Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:42:42 UTC

Tool: KEYMARBLE

Names	KEYMARBLE
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Downloader, Exfiltration
Description	(US-CERT) This malware report contains analysis of one 32-bit Windows executable file, identified as a Remote Access Trojan (RAT). This malware is capable of accessing device configuration data, downloading additional files, executing commands, modifying the registry, capturing screen shots, and exfiltrating data.
Information	<https://www.us-cert.gov/ncas/analysis-reports/AR18-221A> <https://research.checkpoint.com/north-korea-turns-against-russian-targets/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0271/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.keymarble>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:keymarble>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool KEYMARBLE

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=7448c327-ddcc-4319-9bb3-8c4c2b3cf34b