Remote CMD/PowerShell terminal - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:51:51 UTC

Tool: Remote CMD/PowerShell terminal

Names	Remote CMD/PowerShell terminal
Category	Malware
Type	Reconnaissance, Backdoor
Description	(Kaspersky) The malware was first seen packed with VMProtect; when unpacked the sample didn't show any similarities with previously known malware. All the strings and settings were encrypted and obfuscated. Functionality was identified that enables HTTP communication with the C&C server and invokes "processcreate" based on parameters received as a response. The configuration and strings are encrypted using 3DES and Base64 encoding. Data sent to the C&C server is also encrypted using 3DES and Base64. Different keys are used for local and network encryption. The malware starts communicating with the C&C server by sending basic information about the infected machine. The C&C server then replies with the encrypted serialized configuration. The malware basically provides a remote CMD/PowerShell terminal for the attackers, enabling them to execute scripts/commands and receive the results via HTTP requests.
Information	<https://securelist.com/operation-parliament-who-is-doing-what/85237/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Remote CMD/PowerShell terminal

Changed	Name	Country	Observed
APT groups			

	Operation Parliament	[Unknown]	2017	

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