# Win32/Stuxnet Signed Binaries | WeLiveSecurity

*Pierre-Marc Bureau*

On July 17th, ESET identified a new malicious file related to the Win32/Stuxnet worm. This new driver is a significant discovery because the file was signed with a certificate from a company called "JMicron Technology Corp". This is different from the previous drivers which were signed with the certificate from Realtek Semiconductor Corp. It is

19 Jul 2010 - 01:50PM

On July 17th, ESET identified a new malicious file related to the Win32/Stuxnet worm. This new driver is a significant discovery because the file was signed with a certificate from a company called "JMicron Technology Corp". This is different from the previous drivers which were signed with the certificate from Realtek Semiconductor Corp. It is

On July 17th, ESET identified a new malicious file related to the Win32/Stuxnet worm. This new driver is a significant discovery because the file was signed with a certificate from a company called "JMicron Technology Corp". This is different from the previous drivers which were signed with the certificate from Realtek Semiconductor Corp. It is interesting to note that both companies whose code signing certificates were used have offices in Hsinchu Science Park, Taiwan.

The malicious file, named jmidebs.sys, has functions very similar to those originally noted in the system drivers used by Win32/Stuxnet. This driver is responsible for identifying and injecting code into processes running on an infected machine. The injected code seems to be responsible for stealing information. The compilation date for this latest binary is July 14th 2010, much more recent than the files previously seen, which dated from earlier this year.

This new information is important because it provides more information on the people behind Win32/Stuxnet. We rarely see such professional operations. They either stole the certificates from at least two companies or purchased them from someone who stole them.  At this point, it isn't clear whether the attackers are changing their certificate because the first one was exposed or if they are using different certificates in different attacks, but this shows that they have significant resources.

Pierre-Marc Bureau
Senior Researcher

Pierre-Marc Bureau 19 Jul 2010 - 01:50PM