BRAINTRACE

THREAT ADVISORY REPORT

MARCH 18, 2021

braintrace™
INTELLIGENT CYBERSECURITY

braintrace™
INTELLIGENT CYBERSECURITY

TABLE OF CONTENTS

BACKGROUND

This report was created to update our clients on up-and-coming vulnerabilities and exploits that our security experts have discovered. Our team works diligently on researching threats and vulnerabilities to provide you with a safer network. If you have any questions, do not hesitate to contact us.

GOOGLE REMOVED 10 APPS INFECTED WITH DROPPERS FOR FINANCIAL TROJANS

On Checkpoint Research's (CPR) blog, researchers published on January 29 that there is a new dropper on Google Play. The dropper is named Clast82. They discovered that this dropper, spreading through the app store, downloads and installs the AlienBot Banker and MRAT. Researchers that worked discovered this malware include Aviran Hazum, Bohdan Melnykov, Israel Wernik.

Researchers published that after the payload is dropped, it can be transformed from non-malicious to malicious. CPR blog also posted that the same threat actor is behind these ten reported apps. The malicious actors created new developer accounts for each app individually. Some of the impacted apps are Cake VPN, Pacific VPN, eVPN, BeatPlayer, QR/Barcode Scanner MAX, Music Player, tooltipnatorlibrary, and QRecorder. The apps were downloaded more than 15,000 times. On February 9th, Google published that impacted apps were removed from Google Play.

Affected Systems

- Android, Google Play

Vulnerability Overview

Hackers were using open sources android applications to add malicious code. AlienBot is a Malware-as-a-Service (MaaS) type. It enables a bad actor to inject malicious code into victim's financial applications. This way, hackers can gain full privileged access to the victim's device. After the victim installs the malicious payload, Clast82 will execute more than 100 unique payloads. Their final goal is to gain access to the credentials and 2FA codes of financial apps.

Indicators of Compromise

C&C Servers:
boloklava87[.]club
enegal-23[.]net
balabanga90[.]online
dsfikj2dsfmolds[.]top
blakarda[.]site
sponkisn[.]site

SHA256

52adb34cc01aa8d034d71672f3efe02c8617641ee77bf6c5eb6806e834550934

bb49fc80393647d379a8adc8d9dec2f9a21e86620ee950f94cdc341345df459c
232d3a2a172db5d0e02570a8ddbb8377dc5b8507aab85a51faf00631b51b7def
609350daaadee74e6526dee7f533affdbf289f076837a2400017a928531c3da1
804fb97dbe7dc93f7ed37963f120ef5f5f7e6253501bd60f08433b0fd5c3db74
82ea6fc0f57ae82cf7c51a039b6dee7b81b4ece0579a784ee35f02e71b833f3e
80a4380b812df71401733b0b37005e82a96f18b07be5317e82f38658b1551c5a
6f6c16481c0f3a4bd3afcaa9aa881e569c65e067c09efd4ac4828ead29242c95
bbe2e4a68eb2a2589b6b7ba9afefd241f8eb6d8db6fa19fdd4d383311a019567
4d4f8acda2e9b430d5f3a175dbeee9dfcd07a9f26332b1a0b9e94166b1bc077f

A complete list of IOCs can be found on the Checkpoint Research blog:

https://research.checkpoint.com/2021/clast82-a-new-dropper-on-google-play-dropping-the-alienbot-banker-and-mrat/

Recommendation

It is recommended to check if any of these applications were installed on your Android and take proper security precautions. Android users should install full mobile protection on their phones. This way can mitigate similar vulnerabilities.

Reference

https://www.zdnet.com/article/malicious-apps-on-google-play-dropped-banking-trojans-on-user-devices/

WEAK ACLS IN ADOBE COLDFUSION ALLOW PRIVILEGE ESCALATION

Will Domain, a security researcher, revealed a privilege-escalation vulnerability that has been located within the Adobe ColdFusion systems. This vulnerability will allow an unprivileged user the ability to run arbitrary code with SYSTEM privileges. The attacker could easily place a specific DLL file within the directory of Adobe ColdFusion, which would result in the execution of system privileges, which is known as DLL hijacking.

Affected Systems

- Windows systems running ColdFusion

Vulnerability Overview

Adobe ColdFusion is a development platform that is used to quickly build modern web apps. It is easy to use and is known as the backbone of many different modules. Adobe ColdFusion installer does not create a "Secure Access Control List" (ACL) on the actual default directory. An attacker aware of this vulnerability would place a specifically crafted malicious DLL in a location that Windows searches for the actual DLL. Upon finding this vulnerability, Adobe began working with Mr. Domain and came up with a solution which you will find in the recommendation.

