

# Q4 Quarterly Threat Bulletin

The quarterly Uptycs 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 in Windows, Linux and macOS platforms.



# Index

Q4 Threat Bulletin Highlights	<b>3</b>
Critical Alerts	<b>4</b>
CVE-2022-41040 and CVE-2022-41082 - ProxyNotShell Exploit	<b>4</b>
Techniques used by the malware samples	<b>4</b>
Commonly abused commands and utilities	<b>5</b>
Windows utilities abused by malware	<b>5</b>
Linux utilities abused by malware	<b>7</b>
macOS Utilities abused by malware	<b>8</b>
Top prevalent malware families in the wild	<b>9</b>
Uptycs Threat Research articles	<b>16</b>
Top Threat actors in focus	<b>16</b>
Key Vulnerabilities / Exploits	<b>18</b>
Windows	<b>18</b>
Linux	<b>18</b>
macOS	<b>19</b>
Windows/macOS/Linux	<b>19</b>
General recommendations	<b>19</b>

# Q4 Threat Bulletin Highlights

- 1.** The zero-day vulnerabilities CVE-2022-41040 and CVE-2022-41082, collectively known as ProxyNotShell, are found in Windows Exchange email servers and have been observed to be exploited by the Lockbit and Play ransomware gang.
- 2.** In this quarter, we have observed the following prevalent malware:
  - a.** Emotet, QBot and Darkcomet are the most prevalent malware in Q4 2022 observed for Windows platforms.
  - b.** XorDDOS and Gfagyt were seen in large numbers in Q4 2022 on the Linux platform.
  - c.** Shlayer and Bundlore continue to be evergreen in action on macOS.
- 3.** Most Windows malware nominated LOLBin—rundll32.exe—as the most abused utility for Windows and chattr has taken the top spot in abused utilities in Linux.
- 4.** In macOS, openssl and killall are very prevalent utilities as it is widely leveraged by Shlayer and Bundlore.
- 5.** LockBit, a known ransomware group, was identified as the most active group in Q4, by targeting several victims. Other active groups included Alpha, Royal, and Basta.
- 6.** Threat actor activity from Mustang Panda, Lazarus, TA505, APT29, and APT37 has been reported.
- 7.** One Google Chrome zero-day vulnerability, CVE-2022-4262, was reported to be exploited in the wild.
- 8.** Another use-after-free vulnerability, CVE-2022-26486, in WebGPU IPC Framework as used in Firefox, Firefox ESR, Thunderbird was also being exploited in the wild.

