Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:19:44 UTC

Tool: Pyark

Names	Pyark
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Qihoo 360) The APT-C-43 organization is good at launching attacks using phishing emails, and deploys the backdoor program Pyark (Machete) written in python after invading the victim's machine. The network communication mainly relies on FTP and HTTP protocols. After successfully infiltrating the target machine, APT-C-43 organization monitors the target users, steal sensitive data, etc.
Information	<https://blog.360totalsecurity.com/en/apt-c-43-steals-venezuelan-military-secrets-to-provide-intelligence-support-for-the-reactionaries-hpreact-campaign/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0409>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/py.pyark>

Last change to this tool card: 06 September 2023

Download this tool card in JSON format

All groups using tool Pyark

Changed	Name	Country	Observed	
APT groups				
	El Machete	[Unknown]	2010-Mar 2022	

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