Recommendation

ColdFusion will not configure itself securely. To secure against this vulnerability, it is recommended that the user install the Server Auto-Lockdown. The ColdFusion Server Auto-Lockdown installer must be installed in addition to ColdFusion proper. Guides or patches can be seen below:

ColdFusion 2016:
https://wwwimages.adobe.com/content/dam/acom/en/products/coldfusion/pdfs/coldfusion-2016-lockdown-guide.pdf
ColdFusion 2018: https://www.adobe.com/support/coldfusion/downloads.html#cf2018ldg
ColdFusion 2021: https://www.adobe.com/support/coldfusion/downloads.html#cf2021ldg

Patch URL

Please See Patch Recommendation

Reference

https://www.securityweek.com/weak-acls-adobe-coldfusion-allow-privilege-escalation

ADOBE PUBLISHED UPDATES FOR ADOBE CREATIVE CLOUD DESKTOP, FRAMEMAKER, AND CONNECT VULNERABILITIES

On May 9th, Adobe published that they fixed eight vulnerabilities. Most of them are marked as critical because they allow arbitrary code execution. Affected products are Creative Cloud Desktop Application, Adobe Connect, and Adobe Framemaker.

Affected Systems

- Windows, Mac OS

Vulnerability Overview

Affected software should be updated since they allow malicious actors to execute arbitrary code and escalate their privileges. This can lead to installing malware and taking complete control over the victim's device. Other issues that were remedied include command injection, privilege escalation, and input validation bugs.

Recommendation

It is recommended for all affected users to update to the patched software version.

Patch URL

Creative Cloud: https://helpx.adobe.com/security/products/creative-cloud/apsb21-18.html
Connect: https://helpx.adobe.com/security/products/connect/apsb21-19.html
Framemaker: https://helpx.adobe.com/security/products/framemaker/apsb21-14.html

Reference

https://www.zdnet.com/article/adobe-releases-batch-of-security-fixes-for-framemaker-creative-cloud-connect/

UNPATCHED QNAP DEVICES TARGETED IN ATTACKS TO MINE CRYPTOCURRENCY

Unpatched QNAP network-attached storage (NAS) devices are being targeted in a recent flood of attacks by threat actors to take control of the device and download cryptominer malware to mine cryptocurrency. The two vulnerabilities allow for pre-auth remote command execution (RCE) exploited by the threat actors. QNAP patched the vulnerabilities in October 2020. The cryptominer malware being used in the campaign has been named UnityMiner by researchers.

Affected Systems

- NAS devices with QNAP firmware released before August 2020.

Vulnerability Overview

To go unnoticed and hide the mining process from the user, the threat actors customized the program to hide the real CPU memory resource usage information. If the user checks the system usage with the WEB management interface, they will not see the abnormal activity. The malicious malware program, UnityMiner, contains two files: unity_install[.]sh, and Quick[.]tar[.]gz.

The unity_install.sh kills any ongoing process, checks the CPU architecture, and begins downloading the mining kit depending on the architecture. The Quick.tar.gz file consists of the miner startup script, miner configuration file, and the forged manaRequest[.]cgi file. The malware hijacks the device's original manaRequest file. It forwards the HTTP request to the original file of the same name to execute it. It logs the results and modifies the results by subtracting 50 from the CPU status data and deletes the unity process information.

Recommendation

It is recommended for QNAP NAS users to check and update their firmware as soon as possible.

Reference

https://blog.netlab.360.com/qnap-nas-users-make-sure-you-check-your-system/

REDXOR MALWARE TARGETING LINUX SYSTEMS

A new backdoor malware named RedXOR linked to the Winnti Threat Group has been discovered and suspected to target legacy Linux distributions. The name RedXOR comes from the fact that the original sample was found on a legacy Red Hat Enterprise Linux distribution. Its network data-encoding is based upon the XOR algorithm for encryption.

The initial compromise point has not yet been discovered for the original samples taken from VirusTotal sources in Taiwan and Indonesia. As researchers continue to investigate, they are not ruling out common vulnerabilities, misconfigurations, possible lateral movement, and the use of compromised credentials.

Affected Systems

- Linux systems

Vulnerability Overview

After the execution, RedXOR generates a hidden folder called ".po1kitd.thumb" and places it inside the home folder. RedXOR stores malware-related files in this folder along with another hidden folder called ".po1kitd-2a4D53". A binary is then installed to another hidden folder called ".po1kitd-update-k" to implement persistence scripts using "init."

Configuration data related to C2 server addresses, ports, and passwords are then encrypted and stored in the binary. This is followed by communication attempts to the C2 server using TCP to execute commands to use shell commands, tunnel the network, and upload, remove, open, and edit files.

Recommendation

Implement best practices for hardening network devices and for accessing potentially malicious links, attachments, and websites.

Reference

https://threatpost.com/linux-systems-redxor-malware/164689/

RANSOMWARE ATTACKS UNPATCHED EXCHANGE SERVERS

Microsoft published that hackers are using DearCry ransomware to attack unpatched Microsoft Exchange servers. Chinese government hackers are attacking systems that are still exposed to the four vulnerabilities in Exchange servers. Microsoft published that the Chinese hacking group is known as Hafnium. Cybersecurity researchers gave an update that ten other government-supported hacking groups joined Hafnium in recent attacks. Many companies were impacted, including ones in Canada, Denmark, United States, Australia, and Austria.

Affected Systems

- Exchange Servers

Vulnerability Overview

These hacking groups are trying to use bugs in the vulnerable system to install malware. The new ransomware is named Ransom: Win32/DoejoCrypt.A and it can be detected with Microsoft's Defender antivirus. It is recommended to apply the search for indicators since September 1, 2020.

