Issue 8 | Aug 2023

uptycs

Uptycs Quarterly Threat Bulletin

Prepared by the
Uptycs Threat Research Team

The quarterly threat intel bulletin provides insights on the current threat landscape. This intel is derived from our threat intelligence systems, sources, and a world-class threat research team which builds and proactively monitors the latest TTPs (Tactics, Techniques, and Procedures).

Organizations can use this bulletin as a tool to evaluate and form a more robust detection and protection posture against the latest threats on Windows, Linux, and macOS platforms.

Index

Q2 Threat Bulletin Highlights

1. MOVEit SQL Injection vulnerabilities were observed to be actively exploited by cyber-crime actors such as Clop ransomware operators.
2. In this quarter, we've observed the following prevalent malware:
    a. RedLine, AgentTesla, and SnakeKeylogger are the most prevalent malware in Q2 2023 observed for Windows platforms.
    b. Mirai and Gfagyt were seen in large numbers in Q2 2023 on the Linux platform.
    c. Bundlore continues to be evergreen in action on macOS.
3. Most Windows malware nominated LOLBin—rundll32.exe—as the most abused utility for Windows, and crontab has taken the top spot in abused utilities in Linux.
4. In macOS, openssl and curl are prevalent utilities widely leveraged by Shlayer and Bundlore.
5. LockBit, a known ransomware group, was identified as the most active group in Q2 by targeting several victims. Other active groups included BlackCat and Clop ransomware.
6. Threat actor activity from FIN7, Lazarus Group, Earth Longzi, APT28, and Kimsuky has been reported.

Critical Alerts

CVE-2023-35708, CVE-2023-35036, and CVE-2023-34362 - MOVEit SQL Injection Vulnerabilities

MOVEit Transfer is a file transfer software that allows organizations to securely exchange files with external parties. On Jun 1, 2023, Progress released a security advisory on the critical SQL injection vulnerability in MOVEit Transfer software. The vulnerability was warned to be critical in nature and tracked as CVE-2023-34362. All the MOVEit Transfer versions prior to 2020.1.6 (special patch also needs to be applied), 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1) and versions 2020.0.x or older were reported as vulnerable. Threat actors attributed to the Cl0p ransomware group had actively exploited this vulnerability. The attack involved deploying a webshell named human2.aspx in the server's directory. The webshell also used moveitisapi.dll to perform SQL injection and guestaccess.aspx to extract session information. Exploiting the vulnerability can lead to immediate deployment of ransomware or other malicious actions, with the ability to disable antivirus and execute arbitrary code.

The second vulnerability tracked as CVE-2023-35036 affected versions that were released before 2020.1.6 (special patch also needs to be applied), 2021.0.7 (13.0.7), 2021.1.5 (13.1.5), 2022.0.5 (14.0.5), 2022.1.6 (14.1.6), and 2023.0.2 (15.0.2) and versions 2020.0.x or older. This vulnerability allowed an unauthorized attacker, who doesn't have proper authentication, to gain access to the MOVEit Transfer database without permission. By sending a specially crafted malicious payload to certain parts of the MOVEit Transfer web application, the attacker can manipulate and access the content stored in the MOVEit database.

The third vulnerability tracked as CVE-2023-35708 affected versions released before 2020.1.6 (special patch also needs to be applied), 2021.0.8 (13.0.8), 2021.1.6 (13.1.6), 2022.0.6 (14.0.6), 2022.1.7 (14.1.7), and 2023.0.3 (15.0.3) and versions 2020.0.x (12.0) or older. This vulnerability could potentially result in unauthorized access and escalated privileges.

Techniques used by the malware samples

The Uptycs threat research team configured Uptycs XDR in our threat intelligence replication system to detect and label attacker behavior. This system contains the latest known suspicious and malicious files in Windows, Linux, and macOS platforms.

The top techniques/tactics triggered by malware samples are System Binary Proxy Execution (T1218), Impair Defenses (T1562), Scheduled Task/Job (T1053), Command and Scripting Interpreter (T1059), and Service Stop (T1489) described in the MITRE ATT&CK framework. The prevalence of these observed ATT&CK technique IDs is shown below.

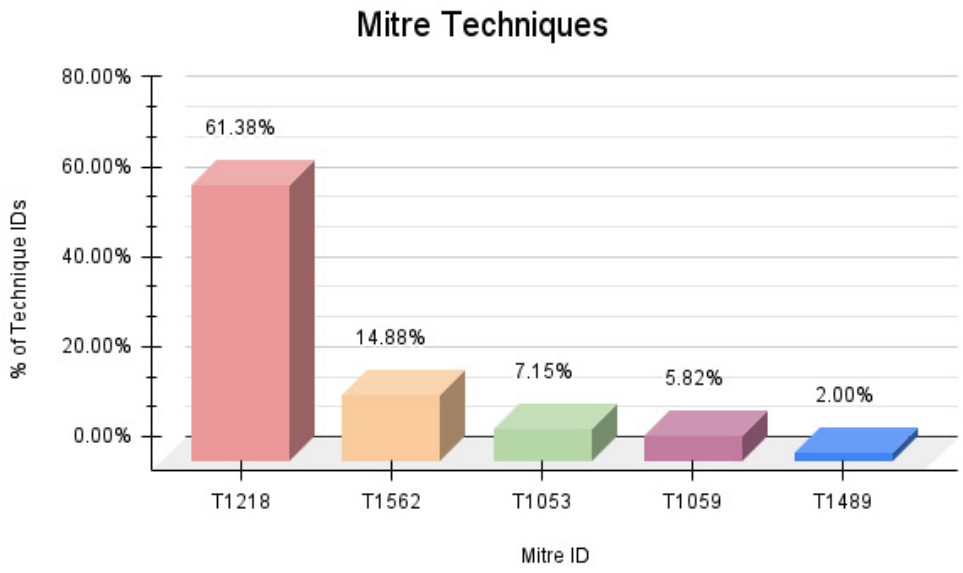

Fig.1–Observed ATT&CK technique IDs

Commonly abused commands and utilities

The malicious samples leverage the target operating systems' built-in utilities in their attack kill chain in an attempt to avoid detection. This method of using built-in utilities to evade defenses is also known as "living off the land." These utilities are mapped to our replication systems' tactics in Windows, Linux, and macOS.

Windows utilities abused by malware

In this quarter, we observed Rundll32.exe as the top abused utility. Powershell.exe, wscript.exe, taskkill.exe, and EQNEDT32.exe were the top abused utilities in Q2 2023. The list of the top 5 Windows utilities abused by malware and their prevalence is shown below.

