Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:00:16 UTC

Tool: ROCK

Names	ROCK yellowalbatross
Category	Malware
Type	Backdoor, Info stealer, Credential stealer
Description	(Qihoo 360) ROCK Trojan plays a main role in the Sphinx attacks. This malware family was developed by the attackers themselves or was customer-made by a third party group. The malware impersonated Word documents, images or installation programs in the attempt to disguise itself as PDF files, pictures or Flash installers to induce the users to click. The main purpose is to steal sensitive information from the victims, such as system information, account & password and search history saved in the browser. It also monitors victims through Skype chatting history, cameras, microphones and keyboard & mouse logging. The information collected will then be encrypted and passed back to specific C2 servers.
Information	<https://docplayer.net/83717233-Sphinx-apt-c-15-targeted-cyber-attack-in-the-middle-east-table-of-contents.html> <https://github.com/securitykitten/malware_references/blob/master/rmshixdAPT-C-15-20160630.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.rock>

Last change to this tool card: 21 May 2020

Download this tool card in JSON format

All groups using tool ROCK

Changed	Name	Country	Observed
APT groups			

	Sphinx	[Unknown]	2014	

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