Meterpreter (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:59:45 UTC

There is no description at this point.

2025-09-04 · Seqrite · Sathwik Ram Prakki, Subhajeet Singha
Operation BarrelFire: NoisyBear targets entities linked to Kazakhstan’s Oil & Gas Sector.
Meterpreter 2025-03-20 · Cisco Talos · Asheer Malhotra, Brandon White, Jungsoo An, Vitor Ventura
UAT-5918 targets critical infrastructure entities in Taiwan
ShortLeash LaZagne JuicyPotato Meterpreter MimiKatz ShortLeash UAT-5918 2024-01-12 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update Q4 2023
FluBot Hook FAKEUPDATES AsyncRAT BianLian Cobalt Strike DCRat Havoc IcedID Lumma Stealer Meterpreter NjRAT Pikabot QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver
2023-09-07 · CISA · CISA
Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475
Meterpreter MimiKatz 2023-08-22 · AhnLab · Sanseo
Analysis of APT Attack Cases Targeting Web Services of Korean Corporations
Ladon Meterpreter MimiKatz Dalbit 2023-06-08 · VMRay · Patrick Staubmann
Busy Bees - The Transformation of BumbleBee
BumbleBee Cobalt Strike Conti Meterpreter Sliver 2023-05-22 · AhnLab · ASEC
Kimsuky Group Using Meterpreter to Attack Web Servers
Kimsuky Meterpreter 2023-04-24 · Kaspersky Labs · Ivan Kwiatkowski, Pierre Delcher
Tomiris called, they want their Turla malware back
KopiLuwak Andromeda Ave Maria GoldMax JLORAT Kazuar Meterpreter QUIETCANARY RATel Roopy Telemiris tomiris Topinambour Storm-0473 2023-04-18 · Mandiant · Mandiant
M-Trends 2023
QUIETEXIT AppleJeus Black Basta BlackCat CaddyWiper Cobalt Strike Dharma HermeticWiper Hive INDUSTROYER2 Ladon LockBit Meterpreter PartyTicket PlugX QakBot REvil Royal Ransom SystemBC WhisperGate 2022-10-03 · Check Point · Marc Salinas Fernandez
Bumblebee: increasing its capacity and evolving its TTPs
BumbleBee Cobalt Strike Meterpreter Sliver Vidar 2022-09-26 · The DFIR Report · The DFIR Report
BumbleBee: Round Two
BumbleBee Cobalt Strike Meterpreter 2022-09-14 · Cybereason · Derrick Masters, Loïc Castel
THREAT ANALYSIS REPORT: Abusing Notepad++ Plugins for Evasion and Persistence
Meterpreter 2022-09-06 · AT&T · Ofer Caspi
Shikitega - New stealthy malware targeting Linux
BotenaGo EnemyBot Meterpreter Monero Miner 2022-09-06 · Check Point · Check Point Research
DangerousSavanna: Two-year long campaign targets financial institutions in French-speaking Africa

AsyncRAT Meterpreter PoshC2 DangerousSavanna 2022-09-01 · Medium michaelkoczwara · Michael Koczwara

Hunting C2/Adversaries Infrastructure with Shodan and Censys

Brute Ratel C4 Cobalt Strike Deimos GRUNT IcedID Merlin Meterpreter Nighthawk PoshC2 Sliver 2022-08-30 · Proofpoint · Michael Raggi, PWC UK, Sveva Vittoria Scenarelli

Rising Tide: Chasing the Currents of Espionage in the South China Sea

scanbox Meterpreter APT40 2022-08-18 · Sophos · Sean Gallagher

Cookie stealing: the new perimeter bypass

Cobalt Strike Meterpreter MimiKatz Phoenix Keylogger Quasar RAT 2022-07-18 · Palo Alto Networks Unit 42 · Unit 42

Obscure Serpens

Cobalt Strike Empire Downloader Meterpreter MimiKatz DarkHydrus 2022-07-07 · IBM · Charlotte Hammond, Kat Weinberger, Ole Villadsen

Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine

AnchorMail BumbleBee Cobalt Strike IcedID Meterpreter 2022-06-01 · Elastic · Andrew Pease, Daniel Stepanic, Derek Ditch, Salim Bitam, Seth Goodwin

