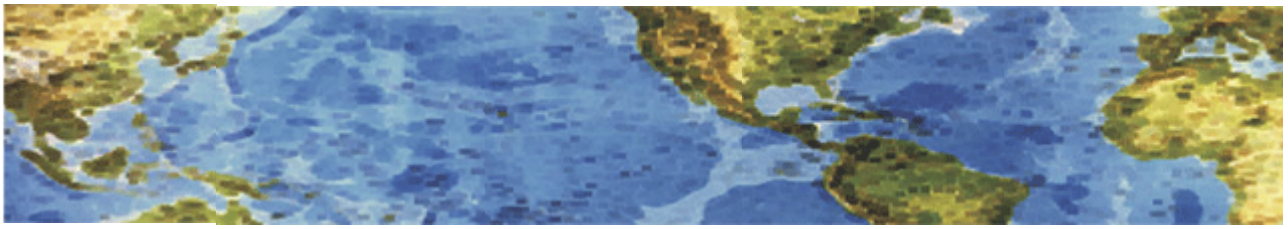
HALL ASSOCIATES



Risk-Based Decision Making Commentary
1 September 2014 Newsletter

Why Your Passwords Should be at Least 24 Characters Long

Earlier this month 1.2 billion other websites were targeted by Russian hackers utilizing a massive "bot" attack. These bots aggressively attempted access to websites with username and password options. Attacks like this serve as a good idea that it's not enough to password-protect everything. You must create strong passwords that make it hard for hackers to get what they want.

Here are two simple rules to follow when developing hacker-proof passwords:

Rule No.1: It's Not Just About Your Password, You Also Need a Strong Username

Too many people use their email address or first underscore last name as a username to make it easy to remember. Well, that also makes a hacker's job easy. Here's the deal: Your username is part of a security access system and should be considered critical security access code. When you see "username" think "code name." Your email address is not a very good code name. We recommend that your username never be associated to your personal information like first or last name, email address or phone number. Here are some good examples of strong code names: BlackJack, SilentHammer, LandShark, NinjaSmoke. Be creative and develop usernames that are just as unique as your passwords.

2. It's All About the Number of Characters

The internet is flooded with guides on strong password development, but you must always plan for a worst-case scenario. For example, a rogue Russian network of hackers decides to penetrate all your access points within the world wide web. They are armed with a super computer that can "brute force" access all your personal and financial information. A brute force attack cannot be stopped. However, it can be delayed for 40-plus years with the right passwords.

Most super computers can run every character on a keyboard 500 times a second, allowing it to run thousands of combinations of characters per minute. So using a # or $ in your password doesn't really make a difference when a computer is running all characters 500 times a second. It's not the complexity of a password that makes it hard to crack; it's the length of the password. The more characters in a password, the longer it will take for a super computer to run through all the possible combinations of characters.

We recommend a 24-character or more password. Sounds crazy, but here are some examples to decrease the stress of it all: HarleyDavidsonStarbucks!!!, FireEarthWindWater4Life!#!. Long passwords with a combination of uppercase and special characters increases possible combinations exponentially, therefore taking a super computer upwards to 40 years to run all possible combinations.

Here's the bottom line: Strong usernames combined with long passwords will increase the security of your online life exponentially. ***This has been said numerous times, but bears repeating until everyone really does it. This article says why.***

http://www.foxbusiness.com/personal-finance/2014/08/29/why-your-passwords-should-be-at-least-24-charcters-long/?intcmp=obnetwork

HALL ASSOCIATES

HardCoded Backdoor Found in China-made Netis, Netcore Routers

Routers manufactured and sold by a Chinese security vendor have a hard-coded password that leaves users with a wide-open backdoor that could easily be exploited by attackers to monitor the Internet traffic. The routers are sold under the brand name Netcore in China, and Netis in other parts of the world, including South Korea, Taiwan, Israel **and the United States.**

According to Trend Micro, the backdoor — a semi-secret way to access the device — allows cybercriminals the possibility to bypass device security and to easily run malicious code on routers and change settings. Netis routers are known for providing the best wireless transfer speed up to 300Mbps, offering a better performance on online gaming, video streaming, and VoIP phone calling.

The Netcore and Netis routers have an open UDP port listening at port 53413, which can be accessed from the Internet side of the router. The password needed to open up this backdoor is hardcoded into the router's firmware. All of the routers – sold under the Netcore brand in China and as Netis outside of the country – appear to have the same password. The backdoor cannot be changed or disabled, essentially offering a way in to any attacker who knows the "secret" string. Using the backdoor, hackers could upload or download hostile code and even modify the settings on vulnerable routers in order to monitor a person's Internet traffic as part of a so-called man-in-the-middle (MitM) attack. By attempting a MitM attack, a potential attacker could intercept users' internet communication, steal sensitive information and even hijack sessions.

Researchers scanned the Internet and found that millions of devices worldwide are potentially vulnerable. Using ZMap to scan vulnerable routers, they found more than two million IP addresses with the open UDP port. Almost all of these routers are in China, with much smaller numbers in other countries, including but not limited to South Korea, Taiwan, Israel, and the United States.

Exploiting this flaw is not too difficult, as a simple port scan can reveal the open UDP ports to anyone using such an online tool. In addition, Trend Micro also found that a configuration file containing a username and password for the web-based administration panel on the router is stored with no encryption protection, allowing an attacker to download it. "*Users have relatively few solutions available to remedy this issue. Support for Netcore routers by open source firmware like dd-wrt and Tomato is essentially limited; only one router appears to have support at all. Aside from that, the only adequate alternative would be to replace these devices.*"

http://thehackernews.com/2014/08/hardcoded-backdoor-found-in-china-made_27.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.686.wb0ao05fi9.eef