

Configuring Zeus: A case study of online crime target selection and knowledge transmission

Alice Hutchings and Richard Clayton
Computer Laboratory
University of Cambridge
Cambridge CB3 0FD
Email: firstname.surname@cl.cam.ac.uk

Abstract—Zeus is a well-known and effective family of ‘man-in-the-browser’ malware. This qualitative case study analyses posts in online cybercrime forums that discuss Zeus configuration. Online cybercriminals were found to share, sell, steal, and trade configuration files. The discussions and advertisements on the forums, which span four years, were found to evolve with market conditions and externalities, including Zeus being offered as a subscription service. The release of tools to decrypt configuration files by security researchers was also closely followed on the forums, and assisted offenders when it came to stealing configuration files from others.

I. INTRODUCTION

Zeus (sometimes called Zbot) is a family of credential stealing malware which first emerged into the cybercrime market in 2007 [2]. It was widely deployed by criminals for around five years, and newer malware based on similar principles is in use to this day. Zeus belongs to a class of malware dubbed ‘man-in-the-browser’ (a play on a ‘man in the middle attack’) in that it runs on end-user machines where it can intercept web browser traffic to extract login credentials or to manipulate the page content displayed to the user. Additionally, it can steal user credentials for FTP (file) and POP3 (email) servers as well as cookies (which could be used to fool websites into treating an attacker as a logged in user). A detailed account of Zeus capabilities was published by SecureWorks in 2010 [33].

Although Zeus is most well-known for its success in compromising financial transactions, it has also been used against a multitude of other targets, including the theft of credentials for webmail accounts and other online services [35]. It achieves its flexibility by means of ‘configuration files’ that indicate which websites are to be targeted, which user submitted fields are to be collected, what webpage rewriting is required and where the results are to be sent.

Zeus should be seen not as malware that targets particular banks but as a platform (besides the malware itself there are other components for receiving stolen data, tracking infections and controlling infected machines) which eases the task of crafting an attack on a particular target. It is simpler to provide a configuration file for Zeus than to develop custom malware from scratch – but this is still not the simplest of tasks and requires skill and experience to achieve results.

In this paper we look at the criminal ecosystem surrounding Zeus. The code was originally ‘closed source’ and one had to purchase a copy from the developer(s). However the source eventually leaked and others extended and improved it. Development of configuration files was orthogonal to this evolution of the base platform, but the complexity of these files seem to have restricted the number of websites actually targeted. Tajalizadehkhoob et al. [35] examined a large number of configuration files and described this lack of development and measured a substantial overlap in the content of different files. As a result, the authors suggested that offenders were not developing configuration files from scratch but were selling, sharing or stealing them.

We further explore this notion that the Zeus platform and its configuration files might not have been ‘easy to use’ with a case study examining online forums for indications as to how offenders shared knowledge about Zeus. We are interested in how they transmitted information about targets between themselves, and how they learnt and developed their skills. While Zeus is the specific subject of this research, we would expect to find that similar issues and information flows arise for the offenders participating in other types of online crime that compromise data and financial security.

This is a qualitative study, using the information we found on online forums to determine the views and amalgamate the experiences of the offenders who wanted to use the Zeus malware. We are not doing quantitative research where we would be attempting to make precise measurements. The majority of papers in the computer science literature are quantitative, in that they count incidents and quantify losses. However, there is also great value in qualitative research, especially when we need to understand the structure and nature of a problem in order to work out what to measure in later studies, or indeed to even assess what sort of experiments might be conducted to provide measurable results.

II. THE HISTORY OF ZEUS

Before reporting on the findings from our study of online forums we set out in this section the details (such as they are known) of the history of Zeus and explain some of the technicalities of how it actually works.

A. Zeus: The authors

There has been some speculation as to who authored Zeus, the number of authors involved, and if authorship has changed over time. Bottazzi and Me [5] claim that a Russian group of five developers known as ‘UpLevel’ started developing Zeus in 2005. In 2011, the source code of Zeus version 2.0.8.9 was leaked. Layton and Azab [25] conducted authorship analysis of this version, concluding that while the majority of the code was written by one author, for some modules it appeared they relied on the assistance of others to add functionality.

In 2010, it was reported that the Zeus author was retiring and the source code had been sold to the author of SpyEye, a competing toolkit [23]. Additionally, since the leak in 2011, there have been many new variants of the toolkit, which have further developed the leaked source code [2], [25].

Developing malware does not come without risks, although jurisdiction does create difficulties for law enforcement. In 2014, Aleksandr Andreevich Panin, believed to be the main author of SpyEye, pleaded guilty to developing and distributing the malware [13]. A Russian national, he was arrested whilst in transit through the United States [13], and later received a nine year, six month sentence for conspiracy to commit wire and bank fraud [24]. His ‘business partner’, Hamza Bendelladj, received a 15 year sentence for helping Panin develop and market the SpyEye kit, as well as running his own botnet [24]. In 2015, the FBI announced a US\$3M bounty for information relating to another Russian individual, who they believe to be the original Zeus author, and controller of a botnet known as ‘GameOver’ [23].

