# MimiKatz (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:21:44 UTC

Varonis summarizes Mimikatz as an open-source application that allows users to view and save authentication credentials like Kerberos tickets. Benjamin Delpy continues to lead Mimikatz developments, so the toolset works with the current release of Windows and includes the most up-to-date attacks.

Attackers commonly use Mimikatz to steal credentials and escalate privileges: in most cases, endpoint protection software and anti-virus systems will detect and delete it. Conversely, pentesters use Mimikatz to detect and exploit vulnerabilities in your networks so you can fix them.

2025-07-21 · Kaspersky Labs ·
The SOC files: Rumble in the jungle or APT41's new target in Africa
Cobalt Strike MimiKatz 2025-07-03 · Rapid7 · Rapid7
Scattered Spider: Rapid7 Insights, Observations, and Recommendations
MimiKatz POORTRY 2025-05-19 · The DFIR Report · 0xtornado, pcsc0ut, Randy Pargman
Another Confluence Bites the Dust: Falling to ELPACO-team Ransomware
Mimic Ransomware MimiKatz 2025-03-20 · Cisco Talos · Asheer Malhotra, Brandon White, Jungsoo An, Vitor Ventura
UAT-5918 targets critical infrastructure entities in Taiwan
ShortLeash LaZagne JuicyPotato Meterpreter MimiKatz ShortLeash UAT-5918 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 2024-10-30 · Palo Alto Networks Unit 42 · Unit 42
Jumpy Pisces Engages in Play Ransomware
Dtrack MimiKatz PLAY Sliver 2024-09-22 · BushidoToken · BushidoToken
The Russian APT Tool Matrix
MimiKatz reGeorg 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 2024-05-23 · Palo Alto Networks Unit 42 · Daniel Frank, Lior Rochberger
Operation Diplomatic Specter: An Active Chinese Cyberespionage Campaign Leverages Rare Tool Set to Target Governmental Entities in the Middle East, Africa and Asia
Agent Racoon CHINACHOPPER Ghost RAT JuicyPotato MimiKatz Ntospy PlugX SweetSpecter TunnelSpecter CL-STA-0043 2023-10-26 · · ANSSI · ANSSI
Attack Campaigns of APT28 since 2021
CredoMap DriveOcean Empire Downloader Graphite MimiKatz Mocky LNK reGeorg 2023-10-10 · Symantec · Threat Hunter Team
Grayling: Previously Unseen Threat Actor Targets Multiple Organizations in Taiwan
Cobalt Strike Havoc MimiKatz Grayling 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 2023-09-07 · CISA · CISA

Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475

Meterpreter MimiKatz 2023-08-22 · · AhnLab · ASEC Analysis Team

Analyzing the new attack activity of the Andariel group

Andardoor MimiKatz QuiteRAT Tiger RAT Volgmer 2023-08-22 · AhnLab · Sanseo

Analysis of APT Attack Cases Targeting Web Services of Korean Corporations

Ladon Meterpreter MimiKatz Dalbit 2023-04-12 · Kaspersky Labs · Seongsu Park

Following the Lazarus group by tracking DeathNote campaign

Bankshot BLINDINGCAN ForestTiger LambLoad LPEClient MimiKatz NedDnLoader Racket Downloader Volgmer 2023-04-03 · Mandiant · Eduardo Mattos, JASON DEYALSINGH, Nick Richard, NICK SMITH, Tyler McLellan

ALPHV Ransomware Affiliate Targets Vulnerable Backup Installations to Gain Initial Access

LaZagne BlackCat MimiKatz 2023-03-16 · Palo Alto Networks Unit 42 · Frank Lee, Scott Roland

Bee-Ware of Trigona, An Emerging Ransomware Strain

Cryakl MimiKatz Trigona 2023-02-13 · AhnLab · kingkimgim

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

Godzilla Webshell ASPXSpy BlueShell CHINACHOPPER Cobalt Strike Ladon MimiKatz Dalbit 2023-01-23 · Kroll · Elio Biasiotto, Stephen Green

