Kaspersky Lab, Microsoft close new 'zero-day' vulnerability

MOSCOW, RUSSIA: Kaspersky Lab has announced that it has co-operated with Microsoft in successfully closing a serious vulnerability in Microsoft Windows.

The vulnerability was classified as being of the 'zero-day' type when it was detected, and has been used b the notorious Stuxnet worm. Worm.Win32.Stuxnet is remarkable in that it is basically an industrial espionag tool - it is designed to gain access to the Siemens WinCC operating system which is responsible for data collection and monitoring production.

Ever since it first emerged in July 2010, IT security specialists have watched Worm.Win32.Stuxnet closel Kaspersky Lab's experts have gone to great lengths to research Stuxnet's capabilities and have discovere that, in addition to the vulnerability when processing LNK and PIF files that was detected originally, it also uses four other vulnerabilities in Windows.

One such example is MS08-067, which was also used by the infamous Kido (Conficker) worm in early 20(The other three vulnerabilities were previously unknown and exist in the current versions of Windows.

Malicious code

Along with MS08-067, Stuxnet also uses another vulnerability to propagate. This exists in the Windows Pri Spooler service and can be used to send malicious code to a remote computer where it is then executed. By virtue of the features of this vulnerability, the infection can spread to computers using a printer or throug shared access to one. Having infected a computer connected to a network, Stuxnet then attempts to spre to other computers.

As soon as Kaspersky Lab's experts detected this vulnerability, they reported it to Microsoft. Microsoft the analysed it themselves and agreed with Kaspersky Lab's findings. The vulnerability was classified as a Pri Spooler Service Impersonation Vulnerability and was rated as 'critical'. Microsoft immediately started working to close the loophole and subsequently released the MS10-061 patch on 14 September 2010.

Kaspersky Lab's experts detected yet another 'zero-day' vulnerability in the Stuxnet code. It was classified as an 'Elevation of Privilege' (EoP) vulnerability which could be exploited by the worm to gain full control o the infected computer. A similar EoP-class vulnerability was detected by Microsoft's experts. Both will be

corrected in future security updates for Windows operating systems.

Stuxnet uses multiple vulnerabilities

Alexander Gostev, chief security expert at Kaspersky Lab, played an active role in identifying the new threa and co-operated closely with Microsoft to resolve the issue. Alexander later published an informative blog post on the topic.

The full version of the blog post is available at www.securelist.com/en/blog/2291/Myrtus_and_Guava_Episode_MS10_061.

The data collected while analysing Stuxnet, including the details of how the vulnerabilities can be exploited will be presented at the Virus Bulletin conference in Canada in September 2010.

"Stuxnet was the first malware program to simultaneously exploit as many as four vulnerabilities," said Alexander Gostev. "This makes Stuxnet truly unique: it is the first threat we have encountered that contains this many surprises in a single package. Before we detected this new vulnerability, it would have been wor a fortune to hackers. Given Stuxnet also uses Realtek and Jmicron digital certificates - and remember too that it was ultimately designed to steal the data stored in Simatic WinCC SCADA - all of this makes this threat truly unprecedented. It has to be said, the malware writers have demonstrated quite remarkable programming skills."

All Kaspersky Lab's products are capable of successfully detecting and neutralizing Worm.Win32.Stuxnet

For more information go to www.kaspersky.com. For the latest on antivirus, anti-spyware, anti-spam and other IT security issues and trends, go to www.viruslist.com.