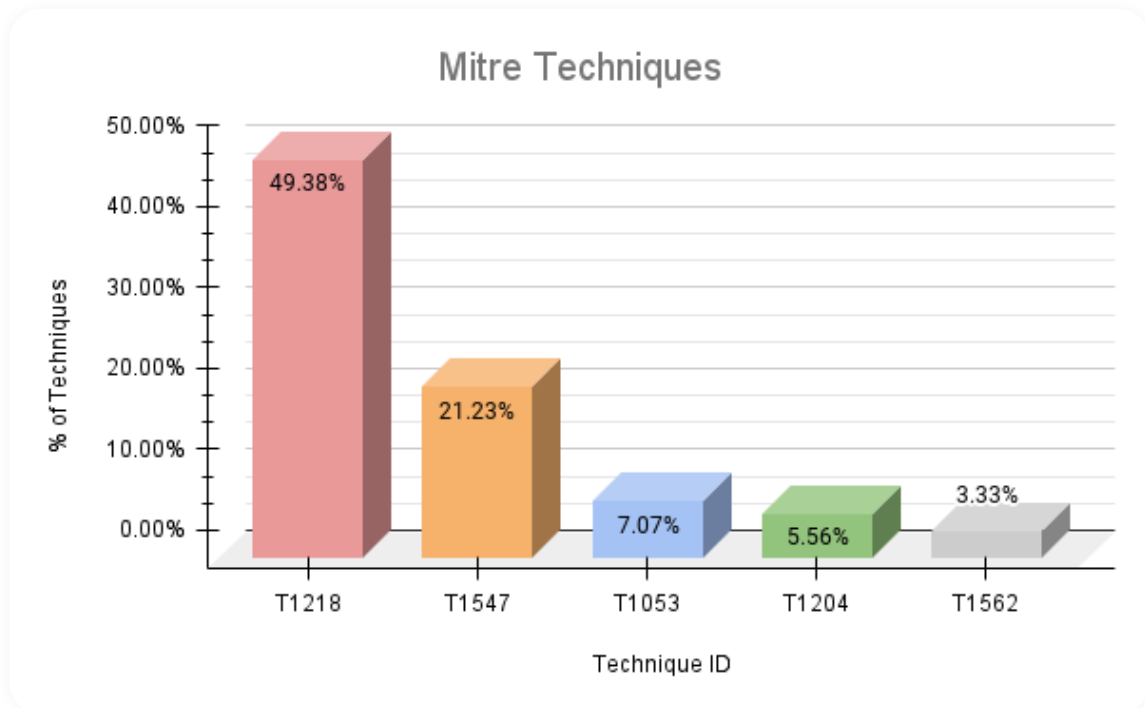
## Critical Alerts

### CVE-2022-41040 and CVE-2022-41082 - ProxyNotShell Exploit

The zero-day vulnerabilities CVE-2022-41040 and CVE-2022-41082, collectively known as ProxyNotShell, were found being actively exploited, affecting Windows Exchange email servers. An attacker could use CVE-2022-41040, a server-side request forgery (SSRF) vulnerability, to become able to exploit the next vulnerability, CVE-2022-41082. Attackers initially used CVE-2022-41040 to gain access to the PowerShell API endpoint (<https://%exchange server domain%/powershell>). An attacker with a known credential combination for a registered account can use this access to execute PowerShell commands in the Exchange environment. The attacker then uses the WSMAN Protocol to gain access to the Web-Based Enterprise Management (WBEM) and launch a shell for further script execution via Windows Remote Management (PsRemoting). An attacker was the “LockBit” ransomware gang, which reportedly began to exploit the Microsoft Exchange flaws in October. The ransomware group “[Play](#)” discovered ways to bypass ProxyNotShell URL rewrite mitigations in December.

### Techniques used by the malware samples

The Uptycs threat research team configured Uptycs EDR 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 [Signed Binary Proxy Execution \(T1218\)](#), [Boot or Logon Autostart Execution \(T1547\)](#), [Scheduled Task/Job \(T1053\)](#), [User Execution \(T1204\)](#), and [Impair Defenses \(T1562\)](#) described in the MITRE ATT&CK framework. The prevalence of these observed ATT&CK technique IDs is shown below.



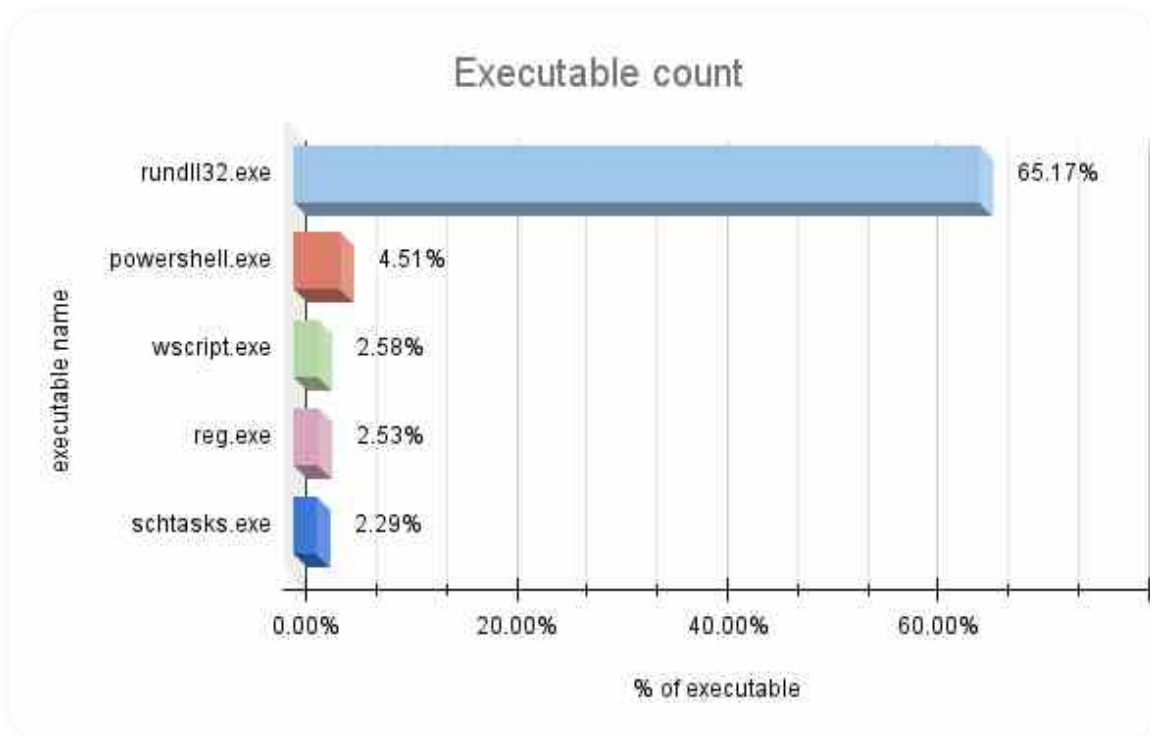
## Commonly abused commands and utilities

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 the tactics in Windows, Linux, and macOS in our replication systems.

### Windows utilities abused by malware

In this quarter, we observed Rundll32.exe to be the top abused utility. Rundll32.exe, wscript.exe, schtasks.exe and Reg.exe were the top abused utilities in Q4 2022.

The list of the top 5 Windows utilities abused by malware and their prevalence is shown below.



### rundll32.exe

Tactic: Defense Evasion

- Rundll32.exe is a crucial part of Microsoft Windows that's made to launch functionality based on Windows DLL (dynamic linked library) files. It is a very often used tool by adversaries to proxy execution of arbitrary malicious code and dump LSASS memory.
- Emotet and Qbot malware have leveraged rundll32.exe to execute their second-stage payload DLL.

## **powershell.exe**

Tactic: Execution, Defense Evasion, and Command & Control

- Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of malicious codes. PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.
- In the latest samples of Emotet, it most often uses LNK decoy files to launch PowerShell in the Execution phase of MITRE ATT&CK Framework.

