GSI ID: 1075

ZEUS CRIMEWARE KIT

RISK FACTOR - HIGH

1.1 OVERVIEW / PLXSert has observed new payloads from the Zeus crimeware kit in the wild. The Zeus framework has evolved from focusing on the harvesting of banking credentials to being used in the control of compromised hosts (zombies) for many types of crime, including distributed denial of service (DDoS) attacks and attacks customized for specific platform-as-a-service (PaaS) and software-as-a-service (SaaS) infrastructures.

The purpose of the Zeus crimeware kit is to infect and control as many hosts as possible, leveraging their resources and extracting sensitive information from their users, which usually leads to identity theft and banking fraud. Other uses of the Zeus framework include crypto-currency mining, spam and DDoS attacks. These add-on uses are monetized in the criminal ecosystem by activities such as work-from-home scams, pay-per-use for crypto currency mining, DDoS-for-hire and credit card crime.

The powerful Zeus framework is frequently part of a chain of attack vectors that seek the infestation, creation and organization of zombie botnets, often for profit. PLXSert has observed network traffic patterns in many DDoS campaigns that match the communication of DDoS source IP addresses as they engage in random-interval callbacks to Zeus and Dirt Jumper command and control (C&C or C2) centers to get new instructions and updated executables.

Malicious actors using Zeus have access to a variety of remote commands. For example, the attacker can request a screenshot of the current desktop and all displayed content on a host device, which could reveal sensitive information. In addition, the attacker could cause a host to download and execute remote and local files and to modify the homepage of the infected computer's Internet browser.

1.2 ORIGIN / The Zeus crimeware kit, believed to have been created by Russian malware developers, was first observed by the security community in the second half of 2007. The use of the kit was directed toward stealing credentials from banking customers as they accessed online services and toward infecting their computers with botnet malware for use in future exploits. Millions of hosts were reported to be infected.

The main characteristic of the Zeus payload was its stealth; it was incredibly difficult to detect. The malware kit allowed malicious actors to execute a variety of customer banking data exfiltration payloads, including man-in-the-browser and form grabbing, as well as executing randomly timed call-home connections to communicate with the C2 while avoiding detection.

The powerful Zeus kit was available in the DDoS underground marketplace for a price that is said to have reached US$10,000. Recently, the use of the kit has expanded beyond the banking industry to other verticals and new features have been added. The Zeus toolkit now allows for the transfer of payloads and executables to infected machines, effectively expanding the use of its compromised hosts for other malicious purposes.

There have been two main branches of Zeus releases: version 1 and version 2. First, the source code for version 2.0.8.9 of the Zeus framework was leaked on the Internet, and more recently version 2.1.0.1 was made available. The Zeus variant named Gameover introduced peer-to-peer (P2P) capabilities that make the detection of communication more difficult, and more recent versions reportedly introduced DDoS payloads.

The Zeus toolkit has become the most used and most effective crimeware kit ever observed by the security community. Its reputation and popularity created rifts and rivalries among malware developers in the crimeware ecosystem, including the appearance of competitive kits such as the so-called Zeus killer, SpyEye. The rivalry is said to have ended with the merger of the code of the Zeus and SpyEye crimeware kits and the retirement of the original Zeus crimeware creator, who was known as Slavik/Monstr. Other popular malware iterations based on the Zeus code include IX, SpyEyeZeus and, more recently, the Citadel botnet.

PLXsert has observed the appearance of new iterations of Zeus payload traffic in parallel with the use of popular DDoS kits, such as Drive, a Dirt Jumper variant. In this threat advisory, PLXsert provides an analysis of the main two branches of Zeus crimeware kits, including their latest payloads and features.

1.3 INDICATORS / The Zeus botnet crimeware kit is composed of two main parts. One part is the web command-and-control panel that allows malicious operators to monitor and execute payloads on compromised hosts. The second part is the builder, which allows the creation of the Zeus bot (zbot) executable, which can be served directly from the panel or from a website. The operator typically sets up a web-based command-and-control center to create a botnet.

The C2 panel is written in PHP and includes all the necessary files required to install the panel. The panel requires the LAMP (Linux, Apache, MySQL and PHP) stack on a Linux server or the XAMMP (Apache, MySQL, PHP and Perl) stack on a Windows server.

The Zeus toolkit requires very little skill to operate. As shown in Figure 1, once the LAMP or XAMMP stack is installed, the Zeus operator simply runs the /install/index.php page and provides some basic information – a username, passwords for the panel and the MySQL database, and the encryption key to be used for bot communication with the control panel (Figure 2).

