Cobalt Strike (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 12:56:04 UTC

Cobalt Strike is a paid penetration testing product that allows an attacker to deploy an agent named 'Beacon' on the victim machine. Beacon includes a wealth of functionality to the attacker, including, but not limited to command execution, key logging, file transfer, SOCKS proxying, privilege escalation, mimikatz, port scanning and lateral movement. Beacon is in-memory/file-less, in that it consists of stageless or multi-stage shellcode that once loaded by exploiting a vulnerability or executing a shellcode loader, will reflectively load itself into the memory of a process without touching the disk. It supports C2 and staging over HTTP, HTTPS, DNS, SMB named pipes as well as forward and reverse TCP; Beacons can be daisy-chained. Cobalt Strike comes with a toolkit for developing shellcode loaders, called Artifact Kit.

The Beacon implant has become popular amongst targeted attackers and criminal users as it is well written, stable, and highly customizable.

2026-02-05 · Palo Alto Networks Unit 42 ·
The Shadow Campaigns: Uncovering Global Espionage
Cobalt Strike UNC6619 2026-02-03 · Kaspersky Labs · Anton Kargin, Georgy Kucherin
The Notepad++ supply chain attack — unnoticed execution chains and new IoCs
Chrysalis Cobalt Strike 2026-01-26 · Zscaler · Sudeep Singh, Yin Hong Chang
APT Attacks Target Indian Government Using GOGITTER, GITSHELLPAD, and GOSHELL | Part 1
Cobalt Strike 2026-01-13 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update July to December 2025
Coper FluBot Joker Aisuru Mirai AsyncRAT BianLian Cobalt Strike DCRat Havoc Latrodectus PureLogs Stealer Quasar RAT Remcos Rhadamanthys Sliver ValleyRAT Venom RAT Vidar XWorm 2026-01-04 · sec0wn · Mo Bustami
From a New Year's surprise to a bag of coal - Analysis of mystery PowerShell
Cobalt Strike 2025-11-20 · Google · Dan Perez, Harsh Parashar, Tierra Duncan
Beyond the Watering Hole: APT24's Pivot to Multi-Vector Attacks
BADAUDIO Cobalt Strike 2025-10-22 · Trend Micro · Daniel Lunghi, Joseph C Chen, Lenart Bermejo, Leon M Chang, Vickie Su
The Rise of Collaborative Tactics Among China-aligned Cyber Espionage Campaigns
Cobalt Strike DracuLoader ShadowPad 2025-10-02 · Cisco Talos · Joey Chen
UAT-8099: Chinese-speaking cybercrime group targets high-value IIS for SEO fraud
Cobalt Strike IISpy UAT-8099 2025-09-29 · The DFIR Report · The DFIR Report
From a Single Click: How Lunar Spider Enabled a Near Two-Month Intrusion
Brute Ratel C4 Cobalt Strike Latrodectus 2025-09-24 · The Hacker News · Ravie Lakshmanan
Chinese Hackers RedNovember Target Global Governments Using Pantegana and Cobalt Strike
Cobalt Strike Leslieloader Pantegana SparkRAT Storm-2077 2025-08-28 · Trend Micro · Nick Dai, Pierre Lee
TAOTH Campaign Exploits End-of-Support Software to Target Traditional Chinese Users and Dissidents
Cobalt Strike Merlin 2025-08-27 · Group-IB · Nikita Rostovcev, Sergei Turner

ShadowSilk: A Cross-Border Binary Union for Data Exfiltration

Cobalt Strike YoroTrooper 2025-07-21 · Kaspersky Labs · Daniil Pogorelov, Denis Kulik

The SOC files: Rumble in the jungle or APT41's new target in Africa

Cobalt Strike MimiKatz 2025-07-17 · Medium Ireneusz Tarnowski · Ireneusz Tarnowski

Dissecting the ClickFix User-Execution Attack and Its Sophisticated Persistence via ADS

Cobalt Strike 2025-07-16 · Proofpoint · Mark Kelly, Proofpoint Threat Research Team

Phish and Chips: China-Aligned Espionage Actors Ramp Up Taiwan Semiconductor Industry Targeting

Cobalt Strike Voldemort UNK_DropPitch UNK_FistBump UNK_SparkyCarp 2025-07-14 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update January to June 2025

Coper FluBot Hook Joker Mirai AsyncRAT BianLian BumbleBee Chaos Cobalt Strike DanaBot DCRat Havoc Latrodectus NjRAT Quasar RAT RedLine Stealer Remcos Rhadamanthys Sliver ValleyRAT WarmCookie XWorm 2025-06-24 · Bridewell · Bridewell

2025 Cyber Threat Intelligence Report

AsyncRAT Brute Ratel C4 Cobalt Strike Fog Ghost RAT Lumma Stealer Meduza Stealer Quasar RAT RedLine Stealer Sliver 2025-06-23 · Rushter · Artem Golubin

Threat Hunting Introduction: Cobalt Strike

Cobalt Strike 2025-06-19 · Hunt.io · Hunt.io

Cobalt Strike Operators Leverage PowerShell Loaders Across Chinese, Russian, and Global Infrastructure

Cobalt Strike 2025-06-15 · Positive Technologies · Stanislav Pyzhov, Vladislav Lunin

Team46 and TaxOff: two sides of the same coin

Cobalt Strike Team46 2025-05-27 · Trend Micro · Joseph C Chen

Earth Lamia Develops Custom Arsenal to Target Multiple Industries

BypassBoss Cobalt Strike JuicyPotato PULSEPACK STOWAWAY VShell Earth Lamia 2025-04-29 · Nextron Systems · Maurice Fielenbach

Nitrogen Dropping Cobalt Strike – A Combination of "Chemical Elements"

Cobalt Strike Nitrogen Loader 2025-04-24 · Mandiant · Mandiant

M-Trends 2025 Report

Akira Black Basta LockBit SystemBC GootLoader LockBit WIREFIRE Akira Black Basta Cobalt Strike LockBit RansomHub SystemBC Pink Sandstorm 2025-03-31 · Seqrite · Sathwik Ram Prakki, Subhajeet Singha

Operation HollowQuill: Malware delivered into Russian R&D Networks via Research Decoy PDFs

Cobalt Strike HollowQuill 2025-03-31 · Trend Micro · Lenart Bermejo, Ted Lee, Theo Chen

The Espionage Toolkit of Earth Alux: A Closer Look at its Advanced Techniques

Godzilla Webshell Cobalt Strike FINALDRAFT RAILSETTER Earth Alux 2025-01-29 · Palo Alto Networks Unit 42 · Lior Rochberger, Yoav Zemah

CL-STA-0048: An Espionage Operation Against High-Value Targets in South Asia

Cobalt Strike MimiKatz PlugX ValleyRAT Winos CL-STA-0048 2025-01-21 · Trend Micro · Leon Chang, Theo Chen

Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions

Cobalt Strike HemiGate ShadowPad SNAPPYBEE SparrowDoor UNC4841 2025-01-10 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update July to December 2024

Coper FluBot Hook Mirai FAKEUPDATES AsyncRAT BianLian Brute Ratel C4 Cobalt Strike DanaBot DCRat

Havoc Latrodectus NjRAT Quasar RAT RedLine Stealer Remcos Rhadamanthys Sliver Stealc 2025-01-07 · Hunt.io · Hunt.io

Golang Beacons and VS Code Tunnels: Tracking a Cobalt Strike Server Leveraging Trusted Infrastructure

Cobalt Strike 2024-12-04 · Rapid7 · Tyler McGraw

Black Basta Ransomware Campaign Drops Zbot, DarkGate, and Custom Malware

Black Basta Cobalt Strike DarkGate SystemBC Zloader 2024-12-03 · Hunt.io · Hunt.io

Rare Watermark Links Cobalt Strike 4.10 Team Servers to Ongoing Suspicious Activity

Cobalt Strike 2024-12-02 · The DFIR Report · The DFIR Report

The Curious Case of an Egg-Cellent Resume

More_eggs Pyramid Cobalt Strike 2024-11-19 · Trend Micro · Trend Micro

Spot the Difference: Earth Kasha's New LODEINFO Campaign And The Correlation Analysis With The APT10 Umbrella

Cobalt Strike LODEINFO NOOPDOOR MirrorFace 2024-11-12 · Recorded Future · Insikt Group

China-Nexus TAG-112 Compromises Tibetan Websites to Distribute Cobalt Strike

Cobalt Strike 2024-11-12 · Recorded Future · Insikt Group

China-Nexus TAG-112 Compromises Tibetan Websites to Distribute Cobalt Strike

Cobalt Strike TAG-112 2024-10-31 · Hunt.io · Hunt.io

Tricks, Treats, and Threats: Cobalt Strike & the Goblin Lurking in Plain Sight

Cobalt Strike 2024-10-24 · Seqrite · Sathwik Ram Prakki, Subhajeet Singha

Operation Cobalt Whisper: Threat Actor Targets Multiple Industries Across Hong Kong and Pakistan

Cobalt Strike Operation Cobalt Whisper 2024-10-23 · Cisco Talos · Edmund Brumaghin, Holger Unterbrink, Jordyn Dunk, Nicole Hoffman

Threat Spotlight: WarmCookie/BadSpace

Cobalt Strike csharp-streamer RAT WarmCookie 2024-10-23 · Cisco Talos · Edmund Brumaghin, Holger Unterbrink, Jordyn Dunk, Nicole Hoffman

Highlighting TA866/Asylum Ambuscade Activity Since 2021

WasabiSeed Cobalt Strike csharp-streamer RAT Resident Rhadamanthys WarmCookie 2024-10-10 · Hunt.io · Hunt.io

Unmasking Adversary Infrastructure: How Certificates and Redirects Exposed Earth Baxia and PlugX Activity

Cobalt Strike PlugX 2024-09-24 · Virus Bulletin · Aragorn Tseng, Chi-Yu You, Cristiana Brafman Kittner, Steve Su

Down the GRAYRABBIT HOle - Exposing UNC3569 and its Modus Operandi

KEYPLUG Cobalt Strike CROSSWALK GRAYRABBIT HelloBot HUI Loader PlugX SiestaGraph 2024-09-19 · Trend Micro · Cyris Tseng, Philip Chen, Pierre Lee, Sunny Lu, Ted Lee

Earth Baxia Uses Spear-Phishing and GeoServer Exploit to Target APAC (IoCs)

Cobalt Strike Earth Baxia 2024-09-19 · Trend Micro · Cyris Tseng, Philip Chen, Pierre Lee, Sunny Lu, Ted Lee

Earth Baxia Uses Spear-Phishing and GeoServer Exploit to Target APAC

Cobalt Strike Earth Baxia 2024-08-29 · Securonix · Den Iyzvyk, Tim Peck

From Cobalt Strike to Mimikatz: A Deep Dive into the SLOW#TEMPEST Campaign Targeting Chinese Users

Cobalt Strike MimiKatz 2024-08-26 · The DFIR Report · The DFIR Report

BlackSuit Ransomware

BlackSuit Cobalt Strike SystemBC 2024-08-23 · TEAMT5 · Still Hsu

Sailing the Seven SEAs: Deep Dive into Polaris' Arsenal and Intelligence Insights

Cobalt Strike Hodur PlugX TONESHELL 2024-08-23 · ITOCHU · Suguru Ishimaru, Yusuke Niwa

Pirates of The Nang Hai: Follow the Artifacts No One Know

Cobalt Strike Xiangoop 2024-08-22 · · NTT · Rintaro Koike

AppDomainManager Injectionを悪用したマルウェアによる攻撃について

Cobalt Strike Earth Baxia 2024-08-21 · TG Soft · C.R.A.M.

Chinese APT abuses MSC files with GrimResource vulnerability

Cobalt Strike Earth Baxia 2024-08-12 · Rapid7 · Tyler McGraw

Ongoing Social Engineering Campaign Refreshes Payloads

Black Basta Cobalt Strike GhostSocks Lumma Stealer SystemBC 2024-08-04 · Twitter (@embee_research) · Embee_research

Decoding a Cobalt Strike Downloader Script With CyberChef

Cobalt Strike 2024-08-01 · Cisco · Ashley Shen, Joey Chen, Vitor Ventura

APT41 likely compromised Taiwanese government-affiliated research institute with ShadowPad and Cobalt Strike

Cobalt Strike ShadowPad 2024-07-25 · SOC Prime · Veronika Telychko

UAC-0057 Attack Detection: A Surge in Adversary Activity Distributing PICASSOLOADER and Cobalt Strike Beacon

Cobalt Strike PicassoLoader Ghostwriter 2024-07-22 · Censys · Censys, Embee_research

A Beginner’s Guide to Hunting Malicious Open Directories

Cobalt Strike Lumma Stealer Vidar 2024-07-18 · Mandiant · Jared Wilson, Jonathan Lepore, Luis Rocha, Mike Stokkel, Pierre Gerlings, RENATO FONTANA, Stephen Eckels

APT41 Has Arisen From the DUST

Cobalt Strike 2024-07-16 · Recorded Future · Insikt Group

TAG-100 Uses Open-Source Tools in Suspected Global Espionage Campaign, Compromising Two Asia-Pacific Intergovernmental Bodies

Cobalt Strike Pantegana 2024-07-10 · Zscaler · Sudeep Singh, Yin Hong Chang

DodgeBox: A deep dive into the updated arsenal of APT41 | Part 1

Cobalt Strike DUSTPAN DUSTTRAP 2024-07-09 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update January to June 2024

Coper FluBot Hook Bashlite Mirai FAKEUPDATES AsyncRAT BianLian Cobalt Strike DCRat Havoc NjRAT QakBot Quasar RAT RedLine Stealer Remcos Rhadamanthys RisePro Sliver 2024-07-02 · Sekoia · Quentin Bourgue

Exposing FakeBat loader: distribution methods and adversary infrastructure

BlackCat Royal Ransom EugenLoader Carbanak Cobalt Strike DICELOADER Gozi IcedID Lumma Stealer NetSupportManager RAT Pikabot RedLine Stealer SectopRAT Sliver SmokeLoader Vidar 2024-06-21 · Elastic · Joe Desimone, Samir Bousseaden

GrimResource - Microsoft Management Console for initial access and evasion

Cobalt Strike 2024-05-23 · Checkpoint · Checkpoint Research

Sharp dragon expands towards africa and the caribbean

5.t Downloader Cobalt Strike SharpPanda 2024-05-23 · Check Point · Check Point

Chinese Espionage Campaign Expands to Target Africa and The Caribbean

5.t Downloader Cobalt Strike 2024-05-15 · Microsoft · Microsoft Threat Intelligence

Threat actors misusing Quick Assist in social engineering attacks leading to ransomware

Black Basta Cobalt Strike QakBot UNC4393 2024-05-15 · Microsoft · Microsoft Threat Intelligence

Threat actors misusing Quick Assist in social engineering attacks leading to ransomware

Black Basta Cobalt Strike QakBot SystemBC 2024-05-14 · Kaspersky · Boris Larin, Mert Degirmenci

QakBot attacks with Windows zero-day (CVE-2024-30051)

Cobalt Strike QakBot 2024-05-10 · Rapid7 Labs · Evan McCann, Thomas Elkins, Tyler McGraw

Ongoing Social Engineering Campaign Linked to Black Basta Ransomware Operators

Black Basta Black Basta Cobalt Strike NetSupportManager RAT 2024-04-24 · Securonix · Den Iyzvyk, Oleg Kolesnikov, Tim Peck

Analysis of Ongoing FROZEN#SHADOW Attack Campaign Leveraging SSLoad Malware and RMM Software for Domain Takeover

Cobalt Strike Latrodectus 2024-04-01 · The DFIR Report · The DFIR Report

From OneNote to RansomNote: An Ice Cold Intrusion

Cobalt Strike IcedID Nokoyawa Ransomware PhotoLoader 2024-03-01 · Medium b.magnezi · 0xMrMagnezi

Malware Analysis - Cobalt Strike

Cobalt Strike 2024-02-09 · Censys · Censys, Embee_research

A Beginners Guide to Tracking Malware Infrastructure

AsyncRAT BianLian Cobalt Strike QakBot 2024-02-08 · YouTube (Embee Research) · Embee_research

Cobalt Strike Decoding and C2 Extraction - 3 Minute Malware Analysis Speedrun

Cobalt Strike 2024-01-26 · Trendmicro · Hara Hiroaki, Masaoki Shoji, Nick Dai, Vickie Su, Yuka Higashi

Spot the Difference: An Analysis of the New LODEINFO Campaign by Earth Kasha

Anel Cobalt Strike LODEINFO NOOPDOOR 2024-01-13 · YouTube (Embee Research) · Embee_research

Cobalt Strike Shellcode Analysis and C2 Extraction

Cobalt Strike 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 2024-01-09 · Recorded Future · Insikt Group

2023 Adversary Infrastructure Report

AsyncRAT Cobalt Strike Emotet PlugX ShadowPad 2024-01-04 · Netresec · Erik Hjelmvik

Hunting for Cobalt Strike in PCAP

Cobalt Strike 2023-12-20 · Twitter (@embee_research) · Embee_research

Defeating Obfuscated Malware Scripts - Cobalt Strike

Cobalt Strike 2023-12-19 · Twitter (@embee_research) · Embee_research

Free Ghidra Tutorials for Beginners

Cobalt Strike DarkGate 2023-12-08 · Twitter (@embee_research) · Embee_research

Ghidra Basics - Manual Shellcode Analysis and C2 Extraction

Cobalt Strike 2023-12-06 · MITRE · MITRE ATT&CK

Cinnamon Tempest

Cobalt Strike HUI Loader PlugX Sliver BRONZE STARLIGHT 2023-12-04 · The DFIR Report · The DFIR Report

SQL Brute Force leads to Bluesky Ransomware

BlueSky Cobalt Strike 2023-11-19 · Twitter (@embee_research) · Embee_research

Combining Pivot Points to Identify Malware Infrastructure - Redline, Smokeloader and Cobalt Strike

Amadey Cobalt Strike RedLine Stealer SmokeLoader 2023-11-14 · Medium joshuapenny88 · Joshua Penny

HostingHunter Series: CHANG WAY TECHNOLOGIES CO. LIMITED

Hook Hydra Cobalt Strike SectopRAT 2023-11-10 · NSFOCUS · NSFOCUS

The New APT Group DarkCasino and the Global Surge in WinRAR 0-Day Exploits

Cobalt Strike Konni DarkCasino Opal Sleet 2023-11-07 · SOCRadar · SOCRadar

New Gootloader Variant “GootBot” Changes the Game in Malware Tactics

GootLoader Cobalt Strike UNC2565 2023-11-06 · Twitter (@embee_research) · Embee_research

