# From ZeuS to Zitmo: Trends in Banking Malware[1]

Najla Etaher[1], George R S Weir[1] and Mamoun Alazab[2]

[1]Department of Computer and Information Sciences
University of Strathclyde
Glasgow, UK
{najla.etaher, george.weir}@strath.ac.uk

[2]Australian National University
Canberra ACT 2601, Australia
mamoun.alazab@anu.edu.au

**Abstract**. In the crimeware world, financial botnets are a global threat to banking organizations. Such malware purposely performs financial fraud and steals critical information from clients' computers. A common example of banking malware is the ZeuS botnet. Recently, variants of this malware have targeted mobile platforms, as The-ZeuS-in-the-Mobile or Zitmo. With the rise in mobile systems, platform security is becoming a major concern across the mobile world, with rising incidence of compromising Android devices. In similar vein, there have been mobile botnet attacks on iPhones, Blackberry and Symbian devices. In this setting, we report on trends and developments of ZeuS and its variants.

## I Introduction

Banks in many countries now provide access through the Internet to customer accounts. Such online services reduce the need for expensive retail offices and paper transactions. More recently, mobile platforms have established another channel for online banking, but these developments mean that financial services have become subject to new varieties of online attack.

From such opportunities, underground markets have arisen through which cybercrooks trade services, such as spam, stolen credit card numbers, and do-it-yourself botnet kits. The most popular DIY botnet kit is financial malware such as ZeuS [1]. Several other types of financial malware have been observed in the wild, including Slapper, Coreflood, Kraken, Sinit, Nugache, Rustock, Conficker, Blackhole and NGR. Such malware is considered the most serious threat to internet security, because it gives perpetrators the potential to remotely control a large number of computers. ZeuS and

[1] This is an authors' draft of a paper published in TrustCom 2015: The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp 1386-1391.

its family are the most advanced credential-stealing Trojans that have been found on the Internet.

In this paper, Section II describes ZeuS and its family of Trojans. In section III, we describe two types of botnet and in particular, mobile botnets. Following this, we discuss predictions on the development of Zeus and its ilk.

# II ZeuS

## *A.* History of ZeuS

The ZeuS Trojan, also called Zbot, WSNPOEM, NTOS, or PRG is the primary malicious software affecting the financial sector, both in terms of its effectiveness and infection rate. Symantec calls this malware "ZeuS, King of the Underground Crime-ware Toolkits" [2]. This banking Trojan first appeared in 2007. In May of 2011, the full source code for the ZeuS toolkit was leaked onto various Internet sites. The availability of this source code is a significant feature that has resulted in an explosion of new variants from the original ZeuS malware [3], and led to the development of several centralized Trojans based on ZeuS, such as ICE IX, KINS, and the more successful Citadel. Also, decentralized Trojans based on ZeuS appeared in September 2011, known also as P2P ZeuS or GameoverZeuS this variety uses a decentralized network infrastructure of compromised personal computers and web servers to execute command-and-control. In May 2014, the Justice Department brought charges against the alleged author of the ZeuS Trojan Evgeniy Mikhailovich Bogachev of Anapa, Russian Federation. In June 2014, the Justice Department launched a multi-national effort to take down the GameoverZeuS and CryptoLocker botnet infrastructures.

The ZeuS Trojan penetrates large numbers of computers to steal data by logging keystrokes and copies of itself to other computers via instant and email messages. Once installed, hackers can control and monitor infected devices to obtain access to unauthorized data such as online accounts and credentials. As ZeuS is a credential-stealing Trojans, it is sold through the underground economy in order to offer services to clients, with bug fixes to the first ZeuS codebase and with different features, for instance, video recording and sandbox detection. The first two variations are based on centralized command and control (C&C) servers. The security community now has the ability to track these command servers and block them. ZeuS botnets have been found responsible for 44% of online malware infections during financial transactions and for approximately 90% of global banking fraud [2]. There were about 3.6 million computers infected by ZeuS in the USA alone during the period of 2009 and 2010. This era is considered the most productive period for ZeuS [4].

The ZeuS Trojan is extremely dynamic and applies obfuscation techniques such as polymorphic, metamorphic encryption and packers in a network of bots [2, 40]. In order to defeat signature-based detection techniques, ZeuS re-encrypts itself automatically in each infection, thereby creating a new signature. Through this concealment facility, ZeuS is able to hide malicious intent and effectively avoid malware signature detection.

The ZeuS toolkit can be used to produce a strain of Trojans designed to damage and steal information. Stealing details for online banking and other login credentials is the major focus of ZeuS. The ZeuS kit can be obtained from underground forums, with older versions available for free, and the newest versions costing many thousands of dollars [5]. The impact of ZeuS infection can be very costly to an organization and differs to that of individuals. Since ZeuS first emerged in 2007, it has continued in its goal of information theft, however, there have been several obvious changes in how it addresses this aim. ZeuS is simple to use and requires minimal technical knowledge [5]. Due to its competitive price and its user-friendly interface, the ZeuS crime-ware toolkit has become a preferred tools for attackers [4]. Banking details, or theft of personal login details can feel terrible to an individual, whereas the impact of infection for an organization can be devastating.

