Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:31:51 UTC

Tool: SombRAT

Names	SombRAT
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Loader, Tunneling
Description	(BlackBerry) The backdoor delivered by the above-mentioned loaders is a C++ compiled executable developed with heavy usage of objects, classes, and interfaces. It has a plugin architecture and basic functionality of a foothold RAT that is mainly used to download and execute other malicious payloads – either as its own plugins or standalone binaries. It can also perform other simple actions, like collecting system information, listing and killing processes, and uploading files to the C2.
Information	<https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced> <https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0615/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sombrat>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool SombRAT

Changed	Name	Country	Observed	
APT groups				
	CostaRicto	[Unknown]	2017	
	UNC2447	[Unknown]	2020	

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