Unpacking Malware With Hardware Breakpoints - Cobalt Strike

Cobalt Strike 2023-11-01 · nccgroup · Mick Koomen

Popping Blisters for research: An overview of past payloads and exploring recent developments

Blister Cobalt Strike 2023-10-23 · Twitter (@embee_research) · Embee_research

Cobalt Strike .VBS Loader - Decoding with Advanced CyberChef and Emulation

Cobalt Strike 2023-10-20 · Twitter (@embee_research) · Embee_research

Decoding a Cobalt Strike .hta Loader Using CyberChef and Emulation

Cobalt Strike 2023-10-18 · Twitter (@embee_research) · Embee_research

Ghidra Tutorial - Using Entropy To Locate a Cobalt Strike Decryption Function

Cobalt Strike 2023-10-12 · Netresec · Erik Hjelmvik

Forensic Timeline of an IcedID Infection

Cobalt Strike IcedID IcedID Downloader 2023-10-12 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q3 2023

FluBot AsyncRAT Ave Maria Cobalt Strike DCRat Havoc IcedID ISFB Nanocore RAT NjRAT QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Stealc Tofsee Vidar 2023-10-10 · Symantec · Threat Hunter Team

Grayling: Previously Unseen Threat Actor Targets Multiple Organizations in Taiwan

Cobalt Strike Havoc MimiKatz Grayling 2023-10-03 · Malware Traffic Analysis · Brad Duncan

2023-10-03 (Tuesday) - PikaBot infection with Cobalt Strike

Cobalt Strike Pikabot 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) 2023-09-22 · Palo Alto Networks Unit 42 · Lior Rochberger, Robert Falcone, Tom Fakterman

Cyberespionage Attacks Against Southeast Asian Government Linked to Stately Taurus, Aka Mustang Panda

Cobalt Strike MimiKatz RemCom ShadowPad TONESHELL 2023-09-12 · · ANSSI · ANSSI

FIN12: A Cybercriminal Group with Multiple Ransomware

BlackCat Cobalt Strike Conti Hive MimiKatz Nokoyawa Ransomware PLAY Royal Ransom Ryuk SystemBC

2023-08-30 · Trend Micro · Gilbert Sison, Hara Hiroaki, Lenart Bermejo, Leon M Chang, Ted Lee

Earth Estries Targets Government, Tech for Cyberespionage

Cobalt Strike HemiGate Earth Estries 2023-08-28 · The DFIR Report · The DFIR Report

HTML Smuggling Leads to Domain Wide Ransomware

Cobalt Strike IcedID Nokoyawa Ransomware 2023-08-18 · d01a · Mohamed Adel

Understanding Syscalls: Direct, Indirect, and Cobalt Strike Implementation

Cobalt Strike 2023-08-18 · TEAMT5 · Still Hsu, Zih-Cing Liao

Unmasking CamoFei: An In-depth Analysis of an Emerging APT Group Focused on Healthcare Sectors in East Asia

CatB Cobalt Strike DoorMe GIMMICK 2023-08-17 · SentinelOne · Aleksandar Milenkoski, Tom Hegel

Chinese Entanglement | DLL Hijacking in the Asian Gambling Sector

Cobalt Strike HUI Loader BRONZE STARLIGHT 2023-08-07 · Recorded Future · Insikt Group

RedHotel: A Prolific, Chinese State-Sponsored Group Operating at a Global Scale

Winnti Brute Ratel C4 Cobalt Strike FunnySwitch PlugX ShadowPad Spyder Earth Lusca 2023-07-29 · Google · Google Cybersecurity Action Team

Threat Horizons August 2023 Threat Horizons Report

SharkBot Cobalt Strike 2023-07-11 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q2 2023

Hydra AsyncRAT Aurora Stealer Ave Maria BumbleBee Cobalt Strike DCRat Havoc IcedID ISFB NjRAT QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Tofsee 2023-07-07 · Lab52 · Lab52

Beyond appearances: unknown actor using APT29's TTP against Chinese users

Cobalt Strike 2023-06-30 · K7 Security · Dhanush

Cobalt Strike's Deployment with Hardware Breakpoint for AMSI Bypass

Cobalt Strike 2023-06-16 · SOC Prime · Veronika Telychko

PicassoLoader and Cobalt Strike Beacon Detection: UAC-0057 aka GhostWriter Hacking Group Attacks the Ukrainian Leading Military Educational Institution

Cobalt Strike PicassoLoader Ghostwriter 2023-06-15 · eSentire · RussianPanda

eSentire Threat Intelligence Malware Analysis: Resident Campaign

Cobalt Strike Resident Rhadamanthys WarmCookie 2023-06-10 · The DFIR Report · The DFIR Report

IcedID Brings ScreenConnect and CSharp Streamer to ALPHV Ransomware Deployment

BlackCat Cobalt Strike IcedID 2023-06-08 · VMRay · Patrick Staubmann

Busy Bees - The Transformation of BumbleBee

BumbleBee Cobalt Strike Conti Meterpreter Sliver 2023-06-08 · Twitter (@embee_research) · Embee_research

Practical Queries for Identifying Malware Infrastructure: An informal page for storing Censys/Shodan queries

Amadey AsyncRAT Cobalt Strike QakBot Quasar RAT Sliver solarmarker 2023-05-11 · cocomelonc · cocomelonc

Malware development trick - part 28: Dump lsass.exe. Simple C++ example.

Cobalt Strike APT3 Keylogger 2023-04-20 · Secureworks · Counter Threat Unit ResearchTeam

Bumblebee Malware Distributed Via Trojanized Installer Downloads

BumbleBee Cobalt Strike 2023-04-20 · Github (dodo-sec) · dodo-sec

An analysis of syscall usage in Cobalt Strike Beacons

Cobalt Strike 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 2023-04-12 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q1 2023

FluBot Amadey AsyncRAT Aurora Ave Maria BumbleBee Cobalt Strike DCRat Emotet IcedID ISFB NjRAT QakBot RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Tofsee Vidar 2023-04-03 · The DFIR Report · The DFIR Report

Malicious ISO File Leads to Domain Wide Ransomware

Cobalt Strike IcedID Mount Locker 2023-03-30 · United States District Court (Eastern District of New York) · Fortra, HEALTH-ISAC, Microsoft

Cracked Cobalt Strike (1:23-cv-02447)

Black Basta BlackCat LockBit RagnarLocker LockBit Black Basta BlackCat Cobalt Strike Cuba Emotet LockBit Mount Locker PLAY QakBot RagnarLocker Royal Ransom Zloader 2023-03-30 · Recorded Future · Insikt Group

With KEYPLUG, China’s RedGolf Spies On, Steals From Wide Field of Targets

KEYPLUG Cobalt Strike PlugX RedGolf 2023-03-30 · eSentire · eSentire Threat Response Unit (TRU)

eSentire Threat Intelligence Malware Analysis: BatLoader

BATLOADER Cobalt Strike ISFB SystemBC Vidar 2023-03-28 · ExaTrack · ExaTrack

Mélofée: a new alien malware in the Panda's toolset targeting Linux hosts

HelloBot Melofee Winnti Cobalt Strike SparkRAT STOWAWAY 2023-03-10 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

From Royal With Love

Cobalt Strike Conti PLAY Royal Ransom Somnia 2023-03-01 · Zscaler · Meghraj Nandanwar, Shatak Jain

OneNote: A Growing Threat for Malware Distribution

AsyncRAT Cobalt Strike IcedID QakBot RedLine Stealer 2023-02-23 · Bitdefender · Bitdefender Team, Martin Zugec

Technical Advisory: Various Threat Actors Targeting ManageEngine Exploit CVE-2022-47966

Cobalt Strike DarkComet QuiteRAT RATel 2023-02-22 · Symantec · Symantec Threat Hunter Team

Hydrochasma: Previously Unknown Group Targets Medical and Shipping Organizations in Asia

Cobalt Strike 2023-02-14 · Cybereason · Cybereason Incident Response (IR) team

GootLoader - SEO Poisoning and Large Payloads Leading to Compromise

GootLoader Cobalt Strike SystemBC 2023-02-13 · Kroll · Laurie Iacono, Stephen Green

Royal Ransomware Deep Dive

Cobalt Strike Royal Ransom 2023-02-13 · AhnLab · kingkimgim

Dalbit (m00nlight): Chinese Hacker Group’s APT Attack Campaign

Godzilla Webshell ASPXSpy BlueShell CHINACHOPPER Cobalt Strike Ladon MimiKatz Dalbit 2023-02-08 · Trend Micro · Ted Lee

Earth Zhulong: Familiar Patterns Target Southeast Asian Firms

Cobalt Strike MACAMAX 1937CN 2023-02-03 · Mandiant · Genevieve Stark, Kimberly Goody

Float Like a Butterfly Sting Like a Bee

BazarBackdoor BumbleBee Cobalt Strike 2023-02-02 · Kroll · Elio Biasiotto, Stephen Green

Hive Ransomware Technical Analysis and Initial Access Discovery

BATLOADER Cobalt Strike Hive 2023-01-30 · Checkpoint · Arie Olshtein

Following the Scent of TrickGate: 6-Year-Old Packer Used to Deploy the Most Wanted Malware

Agent Tesla Azorult Buer Cerber Cobalt Strike Emotet Formbook HawkEye Keylogger Loki Password Stealer (PWS) Maze NetWire RC Remcos REvil TrickBot 2023-01-24 · Fortinet · Geri Revay

The Year of the Wiper

Azov Wiper Bruh Wiper CaddyWiper Cobalt Strike Vidar 2023-01-23 · Kroll · Elio Biasiotto, Stephen Green

Black Basta – Technical Analysis

Black Basta Cobalt Strike MimiKatz QakBot SystemBC 2023-01-16 · Intrinsec · Intrinsec

ProxyNotShell – OWASSRF – Merry Xchange

Cobalt Strike SystemBC 2023-01-05 · Symantec · Threat Hunter Team

Bluebottle: Campaign Hits Banks in French-speaking Countries in Africa

CloudEyE Cobalt Strike MimiKatz NetWire RC POORTRY Quasar RAT BlueBottle 2022-12-15 · Mandiant · Mandiant

Trojanized Windows 10 Operating System Installers Targeted Ukrainian Government

Cobalt Strike STOWAWAY 2022-12-08 · Cisco Talos · Tiago Pereira

Breaking the silence - Recent Truebot activity

Clop Cobalt Strike FlawedGrace Raspberry Robin Silence Teleport 2022-12-06 · EuRepoC · Camille Borrett, Kerstin Zettl-Schabath, Lena Rottinger

Conti/Wizard Spider

BazarBackdoor Cobalt Strike Conti Emotet IcedID Ryuk TrickBot WIZARD SPIDER 2022-12-02 · Palo Alto Networks Unit 42 · Bob Jung, Dominik Reichel, Esmid Idrizovic

Blowing Cobalt Strike Out of the Water With Memory Analysis

Cobalt Strike 2022-11-15 · SOC Prime · Veronika Telychko

Somnia Malware Detection: UAC-0118 aka FRwL Launches Cyber Attacks Against Organizations in Ukraine Using Enhanced Malware Strains

Cobalt Strike Vidar UAC-0118 2022-11-09 · Trend Micro · Hara Hiroaki, Ted Lee

Hack the Real Box: APT41’s New Subgroup Earth Longzhi

Cobalt Strike MimiKatz Earth Longzhi 2022-11-03 · paloalto Netoworks: Unit42 · Chris Navarrete, Durgesh Sangvikar, Matthew Tennis, Siddhart Shibiraj, Yanhui Jia, Yu Fu

Cobalt Strike Analysis and Tutorial: Identifying Beacon Team Servers in the Wild

Cobalt Strike 2022-11-03 · Github (chronicle) · Chronicle

GCTI Open Source Detection Signatures

Cobalt Strike Sliver 2022-11-03 · Group-IB · Rustam Mirkasymov

Financially motivated, dangerously activated: OPERA1ER APT in Africa

Cobalt Strike Common Raven 2022-10-31 · Cynet · Max Malyutin

Orion Threat Alert: Qakbot TTPs Arsenal and the Black Basta Ransomware

Black Basta Cobalt Strike QakBot 2022-10-13 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q3 2022

FluBot Arkei Stealer AsyncRAT Ave Maria BumbleBee Cobalt Strike DCRat Dridex Emotet Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT QakBot RecordBreaker RedLine Stealer Remcos Socelars Tofsee Vjw0rm 2022-10-13 · Microsoft · Microsoft Threat Hunting, MSRC Team

Hunting for Cobalt Strike: Mining and plotting for fun and profit

Cobalt Strike 2022-10-12 · Trend Micro · Ian Kenefick, Lucas Silva, Nicole Hernandez

Black Basta Ransomware Gang Infiltrates Networks via QAKBOT, Brute Ratel, and Cobalt Strike

Black Basta Brute Ratel C4 Cobalt Strike QakBot 2022-10-03 · Check Point · Marc Salinas Fernandez

Bumblebee: increasing its capacity and evolving its TTPs

BumbleBee Cobalt Strike Meterpreter Sliver Vidar 2022-10-03 · Trend Micro · Jaromír Hořejší, Joseph Chen

Water Labbu Abuses Malicious DApps to Steal Cryptocurrency

Cobalt Strike Water Labbu 2022-09-26 · The DFIR Report · The DFIR Report

BumbleBee: Round Two

BumbleBee Cobalt Strike Meterpreter 2022-09-25 · YouTube (Arda Büyükkaya) · Arda Büyükkaya

Cobalt Strike Shellcode Loader With Rust (YouTube)

Cobalt Strike 2022-09-13 · AdvIntel · Advanced Intelligence

AdvIntel's State of Emotet aka "SpmTools" Displays Over Million Compromised Machines Through 2022

Conti Cobalt Strike Emotet Ryuk TrickBot 2022-09-12 · The DFIR Report · The DFIR Report

Dead or Alive? An Emotet Story

Cobalt Strike Emotet 2022-09-07 · Google · Google Threat Analysis Group, Pierre-Marc Bureau

Initial access broker repurposing techniques in targeted attacks against Ukraine

AnchorMail Cobalt Strike IcedID 2022-09-07 · cyble · Cyble

Bumblebee Returns With New Infection Technique

BumbleBee Cobalt Strike 2022-09-06 · Didier Stevens · Didier Stevens

An Obfuscated Beacon – Extra XOR Layer

Cobalt Strike 2022-09-06 · CISA · CISA, FBI, MS-ISAC, US-CERT

Alert (AA22-249A) #StopRansomware: Vice Society

Cobalt Strike Empire Downloader FiveHands HelloKitty SystemBC Zeppelin 2022-09-06 · cocomelonc · cocomelonc

Malware development tricks: parent PID spoofing. Simple C++ example.

Cobalt Strike Konni 2022-09-06 · · INCIBE-CERT · INCIBE

Estudio del análisis de Nobelium

BEATDROP BOOMBOX Cobalt Strike EnvyScout Unidentified 099 (APT29 Dropbox Loader) VaporRage 2022-09-01 · Trend Micro · Trend Micro

Ransomware Spotlight Black Basta

Black Basta Cobalt Strike MimiKatz QakBot 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 · eSentire · eSentire Threat Response Unit (TRU)

Hacker Infrastructure Used in Cisco Breach Discovered Attacking a Top Workforce Management Corporation & an Affiliate of Russia’s Evil Corp Gang Suspected, Reports eSentire

Cobalt Strike FiveHands UNC2447 2022-08-25 · SentinelOne · Jim Walter

BlueSky Ransomware | AD Lateral Movement, Evasion and Fast Encryption Put Threat on the Radar

BlueSky Cobalt Strike JuicyPotato 2022-08-22 · Microsoft · Microsoft

Extortion Economics - Ransomware’s new business model

BlackCat Conti Hive REvil AgendaCrypt Black Basta BlackCat Brute Ratel C4 Cobalt Strike Conti Hive Mount Locker Nokoyawa Ransomware REvil Ryuk 2022-08-19 · nccgroup · Ross Inman

Back in Black: Unlocking a LockBit 3.0 Ransomware Attack

FAKEUPDATES Cobalt Strike LockBit 2022-08-18 · Group-IB · Nikita Rostovtsev

APT41 World Tour 2021 on a tight schedule

Cobalt Strike 2022-08-18 · Trustwave · Pawel Knapczyk

Overview of the Cyber Weapons Used in the Ukraine - Russia War

AcidRain CaddyWiper Cobalt Strike CredoMap DCRat DoubleZero GraphSteel GrimPlant HermeticWiper INDUSTROYER2 InvisiMole IsaacWiper PartyTicket 2022-08-18 · Sophos · Sean Gallagher

Cookie stealing: the new perimeter bypass

Cobalt Strike Meterpreter MimiKatz Phoenix Keylogger Quasar RAT 2022-08-18 · · NSFOCUS · NSFOCUS

New APT group MURENSHARK investigative report: Torpedoes hit Turkish Navy

Cobalt Strike 2022-08-18 · Trustwave · Pawel Knapczyk

Overview of the Cyber Weapons Used in the Ukraine - Russia War

AcidRain CaddyWiper Cobalt Strike CredoMap DCRat DoubleZero GraphSteel GrimPlant HermeticWiper INDUSTROYER2 InvisiMole IsaacWiper PartyTicket 2022-08-17 · Cybereason · Cybereason Global SOC Team

Bumblebee Loader – The High Road to Enterprise Domain Control

BumbleBee Cobalt Strike 2022-08-17 · Secureworks · Counter Threat Unit ResearchTeam

DarkTortilla Malware Analysis

Agent Tesla AsyncRAT Cobalt Strike DarkTortilla Nanocore RAT RedLine Stealer 2022-08-12 · SANS ISC · Brad Duncan

Monster Libra (TA551/Shathak) pushes IcedID (Bokbot) with Dark VNC and Cobalt Strike

Cobalt Strike DarkVNC IcedID 2022-08-11 · Malcat · malcat team

LNK forensic and config extraction of a cobalt strike beacon

Cobalt Strike 2022-08-11 · SecurityScorecard · Robert Ames

The Increase in Ransomware Attacks on Local Governments

BlackCat BlackCat Cobalt Strike LockBit 2022-08-10 · · Weixin · Red Raindrop Team

Operation(верность) mercenary: a torrent of steel trapped in the plains of Eastern Europe