### *B.* ZeuS Functionality

The key purpose of the ZeuS Trojan is to steal online credentials, as specified by the attacker. Among the many actions it performs are information system gathering, online credential information stealing, C&C server contacting and protected storage information stealing [6]. Although technically ZeuS is a crime-ware kit designed to steal money, from other perspectives, it is a new online illegal business enterprise. Within this enterprise different organizations can cooperate in order to commit complex online fraud and theft. This becomes a component in organized cybercriminal organizations. In fact, Eastern European Organized Crime is the cybercriminal underground that is behind ZeuS. Generally, the top ZeuS domains live in Ukraine and Russia [7].

### *C.* ZeuS Crime-ware Tool Components

To steal money, the ZeuS toolkit takes control of devices and causes them to act as spying agents. There are five components that make up the general structure of this toolkit:

1. Control panel: this manages and controls the infected systems and gathers the stolen data and information. It also consists of PHP scripts that observe the botnet and display information to the botmaster.

2. A builder: two files are generated here; the ‘bot.exe’ which is the malware binary and the ‘config.bin’ which is the encrypted configuration file.

3. Configuration files: these comprise two files; the ‘config.txt’ contains crucial configuration information; and the ‘webinjects.txt’ this contains the content injection rules and is responsible for the recognition of targeted websites. The configuration files also modify botnet parameters.

4. Generated encrypted configurations files ‘config.bin’. An encrypted version of the botnet configuration parameters is held in these files.

5. Generated malware binary files ‘bot.exe’. These files infect the victims’ devices as the bot binary [4].

As the ZeuS Trojan is designed to steal sensitive information, it carries a very light foot print. ZeuS is based on the client-server model and requires a C&C server to transfer information through the network. Once a victim’s computer has been infected, stolen data is immediately sent to a bot C&C server through an encrypted ‘HTTP POST’ request. The malware also allows cybercriminals and hackers to inject content into the web page of a bank as it is displayed in the infected computer browser. An infected systems can be controlled remotely, with the stolen data sent to a drop server controlled by the botmaster. ZeuS is a readily available and the most widely-spread malware package contains the required tools to build and control a botnet. While ZeuS mostly operates on computers using Microsoft Windows, Blackberry and Android phones have become targets since 2012 [8, 9].

This banking Trojan spreads through phishing scams, drive-by-downloads and by tricking unsuspecting users into clicking infected links. According to [39], a 2009 survey found that ZeuS had compromised more than 74,000 FTP accounts on websites of businesses worldwide, including NASA, Bank of America, ABC, Business Week, Oracle, Amazon, and Monster.com. After execution, ZeuS automatically gathers any Internet Explorer or FTP passwords contained within Protected Storage [11].

### *D.* ZeuS Variants

GameoverZeuS (P2P): Gameover ZeuS (GOZ) is a further development of the ZeuS Trojan that is built upon a P2P botnet infrastructure. The developers behind P2P ZeuS made several updates to the source code over the years of operating the botnet to improve its resilience against takedown attempts. Cybercriminals used this variant in order to obtain valuable data such as personal information, passwords, credit card numbers, customer data, confidential commercial information or any other data that related to banking [14]. The P2P variant of ZeuS represents a technical evolution away from the centralized botnet model and this infrastructure made disruption and attacker attribution more complicated. Despite this, there are many drawbacks in a P2P network. The decentralized nature of the P2P ZeuS botnet permits investigators to enumerate the infected botnet population by recursively crawling each node's peer list. It is also possible to poison peer lists by injecting fake peer nodes into the P2P network, which has enabled researchers to sinkhole and neutralize P2P botnets (e.g., Storm, Waledac, and Kelihos).

The P2P ZeuS crew receives considerable support from the products and services offered by the underground community, who collectively plan and execute successful cybercriminal operations. Moreover, the large number of available compromised computers and web servers provides a robust and low cost infrastructure for a range of malicious activities [1,12,38].

The single C&C server is a weak point in the malware structural design and it is the target for law enforcement organizations when dealing with ZeuS botnet. To counter this risk, the Zbot variant includes a DGA (domain generation algorithm) that produces

new domain names list to which the bots try to connect in case the C&C server cannot be reached. This feature made the C&C servers difficult and resistant to takedown attempts. The peers in the botnet can act as independent C&C servers and are able to download commands or configuration files between them, as well as sending stolen data to the malicious servers.