B. Zeus: The users

A user who wishes to steal credentials obtains a version of the Zeus toolkit, which contains a builder to create the executable and configuration files [4], [39]. This may be a public, free version, or they may purchase the very latest version, typically through an online marketplace [39]. Despite reports that the toolkit costs thousands of dollars to purchase [1], [39], this is apparently a ‘competitive price’ [4], that is to say, it is not seen as excessive.

Wyke explains the toolkit mechanics in a 2011 Sophos whitepaper [39]. The toolkit user creates a configuration file to customise the malware, to tell it what to do and where to send the data it steals. The ‘builder’ from the toolkit is then used to convert the configuration file to a binary format and encrypt the result. The result is stored on a website and the URL, along with a decryption key, is embedded into a malware executable which is then ‘packed’ to compress the file and obscure its contents (thereby making it harder for anti-virus software to detect [1], [7]).

The malware must then be delivered to victims so that it will be executed and compromise their systems. Common distribution methods include the use of file sharing networks, drive-by-download exploits, and social engineering [7]. Some Zeus toolkit users employed ‘pay-per-install’ services, which distribute the malware to thousands of victims for a fee [7]. In addition, a built-in component of the malware called a

‘spreader’ could cause further systems to be compromised by infecting USB drives, or by sending unauthorised instant messages through victims’ social media accounts [31].

Once downloaded and installed, the malware visits the website where the configuration file is located for instructions on how to behave [39]. The collection of infected computers that have the same malware on it is referred to as a botnet (and the individual computers as ‘bots’ or ‘zombies’). The botnet can be controlled by the Zeus user through a command and control (C&C) server [4], [5].

The C&C server interface is a component of the Zeus toolkit, and permits monitoring of the status of the botnet, the issuing of commands, and the retrieval of data [4], [39]. Any particular version of the toolkit will create a similar executable, but the configuration details will be unique to the user and hence disjoint botnets are created [35]. Therefore, a compromised computer can be infected multiple times and become a member of multiple botnets [39].

The configuration file contains two sections: static and dynamic [4], [39]. The static section of the configuration file includes the instructions that are written into the configuration file when it is built, such as the web address where it is located, and how often updates should be checked for [39]. The dynamic options allow the malware to be customised by the user, and can be remotely updated [39].

As well as the location where data is to be sent, and how to update the executable and configuration, the configuration file contains instructions on what websites are to be targeted, and how. The options include logging keystrokes (keylogging), collecting data entered into web forms (form grabbing), taking snapshots when the mouse is clicked, redirecting the web session to other sites, hijacking DNS requests, and dynamic alterations to web pages (webinjects) [6], [39]. A variety of mechanisms may be used to harvest the Transaction Authentication Numbers (TANs) that are used by some financial institutions for multi-factor authentication, including the installation of malicious phone applications to intercept SMS [6].

The information for webinjects is contained within the configuration, including the URLs of the targeted websites and the modification instructions that cause additional content to be added to the original web pages [4], [6]. For example, additional fields to be completed by a visitor may be inserted into webforms to ask the victim for their PIN or social security number when they access their online banking system [39]. The stolen data, which may include email addresses, passwords, online bank account credentials, credit card numbers, as well as TANs, are then sent to the location referred to in the configuration file [4].

Some webinjects can be used to transfer funds from the victim’s bank account, including mechanisms to hide the transaction and show an amended account balance so that it is undetected by the victim [6]. Attacks using webinjects are typically referred to as ‘Man-in-the-Browser’ (MitB) attacks [6]. Webinjects are tailored to the targeted URL, and may include ways to circumvent security measures that are put in place to prevent attacks [6].

The data stolen using Zeus may be utilised by the user themselves for financial gain, or sold in online black markets. It is within these marketplaces that the Zeus toolkit is purchased [1], [4], [6], [9], [23], [36]. In addition to the sale of hardware and software used for stealing data, and the data that are stolen through their use, the marketplaces facilitate other parts of this underground economy, such as advertising various services to turn data into money [16], [17], [21], [26], [40].

Some of those that have used the Zeus toolkit and established their own botnets have come to police attention. The trend appears to be towards group prosecutions, which includes those who are alleged to be money mules or involved in money laundering. By 2012, at least 24 defendants had been sentenced in the US, including overseas students recruited to open bank accounts using fake identification [12]. In the UK, 14 individuals were arrested in 2010 relating to the use of Zeus. They attempted to steal £4.2M, although successful transactions amounted to £2.8M. Five individuals in this group have been sentenced, with sentences ranging from 40 months to four and a half years in prison. Outcomes for the remaining nine alleged offenders have not been made known [20]. Further prosecutions are likely following five arrests in Ukraine of those suspected of developing, distributing, and exploiting Zeus and SpyEye [11].