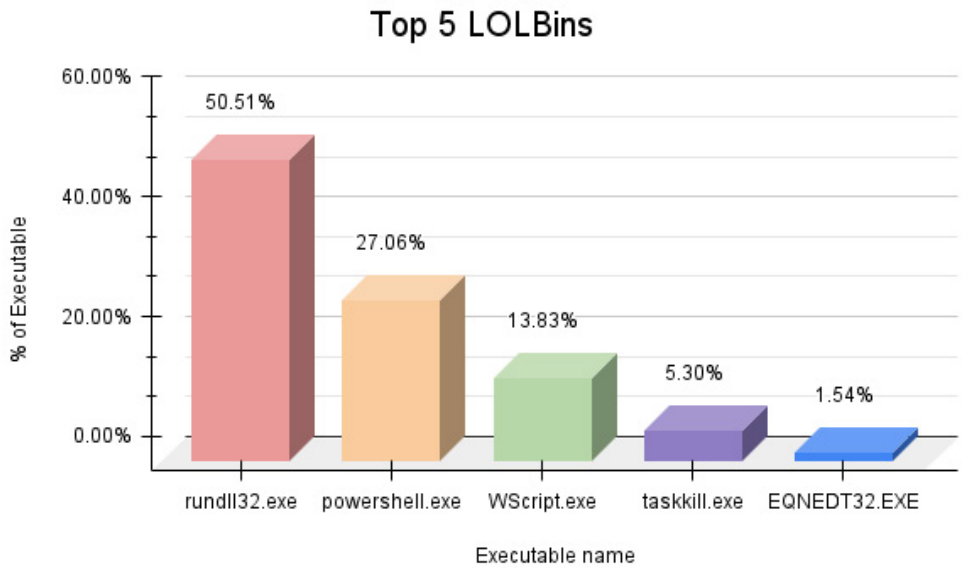

Figure 2–Top 5 Windows utilities abused by malware

Rundll32.exe

Tactic: Execution and Defense Evasion

- Rundll32.exe is a Microsoft-signed binary used to load dynamic link libraries (DLLs) in Windows. Adversaries may abuse rundll32.exe to proxy the execution of malicious code.
- Rundll32.exe is commonly associated with executing DLL payloads.
- Recently, Merdoor and LOBSHOT malware have used the rundll32 utility to launch additional malicious components.

powershell.exe

Tactic: Execution, Defense Evasion, and Discovery

- Adversaries abuse PowerShell in multiple ways for the use of execution of commands, evade detection, obfuscate malicious activity, spawn additional processes, remotely download and execute arbitrary code and binaries, gather information, change system configurations, etc.
- In the recent BATLoader and Emotet campaign activity, the malware used PowerShell script for the evade detection and to launch further payloads.

WScript.exe

Tactic: Execution and Defense Evasion

Wscript.exe, also known as Windows Script Host, appears to be a Microsoft Windows-based process that is being abused for malicious purposes by attackers.

Adversaries may use wscript.exe to execute VBA, VBS, and JS files.

WScript.exe is actively abused to execute FormBook and Remcos RAT malware.

taskkill.exe

Tactic: Impact

Taskkill.exe is a type of executable file developed by Microsoft for the Windows Operating System. This has the function of ending one or more tasks or processes. However, it is also being used by malware authors to terminate processes on the victim system.

Asylum Ambuscade and Rorschach ransomware execute taskkill to kill processes or stop services.

EQNEDT32.EXE

Tactic: Execution and Defense Evasion

- Microsoft Equation Editor, a component of Microsoft Office, is an out-of-process component object model server, and it is an executable file named eqnedt32.exe.
- When a victim views an infected RTF document in Microsoft Word, the vulnerability allows an attacker to execute code remotely.
- Recently, the operator used the Equation Editor vulnerability to download and execute the malware payload, such as Agent Tesla and Remcos RAT.

Linux utilities abused by malware

In this quarter, crontab was the top abused Linux utility, as the Mirai malware on Linux was observed frequently.

The top five Linux utilities abused by malware and their prevalence is shown below.

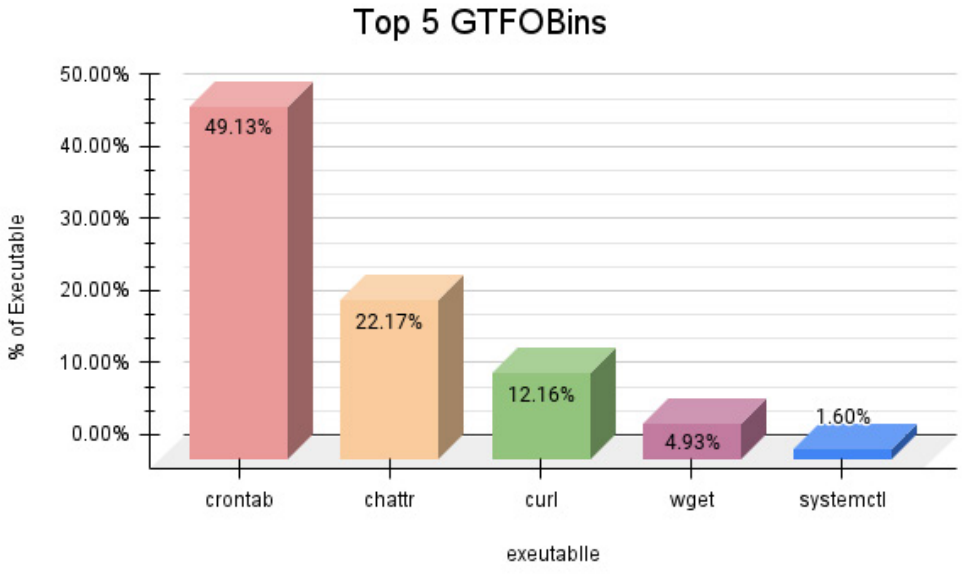

Figure 3–Top five Linux utilities abused by malware

crontab

Tactic: Execution and Persistence

- For Unix-like operating systems, the cron utility is a time-based job scheduler.
- The cron utility is a time-based job scheduler for Unix-like operating systems. The crontab file contains the schedule of cron entries to be run and the specified times for execution.
- An adversary may use cron in Linux or Unix environments to execute programs at system startup or on a scheduled basis for Persistence.
- RapperBot and Mirai botnet malware had recently used this cron utility for the persistence of an attack.