P2P ZeuS is known for its resilience to takedowns because of the P2P connection to its C&C server compared with other variants of ZeuS like IceIX, Citadel and KINS, which employ centralized C&C servers. Centralized ZeuS variants are spread as builder kits in the underground market, offering a chance for users to construct their own ZeuS botnet. But this is no longer available for P2P ZeuS, which is based on a single coherent main P2P network separated into numerous virtual sub-botnets by a hardcoded sub-botnet identifier in each bot binary. Whereas the ZeuS P2P network is maintained and sometimes entirely updated, the sub-botnets are independently controlled to accomplish several malicious actions.

Gameover ZeuS is often propagated through spam and phishing messages. Infected machines can perform unauthorized activities such as sending spam, participate in DDoS attacks, and harvest victim credentials for online services, including banking services [13, 36]. This botnet infects networks but, as a result of its polymorphic nature, has a low detection rates and thereby poses a high persistent risk. Once a device is infected, it is difficult to remove this infection because this version of ZeuS contains a Necurs rootkit. According to SophosLabs, this rootkit can be used to better conceal malware files, and make it more difficult to locate or remove the malware once it is active [15].

The latest version of Gameover ZeuS tried to 'gameover' the anti-virus business. However, in June 2014, a large international effort involving enforcement agencies and security firms, blocked the spread of the Gameover ZeuS botnet and managed to control servers that were important for CryptoLocker (discussed later in this section) [16, 17, 8, 9].

Reviewing the extent of the Gameover ZeuS problem, the latest numbers in Heimdal Security database, and according to detectives in the Bank Info Security and Krebson Security, globally almost 1.2 million Microsoft Windows-based computers were infected up until the takedown operation in June 2014. This figure could increase if the botnet infrastructure is restored, and this is a great concern for the security community [18, 19, 20].

*SpyEye*: SpyEye is a Trojan that targets online banking users. By hijacking the user's webcams and microphones, this malware enables cybercriminals to steal users' account credentials and empty their accounts by means of its keylogger. The SkyEye toolkit is widespread among cybercriminals since they can modify it to attack specific institutions or businesses. Once a targeted user starts an online transaction from his bank account, this Trojan is able to start its operation. Similar to its older cousin, ZeuS, SpyEye is no longer being developed by its original author, but is still broadly used by cybercriminals [9, 8].

*Ice IX:* Ice IX is one of the most sophisticated pieces of financial malware. This is ZeuS variant improved upon source code from ZeuS v2, aiming to evade tracker sites that monitor most ZeuS C&C servers [8, 9].

*Citadel*: After the ZeuS source code release in 2011, the Citadel variant appeared as a popular choice in the underground market for use in financial fraud and to commit

complex 'Man-in-the-Browser' attacks. Citadel has built upon the base capabilities of ZeuS and added numerous developments to the malware. This toolkit expanded the scope of application and enabled the targeting of more varieties of web browser. Citadel also provides a platform for other illegal revenue schemes such as installation of ransomware. According to [21], the Citadel code matches around 75% of the original ZeuS while the remaining 25% comprises new features that are unique to Citadel. Primary among these features are: Local Pharming, More function hooks, C&C server side, Trojan's encryption method, and Video-grabbing [8, 17, 22, 9].

*Carberp*: Carberp is a banking Trojan that is considered to be one of the most broadly spread financial malware in Russia. Like other Trojans in the ZeuS family, Carberp commits financial fraud through its ability to steal crucial data from infected devices and download different data from C&C servers. This malware differs from other banking Trojans because it has several legitimate web resources that are used to gather information and possibly make fraudulent transactions. In addition to injecting a code into web pages, Carberp attempts to exploit some vulnerabilities in the operating systems so as to escalate to administrative privileges [8, 9]. Indications are that cybercriminals have botnets on over 25,000 infected devices.

*Bugat*: This is another banking Trojan derived from ZeuS that targets browsing activities and returns information from e-banking sessions. As well as having similar capabilities to the original ZeuS, Bugat can upload files from an infected PC, download and execute code. Bugat communicates with a C&C server, from which it receives instructions and updates to monetary websites. Attackers insert attractive malicious links in the emails they send to targeted victims in order to spread this malware. When the user clicks a malicious link, they are directed to a fraudulent infected website from where the Bugat executable downloads on to the visitor's system. Collected information is sent to the attacker's remote server [8, 9].

*Shylock*: In similar vein, Shylock is financial malware that aims to retrieve bank credentials for fraudulent purposes. Once installed, the remote C&C servers controlled by the cybercriminals communicate with Shylock to send to and receive data from the infected devices. Like P2P ZeuS, this malware uses a domain generation algorithm produce a number of domains that can be used to interact with infected systems and servers. This malware employs two possible attack vectors. The first is by injecting web pages via JavaScript. This generates a pop-up window that has the user download a (malicious) plugin that appears to be essential for the media display on the website. The second attack vector is through drive-by downloads on compromised websites, e.g., by inserting malicious code in advertisements which are then put on legitimate websites - a method known as malicious advertising [8, 9].