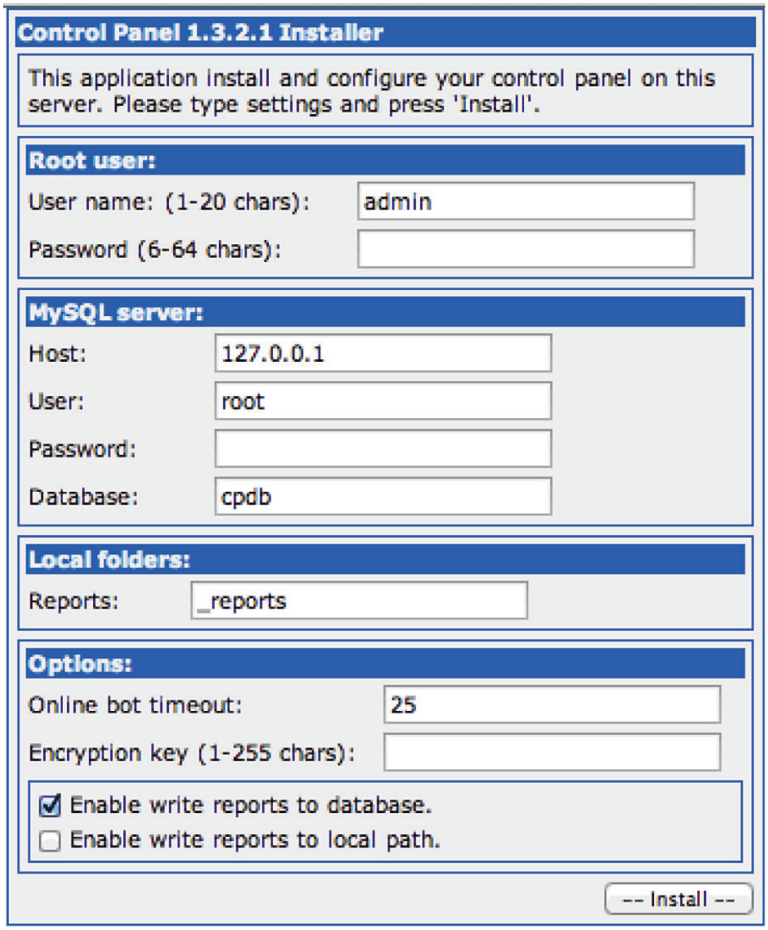

Figure 1: The Zeus 1.3.2.1 easy install of /install/index.php

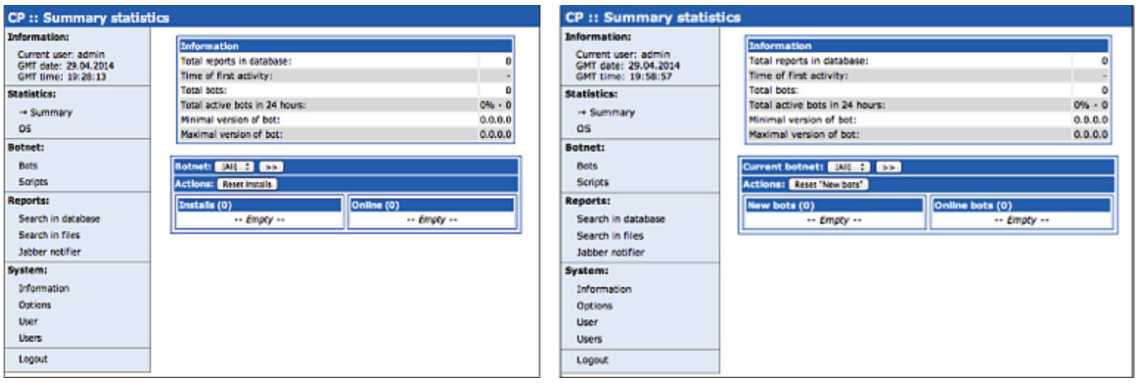

Figure 2: Control panels for Zeus 1.3.2.1 and Zeus 2.0.8.9/2.1.0.1

Once the panel is set, the builder (shown in Figure 3) is used to generate the bot payload to infect the victim PCs. The builder offers options to add parameters for zombies to connect back home. (This step is similar in Zeus versions 1 and 2.) The builder will be executed on a Windows computer or on a Linux computer with the Wine windows application emulator.

The builder has sophisticated features. It can track if a system is infected by a Zeus malware program – and even disinfect the system.

Once the user completes the easy install screen, the builder is used to create the bot.exe payload. This payload is then used in campaigns designed to trick victims into running it to infect systems by way of email phishing or drive-by download campaigns, or by other invasive methods such as exploiting known or unknown vulnerabilities to gain unauthorized access to systems. It is possible to create distinct payloads for distinct botnets that will call back to the same command and control. The Zeus toolkit can control multiple botnets from a single command and control panel.

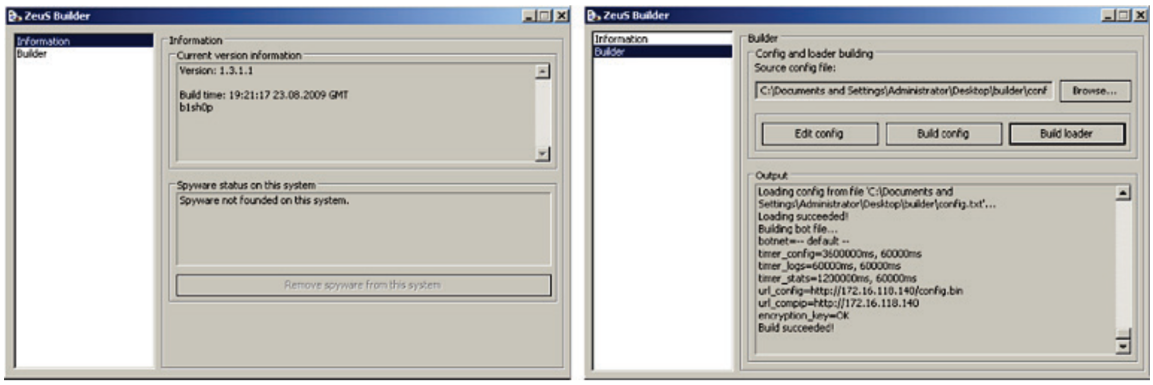

Figure 3: The Zeus 1.3.1.1 builder is used to generate actual Zeus bot payloads to infect systems

1.4 INFECTION / The first iteration of Zeus used several techniques to hide itself on an infected system. Systems infected with Zeus variants have several hidden files in a hidden directory. The hidden lowsec directory is typically located in the system32 directory and includes the Zeus configuration file, the log file and the encrypted payload.

The payload uses Windows API hooks to hide the files. Specifically the NtQueryDirectoryFile API hook is used to filter out the Zeus-related files. As a result, when browsing the system directory via Windows Explorer, a user would not see these hidden files or the directory, as shown in Figure 4. The directory is, however, accessible via the command line (see Figure 5) or by using a rootkit analyzing tool such as GMER.

