Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:31:24 UTC

Tool: SamSam

Names	SamSam Samas
Category	Malware
Type	Ransomware, Big Game Hunting
Description	(US-CERT) After gaining access to a particular network, the SamSam actors escalate privileges for administrator rights, drop malware onto the server, and run an executable file, all without victims' action or authorization. While many ransomware campaigns rely on a victim completing an action, such as opening an email or visiting a compromised website, RDP allows cyber actors to infect victims with minimal detection.
Information	<https://www.us-cert.gov/ncas/alerts/AA18-337A> <https://blog.malwarebytes.com/threat-analysis/2018/06/samsam-ransomware-controlled-distribution/> <http://blog.talosintel.com/2016/03/samsam-ransomware.html> <https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/samsam-ransomware-chooses-its-targets-carefully-wpna.aspx> <https://www.crowdstrike.com/blog/an-in-depth-analysis-of-samsam-ransomware-and-boss-spider/> <https://nakedsecurity.sophos.com/2018/05/01/samsam-ransomware-a-mean-old-dog-with-a-nasty-new-trick-report/> <http://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0370/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.samsam>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:samsam>

Last change to this tool card: 13 July 2020

Download this tool card in JSON format

All groups using tool SamSam

Changed	Name	Country	Observed	
APT groups				
	Boss Spider, Gold Lowell		2015-Nov 2018	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=bd75f106-8065-4882-b343-73e924e16c99