PhiGARo: Automatic Phishing Detection and Incident Response Framework

Martin Husák, Jakub Čegan

{husakm|cegan}@ics.muni.cz

ECTCM 2014

Fribourg, Switzerland

Outline

- Introduction,
- Phishing incident response,
- PhiGARo (phishing incident response tool),
- Phishing honeypots (work in progress),
- Conclusion.

Research Questions

Question I.

How can we effectively handle a phishing incident?

Question II.

Can we automate phishing incident handling?

Question III.

Can we automate phishing incident reporting?

Question IV.

How can we attract phishers to phishing sensors?

Masaryk University

- 40,000 users,
- 15,000 active IP addresses a day,
- Many faculties, subnets, and local administrators,
- 1 security department – CSIRT-MU.

- Not applying strict firewall or e-mail filtering rules,
- Emphasis on open network and academic freedom.

- >100 reported phishing incidents per year,
- Unknown number of unreported incidents.

Tools of the Trade

- Central security contact point,
- Interaction with end-users and local administrators,
- Request tracking software (RT),
- 24 network probes (NetFlow, IPFIX),
- Custom NetFlow analysis tools as an output of R&D.

Phishing incident response

Question I.

How can we effectively handle a phishing incident?

Question II.

Can we automate phishing incident handling?

Question III.

Can we automate phishing incident reporting?

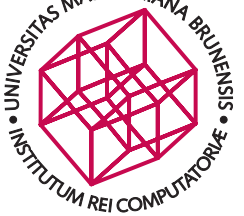
Question IV.

How can we attract phishers to phishing sensors?

Phishing incident response

1. Incident is reported,
2. Searching for victims – checking mailserver logs and network monitoring data,
3. Interpreting the result, filtering false positives,
4. Mitigation – restricting access to phishing websites, filtering e-mails,
5. Send warning to victims,
6. Receive confirmation from victims.

Phishing incident response



- We rely on reports from users,
- Manual handling requires experienced worker,
- The process is laborious and time consuming,
- It may be too late to mitigate the attack.

Phishing incident response

Question I.

How can we effectively handle a phishing incident?

Question II.

Can we automate phishing incident handling?

Question III.

Can we automate phishing incident reporting?

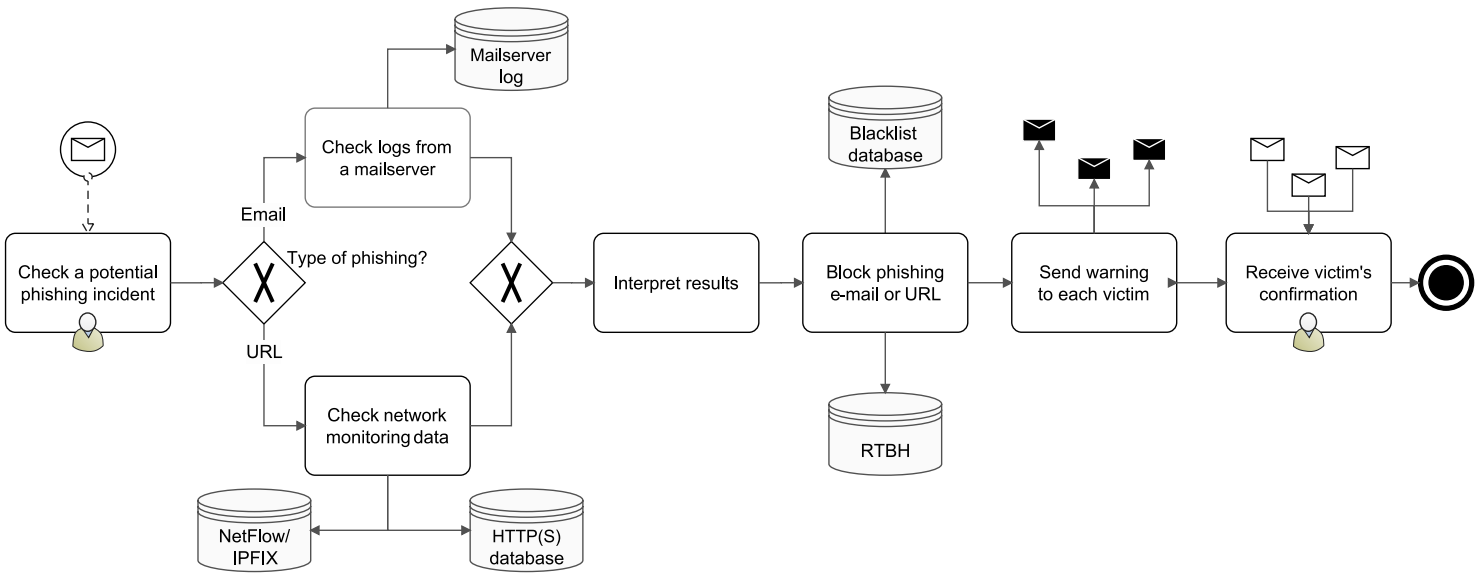
Question IV.

