BLACKCOFFEE (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:07:03 UTC

a backdoor that obfuscates its communications as normal traffic to legitimate websites such as Github and Microsoft's Technet portal.

▶ [TLP:WHITE] win_blackcoffee_auto (20251219 | Detects win.blackcoffee.)
