Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

RATs on the Loose Through Abused Cloudflare Tunnels

Date of Publication	Admiralty Code	TA Number
August 7, 2024	A1	TA2024299

Summary

Attack Commenced: February 2024
Malware: AsyncRAT, GuLoader, PureLogs Stealer, Remcos RAT, VenomRAT, and XWorm
Targeted Region: Worldwide
Targeted Industries: Finance, Manufacturing, Technology
Attack: Threat actors are increasingly exploiting the Cloudflare Tunnel service to disseminate a diverse array of remote access trojans (RATs), such as AsyncRAT, GuLoader, VenomRAT, Remcos RAT, and Xworm. Initially identified in February 2024, this malicious activity has escalated significantly from May through July.

Attack Regions

Attack Details

#1 Threat actors are increasingly exploiting the Cloudflare Tunnel service in their malware campaigns, often using it to distribute a range of remote access trojans (RATs) such as AsyncRAT, GuLoader, VenomRAT, Remcos RAT, and Xworm. First identified in February 2024, this activity surged from May through July.

#2 The campaigns leverage the TryCloudflare feature, which allows attackers to establish a one-time tunnel without requiring an account. TryCloudflare, a free Cloudflare service designed for web development and testing, enables the creation of temporary, internet-accessible servers proxied through Cloudflare's infrastructure.

#3 Attackers entice victims with phishing emails containing URLs or attachments leading to malicious LNK files. Hosting these LNK files on Cloudflare provides several advantages to the adversaries: the traffic appears legitimate due to Cloudflare's reputable service, and the TryCloudflare Tunnel feature ensures anonymity with temporary subdomains.

#4 The free and reliable nature of TryCloudflare means cybercriminals avoid the costs associated with setting up their infrastructure. The phishing emails available in English, French, Spanish, and German, vary in volume from hundreds to tens of thousands and target global organizations.

#5 The email lures also involve business-related themes such as invoices, document requests, package deliveries, and taxes. Upon activation, the payload executes BAT or CMD scripts to launch PowerShell, eventually downloading Python installers that deploy a diverse array of malware families.

Recommendations

Enhance Email Filtering: Deploy robust email filtering solutions to identify and block phishing emails that may contain malicious attachments or URLs. Use machine learning-based email security systems to adapt to evolving phishing tactics and lures.

Monitor and Analyze Traffic: Implement advanced network monitoring tools to detect unusual traffic patterns that may indicate the abuse of services like Cloudflare Tunnels. Regularly review and analyze network traffic logs for anomalies or unauthorized use of tunneling services.

Utilize Application Control and Whitelisting: Implement application whitelisting to allow only approved applications to run on endpoints. Use application control solutions to monitor and block unauthorized or suspicious applications.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**T1566.002** Spearphishing Link
T1566.001 Spearphishing Attachment	**T1059** Command and Scripting Interpreter	**T1059.003** Windows Command Shell	**T1059.001** PowerShell
T1204.002 Malicious File	**T1543** Create or Modify System Process	**T1027** Obfuscated Files or Information	**T1036** Masquerading
T1082 System Information Discovery	**T1083** File and Directory Discovery	**T1046** Network Service Discovery	**T1566** Phishing
T1005 Data from Local System	**T1071** Application Layer Protocol	**T1041** Exfiltration Over C2 Channel	**T1573** Encrypted Channel
T1584 Compromise Infrastructure	**T1059.006** Python	**T1090** Proxy	**T1204** User Execution

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0f1118b30b2da0b6e82f95d9bbf87101d8298a85287f4de58c9655eb8fecd3c6, 0fccf3d1fb38fa337baf707056f97ef011def859901bb922a4d0a1f25745e64f, 3867de6fc23b11b3122252dcebf81886c25dba4e636dd1a3afed74f937c3b998, 53c32ea384894526992d010c0c49ffe250d600b9b4472cce86bbd0249f88eada, a40f194870b54aeb102089108ecf18b3af9b449066a240f0077ff4edbb556e81, a79fbad625a5254d4f7f39461c2d687a1937f3f83e184bd62670944462b054f7
Domain	dcxwq1[.]duckdns[.]org, ride-fatal-italic-information[.]trycloudflare[.]com, spectrum-exactly-knitting-rural[.]trycloudflare[.]com, todfg[.]duckdns[.]org, welxwrm[.]duckdns[.]org, xwor3july[.]duckdns[.]org, ujhn[.]duckdns[.]org, anachyyyyy[.]duckdns[.]org, rvxwrm5[.]duckdns[.]org, ncmomenthv[.]duckdns[.]org, stickers-ext-payment-print[.]trycloudflare[.]com
IPv4	157[.]20[.]182[.]172
MD5	b325d948f463871ff10be13f8ea4b555, 1875b80d552feed0c1bd5592056d109a, 0d79c56f9198117a98334ead5d033974, 1e5fa94c5be0d6f6d57c181c60622b80, e4093e66d377d1f1552220fb7342385f, a8bfb9877be0daf890333c91c88c77d8, c9562d033d5e13674af5b5fdc3e5801c, e618be3fea2925a6637d8fcf05ff5c8a, 1e66092482f2738ff808c2fc076185e6, 58e6b6b4b7f6849749b6374ffbd7fa2e, 9320932e570d27bd88ee600b3961eecc, a84994e9e9de4fd82f721dbf2c8d9c58, 94e1a61c69eb01d7acba395d826824ce, 74502d4da814015cd36620734e248b5f, cff45bdc81bc10205d914dd3a84c74f7, ab95a98ee521483eee3903ab9733639b,

