Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

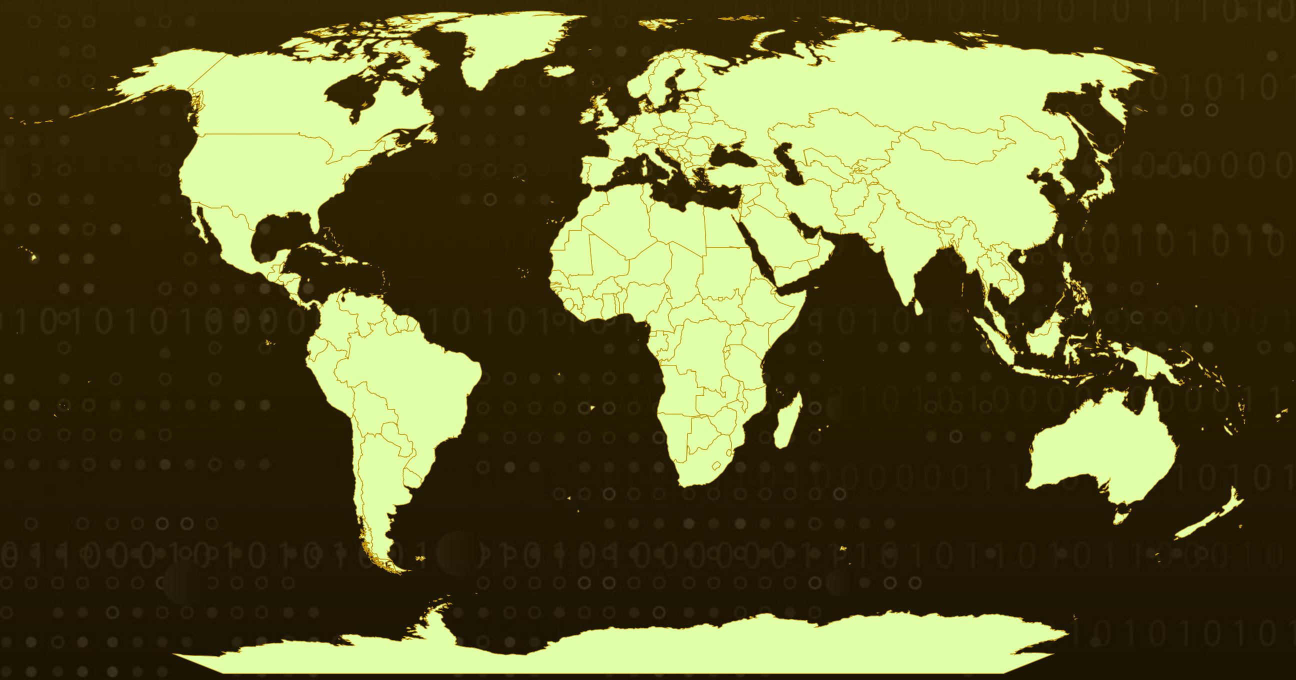
Stealthy AsyncRAT Campaign Leverages TryCloudflare Tunnels for Evasion

Date of Publication	Admiralty Code	TA Number
February 6, 2025	A1	TA2025032

Summary

Attack Discovered: January 2025
Targeted Country: Worldwide
Affected Platform: Windows
Malware: AsyncRAT
Attack: A stealthy malware campaign has been detected deploying AsyncRAT, a remote access trojan (RAT), using Python-based payloads and TryCloudflare tunnels. The attack begins with a phishing email containing a Dropbox link that, when clicked, downloads a ZIP archive, initiating a multi-stage infection process. This allows attackers to secretly gain control over infected systems, exfiltrate sensitive data, and execute commands while evading detection posing a serious cybersecurity threat.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

A newly discovered **AsyncRAT** malware campaign is using TryCloudflare tunnels and Python-based payloads to infiltrate systems, similar to an attack observed in August. Cybercriminals are exploiting legitimate platforms like Dropbox to distribute a ZIP archive that initiates a multi-stage infection process, ultimately executing a malicious Python script.

#2

The attack begins with a phishing email containing a ‘Rechnung herunterladen’ (Download Invoice) button, which hides a Dropbox link. Clicking it downloads a ZIP file that contains an internet shortcut (.URL) leading to a TryCloudflare URL. This URL then retrieves a .LNK file, which, when opened, triggers PowerShell to download a JavaScript (.JS) file. The JavaScript fetches a heavily obfuscated batch (.BAT) file, which downloads another ZIP archive containing the final payload—a malicious Python package which contains the AsyncRAT. To avoid suspicion, the attack also presents a fake invoice PDF to the victim.

#3

Inside the ZIP file (ma.zip) are multiple folders and files, including .BIN, .PY, and .EXE formats, resembling a normal Python setup. However, only the load.py script and a few .BIN files are harmful. The Python script uses Windows API functions like VirtualAlloc() and CreateThread() to execute malicious code stealthily. The campaign employs the Early Bird APC Queue technique to inject malware into processes before their main threads start, helping it bypass security defenses.

#4

The payloads include VenomRAT injected into notepad.exe, XWorm injected into another process, and AsyncRAT delivered into explorer.exe. These allow attackers to take full control of infected systems, steal data, and execute commands while remaining undetected.

#5

This campaign demonstrates how cybercriminals misuse trusted services like Dropbox and TryCloudflare to make their attacks appear legitimate. The use of a fake invoice PDF highlights the growing trend of using low-cost infrastructure to spread infostealers and remote access trojans, making such cyber threats more widespread and accessible.

