NH-ISAC
NATIONAL HEALTH - ISAC

NH-ISAC Daily Security Intelligence Report – November 16, 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

Catholic Charities Healthcare Cyberattack Impacts 4.6K

Catholic Charities announced that its Glens Falls office experienced a healthcare cyberattack on a server containing information of approximately 4,600 current and former clients and several employees.

Unauthorized software was discovered on the server during compute security upgrades, the organization said in its online statement. The incident was discovered on August 30, 2017, with a forensic analysis determining that the server access may date back to 2015.

Link – https://healthitsecurity.com/news/catholic-charities-healthcare-cyberattack-impacts-4.6k

CRIME and INCIDENT REPORT

Ransomware Targets J. Sterling Morton High School Students With Fake Survey

An in-development ransomware named J. Sterling Ransomware has been discovered that targets the high school students of the J. Sterling Morton school district in Cicero, Illinois by pretending to be a student survey. While this ransomware currently does not encrypt files, it shows how a developer can make an effective & targeted ransomware attack.

When run, this ransomware will display a screen called the "J. Sterling Student Survey", which prompts the student to login into the survey and select their school grade. In order to make the survey look legitimate, the developer included the school's logos and slogans. Though the user interface is designed poorly, it could easily trick someone to interact with it.

Link – https://www.bleepingcomputer.com/news/security/ransomware-targets-j-sterling-morton-high-school-students-with-fake-survey/

The Long Tail of Phishing Attacks

Targeted phishing has become the single most effective attack type in the world today. Phishing attacks have been the root cause of the majority of the large-scale data breaches that compromised the sensitive information of millions of individuals and extracted financial gains from some of the world's largest companies.

In March, a spear-phishing scam that used the cover of the tax season and W-2 filings tricked more than 120,000 people into sharing their personal data. Just one month later, Google and Facebook were the victims of an elaborate $100 million phishing attack when employees at both companies unwittingly sent money to overseas bank accounts. In the month following, a highly sophisticated Google Docs attack compromised over a million Gmail accounts in just one hour.

Link – https://www.helpnetsecurity.com/2017/11/16/long-tail-phishing-attacks/

'Reaper': The Professional Bot Herder's Thingbot

This isn't your mama's botnet. This is a proper botnet. If you were the world's best Internet of Things botnet builder and you wanted to show the world how well-crafted an IoT botnet could be, Reaper is what you'd build. It hasn't been seen attacking anyone yet, and that is part of its charm.

The interesting aspect of Reaper is not its current size, but its engineering, and therefore its potential. But from a pure research perspective, we're interested in how Reaper is spreading. Instead of targeting weak auth like a common thingbot, Reaper weaponizes nine (and counting) different IoT vulnerabilities. Consequently, we think the current media focus on “the numbers,” instead of the method, is a tad myopic…

Link – https://www.darkreading.com/partner-perspectives/f5/reaper-the-professional-bot-herders-thingbot/a/d-id/1330439

McAfee's own anti-hacking service exposed users to banking malware

Security firm McAfee has blocked access to malware that appeared to be sent from the company's own network.

The malware was hosted on a third-party website but was shared via a domain associated with McAfee ClickProtect, an email protection service that the company touts as able to "protect your business from hacking." The service is meant to protect against phishing attacks, malware from links in emails, and prevent users from visiting sites that are known to be high risk…

Link – http://www.zdnet.com/article/mcafees-own-anti-hacking-service-exposed-users-to-banking-malware/

Three more Android malware families invade Google Play Store

Collectively downloaded millions of times, 158 fake Android applications containing mobile malware were recently found smuggled into the Google Play Store, according to a trio of separate research reports that were published within days of each other.

Researchers at McAfee did the heaviest lifting, spotting Grobas, a program that pushes unwanted apps, in 144 trojanized apps. Meanwhile, analysts at ESET identified eight apps carrying a multi-stage downloader dubbed Android/TrojanDropper.Agent.BKY, and experts at Malwarebytes found six apps sabotaged with Android/Trojan.AsiaHitGroup, which contains hidden adware and attempts to download an SMS trojan.

Link – https://www.scmagazine.com/three-more-android-malware-families-invade-google-play-store/article/707693/

Spam Bots Bombards Victims with Star Wars Quotes and Links to Gambling Apps

In one of the weirdest things you'll hear today, a spam botnet has been randomly selecting text from a Star Wars novel and sending it to victims, alongside with download links to online gambling apps.

This was not the work of a regular email spam botnet that uses infected computers or hacked sites. Instead, this is a botnet that abuses social media sharing widgets.

While most users think of Twitter and Facebook sharing when thinking of social widgets, most of these type of services also come with a feature named "email-link-to-a-friend."

Link – https://www.bleepingcomputer.com/news/security/spam-bots-bombards-victims-with-star-wars-quotes-and-links-to-gambling-apps/

VULNERABILITY REPORT

Critical Vulnerabilities Patched in Apache CouchDB

An update released last week for Apache CouchDB patched critical vulnerabilities that could have been exploited by malicious actors for privilege escalation and code execution on a significant number of installations.

CouchDB is a document-oriented open source database management system and it’s currently the 28th most popular out of the more than 300 systems tracked by DB-Engines. One of the projects using CouchDB is npm, a package manager for JavaScript and the world's largest software registry.

Link – http://www.securityweek.com/critical-vulnerabilities-patched-apache-couchdb

Critical Flaw Exposes Cisco Collaboration Products to Hacking

A dozen Cisco collaboration products using the company’s Voice Operating System (VOS) are exposed to remote hacker attacks due to a critical vulnerability, users were warned on Wednesday.

According to Cisco, the flaw affects an upgrade mechanism of products based on VOS. A remote, unauthenticated attacker can exploit the security hole, tracked as CVE-2017-12337, to gain access to vulnerable devices with root privileges…

Link – http://www.securityweek.com/critical-flaw-exposes-cisco-collaboration-products-hacking

Amazon, Google Patch Bluetooth Vuln Vaccines in Echo And Home Products

Updated Amazon and Google have automatically patched people's Echo and Home AI assistant devices, respectively, to defend against recently discovered Bluetooth-related security vulnerabilities.

BlueBorne – described in the video below – is the collective name for eight exploitable flaws found in Bluetooth stacks used by major hardware vendors. The eight blunders affect an estimated 5.3 billion Android, iOS, Linux, and Windows devices, California-based IoT security biz Armis disclosed in September. Amazon Echo and Google Home were also vulnerable, but this info was held back pending the development of patches now pushed to endpoints.

Link – http://www.theregister.co.uk/2017/11/15/amazon_echo_blueborne/

Formidable Forms plugin vulnerabilities expose WordPress sites attacks

A researcher from Finland-based company Klikki Oy has discovered several vulnerabilities in the Formidable Forms plugin that expose websites to attacks.

The researcher Jouko Pynnönen from Finland-based company Klikki Oy has discovered several vulnerabilities in the Formidable Forms plugin the expose websites to attacks. The Formidable Forms plugin allows users to easily create contact pages, polls and surveys, and many other kinds of forms, it has more than 200,000 active installs…

Link – http://securityaffairs.co/wordpress/65617/hacking/formidable-forms-plugin-flaws.html

---

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