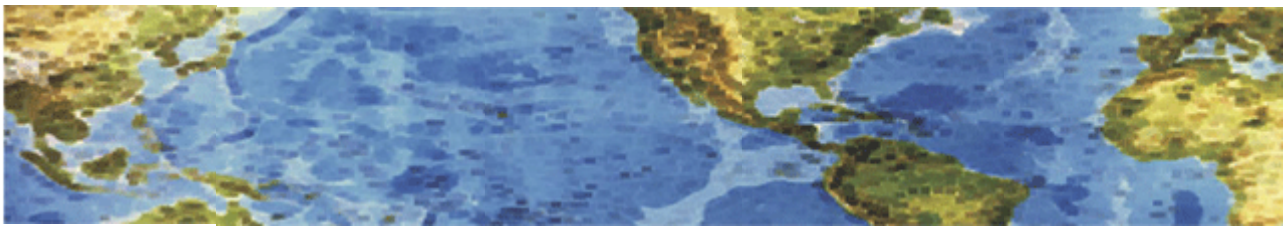
HALL ASSOCIATES



Risk-Based Decision Making Commentary
25 Oct 2013 Newsletter

Hackers Stole $100,00 from Users of a California ISP

In 2013 there has been a dramatic increase in the number of hack attacks attempted against banks, credit unions and utility companies using various techniques including DDoS attack, SQL injection, DNS Hijacking and Zero-Day Flaws. SQL Injection is one of the most common security vulnerabilities on the web and is successful when the web application is not sufficiently secured.

Recently a hacking Group named 'TeamBerserk' claimed on Twitter that, they have stolen $100,000 by leveraging user names and passwords taken from a California ISP Sebastian (Sebastiancorp.com) to access victims' bank accounts. A video proof was uploaded on the Internet, shows that how hackers used a SQL injection attack against the California ISP Sebastian to access their customers' database that included e-mail addresses, user names and clear text passwords and **then used the same data to steal money from those customers.**

Using SQL Injection on an unsecure web application, hackers can determine the structure and location of key databases and can download the database or compromise the database server. In this case, hackers took just 15 minutes to hack into the website **using an automated** SQL Injection tool) -- stole customers' database and then immediately accessed the victims Gmail accounts, linked PayPal accounts and bank accounts. The main problem here is that many people just use the same password over and over. Is your Facebook password the same as your Twitter password and the same as your back account password?

This hack shows **why it's extremely dangerous** to use the same password on more than one Web site. In the POC video, the hacker randomly chooses one username and uses his relative password against Paypal, Gmail and even Citibank account logins and that actually worked **because the victim was using the same passwords for all websites.**

If you are using a single, or only a few, passwords for all of your important accounts, you need to change that. If you have any type of accounts that are accessed online, bank account, credit cards, financial, etc., conduct a thorough security audit on them. Check every time you access the account to see when the last time “you” logged in to see if anyone else has accessed it. Be sure to keep using different and strong passwords for each website.

http://thehackernews.com/2013/10/hacker-stole-100000-from-users-of.html

HALL ASSOCIATES

Obamacare launch spawns 700+ cyber-squatters capitalizing on Healthcare.gov, state exchanges

More than 700 websites have been created with names playing off of Obamacare or Healthcare.gov, making it likely that some Americans will mistakenly hand over private information to unknown third-parties. For instance, there is a website — www.obama-care.us — that brands itself as part of the "Obamacare enrollment team," directs people to an "Obamacare enrollment form" and asks users for their name, address, Social Security number and other contact information. According to a counter at the bottom of the page, more than 3,000 people have visited obama-care.us.

This website does not actually enable people to enroll in Obamacare. It was registered with GoDaddy.com on Sept. 2 — less than a month before the official launch of the health care exchange websites — according to who.is, a website that provides information on internet domains and their owners. The practice of setting up websites with names that are similar to high-profile pages is known as cyber-squatting. It can be used by private businesses looking to siphon traffic away from their competitors, by marketers selling ads to private companies — by visiting a website, you're revealing your interest in a given product — or by identity thieves.

A legitimate website established in 1994 goes by the name "healthcare.com" — exactly the same as the website for the federal health care exchange, except that the official site ends with a dot-gov suffix. That raises the question of why federal officials chose a URL of such similarity to an existing health-related web site. The retired cybersecurity expert guessed, based on his experience in the industry, that healthcare.com could receive as much as 30 percent of traffic intended for the main federal exchange page. He said that cyber-squatters generally siphon 10 to 40 percent of the a site's traffic, adding that the official Obamacare sites will likely be on the upper end of that range, given the large number of squatters.

To prevent cyber-squatting, professional website owners typically purchase domain names that are similar to the main page. "I was shocked to find out that they have not picked up any of these other top-level domains," the cybersecurity expert said. He also provided the Washington Examiner with a list of 221 websites that he identified, using proprietary software, as cyber-squatters taking advantage of the healthcare.gov rollout — websites such as healthcarer.com — and another 499 that he identified as squatting on state exchange websites. Online security expert John McAfee predicted such a problem weeks ago. "There is no central place where I can go and say, 'OK, here are all the legitimate brokers and examiners, for all of the states,' and pick and choose one," McAfee told Fox News' Neil Cavuto. "[I]nstead, any hacker can put a website up, and make it look extremely competitive, and because of the nature of the system — this is health care, after all — they can ask you the most intimate questions and you're freely going to answer them.

Check out http://washingtonexaminer.com/obamacare-launch-spawns-700-cyber-squatters-capitalizing-on-healthcare.gov-state-exchanges/article/2537691 for the entire article.