C. Zeus: The victims and targets

The term ‘victim’ may be confused with ‘target’; however, when considering Zeus we consider the victim to be the person whose computer is infected with the malware (and becomes part of a Zeus botnet) whose credentials may be compromised.

We use the term ‘target’ for any institution (often a bank) which operates a website that a particular version of the malware has been configured to react to when the victim makes a visit.

D. The evolution of Zeus

As with many other types of software, Zeus has adapted and changed with market conditions and externalities. It is important to understand the nature of these changes, as they provide a context to our research findings, which examines how offenders responded to the evolution of the malware.

Zeus was originally ‘closed source’ malware and to obtain a copy users had to purchase a license, which enabled their personal use. As new variants were developed, public versions were released free-of-charge. The public versions were older, or provided less functionality than the private versions [9], [39]. This follows the ‘freemium’ business model, whereby basic products or services are provided at no cost to attract buyers to the premium counterpart [10].

After the source code for Zeus 2.0.8.9 was leaked in 2011, new ways to monetise the malware evolved. Following the ‘as-a-service’ business model, Zeus began being offered as a subscription service. Bottazzi and Me [5] suggest that subscription based services for botnets are attractive for a variety of reasons. For the provider, it maximises earnings by providing the same service to multiple users. For the

user of the service, the benefits are in a reduction in the initial financial outlay, while outsourcing the logistical and maintenance requirements, and reducing the risk of failure to achieve results.

In parallel with this, the leaked source code was used as the basis for developing many new variants of the malware [2]. Particularly successful toolkits that were based on the leaked source code included ‘Citadel’, and a variety of peer-to-peer (P2P) botnets, including ‘GameOver’ [2]. P2P botnets do not use a centralised C&C server, and thus are more resilient to takedown efforts [2].

There have been several efforts to take down Zeus and other botnets, mainly orchestrated by Microsoft. Initially, disruption attempts focused on removing the malware infections. In October 2010, Microsoft added Zeus detection to their Malicious Software Removal Tool, with almost half a million infected computers cleaned up in just the first month [8]. In 2012, Microsoft obtained a court order to, amongst other things, ‘sinkhole’ a Zeus botnet, by redirecting traffic, transferring domain names, and disabling IP addresses [15], [27] (albeit this action was not without controversy, see [22]).

In a later takedown operation against Citadel, a Zeus variant, in 2013, Microsoft obtained an order that allowed it to modify the malicious code, by sending out a ‘stop’ command, and if not cleaned up, placing the victim inside a ‘walled garden’ [15]. Microsoft was once again criticised, as it was argued that they did not obtain the consent of the owner of the infected computer before modifying the code or limiting their access to the Internet [15]. In 2014, an international effort was also successful, if only for a limited time [31], in taking down the P2P botnet ‘GameOver Zeus’, the variant believed to be operated by the original Zeus author [23].

Security researchers, both in academia and industry, have continually monitored Zeus variants, and, in turn, the malware authors have developed new ways to frustrate this. For example, the configuration files in Zeus 1.0 used a simple encryption key, which could be easily decrypted by those who knew the algorithm and, in September 2009, a decryption tool was released [29]. This was overcome with Zeus 2.0, which introduced more layers to encrypt the configuration file [39]. However, this was again defeated in May 2010, when a tool to decrypt these configuration files, developed through reverse engineering, was released for security research [30].

III. A CRIMINOLOGICAL PERSPECTIVE

A. Target selection

Criminological research into target selection by burglars has found that a ‘rational choice’ approach is used. The burglars select unoccupied, accessible, and well situated premises that appeared to contain high value belongings [28], [38]. Hutchings [18] analysed data relating to active and current cybercrime offenders involved in unauthorised access offences and computer frauds to explore how they selected their targets. In some cases, the offender was familiar with the target, although other targets were indiscriminately selected, solely by chance. Nonetheless, Hutchings found that these offenders

were also using a rational choice approach, selecting targets that were perceived to be ‘easy targets’, those with known vulnerabilities, and targets providing a high reward.

In relation to Zeus, Tajalizadehkhoob et al. [35] explored target selection by examining 11 000 configuration files dating from January 2009 to March 2013. The 2 131 botnets identified in this period targeted 2 412 unique domains. Categorised by Alexa, 32% of the targets were financial service providers, 11% were other industry segments, and 57% were uncatagorised. Targets that were consistently under attack were located in 13 countries, and 90% were financial service providers. On average, 119 of the 601 domains attacked each month were new targets, when compared to the previous month. Thus it appears that Zeus users were using a rational choice approach that was optimised for stealing money from banks.

