Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

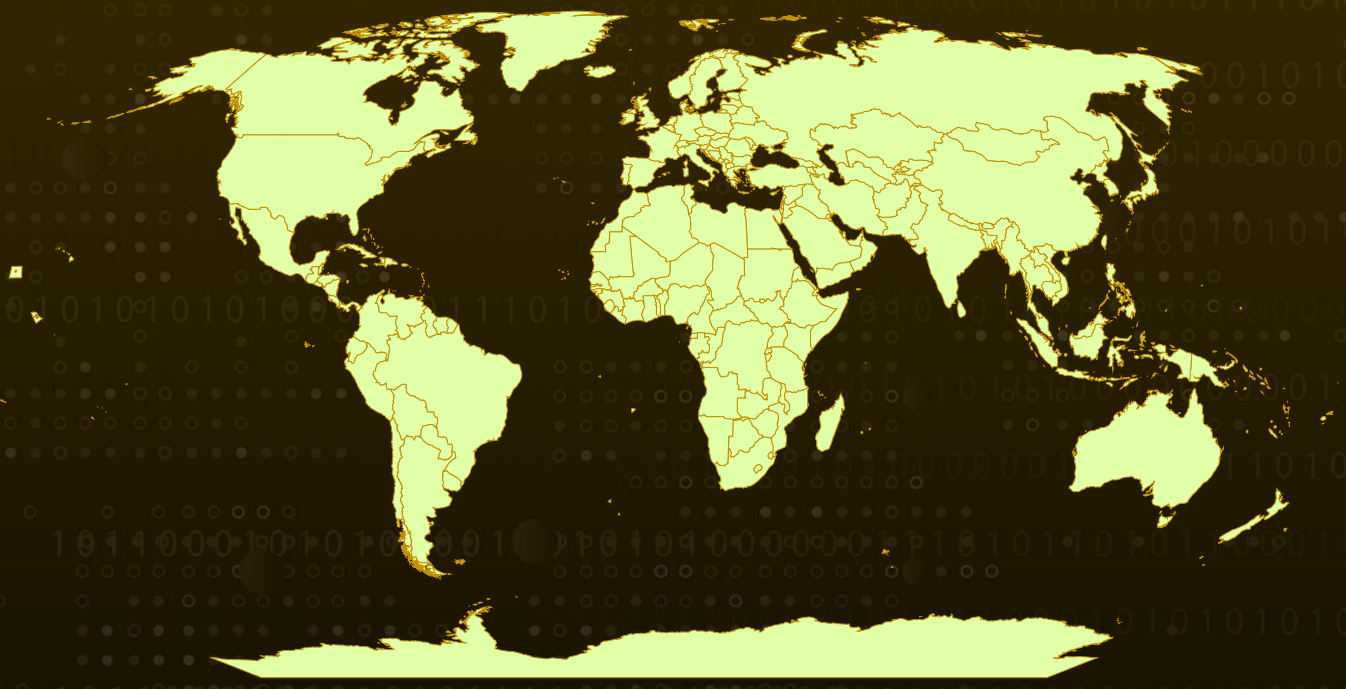
Rising Use of Fake CAPTCHA Pages to Deliver NetSupport RAT

Date of Publication	Admiralty Code	TA Number
June 4, 2025	A1	TA2025173

Summary

First Seen: 2025
Targeted Region: Worldwide
Malware: NetSupport RAT
Affected Platform: Windows
Attack: A new cyberattack campaign uses fake CAPTCHA pages to trick users into running malicious PowerShell scripts, leading to malware infections like NetSupport RAT. These spoofed sites mimic legitimate services and exploit user trust through social engineering. The attack unfolds in multiple stealthy stages to evade detection. It highlights the rising sophistication of human-targeted threats.

Attack Regions



Attack Details

#1 A recent wave of cyberattacks leverages fake CAPTCHA and “prove you are human” verification pages to trick users into infecting their own computers with malware. In these campaigns, attackers set up spoofed websites mimicking legitimate services, such as document signing platforms or code repositories.

#2 When users attempt to verify their identity by clicking on a CAPTCHA, they are presented with unusual instructions, typically, to copy a PowerShell script that has been silently copied to their clipboard and run it via the Windows Run prompt. This social engineering tactic exploits users’ growing familiarity with multi-step online authentication, a behavior sometimes called “click tolerance.”