Black Basta – Technical Analysis

Black Basta Cobalt Strike MimiKatz QakBot 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 2022-11-09 · Trend Micro · Hara Hiroaki, Ted Lee

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

Cobalt Strike MimiKatz Earth Longzhi 2022-10-18 · Intrinsec · CERT Intrinsec, Intrinsec

APT27 – One Year To Exfiltrate Them All: Intrusion In-Depth Analysis

HyperBro MimiKatz 2022-10-11 · · AhnLab · ASEC Analysis Team

From Exchange Server vulnerability to ransomware infection in just 7 days

LockBit MimiKatz 2022-09-29 · Symantec · Threat Hunter Team

Witchetty: Group Uses Updated Toolset in Attacks on Governments in Middle East

CHINACHOPPER Lookback MimiKatz Witchetty 2022-09-13 · Symantec · Threat Hunter Team

New Wave of Espionage Activity Targets Asian Governments

MimiKatz PlugX Quasar RAT ShadowPad Trochilus RAT 2022-09-08 · Cisco Talos · Asheer Malhotra, Jung soo An, Vitor Ventura

Lazarus and the tale of three RATs

MagicRAT MimiKatz VSingle YamaBot 2022-09-07 · Blackberry · Anuj Soni, Ryan Chapman

The Curious Case of “Monti” Ransomware: A Real-World Doppelganger

Conti MimiKatz Veeam Dumper 2022-09-06 · ESET Research · Thibaut Passilly

Worok: The big picture

MimiKatz PNGLoad reGeorg ShadowPad Worok 2022-09-01 · Trend Micro · Trend Micro

Ransomware Spotlight Black Basta

Black Basta Cobalt Strike MimiKatz QakBot 2022-08-25 · Microsoft · Microsoft 365 Defender Research Team, Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC)

MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations

MimiKatz 2022-08-18 · Sophos · Sean Gallagher

Cookie stealing: the new perimeter bypass

Cobalt Strike Meterpreter MimiKatz Phoenix Keylogger Quasar RAT 2022-08-15 · SentinelOne · Vikram Navali

Detecting a Rogue Domain Controller – DCShadow Attack

MimiKatz TrickBot 2022-07-27 · ReversingLabs · Joseph Edwards

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

Cobalt Strike MimiKatz 2022-07-26 · Microsoft · Microsoft 365 Defender Research Team

Malicious IIS extensions quietly open persistent backdoors into servers

CHINACHOPPER MimiKatz 2022-07-26 · Mandiant · Daniel Kapellmann Zafra, Jay Christiansen, Keith Lunden, Ken Proska, Thibault van Geluwe de Berlaere

Mandiant Red Team Emulates FIN11 Tactics To Control Operational Technology Servers

Clop Industroyer MimiKatz Triton 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 2022-06-30 · Kaspersky · Pierre Delcher

The SessionManager IIS backdoor: a possibly overlooked GELSEMIUM artefact

MimiKatz Owlproxy SessionManager 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 · · Infinitum IT · infinitum IT

Charming Kitten (APT35)

LaZagne DownPaper MimiKatz pupy 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 2022-06-01 · CISA · CISA, Department of the Treasury (Treasury), FBI, FINCEN

Joint Cybersecurity Advisory (Product ID AA22-152A): Karakurt Data Extortion Group

MimiKatz 2022-06-01 · CISA · CISA, Department of the Treasury (Treasury), FBI, FINCEN

Alert (AA22-152A): Karakurt Data Extortion Group

MimiKatz 2022-06-01 · Elastic · Andrew Pease, Daniel Stepanic, Derek Ditch, Salim Bitam, Seth Goodwin

CUBA Ransomware Campaign Analysis

Cobalt Strike Cuba Meterpreter MimiKatz SystemBC 2022-05-17 · Trend Micro · Trend Micro Research

Ransomware Spotlight: RansomEXX

LaZagne Cobalt Strike IcedID MimiKatz PyXie RansomEXX TrickBot 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 2022-04-19 · Varonis · Nadav Ovadia