Chattr

Tactic: Defense Evasion and Persistence

- chattr, also known as Change Attribute, is a command line utility that is used to set/unset certain attributes to a file in a Linux system to secure accidental deletion or modification of important files and folders.
- Threat actors will abuse this utility to prevent modification of their malicious files that they have modified for purposes of persistence.
- It's been reported that Kinsing malware executes crontab and chattr commands for persistence and defense evasion.

curl

Tactic: Command-and-control and Defense Evasion

- The curl is a command-line tool that provides user authentication when downloading files from an FTP server and proxy support.
- It can download multiple files in any file format from multiple URLs, initiate file transfer resumption in case of an interruption, and many more.
- RHOMBUS malware has used cURL commands to download new tools for further malicious activity.

wget

Tactic: Privilege Escalation and Command-and-control

- wget is a Linux command-line utility that allows users to download files from the internet. Adversaries use this to download next-stage payloads.
- ChamelDoH threat actor uses the wget command to download a file from the malicious URL.

systemctl

Tactic: Defense Evasion

- Systemctl is a Linux command-line utility used to control and manage systemd and services. However, the attackers abuse this utility to stop EDR services in Linux.
- TeamTNT has used the systemctl utility to establish persistence through the creation of a cryptocurrency mining system service.

LOOBins (macOS Binaries) Utilities abused by malware

LOOBins, also known as Living Off the Orchard, are the macOS Binaries used on OSX systems.

As LoLBins and GTFOBins, LOOBins can also be leveraged for malicious purposes to achieve tactics such as command execution, privilege escalation, persistence, and data exfiltration.

The top five macOS utilities abused by malware and their prevalence is shown below.

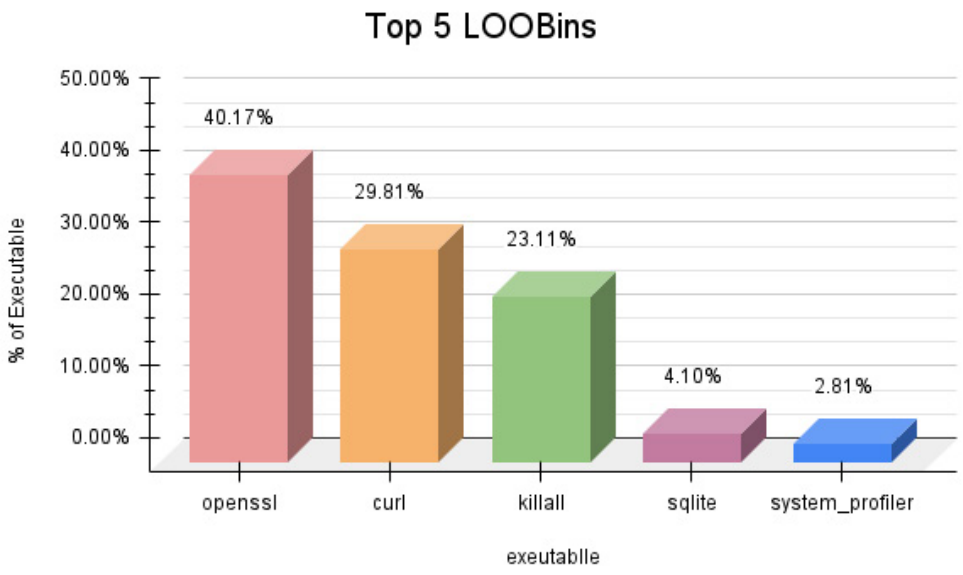

Figure 4–Top five macOS utilities abused by malware

Openssl

Tactic: Defense Evasion

- OpenSSL program is a command line tool for using the various cryptography functions of OpenSSL's crypto library from the shell.
- It has been reported that malicious binaries can use OpenSSL with base64, Advanced Encryption Standard (AES), CBC (Cipher Block Chaining) to prevent security scanners.
- In the recent analysis activity, the Snake malware has been found to use the OpenSSL library for malicious activity.

curl

Tactic: Command and control

- cURL is a command-line tool that lets users transfer data to or from a server using various protocols.
- The malicious binaries download the Bundlore payload to the tmp directory using a curl request to the C2 server.

killall

Tactic: Defense Evasion

- Killall is used to kill the processes specified by command or pattern match.
- Killall Terminal is used to kill the running script's terminal window after the bash script activity is completed.
- Shlayer malware uses several macOS utilities like killall in their attack kill chain.

sqlite

Tactic: Exfiltration

- SQLite is a transactional SQL database engine in macOS generally used to create databases that can be transported across machines.
- By using a malicious SQLite database, the attackers can take a variety of different actions, including compromising the legitimate applications that rely on these databases.
- Shlayer malware leverages sqlite to get the history of downloaded files from the internet in the exfiltration phase of the attack lifecycle.

system_profiler

Tactic: Discovery

- System_profiler (formerly known as System Information) in OSX provides a detailed breakdown of the hardware and software configuration of a Mac.
- Bundlore leverages system_profiler to get system hardware related information via "system_profiler -nospawn -xml SPHardwareDataType -detailLevel full" command.

Top prevalent malware families in the wild

Using our in-house Uptycs EDR armed with YARA process scanning, we identified the following malware families as most prevalent across Linux, Windows, and macOS platforms. The research team has also added coverage of all the TTPs and YARA coverage for the malware processes in the Uptycs platform. Customers can now view the toolkit profiles of the malware when detection is triggered in Uptycs.

The top malware seen across Windows, Linux, and macOS are as follows.

Windows:

Redline Stealer

- RedLine Stealer is a powerful data collection tool capable of extracting login credentials from a wide range of sources, including web browsers, FTP clients, email apps, Steam, instant messaging clients, and VPNs.
- Additionally, it can also collect authentication cookies and card numbers stored in browsers, chat logs, local files, and even cryptocurrency wallet databases.
- Recently, it has also been observed that RedLine malware is being distributed through malicious advertisement campaigns in Google's search engine with themes that are related to AI tools such as Midjourney and ChatGPT.

