NH-ISAC
NATIONAL HEALTH - ISAC

NH-ISAC Daily Security Intelligence Report –October 6, 2017

TLP GREEN

Vulnerabilities and Threats

Apple issues new security update for macOS High Sierra

Apple issued a supplemental security update for macOS High Sierra 10.13 to patch two issues, one of which fixes a keychain password issue discovered last week.

https://www.scmagazine.com/apple-issues-new-security-update-for-macos-high-sierra/article/698537/

PoCs for Two Magento Bugs Released

Security researchers from DefenseCode have released on Wednesday proof-of-concept code for two Magento vulnerabilities patched last month.

The PoCs are included in two advisories the company released for two vulnerabilities researchers discovered in Magento's open-source and cloud-hosted platforms. Both vulnerabilities are a combo of CSRF+XSS bugs (CSRF = cross-site request forgery, XSS = cross-site scripting).

https://www.bleepingcomputer.com/news/security/pocs-for-two-magento-bugs-released/

Video Streams Leak What You're Watching to Attackers With Over 95% Accuracy

Even if a video streaming service is using HTTPS to encrypt its traffic, an attacker can still determine with a very high accuracy what content a user might be watching.

This type of snooping is possible because of an information leak discovered by a team of researchers in MPEG-DASH, a popular streaming technique implemented by today's top video platforms, such as Amazon, Netflix, YouTube, Vimeo, and others.

https://www.bleepingcomputer.com/news/security/video-streams-leak-what-youre-watching-to-attackers-with-over-95-percent-accuracy/

Remote Identification of Encrypted Video Streams (PDF)

https://beautyburst.github.io/beautyburst.pdf

Seamless Campaign Delivers Ramnit Banking Trojan via RIG Expolit Kit

Recent threat hunting had led me to another Seamless gate which used RIG EK to deliver Ramnit banking Trojan. The Seamless campaign, which has been around since at least February 2017, has always Favorited Ramnit as its payload. Often the Ramnit payloads will download additional malware such as AZORult stealer.

The publisher (a website that displays adverts) that I used for this infection chain is very popular in Pakistan. In fact, Alexa ranks it within the top 50 in Pakistan and in the top 4,000 globally. Traffic estimates for the publisher shows that they received an estimated 4.1 million visitors in the last 30 days.

https://malwarebreakdown.com/2017/10/04/seamless-campaign-delivers-ramnit-banking-trojan-via-rig-ek/

Brazilian banking trojan uses legit VMware binary to bypass security

Cybercriminals are using legitimate VMware binary to spread banking trojans in a new phishing campaign targeting the Brazilian financial sector.

The trojan uses an authentic VMware binary to deceive security tools into accepting errant activity and to bypass security checks because if the initial binary, such as vm.png, is accepted, then the security tools assume that subsequent libraries will also be trustworthy, according to a Cisco Talos report.

https://www.scmagazine.com/brazilian-trojan-uses-an-authentic-vmware-binary-to-deceive-security-tools/article/698097/

Unique Infostealer uses phony Pennsylvania Department of Welfare

An infostealer malware in search of credentials, private keys, SSH keys, Bitcoin wallets and more is being distributed via a compromised website using phony Pennsylvania Department of Welfare document as a social engineering lure.

The malware uses Microsoft Intermediate Language payload that is compiled to steal passwords from the victim's system, browser and FTP software, according to an Oct. 4 Zscaler blog post.

https://www.scmagazine.com/infostealer-spreads-via-compromised-website/article/698444/

https://www.zscaler.com/blogs/research/infostealer-spreading-through-compromised-website

Avast urges developers to secure toolchains after hacked build box led to CCleaner disaster

Avast staffers spoke at the Virus Bulletin International Conference in Madrid, Spain, on Thursday to shed more light on their postmortem of the CCleaner fiasco – and urge developers to protect their software's toolchain and distribution systems from hackers.

The widely used utility, which removes unwanted temporary files and registry keys on Windows machines, was backdoored with malicious code in August, as in, miscreants tampered with the software's downloads to introduce a means to remotely control PCs running the code. Nearly 2.3 million computers ended up installing the dodgy version of the tool, and 40 – within companies such as Intel, VMware, Samsung, NEC and Sony – were instructed to download malicious code to commandeer the boxes. This was absolutely a highly targeted espionage caper, it appears.

http://www.theregister.co.uk/2017/10/06/ccleaner_megahack_timeline/

Malicious CHM Files Being Used to Install Brazilian Banking Trojans

Security researcher My name Is discovered a new spam campaign distributing that uses an uncommon attachment to download and install what appears to be a Brazilian banking Trojans onto an affected computer. While most recent malspam campaigns have been using JS or VBS attachments, this particular campaign is using malicious CHM documentation files that execute PowerShell commands to download and install malware.

https://www.bleepingcomputer.com/news/security/malicious-chm-files-being-used-to-install-brazilian-banking-trojans/

Hundreds of Printers Expose Backend Panels and Password Reset Functions Online

A security researcher has found nearly 700 Brother printers left exposed online, allowing access to the password reset function to anyone who knows what to look for.

