

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.



Visit Advertiser website [GO TO PAGE](#)

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.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text	
00055C50	6F	00	6B	00	69	00	65	00	3A	00	5C	00	62	00	2A	00	o.k.i.e.:.b.*.	
00055C60	7B	00	2E	00	2B	00	3F	00	7D	00	5C	00	6E	00	00	00	{...+?.).\n...	
00055C70	3B	00	2D	00	00	00	00	00	3B	00	00	00	75	00	74	00	;.t.	
00055C80	66	00	2D	00	38	00	00	00	7B	00	3C	00	68	00	74	00	f.-.8...{.<.h.t.	
00055C90	6D	00	6C	00	3E	00	7D	00	00	00	00	00	7B	00	3C	00	m.l.>}.{.<.	
00055CA0	2F	00	68	00	74								7D	00	00	00	/h.t.m.l.>}.	
00055CB0	77	00	62	00	00								4D	41	30	47	w.b....MIGfMA0G	
00055CC0	43	53	71	47	53	49	62	33	44	51	45	42	41	51	55	41	CSqGSiB3DQEBAQUA	
00055CD0	41	34	47	4E	41	44	43	42	69	51	4B	42	67	51	44	6B	A4GNADCBiQKBgQDk	
00055CE0	66	4E	6C	2B	53	65	37	6A	6D	37	73	47	53	62	53	53	fNl+Se7jm7sGSrSS	
00055CF0	55	70	56	33	48	55	6C	33	76	45	77	75	68	2B	78	6E	UpV3HU13vEwuh+xn	
00055D00	34	71	42	59	36	61	52	46	4C	39	31	78	30	48	49	67	4qBY6aRFL91x0HIg	
																	ch2AM2r0lLdoV8v1	
																	vtGloPt9QpCljSxS	
																	hnFw8evGrYnqaou7	
																	gLsY5J2B06eq5UW7	
																	+OXgb77WNbU90vyU	
00055D60	62	5A	41	75	63	66	7A	79	30	65	45	31	48	71	74	42	bZAucfzy0eFlHqtB	
00055D70	4E	62	6B	58	69	51	36	53	53	62	71	75	75	76	46	50	NbkXiQ6SSbquuvFP	
00055D80	55	65	70	71	55	45	6A	55	53	51	49	44	41	51	41	42	UepdUEtUSQIDAQAB	
00055D90	00	00	00	00	00	00	00	00	43	54	30	7A	46	6A	33	37JT0zFj57	
00055DA0	48	32	67										46	58	43	73	32	H2gnIRgxNmcFXCs2
00055DB0	4B	53	64										6B	63	53	67	67	KSdvMjosbkEkcSgg
00055DC0	66	6E	4D	2B	5A	33	38	53	4E	67	41	38	47	52	45	58	fnM+238SNgA8GREX	
00055DD0	58	33	4D	35	4A	31	6B	63	4D	6D	59	79	49	68	45	6A	X3M5J1kcNmYyIhEj	
00055DE0	4A	6E	34	77	49	43	51	47	65	32	49	4A	52	67	3D	3D	Jn4wICQGe2IJRg==	
00055DF0	00	00	00	00	53	79	73	74	65	6D	44	72	69	76	65	00SystemDrive.	
00055E00	45	52	6B	31	43	53	6F	7A	55	53	6F	48	4D	67	55	6D	ERklCSozUSoHMgUm	
00055E10	00	00	00	00	45	52	6F	2B	46	54	6B	6B	58	51	4D	69	...ERo+FTkkXQMi	
00055E20	4A	78	41	3D	00	00	00	45	52	34	75	43	43	6B	75		JxA=....ER4uCCKu	