BumbleBee Cobalt Strike 2022-08-08 · The DFIR Report · The DFIR Report

BumbleBee Roasts Its Way to Domain Admin

BumbleBee Cobalt Strike 2022-08-04 · YouTube (Arda Büyükkaya) · Arda Büyükkaya

LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool

Cobalt Strike LockBit 2022-08-03 · Palo Alto Networks Unit 42 · Brad Duncan

Flight of the Bumblebee: Email Lures and File Sharing Services Lead to Malware

BazarBackdoor BumbleBee Cobalt Strike Conti 2022-08-02 · Cisco Talos · Asheer Malhotra, Vitor Ventura

Manjusaka: A Chinese sibling of Sliver and Cobalt Strike

Manjusaka Cobalt Strike Manjusaka 2022-07-30 · cocomelonc

Malware AV evasion - part 8. Encode payload via Z85

Agent Tesla Carbanak Carberp Cardinal RAT Cobalt Strike donut_injector 2022-07-28 · SentinelOne · James Haughom, Julien Reisdorffer, Júlio Dantas

Living Off Windows Defender | LockBit Ransomware Sideloads Cobalt Strike Through Microsoft Security Tool

Cobalt Strike LockBit 2022-07-27 · Trend Micro · Buddy Tancio, Jed Valderama

Gootkit Loader’s Updated Tactics and Fileless Delivery of Cobalt Strike

Cobalt Strike GootKit Kronos REvil SunCrypt 2022-07-27 · ReversingLabs · Joseph Edwards

Threat analysis: Follina exploit fuels 'live-off-the-land' attacks

Cobalt Strike MimiKatz 2022-07-27 · cyble · Cyble Research Labs

Targeted Attacks Being Carried Out Via DLL SideLoading

Cobalt Strike QakBot 2022-07-22 · Binary Ninja · Xusheng Li

Reverse Engineering a Cobalt Strike Dropper With Binary Ninja

Cobalt Strike 2022-07-20 · NVISO Labs · Sasja Reynaert

Analysis of a trojanized jQuery script: GootLoader unleashed

GootLoader Cobalt Strike 2022-07-20 · Advanced Intelligence · Marley Smith, Vitali Kremez, Yelisey Boguslavskiy

Anatomy of Attack: Truth Behind the Costa Rica Government Ransomware 5-Day Intrusion

Cobalt Strike 2022-07-20 · U.S. Cyber Command · Cyber National Mission Force Public Affairs

Cyber National Mission Force discloses IOCs from Ukrainian networks

Cobalt Strike GraphSteel GrimPlant MicroBackdoor 2022-07-20 · Mandiant · Mandiant Threat Intelligence

Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities

Cobalt Strike GraphSteel GrimPlant MicroBackdoor 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 2022-07-18 · Palo Alto Networks Unit 42 · Unit 42

Obscure Serpens

Cobalt Strike Empire Downloader Meterpreter MimiKatz DarkHydrus 2022-07-18 · Censys · Censys

Russian Ransomware C2 Network Discovered in Censys Data

Cobalt Strike DeimosC2 MimiKatz PoshC2 2022-07-13 · Malwarebytes Labs · Hossein Jazi, Roberto Santos

Cobalt Strikes again: UAC-0056 continues to target Ukraine in its latest campaign

Cobalt Strike 2022-07-13 · Palo Alto Networks Unit 42 · Chris Navarrete, Durgesh Sangvikar, Siddhart Shibiraj, Yanhui Jia, Yu Fu

Cobalt Strike Analysis and Tutorial: CS Metadata Encryption and Decryption

Cobalt Strike 2022-07-11 · · Cert-UA · Cert-UA

UAC-0056 attack on Ukrainian state organizations using Cobalt Strike Beacon (CERT-UA#4941)

Cobalt Strike 2022-07-07 · SANS ISC · Brad Duncan

Emotet infection with Cobalt Strike

Cobalt Strike Emotet 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 2022-07-06 · · Cert-UA · Cert-UA

UAC-0056 cyberattack on Ukrainian state organizations using Cobalt Strike Beacon (CERT-UA#4914)

Cobalt Strike 2022-06-30 · Trend Micro · Emmanuel Panopio, James Panlilio, John Kenneth Reyes, Kenneth Adrian Apostol, Melvin Singwa, Mirah Manlapig, Paolo Ronniel Labrador

Black Basta Ransomware Operators Expand Their Attack Arsenal With QakBot Trojan and PrintNightmare Exploit

Black Basta Cobalt Strike QakBot 2022-06-28 · Lumen · Black Lotus Labs

ZuoRAT Hijacks SOHO Routers To Silently Stalk Networks

ZuoRAT Cobalt Strike 2022-06-27 · Kaspersky ICS CERT · Artem Snegirev, Kirill Kruglov

Attacks on industrial control systems using ShadowPad

Cobalt Strike PlugX ShadowPad 2022-06-26 · BushidoToken

Overview of Russian GRU and SVR Cyberespionage Campaigns 1H 2022

Cobalt Strike CredoMap EnvyScout 2022-06-23 · cyble · Cyble Research Labs

Matanbuchus Loader Resurfaces

Cobalt Strike Matanbuchus 2022-06-23 · Secureworks · Counter Threat Unit ResearchTeam

BRONZE STARLIGHT Ransomware Operations Use HUI Loader

ATOMSILO Cobalt Strike HUI Loader LockFile NightSky Pandora PlugX Quasar RAT Rook SodaMaster

BRONZE STARLIGHT 2022-06-21 · Cisco Talos · Chris Neal, Flavio Costa, Guilherme Venere

Avos ransomware group expands with new attack arsenal

AvosLocker Cobalt Strike DarkComet MimiKatz 2022-06-20 · · Cert-UA · Cert-UA

UAC-0098 group cyberattack on critical infrastructure of Ukraine (CERT-UA#4842)

Cobalt Strike 2022-06-17 · SANS ISC · Brad Duncan

Malspam pushes Matanbuchus malware, leads to Cobalt Strike

Cobalt Strike Matanbuchus 2022-06-11 · Twitter (@MsftSecIntel) · Microsoft Threat Intelligence

Tweet on DEV-0401, DEV-0234 exploiting Confluence RCE CVE-2022-26134

Kinsing Mirai Cobalt Strike Lilac Typhoon 2022-06-07 · AdvIntel · Marley Smith, Vitali Kremez, Yelisey Boguslavskiy

BlackCat — In a Shifting Threat Landscape, It Helps to Land on Your Feet: Tech Dive

BlackCat BlackCat Cobalt Strike 2022-06-07 · cyble · Cyble

Bumblebee Loader on The Rise

BumbleBee Cobalt Strike 2022-06-06 · Trellix · Trelix

Growling Bears Make Thunderous Noise

Cobalt Strike HermeticWiper WhisperGate NB65 2022-06-04 · kienmanowar Blog · m4n0w4r, Tran Trung Kien

[QuickNote] CobaltStrike SMB Beacon Analysis

Cobalt Strike 2022-06-03 · AttackIQ · AttackIQ Adversary Research Team, Jackson Wells

Attack Graph Response to US CERT AA22-152A: Karakurt Data Extortion Group

Cobalt Strike MimiKatz 2022-06-02 · Mandiant · Mandiant Intelligence

To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions

FAKEUPDATES Blister Cobalt Strike DoppelPaymer Dridex FriedEx Hades LockBit Macaw MimiKatz Phoenix Locker WastedLocker 2022-06-02 · Mandiant · Mandiant

TRENDING EVIL Q2 2022

CloudEyE Cobalt Strike CryptBot Emotet IsaacWiper QakBot 2022-06-01 · Elastic · Andrew Pease, Daniel Stepanic, Derek Ditch, Salim Bitam, Seth Goodwin

CUBA Ransomware Campaign Analysis

Cobalt Strike Cuba Meterpreter MimiKatz SystemBC 2022-05-25 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

SocGholish Campaigns and Initial Access Kit

FAKEUPDATES Blister Cobalt Strike NetSupportManager RAT 2022-05-24 · BitSight · BitSight, João Batista, Pedro Umbelino

Emotet Botnet Rises Again

Cobalt Strike Emotet QakBot SystemBC 2022-05-24 · The Hacker News · Florian Goutin

Malware Analysis: Trickbot

Cobalt Strike Conti Ryuk TrickBot 2022-05-22 · R136a1 · Dominik Reichel

Introduction of a PE file extractor for various situations

Cobalt Strike Matanbuchus 2022-05-20 · Cybleinc · Cyble

Malware Campaign Targets InfoSec Community: Threat Actor Uses Fake Proof Of Concept To Deliver Cobalt-Strike Beacon

Cobalt Strike 2022-05-20 · AhnLab · ASEC

Why Remediation Alone Is Not Enough When Infected by Malware

Cobalt Strike DarkSide 2022-05-20 · sonatype · Ax Sharma

New 'pymafka' malicious package drops Cobalt Strike on macOS, Windows, Linux

Cobalt Strike 2022-05-19 · InfoSec Handlers Diary Blog · Brad Duncan

Bumblebee Malware from TransferXL URLs

BumbleBee Cobalt Strike 2022-05-19 · InfoSec Handlers Diary Blog · Brad Duncan

Bumblebee Malware from TransferXL URLs

BumbleBee Cobalt Strike 2022-05-18 · PRODAFT Threat Intelligence · PRODAFT

Wizard Spider In-Depth Analysis

Cobalt Strike Conti WIZARD SPIDER 2022-05-17 · Trend Micro · Trend Micro Research

Ransomware Spotlight: RansomEXX

LaZagne Cobalt Strike IcedID MimiKatz PyXie RansomEXX TrickBot 2022-05-12 · Red Canary · Lauren Podber, Tony Lambert

Gootloader and Cobalt Strike malware analysis

GootLoader Cobalt Strike 2022-05-12 · Red Canary · Lauren Podber, Tony Lambert

The Goot cause: Detecting Gootloader and its follow-on activity

GootLoader Cobalt Strike 2022-05-12 · Intel 471 · Intel 471

What malware to look for if you want to prevent a ransomware attack

Conti BumbleBee Cobalt Strike IcedID Sliver 2022-05-12 · TEAMT5 · Leon Chang, Silvia Yeh

The Next Gen PlugX/ShadowPad? A Dive into the Emerging China-Nexus Modular Trojan, Pangolin8RAT (slides)

KEYPLUG Cobalt Strike CROSSWALK FunnySwitch PlugX ShadowPad Winnti SLIME29 TianWu 2022-05-11 · · NTT · Ryu Hiyoshi

Operation RestyLink: Targeted attack campaign targeting Japanese companies

Cobalt Strike 2022-05-11 · InfoSec Handlers Diary Blog · Brad Duncan

TA578 using thread-hijacked emails to push ISO files for Bumblebee malware

BumbleBee Cobalt Strike IcedID PhotoLoader 2022-05-10 · Marco Ramilli's Blog · Marco Ramilli

A Malware Analysis in RU-AU conflict

Cobalt Strike 2022-05-09 · TEAMT5 · TeamT5

Hiding in Plain Sight: Obscuring C2s by Abusing CDN Services

Cobalt Strike 2022-05-09 · Microsoft · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC)

Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself

AnchorDNS BlackCat BlackMatter Conti DarkSide HelloKitty Hive LockBit REvil FAKEUPDATES Griffon ATOMSILO BazarBackdoor BlackCat BlackMatter Blister Cobalt Strike Conti DarkSide Emotet FiveHands Gozi HelloKitty Hive IcedID ISFB JSSLoader LockBit LockFile Maze NightSky Pandora Phobos Phoenix Locker PhotoLoader QakBot REvil Rook Ryuk SystemBC TrickBot WastedLocker BRONZE STARLIGHT 2022-05-09 · The DFIR Report · The DFIR Report

SEO Poisoning – A Gootloader Story

GootLoader LaZagne Cobalt Strike GootKit 2022-05-09 · cocomelonc · cocomelonc

Malware development: persistence - part 4. Windows services. Simple C++ example.

Anchor AppleJeus Attor BBSRAT BlackEnergy Carbanak Cobalt Strike DuQu 2022-05-08 · IronNet · Brent Eskridge, Joey Fitzpatrick, Michael Leardi

Tracking Cobalt Strike Servers Used in Cyberattacks on Ukraine

Cobalt Strike 2022-05-06 · The Hacker News · Ravie Lakshmanan

This New Fileless Malware Hides Shellcode in Windows Event Logs

Cobalt Strike 2022-05-06 · Palo Alto Networks Unit 42 · Chris Navarrete, Durgesh Sangvikar, Siddhart Shibiraj, Yanhui Jia, Yu Fu

Cobalt Strike Analysis and Tutorial: CS Metadata Encoding and Decoding

Cobalt Strike 2022-05-06 · Twitter (@MsftSecIntel) · Microsoft Security Intelligence

Twitter Thread on initial infeciton of SocGholish/ FAKEUPDATES campaigns lead to BLISTER Loader, CobaltStrike, Lockbit and followed by Hands On Keyboard activity

FAKEUPDATES Blister Cobalt Strike LockBit 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 2022-05-04 · Twitter (@felixw3000) · Felix

Twitter Thread with info on infection chain with IcedId, Cobalt Strike, and Hidden VNC.

Cobalt Strike IcedID PhotoLoader 2022-05-04 · Kaspersky · Denis Legezo

A new secret stash for “fileless” malware

Cobalt Strike 2022-05-03 · Cluster25 · Cluster25

The Strange Link Between A Destructive Malware And A Ransomware-Gang Linked Custom Loader: IsaacWiper Vs Vatet

Cobalt Strike IsaacWiper PyXie 2022-05-03 · Recorded Future · Insikt Group®

SOLARDEFLECTION C2 Infrastructure Used by NOBELIUM in Company Brand Misuse

Cobalt Strike EnvyScout 2022-05-03 · Recorded Future · Insikt Group

SOLARDEFLECTION C2 Infrastructure Used by NOBELIUM in Company Brand Misuse

Cobalt Strike 2022-05-02 · · Macnica · Hiroshi Takeuchi

Attack Campaigns that Exploit Shortcuts and ISO Files

Cobalt Strike 2022-05-02 · Cisco Talos · JAIME FILSON, Kendall McKay, Paul Eubanks

Conti and Hive ransomware operations: Leveraging victim chats for insights

Cobalt Strike Conti Hive 2022-04-28 · PWC · PWC UK

Cyber Threats 2021: A Year in Retrospect (Annex)

Cobalt Strike Conti PlugX RokRAT Inception Framework Red Menshen 2022-04-28 · Mandiant · Anders Vejlby, John Wolfram, Nick Simonian, Sarah Hawley, Tyler McLellan

Trello From the Other Side: Tracking APT29 Phishing Campaigns

Cobalt Strike 2022-04-27 · Sentinel LABS · James Haughom, Jim Walter, Júlio Dantas

LockBit Ransomware Side-loads Cobalt Strike Beacon with Legitimate VMware Utility

Cobalt Strike LockBit 2022-04-27 · Mandiant · Mandiant

Assembling the Russian Nesting Doll: UNC2452 Merged into APT29

Cobalt Strike Raindrop SUNBURST TEARDROP 2022-04-27 · · ANSSI · ANSSI

LE GROUPE CYBERCRIMINEL FIN7

Bateleur BELLHOP Griffon SQLRat POWERSOURCE Andromeda BABYMETAL BlackCat BlackMatter BOOSTWRITE Carbanak Cobalt Strike DNSMessenger Dridex DRIFTPIN Gameover P2P MimiKatz Murofet Qadars Ranbyus SocksBot 2022-04-27 · Sentinel LABS · James Haughom, Jim Walter, Júlio Dantas

LockBit Ransomware Side-loads Cobalt Strike Beacon with Legitimate VMware Utility

Cobalt Strike LockBit BRONZE STARLIGHT 2022-04-27 · Trendmicro · Daniel Lunghi, Jaromír Hořejší

Operation Gambling Puppet

reptile oRAT AsyncRAT Cobalt Strike DCRat Ghost RAT PlugX Quasar RAT Trochilus RAT Earth Berberoka 2022-04-27 · Trendmicro · Trendmicro

IOCs for Earth Berberoka - Windows

AsyncRAT Cobalt Strike PlugX Quasar RAT Earth Berberoka 2022-04-26 · Intel 471 · Intel 471

Conti and Emotet: A constantly destructive duo

Cobalt Strike Conti Emotet IcedID QakBot TrickBot 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 2022-04-25 · The DFIR Report · The DFIR Report

Quantum Ransomware

Cobalt Strike IcedID 2022-04-25 · Morphisec · Morphisec Labs

New Core Impact Backdoor Delivered Via VMware Vulnerability

Cobalt Strike JSSLoader 2022-04-21 · ZeroSec · Andy Gill

Understanding Cobalt Strike Profiles - Updated For Cobalt Strike 4.6

Cobalt Strike 2022-04-19 · Blake's R&D · bmcder02

Extracting Cobalt Strike from Windows Error Reporting

Cobalt Strike 2022-04-19 · Varonis · Nadav Ovadia

Hive Ransomware Analysis

Cobalt Strike Hive MimiKatz 2022-04-18 · SentinelOne · James Haughom

From the Front Lines | Peering into A PYSA Ransomware Attack

Chisel Chisel Cobalt Strike Mespinoza 2022-04-18 · vanmieghem · Vincent Van Mieghem

A blueprint for evading industry leading endpoint protection in 2022

Cobalt Strike 2022-04-18 · AdvIntel · Vitali Kremez, Yelisey Boguslavskiy

Enter KaraKurt: Data Extortion Arm of Prolific Ransomware Group

AvosLocker BazarBackdoor BlackByte BlackCat Cobalt Strike HelloKitty Hive Karakurt 2022-04-14 · Cynet · Max Malyutin

Orion Threat Alert: Flight of the BumbleBee

BumbleBee Cobalt Strike 2022-04-13 · ESET Research · Jean-Ian Boutin, Tomáš Procházka

ESET takes part in global operation to disrupt Zloader botnets

Cobalt Strike Zloader 2022-04-13 · Microsoft · Microsoft 365 Defender Threat Intelligence Team

Dismantling ZLoader: How malicious ads led to disabled security tools and ransomware

BlackMatter Cobalt Strike DarkSide Ryuk Zloader 2022-04-08 · Infinitum Labs · Arda Büyükkaya