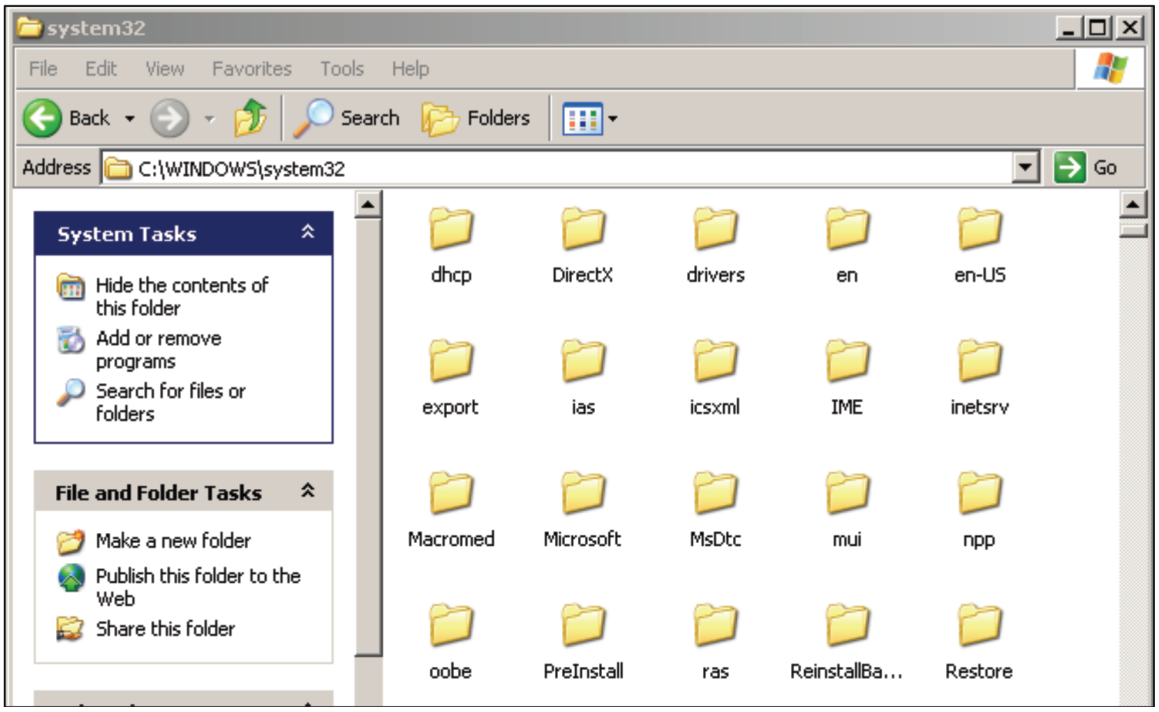

Figure 4: The lowsec directory created by Zeus infection is hidden

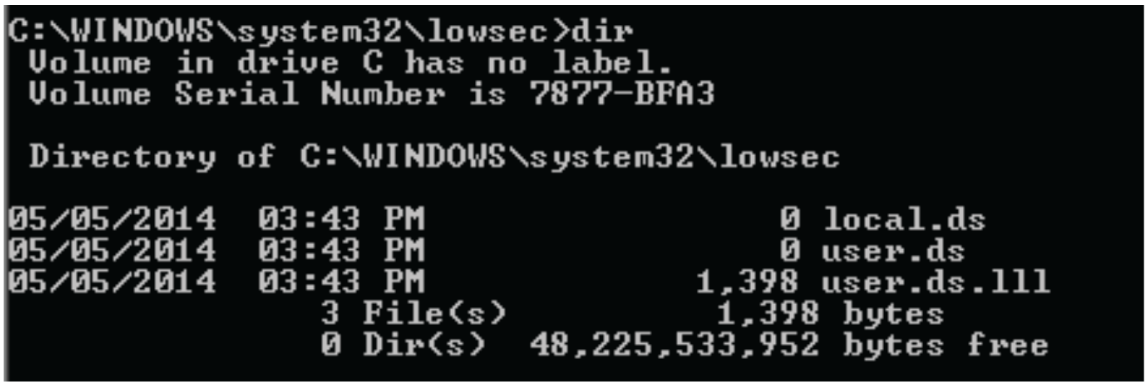

Figure 5: The directory (dir) command shows the hidden directory created by the Zeus payload

Zeus payloads generated by the builder come in an obfuscated format. De-obfuscation is required to recognize the payload code. Alternately, memory forensics tools such as Volatility can be used to extract injected code artifacts. Zeus uses decryption layers to de-obfuscate itself in memory, thus providing the malware with effective protection against static analysis tools like IDA Pro and other disassemblers. Once the payload has been decrypted and run on a host system, a configuration file will be downloaded from a predetermined location and also decrypted in memory.

Upon execution, the malware will attempt to infect other processes on the same system via remote thread injection. The most commonly infected processes are winlogon.exe, svchost.exe and explorer.exe. A typical technique to spot the code that resides in memory of an infected process is to look at the heap allocated data using a debugger tool; the Zeus code will reside in high memory locations due to its remote thread injection technique.

Utilizing memory forensics tools on an infected host can yield information on the location of the code that Zeus injects into other processes, along with the hooked APIs in the infected processes. Figure 6 shows an excerpt from the Volatility memory forensics tool showing a hooked API routine made by Zeus inside of the svchost process.

```
Hooked API's
Hook mode: Usermode
Hook type: Import Address Table (IAT)
Process: 1120 (svchost.exe)
Victim module: kernel32.dll (0x7c800000 - 0x7c8f6000)
Function: ntdll.dll!NtCreateThread
Hook address: 0xec5080
Hooking module: <unknown>

Disassembly(0):
0xec5080 55              PUSH EBP
0xec5081 8bec            MOV EBP, ESP
0xec5083 53              PUSH EBX
0xec5084 ff7524          PUSH DWORD [EBP+0x24]
0xec5087 8b5d1c          MOV EBX, [EBP+0x1c]
0xec508a ff7520          PUSH DWORD [EBP+0x20]
0xec508d b83b50ec00      MOV EAX, 0xec503b
0xec5092 ff7518          PUSH DWORD [EBP+0x18]
0xec5095 2b              DB 0x2b
0xec5096 05              DB 0x5
0xec5097 18              DB 0x18
```

Figure 6: A hooked API located in infected svchost process as shown by the Volatility tool

Looking through the memory of the hook address will reveal several subroutines that Zeus has injected into the target processes.

Another way to identify an infection by some of the early Zeus variants is their use of a unique mutex. While the mutex will vary depending on the configuration of the Zeus payload, it has been observed that the string _AVIRA_XXXX will typically be a strong indicator of a Zeus infection. Mutexes are a common method used by malware and other software to keep track of their presence on a target system. The Zeus mutex is shown in Figure 7.

```
0x060c76b0     2     1      1 0x00000000          _AVIRA_2108
```

Figure 7: A mutex resident on a Zeus-infected system as seen by the Volatility tool

In order to survive reboots, the Zeus malware makes Windows registry modifications, adding itself to the Userinit key, as shown in Figure 8. This behavior is consistent across all versions of the Zeus payload analyzed by PLXSert. In addition, the sdra64 executable is typically associated to version 1 of the Zeus crimeware kit payload.

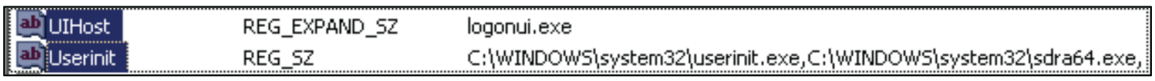

Figure 8: This Zeus registry entry enables startup persistence

Once Zeus is executed, it injects code into a number of predetermined processes to enable communication with the command and control and to process commands and propagate its infection to the host system. The code in memory also places persistent API hooks on several Windows functions in DLLs such as WININET.dll, ws2_32.dll, kernel32.dll and user32.dll as shown in Figure 6. Another system change is the modification of the registry to disable firewall rules.

1.5 REMOTE COMMAND EXECUTION / The Zeus panel comes with a number of remote commands, shown in the command help list in Figure 9. These commands can be executed on infected zombies and range from operating system administrative tasks and remote file execution to controlling the behavior of web browsers.

```
$_COMMANDS_LIST = array
(
  'reboot'   => 'Reboot computer.',
  'kos'      => 'Kill OS.',
  'shutdown' =>  'Shutdown computer.',

  'bc_add [service] [ip] [port]' => 'Add backconnect for [service] using server witn address [ip]:[port].',
  'bc_del [service] [ip] [port]' => 'Remove backconnect for [service] (mask is allowed) that use connection to [ip

  'block_url [url]'   => 'Disable access to [url] (mask is allowed).',
  'unblock_url [url]' => 'Enable access to [url] (mask is allowed).',

  'block_fake [url]'   => 'Disable executing of HTTP-fake/inject with mask [url] (mask is allowed).',
  'unblock_fake [url]' => 'Enable executing of HTTP-fake/inject with mask [url] (mask is allowed).',

  'rexec [url] [args]'   => 'Download and execute the file [url] with the arguments [args] (optional).',
  'rexeci [url] [args]'  => 'Download and execute the file [url] with the arguments [args] (optional) using intera
  'lexec [file] [args]'  => 'Execute the local file [file] with the arguments [args] (optional).',
  'lexeci [file] [args]' => 'Execute the local file [file] with the arguments [args] (optional) using interactive

  'addsf [file_mask...]' => 'Add file masks [file_mask] for local search.',
  'delsf [file_mask...]' => 'Remove file masks [file_mask] from local search.',
  'getfile [path]'       => 'Upload file or folder [path] to server.',

  'getcerts'          => 'Upload certificates from all stores to server.',
  'resetgrab'         => 'Upload to server the information from the protected storage, cookies, etc.',
  'upcfg [url]'       => 'Update configuration file from url [url] (optional, by default used standard url)',
  'rename_bot [name]' => 'Rename bot to [name].',
  'getmff'            => 'Upload Macromedia Flash files to server.',
  'delmff'            => 'Remove Macromedia Flash files.',
  'sethomepage [url]' => 'Set homepage [url] for Internet Explorer.'
);
```

Figure 9: A command help listing in the Zeus 1.3 panel shows the available remote commands

Once the victim is infected, the victim bot will call the command-and-control panel. The information about the bot will show up in the information table within the panel, as shown in Figure 10. The control panel features many information-gathering tools for identifying the location and number of bots, the version of the bots, and information about different botnets and operating systems.

