COZYDUKE (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:47:36 UTC

COZYDUKE

aka: CozyCar, Cozer, CozyBear, EuroAPT

Actor(s): APT29

CozyDuke is not simply a malware toolset; rather, it is a modular malware platform formed around a core backdoor component. This component can be instructed by the C&C server to download and execute arbitrary modules, and it is these modules that provide CozyDuke with its vast array of functionality. Known CozyDuke modules include:

- Command execution module for executing arbitrary Windows Command Prompt commands
- Password stealer module
- NT LAN Manager (NTLM) hash stealer module
- System information gathering module
- Screenshot module

References

There is no Yara-Signature yet.