B. Knowledge transmission

Sutherland [32] theorised that criminal behaviour is normal behaviour learnt in interaction with others. Sutherland’s ‘theory of differential association’ consists of nine specific points. Summarised, these points indicate that criminal behaviour is learnt in interaction with other persons in intimate personal groups. What is learnt includes both the techniques of committing crime, and ‘motives, drives, rationalisations and attitudes’ [34] either favourable or unfavourable to committing crime. Crime is committed when those definitions favourable to committing crime exceed those unfavourable to crime [34].

There are two basic elements of differential association. The first is the cognitive element, or the content of what is learnt. This includes the specific techniques to commit crime, whether it be lock breaking or, in the case of Zeus, technical expertise, as well as the definitions favourable to committing crime [37]. Sutherland [34] did not specify the learning mechanisms, simply stating that “the process of learning criminal behaviour . . . involves all of the mechanisms that are involved in any other learning”. The second element of differential association is the associations with other people in intimate personal groups where the learning takes place [37].

In relation to cybercrime, there is strong evidence that the associations with others take place online, particularly through the use of IRC and online forums [9], [14], [16], [19], [21], [40], [41]. Hutchings’ [19] analysis of court documents and interviews with offenders and law enforcement officers found that cybercrime offenders are highly networked and cooperate with each other to commit offences. This takes place in online marketplaces, which enable and facilitate organised crime through the sale of malware to conduct attacks, the data obtained from attacks, such as compromised credentials, and services offered by skilled specialists [21].

IV. RESEARCH QUESTIONS

The aim of the current research is to explore three topics relating to how Zeus financial malware is discussed by offenders in online stolen data forums. The first question relates to target selection; specifically what evidence is there for offenders

sharing, stealing, or selling configurations for different targets? The second question is what information is transmitted and shared between offenders about how to use configuration files? The third question asks how these discussions have changed with the evolution of the malware?

V. RESEARCH METHODOLOGY

To conduct our study, we relied on a dataset of cybercrime forum contents that had been seized, taken down, or leaked, covering various periods of time that go back as far as 2002. This law-enforcement curated dataset includes around 120 forums of various sizes and it has been carefully indexed.

The dataset was searched for the presence of posts using the combination of ‘configuration’ and ‘config’, with ‘zeus’ and its synonyms, ‘zbot’ and ‘z-bot’. Only messages that would have been public were searched and retrieved. The researchers did not have direct access to the datasets, but specified the terms to be used for searching and then received the results of the searches for analysis.

The searches turned up 65 separate communications on nine forums, dating from November 2008 to October 2012. The results provided included the forum name, the username, the board, name of the thread, date and time, and the content of the messages. The communications were in English (60.0%), German (6.2%), and Russian (33.8%). Experienced computer science researchers with native language skills and subject matter expertise translated the German and Russian posts.

The forum content was analysed using qualitative content analysis procedures. A qualitative research design was selected for its ability to provide a deeper understanding of offending behaviour than may be achieved through a quantitative design. Qualitative research captures nuances and provides richness to data that may not otherwise be quantifiable [3].

The content provided in the next section has been provided verbatim, either as it appears in the original data or how it has been translated. On occasion, potentially identifying information has been removed, quotes have been reduced for reasons of parsimony, and sometimes explanations have been provided for the reader.

VI. RESEARCH FINDINGS

A. What evidence is there that offenders share, steal, or sell configurations for different targets?

It appears that there are multiple ways in which information and data for configuring Zeus is transmitted between participants on the discussion forums. Indications that offenders shared, stole, and sold configurations could be found. Additionally, as will be discussed in the findings relating to the second research question, it was found that offenders traded in configuration files.

The earliest exchange, dating from 2008, starts with the question “Hi, I got ahold of Zeus 1.1 but its missing the config file. Can anyone point me to where I can find one?” The response, received the same day, includes what appears to be a list of webinjects. In total, 162 targets are listed, mainly banks and financial institutions located worldwide, as well as

social media, online trading, and gambling sites. Interestingly, one of the targets listed is webmoney.ru, a Russian payment provider often used in stolen data markets.

There was some indication, albeit limited, that configuration files for Zeus were being sold. In 2009, an advertisement for Zeus was posted that offered the binary file for 150Wme (Web-Money), or the builder for €3 500 (approximately US\$4,400 at the time). The advertisement included a reference to a configuration file, indicating that it was included in the offer. The advertisement, which was in German, had been posted multiple times on the one forum under a single username.

In relation to stealing configurations, there was an indication that this took place, however it was frowned upon. An exchange from 2009, translated from Russian, begins with a query about restoring an encrypted configuration file. A terse response was received shortly after: "There are no such in public and will not be any time soon. PS: do not spam in pm". While 'public' may have referred to a public version of the malware, in this case, it may refer to the board being publicly accessible, and that such matters should not be discussed there. The reference to private messages ('pm'), could hence be understood that the person does not want to be contacted about getting access to private boards, or does not want to provide assistance. A few days later, no response having been received, the original poster again asked for guidance. This time, the response was aggressive in nature:

It is not good to steal from your own people. Those who unpack other people's configs are not just a deceivers but bitches. Instead of being useful to do something they do bull shit. Where are you fuck come from!?