Threat Spotlight: Conti Ransomware Group Behind the Karakurt Hacking Team

Cobalt Strike MimiKatz 2022-04-07 · InQuest · Nick Chalard, Will MacArthur

Ukraine CyberWar Overview

CyclopsBlink Cobalt Strike GraphSteel GrimPlant HermeticWiper HermeticWizard MicroBackdoor PartyTicket Saint Bot Scieron WhisperGate 2022-04-07 · splunk · Splunk Threat Research Team

You Bet Your Lsass: Hunting LSASS Access

Cobalt Strike MimiKatz 2022-04-06 · Github (infinitumlabs) · Arda Büyükkaya

Karakurt Hacking Team Indicators of Compromise (IOC)

Cobalt Strike 2022-04-04 · Mandiant · Brendan McKeague, Bryce Abdo, Ioana Teaca, Zander Work

FIN7 Power Hour: Adversary Archaeology and the Evolution of FIN7

Griffon BABYMETAL Carbanak Cobalt Strike JSSLoader Termite 2022-03-31 · nccgroup · Alex Jessop, Nikolaos Pantazopoulos, RIFT: Research and Intelligence Fusion Team, Simon Biggs

Conti-nuation: methods and techniques observed in operations post the leaks

Cobalt Strike Conti QakBot 2022-03-31 · SC Media · SC Staff

Novel obfuscation leveraged by Hive ransomware

Cobalt Strike Hive 2022-03-30 · Prevailion · Prevailion

Wizard Spider continues to confound

BazarBackdoor Cobalt Strike Emotet 2022-03-30 · Bleeping Computer · Bill Toulas

Phishing campaign targets Russian govt dissidents with Cobalt Strike

Unidentified PS 002 (RAT) Cobalt Strike 2022-03-29 · Malwarebytes Labs · Hossein Jazi

New spear phishing campaign targets Russian dissidents

Unidentified PS 002 (RAT) Cobalt Strike 2022-03-29 · SentinelOne · Antonis Terefos, James Haughom, Jeff Cavanaugh, Jim Walter, Nick Fox, Shai Tilias

From the Front Lines | Hive Ransomware Deploys Novel IPfuscation Technique To Avoid Detection

Cobalt Strike Hive 2022-03-28 · Medium walmartglobaltech · Jason Reaves

CobaltStrike UUID stager

Cobalt Strike 2022-03-25 · nccgroup · Yun Zheng Hu

Mining data from Cobalt Strike beacons

Cobalt Strike 2022-03-25 · GOV.UA · State Service of Special Communication and Information Protection of Ukraine (CIP)

Who is behind the Cyberattacks on Ukraine's Critical Information Infrastructure: Statistics for March 15-22

Xloader Agent Tesla CaddyWiper Cobalt Strike DoubleZero GraphSteel GrimPlant HeaderTip HermeticWiper IsaacWiper MicroBackdoor Pandora RAT 2022-03-22 · NVISO Labs · Didier Stevens

Cobalt Strike: Overview – Part 7

Cobalt Strike 2022-03-22 · Red Canary · Red Canary

2022 Threat Detection Report

FAKEUPDATES Silver Sparrow BazarBackdoor Cobalt Strike GootKit Yellow Cockatoo RAT 2022-03-21 · Threat Post · Lisa Vaas

Conti Ransomware V. 3, Including Decryptor, Leaked

Cobalt Strike Conti TrickBot 2022-03-21 · eSentire · eSentire Threat Response Unit (TRU)

Conti Affiliate Exposed: New Domain Names, IP Addresses and Email Addresses Uncovered

HelloKitty BazarBackdoor Cobalt Strike Conti FiveHands HelloKitty IcedID 2022-03-17 · Google · Benoit Sevens, Google Threat Analysis Group, Vladislav Stolyarov

Exposing initial access broker with ties to Conti

BazarBackdoor BumbleBee Cobalt Strike Conti 2022-03-16 · SANS ISC · Brad Duncan

Qakbot infection with Cobalt Strike and VNC activity

Cobalt Strike QakBot 2022-03-16 · InfoSec Handlers Diary Blog · Brad Duncan

Qakbot infection with Cobalt Strike and VNC activity

Cobalt Strike QakBot 2022-03-16 · paloalto Netoworks: Unit42 · Andrew Guan, Chris Navarrete, Durgesh Sangvikar, Siddhart Shibiraj, Yanhui Jia, Yu Fu

Cobalt Strike Analysis and Tutorial: How Malleable C2 Profiles Make Cobalt Strike Difficult to Detect

Cobalt Strike 2022-03-15 · SentinelOne · Amitai Ben Shushan Ehrlich

Threat Actor UAC-0056 Targeting Ukraine with Fake Translation Software

Cobalt Strike GraphSteel GrimPlant SaintBear 2022-03-15 · Prevailion · Matt Stafford, Sherman Smith

What Wicked Webs We Un-weave

Cobalt Strike Conti 2022-03-14 · Bleeping Computer · Bill Toulas

Fake antivirus updates used to deploy Cobalt Strike in Ukraine

Cobalt Strike 2022-03-12 · Arash's Blog · Arash Parsa

Analyzing Malware with Hooks, Stomps, and Return-addresses

Cobalt Strike 2022-03-11 · · Cert-UA

Cyberattack on Ukrainian state authorities using the Cobalt Strike Beacon (CERT-UA#4145)

Cobalt Strike 2022-03-09 · Bleeping Computer · Ionut Ilascu

CISA updates Conti ransomware alert with nearly 100 domain names

BazarBackdoor Cobalt Strike Conti TrickBot 2022-03-09 · BreachQuest · Bernard Silvestrini, Marco Figueroa, Napoleon Bing

The Conti Leaks | Insight into a Ransomware Unicorn

Cobalt Strike MimiKatz TrickBot 2022-03-08 · Mandiant · Douglas Bienstock, Geoff Ackerman, John Wolfram, Rufus Brown, Van Ta

Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments

KEYPLUG Cobalt Strike LOWKEY 2022-03-07 · The DFIR Report · The DFIR Report

2021 Year In Review

Cobalt Strike 2022-03-04 · Telsy · Telsy

Legitimate Sites Used As Cobalt Strike C2s Against Indian Government

Cobalt Strike 2022-03-03 · Trend Micro · Trend Micro Research

Cyberattacks are Prominent in the Russia-Ukraine Conflict

BazarBackdoor Cobalt Strike Conti Emotet WhisperGate 2022-03-01 · VirusTotal · VirusTotal

VirusTotal's 2021 Malware Trends Report

Anubis AsyncRAT BlackMatter Cobalt Strike DanaBot Dridex Khonsari MimiKatz Mirai Nanocore RAT Orcus RAT 2022-02-24 · Fortinet · Fred Gutierrez

Nobelium Returns to the Political World Stage

Cobalt Strike 2022-02-24 · Cynet · Max Malyutin

New Wave of Emotet – When Project X Turns Into Y

Cobalt Strike Emotet 2022-02-23 · AdvIntel · Vitali Kremez, Yelisey Boguslavskiy

24 Hours From Log4Shell to Local Admin: Deep-Dive Into Conti Gang Attack on Fortune 500 (DFIR)

Cobalt Strike Conti 2022-02-23 · SophosLabs Uncut · Andrew Brandt

Dridex bots deliver Entropy ransomware in recent attacks

Cobalt Strike Dridex Entropy 2022-02-23 · cyber.wtf blog · Luca Ebach

What the Pack(er)?

Cobalt Strike Emotet 2022-02-22 · Bleeping Computer · Bill Toulas

Vulnerable Microsoft SQL Servers targeted with Cobalt Strike

Cobalt Strike Kingminer Lemon Duck 2022-02-22 · eSentire · eSentire Threat Response Unit (TRU)

IcedID to Cobalt Strike In Under 20 Minutes

Cobalt Strike IcedID PhotoLoader 2022-02-21 · The DFIR Report

Qbot and Zerologon Lead To Full Domain Compromise

Cobalt Strike QakBot 2022-02-21 · ASEC

Cobalt Strike Being Distributed to Vulnerable MS-SQL Servers

Cobalt Strike Lemon Duck 2022-02-20 · Medium SOCFortress · SOCFortress

Detecting Cobalt Strike Beacons

Cobalt Strike 2022-02-18 · Huntress Labs · Matthew Brennan

Hackers No Hashing: Randomizing API Hashes to Evade Cobalt Strike Shellcode Detection

Cobalt Strike 2022-02-16 · Security Onion · Doug Burks

Quick Malware Analysis: Emotet Epoch 5 and Cobalt Strike pcap from 2022-02-08

Cobalt Strike Emotet 2022-02-15 · eSentire · eSentire Threat Response Unit (TRU)

Increase in Emotet Activity and Cobalt Strike Deployment

Cobalt Strike Emotet 2022-02-10 · Cybereason · Cybereason Global SOC Team

Threat Analysis Report: All Paths Lead to Cobalt Strike - IcedID, Emotet and QBot

Cobalt Strike Emotet IcedID QakBot 2022-02-09 · vmware · VMWare

Exposing Malware in Linux-Based Multi-Cloud Environments

ACBackdoor BlackMatter DarkSide Erebus HelloKitty Kinsing PLEAD QNAPCrypt RansomEXX REvil Sysrv-hello TeamTNT Vermilion Strike Cobalt Strike 2022-01-31 · CyberArk · Arash Parsa

Analyzing Malware with Hooks, Stomps and Return-addresses

Cobalt Strike 2022-01-28 · Morphisec · Morphisec Labs

Log4j Exploit Hits Again: Vulnerable Unifi Network Application (Ubiquiti) at Risk

Cobalt Strike 2022-01-27 · JSAC 2021 · Hajime Yanagishita, Kiyotaka Tamada, Suguru Ishimaru, You Nakatsuru

What We Can Do against the Chaotic A41APT Campaign

CHINACHOPPER Cobalt Strike HUI Loader SodaMaster 2022-01-26 · Blackberry · Codi Starks, Ryan Gibson, Will Ikard

Log4U, Shell4Me

Cobalt Strike 2022-01-25 · Cynet · Orion Threat Research and Intelligence Team

Threats Looming Over the Horizon

Cobalt Strike Meterpreter NightSky 2022-01-24 · The DFIR Report · The DFIR Report

Cobalt Strike, a Defender’s Guide – Part 2

Cobalt Strike 2022-01-20 · Morphisec · Michael Gorelik

Log4j Exploit Hits Again: Vulnerable VMWare Horizon Servers at Risk

Cobalt Strike 2022-01-19 · Sophos · Colin Cowie, Mat Gangwer, Sophos MTR Team, Stan Andic

Zloader Installs Remote Access Backdoors and Delivers Cobalt Strike

Cobalt Strike Zloader 2022-01-19 · Elastic · Andrew Pease, Daniel Stepanic, Derek Ditch, Seth Goodwin

Collecting Cobalt Strike Beacons with the Elastic Stack

Cobalt Strike 2022-01-19 · Elastic · Andrew Pease, Daniel Stepanic, Derek Ditch, Seth Goodwin

Extracting Cobalt Strike Beacon Configurations

Cobalt Strike 2022-01-19 · Blackberry · The BlackBerry Research & Intelligence Team

Kraken the Code on Prometheus

Prometheus Backdoor BlackMatter Cerber Cobalt Strike DCRat Ficker Stealer QakBot REvil Ryuk 2022-01-18 · Recorded Future · Insikt Group®

2021 Adversary Infrastructure Report

BazarBackdoor Cobalt Strike Dridex IcedID QakBot TrickBot 2022-01-17 · Trend Micro · Cedric Pernet, Daniel Lunghi, Gloria Chen, Jaromír Hořejší, Joseph Chen, Kenney Lu

Delving Deep: An Analysis of Earth Lusca’s Operations

BIOPASS Cobalt Strike FunnySwitch JuicyPotato ShadowPad Winnti Earth Lusca 2022-01-16 · forensicitguy · Tony Lambert

Analyzing a CACTUSTORCH HTA Leading to Cobalt Strike

CACTUSTORCH Cobalt Strike 2022-01-15 · Huntress Labs · Team Huntress

Threat Advisory: VMware Horizon Servers Actively Being Hit With Cobalt Strike (by DEV-0401)

Cobalt Strike 2022-01-11 · Cybereason · Chen Erlich, Daichi Shimabukuro, Niv Yona, Ofir Ozer, Omri Refaeli

Threat Analysis Report: DatopLoader Exploits ProxyShell to Deliver QBOT and Cobalt Strike

Cobalt Strike QakBot Squirrelwaffle 2022-01-11 · Twitter (@cglyer) · Christopher Glyer

Thread on DEV-0401, a china based ransomware operator exploiting VMware Horizon with log4shell and deploying NightSky ransomware

Cobalt Strike NightSky 2022-01-11 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

Signed DLL campaigns as a service

BATLOADER Cobalt Strike ISFB Zloader 2022-01-09 · forensicitguy · Tony Lambert

Inspecting a PowerShell Cobalt Strike Beacon

Cobalt Strike 2022-01-06 · Sekoia · sekoia

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

Cobalt Strike EnvyScout 2022-01-01 · Silent Push · Silent Push

Consequences- The Conti Leaks and future problems

Cobalt Strike Conti 2021-12-29 · Blake's R&D · Blake

Cobalt Strike DFIR: Listening to the Pipes

Cobalt Strike 2021-12-29 · CrowdStrike · Benjamin Wiley, Falcon OverWatch Team

OverWatch Exposes AQUATIC PANDA in Possession of Log4Shell Exploit Tools During Hands-on Intrusion Attempt

Cobalt Strike 2021-12-28 · Morphus Labs · Renato Marinho

Attackers are abusing MSBuild to evade defenses and implant Cobalt Strike beacons

Cobalt Strike 2021-12-22 · Telsy · Telsy Research Team

Phishing Campaign targeting citizens abroad using COVID-19 theme lures

Cobalt Strike 2021-12-16 · Red Canary · The Red Canary Team

Intelligence Insights: December 2021

Cobalt Strike QakBot Squirrelwaffle 2021-12-16 · TEAMT5 · Aragorn Tseng, Charles Li, Peter Syu, Tom Lai

Winnti is Coming - Evolution after Prosecution

Cobalt Strike FishMaster FunnySwitch HIGHNOON ShadowPad Spyder 2021-12-10 · Accenture · Accenture

Karakurt rises from its lair

Cobalt Strike Karakurt 2021-12-07 · Bleeping Computer · Lawrence Abrams

Emotet now drops Cobalt Strike, fast forwards ransomware attacks

Cobalt Strike Emotet 2021-12-06 · CERT-FR · CERT-FR

Phishing campaigns by the Nobelium intrusion set

Cobalt Strike 2021-12-06 · Mandiant · Ashraf Abdalhalim, Ben Read, Doug Bienstock, Gabriella Roncone, Jonathan Leathery, Josh Madeley, Juraj Sucik, Luis Rocha, Luke Jenkins, Manfred Erjak, Marius Fodoreanu, Microsoft Detection and Response Team (DART), Microsoft Threat Intelligence Center (MSTIC), Mitchell Clarke, Parnian Najafi, Sarah Hawley, Wojciech Ledzion

Suspected Russian Activity Targeting Government and Business Entities Around the Globe (UNC2452)

Cobalt Strike CryptBot 2021-12-02 · CERT-FR · CERT-FR

Phishing Campaigns by the Nobelium Intrusion Set

Cobalt Strike 2021-11-30 · Symantec · Symantec Threat Hunter Team

Yanluowang: Further Insights on New Ransomware Threat

BazarBackdoor Cobalt Strike FiveHands 2021-11-29 · Mandiant · Brandan Schondorfer, Tyler McLellan

Kitten.gif: Meet the Sabbath Ransomware Affiliate Program, Again

Cobalt Strike ROLLCOAST 2021-11-29 · The DFIR Report · The DFIR Report

CONTInuing the Bazar Ransomware Story

BazarBackdoor Cobalt Strike Conti 2021-11-19 · Trend Micro · Abdelrhman Sharshar, Mohamed Fahmy, Sherif Magdy

Squirrelwaffle Exploits ProxyShell and ProxyLogon to Hijack Email Chains

Cobalt Strike QakBot Squirrelwaffle 2021-11-17 · Trend Micro · Abdelrhman Sharshar, Mohamed Fahmy, Ryan Maglaque, Sherif Magdy

Analyzing ProxyShell-related Incidents via Trend Micro Managed XDR

Cobalt Strike Cotx RAT 2021-11-17 · nviso · Didier Stevens

Cobalt Strike: Decrypting Obfuscated Traffic – Part 4

Cobalt Strike 2021-11-17 · Twitter (@Unit42_Intel) · Unit 42

Tweet on Matanbuchus Loader used to deliver Qakbot (tag obama128b) and follow-up CobaltStrike

Cobalt Strike QakBot 2021-11-17 · Black Hills Information Security · Kyle Avery

DNS Over HTTPS for Cobalt Strike

Cobalt Strike 2021-11-16 · Cisco · Asheer Malhotra, Chetan Raghuprasad, Vanja Svajcer

Attackers use domain fronting technique to target Myanmar with Cobalt Strike

Cobalt Strike 2021-11-16 · Blackberry · Dean Given, Eoin Wickens, Jim Simpson, Marta Janus, T.J. O'Leary, Tom Bonner

Finding Beacons in the dark

Cobalt Strike 2021-11-16 · IronNet · IronNet Threat Research, Joey Fitzpatrick, Morgan Demboski, Peter Rydzynski

How IronNet's Behavioral Analytics Detect REvil and Conti Ransomware

Cobalt Strike Conti IcedID REvil 2021-11-15 · TRUESEC · Fabio Viggiani

ProxyShell, QBot, and Conti Ransomware Combined in a Series of Cyberattacks

Cobalt Strike Conti QakBot 2021-11-13 · Just Still · Still Hsu

Threat Spotlight - Domain Fronting

Cobalt Strike 2021-11-12 · Malwarebytes · Hossein Jazi

A multi-stage PowerShell based attack targets Kazakhstan

Cobalt Strike 2021-11-11 · Cynet · Max Malyutin

A Duck Nightmare Quakbot Strikes with QuakNightmare Exploitation

Cobalt Strike QakBot 2021-11-10 · Sekoia · Cyber Threat Intelligence team

Walking on APT31 infrastructure footprints

Rekoobe Unidentified ELF 004 Cobalt Strike 2021-11-10 · AT&T · Josh Gomez

Stories from the SOC - Powershell, Proxyshell, Conti TTPs OH MY!