*Torpig*: Torpig is another sophisticated and complex variety of financial malware that targets private and financial information, including bank account and credit card details. Torpig botnets may send spam emails and commit unauthorised transactions. In addition, Torpig generates domains names using a domain generation algorithm to locate the C&C servers. The attack vector for this Trojan is drive-by downloads [8, 9]. According to [11], investigation of the largest banking botnets from 2013 shows that 900 financial organizations have been targeted all over the world. This source indicates that Gameover ZeuS has the highest percentage impact at 38%, followed by Citadel with 33 %, then ZeuS with approximately 13%. Most of these malware breaches are at US financial institutions with more than half of these botnets focused on the 25 biggest

financial organizations, not only in the US but also in other mature markets like the UK, Canada, Germany, France, Spain, and Italy [23].

*CryptoLocker*: This is a ransomware Trojan that infects the victim's system via seemingly legitimate email attachment, from a well-known institution or company. This well-known malware encrypts system files and demands a ransom in exchange for the decryption key. Not only does it access private data or steals user's money, but once it encrypts user's information, nobody can decrypt these files again. After encryption, CryptoLocker displays a ransom window stating that the user should pay an amount of money in a specific time in order to recover files. Although CryptoLocker can be removed, the encrypted files cannot be recovered without the key. In addition, CryptoLocker is dangerous since the victims' confidential information is compromised. According to federal authorities, in April 2014 CryptoLocker infected more than 234,000 computers, half of them located in the US [20].

As noted earlier, in June 2014, servers that were important for CryptoLocker were affected by a global takedown effort when the spread of the Gameover ZeuS botnet was blocked. Ransomware continues to evolve, especially in the form of file-encrypting malware. Recently, ransomware has begun to target mobile devices. Availability of malware source code and generation tools has helped cybercrooks to reach mobile platforms [24].

### *E.* Typical spreading method for financial malware

Most financial malware is spread by one of two methods:

- *Drive-by downloads*: a drive-by download happens when the user visits a website or clicks a misleading pop-up window.
- *Spam campaigns*: the user receives an e-mail message from a well-known organization with some false banking information attached or with a link included in the e-mail. Once, the user clicks the link or downloads the attached file to the e-mail, the system will be infected [10,37].

In the next section, we consider the architecture of centralized botnets like ZeuS and decentralized botnets like Gameover ZeuS.

## III Botnets

### *A.* Overview

Botnets pose a serious threat to Internet security. A botnet is a network of compromised machines under the control of a malicious entity, typically referred to as the botmaster. The compromised computers, called bots, are controlled by a C&C server in order to engage in malicious activities such as sending spam, stealing login credentials, stealing personal information or participating in distributed denial of service (DDOS) attacks on other systems (such as government or commercial websites). These bots are

designed to take over many Internet hosts. Botnet threats are complex since the sets of participating computers can be assigned various tasks, including seeking out and infecting further hosts. According to [39], such systems have been used by hackers seeking to bring down web sites such as the British Serious Organized Crime Agency and the US Central Intelligence Agency.

### *B.* Types of Botnets

There are two principal botnet architectures: centralized and peer to peer. Some botnets, like Conficker and ZeuS, change their architectures in new variants from centralized to P2P. Recent botnets mostly use HTTP, TCP and UDP as their communication protocol. However, some botnets, like Gameover ZeuS, use specialised P2P network protocols [16]. Some generic characteristics of several real world botnets (Conficker, Kraken, Rustock, Storm, TDL4, Torpig, Waledac, ZeuS and P2P ZeuS) are described by [24]

#### *1. Centralised botnets.*

The most common type of botnet is the centralized form in which all computers are joined to a single C&C. The C&C looks for new bots to connect, then registers these bots in its database, sends them commands selected by the botnet owner by tracking their status. These botnets are easy to create, to manage and also they respond to instructions very quickly. Nevertheless, centralised botnets are relatively easy to combat. If the C&C is put out of commission, the whole botnet is neutralised. All bots in the centralised botnet are visible to the C&C.

#### *2. Hierarchical (Decentralized or P2P) botnets.*

For centralized botnets, if a bot is found and interrupted, the central C&C server can be recognized. The entire botnet is disabled when the server is taken down. In order to avoid this, and in particular, to overcome the inherent drawback and shortcoming of the centralized botnets, peer-to-peer botnets are designed. P2P technologies have been used to create hierarchical botnets. In a decentralized botnet, bots connect to several infected machines on a bot network rather than to a C&C centre. Instructions are transmitted from one bot to another. Each of them has a list of many neighbours, and any command received by a bot from one of its neighbours will be sent to the other bots, further distributing it across the zombie network. In this case, in order to control the entire botnet by the cybercriminal, they need to have access to at least one computer on the zombie network. Practically, building P2P botnets is a difficult job, because each recently infected device requires to be provided with bots list to which it will connect on the zombie network. Combating centralized botnets is a much easier task than combating decentralized networks as an active P2P botnet has not got a control centre. Botmaster just needs to have control of one bot to control the botnet. Although

disrupting this kind of botnets is difficult, designing and managing this kind of botnets is difficult for the botmaster [25].

