Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:34:37 UTC

Tool: WARPWIRE

Names	WARPWIRE
Category	Malware
Type	Credential stealer
Description	(Mandiant) WARPWIRE is a credential harvester written in Javascript that is embedded into a legitimate Connect Secure file. WARPWIRE targets plaintext passwords and usernames which are submitted via a HTTP GET request to a command and control (C2) server. WARPWIRE captures credentials submitted during the web logon to access layer 7 applications, like RDP. Captured credentials are Base64-encoded with btoa() before they are submitted to the C2 via a HTTP GET request.
Information	<https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day>
MITRE ATT&CK	<https://attack.mitre.org/software/S1116>

Last change to this tool card: 19 June 2024

Download this tool card in JSON format

All groups using tool WARPWIRE

Changed	Name	Country	Observed	
APT groups				
	UNC5221, UTA0178		2022-Mar 2025	

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