800 expire 600
minimum;1250571913;NO
UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;66.0-25.97.100.194.in-addr.arpa;UNRES
OLVED;UNRESOLVED;UNRESOLVED;ns6.masterplanet.fi hostmaster.masterplanet.fi 2007012742 serial 28800 refresh 14400 retry 360000
0 expire 86400 minimum;1250571913;NO
UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;2.0-25.97.100.194.in-addr.arpa;UNRESO
LVED;UNRESOLVED;UNRESOLVED;ns6.masterplanet.fi hostmaster.masterplanet.fi 2007012742 serial 28800 refresh 14400 retry 3600000
 expire 86400 minimum;1250571913;NO
UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;UNRESOLVED;160.128-255.58.73.62.in-addr.arpa;UNR
ESOLVED;UNRESOLVED;UNRESOLVED;ns.daous.com postmaster.daous.com 2005101028 serial 28800 refresh 7200 retry 604800 expire 600
minimum;1250571913;NO

Testing for the existence of malware
http://www.s[redacted]i.com/ Tue, 18 Aug 2009 05:05:13 +0000
200
Found AS contacts for AS 39324: [redacted]
Testing for the existence of malware
http://www.kolumbus.fi/r[redacted]i/ Tue, 18 Aug 2009 05:05:13 +0000
200
Found AS contacts for AS 3336: abuse@elisa.fi
Testing for the existence of malware
http://www.7[redacted]s.com/ Tue, 18 Aug 2009 05:05:14 +0000
200
Found AS contacts for AS 3336: abuse@elisa.fi
Testing for the existence of malware
http://www.r[redacted]a.fi Tue, 18 Aug 2009 05:05:14 +0000
200
Found AS contacts for AS 3336: abuse@elisa.fi
Testing for the existence of malware
http://www.u[redacted]a.net/H[redacted]u/ - malware taken off siteTue, 18 Aug 2009 05:05:14 +0000
403
http://www.u[redacted]a.net/ - malware taken off siteTue, 18 Aug 2009 05:05:14 +0000
403

