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.

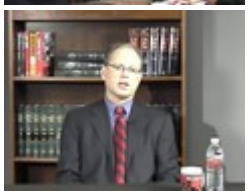
Security firm Websense says a Google search shows more than 1.5 million URLs with the nasty script. Because Google counts unique URLs and not domains or websites, the number is likely inflated. "It's safe to say it's in the hundreds of thousands," Websense said Thursday in a blog post. The attack is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

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.

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 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: