CHINACHOPPER (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:40:39 UTC

CHINACHOPPER

Actor(s): APT41, EMISSARY PANDA, GALLIUM, HAFNIUM, Hurricane Panda, Leviathan

---

a simple code injection webshell that executes Microsoft .NET code within HTTP POST commands. This allows the shell to upload and download files, execute applications with web server account permissions, list directory contents, access Active Directory, access databases, and any other action allowed by the .NET runtime.

References

2025-03-24 · SYGNIA ·
Weaver Ant, the Web Shell Whisperer: Tracking a Live China-nexus Operation
CHINACHOPPER reGeorg

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

2024-04-19 · · Spiegel Online · Christoph Giesen, Hakan Tanriverdi, Simon Hage
VW-Konzern wurde jahrelang ausspioniert – von China?
CHINACHOPPER PlugX

2023-06-16 · Palo Alto Networks: Cortex Threat Research · Lior Rochberger
Through the Cortex XDR Lens: Uncovering a New Activity Group Targeting Governments in the Middle East and Africa
CHINACHOPPER Ladon Yasso CL-STA-0043

2023-02-13 · AhnLab · kingkimgim
Dalbit (m00nlight): Chinese Hacker Group’s APT Attack Campaign
Godzilla Webshell ASPXSpy BlueShell CHINACHOPPER Cobalt Strike Ladon MimiKatz Dalbit

2022-12-24 · Medium (@DCSO_CyTec) · Denis Szadkowski, Hendrik Baecker, Jiro Minier, Johann Aydinbas
APT41 — The spy who failed to encrypt me

CHINACHOPPER

2022-09-29 · Symantec · Threat Hunter Team

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

CHINACHOPPER Lookback MimiKatz Witchetty

2022-07-26 · Microsoft · Microsoft 365 Defender Research Team

Malicious IIS extensions quietly open persistent backdoors into servers

CHINACHOPPER MimiKatz

2022-07-18 · Palo Alto Networks Unit 42 · Unit 42

Iron Taurus

CHINACHOPPER Ghost RAT Wonknu ZXShell APT27

2022-06-15 · Security Joes · Charles Lomboni, Felipe Duarte, Venkat Rajgor

Backdoor via XFF: Mysterious Threat Actor Under Radar

CHINACHOPPER

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

2021-11-03 · Cisco Talos · Caitlin Huey, Chetan Raghuprasad, Vanja Svajcer

Microsoft Exchange vulnerabilities exploited once again for ransomware, this time with Babuk

Babuk CHINACHOPPER

2021-09-03 · FireEye · Adrian Sanchez Hernandez, Alex Pennino, Andrew Rector, Brendan McKeague, Govand Sinjari, Harris Ansari, John Wolfram, Joshua Goddard, Yash Gupta

PST, Want a Shell? ProxyShell Exploiting Microsoft Exchange Servers

CHINACHOPPER HTran

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

2021-06-10 · ESET Research · Adam Burgher

BackdoorDiplomacy: Upgrading from Quarian to Turian

CHINACHOPPER DoublePulsar EternalRocks turian BackdoorDiplomacy

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

2021-05-06 · Trend Micro · Arianne Dela Cruz, Cris Tomboc, Jayson Chong, Nikki Madayag, Sean Torre
Proxylogon: A Coinminer, a Ransomware, and a Botnet Join the Party
BlackKingdom Ransomware CHINACHOPPER Lemon Duck Prometei

2021-05-05 · Symantec · Threat Hunter Team
Multi-Factor Authentication: Headache for Cyber Actors Inspires New Attack Techniques
CHINACHOPPER

2021-04-27 · Trend Micro · Janus Agcaoili
Hello Ransomware Uses Updated China Chopper Web Shell, SharePoint Vulnerability
CHINACHOPPER Cobalt Strike

2021-04-16 · Trend Micro · Nitesh Surana
Could the Microsoft Exchange breach be stopped?
CHINACHOPPER

2021-04-15 · Palo Alto Networks Unit 42 · Robert Falcone
Actor Exploits Microsoft Exchange Server Vulnerabilities, Cortex XDR Blocks Harvesting of Credentials
CHINACHOPPER

