NH-ISAC Daily Security Intelligence Report – November 27, 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

Imgur Confirms Breach, 1.7 Million Users Affected

Popular image hosting website Imgur has announced on Friday that hackers stole usernames and passwords of 1.7 million of its users. The breach dates back to 2014, when Imgur still encrypted the stored passwords with the SHA-256 algorithm, which has since been found too weak to withstand brute forcing.

The company made sure to note that the compromised account information included only email addresses and passwords, as they've never asked for users' real names, addresses, phone numbers, or other personally-identifying information…

Link – https://www.helpnetsecurity.com/2017/11/27/imgur-breach/

Name+DOB+SSN=FAFSA Data Gold Mine

KrebsOnSecurity has sought to call attention to online services which expose sensitive consumer data if the user knows a handful of static details about a person that are broadly for sale in the cybercrime underground, such as name, date of birth, and Social Security Number. Perhaps the most eye-opening example of this is on display at fafsa.ed.gov, the

Web site set up by the U.S. Department of Education for anyone interested in applying for federal student financial aid.

Short for the Free Application for Federal Student Aid, FAFSA is an extremely lengthy and detailed form required at all colleges that accept and award federal aid to students…

Link – https://krebsonsecurity.com/2017/11/namedobssnfafsa-data-gold-mine/

Data Breach Hits Department of Social Services Credit Card System

The Department of Social Services has written to 8,500 current and former employees warning them their personal data held by a contractor has been breached.

In letters sent in early November the department alerted the employees to "a data compromise relating to staff profiles within the department's credit card management system prior to 2016"…

Link – https://www.theguardian.com/technology/2017/nov/24/data-breach-hits-department-of-social-services-credit-card-system

CRIME and INCIDENT REPORT

Necurs Returns with New Scarab Ransomware Campaign

The world's largest spam botnet, Necurs, is delivering a new version of the Scarab ransomware. The campaign started at 07:30 UTC on Thanksgiving Day. By 13:30 UTC, security firm Forcepoint had already blocked more than 12.5 million Necurs emails.

The new campaign was also noted by F-Secure. "This morning at 9AM (Helsinki time, UTC +2) we observed the start of a campaign with malicious .vbs script downloaders compressed with 7zip," blogged researcher Paivi Tynninen on Thursday…

Link – http://www.securityweek.com/necurs-returns-new-scarab-ransomware-campaign

Newly Published Exploit Code Used to Spread Marai Variant

Qihoo 360 Netlab researchers reported on Friday that they are tracking an uptick in botnet activity associated with a variant of Mirai. Targeted are ports 23 and 2323 on

internet-connected devices made by ZyXEL Communications that are using default admin/CentryL1nk and admin/QwestM0dem telnet credentials.

"About 60 hours ago, since 2017-11-22 11:00, we noticed big upticks on port 2323 and 23 scan traffic, with almost 100k unique scanner IP came from Argentina," wrote researchers in a blog post on Friday. "After investigation, we are quite confident to tell this is a new Mirai variant."…

Link – https://threatpost.com/newly-published-exploit-code-used-to-spread-marai-variant/128998/

Additional link - https://www.bleepingcomputer.com/news/security/mirai-activity-picks-up-once-more-after-publication-of-poc-exploit-code/

Golden SAML Attack Lets Attackers Forge Authentication to Cloud Apps

A new technique called "Golden SAML" lets attackers forge authentication requests and access the cloud-based apps of companies that use SAML-compatible domain controllers (DCs) for the authentication of users against cloud services...

Link – https://www.bleepingcomputer.com/news/security/golden-saml-attack-lets-attackers-forge-authentication-to-cloud-apps/

A Verge specific node wallets hacked, crooks stole $655,000 from CoinPouch XVG Verge wallets

CoinPouch publicly disclosed the hack of a Verge specific node wallets and the theft if $655,000 from its XVG Verge wallets.

A mystery surrounds the recent hack of CoinPouch wallet app, users lost over $655,000 worth of Verge cryptocurrency. On Tuesday, the maintainers of the CoinPouch multi-currency wallet app published a statement that disclosed a security breach that affected its users who stored Verge currency in their wallets...

Link – http://securityaffairs.co/wordpress/66033/hacking/coinpouch-security-breach-verge.html

NEWS REPORT

Cybercrime Laws: What Internet Fraud Victims Need to Know

As the Internet continues to be an important part of our lives, it also becomes a more dangerous avenue for cybercrime. The risk increases as the massive online community's use of the Internet becomes more rampant. And despite the public being aware of cybersecurity issues, anonymous online criminals are able find more victims and creative ways to commit Internet fraud with the use of Internet services or software programs with web access.

