Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

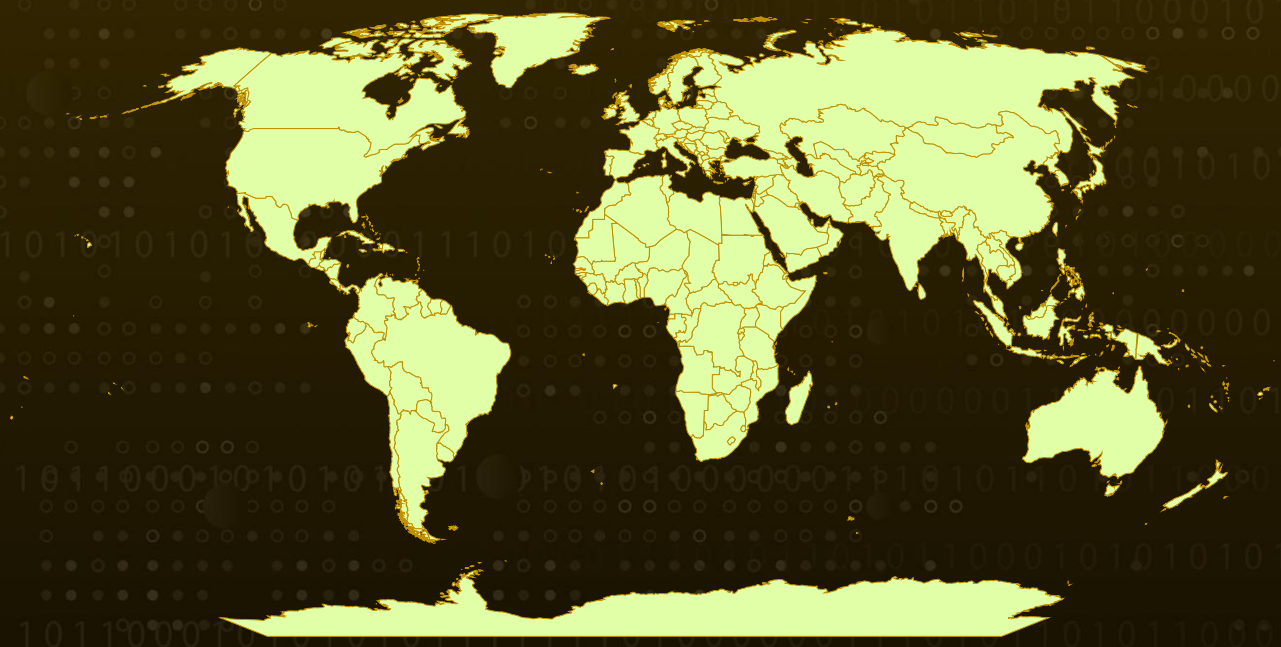
AsyncRAT Behind the Cloudflare Curtain

Date of Publication	Admiralty Code	TA Number
January 13, 2026	A1	TA2026012

Summary

Attack Commenced: 2026
Targeted Region: Worldwide
Malware: AsyncRAT
Affected Platform: Windows
Attack: This AsyncRAT campaign highlights how modern attackers quietly blend into everyday digital routines, turning something as ordinary as an invoice email into a full-scale system compromise. By abusing trusted services like Dropbox and Cloudflare, the attackers masked their activity behind familiar platforms. At the same time, Python-based scripts and native Windows tools handled the heavy lifting in the background. Victims were misled with legitimate-looking PDFs as the malware installed itself, established persistence, and injected AsyncRAT directly into common system processes. The result was a stealthy, cloud-assisted intrusion that favored patience and persistence over noise, underscoring how today's threats increasingly rely on trust, automation, and subtle deception rather than overt exploitation.

Attack Regions



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

Attack Details

#1

AsyncRAT continues to stand out as a widely abused remote access trojan, largely because it combines powerful surveillance capabilities with ease of deployment. Threat actors favor it for features such as keylogging, screen capture, remote command execution, and its modular design, which allows operators to tailor the malware to their needs. In this campaign, Python played a central role throughout the infection chain, automating multiple stages of execution. The attack began with a Windows Script Host file that pulled additional scripts from a WebDAV server hosted behind Cloudflare's free-tier infrastructure, allowing malicious traffic to blend in with legitimate services and evade scrutiny. While similar techniques have been observed before, notable changes in script behavior and payload delivery highlight ongoing refinement by the attackers.

#2

The compromise itself started with carefully crafted phishing emails that lured victims into opening Dropbox-hosted Internet Shortcut (.url) files. These shortcuts redirected users to multi-stage scripts delivered through TryCloudflare domains, initiating a complex infection sequence. The scripts installed a Python runtime, established persistence via the Startup folder, and ultimately injected malicious code into explorer.exe. The final stage delivered AsyncRAT, reflecting a relatively high level of technical sophistication and a clear focus on long-term system control rather than opportunistic infection.

