Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:49:33 UTC

Tool: ThreatNeedle

Names	ThreatNeedle DRATzarus
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Downloader
Description	(Kaspersky) Upon opening a malicious document and allowing the macro, the malware is dropped and proceeds to a multistage deployment procedure. The malware used in this campaign belongs to a known malware cluster we named ThreatNeedle. We attribute this malware family to the advanced version of Manuscrypt (a.k.a. NukeSped), a family belonging to the Lazarus group. We previously observed the Lazarus group utilizing this cluster when attacking cryptocurrency businesses and a mobile game company. Although the malware involved and the entire infection process is known and has not changed dramatically compared to previous findings, the Lazarus group continued using ThreatNeedle malware aggressively in this campaign.
Information	<https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Lazarus-targets-defense-industry-with-Threatneedle-En.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0665/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.dratzarus>

Last change to this tool card: 13 October 2023

Download this tool card in JSON format

All groups using tool ThreatNeedle

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=ee9fefb9-5621-47c4-b035-26aa2f936ad9