NH-ISAC Daily Security Intelligence Report – November 20, 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

Unprotected Pentagon Database Stored 1.8 Billion Internet Posts

Researchers have found an unprotected database storing 1.8 billion posts collected from social media services, news websites and forums by a contractor for the U.S. Department of Defense.

The data was discovered on September 6 by Chris Vickery, director of risk research at cyber resilience firm UpGuard, inside an AWS S3 storage bucket that was accessible to any user with an AWS account.

Link – http://www.securityweek.com/unprotected-pentagon-database-stored-18-billion-internet-posts

Confidential Information Of 9,500 Patients at the Medical College of Wisconsin Compromised

Confidential medical information or other personal data of 9,500 patients at the Medical College of Wisconsin was compromised by a targeted attack on the school's email system in July, the Medical College said Friday.

The compromised email accounts contained one or more of the following types of information: patients' names, home addresses, dates of birth, medical record numbers, health insurance information, dates of service, surgical information, diagnosis or medical condition, and treatment information

Link – http://www.jsonline.com/story/money/business/health-care/2017/11/17/confidential-information-9-500-patients-medical-college-wisconsin-compromised/876496001/

210 Government Websites Made Public Aadhaar Details, Says Database Body

New Delhi:More than 200 central and state government websites publicly displayed details such as names and addresses of some Aadhaar beneficiaries, the Unique Identification Authority of India has said.

In response to a Right to Information (RTI) query, the Aadhaar-issuing body said that it took note of the breach and got the data removed from those websites. It did not specify when the breach took place. The Aadhaar details were never made public from or by the UIDAI, it added.

Link – https://www.ndtv.com/business/aadhaar-data-breach-210-government-websites-displayed-private-data-says-uidai-1777380

CRIME and INCIDENT REPORT

Android Bug Lets Attackers Record Audio & Screen Activity on 3 of 4 Smartphones

Android smartphones running Lolipop, Marshmallow, and Nougat, are vulnerable to an attack that exploits the MediaProjection service to capture the user's screen and record system audio. Based on the market share of these distributions, around 77.5% of all Android devices are affected by this vulnerability…

Link – https://www.bleepingcomputer.com/news/security/android-bug-lets-attackers-record-audio-and-screen-activity-on-3-of-4-smartphones/

A Banking Trojan That Steals Gmail, Facebook, Twitter and Yahoo Password

The IT security researchers at Bitdefender have discovered a banking malware that apparently has been developed after keeping the dangerous Zeus trojan in mind. Dubbed

Terdot by researchers the trojan was first identified in June 2016. It is capable of injecting visited web pages with HTML code to conduct man-in-the-middle (MitM) attacks and steal banking data including credit card information…

Link – https://www.hackread.com/banking-trojan-steals-gmail-facebook-twitter-yahoo-password/

Mobile Malware Incidents Hit 100% of Businesses

Attempted malware infections against BYOD and corporate mobile devices are expected to continue to grow, new data shows. Every business with BYOD and corporate mobile device users across the globe has been exposed to mobile malware, with an average of 54 attempts per company played out within a 12-month period, according to a Check Point report released today.

The study, based on data collected from Check Point SandBlast Mobile deployments at 850 organizations, is the latest sign of growth in mobile malware incidents…

Link – https://www.darkreading.com/mobile/mobile-malware-incidents-hit-100--of-businesses/d/d-id/1330453

Fraudster Tied to 'The Dark Overlord' Jailed for 3 Years

A British man who was initially arrested on suspicion of hacking English socialite Pippa Middleton's iCloud account has been sentenced to serve a three-year prison sentence after he pleaded guilty to a number of unrelated fraud and blackmail offenses.

Nathan Wyatt, 36, of Wellingborough, England, appeared at Southwark Crown Court on Sept. 14, where he pleaded guilty to 20 counts of fraud by false representation, two counts of blackmail and one count of possession of an identity document with intent to deceive. His offenses included using malware to steal files from a British law firm then trying to ransom them back for €10,000 ($12,000) in bitcoins.