Cobalt Strike Conti 2021-11-09 · Cybereason · Aleksandar Milenkoski, Eli Salem

THREAT ANALYSIS REPORT: From Shatak Emails to the Conti Ransomware

Cobalt Strike Conti 2021-11-05 · Blackberry · The BlackBerry Research & Intelligence Team

Hunter Becomes Hunted: Zebra2104 Hides a Herd of Malware

Cobalt Strike DoppelDridex Mount Locker Phobos StrongPity 2021-11-05 · Twitter (@Unit42_Intel) · Unit 42

Tweet on TA551 (Shathak) BazarLoader infection with CobaltStrike and DarkVNC drops

BazarBackdoor Cobalt Strike 2021-11-03 · nviso · Didier Stevens

Cobalt Strike: Using Process Memory To Decrypt Traffic – Part 3

Cobalt Strike 2021-11-03 · Didier Stevens · Didier Stevens

New Tool: cs-extract-key.py

Cobalt Strike 2021-11-02 · Intel 471 · Intel 471

Cybercrime underground flush with shipping companies’ credentials

Cobalt Strike Conti 2021-11-02 · unh4ck · Cyb3rSn0rlax

Detecting CONTI CobaltStrike Lateral Movement Techniques - Part 2

Cobalt Strike Conti 2021-11-02 · boschko.ca blog · Olivier Laflamme

Cobalt Strike Process Injection

Cobalt Strike 2021-11-01 · Accenture · Curt Wilson, Heather Larrieu, Katrina Hill

Diving into double extortion campaigns

Cobalt Strike MimiKatz 2021-11-01 · The DFIR Report · @iiamaleks, @samaritan_o

From Zero to Domain Admin

Cobalt Strike Hancitor 2021-10-29 · Europol · Europol

12 targeted for involvement in ransomware attacks against critical infrastructure

Cobalt Strike Dharma LockerGoga MegaCortex TrickBot 2021-10-29 · · Національна поліція України · Національна поліція України

Cyberpolice exposes transnational criminal group in causing $ 120 million in damage to foreign companies

Cobalt Strike Dharma LockerGoga MegaCortex TrickBot 2021-10-27 · nviso · Didier Stevens

Cobalt Strike: Using Known Private Keys To Decrypt Traffic – Part 2

Cobalt Strike 2021-10-26 · Cisco Talos · Edmund Brumaghin, Mariano Graziano, Nick Mavis

SQUIRRELWAFFLE Leverages malspam to deliver Qakbot, Cobalt Strike

Cobalt Strike QakBot Squirrelwaffle 2021-10-26 · unh4ck · Hamza OUADIA

Detecting CONTI CobaltStrike Lateral Movement Techniques - Part 1

Cobalt Strike Conti 2021-10-26 · ANSSI

Identification of a new cyber criminal group: Lockean

Cobalt Strike DoppelPaymer Egregor Maze PwndLocker QakBot REvil 2021-10-21 · nviso · Didier Stevens

Cobalt Strike: Using Known Private Keys To Decrypt Traffic – Part 1

Cobalt Strike 2021-10-21 · CrowdStrike · Alex Clinton, Tasha Robinson

Stopping GRACEFUL SPIDER: Falcon Complete’s Fast Response to Recent SolarWinds Serv-U Exploit Campaign

Cobalt Strike FlawedGrace TinyMet 2021-10-18 · The DFIR Report · The DFIR Report

IcedID to XingLocker Ransomware in 24 hours

Cobalt Strike IcedID Mount Locker 2021-10-18 · paloalto Netoworks: Unit42 · Brad Duncan

Case Study: From BazarLoader to Network Reconnaissance

BazarBackdoor Cobalt Strike 2021-10-18 · Symantec · Threat Hunter Team

Harvester: Nation-state-backed group uses new toolset to target victims in South Asia

Cobalt Strike Graphon 2021-10-14 · Medium walmartglobaltech · Jason Reaves

Investigation into the state of NIM malware Part 2

Cobalt Strike NimGrabber Nimrev Unidentified 088 (Nim Ransomware) 2021-10-13 · Blackberry · BlackBerry Research & Intelligence Team

BlackBerry Shines Spotlight on Evolving Cobalt Strike Threat in New Book

Cobalt Strike 2021-10-12 · Mandiant · Alyssa Rahman

Defining Cobalt Strike Components So You Can BEA-CONfident in Your Analysis

Cobalt Strike 2021-10-11 · Accenture · Accenture Cyber Threat Intelligence

Moving Left of the Ransomware Boom

REvil Cobalt Strike MimiKatz RagnarLocker REvil 2021-10-08 · 0ffset Blog · Chuong Dong

SQUIRRELWAFFLE – Analysing The Main Loader

Cobalt Strike Squirrelwaffle 2021-10-07 · Netskope · Ghanashyam Satpathy, Gustavo Palazolo

SquirrelWaffle: New Malware Loader Delivering Cobalt Strike and QakBot

Cobalt Strike QakBot Squirrelwaffle 2021-10-07 · Mandiant · Mandiant Research Team

FIN12 Group Profile: FIN12 Priotizes Speed to Deploy Ransomware Aginst High-Value Targets

Cobalt Strike Empire Downloader TrickBot 2021-10-06 · Blackberry · Blackberry Research

Finding Beacons in the Dark

Cobalt Strike 2021-10-05 · Blackberry · The BlackBerry Research & Intelligence Team

Drawing a Dragon: Connecting the Dots to Find APT41

Cobalt Strike Ghost RAT 2021-10-04 · The DFIR Report · The DFIR Report

BazarLoader and the Conti Leaks

BazarBackdoor Cobalt Strike Conti 2021-10-04 · Sophos · Chaitanya Ghorpade, Kajal Katiyar, Krisztián Diriczi, Rahil Shah, Sean Gallagher, Vikas Singh

Atom Silo ransomware actors use Confluence exploit, DLL side-load for stealthy attack

ATOMSILO Cobalt Strike 2021-10-03 · Github (0xjxd) · Joel Dönne

SquirrelWaffle - From Maldoc to Cobalt Strike

Cobalt Strike Squirrelwaffle 2021-10-01 · 0ffset Blog · Chuong Dong

SQUIRRELWAFFLE – Analysing the Custom Packer

Cobalt Strike Squirrelwaffle 2021-09-30 · CrowdStrike · Falcon OverWatch Team

Hunting for the Confluence Exploitation: When Falcon OverWatch Becomes the First Line of Defense

Cobalt Strike 2021-09-30 · PT Expert Security Center

Masters of Mimicry: new APT group ChamelGang and its arsenal

Cobalt Strike 2021-09-30 · PTSecurity · PT ESC Threat Intelligence

Masters of Mimicry: new APT group ChamelGang and its arsenal

Cobalt Strike 2021-09-29 · Advanced Intelligence · Vitali Kremez, Yelisey Boguslavskiy

Backup “Removal” Solutions - From Conti Ransomware With Love

Cobalt Strike Conti 2021-09-29 · Malware Traffic Analysis · Brad Duncan

2021-09-29 (Wednesday) - Hancitor with Cobalt Strike

Cobalt Strike Hancitor 2021-09-29 · Malware Traffic Analysis · Brad Duncan

Hancitor with Cobalt Strike

Cobalt Strike Hancitor 2021-09-28 · Zscaler · Avinash Kumar, Brett Stone-Gross

Squirrelwaffle: New Loader Delivering Cobalt Strike

Cobalt Strike Squirrelwaffle 2021-09-27 · Cynet · Max Malyutin

A Virtual Baffle to Battle Squirrelwaffle

Cobalt Strike Squirrelwaffle 2021-09-26 · NSFOCUS · Jie Ji

Insights into Ransomware Spread Using Exchange 1-Day Vulnerabilities 1-2

Cobalt Strike LockFile 2021-09-24 · Trend Micro · Warren Sto.Tomas

Examining the Cring Ransomware Techniques

Cobalt Strike Cring MimiKatz 2021-09-22 · CISA · US-CERT

Alert (AA21-265A) Conti Ransomware

Cobalt Strike Conti 2021-09-21 · Medium elis531989 · Eli Salem

The Squirrel Strikes Back: Analysis of the newly emerged cobalt-strike loader “SquirrelWaffle”

Cobalt Strike Squirrelwaffle 2021-09-21 · GuidePoint Security · Drew Schmitt

A Ransomware Near Miss: ProxyShell, a RAT, and Cobalt Strike

Cobalt Strike 2021-09-21 · Sophos · Andrew Brandt, Chaitanya Ghorpade, Krisztián Diriczi, Shefali Gupta, Vikas Singh

Cring ransomware group exploits ancient ColdFusion server

Cobalt Strike Cring 2021-09-21 · skyblue.team blog · skyblue team

Scanning VirusTotal's firehose

Cobalt Strike 2021-09-21 · eSentire · eSentire

Ransomware Hackers Attack a Top Safety Testing Org. Using Tactics and Techniques Borrowed from Chinese Espionage Groups

Cobalt Strike MimiKatz UNC215 2021-09-17 · Medium inteloperator · Intel Operator

The default: 63 6f 62 61 6c 74 strike

Cobalt Strike 2021-09-17 · Malware Traffic Analysis · Brad Duncan

2021-09-17 - SQUIRRELWAFFLE Loader with Cobalt Strike

Cobalt Strike Squirrelwaffle 2021-09-17 · CrowdStrike · Falcon OverWatch Team

Falcon OverWatch Hunts Down Adversaries Where They Hide

BazarBackdoor Cobalt Strike 2021-09-16 · RiskIQ · RiskIQ

Untangling the Spider Web: The Curious Connection Between WIZARD SPIDER’s Ransomware Infrastructure and a Windows Zero-Day Exploit

Cobalt Strike Ryuk 2021-09-16 · Medium Shabarkin · Pavel Shabarkin

Pointer: Hunting Cobalt Strike globally

Cobalt Strike 2021-09-16 · Twitter (@GossiTheDog) · Kevin Beaumont

Tweet on some unknown threat actor dropping Mgbot, custom IIS modular backdoor and cobalstrike using exploiting ProxyShell

Cobalt Strike MgBot 2021-09-15 · Microsoft · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC)

Analyzing attacks that exploit the CVE-2021-40444 MSHTML vulnerability

Cobalt Strike 2021-09-14 · Recorded Future · Insikt Group®

Full-Spectrum Cobalt Strike Detection

Cobalt Strike 2021-09-13 · The DFIR Report · The DFIR Report

BazarLoader to Conti Ransomware in 32 Hours

BazarBackdoor Cobalt Strike Conti 2021-09-12 · Medium michaelkoczwara · Michael Koczwara

Mapping and Pivoting from Cobalt Strike C2 Infrastructure Attributed to CVE-2021-40444

Cobalt Strike 2021-09-10 · Gigamon · Joe Slowik

Rendering Threats: A Network Perspective

BumbleBee Cobalt Strike 2021-09-09 · Trend Micro · Trend Micro

Remote Code Execution 0-Day (CVE-2021-40444) Hits Windows, Triggered Via Office Docs

BumbleBee Cobalt Strike 2021-09-08 · Arash's Blog · Arash Parsa

Hook Heaps and Live Free

Cobalt Strike 2021-09-07 · Medium michaelkoczwara · Michael Koczwara

Cobalt Strike C2 Hunting with Shodan

Cobalt Strike 2021-09-06 · kienmanowar Blog · m4n0w4r

Quick analysis CobaltStrike loader and shellcode

Cobalt Strike 2021-09-03 · Sophos · Anand Ajjan, Andrew Ludgate, Gabor Szappanos, Peter Mackenzie, Sean Gallagher, Sergio Bestulic, Syed Zaidi

Conti affiliates use ProxyShell Exchange exploit in ransomware attacks

Cobalt Strike Conti 2021-09-03 · Trend Micro · Mohamad Mokbel

The State of SSL/TLS Certificate Usage in Malware C&C Communications

AdWind ostap AsyncRAT BazarBackdoor BitRAT Buer Chthonic CloudEyE Cobalt Strike DCRat Dridex

FindPOS GootKit Gozi IcedID ISFB Nanocore RAT Orcus RAT PandaBanker Qadars QakBot Quasar RAT Rockloader ServHelper Shifu SManager TorrentLocker TrickBot Vawtrak Zeus Zloader 2021-09-02 · Twitter (@th3_protoCOL) · Colin, GaborSzappanos

Tweet on Confluence Server exploitation (CVE-2021-26084) in the wild and cobaltsrike activity (mentioned in replies by GaborSzappanos)

Cobalt Strike 2021-09-02 · Medium michaelkoczwara · Michael Koczwara

Cobalt Strike PowerShell Payload Analysis

Cobalt Strike 2021-09-01 · YouTube (Black Hat) · Aragorn Tseng, Charles Li

Mem2Img: Memory-Resident Malware Detection via Convolution Neural Network

Cobalt Strike PlugX Waterbear 2021-08-31 · BreakPoint Labs · BreakPoint Labs

Cobalt Strike and Ransomware – Tracking An Effective Ransomware Campaign

Cobalt Strike 2021-08-30 · · Qianxin · Red Raindrop Team

Operation (Thủy Tinh) OceanStorm: The evil lotus hidden under the abyss

Cobalt Strike MimiKatz 2021-08-29 · The DFIR Report · The DFIR Report

Cobalt Strike, a Defender’s Guide

Cobalt Strike 2021-08-27 · Morphisec · Morphisec Labs

ProxyShell Exchange Exploitation Now Leads To An Increasing Amount Of Cobaltstrike Backdoors

Cobalt Strike 2021-08-27 · Aon · Aon’s Cyber Labs, Noah Rubin

Cobalt Strike Configuration Extractor and Parser

Cobalt Strike 2021-08-25 · Trend Micro · Hara Hiroaki, Ted Lee

Earth Baku An APT Group Targeting Indo-Pacific Countries With New Stealth Loaders and Backdoor

Cobalt Strike DUSTPAN SideWalk 2021-08-24 · ESET Research · Mathieu Tartare, Thibaut Passilly

The SideWalk may be as dangerous as the CROSSWALK

Cobalt Strike CROSSWALK SideWalk SparklingGoblin 2021-08-24 · Trend Micro · Hara Hiroaki, Ted Lee

Earth Baku Returns

Cobalt Strike CROSSWALK DUSTPAN SideWalk 2021-08-23 · FBI · FBI

Indicators of Compromise Associated with OnePercent Group Ransomware

Cobalt Strike MimiKatz 2021-08-23 · Youtube (SANS Digital Forensics and Incident Response) · Chad Tilbury

Keynote: Cobalt Strike Threat Hunting

Cobalt Strike 2021-08-19 · Blackberry · BlackBerry Research & Intelligence Team

BlackBerry Prevents: Threat Actor Group TA575 and Dridex Malware

Cobalt Strike Dridex TA575 2021-08-19 · Sekoia · sekoia

An insider insights into Conti operations – Part two

Cobalt Strike Conti 2021-08-18 · Intezer · Ryan Robinson

Cobalt Strike: Detect this Persistent Threat

Cobalt Strike 2021-08-17 · Advanced Intelligence · Vitali Kremez, Yelisey Boguslavskiy

Hunting for Corporate Insurance Policies: Indicators of [Ransom] Exfiltration

Cobalt Strike Conti 2021-08-17 · Sekoia · sekoia

An insider insights into Conti operations – Part one

Cobalt Strike Conti 2021-08-17 · Medium michaelkoczwara · Michael Koczwara

Cobalt Strike Hunting — DLL Hijacking/Attack Analysis

Cobalt Strike 2021-08-15 · Symantec · Threat Hunter Team

The Ransomware Threat

Babuk BlackMatter DarkSide Avaddon Babuk BADHATCH BazarBackdoor BlackMatter Clop Cobalt Strike Conti DarkSide DoppelPaymer Egregor Emotet FiveHands FriedEx Hades IcedID LockBit Maze MegaCortex MimiKatz QakBot RagnarLocker REvil Ryuk TrickBot WastedLocker 2021-08-11 · Advanced Intelligence · Vitali Kremez

Secret "Backdoor" Behind Conti Ransomware Operation: Introducing Atera Agent

Cobalt Strike Conti 2021-08-09 · IstroSec · Ladislav Bačo

APT Cobalt Strike Campaign targeting Slovakia (DEF CON talk)

Cobalt Strike 2021-08-05 · Secureworks · Counter Threat Unit ResearchTeam

Detecting Cobalt Strike: Government-Sponsored Threat Groups (APT32)

Cobalt Strike 2021-08-05 · Red Canary · Brian Donohue, Dan Cotton, Tony Lambert

When Dridex and Cobalt Strike give you Grief

Cobalt Strike DoppelDridex DoppelPaymer 2021-08-04 · Secureworks · Counter Threat Unit ResearchTeam

Detecting Cobalt Strike: Cybercrime Attacks (GOLD LAGOON)

Cobalt Strike 2021-08-04 · Sentinel LABS · Gal Kristal

Hotcobalt – New Cobalt Strike DoS Vulnerability That Lets You Halt Operations

Cobalt Strike 2021-08-04 · CrowdStrike · CrowdStrike Intelligence Team, CrowdStrike IR, Falcon OverWatch Team

PROPHET SPIDER Exploits Oracle WebLogic to Facilitate Ransomware Activity

Cobalt Strike Egregor Mount Locker Prophet Spider 2021-08-03 · Cybereason · Assaf Dahan, Daniel Frank, Lior Rochberger, Tom Fakterman

DeadRinger: Exposing Chinese Threat Actors Targeting Major Telcos

CHINACHOPPER Cobalt Strike MimiKatz Nebulae 2021-08-02 · Youtube (Forschungsinstitut Cyber Defense) · Alexander Rausch, Konstantin Klinger

The CODE 2021: Workshop presentation and demonstration about CobaltStrike

Cobalt Strike 2021-08-01 · The DFIR Report · The DFIR Report

BazarCall to Conti Ransomware via Trickbot and Cobalt Strike

BazarBackdoor Cobalt Strike Conti TrickBot 2021-07-30 · Twitter (@Unit42_Intel) · Unit 42

Tweet on BazarLoader infection leading to cobaltstrike and Powershell script file for PrintNightmare vulnerability

BazarBackdoor Cobalt Strike 2021-07-29 · Rasta Mouse · Rasta Mouse

NTLM Relaying via Cobalt Strike

Cobalt Strike 2021-07-29 · Microsoft · Microsoft 365 Defender Threat Intelligence Team

BazaCall: Phony call centers lead to exfiltration and ransomware

BazarBackdoor Cobalt Strike 2021-07-27 · Blackberry · BlackBerry Research & Intelligence Team

Old Dogs New Tricks: Attackers Adopt Exotic Programming Languages

elf.wellmess ElectroRAT BazarNimrod Buer Cobalt Strike Remcos Snake TeleBot WellMess Zebrocy 2021-07-25 · Medium svch0st · svch0st

Guide to Named Pipes and Hunting for Cobalt Strike Pipes

Cobalt Strike 2021-07-22 · Medium michaelkoczwara · Michael Koczwara

Cobalt Strike Hunting — simple PCAP and Beacon Analysis

Cobalt Strike 2021-07-19 · The DFIR Report · The DFIR Report

IcedID and Cobalt Strike vs Antivirus

Cobalt Strike IcedID 2021-07-14 · Kaspersky · Aseel Kayal, Mark Lechtik, Paul Rascagnères

LuminousMoth APT: Sweeping attacks for the chosen few

Cobalt Strike 2021-07-14 · MDSec · Chris Basnett

Investigating a Suspicious Service

Cobalt Strike 2021-07-14 · Google · Clement Lecigne, Google Threat Analysis Group, Maddie Stone

How We Protect Users From 0-Day Attacks (CVE-2021-21166, CVE-2021-30551, CVE-2021-33742, CVE-2021-1879)

Cobalt Strike 2021-07-13 · YouTube (Matt Soseman) · Matt Soseman

Solarwinds and SUNBURST attacks compromised my lab!

