Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:10:33 UTC

Tool: WHEATSCAN

Names	WHEATSCAN
Category	Malware
Type	Vulnerability scanner
Description	(FireEye) After gaining initial access, the operators conduct credential harvesting and extensive internal network reconnaissance. This includes running native Windows commands on compromised servers, executing AdFind on the Active Directory, and scanning the internal network with numerous publicly available tools and a non-public scanner we named WHEATSCAN. The operators made a consistent effort to delete these tools and remove any residual forensic artifacts from compromised systems.
Information	<https://www.fireeye.com/blog/threat-research/2021/08/unc215-chinese-espionage-campaign-in-israel.html>

Last change to this tool card: 01 November 2021

Download this tool card in JSON format

All groups using tool WHEATSCAN

Changed	Name	Country	Observed	
APT groups				
	UNC215		2019	

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