Issue 10 | Dec. 2023

Uptycs Quarterly Threat Bulletin

Prepared by the
Uptycs Threat Research Team

The quarterly threat intel bulletin provides insights into 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 to evaluate and form a more robust detection and protection posture against the latest Windows, Linux, and macOS threats.

Index

Q4 threat bulletin highlights

In Q4 2023, our focus is on significant cybersecurity incidents and trends. During the quarter, we witnessed cybercriminals' aggressive exploitation of the Apache ActiveMQ vulnerability, predominantly to deploy HelloKitty ransomware.

Malware Prevalence Trends:

- Windows: The dominant malware strains were Amadey, AgentTesla, and RedLine.
- Linux: Mirai and Gfagyt marked their significant presence.
- macOS: Bundlore maintained its ongoing activity.

Utility Abuse Insights:

- Windows: Rundll32.exe, a LOLBin, was notably the most exploited utility.
- Linux: Crontab utility saw the highest misuse.
- macOS: OpenSSL and curl were primarily manipulated by Bundlore malware.

The quarter also highlighted the LockBit ransomware group as the foremost active entity, with Clop, Play, and BlackCat also making significant moves. Additionally, notable activities were observed from threat actors such as Lazarus Group, SideWinder, Kimsuky, Arid Viper, and APT29, marking a quarter dense with cybersecurity challenges.

Comparative analysis: Key vulnerabilities, malware, and threat actors in Q3 and Q4 2023

Wildly exploited vulnerabilities

Q3 2023 saw multiple threat actors exploiting a zero-day vulnerability in WinRAR software [CVE-2023-38831] to deploy malicious payloads.

In Q4 2023, a critical vulnerability in Apache ActiveMQ [CVE-2023–46604] was exploited extensively, notably by HelloKitty ransomware targeting outdated systems to execute arbitrary code via insecure deserialization.

Cross-platform exploited vulnerabilities

The Q3 report highlighted six cross-platform vulnerabilities, primarily in Google Chrome and Oracle VirtualBox.

In Q4, vulnerabilities in Google Chrome continued to be exploited across all three platforms, along with major ones in Splunk Enterprise, JetBrains, and Firefox.

Top malware

For Windows, stealer-based campaigns remained consistent, with RedLine, Agent Tesla, and Amadey persisting as the most prevalent malware in both quarters.

Linux-platform threats remained constant with Mirai and Gafgyt, exploiting vulnerabilities in IoT devices.

On macOS, Bundlore malware continued targeting users through fake installers in both quarters.

Top utilities

The most abused Windows utilities in both quarters were Rundll32.exe, Wscript.exe, and Powershell.exe. While CMD.exe and EQNEDT32.exe were prominent in Q3, Reg.exe, and Mshta.exe were more prevalent in Q4.

Crontab, Chattr, and Wget remained the most abused Linux utilities. Dash and curl were predominant in Q3, but in Q4, find, and Systemctl were more commonly misused.

On macOS, the utilities Openssl, curl, killall, sqlite, and system_profiler continued to be exploited by threat actors.

See figures 1–6 for top abused utilities in Q3 and Q4, below.

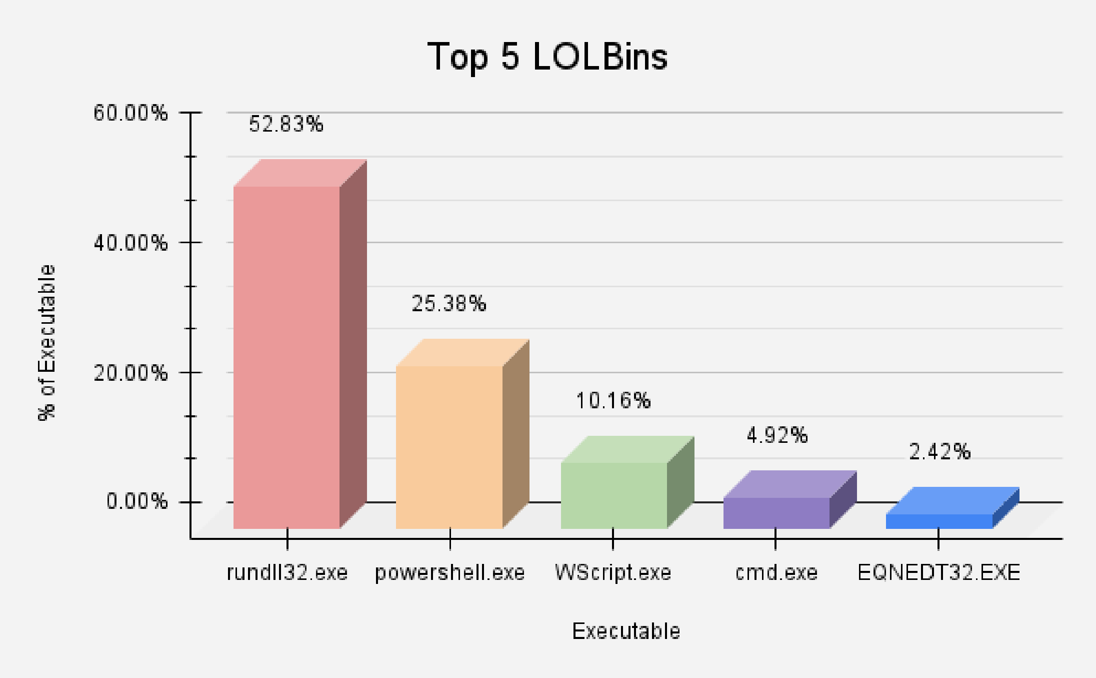


Figure 1–Q3 report (TOP 5 LOLBINS)

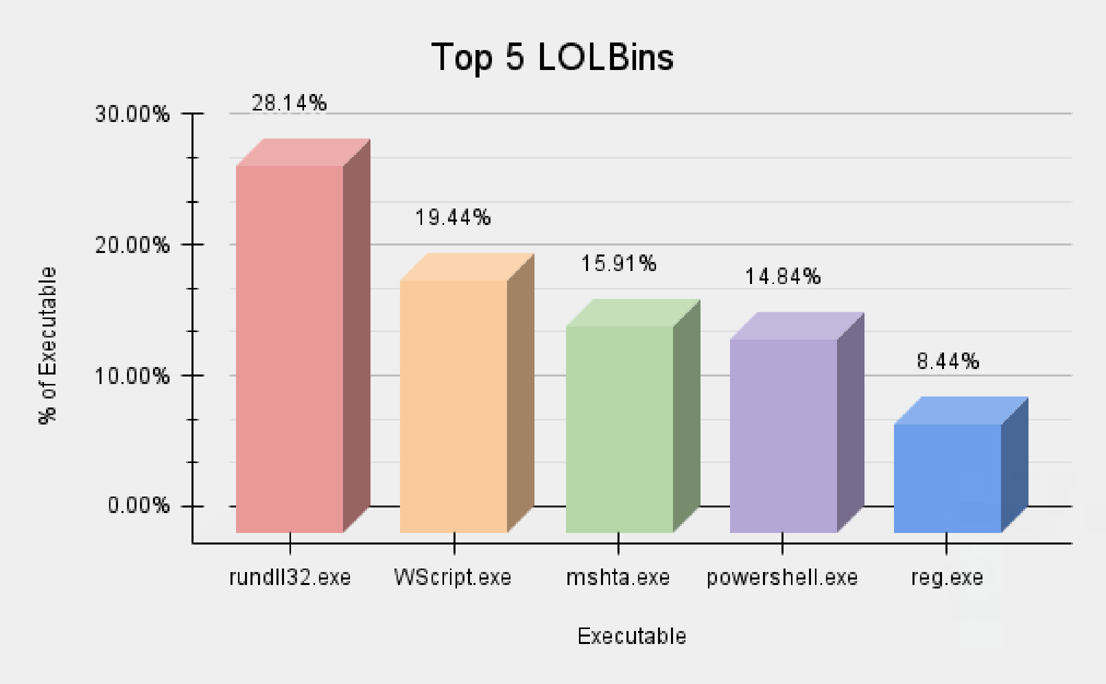


Figure 2–Q4 report (TOP 5 LOLBINS)

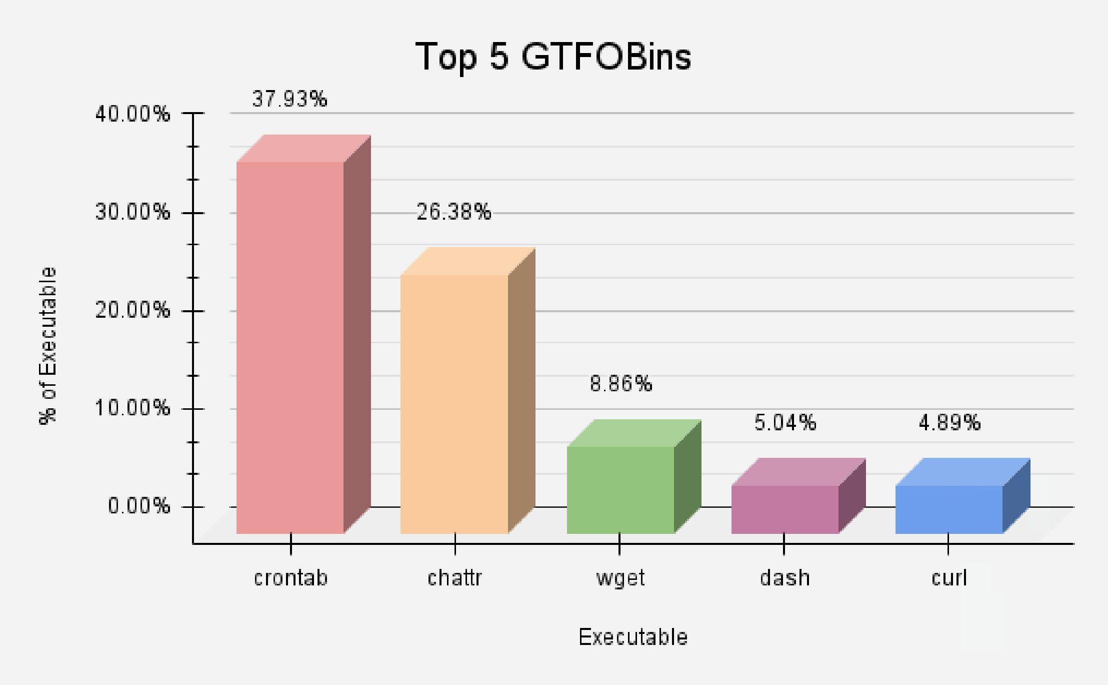


Figure 3–Q3 report (TOP 5 GTFOBINS)

