NH-ISAC
NATIONAL HEALTH - ISAC

NH-ISAC Daily Security Intelligence Report – November 30, 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

Insiders Accused of Stealing Personal Data from Homeland Security

It was an audacious scheme: an attempted inside job at the office of a federal watchdog agency, where the cops, the authorities said, became the robbers.

Three employees in the inspector general’s office for the Department of Homeland Security stole a computer system that contained sensitive personal information of about 246,000 agency employees, according to three United States officials and a report sent to Congress last week. They planned to modify the office’s proprietary software for managing investigative and disciplinary cases so that they could market and sell it to other inspector general offices across the federal government...

Link – https://www.nytimes.com/2017/11/28/us/politics/homeland-security-personal-data-software-stolen.html

Senate GOP campaign arm stole donor data from House Republicans

Staffers for Senate Republicans’ campaign arm seized information on more than 200,000 donors from the House GOP campaign committee over several months this year by breaking into its computer system, three sources with knowledge of the breach told POLITICO.

The unauthorized raid on the National Republican Congressional Committee's data created a behind-the-scenes rift with the National Republican Senatorial Committee, according to the sources, who described NRCC officials as furious. It comes at a time when House Republicans are focused on preparing to defend their 24-seat majority in the 2018 midterm elections. And it has spotlighted Senate Republicans' deep fundraising struggles this year, with the NRSC spending more than it raised for four months in a row...

Link – https://www.politico.com/story/2017/11/29/campaign-data-stolen-republicans-house-senate-196238

The Shipping Giant Clarkson Has Suffered A Security Breach

Clarkson confirmed the hackers may release some of the stolen data, it hasn't provided further details due to the ongoing law enforcement investigation. The information disclosed by the company suggests cyber criminals blackmailed the company requesting the payment of a ransom in order to avoid having its data leaked online. According to Clarkson, the hackers compromised a single user account to access the systems of the shipping giant..

Link – http://securityaffairs.co/wordpress/66172/cyber-crime/clarkson-security-breach.html

Massive Malaysian Telco Data Breach Might Be an Inside Job

INVESTIGATORS in Malaysia have suggested the massive personal data leak of 46 million mobile phone accounts was linked to a subcontractor of the Southeast Asian country's very own Internet regulators.

On Monday, Inspector-General of Police Mohamad Fuzi Harun said investigators were tracking down the owner of an e-mail account which could help solve the case. The official's comment came following reports on the discovery of several file names containing the words PCBS and SKMM, which at least six telecommunications companies used as references related to the leaked data…

Link – http://techwireasia.com/2017/11/massive-malaysian-telco-data-breach-appears-to-be-an-inside-job/

CRIME and INCIDENT REPORT

Fake Windows Troubleshooting Support Scam Uploads Screenshots & Uses Paypal

A new tech support scam has been discovered that shows a fake BSOD, or Blue Screen of Death, on the infected computer and then displays an application that pretends to be a Troubleshooter for Windows. This Troubleshooter will then state that your computer cannot be fixed, blocks you from using Windows, and prompts you to purchase a program using PayPal to fix the "detected problems" and unlock the screen...

Link – https://www.bleepingcomputer.com/news/security/fake-windows-troubleshooting-support-scam-uploads-screenshots-and-uses-paypal/

Android Malware Steals Data from Social Media Apps

A newly discovered backdoor that has managed to infect over one thousand Android devices was designed to steal sensitive data from popular social media applications, Google reveals.

Dubbed Tizi, the malware comes with rooting capabilities and has been already used in a series of targeted attacks against victims in African countries such as Kenya, Nigeria, and Tanzania. Discovered by the Google Play Protect team in September 2017, the backdoor appears to have been in use since October 2015...

Link – http://www.securityweek.com/android-malware-steals-data-social-media-apps

Websites Use Your CPU To Mine Cryptocurrency Even When You Close Your Browser

Researchers have discovered a new technique that lets hackers and unscrupulous websites perform in-browser, drive-by cryptomining even after a user has closed the window for the offending site.

Over the past month or two, drive-by cryptomining has emerged as a way to generate the cryptocurrency known as Monero. Hackers harness the electricity and CPU resources of millions of unsuspecting people as they visit hacked or deceitful websites. One researcher recently documented 2,500 sites actively running cryptomining code in visitors' browsers, a figure that, over time, could generate significant revenue. Until now, however, the covert mining has come with a major disadvantage for the attacker or website operator: the mining stops as soon as the visitor leaves the page or closes the page window...

