# HyperBro (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 12:58:07 UTC

HyperBro is a RAT that has been observed to target primarily within the gambling industries, though it has been spotted in other places as well. The malware typically consists of 3 or more components: a) a genuine loader typically with a signed certification b) a malicious DLL loader loaded from the former component via DLL hijacking c) an encrypted and compressed blob that decrypts to a PE-based payload which has its C2 information hardcoded within.

2023-07-18 · Mandiant ·
Stealth Mode: Chinese Cyber Espionage Actors Continue to Evolve Tactics to Avoid Detection
BPFDoor SALTWATER SEASPY SideWalk ZuoRAT Daxin HyperBro HyperSSL Waterbear 2022-10-18 · Intrinsec · CERT Intrinsec, Intrinsec
APT27 – One Year To Exfiltrate Them All: Intrusion In-Depth Analysis
HyperBro MimiKatz 2022-08-12 · Trend Micro · Daniel Lunghi, Jaromír Hořejší
Iron Tiger Compromises Chat Application Mimi, Targets Windows, Mac, and Linux Users
Rshell HyperBro Earth Berberoka 2022-08-12 · Trend Micro · Daniel Lunghi, Jaromír Hořejší
Iron Tiger Compromises Chat Application Mimi, Targets Windows, Mac, and Linux Users (IOCs)
HyperBro 2022-08-12 · Sekoia · Threat & Detection Research Team
LuckyMouse uses a backdoored Electron app to target MacOS
HyperBro 2022-02-07 · Cyware · Cyware
APT27 Group Targets German Organizations with HyperBro
HyperBro 2022-01-26 · BleepingComputer · Sergiu Gatlan
German govt warns of APT27 hackers backdooring business networks
HyperBro 2022-01-26 · Bundesamt für Verfassungsschutz · Bundesamt für Verfassungsschutz
Current cyber attack campaign against German business enterprises by APT27
HyperBro 2021-08-10 · FireEye · Israel Research Team, U.S. Threat Intel Team
UNC215: Spotlight on a Chinese Espionage Campaign in Israel
HyperBro HyperSSL MimiKatz 2021-04-29 · ESET Research · Andy Garth, Daniel Chromek, Matthieu Faou, Robert Lipovsky, Tony Anscombe
ESET Industry Report on Government: Targeted but not alone
Exaramel Crutch Exaramel HyperBro HyperSSL InvisiMole XDSpy 2021-04-09 · Trend Micro · Daniel Lunghi, Kenney Lu
Iron Tiger APT Updates Toolkit With Evolved SysUpdate Malware
HyperBro HyperSSL APT27 2020-12-10 · ESET Research · Mathieu Tartare
Operation StealthyTrident: corporate software under attack
HyperBro PlugX Tmanger TA428 2020-12-10 · ESET Research · Mathieu Tartare
Operation StealthyTrident: corporate software under attack
HyperBro PlugX ShadowPad Tmanger 2020-12-09 · Avast Decoded · Igor Morgenstern, Luigino Camastra

APT Group Targeting Governmental Agencies in East Asia

LaZagne Albaniiutas HyperBro MimiKatz PolPo Tmanger TaskMasters 2020-12-09 · Avast Decoded · Igor Morgenstern, Luigino Camastra

APT Group Targeting Governmental Agencies in East Asia

Albaniiutas HyperBro PlugX Tmanger TA428 2020-12-09 · Avast Decoded · Igor Morgenstern, Luigino Camastra

APT Group Targeting Governmental Agencies in East Asia

Albaniiutas HyperBro PlugX PolPo Tmanger 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 2020-10-30 · YouTube (Kaspersky Tech) · Kris McConkey

Around the world in 80 days 4.2bn packets

Cobalt Strike Derusbi HyperBro Poison Ivy ShadowPad Winnti 2020-09-30 · Team Cymru · Jacomo Piccolini, James Shank

Pandamic: Emissary Pandas in the Middle East

HyperBro HyperSSL 2020-06-03 · Trend Micro · Daniel Lunghi

How to perform long term monitoring of careless threat actors

BBSRAT HyperBro Trochilus RAT 2020-03-25 · Team Cymru · Team Cymru

How the Iranian Cyber Security Agency Detects Emissary Panda Malware

HyperBro 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 2020-02-17 · Talent-Jump Technologies · Theo Chen, Zero Chen

CLAMBLING - A New Backdoor Base On Dropbox

HyperBro PlugX 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 2019-06-13 · ae CERT · ae CERT

Advanced Notification of Cyber Threats against Family of Malware Giving Remote Access to Computers

HyperBro HyperSSL 2019-02-27 · Secureworks · CTU Research Team

A Peek into BRONZE UNION's Toolbox

Ghost RAT HyperBro ZXShell 2018-06-13 · Kaspersky Labs · Denis Legezo

LuckyMouse hits national data center to organize country-level waterholing campaign

HyperBro APT27

▶ [TLP:WHITE] win_hyperbro_auto (20251219 | Detects win.hyperbro.)

---