NH-ISAC Daily Security Intelligence Report – September 22, 2017

*This information is marked TLP **GREEN**: This information is marked TLP GREEN: Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.*

BREACH REPORT

Neurology Foundation Unauthorized PHI Access Could Affect 12K

Rhode Island-based The Neurology Foundation, Inc. (Foundation) recently announced that an employee had been making unauthorized PHI access. The employee had been using a company credit card to make unauthorized purchases, but it was discovered that the individual had also transferred certain Foundation data onto a hard drive stored in the employee's home.

"The storage of Foundation data on external media is not permitted by the Foundation and the Foundation has since recovered the hard drive," the organization said..

Link – https://healthitsecurity.com/news/neurology-foundation-unauthorized-phi-access-could-affect-12k

Passwords to Over a Half Million Car Tracking Devices Leaked Online

We've seen a lot of data breaches this year: some big, some small, some that are dangerous, and some that are just embarrassing. But if we were to name one as the creepiest data breach of 2017, this leak of logins for car tracking devices might take the cake.

The Kromtech Security Center recently found over half a million records belonging to SVR Tracking, a company that specializes in "vehicle recovery," publicly accessible online. SVR provides its customers with around-the-clock surveillance of cars and trucks, just in case those vehicles are towed or stolen…

Link – https://gizmodo.com/passwords-to-access-over-a-half-million-car-tracking-de-1818624272

CRIME and INCIDENT REPORT

DDoS Extortion Group Sends Ransom Demand to Thousands of Companies

A group of DDoS extortionists using the name of Phantom Squad has sent out a massive spam wave to thousands of companies all over the globe, threating DDoS attacks on September 30, if victims do not pay a ransom demand. The emails spreading the ransom demands were first spotted by security researcher Derrick Farmer and the threats appear to have started on September 19 and continued ever since. Several experts who reviewed the emails and ransom demands reached the conclusion that the group does not possess the firepower to launch DDoS attacks on so many targets on the same day, and is most likely using scare tactics hoping to fool victims into paying…

Link – https://www.bleepingcomputer.com/news/security/ddos-extortion-group-sends-ransom-demand-to-thousands-of-companies/

Remotely Locked Apple Devices Being Held Ffr Ransom

Some Apple product owners have found themselves on the receiving end of a new ransom attack that has someone locking their device most likely using stolen iCloud credentials and the initiating the Find My iPhone remote lock feature.

MacRumors is reporting that the owners of the locked device have received messages demanding a payment for the passcode. One screen shot shows the attacker requiring $50 in bitcoin for the code to unlock the device.

Link – https://www.scmagazine.com/remotely-locked-apple-devices-being-held-for-ransom/article/690314/

Hackers behind CCleaner compromise were after Intel, Microsoft, Cisco

There is a new twist in the CCleaner hack saga: the attackers apparently didn't set out to compromise as many machines as possible.

According to Cisco, their actual targets were computers at a number of huge tech companies like Intel, Microsoft, Linksys, Dlink, Google, Samsung and Cisco, telecoms such as O2 and Vodafone, and (the odd man out) Gauselmann, a manufacturer of gaming machines...

Link – https://www.helpnetsecurity.com/2017/09/21/ccleaner-compromise-targets/

The Dark Overlord cybergang threatens kids in its latest attack

A cyber gang calling itself The Dark Overlord Solution late last week sent an unusually threatening ransom note to the Columbia Falls (Montana) school district forcing officials to shutter its schools to ensure the safety of the students.

Link – https://www.scmagazine.com/the-dark-overlord-cybergang-threatens-kids-in-its-latest-attack/article/690482/

IoT Botnet Retooled to Send Email Spam

It has become the norm that when someone says "IoT botnet" most security aficionados think of DDoS attacks.

While most IoT botnets are, in fact, used for DDoS attacks, in recent months, quite a few IoT malware strains that are usually used to assemble these botnets have added other features besides DDoS functions.

