



NETMANAGEIT

Intelligence Report

Microsoft Zero Day Vulnerability

CVE-2023-36884 Being Actively Exploited

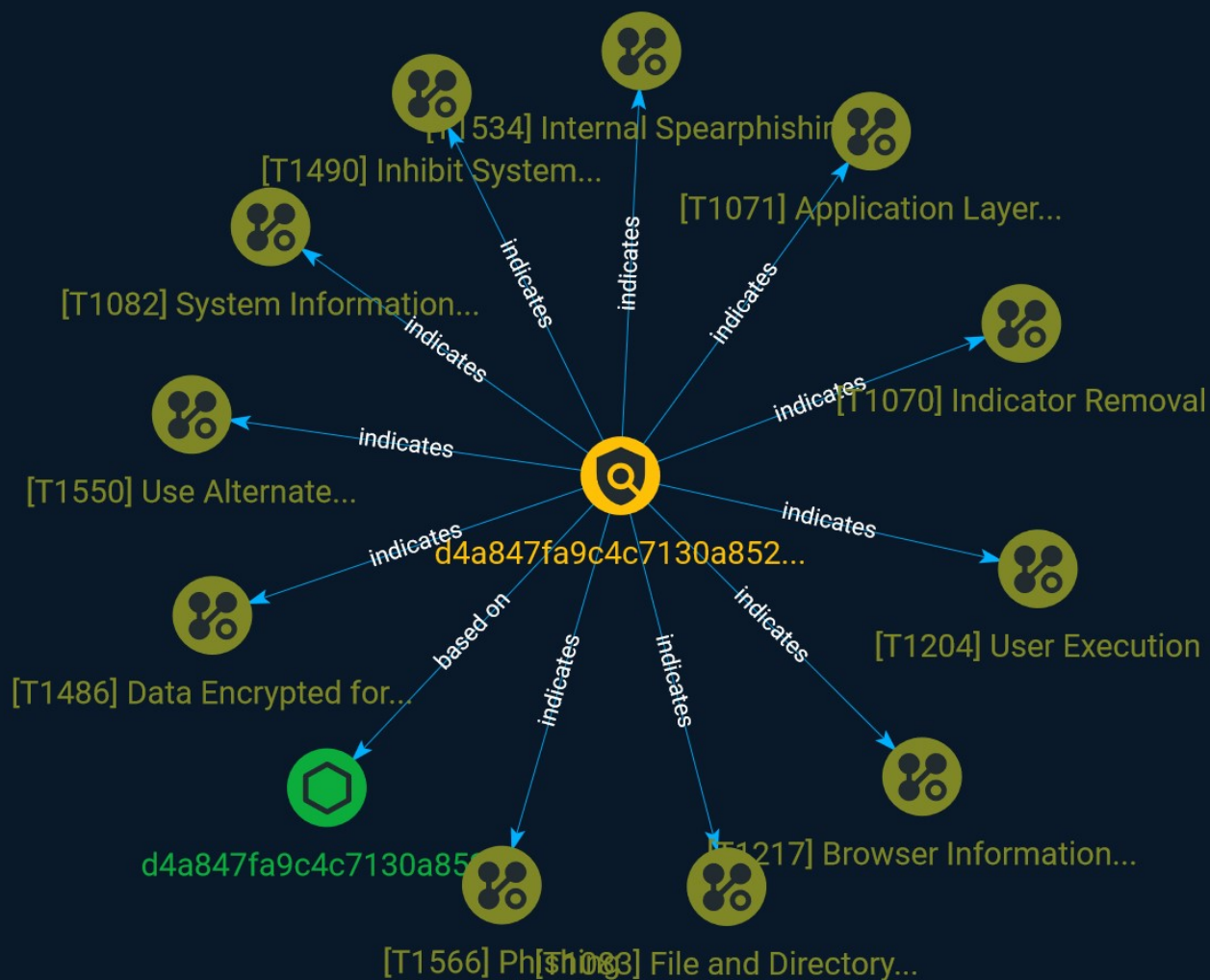


Table of contents

Overview

● Description	3
● Confidence	3

Entities

● Indicator	4
● Attack-Pattern	5

Observables

● StixFile	14
------------	----

External References

● External References	15
-----------------------	----

Overview

Description

CRIL analyzes the impact of a Zero-Day Exploit for CVE-2023-36884 in cyber espionage and ransomware operations.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Indicator

Name

d4a847fa9c4c7130a852a2e197b205493170a8b44426d9ec481fc4b285a92666

Pattern Type

stix

Pattern

[file:hashes:'SHA-256' =
'd4a847fa9c4c7130a852a2e197b205493170a8b44426d9ec481fc4b285a92666']

Attack-Pattern

Name
Internal Spearphishing
ID
T1534
Description

Adversaries may use internal spearphishing to gain access to additional information or exploit other users within the same organization after they already have access to accounts or systems within the environment. Internal spearphishing is multi-staged campaign where an email account is owned either by controlling the user's device with previously installed malware or by compromising the account credentials of the user. Adversaries attempt to take advantage of a trusted internal account to increase the likelihood of tricking the target into falling for the phish attempt.(Citation: Trend Micro When Phishing Starts from the Inside 2017) Adversaries may leverage [Spearphishing Attachment](<https://attack.mitre.org/techniques/T1566/001>) or [Spearphishing Link](<https://attack.mitre.org/techniques/T1566/002>) as part of internal spearphishing to deliver a payload or redirect to an external site to capture credentials through [Input Capture](<https://attack.mitre.org/techniques/T1056>) on sites that mimic email login interfaces. There have been notable incidents where internal spearphishing has been used. The Eye Pyramid campaign used phishing emails with malicious attachments for lateral movement between victims, compromising nearly 18,000 email accounts in the process.(Citation: Trend Micro When Phishing Starts from the Inside 2017) The Syrian Electronic Army (SEA) compromised email accounts at the Financial Times (FT) to steal additional account credentials. Once FT learned of the campaign and began warning employees of the threat, the SEA sent phishing emails mimicking the Financial Times IT department and were able to compromise even more users.(Citation: THE FINANCIAL TIMES LTD 2019.)