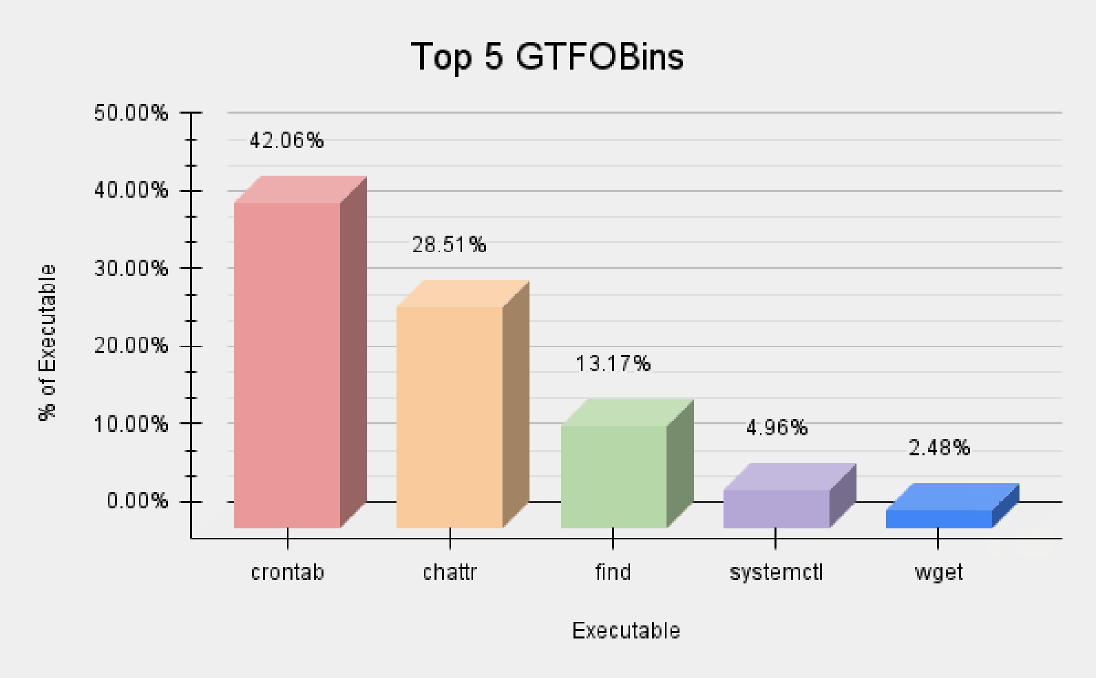


Figure 4–Q3 report (TOP 5 GTFOBINS)

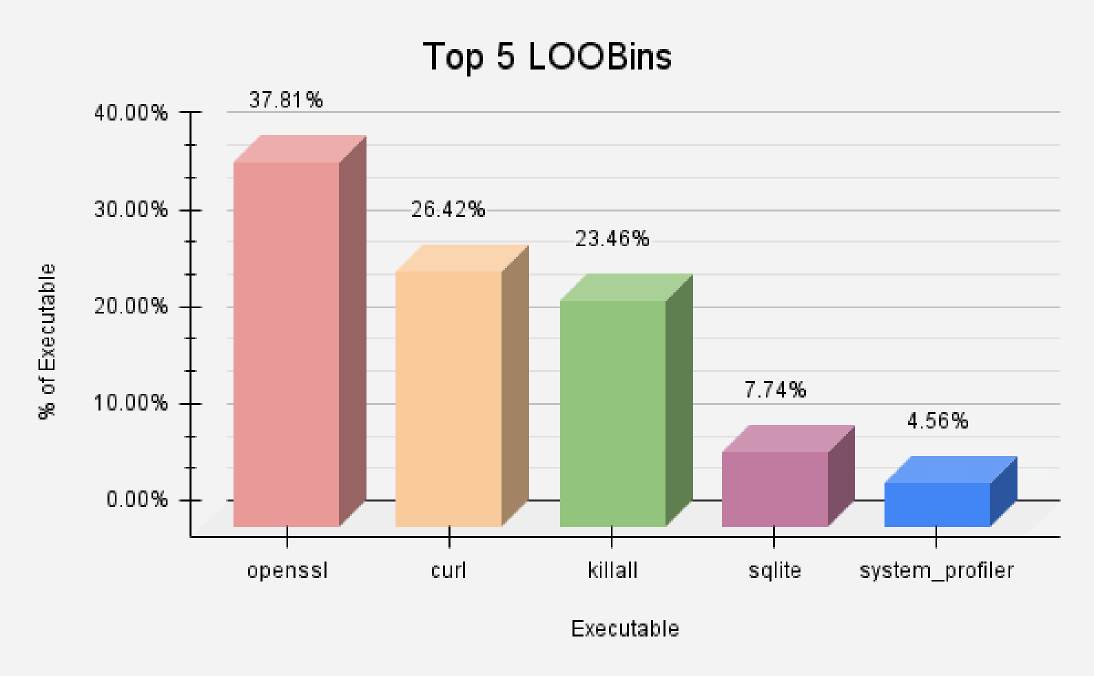


Figure 5–Q3 report (TOP 5 LOOBINS)

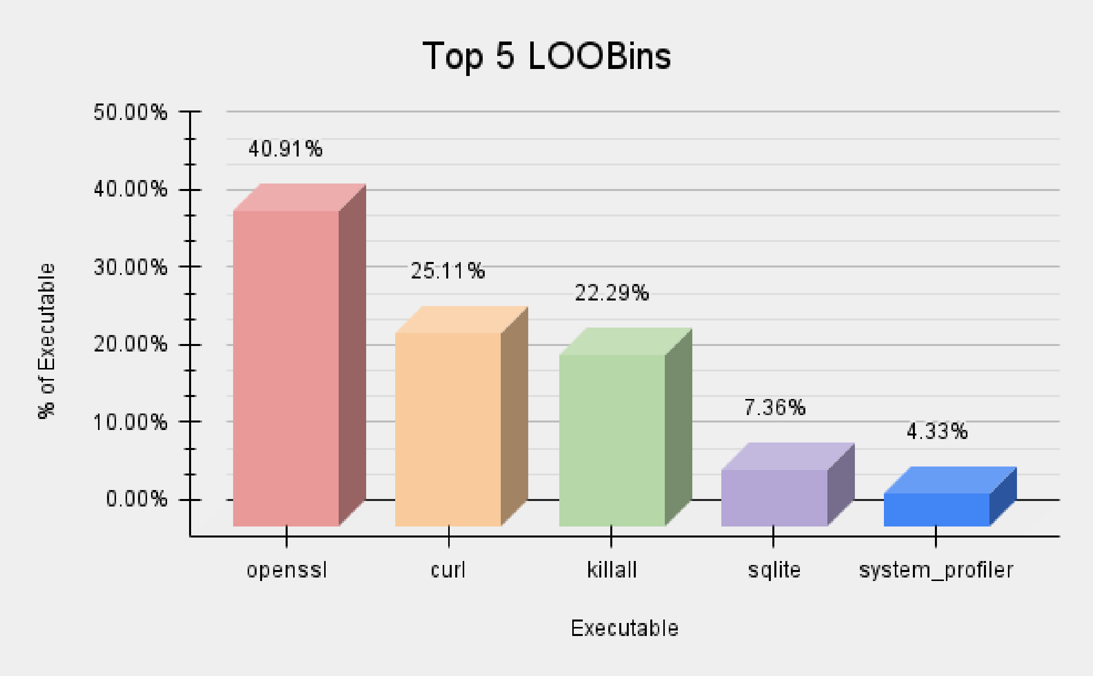


Figure 6–Q4 report (TOP 5 LOOBINS)

Threat actors

Lazarus Group remained a top APT actor. In Q3, other active APTs were APT35, OilRig, Turla, and APT27. In Q4, SideWinder, Kimsuky, Arid Viper, and APT29 were notably active.

Mitre techniques

Both quarters saw System Binary Proxy Execution (T1218), Command and Scripting Interpreter (T1059), and Scheduled Task/Job (T1053) as top tactics. Q3 included Hide Artifacts (T1564) and Impair Defenses (T1562), while Q4 saw Event Triggered Execution (T1546) and Subvert Trust Controls (T1553) being used.

See figures 7-8 for MITRE Techniques in Q3 and Q4, below.