B. What information is transmitted and shared between offenders about how to use configuration files?

All of the information we found that discussed the detail of Zeus configuration was shared in response to a question being posed, for example:

Hey, I've never configured zeus before so I was wondering if someone could look at my entries under WebFilters and tell me if they are formatted correctly, or if it will break my .exe. Thanks :) [...]

Not all questions elicited a response, and initially this post went unanswered. The following day, the author of the above post commented on the lack of advice, yet also provided the answer to the question they had asked:

Thanks again for all the help, you guys have been great. :rolleyes: If any other Zeus newbies are wondering, the method above IS correct, but I would not recommend leaving the addresses so open, it will fill your logs with junk. Instead specify the path to the bank log in page, not just the bank web page. The downside to this is that unless you take the time to manually find every form page on the website and enter it into the list, you may miss out on some extra data if the user starting filling out a loan application

online or something. If anyone disagrees with this, please let me know so I can fix my config file. I'm learning this as I go. [...]

This post then generated an exchange with an additional three users around various versions of Zeus. Some of the discussions about which versions to use included a focus on security, with references to cleaning out any backdoors placed there by the author, and bots being stolen when public versions of the toolkit were used. Also discussed in this thread was the use of spreading mechanisms to disseminate the malware:

I have read in like 4 forums that 1.2.9.x is newest private, still no built in ff [Firefox browser] or wmz [compressed enhanced metafile for windows] grabber from what I read. Looks like you need to purchase the modules to give that ability. Regarding your advice, i'm looking for a good worm to bind to. Have you ever found something like a spreader? you just bind your exe to it and it will do lan spread/p2p spread/torrent posting/warez posting etc. ?? that would be great.

The response refers to the trade, as well as sale, of configuration details:

I want to know the updates of new version,yes, ff grabber is not built in the builder its a external library, [username] seems that he have it but dont want to sell or trade lol There are many spreaders public also private if you want to pay for it, but you just can use any RAT crypt it and add spreading options (usb is good, torrent/gnutella also)

There were additional references to the trade of information elsewhere in the data. One username was used to post in two forums, indicating that they have a builder and have infected bots. They have several troubleshooting queries as they cannot see the bots on cpanel (a web hosting control panel), and seek information about the configuration file. The messages are similar in content, and posted within half an hour of each other. However, in the later post the user refers to previous assistance provided (emphasis added):

i have set-up zeus but bots not joining cpanel, am sure i got a bot coz i copy the created zeus bot.exe to my friend's pc and run it there, so am sure his pc is infected but it didnt join the cpanel, why these? secondly, am having problem with the config, below is an extract from the zeus config file: [...] this will be the config.bin file i get when i click on create config on the zeus builder,right? [...] should i leave this as it is? coz i cant find any .php file called ip.php in the zeus package, if need to change, what i change it to? encryption_key "secret key" the encryption key i put here must be same with the one i put into zeus during installation,right? [...] I cant find any cfg1.bin file in the zeus package? and when i click build config **as you guys suggested**, its wants to save it as "config.bin" ...where would i find the cfg1.bin

file or i should leave as it is? Help me on these guys, please.

It appears that the earlier post goes unanswered, however the post referred to above elicits a response that refers to assistance given in exchange, or bartered, for something unknown, which is claimed was not received:

[username] i helped you to sut up this shit where is ur part of deal ????????????

There were additional cases where the same username was used in multiple different forums, presumably by the same individual. One username in particular was found posing questions about Zeus configuration, as well as participating in discussions on this topic, such as the following relating to capturing screenshots for specified URLs:

To elaborate on this a bit further, you can set filters in the zeus config to take a screen shot every time the mouse is clicked on a specific web page. so for example, every time they click on a letter on the virtual keyboard it captures the image so you can see what letters/numbers they click on.

There were some indications that, once assistance was provided, posts were deleted and hence they were not available for this study. One thread on a Russian-language forum contained a threat titled 'Zeus config entry', which contained the sole comment 'delete plz'. Another thread title translated from German to 'close + del please'. While the original post had indeed been deleted, it could be seen that the discussion originally related to Zeus configuration, as the conversation had continued:

There is also an option for this on the WEBpanel and config can indeed be updated independently from the server. Thus, it's not a problem at all.

Two posts were found that linked and quoted excerpts from news stories and blogs that related to Zeus. One related to the methods that offenders were using, while the other post was in relation to the work done by the security industry to track the malware.

