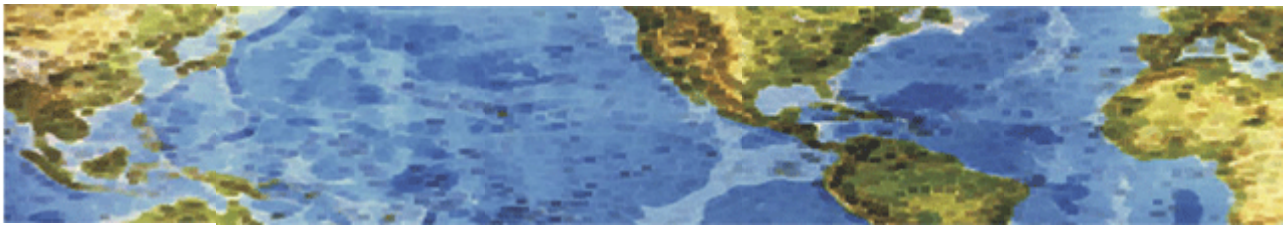
HALL ASSOCIATES



Risk-Based Decision Making Commentary
17 April 2013 Newsletter

Scammers Target People With Fake E-Mails About the Boston Explosions

On April 17, 2013, the MS-ISAC became aware of a spam campaign using the Boston Marathon bombings that occurred on April 15, 2013. Users are sent an e-mail that contains a link to a URL hosting an exploit (CVE-2012-1723 – Vulnerability in Java Runtime Environment component) which, if successful, installs malware on the end users system.

Subject lines used in the spam emails:

"2 Explosions at Boston Marathon" ; "Aftermath to explosion at Boston Marathon"; "Boston Explosion Caught on Video"; "BREAKING - Boston Marathon Explosion"; "Video of Explosion at the Boston Marathon 2013"; "Runner captures. Marathon Explosion"; 2 Explosions at Boston Marathon; "Aftermath to explosion at Boston Marathon"; "Arbitron. Dial Global. Boston Bombings"; "Boston Explosion Caught on Video"; "Explosion at Boston Marathon"; "Opinion: Boston Marathon Explosions made by radical Gays? Really? - CNN.com"; "Opinion: Boston Marathon Explosions - Romney Benefits? - CNN.com"; "Opinion: Boston Marathon Worse Sensation - Osama bin Laden still alive!? - CNN.com"; "Opinion: FBI knew about bombs 3 days before Boston Marathon - Why and Who Benefits? - CNN.com"; "Opinion: Osama Bin Laden video about Boston Marathon Explosions - bad news for all the world. - CNN.com".

Recommendations:

- ***Educate users on spam campaigns which uses recent events or celebrities' names as a lure.***
- ***Encourage users to not click on suspicious links or open suspicious attachments they may receive.***
- Ensure that your IT system has appropriate patches provided by Microsoft, Oracle, Adobe and other third party application providers to vulnerable systems immediately after appropriate testing.

Reference: https://isc.sans.edu/diary/Boston-Related+Malware+Campaigns+Have+Begun/

This is the latest in a long, ever-evolving strategy to infect your computer via drive-by malware downloads, which attack computers as soon as your web browser lands on a corrupted site. Previous email scams have used events or celebrities' names to lure users. If you receive an email message from someone you don't know, don't open the link inside without checking to see where they lead. By paying attention to details and treating ALL links with skepticism, you can avoid many of the pitfalls that lead to malware infections.

HALL ASSOCIATES

Schnuck's Data Breach Exposes 2.4 Million Credit Cards

The St. Louis-based supermarket chain was alerted to the breach on March 15 by the company's payment processor, which said there had been fraudulent activity on several cards recently used at Schnucks stores. It wasn't until March 28 that Schnucks, which operates 100 stores in four states, was finally able to locate the security hole. It took another day and a half for the company to contain the breach, which was made public March 30. In a statement yesterday (April 15) updating customers, Schnucks warned that customers who used their cards at 79 different Schnucks stores between December 2012 and March 29 may have been affected. The statement noted that only card numbers and expiration dates had been compromised, and that no names or addresses were attached.

Schnucks hired a breach-mitigation firm on March 19, five days after the supermarket chain had learned of the leak and ruled out an insider or point-of-sale malware as the source. Even then, it took nine days to fix the flaw. While the firm worked to plug the hole, Schnucks' customers' credit-card details continued to be exposed.

Schnucks' statement tried to explain why Schnucks had waited two weeks to notify customers of the data breach. "A cyber-attack is not like a bank robbery where you know immediately when it occurred and who was affected," the statement said. "The investigation of a cyber-attack requires painstaking analysis of digital evidence that takes time in order to determine what happened," it continued. "The forensic investigation firm found the first indication of an issue on March 28, we contained the issue by March 30, and we have been working to identify affected stores and card numbers since then."

Schnucks' inability to quickly locate and mitigate the leak may be due to increasingly sophisticated methods on the part of cybercriminals, who pose a growing threat to businesses and consumers alike.

http://www.technewsdaily.com/17765-schnucks-data-breach.html?cmpid=520746