Top 10 most dangerous malware types with bank accounts

Zeus, SpyEye, Ice IX or Citadel are notorious malware software that can infiltrate user computers, poison and steal personal information and financial data on online bank accounts. online.

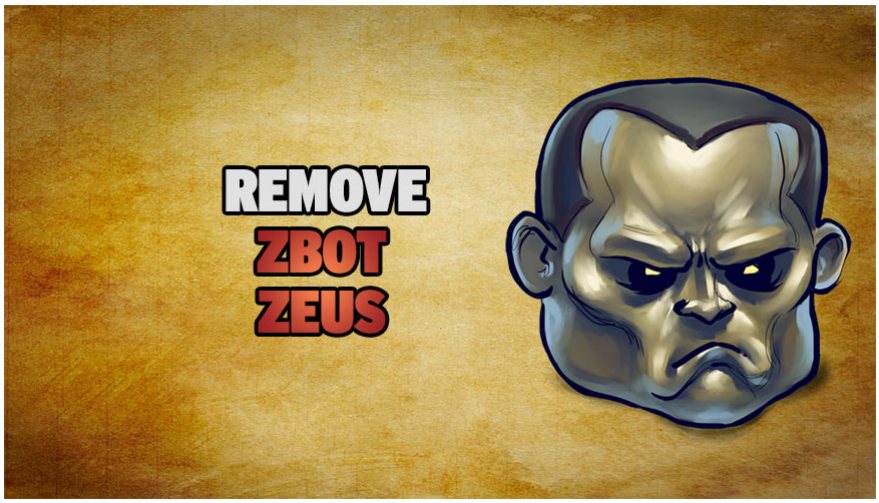
In early June 2014, a coordinated effort called Operation Tovar with the participation of US, European enforcement agencies and security agencies around the world to prevent the spread of Zeus Gameover botnet and control Control servers against CryptoLocker attack - a very famous ransomware means "ransom virus" when controlling the victim's computer will encrypt the system files, and at the same time ransom warning if you want to exchange for decoding key.

Gameover Zeus and CryptoLocker are not the only two names. There are also many variants and other types of Trojans stealing information from other users, but you also need to pay attention if you don't want a good day to cry because you don't understand all the money in your account. " that fly "!

Here are 10 malicious software that anyone who has, will and will open a bank account.

1. Zbot / Zeus

Zeus, also known as Zbot, is a notorious trojan capable of poisoning **computers running Windows operating systems** and then stealing account information, including usernames and passwords. as well as other related financial data. Once installed, it will proceed to download configuration files and updates from the Internet. Computer criminals can completely create these Zeus files by using the trojan builder tools available on some websites.



Zeus was created to steal user data from infected systems, including **system information, passwords, bank accounts or other financial data** and can be customized to gather information in some specific countries using a variety of transformation methods. With the information retrieved, computer criminals can log into bank accounts and carry out a series of unauthorized transfer transactions through a complex network of many computers.

Zbot / Zeus is created based on a client-server model and requires the **Command and Control server (command** -line servers) to send and receive information over the network. This Command and Control server is considered a weakness of malware architectures so law enforcement forces can use it to destroy Zeus.

However, that inherent weakness has been noticed by hackers. The latest variant of Zeus / Zbot includes a **domain generation algorithm (DGA) that** will enable Command and Control servers to resist any intrusion. DGA will create a list of domains that bots want to connect to when the central server is inaccessible.

According to many experts, Zeus has evolved over a long period of time and has actually become a "super-malicious" software. This malware is capable of executing many information-stealing functions such as stealing data sent in HTTP forms, stealing confidential information of accounts stored in Windows, stealing financial information. FTP and POP accounts, stealing / deleting HTTP and flash cookies, modifying HTML pages of the website with the aim of stealing information, redirecting victims from target sites to websites that the attacker controls , lost the function of taking screenshots of the computer, deleting important registry entries or making the computer unable to boot .

