Cyber criminals ready to pry open Windows 8

Fake search results, phishing e-mails spreading on Microsoft's new operating system

K. V. Kurmanath

Hyderabad, Nov. 6

Even as Microsoft is rolling out its new Operating System Windows 8, cyber criminals are ready with malware and spam to cash in on the huge interest in the OS.

Internet security solutions firms have already noticed suspicious activity.

Amit Nath, Country Manager - India and SAARC of Trend Micro, has said it is typical for cyber criminals to piggyback on the highly-anticipated release of any latest technology to take their malware, spam and malicious apps to new heights. "They have leveraged Windows 8 as well. Fake scanning results and phishing e-mails have emerged to question the security of Windows 8," he said.

Govind Rammurthy, Managing Director and Chief Executive Officer of eScan, draws our attention to a tweet posted by VUPEN, a French organisation which specialises in finding vulnerabilities. "Our first day for Win8+IE10 with HiASLR/AntiROP/DEP & Prot 'Mode sandbox bypass (Flash not needed) is ready for customers. Welcome #Windows8".

"For many this is a meaningless tweet. But for security organisations this is a warning bell. It is an indicator that there exists a bug in IE10," he pointed out.

Also, 'Flash' has now been integrated with IE 10 in Windows 8, which is in line with Google's integration of Flash Player with Chrome. Due to this, the onus is on Microsoft to issue a patch, and not on Adobe.

"We were alerted to two threats that leverage the release of this new OS. The first one is a typical FAKEAV. Detected as TROJ_FAKEAV.EHM, this malware may be encountered when users visit malicious sites," he said.

The malware displays a fake scanning result to intimidate users to purchase the fake anti-virus program – just like your run-of-the-mill FAKEAV variant.

The other threat is a phishing e-mail that entices users to visit a Web site where they can download Windows 8 for free.

Sanket Akerkar, Managing Director, Microsoft Corporation, has said that it (finding vulnerabilities and plugging them) is an ongoing and continuous process. "If you take your eyes off the ball, someone attacks it," he said.

kurmanath.kanchi @thehindu.co.in