

March 31, 2010 Hot topics : desktop security network security Trojans malware wpa sec i

Free Newsletters : Security Daily

eSecurityPlanet.com Features All Features»

Service providers can build the foundation for the next-generation Internet. See what's possible with the Cisco CRS-3, delivering 3x the scale and 2x the service intelligence.

Microsoft: IE's Defense in Depth Not Fool-Proof

March 30, 2010

By Stuart J.

Johnston

[Submit Feedback](#)

»

[More by Author »](#)

Less than a week after a [white hat hacker](#) took mere minutes to take over Internet Explorer 8 running on Windows 7, Microsoft has responded that its "defense in depth" strategy isn't meant to altogether stop such attacks, but rather to delay them.

But a hacker presenting at the [CanSecWest conference in Vancouver](#), wasn't delayed much at all as he quickly defeated Microsoft's defense in depth measures for Windows 7 running IE8. (To be fair, hackers also quickly defeated security in Firefox and Safari.)

One of the two Microsoft "defense in depth" features that the exploit took advantage of is what's called, "[Data Execution Prevention](#)" or, "DEP." Its aim is to keep code that has been loaded into non-executable memory locations from being allowed to execute.

The hacker also claimed to use a second security protection feature as part of the successful takeover -- known in the hacker community as [Pwn2own](#). However, due to the rules of the contest, he couldn't reveal the entire exploit.

Friday, in a post to the [Windows Security blog](#), IE team spokesperson Pete LePage, tried to put the events into focus.

"Protecting Windows customers is an absolute priority for the Internet Explorer engineering team," LePage said in his post.

Besides DEP, LePage also cited other defense in depth measures included in Windows 7 and IE8, including [Address Space Layout Randomization \(ASLR\)](#), meant to randomly locate key pieces of code so that an attacker can't easily figure out how and where to attack, particularly with buffer overflow exploits. Another measure he mentioned is Protected Mode, a feature in Windows 7 and Windows Vista that runs IE in a reduced privileges mode.

LePage, however, said that nothing is a panacea and that one of the purposes of [defense in depth](#) is to slow the bad guys down, if not stop them dead in their tracks.

Related Articles

- ▶ [Apple Patches 88 Security Vulnerabilities](#)
- ▶ [IE8, Firefox, Safari, and](#)

"One way to think about what defense in depth techniques do is similar to the features offered by fire-proof safes that make them last longer in a fire. Without defense in depth techniques, a fire-proof safe may only protect its contents for an hour or two. A stronger fire-proof safe with several defense in depth features still won't guarantee the

- @ [Email Article](#)
- [Print Article](#)
- [Comment on this article](#)
- [Share Articles](#) ▼

POWER7 Systems™ from IBM are designed to:

- Minimize complexity
- Improve efficiency across workloads
- Automate processes

Power your planet >

Smarter systems for a Smarter Planet

Learn Forefront

[Create a Seamless Remote Experience with Forefront UAG](#)
Remote access solutions are often built on products from numerous vendors, creating a headache for IT managers trying to support secure network access for employees and partners. Microsoft has a solution that can help.

[Modernize your Web Security](#)
Here are some of the key reasons to switch from your existing solution(s) to Forefront Threat Management Gateway 2010.

[More Secure Web Access and Protection with Forefront TMG](#)
Forefront Product Unit Manager David Cross talks about the new Threat Management Gateway 2010 release.

[Click Here for more Forefront Resources](#)

[iPhone Fall to Pwn2own Hackers](#)

valuables forever, but adds significant time and protection to how long the contents will last," LePage's post said.

▶ [Want PC Security? Remove Admin Rights](#)

LePage continued with the fire-proof safe analogy. "Defense in depth techniques aren't designed to prevent every attack forever, but to instead make it significantly harder to exploit a vulnerability."

▶ [Security Is the Top Priority for CEOs: Survey](#)

Perhaps a little ironically, he cited both DEP and ASLR as key components of that strategy, while admitting that both have been used to break into systems running Windows and IE.

Administrator rights enable risk?

Meanwhile, a [report](#) compiled by privileged access lifecycle management vendor [BeyondTrust](#) and released Monday, found that a majority of Microsoft security vulnerabilities can be mitigated, if not totally blocked, by [removing administrators' rights](#) from most users desktops.

All-in-all, however, at least one analyst feels that demonstrations are useful, but don't change the facts on the ground.

"The reality is there is no perfect security...but even if you've got something that will keep them out, a determined individual will still get through," Rob Enderle, principal analyst at [the Enderle Group](#), told [InternetNews.com](#).

"However, if you make something that's really secure [the bad guys] will go elsewhere," Enderle added.

A recent IBM-funded survey by Traverse City, Mich. security researcher, [Poneman Institute queried 115 C-level executives in the U.K.](#) Its findings were not heartening for those who might think their systems are secure. All of the respondents said they had experienced [attacks on their data](#) in the past year.

Stuart J. Johnston is a contributing writer at [InternetNews.com](#), the news service of [Internet.com](#), the network for technology professionals.

Tags : [Microsoft](#), [security](#), [hackers](#), [PWN2OWN](#), [white hat](#)

1

Free Trial and Beta Versions of Forefront

Sponsored by Microsoft



Forefront helps businesses protect against viruses, worms, spam, and inappropriate content. Click here to download free trial and beta versions of Microsoft Forefront products today.

0 Comments ([click to add your comment](#))



Comment and Contribute

Your name/nickname

Microsoft Because it's everybody's business

Related Resource:
Check out the new features of SharePoint 2010. Download the fact sheet.

On the Forums

[Visit the Forums](#) »

Latest

Most Views

Most Replies

How to design ITIL-CMDB schema
Today 12:02 PM by thirumaran

IT On Call Allowances
3-29-2010 06:12 PM by stevenmahoney

Cloud Computing
3-29-2010 01:11 PM by sb1

Partners

Business Email
Desktop Computers
Colocation
Premium Bandwidth
IT Legal Contracts
Liability Insurance
IP Services
Website Hosting
Car Donations
Dedicated Servers
Phone Cards
PDA Phones & Cases
Boat Donations
prepaid calling card

More IT Management

CIO Update
Datamation
eSecurity Planet
ITSMWatch
Intranet Journal
IT Career Planet
Project Manager Planet
Security Definitions

Resources

MARKETPLACE

[Microsoft SQL Server® Value Calculator](#)

Reduce Costs & Increase Value with Microsoft SQL Server® 2008. Download Today!

[Microsoft.com/EverybodysBusiness](#)

[Microsoft Business Resource Center](#)

Get access to FREE personalized help to get more from your Microsoft software.

[Microsoft.com/Business](#)

[Windows Server® 2008 Hyper-V - Download](#)

Lower Costs, Improve IT Service, Deliver Value & More. Read about the Benefits.

[Microsoft.com/EverybodysBusiness](#)

[Free Guide to IT Asset Management](#)

Free 10 page Buyer's Guide for IT. A Must Read for IT Before You Buy.

[KACE.com/IT-Guide](#)

[Advertise Here](#)