### *C.* Mobile Botnets and Malicious Activities

Mobile systems is a fast-developing IT area and, as mobile devices become more widely used, their role and their security is a growing concern internationally. Inevitably, mobile phones and networks are subject to the threat of mobile botnets. A mobile botnet may refer to a collection of compromised smartphones that are under control of botmasters using C&C servers. Although computer-based botnets have become a severe threat to computer systems - as common platforms for some attacks, mobile botnets are presently not as popular for reasons such as resource issues, limited battery power, and Internet access constraints. Accordingly, the occurrence of practical mobile botnets and related research are presently both very limited. Nevertheless, this is likely to change with the spread of smartphones, now used by billions of clients due to their increasing computing ability and efficient Internet access. Furthermore, smartphones are commonly used to store a huge amount of sensitive data that may be used in online payment transactions [26].

Unfortunately, many users do not pay attention to the security updates on these devices so these devices are often not well-protected compared to computers and their networks. Mobile botnets (Mobot) have not yet been widely manifested, as they have only recently migrated to mobile infrastructures. Although these botnets tend to develop rapidly, so do takedowns.

The following section gives examples of current mobile botnets in order to highlight their presence and their negative effects on mobile network environments [27]. The growth of open-source smartphone platforms such as Android affords more opportunity for hackers to perform malicious activities [26].

Mobile botnet attack vectors are investigated by [28]. Through identification of significant parameters from their taxonomy, [28] conducted a comparison to explore effects of existing mobile botnets. Another study by [27], presents an overview of mobile botnets, trends and characteristics through a survey of well-known Android malware applications [29]. The most recent attacks on Android devices are ZeuS in the Mobile or Zitmo, DroidDream, Android.Bmaster, Ikee.B, AnserverBot, TigerBot, and Geimini. There have also been mobile botnet attacks on iPhones (SMS attacks), Blackberry and Symbian devices. This section gives an overview of some recent mobile botnets (summarized in Table 1).

| Botnet Name | Creation/ detection date | Platform | Spread Technique | Functionality | Specific Features |
|---|---|---|---|---|---|
| Ikee.B | November 2009 | Apple iPhone | Self-Propagation | Carries a malicious payload (data exfiltration), and probes C&C for new control instructions, generates revenue and steals private data | Specific Targeted Victims, Specific Geographical Distribution |
| Geimini | December 2010 | Android mobile devices | Opens a back door and transmits information from the device to a specific URL | Steals privacy related info, sends location info, IMEI and IMSI info, sends & reads SMS and erase traces, addresses book to a server, and list of installed apps, downloads and prompts user to install apps, launches a web browser with given URL. | Able to infect legitimate applications |
| Zitmo | September 2010 | Android, Symbian, Windows Mobile, BlackBerry | Infected SMS, social engineering techniques | Unauthorized transactions, including mobile banking attacks, mobile transaction number (mTAN) thefts. | Specific Targeted Victims: European users |
| AnserverBot | September 2011 | Android mobile devices | Trojan Applications, social engineering techniques | Installs backdoor to get sensitive private data, sends fake SMS, uses different techniques to regularly check self-security and integrity | Self-protection, two layers C&C. using Java reflection-based method invocation, self-verification of signatures, aggressive code obfuscation and data encryption, dynamic code loading to evade detection |
| DroidDream | February 2012 | Android mobile devices | Exploit Techniques Trojanised Applications | Rooted phone via Android Debug Bridge vulnerability, sent premium-rate SMS messages at night, download malicious apps, and steals private data | Specific Operational Times: 11 pm to 8 am. |
| Android.Bmaster | February 2012 | Android mobile devices | Exploit Techniques Trojanised Applications | Opens a back door, downloads files, steals potentially confidential info from compromised device, and generates revenue. | Specific geographical dissemination: China. |
| TigerBot | April 2012 | Android mobile devices | Trojanised Applications | Allows remote access & can be controlled via SMS messages. Steals contacts lists & screenshots, changes network settings, and controls running processes. Private data theft; Change Device Settings | Self- Protection |
| HijackRAT | 2014 | Android mobile devices | Downloaded Applications | Steals &sends SMS, initiates nasty app updates, steals contacts, scans for authentic banking apps installed on the victim's device and swap them with imitations utilities, steals banking credentials, private data theft, Spoofing, and remote access. | Masks as 'Google Service Framework', Binds both the newest & older hijacking techniques, tries to deactivate any mobile security/ antivirus software on Android |

Table 1: An overview of recent mobile botnets

ZeuS-in-the-mobile (ZitMo) is an innovative example of mobile malware. The ZeuS botnet has transferred from PCs to mobile devices and as a result targeted online banking. It is designed to use social engineering techniques to steal mobile transaction authorization numbers (mTAN) that are sent in SMS messages by banks to its customers' mobile devices. An SMS is sent with a fake URL asking the user to download a security question that is, in reality, the Zeus-in-the-mobile bot. One of the distinguished features of Zitmo is the range of supported operating systems, such as Symbian, BlackBerry, Windows Mobile, and Android. Small groups of mobile users in several European countries, customers of specific banks, have recently been attacked by Zitmo [27, 29, 25, 30].

