Threat Bulletin – May 6th to 24th, 2023

Table of Contents

CyFlare, LLC
21 Goodway Drive, Suite A4
Rochester, NY 14623

P: +1 877-729-3527
E: sales@cyflare.com

CyFlare, LLC
21 Goodway Drive, Suite A4
Rochester, NY 14623

P: +1 877-729-3527
E: sales@cyflare.com

Threat 1: New Ransomware Strain 'CACTUS' Exploits VPN Flaws to Infiltrate Networks

- https://thehackernews.com/2023/05/new-ransomware-strain-cactus-exploits.html
- https://www.kroll.com/en/insights/publications/cyber/cactus-ransomware-prickly-new-variant-evades-detection

1.1 – Affected Entities: Vulnerable VPN devices

1.2 – Detailed Description:

- Cybersecurity researchers have shed light on a new ransomware strain called CACTUS that has been found to leverage known flaws in VPN appliances to obtain initial access to targeted networks.
- Once inside the network, CACTUS actors attempt to enumerate local and network user accounts in addition to reachable endpoints before creating new user accounts and leveraging custom scripts to automate the deployment and detonation of the ransomware encryptor via scheduled tasks.
- Following successful exploitation of vulnerable VPN devices, an SSH backdoor is set up to maintain persistent access, and a series of PowerShell commands are executed to conduct network scanning and identify a list of machines for encryption.
- Also taken are steps to disable and uninstall security solutions and extract credentials from web browsers and the Local Security Authority Subsystem Service (LSASS) for escalating privileges.
- Privilege escalation is succeeded by lateral movement, data exfiltration, and ransomware deployment, which is achieved using a PowerShell script.

1.3 – Recommendation:

- Ensure that all enterprise systems are current and enforce the least privileged principle.

1.4 – SOC Response:

- The SOC is currently developing queries and ATH rules using our threat emulation platform to detect and notify clients of any activity related to Cactus Ransomware.

Threat 2: New 'MichaelKors' Ransomware-as-a-Service Targeting Linux and VMware ESXi Systems

- https://thehackernews.com/2023/05/new-michaelkors-ransomware-as-service.html
- https://www.crowdstrike.com/blog/hypervisor-jackpotting-lack-of-antivirus-support-opens-the-door-to-adversaries/

2.1 – Affected Entities: VMware EXSI

2.2 – Detailed Description:

- A new ransomware-as-service (RaaS) operation called MichaelKors has become the latest file-encrypting malware to target Linux and VMware ESXi systems.
- VMware ESXi hypervisors are becoming an attractive target because the software runs directly on a physical server, granting a potential attacker the ability to run malicious ELF binaries and gain unfettered access over the machine's underlying resources.
- Attackers looking to breach ESXi hypervisors can use compromised credentials, gain elevated privileges, laterally move through the network, or escape the confines of the environment via known flaws to advance their motives.

2.3 – Recommendations:

- Organizations are recommended to avoid direct access to ESXi hosts, enable two-factor authentication, take periodic backups of ESXi datastore volumes, apply security updates, and conduct security posture reviews.

Threat 3: Ransomware Hackers Using AuKill Tool to Disable EDR Software Using BYOVD Attack

- https://thehackernews.com/2023/04/ransomware-hackers-using-aukill-tool-to.html
- https://news.sophos.com/en-us/2023/04/19/aukill-edr-killer-malware-abuses-process-explorer-driver/

3.1 – Affected Entities: Microsoft utility, Process Explorer

3.2 – IOCs:

- f7b0369169dff3f10e974b9a10ec15f7a81dec54
- ff11360f6ad22ba2629489ac286b6fdf4190846e

3.3 – Detailed Description:

- Threat actors are employing a previously undocumented "defense evasion tool" dubbed AuKill that's designed to disable endpoint detection and response (EDR) software using a Bring Your Own Vulnerable Driver (BYOVD) attack.

