- Members Log In
- Site Assistance
- Newsletters
- RSS Feeds

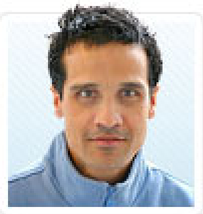
- Home
- News
- Blogs
- White Papers
- Downloads
- Reviews

- Podcasts
- Between the Lines
- Berlind's Testbed
- All About Microsoft
- Enterprise Web 2.0
- Chipland
- Zero Day
- RSS Feeds

home / blogs
Zero Day

search
Search Go!

Ryan Naraine



Tracking the hackers

- Subscribe
- Alerts
- Bio

Pick a blog category view

April 23rd, 2007

Russinovich: Malware will thrive, even with Vista’s UAC

Posted by Ryan Naraine @ 12:24 pm Categories: Patch Watch, Hackers, Zero-day attacks, Microsoft, Windows Vista, Browsers, Rootkits, Vulnerability research, Responsible disclosure, Spam and Phishing, Botnets, Exploit

ADD YOUR OPINION

+8

30 votes **Worthwhile?**

Despite all the anti-malware roadblocks built into Windows Vista, a senior Microsoft official is lowering the security expectations, warning that viruses, password-stealing Trojans and rootkits will continue to thrive as malware authors adapt to the new operating system.

Mark Russinovich (right), technical fellow in Microsoft's Platform and Services Division, used the spotlight of the CanSecWest security conference in Vancouver to discuss the implementation of UAC (User Account Control) in Windows Vista and made it clear that the feature is not meant to be a security barrier.

"It's a best effort to raise the bar and stop malware from making changes to the operating system but it's not a security boundary," Russinovich said of UAC, the oft-criticized mechanism that requires that all users run without full admin rights.

In a straightforward assessment of the threat landscape in a Vista world, Russinovich described malware authors as ISVs that will code for a standard user environment.

"There is no guarantee that malware can't hijack the elevation process or compromise an elevated application," Russinovich said after providing a blow-by-blow description of how UAC works in tandem with Internet Explorer (with Protected Mode) to limit the damage from malicious files.

Even in a standard user world, he stressed that malware can still read all the user's data; can still hide with user-mode rootkits; and can still control which applications (anti-virus scanners) the user can access.

"We'll see malware developing its own elevation techniques," Russinovich said. He demonstrated a social engineering attack scenario where a fake elevation prompt can be used to trick users into clicking "allow" to give elevated rights to a malicious file.

He predicted a world where malware authors create programs that elevate rights to jump accounts and disable security or develop general and application-specific elevation hijacking.

"You will see malware spoofing over-the-shoulder credential prompt and even launching a medium integrity level process int he administrator's account," Russinovich said.

At this level, the malware author has access to all the administrators data and can inject itself into the admin's account (e.g. the Runkey) to use additional elevation techniques.

"The malware author will say, 'I can live in a Vista world without needing to take over the entire box'. They will end up thriving in the standard user environment, setting up botnets, grabbing your keystrokes," he declared.

Russinovich stressed that UAC's fundamental contribution is to make it possible (in most cases) to run as standard user to protect the system and other users on the system.

"Elevations are a convenience and not a security boundary," Russinovich reiterated, hinting that Windows will evolve further to promote the standard user concept with things like per-user installations and secure elevations.

> stating that malware will evolve to run as standard user, where it can accomplish many of its goals, not that Vista somehow enables malware — in fact, ASLR, service security hardening, Defender, SDL, and other security enhancements raise the security bar in Vista.

- Blog This
- E-mail
- Print
- Sphere
-

* Ryan Naraine is a freelance writer specializing in Internet and computer security issues. He can be reached at *naraine SHIFT 2 gmail.com*
Previous postNext post

Talkback - Add your opinion

Permissions aren't an O/S issue, it's a people issue

Why in the world would you think that Vista doesn't have the same general type of permissions?
... *(Read the rest)*

- Malware will always exist voska -- 04/23/07
- Another article on Vista UAC ju1ce -- 04/23/07
- Well, it really is Microsoft's fault John Zern -- 04/23/07
- Jesus... who did the airbrushing on Russinovich's photo? (nt) John E Wahd -- 04/23/07
- Of course it'll thrive. Human nature transcends any operating system. HypnoToad72 -- 04/23/07
- Microsoft is backpedaling on Vista security!! 😮 TechExec2 -- 04/23/07
- Microsoft is backpedaling on Vista security!! 😮 (fixed) TechExec2 -- 04/23/07
- Thrive? p_user_001 -- 04/23/07
- A possible attackers way could be... ischilling -- 04/24/07
- Softening the blow frgough -- 04/24/07
- I like this guy Resuna -- 04/24/07
- MICROSOFT SHOULD SEEK GOVERNMENT HELP BALTHOR -- 04/24/07
- It was a noble effort jajanes -- 04/25/07
- hardware, hardware, hardware gdstark13 -- 04/25/07
- More code, more bugs, more holes tygrus -- 04/25/07
- MS Employee's admit Vista failure spacecase -- 04/26/07
- Talk about misinformation! CobraA1 -- 04/29/07
- Add your opinion

One Trackback

The URI to TrackBack this entry is:
http://blogs.zdnet.com/security/wp-trackback.php?p=175

- **Russinovich: Malware will thrive, even with Vista's UAC**
  Russinovich: Malware will thrive, even with Vista's UAC by ZDNet's Ryan Naraine — Despite all the anti-malware roadblocks built into Windows Vista, a senior Microsoft official is lowering the security expectations, warning that viruses, ...

- VoIP Migration Strategies *ShoreTel*
- Best Practices for Migrating to Exchange 2007 *Quest Software*
- AMR Research Alert: Rethinking Core Competencies *IBM*
- ShoreTel Pumps Up Efficiency at Houston Heart Center with Reliable, Easy-To-Use VoIP Solution *ShoreTel*
- Automating Network Management: Leveraging Dynamic Reconfiguration for Utility Computing *Cassatt*
- Footwear Company, Dr. Martens, 'Steps Up' with ShoreTel *ShoreTel*