#3

Behind the scenes, the infection chain relied heavily on native Windows processes and scripts. Services such as svchost.exe activated the WebClient service to communicate with WebDAV servers, while rundll32.exe and Windows Script files orchestrated the retrieval and execution of additional payloads. The initial script, as.wsh, fetched and launched anc.wsf, which in turn downloaded and executed multiple batch files. One batch file silently installed a Python environment, while another displayed a legitimate PDF to distract the user, masking the malicious activity taking place in parallel.

#4

Once Python was in place, the attackers focused on persistence and payload execution. Startup scripts ensured the malware survived reboots, while Python-based loaders injected shellcode into explorer.exe using advanced techniques such as asynchronous procedure call injection. The final payload, AsyncRAT, was delivered in an encrypted binary form and decrypted at runtime using locally stored keys. Additional folders and files on the same infrastructure suggest the attackers maintained a flexible toolkit capable of supporting multiple backdoors and infection scenarios. Overall, this campaign illustrates how modern threat actors combine cloud services, scripting languages, and deceptive tactics to build resilient, stealthy malware operations that are difficult to detect and disrupt.

Recommendations

Be Cautious With "Invoice" Emails, Even If They Look Routine: Attackers often disguise malware as invoices or order confirmations to trigger quick clicks. Employees should pause before opening ZIP files or shortcuts, especially when the email is unexpected or urges immediate action. When in doubt, verify the sender through a trusted channel.

Do Not Open Shortcut (.Url) Files or Zipped Links From Emails: Internet Shortcut files are rarely needed for legitimate business purposes and are increasingly abused by attackers. Organizations should block or restrict these file types at the email gateway and educate users that PDFs should never arrive as shortcuts.

Limit the Abuse of Built-in Windows Tools: This attack relied on native tools like Windows Script Host, PowerShell, and batch files to stay hidden. Where possible, restrict or monitor the use of these tools, especially on systems that do not require scripting for daily operations.

Watch For Unusual Python Activity On User Machines: The installation of Python on endpoints that do not typically use it can be a strong warning sign. Security teams should monitor for unexpected Python downloads, execution of python.exe, or scripts running at startup.

Monitor Trusted Cloud Services For Suspicious Behavior: Threat actors increasingly abuse legitimate platforms such as Cloudflare, Dropbox, and WebDAV to hide malicious traffic. Network and endpoint monitoring should focus on abnormal patterns rather than assuming trusted domains are always safe.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing
T1566.002 Spearphishing Link	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.003 Windows Command Shell

T1059.006 Python	T1204 User Execution	T1204.001 Malicious Link	T1204.002 Malicious File
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1027 Obfuscated Files or Information	T1036 Masquerading
T1036.007 Double File Extension	T1055 Process Injection	T1218 System Binary Proxy Execution	T1218.011 Rundll32
T1102 Web Service	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1105 Ingress Tool Transfer
T1573 Encrypted Channel	T1041 Exfiltration Over C2 Channel	T1056 Input Capture	T1056.001 Keylogging

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3475330b22f8652e713311689085a5ec24d03ce68d229e43afe89ed2f05a4a01, 33696190e43ede407b1b4903b10cafda0e49376d8ce0c85f01197f7c5073bc04, e8abdc2f58bb7391eb541e4c06467f422549a79740a3a1ad2979d48595555400, af22cd07ebfcba8d457a1bfacee7b66c60846de1b1d7ab356398dac696984ced, 41a01b6f2c4dc340cf35fab38c732e5d2660bedb15e3912d9970d724e20b4f71, 403784357e6402433153d47c2362f26cc26e135a1305393cea074574d3027af5, 47fe42924e00e92e3b297426a8ce3aa39864fbf6e7ae65893b4f5dbe0ea8176c, 0948683788167caec8ec5552b88cf66e3c0a5c6d99b3843317f5c794400b401f, 201c4c502678c41ba2dbb196cfe0f9f61371c10fdf947f1682eff8202f4ce580, 0aa3250cfb6d7defc68d6d7ddfbdee05a2329a20d944e8d4bb0e6b7f5a85caee,

