Sakula RAT - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:59:13 UTC

Tool: Sakula RAT

Names	Sakula RAT Sakula Sakurel VIPER
Category	Malware
Type	Backdoor, Downloader, Exfiltration
Description	(SecureWorks) Sakula uses HTTP GET and POST communication for command and control (C2). Network communication is obfuscated with single-byte XOR encoding. Sakula also leverages single-byte XOR encoding to obfuscate various strings and files embedded in the resource section, which are subsequently used for User Account Control (UAC) bypass on both 32 and 64-bit systems.
Information	<https://www.secureworks.com/research/sakula-malware-family> <https://cyberthreatintelligenceblog.wordpress.com/2018/11/16/c0ld-case-from-aerospace-to-chinas-interests/> <https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016/june/sakula-an-adventure-in-dll-planting/> <https://github.com/nccgroup/Cyber-Defence/tree/master/Technical%20Notes/Sakula>
MITRE ATT&CK	<https://attack.mitre.org/software/S0074/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sakula_rat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Sakula>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Sakula RAT

Changed	Name	Country	Observed

APT groups

	APT 31, Judgment Panda, Zirconium		2016-Mar 2024	
	Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens		2010-Oct 2018	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=60bcd6ad-2ac9-4ca8-82d2-54b200d0b098