Special!!! ZeuS Botnet for Dummies

Archived: 2026-04-05 17:04:40 UTC

MalwareIntelligence is a site dedicated to research on all matters relating to anti-malware security, criminology computing and information security in general, always from a perspective closely related to the field of intelligence.

Special!!! ZeuS Botnet for Dummies

After dealing with some emphasis on the activities of the most active botnets now, ZeuS, let's see a more detailed description of their crime.

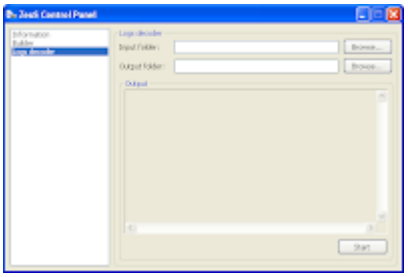
If we talk about malware and botnets, no doubt ZeuS has a particular advantage due to the amount of zombies that are part of its campus. ZeuS is designed to steal any information that is stored on the computers of victims remotely and carry out other attacks aimed at stealing information such as phishing.

Therefore, we could say that ZeuS is a spyware, but also has capabilities for other types of malware such as backdoors, trojans and viruses. However, the author mentions in the installation manual that you don't like to call any of these forms in this crimeware, but will refer to it as a "bot software".

Although we know the external face of ZeuS (the web interface management and control of zombies), has certain features that are constantly evolving and professionalize achieving greater flexibility and adaptability to ensure operation on different versions of Windows. This makes ZeuS a latent threat and very dangerous for any information system.

In this sense, ZeuS also ensures performance "working" on the privilege level 3 (where the applications are) the operating system to avoid incompatibilities between the implementation of equipment and devices (which operate at lower levels). Though it may seem an irrelevant fact, this allows greater flexibility and hence a higher yield at the time of the fraudulent and criminal activities for which it was conceived.

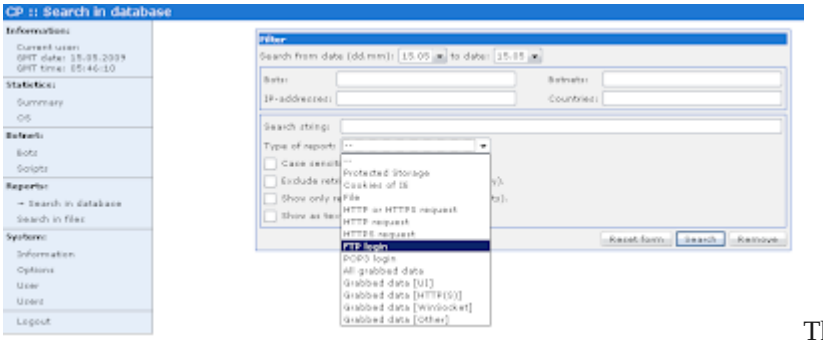
The latest version of ZeuS is written with version 9 of the C + + language, and among the features that have this web application (malicious), we can mention:



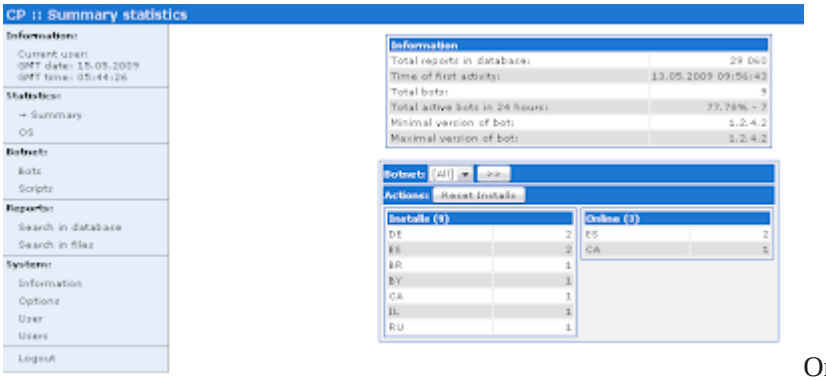
Monitor network traffic (sniffer) TCP.
Intercepts the FTP and POP3 connections from any port.
Intercepts HTTP and HTTPS requests from all applications that work with the library wininet.dll (eg IE). This demystifies the myth in which ZeuS uses a BHO to intercept applications through IE.

Functions server (socks4/4a/5).
Backconnect for all of the infected computer services (RDP, Socks, FTP, etc.).
Get screenshots in real time.
Ability to conduct phishing attacks.
Incorporates anti-analysis mechanisms.
Constructor of the trojan that spreads and configuration file.
Polymorphic encryption.

Another technical detail is that all communication is done by ZeuS through a symmetric encryption algorithm (RC4).



The server is the heart of ZeuS, and any botnet, and who is to obtain all records of infected computers that are part of the botnet and execute commands remotely.



On the other hand, many botnets using virtual servers to their criminal operations. However, this plays against the botnet when is very large, if ZeuS, as usually, the virtual servers don't have too many resources, so it's customary for botmaster using dedicated servers to host the bot. This is an important fact to keep in mind during the research side.

Accordingly, and as every application requires a minimum of resources to run satisfactorily, in the case of this botnet, the requirements are just to have 2GB of RAM and 2x frequency of 2 GHz CPU. As we see, the minimum requirements aren't at all a constraint VIP. Anyone can implement ZeuS, even without these minimum requirements.

Furthermore, it's assumed that the computer is running an HTTP server with PHP (the language is generally develop these crimeware) and MySQL (to create the database with statistical information that shows your activity). Another requirement is Zend Optimizer, which is necessary to protect and optimize the scripts.

With regard to updates, ZeuS is also can be "groomed" by newer versions without too much effort. During the last six months have been released five versions (based on each one approx. 35 days) with correction of errors, changes and new features, not the versions with smaller arrangements.

After looking at the diagram, many wonder what the number of each version. A teaching mode could say that if we have the "A.B.C.D" ...

A means a complete package of crimeware.
B represents changes that cause total or partial incompatibility with earlier versions.
C specifies error correction, added functionality, improvements, etc..
D is the number of refuds (changes) to the current version.

This is just a screenshot of what can and ZeuS represents in terms of skills and maneuvers that have an environment within which criminal crimeware applications are the main actors.

Related information this Blog

Botnet. Securización en la nueva versión de ZeuS
ZeuS Carding World Template. Jugando a cambiar la cara de la botnet
Entidades financieras en la mira de la botnet ZeuS. Segunda parte
Entidades financieras en la mira de la botnet ZeuS. Primera parte
ZeuS Botnet. Masiva propagación de su troyano. Segunda parte
ZeuS Botnet. Masiva propagación de su troyano. Primera parte
LuckySploit, la mano derecha de ZeuS

Jorge Mieres
