Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:17:16 UTC

Tool: BIFROST

Names	BIFROST elf.bifrose
Category	Malware
Type	Backdoor, Keylogger, Info stealer
Description	(Talos) Bifrost is a backdoor with more than 10 variants. Bifrost uses the typical server, server builder, and client backdoor program configuration to allow a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. Bifrost contains standard RAT features including a file manager, screen capture utility, keylogging, video recording, microphone and camera monitoring, and a process manager. In order to mark its presence in the system, Bifrost uses a mutex that may be named 'Bif1234,' or 'Tr0gBot.'
Information	<https://blog.talosintelligence.com/2019/03/threat-roundup-for-feb-22-to-march-1.html> <https://teamt5.org/tw/posts/technical-analysis-on-backdoor-bifrost-of-the-Chinese-apt-group-huapi/> <https://unit42.paloaltonetworks.com/new-linux-variant-bifrost-malware/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.bifrost>

Last change to this tool card: 07 March 2024

Download this tool card in JSON format

All groups using tool BIFROST

Changed	Name	Country	Observed	
APT groups				
	BlackTech, Circuit Panda, Radio Panda		2010-Oct 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=de095ac7-5aa3-41b1-8ea2-18ef7160715c