RedXOR (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 02:12:38 UTC

RedXOR

RedXOR is a sophisticated backdoor targeting Linux systems disguised as polkit daemon and utilizing network data encoding based on XOR. Believed to be developed by Chinese nation-state actors, this malware shows similarities to other malware associated with the Winnti umbrella threat group.

RedXOR uses various techniques such as open-source LKM rootkits, Python pty shell, and network data encoding with XOR. It also employs persistence methods and communication with a Command and Control server over HTTP.

The malware can execute various commands including system information collection, updates, shell commands, and network tunneling.

References

There is no Yara-Signature yet.
