Detecting malicious code 'super dangerous'

Security researchers have discovered a very malicious type of malicious code that has infected and stole user information on millions of PCs.

Security researchers have discovered a very malicious type of malicious code that has infected and stole user information on millions of PCs .

'Shoot' 4,500 websites

Joe Stewart, director of SecureWorks 'malware research division, affirmed:' *Clampi is the most professional line of malware stealing I've ever seen. Very few lines of malicious code are highly complex and widely spread like this malicious code* . '

SecureWorks estimates that the number of PCs infected with Clampi ranges from 100,000 to over 1 million. This is the malicious code that attacks the Windows operating system. ' *We do not have any effective measures to accurately count the number of infected PCs* '.

Clampi's goal is for users of 4,500 websites to use various personal financial information such as banking, securities brokerage, credit cards, insurance, job search, e-commerce .

Stewart confirmed that 4,500 is a "really shocking" number. ' *There are a lot of malicious code stealing personal financial information that exists on the Internet, but usually they target only about 20 or 30 websites. Clampi targets 4,500 websites* '.

Source: ***Flickr*** Hackers infect Clampi to a user's PC by forcing them to open an email attachment or using multi-attack auto-attack tools that attack Windows operating system errors.

Once successfully infected with the PC, Clampi will closely monitor the browsing process of the people. If the user accesses one of the 4,500 websites mentioned above, Clampi will immediately record account information, username, PIN code and other personal information.

Clampi will transfer all the information it steals to a hacker server. These guys will then use that information to steal all the money in the user's account, use credit card information to buy goods or simply keep there when needed to use it. .

…toxic

Actually, if you only look at the above characteristics, Clampi is like most of the malicious code 'keylogger' or spyware (spyware), but not yet see the true malicious and dangerous nature of this malicious code. .

Stewart expert said Clampi differs from other malicious lines in operating scale and security encryption. This malicious code uses a multi-layer encryption solution and various tricks to hide the source code, making it impossible for security researchers to investigate in detail how it works.

' *Even the method of encapsulating the source code that the developers of Clampi use is very complicated, it is very difficult to reverse the reverse engineer for research* ,' said Stewart. ' *I can say that this is the most difficult to reverse code malicious code I have ever encountered* '.

Specifically, Mr. Stewart said Clampi developers have used source code tools that run on virtual machines. All information for packaging is taken from the microprocessor chip script on the virtual machine. Therefore, each time encapsulating the source code once, using different information. ' *We cannot use traditional reverse engine tools to work with Clampi* '.

Clampi encodes the entire flow of data traveling back and forth between the infected PC and the hacker's server.

This data stream is encoded in different layers. Specifically, the 448-bit encrypted network communication data stream. Not only that, every line of code that attacked Clampi was also encoded by independent methods.

To avoid detection by malicious software, Clampi hides active modules in carefully encrypted Windows Registry keys.

Operation scale

Clampi's scale is also different from the malicious code specializing in stealing financial information. ' *Clampi not only targets bank websites but also sites that users provide personal information that could be used to steal their money* ,' Stewart said.

Of the 4,500 websites mentioned above, there are military portals, online casinos, advertisements, news, credit collateral, etc. These websites are hosted on servers located in more than 70 countries. different.

Not only is the foundation behind the support of Clampi's operations very large. It cannot be confirmed with certainty, but the signs that seem to be behind those who snatched the Clampi controller somewhere in Russia or Eastern Europe.

' *It seems that there is only one group of hackers controlling Clampi* ,' said Stewart. ' *There are no any hackers forums about Clampi. Therefore, the information about this malicious code is not nearly as much. The group of hackers controlling Clampi also works very secretly* . '

Stewart has been monitoring Clampi since 2007 until now. Previously this line of malicious code was very quiet and it was not until the beginning of this year that it began to boom strongly.

Mr. Stewart said it was very difficult to find the last clue to summarize the gang of hackers who took control of the Clampi. One reason is simply that the server used by hackers to control Clampi is not under the control of any commercial service provider that hides itself among infected PCs.

' *Clampi is now spreading widely on Microsoft networks using technology and operating systems in a way similar to the computer worm. Apparently Clampi is far more dangerous than Conficker* '.