Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:06:18 UTC

Tool: REPTILE

Names	REPTILE
Category	Malware
Type	Backdoor
Description	(Mandiant) To achieve persistent access on the FortiManager device, the threat actor deployed a backdoor with the filename /bin/klogd (MD5: 53a69adac914808eced2bf8155a7512d) that Mandiant refers to as REPTILE, a variant of a publicly available Linux kernel module (LKM) rootkit. With the assistance of TABLEFLIP, the threat actor was able to successfully forward traffic and access the REPTILE backdoor using iptables traffic redirection rules. Once executed, REPTILE created a packet socket to receive OSI layer 2 packets. When a packet was received, the backdoor would perform the check seen in the pseudocode in Figure 20 to determine if a magic string was present.
Information	<https://cloud.google.com/blog/topics/threat-intelligence/fortinet-malware-ecosystem/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.reptile>

Last change to this tool card: 27 August 2024

Download this tool card in JSON format

All groups using tool REPTILE

Changed	Name	Country	Observed	
APT groups				
	UNC3886		2021-Early 2025	

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