Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:56:52 UTC

Tool: BLINDINGCAN

Names	BLINDINGCAN DRATzarus RAT AIRDRY ZetaNile
Category	Malware
Type	Reconnaissance, Backdoor, Dropper, Loader, Downloader
Description	(US-CERT) Working with U.S. Government partners, DHS and FBI identified Remote Access Trojan (RAT) malware variants used by the North Korean government. This malware variant has been identified as BLINDINGCAN. --Begin built-in functions-- Retrieve information about all installed disks, including the disk type and the amount of free space on the disk Create, start, and terminate a new process and its primary thread Search, read, write, move, and execute files Get and modify file or directory timestamps Change the current directory for a process or file Delete malware and artifacts associated with the malware from the infected system --End built-in functions--
Information	<https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a> <https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf> <https://www.hvs-consulting.de/media/downloads/ThreatReport-Lazarus.pdf> <https://www.sentinelone.com/blog/the-blindingcan-rat-and-malicious-north-korean-activity/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0520/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.blindingcan>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool BLINDINGCAN

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=5a84e5db-d28b-43f4-9bde-49b2bdbdc100