Cybercrime has become a leading concern in the legal community as criminals continue to spread troublesome viruses, access private business/financial information, commit cyber espionage, spread different variations of malware, execute property and identity theft, spread malicious online content, and invade computer system processes that may threaten or cause danger to the government or its citizens...

Link – https://www.tripwire.com/state-of-security/security-awareness/cybercrime-laws-what-internet-fraud-victims-need-to-know/

US officials not told Russia tried to target personal emails

The FBI failed to notify scores of U.S. officials that Russian hackers were trying to break into their personal Gmail accounts despite having evidence for at least a year that the targets were in the Kremlin's crosshairs, The Associated Press has found.

Nearly 80 interviews with Americans targeted by Fancy Bear, a Russian government-aligned cyberespionage group, turned up only two cases in which the FBI had provided a heads-up. Even senior policymakers discovered they were targets only when the AP told them, a situation some described as bizarre and dispiriting...

Link – https://www.militarytimes.com/news/pentagon-congress/2017/11/26/us-officials-not-told-russia-tried-to-target-personal-emails/

Upcoming Firefox Feature Could Warn Users When Their Password Gets Stolen

Mozilla is piloting a program with the aim to introduce a feature in Firefox that will notify users when their credentials may have been leaked or stolen in a data breach.

In a GitHub repo set up for the initiative, Bengaluru, India-based Mozilla developer Nihanth Subramanya explains the reasons behind the “Breach Alerts Prototype” and how his company would like to tackle the issue. Data breaches have become common, and everything from email addresses and passwords to credit card details and personal information can be leaked or stolen by bad actors, Subramanya argues...

Link – https://hotforsecurity.bitdefender.com/blog/upcoming-firefox-feature-could-warn-users-when-their-password-gets-stolen-19275.html

Android Commercial Spyware

There’s certainly no shortage of commercial spying apps for Android, with most positioned as parental control tools. In reality, however, these apps barely differ from spyware, with the exception perhaps of the installation method. There’s no need to even resort to Tor Browser or other darknet activity either – all you need to do is type something like “android spy app” into Google...

Link – https://securelist.com/android-commercial-spyware/83098/

Facebook Tool Will Reveal If You Were Fooled By Russian Propaganda

Facebook said on Wednesday that it’s building a portal that will let some users see if they liked or followed Russian propaganda from Internet Research Agency Facebook Pages or Instagram accounts between January 2015 and August 2017...

Link – https://nakedsecurity.sophos.com/2017/11/27/facebook-tool-will-reveal-if-you-were-fooled-by-russian-propaganda/

VULNERABILITY REPORT

systemd Vulnerability Leads to Denial of Service on Linux

Many Linux distributions are at risk due to a recently disclosed flaw in systemd: a flaw in its DNS resolver could cause a denial-of-service attack on vulnerable systems. The vulnerability is exploited by having the vulnerable system send a DNS query to a DNS server controlled by the attackers. The DNS server would then return a specially crafted

query, causing systemd to enter an infinite loop that pins the system's CPU usage to 100%. This vulnerability was assigned CVE-2017-15908…

Link – http://blog.trendmicro.com/trendlabs-security-intelligence/systemd-vulnerability-leads-to-denial-of-service-on-linux/

Unix Mailer Exim Is Affected by Rce, Dos Vulnerabilities. Apply The Workaround Asap

Exim is a message transfer agent (MTA) developed at the University of Cambridge for use on Unix systems connected to the Internet, it is the most popular MTA on the Internet. The Internet mail message transfer agent warned of flaws through the public bug tracker, an unfortunate choice to disclose it because the notice could be ignored...

Link – http://securityaffairs.co/wordpress/66043/hacking/exim-unix-mailer-flaws.html

You need to patch your Samba installation as soon as possible

The major Linux distributions (Red Hat, Ubuntu, Debian and others) rolled out security patches for a use-after-free error, tracked as CVE-2017-14746, affecting all versions of SAMBA since 4.0.

Administrations have to apply the fixes to their distributions, another possibility consists in turning off SAMBA 1, and operation that could hide some difficulties. According to the project's advisory, an attacker can use a malicious SMB1 request to control the contents of heap memory via a deallocated heap pointer…

Link – http://securityaffairs.co/wordpress/65923/hacking/samba-flaws.html

Symantec Patches Certificate Spoofing Flaw in Install Norton Product

Symantec patched a certificate spoofing vulnerability in its Install Norton Security product that occurs when downloading Norton for Mac

The exploit was caused by the CVE-2017-15528 vulnerability which had a Low Severity Rating but could allow an attacker to spoof a target site or carry out man-in-the-middle attacks, according to a Nov. 21 security advisory…

Link – https://www.scmagazine.com/symantec-patches-install-norton-security-certificate-spoof-vulnerability/article/709185/

_____

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