Hive Ransomware Analysis

Cobalt Strike Hive MimiKatz 2022-04-08 · Infinitum Labs · Arda Büyükkaya

Threat Spotlight: Conti Ransomware Group Behind the Karakurt Hacking Team

Cobalt Strike MimiKatz 2022-04-07 · splunk · Splunk Threat Research Team

You Bet Your Lsass: Hunting LSASS Access

Cobalt Strike MimiKatz 2022-04-05 · Symantec · Threat Hunter Team

Cicada: Chinese APT Group Widens Targeting in Recent Espionage Activity

MimiKatz SodaMaster 2022-04-05 · Symantec · Threat Hunter Team

Cicada: Chinese APT Group Widens Targeting in Recent Espionage Activity

MimiKatz APT10 2022-03-25 · Dragos · Conor McLaren, Dragos

How Dragos Activity Groups Obtain Initial Access into Industrial Environments

MimiKatz 2022-03-09 · BreachQuest · Bernard Silvestrini, Marco Figueroa, Napoleon Bing

The Conti Leaks | Insight into a Ransomware Unicorn

Cobalt Strike MimiKatz TrickBot 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 2022-02-03 · Symantec · Symantec Threat Hunter Team

Antlion: Chinese APT Uses Custom Backdoor to Target Financial Institutions in Taiwan

MimiKatz xPack Antlion 2021-12-14 · Symantec · Threat Hunter Team

Espionage Campaign Targets Telecoms Organizations across Middle East and Asia

MimiKatz 2021-12-06 · Microsoft · Microsoft Digital Security Unit (DSU), Microsoft Threat Intelligence Center (MSTIC)

NICKEL targeting government organizations across Latin America and Europe

MimiKatz 2021-12-06 · Notice of Pleadings · Microsoft

Complaint filed by Microsoft against NICKEL/APT15

MimiKatz 2021-12-06 · PARAFLARE · Melanie Ninovic

Attack Lifecycle Detection of an Operational Technology Breach

MimiKatz 2021-11-18 · Microsoft · Microsoft Digital Security Unit (DSU), Microsoft Threat Intelligence Center (MSTIC)

Iranian targeting of IT sector on the rise

MimiKatz ShellClient RAT Cuboid Sandstorm 2021-11-05 · Twitter (@inversecos) · inversecos

TTPs used by Pysa Ransonmware group

Mespinoza MimiKatz 2021-11-01 · Accenture · Curt Wilson, Heather Larrieu, Katrina Hill

Diving into double extortion campaigns

Cobalt Strike MimiKatz 2021-10-25 · CrowdStrike · Falcon OverWatch Team

OverWatch Elite In Action: Prompt Call Escalation Proves Vital to Containing Attack

MimiKatz 2021-10-15 · Volatility Labs · Volatility Labs

Memory Forensics R&D Illustrated: Detecting Mimikatz's Skeleton Key Attack

MimiKatz 2021-10-11 · Accenture · Accenture Cyber Threat Intelligence

Moving Left of the Ransomware Boom

REvil Cobalt Strike MimiKatz RagnarLocker REvil 2021-09-24 · Trend Micro · Warren Sto.Tomas

Examining the Cring Ransomware Techniques

Cobalt Strike Cring MimiKatz 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 2021-09-14 · McAfee · Christiaan Beek

Operation 'Harvest': A Deep Dive into a Long-term Campaign

MimiKatz PlugX Winnti 2021-09-09 · Symantec · Threat Hunter Team

Grayfly: Chinese Threat Actor Uses Newly-discovered Sidewalk Malware

CROSSWALK MimiKatz SideWalk 2021-08-30 · · Qianxin · Red Raindrop Team

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

Cobalt Strike MimiKatz 2021-08-23 · FBI · FBI

Indicators of Compromise Associated with OnePercent Group Ransomware

Cobalt Strike MimiKatz 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 2021-08-10 · FireEye · Israel Research Team, U.S. Threat Intel Team

