NH-ISAC Daily Security Intelligence Report – November 29, 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

Classified U.S. Army Data Found on Unprotected Server

Tens of gigabytes of files apparently belonging to the United States Army Intelligence and Security Command (INSCOM), including classified information, were stored in an unprotected AWS S3 bucket, cyber resilience firm UpGuard reported on Tuesday.

According to the company, its director of cyber risk research, Chris Vickery, discovered the data on an AWS subdomain named "inscom" in late September.Fort Belvoir, Virginia-based INSCOM is an intelligence command operated by both the U.S. Army and the National Security Agency (NSA)…

Link – http://www.securityweek.com/classified-us-army-data-found-unprotected-server

Cottage Health Fined $2M By Calif. AG for Two Breaches

In the first breach, which occurred in 2013, an unencrypted server without basic security like password protection and firewalls made the records of 50,000 patients accessible online. The second, in 2015, resulted in the records of 4,596 patients being accessible online for almost two weeks…

Link – https://www.scmagazine.com/cottage-health-fined-2m-by-calif-ag-for-two-breaches/article/710165/

Data Breaches Within the Retail and Hospitality Industries

The holiday season is upon us, with consumers hastily laying travel plans between time spent browsing for gifts for loved ones. During this season, a few also remember that major retail breaches have long-lasting and far-reaching effects with settlements dragging into the years and occasionally costing companies up to billions of dollars.

More recently, the public has become acquainted with point of sale (POS) breaches impacting large hotel and restaurant chains, sometimes compromising millions of consumer payment cards. Risking accusations of grinchlike behavior, BitSight researchers turned a discerning eye on the Retail and Hospitality industries to gain an understanding of their security performance…

Link – https://www.bitsighttech.com/blog/data-breaches-within-retail-and-hospitality-industries

UK Shipping Company Clarksons Confirms Breach

British shipping company Clarkson has 'fessed up to a data breach, saying a miscreant has accessed its systems and the public should expect some of it to be made public.

Clarkson PLC declined to answer The Register's inquiry about how much data had been compromised or whether it belonged to customers and merely referred us to the company's announcement (PDF) for any additional information...

Link – http://www.theregister.co.uk/2017/11/29/clarksons_got_some_data_stolen/

CRIME and INCIDENT REPORT

OpenEMR Flaw Leaves Millions Of Medical Records Exposed To Attackers

A vulnerability in the free, open source electronic medical record and medical practice management software OpenEMR can be exploited to steal patients’ medical records and other personally identifiable information, Risk Based Security warns.

OpenEMR is used all over the world. 2012 estimates put the number of US installations (physician offices and other small healthcare facilities) over 5,000, and global numbers

over 15,000. Among the users are the International Planned Parenthood Federation and the Peace Corps.

The flaw was discovered by company researchers while reviewing previously discovered security issues in OpenEMR, and responsibly disclosed to the developers. The fix has been pushed out in early November, in the 6th patch for OpenEMR v5.0.0…

Link – https://www.helpnetsecurity.com/2017/11/29/openemr-flaw-medical-records-exposed/

IoT, Android Botnets Emerge as Powerful DDoS Tools: Akamai

Distributed denial of service (DDoS) attacks observed during the third quarter employed familiar vectors, but a newcomer that made headlines for abusing Android devices is expected to evolve, a new Akamai report suggests.

This new threat is the Android-based WireX botnet, which managed to infect 150,000 devices within a matter of weeks, the company's Third Quarter, 2017 State of the Internet / Security Report (PDF), points out. Distributed through legitimate-looking infected apps in Google Play, the botnet managed to spread fast and might have grown even bigger if it wasn't for the joint effort of several tech companies...

Link – http://www.securityweek.com/iot-android-botnets-emerge-powerful-ddos-tools-akamai

NEWS REPORT

Data Breaches Hurt Loyalty

A majority (70%) of consumers would stop doing business with a company if it experienced a data breach, according to a survey of more than 10,000 consumers worldwide conducted by Vanson Bourne. In addition, seven in ten consumers (69%) feel businesses don't take the security of customer data very seriously.

Despite these concerns, consumers are failing to adequately secure themselves, with 56% still using the same password for multiple online accounts. Even when businesses offer robust security solutions, such as two-factor authentication, 41% of consumers admit to

not using the technology to secure social media accounts, leaving them vulnerable to data breaches….

Link – https://www.helpnetsecurity.com/2017/11/28/data-breaches-hurt-loyalty/

All Aboard! Applying the Security Immune System Approach to the Railroad Industry

What happens when cybercriminals target critical infrastructure such as railroads? The good news is that this type of attack is difficult to pull off — but certainly not impossible. Such an incident would most likely stop the train, resulting in financial loss and reputational damage, but nothing more than what we've already seen when cyberattacks hit organizations in other industries, such as financial services and health care...

Link – https://securityintelligence.com/all-aboard-applying-the-security-immune-system-approach-to-the-railroad-industry/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+SecurityIntelligence+%28Security+Intelligence%29

VULNERABILITY REPORT

Critical Apple Login Bug Puts Macos High Sierra Systems at Risk

A major bug in Apple's macOS gives anyone with physical access to a computer running the latest version of the High Sierra operating system admin access simply by putting "root" in the user name field.

The bug was publicized Tuesday by developer Lemi Orhan Ergin, founder of Software Craftsmanship Turkey, via Twitter. His tweet he simply stated…..

Link – https://threatpost.com/critical-apple-login-bug-puts-macos-high-sierra-systems-at-risk/129028/

Additional Link - https://www.forbes.com/sites/thomasbrewster/2017/11/28/apple-macos-high-sierra-guilty-of-really-stupid-password-bug/#5605141611d5

'Dumb' MacOS Bug Allows Anyone to Get Admin Privileges Without a Password

A new bug on MacOS allows any user to log in as the full-privilege admin user “root” just by entering root as login and pressing enter…

Link – https://motherboard.vice.com/en_us/article/3kvxg5/apple-mac-bug-root-admin-without-password

_____

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