Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:43:51 UTC

Tool: JhoneRAT

Names	JhoneRAT
Category	Malware
Type	Reconnaissance, Backdoor, Downloader, Dropper
Description	(Talos) Today, Cisco Talos is unveiling the details of a new RAT we have identified we're calling 'JhoneRAT.' This new RAT is dropped to the victims via malicious Microsoft Office documents. The dropper, along with the Python RAT, attempts to gather information on the victim's machine and then uses multiple cloud services: Google Drive, Twitter, ImgBB and Google Forms. The RAT attempts to download additional payloads and upload the information gathered during the reconnaissance phase. This particular RAT attempts to target a very specific set of Arabic-speaking countries. The filtering is performed by checking the keyboard layout of the infected systems.
Information	<https://blog.talosintelligence.com/2020/01/jhonerat.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.jhone_rat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:JhoneRAT>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool JhoneRAT

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

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