QUICKCAFE (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:51:09 UTC

js.quickcafe (Back to overview)

QUICKCAFE

Actor(s): Lazarus Group

QUICKCAFE is an encrypted JavaScript downloader for QUICKRIDE.POWER that exploits the ActiveX M2Soft vulnerabilities. QUICKCAFE is obfuscated using JavaScript Obfuscator.

References

2017-12-19 · Proofpoint · Darien Huss
North Korea Bitten by Bitcoin Bug
QUICKCAFE PowerSpritz Ghost RAT PowerRatankba

There is no Yara-Signature yet.