- The AuKill tool abuses an outdated version of the driver used by version 16.32 of the Microsoft utility, Process Explorer, to disable EDR processes before deploying either a backdoor or Ransomware on the target system.
- The BYOVD technique relies on threat actors misusing a legitimate but out-of-date and exploitable driver signed by Microsoft (or using a stolen or leaked certificate) to gain elevated privileges and turn off security mechanisms.
- By using valid, susceptible drivers, the idea is to bypass a key Windows safeguard known as Driver Signature Enforcement that ensures a valid code signing authority has signed kernel-mode drivers before they are allowed to run.

3.4 – Recommendation:

- It is highly suggested to check if your endpoint security product implements and enables tamper protection. This feature provides a strong layer against such types of attacks.

Threat 4: Fake in-browser Windows updates push Aurora info-stealer malware

- https://www.bleepingcomputer.com/news/security/fake-in-browser-windows-updates-push-aurora-info-stealer-malware/
- https://blog.morphisec.com/in2al5d-p3in4er

4.1 – Affected Entities: Fake in-browser Windows Updates

4.2 – IOCs:

- activessd[.]ru
- clickaineasdfer[.]ru
- oled8kultra[.]site
- evatds[.]ru
- cv-builder[.]site
- 66383d931f13bcdd07ca6aa50030968e44d8607cf19bdaf70ed4f9ac704ac4d1
- 380978251b2c661ff15b2610763770dfa14fb360ad0ca64243e0d5d5893952cb

4.3 – Detailed Description:

- A recently spotted malvertising campaign tricked users with an in-browser Windows update simulation to deliver the Aurora information-stealing malware. The malvertising operation relies on popunder ads on adult content websites with high-traffic adult content and redirects potential victims to a malware-serving location.
- Popunder ads are cheap 'pop-up' ads that launch behind the active browser window, staying hidden from the user until they close or move the main browser window. The threat actor devised an imaginative idea where the popunder renders a full-screen browser window that simulates a Windows system update screen.

- All the IOCs mentioned above served for download a file named "ChromeUpdate.exe," revealing the deception of the full-screen browser screen; however, some users were still tricked into deploying the malicious executable.

4.4 – Recommendation:

- Have Admins block these IOCs on their network firewalls to help prevent such an attack.

Threat 5: Researchers Discover 3 Vulnerabilities in Microsoft Azure API Management Service

- https://thehackernews.com/2023/05/researchers-discover-3-vulnerabilities.html
- https://ermetic.com/blog/azure/when-good-apis-go-bad-uncovering-3-azure-api-management-vulnerabilities/

5.1 – Affected Entities: Microsoft Azure API Management Service

5.2 – IOCs: No IOCs found

5.3 – Detailed Description:

- Three new security flaws have been disclosed in Microsoft Azure API Management service that could be abused by malicious actors to gain access to sensitive information or backend services.
- This includes two server-side request forgery (SSRF) flaws and one instance of unrestricted file upload functionality in the API Management developer portal, according to Israeli cloud security firm Ermetic.
- By abusing the SSRF vulnerabilities, attackers could send requests from the service's CORS Proxy and the hosting proxy itself, access internal Azure assets, deny service and bypass web application firewalls.
- Exploitation of SSRF flaws can result in loss of confidentiality and integrity, permitting a threat actor to read internal Azure resources and execute unauthorized code.

5.4 – Recommendation:

- Update Microsoft Azure API Management service with the latest security patches

Threat 6: Cisco phone adapters vulnerable to RCE attacks, no fix available

- https://www.bleepingcomputer.com/news/security/cisco-phone-adapters-vulnerable-to-rce-attacks-no-fix-available/

6.1 – Affected Entities: Cisco Phone Adapters

6.2 – Detailed Description:

- Cisco has disclosed a vulnerability in the web-based management interface of Cisco SPA112 2-Port Phone Adapters, allowing an unauthenticated, remote attacker to execute arbitrary code on the devices.
- This vulnerability is caused by a missing authentication process within the firmware upgrade function. This can allow an attacker to execute arbitrary code on the affected device with full privileges.
- Gaining access to these devices could help a threat actor spread laterally on a network without detection, as security software does not commonly monitor these types of devices.
- Since Cisco SPA112 has reached the end of its life, it is no longer supported by the vendor and will not receive a security update. Also, Cisco has provided no mitigations for this vulnerability.

