NH-ISAC
NATIONAL HEALTH - ISAC

NH-ISAC Daily Security Intelligence Report – November 28, 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

Bulletproof 360 Website Was Hacked. Personal and Financial Data Exposed

The firm Bulletproof 360, Inc. manufactures coffee and tea products, and dietary supplements for upgrading mind and body. It serves customers online, as well as through stores in the United States and internationally.

The company specializing in butter-infused coffee confirmed that the attackers injected malicious code into its website stealing payment card details for months.

Bulletproof 360 Inc. revealed that from May 20 to October 19, except on October 14, crooks have stolen personal and financial information customers entered on its website…

Link – http://securityaffairs.co/wordpress/66100/data-breach/bulletproof-360-hacked.html

Black Box, Red Disk: How Top Secret NSA and Army Data Leaked Online

In the wake of a string of data exposures originating from Pentagon intelligence-gathering agencies, the most recent of which revealed the workings of a massive, worldwide social media surveillance program, the UpGuard Cyber Risk Team can now disclose another. Critical data belonging to the United States Army Intelligence and

Security Command (INSCOM), a joint US Army and National Security Agency (NSA) Defense Department command tasked with gathering intelligence for US military and political leaders, leaked onto the public internet, exposing internal data and virtual systems used for classified communications to anyone with an internet connection.

With a middling CSTAR cyber risk score of 589 out of a maximum of 950, INSCOM’s web presence provides troubling indications of gaps in their cybersecurity - exemplified by the presence of classified data within this publicly accessible data repository…

Link – https://www.upguard.com/breaches/cloud-leak-inscom

$2M Settlement Reached in Cottage Health Data Breach Case

Cottage Health System recently reached a $2 million settlement with the California Attorney General’s office after two separate health data breach incidents that took place in 2013 and 2015. In total, more than 50,000 patients had their medical information publicly available from the data breaches.

“When patients go to a hospital to seek medical care, the last thing they should have to worry about is having their personal medical information exposed,” Attorney General Xavier Becerra said in a statement. “The law requires health care providers to protect patients' privacy. On both of these counts, Cottage Health failed.” …

Link – https://healthitsecurity.com/news/2m-settlement-reached-in-cottage-health-data-breach-case

CRIME and INCIDENT REPORT

Cobalt Hackers Exploit 17-Year-Old Vulnerability in Microsoft Office The notorious Cobalt hacking group has started to exploit a 17-year-old vulnerability in Microsoft Office that was addressed earlier this month, security researchers claim.

Fixed in Microsoft's November 2017 Patch Tuesday security updates and found by Embedi security researchers in the Microsoft Equation Editor (EQNEDT32.EXE), the bug is identified as CVE-2017-11882.

The issue was found in a component that remained unchanged in Microsoft's Office suite since November 9, 2000, and appears to have been patched manually instead of being corrected directly in the source code, an analysis 0patch published last week reveals…

Link – http://www.securityweek.com/cobalt-hackers-exploit-17-year-old-vulnerability-microsoft-office

Fake Symantec Site Spreads Osx.Proton Password Stealer

Researchers said the registration information on the domain, at first glance, appears to be legit because it uses the same name and address as the real Symantec site, but the email address used to register the domain is a dead giveaway with a legitimate SSL certificate that is issued by Comodo rather than Symantec's own certificate authority...

Link – https://www.scmagazine.com/osxproton-spread-via-fake-symantec-blog/article/709695/

Google Discovers New Tizi Android Spyware

Google's security team discovered a new strain of Android malware, named Tizi, and which has been used primarily to target users in African countries. Categorized as spyware, Google says Tizi can carry out a wide range of operations, but most focus on social media apps and activity...

Link – https://www.bleepingcomputer.com/news/security/google-discovers-new-tizi-android-spyware/

Ransomware Attack Involving Scarab Malware Sends Over 12M Emails in 6 Hours

Security researchers at the Austin based Anti-virus software firm Forcepoint have discovered a massive spam ransomware campaign in which the Scarab malware destroys all your files if you don't pay the ransom, which is asked in Bitcoin...

Link – https://www.hackread.com/ransomware-attack-scarab-malware-sends-12m-emails-in-6-hours/

A look at the Top Seven Ransomware Attacks In The Past Decade

In part one of this series, we discussed exactly what ransomware is, including the effects of and motives behind different types of attacks. In this second article, I'll look at the top seven ransomware attacks within the past decade and how they managed to infiltrate networks around the word....

Link – https://www.helpnetsecurity.com/2017/11/28/top-seven-ransomware-attacks/

NEWS REPORT

Agari: Healthcare DMARC Adoption Report (PDF)

98% of top healthcare organizations have left customers and businesses partners unprotected from Phishing. At the same time healthcare is the top sector cyber criminals target.

As an answer to this, the NH-ISAC has asked its members to take a pledge to adopt DMARC in 2018. The Department of Homeland Security (DHS) also issued a binding directive mandating that federal agencies adopt DMARC and implement a policy of p=reject by Oct, 2018...

Link – https://www.agari.com/healthcare-dmarc-adoption-report/

The Vulnerable Internet of Things

Numerous smart watches, coffee makers, vacuum cleaners, and even cars are now part of what is called the Internet of Things (IoT), a catch-all term for the connected devices we're growing to love and rely on. At least in theory, the IoT should make our lives simpler and more convenient; hence its rising popularity...

Link – https://usa.kaspersky.com/blog/internet-of-vulnerabilities/14151/

VULNERABILITY REPORT

Bulletin (SB17-331) Vulnerability Summary for the Week of November 20, 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/SB17-331

University Hospital Patient Information Was Potentially Vulnerable to Hackers

A Maroon investigation found that weaknesses in the University's network could allow hackers to steal sensitive information from networked printers, as well as access and, in some cases, control cameras and other connected devices…

Link- https://www.chicagomaroon.com/article/2017/11/28/university-chicago-hospital-patient-information-vulnerable/

No Key Required: How Thieves Use Relay Boxes t0 Steal Cars

Getting in your car and starting it without having to pull the key out of your pocket is one of the small conveniences that come with many modern vehicles. Unfortunately, the capability is also convenient for car thieves.

As demonstrated in the above video, made available by the West Midlands Police, criminals equipped with relay boxes can unlock cars and drive away with them in under a minute…

Link – https://www.helpnetsecurity.com/2017/11/28/use-relay-boxes-steal-cars/

PowerDNS Patches Five Security Holes In Widely Used Nameserver Software

PowerDNS, the company behing the popular open source DNS software of the same name, has pushed out security updates and patches for its Authoritative Server and Recursor offerings that, among other things, fix five security vulnerabilities of note…

Link – https://www.helpnetsecurity.com/2017/11/28/powerdns-patches-five-security-holes/

Image Removal Vulnerability in Facebook Polling Feature

A security researcher found a way to delete any picture on Facebook, irrespective of whether it's public or private, by cunning use of polls.

Pouya Daribi was digging around in the software used by Facebook users to set up quick opinion polls on their profile pages. When creating these informal surveys, the social media addicts can select photos to appear alongside the questions, and the ID codes for these pictures are embedded in the HTML form submitted to Facebook's servers…

Link – http://www.theregister.co.uk/2017/11/27/facebook_flaw_kills_any_picture/

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