C. How have these discussions changed with the evolution of the malware?

Earlier, we refer to a thread that discusses decrypting the configuration file, with the original poster being accused of stealing the configuration file. The thread did not end there, as a few days later another user joined in the conversation, providing a link to a decryption tool [29], which had been released only the month before:

[...] Here is decryption tool: [URL] There you will need to run a ZeuS build first, then run the decryptor and specify the path to the config that needs decoding. In general, if you do not succeed, try to revers engineer Zeus code. The author skillfully described everything.

When the new tool was released in 2010, which allowed configuration files for Zeus 2.0 to be decrypted, a link was disseminated on one of the forums the subsequent day. Four

months later, on another forum, a tutorial on how to use the tool is posted in Russian:

Hello everyone. Today we will use Config Decryptor for ZeuS 2.0 This software will not help you if you dont have a bot on the workstation with configuration. So go ahead .. You need these: 1) VMware-workstation (any version. I use 5 – it is easier and simpler) 2) Config Decryptor for ZeuS 2.0 3) 3) Sober head and straight arms. [step-by-step instructions] Open the file Config and start looking and analyzing it's contents =) Good luck to all

The resulting discussion indicated that some users had decrypted the configuration files, although their perception of the value varied:

Very big cons is that the result is a complete mess with injects. there are some people who founds this mess completely useful:) As dear [username] said to me: it is better to rewrite everything from scratch than collect unclear pieces!

A further development following the evolution of Zeus is the advertisement of a Zeus subscription service, which includes webinjects and configuration, as well as 1 000 installs, for a monthly fee. This advertisement, which follows the 'as-a-service' business model, came out shortly after the source code for version 2.0.8.9 was leaked:

[RESELLING] Zeus 2.0.8.9 FULL SETUP + WE-BINJECTS + VNC + INSTALLS Hello Guys, I'm reselling my account of Zeus 2.0.8.9 bin which included: – Zeus 2.0.8.9 already installed and ready to use; – Zeus Webinjects included; – Zeus Config.bin; – Zeus .EXE FUD; – Zeus VNC + tutorial; – Zeus 1k Installs (worldwide) included. Is hosted on offshore hosting and have a bulletproof domain. First month is free (included on price). If you want to continue using it you have to pay \$50 / month. Price: \$250 (LR or WMZ) ESCROW WELCOMED

There were also indications that the leak of the source code may have encouraged others to become involved with trying out Zeus when they had not otherwise:

Hello, venerable carders. I assume that with the leak of the Zeus 2.0.8.9 source code many have attempted to play with the code. For many of us it makes no sense to buy expensive bullet-proof hosting services before we have a working and fully undetectable Zeus binary configured to work with our specific IP address. I have attempted to set up a typical web server on my computer and see if Zeus 2.0.8.9 source code can produce anything workable. So far I have been unsuccessful. The produced binary seems to infect the computer but it does not show up in the control panel for some reason. I suggest we join forces together and share ideas to produce something that will be of benefit to everyone here on the forum. [...]

VII. DISCUSSION AND CONCLUSION

Our qualitative analysis of cybercrime forum data provides solid support for the suggestion put forward by Tajalizadehkhoob et al. [35] in their quantitative study that configuration files must have been “shared, sold, and stolen”.

We found that cybercrime offenders utilising Zeus toolkits face a number of risks. Not only may they have their configuration files stolen, but also the malware they use may contain backdoors, leading to the credentials they steal being subsequently stolen by others, and their botnets taken over. They may also fall victim to the malware themselves, with a webinject for WebMoney, a popular digital currency used in stolen data markets for accepting payments, included with a bundle of other targets that had been shared. In addition to sharing, selling, and stealing, offenders referred to the trading of configuration files.

Our results also provide evidence that individual offenders are active on multiple forums, and that questions posed on some forums were more likely to elicit a response than others. Care was also taken by offenders to delete some messages, presumably when they no longer served a purpose, and to curtail the type of questions that were asked on publicly facing discussion boards. However, answers to questions were also provided, even when no longer required, so that they could be of assistance to others at a future date.

Discussions about Zeus changed and reacted to the evolution of the malware. The leaking of the source code was rapidly followed by offenders seeking to monetise the now-free software by providing an ‘as-a-service’ subscription, which includes hosting, configuration and installs. The release of tools to decrypt configuration files was also closely followed and disseminated on the forums.

Posts show that, assuming the accuser is correct and offenders are stealing configuration files from others, the tools used for security research may be used for nefarious purposes. We caution against using this finding to argue that tools to decrypt configuration files should not be developed or publicly released, as they may be used for bad as well as good.

Trust is an important element of the online forums, enabling the sharing of information. However, by promoting distrust, such as the fear that others will steal from them more than they are willing to share, it may have an overall disruptive effect.

While we have attempted to overcome the significant difficulties associated with this challenging area of research, a number of limitations of our research design must be highlighted. Firstly, the data may not include the most experienced criminals that used Zeus, particularly if their skills are already well developed and they employ good operational security. It may be that it only the recent entrants to the field who are willing to post questions and share their experiences.