6.3 – Recommendation:

- Replace the impacted phone adapters with Cisco ATA 190 Series Analog Telephone Adapter or implement additional security layers.

Threat 7: Attacks increasingly use malicious HTML email attachments

- https://www.csoonline.com/article/3695075/attacks-increasingly-use-malicious-html-email-attachments.html
- https://blog.barracuda.com/2023/05/03/threat-spotlight-malicious-html-attachments-doubles/

7.1 – Affected Entities: HTML Emails

7.2 – Detailed Description:

- Researchers warn that attackers rely more on malicious HTML files in their attacks, with malicious files now accounting for half of all HTML attachments sent via email.
- HTML is flexible in terms of what types of attacks it can enable. One of the most common use cases is credential phishing with attackers crafting HTML attachments that, when opened, masquerade as the login page for various services.
- This can also be dynamic, with the HTML including JavaScript code redirecting the user to a phishing site.

- Protection against malicious HTML-based attacks should consider the entire email carrying HTML attachments, looking at all redirects, and analyzing the content of the email for malicious intent.

7.3 – Recommendation:

- Training employees to spot and report malicious HTML attachments and to be wary of such attachments from unknown sources is also essential.
- Choose email security solutions that evaluate the entire email context, not just the attachment's contents.

Threat 8: CVE-2023-28231: RCE in the Microsoft Windows DHCPv6 Service

- https://www.zerodayinitiative.com/blog/2023/5/1/cve-2023-28231-rce-in-the-microsoft-windows-dhcpv6-service
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28231

8.1 – Affected Entities: Microsoft Windows DHCPv6 Service

8.2 – Detailed Description:

- A heap-based buffer overflow has been reported in Microsoft DHCPv6 Server.
- The vulnerability is due to improper processing of DHCPv6 Relay-forward messages.
- A remote attacker can exploit this vulnerability by sending crafted DHCPv6 Relay-forward messages to the target server.
- Successful exploitation could result in the execution of arbitrary code with administrative privileges.
- To detect an attack exploiting this vulnerability, the detection device must monitor and parse traffic on UDP ports 546 and 547 and be capable of inspecting DHCPv6 packets on UDP port 547.

8.3 – Recommendation:

- Microsoft Addresses this vulnerability in their April 2023 Security patch release. Admins should take steps to have their systems running on the latest security patches installed.

Threat 9: Hackers target vulnerable Veeam backup servers exposed online

- https://www.bleepingcomputer.com/news/security/hackers-target-vulnerable-veeam-backup-servers-exposed-online/
- https://labs.withsecure.com/publications/fin7-target-veeam-servers
- https://github.com/WithSecureLabs/iocs/blob/master/FIN7VEEAM/iocs.csv

9.1 – Affected Entities: Veeam

9.2 – IOCs:

- 8687b6b1508a93556d6e30d14e5c4ee9971f2d80
- 194.87.148.41
- powershell.exe -noni -nop -exe bypass -f \\XXX.XXX.XXX.XXX\ADMIN$\temp\nFcv5ke38cnE.ps1
- reg query "HKLM\software\veeam\veeam backup and replication."