## **wscript.exe**

Tactic: Execution and Defense Evasion

- Wscript.exe, also known as Windows Script Host, appears to be a Microsoft Windows-based process that can occasionally be misused for malicious purposes. Cybercriminals use the names of various legitimate processes/files to disguise malicious files.
- REvil utilizes WScript scripts to execute. The malicious JavaScript attachment has an obfuscated PowerShell script that executes the malware.

## **reg.exe**

Tactic: Defense Evasion

- Reg is a Windows utility used to interact with the Windows Registry. It can be used at the command-line interface to query, add, modify, and remove information.
- Agent Tesla, Lokibot, njRAT, and many other malware families use this technique to modify/create/delete to bypass its execution.

## **Schtasks.exe**

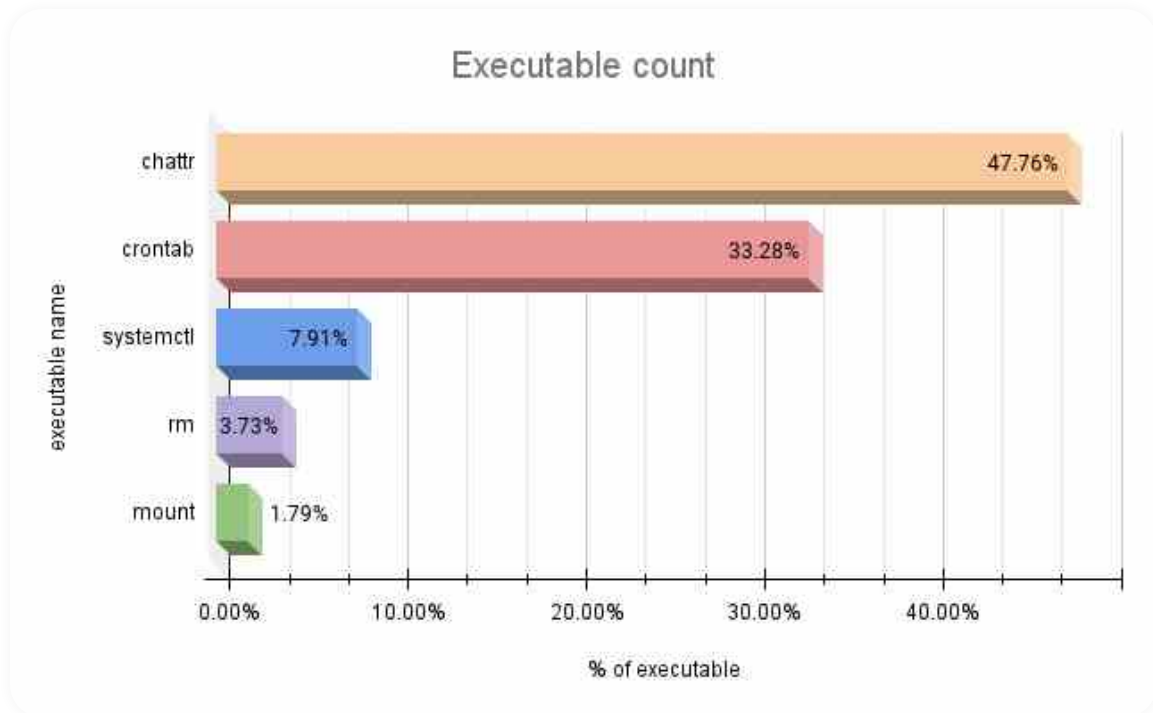
Tactic: ExecutionImpact and Defense Evasion

- Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges).
- StrifeWater RAT has created a scheduled task for persistence.

## Linux utilities abused by malware

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

The top 5 Linux utilities abused by malware and their prevalence is shown below.



### chatr

Tactic: Defense Evasion

- The chatr in Linux is used to set/unset certain attributes of a file. Adversaries use this for changing the permission of the system files or to make their dropped files immutable so that a user cannot delete them.
- Kinsing malware uses this utility to change permissions of ssh\_authorized keys, /etc/passwd files in the Defense Evasion phase of the attack lifecycle.

### crontab

Tactic: Persistence

- In Linux, the crontab command opens the cron table for editing the list of tasks scheduled to run at regular time intervals on the system.
- We have observed XorDDOS leveraging crontab for persistence.

### Systemctl

Tactic: Persistence

- The systemctl command is a utility to manage systemd and service manager in Linux.
- Coinminers use systemctl utility to disable security solution agents like Aliyun, bcm agents.

## rm

Tactic: Impact

- The rm command is a utility to remove/delete files from the system in Linux.
- Gafgyt uses the rm utility to delete artifacts and files on the system.

