Can a Rootkit Be Certified for Vista?

March 16 2007

A roomful of hackers, CIOs and CSOs agree that Microsoft's given us the most secure version of Windows yet, but their approval is served up with a garnish of "excepts," "howevers" and "althoughs."

Forget what Microsoft says about Vista being the most secure version of Windows yet. More to the point, what do the hackers think of it?

In a nutshell, they think it's an improvement, but at the end of the day, it's just like everything else they dissect - that is, breakable.

"Not all bugs are being detected by Vista," pointed out famed hacker H.D. Moore. "Look at how a hacker gets access to the driver: Right now I'm working on Microsoft's automated process to get Metasploit-certified. It - only - costs $500."

Moore is the founder of the Metasploit Project and a core developer of the Metasploit Framework - the leading open-source exploit development platform - and is also director of security research at BreakingPoint Systems. The irony of his statement lies in the idea that Vista trusts Microsoft-certified programs - programs that can include a hacker exploit platform that walks through the front door for a mere $500 and a conveyor-belt approval process.

Moore was one of a handful of white-hat hackers in the audience of a session on Vista security here at Ziff Davis Enterprise's 2007 Security Summit on March 14. The session, titled "Vista: How Secure Are We?," was presented by David Tan, co-founder and chief technology officer at CHIPS Computer Consulting.

By Moore's side were equally prestigious hackers Joanna Rutkowska - security researcher at COSEINC - and Jon "Johnny Cache" Ellch, author of "Hacking Exposed Wireless."

For her part, Rutkowska granted that yes, one way to own a Vista system is by getting a rootkit certified, but if you want a compromised system, you don't even have to waste your time and money with certification - "It can be a graphics card with a stupid bug," she said. "You can't do anything about it. You can't sue the vendor for introducing a bug. You can't prove it was done intentionally."

Until Microsoft or some security vendor concocts a black list for buggy drivers, Rutkowska said, Vista is potential toast. Of course, bugs can always be detected in memory, right? Except - oops! - Rutkowska demonstrated a few weeks ago at Black Hat that exploits can in fact tinker with memory to hide their footprints.

But before the hackers, and Tan himself, pointed out Vista's security weak points, Tan outlined the improvements to the new operating

system's security features. He praised Microsoft's Trustworthy Computing initiative and the company's reshaped development cycle for the "phenomenal effort" that has produced products such as SQL Server 2005 - a version of the database that to date hasn't had a single major vulnerability or exploit attached to it. "Microsoft deserves to be applauded for that," he said.

In keeping with that improved attention to security, Microsoft has added a slew of security features to Vista in the two areas you need to worry about in a client operating system, Tan said: namely, protecting the system and protecting data.

Those features include UAC (User Access Control), a feature that forces users to work in restricted accounts instead of with the rights of system administrators that they had traditionally been granted in previous Windows versions. UAC is active by default for all users - although it can be turned off - and even administrator accounts only get medium-integrity level rights in Vista.

UAC has been criticized on the basis of the debatable annoyance level pertaining to its warning boxes, which pop up in colors (orangey-red for caution, bluish-green for safe) and ask users if they really want to proceed with given actions. Rutkowska kicked off the criticism of UAC when she wrote in her blog that, although UAC is "the most important security mechanism introduced in Vista," it "can be bypassed in many ways."

Rutkowska's observations were soon followed by Symantec research scientist Ollie Whitehouse's Feb. 20 posting titled "An Example of Why UAC Prompts in Vista Can't Always Be Trusted," due to the ease in which social engineering can be used to trick users into approving illicit user privilege escalation.

During his presentation, Tan voiced concern that frequent UAC consent dialog boxes will blend together to create a "click here to get work done" attitude. "Frequent UAC consent dialog boxes - will this force users to turn off the function?" he said. "Users will eventually get annoyed with it if it impacts their normal day-to-day activity."

However, Rutkowska said she was bewildered at the frequent arguments that the boxes are annoying. "I've been using Vista two months now," she said, and within a few days of installation, she's rarely presented with a UAC dialog box. "I think UAC, from a technical point of view, is a very good thing," she said. "For normal users, this is - a good security mechanism."

One thing Rutkowska said she doesn't like, however, is Microsoft's attitude. After the UAC criticisms started making the rounds, Microsoft began to stress that UAC is not a hard security boundary, like a firewall - rather, it's more of a guidance tool.

Unfortunately, that attitude means that Microsoft won't consider potential avenues of attack to be bugs, Rutkowska pointed out. " - Illicitly - elevating from low- to high-level - user privileges - won't be considered a security bug," she said - when in fact such escalation is a good indication that a machine has been compromised.

Another feature that protects the system in Vista is Windows Defender, included previously as a separate Windows download. Defender detects and removes any unwanted application, actively monitoring protected areas. The feature is integrated with group policy and thus works with Active Directory.

Another system-protecting feature is Vista's new Windows Firewall, which expands on the firewall included in Windows XP SP2 but improves on it by offering two-way protection. The earlier version didn't

offer outbound infection - an omission that meant an infected machine wouldn't be stopped from spreading a virus outside of the network.

The final system protection feature added to Vista is Windows Security Center, which checks and displays the status of the Firewall, automatic updates, malware protection (Windows Defender) and other security settings, including third-party security software such as anti-virus programs.

Tan also criticized Vista's recognition of installation programs, which checks compatibility databases, heuristics and a program's embedded manifest - which declares to an operating system what it is. The potential dangers of Vista's handling of installers, Tan said, is that all installers run with administrative privileges, have full access to the file system and registry, and have the ability to load kernel drivers.

"As soon as you click OK, that application has complete administrative capabilities, including downloading and installing rootkits," he said.

Tan also criticized Internet Explorer 7 for its lack of Protected Mode in the version that runs on Vista. Protected Mode makes the browser run in a sandbox - i.e., it has limited read access to system components and can't download Trojans or spyware from malicious sites.

That accounts for new system protection in Vista. As for data protection, the new operating system comes with BitLocker Drive Encryption - a feature that encrypts the entire Windows volume, protecting against data being stolen when a laptop is stolen or lost. Tan's only criticism of that feature was that it's available in only the Enterprise and Ultimate versions of Vista and is lacking in the Business version.

Other data protection features in Vista include EFS (Encrypting File System), used to encrypt files and folders; Rights Management Services,

used to encrypt files persistently so they can't be e-mailed outside of the organization without proper server permissions; and Device Control, which enables better management of plug-and-play devices such as USB drives.

Tan also touched on PatchGuard, which locks down the kernel completely but also locks out some third-party applications, including anti-virus programs. Besides the ire that this drew from security software vendors, PatchGuard was actually cracked soon after Vista's introduction.

Other flawed security solutions in Vista include Windows Defender's lackluster performance, blocking a mere 47 percent of spyware in quick-scan mode in anti-virus testing. OneCare also fell "well short" in Virus Bulletin's VB100 test and flunk AV-Comparative's test altogether.

"So Microsoft definitely still has some work to do in those areas," Tan said. Besides all that, a critical remote code execution bug in Vista's vector markup language was released on Jan. 9; in testing of Vista's strength against legacy exploits, Vista was found to have exploits that would survive exploits in every category except rootkits; key enhancements to Vista security are only available on 64-bit platforms; and you need new hardware platforms to fully support Vista, Tan said.

Cumulatively, it sounds bad, Tan said, but hackers and Tan agreed: significant strides have been made in securing Vista. "It's a security evolution, not a revolution," Tan said. "Vista is not a security solution - it is a more a secure version of Windows."