DroidDream is a mobile botnet-based malware that first appeared in 2011 and exploits Android-based mobile systems in order to gain root access to these devices to obtain unique identification information such as product ID, or model number of the mobile device. Once the system has been infected, the compromised device can install and download another application and extra executable programs and features without the user noticing, while providing backdoor root access for criminals. The additional application prevents the removal of DroidDream, and then sends sensitive information to its C&C server, such as the user's country, and device model. In order to root the smartphone, DroidDream uses two different tools which are rageagainstthecage and exploid. This Trojan works stealthily, at night, at a time that the mobiles are not used. DroidDream aims to be a quiet Mobot [27, 25, 29, 28, 30].

Android.Bmaster infects mobile phones, through a range of exploits and Trojan applications in order to generate money through telephony, video or SMS services. Symantec has described it as "A Million-Dollar Mobile Botnet" since it has gained millions of dollars through its services [31]. Moreover, this malware records a range of information on the infected users to its C&C server. Recently, criminals and attackers illegally gained millions of dollars using this Trojan. This is due to the high rate of infected mobile phones across the world [27, 25, 30].

IKee.B is a malicious program that targets and infects jail broken iPhones in order to obtain data and information. This botnet is considered to be a proof-of concept that botnets work on mobile phones with nearly the same functionality as computer-based botnets. Dynamically the IKee.B botnet scans the network of the iPhone IP addresses. IKee.B tries a self-propagation technique in order to infect other vulnerable iPhone devices that are located in other countries and sends stolen confidential data to its C&C server in Lithuania over Wi-Fi networks or 3G. When IKee.B is activated on an iPhone, it can change default passwords, send financial information in SMS messages to a remote server and also connect via HTTP to a remote server to download other components. The only defensive action against this infection is to fully reset the iPhone and restore all settings to factory defaults [27, 25, 28, 30].

In 2011, NetQin Security Research Centre identified a sophisticated new Android malware known as AnserverBot. In order to infect mobile phones and steal sensitive data, AnserverBot installs a backdoor. The malware attaches itself to standard applications, sends fake SMS messages and uses social engineering. To evade detection, it employs Java reflection-based method invocation, self-verification of

signatures, aggressive code obfuscation and data encryption, and dynamic code loading, as well as detection and removal of any mobile security software. In addition to regularly checking its own security and integrity, AnserverBot has a double layer C&C tool that operates over public blogs. Installed security software can be detected by AnserverBot and may be deactivated or removed [27, 25, 32, 30]. TigerBot is unusual in being completely controlled via SMS messages. This botnet has the abilities to record calls and to gather private information. C&C messages can be received as SMS messages by TigerBot, and will be invisible to the mobile device user. This malware operates mainly as spyware and uses common application names and icons, such as Google search [27]. Mobile network operators (MNO) might pay more attention to the detection of mobile botnet since they will be affected by losses through malware activity [30].

Geinimi is a backdoor Trojan that has been injected into many different Android applications. Such malware disturbs the normal operation of Android devices and seeks unauthorized access to stored credentials. Geinimi has many capabilities, for example, it can fake legitimate banking applications and steal private information. In addition, can relay location information, download and make the user install applications. This malware also communicates with the server via SMS messages, remove traces, launches a web browser with given URL, sends phone and subscriber information, including the user's address books [29, 28, 33, 30].

The HijackRAT Trojan comes attached to a malicious Android application and combines both the newest and older hijacking methods. HijackRAT masks itself as 'Google Service Framework' and allows hackers remote control of the victim's device. The App can steal and relay SMS messages, initiate malware updates, steal contacts, scan for authentic banking apps and swap them for imitation utilities. HijackRAT also tries to deactivate any antivirus software installed on the infected Android device. [34].

## IV Discussion

ZeuS is the most significant financial malware created so far and there is little evidence that its impact is fading. Because of its wide distribution, ZeuS threatens a broader number of organizations, even outside the financial sector. ZeuS attacks are still occurring and may increase as cybercriminals develop more sophisticated concealment and evasion techniques in order to widen infection to many more users across the globe. Already, the transition to hybrid centralized or hybrid decentralized botnets poses obstacles to takedown. We may also anticipate a move to Cloud-based malware. On the positive side, with recent improvements in anti-malware techniques, the impact of ZeuS functions may be limited. Of course, we should expect more advanced ZeuS versions in due course.

