Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:21:20 UTC

Tool: Downeks

Names	Downeks
Category	Malware
Type	Downloader
Description	(Palo Alto) The initial infection vector in this attack is not clear, but it results in installing the “Downeks” downloader, which in turn infects the victim computer with the “QuasarRAT”. Downeks uses third party websites to determine the external IP of the victim machine, possibly to determine victim location with GeoIP. It also drops decoy documents in an attempt to camouflage the attack.
Information	<https://unit42.paloaltonetworks.com/unit42-downeks-and-quasar-rat-used-in-recent-targeted-attacks-against-governments/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.downeks>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Downeks>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Downeks

Changed	Name	Country	Observed	
APT groups				
	Molerats, Extreme Jackal, Gaza Cybergang	[Gaza]	2012-Jul 2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=16b197ca-adb0-46c1-a237-f48442021c0b