Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:07:40 UTC

APT group: UNC2447

Names	UNC2447 *(FireEye)*
Country	[Unknown]
Motivation	Financial gain
First seen	2020
Description	(FireEye) Mandiant has observed an aggressive financially motivated group, UNC2447, exploiting one SonicWall VPN zero-day vulnerability prior to a patch being available and deploying sophisticated malware previously reported by other vendors as SOMBRAT. Mandiant has linked the use of SOMBRAT to the deployment of ransomware, which has not been previously reported publicly. UNC2447 monetizes intrusions by extorting their victims first with FIVEHANDS ransomware followed by aggressively applying pressure through threats of media attention and offering victim data for sale on hacker forums. UNC2447 has been observed targeting organizations in Europe and North America and has consistently displayed advanced capabilities to evade detection and minimize post-intrusion forensics.
Observed	Countries: Europe and North America.
Tools used	7-Zip, AdFind, BloodHound, Cobalt Strike, DeathRansom, FIVEHANDS, FOXGRABBER, HELLOKITTY, Mimikatz, PCHUNTER, RagnarLocker, RCLONE, ROUTERSCAN, S3BROWSER, SombRAT, WARPRISM, ZAP.
Information	<https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html>

Last change to this card: 15 May 2021

Download this actor card in PDF or JSON format
