VenomLNK (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:12:14 UTC

win.venom_lnk (Back to overview)

VenomLNK

VenomLNK is the initial phase of the more_eggs malware-as-a-service. It is a poisoned .lnk file that depends on User Execution and points to LOLBINs (often cmd.exe) with additional obfuscated scripting options. This typically initiates WMI abuse and TerraLoader, which can load additional functionality through various plugins.

References

2023-01-24 · eSentire · Joe Stewart, Keegan Keplinger
Unmasking Venom Spider
More_eggs TerraPreter TerraLoader VenomLNK

2022-04-21 · eSentire · eSentire Threat Response Unit (TRU)
Hackers Spearphish Corporate Hiring Managers with Poisoned Resumes, Infecting Them with the More_Eggs Malware, Warns eSentire
More_eggs TerraLoader VenomLNK

2021-04-05 · eSentire · eSentire
Hackers Spearphish Professionals on LinkedIn with Fake Job Offers, Infecting them with Malware, Warns eSentire
More_eggs TerraPreter TerraLoader VenomLNK

2020-07-20 · QuoIntelligence
Golden Chickens: Evolution Oof the MaaS
More_eggs TerraLoader TerraStealer VenomLNK

2020-01-27 · QuoScient · QuoScient
The Chicken Keeps Laying New Eggs: Uncovering New GC MaaS Tools Used By Top-tier Threat Actors
TerraRecon TerraStealer TerraTV VenomLNK

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.venom_lnk