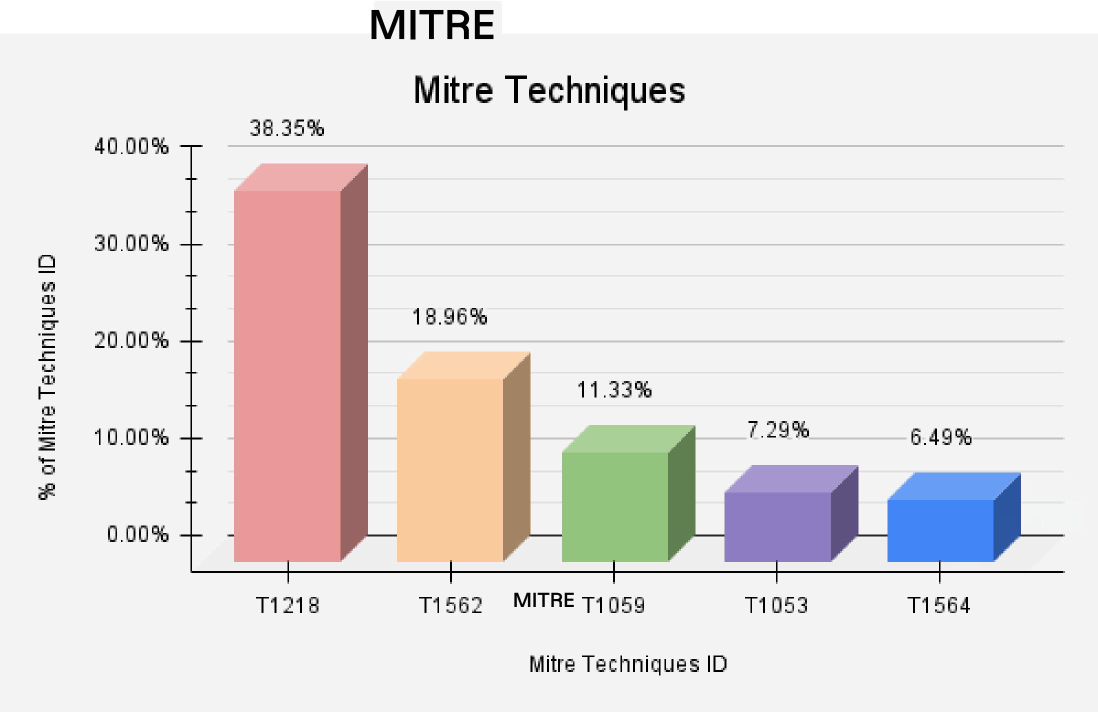


Figure 7–Q3 report (MITRE Techniques)

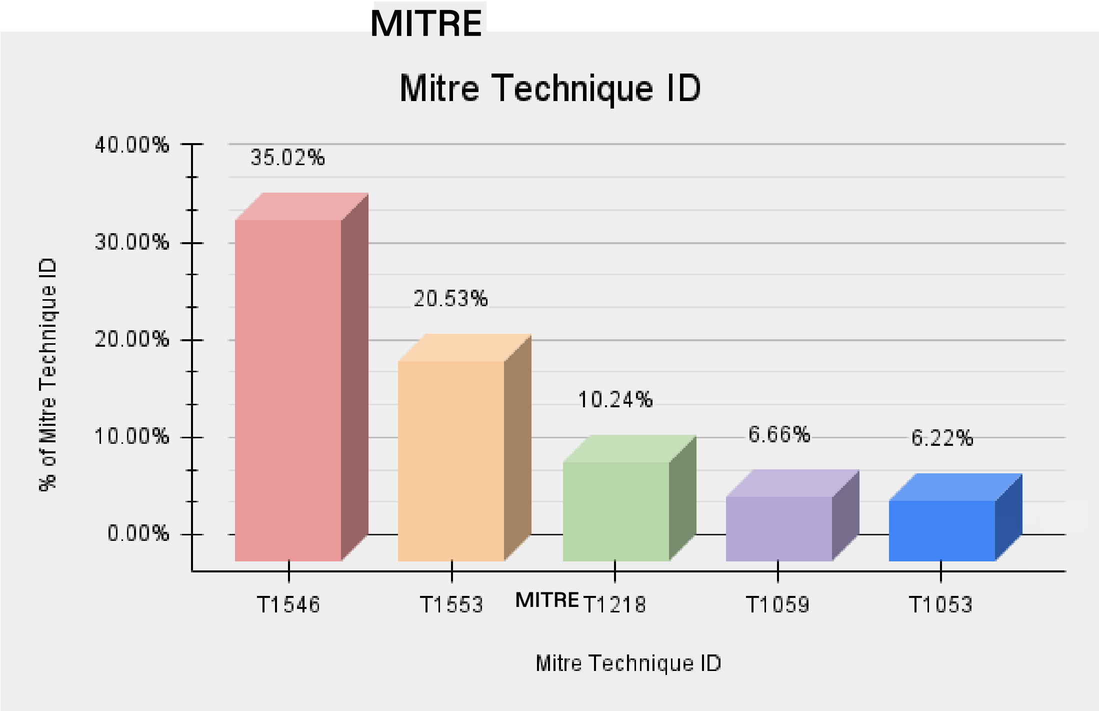


Figure 8–Q4 report (Mitre Techniques)

Highlighted ransomware groups

In Q3, Clop ransomware was the most active, followed by Mallox, Cyclops, LockBit, and BlackCat. In Q4, LockBit took the lead, with Clop, Play, and BlackCat also active.

Q3 and Q4 threat research articles

Q3 featured five blogs, including a white paper on Stealer activity, two blogs on vulnerabilities, one on QwixxRAT malware, and advanced research on Lateral Movement Detection.

Q4 saw ten blogs covering vulnerabilities in Confluence Server, Apache ActiveMQ, Splunk, and Linux-based exploits, a report on WinRAR vulnerability exploitation, blogs on Remcos RAT and GhostSec's GhostLocker Ransomware, and a Phishing advisory on USPS Smishing campaigns.

Q4 2023 cybersecurity insights: In-depth threat analysis and trends

Critical alerts

CVE-2023-46604 - Remote Code Execution Vulnerability in Apache ActiveMQ

A critical vulnerability in Apache ActiveMQ, identified as CVE-2023–46604 and rated with a CVSS score of 9.8, put the cybersecurity community on high alert. Apache ActiveMQ, a widely used open-source message broker, is integral to the infrastructure of prominent platforms like Apache Camel, Red Hat AMQ, Amazon MQ, Apache TomEE, Eclipse, and Mule.

This vulnerability has been exploited in recent HelloKitty ransomware attacks, targeting systems with outdated security measures to execute arbitrary code through insecure deserialization. Attackers have deployed ransomware through deceptive .png files, using MSIExec for installation. Despite initial failures in encrypting data, the .NET DLL payload successfully encrypted files, prompting victims to contact specific email addresses for ransom instructions.

Techniques used by the malware samples

The Our Uptycs XDR, configured in our threat intelligence replication system, effectively detects and labels attacker behavior across Windows, Linux, and macOS platforms. This system houses the latest known suspicious and malicious files.

The top techniques/tactics triggered by malware samples, aligned with the MITRE ATT&CK framework, are Event Triggered Execution (T1546), Subvert Trust Controls (T1553), System Binary Proxy Execution (T1218), Command and Scripting Interpreter (T1059), and Scheduled Task/Job (T1053).

The prevalence of these observed ATT&CK technique IDs is depicted in Figure 9, below.

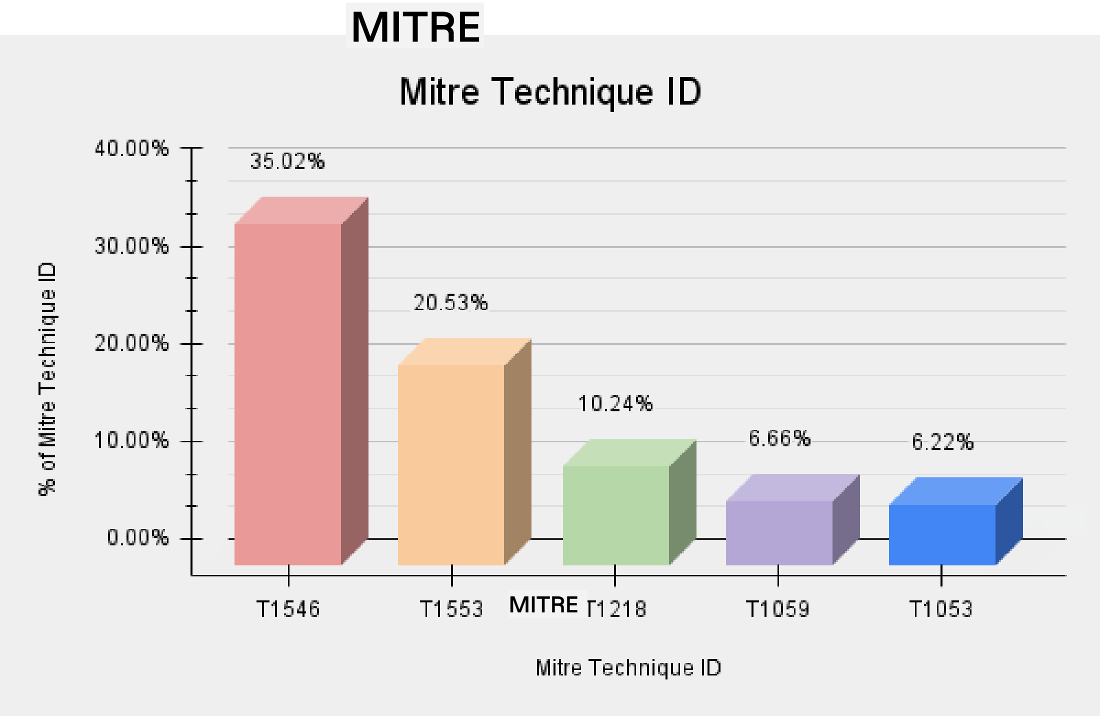


Fig.9–Observed ATT&CK technique IDs

Commonly abused commands and utilities

Malicious samples often utilize built-in utilities of target operating systems in their attack sequences to evade detection, a technique known as "Living off the Land." These utilities correspond to our replication systems' tactics across Windows, Linux, and macOS platforms.

Windows utilities abused by malware

This quarter, Rundll32.exe was the most exploited utility on Windows systems by attackers. Other frequently abused utilities included WScript.exe, mshta.exe, powershell.exe, and reg.exe.

Figure 10 illustrates the top 5 Windows utilities misused by malware and their prevalence.