2021-03-26 · Imperva · Daniel Johnston
Imperva Observes Hive of Activity Following Hafnium Microsoft Exchange Disclosures
CHINACHOPPER

2021-03-25 · Microsoft · Tom McElroy
Web Shell Threat Hunting with Azure Sentinel
CHINACHOPPER

2021-03-25 · Microsoft · Microsoft 365 Defender Threat Intelligence Team
Analyzing attacks taking advantage of the Exchange Server vulnerabilities
CHINACHOPPER

2021-03-21 · Twitter (@CyberRaiju) · Jai Minton
Twitter Thread with analysis of .NET China Chopper
CHINACHOPPER

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

2021-03-15 · Trustwave · Joshua Deacon
HAFNIUM, China Chopper and ASP.NET Runtime

CHINACHOPPER

2021-03-11 · DEVO · Fran Gomez

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

CHINACHOPPER MimiKatz

2021-03-11 · Cyborg Security · Josh Campbell

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

CHINACHOPPER Cobalt Strike PowerCat

2021-03-11 · Palo Alto Networks Unit 42 · Unit 42

Microsoft Exchange Server Attack Timeline

CHINACHOPPER

2021-03-10 · DomainTools · Joe Slowik

Examining Exchange Exploitation and its Lessons for Defenders

CHINACHOPPER

2021-03-10 · PICUS Security · Süleyman Özarslan

Tactics, Techniques, and Procedures (TTPs) Used by HAFNIUM to Target Microsoft Exchange Servers

CHINACHOPPER

2021-03-10 · Lemon's InfoSec Ramblings · Josh Lemon

Microsoft Exchange & the HAFNIUM Threat Actor

CHINACHOPPER

2021-03-09 · YouTube (John Hammond) · John Hammond

HAFNIUM - Post-Exploitation Analysis from Microsoft Exchange

CHINACHOPPER

2021-03-09 · Red Canary · Brian Donohue, Katie Nickels, Tony Lambert

Microsoft Exchange server exploitation: how to detect, mitigate, and stay calm

CHINACHOPPER

2021-03-09 · PRAETORIAN · Anthony Weems, Dallas Kaman, Michael Weber

Reproducing the Microsoft Exchange Proxylogon Exploit Chain

CHINACHOPPER

2021-03-09 · Palo Alto Networks Unit 42 · Unit 42

Remediation Steps for the Microsoft Exchange Server Vulnerabilities

CHINACHOPPER

2021-03-08 · Palo Alto Networks Unit 42 · Jeff White

Analyzing Attacks Against Microsoft Exchange Server With China Chopper Webshells

CHINACHOPPER

2021-03-08 · Symantec · Threat Hunter Team
How Symantec Stops Microsoft Exchange Server Attacks
CHINACHOPPER MimiKatz

2021-03-07 · TRUESEC · Rasmus Grönlund
Tracking Microsoft Exchange Zero-Day ProxyLogon and HAFNIUM
CHINACHOPPER

2021-03-05 · Huntress Labs · Huntress Labs
Operation Exchange Marauder
CHINACHOPPER

2021-03-05 · Wired · Andy Greenberg
Chinese Hacking Spree Hit an ‘Astronomical’ Number of Victims
CHINACHOPPER

2021-03-04 · Huntress Labs · Huntress Labs
Operation Exchange Marauder
CHINACHOPPER

2021-03-04 · FireEye · Andrew Thompson, Chris DiGiamo, Matt Bromiley, Robert Wallace
Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities
CHINACHOPPER HAFNIUM

2021-03-04 · CrowdStrike · The Falcon Complete Team
Falcon Complete Stops Microsoft Exchange Server Zero-Day Exploits
CHINACHOPPER HAFNIUM

2021-03-03 · MITRE · MITRE ATT&CK
HAFNIUM
CHINACHOPPER HAFNIUM

2021-03-03 · Huntress Labs · Huntress Labs
Mass exploitation of on-prem Exchange servers :(
CHINACHOPPER HAFNIUM

2021-03-03 · Huntress Labs · John Hammond
Rapid Response: Mass Exploitation of On-Prem Exchange Servers
CHINACHOPPER HAFNIUM