Cobalt Strike Raindrop SUNBURST TEARDROP 2021-07-09 · InfoSec Handlers Diary Blog · Brad Duncan

Hancitor tries XLL as initial malware file

Cobalt Strike Hancitor 2021-07-08 · Avast Decoded · Threat Intelligence Team

Decoding Cobalt Strike: Understanding Payloads

Cobalt Strike Empire Downloader 2021-07-08 · Recorded Future · Insikt Group

Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan Using Winnti and Other Tooling

Cobalt Strike Earth Lusca 2021-07-07 · Trustwave · Nikita Kazymirskyi, Rodel Mendrez

Diving Deeper Into the Kaseya VSA Attack: REvil Returns and Other Hackers Are Riding Their Coattails

Cobalt Strike REvil 2021-07-07 · McAfee · McAfee Labs

Ryuk Ransomware Now Targeting Webservers

Cobalt Strike Ryuk 2021-07-07 · Trend Micro · Gloria Chen, Jaromír Hořejší, Joseph C Chen, Kenney Lu

BIOPASS RAT: New Malware Sniffs Victims via Live Streaming

BIOPASS Cobalt Strike Derusbi 2021-07-06 · Twitter (@MBThreatIntel) · Malwarebytes Threat Intelligence

Tweet on a malspam campaign that is taking advantage of Kaseya VSA ransomware attack to drop CobaltStrike

Cobalt Strike 2021-07-05 · Trend Micro · Abraham Camba, Buddy Tancio, Catherine Loveria, Ryan Maglaque

Tracking Cobalt Strike: A Trend Micro Vision One Investigation

Cobalt Strike 2021-07-03 · Medium AK1001 · AK1001

Analyzing Cobalt Strike PowerShell Payload

Cobalt Strike 2021-07-02 · MalwareBookReports · muzi

Skip the Middleman: Dridex Document to Cobalt Strike

Cobalt Strike Dridex 2021-07-01 · The Record · Catalin Cimpanu

Mongolian certificate authority hacked eight times, compromised with malware

Cobalt Strike 2021-07-01 · Avast Decoded · Igor Morgenstern, Jan Vojtěšek, Luigino Camastra

Backdoored Client from Mongolian CA MonPass

Cobalt Strike FishMaster 2021-07-01 · Avast Decoded · Igor Morgenstern, Jan Vojtěšek, Luigino Camastra

Backdoored Client from Mongolian CA MonPass

Cobalt Strike Earth Lusca 2021-06-30 · Group-IB · Oleg Skulkin

REvil Twins Deep Dive into Prolific RaaS Affiliates' TTPs

Cobalt Strike REvil 2021-06-29 · Proofpoint · Daniel Blackford, Selena Larson

Cobalt Strike: Favorite Tool from APT to Crimeware

Cobalt Strike 2021-06-29 · Accenture · Accenture Security

HADES ransomware operators continue attacks

Cobalt Strike Hades MimiKatz 2021-06-28 · The DFIR Report · The DFIR Report

Hancitor Continues to Push Cobalt Strike

Cobalt Strike Hancitor 2021-06-22 · Twitter (@Cryptolaemus1) · Cryptolaemus, dao ming si, Kirk Sayre

Tweet on TA575, a Dridex affiliate delivering cobaltstrike (packed withe Cryptone) directly via the macro docs

Cobalt Strike Dridex 2021-06-22 · CrowdStrike · The Falcon Complete Team

Response When Minutes Matter: Falcon Complete Disrupts WIZARD SPIDER eCrime Operators

Cobalt Strike 2021-06-20 · The DFIR Report · The DFIR Report

From Word to Lateral Movement in 1 Hour

Cobalt Strike IcedID 2021-06-18 · SecurityScorecard · Ryan Sherstobitoff

SecurityScorecard Finds USAID Hack Much Larger Than Initially Thought

Cobalt Strike 2021-06-17 · Binary Defense · Brandon George

Analysis of Hancitor – When Boring Begets Beacon

Cobalt Strike Ficker Stealer Hancitor 2021-06-16 · · Національної поліції України · Національна поліція України

Cyberpolice exposes hacker group in spreading encryption virus and causing half a billion dollars in damage to foreign companies

Clop Cobalt Strike FlawedAmmyy 2021-06-16 · FireEye · Jared Wilson, Justin Moore, Mike Hunhoff, Nick Harbour, Robert Dean, Tyler McLellan

Smoking Out a DARKSIDE Affiliate's Supply Chain Software Compromise

Cobalt Strike SMOKEDHAM 2021-06-16 · Mandiant · Jared Wilson, Jordan Nuce, Justin Moore, Mike Hunhoff, Nick Harbour, Robert Dean, Tyler McLellan

Smoking Out a DARKSIDE Affiliate's Supply Chain Software Compromise

Cobalt Strike SMOKEDHAM 2021-06-16 · Mandiant · Jared Wilson, Jordan Nuce, Justin Moore, Mike Hunhoff, Nick Harbour, Robert Dean, Tyler McLellan

Smoking Out a DARKSIDE Affiliate's Supply Chain Software Compromise

DarkSide Cobalt Strike DarkSide SMOKEDHAM UNC2465 2021-06-15 · Secureworks · Counter Threat Unit ResearchTeam

Hades Ransomware Operators Use Distinctive Tactics and Infrastructure

Cobalt Strike Hades 2021-06-12 · Twitter (@AltShiftPrtScn) · Peter Mackenzie

A thread on RagnarLocker ransomware group's TTP seen in an Incident Response

Cobalt Strike RagnarLocker 2021-06-10 · Group-IB · Nikita Rostovcev

Big airline heist APT41 likely behind massive supply chain attack

Cobalt Strike 2021-06-09 · Twitter (@RedDrip7) · RedDrip7

Tweet on in the wild exploit of CVE-2021-26868 (according to @_clem1)

Cobalt Strike 2021-06-04 · Inky · Roger Kay

Colonial Pipeline Ransomware Hack Unleashes Flood of Related Phishing Attempts

Cobalt Strike 2021-06-04 · Twitter (@alex_lanstein) · Alex Lanstein

Tweet on UNC2652/NOBELIUM targeting IOS users exploiting CVE-2021-1879

Cobalt Strike 2021-06-02 · Medium CyCraft · CyCraft Technology Corp

China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware

Cobalt Strike ColdLock 2021-06-02 · Sophos · Sean Gallagher

AMSI bypasses remain tricks of the malware trade

Agent Tesla Cobalt Strike Meterpreter 2021-06-01 · SentinelOne · Juan Andrés Guerrero-Saade

NobleBaron | New Poisoned Installers Could Be Used In Supply Chain Attacks

Cobalt Strike 2021-06-01 · Microsoft · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center

(MSTIC)

New sophisticated email-based attack from NOBELIUM

Cobalt Strike 2021-06-01 · Department of Justice · Office of Public Affairs

Justice Department Announces Court-Authorized Seizure of Domain Names Used in Furtherance of Spear-Phishing Campaign Posing as U.S. Agency for International Development

Cobalt Strike 2021-06-01 · SANS · Jake Williams, Kevin Haley

A Contrarian View on SolarWinds

Cobalt Strike Raindrop SUNBURST TEARDROP 2021-05-29 · Twitter (@elisalem9) · Eli Salem

Tweet on obfuscation mechanism and extraction procedure of COBALTSTRIKE beacon module used by NOBELIUM/UNC2452

Cobalt Strike 2021-05-28 · CISA · US-CERT

Malware Analysis Report (AR21-148A): Cobalt Strike Beacon

Cobalt Strike 2021-05-28 · CISA · US-CERT

Alert (AA21-148A): Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs

Cobalt Strike 2021-05-28 · Microsoft · Microsoft Threat Intelligence Center (MSTIC)

Breaking down NOBELIUM’s latest early-stage toolset

BOOMBOX Cobalt Strike 2021-05-27 · Volexity · Damien Cash, Josh Grunzweig, Matthew Meltzer, Sean Koessel, Steven Adair, Thomas Lancaster

Suspected APT29 Operation Launches Election Fraud Themed Phishing Campaigns

Cobalt Strike 2021-05-26 · DeepInstinct · Ron Ben Yizhak

A Deep Dive into Packing Software CryptOne

Cobalt Strike Dridex Emotet Gozi ISFB Mailto QakBot SmokeLoader WastedLocker Zloader 2021-05-25 · Huntress Labs · Matthew Brennan

Cobalt Strikes Again: An Analysis of Obfuscated Malware

Cobalt Strike 2021-05-21 · blackarrow · Pablo Ambite

Leveraging Microsoft Teams to persist and cover up Cobalt Strike traffic

Cobalt Strike 2021-05-21 · · LAC · Yoshihiro Ishikawa

Targeted attack by 'Cobalt Strike loader' that exploits Microsoft's digital signature-Attacker group APT41

Cobalt Strike DUSTPAN 2021-05-19 · Intel 471 · Intel 471

Look how many cybercriminals love Cobalt Strike

BazarBackdoor Cobalt Strike Hancitor QakBot SmokeLoader SystemBC TrickBot 2021-05-19 · Medium Mehmet Ergene · Mehmet Ergene

Enterprise Scale Threat Hunting: Network Beacon Detection with Unsupervised ML and KQL — Part 2

Cobalt Strike 2021-05-18 · Sophos · Greg Iddon, John Shier, Mat Gangwer, Peter Mackenzie

The Active Adversary Playbook 2021

Cobalt Strike MimiKatz 2021-05-17 · Talos · Brad Garnett

Case Study: Incident Response is a relationship-driven business

Cobalt Strike 2021-05-16 · NCSC Ireland · NCSC Ireland

Ransomware Attack on Health Sector - UPDATE 2021-05-16

Cobalt Strike Conti 2021-05-14 · Blue Team Blog · Auth 0r

DarkSide Ransomware Operations – Preventions and Detections.

Cobalt Strike DarkSide 2021-05-14 · GuidePoint Security · Drew Schmitt

From ZLoader to DarkSide: A Ransomware Story

DarkSide Cobalt Strike Zloader 2021-05-13 · AWAKE · Kieran Evans

Catching the White Stork in Flight

Cobalt Strike MimiKatz RMS 2021-05-12 · The DFIR Report

Conti Ransomware

Cobalt Strike Conti IcedID 2021-05-12 · Medium Mehmet Ergene · Mehmet Ergene

Enterprise Scale Threat Hunting: Network Beacon Detection with Unsupervised ML and KQL — Part 1

Cobalt Strike 2021-05-11 · FireEye · Alyssa Rahman, Andrew Moore, Brendan McKeague, Jared Wilson, Jeremy Kennelly, Jordan Nuce, Kimberly Goody

Shining a Light on DARKSIDE Ransomware Operations

Cobalt Strike DarkSide 2021-05-11 · Mal-Eats · mal_eats

Campo, a New Attack Campaign Targeting Japan

AnchorDNS BazarBackdoor campoloader Cobalt Strike Phobos Snifula TrickBot Zloader 2021-05-10 · ZERO.BS · ZEROBS

Cobaltstrike-Beacons analyzed

Cobalt Strike 2021-05-10 · Mal-Eats · mal_eats

Overview of Campo, a new attack campaign targeting Japan

AnchorDNS BazarBackdoor Cobalt Strike ISFB Phobos TrickBot Zloader 2021-05-07 · Medium svch0st · svch0st

Stats from Hunting Cobalt Strike Beacons

Cobalt Strike 2021-05-07 · TEAMT5 · Aragorn Tseng, Charles Li

Mem2Img: Memory-Resident Malware Detection via Convolution Neural Network

Cobalt Strike PlugX Waterbear 2021-05-07 · SophosLabs Uncut · Rajesh Nataraj

New Lemon Duck variants exploiting Microsoft Exchange Server

CHINACHOPPER Cobalt Strike Lemon Duck 2021-05-07 · Cisco Talos · Andrew Windsor, Caitlin Huey, Edmund Brumaghin

Lemon Duck spreads its wings: Actors target Microsoft Exchange servers, incorporate new TTPs

CHINACHOPPER Cobalt Strike Lemon Duck 2021-05-05 · SophosLabs Uncut · Andrew Brandt, Gabor Szappanos, Peter Mackenzie, Vikas Singh

Intervention halts a ProxyLogon-enabled attack

Cobalt Strike 2021-05-05 · TRUESEC · Mattias Wåhlén

Are The Notorious Cyber Criminals Evil Corp actually Russian Spies?

Cobalt Strike Hades WastedLocker 2021-05-04 · Medium sergiusechel · Sergiu Sechel

Improving the network-based detection of Cobalt Strike C2 servers in the wild while reducing the risk of false positives

Cobalt Strike 2021-05-02 · The DFIR Report · The DFIR Report

Trickbot Brief: Creds and Beacons

Cobalt Strike TrickBot 2021-04-29 · NTT · Threat Detection NTT Ltd.

The Operations of Winnti group

Cobalt Strike ShadowPad Spyder Winnti Earth Lusca 2021-04-29 · FireEye · Justin Moore, Raymond Leong, Tyler McLellan

UNC2447 SOMBRAT and FIVEHANDS Ransomware: A Sophisticated Financial Threat

Cobalt Strike FiveHands HelloKitty 2021-04-27 · Trend Micro · Janus Agcaoili

Hello Ransomware Uses Updated China Chopper Web Shell, SharePoint Vulnerability

CHINACHOPPER Cobalt Strike 2021-04-27 · Trend Micro · Earle Earnshaw, Janus Agcaoili

Legitimate Tools Weaponized for Ransomware in 2021

Cobalt Strike MimiKatz 2021-04-26 · getrevue · Twitter (@80vul)

Hunting Cobalt Strike DNS redirectors by using ZoomEye

Cobalt Strike 2021-04-26 · nviso · Maxime Thiebaut

Anatomy of Cobalt Strike's DLL Stager

Cobalt Strike 2021-04-24 · · Non-offensive security · Non-offensive security team

Detect Cobalt Strike server through DNS protocol

Cobalt Strike 2021-04-23 · Twitter (@vikas891) · Vikas Singh

Tweet on DOPPEL SPIDER using Intensive/Multiple Injected Cobalt Strike Beacons with varied polling intervals

Cobalt Strike DoppelPaymer 2021-04-22 · Twitter (@AltShiftPrtScn) · Peter Mackenzie

Twwet On TTPs seen in IR used by DOPPEL SPIDER

Cobalt Strike DoppelPaymer 2021-04-21 · SophosLabs Uncut · Anand Aijan, Andrew Brandt, Markel Picado, Michael Wood, Sean Gallagher, Sivagnanam Gn, Suriya Natarajan

Nearly half of malware now use TLS to conceal communications

Agent Tesla Cobalt Strike Dridex SystemBC 2021-04-20 · Medium walmartglobaltech · Jason Reaves

CobaltStrike Stager Utilizing Floating Point Math

Cobalt Strike 2021-04-19 · Netresec · Erik Hjelmvik

Analysing a malware PCAP with IcedID and Cobalt Strike traffic

Cobalt Strike IcedID 2021-04-18 · YouTube (dist67) · Didier Stevens

Decoding Cobalt Strike Traffic

Cobalt Strike 2021-04-14 · InfoSec Handlers Diary Blog · Brad Duncan

April 2021 Forensic Quiz: Answers and Analysis

Anchor BazarBackdoor Cobalt Strike 2021-04-12 · Inde · Chris Campbell

A Different Kind of Zoombomb

Cobalt Strike 2021-04-09 · F-Secure · Giulio Ginesi, Riccardo Ancarani

Detecting Exposed Cobalt Strike DNS Redirectors

Cobalt Strike 2021-04-07 · Medium sixdub · Justin Warner

Using Kaitai Struct to Parse Cobalt Strike Beacon Configs

Cobalt Strike 2021-04-05 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

TrickBot Crews New CobaltStrike Loader

Cobalt Strike TrickBot 2021-04-01 · DomainTools · Joe Slowik

COVID-19 Phishing With a Side of Cobalt Strike

Cobalt Strike 2021-04-01 · Palo Alto Networks Unit 42 · Brad Duncan

Hancitor's Use of Cobalt Strike and a Noisy Network Ping Tool

Cobalt Strike Hancitor Moskalvzapoe 2021-03-31 · Red Canary · Red Canary

2021 Threat Detection Report

Shlayer Andromeda Cobalt Strike Dridex Emotet IcedID MimiKatz QakBot TrickBot 2021-03-30 · GuidePoint Security · Drew Schmitt

Yet Another Cobalt Strike Stager: GUID Edition

Cobalt Strike 2021-03-29 · The DFIR Report · The DFIR Report

Sodinokibi (aka REvil) Ransomware

Cobalt Strike IcedID REvil 2021-03-21 · Blackberry · Blackberry Research

2021 Threat Report

Bashlite FritzFrog IPStorm Mirai Tsunami elf.wellmess AppleJeus Dacls EvilQuest Manuscrypt Astaroth BazarBackdoor Cerber Cobalt Strike Emotet FinFisher RAT Kwampirs MimiKatz NjRAT Ryuk SmokeLoader TrickBot 2021-03-21 · YouTube (dist67) · Didier Stevens

Finding Metasploit & Cobalt Strike URLs

Cobalt Strike 2021-03-18 · PRODAFT Threat Intelligence · PRODAFT

SilverFish GroupThreat Actor Report

Cobalt Strike Dridex Koadic 2021-03-18 · DeepInstinct · Ben Gross

Cobalt Strike – Post-Exploitation Attackers Toolkit

Cobalt Strike 2021-03-16 · McAfee · McAfee ATR

Technical Analysis of Operation Diànxùn

Cobalt Strike 2021-03-16 · Elastic · Joe Desimone

Detecting Cobalt Strike with memory signatures

Cobalt Strike 2021-03-11 · Cyborg Security · Josh Campbell

You Don't Know the HAFNIUM of it...