Testing for the existence of malware
http://www.k[redacted]s.fi/index.php Tue, 18 Aug 2009 05:05:14 +0000
200
Found AS contacts for AS 16023: [redacted]
```

Appendix IV Sample Autoreporter output

Incident reports produced by Autoreporter [20],[46],[47] contain several complementary data formats to suit the varying needs of the recipients. The only supported transport method is e-mail. This sample output produced by Autoreporter has been filed under incident ticket *[FICORA #378078]* [122]. Portions indicating passwords or potentially revealing personal information have been redacted.

Human-readable portion

For the benefit of human handlers the message body contains explanation of the reporting format and a short introduction to the handling of the given incident type. Identical texts are provided in Finnish, Swedish and English to suit both domestic and international recipients. The recipient is advised to visit a special web site maintained by CERT-FI to find more detailed descriptions of the various incident types. The URL and associated passwords have been redacted to protect the data sources.

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

CERT-FI:n saamien tietojen mukaan alla olevissa verkkonne
IP-osoitteissa on havaittu ongelmia. Ongelmiin liittyvät tiedot
ovat mukana myös liitetiedostoina sekä CSV- että XML-muodossa.
Aikaleimat ovat UTC:ta.

Alla esitetyt tiedot ovat seuraavassa muodossa:
ASN | IP | TIMESTAMP (UTC) | PTR/DNAME | CC | TYPE | CASE | INFO

Tässä CC tarkoittaa maakoodia, TYPE havaitun ongelman tyyppiä ja
CASE CERT-FI:n tapaukselle asettamaa tapausnumeroa. INFO-sarake on
varattu lisätietoja varten. Kyseinen sarake sisältää aina raportin
tietolähteen anonyymin tunnisteen (Datasource).
Ongelmien eri tyypit ja niihin liittyvät mahdolliset lisätiedot
ovat kuvattu tarkemmin osoitteessa:
https://www.cert.fi/[redacted]
Tarvittava käyttäjätunnus/salasana on: [redacted]

Tämä raportti sekä raportin liitetiedostot ovat sähköisesti
allekirjoitettu Autoreporter-palvelun PGP-avaimella. Avaimen voi
noutaa osoitteesta:
https://www.cert.fi/attachments/pgpavaimet/5kesJKIXH/CERT-FI_Autoreporter.txt

Tarkempia tietoja voi tarvittaessa kysyä CERT-FI:ltä.
- - - -

CERT-FI har mottagit information om eventuella datasäkerhetsproblem
gällande IP-adresser i ert nätverk. Informationen är även inkluderad
som bilagor i både CSV- and XML-format. Tidsangivelsen är i UTC-tid.

Informationen här under är given enligt följande format:
ASN | IP | TIMESTAMP (UTC) | PTR/DNAME | CC | TYPE | CASE | INFO

Fältet med CC indikerar landskod, TYPE indikerar vilken typ av
problem det är fråga om och CASE-fältet innehåller det nummer
CERT-FI har gett åt detta fall. INFO-fältet är reserverat för
eventuell tilläggsinformation. Fältet innehåller alltid ett anonymt
id-värde som uppger rapportens datakälla (Datasource).
Ytterligare information om de olika problemtyperna samt om den
eventuella tilläggsinformationen finns tillgänglig på adressen:
https://www.cert.fi/[redacted]
Logga in med användarnamn/lösenord: [redacted]

Denna rapport samt de inkluderade bilagorna är elektroniskt
```

```
signerade med Autoreporter-tjänstens PGP-nyckel. Nyckeln kan laddas
ned på adressen:
https://www.cert.fi/attachments/pgpavaimet/5kesJKIXH/CERT-FI_Autoreporter.txt

Var vänlig och kontakta CERT-FI om ytterligare information behövs.
- - - -

CERT-FI has received information regarding IP-addresses in your
network which may have security problems. The information regarding
the problems is also included as attachments in both CSV and XML
formats. All timestamps are according to UTC.

The information below is presented in the following format:
ASN | IP | TIMESTAMP (UTC) | PTR/DNAME | CC | TYPE | CASE | INFO

Here CC refers to the country code, TYPE to the type of the security
problem, and CASE to the tracking number CERT-FI has assigned to this
case. The INFO column is reserved for any additional information. The
column always includes an anonymous identifier for the datasource
that is used in the report.
The different types and any additional information are described in
more detail on:
https://www.cert.fi/[redacted]
Login with username/password: [redacted]

This report and the included attachments are electronically signed
using the PGP-key of Autoreporter. The key is available at:
https://www.cert.fi/attachments/pgpavaimet/5kesJKIXH/CERT-FI_Autoreporter.txt

If more information is needed, please contact CERT-FI.
- - - -

15496 | 130.233.1[redacted] | 2010-04-26 12:30:20 | | FI | Bot | 378078 | Datasource: B,
downadup srcport: 1251, Request: GET /search?q=0 HTTP/1.0
15496 | 130.233.1[redacted] | 2010-04-26 14:46:28 | | FI | Bot | 378078 | Datasource: B, d
ownadup C&C: 149.20.56.32:80, srcport: 3068, Request: GET /search?q=0 HTTP/1.0


Regards,

CERT-FI Autoreporter
CERT-FI duty desk: +358 9 6966 510
E-mail: cert@ficora.fi

- ----------------------------------------
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.2.2 (GNU/Linux)

iD8DBQFL18D9C0cbSwHiACsRAnhJAJ9pTq0giJWbwt6hBCLkTuwht3zqJgCghzhe
QmlkF8ZwA0nXikZquRDhbO4=
=prI3
-----END PGP SIGNATURE-----
```

Following the message body is a set of MIME encoded attachments containing CSV and XML representation of the same data. The attachments are PGP signed.

Data formatted using CSV notation

Instead of using comma to separate the columns the CSV file is actually using pipe symbol as seen in the snippet below.

```
15496 | 130.233.1[redacted] | 2010-04-26 12:30:20 | | FI | Bot | 378078 | Datasource: B,
 downadup srcport: 1251, Request: GET /search?q=0 HTTP/1.0
15496 | 130.233.1[redacted] | 2010-04-26 14:46:28 | | FI | Bot | 378078 | Datasource: B,
 downadup C&C: 149.20.56.32:80, srcport: 3068, Request: GET /search?q=0 HTTP/1.0
```