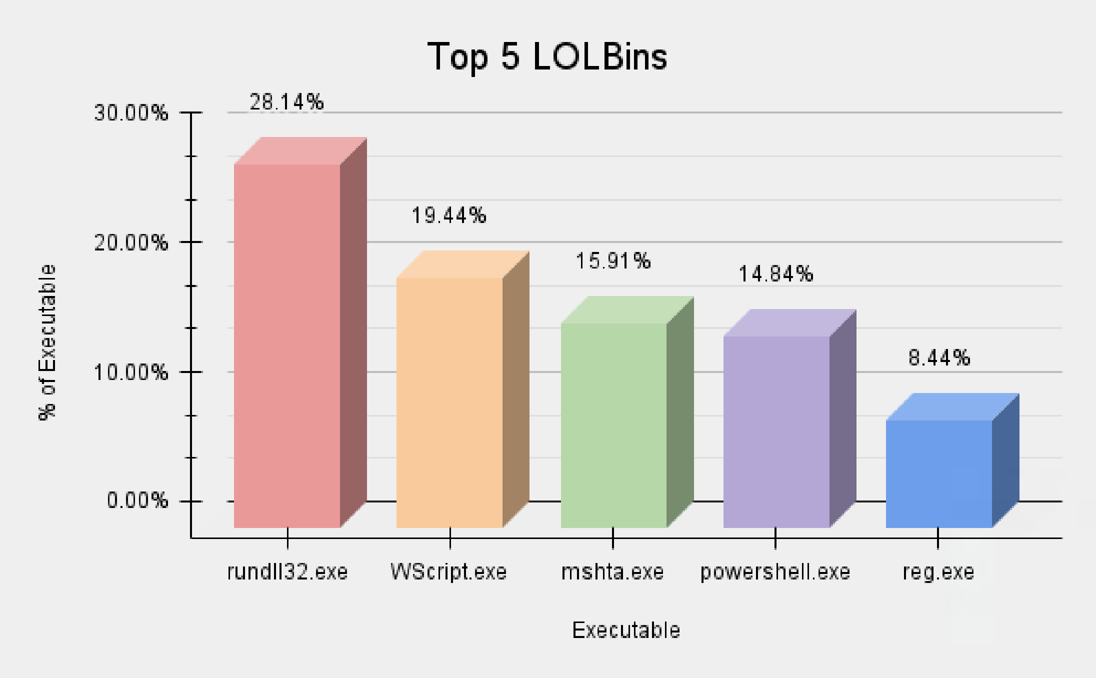


Figure 10–Top 5 Windows utilities abused by malware

1. **Rundll32.exe (Tactics: Execution and Defense Evasion):** Commonly used for executing DLL payloads, this utility has been notably utilized in the Quasar RAT campaign.
2. **WScript.exe (Tactics: Execution and Defense Evasion):** This scripting host utility has been actively exploited to execute Konni and SmokeLoader malware.
3. **Mshta.exe (Tactic: Defense Evasion):** Known for executing HTA files, it's been used by LockBit 3.0 affiliates for malicious HTA file execution.
4. **Powershell.exe (Tactics: Execution, Persistence, Defense Evasion, Discovery):** Used for various malicious activities, including backdoor installation, data exfiltration, and ransomware deployment. DarkTail malware notably used encoded PowerShell scripts for C2 server communication.
5. **Reg.exe (Tactic: Defense Evasion):** Agent Tesla, Lokibot, njRAT, and other malware families have exploited this utility for registry modifications.

Linux utilities abused by malware

This quarter, Crontab was the most abused Linux utility, frequently observed in Mirai malware attacks.

Figure 11 shows the top five Linux utilities misused by malware, including their prevalence.

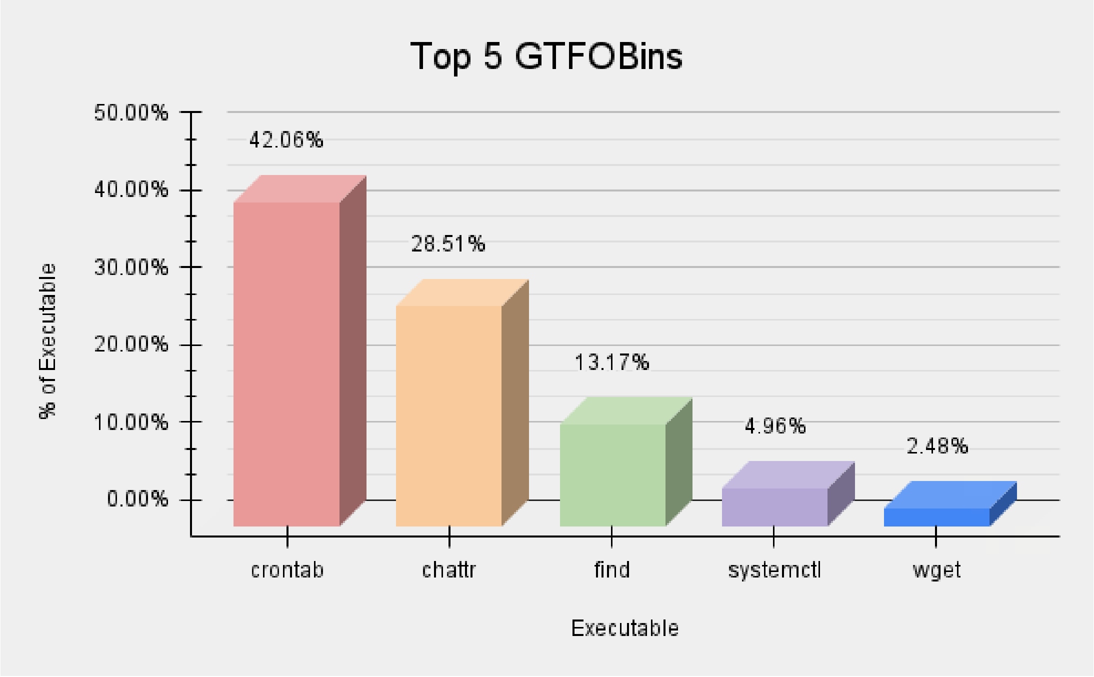


Figure 11–Top five Linux utilities abused by malware

1. **Crontab (Tactics: Execution, Persistence):** Used for scheduling tasks, APT36 threat actors have exploited it for persistence.
2. **Chattr (Tactics: Defense Evasion, Persistence)**: This file attribute tool has been used by TeamTNT for campaign activities.
3. **Find (Tactic: Credential Access)**: Employed by Watchbog malware for searching SSH keys.
4. **Systemctl (Tactic: Defense Evasion):** Abused to stop EDR services, with TeamTNT creating mining services using it.
5. **Wget (Tactics: Privilege Escalation, Command-and-Control):** Often used to download and execute Mirai malware.

LOOBins (macOS Binaries) utilities abused by malware

LOOBins, or Living Off the Orchard binaries, are macOS utilities that can be leveraged for malicious purposes, including command execution, privilege escalation, persistence, and data exfiltration.

Figure 12 details the top five macOS utilities exploited by malware and their prevalence.

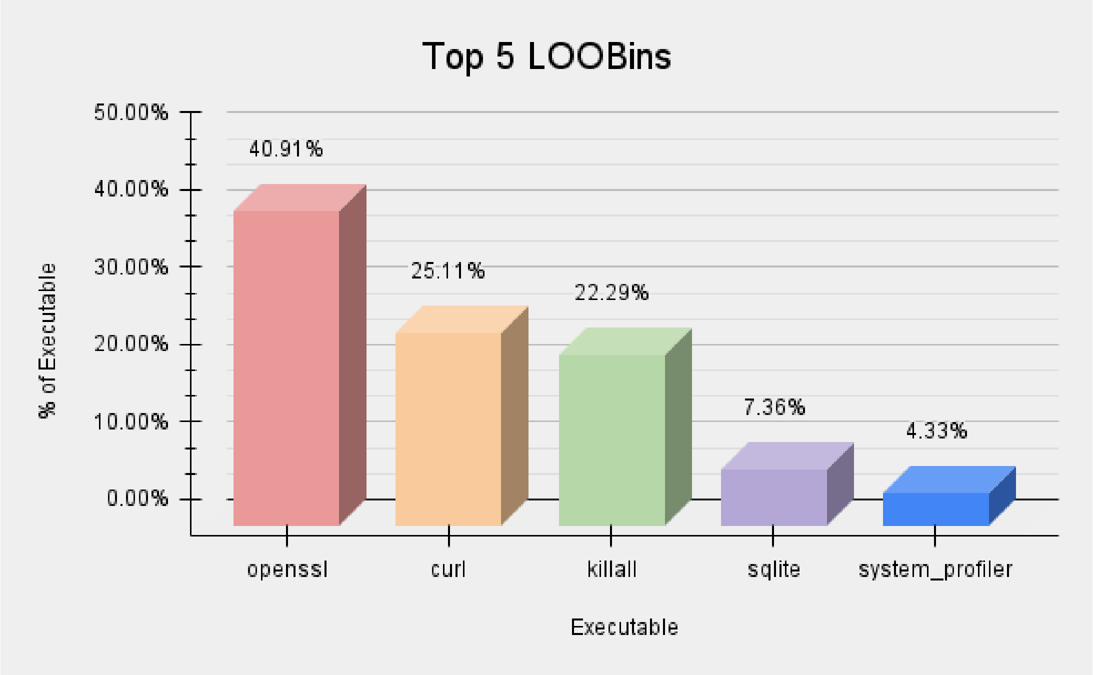


Figure 12–Top five macOS utilities abused by malware

1. **Openssl (Tactic: Defense Evasion):** Used by Snake malware, it can encrypt data with base64, AES, and CBC.
2. **curl (Tactic: Command and Control):** Utilized by Bundlore malware to download payloads.
3. **killall (Tactic: Defense Evasion):** Employed by Shlayer malware to close script windows post-execution.
4. **sqlite (Tactic: Exfiltration):** Used by Shlayer malware to access internet download history.
5. **system_profiler (Tactic: Discovery):** Bundlore uses this to gather system hardware information.