Secondly, the data does not capture other ways that knowledge is transmitted, such as IRC, face-to-face communications, or private boards. While the number of forums that were included in the dataset is extensive they are only available

for research because these were the forums that were targeted for takedown or seizure, or that compromised and leaked. This selection process may have introduced bias into our results.

VIII. ACKNOWLEDGEMENTS

The work would not have been possible without the invaluable assistance of the National Cyber-Forensics & Training Alliance (NCFTA), Ross Anderson, Ruslan Bukin, Sergio Pastrana, Daniel Thomas and Bjoern A Zeeb.

IX. FUNDING

This work was supported by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHSS&T/CSD) Broad Agency Announcement 11.02, the Government of Australia and SPAWAR Systems Center Pacific [contract number N66001-13-C-0131] (to 30 September 2016); and the UK Engineering and Physical Sciences Research Council (EPSRC) [grant EP/M020320/1] for the University of Cambridge, Cambridge Cybercrime Centre (from 1 October 2016). The opinions, findings, and conclusions or recommendations expressed are those of the authors and do not reflect those of the aforementioned agencies.

REFERENCES

- [1] Alazab, M., Venkatraman, S., Watters, P., Alazab, M. and Alazab, A.: Cybercrime: the case of obfuscated malware. *Global Security, Safety and Sustainability & e-Democracy*, 204–211, Springer (2012).
- [2] Andriess, D., Rossow, C., Stone-Gross, B., Plohmann, D. and Bos, H.: Highly resilient peer-to-peer botnets are here: an analysis of Gameover Zeus. *8th International Conference on Malicious and Unwanted Software* (2013).
- [3] Berg, B. L.: *Qualitative Research Methods for the Social Sciences* (6th ed.). Boston: Pearson Education, Inc (2007).
- [4] Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M. and Wang, L.: On the analysis of the zeus botnet crimeware toolkit. *Eighth Annual International Conference on Privacy Security and Trust (PST)* (2010).
- [5] Bottazzi, G. and Me, G.: *The Botnet Revenue Model*. *7th International Conference on Security of Information and Networks* (2014).
- [6] Boutin, J.-I.: The evolution of webinjects. *Virus Bulletin Conference* (2014).
- [7] Caballero, J., Grier, C., Kreibich, C. and Paxson, V.: *Measuring Pay-per-Install: The Commoditization of Malware Distribution*. *Usenix Security Symposium* (2011).
- [8] Campana, T. J., Faulhaber, J., Henry, P., McCormack, M., Simorjay, F. and Stewart, H.: *Battling the Zbot Threat: Security Intelligence Report*. Redmond: Microsoft (2010).
- [9] Chu, B., Holt, T. J. and Ahn, G. J.: *Examining the Creation, Distribution and Function of Malware On-Line: Technical Report for National Institute of Justice*. NIJ Grant No. 2007IJCX0018 (2010).
- [10] de la Iglesia, J. L. M. and Gayo, J. E. L.: *Doing business by selling free services*. In M. D. Lytras, E. Damiani & P. Ordez de Pablos (Eds.), *Web 2.0: The Business Model*, 89–103, Springer (2009).
- [11] Europol: *Major cybercrime crime dismantled by joint investigation team*. 25 June 2015. Retrieved February 6, 2017, from <https://www.europol.europa.eu/content/major-cybercrime-ring-dismantled-joint-investigation-team> (2015).
- [12] Federal Bureau of Investigation: *Another cyber fraud defendant charged in Operation Aching mules sentenced in Manhattan Federal Court*. 23 March 2012. Retrieved February 6, 2017, from <https://www.fbi.gov/newyork/press-releases/2012/another-cyber-fraud-defendant-charged-in-operation-aching-mules-sentenced-in-manhattan-federal-court> (2012).