Hackers are using open-source tools to search for vulnerable Microsoft Exchange Servers. The encrypted file will appear under the file extension .CRYPT. When a computer is fully encrypted, victims will see 'readme.txt' on the Windows desktop. In that file, victims will notice two emails with instructions to contact hackers. Victims will be requested to pay a ransom so they can recover their files.

Recommendation

It is recommended to update the Microsoft Exchange server as soon as possible and create offline backups of Exchange servers. Affected users can use Microsoft Defender to scan their computers to ensure no traces of known indicators of compromise for Ransom: Win32/DoejoCrypt.A.

Patch URL

https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/?ranMID=24542&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-HRUtPoyNOXoolYam5PC.Uw&epi=je6NUbpObpQ-HRUtPoyNOXoolYam5PC.Uw&irgwc=1&OCID=AID2000142_aff_7593_1243925&tduid=%28ir__3acp1bm1fkkfqlvxkk0sohzi9f2xponewpxkmciw00%29%287593%29%281243925%29%28je6NUbpObpQ-HRUtPoyNOXoolYam5PC.Uw%29%28%29&irclickid=_3acp1bm1fkkfqlvxkk0sohzi9f2xponewpxkmciw00

Reference

https://www.zdnet.com/article/microsoft-watch-out-for-this-new-ransomware-threat-to-unpatched-exchange-email-servers/

NIMZALOADER: STRANGE MALWARE LANGUAGE, HARDER TO DETECT

A new malware dubbed NimzaLoader is now being distributed by a prolific cybercriminal operation. This malware was developed in hopes that by choosing a different malware language, it would be harder to detect and analyze. The use of the Nim programing language is very uncommon for malware in the threat world and has already targeted 100 different organizations.

Affected Systems

- Windows-based systems

Vulnerability Overview

NimzaLoader is thought to be the work of TA800, a cybercriminal hacking group that is usually associated with ransomware attacks delivered by BazarLoader. TA800 has often supported unique types of malware, and with NimzaLoader being written in a different and rare language, it has another method of attack.

NimzaLoader, like a lot of other malware attacks, is distributed thru phishing emails. These emails will link the user to a fake pdf download in which it will immediately download the malware into the system. On Feb 3rd, 2021, a spear-phishing message was observed showing very personal details within the email. The email addressed to the victim went on to ask them to check over their presentation, and please click on the email's presentation link to look it over. If one were to click on the link, they are taken to the NimzaLoader executable.

NimzaLoader uses mostly encrypted strings, using an XOR-based algorithm and a single key per string. Most of the strings contain command names giving them the ability to inject shellcodes and execute PowerShell scripts.

Recommendation

Keeping your systems updated and all patches current, keeping current backups of data, and making sure the antivirus and spyware are present and in place are some of the recommendations to avoid a breach. Refrain from opening any suspicious-looking emails, attachments, and continued training on spotting phishing emails are recommended as well at this time.

Reference

https://www.zdnet.com/article/this-malware-was-written-in-an-unusual-programming-language-to-stop-it-from-being-detected/

DARKSIDE 2.0 RANSOMWARE PROMISES FASTEST EVER ENCRYPTION SPEEDS

Intelligence experts are warning of a new version of a long-time ransomware found on dark web community forums XSS and Exploit called Darkside 2.0. This more recent version carries faster encryption speeds, VoIP calling abilities, and the capability of targeting virtual machines. This newer version will give victims even less time to stop the encryption once it has started.

Affected Systems

- Windows and Linux systems as well as Network Area Storage devices

Vulnerability Overview

The original Darkside ransomware started targeting enterprises back in August of 2020 and earned millions in payouts during its life. January of 2021, a Romanian cybersecurity firm released a decryptor that allows victims to recover their files without paying the ransom. Here it is March of 2021, and "Darkside" is back but stronger. Darkside 2.0 is said to now have the means to target VMware ESXi vulnerabilities, which means that it can hijack virtual machines and encrypt the virtual hard drives.

The ransomware also now can make VoIP calls to the victims, partners, and even journalists. Enacting more pressure and scare tactics against its victims into paying the ransom. However, the new arrival and updated version of this ransomware kept some of its predecessor's traits. The Darkside group still mandates that "Darkside 2.0" not be targeted against healthcare and vaccine distribution centers, schools, and non-profit organizations. This is still highly unusual for a ransomware-as-a-service (RaaS) operation. Not only are these targets not allowed, but the group donated last October $10,000 of the money stolen from corporate victims to different charities. If this was an actual way to give back to the community or a new way to launder funds, no one is for sure.

Recommendation

Keeping all systems updated is highly recommended and keeping current backups of all system files. When opening links within emails as well as entering website addresses, use extreme caution. Verify that the website address is entered correctly as well as the email is from a verified source. Using and maintaining antivirus software and firewalls will also help to filter malicious traffic as well.

Reference

https://www.infosecurity-magazine.com/news/darkside-20-ransomware-fastest/

PROTECTING OUR SYSTEMS AGAINST NATION STATE THREAT ACTORS

Cybercrime keeps evolving and increasing in 2021 too. Highly sophisticated malware and nation-state threat actors have caused cybersecurity to become a top priority for defending organizations. While script kiddies, hacktivists, and cybercriminals have limited technical and financial resources, nation-state actors do not have any limitations. Understanding the tactics and techniques of state-sponsored actors, which have been around even before the birth of many cybersecurity concepts, should be at the center of our defensive mechanisms. Moreover, getting prepared for a worst-case scenario cyber-attack from a nation-state threat actor is expected to provide a robust enough defense mechanism against other cyber criminals too.

