NH-ISAC Daily Security Intelligence Report – September 21, 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

Equifax Breach: Setting the Record Straight

Bloomberg published a story this week citing three unnamed sources who told the publication that Equifax experienced a breach earlier this year which predated the intrusion that the big-three credit bureau announced on Sept. 7. To be clear, this earlier breach at Equifax is not a new finding and has been a matter of public record for months. Furthermore, it was first reported on this Web site in May 2017.

In my initial Sept. 7 story about the Equifax breach affecting more than 140 million Americans, I noted that this was hardly the first time Equifax or another major credit bureau has experienced a breach impacting a significant number of Americans…

Link – https://krebsonsecurity.com/2017/09/equifax-breach-setting-the-record-straight/

Experian Site Can Give Anyone Your Credit Freeze PIN

An alert reader recently pointed my attention to a free online service offered big-three credit bureau Experian that allows anyone to request the personal identification number (PIN) needed to unlock a consumer credit file that was previously frozen at Experian.

The first hurdle for instantly revealing anyone's freeze PIN is to provide the person's name, address, date of birth and Social Security number (all data that has been jeopardized in breaches 100 times over — including in the recent Equifax breach — and that is broadly for sale in the cybercrime underground)…

Link – https://krebsonsecurity.com/2017/09/experian-site-can-give-anyone-your-credit-freeze-pin/

Equifax Directed Consumers to Fake Phishing Site for Weeks

You can now add another blunder to the already long list of Equifax's missteps in the wake of the massive breach it announced earlier this month: the company has been pointing affected customers to a fake phishing site…

Link – https://www.helpnetsecurity.com/2017/09/21/equifax-phishing/

SEC Discloses Edgar Corporate Filing System Was Hacked in 2016

The top U.S. markets regulator disclosed Wednesday that hackers penetrated its electronic system for storing public-company filings last year and may have traded on the information.

The Securities and Exchange Commission's chairman, Jay Clayton, revealed the breach in an unusual and lengthy statement issued Wednesday evening that didn't provide many details about the intrusion, including the extent of any illegal trading…

Link – https://www.wsj.com/articles/sec-discloses-edgar-corporate-filing-system-was-hacked-in-2016-1505956552

CRIME and INCIDENT REPORT

Iranian Cyberspy Group Targets Aerospace, Energy Firms

An Iranian APT group with the ability to carry out destructive attacks has been waging a sophisticated cyber espionage campaign against organizations in the aerospace and energy sectors in the US, Saudi Arabia, and South Korea.

APT33 has been active since at least 2013 and appears focused on gathering information that could help Iran bolster its capabilities in the aviation and petrochemical industries, FireEye said in an advisory Wednesday…

Link – https://www.darkreading.com/attacks-breaches/iranian-cyberspy-group-targets-aerospace-energy-firms/d/d-id/1329940?

Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware

Over the past few years, we have been tracking a separate, less widely known suspected Iranian group with potential destructive capabilities, whom we call APT33. Our analysis reveals that APT33 is a capable group that has carried out cyber espionage operations since at least 2013. We assess APT33 works at the behest of the Iranian government…

Link – https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

FedEx Profit Takes $300 Million Hit After Malware Attack

TNT Express, which FedEx acquired last year for $4.8 billion, was one of several major companies whose systems were infected with NotPetya malware (also known as Nyetya, PetrWrap, exPetr, GoldenEye, and Diskcoder.C) in late June.

The company reported a few weeks after the attack that the incident had a significant impact on its operations and communications. FedEx admitted at the time that it was possible TNT would not be able to fully restore all affected systems and recover all the critical business data encrypted by NotPetya…

Link – http://www.securityweek.com/fedex-profit-takes-300-million-hit-after-malware-attack

New FinFisher surveillance campaigns: Are internet providers involved?

New surveillance campaigns utilizing FinFisher, infamous spyware known also as FinSpy and sold to governments and their agencies worldwide, are in the wild. Besides featuring technical improvements, some of these variants have been using a cunning,

previously-unseen infection vector with strong indicators of major internet service provider (ISP) involvement.

FinFisher has extensive spying capabilities, such as live surveillance through webcams and microphones, keylogging, and exfiltration of files. What sets FinFisher apart from other surveillance tools, however, are the controversies around its deployments. FinFisher is marketed as a law enforcement tool and is believed to have been used also by oppressive regimes…

Link – https://www.welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/

The Shark CryptoMix Ransomware Variant Smells Blood in the Water

Today, I discovered a new variant of the CryptoMix ransomware that is appending the .SHARK extension to encrypted file names. This family of ransomware usually releases a new version almost every week, if not sooner, so it is a bit surprising to see them take almost three weeks to release this variant.

This article will provide a brief summary of what has changed in this new variant. As we are always looking for weaknesses, if you are a victim of this variant and decide to pay the ransom, please send us the decryptor so we can take a look at it. You can also discuss or receive support for Cryptomix ransomware infections in our dedicated Cryptomix Help & Support Topic…

Link – https://www.bleepingcomputer.com/news/security/the-shark-cryptomix-ransomware-variant-smells-blood-in-the-water/

CCleaner targeted top tech companies in attempt to lift IP

Cisco's security limb Talos has probed the malware-laden CCleaner utility that Avast so kindly gave to the world and has concluded its purpose was to create secondary attacks that attempted to penetrate top technology companies. Talos also thinks the malware may have succeeded in delivering a payload to some of those firms targeted.

The malware that made its way into CCleaner gathers information about its host and sends it to what Talos calls the "C2 server". Whoever is behind the malware then reviews

the hosts its code has compromised. It then tries to infect some of those hosts with what Talos characterises as "specialized secondary payloads".

Link – http://www.theregister.co.uk/2017/09/21/ccleaner_secondary_payload_targeted_top_tech_companies/

NEWS REPORT

FTC Providing Partial Refunds for Advanced Tech Support Victims

Last month, the FTC announced the recovery of 10 million dollars from Advanced Tech Support, one of the most successful US-based tech support scammers ever. This money will be put towards partial refunds for victims of ATS who purchased products or services from them between April 2012 and November 2014. Per the FTC announcement, the deadline for a refund is October 27…

Link – https://blog.malwarebytes.com/security-world/2017/09/ftc-providing-partial-refunds-for-advanced-tech-support-victims/

VULNERABILITY REPORT

Attackers Can Use HVAC Systems to Control Malware on Air-Gapped Networks

Heating, ventilation, and air conditioning (HVAC) systems can be used as a means to bridge air-gapped networks with the outside world, allowing remote attackers to send commands to malware placed inside a target's isolated network.

This type of attack scenario — codenamed HVACKer by its creators — relies on custom-built malware that is capable of interacting with a computer's thermal sensors to read temperature variations and convert these fluctuations into zeros and ones — binary code.Link – https://www.bleepingcomputer.com/news/security/attackers-can-use-hvac-systems-to-control-malware-on-air-gapped-networks/