Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:01:24 UTC

Tool: ObliqueRAT

Names	ObliqueRAT Oblique RAT
Category	Malware
Type	Reconnaissance, Backdoor, Dropper, Exfiltration
Description	(Talos) Cisco Talos has recently discovered a new campaign distributing a malicious remote access trojan (RAT) family we're calling 'ObliqueRAT.' Cisco Talos also discovered a link between ObliqueRAT and another campaign from December 2019 distributing Crimson RAT sharing similar maldocs and macros. CrimsonRAT has been known to target diplomatic and government organizations in Southeast Asia.
Information	<https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf> <https://securelist.com/transparent-tribe-part-2/98233/> <https://www.secrss.com/articles/24995> <https://blog.talosintelligence.com/2020/02/obliquerat-hits-victims-via-maldocs.html> <https://blog.talosintelligence.com/2021/02/obliquerat-new-campaign.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0644/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.oblique_rat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:obliquerat>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool ObliqueRAT

Changed	Name	Country	Observed
APT groups			

	Transparent Tribe, APT 36		2013-Mar 2025	

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