Zeus / Zbot is also known by many other names including PRG and Infostealer, whose "achievements" infect 3.6 million systems in the United States. In 2009, security analysts discovered Zeus spread malware to more than 70,000 bank accounts and organizations, including NASA and Bank of America.

2. Zeus Gameover (P2P)

Zeus Gameover is a variant of the "Zeus family" that performs the task of stealing user financial information through **a bonet network using peer-to-peer architecture.**

Zeus Gameover does not need to use Command and Control servers because the peer (computers) created in the bonet network can act as a standalone Command and Control server and can download the final commands or configuration files. , will proceed to send stolen data to malicious servers (malicious server).

Zeus Gameover is used by computer criminals to collect financial information including usernames, passwords, credit card numbers and other personal information they find useful. Zeus Gameover, according to reviews, has infected about 1 million computers worldwide.

3. SpyEye

A follow-up member of the "big Zeus family" is SpyEye, a data-theft malicious software (similar to Zeus) that was created to **steal money from online bank accounts** through **theft. Personal information, security codes and financial data.**

SpyEye also includes a **keylogger** capable of accessing login information from users' online banking accounts, which is very popular among computer criminals because it can be customized to attack organizations or infiltrate certain types of financial data.

SpyEye may interfere with a financial transaction as soon as a user starts performing online activities related to his account.

4. Ice IX

Ice IX is an edited variant of Zeus and is also one of the most sophisticated types of malware currently in existence.

Ice IX is used by computer criminals in order **to distribute malicious code similar to other malware to steal user's financial and personal information** such as email login or password and online bank account.

Like Zeus, Ice IX can also control the content displayed on online banking websites by infecting registration forms or information forms. From there, hackers can easily access the information they want.

Compared to the other members of the "Zeus family", Ice IX has more powerful abilities, the most important of which is the self-defense mechanism that allows it to evade tracking sites and monitor virtually all Command and Control servers are controlled by Zeus.

5. Citadel

Citadel appeared after the source code of Zeus leaked in 2011. Due to the open source nature, cybercriminals conducted a review and revision of Zeus to create Citadel for the purpose of serving many other malicious attacks.

For computer criminals, Citadel is an improved set of tools that they can use to **deceive users for the purpose of stealing personal information and bank accounts.** After that, the data will be used to access online accounts and perform illegal transactions.

6. Carberp

Carberp is a trojan created to help hackers steal personal information from online banking platforms accessed by infected computers.

The Trojan's behavior is similar to other malware in the "Zeus family" and is capable of stealing information from other malicious code-fighting applications. Carberp can steal sensitive data from malicious devices and download new data from Command and Control servers.

Carberp is one of the most popular financial data theft malware in Russia , mainly attacking banking systems and companies with financial transactions are done with numbers. large amounts. Carberp not only "releases" the malicious code into web pages, but also creates many holes in the system it attacks in order to hijack administrative rights.

Spread through many typical methods of using infected files such as attaching to email, drive-by download (attack by downloading automatically, used to install viruses and spyware onto the computer user properties, through which computer control is completely controlled) or clicking on fake pop-up modifications, the difference of this malware is that a large number of mainstream online resources are used. to gather information and potentially create illegal transactions. According to calculations, through Carperb, computer crimes have deployed bonet networks on more than 25,000 contaminated devices.

7. Bugat

Bugat is a kind of trojan that has many abilities similar to Zeus, especially used by computer crimes to steal financial information.

Bugat aimed at web surfing is done on the infected computer and collects information while the user is conducting transactions with online bank accounts. It can upload files from an infected computer, download and execute a variety of processes or steal information via the FTP protocol.

Bugat can also communicate with a Command and Control server from where it receives instructions and updates to the list of financial sites it targets. After that, the information collected will be sent to the remote computer of the computer crime.

To spread this malware, hackers mainly insert malicious links into emails that they send to target users. When a user clicks on the infected link, they will be redirected to an illegal website where Bugat executes the download process on the system.

