Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:26:55 UTC

Tool: HARDRAIN

Names	HARDRAIN
Category	Malware
Type	Backdoor, Tunneling
Description	(US-CERT) This report provides analysis of three (3) malicious executable files. The first two (2) files are 32-bit Windows executables that function as Proxy servers and implement a 'Fake TLS' method similar to the behavior described in a previously published NCCIC report, MAR-10135536-B. The third file is an Executable Linkable Format (ELF) file designed to run on Android platforms as a fully functioning Remote Access Tool (RAT).
Information	<https://www.us-cert.gov/sites/default/files/publications/MAR-10135536-F.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0246/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.hardrain> <https://malpedia.caad.fkie.fraunhofer.de/details/win.hardrain>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:HARDRAIN>

Last change to this tool card: 22 April 2020

Download this tool card in JSON format

All groups using tool HARDRAIN

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

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