EnvyScout (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 02:50:33 UTC

win.envyscout (Back to overview)

EnvyScout

aka: ROOTSAW

There is no description at this point.

References

2023-09-22 · Mandiant · Dan Black, Josh Atkins, Luke Jenkins
Backchannel Diplomacy: APT29’s Rapidly Evolving Diplomatic Phishing Operations
Brute Ratel C4 Cobalt Strike EnvyScout GraphDrop QUARTERRIG sRDI Unidentified 107 (APT29)

2023-04-13 · · CERT.PL · CERT.PL
CERT Polska and SKW warn against the activities of Russian spies
BOOMBOX EnvyScout SUNBURST

2023-03-14 · Blackberry · BlackBerry Research & Intelligence Team
NOBELIUM Uses Poland's Ambassador’s Visit to the U.S. to Target EU Governments Assisting Ukraine
EnvyScout GraphicalNeutrino

2023-03-10 · Mrtiepolo · Gianluca Tiepolo
Sophisticated APT29 Campaign Abuses Notion API to Target the European Commission
BEATDROP EnvyScout GraphicalNeutrino tDiscoverer VaporRage

2022-09-06 · · INCIBE-CERT · INCIBE
Estudio del análisis de Nobelium
BEATDROP BOOMBOX Cobalt Strike EnvyScout Unidentified 099 (APT29 Dropbox Loader) VaporRage

2022-07-19 · Palo Alto Networks Unit 42 · Mike Harbison, Peter Renals
Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive
Cobalt Strike EnvyScout Gdrive

2022-07-08 · · Cert-AgID · Cert-AgID
Il malware EnvyScout (APT29) è stato veicolato anche in Italia
EnvyScout Unidentified 098 (APT29 Slack Downloader)

2022-06-26 · BushidoToken

Overview of Russian GRU and SVR Cyberespionage Campaigns 1H 2022

Cobalt Strike CredoMap EnvyScout

2022-05-03 · Recorded Future · Insikt Group®

SOLARDEFLECTION C2 Infrastructure Used by NOBELIUM in Company Brand Misuse

Cobalt Strike EnvyScout

2022-01-06 · Sekoia · sekoia

NOBELIUM’s EnvyScout infection chain goes in the registry, targeting embassies

Cobalt Strike EnvyScout

There is no Yara-Signature yet.