In conjunction with such malware developments, we can expect to see new forms of aggressive attacks, such as water-holing and spear-phishing. As cybercriminals continue to evolve such tactics, security firms must maintain vigilance and strive to

combat such attacks through advances in anti-malware software. More directed development of ZeuS-based botnets may be linked to state-sponsored attacks, with associated loss of international trust, as occurred after Edward Snowden's disclosures.

Although the takedown operation against Gameover ZeuS succeeded in cutting its communication infrastructure, Gameover ZeuS has now switched from P2P infrastructures to DGAs [35, 23]. Two new versions using this evasion technique have been discovered in the wild. Significantly, the Gameover ZeuS botnet was not entirely destroyed, only interrupted. Although the takedown almost quashed the Cryptolocker malware, similar ransomware has since increased in new applications such as Cryptowall and cryptosimple. Furthermore, this variety of malware has recently targeted mobile devices [24].

Indications are that anonymous and untrustworthy app stores will increase as a source of mobile malware, driven by malvertising. Ransomware is expected to spread across a wider range of mobile devices, using more sophisticated measures to avoid early detection and a move to new ransom payment methods with the rise in crypto-currencies.

The ready availability of source code and malware kits has helped cybercrooks target mobile platforms but many cybercriminal groups will continue to target traditional platforms, such as PCs. The prevalence of legacy systems, including MS-Windows, Apple Macintosh and Linux, means that vulnerabilities in operating systems will continue to offer opportunities for malware infection.

## V Conclusion

ZeuS is the most significant banking malware currently in existence. It is a crime-ware tool that aims at stealing users' online banking credentials. This Trojan is still evolving and will continue to pose a serious threat to online users and organisations. The scope of threat from ZeuS and its derivatives has been growing as the functionality of its toolkit expands. Mobile malware is a new frontier and the rise in mobile devices means a rise in mobile botnets. All internet and mobile device users are potential targets and the threat will increase as malware continues to extend in functionality, availability and ease of use.

### REFERENCES

[1] Stone-Gross, B., Dell SecureWorks Counter Threat Unit (TM) Threat Intelligence (2012). Dell Secureworks. The lifecycle of Peer-to-Peer (Gameover) ZeuS. Available at

http://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/

[2] Alazab, M., Venkatraman, S., Watters, P., Alazab, M., & Alazab, A. (2012). Cybercrime: the case of obfuscated malware. In *Global Security, Safety and Sustainability & e-Democracy* (pp. 204-211). Springer Berlin Heidelberg.

[3] Kruse, P. (2011). Csis: Complete ZeuS Sourcecode Has Been Leaked to the Masses. Available at https://http://www.csis.dk/en/csis/blog/3229/

[4] Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M., & Wang, L. (2010, August). On the analysis of the ZeuS botnet crimeware toolkit. In *Privacy Security and Trust (PST),2010 Eighth Annual International Conference on* (pp. 31-38). IEEE.

[5] Wyke, J. (2011). What is ZeuS?. *A Sophos Labs technical paper.*

[6] Falliere, N., & Chien, E. (2009). ZeuS: King of the Bots. *Symantec Security Response (http://bit. ly/3VyFV1)*.

[7] Micro, I. T. (2010). ZeuS: A persistent criminal enterprise. *Retrieved February*,*6*, 2011.

[8] Heimdal Security, (2014a). The Top 10 Most Dangerous Malware That Can Empty Your Bank Account. Available at https://heimdalsecurity.com/blog/top-financial-malware/

[9] Secureworks (2013). Top Banking Botnets of 2013. Available at http://www.secureworks.com/cyber-threat-intelligence/threats/top-banking-botnets-of-2013/

[10] Alazab, M., Layton, R., Broadhurst, R., & Bouhours, B. (2013, November). Malicious Spam Emails Developments and Authorship Attribution. In*Cybercrime and Trustworthy Computing Workshop (CTC), 2013 Fourth* (pp. 58-68). IEEE.

[11] SecureWorks(2010). SecureWorks Counter Threat Unit SM (CTU). ZeuS Banking Trojan Report. Available at http://www.secureworks.com/cyber-threat-intelligence/threats/ZeuS/

[12] Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An Analysis of the Nature of Groups Engaged in Cyber Crime. *An Analysis of the Nature of Groups engaged in Cyber Crime, International Journal of Cyber Criminology*, *8*(1), 1-20.

[13] US-CERT (2014).GameoverZeuSP2P Malware. Available at https://www.us-cert.gov/ncas/alerts/TA14-150A.

[14] Alazab, M. (2015). Profiling and classifying the behavior of malicious codes.*Journal of Systems and Software*, *100*, 91-102.

[15] SophosLabs, (2014). SophosLabs: Gameover banking malware now has a rootkit for better concealment. Available at http://blogs.sophos.com/2014/03/04/sophoslabs-gameover-banking-malware-now-has-a-rootkit-for-better-concealment/.