CUBA Ransomware Campaign Analysis

Cobalt Strike Cuba Meterpreter MimiKatz SystemBC 2022-05-05 · Cisco Talos · Aliza Berk, Asheer Malhotra, Jung soo An, Justin Thattil, Kendall McKay

Mustang Panda deploys a new wave of malware targeting Europe

Cobalt Strike Meterpreter PlugX PUBLOAD 2022-04-26 · Trend Micro · Lord Alfred Remorin, Ryan Flores, Stephen Hilt

How Cybercriminals Abuse Cloud Tunneling Services

AsyncRAT Cobalt Strike DarkComet Meterpreter Nanocore RAT 2022-01-25 · Cynet · Orion Threat Research and Intelligence Team

Threats Looming Over the Horizon

Cobalt Strike Meterpreter NightSky 2021-12-20 · Bleeping Computer · Lawrence Abrams

Log4j vulnerability now used to install Dridex banking malware

DoppelDridex Meterpreter 2021-09-16 · Lumen · Black Lotus Labs

No Longer Just Theory: Black Lotus Labs Uncovers Linux Executables Deployed as Stealth Windows Loaders

PrivetSanya Meterpreter 2021-09-07 · Counter Craft · Counter Craft

Shellcode Detection Using Real-Time Kernel Monitoring

Meterpreter 2021-09-02 · · AhnLab · ASEC Analysis Team

Attacks using metasploit meterpreter

Appleseed Meterpreter 2021-06-02 · Sophos · Sean Gallagher

AMSI bypasses remain tricks of the malware trade

Agent Tesla Cobalt Strike Meterpreter 2021-03-25 · Recorded Future · Insikt Group®

Suspected Chinese Group Calypso APT Exploiting Vulnerable Microsoft Exchange Servers

Meterpreter PlugX 2021-01-07 · Recorded Future · Insikt Group®

Aversary Infrastructure Report 2020: A Defender's View

Octopus pupy Cobalt Strike Empire Downloader Meterpreter PoshC2 2021-01-06 · Red Canary · Tony Lambert

Hunting for GetSystem in offensive security tools

Cobalt Strike Empire Downloader Meterpreter PoshC2 2021-01-01 · Secureworks · SecureWorks

Threat Profile: GOLD WINTER

Cobalt Strike Hades Meterpreter GOLD WINTER 2021-01-01 · Secureworks · SecureWorks

Threat Profile: GOLD FRANKLIN

Grateful POS Meterpreter MimiKatz RemCom FIN6 2020-11-17 · cyble · Cyble

OceanLotus Continues With Its Cyber Espionage Operations

Cobalt Strike Meterpreter 2020-10-27 · US-CERT · US-CERT

Alert (AA20-301A): North Korean Advanced Persistent Threat Focus: Kimsuky

BabyShark GREASE MECHANICAL Meterpreter Kimsuky 2020-10-11 · Github (StrangerealIntel) · StrangerealIntel

Chimera, APT19 under the radar ?

Cobalt Strike Meterpreter 2020-10-01 · Wired · Andy Greenberg

Russia’s Fancy Bear Hackers Likely Penetrated a US Federal Agency

Cobalt Strike Meterpreter 2020-09-24 · US-CERT · US-CERT

Analysis Report (AR20-268A): Federal Agency Compromised by Malicious Cyber Actor

Cobalt Strike Meterpreter 2018-10-04 · Kaspersky Labs · GReAT

Shedding Skin – Turla’s Fresh Faces

KopiLuwak Agent.BTZ Cobra Carbon System Gazer Meterpreter Mosquito Skipper 2018-10-01 · Group-IB · Group-IB

Hi-Tech Crime Trends 2018

BackSwap Cobalt Strike Cutlet Meterpreter 2017-12-11 · Group-IB · Group-IB

MoneyTaker 1.5 YEARS OF SILENT OPERATIONS

Citadel Kronos Meterpreter 2017-06-09 · Morphisec · Michael Gorelik

FIN7 Takes Another Bite at the Restaurant Industry

Meterpreter FIN7 2011-07-10 · Michael Schierl

Facts and myths about antivirus evasion with Metasploit

Meterpreter

▶ [TLP:WHITE] win_meterpreter_auto (20251219 | Detects win.meterpreter.)