#3 Once executed, the PowerShell script initiates a multi-stage infection chain. The initial script downloads additional scripts or payloads from remote servers, often in several steps to evade detection by traditional security tools. The downloaded content is then executed, which may involve unpacking files and launching further processes. Ultimately, the final payload, commonly a remote access trojan (RAT) such as NetSupport RAT is installed, granting attackers control over the victim’s machine and access to sensitive data.

#4 Unlike traditional malware that exploits system vulnerabilities, this attack relies entirely on social engineering. Its success depends on user actions and the trust evoked by familiar-looking websites. The campaigns are supported by a distributed infrastructure of malicious domains and hosting services, often spread via phishing emails, social media, or search engine results. By combining deceptive design with multi-stage payload delivery, these attacks demonstrate the growing sophistication of human-centered cyber threats.

#5 There has been a significant increase in these attacks throughout 2024 and into 2025, with campaigns targeting a wide range of individuals and organizations. The evolving tactics, such as embedding malware in non-executable files and using multi-stage delivery chains, highlight the need for ongoing user education, robust endpoint security, and policies that restrict the execution of untrusted scripts. As these fake CAPTCHA attacks continue to proliferate, vigilance and skepticism remain crucial defenses for both individuals and organizations.

Recommendations

- **Avoid Copy-Pasting Scripts:** Refrain from copying and pasting scripts into the Windows Run prompt, especially from unverified sources.
- **Verify Website Authenticity:** Always double-check the URL and SSL certificates of websites before interacting with them.
- **Exercise Caution with CAPTCHA Prompts:** Be skeptical of CAPTCHA-like verifications that instruct you to run commands, as legitimate CAPTCHAs do not require script execution.
- **Monitor Network Traffic:** Regularly analyze network traffic for unusual patterns or connections to unknown command-and-control (C2) servers. This can aid in early detection of malware communications.
- **Restrict Administrative Privileges:** Limit administrative rights to essential personnel only. This minimizes the potential impact of malware attempting to perform unauthorized actions or lateral movement within the network.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0003 Persistence
TA0011 Command and Control	TA0040 Impact	T1189 Drive-by Compromise	T1656 Impersonation
T1027 Obfuscated Files or Information	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1566.003 Spearphishing via Service
T1566 Phishing	T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1204 User Execution
T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	431b0b19239fc5e0eeaee70cd6e807868142e8cd0b2b6b1bd4a7a2cc8eb57d15, ab8fdde9fb9b88c400c737d460dcbf559648dc2768981bdd68f55e1f98292c2a, b2daa2b5afb389828e088ec8b27c0636bdad94b2ef71dcf8034ee601cb60d8d6, 58874c0dc26a78cdc058f84af9967f31b3c43173edc7515fa400e6ef8386205f, b258de3b7ef42b4f4bfb0fb5ffe7c55df6aef01cc591abe34a70d1ff82130cd5, e9fe19455642673b14c77d18a1e7ed925f23906bf11237dfafd7fb2cba1f666d, 1a128f6748d71d02c72ba51268be181143405830a4e48dfa53bf3d6ed3391211, 89043d2817d1bb4cb57ed939823dca0af9ae412655a6c75c694cb13d088efe5a, 8ffacc942d1c3f45e797369a1f4cbd5dcd84372abf979b06220236d5a5cea649, b3e879b5952988fb0c656240365db8f01198f9d83cd2a3ec0e2a8ee172e20a11, c6907acabf2edf0be959c64a434e101963f7c18dcf79f116e0ce6b5ced5dd08c, 07576e1db7e7bd0f7d2c54b6749fdd73c72dba8c2ba8ab110b305cfc10c93c80, 80b274871e5024dfa9e513219fe3df82cc8fe4255010bd5d04d23d5833962c10, d7fadf7ef45c475bd9a759a771d99ccf95edfa8a0c101ce2439a07b66c2e5c72, f9a241a768397efb4b43924fbd32186fcb1c88716fff3085d3ddcdd322d3404f
IPv4	185[.]209[.]21[.]241, 91[.]211[.]249[.]44, 95[.]215[.]204[.]156, 91[.]211[.]249[.]44, 194[.]26[.]232[.]180, 170[.]130[.]55[.]203, 212[.]86[.]115[.]52