Top prevalent malware families in the wild

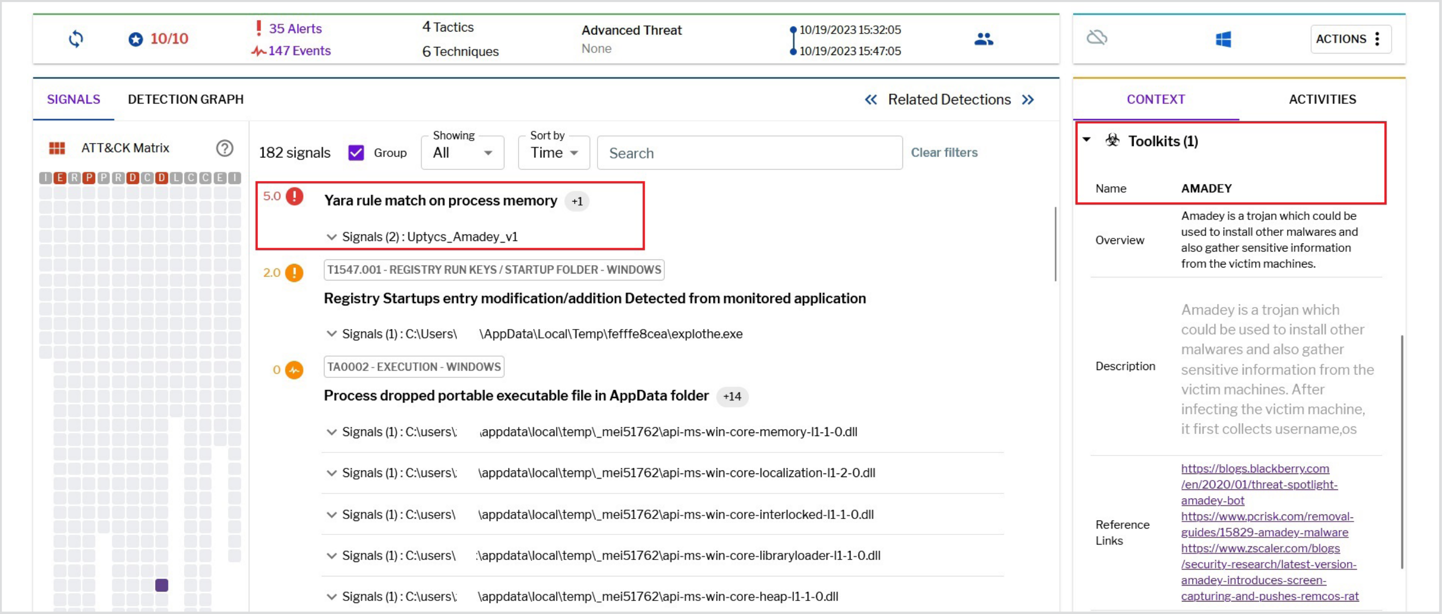
Utilizing our in-house Uptycs EDR, equipped with YARA process scanning, we have identified the most prevalent malware families across Linux, Windows, and macOS platforms. Our research team has enhanced our platform with comprehensive TTPs and YARA coverage for these malware processes. Uptycs customers can now access detailed toolkit profiles of this malware when detections are triggered.

Here are the top malware identified across Windows, Linux, and macOS platforms:

Windows malware:

Amadey

Amadey is a versatile botnet malware functioning as a loader or infostealer. It can conduct reconnaissance, data exfiltration, and load additional payloads. Targeting all Microsoft Windows versions, Amadey loaders are widely used by threat actors for malware distribution and botnet expansion. The "Socks5Systemz" proxy botnet has recently been implicated in global infections attributed to PrivateLoader and Amadey loaders.



5.0 Yara rule match on process memory +1

Signals (2) : Uptycs_Amadey_v1

2.0 T1547.001 - REGISTRY RUN KEYS / STARTUP FOLDER - WINDOWS

Registry Startups entry modification/addition Detected from monitored application

Signals (1) : C:\Users\ \AppData\Local\Temp\fefffe8cea\explothe.exe

0 TA0002 - EXECUTION - WINDOWS

Process dropped portable executable file in AppData folder +14

Signals (1) : C:\users\ \appdata\local\temp_mei51762\api-ms-win-core-memory-l1-1-0.dll

Signals (1) : C:\users\ \appdata\local\temp_mei51762\api-ms-win-core-localization-l1-2-0.dll

Signals (1) : C:\users\ \appdata\local\temp_mei51762\api-ms-win-core-interlocked-l1-1-0.dll

Signals (1) : C:\users\ :\appdata\local\temp_mei51762\api-ms-win-core-libraryloader-l1-1-0.dll

Signals (1) : C:\users\ \appdata\local\temp_mei51762\api-ms-win-core-heap-l1-1-0.dll

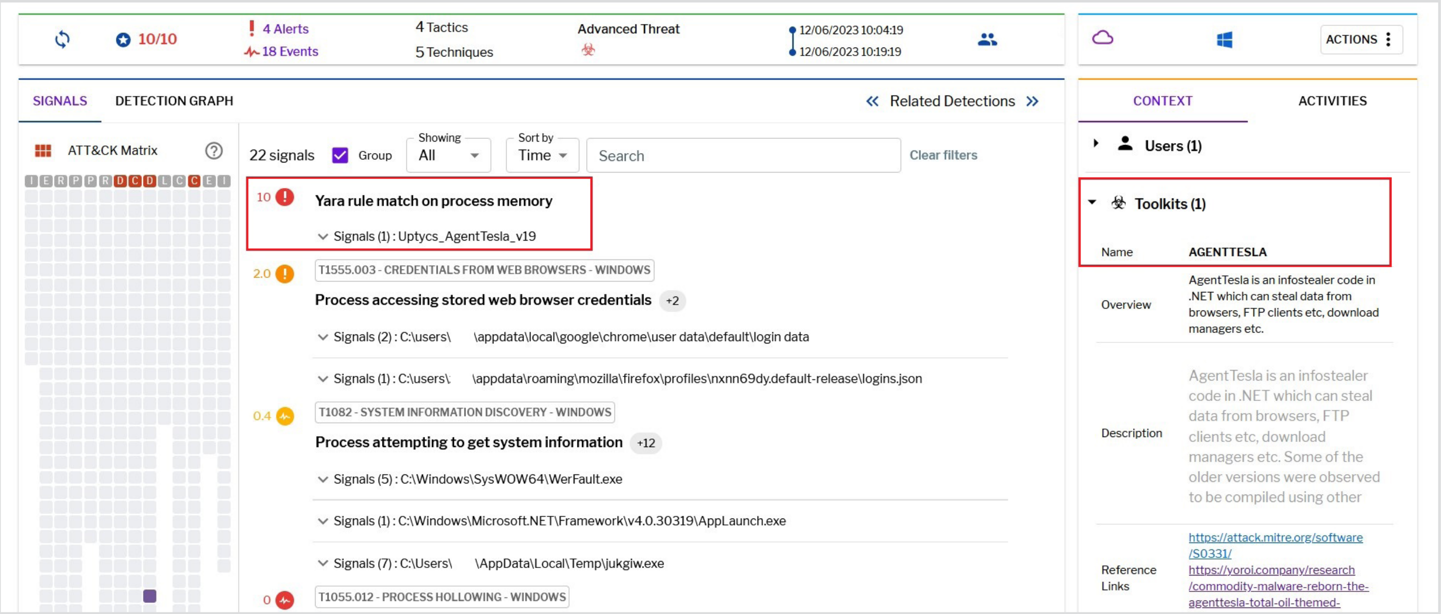
Toolkits (1)

Name	AMADEY
Overview	Amadey is a trojan which could be used to install other malwares and also gather sensitive information from the victim machines.
Description	Amadey is a trojan which could be used to install other malwares and also gather sensitive information from the victim machines. After infecting the victim machine, it first collects username,os
Reference Links	https://blogs.blackberry.com/en/2020/01/threat-spotlight-amadey-bot https://www.pcrisk.com/removal-guides/15829-amadey-malware https://www.zscaler.com/blogs/security-research/latest-version-amadey-introduces-screen-capturing-and-pushes-remcos-rat

Figure 13–Uptycs XDR detection of Amadey

AgentTesla

Agent Tesla, a .NET-based RAT and data stealer, specializes in gaining initial access and exfiltrating sensitive data such as keystrokes and login credentials. A recent phishing campaign spread a new Agent Tesla variant using a Microsoft Excel document, exploiting CVE-2017-11882 and CVE-2018-0802 vulnerabilities in Microsoft Office.