Name

Browser Information Discovery

ID

T1217

Description

Adversaries may enumerate information about browsers to learn more about compromised environments. Data saved by browsers (such as bookmarks, accounts, and browsing history) may reveal a variety of personal information about users (e.g., banking sites, relationships/interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.(Citation: Kaspersky Autofill) Browser information may also highlight additional targets after an adversary has access to valid credentials, especially [Credentials In Files](<https://attack.mitre.org/techniques/T1552/001>) associated with logins cached by a browser.

Specific storage locations vary based on platform and/or application, but browser information is typically stored in local files and databases (e.g., `%APPDATA%/Google/Chrome`).(Citation: Chrome Roaming Profiles)

Name

Use Alternate Authentication Material

ID

T1550

Description

Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls. Authentication processes generally require a valid identity (e.g., username) along with one or more authentication factors (e.g., password, pin, physical smart card, token generator, etc.). Alternate authentication material is legitimately generated by systems after a user or application successfully authenticates by providing a valid identity and the required authentication factor(s). Alternate authentication material may also be generated during the identity creation process. (Citation: NIST Authentication)(Citation: NIST MFA) Caching alternate authentication material allows the system to verify an identity has successfully authenticated without asking the user to reenter authentication factor(s). Because the alternate authentication must be maintained by the system—either in memory or on disk—it may be at risk of being stolen through [Credential Access](https://attack.mitre.org/tactics/TA0006) techniques. By stealing alternate authentication material, adversaries are able to bypass system access controls and authenticate to systems without knowing the plaintext password or any additional authentication factors.

Name

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](<https://attack.mitre.org/techniques/T1564/008>)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL,

download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Inhibit System Recovery

ID

T1490

Description

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable_notif_synology_ransom) A number of native Windows utilities have been used by adversaries to disable or delete system recovery features: * `vssadmin.exe` can be used to delete all volume shadow copies on a system - `vssadmin.exe delete shadows /all /quiet` * [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) can be used to delete volume shadow copies - `wmic shadowcopy delete` * `wbadmin.exe` can be used to delete the Windows Backup Catalog - `wbadmin.exe delete catalog -quiet` * `bcdedit.exe` can be used to disable automatic Windows recovery features by modifying boot configuration data - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no` * `REAgentC.exe` can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system On network devices, adversaries may leverage [Disk Wipe](https://attack.mitre.org/techniques/T1561) to delete backup firmware images and reformat the file system, then [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations. Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet

Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack)(Citation: Rhino Security Labs AWS S3 Ransomware)

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](<https://attack.mitre.org/techniques/T1566>). While [User Execution](<https://attack.mitre.org/techniques/T1204>) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](<https://attack.mitre.org/techniques/T1534>). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](<https://attack.mitre.org/techniques/T1219>), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](<https://attack.mitre.org/techniques/T1204>). For example, tech support scams can be facilitated through [Phishing](<https://attack.mitre.org/techniques/T1566>), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](<https://attack.mitre.org/techniques/T1219>).(Citation: Telephone Attack Delivery)

Name

Data Encrypted for Impact

ID

T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](<https://attack.mitre.org/techniques/T1222>) or [System Shutdown/Reboot](<https://attack.mitre.org/techniques/T1529>), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](<https://attack.mitre.org/techniques/T1078>), [OS Credential Dumping](<https://attack.mitre.org/techniques/T1003>), and [SMB/Windows Admin Shares](<https://attack.mitre.org/techniques/T1021/002>).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](<https://attack.mitre.org/techniques/T1491/001>), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

File and Directory Discovery

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](<https://attack.mitre.org/techniques/T1083>) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include ``dir``, ``tree``, ``ls``, ``find``, and ``locate``. (Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](<https://attack.mitre.org/techniques/T1106>). Adversaries may also leverage a [Network Device CLI](<https://attack.mitre.org/techniques/T1059/008>) on network devices to gather file and directory information (e.g. ``dir``, ``show flash``, and/or ``nvram``). (Citation: US-CERT-TA18-106A)

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](<https://attack.mitre.org/techniques/T1082>) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](<https://attack.mitre.org/software/S0096>) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](<https://attack.mitre.org/techniques/T1059/008>) on network devices to gather detailed system information (e.g. `show version`). (Citation: US-CERT-TA18-106A) [System Information Discovery](<https://attack.mitre.org/techniques/T1082>) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment. (Citation: OSX.FairyTale) (Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine. (Citation: Amazon Describe Instance) (Citation: Google Instances Resource) (Citation: Microsoft Virtual Machine API)

StixFile

Value

d4a847fa9c4c7130a852a2e197b205493170a8b44426d9ec481fc4b285a92666

External References

-
- <https://otx.alienvault.com/pulse/64b5508de8c6ec231d0e45d5>
-
- <https://blog.cyble.com/2023/07/12/microsoft-zero-day-vulnerability-cve-2023-36884-being-actively-exploited/>