UNC215: Spotlight on a Chinese Espionage Campaign in Israel

HyperBro HyperSSL MimiKatz 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 2021-07-20 · Secureworks · Counter Threat Unit ResearchTeam

Ongoing Campaign Leveraging Exchange Vulnerability Potentially Linked to Iran

CHINACHOPPER MimiKatz RGDoor 2021-06-29 · Accenture · Accenture Security

HADES ransomware operators continue attacks

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

The Active Adversary Playbook 2021

Cobalt Strike MimiKatz 2021-05-13 · AWAKE · Kieran Evans

Catching the White Stork in Flight

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

Legitimate Tools Weaponized for Ransomware in 2021

Cobalt Strike MimiKatz 2021-03-31 · Red Canary · Red Canary

2021 Threat Detection Report

Shlayer Andromeda Cobalt Strike Dridex Emotet IcedID MimiKatz QakBot TrickBot 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 2021-03-19 · Bundesamt für Sicherheit in der Informationstechnik · CERT-Bund

Microsoft Exchange Schwachstellen Detektion und Reaktion (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)

CHINACHOPPER MimiKatz 2021-03-11 · DEVO · Fran Gomez

Detection and Investigation Using Devo: HAFNIUM 0-day Exploits on Microsoft Exchange Service

CHINACHOPPER MimiKatz 2021-03-10 · ESET Research · Mathieu Tartare, Matthieu Faou, Thomas Dupuy

Exchange servers under siege from at least 10 APT groups

Microcin MimiKatz PlugX Winnti APT27 APT41 Calypso Tick ToddyCat Tonto Team Vicious Panda 2021-03-08 · Symantec · Threat Hunter Team

How Symantec Stops Microsoft Exchange Server Attacks

CHINACHOPPER MimiKatz 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 2021-01-29 · Trend Micro · Trend Micro

Chopper ASPX web shell used in targeted attack

CHINACHOPPER MimiKatz 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 2021-01-18 · · Bundesamt für Verfassungsschutz · Bundesamt für Verfassungsschutz

BfV Cyber-Brief Nr. 01/2021 : Vorgehensweise von APT31

MimiKatz 2021-01-15 · Swisscom · Markus Neis

Cracking a Soft Cell is Harder Than You Think

Ghost RAT MimiKatz PlugX Poison Ivy Trochilus RAT 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 FRANKLIN

Grateful POS Meterpreter MimiKatz RemCom FIN6 2021-01-01 · Secureworks · SecureWorks

Threat Profile: GOLD BURLAP

Empire Downloader Mespinoza MimiKatz GOLD BURLAP 2020-12-21 · · SlideShare (yurikamuraki5) · Yurika Kakiuchi

Active Directory 侵害と推奨対策

MimiKatz 2020-12-15 · HvS-Consulting AG · HvS-Consulting AG

Greetings from Lazarus: Anatomy of a cyber espionage campaign

BLINDINGCAN MimiKatz Lazarus Group 2020-12-15 · HvS-Consulting AG · HvS-Consulting AG

Greetings from Lazarus Anatomy of a cyber espionage campaign

BLINDINGCAN HTTP(S) uploader MimiKatz 2020-12-09 · Avast Decoded · Igor Morgenstern, Luigino Camastra

APT Group Targeting Governmental Agencies in East Asia

LaZagne Albaniiutas HyperBro MimiKatz PolPo Tmanger TaskMasters 2020-12-04 · Theta · Hamish Krebs

Snakes & Ladders: the offensive use of Python on Windows

MimiKatz 2020-11-30 · FireEye · Mitchell Clarke, Tom Hall

It's not FINished The Evolving Maturity in Ransomware Operations

Cobalt Strike DoppelPaymer MimiKatz QakBot REvil 2020-11-30 · Yoroi · Antonio Pirozzi, Luca Mella, Luigi Martire