How can we attract phishers to phishing sensors?

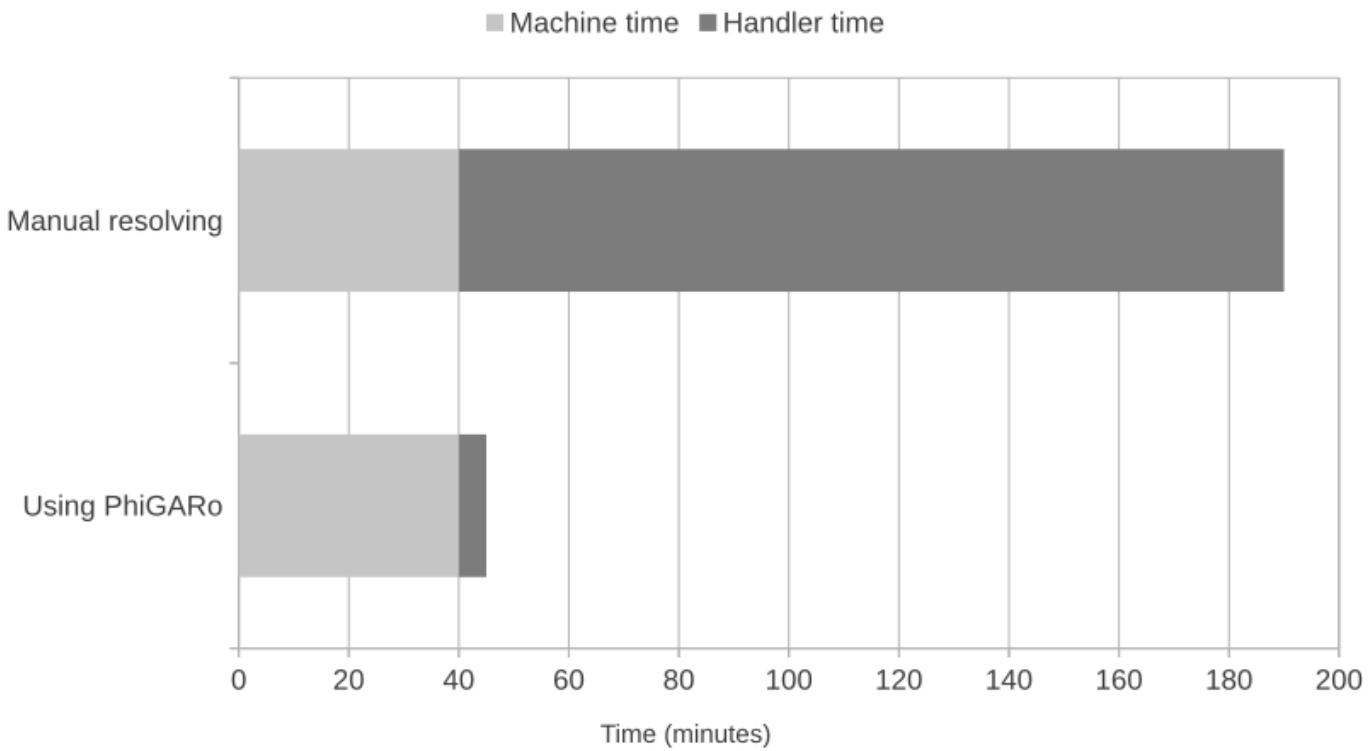
PhiGARo

- Phishing: Gather, Analyze, React, and Distribute,
- Semi-automatic phishing incident response tool,
- Modular architecture,
- Incident handler runs PhiGARo after receiving phishing report,
- PhiGARo performs the incident handling routine,
- Incident handler receives confirmation from victims.

PhiGARo


Mailserver log
Check logs from a mailserver
Email
Check a potential phishing incident
Type of phishing?
URL
Check network monitoring data
NetFlow/ IPFIX
HTTP(S) database
Blacklist database
Interpret results
Block phishing e-mail or URL
RTBH
Send warning to each victim
Receive victim's confirmation

PhiGARo


Machine time
Handler time
Manual resolving
Using PhiGARo
0
20
40
60
80
100
120
140
160
180
200
Time (minutes)

PhiGARo modules

- Request Tracker integration,
- URL expander and URL redirection uncloaking,
- Sendmail log parsing module,
- NetFlow/IPFIX module (network traffic monitoring),
- HTTP(S) module (extended flow monitoring),
- E-mail blocking API,
- RTBH API (blocking of network traffic),
- Reporting phishing hosted on Google Docs,
- Storage of phishing pages (screenshots),
- Phishing form filling simulator.

Phishing detection

Question I.

How can we effectively handle a phishing incident?

Question II.

Can we automate phishing incident handling?

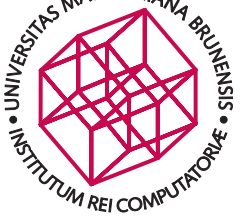
Question III.

Can we automate phishing incident reporting?

Question IV.

How can we attract phishers to phishing sensors?

