Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:49:16 UTC

Tool: CORALDECK

Names	CORALDECK
Category	Malware
Type	Exfiltration, Dropper
Description	(FireEye) CORALDECK is an exfiltration tool that searches for specified files and exfiltrates them in password protected archives using hardcoded HTTP POST headers. CORALDECK has been observed dropping and using Winrar to exfiltrate data in password protected RAR files as well as WinImage and zip archives.
Information	<https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0212/>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool CORALDECK

Changed	Name	Country	Observed	
APT groups				
	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

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