NH-ISAC Daily Security Intelligence Report – November 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

Uber Paid Hackers to Delete Stolen Data on 57 Million People

Hackers stole the personal data of 57 million customers and drivers from Uber Technologies Inc., a massive breach that the company concealed for more than a year. This week, the ride-hailing firm ousted its chief security officer and one of his deputies for their roles in keeping the hack under wraps, which included a $100,000 payment to the attackers.

Compromised data from the October 2016 attack included names, email addresses and phone numbers of 50 million Uber riders around the world, the company told Bloomberg on Tuesday. The personal information of about 7 million drivers was accessed as well, including some 600,000 U.S. driver's license numbers. No Social Security numbers, credit card information, trip location details or other data were taken, Uber said…

Link – https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

Should Uber Users be Worried About Data Hack?

The theft of the personal data of 57 million Uber riders and drivers highlights how vulnerable we make ourselves when we install apps on our mobile phones and tablet computers..

Link – http://www.securityweek.com/should-uber-users-be-worried-about-data-hack

CRIME and INCIDENT REPORT

Fund Targets Victims Scammed Via Western Union

If you, a friend or loved one lost money in a scam involving Western Union, some or all of those funds may be recoverable thanks to a more than half-billion dollar program set up by the U.S. Federal Trade Commission.

In January 2017, Englewood, Colo.-based Western Union settled a case with the FTC and the Department of Justice wherein it admitted to multiple criminal violations, including willfully failing to maintain an effective anti-money laundering program and aiding and abetting wire fraud. As part of the settlement, the global money transfer business agreed to forfeit $586 million…

Link – https://krebsonsecurity.com/2017/11/fund-targets-victims-scammed-via-western-union/

Holiday Season Scams: Fake Deals, Fake Stores, Fake Opportunities

Black Friday is widely regarded as the beginning of the US (and increasingly global) Christmas shopping season. Cyber Monday, which comes three days later, was created to persuade people to shop online more. They are a huge boon for retailers, both online and offline, but also for cybercriminals…

Link – https://www.helpnetsecurity.com/2017/11/22/holiday-season-scams/

'Advanced' Cyber Attack Targets Saudi Arabia

Saudi authorities said Monday they had detected an "advanced" cyber attack targeting the kingdom, in a fresh attempt by hackers to disrupt government computers.

The government's National Cyber Security Centre said the attack involved the use of "Powershell", but it did not comment on the source of the attack or which government bodies were targeted.

Link – http://www.securityweek.com/advanced-cyber-attack-targets-saudi-arabia

qkG Filecoder: Self-Replicating, Document-Encrypting Ransomware

We encountered a few interesting samples of a file-encoding ransomware variant implemented entirely in VBA macros called qkG (detected by Trend Micro as RANSOM_CRYPTOQKG.A). It's a classic macro malware infecting Microsoft Word's Normal template (normal.dot template) upon which all new, blank Word documents are based…

Link – http://blog.trendmicro.com/trendlabs-security-intelligence/qkg-filecoder-self-replicating-document-encrypting-ransomware/

Additional Link - https://www.bleepingcomputer.com/news/security/qkg-ransomware-encrypts-only-word-documents-hides-and-spreads-via-macros/

NEWS REPORT

A CISO Sizes Up Healthcare Security Threats for 2018

In the year ahead, cyber threats to the healthcare sector will continue to evolve from attacks primarily involving the theft of health data to assaults aimed at disrupting organizations' operations, predicts Sean Murphy, CISO of health insurer Premera Blue Cross.

"I see more disruption in the industry around cybersecurity - it's more than data exfiltration as a concern. I see more ransomware attacks and denial-of-service attacks ... and more of an effort to disrupt the system, the critical infrastructure even more so than trying to get at the data," he says in an interview with Information Security Media Group…

Link – https://www.healthcareinfosecurity.com/interviews/ciso-sizes-up-healthcare-security-threats-for-2018-i-3769

House Committee Urges HHS Action on Medical Device Risks

A House committee is urging the Department of Health and Human Services to act soon on a recommendation made by its cybersecurity task force earlier this year: Develop a description of the the cyber risks of all components of medical devices and other

healthcare technologies. The move is seen as an important initial step toward ensuring the cybersecurity of the technologies…

Link – https://www.databreachtoday.com/house-committee-urges-hhs-action-on-medical-device-risks-a-10466

VULNERABILITY REPORT

Bulletin (SB17-324) Vulnerability Summary for the Week of November 13, 2017

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard…

Link – https://www.us-cert.gov/ncas/bulletins/SB17-324

More Industrial Products at Risk of KRACK Attacks

An increasing number of vendors have warned customers over the past weeks that their industrial networking products are vulnerable to the recently disclosed Wi-Fi attack method known as KRACK.

The KRACK (Key Reinstallation Attack) flaws affect the WPA and WPA2 protocols and they allow a hacker within range of the targeted device to launch a man-in-the-middle (MitM) attack and decrypt or inject data. A total of ten CVE identifiers have been assigned to these security bugs…

Link – http://www.securityweek.com/more-industrial-products-risk-krack-attacks

HP to Release Patch This Week for Printer Security Bugs

HP said it would release firmware patches later this week for several security bugs reported to the company by various cyber-security experts. The firmware patches address a slew of bugs, among which the most severe is a remote code execution (RCE) flaw discovered and reported by Stephen Breen of NTT Security.

The RCE bug (CVE-2017-2750) affects HP's top-of-the-line enterprise printer series such as LaserJet and PageWide, but also some OfficeJet and ScanJet models. A full list of affected products is available in the HP security advisory…

Link – https://www.bleepingcomputer.com/news/security/hp-to-release-patch-this-week-for-printer-security-bugs/

Symantec updates Management console product

Symantec released an update to its Management Console product to patch a vulnerability that can leave users susceptible to a directory traversal exploit.

The exploit can be leveraged when there is insufficient security validation / sanitization of user-supplied input file names, such that characters representing "traverse to parent directory" are passed through to the file APIs, according to a Nov. 20 security update...

Link – https://www.scmagazine.com/symantec-security-updates-management-console-directory-traversal/article/708985/

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