New SysJoker backdoor targets Windows, macOS, and Linux

By Bill Toulas

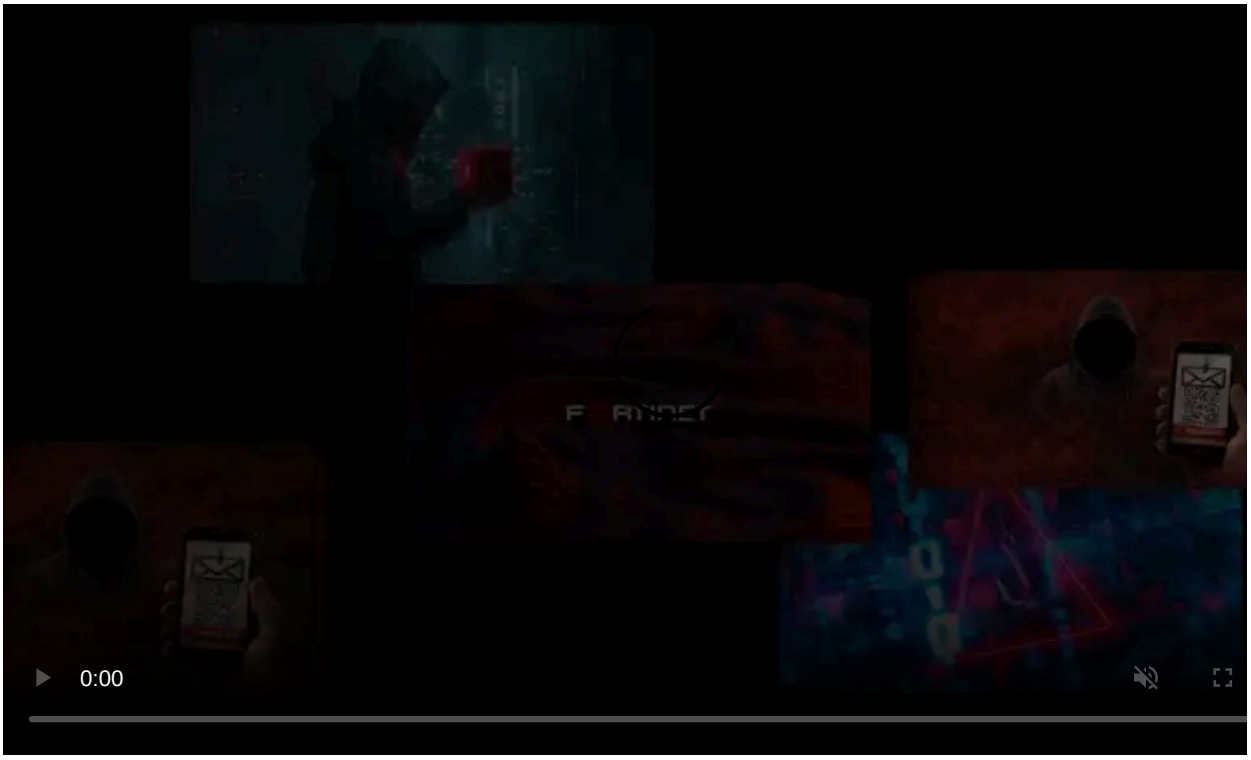
Published: 2022-01-11 · Archived: 2026-04-05 23:04:29 UTC

