NH-ISAC Daily Security Intelligence Report – November 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.*

CRIME and INCIDENT REPORT

Using Unsecured IoT Devices, DDoS Attacks Doubled in the First Half of 2017

According to a report recently published by the security firm Corero the number of DDoS Attacks doubled in the First Half of 2017 due to unsecured IoT. Denial of Service (DoS) attacks have been around as long as computers have been networked. But if your business relies on the Internet to sell products or collaborate, a DoS attack is more than a nuisance, it can be critical.

Over the past few years, the number of DoS attacks has continued to slowly grow in a "cat and mouse" evolution — bad actors get a slightly stronger attack, and network vendors come up with slightly more resilient equipment to defend. Generally the attacks came from botnets comprised of infected computers and servers. The cost of acquiring and keeping these systems in the botnet was relatively expensive, so there was an economic limiter on how fast the attacks would grow. Then Mirai happened in 2016 and everything changed…

Link - http://securityaffairs.co/wordpress/65827/hacking/iot-devices-ddos-attacks.html

Cryptocurrency Startup Claims Hackers Stole $30.95 Million

In an official statement posted on its website yesterday, Tether, a startup that offers 1-to-1 dollar-backed digital tokens [USDT], said a hacker stole funds worth $30,950,010. Tether claims the hack took place on Sunday, November 19, and the hacker removed funds from the main Tether Treasury wallet and moved it to the 16tg2RJuEPtZooy18Wxn2me2RhUdC94N7r address.

"As Tether is the issuer of the USDT managed asset, we will not redeem any of the stolen tokens, and we are in the process of attempting token recovery to prevent them from entering the broader ecosystem," the company said.

Link – https://www.bleepingcomputer.com/news/security/cryptocurrency-startup-claims-hackers-stole-30-95-million/

North Korean Hackers Target Android Users in South

At least two cybersecurity firms have noticed that the notorious Lazarus threat group, which many experts have linked to North Korea, has been using a new piece of Android malware to target smartphone users in South Korea.

Both McAfee and Palo Alto Networks published blog posts on Monday describing the latest campaign attributed to the threat actor also known as Hidden Cobra. The group is believed to be responsible for several high-profile attacks, including ones targeting Sony and financial institutions, and possibly even the recent WannaCry ransomware attack. Some of the operations tied to this group are Operation Blockbuster, Dark Seoul and Operation Troy…

Link – http://www.securityweek.com/north-korean-hackers-target-android-users-south

Correcting the Record on vDOS Prosecutions

KrebsOnSecurity recently featured a story about a New Mexico man who stands accused of using the now-defunct vDOS attack-for-hire service to hobble the Web sites of several former employers. That piece stated that I wasn't aware of any other prosecutions related to vDOS customers, but as it happens there was a prosecution in the United Kingdom earlier this year of a man who's admitted to both using and helping to administer vDOS. Here's a look at some open-source clues that may have led to the U.K. man's arrest.

In early July 2017, the West Midlands Police in the U.K. arrested 19-year-old Stockport resident Jack Chappell and charged him with aiding the vDOS co-founders — two Israeli men who were arrested late year and charged with running the service...

Link – https://krebsonsecurity.com/2017/11/correcting-the-record-on-vdos-prosecutions/

NEWS REPORT

Lawmaker to HHS: Label Software in Medical Devices

The Trump administration should convene a national effort in partnership with the private sector to ensure that the owners and operators of medical devices, hospital IT networks and electronic health records systems can find out what software and other components are in the products they buy, says the chairman of the powerful House Energy and Commerce Committee.

In a letter Thursday to acting Health and Human Services Secretary Eric Hargen, committee Chairman Greg Walden, R-Ore., notes a congressionally chartered task force on health care cybersecurity earlier this year recommended such transparency requirements…

Link – https://www.cyberscoop.com/lawmakers-hhs-label-software-medical-devices-corman-walden/

No, You're Not Being Paranoid. Sites Really Are Watching Your Every Move

If you have the uncomfortable sense someone is looking over your shoulder as you surf the Web, you're not being paranoid. A new study finds hundreds of sites—including microsoft.com, adobe.com, and godaddy.com—employ scripts that record visitors' keystrokes, mouse movements, and scrolling behavior in real time, even before the input is submitted or is later deleted.

Session replay scripts are provided by third-party analytics services that are designed to help site operators better understand how visitors interact with their Web properties and identify specific pages that are confusing or broken. As their name implies, the scripts allow the operators to re-enact individual browsing sessions. Each click, input, and scroll can be recorded and later played back…

Link – https://arstechnica.com/tech-policy/2017/11/an-alarming-number-of-sites-employ-privacy-invading-session-replay-scripts/

Amazon, Microsoft Launch Secret Cloud Servers for the US Intelligence Community

Today, Amazon announced a new offering named "AWS Secret Region," which is a cloud server region for use only by US intelligence agencies and their third-party contractors.

With the launch of this new Secret Region, AWS becomes the first and only commercial cloud provider to offer regions to serve government workloads across the full range of data classifications, including Unclassified, Sensitive, Secret, and Top Secret. By using the cloud, the U.S. Government is better able to deliver necessary information and data to mission stakeholders," said Amazon in a press release…

Link – https://www.bleepingcomputer.com/news/government/amazon-microsoft-launch-secret-cloud-servers-for-the-us-intelligence-community/

How a Wi-Fi Pineapple Can Steal Your Data (And How to Protect Yourself from It)

Yes, my friend, the device you are looking for is a Wi-Fi Pineapple, which can turn anyone from hack to hacker for the low, low price of $99. Since it is so cheap and easy to use, it's important to understand how the Pineapple works in order to protect yourself against its attacks…

Link – https://motherboard.vice.com/en_us/article/pa39xv/pineapple-wifi-how-to-mitm-hack?trk_source=header-logo

VULNERABILITY REPORT

Intel Chip Flaws Expose Millions of Devices to Attacks

Intel has conducted an in-depth security review of its Management Engine (ME), Trusted Execution Engine (TXE) and Server Platform Services (SPS) technologies and discovered several vulnerabilities. The company has released firmware updates, but it could take some time until they reach the millions of devices exposed to attacks due to these flaws.

Intel's ME solution, which some members of the industry have classified as a backdoor, allows users to remotely manage computers via the Intel Active Management Technology (AMT)…

Link – http://www.securityweek.com/intel-chip-flaws-expose-millions-devices-attacks

Additional Link - https://www.bleepingcomputer.com/news/security/intel-fixes-critical-bugs-in-management-engine-its-secret-cpu-on-chip/

US-CERT Warns of ASLR Implementation Flaw in Windows

The U.S. Computer Emergency Readiness Team is warning of a vulnerability in Microsoft's implementation of Address Space Layout Randomization that affects Windows 8, Windows 8.1 and Windows 10. The vulnerability could allow a remote attacker to take control of an affected system.

Address Space Layout Randomization (ASLR) is championed as a system hardening technology used in most major desktops and mobile operating systems. ASLR is used to thwart memory-based code-execution attacks. iOS, Android, Windows, macOS and Linux each use ASLR to keep systems safer…

Link – https://threatpost.com/us-cert-warns-of-aslr-implementation-flaw-in-windows/128948/

EJB

Operations

National Health ISAC (NH-ISAC)

Global Situational Awareness Center

226 North Nova Road, Suite 391

Ormond Beach, Florida 32174

www.nhisac.org

twitter.com/NHISAC