10 Yara rule match on process memory
Signals (1) : Uptycs_AgentTesla_v19

2.0 T1555.003 - CREDENTIALS FROM WEB BROWSERS - WINDOWS
Process accessing stored web browser credentials +2
Signals (2) : C:\users\ \appdata\local\google\chrome\user data\default\login data
Signals (1) : C:\users\ \appdata\roaming\mozilla\firefox\profiles\nxnn69dy.default-release\logins.json

0.4 T1082 - SYSTEM INFORMATION DISCOVERY - WINDOWS
Process attempting to get system information +12
Signals (5) : C:\Windows\SysWOW64\WerFault.exe
Signals (1) : C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Signals (7) : C:\Users\ \AppData\Local\Temp\jukgiw.exe

0 T1055.012 - PROCESS HOLLOWING - WINDOWS

Users (1)

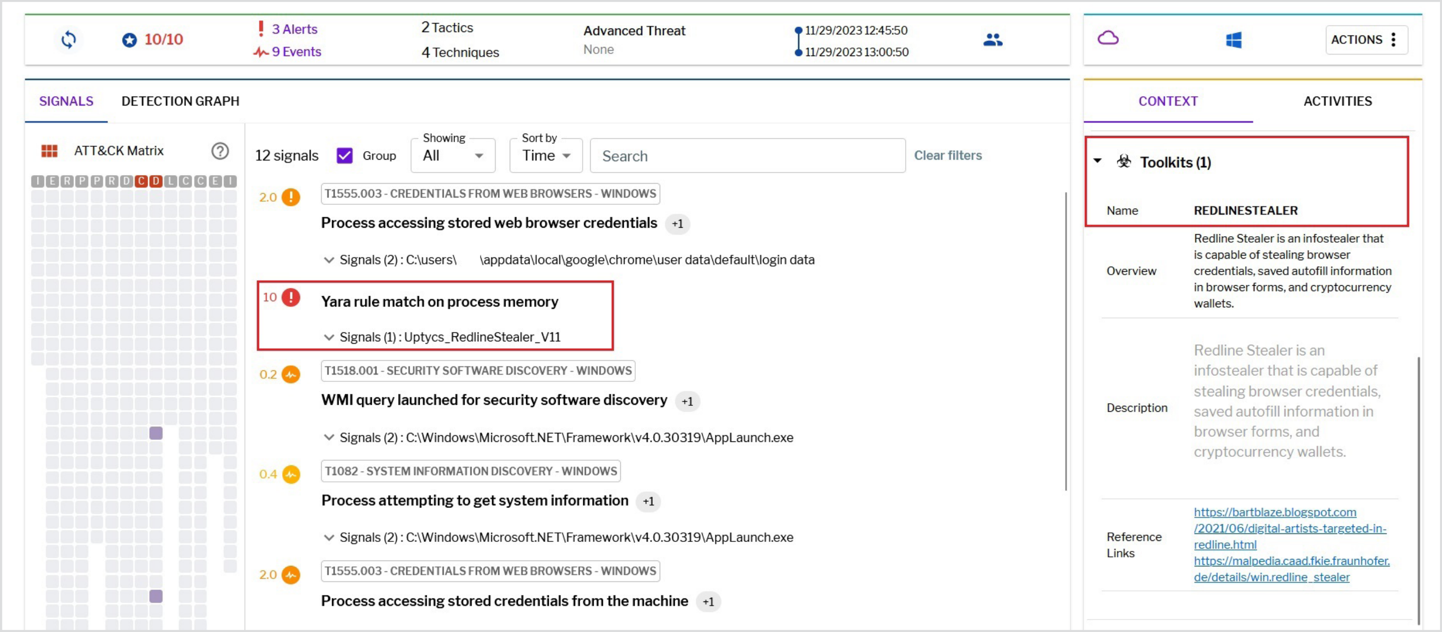
Toolkits (1)

Name	AGENTTESLA
Overview	AgentTesla is an infostealer code in .NET which can steal data from browsers, FTP clients etc, download managers etc.
Description	AgentTesla is an infostealer code in .NET which can steal data from browsers, FTP clients etc, download managers etc. Some of the older versions were observed to be compiled using other
Reference Links	https://attack.mitre.org/software/S0331/ https://yoroi.company/research/commodity-malware-reborn-the-agenttesla-total-oil-themed-

Figure 14–Uptycs XDR detection of AgentTesla

RedLine Stealer

RedLine Stealer, a potent data collection tool, extracts login credentials from numerous sources and gathers comprehensive system information. Delivery methods include phishing emails and disguising the malware as popular or cracked software. It has recently incorporated the “ScrubCrypt” obfuscation tool in its attacks.



2.0 T1555.003 - CREDENTIALS FROM WEB BROWSERS - WINDOWS
Process accessing stored web browser credentials +1
Signals (2) : C:\users\ \appdata\local\google\chrome\user data\default\login data

10 Yara rule match on process memory
Signals (1) : Uptycs_RedlineStealer_V11

0.2 T1518.001 - SECURITY SOFTWARE DISCOVERY - WINDOWS
WMI query launched for security software discovery +1
Signals (2) : C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

0.4 T1082 - SYSTEM INFORMATION DISCOVERY - WINDOWS
Process attempting to get system information +1
Signals (2) : C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

2.0 T1555.003 - CREDENTIALS FROM WEB BROWSERS - WINDOWS
Process accessing stored credentials from the machine +1

Toolkits (1)

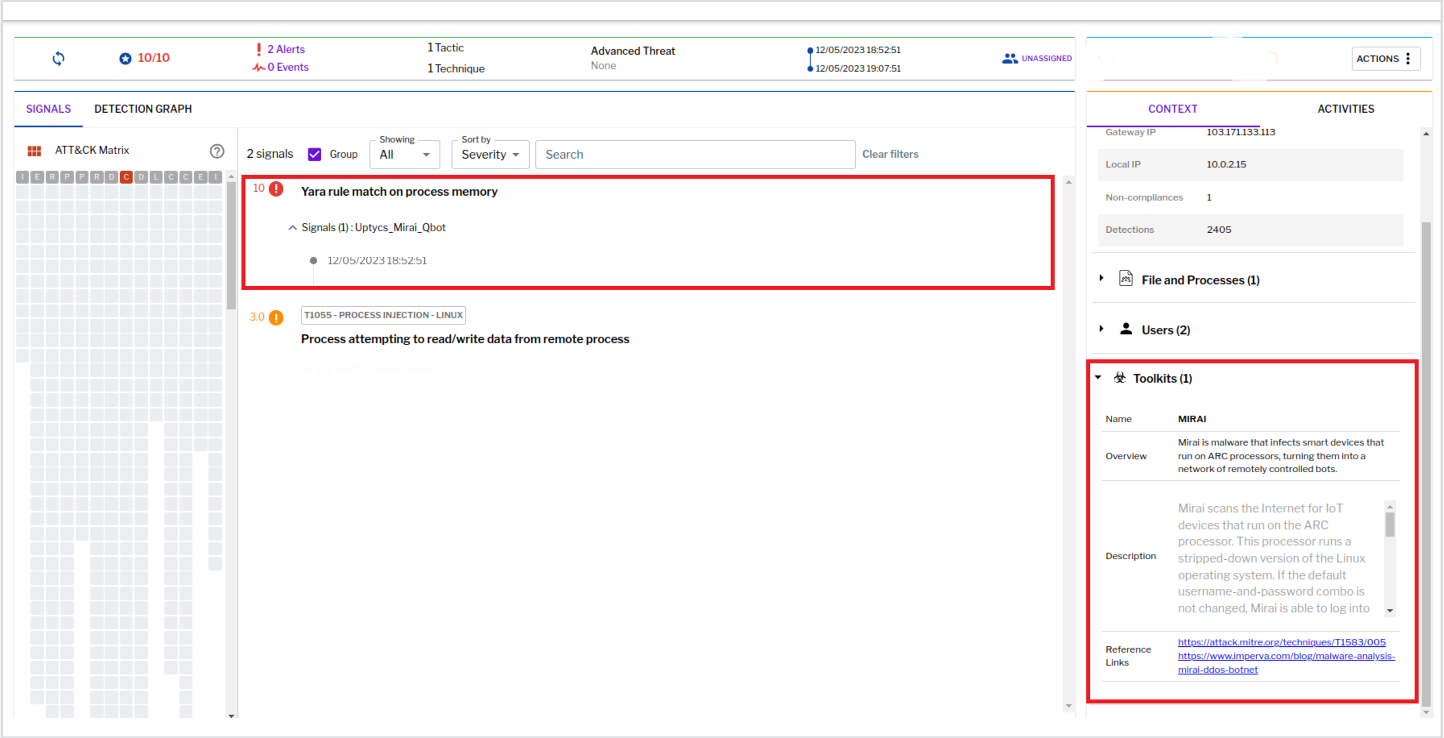
Name	REDLINESTEALER
Overview	Redline Stealer is an infostealer that is capable of stealing browser credentials, saved autofill information in browser forms, and cryptocurrency wallets.
Description	Redline Stealer is an infostealer that is capable of stealing browser credentials, saved autofill information in browser forms, and cryptocurrency wallets.
Reference Links	https://bartblaze.blogspot.com/2021/06/digital-artists-targeted-in-redline.html https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer

Figure 15–Uptycs XDR detection of Redline

Linux malware:

Mirai

The Mirai botnet infects IoT devices, exploiting vulnerabilities for malicious code injection. Recent Mirai versions have added payloads targeting Linux-based routers, exploiting zero-day vulnerabilities for DDoS attacks.



