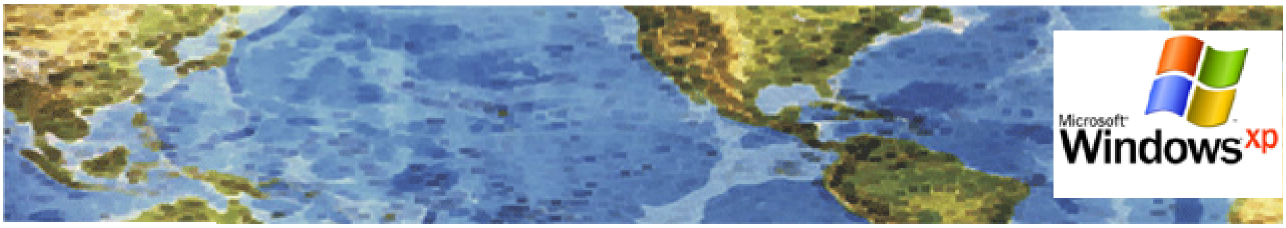
HALL ASSOCIATES



Risk-Based Decision Making Commentary
1 September 2013 Newsletter

Recent Retail Breaches Connected

A malware attack that exploited a point-of-sale software vulnerability within systems used by a select group of Kentucky and Southern Indiana retailers has now been linked to attacks against grocery chain Schnuck Markets Inc. and four other merchants. One federal investigator says all of the attacks have been traced to an overseas hacker, and cooperation with international law enforcement is expected to bring this case to a close soon. The attacks that breached POS systems and networks at Schnucks, as well as retailers in Kentucky and Southern Indiana, share a number of characteristics. The Secret Service has determined that the malware used in the attacks and the methods of entry all trace back to a single hacker using an overseas IP address. The tethering of these attacks illustrates why it's so critical for banking institutions to regularly communicate with card brands about the fraud trends they are detecting.

Common Attack Patterns

Recent breaches that followed similar attack patterns include the malware attacks against supermarket chain Bashas' Family of Stores and convenience store chain MAPCO Express, as well the cyber-attack against retail tool store chain Harbor Freight Tools, and a suspected breach at supermarket chain Raley's Family of Fine Stores. In all of these attacks, card numbers were targeted and compromised. And although the type of malware used in the attacks has not been revealed publicly, issuers say they suspect most of these attacks likely resulted from a single or similar strain. All of these cards were compromised and sold in a forum. **Within 72 hours of the breaches, cards were being used**, so the fraud occurred very quickly.

Impact on Issuers

Evidence of fraud linked to the Kentucky-Indiana breach as well as the still-under-investigation Raley's breach, continues to trickle in, but the attack against Kentucky and Southern Indiana retailers resulted in fraud losses that were five times greater than any other previous breach in the region. MasterCard and Visa released alerts about the merchants that had been affected. The local reseller who provided the remote-access software, which the malware exploited, has not been identified in those alerts.

Retail malware attacks are plaguing banking institutions because it's challenging to trace to the source. It's been a long line of succession this year, and a predominant amount of the attacks have been at grocery stores. But one thing banks and credit unions need to be aware of is when we start to have inconclusive evidence, it may be challenging to find a common point of compromise. Sometimes it's a processor breach, which may not lead them to a specific retailer.

http://www.govinfosecurity.com/recent-retail-breaches-connected-a-6022/op-1

Malicious software pretends to be your friend, hijacks your Facebook account

Next time your friend appears to send you a strange video link, **think twice about clicking on it -- it could infect your computer**. According to the New York Times, Facebook is being used to spread malicious software that acts like a message or email to gain access to your account and browser information. The software masquerading as an email or Facebook message notifies users that they have been tagged in a post and includes a link in the message. The link then directs you to a website where it asks to install a browser extension in order to play a video.

If the browser extension is installed, it can gain access to any sensitive information stored in your browser including passwords and log-in information. And once the extension is installed, it is tough to remove because it blocks user access to browser settings. According to researchers who discovered this Facebook malware, it is affecting as many as 40,000 users per hour and has infected 800,000 people so far. The malware was originally designed to specifically target users of Google Chrome, but has since spread to Mozilla Firefox as well.

Attacks through social network messages are fairly common and once someone has been infected, they often become a carrier of the malware for their friends. Receiving a message from a friend through a social network doesn't raise as many flags as messages from unknown users and while the message might seem strange, **people tend to be more apt to click the link**.

These kinds of attacks also take advantage of a user's apathy towards computer permissions, since unsuspecting people will often click "accept" to a prompt without thinking about it. Facebook is aware of the malware and is blocking and clearing the links wherever they are found. Google has already disabled the extension in their Chrome browser. While this particular malware is being addressed, the tactic is common enough that it will most likely come up again. Luckily, these kinds of malicious software require a level of participation in order to be effective**. To protect yourself from being fooled, make sure to never allow an extension to be installed that you didn't specifically want, and always be suspicious of strange messages, even if they are from people you normally trust.**

http://central.gdgt.com/2013/08/27/malicious-software-pretends-to-be-your-friend/?icid=maing-grid7|main5|dl19|sec1_lnk2%26pLid%3D364449