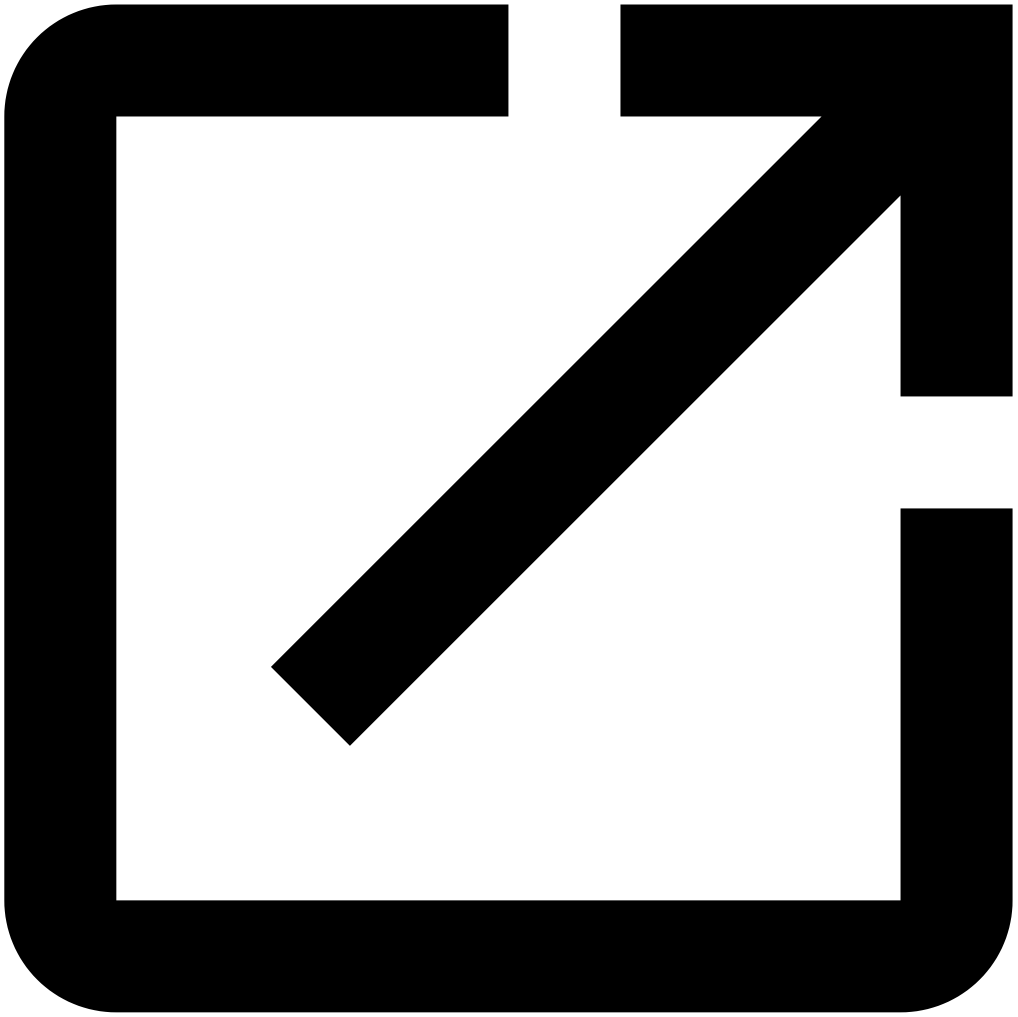
A new multi-platform backdoor malware named 'SysJoker' has emerged in the wild, targeting Windows, Linux, and macOS with the ability to evade detection on all three operating systems.

The discovery of the new malware comes from researchers at Intezer who first saw signs of its activity in December 2021 after investigating an attack on a Linux-based web server.

The first uploads of the malware sample on VirusTotal occurred in H2 2021, which also aligns with the C2 domain registration times.

The security analysts have now published a detailed technical report on SysJoker, which they shared with Bleeping Computer before publication.


0:00



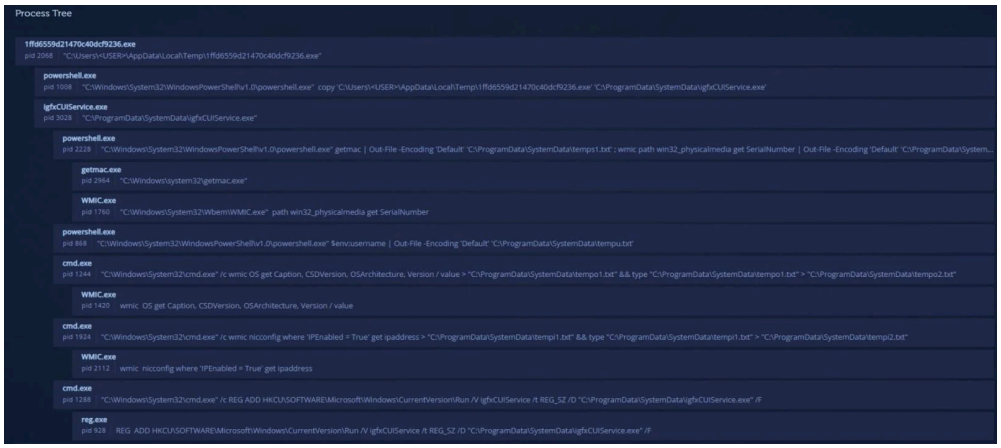
A Joker that doesn't like to draw attention

The malware is written in C++, and while each variant is tailored for the targeted operating system, they are all undetected on VirusTotal, an online malware scanning site that uses 57 different antivirus detection engines.

