Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:49:35 UTC

Tool: SysJoker

Names	SysJoker
Category	Malware
Type	Backdoor
Description	(Intezer) In December 2021, we discovered a new multi-platform backdoor that targets Windows, Mac, and Linux. The Linux and Mac versions are fully undetected in VirusTotal. We named this backdoor SysJoker. SysJoker was first discovered during an active attack on a Linux-based web server of a leading educational institution. After further investigation, we found that SysJoker also has Mach-O and Windows PE versions. Based on Command and Control (C2) domain registration and samples found in VirusTotal, we estimate that the SysJoker attack was initiated during the second half of 2021. SysJoker masquerades as a system update and generates its C2 by decoding a string retrieved from a text file hosted on Google Drive. During our analysis the C2 changed three times, indicating the attacker is active and monitoring for infected machines. Based on victimology and malware's behavior, we assess that SysJoker is after specific targets.
Information	<https://intezer.com/blog/research/new-backdoor-sysjoker/> <https://intezer.com/blog/research/wildcard-evolution-of-sysjoker-cyber-threat/> <https://blogs.vmware.com/security/2022/03/%e2%80%afsysjoker-an-analysis-of-a-multi-os-rat.html> <https://research.checkpoint.com/2023/israel-hamas-war-spotlight-shaking-the-rust-off-sysjoker/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.sysjoker> <https://malpedia.caad.fkie.fraunhofer.de/details/osx.sysjoker> <https://malpedia.caad.fkie.fraunhofer.de/details/win.sysjoker>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool SysJoker

Changed	Name	Country	Observed	
APT groups				
	Operation Electric Powder	[Unknown]	2016	
	WildCard	[Unknown]	2021	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7f9085f8-5b43-4620-aec8-6cc4cd7eb108