Bifrost (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:35:55 UTC

Bifrost

aka: elf.bifrose

Actor(s): BlackTech

Linux version of the bifrose malware that originally targeted Windows platform only. The backdoor has the ability to perform file management, start or end a process, or start a remote shell. The connection is encrypted using a modified RC4 algorithm.

References

Yara Rules

▶ [TLP:WHITE] elf_bifrost_w0 (20210331 | HUAPI UNIX BiFrost RAT)

Download all Yara Rules