TYPE	VALUE
MD5	42f067738951f58979ce7267456ff05a, 987b4d5ab393fb625813d240f0329fa1, e80bc60a63f437f01e30ad6414988d65, 91ff771b1f48c809167a37862b14f070, 83105bbdfb9b25c0abf68a3ca5401801, de2a195f2ff18433ccfd0f1d9dae07ef, c741fbaeeb14a9a95d6fb201e9e0bd6e

References

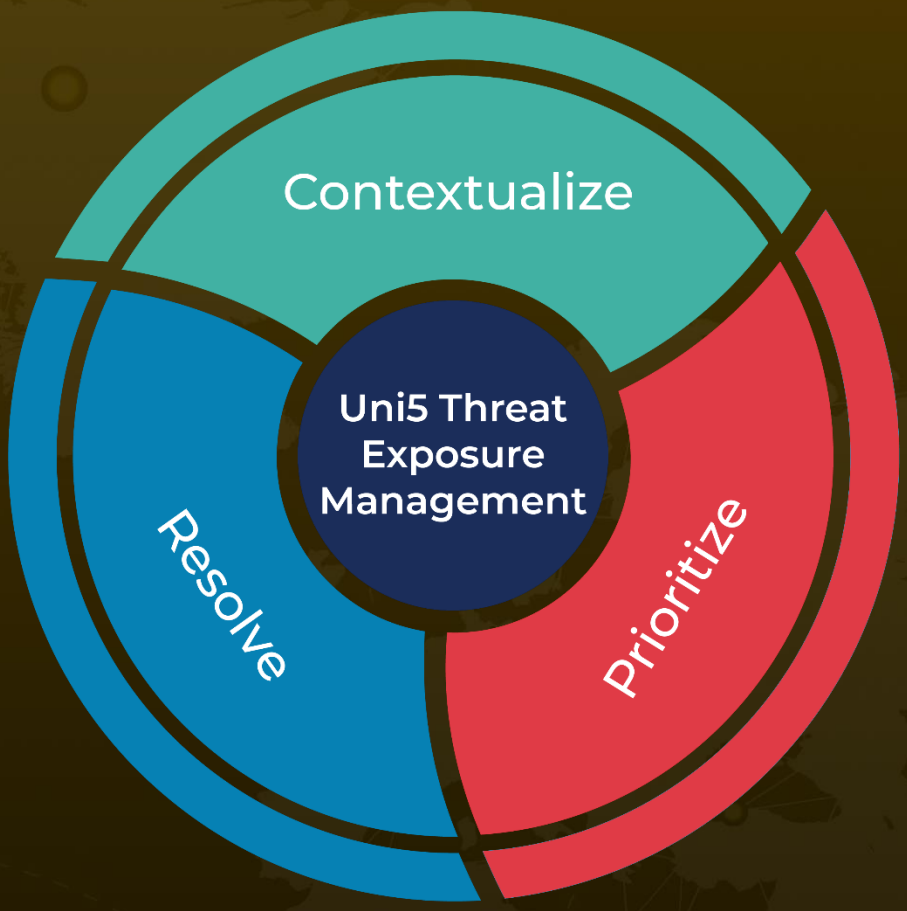
https://www.esentire.com/blog/quartet-of-trouble-xworm-asyncrat-venomrat-and-purelogs-stealer-leverage-trycloudflare

https://www.proofpoint.com/us/blog/threat-insight/threat-actor-abuses-cloudflare-tunnels-deliver-rats

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 7, 2024 • 6:30 AM

More at www.hivepro.com