EVILNUM (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 12:54:57 UTC

js.evilnum (Back to overview)

EVILNUM

According proofpoint, EvilNum is a backdoor that can be used for data theft or to load additional payloads. The malware includes multiple interesting components to evade detection and modify infection paths based on identified antivirus software.

References

2022-06-27 · Zscaler · Sahil Antil, Sudeep Singh
Return of the Evilnum APT with updated TTPs and new targets
EVILNUM EVILNUM

2021-01-04 · · NSFOCUS · NSFOCUS
Steganography, Little Fire Dragon and AGENTVX: A Detailed Analysis of APT Organization EVILNUM's New Attack Activities
EVILNUM

2020-11-03 · Kaspersky Labs · GReAT
APT trends report Q3 2020
WellMail EVILNUM Janicab Poet RAT AsyncRAT Ave Maria Cobalt Strike Crimson RAT CROSSWALK Dtrack LODEINFO MoriAgent Okrum PlugX POISONPLUG Rover ShadowPad SoreFang Winnti

2020-08-24 · Kaspersky Labs · Ivan Kwiatkowski, Maher Yamout, Pierre Delcher
Lifting the veil on DeathStalker, a mercenary triumvirate
EVILNUM Janicab Evilnum

2020-07-10 · Github (eset) · Matías Porolli
Evilnum — Indicators of Compromise
EVILNUM More_eggs EVILNUM TerraStealer

2020-07-09 · ESET Research · Matías Porolli
More evil: A deep look at Evilnum and its toolset

EVILNUM More_eggs EVILNUM TerraPreter TerraStealer TerraTV Evilnum

2020-06-04 · · Chianxin Virus Response Center

脚本系贼寇之风兴起，买卖体系堪比勒索软件

EVILNUM More_eggs

2020-05-06 · Prevailion · Danny Adamitis

Phantom in the Command Shell

EVILNUM

2019-08-01 · ClearSky · ClearSky Cyber Security

2019 H1 Cyber Events Summary Report

EVILNUM Cardinal RAT SappyCache

2019-03-19 · Palo Alto Networks Unit 42 · Josh Grunzweig, Tom Lancaster

Cardinal RAT Sins Again, Targets Israeli Fin-Tech Firms

EVILNUM Cardinal RAT EVILNUM

2018-05-24 · pwncode.io blog · c0d3inj3cT

JavaScript based Bot using Github C&C

EVILNUM

There is no Yara-Signature yet.

Source: https://malpedia.caad.fkie.fraunhofer.de/details/js.evilnum