## mount

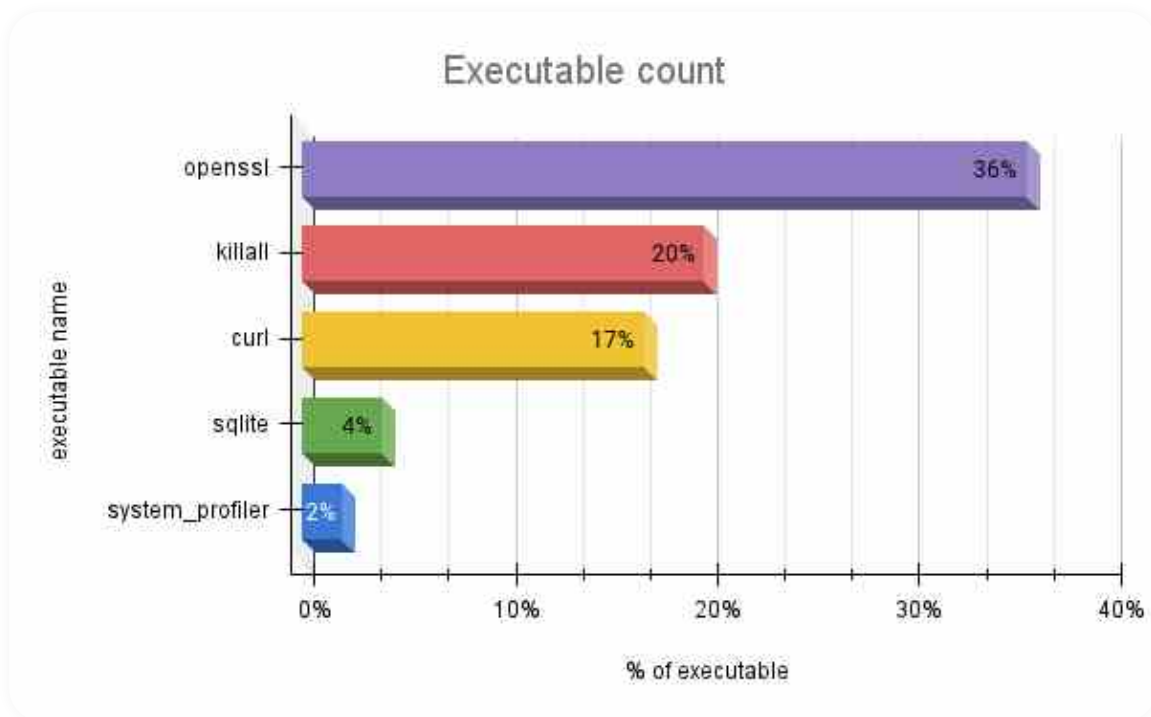
Tactic: Defense Evasion

- The mount command is a utility to mount or unmount “file systems”.
- Cryptomung uses the mount to mount the “file system” into the system.

## macOS Utilities abused by malware

In this quarter, we continue to see macOS malware contributed by Shlayer.

The top 5 macOS utilities abused by malware and their prevalence is shown below.



## Openssl

Tactic: Defense Evasion

- OpenSSL is an open-source command line tool that is commonly used to generate private keys, create CSRs, install your SSL/TLS certificate, and identify certificate information.
- Shlayer malware leverages Openssl often in conjunction with base64, to encode and decode malware to hide it from detection in the Defense Evasion phase of the attack lifecycle.



## killall

Tactic: Defense Evasion

- killall is a macOS utility for terminating running processes on your system based on name.
- Shlayer malware uses killall to kill the running script's terminal window after bash script activity is completed in the Defense Evasion phase of the attack lifecycle.

## curl

Tactic: Command and control

- Curl is a macOS command-line tool (curl) used for transferring data using various network protocols.
- Shlayer malware leverages curl to download payloads in the Command & Control phase of the attack lifecycle.

## sqlite

Tactic: Exfiltration

- SQLite is a transactional SQL database engine present in macOS generally used to create databases that can be transported across machines.
- 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 is a command line utility in macOS used for displaying system related configuration.
- 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 added YARA coverage for the malware processes in the Uptycs platform. Customers can now view the toolkit profiles of this malware when detection is triggered in Uptycs.

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

### Windows

- Qbot
- Emotet
- Darkcomet

### Linux

- XorDDOS
- Gafgyt

### macOS

- Shlayer & Bundlore

## Emotet

The Emotet banking trojan was first identified in 2014. Emotet was originally designed as a banking malware that attempted to sneak onto victim computers and steal sensitive and private information.

The malware also attempts to proliferate within a network by brute forcing user credentials and writing to shared drives. Emotet is difficult to combat because of its 'worm-like' features that enable network-wide infections.

Additionally, Emotet uses modular Dynamic Link Libraries to continuously evolve and update its capabilities.

The screenshot displays a security dashboard interface. At the top, there are navigation elements including '10/10', 'Alerts', '0 Events', 'Tactic', 'Technique', 'Advanced Threat', and a date range from '02/09/2023 14:38:01' to '02/09/2023 14:54:01'. The main area is divided into 'SIGNALS' and 'DETECTION GRAPH'. The 'SIGNALS' section shows a list of signals under the category 'Bad IP - Malware'. A red box highlights a specific signal: 'Yara rule match on process memory' with a sub-entry 'Signals (1): Uptycis\_Emotet\_v8'. To the right, a 'CONTEXT' panel provides details for the 'EMOTET' toolkits, including its aliases, overview, and description. The description states: 'Emotet is a banking trojan first seen in 2014 which can steal credentials stored in browsers and other data. It is known to spread through spam emails.' Reference links are also provided.