[16] Andriesse, D., Rossow, C., Stone-Gross, B., Plohmann, D., & Bos, H. (2013, October). Highly resilient peer-to-peer botnets are here: An analysis of Gameover ZeuS. In Malicious and Unwanted Software: The Americas (MALWARE), 2013 8th International Conference on Malware (pp. 116-123). IEEE.

[17] Files, 2013. F. M. *Online banking fraud mitigation* (Doctoral dissertation, Delft University of Technology).

[18] Heimdal Security (2014b). Everything You Need to Know about the Notorious ZeuS Gameover Malware. Available on https://heimdalsecurity.com/blog/ZeuS-gameover/

[19] Krebsonsecurity, (2014). 'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge. Available on

http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-ZeuS-botnet-cryptolocker-scourge/

[20] Bank Info Security. (2014). Botnet Takedown: A Lasting Impact? Available at http://www.bankinfosecurity.com/malware-takedown-lasting-impact-a-6903/op-1

[21] Kim, Seil, et al. A study on static analysis model of mobile application for privacy protection. *Computer Science and Convergence*. Springer Netherlands, 2012. 529-540.

[22] Milletary, J. (2012). Citadel Trojan Malware Analysis. *http://botnetlegalnotice. com/citadel/files/Patel_Decl_Ex20. pdf*

[23] SC Magazine, (2014). Two new GameoverZeuS variants in the wild. Available at http://www.scmagazine.com/two-new-gameover-ZeuS-variants-in-the-wild/article/365647/

[24] Soltani, S., Seno, S. A. H., Nezhadkamali, M., & Budiarto, R. (2014). A survey on real world botnets and detection mechanisms. *International Journal of Information and Network Security (IJINS)*, *3*(2).

[25] Kilari, V. T. (2013). Detection of Advanced Bots in Smartphones through User Profiling (Doctoral dissertation, Arizona State University).
http://repository.asu.edu/attachments/126014/content/Kilari_asu_0010N_13546.pdf

[26] Lihua, C. X. F. B. Y., & Tianning, L. X. Z. Andbot: Towards Advanced Mobile Botnets.
https://www.usenix.org/legacy/event/leet11/tech/full_papers/Xiang.pdf

[27] Eslahi, M., Salleh, R., & Anuar, N. B. (2012, December). MoBots: A new generation of botnets on mobile devices and networks. In *Computer Applications and Industrial Electronics (ISCAIE), 2012 IEEE Symposium on* (pp. 262-266). IEEE.

[28] Karim, A., Shah, S. A. A., & Salleh, R. (2014). Mobile Botnet Attacks: A Thematic Taxonomy. In *New Perspectives in Information Systems and Technologies, Volume 2* (pp. 153-164). Springer International Publishing.

[29] Pieterse, H., & Olivier, M. S. (2012, August). Android botnets on the rise: Trends and characteristics. In *Information Security for South Africa (ISSA), 2012* (pp. 1-5). IEEE.

[30] Paganini., P. (2013). Mobile Botnets: From anticipation to reality. Available at http://securityaffairs.co/wordpress/12862/malware/mobile-botnets-from-anticipation-to-reality.html

[31] Infosec Institute (2012). Botnets and cybercrime – Introduction. Available at http://resources.infosecinstitute.com/botnets-and-cybercrime-introduction/

[32] Zhou, X. Y., & Jiang, X. (2011). *An analysis of the anserverbot trojan*. Tech. Rep., 9 2011. Available at http://www.csc.ncsu.edu/faculty/jiang/pubs/AnserverBot_Analysis.pdf

[33] AVG Threat Labs, Android/Geinimi. Available at http://www.avgthreatlabs.com/virus-and-malware-information/info/Android-geinimi-a/

[34] The Hacker News. (2014). New Android Malware 'HijackRAT' Attacks Mobile Banking Users. Available at http://thehackernews.com/2014/07/new-Android-malware-hijackrat-attacks.html

[35]OpenDNS SecurityLabs (2014). GameoverZeuS Switches From P2P to DGA. Available at http://labs.opendns.com/2014/07/11/gameover-ZeuS-switches-p2p-dga/

[36] [14] FBI. (2012). Malware Targets Bank Accounts 'Gameover' Delivered via Phishing E-Mails. Available at

http://www.fbi.gov/news/stories/2012/january/malware_010612/malware_010612

[37] Alazab, M., & Broadhurst, R. (2014). Spam and Criminal Activity. *Trends and Issues (Australian Institute of Criminology) Forthcoming*.

[38] Virus Bulletin (2014). Game over for GameoverZeuS botnet? Available at https://www.virusbtn.com/blog/2014/06_05.xml

[39] Maheshwari, N. Botnets - Secret Puppetry with Computers. . Available at http://www.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/presentations/2012/topic11-final/report.pdf

[40] Alazab, M., Venkataraman, S., & Watters, P. (2010, July). Towards understanding malware behaviour by the extraction of API calls. In *Cybercrime and Trustworthy Computing Workshop (CTC), 2010 Second* (pp. 52-59). IEEE.