POWERPLANT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:18:33 UTC

ps1.powerplant (Back to overview)

POWERPLANT

Actor(s): FIN7

This powershell code is a PowerShell written backdoor used by FIN7. Regarding to Mandiant that is was revealed to be a "vast backdoor framework with a breadth of capabilities, depending on which modules are delivered from the C2 server."

References

There is no Yara-Signature yet.