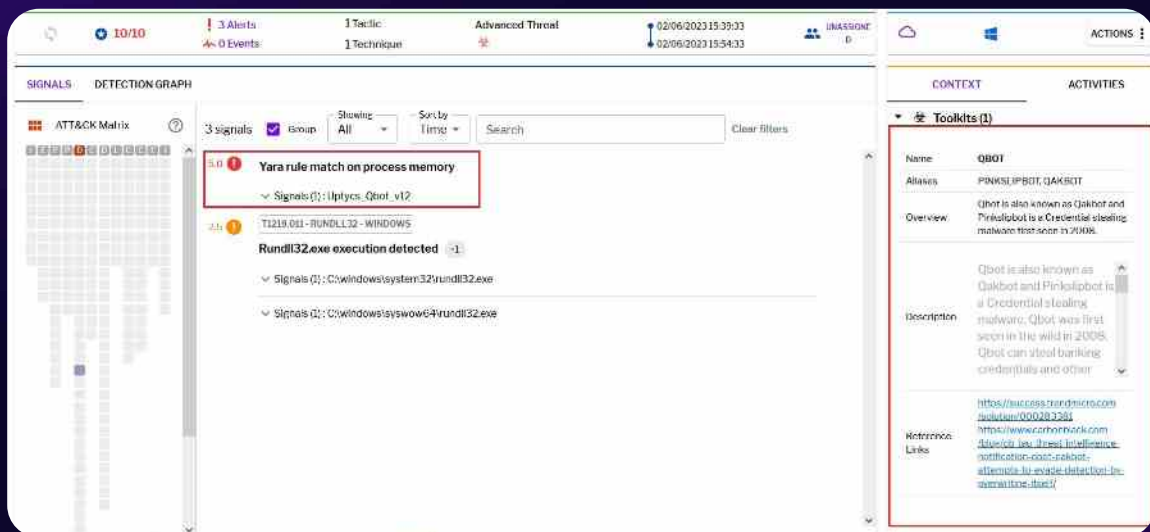
## Windows

### QBot

QBot, also known as Qakbot, QBot, QuackBot, and Pinkslipbot, is a Banking Trojan that was first observed in 2007.

Qbot uses multiple attack vectors to infect victims. QBot is distributed through phishing emails containing malicious documents, attachments, or password-protected archives with the documents attached.

QBot continues to grow and develop, with more capabilities and new techniques. Its main purpose is to steal banking data. However, its developers have also developed functionalities that allow QBot to spread itself, evade detection and debugging, and install additional malware on compromised machines, such as Cobalt Strike, REvil, ProLock, and Egregor ransomware.



The screenshot displays a security dashboard interface. At the top, it shows '10/10' alerts, '3 Alerts', '0 Events', '1 Tactic', '1 Technique', 'Advanced Threat', and a timestamp of '02/06/2023 15:39:03'. The main section is titled 'SIGNALS DETECTION GRAPH' and shows a tree view of signals. A red box highlights the signal 'Yara rule match on process memory' (Severity 3.0) with a sub-signal 'Signals (1): I:\pt\cs: Qbot\_v12'. Below it, another signal 'Rundll32.exe execution detected' (Severity 1) is shown with sub-signals for 'C:\windows\system32\rundll32.exe' and 'C:\windows\system32\rundll32.exe'. On the right side, a 'CONTEXT' panel for 'Toolkits (1)' is visible, listing 'QBOT' with aliases 'PINKSLIPBOT, QAKBOT' and a description: 'Qbot is also known as Qakbot and Pinksipbot is a Credential stealing malware first seen in 2008.' It also includes a 'References' section with links to security blogs.

## Windows

### Darkcomet

DarkComet is a remote access trojan developed in 2008. It is a malicious program designed to remotely control or administer a victim's computer, steal private data and spy on the victim.

DarkComet got viral in 2012 after the Syrian incident: the government used the RAT to spy and destroy the protestor's network.

It's a standard remote control malware – a hacker rules over the infected computer and gets access to the camera and microphone.

The screenshot displays a security dashboard interface. At the top, it shows '10/10' status, '6 Alerts', and '0 Events'. The main area is titled 'SIGNALS' and 'DETECTION GRAPH'. It lists several signals, with 'Bad domain - Malware' and 'Yara rule match on process memory' highlighted with red boxes. The 'Yara rule match on process memory' signal is further detailed with 'Signals (1): Uotvcs\_Darkcomet\_VI'. Below this, there is a section for 'Attrib.exe execution detected' with 'Signals (1): C:\windows\system32\attrib.exe'. On the right side, there is a 'CONTEXT' and 'ACTIVITIES' panel. Under 'Toolkits (1)', there is a detailed entry for 'DARKCOMET', including an overview and a description: 'Darkcomet is a RAT that has the capability to collect sensitive data from victims. This RAT gets silently installed on the victim machines. The RAT spies network.' A reference link is also provided: 'https://blog.malwarebytes.com/threat-analysis/2012/02/02/021202-attrib-rat-scan-3-darkcomet/'. The interface also includes a search bar, filters, and a 'Clear Filters' button.

## XorDDoS

XOR DDoS is a Linux Trojan malware with rootkit capabilities that were used to launch large-scale DDoS attacks. Its name stems from the heavy usage of XOR encryption in both malware and network communication to the C&Cs. It is built for multiple Linux architectures like ARM, x86, and x64.

