Threat Group Cards: A Threat Actor Encyclopedia

Tool: TAINTEDSCRIBE

Names	TAINTEDSCRIBE
Category	Malware
Type	Backdoor
Description	(US-CERT) Working with U.S. Government partners, DHS, FBI, and DoD identified Trojan malware variants used by the North Korean government. This malware variant has been identified as TAINTEDSCRIBE.
Information	<https://www.us-cert.gov/ncas/analysis-reports/ar20-133b> <https://blog.reversinglabs.com/blog/hidden-cobra>
MITRE ATT&CK	<https://attack.mitre.org/software/S0586/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.taintedscribe>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool TAINTEDSCRIBE

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

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