On Windows, SysJoker employs a first-stage dropper in the form of a DLL, which uses PowerShell commands to do the following:

- fetch the SysJoker ZIP from a GitHub repository,
- unzip it on "C:\ProgramData\RecoverySystem\",
- execute the payload.

The malware then sleeps for up to two minutes before creating a new directory and copies itself as an Intel Graphics Common User Interface Service ("igfxCUIService.exe").



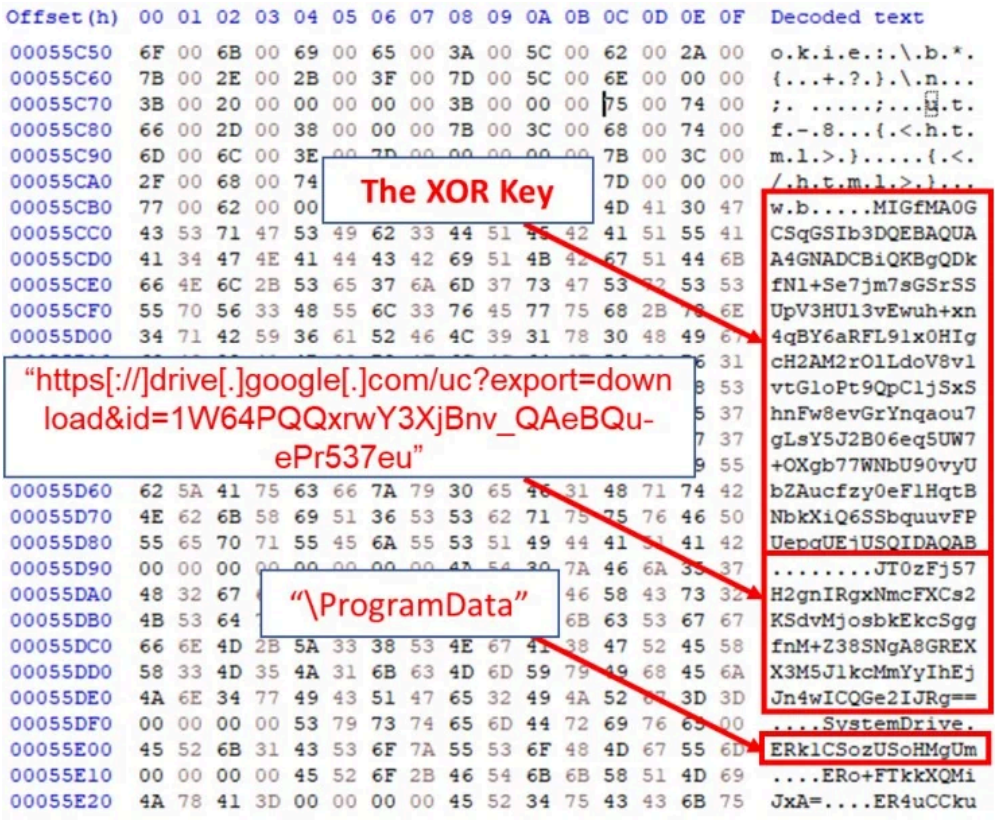
Full execution process for SysJoker on Windows
Source: Intezer

"Next, SysJoker will gather information about the machine using Living off the Land (LOtL) commands. SysJoker uses different temporary text files to log the results of the commands," explains Intezer's report.

"These text files are deleted immediately, stored in a JSON object and then encoded and written to a file named "microsoft_Windows.dll"."

After gathering system and network data, the malware will create persistence by adding a new registry key (HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run). Random sleep times are interposed between all functions leading to this point.

The next step for the malware is to reach out to the actor-controlled C2 server, and for this, it uses a hardcoded Google Drive link.