TYPE	VALUE
SHA256	f3564370f1b243ca0bb6b31afe8f4bb11c35218e340dba94d4481218385be277, 7600f3d353aa29512dfc0cbc4aa0481453c078692174384a8da668ff1c6bd65a, b1032815b078aad59eb3bd32c29dee4621b37e516e679e84cb7d1c11c3eaff15, 4a75881d1ea48ae165ab7069dbfe398882d982e6a860c29ed1d940c4f285c871, e6cdcf2cdd49ac3ca256f30a7b5d11a9953748b5820b73845afcd7f9439d6290, 9e3a9db6942f7c42da4c53b5294604b232354002cee16f554a82edb1cf69c82f, 667d8cbd146c7e4c6dc674ff4219d3a7e682d6464e777a107e6207a7070bf626, D035d396ae5cda562d4e674b66eeda52a55510fe5c1d379930bff5bfcce10f13
Filenames	ne.py, Rechnung zu Auftrag W19248960825.pdf.url, myfile.tar, we.html, new.html, vio.bat, xeno.bat, ahke.bat, olsm.bat, anc.wsf, wa.wsh, as.wsh, Rechnung_2025_10_33828247000801.pdf.lnk, ow/new.bin, new.bin, ab/new.bin, DATEV-Rechnung Nr.53511122025.pdf.zip, LEXWARE0019.pdf.url
Domains	owners-insertion-rentals-pursuit[.]trycloudflare[.]com, plus-condos-thy-redeem[.]trycloudflare[.]com, citysearch-packed-bacterial-receptors[.]trycloudflare[.]com, strength-blind-bristol-ten[.]trycloudflare[.]com, syracuse-seeks-wilson-row.trycloudflare[.]com, license-appointed-asset-pulled[.]trycloudflare[.]com, pie-references-chart- ozone[.]trycloudflare[.]com
IPv4	43[.]157[.]118[.]169, 158[.]94[.]209[.]23

TYPE	VALUE
URLs	hxxp://dl[.]dropboxusercontent[.]com/scl/fi/50mvsqpvyxid7m39g773l/Rechnung-zu-Auftrag-W19248960825.pdf.zip?rlkey=rtgatrazvz9rbqtxbj9rtf7os&st=t318uel6&dl=0, hxxps://dl[.]dropboxusercontent[.]com/scl/fi/5uvu1977pm1v8e5w9dujx/LEXWARE0019.pdf.zip?rlkey=n9y56p52jbsgujjk84pnvdrrf&st=fqekaosq&dl=0

References

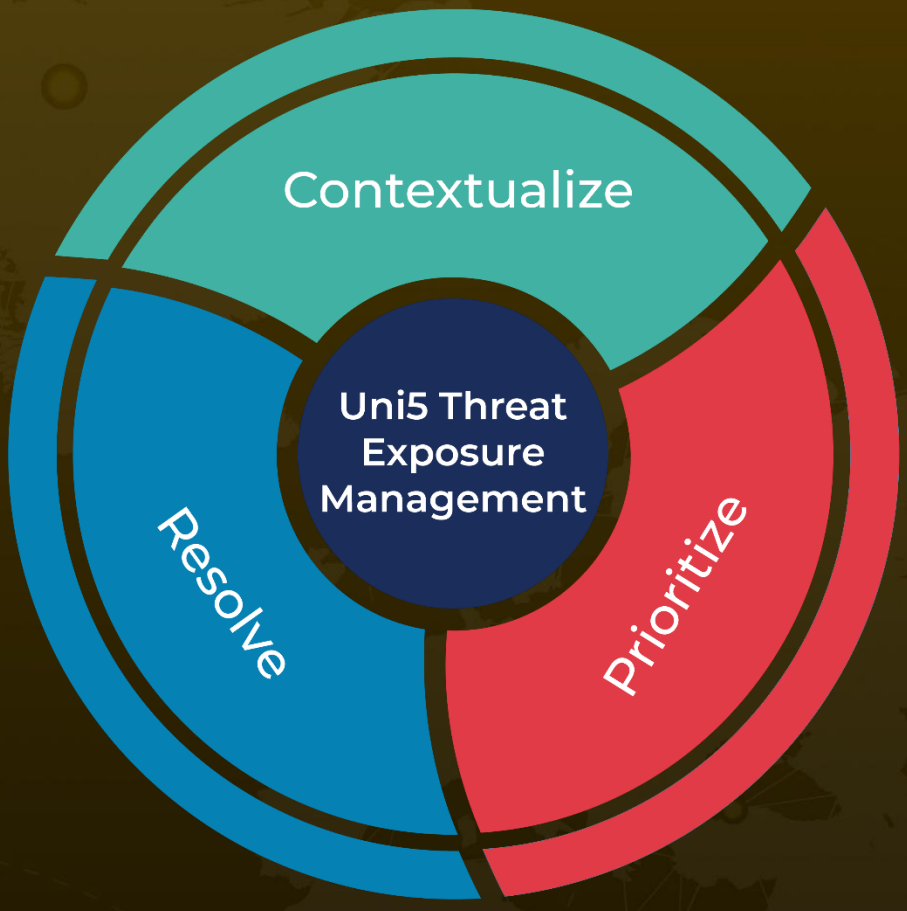
https://www.trendmicro.com/en_us/research/26/a/analyzing-a-a-multi-stage-asyncrat-campaign-via-mdr.html

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

January 13, 2026 • 8:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com