Even though the main payload of Zeus targets Microsoft Windows operating systems (from XP to 8), there are also payloads for Linux, Mac OS and Android operating systems.

While the Zeus framework has been iterated only a few times, an abundant number of modifications have been shared on the Internet. The Zeus Gameover P2P is a major iteration of Zeus that introduced a peer-to-peer communication protocol. Gameover also introduced encrypted traffic between infected hosts, making network analysis more difficult. Furthermore, a Gameover version was reported to introduce DDoS capabilities. A detailed paper on the P2P variant of Zeus is available on the CERT Polska webpage.

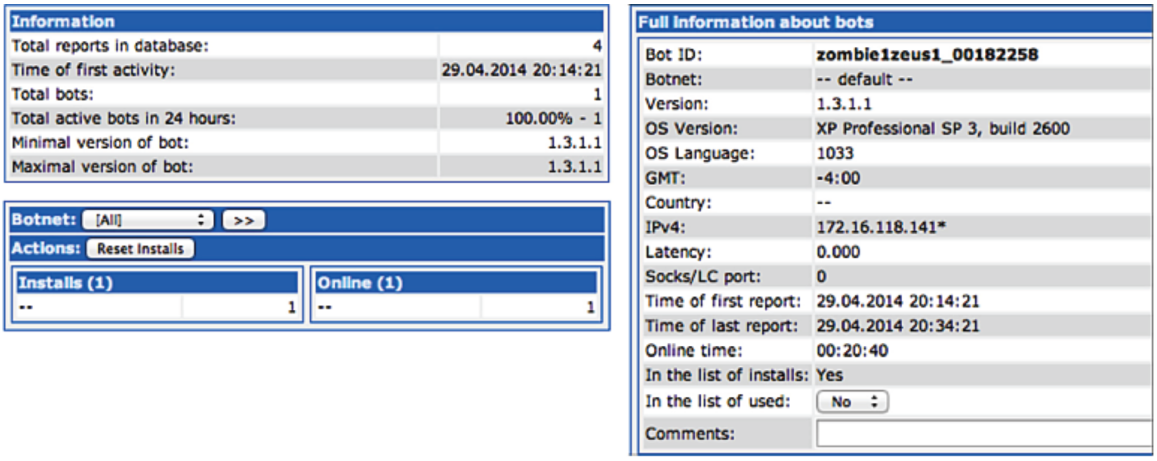

Figure 10: Details about the infected bots are shown in the Zeus command-and-control panel

Having readied the bot payload and command and control, a malicious actor will proceed to harness as many victim systems as possible. This is usually accomplished through spam email campaigns that entice prospective victims to run executables by saying that the files serve other purposes or by embedding a payload into a downloadable executable. A malicious actor may later create additional payloads that the infected bots will automatically download and execute.

Once malicious actors have infected zombies under their control, they can manage the zombies through the command and control panel, as shown in Figure 11. The attacker is also capable of gathering information about the infected system, including getting a screenshot of the current active desktop.

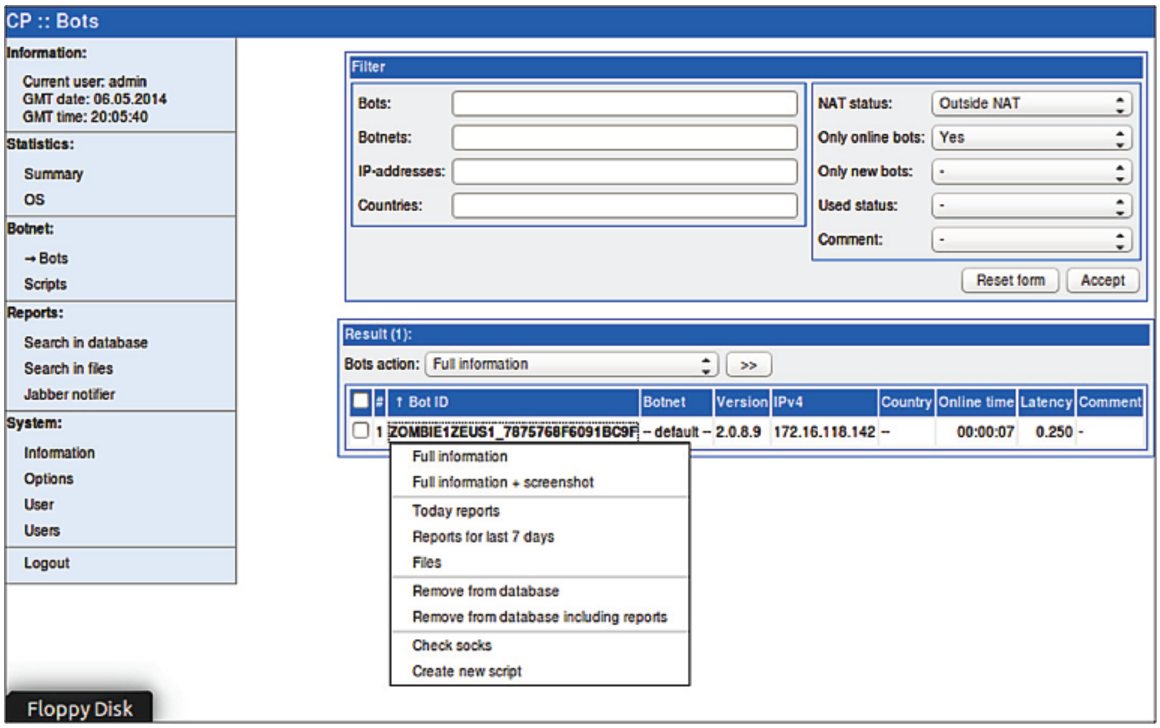

Figure 11: Menu items available to the attacker to manipulate compromised hosts. Zeus offers the unusual feature of being able to manipulate one or more botnets.

In addition to gathering information about the infected zombies, the malicious actors have the ability to generate scripts that can be executed by the bot payload. The bots will make random-interval calls back to the C2 to check for available script commands to execute. These scripts may range from downloading and executing remote and local files to modifying the homepage of an infected computer's Internet browser.

