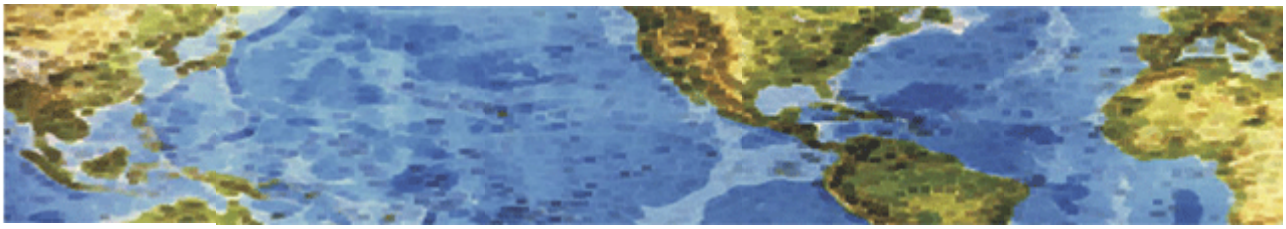
HALL ASSOCIATES



Risk-Based Decision Making Commentary
February 2013 Newsletter #2

Multiple Google Chrome Vulnerabilities Could Allow for Remote Code Execution

MS-ISAC ADVISORY NUMBER: 2013-023 **DATE(S) ISSUED:** 02/22/2013

Multiple vulnerabilities have been discovered in Google Chrome that could allow remote code execution, the bypass of security restrictions, or cause denial-of-service conditions. Google Chrome is a web browser used to access the Internet. Details are not currently available that depict accurate attack scenarios, but it is believed that some of the vulnerabilities can likely be exploited if a user visits, or is redirected to a specially crafted web page.

Successful exploitation of these vulnerabilities may result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Google Chrome for Windows and Linux versions prior to 25.0.1364.97

Google Chrome for Mac versions prior to 25.0.1364.99

Successful exploitation of some of the above vulnerabilities could result in an attacker gaining the same privileges as the user. Depending on the privileges associated with the user, an attacker could install programs; view, change, delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

We recommend the following actions be taken:

Update vulnerable Google Chrome products immediately after appropriate testing by following the steps outlined by Google here:

http://support.google.com/chrome/bin/answer.py?hl=en&answer=95414

Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

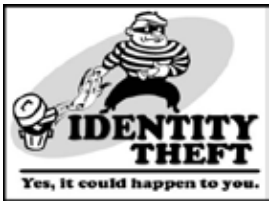
Remind users not to visit un-trusted websites, follow links, or open files provided by unknown or un-trusted sources.

REFERENCES:

Multi-State Information Sharing and Analysis Center : Center for Internet Security

31 Tech Valley Drive, Suite 2 East Greenbush, NY 12061 (518) 266-3460/1-866-787-4722

HALL ASSOCIATES



Small firm hit by 3-year hacking campaign puts face on growing cyber problem

For three straight years, a group of Chinese hackers waged a cyber war against a family-owned, eight-person software firm in California, according to court records. It started when Solid Oak Inc. founder Brian Milburn claims he discovered that China was stealing his company's parental filtering software, CYBERsitter. The theft hurt their business and sales, which was bad enough. But twelve days after he publicly accused Chinese hackers, he says he was inundated by attempts to bring down his Santa Barbara-based business.

Hackers broke into the company's system, shut down its email and web servers, spied on employees using their own webcams and gained access to sensitive company files. "We started watching sales go down," Milburn told FoxNews.com Thursday. "We depend on cash flow and it's not like we're Apple or Dell who have lots of money. We needed to pay our bills, pay our employees and pay our salaries."

So Milburn waged his own one-man cyber fight against one of the most prolific and patient hacking teams around. He didn't have help from authorities, lacked the cash larger companies have and faced an unknown giant pretty much on his own -- and, last year, won a $2.2 billion settlement, from a decision in federal court in California. Milburn's case is rare in that it ended with a big judgment -- though he declined to say whether he's received the money. But, while Solid Oak is one of the few small companies that have spoken out in detail about being victimized by hackers, the threat of cyber-assault has become all too common.

Adam Levin, co-founder and chairman of Identity Theft 911, says that for most companies it's not a matter of if they will have a breach but when. "No company is ultimately immune to this," he told FOXBusiness.com. "A lot of the times this happens from spear-phishing -- employees at companies are opening things they think are from people within their organization or things that they think are related to their companies. They open the door, and we get killed."

According to cybersecurity experts, high tech spies have been targeting small- to medium-sized companies at alarming rates. Businesses that make the leap to computerized systems often leave their digital identities exposed and primed to be plucked by hackers.

Read more: http://www.foxnews.com/politics/2013/02/22/small-businesses-big-targets-for-cyber-snoops/?intcmp=obinsite#ixzz2LehmpkYc