CHINACHOPPER Cobalt Strike PowerCat 2021-03-11 · Qurium · Qurium

Myanmar – Multi-stage malware attack targets elected lawmakers

Cobalt Strike 2021-03-10 · Proofpoint · Dennis Schwarz, Matthew Mesa, Proofpoint Threat Research Team

NimzaLoader: TA800’s New Initial Access Malware

BazarNimrod Cobalt Strike 2021-03-09 · splunk · Security Research Team

Cloud Federated Credential Abuse & Cobalt Strike: Threat Research February 2021

Cobalt Strike 2021-03-08 · The DFIR Report · The DFIR Report

Bazar Drops the Anchor

Anchor BazarBackdoor Cobalt Strike 2021-03-08 · Youtube (SANS Digital Forensics and Incident Response) · Adam Pennington, Jen Burns, Katie Nickels

STAR Webcast: Making sense of SolarWinds through the lens of MITRE ATT&CK(R)

Cobalt Strike SUNBURST TEARDROP 2021-03-07 · InfoSec Handlers Diary Blog · Didier Stevens

PCAPs and Beacons

Cobalt Strike 2021-03-01 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

Nimar Loader

BazarBackdoor BazarNimrod Cobalt Strike 2021-03-01 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

Investigation into the state of Nim malware

BazarNimrod Cobalt Strike 2021-02-26 · CrowdStrike · Eric Loui, Sergei Frankoff

Hypervisor Jackpotting: CARBON SPIDER and SPRITE SPIDER Target ESXi Servers With Ransomware to Maximize Impact

DarkSide RansomEXX Griffon Carbanak Cobalt Strike DarkSide IcedID MimiKatz PyXie RansomEXX REvil 2021-02-25 · FireEye · Brendan McKeague, Bryce Abdo, Van Ta

So Unchill: Melting UNC2198 ICEDID to Ransomware Operations

MOUSEISLAND Cobalt Strike Egregor IcedID Maze SystemBC 2021-02-24 · Github (AmnestyTech) · Amnesty International

Overview of Ocean Lotus Samples used to target Vietnamese Human Rights Defenders

OceanLotus Cobalt Strike KerrDown 2021-02-24 · · VMWare Carbon Black · Takahiro Haruyama

Knock, knock, Neo. - Active C2 Discovery Using Protocol Emulation

Cobalt Strike 2021-02-23 · CrowdStrike · CrowdStrike

2021 Global Threat Report

RansomEXX Amadey Anchor Avaddon BazarBackdoor Clop Cobalt Strike Conti Cutwail DanaBot DarkSide DoppelPaymer Dridex Egregor Emotet Hakbit IcedID JSOutProx KerrDown LockBit Mailto Maze MedusaLocker Mespinoza Mount Locker NedDnLoader Nemty Pay2Key PlugX Pushdo PwndLocker PyXie QakBot Quasar RAT RagnarLocker Ragnarok RansomEXX REvil Ryuk Sekhmet ShadowPad SmokeLoader Snake SUNBURST SunCrypt TEARDROP TrickBot WastedLocker Winnti Zloader Evilnum OUTLAW SPIDER RIDDLE SPIDER SOLAR SPIDER VIKING SPIDER 2021-02-11 · Twitter (@TheDFIRReport) · The DFIR Report

Tweet on Hancitor Activity followed by cobaltsrike beacon

Cobalt Strike Hancitor 2021-02-09 · Securehat · Securehat

Extracting the Cobalt Strike Config from a TEARDROP Loader

Cobalt Strike TEARDROP 2021-02-09 · Cobalt Strike · Raphael Mudge

Learn Pipe Fitting for all of your Offense Projects

Cobalt Strike 2021-02-03 · InfoSec Handlers Diary Blog · Brad Duncan

Excel spreadsheets push SystemBC malware

Cobalt Strike SystemBC 2021-02-02 · Committee to Protect Journalists · Madeline Earp

How Vietnam-based hacking operation OceanLotus targets journalists

Cobalt Strike 2021-02-02 · Twitter (@TheDFIRReport) · The DFIR Report

Tweet on recent dridex post infection activity

Cobalt Strike Dridex 2021-02-02 · · CRONUP · Germán Fernández

De ataque con Malware a incidente de Ransomware

Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DanaBot Dharma Dridex Egregor Emotet Empire Downloader FriedEx GootKit IcedID MegaCortex Nemty Phorpiex PwndLocker PyXie QakBot RansomEXX REvil Ryuk SDBbot SmokeLoader TrickBot Zloader 2021-02-01 · pkb1s.github.io · Petros Koutroumpis

Relay Attacks via Cobalt Strike Beacons

Cobalt Strike 2021-02-01 · AhnLab · ASEC Analysis Team

BlueCrab ransomware, CobaltStrike hacking tool installed in corporate environment

Cobalt Strike REvil 2021-01-31 · The DFIR Report · The DFIR Report

Bazar, No Ryuk?

BazarBackdoor Cobalt Strike Ryuk 2021-01-28 · TrustedSec · Adam Chester

Tailoring Cobalt Strike on Target

Cobalt Strike 2021-01-28 · · AhnLab · ASEC Analysis Team

BlueCrab ransomware constantly trying to bypass detection

Cobalt Strike REvil 2021-01-26 · Twitter (@swisscom_csirt) · Swisscom CSIRT

Tweet on Cring Ransomware groups using customized Mimikatz sample followed by CobaltStrike and dropping Cring rasomware

Cobalt Strike Cring MimiKatz 2021-01-20 · Microsoft · Microsoft 365 Defender Research Team, Microsoft Cyber Defense Operations Center (CDOC), Microsoft Threat Intelligence Center (MSTIC)

Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop

Cobalt Strike SUNBURST TEARDROP 2021-01-18 · Symantec · Threat Hunter Team

Raindrop: New Malware Discovered in SolarWinds Investigation

Cobalt Strike Raindrop SUNBURST TEARDROP 2021-01-17 · Twitter (@AltShiftPrtScn) · Peter Mackenzie

Tweet on Conti Ransomware group exploiting FortiGate VPNs to drop in CobaltStrike loaders

Cobalt Strike Conti 2021-01-15 · Medium Dansec · Dan Lussier

Detecting Malicious C2 Activity -SpawnAs & SMB Lateral Movement in CobaltStrike

Cobalt Strike 2021-01-14 · PTSecurity · PT ESC Threat Intelligence

Higaisa or Winnti? APT41 backdoors, old and new

Cobalt Strike CROSSWALK FunnySwitch PlugX ShadowPad 2021-01-12 · BrightTALK (FireEye) · Ben Read, John Hultquist

UNC2452: What We Know So Far

Cobalt Strike SUNBURST TEARDROP 2021-01-12 · Fox-IT · Wouter Jansen

Abusing cloud services to fly under the radar

Cobalt Strike 2021-01-11 · The DFIR Report · The DFIR Report

Trickbot Still Alive and Well

Cobalt Strike TrickBot 2021-01-11 · SolarWinds · Sudhakar Ramakrishna

New Findings From Our Investigation of SUNBURST

Cobalt Strike SUNBURST TEARDROP 2021-01-10 · Medium walmartglobaltech · Jason Reaves

MAN1, Moskal, Hancitor and a side of Ransomware

Cobalt Strike Hancitor SendSafe VegaLocker Moskalvzapoe 2021-01-09 · Connor McGarr's Blog · Connor McGarr

Malware Development: Leveraging Beacon Object Files for Remote Process Injection via Thread Hijacking

Cobalt Strike 2021-01-09 · Marco Ramilli's Blog · Marco Ramilli

Command and Control Traffic Patterns

ostap LaZagne Agent Tesla Azorult Buer Cobalt Strike DanaBot DarkComet Dridex Emotet Formbook IcedID ISFB NetWire RC PlugX Quasar RAT SmokeLoader TrickBot 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 2021-01-05 · Trend Micro · Trend Micro Research

Earth Wendigo Injects JavaScript Backdoor to Service Worker for Mailbox Exfiltration

Cobalt Strike Earth Wendigo 2021-01-04 · Medium haggis-m · Michael Haag

Malleable C2 Profiles and You

Cobalt Strike 2021-01-01 · Talos · Talos Incident Response

Cobalt Strikes Out

Cobalt Strike 2021-01-01 · Talos · Talos Incident Response

Evicting Maze

Cobalt Strike Maze 2021-01-01 · SecureWorks

Threat Profile: GOLD DRAKE

Cobalt Strike Dridex FriedEx Koadic MimiKatz WastedLocker Evil Corp 2021-01-01 · Secureworks · SecureWorks

Threat Profile: GOLD WINTER

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

Threat Profile: GOLD WATERFALL

Cobalt Strike DarkSide GOLD WATERFALL 2021-01-01 · Mandiant · Mandiant

M-TRENDS 2021

Cobalt Strike SUNBURST 2021-01-01 · · Github (WBGlIl) · WBGlIl

A book on cobaltstrike

Cobalt Strike 2021-01-01 · Symantec · Symantec Threat Hunter Team

Supply Chain Attacks:Cyber Criminals Target the Weakest Link

Cobalt Strike Raindrop SUNBURST TEARDROP 2021-01-01 · AWAKE · Awake Security

Breaking the Ice: Detecting IcedID and Cobalt Strike Beacon with Network Detection and Response (NDR)

Cobalt Strike IcedID PhotoLoader 2020-12-26 · Medium grimminck · Stefan Grimminck

Spoofing JARM signatures. I am the Cobalt Strike server now!

Cobalt Strike 2020-12-22 · TRUESEC · Mattias Wåhlén

Collaboration between FIN7 and the RYUK group, a Truesec Investigation

Carbanak Cobalt Strike Ryuk 2020-12-21 · Fortinet · Udi Yavo

What We Have Learned So Far about the “Sunburst”/SolarWinds Hack

Cobalt Strike SUNBURST TEARDROP 2020-12-20 · Randhome · Etienne Maynier

Analyzing Cobalt Strike for Fun and Profit

Cobalt Strike 2020-12-15 · Github (sophos-cybersecurity) · Sophos Cyber Security Team

solarwinds-threathunt

Cobalt Strike SUNBURST 2020-12-15 · PICUS Security · Süleyman Özarslan

Tactics, Techniques, and Procedures (TTPs) Used in the SolarWinds Breach

Cobalt Strike SUNBURST 2020-12-14 · Palo Alto Networks Unit 42 · Unit 42

Threat Brief: SolarStorm and SUNBURST Customer Coverage

Cobalt Strike SUNBURST 2020-12-11 · Blackberry · BlackBerry Research and Intelligence team

MountLocker Ransomware-as-a-Service Offers Double Extortion Capabilities to Affiliates

Cobalt Strike Mount Locker 2020-12-10 · Intel 471 · Intel 471

No pandas, just people: The current state of China’s cybercrime underground

Anubis SpyNote AsyncRAT Cobalt Strike Ghost RAT NjRAT 2020-12-10 · Palo Alto Networks Unit 42 · Unit42

Threat Brief: FireEye Red Team Tool Breach

Cobalt Strike 2020-12-09 · Cisco · Caitlin Huey, David Liebenberg

Quarterly Report: Incident Response trends from Fall 2020

Cobalt Strike IcedID Maze RansomEXX Ryuk 2020-12-09 · InfoSec Handlers Diary Blog · Brad Duncan

Recent Qakbot (Qbot) activity

Cobalt Strike QakBot 2020-12-09 · FireEye · Mitchell Clarke, Tom Hall

It's not FINished The Evolving Maturity in Ransomware Operations (SLIDES)

Cobalt Strike DoppelPaymer QakBot REvil 2020-12-08 · Cobalt Strike · Raphael Mudge

A Red Teamer Plays with JARM

Cobalt Strike 2020-12-02 · Red Canary · twitter (@redcanary)

Tweet on increased #Qbot activity delivering Cobalt Strike & #Egregor ransomware

Cobalt Strike Egregor QakBot 2020-12-01 · mez0.cc · mez0

Cobalt Strike PowerShell Execution

Cobalt Strike 2020-12-01 · 360.cn · jindanlong

Hunting Beacons

Cobalt Strike 2020-11-30 · Microsoft · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC)

Threat actor (BISMUTH) leverages coin miner techniques to stay under the radar – here's how to spot them

Cobalt Strike 2020-11-30 · FireEye · Mitchell Clarke, Tom Hall

It's not FINished The Evolving Maturity in Ransomware Operations

Cobalt Strike DoppelPaymer MimiKatz QakBot REvil 2020-11-27 · · Macnica · Hiroshi Takeuchi

Analyzing Organizational Invasion Ransom Incidents Using Dtrack

Cobalt Strike Dtrack 2020-11-26 · Cybereason · Cybereason Nocturnus, Lior Rochberger

Cybereason vs. Egregor Ransomware

Cobalt Strike Egregor IcedID ISFB QakBot 2020-11-25 · SentinelOne · Jim Walter

Egregor RaaS Continues the Chaos with Cobalt Strike and Rclone

Cobalt Strike Egregor 2020-11-20 · · 360 netlab · JiaYu

Blackrota, a highly obfuscated backdoor developed by Go

Cobalt Strike 2020-11-20 · F-Secure Labs · Riccardo Ancarani

Detecting Cobalt Strike Default Modules via Named Pipe Analysis

Cobalt Strike 2020-11-20 · ZDNet · Catalin Cimpanu

The malware that usually installs ransomware and you need to remove right away

Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DoppelPaymer Dridex Egregor Emotet FriedEx MegaCortex Phorpiex PwndLocker QakBot Ryuk SDBbot TrickBot Zloader 2020-11-17 · cyble · Cyble

OceanLotus Continues With Its Cyber Espionage Operations

Cobalt Strike Meterpreter 2020-11-17 · Salesforce Engineering · John Althouse

Easily Identify Malicious Servers on the Internet with JARM

Cobalt Strike TrickBot 2020-11-15 · Trustnet · Michael Wainshtain

From virus alert to PowerShell Encrypted Loader

Cobalt Strike 2020-11-09 · Bleeping Computer · Ionut Ilascu

Fake Microsoft Teams updates lead to Cobalt Strike deployment

Cobalt Strike DoppelPaymer NjRAT Predator The Thief Zloader 2020-11-06 · Cobalt Strike · Raphael Mudge

Cobalt Strike 4.2 – Everything but the kitchen sink

Cobalt Strike 2020-11-06 · Advanced Intelligence · Vitali Kremez

Anatomy of Attack: Inside BazarBackdoor to Ryuk Ransomware "one" Group via Cobalt Strike

BazarBackdoor Cobalt Strike Ryuk 2020-11-06 · Volexity · Steven Adair, Thomas Lancaster, Volexity Threat Research

OceanLotus: Extending Cyber Espionage Operations Through Fake Websites

Cobalt Strike KerrDown APT32 2020-11-06 · Palo Alto Networks Unit 42 · CRYPSIS, Drew Schmitt, Ryan Tracey

Indicators of Compromise related to Cobaltstrike, PyXie Lite, Vatet and Defray777

Cobalt Strike PyXie RansomEXX 2020-11-05 · The DFIR Report · The DFIR Report

Ryuk Speed Run, 2 Hours to Ransom

BazarBackdoor Cobalt Strike Ryuk 2020-11-05 · Twitter (@ffforward) · TheAnalyst

Tweet on Zloader infection leads to Cobaltstrike Installation and deployment of RYUK

Cobalt Strike Ryuk Zloader 2020-11-04 · VMRay · Giovanni Vigna

Trick or Threat: Ryuk ransomware targets the health care industry

BazarBackdoor Cobalt Strike Ryuk TrickBot 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 2020-11-03 · InfoSec

Handlers Diary Blog · Renato Marinho

Attackers Exploiting WebLogic Servers via CVE-2020-14882 to install Cobalt Strike

Cobalt Strike 2020-10-30 · Github (ThreatConnect-Inc) · ThreatConnect

UNC 1878 Indicators from Threatconnect

BazarBackdoor Cobalt Strike Ryuk 2020-10-30 · YouTube (Kaspersky Tech) · Kris McConkey

Around the world in 80 days 4.2bn packets

Cobalt Strike Derusbi HyperBro Poison Ivy ShadowPad Winnti 2020-10-29 · Github (Swisscom) · Swisscom CSIRT

List of CobaltStrike C2's used by RYUK

Cobalt Strike 2020-10-29 · Red Canary · The Red Canary Team

A Bazar start: How one hospital thwarted a Ryuk ransomware outbreak

Cobalt Strike Ryuk TrickBot 2020-10-29 · RiskIQ · RiskIQ

Ryuk Ransomware: Extensive Attack Infrastructure Revealed

Cobalt Strike Ryuk 2020-10-28 · FireEye · Douglas Bienstock, Jeremy Kennelly, Joshua Shilko, Kimberly Goody, Steve Elovitz

Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser

BazarBackdoor Cobalt Strike Ryuk UNC1878 2020-10-27 · Sophos Managed Threat Response (MTR) · Greg Iddon

MTR Casebook: An active adversary caught in the act

Cobalt Strike 2020-10-18 · The DFIR Report · The DFIR Report

Ryuk in 5 Hours

BazarBackdoor Cobalt Strike Ryuk 2020-10-14 · Sophos · Sean Gallagher

They’re back: inside a new Ryuk ransomware attack

Cobalt Strike Ryuk SystemBC 2020-10-14 · RiskIQ · Jon Gross, Steve Ginty

A Well-Marked Trail: Journeying through OceanLotus's Infrastructure

Cobalt Strike 2020-10-12 · Advanced Intelligence · Roman Marshanski, Vitali Kremez

"Front Door" into BazarBackdoor: Stealthy Cybercrime Weapon

BazarBackdoor Cobalt Strike Ryuk 2020-10-11 · Github (StrangerealIntel) · StrangerealIntel

Chimera, APT19 under the radar ?