9.3 – Detailed Description:

- Veeam backup servers are being targeted by at least one group of threat actors known to work with multiple high-profile ransomware gangs.
- Tracked as CVE-2023-27532, the security issue exposes encrypted credentials stored in the VBR configuration to unauthenticated users in the backup infrastructure. This could be used to access the backup infrastructure hosts.
- The threat actor initially executed the PowerTrash PowerShell script, seen in past attacks attributed to FIN7, that included a payload, the DiceLoader/Lizar backdoor to be executed on the compromised machine.
- Once they got access to the host, the hackers used their malware, various commands, and custom scripts to collect system and network information and credentials from the Veeam backup database.
- Persistence for DiceLoader was achieved through a custom PowerShell script called PowerHold, the researchers at WithSecure say, adding that the threat actor also attempted lateral movement using stolen credentials, testing their access with WMI invocations and 'net share' commands.

9.4 – Recommendation:

- Patch and configure their backup servers appropriately as outlined in KB4424: CVE-2023-27532.

Threat 10: VMware Releases Critical Patches for Workstation and Fusion Software

- https://thehackernews.com/2023/04/vmware-releases-critical-patches-for.html
- https://www.vmware.com/security/advisories/VMSA-2023-0008.html

10.1 – Affected Entities: VMware

10.2 – Detailed Description:

- VMware has released updates to resolve multiple security flaws impacting its Workstation and Fusion software, the most critical of which could allow a local attacker to achieve code execution.
- CVE-2023-20869 is described as a stack-based buffer-overflow vulnerability that resides in the functionality for sharing host Bluetooth devices with the virtual machine.
- A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the VMX process runs on the host.
- Also patched by VMware is an out-of-bounds read vulnerability affecting the same feature (CVE-2023-20870), that could be abused by a local adversary with admin privileges to read sensitive information contained in hypervisor memory from a virtual machine.

10.3 – Recommendation:

- Updating VMware Workstation & Fusion to 17.0.2 & 13.0.2 respectively.
- VMware is suggesting that users turn off Bluetooth support on the virtual machine.

Threat 11: Thousands of Apache Superset servers exposed to RCE attacks

- https://www.bleepingcomputer.com/news/security/thousands-of-apache-superset-servers-exposed-to-rce-attacks/
- https://www.horizon3.ai/cve-2023-27524-insecure-default-configuration-in-apache-superset-leads-to-remote-code-execution/

11.1 – Affected Entities: Apache Superset Servers

11.2 – Detailed Description:

- Apache Superset is vulnerable to authentication bypass and remote code execution at default configurations, allowing attackers to potentially access and modify data, harvest credentials, and execute commands.
- Apache Superset used a default Flask Secret Key to sign authentication session cookies. As a result, attackers can use this default key to forge session cookies that allow them to log in with administrator privileges to servers that did not change the key.
- This default configuration is currently detectable in about 2,000 internet-exposed servers belonging to universities, corporations of varying sizes, government organizations, and more.

- This widely used default Flask secret key is known to attackers who may use flask-unsign and forge their own cookies to gain administrator access on the target, accessing connected databases or executing arbitrary SQL statements on the application server.

11.3 – Recommendation:

- Apache has advised admins to change the secret keys from the default configurations to prevent exploitation.

Threat 12: KeePass Exploit Allows Attackers to Recover Master Passwords from Memory

- https://thehackernews.com/2023/05/keepass-exploit-allows-attackers-to.html
- https://github.com/vdohney/keepass-password-dumper

12.1 – Affected Entities: KeePass

12.2 – Detailed Description:

- A proof-of-concept (PoC) has been made available for a security flaw impacting the KeePass password manager that could be exploited to recover a victim's master password in cleartext under specific circumstances.
- The issue, tracked as CVE-2023-32784, impacts KeePass versions 2.x for Windows, Linux, and macOS, and is expected to be patched in version 2.54, which is likely to be released early next month.
- The vulnerability concerns how a custom text box field for entering the master password handles user input. Specifically, it has been found to leave traces of every character the user types in the program memory.
- This leads to a scenario whereby an attacker could dump the program's memory and reassemble the password in plaintext except for the first character.

12.3 – Recommendation:

- Users are advised to update to KeePass 2.54 once it becomes available.