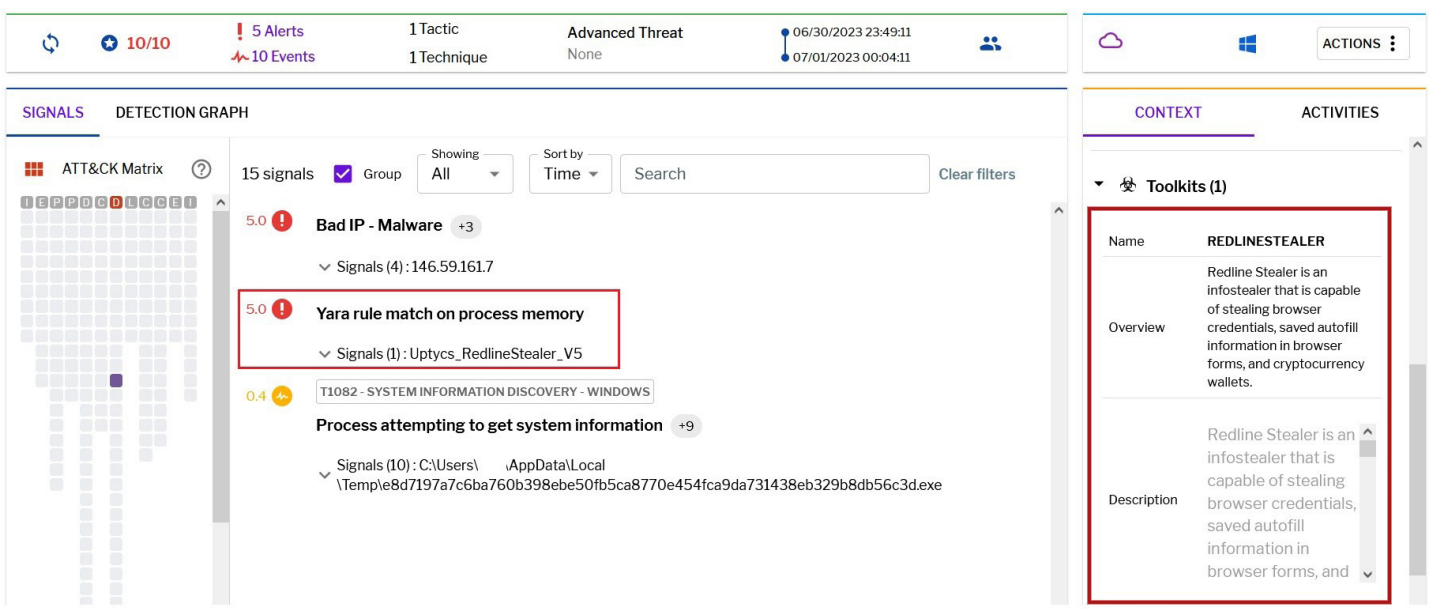

Figure 5–Uptycs XDR detection of RedlineStealer

AgentTesla

- Agent Tesla is one of the leading malware threats organizations face with the ability to steal various types of sensitive information from an organization's infected computers.
- Agent Tesla is a .Net-based Remote Access Trojan (RAT) and data stealer for gaining initial access often used for Malware-As-A-Service (MaaS).
- Agent Tesla is primarily an information stealer with the ability to monitor keystrokes, capture screenshots, steal credentials, and exfiltrate back to the threat actor using a variety of protocols.
- Agent Tesla malware spreads primarily via phishing emails where users are lured into executing malicious files disguised as Microsoft Office documents, zip, image files, etc.
- When executed, these initial payloads connect to a remote command and control (C2) server to download later stages of the malware.
- After initial access, persistence is achieved by modifying the registry Run keys or creating scheduled tasks. The malware then proceeds to collect data from browsers, mail, and VPN clients and exfiltrate using various protocols or applications (SMTP, FTP, Telegram, Discord, etc.).

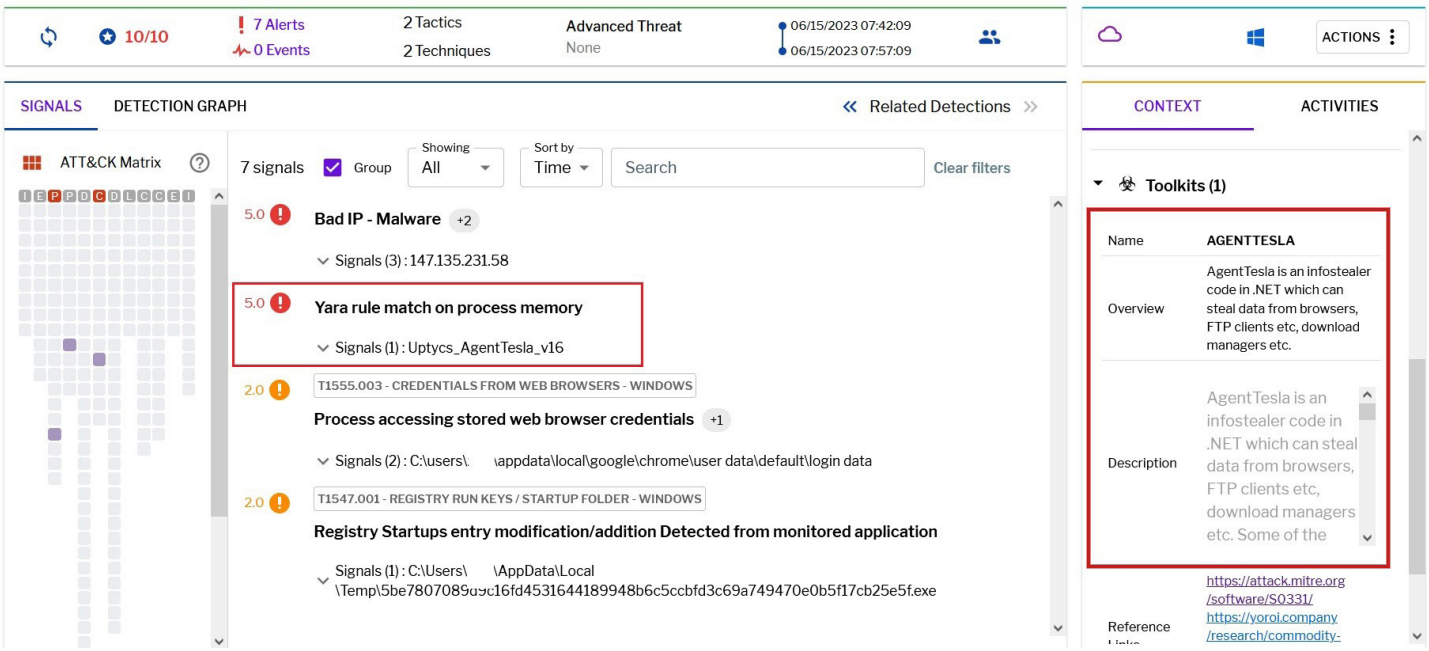

Figure 6–Uptycs XDR detection of AgentTesla

Snake Keylogger

- Snake Keylogger is a modular malware program that was created using the .NET developer platform.
- It was first discovered in the wild in November 2020. Snake Keylogger acts as an info-stealer that exfiltrates sensitive information from infected systems, has keyboard logging and screenshot capabilities, and the ability to extract information from systems' clipboards.
- When a Snake Keylogger is sent to a potential victim, it is contained within an attachment.
- If the recipient opens the attachment, they are asked to open a DOCX file. This DOCX file contains a macro that allows for the launch of Snake Keylogger. If the victim uses a version of Microsoft Office with security vulnerabilities, the keylogger can exploit them and infect the device.