Cobalt Strike Meterpreter 2020-10-08 · The DFIR Report · The DFIR Report

Ryuk’s Return

BazarBackdoor Cobalt Strike Ryuk 2020-10-08 · Bayerischer Rundfunk · Ann-Kathrin Wetter, Hakan Tanriverdi, Kai Biermann, Max Zierer, Thi Do Nguyen

There is no safe place

Cobalt Strike 2020-10-02 · Health Sector Cybersecurity Coordination Center (HC3) · Health Sector Cybersecurity Coordination Center (HC3)

Report 202010021600: Recent Bazarloader Use in Ransomware Campaigns

BazarBackdoor Cobalt Strike Ryuk TrickBot 2020-10-01 · US-CERT · US-CERT

Alert (AA20-275A): Potential for China Cyber Response to Heightened U.S.-China Tensions

CHINACHOPPER Cobalt Strike Empire Downloader MimiKatz Poison Ivy 2020-10-01 · Wired · Andy Greenberg

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

Cobalt Strike Meterpreter 2020-09-29 · CrowdStrike · Kareem Hamdan, Lucas Miller

Getting the Bacon from the Beacon

Cobalt Strike 2020-09-29 · Github (Apr4h) · Apra

CobaltStrikeScan

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

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

Cobalt Strike Meterpreter 2020-09-22 · vmware · Omar Elgebaly, Takahiro Haruyama

Detecting Threats in Real-time With Active C2 Information

Agent.BTZ Cobalt Strike Dacls NetWire RC PoshC2 Winnti 2020-09-21 · Cisco Talos · Joe Marshall, JON MUNSHAW, Nick Mavis

The art and science of detecting Cobalt Strike

Cobalt Strike 2020-09-18 · Trend Micro · Trend Micro

U.S. Justice Department Charges APT41 Hackers over Global Cyberattacks

Cobalt Strike ColdLock SharPyShell 2020-09-03 · · Viettel Cybersecurity · vuonglvm

APT32 deobfuscation arsenal: Deobfuscating một vài loại Obfucation Toolkit của APT32 (Phần 2)

Cobalt Strike 2020-09-01 · Cisco Talos · Caitlin Huey, David Liebenberg

Quarterly Report: Incident Response trends in Summer 2020

Cobalt Strike LockBit Mailto Maze Ryuk 2020-08-31 · The DFIR Report · The DFIR Report

NetWalker Ransomware in 1 Hour

Cobalt Strike Mailto MimiKatz 2020-08-20 · · Seebug Paper · Malayke

Use ZoomEye to track multiple Redteam C&C post-penetration attack frameworks

Cobalt Strike Empire Downloader PoshC2 2020-08-19 · · TEAMT5 · TeamT5

調查局 08/19 公布中國對台灣政府機關駭侵事件說明

Cobalt Strike Waterbear 2020-08-14 · Twitter (@VK_intel) · Vitali Kremez

Tweet on Zloader infection leading to Cobaltstrike Installation

Cobalt Strike Zloader 2020-08-06 · Wired · Andy Greenberg

Chinese Hackers Have Pillaged Taiwan's Semiconductor Industry

Cobalt Strike MimiKatz Winnti Red Charon 2020-08-04 · BlackHat · Chung-Kuan Chen, Inndy Lin, Shang-De Jiang

Operation Chimera - APT Operation Targets Semiconductor Vendors

Cobalt Strike MimiKatz Winnti Red Charon 2020-07-29 · Kaspersky Labs · GReAT

APT trends report Q2 2020

PhantomLance Dacls Penquin Turla elf.wellmess AppleJeus Dacls AcidBox Cobalt Strike Dacls EternalPetya Godlike12 Olympic Destroyer PlugX shadowhammer ShadowPad Sinowal VHD Ransomware Volgmer WellMess X-Agent XTunnel 2020-07-26 · Shells.System blog · Askar

In-Memory shellcode decoding to evade AVs/EDRs

Cobalt Strike 2020-07-22 · On the Hunt · Newton Paul

Analysing Fileless Malware: Cobalt Strike Beacon

Cobalt Strike 2020-07-21 · Malwarebytes · Hossein Jazi, Jérôme Segura

Chinese APT group targets India and Hong Kong using new variant of MgBot malware

KSREMOTE Cobalt Strike MgBot Evasive Panda 2020-07-07 · MWLab · Ladislav Bačo

Cobalt Strike stagers used by FIN6

Cobalt Strike 2020-07-01 · Contextis · Lampros Noutsos, Oliver Fay

DLL Search Order Hijacking

Cobalt Strike PlugX 2020-06-23 · Symantec · Critical Attack Discovery and Intelligence Team

Sodinokibi: Ransomware Attackers also Scanning for PoS Software, Leveraging Cobalt Strike

Cobalt Strike REvil 2020-06-23 · NCC Group · Michael Sandee, Nikolaos Pantazopoulos, Stefano Antenucci

WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group
Cobalt Strike ISFB WastedLocker 2020-06-22 · Sentinel LABS · Jason Reaves, Joshua Platt
Inside a TrickBot Cobalt Strike Attack Server
Cobalt Strike TrickBot 2020-06-22 · Talos Intelligence · Asheer Malhotra
IndigoDrop spreads via military-themed lures to deliver Cobalt Strike
Cobalt Strike IndigoDrop 2020-06-19 · Zscaler · Atinderpal Singh, Nirmal Singh, Sahil Antil
Targeted Attack Leverages India-China Border Dispute to Lure Victims
Cobalt Strike 2020-06-19 · Youtube (Raphael Mudge) · Raphael Mudge
Beacon Object Files - Luser Demo
Cobalt Strike 2020-06-18 · Australian Cyber Security Centre · Australian Cyber Security Centre (ACSC)
Advisory 2020-008: Copy-Paste Compromises –tactics, techniques and procedures used to target multiple Australian networks
TwoFace Cobalt Strike Empire Downloader 2020-06-17 · Malwarebytes · Hossein Jazi, Jérôme Segura
Multi-stage APT attack drops Cobalt Strike using Malleable C2 feature
Cobalt Strike 2020-06-15 · NCC Group · Exploit Development Group
Striking Back at Retired Cobalt Strike: A look at a legacy vulnerability
Cobalt Strike 2020-06-09 · Github (Sentinel-One) · Gal Kristal
CobaltStrikeParser
Cobalt Strike 2020-05-14 · Lab52 · Dex
The energy reserves in the Eastern Mediterranean Sea and a malicious campaign of APT10 against Turkey
Cobalt Strike HTran MimiKatz PlugX Quasar RAT 2020-05-11 · SentinelOne · Gal Kristal
The Anatomy of an APT Attack and CobaltStrike Beacon’s Encoded Configuration
Cobalt Strike 2020-04-24 · The DFIR Report · The DFIR Report
Ursnif via LOLbins
Cobalt Strike LOLSnif TeamSpy 2020-04-16 · Medium CyCraft · CyCraft Technology Corp
Taiwan High-Tech Ecosystem Targeted by Foreign APT Group: Digital Skeleton Key Bypasses Security Measures
Cobalt Strike MimiKatz Red Charon 2020-04-02 · Darktrace · Max Heinemeyer
Catching APT41 exploiting a zero-day vulnerability
Cobalt Strike 2020-03-26 · VMWare Carbon Black · Scott Knight
The Dukes of Moscow
Cobalt Strike LiteDuke MiniDuke OnionDuke PolyglotDuke PowerDuke 2020-03-25 · Wilbur Security · JW
Trickbot to Ryuk in Two Hours
Cobalt Strike Ryuk TrickBot 2020-03-25 · FireEye · Christopher Glyer, Dan Perez, Sarah Jones, Steve Miller
This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits
Speculoos Cobalt Strike 2020-03-22 · Malware and Stuff · Andreas Klopsch
Mustang Panda joins the COVID-19 bandwagon
Cobalt Strike 2020-03-20 · RECON INFOSEC · Luke Rusten
Analysis Of Exploitation: CVE-2020-10189 (exploited by APT41)
Cobalt Strike 2020-03-04 · Cobalt Strike · Raphael Mudge
Cobalt Strike joins Core Impact at HelpSystems, LLC
Cobalt Strike 2020-03-04 · CrowdStrike · CrowdStrike
2020 CrowdStrike Global Threat Report

MESSAGETAP More_eggs 8.t Dropper Anchor BabyShark BadNews Clop Cobalt Strike CobInt Cobra Carbon System Cutwail DanaBot Dharma DoppelDridex DoppelPaymer Dridex Emotet FlawedAmmyy FriedEx Gandcrab Get2 IcedID ISFB KerrDown LightNeuron LockerGoga Maze MECHANICAL Necurs Nokki Outlook Backdoor Phobos Predator The Thief QakBot REvil RobinHood Ryuk SDBbot Skipper SmokeLoader TerraRecon TerraStealer TerraTV TinyLoader TrickBot Vidar Winnti ANTHROPOID SPIDER APT23 APT31 APT39 APT40 BlackTech BuhTrap Charming Kitten CLOCKWORK SPIDER DOPPEL SPIDER FIN7 Gamaredon Group GOBLIN PANDA MONTY SPIDER MUSTANG PANDA NARWHAL SPIDER NOCTURNAL SPIDER PINCHY SPIDER SALTY SPIDER SCULLY SPIDER SMOKY SPIDER Thrip VENOM SPIDER VICEROY TIGER 2020-03-03 · PWC UK · PWC UK

Cyber Threats 2019:A Year in Retrospect

KevDroid MESSAGETAP magecart AndroMut Cobalt Strike CobInt Crimson RAT DNSpionage Dridex Dtrack Emotet FlawedAmmyy FlawedGrace FriedEx Gandcrab Get2 GlobeImposter Grateful POS ISFB Kazuar LockerGoga Nokki QakBot Ramnit REvil Rifdoor RokRAT Ryuk shadowhammer ShadowPad Shifu Skipper StoneDrill Stuxnet TrickBot Winnti ZeroCleare APT41 MUSTANG PANDA Sea Turtle 2020-02-20 · McAfee · Christiaan Beek, Darren Fitzpatrick, Eamonn Ryan

CSI: Evidence Indicators for Targeted Ransomware Attacks – Part II

Cobalt Strike LockerGoga Maze MegaCortex 2020-02-19 · FireEye · FireEye

M-Trends 2020

Cobalt Strike Grateful POS LockerGoga QakBot TrickBot 2020-02-18 · Trend Micro · Cedric Pernet, Daniel Lunghi, Jamz Yaneza, Kenney Lu

Uncovering DRBControl: Inside the Cyberespionage Campaign Targeting Gambling Operations

Cobalt Strike HyperBro PlugX Trochilus RAT Operation DRBControl 2020-02-18 · Cisco Talos · Vanja Svajcer

Building a bypass with MSBuild

Cobalt Strike GRUNT MimiKatz 2020-02-13 · Qianxin · Qi Anxin Threat Intelligence Center

APT Report 2019

Chrysaor Exodus Dacls VPNFilter DNSRat Griffon KopiLuwak More_eggs SQLRat AppleJeus BONDUPDATER Agent.BTZ Anchor AndroMut AppleJeus BOOSTWRITE Brambul Carbanak Cobalt Strike Dacls DistTrack DNSpionage Dtrack ELECTRICFISH FlawedAmmyy FlawedGrace Get2 Grateful POS HOPLIGHT Imminent Monitor RAT jason Joanap KerrDown KEYMARBLE Lambert LightNeuron LoJax MiniDuke PolyglotDuke PowerRatankba Rising Sun SDBbot ServHelper Snatch Stuxnet TinyMet tRat TrickBot Volgmer X-Agent Zebrocy 2020-01-01 · Secureworks · SecureWorks

BRONZE MOHAWK

AIRBREAK scanbox BLACKCOFFEE CHINACHOPPER Cobalt Strike Derusbi homefry murkytop SeDll APT40 2020-01-01 · Secureworks · SecureWorks

BRONZE PRESIDENT

CHINACHOPPER Cobalt Strike PlugX MUSTANG PANDA 2020-01-01 · Secureworks · SecureWorks

BRONZE RIVERSIDE

Anel ChChes Cobalt Strike PlugX Poison Ivy Quasar RAT RedLeaves APT10 2020-01-01 · Secureworks · SecureWorks

GOLD DUPONT

Cobalt Strike Defray PyXie GOLD DUPONT 2020-01-01 · Secureworks · SecureWorks

GOLD KINGSWOOD

More_eggs ATMSpitter Cobalt Strike CobInt MimiKatz 2020-01-01 · Secureworks · SecureWorks

GOLD NIAGARA

Bateleur Griffon Carbanak Cobalt Strike DRIFTPIN TinyMet FIN7 2020-01-01 · Secureworks · SecureWorks

TIN WOODLAWN

Cobalt Strike KerrDown MimiKatz PHOREAL RatSnif Remy SOUNDBITE APT32 2020-01-01 · Secureworks · SecureWorks

GOLD KINGSWOOD

More_eggs ATMSpitter Cobalt Strike CobInt MimiKatz Cobalt 2019-12-12 · FireEye · Chi-en Shen, Oleg Bondarenko

Cyber Threat Landscape in Japan – Revealing Threat in the Shadow

Cerberus TSCookie Cobalt Strike Dtrack Emotet Formbook IcedID Icefog IRONHALO Loki Password Stealer (PWS) PandaBanker PLEAD POISONPLUG TrickBot BlackTech 2019-12-05 · Raphael Mudge

Cobalt Strike 4.0 – Bring Your Own Weaponization

Cobalt Strike 2019-12-05 · · Github (blackorbird) · blackorbird

APT32 Report

Cobalt Strike 2019-11-29 · Deloitte · Thomas Thomasen

Cyber Threat Intelligence & Incident Response

Cobalt Strike 2019-11-19 · FireEye · Kelli Vanderlee, Nalani Fraser

Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions

MESSAGETAP TSCookie ACEHASH CHINACHOPPER Cobalt Strike Derusbi Empire Downloader Ghost RAT HIGHNOON HTran MimiKatz NetWire RC POISONPLUG Poison Ivy pupy Quasar RAT ZXShell 2019-11-05 · tccontre Blog · tccontre

CobaltStrike - beacon.dll : Your No Ordinary MZ Header

Cobalt Strike 2019-09-23 · MITRE · MITRE ATT&CK

APT41

Derusbi MESSAGETAP Winnti ASPXSpy BLACKCOFFEE CHINACHOPPER Cobalt Strike Derusbi Empire Downloader Ghost RAT MimiKatz NjRAT PlugX ShadowPad Winnti ZXShell APT41 2019-09-22 · Check Point Research · Check Point Research

Rancor: The Year of The Phish

8.t Dropper Cobalt Strike 2019-06-13 · Sekoia · sekoia

Hunting and detecting Cobalt Strike

Cobalt Strike 2019-06-04 · Bitdefender · Bitdefender

An APT Blueprint: Gaining New Visibility into Financial Threats

More_eggs Cobalt Strike 2019-05-08 · Verizon Communications Inc. · Verizon Communications Inc.

2019 Data Breach Investigations Report

BlackEnergy Cobalt Strike DanaBot Gandcrab GreyEnergy Mirai Olympic Destroyer SamSam 2019-04-24 · Weixin · Tencent

"Sea Lotus" APT organization's attack techniques against China in the first quarter of 2019 revealed

Cobalt Strike SOUNDBITE 2019-04-15 · PenTestPartners · Neil Lines

Cobalt Strike. Walkthrough for Red Teamers

Cobalt Strike 2019-04-01 · · Macnica Networks · Macnica Networks

OceanLotus Attack on Southeast Asian Automotive Industry

CACTUSTORCH Cobalt Strike 2019-04-01 · · Macnica Networks · Macnica Networks

Trends in Cyber Espionage Targeting Japan 2nd Half of 2018

Anel Cobalt Strike Datper PLEAD Quasar RAT RedLeaves taidoor Zebrocy 2019-03-24 · One Night in Norfolk · Kevin Perlow

JEShell: An OceanLotus (APT32) Backdoor

Cobalt Strike KerrDown 2019-02-27 · Morphisec · Alon Groisman, Michael Gorelik

New Global Cyber Attack on Point of Sale Sytem

Cobalt Strike 2019-02-26 · Fox-IT · Fox IT

Identifying Cobalt Strike team servers in the wild

Cobalt Strike 2018-11-19 · FireEye · Andrew Thompson, Ben Withnell, Jonathan Leathery, Matthew Dunwoody, Michael Matonis, Nick Carr

Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign

Cobalt Strike 2018-11-18 · Stranded on Pylos Blog · Joe

CozyBear – In from the Cold?

Cobalt Strike APT29 2018-10-01 · FireEye · Katie Nickels, Regina Elwell

ATT&CKing FIN7

Bateleur BELLHOP Griffon ANTAK POWERPIPE POWERSOURCE HALFBAKED BABYMETAL Carbanak

Cobalt Strike DNSMessenger DRIFTPIN PILLOWMINT SocksBot 2018-10-01 · · Macnica Networks · Macnica Networks

Trends in cyber espionage (targeted attacks) targeting Japan | First half of 2018

Anel Cobalt Strike Datper FlawedAmmyy Quasar RAT RedLeaves taidoor Winnti xxmm 2018-10-01 · Group-IB · Group-IB

Hi-Tech Crime Trends 2018

BackSwap Cobalt Strike Cutlet Meterpreter 2018-08-03 · JPCERT/CC · Takuya Endo, Yukako Uchida

Volatility Plugin for Detecting Cobalt Strike Beacon

Cobalt Strike 2018-07-31 · Github (JPCERTCC) · JPCERT/CC

Scanner for CobaltStrike

Cobalt Strike 2018-05-21 · · LAC · Yoshihiro Ishikawa

Confirmed new attacks by APT attacker group menuPass (APT10)

Cobalt Strike 2017-06-06 · FireEye · Ian Ahl

Privileges and Credentials: Phished at the Request of Counsel

Cobalt Strike 2017-06-06 · Mandiant · Ian Ahl

Privileges and Credentials: Phished at the Request of Counsel

Cobalt Strike APT19 2017-04-26 · Youtube (Kaspersky) · Kaspersky

China's Evolving Cyber Operations: A Look into APT19's Shift in Tactics

Cobalt Strike APT19 2016-10-11 · Symantec · Symantec Security Response

Odinaff: New Trojan used in high level financial attacks

Cobalt Strike KLRD MimiKatz Odinaff 2012-01-01 · Cobalt Strike · Cobalt Strike

Cobalt Strike Website

Cobalt Strike

▶ [TLP:WHITE] win_cobalt_strike_auto (20251219 | Detects win.cobalt_strike.)