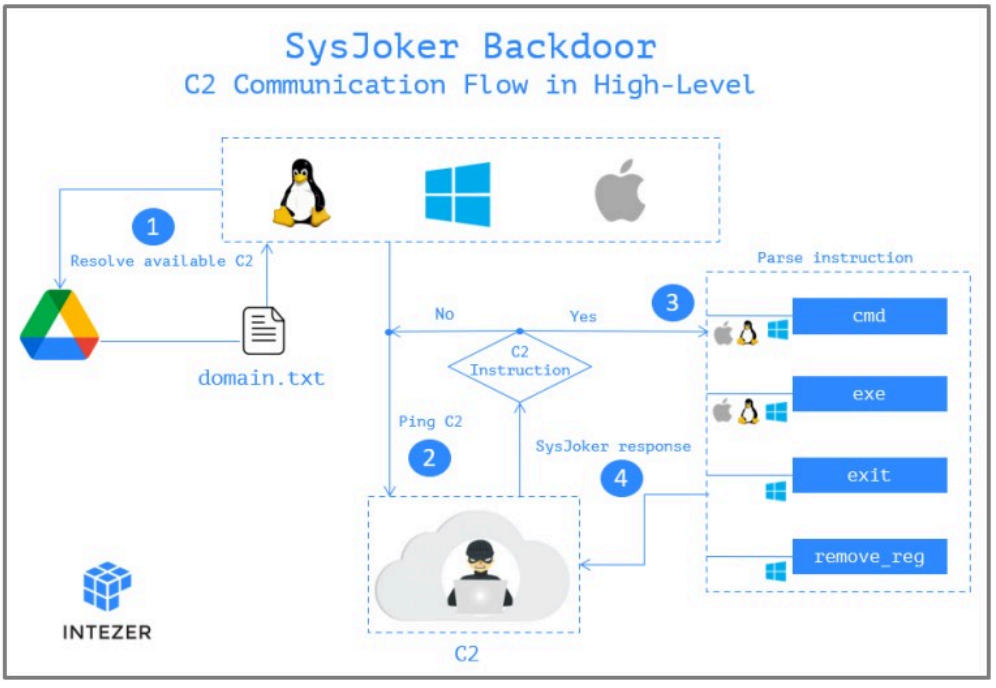
Resolving the hardcoded Google Drive link

Source: Intezer

The link hosts a "domain.txt" file that the actors regularly update to provide available servers to live beacons. This list constantly changes to avoid detection and blocking.

The system information collected in the first stages of the infection is sent as the first handshake to the C2. The C2 replies with a unique token that serves as the identifier of the infected endpoint.

From there, the C2 may instruct the backdoor to install additional malware, run commands on the infected device, or command the backdoor to remove itself from the device. Those last two instructions haven't been implemented yet, though.



SysJoker C2 communications diagram
Source: Intezer

While the Linux and macOS variants do not have a first-stage dropper in the form of a DLL, they ultimately perform the same malicious behavior on the infected device.

Detection and prevention

Intezer has provided full indicators of compromise (IOCs) in their report that admins can use to detect the presence of SysJoker on an infected device.

Below, we have outlined some of the IOCs for each operating system.

On Windows, the malware files are located under the "C:\ProgramData\RecoverySystem" folder, at C:\ProgramData\SystemData\igfxCUIService.exe, and C:\ProgramData\SystemData\microsoft_Windows.dll. For persistence, the malware creates an Autorun "Run" value of "igfxCUIService" that launches the igfxCUIService.exe malware executable.

On Linux, the files and directories are created under "/.Library/" while persistence is established by creating the following cron job: @reboot (/.Library/SystemServices/updateSystem).

On macOS, the files are created on "/Library/" and persistence is achieved via LaunchAgent under the path: /Library/LaunchAgents/com.apple.update.plist.

The C2 domains shared in the Intezer report are the following:

- https[://]bookitlab[.]tech
- https[://]winaudio-tools[.]com
- https[://]graphic-updater[.]com
- https[://]github[.]url-mini[.]com
- https[://]office360-update[.]com
- https[://]drive[.]google[.]com/uc?export=download&id=1-NVty4YX0dPHdxkgMrbdCldQCpCaE-Hn
- https[://]drive[.]google[.]com/uc?export=download&id=1W64PQQxrwY3XjBnv_QaeBQu-ePr537eu

If you found that you have been compromised by SysJoker, follow these three steps:

1. Kill all processes related to the malware and manually delete the files and the relevant persistence mechanism.
2. Run a memory scanner to ensure that all malicious files have been uprooted from the infected system.
3. Investigate the potential entry points, check firewall configurations, and update all software tools to the latest available version.

Source: https://www.bleepingcomputer.com/news/security/new-sysjoker-backdoor-targets-windows-macos-and-linux/