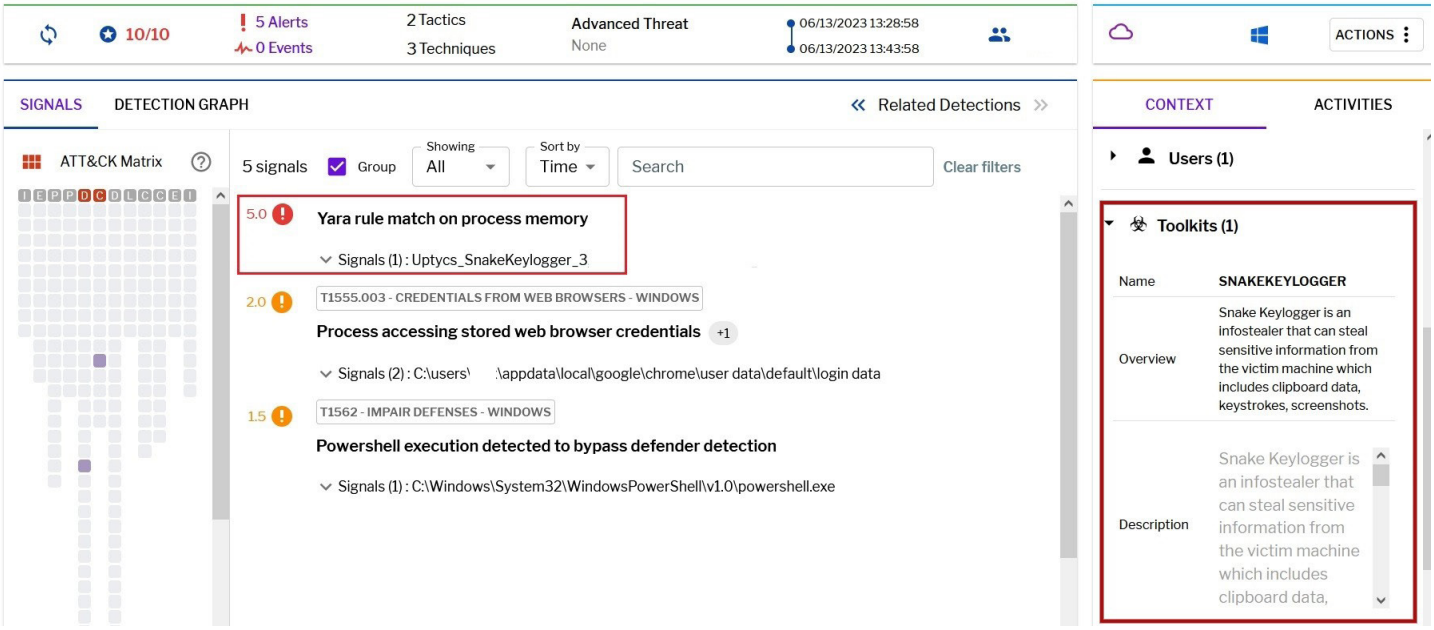

Figure 7–Uptycs XDR detection of SnakeKeylogger

Linux:

Mirai

- Mirai malware targets consumer devices like smart cameras, home routers, thermostats, baby monitors, and refrigerators, turning them into a zombie network of remote-controlled bots. Threat actors use Mirai botnets to target computer systems in massive distributed denial of service (DDoS) attacks.
- By targeting the Linux OS that many Internet of Things (IoT) devices run on, Mirai malware is designed to exploit smart gadget vulnerabilities and link them to a network of infected devices known as a botnet.
- Once a part of the botnet, hijacked hardware is co-opted to conduct further attacks as part of a herd of zombie machines.

