Experts Warn of New Windows Shortcut Flaw — Krebs on Security

Researchers have discovered a sophisticated new strain of malicious software that piggybacks on USB storage devices and leverages what appears to be a previously unknown security vulnerability in the way **Microsoft Windows** processes shortcut files.

Update, July 16, 7:49 p.m. ET: Microsoft just released an advisory about this flaw, available here. Microsoft said it stems from a vulnerability in the "Windows shell" (Windows Explorer, e.g.) that is present in every supported version of Windows. The advisory includes steps that can mitigate the threat from this flaw.

Original post:

VirusBlokAda, an anti-virus company based in Belarus, said that on June 17 its specialists found two new malware samples that were capable of infecting a fully-patched **Windows 7** system if a user were to view the contents of an infected USB drive with a common file manager such as Windows Explorer.

USB-borne malware is extremely common, and most malware that propagates via USB and other removable drives traditionally has taken advantage of the Windows Autorun or Autoplay feature. But according to VirusBlokAda, this strain of malware leverages a vulnerability in the method Windows uses for handling shortcut files.

Shortcut files — or those ending in the ".lnk" extension — are Windows files that link (hence the "lnk" extension) easy-to-recognize icons to specific executable programs, and are typically placed on the user's Desktop or Start Menu. Ideally, a shortcut doesn't do anything until a user clicks on its icon. But VirusBlokAda found that these malicious shortcut files are capable of executing automatically if they are written to a USB drive that is later accessed by Windows Explorer.

"So you just have to open infected USB storage device using [Windows] Explorer or any other file manager which can display icons (for i.e. Total Commander) to infect your Operating System and allow execution of the malware," wrote **Sergey Ulasen**, an anti-virus expert with the company, in an advisory published this month.

Ulasen said the malware installs two drivers: "mrxnet.sys" and "mrxcls.sys." These so-called "rootkit" files are used to hide the malware itself so that it remains invisible on the USB storage device. Interestingly, Ulasen notes that both driver files are signed with the digital signature of Realtek Semiconductor Corp., a legitimate hi-tech company.

Ulasen said he reached out to Microsoft and to Realtek but got a response from neither. **Jerry Bryant**, group manager of response communications at Microsoft, told KrebsOnSecurity.com Wednesday that "Microsoft is investigating new public claims of malware propagating via USB storage devices. When we have completed our investigations we will take appropriate action to protect users and the Internet ecosystem."

If this truly is a new vulnerability in Windows, it could soon become a popular method for spreading malware. But for now, this threat seems fairly targeted: Independent security researcher Frank Boldewin said he had an opportunity to dissect the malware samples, and observed that they appeared to be looking for Siemens WinCC SCADA systems, or machines responsible for controlling the operations of large, distributed systems, such as manufacturing and power plants.

"Looks like this malware was made for espionage," Boldewin said.

Tags: .lnk extension, espionage, Frank Boldewin, Jerry Bryant, microsoft, mrxcls.sys, mrxnet.sys, Realtek Semiconductor Corp., sergey ulasen, Siemens WinCC Scada, Stuxnet, VirusBlokada, windows shortcut flaw

This entry was posted on Thursday, July 15th, 2010 at 1:24 am and is filed under A Little Sunshine, Latest Warnings. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.