Endpoint Protection

symantec.com/connect/blogs/trojankoredos-comes-unwelcomed-surprise

Back to Library

Trojan.Koredos Comes with an Unwelcomed Surprise

1 Recommend

Mar 11, 2011 07:13 AM

Shunichi Imano

Recent Distributed Denial of Service (DDoS) attacks on a number South Korean websites have been in news for the past week. The threat responsible for carrying out these attacks is Trojan.Koredos.

This attack is reminiscent of another attack, launched on July 4th, 2009 against the U.S. and South Korean governments, as well as financial and media websites. For now, the attack has subsided and the affected sites can be accessed without any issues. However, the computers have not been cleaned for the Trojan.Koredos infection will be greeted with a surprise well after the initial infection, which we will detail in this blog.

Attacks such as this usually involve a command and control (C&C) server that sends commands to the compromised computers, resulting in systematic and coordinated attacks. In this case, the commands do not come from a C&C—they are hidden inside the threat.

There are many components involved in the attack, and that alone indicates some level of sophistication. Of those files, the destructive behavior is carried out by the s[RANDOM LETTERS]svc.dll file. While we have seen several variants of this .dll, the end result is the same—the master boot record (MBR) of the compromised computer is destroyed.

Some variants scan the fixed drives of compromised computers for files with various extensions, which are used by software predominantly used in Korea (i.e. .alz, .gul, and .hwp). This strongly suggests the threat targets computers located in Korea.
Figure 1 – Heatmap showing Trojan.Koredos infections.

Figure 2 – The threat searching for file extensions.

The threat overwrites the files with all zeros. Additionally, if the file size is larger than or equal to 10,485,760 bytes, the threat simply deletes the files. If a file does not meet the previous condition, the threat creates a .cab file using the original file name, and deletes the original file. In other cases deleted files can be restored using various methods, but since the threat overwrites the files with zeros, the original file cannot be restored.

The threat destroys the MBR of all drives if one of the following conditions is met:

- The %System%\noise03.dat file is missing. The noise3.dat file is a part of Trojan.Koredos that contains a number 7 within it. This is the number of days the destruction functionality gets triggered. One interesting part is that the number can be overwritten, though the threat can only distinguish up to 10. (Any number over 10 will be interpreted as 7.) This means the maximum life of the compromised computer is 10 days.

  Figure 3 – Creating the noise03.dat file with the date and time of infection and days to attack.

- A %System%\dnsec.dat file exists, and its first four bytes are all zero. The dnsec.dat file is also a component of W32.Koredos that works with other threat components.

  Figure 4 – Overwriting files with zeros and checking that the file size is greater than 10,485,760 bytes.

- The current date and time is later than 7 days, or equal to the number in %SYSTEM%\noise03.dat at the time of first infection.

- The current date and time is equal to or longer than 7 to 10 days after first infection. As explained previously, the number can manually overwritten in the %System%\noise03.dat file, but the operating system will be destroyed.

  Figure 5 – Checking that 7 to 10 days have passed.

In short, the infected computers can live up to 10 days if they are not cleaned. Symantec provides protection against the threat. Please make sure you keep virus definitions up-to-date to keep your valuable data safe from the destructive threat.

Thanks to Masaki Suenaga for his contributions to this blog.

Statistics

0 Favorited

0 Views

0 Files

0 Shares

0 Downloads

Tags and Keywords

Related Entries and Links

No Related Resource entered.