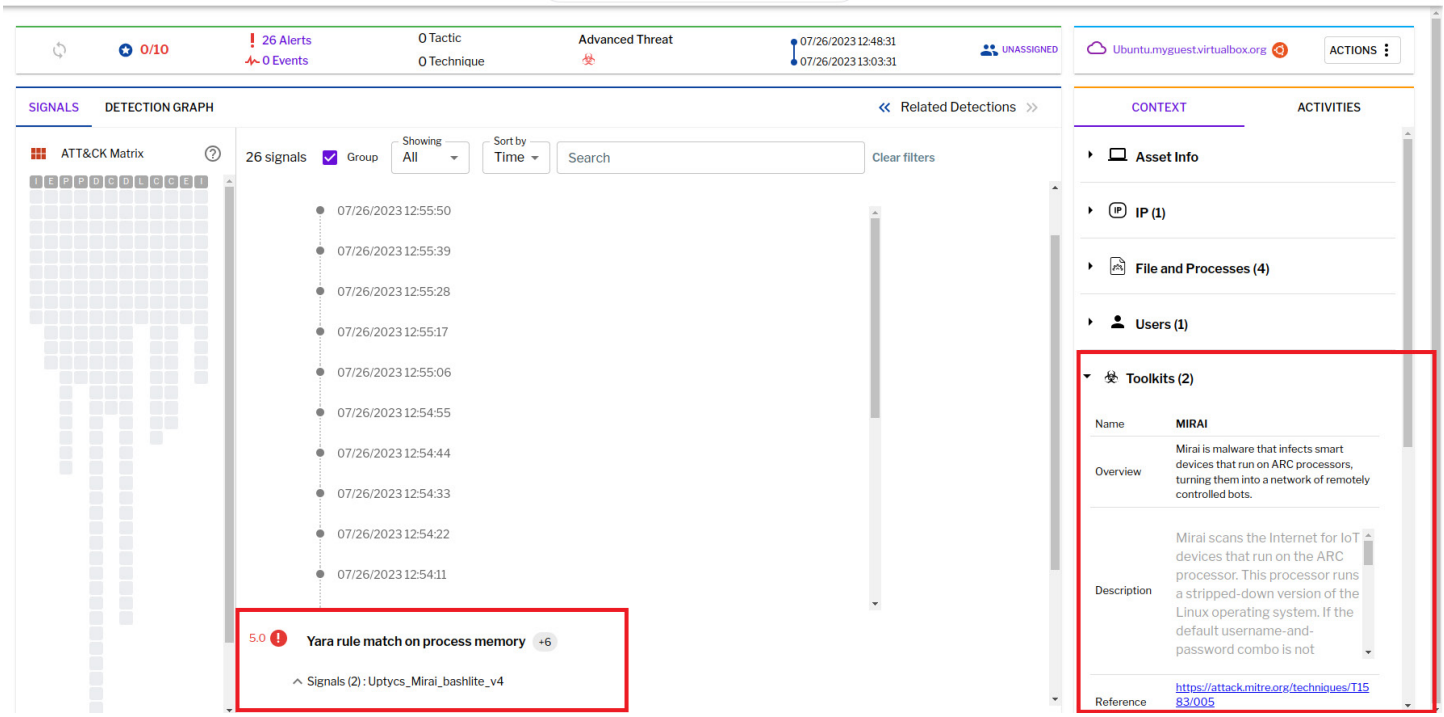

Figure 8–Uptycs XDR detection of Mirai malware

Gafgyt

- GAFGYT, also known as BASHLITE, was first discovered in 2014 is a Linux-based IoT botnet primarily targets any vulnerable IoT devices and uses the device to launch large-scale distributed denial-of-service attacks.
- These botnets can be used to target websites or servers, and they have been used to disrupt a wide range of online services.
- Gafgyt malware typically spreads through phishing emails or by exploiting vulnerabilities in poorly secured Internet of Things (IoT) devices, such as routers and cameras.

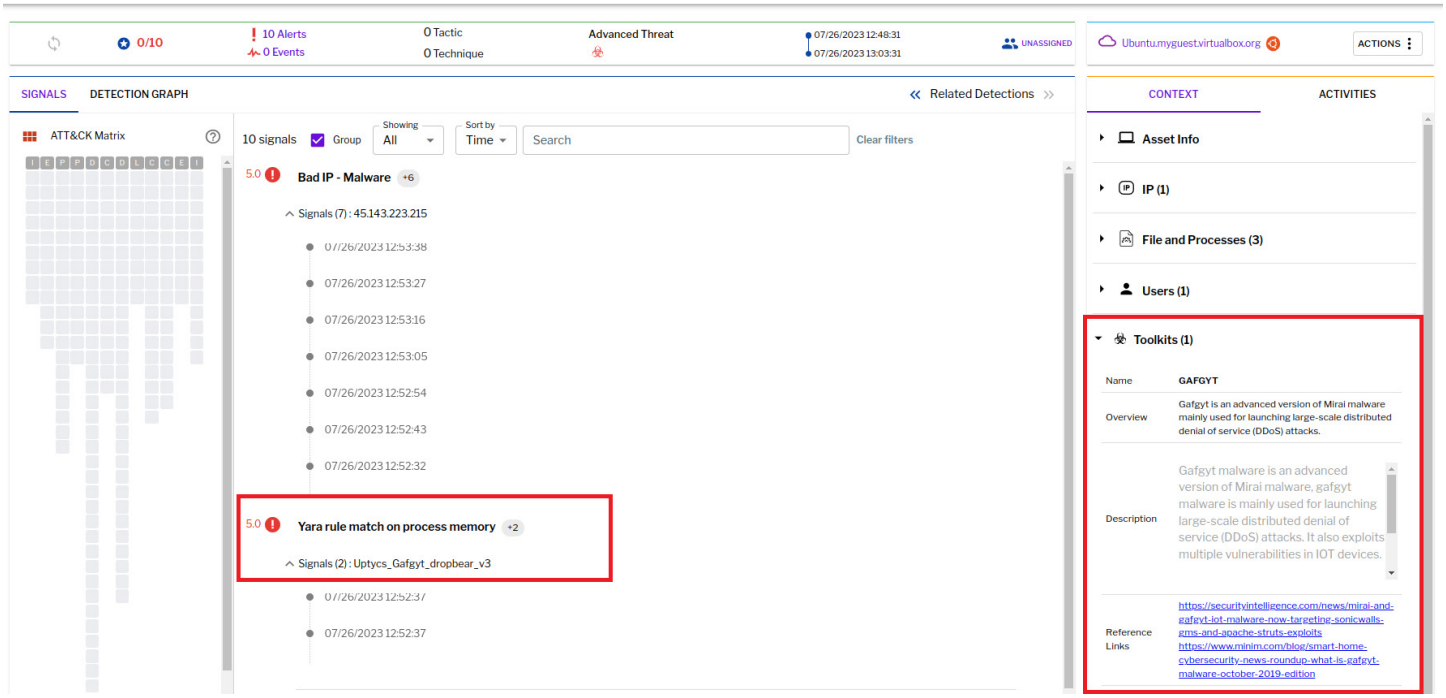

Figure 9–Uptycs XDR detection of Gafgyt malware

MacOS:

Bundlore

- Bundlore is an adware written for macOS that has been used since at least 2015. Though categorized as adware, Bundlore has many features associated with more traditional backdoors.
- It appears in the form of an installer, often asking to download legitimate software or, in fact, software that appears legitimate. Within this installer, there is malware with the ability to bundle illegal software, such as spyware, adware, and other malicious viruses.
- One of the ways that Bundlore malware gets into macOS is through a fake Adobe Flash Player installer.
- The installer will load an invisible helper file, which in turn loads a shell script, which then downloads and executes Bundlore from a malicious domain.
- Some other adware that might pop up on macOS due to a Bundlore infection may include CinemaPlusPro, FlashMall, MyShopcoupon, and many others.