Affected Systems

- All Systems

Vulnerability Overview

In general, the following area seen as headwinds against strong defense practices in protecting systems against intrusion:

- Lack of training of the employees for social engineering and phishing attacks.
- Lack of a well-trained and prepared incident response team.
- Lack of on-time patch management policies.
- Lack of proper configurations.

As such, reviewing and implementing corrections, and even auditing for these issues once in a while can be a great benefit to the defense of any organization.

Recommendation

Recommendations for the issues that were noted include

- User training programs for identifying and resisting social engineering attacks. It should not be a one-time workshop event related to phishing attacks or business-ethics. Instead, it must be an ongoing learning and practicing process to detect any possible intrusion attempts.
- Ensure Security Operations Team (SecOps) be well trained, adequate, and prepared for the incidents.
- Ensure you have a strong MSSP (Managed Security Service Provider), having a well-trained, highly skilled team to confront cyber threats at any level, from script kiddies to nation-state actors.
- Foster a company culture where any employee would step forward and inform the management about any kind of illegal attempts, including bribery or blackmailing.
- Keep your security stack up to date. Nation-state threat actors are the cruelest predators of the cybersecurity realm as they have top-notch members with substantial resources, time, and skills. Keeping defenses up to date with the appropriate tools, continuous training, and best practices in place is very likely to protect our organizations even from the most challenging adversaries like nation-state actors.
- Keep your systems patched on time and configured correctly. Keep in mind that even very sophisticated state actors are known to exploit previously known vulnerabilities.
- Nation-state threat actors are the cruelest predators of the cybersecurity realm. They have top-notch staff with unlimited financial resources, time, and skills. Keeping our defenses up to date with the appropriate tools, continuous training, and best practices in place is very likely to protect our organizations even from the most challenging adversaries like nation-state actors.

Reference

https://threatpost.com/defending-against-state-threat-actors/162518/

NANOCORE RAT MALSPAM CAMPAIGN

Trustwave SpiderLabs published an article on how the NanoCore Remote Access Trojan (RAT) malspam campaign is actively getting past email defenses by abusing file extensions, similar to a LokiBot malspam campaign that was seen in 2019. If the NanoCore RAT is allowed to inject itself onto a victim's device, the RAT will send files, documents, clipboard data, and other such information to the C2 server.

Affected Systems

- All Systems

Vulnerability Overview

The emails analyzed by SpiderLabs spoofed themselves such that they appear to come from purchase managers from various organizations and included an attachment of a binary icon image file with appended RAR compressed data with the NanoCore RAT malware. If the malspam email successfully evades detection, the victim needs to extract and execute the compressed .EXE file with either 7Zip or WinRAR.

Indicators of Compromise

C2 URLs:
shtf[.]pw
uyeco[.]pw

Attachment:
NEW PURCHASE ORDER.pdf.zipx (480092 bytes) SHA1:
DF46A893B51D8ADE0CCDEF7E375FB387E2560720
New Purchase Order.pdf (2).zipx (403050 bytes) SHA1:
C93FBA54357E90235202F58DA1FEFF7AB1142F65

NanoCore RAT:
NEW PURCHASE ORDER.exe (635904 bytes) SHA1:
E99F6B9BD787679666F8C54B9A834D6ACECFA622
New purchase order (3).exe (431104 bytes) SHA1: FD958C365B6BFA5EF34779831773EC92C041A5D5

Recommendation

Maintain social engineering awareness and scan for IOCs where necessary.

Reference

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/image-file-trickery-part-ii-fake-icon-delivers-nanocore/

A NEW HIGHLY DAMAGING RANSOMWARE ATTACK: HELLOKITTY

HelloKitty belongs to a ransomware family which was detected last year. Game Studio CD Projekt Red was one of the victims of this damaging cyberattack. Even though HelloKitty ransomware is not so sophisticated as the other infamous malware such as Ryuk and Revil, it is still impactful enough to inflict substantial damage to many organizations. It is delivered through phishing attacks or secondary infections. Once the files are encrypted, the victims must pay a ransom via a TOR address.

Affected Systems

- All systems

Vulnerability Overview

Once exploited, HelloKitty Ransomware attempts to knock out and kill some critical processes, especially those having the potential to interfere with encryption. These processes are known to be associated with some platforms such as SharePoint, MSSQL, and IIS. Once the target processes have been killed through taskkill.exe and net.exe., encryption is initiated using cryptographic algorithms such as AES-256 & RSA-2048 NTRU+AES-128.

The only effective defense against HelloKitty Ransomware attack is through prevention since there is no discovered weaknesses in the cryptographic algorithm used or a 3rd party support service for decrypting the files at the moment yet.

Indicators of Compromise

SHA1:
fadd8d7c13a18c251ded1f645ffea18a37f1c2de

SHA256:
501487b025f25ddf1ca32deb57a2b4db43ccf6635c1edc74b9cff54ce0e5bcfe

Recommendation

As usual, we do recommend patching and deploying endpoint monitoring where possible.

