Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:04:41 UTC

Tool: PowerExchange

Names	PowerExchange
Category	Malware
Type	Backdoor
Description	(Symantec) PowerShell-based malware that can log into an Exchange Server with hardcoded credentials and monitor for emails sent by the attackers. It uses an Exchange Server as a C&C. Mails received with '@@' in the subject contain commands sent from the attackers which allows them to execute arbitrary PowerShell commands, write files and steal files. The malware creates an Exchange rule (called ‘defaultexchangerules’) to filter these messages and move them to the Deleted Items folder automatically.
Information	<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/crambus-middle-east-government>
MITRE ATT&CK	<https://attack.mitre.org/software/S1173>

Last change to this tool card: 28 June 2025

Download this tool card in JSON format

All groups using tool PowerExchange

Changed	Name	Country	Observed	
APT groups				
	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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