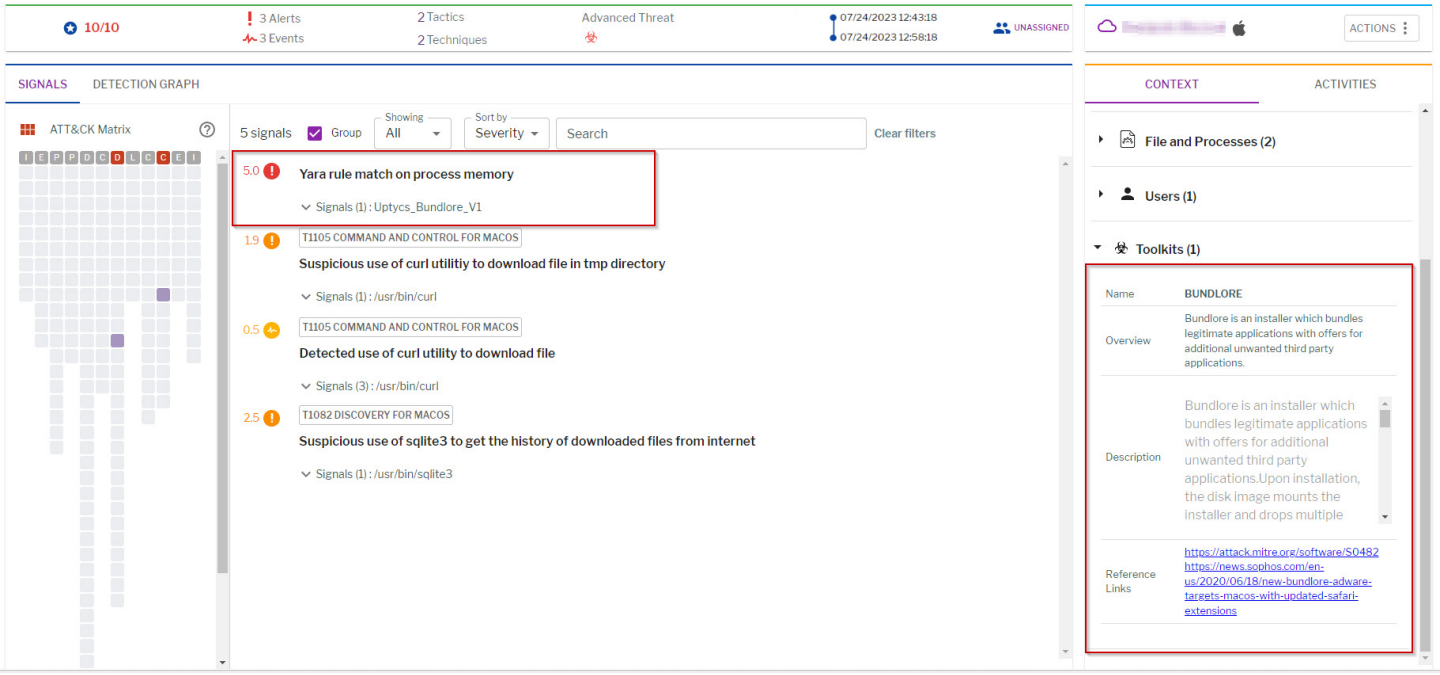

Figure 10–Uptycs XDR detection of Bundlore adware

Uptycs threat research articles

From Protection to Intrusion: Uncovering Potentially Exploitable vm2 Vulnerabilities: This research article provides insight into a vulnerability that has been discovered in the widely used vm2 library, which raises concerns about the integrity of its sandboxing capabilities. The vulnerability discovered allows attackers to bypass the built-in sandbox and gain unauthorized access, thus enabling them to execute arbitrary code within the environment.

Exploring a Dual Threat: Cyclops Ransomware & Stealer Combo: This research article details the Cyclops group, which is particularly proud of having created ransomware capable of infecting all three major platforms: Windows, Linux, and macOS. In addition to offering ransomware services, this entity also supplies a separate binary specifically geared to steal sensitive data, such as an infected computer name and a number of processes.

Deciphering APT-36's Latest Linux Malware Campaign: Unveiling Cyber Espionage in India: This research article details a newly discovered Linux malware known as Poseidon, deployed by the APT-36 group, also known as Transparent Tribe. Transparent Tribe used the Kavach authentication tool as a cover to deliver the Poseidon payload. Kavach is a two-factor authentication (2FA) solution provided by the Indian government for secure access to their email services.

Zaraza Bot Credential Stealer Targets Browser Passwords: This research article details the newly identified variant of credential-stealing malware, dubbed Zaraza bot, that uses telegram as its command and control. This botnet was stealing login credentials from 38 web browsers, including Google Chrome, Microsoft Edge, Opera, AVG Browser, Brave, and Yandex.

RTM Locker Ransomware as a Service (RaaS) Now Suits Up for Linux Architecture: This research article details a newly discovered ransomware binary attributed to the ransomware-as-a-service (RaaS) provider RTM group. This is the first time the group has created a Linux binary infecting Linux, NAS, and ESXi hosts, and it appears to be inspired by Babuk ransomware's leaked source code.

3CX Supply Chain Cyber Attack: An increase in Supply chain attacks in recent years. This research article details an attack campaign where the threat actor employed a DLL side-loading technique to target the legitimate 3CXDesktopApp signed binary. This attack has been observed on Windows and macOS systems.

Meduza Stealer: What Is It & How Does It Work?: This research article details a newly discovered Meduza Stealer specifically designed to target Windows users and organizations to steal users' browsing activities, extracting a wide array of browser-related data.

Top Threat actors in focus

Fin7

FIN7, also called Carbanak and ITG14, is a prolific Russian-speaking cybercriminal syndicate known to employ an array of custom malware to deploy additional payloads and broaden its monetization methods.

The latest intrusion wave involves the use of Dave Loader, a crypter previously attributed to the Conti group (also known as Gold Blackburn, ITG23, or Wizard Spider), to deploy the Domino backdoor.

Domino's potential connections to FIN7 come from source code overlaps with DICELOADER. The malware is designed to gather basic sensitive information and retrieve encrypted payloads from a remote server.

The Domino backdoor and loader are said to have been used to install Project Nemesis since at least October 2022.

Lazarus Group

Lazarus Group has earned its reputation as high-profile nation-backed threat actors, mainly targeting cryptocurrency companies.

This active North Korean APT organization mainly targets financial institutions and cryptocurrency exchanges.

Lazarus Group recently has been attributed to a campaign to target Linux users by distributing the SimplexTea backdoor via an OpenDrive cloud storage account.

BlueNoroff, also called Lazarus Group, targets macOS users with the RustBucket malware. This malware arrives with capabilities to establish persistence and avoid detection by security software.

Earth Longzhi

Earth Longzhi, a subgroup of APT41, was first documented by the cybersecurity firm in November 2022, detailing its attacks against various organizations located in East and Southeast Asia as well as Ukraine.

In the recent campaign, Earth Longzhi also targets organizations based in Taiwan, Thailand, the Philippines, and Fiji.

Attack chains mounted by the threat actor leverage vulnerable public-facing applications as entry points to deploy the BEHINDER web shell and then leverage that access to drop additional payloads, including a new variant of a Cobalt Strike loader called CroxLoader.