Reference

https://labs.sentinelone.com/hellokitty-ransomware-lacks-stealth-but-still-strikes-home/

CRYPTOMINING MALWARE SEEN TARGETING UNPATCHED SERVERS

A botnet that was first observed in November 2020 is now mining for the cryptocurrency Monero (XMR) through vulnerable Elasticsearch and Jenkins servers. These attacks' main targets are outdated or unpatched Jenkins servers vulnerable to remote command executions related to CVE-2015-1427. These servers are found by scanning cloud servers to detect ones that meet certain criteria and then sending a malicious packet its way. It is estimated that over 5,000 servers have already been compromised by zoMiner.

Affected Systems

- Unpatched or outdated Jenkins and Elasticsearch servers

Vulnerability Overview

zoMiner previously targeted remote command execution vulnerabilities in WebLogic's pre-authentication security. More recently, zoMiner has been observed with enhanced malware regarding detecting and infecting vulnerable Elasticsearch and Jenkins servers with remote command execution.

After a server has been infected, zoMiner runs a shell script that detects and removes previously installed cryptominers. This is followed by creating a cron entry where other scripts are stored and executed through Pastebin. Finally, the XMR miner, config file, and startup script run in the background.

Recommendation

Keep all servers up to date with the latest patches available.

Reference

https://www.bleepingcomputer.com/news/security/z0miner-botnet-hunts-for-unpatched-elasticsearch-jenkins-servers/

ACTIVE SEO TECHNIQUE USED TO SPREAD MALWARE

A new technique utilizing Google's Search Engine Optimization (SEO) has been in recent circulation, which has led hackers to deploy various malware payloads. The attack was traced to the prominent framework known as Gootloader (a network thought to be numbered at over 400 servers), used in the Gootkit Rat and other malicious services' infection process. As of the time this article was written, the observed attacks have been located throughout France, Germany, South Korea, and the United States. Additionally, there is no defined research on what exact method (malware hijack, brute-force, credential theft) that the Gootloader operators are using to gain system access.

Affected Systems

- ImagingDevices.exe and Embarcadero External Translation Manger

Vulnerability Overview

This particular campaign relies heavily on SEO tricks and human psychology to penetrate a targeted website. By ranking high within Google's search engine results, any lurking malware from groups such as Kronos, Cobalt, and REvil ransomware can easily corrupt victim's networks through their collage of hacked WordPress locations. Known examples have ranged from poisoned SEO fake forum posts to simple Google links posted within a forum. Evidence of CMS changes has also been verified, leaving a trail of phony message boards to tempt any incoming visitors in what would be believed as a trusted domain.

Recommendation

As fraud becomes more prevalent, it is increasingly essential for end users to become more aware of these methodologies and detect their signs. By also implementing verified third-party detection tools before visitation, one can significantly cut down on these risks when navigating any new or unknown territories on the Internet.

Reference

https://cyware.com/news/hackers-using-tricky-seo-technique-to-deliver-malware-payloads-f02532c8

NEW ZHTRAP BOTNET MALWARE DEPLOYS HONEYPOTS TO FIND MORE TARGETS

There is a new botnet out and it is searching for contaminated routers, DVRs, and other UPnP devices. ZHtrap is searching for these devices in hopes that it will be able to turn them into honeypots that will assist in finding other targets to infect. Honeypots are typically used as a security tool to deflect or counteract malicious attempts. This time around, though, the attackers are using security tools for their malicious use.

Affected Systems

- Routers, DVR's and Universal Plug and Play protocols.

Vulnerability Overview

ZHtrap is loosely based on Mirai's source code and supports x86, ARM, MIPS, and other CPU architectures. The botnet searches for weak/infected devices. Once it has taken over, this device will prevent other malicious malware from entering and block all attempts to run different and new commands. The botnet will then begin scanning for other devices with open vulnerabilities to take over and infect and connect to its module. Once infected, the botnet will start listening to 23 different ports and gathering IPs. The ZHtrap botnet also has backdoor capabilities that give the attackers the ability to not infect other devices and download and execute different malicious payloads into the machines.

Recommendation

Keeping all systems updated is highly recommended. The botnets use unpatched vulnerabilities to spread and cause the most damage. Deploying multi-factor authentication or other authentication processes in the case of an infection can control the malware's spreading.

Reference

https://www.bleepingcomputer.com/news/security/new-zhtrap-botnet-malware-deploys-honeypots-to-find-more-targets/

SECOMEA SITEMANAGER AND GATEMANAGER VULNERABILITIES

On March 5th, Secomea publicly disclosed critical and high severity vulnerabilities. Tenable has yet to add detection plugins for these vulnerabilities. Neither technical details nor exploits are publicly available for either of the vulnerabilities at this time.

Affected Systems

- SiteManager and GateManager before 9.4.620527004

Vulnerability Overview

A brief description of the disclosed vulnerabilities is listed below:

CVE-2020-29020
Base Score: 9.1 Critical
CWE-284: Improper Access Control
The Secomea SiteManager web service below 9.4.620527004 contains an improper access control vulnerability in an undisclosed WEB UI component that can be manipulated to cause a privilege escalation condition. A remote attacker can exploit this vulnerability to access the WEB UI from the Internet.