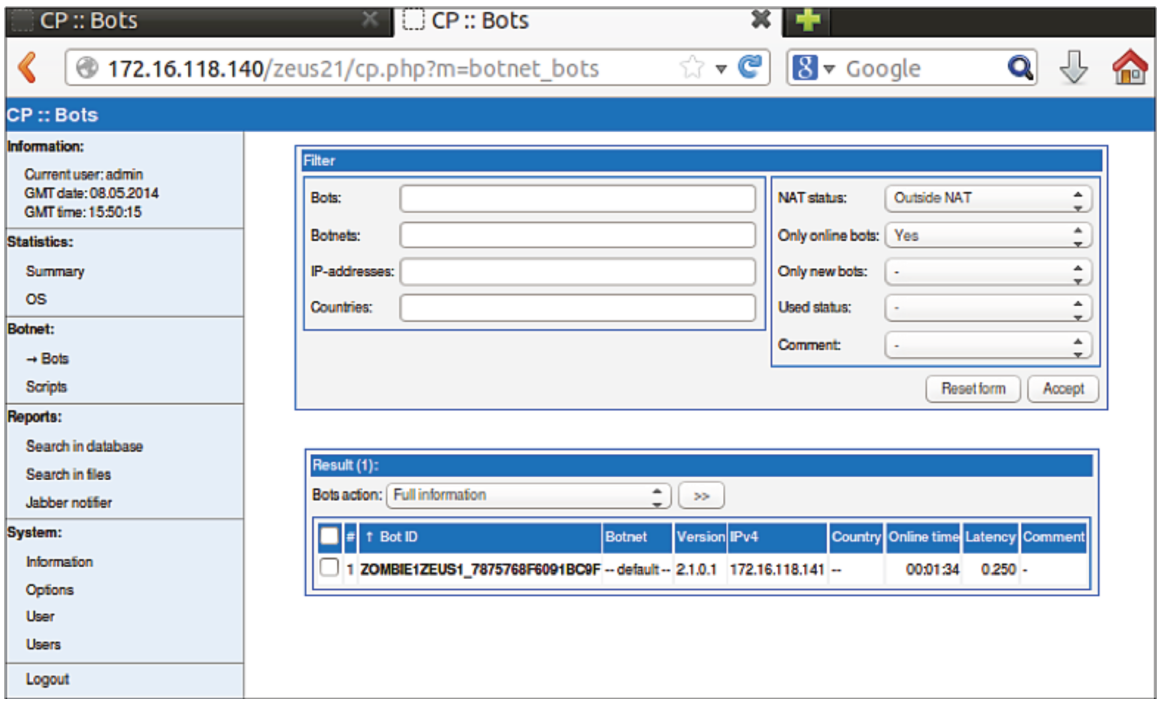

Figure 12: The control panel of Zeus 2.1 displays a successful infection with bot identification

The Zeus framework allows operators to place executables on the zombie systems they control. PLXSert has observed traffic in DDoS attack campaigns where the Zeus framework and the Dirt Jumper DDoS toolkit appear to be combined, specifically Zeus appears to be used to build the botnet and drop DDoS malware payloads such as Dirt Jumper onto them. Dirt Jumper is one of the most used DDoS kits in the underground marketplace. Zeus operators first create a Dirt Jumper control panel, prepare the executable (shown in Figure 13), and then use Zeus to download and execute the DDoS executable.

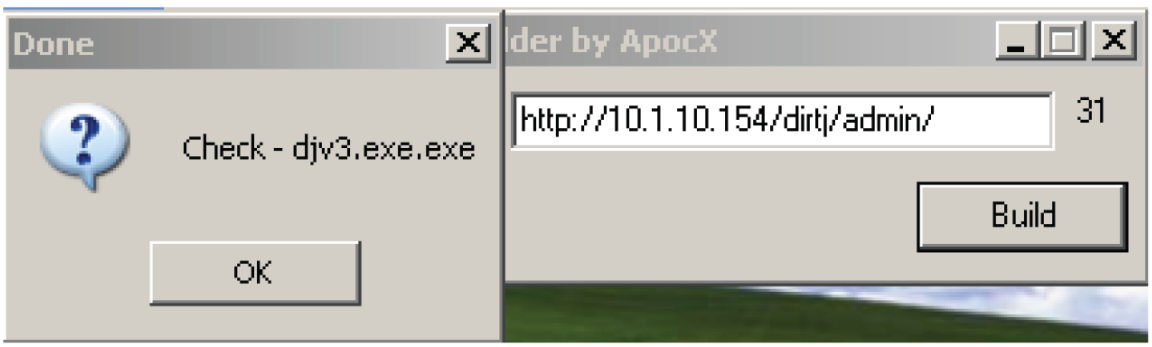

Figure 13: The creation of a Dirt Jumper executable

Utilizing the scripting interface shown in Figure 14, attackers can command their infected hosts to download and execute the remote file location of a DDoS executable such as Drive. This capability provides a malicious actor with the means to launch a large-scale DDoS attack.

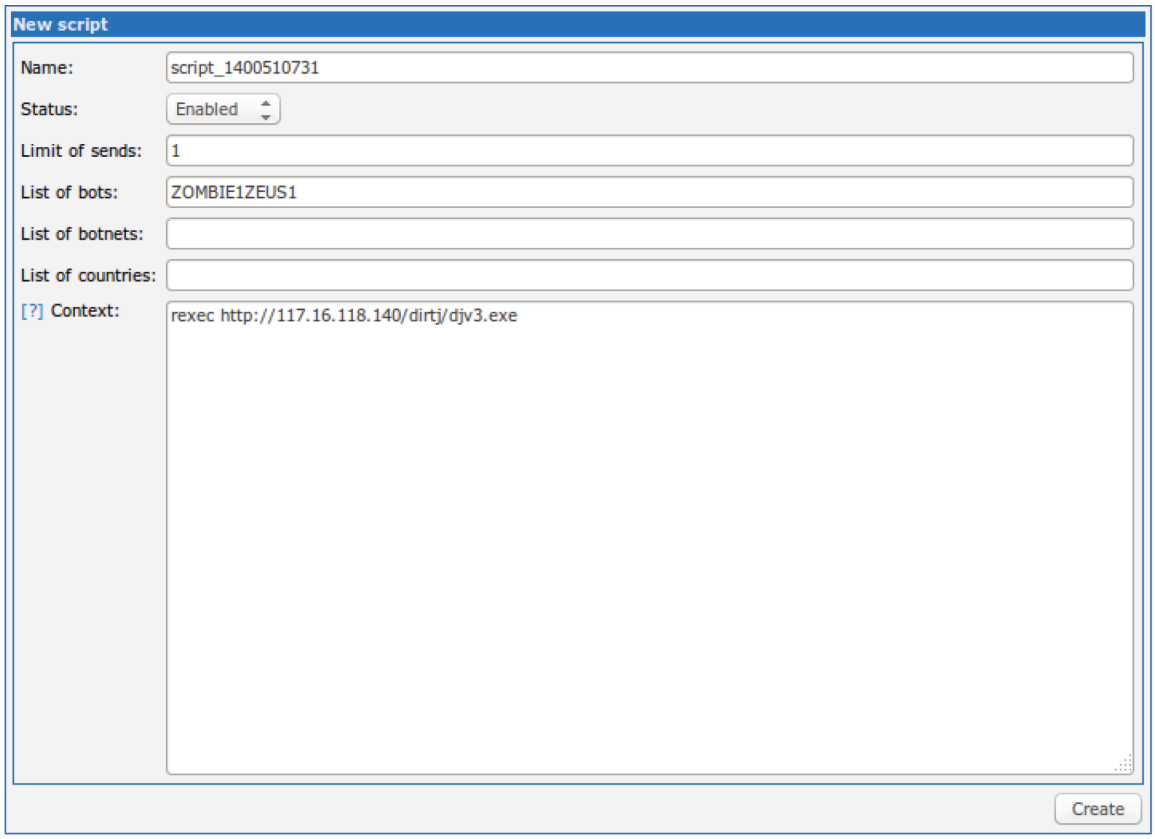

Figure 14: The scripting feature in the command and control panel allows the download execution of the Dirt Jumper payload on a host system

Once the victim downloads and executes the DDoS payload, the victim will connect back to the attacker's Dirt Jumper v3 local command and control panel, as shown in Figure 15.