Discovered by Ankit Anubhav, Principal Researcher at NewSky Security, the printers offer full access to their administration panel over the Internet.

https://www.bleepingcomputer.com/news/security/hundreds-of-printers-expose-backend-panels-and-password-reset-functions-online/

Homograph attacks explained

In April, Xudong Zheng, a security enthusiast based in New York, found a flaw in some modern browsers in the way they handle domain names. While Chrome, Firefox, and Opera already have security measures in place to cue users that they might be visiting a destination they thought was legitimate, at that time these browsers did not flag a fake domain name that used all Latin look-alike characters taken from another foreign language. Zheng demonstrated this when he created and registered a proof-of-concept (PoC) page for the domain, apple.com, which was written in pure Cyrillic characters.

https://blog.malwarebytes.com/101/2017/10/out-of-character-homograph-attacks-explained/

Bypassing Intel Boot Guard

In recent years, there is an increasing attention to the UEFI BIOS security. As a result, there are more advanced technologies created to protect UEFI BIOS from illegal modifications. One of such technologies is Intel Boot Guard (BG) – a hardware-assisted BIOS integrity verification mechanism available since Haswell microarchitecture (2013). So-called «UEFI rootkits killer» this technology is designed to create a trusted boot chain (where a current boot component cryptographically measures/verifies the integrity of the next one) with Root-of-Trust locked into hardware.

https://embedi.com/blog/bypassing-intel-boot-guard

Common Types of Cyberattacks in Education and What We Can Learn from Them

Cybercriminals have increasingly taken notice of schools and universities as profitable targets for cyberattacks. A key reason for this is the types of information schools keep on students, parents, and staff.

Typically, upon infiltrating an institution's network, cybercriminals will probe for, find, and exfiltrate valuable user data. This could be anything from health records, financial information, or any other personally identifiable information, such as social security numbers. Cybercriminals typically then take this data and sell it on the dark web for a profit. For this reason, healthcare providers and retailers are often high-target industries facing cyberattacks. However, because schools usually keep records of students' and staffs' health, financial, and personal information, they have now become a one-stop shop.

https://blog.fortinet.com/2017/10/06/common-types-of-cyberattacks-in-education-and-what-we-can-learn-from-them

Cyber Incidents and Cyber Crime

Russian government hackers used antivirus software to steal U.S. cyber capabilities

Russian government hackers lifted details of U.S. cyber capabilities from a National Security Agency employee who was running Russian antivirus software on his computer, according to several individuals familiar with the matter.

https://www.washingtonpost.com/world/national-security/russian-government-hackers-exploited-antivirus-software-to-steal-us-cyber-capabilities/2017/10/05/a01bf546-a9fc-11e7-92d1-58c702d2d975_story.html

Russian Theft of NSA Secrets: Many Questions, Few Answers

The bombshell report from the Wall Street Journal, quickly followed up by the Washington Post, has put further pressure on Kaspersky Lab, the well-known security company the U.S. government has accused of collaborating with the Russian government.

But many questions and details about the incident remain unanswered. Here's a roundup of the issues in play.

https://www.healthcareinfosecurity.com/russian-theft-nsa-secrets-many-questions-few-answers-a-10361

City of Englewood, Colorado hit with ransomware

The city of Englewood, Colo. was hit with a ransomware attack which brought down the city's internal network.

The attack left the city's civic center unable to process credit cards and the city's library unable to place items on hold or accept late fines, according to an Oct. 4 press release.

https://www.scmagazine.com/the-city-of-englewood-colo-was-hit-with-a-ransomware-attack/article/698236/

Government, Law, and Critical Infrastructure

Russia may have tested cyber weapons on Latvia

According to intelligence experts the recent Zapad drills conducted by Russia simulated an attack on all Baltic countries, it included the use of cyber weapons.

http://securityaffairs.co/wordpress/63918/cyber-warfare-2/zapad-drills.html

Security Industry Tools and Reports

AlienVault: 2017 Ransomware Report (PDF, requires registration):

https://www.alienvault.com/blogs/security-essentials/2017-ransomware-report

____

OP

Operations

NH-ISAC, Inc.
226 North Nova Road, Suite 391
Ormond Beach, Florida 32174

twitter.com/NHISAC

www.nhisac.org