This malware performs C&C communication in both directions using a hard-coded XOR key, hence its name XOR DDoS.

The screenshot displays a security dashboard interface. At the top, there is a navigation bar with various status indicators: 10/10, 2 Alerts, 1 Event, 2 Tactics, 2 Techniques, Advanced Threat, and a user profile labeled UNASSIGNED. The main content area is divided into two tabs: SIGNALS and DETECTION GRAPH. The SIGNALS tab is active, showing a list of three signals. The first signal, highlighted with a red box, is a Yara rule match on process memory (5.0) with the signal ID Uptycs\_XorDDoS\_v2. The second signal (2.5) is T1204.002 USER EXECUTION\_LINUX, and the third (0.1) is T1057 DISCOVERY FOR LINUX. The right-hand sidebar contains a CONTEXT section with tabs for Asset Info, File and Processes (2), and Users (1). Below this is a Toolkits (1) section, also highlighted with a red box, which provides details for XorDDoS, including its name, overview, description, and reference links.

Name	XORDDOS
Overview	XorDdos is a linux based malware which is used to launch larger scale Ddos attacks.It also has rootkit capabilities.
Description	XorDdos is a linux based malware which is used to launch larger scale Ddos attacks.It also has rootkit capabilities. It is named on the basis of its feature of using XOR encryption algorithm while C2 communication. Some of its
Reference Links	<a href="https://sucrress.trendmicro.com/solutions/000278087">https://sucrress.trendmicro.com/solutions/000278087</a>

# Linux

## Gafgyt

Gafgyt (also known as Bashlite) first made its appearance back in 2014, and is a prominent malware family for \*nix systems, which mainly target vulnerable IoT devices like Huawei routers, Realtek routers and ASUS devices.

Gafgyt also uses some of the existing exploits (CVE-2017-17215, CVE-2018-10561) to download the next stage payloads.

Gafgyt malware variants have very similar functionality to Mirai, as a majority of the code was copied.

The screenshot displays a security dashboard with a top navigation bar showing 10/10 status, 4 Alerts, 5 Tactics, 8 Techniques, and an Advanced Threat indicator. The main area is titled 'SIGNALS' and 'DETECTION GRAPH'. On the left, there is an ATT&CK Matrix. The central list of signals includes:

- 2.0 T1548.003 PRIVILEGE ESCALATION FOR LINUX: Process using runuser utility to execute command in privilege. Signals (1): /usr/sbin/runuser.
- 2.5 T1204.002 USER EXECUTION\_LINUX: Process dropped executable file in monitored directories. Signals (1): /home/mao/Downloads/e5b0bc154e0f8911e5057958aa0d93874194ad41e85159f3b0cfa86a3d5e1d4c.tif.
- 5.0 Yara rule match on process memory -1: Signals (2): Uptycs\_Gafgyt\_CVE\_2017\_17215v3.
- 0.1 T1083 DISCOVERY FOR LINUX: Process using ls utility to list files and directories -18. Signals (19): /usr/bin/ls.
- 0 T1059.004 EXECUTION\_LINUX: Z\_Beta\_Process starting interactive shell -2. Signals (3): /usr/bin/bash.
- 2.0 T1069.002 DISCOVERY FOR LINUX: Process using groups utility to get group policies -2. Signals (3): /usr/bin/groups.

The right sidebar shows 'CONTEXT' and 'ACTIVITIES'. Under 'Toolkits (1)', the GAFGYT toolkit is detailed:

- 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://securityvibe@secops.com/news/mirai-and-gafgyt-iot-malware-now-targets-smart-walls-sms-and-garage-locks-exploits>, <https://www.mitm.com/blog/smart-home-iot-security-news-roundup-what-is-mirai-malware-october-2018-edition>

## Shlayer & Bundlore

Shlayer is a trojan virus specifically targeted toward Mac systems. Its primary function is to download malicious code via fake applications and flash updates. Once the Shlayer virus is installed on a system, it begins to download and install malware focused on the proliferation of ads, otherwise known as adware. The adware installed and downloaded by Shlayer forces advertising into Mac's browser and can even intercept browser searches to modify the results to promote more ads.

Shlayer initially arrives on the device using a mountable disk image (.dmg) file. It masquerades as a legitimate Adobe Flash Player update and contains a shell script that uses OpenSSL to decrypt the hidden payload. The shell script could provide backdoor capabilities to attackers while the initial .dmg file runs in the background as a trojan downloader. Upon initialization, it collects system information and sends the collected data to the attacker's command-and-control (C2) server. It then searches for the .app extension in the current working folder path and sets execution permission using the following command to launch the child process. After successful execution, it creates an additional child process that downloads the base64-encoded file and decodes the base64 script file. This is used for setting environment variables for the process being spawned.

