MUST READ: Amazon announces everything Alexa but the kitchen sink

Stuxnet attackers used 4 Windows zero-day exploits

The attackers behind the recent Stuxnet worm attack used four different zero-day security vulnerabilities to burrow into -- and spread around -- Microsoft's Windows operating system.

By Ryan Naraine for Zero Day | September 14, 2010 -- 11:18 GMT (21:18 AEST) | Topic: Windows

(http://blogs.zdnet.com/security/?p=7347)

(http://blogs.zdnet.com/secu
p=7347)

The attackers behind the recent Stuxnet worm attack (https://www.zdnet.com/blog/security/ms-ships-temporary-fix-it-for-windows-shortcut-zero-day-attacks/6916) used four different zero-day security vulnerabilities to burrow into -- and spread around -- Microsoft's Windows operating system, according to a startling disclosure from the world's largest software maker.

Two of the four vulnerabilities are still unpatched.

As new details emerge to shine a brighter light on the Stuxnet attack, Microsoft said the attackers initially targeted the old MS08-067 vulnerability (used in the Conficker attack), a new LNK (Windows Shortcut) flaw to launch exploit code on vulnerable Windows systems and a zero-day bug in the Print Spooler Service that makes it possible for malicious code to be passed to, and then executed on, a remote machine.

(http://twitter.com/ryanaraine)

(http://twitter.com/ryanaraine)

The malware also exploited two different elevation of privilege holes to gain complete control over the affected system. These two flaws are still unpatched.

Kaspersky Lab (disclosure: my employer (https://www.zdnet.com/blog/security/page/disclosure/324)) discovered two of the three new zero-days and worked closely with Microsoft during the research and patch-creation process.

AS ATTACKS ESCALATE, MICROSOFT SHIPS EMERGENCY WINDOWS PATCH (HTTPS://WWW.ZDNET.COM/BLOG/SECURITY/AS-ATTACKS-ESCALATE-MICROSOFT-SHIPS-EMERGENCY-WINDOWS-PATCH/7027)

As part of today's Patch Tuesday releases, Microsoft shipped MS10-061 with a fix for the Print Spooler Service Impersonation flaw. This update is rated "critical" for all supported versions of Windows.
The LNK vulnerability was patched with an emergency fix (https://www.zdnet.com/blog/security/as-attacks-escalate-microsoft-ships-emergency-windows-patch/7027) in August 2010.

Patches for the two elevation-of-privilege flaws are still outstanding.

According to Kaspersky Lab's Alexander Gostev, the Stuxnet attack (http://www.securelist.com/en/blog/2291/Myrtus_and_Guava_Episode_MS10_061) was one of a kind.

"The fact that Stuxnet targets not four previously unidentified vulnerabilities makes the worm a real standout among malware," Gostev said.

"It's the first time we've come across a threat that contains so many 'surprises'," Gostev added, noting that the worm also used signed digital certificates stolen from RealTek and JMicron and also exploited security problems in the Simatic WinCC SCADA systems.

"Stuxnet was undoubtedly created by professionals who've got a thorough grasp of antivirus technologies and their weaknesses, as well as information about as yet unknown vulnerabilities and the architecture and hardware of WinCC and PSC7," Gostev added.

There have been rumblings that Stuxnet may be linked to nation-state (http://threatpost.com/en_us/blogs/stuxnet-attack-shows-signs-nation-state-involvement-experts-say-080410) cyber-attacks.

RELATED TOPICS: ENTERPRISE SOFTWARE | MICROSOFT | WINDOWS 10 | PCS | REVIEWS

LOG IN TO COMMENT | Community Guidelines

Join Discussion