XML formatted report in IODEF notation

XML version of the same report uses IODEF compatible representation. This reporting format is meant for automated processing of the incident reports.


```
<?xml version="1.0" ?>
<IODEF-Document lang="en" version="1.00" xmlns="urn:ietf:params:xml:ns:iodef-1.0" xmlns:
xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="https://www.cert.fi/
[redacted]"><Incident purpose="mitigation"><IncidentID name="https://www.cert.fi/">378078
</IncidentID><ReportTime>2010-04-26T12:30:20+00:00</ReportTime><Assessment><Impact lang=
"en" type="admin">Datasource: B, downadup srcport: 1251, Request: GET /search?q=0 HTTP/1
.0</Impact></Assessment><Contact role="creator" type="organization"><ContactName>CERT-FI
</ContactName><Email>cert@ficora.fi</Email><Telephone>+35896966510</Telephone></Contact>
<EventData><Description>Bot</Description><Expectation action="investigate"/><EventData><
Flow><System category="source"><Node><Address category="ipv4-addr">130.233.1[redacted]</A
ddress><Address category="asn">15496</Address></Node></System></Flow></EventData></Event
Data></Incident><Incident purpose="mitigation"><IncidentID name="https://www.cert.fi/">3
78078</IncidentID><ReportTime>2010-04-26T14:46:28+00:00</ReportTime><Assessment><Impact
lang="en" type="admin">Datasource: B, downadup C&amp;amp;C: 149.20.56.32:80, srcport: 3068,
Request: GET /search?q=0 HTTP/1.0</Impact></Assessment><Contact role="creator" type="org
anization"><ContactName>CERT-FI</ContactName><Email>cert@ficora.fi</Email><Telephone>+35
896966510</Telephone></Contact><EventData><Description>Bot</Description><Expectation act
ion="investigate"/><EventData><Flow><System category="source"><Node><Address category="i
pv4-addr">130.233.1[redacted]</Address><Address category="asn">15496</Address></Node></Sy
stem></Flow></EventData></EventData></Incident></IODEF-Document>
```


For the benefit of the reader, Figure 34 exhibits the same XML report as above, but formatted in a way more comprehensible to humans.

```
<?xml version="1.0" ?>
- <IODEF-Document lang="en" version="1.00" xmlns="urn:ietf:params:xml:ns:iodef-1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  - <Incident purpose="mitigation">
      <IncidentID name="https://www.cert.fi/">378078</IncidentID>
      <ReportTime>2010-04-26T12:30:20+00:00</ReportTime>
    - <Assessment>
        <Impact lang="en" type="admin">Datasource: B, downadup srcport: 1251, Request: GET /search?q=0 HTTP/1.0</Impact>
      </Assessment>
    - <Contact role="creator" type="organization">
        <ContactName>CERT-FI</ContactName>
        <Email>cert@ficora.fi</Email>
        <Telephone>+35896966510</Telephone>
      </Contact>
    - <EventData>
        <Description>Bot</Description>
        <Expectation action="investigate" />
      - <EventData>
        - <Flow>
          - <System category="source">
            - <Node>
                <Address category="ipv4-addr">130.233.1[redacted]</Address>
                <Address category="asn">15496</Address>
              </Node>
            </System>
          </Flow>
        </EventData>
      </EventData>
    </Incident>
  - <Incident purpose="mitigation">
      <IncidentID name="https://www.cert.fi/">378078</IncidentID>
      <ReportTime>2010-04-26T14:46:28+00:00</ReportTime>
    - <Assessment>
        <Impact lang="en" type="admin">Datasource: B, downadup C&C: 149.20.56.32:80, srcport: 3068, Request: GET /search?q=0 HTTP/1.0</Impact>
      </Assessment>
    - <Contact role="creator" type="organization">
        <ContactName>CERT-FI</ContactName>
        <Email>cert@ficora.fi</Email>
        <Telephone>+35896966510</Telephone>
      </Contact>
    - <EventData>
        <Description>Bot</Description>
        <Expectation action="investigate" />
      - <EventData>
        - <Flow>
          - <System category="source">
            - <Node>
                <Address category="ipv4-addr">130.233.1[redacted]</Address>
                <Address category="asn">15496</Address>
              </Node>
            </System>
          </Flow>
        </EventData>
      </EventData>
    </Incident>
</IODEF-Document>
```


Figure 34 – XML report produced by Autoreporter. The rendering is done using Internet Explorer 8.