The screenshot shows a security dashboard with the following details:

- Top Bar:** 10/10 status, 3 Alerts, 3 Events, 2 Tactics, 2 Techniques, Advanced Threat, 12/01/2022 23:35:34, UNASSIGNED, and ACTIONS menu.
- SIGNALS:** 5 signals, Group, Showing: All, Sort by: Severity, Search, Clear filters.
- Signal List:**
  - 5.0 (Critical):** Yara rule match on process memory. Signals (1): Uptycs\_Bundlore\_V1.
  - 1.9 (Low):** T1105 COMMAND AND CONTROL FOR MACOS. Suspicious use of curl utility to download file in tmp directory. Signals (1): /usr/bin/curl.
  - 0.5 (Info):** T1105 COMMAND AND CONTROL FOR MACOS. Detected use of curl utility to download file. Signals (3): /usr/bin/curl.
  - 2.5 (Medium):** T1082 DISCOVERY FOR MACOS. Suspicious use of sqlite3 to get the history of downloaded files from internet. Signals (1): /usr/bin/sqlite3.
- CONTEXT - ACTIVITIES:**
  - 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-updater-cache-extension>

## Uptycs Threat Research articles

### [Agent Tesla Malware Analysis: WSHRAT Acting As A Dropper:](#)

This research article details the new Agent Tesla malware attack campaign. Here the threat actors were trying to drop Agent Tesla malware via WSHRAT malware.

### [OpenSSL Buffer Overflow Vulnerabilities CVE-2022-3602 and CVE-2022-3786:](#)

This research article details the two vulnerabilities that affected OpenSSL versions 3.0.0 to 3.0.6. This blog post provides resources to Uptycs customers to help inventory and prioritize vulnerable systems for patching.

### [Text4Shell \(CVE-2022-42889\) Queries: Java Vulnerability Scanning With osquery:](#)

This research article details a new vulnerability in the Java source code library, dubbed Text4Shell, in Apache Commons Text versions 1.5 through 1.9. This blog provides insights to figure out which systems might have vulnerable software and then prioritize remediation.

## Top Threat actors in focus

### [APT37](#)

APT37 has likely been active since at least 2012 and focuses on targeting the public and private sectors primarily in South Korea.

Recently, Google has revealed that a group of North Korean hackers tracked as APT37 exploited an Internet Explorer vulnerability CVE-2022-41128 (known as a zero-day) to infect South Korean targets with malware.

Google was made aware of this recent attack on October 31 when multiple VirusTotal submitters from South Korea uploaded a malicious Microsoft Office document named "221031 Seoul Yongsan Itaewon accident response situation (06:00).docx."

Once opened on the victims' devices, the document would deliver an unknown payload after downloading a rich text file (RTF) remote template that would render remote HTML using Internet Explorer. Loading the HTML content that delivered the exploit remotely allows the attackers to exploit the IE zero-day even if the targets weren't using it as their default web browser.

### [Lazarus Group](#)

The Lazarus hacking group is one of the top cybersecurity threats from North Korea. Since 2009, HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims; some intrusions have resulted in the exfiltration of data while others have been disruptive in nature.

The North Korean 'Lazarus' hacking group has also been linked to a new attack spreading fake cryptocurrency apps under the made-up brand, "BloxHolder," to install the AppleJeus malware for initial access to networks and steal crypto assets.



Another new characteristic in recent AppleJeus samples is that all its strings and API calls are now obfuscated using a custom algorithm, making them stealthier against security products.

Although Lazarus' focus on cryptocurrency assets is well documented, the North Korean hackers remain fixed on their goal to steal digital money, constantly refreshing themes and improving tools to stay as stealthy as possible.

### **TA505**

TA505 is a financially motivated threat actor group believed to have been operating for almost a decade. In more recent years, it is believed that the group is responsible for operating the Clop ransomware after compromising corporate networks by using a variety of remote administration malware such as SDBbot, FlawedAmmy, and FlawedGrace, which were downloaded via Get2, Gelup or Mirrorblast. Over time, the group has become more sophisticated by adopting a diverse set of tactics, techniques, and procedures (TTPs).

The threat actor is also using a new custom data exfiltration tool called Teleport. Analysis of Silence's attacks over the past months revealed that the gang delivered Clop ransomware typically deployed by TA505 hackers, which are associated with the FIN11 group.

In a small number of attacks, the hackers had also infected systems with Truebot (Silence. Downloader) after exploiting a critical vulnerability in Netwrix Auditor servers tracked as CVE-2022-31199.

### **Mustang Panda**

Mustang Panda is a China-based APT group that has been identified as a cyber espionage threat actor. The group was first detected in 2017 and may have been active since 2014. Mustang Panda, also called Bronze President, Earth Preta, HoneyMyte, and Red Lich is a China-based espionage actor believed to be active since at least July 2018. The group is known for its use of malware such as China Chopper and PlugX to collect data from compromised environments.

The latest findings from Trend Micro show that Mustang Panda continues to evolve its tactics in a strategy to evade detection and adopt infection routines that lead to the deployment of bespoke malware families like TONEINS, TONESHELL, and PUBLOAD.

Initial access is facilitated through decoy documents that cover controversial geopolitical themes to entice the targeted organizations into downloading and triggering the malware.

### **APT29**

The Russia-linked APT29 nation-state actor has been found leveraging a lesser-known Windows feature called Credential Roaming following a successful phishing attack against an unnamed European diplomatic entity.

APT29, a Russian espionage group also called Cozy Bear, Iron Hemlock, and The Dukes, is known for its intrusions aimed at collecting intelligence that align with the country's strategic objectives. It's believed to be sponsored by the Foreign Intelligence Service (SVR).

One of the LDAP attributes queried by APT29, per the Google subsidiary, concerned ms-PKI-Credential-Roaming-Tokens, which handles the storage of encrypted user credential token BLOBs for roaming.