2021-03-02 · Twitter (@ESETresearch) · ESET Research
Tweet on Exchange RCE
CHINACHOPPER HAFNIUM

2021-03-02 · Rapid7 Labs · Andrew Christian

Rapid7's InsightIDR Enables Detection And Response to Microsoft Exchange Zero-Day

CHINACHOPPER HAFNIUM

2021-03-02 · Volexity · Josh Grunzweig, Matthew Meltzer, Sean Koessel, Steven Adair, Thomas Lancaster

Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities

CHINACHOPPER HAFNIUM

2021-03-02 · Microsoft · Microsoft 365 Defender Threat Intelligence Team, Microsoft 365 Security, Microsoft Threat Intelligence Center (MSTIC)

HAFNIUM targeting Exchange Servers with 0-day exploits

CHINACHOPPER HAFNIUM

2021-01-29 · Trend Micro · Trend Micro

Chopper ASPX web shell used in targeted attack

CHINACHOPPER MimiKatz

2021-01-01 · DomainTools · Joe Slowik

Conceptualizing a Continuum of Cyber Threat Attribution

CHINACHOPPER SUNBURST

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

2020-10-01 · 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

2020-09-15 · US-CERT · US-CERT

Alert (AA20-259A): Iran-Based Threat Actor Exploits VPN Vulnerabilities

CHINACHOPPER Fox Kitten

2020-09-15 · US-CERT · US-CERT

Malware Analysis Report (AR20-259A): Iranian Web Shells

CHINACHOPPER

2020-07-21 · Department of Justice · Department of Justice

Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research

CHINACHOPPER BRONZE SPRING

2020-02-21 · ADEO DFIR · ADEO DFIR

APT10 Threat Analysis Report

CHINACHOPPER HTran MimiKatz PlugX Quasar RAT

2020-01-01 · FireEye · Mandiant, Mitchell Clarke, Tom Hall

Mandiant IR Grab Bag of Attacker Activity

TwoFace CHINACHOPPER HyperBro HyperSSL

2020-01-01 · Secureworks · SecureWorks

BRONZE UNION

9002 RAT CHINACHOPPER Enfal Ghost RAT HttpBrowser HyperBro owaauth PlugX Poison Ivy ZXShell APT27

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 PRESIDENT

CHINACHOPPER Cobalt Strike PlugX MUSTANG PANDA

2020-01-01 · Secureworks · SecureWorks

BRONZE MOHAWK

AIRBREAK scanbox BLACKCOFFEE CHINACHOPPER Cobalt Strike Derusbi homefry murkytop SeDll APT40

2020-01-01 · Secureworks · SecureWorks

BRONZE EXPRESS

9002 RAT CHINACHOPPER IsSpace NewCT PlugX smac APT26

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

2019-08-27 · Cisco Talos · Paul Rascagnères, Vanja Svajcer

China Chopper still active 9 years later

CHINACHOPPER

2019-08-19 · FireEye · Alex Pennino, Matt Bromiley
GAME OVER: Detecting and Stopping an APT41 Operation
ACEHASH CHINACHOPPER HIGHNOON

2019-06-25 · Cybereason · Cybereason Nocturnus
OPERATION SOFT CELL: A WORLDWIDE CAMPAIGN AGAINST TELECOMMUNICATIONS PROVIDERS
CHINACHOPPER HTran MimiKatz Poison Ivy Operation Soft Cell

2019-05-28 · Palo Alto Networks Unit 42 · Robert Falcone, Tom Lancaster
Emissary Panda Attacks Middle East Government Sharepoint Servers
CHINACHOPPER HyperSSL

2019-01-01 · MITRE · MITRE ATT&CK
Tool description: China Chopper
CHINACHOPPER

2018-03-16 · FireEye · FireEye
Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries
badflick BLACKCOFFEE CHINACHOPPER homefry murkytop SeDll APT40

2017-12-20 · CrowdStrike · Adam Kozy
An End to “Smash-and-Grab” and a Move to More Targeted Approaches
CHINACHOPPER

2013-08-07 · FireEye · Dennis Hanzlik, Ian Ahl, Tony Lee
Breaking Down the China Chopper Web Shell - Part I
CHINACHOPPER

There is no Yara-Signature yet.