This recently reported campaign abuses a Windows Defender executable to perform DLL sideloading while exploiting a vulnerable driver to disable security products installed on the hosts via a Bring your own vulnerable driver [BYOVD] attack.

Earth Longzhi uses a new way to disable security products, a technique we've dubbed stack rumbling via Image File Execution Options [IFEO], which is a denial-of-service [DoS] technique.

APT28

The APT28 group, also known as Fancy Bear, Pawn Storm, Sofacy Group, Sednit, and STRONTIUM, has been active since at least 2007 and has targeted governments, militaries, and security organizations worldwide.

In a recent report, APT28 has exploited the known vulnerability [CVE-2017-6742] to carry out reconnaissance and deploy malware on unpatched Cisco routers.

Additionally, APT28 has breached the Roundcube email servers that belong to multiple Ukrainian organizations, including government entities.

In those particular attacks, the group leveraged news about the ongoing conflict between Russia and Ukraine to trick recipients into opening malicious emails that would exploit Roundcube Webmail vulnerabilities to hack into unpatched servers.

After breaching the email servers, they deployed malicious scripts that redirected the incoming emails of targeted individuals to an email address under the attackers' control.

Kimsuky

Kimsuky, the North Korea-linked APT group, has continuously enhanced its attack toolkits and performed political espionage and other activities.

Recently, a social engineering campaign used by the Kimsuky has targeted the experts in North Korean affairs by engaging in extensive email correspondence with the victims and using spoofed URLs, websites mimicking legitimate web platforms, and weaponized documents.

The attackers have delivered the reconnaissance tool named ReconShark. This malware is considered an evolution of Kimsuky's BabyShark malware.

Kimsuky group also started using the AlphaSeed malware, written in the Go language. This malware receives and executes commands from Naver Mail and collects and steals information from the infected system.

Key Vulnerabilities / Exploits

The key vulnerabilities/exploits seen across Windows, Linux, and macOS platforms are as follows.

Windows

CVE-2023-29336 - Microsoft Windows Win32k Elevation of Privilege Vulnerability

CVE-2023-29325 - Microsoft Windows OLE Remote Code Execution Vulnerability

CVE-2023-24932 - Microsoft Windows Secure Boot Security Feature Bypass Vulnerability

CVE-2023-29363 - Microsoft Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability

CVE-2023-32014 - Microsoft Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability

CVE-2023-32015 - Microsoft Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability

CVE-2023-28252 - Windows Common Log File System Driver Elevation of Privilege Vulnerability

CVE-2023-21554 - Microsoft Message Queuing Remote Code Execution Vulnerability

CVE-2023-20178 - Cisco AnyConnect Secure Mobility Client Privilege Escalation Vulnerability

CVE-2023-34362 - MOVEit SQL Injection Vulnerability

CVE-2023-35036 - MOVEit SQL Injection Vulnerability

CVE-2023-35708 - MOVEit SQL Injection Vulnerability

Linux

CVE-2023-32233 - Linux Kernel Use-After-Free in Netfilter nf_tables

CVE-2023-33246 - Apache RocketMQ Remote Code Execution Vulnerability

CVE-2023-35829 - Linux kernel Use-After-Free in rkvdec_remove

CVE-2023-29017 - VM2 Sandbox Escape Vulnerability

CVE-2023-29199 - VM2 Sandbox Escape Vulnerability

CVE-2023-30547 - VM2 Sandbox Escape Vulnerability

CVE-2023-32314 : VM2 Sandbox Escape Vulnerability

macOS

CVE-2023-32409 - Sandbox Escape Vulnerability fixed in macOS Ventura 13.4 and Safari 16.5

CVE-2023-28204 - Information Disclosure Vulnerability fixed in macOS Ventura 13.4 and Safari 16.5

CVE-2023-32373 - Remote Code Execution Vulnerability fixed in macOS Ventura 13.4 and Safari 16.5

CVE-2023-32434 - Arbitrary Code Execution Vulnerability fixed in macOS Ventura 13.4.1, macOS Monterey 12.6.7 and macOS Big Sur 11.7.8

CVE-2023-32439 - Remote Code Execution Vulnerability fixed in macOS Ventura 13.4.1 and Safari 16.5.1

CVE-2023-32435 - Remote Code Execution Vulnerability fixed in macOS Ventura 13.3 and Safari 16.4

CVE-2023-28205 - Arbitrary Code Execution Vulnerability fixed in macOS Ventura 13.3.1 and Safari 16.4.1

CVE-2023-28206 - Arbitrary Code Execution Vulnerability fixed in macOS Ventura 13.3.1 and Safari 16.4.1

Windows/macOS/Linux

Below are the vulnerabilities affecting Windows, Linux and macOS environments.

CVE-2023-28879 - Ghostscript Buffer Overflow Vulnerability

CVE-2023-2033 - Google Chrome Type Confusion Vulnerability in V8 engine

CVE-2023-22501 - Jira Service Management Server and Data Center Authentication Vulnerability

CVE-2023-2136 - Google Chrome Integer Overflow in Skia

CVE-2023-25690 - Apache HTTP Server HTTP Request Smuggling Vulnerability

CVE-2023-26360 - Adobe ColdFusion Arbitrary Code Execution Vulnerability

CVE-2023-3079 - Google Chrome Type Confusion Vulnerability in V8 engine

General recommendations

- Incident response teams must carefully investigate the parent process spawning the execution of the following utilities:
  - **Windows** - rundll32.exe, powershell.exe, wscript.exe, taskkill.exe, and EQNEDT32.exe utilities
  - **Linux** - chattr, curl, crontab, wget, and Systemctl utilities
  - **macOS** - Openssl, killall, curl, sqlite, and system_profiler utilities
- Few best cyber hygiene practices that prevent malware attacks include the following:
  - Regularly update the software.
  - Avoid opening suspicious links and attachments.
  - Ensure to activate multi-factor authentication.
  - Regularly back up your important data.
  - Ensure to adopt strong password policies.

About Uptycs

Uptycs, the first unified CNAPP and XDR platform, reduces risk by prioritizing your responses to threats, vulnerabilities, misconfigurations, sensitive data exposure, and compliance mandates across your modern attack surface—all from a single UI. This includes the ability to tie together threat activity as it traverses on-prem and cloud boundaries, delivering a more cohesive enterprise–wide security posture. Choose Uptycs MDR for fully managed detection and response.

Shift up your cybersecurity with Uptycs. Visit Uptycs.com

uptycs