Link – https://www.bleepingcomputer.com/news/security/iot-botnet-retooled-to-send-email-spam/

NEWS REPORT

Three Things to Know About the Dark Web

One of the more curious aspects about the dark web is that it didn't start out as such a dark place: it began with bulletin boards in the 80s and 90s – the markets of that day – and continued in the early 2000s, when Freenet launched as a private peer-to-peer network for sharing content. At about the same time, the United States Naval Research

Laboratory came up with what would be called The Onion Routing project, or Tor, with the intention of shielding US intelligence communications online…

Link - https://www.helpnetsecurity.com/2017/09/21/three-things-know-dark-web/

Why Size Doesn't Matter in DDoS Attacks

Distributed denial-of-service (DDoS) attacks have increased, and research shows that on average, a DDoS attack can cost an organization more than $2.5 million in revenue. As a small or medium-sized business owner, you may be thinking "hackers only use DDoS on the big boys" or "I'm not big enough for them to care." But these disruptive attacks are getting worse, and they're moving downstream. Today, they affect everyone from the largest organizations to smaller companies that are being hit either directly, or as a by-product of one of their service providers being attacked…

Link - https://www.darkreading.com/cloud/why-size-doesnt-matter-in-ddos-attacks-/a/d-id/1329897?

Canada securities watchdog to review cyber security after SEC hack

An umbrella group representing each of Canada's provincial securities regulators said on Thursday it will conduct an additional cyber security review after a breach at Wall Street's top regulator.

The Canadian Securities Administrators (CSA) said in response to queries that its regular reviews on national systems and data have found no evidence of its systems being compromised.

Link – https://www.reuters.com/article/sec-cyber-canada/canada-securities-watchdog-to-review-cyber-security-after-sec-hack-idUSL2N1M21Q9

ISO decides not to approve two NSA encryption algorithms, citing trust issues

The International Organization for Standardization (ISO) decided not to approve the NSA encryption algorithms Speck and Simon after expressing concerns that the NSA was able to crack the encryption techniques and would thus gain a back door into coded transmissions.

The decision follows a three year dispute behind closed doors around the world between academic and industry experts from countries including Germany, Japan and Israel about whether or not the two data encryption techniques would be set as global encryption standards, according to Reuters…

Link - https://www.scmagazine.com/iso-refuses-to-approve-nsa-encryption-algorithms-as-industry-standards/article/690470/

VULNERABILITY REPORT

Newest Joomla! release eliminates information disclosure flaws

The Joomla! Project this week released version 3.8 of its open-source content management system, which fixes two information disclosure vulnerabilities.

The first of these bugs, designated CVE-2017-14596, resides in the LDAP authentication plug-in, and affects versions 1.5.0 through 3.7.5. According to a Joomla! Developer Network advisory, the medium-severity flaw consists of inadequate escaping in the plugin, which can result in the disclosure of usernames and passwords.

Link – https://www.scmagazine.com/newest-joomla-release-eliminates-information-disclosure-flaws/article/690303/

Struts Vulnerabilities Run Rampant

Equifax confirmed the attack vector used in its data breach to be CVE-2017-5638, a vulnerability patched last March 2017 via S2-045. The vulnerability was exploited to gain unauthorized access to highly sensitive data of approximately 143 million U.S. and 400,000 U.K. customers, as well as 100,000 Canadian consumers. This vulnerability was first disclosed in March, almost immediately followed by publicly available POCs, weaponized exploits, and scanners produced by third parties…

Link – http://blog.trendmicro.com/trendlabs-security-intelligence/apache-struts-vulnerabilities-run-rampant/

Hacking into Internet Connected Light Bulbs

The subject of this blog, the LIFX light bulb, bills itself as the light bulb reinvented; a "WiFi enabled multi-color [sic], energy efficient LED light bulb" that can be controlled

from a smartphone [1]. We chose to investigate this device due to its use of emerging wireless network protocols, the way it came to market and its appeal to the technophile in all of us.

The LIFX project started off on crowd funding website Kickstarter in September 2012 where it proved hugely popular, bringing in over 13 times its original funding target.

Link – https://www.contextis.com/blog/hacking-into-internet-connected-light-bulbs