BLINDTOAD (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:35:45 UTC

win.blindtoad (Back to overview)

BLINDTOAD

Actor(s): Lazarus Group

BLINDTOAD is 64-bit Service DLL that loads an encrypted file from disk and executes it in memory.

References

2020-05-04 · ADEO DFIR · ADEO DFIR
APT38 Lazarus Threat Analysis Report
BLINDTOAD ELECTRICFISH

2018-11-20 · Trend Micro · Joelson Soares, Lenart Bermejo
Lazarus Continues Heists, Mounts Attacks on Financial Organizations in Latin America
BLINDTOAD

2018-01-01 · FireEye · FireEye
APT38
Bitsran BLINDTOAD BOOTWRECK Contopee DarkComet DYEPACK HOTWAX NESTEGG PowerRatankba REDSHAWL WORMHOLE Lazarus Group

2017-10-16 · BAE Systems · Hirman Muhammad bin Abu Bakar, James Wong, Sergei Shevchenko
Taiwan Heist: Lazarus Tools and Ransomware
BLINDTOAD Lazarus Group

There is no Yara-Signature yet.