Link – https://arstechnica.com/information-technology/2017/11/sneakier-more-persistent-drive-by-cryptomining-comes-to-a-browser-near-you/

Phishing thieves target Anne Arundel school paychecks, steal $57,000

Thieves used a phishing attack to redirect the paychecks of 36 Anne Arundel County school employees, getting away with roughly $57,000, school officials said Tuesday. An unidentified individual or individuals used stolen passwords or other credentials to move the Nov. 22 direct deposit paychecks for the employees to another account.

"I don't want to go into specifics of what occurred because it could compromise the investigation, but it is certainly possible these employees clicked on spam email at some point and that enabled the perpetrators of this crime to access those 36 accounts," said Bob Mosier, a spokesman for Anne Arundel County Public Schools...

Link – http://www.capitalgazette.com/news/schools/ac-cn-schools-hack-20171128-story.html

A Deep Dive Analysis of the FALLCHILL Remote Administration Tool

Advanced Persistent Threat (APT) groups pose a great threat to global security. Over the years, many threat groups have emerged but none have attracted more attention than North Korean groups due to the ongoing nature of the conflict between North Korea and the west. That, together with the great damage done so far by this threat group (most well-known are the infamous Sony attacks and the related Operation Blockbuster), has prompted significant institutional interest. The U.S. Government in particular refers to the malicious threat actor connected to the North Korean government as HIDDEN COBRA…

Link – https://blog.fortinet.com/2017/11/28/a-deep-dive-analysis-of-the-fallchill-remote-administration-tool

UBoatRAT Navigates East Asia

Palo Alto Networks Unit 42 has identified attacks with a new custom Remote Access Trojan (RAT) called UBoatRAT. The initial version of the RAT, found in May of 2017, was simple HTTP backdoor that uses a public blog service in Hong Kong and a compromised web server in Japan for command and control. The developer soon added various new features to the code and released an updated version in June. The attacks with the latest variants we found in September have following characteristics...

Link – https://researchcenter.paloaltonetworks.com/2017/11/unit42-uboatrat-navigates-east-asia/

NEWS REPORT

FDA clears AliveCor's Kardiaband as the first medical device accessory for the Apple Watch

The Food and Drug Administration has just cleared AliveCor's Kardiaband EKG reader as the first medical device accessory for the Apple Watch. Europe has been able to use a version of the Kardiaband for Apple Watch for some time now but, thanks to the new FDA approval, the device can now be used in the U.S., marking the first time an Apple Watch accessory will be able to be used as a medical device in the States.

Up until now, AliveCor has used the KardiaMobile device, which was stuck to the back of your smartphone and paired with an app to detect abnormal heart rhythm and atrial fibrillation (AFib). The new Apple Watch accessory, Kardiaband, clicks into a slot on the Watch band to do the same thing…

Link – https://techcrunch.com/2017/11/30/fda-clears-alivecors-kardiaband-as-the-first-medical-device-accessory-for-the-apple-watch/

Judge Orders Coinbase to Hand Over Details of 14,355 US Users to the IRS

A federal judge in California has ruled today that US-based cryptocurrency exchange portal Coinbase must hand over details of over 14,000 users to the US Internal Revenue Service (IRS). The decision is part of a lawsuit the IRS filed against Coinbase in November 2016. Initially, the IRS tried to force Coinbase to hand over the personal details of all US citizens who had conducted Bitcoin trade operations on the platform between January 1, 2013, and December 31, 2015...

Link – https://www.bleepingcomputer.com/news/technology/judge-orders-coinbase-to-hand-over-details-of-14-355-us-users-to-the-irs/

VULNERABILITY REPORT

Patch for macOS Root Access Flaw Breaks File Sharing

The patch released by Apple on Wednesday for a critical root access vulnerability affecting macOS High Sierra appears to break the operating system's file sharing functionality in some cases. The company has provided an easy fix for affected users.

The flaw, tracked as CVE-2017-13872, allows an attacker to gain privileged access to a device running macOS High Sierra by logging in to the root account via the graphical user interface with the username "root" and any password. Apple has disabled the root account by default and when users attempt to log in to this account, the password they enter is set as its password. If the password field is left blank, there will be no password on the root account..

Link – http://www.securityweek.com/patch-macos-root-access-flaw-breaks-file-sharing

Triggered via malicious files, flaws in Cisco WebEx players can lead to RCE

Cisco has plugged six security holes in Cisco WebEx Network Recording Player for Advanced Recording Format (ARF) and WebEx Recording Format (WRF) files that could be exploited by remote attackers to execute malicious code on a target system…

Link – https://www.helpnetsecurity.com/2017/11/30/cisco-webex-flaws/

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