

Welcome Guest. [Log In](#) [Register](#) [Benefits](#)

InformationWeek

THE BUSINESS VALUE OF TECHNOLOGY

Search



[Home](#) [News](#) [Blogs](#) [Video](#) [Slideshows](#)

[Software](#) [Security](#) [Hardware](#) [Mobility](#) [Windows](#) [Internet](#) [Global CIO](#) [Government](#) [Healthcare](#) [Finance](#)

[Application Security](#)

[Attacks/Breaches](#)

[Encryption](#)

[End User/Client Security](#)

[Perimeter Security](#)

[Privacy](#)

[Security Administration/Management](#)

[Security Blog](#)

[Security Reviews](#)

[St...](#)

[St...](#)

[Vi...](#)



Servers from Penguin Computing feature the Intel® Xeon® processor.

Relion 750 • One or Two Intel® Xeon® 5600 Series Quad- or Six- Core Processors

- QuickPath Interconnect, • Optimized for Low Power and Efficient Cooling
- Up to 6.4 GT/s I/O Link • Up to 64GB of DDR3 RAM



Buy now

[Tweet](#) 23

Like 323

[Share](#)

[Permalink](#)



LizaMoon SQL Injection Attack Hits Websites

The scareware sends users to a bogus Web page warning them that their PCs are infected with malware and tries to sell them an anti-virus application.

By [Antone Gonsalves](#) InformationWeek

April 1, 2011 04:12 PM

Hundreds of thousands of website URLs have been compromised in a massive malware attack that tries to trick people into buying fake anti-virus software to remove bogus infections, security experts said.

Dubbed LizaMoon, unidentified perpetrators of the scareware campaign inject script into legitimate URLs, so when people try to access the website, they get redirected to a page warning them that their PCs are infected with malware that can be removed by downloading a free AV application called Windows Stability Center. The software eventually will find bogus threats that will require victims to buy a more robust product, using their credit cards.



(click image for larger view)

Slideshow: 10 Massive Security Breaches

More Security Insights

White Papers

- [Messaging and Web Security Best Practices for 2011 and Beyond](#)
- [Security Threat Report: Mid-Term Report: Attack Toolkits and](#)

Security firm Websense says a Google search shows more than 1.5 million URLs with the nasty script. Because Google counts unique URLs and not domains or websites, the number is likely inflated. "It's safe to say it's in the hundreds of thousands," Websense said Thursday in a [blog post](#). The attack is worldwide, with U.S. PC users making up roughly half those getting redirected to the bogus warning page.

CTO Edge
"Most In
Enterpris
Product
is the B
VDX 672
Center S

LEARN MORE

THIS WEEK



[Back Issues](#)

Malicious Websites

Reports

- [Breach Diaries](#)
- [Virtual Servers, Real Risks](#)

Videos



CEO Phillip Dunkelberger explains how his company has built an eco system that highlights disk encryption, file transfers to mainframe, and encryption management.

the same page.

Websense said the first domain may have been infected with the LizaMoon script as early as Oct. 21, 2010, but the evidence is inconclusive. The first confirmed case that Websense knows of was in December 2010. That infection was identified as LizaMoon until Thursday.

Get up to speed on IT innovations in cloud computing, virtualization, security, and more at Interop Las Vegas, May 8-12. [Register now.](#)

Care to Comment?

Subject (max length: 75):

Comment:

LizaMoon, named after the first domain Websense discovered with the malicious script March 29, is believed to be a SQL injection, which is when hackers [get their script into a Microsoft SQL Server database](#) that then adds it to a site's URL. SQL injections is [one of the most common forms](#) of attacking Web sites and back end databases.

Learn to create effective countermeasures that security experts can deploy to protect users from related threats.

[Best Practices for Protecting Against Blackhat SEO Attacks](#)

LizaMoon code has been found in SQL Server 2003 and 2005. Websense does not believe hackers are exploiting a vulnerability in the database. They are more likely penetrating Web systems used by the sites, such as outdated content management and blog systems. Security experts are still trying to determine exactly how the SQL injection occurs.

Fortunately, people heading to a hijacked URL are only redirected once. If the bogus warning page is ignored, then people can go on their way without being continuously sent to

FEATURE

TECHNOLO

- [Special Req Federal Da](#)
- [Information](#)
- [Simplify rer](#)
- [Confidently Integrated](#)
- [Gain IT ass](#)

FEATURE

Databases at Security (ES)

This recently | current state (depends upon also offers cor security across

INFORMA

FEATURED ANA Strategy: VI

FEATURED ANA Informed Cl

Subscribe Analytics

Find hundreds peers, and bes \$39 per month

Exclusive Res CIO Guides Best Practice: Technology A ROI Methodo