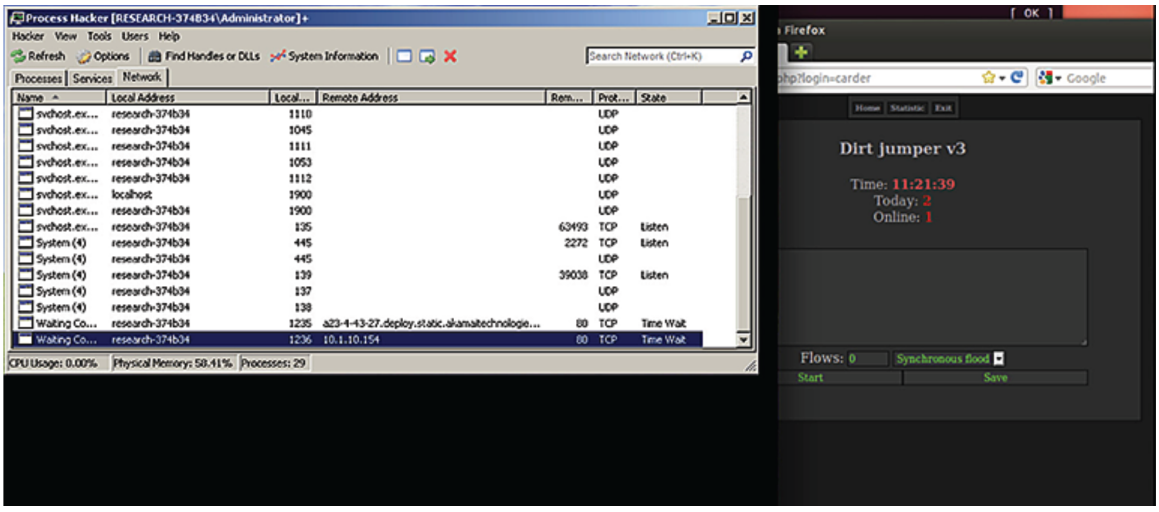

Figure 15: A Zeus-infected host connects to the Dirt Jumper v3 command and control panel

The Zeus crimeware framework is not only one of the most used crimeware kits for stealing banking credentials and credit card information, it has become a versatile tool for criminals with the intent and technical skills to customize its use to target other industry verticals as well.

Although Zeus/Gameover version reportedly introduced DDoS capabilities, PLXSert has no evidence that the Zeus framework kit can orchestrate significant DDoS campaigns by itself, but if combined with other DDoS toolkits, the capabilities of the Zeus framework would enable malicious actors to use it as a powerful DDoS botnet builder.

1.6 LAB SIMULATION: ATTACKING THE CLOUD / Lately the Zeus framework has been observed targeting cloud-based applications through SaaS/PaaS infrastructures. The leak of the Zeus source code and the ability of malicious actors to adapt it to create customized payloads and to attack specific cloud-based applications is driving its use as a multi-vector attack crimeware kit, resulting in campaigns with multiple, previously unseen combinations of attack vectors.

By customizing payloads, criminal actors are using the Zeus framework to gather and exfiltrate specific information from targeted sites, such as application login credentials. With the widespread use of cloud services in many businesses, often from places outside the hardened corporate environment, criminals are finding ways to target cloud-based applications.

The targeting of SaaS/PaaS instances is particularly favored by criminals because these platforms are a gateway to abuse and allow attackers to exploit cloud vendors that have extensive bandwidth and processing power. By targeting SaaS/PaaS, cybercriminals take advantage of the resources of both the end users and the providers. The providers' defense technologies allow the attackers the advantage of gaining anonymity behind the providers' cloud-based infrastructure.

There are indicators that suggest these types of attacks are already being used against well-known SaaS/PaaS vendors. PLXSert has observed well-known cloud-services vendors among the sources of many DDoS campaigns. Malicious actors are now targeting vendors for which the attacks can leverage infrastructure resources while also harvesting exfiltrated user data that can be used to target other verticals.

1.6A WEBINJECTS / A particularly powerful feature used to attack specific applications is the webinjects configuration in the Zeus framework. Attackers use the webinjects configuration to customize attacks for specific cloud-based applications. This feature is commercialized in the underground – malicious actors sell customized Zeus webinjects for these purposes. In the past, webinjects were customized specifically for banking sites. Webinjects are now being adapted to target specific web applications.

The Zeus crimeware kit has many features that are used by attackers to grab login credentials and to monitor the web usage of victims. If these victims are part of a particular organization, corporation or use cloud services, it is a matter of time until enough information is exfiltrated to customize an attack via webinjects or customized scripts that may lead to the actual compromise of such organizations, corporations or cloud services. A recent example of this type of attack was the targeting of a customer relationship management (CRM) platform accessed by businesses from the web.

PLXSert tested this capability of the Zeus framework in a lab environment by modifying the webinjects file to target an application that simulates a banking application site. The application used for this test was McAfee Hacme Bank v2.0, a learning platform provided by McAfee to promote secure software development. In general, the following modification of the webinject code could apply to any web application in any industry.

The webinject file shown in Figure 16 is used to craft special code that adds or modifies the HTML web page to be displayed to the user by the infected computer's browser. Malicious actors can customize the display to harvest data as the user accesses web-based services.

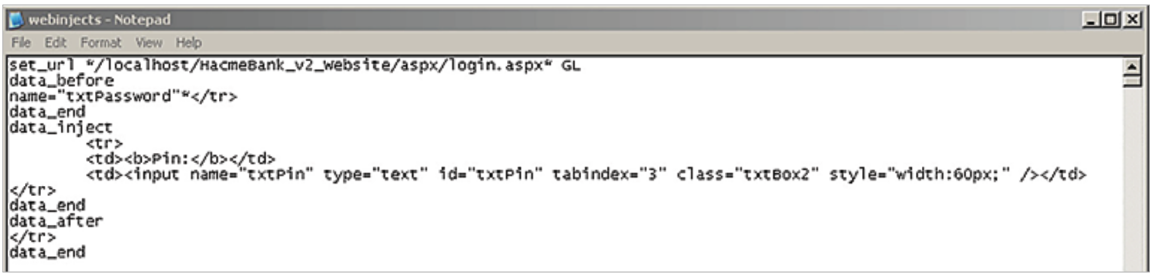

Figure 16: The webinject file is used by attackers to customize attacks for specific sites and applications

The screenshot in Figure 17 shows the login page of the Hacme Bank before it was infected by Zeus using a modified webinject. The webinjects are typically used to modify or capture data in certain fields of a webpage, which then can be used for data aggregation. The attacker will craft a webinject systematically to add elements to a specific webpage to trick its users into providing personal information about themselves or sensitive credentials.