8. Shylock

Shylock is a malicious code designed to retrieve user information in order to serve illegal activities.

Once installed, Shylock will communicate with remote Command and Control servers controlled by computer criminals, send and receive data from / to poisoned PCs.

Similar to Zeus Gameover, this malware can make the most of DGA - used to create multiple domains for receiving commands between the malicious server and the infected systems.

Through **drive-by download** , Shylock will be distributed to compromised websites and through **malicious** advertising - the type of online advertising with malicious code aimed at distributing malware that requires users to install the part Unintended software or secretly install cookie tracking files to collect information or track user surfing habits.

Another popular way to spread this malware is to insert **malicious JavaScript** into a web page, then create a pop-up that requires users to download an essential plugin for web-based media playback.

9. Torpig

Torpig is a very sophisticated malware designed to gather sensitive information like bank accounts instead of credit card information.

Bonet Torpig - a network of computers that have been compromised and controlled by computer criminals - is the main method they use to send spam emails or steal users' personal information from bank accounts online goods. Torpig also uses DGA to create domain names and locate the hacker Command and Server server.

The user's computer may be infected by drive-by download or the website may be modified to display a message asking users to indicate JavaScript code from a website controlled by a hacker. From there, they conduct phishing attacks on computers that have been poisoned to collect sensitive data.

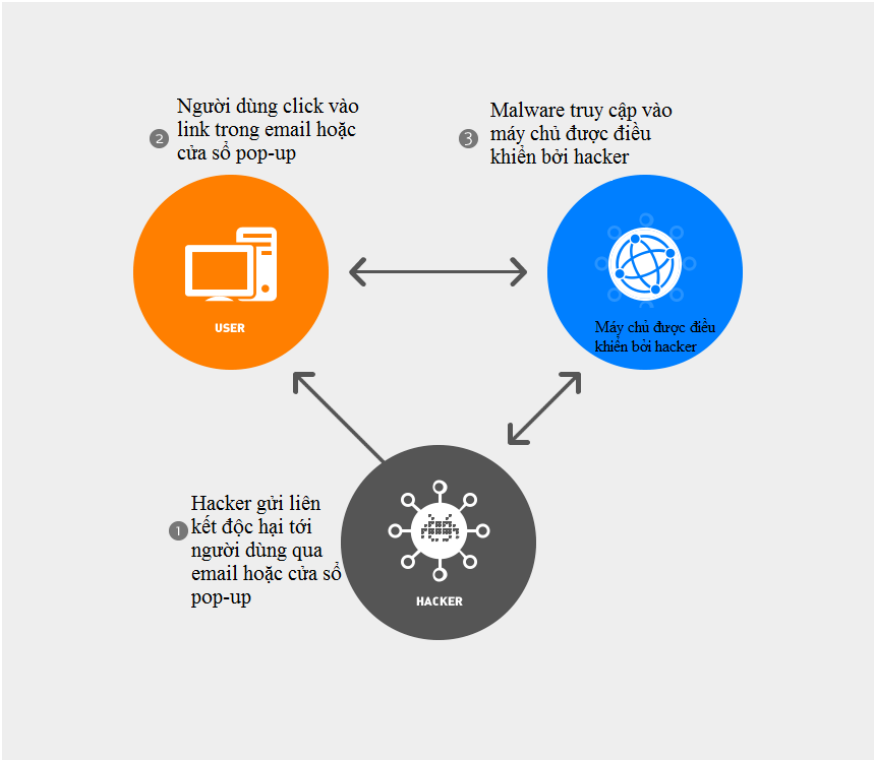
10. CryptoLocker

CryptoLocker will encrypt the user's data and display a message confirming that your personal information will be decrypted if the ransom amount is paid in a limited time. Although CryptoLocker can be removed by many security solutions, there is no way to decrypt files that have been locked.

CryptoLocker is one of the scariest malware ever created, not only because of its ability to steal money, but also because it can easily access private data and once encrypted information is It is impossible to decipher. This Ransomware is extremely dangerous because affected computers will be exposed to confidential (and compromised) information and users will also lose all files without any chance to recover. .