10/10

2 Alerts
0 Events

1 Tactic
1 Technique

Advanced Threat
None

12/05/2023 18:52:51
12/05/2023 19:07:51

UNASSIGNED

2 signals ☑ Group
Showing: All
Sort by: Severity

10 Yara rule match on process memory
Signals (1) : Uptycs_Mirai_Qbot
12/05/2023 18:52:51

3.0 T1055 - PROCESS INJECTION - LINUX
Process attempting to read/write data from remote process

Gateway IP	103.171.133.113
Local IP	10.0.2.15
Non-compliances	1
Detections	2405

File and Processes (1)

Users (2)

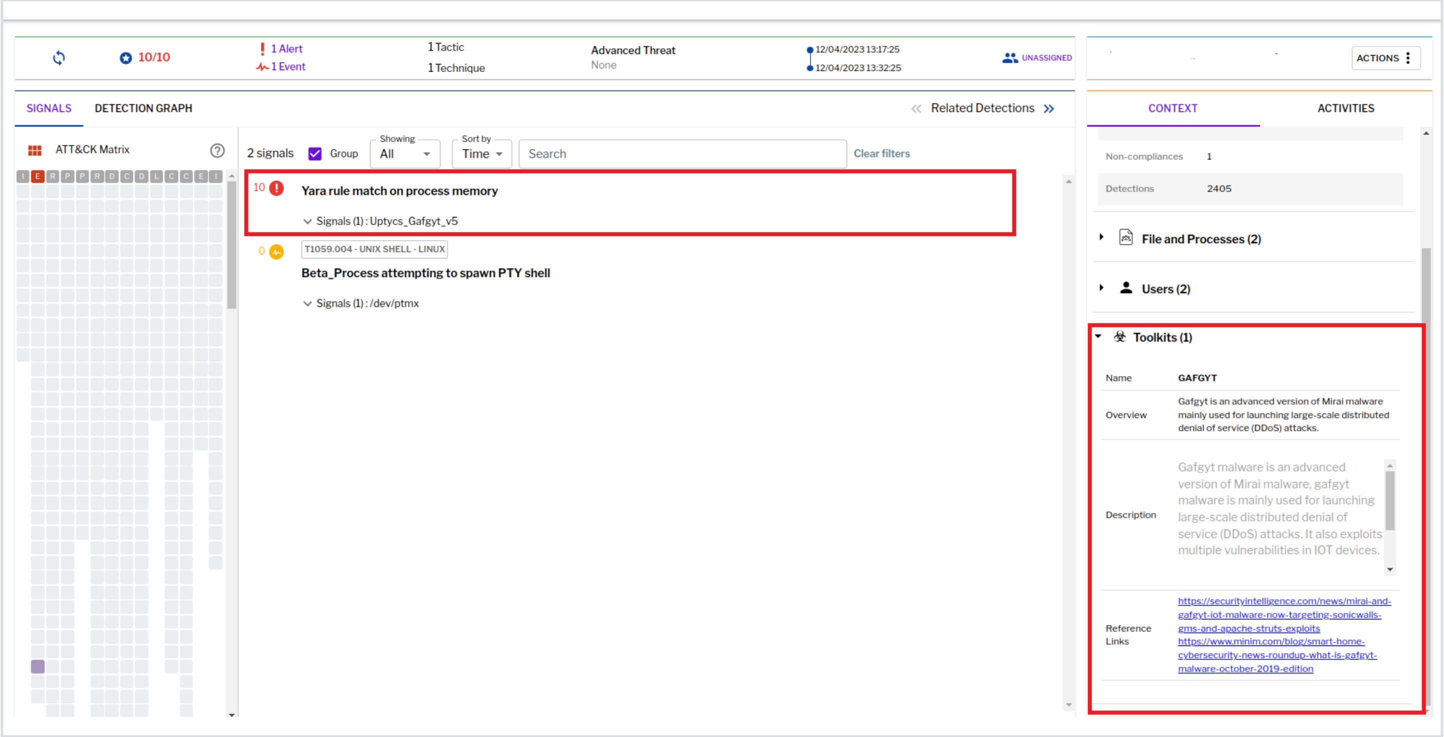
Toolkits (1)

Name	MIRAI
Overview	Mirai is malware that infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots.
Description	Mirai scans the Internet for IoT devices that run on the ARC processor. This processor runs a stripped-down version of the Linux operating system. If the default username-and-password combo is not changed, Mirai is able to log into
Reference Links	https://attack.mitre.org/techniques/T1583/005 https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet

Figure 16–Uptycs XDR detection of Mirai malware

Gafgyt

Gafgyt, targeting vulnerable IoT devices, particularly routers, spreads through phishing emails or exploits unpatched vulnerabilities. A recent focus has been on CVE-2017-18368, an unauthenticated command injection vulnerability.



10/10

1 Alert
1 Event

1 Tactic
1 Technique

Advanced Threat
None

12/04/2023 13:17:25
12/04/2023 13:32:25

2 signals

10 Yara rule match on process memory

Signals (1) : Uptycs_Gafgyt_v5

0 T1059.004 - UNIX SHELL - LINUX

Beta_Process attempting to spawn PTY shell

Signals (1) : /dev/ptmx

Non-compliances	1
Detections	2405

File and Processes (2)

Users (2)

Toolkits (1)

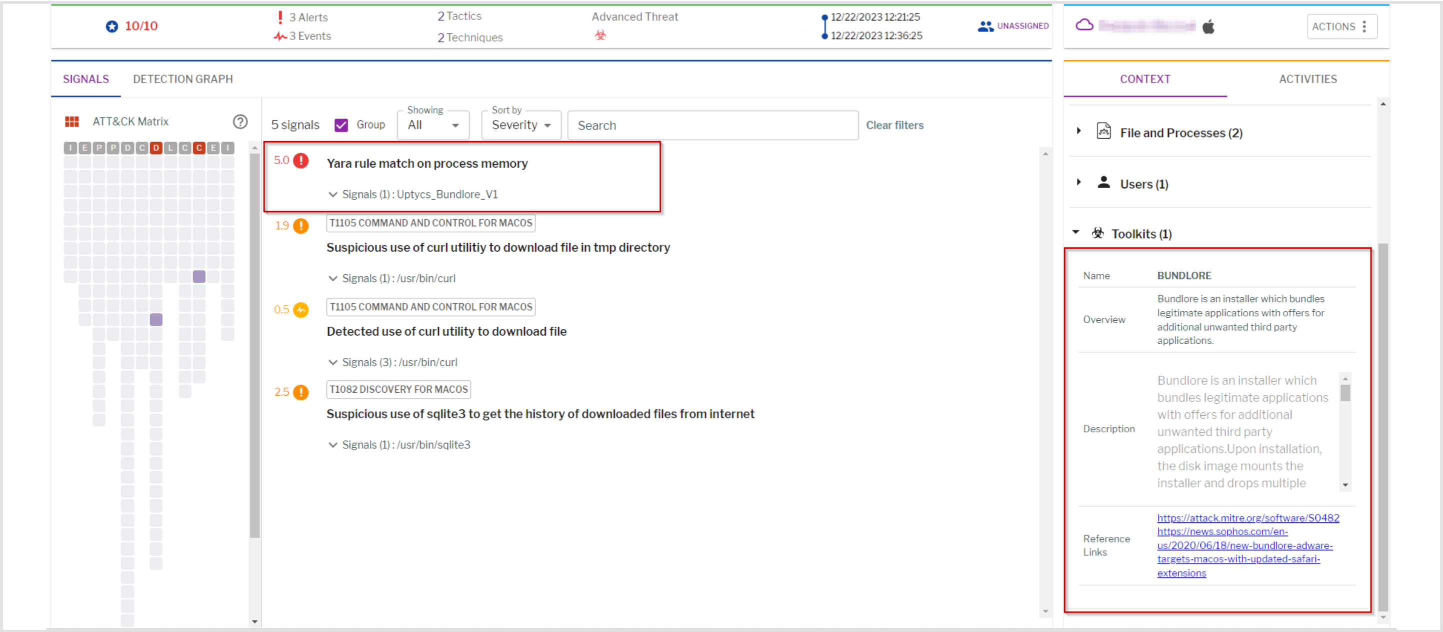
Name	GAFGYT
Overview	Gafgyt is an advanced version of Mirai malware mainly used for launching large-scale distributed denial of service (DDoS) attacks.
Description	Gafgyt malware is an advanced version of Mirai malware, gafgyt malware is mainly used for launching large-scale distributed denial of service (DDoS) attacks. It also exploits multiple vulnerabilities in IOT devices.
Reference Links	https://securityintelligence.com/news/mirai-and-gafgyt-iot-malware-now-targeting-sonicwalls-gms-and-apache-struts-exploits https://www.minim.com/blog/smart-home-cybersecurity-news-roundup-what-is-gafgyt-malware-october-2019-edition

Figure 17–Uptycs XDR detection of Gafgyt malware

MacOS malware:

Bundlore

Bundlore, an adware-turned-backdoor since 2015, deceives users with fake software installers, notably using a bogus Adobe Flash Player installer. Once installed, it executes a chain of actions to download and run Bundlore from a malicious domain.



5.0 Yara rule match on process memory
Signals (1) : Uptycs_Bundlore_V1

1.9 T1105 COMMAND AND CONTROL FOR MACOS
Suspicious use of curl utilitiy to download file in tmp directory
Signals (1) : /usr/bin/curl

0.5 T1105 COMMAND AND CONTROL FOR MACOS
Detected use of curl utility to download file
Signals (3) : /usr/bin/curl

2.5 T1082 DISCOVERY FOR MACOS
Suspicious use of sqlite3 to get the history of downloaded files from internet
Signals (1) : /usr/bin/sqlite3

File and Processes (2)

Users (1)

Toolkits (1)

Name	BUNDLORE
Overview	Bundlore is an installer which bundles legitimate applications with offers for additional unwanted third party applications.
Description	Bundlore is an installer which bundles legitimate applications with offers for additional unwanted third party applications.Upon installation, the disk image mounts the installer and drops multiple
Reference Links	https://attack.mitre.org/software/S0482 https://news.sophos.com/en-us/2020/06/18/new-bundlore-adware-targets-macos-with-updated-safari-extensions

Figure 18–Uptycs XDR detection of Bundlore adware

Q4 threat research articles

Double Trouble: Quasar RAT's Dual DLL Sideloading in Focus

The Uptycs Threat Research Team has uncovered a complex sideloading tactic used by Quasar RAT, utilizing two commonly trusted Microsoft files - "ctfmon.exe" and "calc.exe." This analysis offers insights into the sophisticated design of these sideloading techniques and their stealthy deployment of malicious payloads.

Read more about Quasar RAT's tactics

Heads Up: New Security Patch for Curl Vulnerability 2023

A significant flaw in curl, a widely-used data transfer tool, prompted an in-depth investigation by the Uptycs Research Team. Initially discussed on Curl's GitHub repository, the team's findings highlight the urgency for an update to address this vulnerability.

Explore our findings on the curl vulnerability

Confluence Server's Zero-Day Vulnerability CVE-2023-22515

Atlassian recently reported a zero-day vulnerability in its Confluence Server, which is now actively targeted by advanced threat actors. The vulnerability allows unauthorized attackers to create new administrator accounts with just three HTTP requests.