CVE-2020-29030
Base Score: 8.1 High
CWE-352: Cross-Site Request Forgery (CSRF)
The Secomea GateManager below 9.4.620527004 Web GUI component contains a Cross-Site Request Forgery (CSRF) vulnerability that can be exploited remotely by an attacker without authentication but may require user interaction. Successful exploitation of this vulnerability can lead to the execution of malicious code.

Recommendation

Apply vendor patch after appropriate testing

Patch URL

https://www.secomea.com/support/cybersecurity-advisory/

Reference

https://www.secomea.com/support/cybersecurity-advisory/#3217

REVIL RANSOMWARE NOW THREATENS TO EXPOSE COMPROMISES TO MEDIA AND BUSINESS PARTNERS

Over the past few months, we have seen ransomware gangs' rise using new pressure tactics to get companies to pay ransom payments. Traditionally, the threat of losing files was enough to get victims to pay their attackers, but times have changed. Recently, we have seen companies such as Avadonn adding the threat of distributed denial-of-service (DDOS) attacks to their arsenal. Revil has now added this tactic. Additionally, they are threatening victims with VOIP attacks to business partners and even the media.

Affected Systems

- Any System Vulnerable to Ransomware

Vulnerability Overview

A security researcher named 3xport recently announced that Revil is now using both DDOS and VOIP threats in addition to the threat of losing encrypted files. The DDOS attacks are known to take place on Layers 3 and 7 of the OSI model. These actors are also using threats of VOIP calls to media/business partners as a way to increase the pressure/urgency to pay up. Though the DDOS attack costs an extra fee for the attackers, it is concerning that the additional VOIP threat is free.

Recommendation

User education regarding social engineering attacks, proper network architecture, and good monitoring are strong defenses against most attacks of this type. Further, please ensure your backup policies and practices are tested and operational.

Reference

https://www.bleepingcomputer.com/news/security/ransomware-gang-plans-to-call-victims-business-partners-about-attacks/

CISCO DLL HIJACKING VULNERABILITY

Cisco has provided many products such as routers and firewalls throughout the years. Cisco also provides endpoint protection through their Advanced Malware Protection (AMP) product and provides advanced threat detection through Cisco's technology. The vulnerability disclosed in this article is associated with Dynamic Link Libraries (DLL). DLLs are used to allow programs to function with the Windows operating system and determines how to allocate resources to run a program.

Affected Systems

- Earlier versions from 7.3.3 of Cisco AMP for Windows machines and previous versions from 7.3.12 of Immunet for Windows machines

Vulnerability Overview

The vulnerability of the affected Cisco products could allow an attacker to perform a DLL hijack and eventually lead the attacker to execute arbitrary code with system-level privileges. There is the possibility of an attacker injecting a malicious DLL file into the system. This is possible because of incorrect handling of directory search paths when the associated program is executed. To successfully exploit this, the attacker would have to be authenticated to the target machine to exploit this vulnerability.

Recommendation

Update to the latest version

Reference

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-amp-imm-dll-5PAZ3hRV

FOUR BEST PRACTICE PRINCIPLES FOR HEALTH CARE ORGANIZATIONS TO PROTECT THEIR NETWORK SECURITY

Cyberattacks' number and diversity in health care organizations continue to rise since Health Care Organizations keep becoming very lucrative and easy targets for adversaries. It has been reported by the Department of Health and Human Services that a substantial increase of around 50% in data breaches had been observed in the first six months of 2020.

Affected Systems

- Healthcare systems

Vulnerability Overview

The primary issues of concerns for administrators in these environments were noted to be:

- Legacy cyberdefense infrastructure,
- Weak or no authentication,
- Inadequate cybersecurity budgets and resources.

Given these considerations, continual attack vectors exploiting older device vulnerabilities and default or weak password bugs should be expected. Further, inadequate training of staff in all silos should be of concern to any organization.

Recommendation

As such, we recommend the following, also known as the Core Principles of Hardening:

- Strong authentication (Strong and complex passwords, password history and age, multi-factor authentication).
- Hardening the access to DATA, such as with data encryption where possible and in all phases (at rest, in motion, at work), and least-privilege or role-based access controls.
- Network segmentation (LANs, VLANs) and monitoring.
- Filtering your traffic (Allow lists for applications, URLs, IPs, filetypes).

The decision-makers who have been historically evaluating cyber risks as low when compared with the numerous medical risks should consider that the risk of a data breach for their organization as should re-evaluate as attacks such as ransomware and PII loss are at all-time highs.

Reference

https://www.darkreading.com/attacks-breaches/4-ways-health-centers-can-stop-the-spread-of-cyberattacks/a/d-id/1340203

GAFGYT BOTNET ATTACKS D-LINK AND IOT DEVICES

The new Gafgyt botnet malware is now relying on Tor connections to attack D-Link and IoT devices. Researchers described it as a new type of Gafgyt botnet that hides its malicious activity using Tor connections. The first generation of Gafgyt botnet was first discovered in 2014, where its primary goal was for executing distributed denial-of-service (DDoS) attacks. On February 15, 2021, researchers came across a new type of Gafgyt named Gafgyt_tor.