CryptoLocker is a trojan that can infect your system in many ways but usually through email attachments from well-known companies or organizations. This is also the main object that hackers aim to perform fake attacks.

Typical spread methods of malware



The chart shows the main mode of transmission of malware

Mostly, they will be distributed through the following paths:

1. Spam campaigns

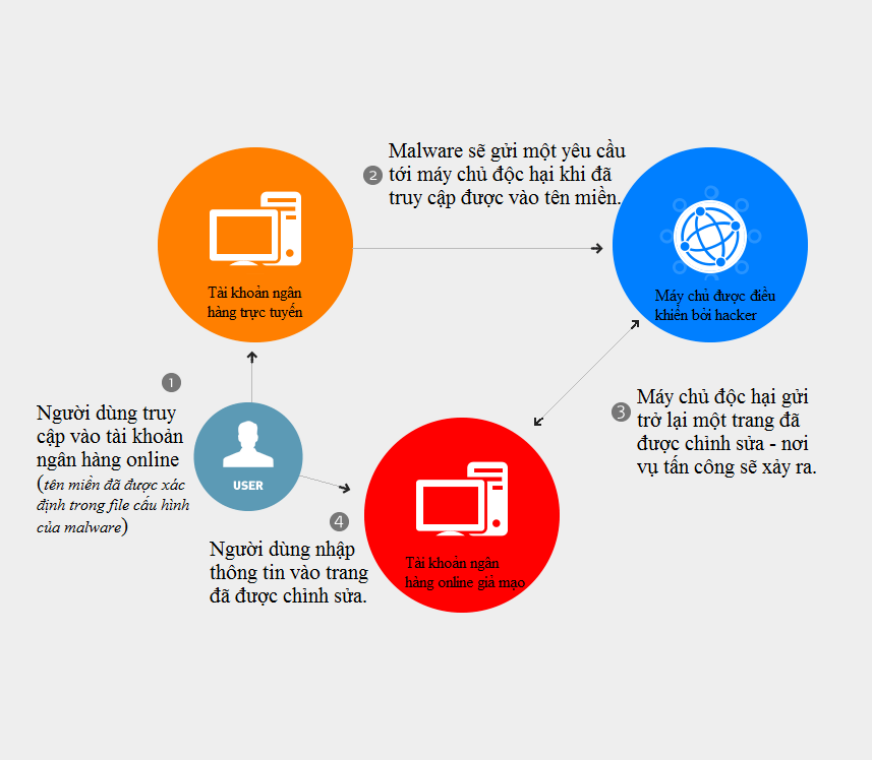
Users receive emails from a well-known organization with some false bank information or a fake link attached. The system will start poisoning when the user touches the link or downloads the attachments, usually disguised as an important bill or job announcement.

2. Drive-by download (automatic download)

The automatic download process will be done when a user visits a website or clicks on a **fake pop-up window.**

What would a common malware attack look like?

We will start from the point where a working computer is normally poisoned by a malware that steals data. As mentioned above, they will spread to user devices in one of three forms: email attachments (or links), automatic downloads or fake pop-ups.



The chart describes the attack process of malware

Stages occur during an attack:

1. Users access online banking accounts. Domain names will be determined on the configuration file downloaded by malware from malicious servers controlled by hackers.

2. The malicious code will send a request to the cybercriminal-controlled malicious server and inform that the user is trying to access a specific domain name in the configuration file.
3. Malicious server identifies the page that will attack - usually the login page.
4. When a user accesses that page, the malware sends a message to the malicious server asking to return a modified page to the user's browser.
5. The edited page will cause users to believe that they are entering information into a normal page on the account, but that is actually the page created by the hacker himself.

These are the most typical steps of a phishing attack. However, methods and tools will be changed from traditional intrusions to using a keylogger software to withdraw money directly from online bank accounts.