Investigating its inner workings further, Mandiant researchers highlighted the discovery of an arbitrary file write vulnerability that could be weaponized by a threat actor to achieve remote code execution in the context of the logged-in victim.

## Key Vulnerabilities / Exploits

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

Threat books as well know

### Windows

- [CVE-2022-41128](#) - Remote Code Execution Vulnerability in the Windows Scripting Language 'JScript9'
- [CVE-2022-41091 / CVE-2022-41049](#) - Security Feature Bypass Vulnerability in Windows Mark of the Web (MOTW)
- [CVE-2022-44698](#) - Security Feature Bypass Vulnerability in Windows SmartScreen
- [CVE-2022-41076](#) - Remote Code Execution Vulnerability (referred as TabShell) in PowerShell
- [CVE-2022-41080 / CVE-2022-41040](#) - Elevation of Privilege Vulnerability in Microsoft Exchange Server
- [CVE-2022-41073](#) - Elevation of Privilege Vulnerability in Microsoft Windows Print Spooler
- [CVE-2022-41125](#) - Elevation of Privilege Vulnerability in Windows CNG Key Isolation Service
- [CVE-2022-41082](#) - Remote Code Execution Vulnerability in the Microsoft Exchange Server
- [CVE-2022-41033](#) - Elevation of Privilege Vulnerability in Windows COM+ Event System Service
- [CVE-2022-41034](#) - Remote Code Execution Vulnerability in Visual Studio Code

### Linux

- [CVE-2022-47939](#) - Remote Code Execution Vulnerability in Linux Kernel ksmbd
- [CVE-2022-32221](#) - Use-After-Free Vulnerability in Curl causing sensitive information disclosure
- [CVE-2022-30123](#) - Sequence Injection Vulnerability in Rack middleware in Ruby
- [CVE-2022-3643](#) - DoS during processing structured packets in Xen netback driver in the Linux kernel
- [CVE-2022-3515](#) - Integer Overflow in Libksba library within the CRL parser allowing Remote Code Execution by passing a malicious S/MIME attachment.
- [CVE-2022-47629](#) - Integer Overflow in Libksba library within the CRL parser
- [CVE-2022-37454](#) - Integer Overflow in Keccak XKCP SHA-3 causing arbitrary code execution or eliminating expected cryptographic properties.
- [CVE-2022-42915](#) - Double free vulnerability in Curl

- [CVE-2022-44640](#) - Invalid Free in the ASN.1 codec in the Heimdal package allows remote attackers to execute arbitrary code.
- [CVE-2022-40664](#): Authentication Bypass Vulnerability in Apache Shiro when forwarding or including via RequestDispatcher.

## macOS

- [CVE-2022-42856](#): A type confusion issue in macOS leading to arbitrary code execution.
- [CVE-2022-46689](#): A race condition issue allowing arbitrary code execution with Kernel privileges.
- [CVE-2022-42821](#): A logic issue in macOS allows to bypass of Gatekeeper checks.
- [CVE-2022-32941](#): A buffer overflow vulnerability that may result in arbitrary code execution.
- [CVE-2022-42842](#): This vulnerability exists in the macOS Kernel allowing kernel code execution and was addressed with improved memory handling
- [CVE-2022-42915](#): A double free error in curl as used in macOS may lead to memory leak and was addressed by updating to curl version 7.86.0
- [CVE-2022-42808](#): An out-of-bounds write issue causing kernel code execution, which was addressed with improved bounds checking.
- [CVE-2022-42813](#): A certificate validation issue present in the handling of WKWebView a maliciously crafted certificate may lead to arbitrary code execution.
- [CVE-2022-32221](#): An error in curl as used in macOS in the logic for reused handle when it is changed from a PUT to a POST request.
- [CVE-2022-42837](#): An issue existed in the parsing of URL which may cause unexpected app termination or arbitrary code execution.

## Windows/macOS/Linux

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

- [CVE-2022-26486](#): Use-after-free in WebGPU IPC Framework as used in Firefox, Firefox ESR, Thunderbird
- [CVE-2022-26485](#): Use-after-free in XSLT parameter processing as used in Firefox, Firefox ESR, Thunderbird
- [CVE-2022-4262](#): Type Confusion in V8 as used in Google Chrome.

## 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, reg.exe, and Schtasks.exe utilities
  - **Linux** - chatr, crontab, Systemctl, rm, and mount utilities
  - **macOS** - Openssl, killall, curl, sqlite, and system\_profiler utilities
- With the number of malware attacks exploiting zero-day vulnerabilities CVE-2022-41040 and CVE-2022-41082 in Microsoft Windows Exchange email servers, organizations must examine the Exchange file structure and look for anomalous .aspx files which could indicate a webshell.
- With increase in ransomware, info-stealers, Banking Trojans and data leaks through phishing attacks carried out on several high-profile victims, protecting your online passwords by following password policies and usage of Multi Factor Authentication (MFA) is recommended to increase overall security posture.

## About Uptycs

Uptycs, the first unified CNAPP and XDR solution, 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, thus delivering a more cohesive enterprise-wide security posture.

Start with your Detection Cloud, Google-like search, and the attack surface coverage you need today. Be ready for what's next.

**Shift up with Uptycs.**