Affected Systems

- D-Link and IoT devices

Vulnerability Overview

Gafgyt_tor utilizes Tor connection to avoid being detected by concealing its command-and-control (C2) communications and encrypting sample strings. This was the first time Gafgyt was discovered using this C2 communications technique to avoid being detected. The C2 technique use by Gafgyt_tor is solely based on Tor connections. Tor enables anonymous connections without being seen or blocked.

Gafgyt_tor botnet is associate with setting up weak passwords through IoT devices and exploiting remote code execution flaws, remote code execution vulnerability in Liferay enterprise program, and Citrix application Delivery controller flaw. According to researchers, Gafgyt_tor's code has two functions; the first is to add Tor proxy functionality to hand the IP server's address and show the propagated changes.

Gafgyt_tor's consists of tor_socket_init function that handles creating a list of proxy nodes consisting of IPs and a port. Proxy nodes are gradually added to the list, and it will randomize a node to start a Tor connection using tor_retrieve_addr and tor_retrieve_port. After the connection with C2 is begun, the botnet will send a request for wvp3te7pkfczmnnl[.]onion via the darknet, and it will then wait for commands. Gafgyt_tor also included LDSERVER to enable bad actors to change to a different download server if one server is being blocked.

Recommendation

It is recommended to keep your D-Link and IoT devices up to date with the latest patches.

Reference

https://threatpost.com/d-link-iot-tor-gafgyt-variant/164529/

SAMSUNG PATCHES 11 HIGH/CRITICAL BUGS

Samsung has released March 2021 security updates for Android devices regarding 11 bugs related to the operating system, runtime, and more. These patches also affect Android device's built-in apps such as Display, Calendar, Social Platform, and SmartThings. Each bug being patched has a categorical rating of high or critical.

Affected Systems

- Android devices

Vulnerability Overview

These bugs cover issues from vulnerabilities in the Bluetooth Service Discovery Protocol implementation, allowing remote code execution through malicious Bluetooth transmissions, null pointer issues, and Google Play. The list of CVEs that were patched is listed below:

Android Runtime Bugs:

- CVE-2021-0395

Framework Bugs:

- CVE-2021-0391
- CVE-2021-0398

System Bugs:

- CVE-2021-0397
- CVE-2017-14491
- CVE-2021-0393
- CVE-2021-0396
- CVE-2021-0390
- CVE-2021-0392
- CVE-2021-0394

Google Play Bugs:

- CVE-2021-0390

Recommendation

Keep all devices up to date with the latest patches available. Refer to your manufacturer’s documentation for updating instructions if necessary.

Reference

https://www.bleepingcomputer.com/news/security/samsung-fixes-critical-android-bugs-in-march-2021-updates/

RECAPTCHA PHISHING ATTACKS STEALS O365 CREDENTIALS

Microsoft O365 credentials are targeted for the new Google reCAPTCHA phishing emails. Bad actors use a forgery Google reCAPTCHA and top-level domain (TLD) landing pages that have targeted victims' companies' logos to trick victims into inputting their O365 credentials. Over the last three months, employees in the banking and IT industry were affected with at least 2,500 Google reCAPTCHA phishing emails. Google reCAPTCHA service enables protection for web spams. It uses a Turing test to distinguish between humans and bots.

Affected Systems

- Microsoft O365 users

Vulnerability Overview

The phishing email will first take victims to a forgery Google reCAPTCHA page. For example, a screen where you need to click on palm tree images and confirm you are not a robot. After the victims have passed their reCAPTCHA, it will take them to a landing page to prompt them for their O365 credentials.

This type of attack is called a whaling phishing attack targeting senior-level employees who are likely to access the company's sensitive information. One example of a fake phishing email is the one with voicemail attachments. This phishing email looks like an automated email from the unified communication tools with an attachment (.HTM) file extension. When the email recipients click on the attachment, they will go through the fake reCAPTCHA test.

After completing the test, email recipients will be taken to the Microsoft login screen. This screen page will also have a customized logo from the victims' companies to make this look like a legitimate email. Victims will be prompt for their credentials and redirected to a page that said the credentials validated successfully. The email recipient will be able to listen to a fake voicemail message. According to researchers, the phishing pages are hosted on generic top-level domains, .xyz, .club, and .online, typically used by hackers.

Recommendation

To protect yourself from a reCAPTCHA phishing attack, it is recommended to add multi-factor authentication, password manager, Proofpoint Email Protection, and be very cautious when opening email attachments.

Reference

https://threatpost.com/google-recaptcha-phishing-office-365/164566/

APPLE RELEASES OUT-OF-BAND PATCH FOR CRITICAL RCE FLAW

Apple is not prone to releasing patches on an emergency basis. However, that is what the technology giant recently did with addressing a critical bug that could allow for remote code execution (RCE) on, quite literally, billions of devices.

Affected Systems

- Apple iOS, macOS, watchOS, and Safari

Vulnerability Overview

Covered by CVE-2021-1844, the issue was discovered by researchers with Google's Threat Analysis and Microsoft's Browser Vulnerability Research groups. The problem stems from a memory corruption issue that may lead to an attacker executing code via specifically crafted web content, such as web pages. The issue was not related to three zero-day flaws previously disclosed by the company.

