Agent Racoon (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:29:42 UTC

Agent Racoon

Agent Racoon is a .NET-based backdoor malware that leverages DNS for covert C2 communication, employing randomized subdomains and Punycode encoding to evade detection. It features encrypted communication using a unique key per sample, supports remote command execution, and facilitates file transfers. Despite lacking an inherent persistence mechanism, it relies on external methods like scheduled tasks for execution. The malware, active since at least 2020, has targeted organizations in the U.S., Middle East, and Africa, including non-profits and government sectors. It disguises itself as legitimate binaries such as Google Update and MS OneDrive Updater, using obfuscation techniques like Base64 encoding and timestamp modifications to avoid detection.

References

There is no Yara-Signature yet.