NH-ISAC Daily Security Intelligence Report – November 17, 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

Drone Maker DJI Left Its Private SSL, Firmware Keys Open on Github for Years

Chinese drone maker DJI left the private key for its dot-com's HTTPS certificate exposed on GitHub for up to four years, according to a researcher who gave up with the biz's bug bounty process.

By leaking the wildcard cert key, which covers *.dji.com, DJI gave miscreants the information needed to create spoof instances of the manufacturer's website with the correct HTTPS certificate, and silently redirect victims to the malicious forgeries and downloads via standard man-in-the-middle attacks. Hackers could also use the key to decrypt and tamper with intercepted network traffic to and from its web servers.

Link – http://www.theregister.co.uk/2017/11/16/dji_private_keys_left_github/

CRIME and INCIDENT REPORT

Lloyds' Avios Reward credit cardholders report fraudulent activity

Thousands of Lloyds Avios Rewards American Express credit card customers have been targeted by fraudsters, the bank has admitted. Reports first emerged on air miles site Head for Points, where readers asked if the credit card had suffered a major data breach.

One said: "About a week ago my wife's Lloyds Avios Amex card was used fraudulently by someone over in New York for a few different things so we called Lloyds to talk about this and get the card cancelled and a replacement sent out."

Link – http://www.theregister.co.uk/2017/11/17/lloyds_customers_affected_by_data_breach/

Middle East 'MuddyWater' Attacks Difficult to Clear Up

Long-lasting targeted attacks aimed at entities in the Middle East are difficult to attribute despite being analyzed by several researchers, Palo Alto Networks said this week.

Dubbed “MuddyWater” by the security firm because of the high level of confusion they have already created, the attacks took place between February and October 2017. The campaign has made use of a variety of malicious documents, and hit targets in Saudi Arabia, Iraq, Israel, United Arab Emirates, Georgia, India, Pakistan, Turkey, and the United States to date…

Link – http://www.securityweek.com/middle-east-muddywater-attacks-difficult-clear

Tennessee City Still Not Recovered from Ransomware Attack

The City of Spring Hill, Tenn. is still suffering from the effects of a ransomware attack that struck the municipality in early November when government officials refused to pay the $250,000 ransom demanded by the cybercriminals…

Link – https://www.scmagazine.com/tennessee-city-still-not-recovered-from-ransomware-attack/article/707847/

Dark Web Shops Are Leaking IPs Left and Right

The takedown of three major Dark Web markets by law enforcement officials over the summer has driven many vendors of illegal products to set up their own shops that, in many cases, are not properly configured and are leaking the underlying server's IP address…

Link – https://www.bleepingcomputer.com/news/security/dark-web-shops-are-leaking-ips-left-and-right/

Scammers Steal S$80K from Woman Using Fake Police Website

Scammers stole S$80,000 from a woman by tricking her into visiting a fake phishing website for the Singapore Police Force (SPF). On 13 November, local law enforcement received a report from the woman that someone had stolen several thousand Singapore dollars from her bank account.

She told investigators that the trouble started sometime earlier when she received a call from someone claiming to be a Singapore Police Force officer. They told her that someone was abusing her bank account for the purpose of committing money laundering. To help stop those fake criminals, the caller requested that the woman provide her personal information. She complied, and the call ended shortly thereafter.

Link – https://www.tripwire.com/state-of-security/latest-security-news/scammers-steal-s80k-woman-using-fake-police-website/

Dark Web Shops Are Leaking IPs Left and Right

The takedown of three major Dark Web markets by law enforcement officials over the summer has driven many vendors of illegal products to set up their own shops that, in many cases, are not properly configured and are leaking the underlying server's IP address.

In case of Dark Web portals, leaking the real-world IP address means law enforcement can move in, seize the server, and possibly track down the illegal shop's owner and much of his clientele.

Link – https://www.bleepingcomputer.com/news/security/dark-web-shops-are-leaking-ips-left-and-right/

NEWS REPORT

Critical Security Lessons from the Financial Sector

To improve cybersecurity, the healthcare sector should consider adopting some of the best practices implemented in the financial sector, especially those related to supply chain security and information sharing on cyberattacks, says security expert Greg Garcia.

Garcia, who was recently named the first executive director for cybersecurity at the Healthcare and Public Health Sector Coordinating Council, formerly served as executive director at the council for the financial services sector…

Link – https://www.healthcareinfosecurity.com/interviews/critical-security-lessons-from-financial-sector-i-3766

Google Discloses Details of $100,000 Chrome OS Flaws

Google has made public the details of a code execution exploit chain for Chrome OS that has earned a researcher $100,000.

In March 2015, Google announced its intention to offer up to $100,000 for an exploit chain that would lead to a persistent compromise of a Chromebox or Chromebook in guest mode via a web page. Prior to that, the company had offered $50,000 for such an exploit.

A researcher who uses the online moniker Gzob Qq informed Google on September 18 that he had identified a series of vulnerabilities that could lead to persistent code execution on Chrome OS, the operating system running on Chromebox and Chromebook devices…

Link – http://www.securityweek.com/google-discloses-details-100000-chrome-os-flaws

VULNERABILITY REPORT

Oracle Issues Emergency Patches For 'JoltandBleed' Vulnerabilities

Oracle pushed out an emergency update for vulnerabilities affecting several of its products that rely on its proprietary Jolt protocol. The bugs were discovered by researchers at ERPScan who named the series of five vulnerabilities JoltandBleed.

The vulnerabilities are severe, with two of the bugs scoring 9.9 and 10 on the CVSS scale. Products affected include Oracle PeopleSoft Campus Solutions, Human Capital

Management, Financial Management, and Supply Chain Management, as well other product using the Tuxedo 2 application server…

Link – https://threatpost.com/oracle-issues-emergency-patches-for-joltandbleed-vulnerabilities/128922/

Amazon Key Flaw Could Let a Courier Disable Your Cloud Cam

Amazon recently weirded out much of the internet when it unveiled its Key delivery service that lets its couriers open your home and deliver packages while you're away. A key part of that is the Cloud Cam security camera that confirms deliveries and shows that your house remains un-ransacked. Now, researchers from Rhino Security Labs have shown that it's possible, under rare circumstances, to hack the camera so that everything looks fine while someone takes all your stuff…

Link – https://www.engadget.com/2017/11/16/amazon-key-hack-cloud-cam/

Github Will Warn Developers About Vulnerable Dependencies in Their Projects

GitHub — the Internet largest code hosting service — is rolling out a new security feature through which it hopes to reduce the number of vulnerable projects hosted and distributed through its platform. This new security feature has no special name, but it's being added to a GitHub feature known as the Dependency Graph.

The Dependency Graph is a section in each GitHub project's "Insights" tab. The graph shows a tree-like structure of all the libraries that are loaded inside a coding project based on manifest files included in each project.

Link – https://www.bleepingcomputer.com/news/security/github-will-warn-developers-about-vulnerable-dependencies-in-their-projects/

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