- [13] Federal Bureau of Investigation: Cyber criminal pleads guilty to developing and distributing notorious SpyEye malware. 28 January 2014. Retrieved February 6, 2017, from <https://www.fbi.gov/atlatlanta/press-releases/2014/cyber-criminal-pleads-guilty-to-developing-and-distributing-notorious-spyeye-malware> (2014).
- [14] Franklin, J., Paxson, V., Perrig, A. and Savage, S.: An inquiry into the nature and causes of the wealth of Internet miscreants. ACM Conference on Computer and Communications Security (CCS), Virginia (2007).
- [15] Hiller, J. S.: Civil cyberconflict: Microsoft, cybercrime, and botnets. *Santa Clara Computer & High Technology Law Journal*, 31(2), 163–313 (2015).
- [16] Holt, T. J.: Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, 31(2), 165–177 (2013).
- [17] Holt, T. J. and Lampke, E.: Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies: A Critical Journal of Crime, Law and Society*, 23(1), 33–50 (2010).
- [18] Hutchings, A.: Hacking and fraud: Qualitative analysis of online offending and victimization. In K. Jaishankar & N. Ronel (Eds.), *Global Criminology: Crime and Victimization in the Globalized Era*, 93–114, Boca Raton: CRC Press (2013).
- [19] Hutchings, A.: Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law & Social Change*, 62(1), 1–20 (2014).
- [20] Hutchings, A.: Cambridge Computer Crime Database. Retrieved January 25, 2017, from <http://www.cl.cam.ac.uk/~ah793/cccd.html> (2017).
- [21] Hutchings, A. and Holt, T. J. A crime script analysis of the online stolen data market. *British Journal of Criminology*, 55(3), 596–614 (2015).
- [22] Krebs, B.: Microsoft responds to critics over botnet bruhaha. 16 April 2012. Retrieved February 6, 2017, from <http://krebsonsecurity.com/2012/04/microsoft-responds-to-critics-over-botnet-bruhaha/> (2012).
- [23] Krebs, B.: FBI: \$3M bounty for ZeuS trojan author. 25 February 2015. Retrieved February 6, 2017, from <http://krebsonsecurity.com/2015/02/fbi-3m-bounty-for-zeus-trojan-author/> (2015).
- [24] Krebs, B.: SpyEye makers get 24 years in prison. 20 April 2016. Retrieved February 6, 2017 from <http://krebsonsecurity.com/2016/04/spyeye-makers-get-24-years-in-prison/> (2016).
- [25] Layton, R. and Azab, A. Authorship analysis of the Zeus botnet source code. Fifth Cybercrime and Trustworthy Computing Conference (CTC) (2014).
- [26] Motoyama, M., McCoy, D., Levchenko, K., Savage, S. and Voelker, G. M. An analysis of underground forums. ACM SIGCOMM Conference on Internet Measurement, Berlin (2011).
- [27] Nadji, Y., Antonakakis, M., Perdisci, R., Dagon, D. and Lee, W.: Beheading hydras: performing effective botnet takedowns. ACM SIGSAC Conference on Computer & Communications Security, Berlin (2013).
- [28] Neel, C. and Taylor, M. Examining burglars’ target selection: Interview, experiment or ethnomethodology? *Psychology, Crime and Law*, 6(1), 45–59 (2000).
- [29] Shevchenko, S.: Time to revisit Zeus almighty. 16 September 2009. Retrieved February 6, 2017, from <http://blog.threatexpert.com/2009/09/time-to-revisit-zeus-almighty.html> (2009).
- [30] Shevchenko, S.: Config decryptor for Zeus 2.0. 2 May 2010. Retrieved February 6, 2017, from <http://blog.threatexpert.com/2010/05/config-decryptor-for-zeus-20.html> (2010).
- [31] Sood, A., Zeadally, S. and Enbody, R. An Empirical Study of HTTP-based Financial Botnets. *IEEE Transactions on Dependable and Secure Computing*, PP(99), 1–16 (2014).
- [32] Sutherland, E. H.: *White Collar Crime: The Uncut Version*. New Haven: Yale University Press (1949).
- [33] Stevens, K. and Jackson, D.: ZeuS Banking Trojan Report. 10 March 2010. Retrieved February 3, 2017 from <https://www.secureworks.com/research/zeus>
- [34] Sutherland, E. H., Cressey, D. R. and Luckenbill, D. F. *Principles of Criminology* (11th ed.). Lanham: General Hall (1992).
- [35] Tajalizadehkhooob, S., Asghari, H., Gañán, C. and van Eeten, M.: Why Them? Extracting intelligence about target selection from Zeus financial malware. Workshop on the Economics of Information Security, State College, PA (2014).
- [36] Thomas, K., Huang, D. Y., Wang, D., Bursztein, E., Grier, C., Holt, T. J., Kruegel, C., McCoy, D., Savage, S. and Vigna, G.: Framing Dependencies Introduced by Underground Commoditization. Workshop on the Economics of Information Security, Delft (2015).
- [37] Vold, G. B., Bernard, T. J. and Snipes, J. B. *Theoretical Criminology* (5th ed.). New York: Oxford University Press, Inc (2002).
- [38] Wright, R., Logie, R. H. and Decker, S. H. Criminal expertise and offender decision making: An experimental study of the target selection process in residential burglary. *Journal of Research in Crime and Delinquency*, 32(1), 39–53 (1995).
- [39] Wyke, J.: *What is Zeus? A SophosLabs Technical Paper*. Boston: Sophos Ltd (2011).
- [40] Yip, M., Webber, C. and Shadbolt, N.: Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*, 23(4), 516–539 (2013).
- [41] Zhang, X., Tsang, A., Yue, W. T. and Chau, M.: The classification of hackers by knowledge exchange behaviors. *Information Systems Frontiers*, 1–13 (2015).