Recommendations

Enhanced Email Security: Enhance email security by Implementing advanced spam filters, anti-phishing solutions, and email authentication protocols. Educate employees about identifying and reporting suspicious emails to prevent successful phishing attempts. Deploy advanced email filtering solutions to detect and block phishing emails containing malicious links or attachments.

Restrict Script Execution: Prevent untrusted scripts from running automatically by disabling the execution of .LNK, .JS, .BAT, and similar files. This helps block unauthorized payloads and reduces the risk of malware infections.

Monitor and Block Suspicious Traffic: Keep a close watch on network activity to detect and block unusual connections, especially those leveraging TryCloudflare tunnels or Dropbox URLs for malware delivery.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0010 Exfiltration
TA0011 Command and Control	T1566 Phishing	T1566.002 Spearphishing Link	T1204 User Execution
T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.006 Python
T1059.007 JavaScript	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information	T1132 Data Encoding
T1055 Process Injection	T1571 Non-Standard Port	T1036 Masquerading	

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//inventory-card-thumbzilla-ip[.]trycloudflare[.]com/DE/, hxxps[.]//mercy-synopsis-notify-motels[.]trycloudflare[.]com/ma[.]zip, hxxp[:]//sufficiently-points-est-minimize[.]trycloudflare[.]com/ma[.]zip
IPv4	62[.]60[.]190[.]141, 62[.]60[.]190[.]196
SHA1	55724b766dd1fe8bf9dd4cb7094b83b88d57d945, 4483561a49791a7cd684258e9f1623fe7dfba772, 0aa1b8fba8d7bd19a0064edfdf86c027da253644, 659ecdeb19b8e49be61fe41e8796d1215272b16e, cd61de9e4003ba568ae76f064935addb106a6d6d, 0221ec304905a758d9b47d6a631622b7dcf3c1f5, 4747ee49bdf31351c025049d8c3b7fef831be77c, 8ef36a4865f4a73a4e8fe4b90e5eff4a7feb3647, ae1dece09c2b627d8d3fe1c1f758db9ca6d5820c, 8dc9071a46a019547c8355a155d9c3c3b154e7a2, 098c369c904e8c328df40062190aff009e02d369, ff6186eef1c17a2668c6013d38fecead4f507556

References

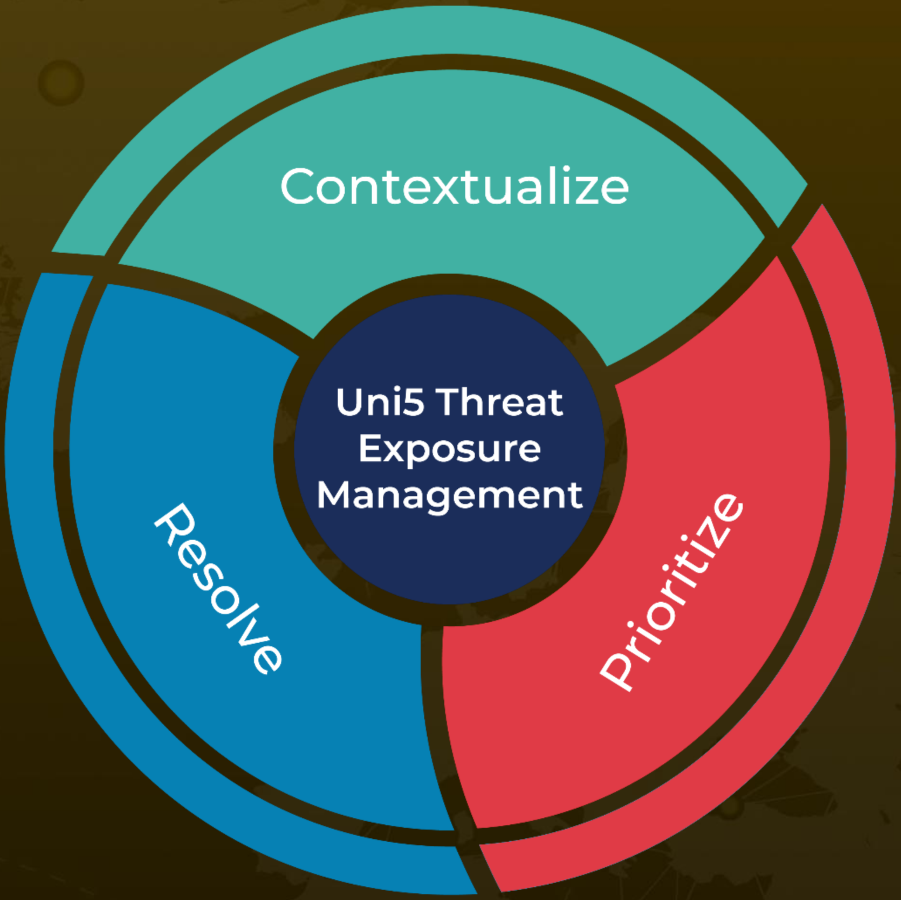
https://www.forcepoint.com/blog/x-labs/asyncrat-reloaded-python-trycloudflare-malware

https://www.hivepro.com/threat-advisory/a-new-face-of-asyncrat-utilizes-wsf-scripts-to-spread/

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

February 6, 2025 • 5:45 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com