Recommendation

No specific workarounds were given for this issue other than to patch. As such, please update as soon as possible.

Reference

https://thehackernews.com/2021/03/apple-issues-patch-for-remote-hacking.html

THIRD ZERO-DAY GOOGLE CHROME VULNERABILITY IN THE YEAR OF 2021

Security updates are a crucial part of information technology and should be overlooked frequently by organizations that utilize technology. Vendors provide software that sometimes has millions of code lines, and sometimes mistakes are made and even caught by people who do not have great intentions. These bad intentions sometimes lead to executions of these vulnerabilities in the wild or the real world.

A recent vulnerability discovered was with the Google Chrome browser, and if you have not yet, please update your Google browser to the latest version.

Affected Systems

- Google Chrome Browser version < Chrome 89.0.4389.90

Vulnerability Overview

The vulnerability discovered allows for arbitrary code execution, and Google has seen this vulnerability exploited in the real world but has not provided any more information on this vulnerability.

The vulnerability occurs because of a bug in the Blink rendering engine. The bug is use-after-free, a condition of previously freed memory and how it references memory. This could lead it to point to somewhere else and cause it to crash or execute code, leading to arbitrary code execution. This is the third zero-day patch for Chrome this year, and users should update their Chrome browsers to the latest version.

Recommendation

Update Google Chrome to the latest version.

Reference

https://www.bleepingcomputer.com/news/security/google-fixes-second-actively-exploited-chrome-zero-day-this-month/?&web_view=true

VERKADA SECURITY CAMERA BREACHED

A Silicon Valley startup company Verkada, which provides an easy-to-use online security camera management solution, was breached by a group of hackers that called themselves "Advanced Persistent Threat 69420". They claimed to have breached Verkada and gained unauthorized access to 150,000 security cameras' live feeds surveillance footage from many organizations including Tesla, Cloudflare, hospitals, law-enforcement departments, schools, and prisons.

Affected Systems

- Verkada's Clients

Vulnerability Overview

The hackers have provided video footage from Verkada clients' cameras to prove the breach to Bloomberg. One of the pieces of footage was from the Tesla factory located in Shanghai, China. The footage showed assembly workers working on the line. There were about 222 cameras from Tesla factories and warehouses that hackers claimed to have unauthorized access.

One of the hackers named Tillie Kottmann revealed the group's breach intention was to show the scope to which camera surveillance exists. They also wanted to demonstrate how vulnerable the systems are for exposing sensitive camera footage that could become HIPAA/HITECH violations.

To Gain unauthorized access to Verkada, hackers use a "root" account they found publicly on the Internet to access all of Verkada clients' cameras. Hackers immediately lost access to the cameras after Verkada get notified about the breach. Verkada has disabled all internal administrator accounts to prevent unauthorized access from hackers.

According to Hank Schless, a security expert, this incident was most likely done through a spear-phishing attack that uses social engineering techniques to steal companies' sensitive credentials from lower-level employees.

Recommendation

Conduct regular Employee Security Awareness training for employees and make sure your video surveillance system is up to date with patching.

Reference

https://threatpost.com/breach-verkada-security-camera-tesla-cloudflare/164635/

TWITTER ADS USED FOR CRYPTOCURRENCY SCAMS

Malicious actors are using Promoted tweets to scam Twitter users by advertising cryptocurrency giveaways. These scammers would usually takeover credible Twitter accounts that would appear trustworthy to this social network's regular users. Some of the account names used were Tesla, Gemini Exchange, and Social Capital. How successful this scam is speaks to the amount of money scammers generated with Elon Musk's fake giveaway. They gained more than $580,000 in just one week. Scamming tweets will have URLs listed on the advertisement. When the victim clicks on this URL, they will be redirected to the malicious website that will look like a dedicated web page.

Affected Systems

- Twitter

Vulnerability Overview

The Twitter articles were assuring readers that if they make a bitcoin payment to a promoted address, they will receive twice as much back. Researchers noticed a pattern that hackers were usually hacking accounts that were dormant. This way, they can continue with their scams without being seen by the account owner. Hackers would usually immediately change the email address to prevent the account owner from recovering it quickly. Researchers are assuming that the reason behind this vulnerability is a hacked back-end admin panel. Malicious attackers overcame even two-factor authentication that many accounts had as an extra level of protection.

Indicators of Compromise

Cryptocurrency:

Ethereum:

0xc77Ec8E5bbB723e6cEa13fD33bfF53262bb02b86 - 0.118890894374483125 Ether
0xE1a6d4699Bd6520ADdEcD46b52dd2eFC833142ED - 0.915305158603885603 Ether

Bitcoin:

1MoP7JTQuJE8K9pv8mV9uwo5efCgRtLYNU - 0.02196955 BTC
1MUSK2xaUCQmdEM8DrUJQ9RSgTdLqnKium - 0.54653960 BTC
1Musk7UAHXM6YBtccdaqK7ttsRxSTUSDVH - 0.11815051 BTC

Recommendation

It is recommended to follow regular cybersecurity protocols and be informed about recent malicious trends so these types of scams can be identified and prevented.

Reference

https://www.bleepingcomputer.com/news/security/scammers-promote-fake-cryptocurrency-giveaways-via-twitter-ads/