

INSIGHTS FOR SOC TEAMS

H1 2026 Cyber Risk Report



REPORTING PERIOD
January - June 2026
any.run

Executive Summary

1

Attackers are abusing trusted infrastructure

Threat actors increasingly hide inside legitimate tools, websites, authentication flows, cloud services, and public platforms.

2

Phishing is becoming harder to validate

Custom fake CAPTCHAs, browser fingerprinting, calendar invites, and device-code flows make phishing attacks harder to detect.

3

Identity compromise is moving beyond password theft

Infostealers and device-code phishing allow attackers to abuse tokens, sessions, cookies, recovery paths, and OAuth flows to maintain access.

4

Business processes are becoming attack paths

Tax notifications, payment portals, government services, fines, refunds, and administrative requests are being used to target companies.

5

Cross-platform and cloud-first environments increase exposure

Attacks now span Windows, Linux, macOS, developer workstations, cloud workloads, containers, and CI/CD environments.

6

Static IOC-based detection is losing effectiveness

Many threats avoid static indicators by using runtime infrastructure, legitimate services, dead-drop resolvers, and dynamic delivery chains.

7

Decision-makers should invest in earlier detection and broader visibility

Security teams need to close visibility gaps earlier by exposing phishing flows, malware behavior, browser activity, and threat context.

Trend 1: Custom fake CAPTCHAs are making phishing more evasive

In phishing attacks, threat actors are increasingly using custom fake CAPTCHA pages instead of common providers.

These pages act as an anti-bot and anti-sandbox gateway before the phishing site. Attackers also often add fingerprinting to track specific victims.

+437%

FakeCaptcha attacks from Q1 to Q2 2026

SOC & Business Impact

Evasion Breaks Standard Heuristics

Custom fake CAPTCHAs change the expected phishing flow, weakening simple detection logic and making attacks less likely to detonate in analysis.

One-Shot Pages Reduce Investigation Visibility

Phishing pages may work for the original victim but fail later during SOC investigation, making it harder to reproduce the attack.

Kill Chain Reconstruction Becomes Harder

When the page cannot be analyzed fully, teams lose visibility into the attack path, related threat activity, and indicators for detection and response.

Cut MTTR by 21 Min with Interactive Sandbox

ANY.RUN

Speed up alert triage with fast file and URL investigation, using live behavioral analysis to validate threats and support confident escalation decisions. With a median threat detection time of 14 seconds and 90% of threats visible within 60 seconds, analysts reach verdicts faster while reducing investigation bottlenecks across high-volume SOC operations.

Teams using ANY.RUN report 30% fewer Tier 1 to Tier 2 escalations, helping SOC leaders increase throughput without adding equivalent analyst workload.



Integrate ANY.RUN in your SOC →



Risk Mitigation Playbook

Strategic Focus

Apply a shift-left approach to phishing detection by identifying incidents as early as the fake CAPTCHA is observed, rather than only after credential entry or full phishing-page loading.

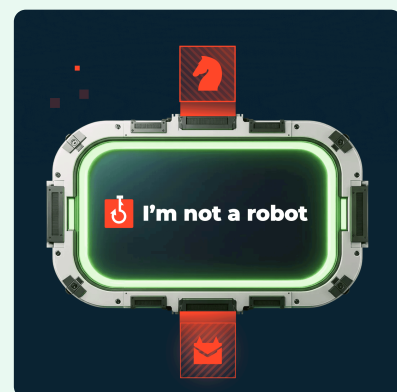
Operational Steps

- Use DPI inspection of web content in detection technologies, such as YARA rules or similar methods.
- To bypass attacker evasion, utilize interactive sandboxing combined with residential proxies to mask the analysis environment's nature.
- For any confirmed gateway interaction, the response protocol must include immediate session revocation and credential resets.

See also

ClickFix Explosion: Cross-Platform Social Engineering Turns Users Into Malware Installers

Explore how fake CAPTCHA-style lures appear in real ClickFix attacks.