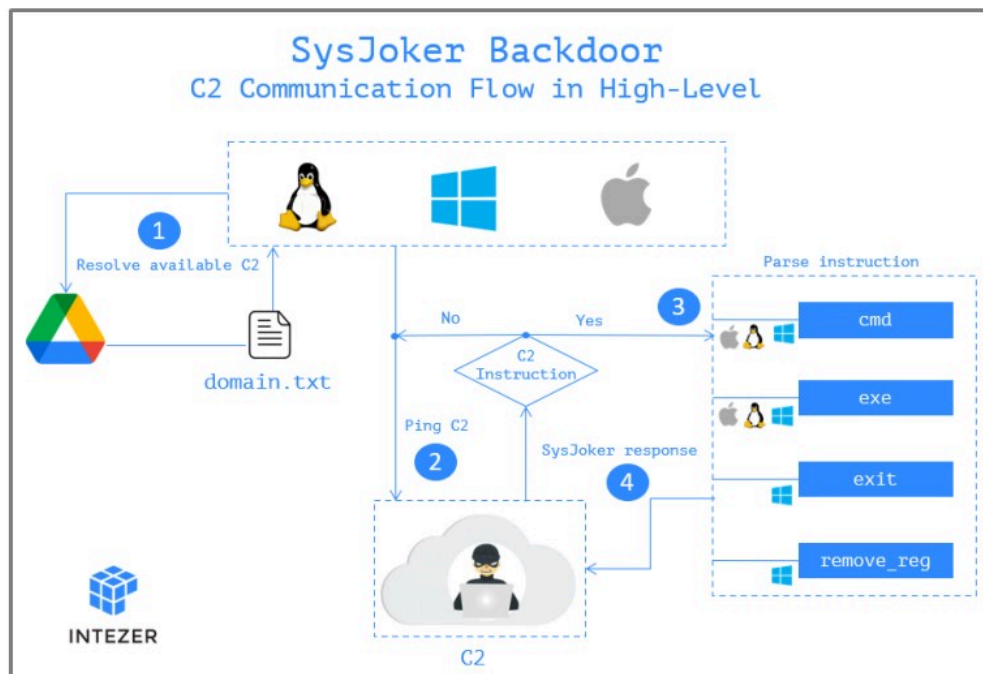
Resolving the hardcoded Google Drive link

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).

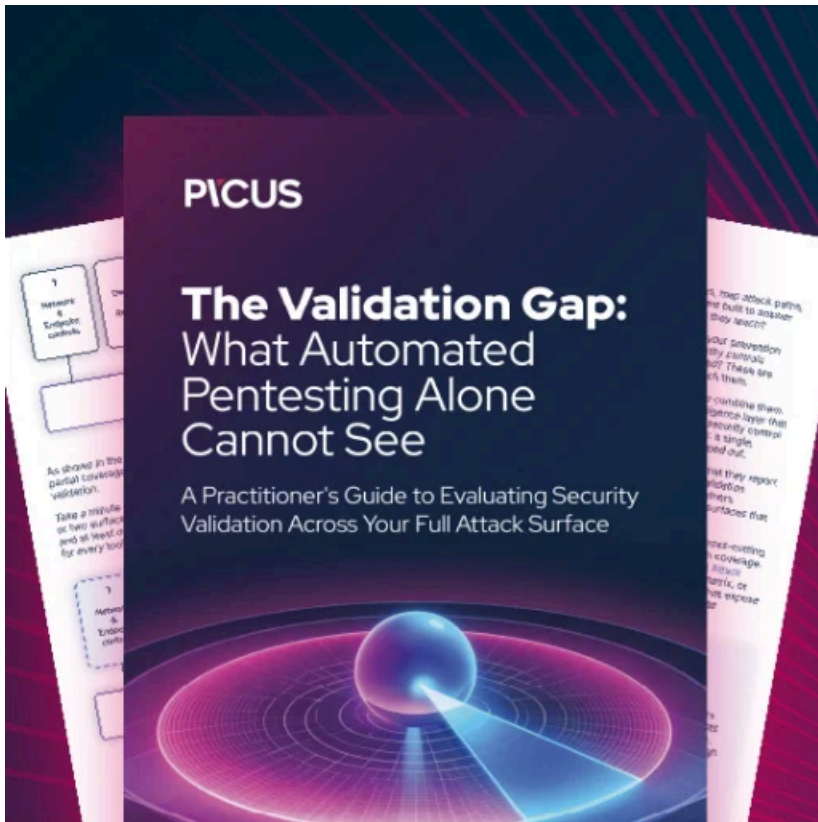
On macOS, the files are created on "/Library/" and persistence is achieved via LaunchAgent under the path: /Library/LaunchAgents/com.apple.update.plist.

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

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



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

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