Shadows From The Past Threaten Italian Enterprises

Rekoobe LaZagne Responder MimiKatz win.rekoobe 2020-11-27 · PTSecurity · Alexey Vishnyakov, Denis Goydenko

Investigation with a twist: an accidental APT attack and averted data destruction

TwoFace CHINACHOPPER HyperBro MegaCortex MimiKatz 2020-10-23 · F-Secure Labs · Guillaume Couchard, Qimin Wang, Thiam Loong Siew

Catching Lazarus: Threat Intelligence to Real Detection Logic - Part Two

MimiKatz 2020-10-20 · F-Secure · F-Secure Consulting

Incident Readiness: Preparing a proactive response to attacks

MimiKatz 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 2020-09-17 · FBI · FBI

FBI PIN Number 20200917-001: IRGC-Associated Cyber Operations Against US Company Networks

MimiKatz Nanocore RAT 2020-08-31 · The DFIR Report · The DFIR Report

NetWalker Ransomware in 1 Hour

Cobalt Strike Mailto MimiKatz 2020-08-10 · ZDNet · Catalin Cimpanu

FBI says an Iranian hacking group is attacking F5 networking devices

MimiKatz 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 2020-06-24 · Counter Threat Unit ResearchTeam

BRONZE VINEWOOD Targets Supply Chains

MimiKatz Trochilus RAT APT31 2020-06-18 · · Bundesamt für Verfassungsschutz · Bundesamt für Verfassungsschutz

BfV Cyber-BriefNr. 01/2020 - Hinweis auf aktuelle Angriffskampagne

Ketrican MimiKatz 2020-05-28 · Kaspersky Labs · Vyacheslav Kopeytsev

Steganography in targeted attacks on industrial enterprises

MimiKatz 2020-05-27 · FBI · FBI

Alert Number MI-000148-MW: APT Actors Exploiting Fortinet Vulnerabilities to Gain Access for Malicious Activity

MimiKatz 2020-05-21 · ESET Research · Martin Smolár, Mathieu Tartare

No “Game over” for the Winnti Group

ACEHASH HTran MimiKatz PipeMon 2020-05-21 · Bitdefender · Bogdan Rusu, Liviu Arsene

Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia

MimiKatz Remexi 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 2020-05-14 · Avast Decoded · Luigino Camastra

APT Group Planted Backdoors Targeting High Profile Networks in Central Asia

BYEBY Ghost RAT Microcin MimiKatz Vicious Panda 2020-05-07 · REDTEAM.PL · Adam Ziaja

Sodinokibi / REvil ransomware

Maze MimiKatz REvil 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 2020-03-05 · Microsoft · Microsoft Threat Protection Intelligence Team

Human-operated ransomware attacks: A preventable disaster

Dharma DoppelPaymer Dridex EternalPetya Gandcrab Hermes LockerGoga MegaCortex MimiKatz REvil RobinHood Ryuk SamSam TrickBot WannaCryptor PARINACOTA 2020-02-21 · ADEO DFIR · ADEO DFIR

APT10 Threat Analysis Report

CHINACHOPPER HTran MimiKatz PlugX Quasar RAT 2020-02-19 · Lexfo · Lexfo

The Lazarus Constellation A study on North Korean malware

FastCash AppleJeus BADCALL Bankshot Brambul Dtrack Duuzer DYEPACK ELECTRICFISH HARDRAIN Hermes HOPLIGHT Joanap KEYMARBLE Kimsuky MimiKatz MyDoom NACHOCHEESE NavRAT PowerRatankba RokRAT Sierra(Alfa,Bravo, ...) Volgmer WannaCryptor 2020-02-18 · Cisco Talos · Vanja Svajcer

Building a bypass with MSBuild

Cobalt Strike GRUNT MimiKatz 2020-02-02 · uf0 Blog · Matteo Malvica

Uncovering Mimikatz ‘msv’ and collecting credentials through PyKD

MimiKatz 2020-01-01 · Secureworks · SecureWorks

BRONZE ATLAS

Speculoos Winnti ACEHASH CCleaner Backdoor CHINACHOPPER Empire Downloader HTran MimiKatz PlugX Winnti APT41 2020-01-01 · Secureworks · SecureWorks