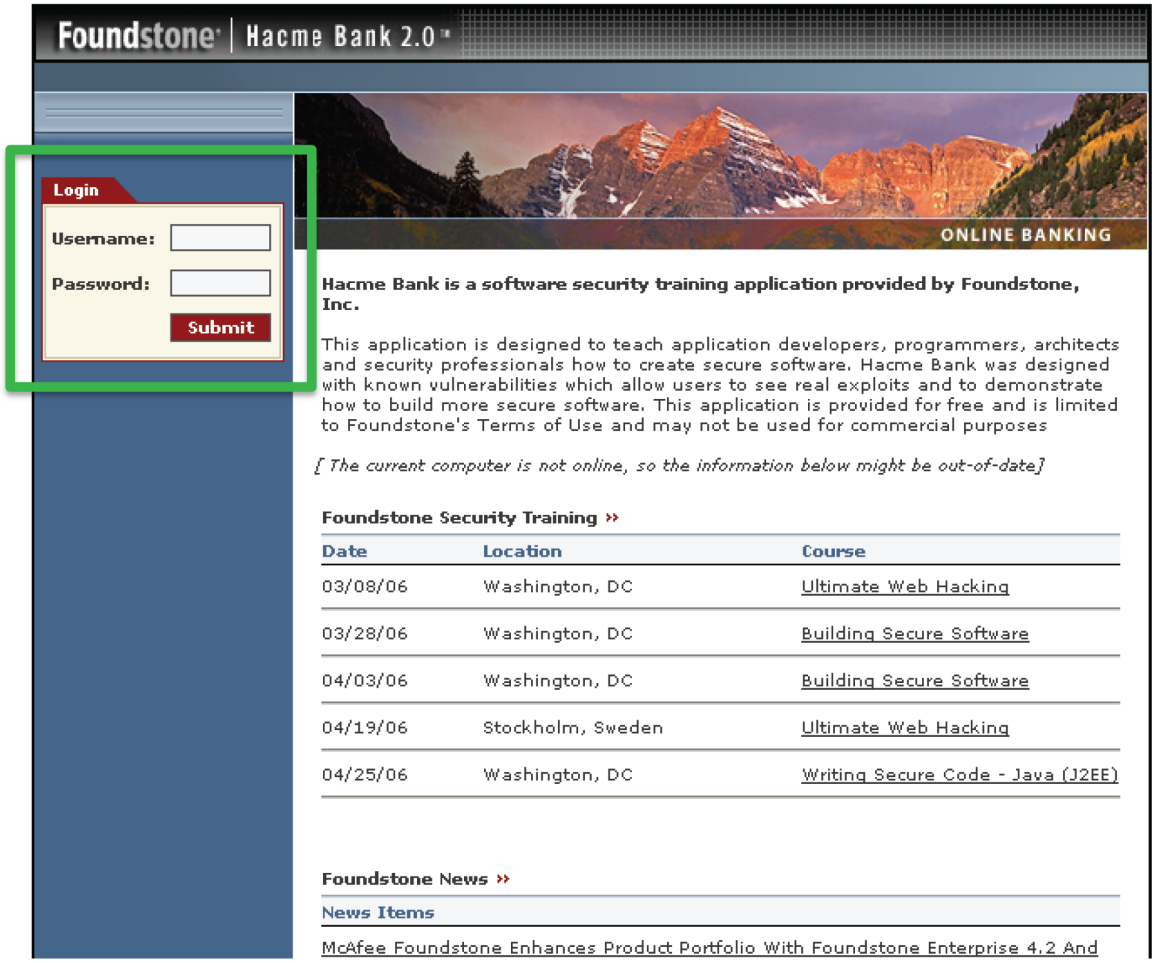

Figure 17: The login screen for McAfee Hacme Dank 2.0 before web injection

In the lab exercise, an additional login field was added to the banking webpage via webinjects, as shown in Figure 18. For a typical user this change may not raise alarms, because it is presented as part of the login process and could be assumed to be a legitimate change to the webpage. A webinject such as this one, which requests the user's banking PIN number, may mislead users into inputting sensitive information in the fake field.

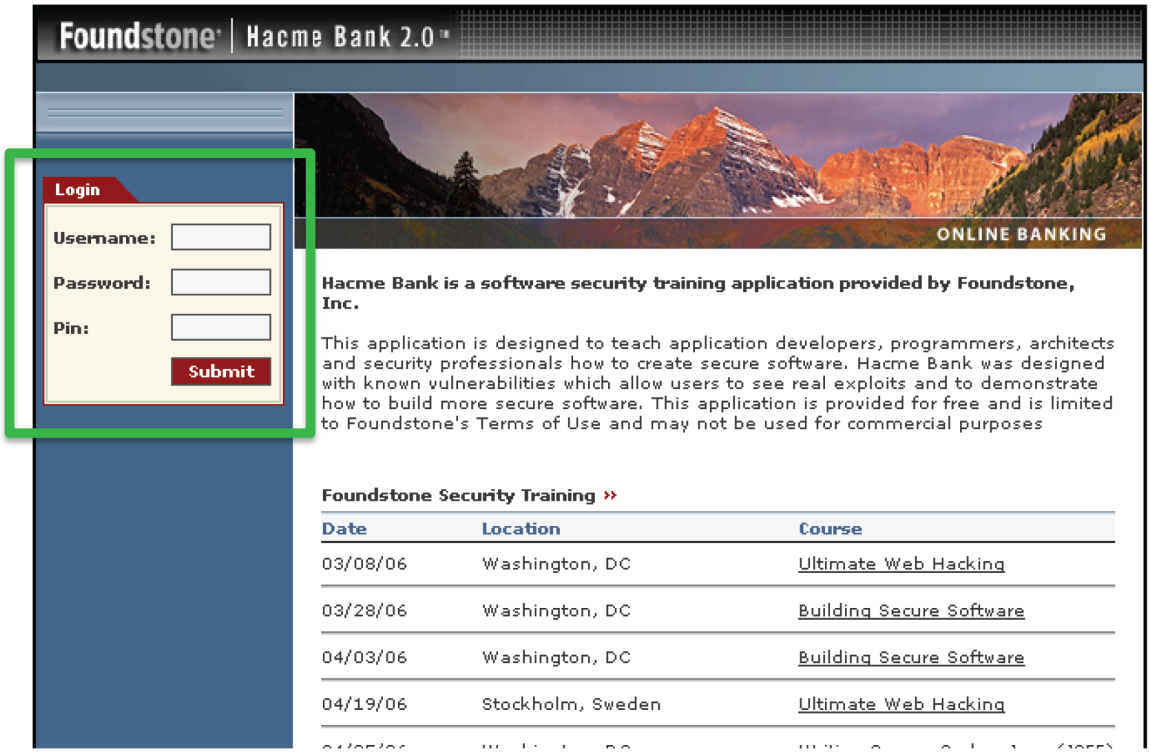

Figure 18: The Hacme Bank login page with an additional field injected to harvest the user's PIN in addition to login credentials.

Once the user has entered the information, it will be harvested, transferred and indexed in the searchable database of the Zeus control panel, allowing the malicious actors to access the information, as shown in Figure 19.