Phishing detection

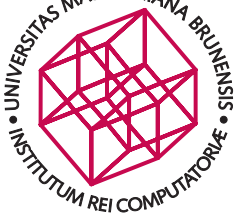


- Reliance on user reports is insufficient,
- Existing methods focus on filtering e-mail on mailservers or mailboxes,
- Keyword search, data mining, machine learning...
- Maintaining common phishing reporting tool in large networks is difficult.

Honeypots

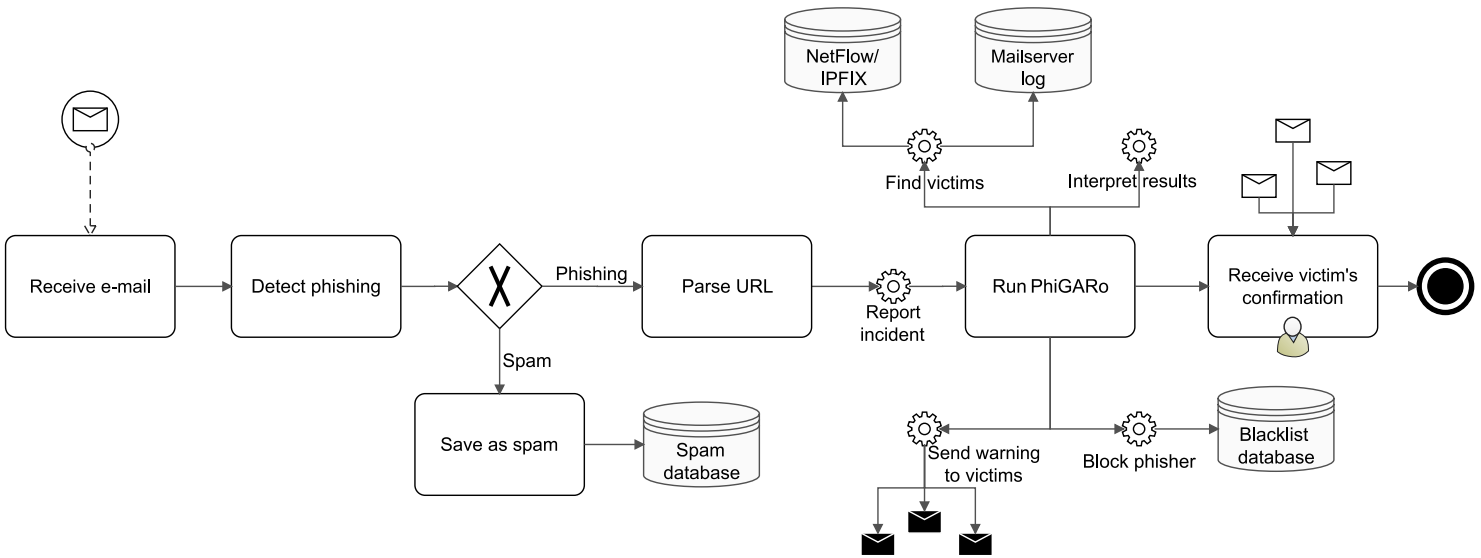
- System resources whose value lies in illicit use,
- Honeypots are generally free of false positives,
- Spamtrap – honeypot e-mail address or mailserver deployed to collect spam,
- Honeytoken – e-mail address, account name…

Honeypots



- Mailserver honeypot is deployed in the network,
- Phishing detection method is set up at the honeypot,
- Incoming e-mails are checked if they contain phishing,
- Recognized phishing is reported to PhiGARo,
- PhiGARo automatically starts handling the incident.

Phishing detection



Attracting attackers

Question I.

How can we effectively handle a phishing incident?

Question II.

Can we automate phishing incident handling?

Question III.

Can we automate phishing incident reporting?

Question IV.

How can we attract phishers to phishing sensors?

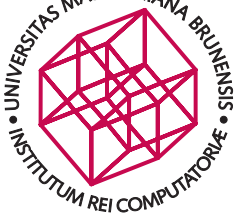
Attracting attackers

- Honeytokens are placed to be accessible by web crawlers, e-mail harvester…
- Responding to earlier phishing from honeytoken e-mail addresses,
- Using PhiGARo to respond automatically (extension of form filling simulator),
- Black market poisoning (advanced).

Attracting attackers

- Concept of *Virtual organization*,
- Custom domain, honeytokens, web content, etc. assigned to honeypots,
- Increasing trustworthiness of a honeypots and honeytokens,
- Adversary checks the domain, visits website, and is persuaded that the honeytokens are valid.

Conclusion



- **Manual phishing incident handling is laborious.**
- **The process of incident handling is automated by the phishing incident response tool PhiGARo.**
- **PhiGARo is publicly available as a modular tool at:** `http://www.muni.cz/ics/services/csirt/tools/phigaro?lang=en`
- **We propose using honeypots to overcome reliance on user reports.**
- **A concept of *Virtual organization* was discussed to attract phishers to honeypots.**

Thank you for your attention.

Martin Husák, Jakub Čegan
{husakm|cegan}@ics.muni.cz