BRONZE VINEWOOD

MimiKatz Trochilus RAT APT31 2020-01-01 · Secureworks · SecureWorks

COBALT HICKMAN

MimiKatz Remexi APT39 2020-01-01 · Secureworks · SecureWorks

GOLD DRAKE

Dridex Empire Downloader FriedEx Koadic MimiKatz 2020-01-01 · Secureworks · SecureWorks

GOLD KINGSWOOD

More_eggs ATMSpitter Cobalt Strike CobInt MimiKatz 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 · Microsoft · Microsoft Threat Intelligence Center

GALLIUM: Targeting global telecom

CHINACHOPPER Ghost RAT HTran MimiKatz Poison Ivy GALLIUM 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 2019-09-23 · 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 2019-06-25 · Cybereason · Cybereason Nocturnus

OPERATION SOFT CELL: A WORLDWIDE CAMPAIGN AGAINST TELECOMMUNICATIONS PROVIDERS

CHINACHOPPER HTran MimiKatz Poison Ivy Operation Soft Cell 2019-05-10 · XPN Blog · Adam Chester

Exploring Mimikatz - Part 1 - WDigest

MimiKatz 2019-04-04 · CrowdStrike · Harlan Carvey

Mimikatz in the Wild: Bypassing Signature-Based Detections Using the “AK47 of Cyber”

MimiKatz 2019-03-27 · Symantec · Critical Attack Discovery and Intelligence Team

Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.

DarkComet MimiKatz Nanocore RAT NetWire RC pupy Quasar RAT Remcos StoneDrill TURNEDUP APT33 2019-01-04 · Github (gentilkiwi) · Benjamin Delpy

mimikatz Repository

MimiKatz 2018-07-25 · Symantec · Critical Attack Discovery and Intelligence Team, Network Protection Security Labs

Leafminer: New Espionage Campaigns Targeting Middle Eastern Regions

Imecab MimiKatz Sorgu RASPITE 2018-02-28 · Symantec · Critical Attack Discovery and Intelligence Team

Chafer: Latest Attacks Reveal Heightened Ambitions

MimiKatz Remexi 2018-02-15 · Secureworks · Counter Threat Unit ResearchTeam

SamSam Ransomware Campaigns

MimiKatz reGeorg SamSam BOSS SPIDER 2017-12-04 · RSA · Jack Wesley Riley

The Shadows of Ghosts Inside the response of a unique Carbanak intrusion

GOTROJ MimiKatz 2017-11-09 · Wired · Andy Greenberg

He Perfected a Password-Hacking Tool—Then the Russians Came Calling

MimiKatz 2017-05-31 · MITRE · MITRE ATT&CK

Sandworm Team

CyclopsBlink Exaramel BlackEnergy EternalPetya Exaramel GreyEnergy KillDisk MimiKatz Olympic Destroyer Sandworm 2017-05-31 · MITRE · MITRE ATT&CK

PittyTiger

Enfal Ghost RAT MimiKatz Poison Ivy APT24 2017-02-27 · Symantec · A L Johnson

Shamoon: Multi-staged destructive attacks limited to specific targets

DistTrack MimiKatz Rocket Kitten 2016-10-11 · Symantec · Symantec Security Response

Odinaff: New Trojan used in high level financial attacks

Cobalt Strike KLRD MimiKatz Odinaff 2016-03-30 · Secureworks · Counter Threat Unit ResearchTeam

Ransomware Deployed by Adversary with Established Foothold

MimiKatz reGeorg SamSam BOSS SPIDER 2011-04-28 · Gentil Kiwi

Un observateur d’événements aveugle…

MimiKatz

- ▶ [TLP:WHITE] win_mimikatz_auto (20251219 | Detects win.mimikatz.)
- ▶ [TLP:WHITE] win_mimikatz_w0 (20171230 | mimikatz)

---