Link – https://www.healthcareinfosecurity.com/fraudster-tied-to-the-dark-overlord-jailed-for-3-years-a-10462

NEWS REPORT

Another Tor Browser Feature Makes It into Firefox: First-Party Isolation

Unbeknown to most users, Mozilla added a privacy-enhancing feature to the Firefox browser over the summer that can help users block online advertisers from tracking them across the Internet.

The feature is named First-Party Isolation (FPI) and was silently added to the Firefox browser in August, with the release of Firefox 55…

Link –

https://www.bleepingcomputer.com/news/software/another-tor-browser-feature-makes-it-into-firefox-first-party-isolation/

Kids' Smartwatches Banned in Germany Over Spying Concerns

German parents are being told to destroy smartwatches they have bought for their children after the country's telecoms regulator put a blanket ban in place to prevent sale of the devices, amid growing privacy concerns.

Jochen Homann, president of the Federal Network Agency, told BBC News that the so-called smartwatches, typically aimed at children between the ages of five and 12 years old, are classified as spying devices:

> "Via an app, parents can use such children's watches to listen unnoticed to the child's environment and they are to be regarded as an unauthorised transmitting system. According to our research, parents' watches are also used to listen to teachers in the classroom."

Link – https://www.welivesecurity.com/2017/11/20/kids-smartwatches-banned-germany-spying-concerns/

Why Hackers Reuse Malware

Software developers love to reuse code wherever possible, and hackers are no exception. While we often think of different malware strains as separate entities, the reality is that most new malware recycles large chunks of source code from existing malware with some changes and additions (possibly taken from other publically released vulnerabilities and tools)...

Link – https://www.helpnetsecurity.com/2017/11/20/hackers-reuse-malware/

VULNERABILITY REPORT

Wireless Security Lessons from the WPA2 Vulnerability

When I began writing about the wireless security lessons learned from the WPA2 vulnerability, I decided to start looking into my own level of exposure. My home network runs WPA2 on a combination cable modem/wireless router leased by my internet service provider (ISP), so I assumed the cable company might have sent me an alert. A search of previous emails turned up nothing.

I visited the ISP's website for instructions, but there were no alerts on the home page and no messages. I asked the automated assistant about the status of a patch and it responded with the chatbot equivalent of a blank stare. There were a couple of questions posted in the community forums, but no one from the ISP had responded.

Link – https://securityintelligence.com/wireless-security-lessons-from-the-wpa2-vulnerability/

GitHub Warns Developers When Using Vulnerable Libraries

Code hosting service GitHub now warns developers if certain software libraries used by their projects contain any known vulnerabilities and provides advice on how to address the issue.

GitHub recently introduced the Dependency Graph, a feature in the Insights section that lists the libraries used by a project. The feature currently supports JavaScript and Ruby, and the company plans on adding support for Python next year…

Link – http://www.securityweek.com/github-warns-developers-when-using-vulnerable-libraries

Moxa NPort Devices Vulnerable to Remote Attacks

Firmware updates released by Moxa for some of its NPort serial device servers patch several high severity vulnerabilities that can be exploited remotely. These types of devices were targeted in the 2015 attack on Ukraine's energy sector.

According to an advisory published by ICS-CERT, the flaws affect NPort 5110 versions 2.2, 2.4, 2.6 and 2.7, NPort 5130 version 3.7 and prior, and NPort 5150 version 3.7 and

prior. The security holes have been patched with the release of version 2.9 for NPort 5110 and version 3.8 for NPort 5130 and 5150…

Link – http://www.securityweek.com/moxa-nport-devices-vulnerable-remote-attacks

F5 BIG-IP patched for DROWN crypto vulnerability (CVE-2017-6168)

If you're an F5 BIG-IP sysadmin, get patching: there's a bug in the company's RSA implementation that can give an attacker access to encrypted messages.

As the CVE assignment stated: “a virtual server configured with a Client SSL profile may be vulnerable to an Adaptive Chosen Ciphertext attack (AKA Bleichenbacher attack) against RSA, which when exploited, may result in plaintext recovery of encrypted messages and/or a Man-in-the-middle (MiTM) attack, despite the attacker not having gained access to the server's private key itself.”

Link – http://www.theregister.co.uk/2017/11/20/f5_crypto_weakness/

_____

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