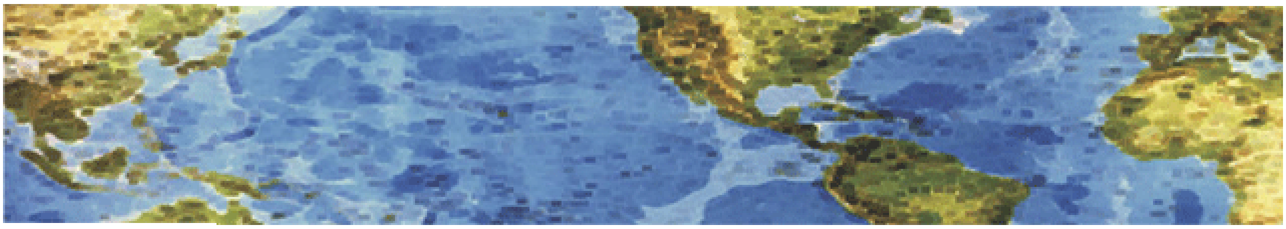
HALL ASSOCIATES



Risk-Based Decision Making Commentary
9 August 2013 Newsletter

California Escrow Firm Shuttered after Losing $1.5 Million

A California escrow firm has been run out of business and its 9 employees laid off after a remote access Trojan planted on its computer system drained it of $1.5 million.   The funds got transferred in three fraudulent wire transfers. The first one, about $430K, went to Moscow and the other two, totaling $1.1 million, went to the Chinese province of Heilongjiang. The problems at this firm began in December 2012 with the first transfer. **Now, whatever money the firm has left is under the control of a court-appointed state receiver, who plans to sue the victimized company's bank in an effort to claw back the stolen funds.** The firm got the money sent to Moscow back, but has been unable to recover the funds sent to China.

When the firm reported the crime to California State regulators (required by state law), it was given 3 days to scrape together enough to replace the looted amount. When they were unable to do so, the state stepped in and closed it down. And up until a few weeks ago, all remaining funds have been locked up in a state-established conservatorship. The receiver is asking why the bank did not slam the brakes on the out-of-character overseas transfers. This firm had never sent wires overseas before, so why did the bank not pick up a phone and confirm the requested transactions? More information is available at nakedsecurity.sophos.com/2013/08/08.

Cybercriminals and nation-states attacking small businesses through their financial/accounting systems is indicative of a major trend over the past few years. Several security firms and the federal government has developed numerous "Banking Best Practices for Businesses". I have noted some of them below.

1. **Use a dedicated system to access your financial institution's site.** This machine should be restricted from visiting all but the handful of sites necessary to interact with a financial institution and manage your finances. This approach **ONLY** works if you access your financial institution's site **ONLY** from a locked-down, dedicated machine. Making occasional exceptions or using your smartphone undermines the whole purpose of this approach.
2. **Remove any unneeded software from your dedicated machine/system**. In particular, unneeded plugins such as Java should be eliminated.
3. **Use a bookmark to access your financial institutions site.** Avoid manually typing the address into a browser since a fat-fingered keystroke might send you to a look-alike phishing site or one that contains malware.
4. **If offered, take advantage of ACH Positive Pay.** Any item that fails to meet the criteria you set up will cause you to be notified via e-mail or text message before it is completed.
5. **Require two people to sign off on every transaction**. This is a fundamental anti-fraud technique.

HALL ASSOCIATES

MALWARE:

THE HIDDEN THREAT TO YOUR BUSINESS

Whether it's a Trojan horse, a worm, or a virus, battling computer malware is a full-time profession for software epidemiologists. Despite the fact that they are highly sophisticated, there are simple steps you can take to safeguard your business and your data from infectious software. Take a look at recent trends in computer infection and see how a little malware can cost you more than just a little lost productivity.

A cyber-attack that hit Harbor Freight Tools and likely exposed card data processed at all 400 of its retail tool stores could rank among one of the biggest retail breaches this year. Card fraud linked to retail breaches is a growing concern for banking institutions. Attacks on retailers ranked among the top two most common reasons for card-related fraud losses in the last 12 months.

Although Harbor Freight has not stated the number of cards potentially affected by the attack that hit its corporate network, three separate card issuers have confirmed that fraud linked to the tool store breach is growing, with new advisories about possible compromised card numbers coming out from card brands on a nearly daily basis. One issuer says more than 10,000 of its cardholders have so far been impacted; another issuer estimates more than 20,000 of its cardholders have been affected.

In a July 20 statement about the cyber-attack, the Harbor Freight President said the breach was "similar to attacks being reported by other national retailers," apparently making reference to **malware** attacks that have targeted other merchants, such as **Schnucks, Raley's**, upscale restaurant chain **Roy's Holdings Inc.** and convenience store chain **MAPCO Express**.
Now, one card fraud expert, who also asked to remain anonymous, says it seems, based on forensics details being revealed by various sources, that Harbor Freight's corporate network was attacked **by three different strains of malware - two of which had never been seen before.** All of the malware strains were equipped with built-in security features to prevent reverse-engineering detection.

The Harbor Freight breach affected transactions conducted between June 14 and July 20, according to advisories from Visa and MasterCard shared with Information Security Media Group. Issuers say they believe the breach many have occurred sooner. Another issuer says fraudulent transactions linked to the breach have ramped up within the last two weeks, signaling that the compromised numbers were likely sold in an underground forum. "We haven't necessarily experienced a large loss yet, but I think we are just at the beginning of this thing," that issuer notes. And a third issuer points out that fraudulent transactions associated with cards compromised in the Harbor Freight attack **are showing up throughout the world.** "We have seen significant attempts linked to Harbor throughout the world, as their aggressiveness in using the cards is increasing," that issuer points out.

The Harbor Freight incident is one in a growing series of cyber-attacks affecting retailers. For additional information, check out http://www.bankinfosecurity.com/new-retail-breach-among-2013s-biggest-a-5970/op-1.