TYPE	VALUE
Domains	0xpaste[.]com, aitradingview[.]app, aitradingview[.]dev, batalia-dansului[.]xyz, battalia-dansului[.]com, betamodetradingview[.]dev, betatradingview[.]app, betatradingview[.]dev, charts-beta[.]dev, codepaste[.]io, dans-lupta[.]xyz, dev-beta[.]com, devbetabeta[.]dev, devchart[.]ai, developer-ai[.]dev, developerbeta[.]dev, developer-beta[.]dev, developer-mode[.]dev, developer-package[.]dev, developer-update[.]dev, devmodebeta[.]dev, devmode-beta[.]dev, devtradingview[.]ai, devtradingview[.]net, dev-update[.]dev, docusign[.]sa[.]com, docusign[.]za[.]com, docusimg[.]sa[.]com, docusingl[.]sa[.]com, docusingle[.]sa[.]com, gitcodes[.]app, gitcodes[.]io, gitcodes[.]net, gitcodes[.]org, gitpaste[.]com, givcodes[.]com, hubofnotion[.]com, jeffsorsonblog[.]dev, loyalcompany[.]net, mhousecreative[.]com, modedev[.]ai, modedeveloper[.]ai, modedeveloper[.]com, modedevs[.]ai, nsocks[.]net,

TYPE	VALUE
Domains	oktacheck[.]it[.]com, pasteco[.]com, pastefy[.]com, pastefy[.]net, pastefy[.]pro, tradingviewai[.]dev, tradingview-ai[.]dev, tradingviewbeta[.]dev, tradingview-beta[.]dev, tradingviewdev[.]com, tradingviewindicator[.]dev, tradingviewtool[.]com, tradingviewtoolz[.]com, tradingviewtradingview[.]dev, updatebeta[.]app

References

https://dti.domaintools.com/how-threat-actors-exploit-human-trust/

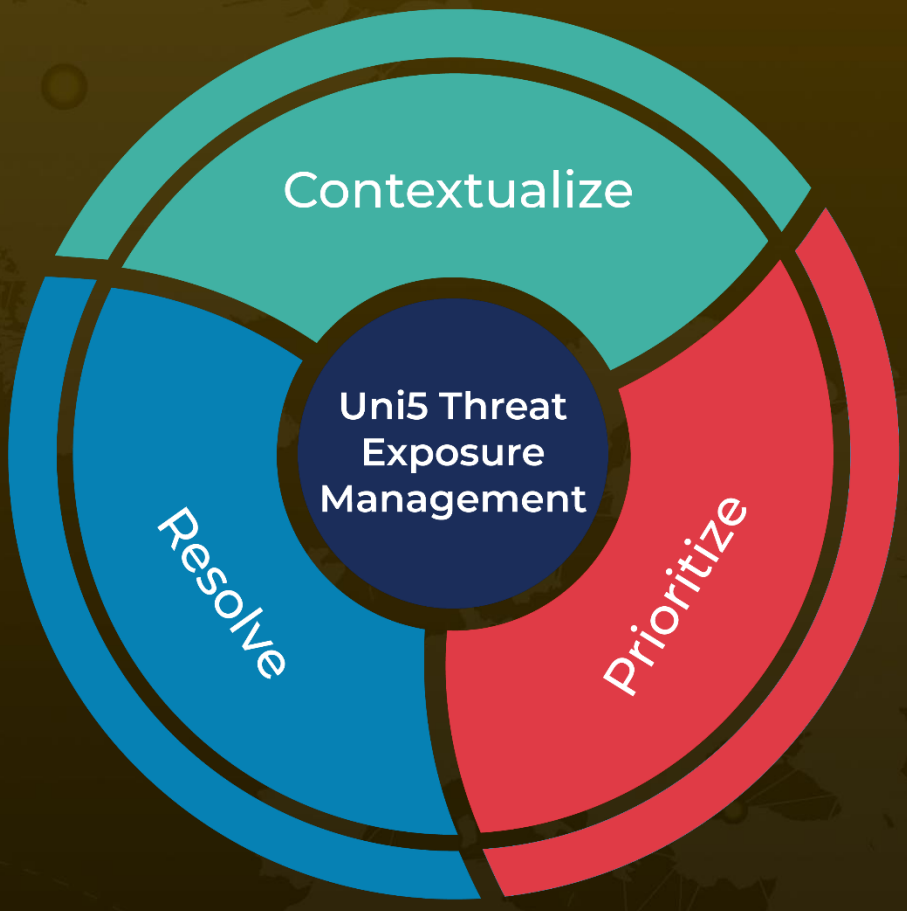
https://github.com/DomainTools/SecuritySnacks/blob/main/2025/Prove-You-Are-Human.csv

https://hivepro.com/threat-advisory/lumma-stealer-strikes-again-with-fake-captchas-and-advanced-evasion/

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

June 4, 2025 • 7:30 AM

More at www.hivepro.com