eWEEK ENTERPRISE NEWS & REVIEWS

Spam Attack Steals High-Level Execs' Data

May 29, 2007

By Brian Prince

The Better Business Bureau has issued a fraud alert regarding the resurgence of a spam attack that targets high-level executives in various industries.

The spam e-mails purport to be sent by the BBB in an effort to entice users to click on a malicious link. The SANS Institute reported a similar wave of targeted spam attacks using the BBB name in March.

SecureWorks, a managed security services provider, discovered a cache of stolen data from the scam that included bank and credit card account numbers from 1,400 high-level executives. For the scam to work, the victim must click on a link within the spam e-mail, which then downloads a Trojan virus.

RELATED LINKS

For Mother's Day, Try Some Spam

Welcome to the Spam Economy

Cloudmark Combats Rising Tide of Spam

Spammers' Fake Newsletters Slip by E-Mail Filters

Report: Spamming Soared in 2006

Is there a unified economy of spam? Click here to read more.

Once downloaded, the Trojan steals all interactive data sent from the victim's Internet Explorer browser to remote Web sites, including data entered into SSL (Secure Sockets Layer) Web sites.

On the SecureWorks Web site, Joe Stewart, a senior analyst at the Atlanta-based company, wrote that SSL encryption is of no use in stopping the theft of sensitive data because the BHO (browser helper object) intercepts the request before it is encrypted.

"Fortunately, only Internet Explorer is capable of loading the BHO, so users of other Web browsers are not affected in this case," he wrote.

"The effectiveness of this attack would be greatly diminished if it were massively spammed," Stewart said in an interview with eWEEK. "First, it would have gotten wider attention from the start—making the social-engineering ploy less effective as more people become aware of it—and second, there would be tons and tons of data being logged from all kinds of users that are just posting data to blogs, comment forms, surveys, etc., making it harder to sift through to find the high-value targets and data."

As of May 25, there were 1,400 victims and there were 145MB of data in the repository uncovered by SecureWorks. The cache of data contained bank and credit card account numbers, Social Security numbers, online payment accounts, prescription information, home addresses, user names, passwords, and other personal information. The repository was shut down by the ISP, Stewart said.

"Getting data from SSL streams is not all that new, actually—I hope people aren't under the impression that SSL encryption has been protecting them from malware stealing their data—SSL only provides privacy for the traffic out on the network," Stewart said. "Once someone manages to get their malware onto your system, they can pretty much see any data you are working with if they want to badly enough."