Learn more about this Confluence Server vulnerability

A New Critical Confluence Server Vulnerability Surfaces CVE-2023-22518

Following the zero-day vulnerability CVE-2023-22515, the Uptycs Threat Research Team identified another critical vulnerability, CVE-2023-22518, in Atlassian Confluence. This latest threat enables attackers to reset a Confluence instance and create new administrator accounts.
Read the latest report on CVE-2023-22518

Looney Tunables (CVE-2023-4911): Unexpected Input Compromises System

The “Looney Tunables” exploit, CVE-2023-4911, discovered by Uptycs in various Linux systems, affects the GLIBC_TUNABLES feature of the GNU C Library.
Discover more about Looney Tunables

GhostSec: From Fighting ISIS to Possibly Targeting Israel with RaaS

“GhostSec,” initially known for its actions against ISIS, has been observed potentially targeting Israel with a new Ransomware-as-a-Service, GhostLocker, promoted via Telegram.
Understand GhostSec’s latest campaign

Mitigate CVE-2023-46604: Apache ActiveMQ’s Critical Vulnerability

A critical vulnerability in Apache ActiveMQ, CVE-2023–46604, raises concerns over potential HelloKitty ransomware attacks on vulnerable systems. The Uptycs team concisely explains the exploitation mechanisms behind this vulnerability.
Learn how to mitigate CVE-2023-46604

WinRAR CVE-2023-38831 Vulnerability Draws Attention from APTs

CVE-2023-38831, a vulnerability in WinRAR, has become a focal point for various APT groups. The Uptycs Threat Intel Team delves into how these groups exploit this security flaw using diverse tactics.
Explore the APTs’ exploitation of WinRAR

Unraveling CVE-2023-46214: A Deep Dive into Splunk RCE Vulnerability

CVE-2023-46214, an RCE vulnerability in Splunk, poses a significant threat to data analytics infrastructures. Our blog comprehensively analyzes this vulnerability and its potential for exploitation.
Read our in-depth analysis of CVE-2023-46214

Threat Advisory: USPS Smishing Scam with Potential Links to China

A surge in USPS-targeted phishing campaigns, potentially linked to Chinese actors, has been identified by the Uptycs Threat Intelligence Team. Over 1,400 active phishing sites have been discovered globally.
Get the full threat advisory on the USPS scam

Top threat actors in focus

Lazarus Group

The Lazarus Group, linked to North Korea, has been implicated in a global campaign, notably exploiting the Log4j vulnerabilities to deploy RATs on compromised hosts. Active since 2009, this sophisticated APT group has targeted entities in the blockchain and cryptocurrency sectors through spear-phishing and malware. Their "Operation Blacksmith" campaign uses DLang-based malware families, including NineRAT, DLRAT, and BottomLoader, to exploit CVE-2021-44228 against VMWare Horizon servers.

SideWinder

SideWinder APT, known by aliases including Razor Tiger and T-APT-04, is a suspected Indian group targeting Pakistani government organizations since 2012. They use email spear-phishing, document exploitation, and DLL side-loading techniques. A recent campaign involved a malicious Word document targeting Nepalese officials, deploying a complex array of scripts and the Nim backdoor.

Kimsuky

North Korea's Kimsuky APT group, operational since 2013, continues to sophisticate its methods, now leveraging legitimate remote desktop tools and custom malware. They target national defense, diplomatic, and academic sectors, often deploying backdoors and infostealers. Notably, they use Remote Desktop Protocol [RDP] and custom versions of TinyNuke or TightVNC for remote control.

Arid Viper

AridViper, associated with the Middle East and suspected ties to Hamas, targets Arabic-speaking countries with custom malware and sophisticated social engineering. Known for deploying backdoors, spyware, and advanced mobile malware, AridViper's tactics include spear-phishing emails and malicious websites designed to mimic legitimate sources.

APT29

APT29, also known as The Dukes, Cozy Bear, or Nobelium, is a prominent cyber espionage group likely associated with Russia's Foreign Intelligence Service (SVR). APT29 commonly use HTML Smuggling techniques and malicious ISO images to deliver their malware while evading security measures. APT29 has been reported in active campaign through targeting the victim by spear-phishing email, using the lure of a diplomatic car for sale. The RAR attachment featured CVE-2023-3883, a vulnerability which enables threat actors to insert malicious folders with the same name as benign files in the zip archive. APT29 has also used 'Ngrok' to host their next-stage PowerShell payloads and establish covert communication channels.

Key vulnerabilities / exploits

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

Windows

CVE-2023-36563 - Microsoft WordPad Information Disclosure Vulnerability

CVE-2023-41763 - Skype for Business Elevation of Privilege Vulnerability

CVE-2023-36584 - Windows Mark of the Web Security Feature Bypass Vulnerability

CVE-2023-36036 - Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability

CVE-2023-36033 - Microsoft Windows DWM Core Library Elevation of Privilege Vulnerability

CVE-2023-36025 - Microsoft Windows SmartScreen Security Feature Bypass Vulnerability

CVE-2023-36038 - ASP.NET Core Denial of Service Vulnerability

CVE-2023-40044 - Progress WS_FTP Server Critical Deserialization Vulnerability

CVE-2023-45685 - Titan MFT and Titan SFTP server Remote Code Execution Vulnerability

CVE-2023-43208 - NextGen Healthcare Mirth Connect RCE Vulnerability

Linux

CVE-2023-4911 - Local Privilege Escalation Vulnerability in the GNU C Library 'ld.so' in Linux

CVE-2023-39191 - Linux Kernel eBPF Improper Input Validation Privilege Escalation Vulnerability

CVE-2023-43115 - Artifex Ghostscript Remote Code Execution Vulnerability

CVE-2023-43641 - Libcue Library Out-of-bounds Array Access Vulnerability

CVE-2023-45685 - Titan MFT and Titan SFTP server Remote Code Execution Vulnerability

CVE-2023-5631 - Critical XSS Vulnerability in Roundcube Email Client Exploited by Winter Vivern Threat Group

CVE-2023-43208 - NextGen Healthcare Mirth Connect RCE Vulnerability

CVE-2023-46604 - Apache ActiveMQ Remote Code Execution Vulnerability

CVE-2023-34212 - Apache NiFi Deserialization Vulnerability

CVE-2023-49083 - NULL-Pointer Dereference and Segfault Vulnerability In Cryptography Python Package

CVE-2023-22515 : Privilege Escalation Vulnerability in Confluence Data Center and Server

CVE-2023-22518 : Improper Authorization Vulnerability in Confluence Data Center and Server

macOS

CVE-2023-42916 - Out-of-bounds Read Vulnerability in macOS and Apple Safari

CVE-2023-42917 - Memory Corruption Vulnerability in macOS and Apple Safari

CVE-2023-22524 - Remote Code Execution Vulnerability in Atlassian Companion App for MacOS

CVE-2023-41976 - Use-after-free Error in macOS and Apple Safari

CVE-2023-42852 - WebKit Arbitrary Code Execution in macOS and Apple Safari

CVE-2023-42890 - Webkitgtk Arbitrary Code Execution in macOS and Apple Safari

Vulnerabilities affecting **Windows, Linux** and **macOS** environments:

CVE-2023-7024 : Google Chrome Heap Corruption Vulnerability

CVE-2023-42793 : JetBrains TeamCity Authentication Bypass Vulnerability

CVE-2023-44487 : HTTP/2 Rapid Reset Attack Denial-of-Service Vulnerability

CVE-2023-46214 : Remote Code Execution (RCE) in Splunk Enterprise

CVE-2023-6345 : Integer Overflow in Google Chrome Leading To Sandbox Escape

CVE-2023-5730 : Memory Safety Vulnerability in Firefox, Thunderbird and ESR 115.4

CVE-2023-5731 : Memory Safety Vulnerability in Firefox

CVE-2023-3765 - Critical Path Traversal Vulnerability in Mlflow

General recommendations

Incident response teams should rigorously investigate the parent processes responsible for triggering the execution of key utilities across different operating systems:

- Windows: Pay close attention to rundll32.exe, wscript.exe, mshta.exe, powershell.exe, and reg.exe utilities.
- Linux: Monitor the use of crontab, chattr, find, systemctl, and wget utilities.
- macOS: Scrutinize activities involving Openssl, killall, curl, sqlite, and system_profiler utilities.

To enhance security against malware attacks, organizations are recommended to follow these cyber hygiene best practices:

1. Software Updates: Regularly update all software to patch vulnerabilities.
2. Strong Password Policies: Implement and enforce robust password policies.
3. Multi-Factor Authentication: Activate multi-factor authentication to add an extra layer of security.

4. Caution with Suspicious Links: Avoid opening links and attachments from unknown or untrustworthy sources.

5. Data Backup: Regularly back up important data to prevent loss during a cyber attack.

Implementing these practices can significantly strengthen an organization's defense against various cyber threats.

Conclusion

As we wrap up this edition of the Uptycs Quarterly Threat Bulletin for Q4 2023, it's clear that the sophistication of cyber threats continues to rise, highlighting the critical need for advanced cybersecurity tools and strategies. This quarter has demonstrated the ingenuity of malware evolution and the emergence of new vulnerabilities and brought to light the relentless and innovative tactics employed by threat actors.

Our in-depth analysis throughout this bulletin underscores the indispensable role of sophisticated cybersecurity solutions in today's digital landscape. To counter these threats effectively, organizations must understand the latest adversarial trends and equip themselves with the most advanced defenses.

At Uptycs, our commitment to empowering organizations with cutting-edge security insights and solutions is unwavering. We strive to ensure that our clients are well-prepared and resilient against the multifaceted cyber threats they face.

We will continue to be at the forefront of threat intelligence, offering actionable insights and robust tools to help secure the digital frontier. We encourage our readers to stay informed and proactive, making cybersecurity an integral part of their operational ethos.

Thank you for placing your trust in Uptycs. Together, we are building a more secure and resilient digital future.

.