View report (HTTP request, 273 bytes)	
Bot ID:	**malwarea_ad4faa_000630d6**
Botnet:	-- default --
Version:	1.3.1.1
OS Version:	XP Professional SP 3, build 2600
OS Language:	1033
Local time:	14.05.2014 14:04:54
GMT:	-4:00
Session time:	01:13:54
Report time:	14.05.2014 18:05:00
Country:	--
IPv4:	192.168.200.132
Comments for bot:	-
In the list of used:	No
Process name:	C:\Program Files\Internet Explorer\iexplore.exe
User of process:	-
Source:	http://localhost/HacmeBank_v2_Website/aspx/login.aspx

```
http://localhost/HacmeBank_v2_Website/aspx/login.aspx
Referer: http://localhost/HacmeBank_v2_Website/aspx/login.aspx
Keys: jvjv5687891234
Data:

__VIEWSTATE=dDwtMjcwNDc2NTExOzs%2BKaVjdDukMQCrjL%2BTJBtrWKxFt3k%3D
txtUserName=jv
txtPassword=jv789
txtPin=1234
btnSubmit=Submit
```

Figure 19: Information gathered from a simulated target includes username, password and PIN number

Figure 20 shows that the search capabilities in the Zeus tool allow attackers who have harvested a large numbers of compromised hosts to data mine to identify users who accessed websites and applications of specific corporations or cloud services providers. Attackers may then create their own webinjects and scripts to attack those sites.

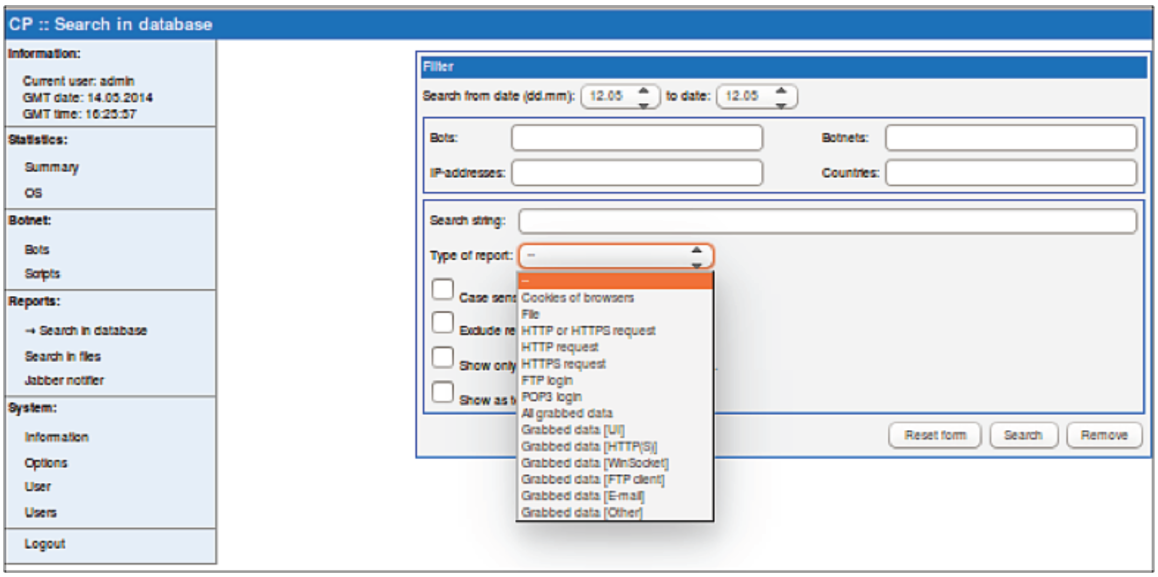

Figure 20: Search capabilities of the database in the Zeus control panel

1.7 RECOMMENDED MITIGATION / Zeus payloads can be customized and obfuscated, effectively preventing detection. Some Zeus tracking organizations estimate the antivirus detection rate for Zeus at only 39%. PLXsert expects the further modification, adaptation and enhancement of the Zeus malware toolkit, including hybrid payloads with other crimeware kits, will continue, as will its distribution and further infestation across platforms, including Windows, Mac OS, Linux and phone operating systems, such as Android and iOS.

PLXsert recommends the following mitigation actions:

- Zeus is mainly a client-based attack vector. Users are tricked into running programs that infest their devices, so organizational security policies and user education can help. Enforce security policies for system security and patches and updates. Educate users about how this type of attack is executed from email clients and web browsers.

- Clean-up effort by the security community is fundamental. Initiatives such as ZeuS Tracker are necessary to contain and manage this threat. Takedown follow-up efforts must also be implemented to reduce the number of infected command and control centers.

- Learn how to prevent, detect and remove Zeus infections. Symantec Security Response provides extensive information to help you do this.

- Write Snort rules for Zeus traffic. Sourcefire VRT Labs has an excellent source for writing Snort rules based on Zeus traffic.

1.8 CONCLUSION / The Zeus crimeware kit has become a versatile framework used by criminals to customize attacks targeting many industry verticals in addition to banking. The Zeus code is being used to target PaaS/SaaS vendors to take advantage of their resources, bandwidth, reputation and defenses. The Zeus framework is also actively used to build large botnets, which are being used in DDoS campaigns in combination with DDoS toolkits such as Dirt Jumper.

Most of the changes of the Zeus code appeared between versions 1 and 2. It appears that major development has stopped with the alleged retirement of the creator. However, modifications and payloads have been introduced in variants such as Zeus Gameover, which includes P2P capability and reportedly DDoS payloads. There are many other crimeware kits built upon Zeus, but they seem to focus on front-end GUI modifications, and they do not seem to be as effective or widely used.

PLXSert expects further customization and the continued use of the Zeus toolkit, which is likely to include the enhancement of current payloads, creation of hybrid payloads from other crimeware toolkits and the introduction of payloads customized to target specific verticals, platforms, organizations and cloud services vendors. Criminal demand will drive malicious actors to develop payloads and features, seeking distribution and monetization in the crime ecosystem. The popularity of Zeus crimeware will continue due to its ease of use, easy setup and versatility.

1.9 APPENDIX /

- Technical report: ZeuS-P2P monitoring and analysis, CERT Polska – http://www.cert.pl/PDF/2013-06-p2p-rap_en.pdf
- The Adollon Blog – http://www.adallom.com/blog/a-new-zeus-variant-targeting-salesforce-com-accounts-research-and-analysis/
- ZeuS Tracker – https://zeustracker.abuse.ch/
- Trojan.Zbot – Removal, Symantec – http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99&tabid=3
- Zeus Trojan Analysis, VRT Labs – https://labs.snort.org/papers/zeus.html

The Prolexic Security Engineering and Research Team (PLXsert) monitors malicious cyber threats globally and analyzes these attacks using proprietary techniques and equipment. Through research, digital forensics and post-event analysis, PLXsert is able to build a global view of security threats, vulnerabilities and trends, which is shared with customers and the security community. By identifying the sources and associated attributes of individual attacks, along with best practices to identify and mitigate security threats and vulnerabilities, PLXsert helps organizations make more informed, proactive decisions.

Akamai® is a leading provider of cloud services for delivering, optimizing and securing online content and business applications. At the core of the company's solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 40 offices around the world. Our services and renowned customer care enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on *www.akamai.com/locations*