[Read article](#)

Trend 2: Browser fingerprinting helps attackers avoid detection

Nearly all major PhaaS frameworks now use browser fingerprinting to check the client environment (e.g., device type, OS, and region).

The goal is to control who reaches the phishing page and redirect bots or sandboxes to legitimate websites to reduce suspicion.

SOC & Business Impact

Dynamic Analysis Becomes Less Reliable

Browser fingerprinting increases the risk that samples will not detonate, especially when teams rely on scratch-built analysis environments such as headless browsers with specific configurations.

Detection and Response Take Longer

When attacks are harder to identify and reproduce, detection rates can decrease, triage and forensics become more difficult, and MTTD/MTTR may increase.

Investigation Efforts Face Bottlenecks

Security teams struggle with triage when malicious content is geofenced or filtered by OS, making it nearly impossible to map the full kill chain without specialized tools that can mimic real-user conditions.

Use analysis environments that can better reproduce real-user browser conditions and expose browser-first phishing behavior.

For phishing attacks that rely on fingerprinting, standard file-based sandboxing is often not enough. Teams need strong URL analysis capabilities that support full dynamic investigation.

- Use residential proxies and register non-standard Browser API calls, adding Canvas objects to the DOM, and collection of browser properties.
- Analyze suspicious pages using a browser that bucketizes API property values that mask the system-specific details.
- Integrate ANY.RUN's Interactive Sandbox for interactive analysis of browser-based phishing, including visibility into DOM changes.

Closing Phishing Blind Spots with In-Browser Data Inspection

[Read article](#)

Trend 3: Infostealers become an identity theft system

Infostealers are shifting from being credential stealing malware to a more structured, affiliate-driven system for identity abuse.

Instead of collecting passwords, attackers increasingly target session tokens, cookies, recovery paths, crypto-wallet data, and other artifacts that can help them take over accounts or resell access.

SOC & Business Impact

Password Reset No Longer Closes the Incident

If attackers retain valid sessions, cookies, or recovery paths, access can continue even after credentials are reset.

Identity Compromise Outlives Endpoint Cleanup

The endpoint may appear clean while the user identity remains compromised through an active session.

Account Takeover Risk Increases

Delayed detection can enable fast account takeover, continued unauthorized access, and resale of compromised accounts or sessions.

Risk Mitigation Playbook

Strategic Focus

Treat infostealer incidents as large-scale identity compromise rather than merely a credential theft. The response procedures should involve monitoring and correlation of different artifacts.

Operational Steps

- Implement alerting for anomalous session creation, session token replays, and unusual account recovery flows.
- Monitor for specific execution markers characteristic of modern MaaS operations like the use of PowerShell scripting, DLL injections etc.
- Analysts must validate the full redirect chain and investigate the origin of any suspicious files, marking "trust abuse" as an incident category.

See also

Stay updated on the latest stealer attacks

Use queries like: **threatName:"stealer" AND submissionCountry:"US"** in TI Lookup to uncover threats in your industry and region.

[Search in TI Lookup](#)



Trend 4: Malicious LNK files remain a common phishing entry point

Attackers increasingly disguise malicious LNK files as legitimate documents. These include contracts, financial reports, and instructions, typically inside archives. When opened, the file launches destructive commands, which were embedded into its metadata.

This allows threat actors to execute malicious code in memory in a concealed way, using a decoy.

+119.2%

**Attacks using LNK files
from Q1 to Q2 2026**

SOC & Business Impact

Trusted Execution Bypasses Standard Controls

Malicious LNK files can bypass standard SEG and EPP controls because execution starts through trusted utilities and is hidden behind what looks like a legitimate document.

Investigation and Retrospective Analysis Become Harder

Because the activity is concealed inside a document-like workflow, it becomes harder to detect, investigate, and analyze retrospectively.

Strategic Focus

Treat LNK files in emails and archives as high-risk objects, never relying on their seemingly legitimate nature.

Operational Steps

- Prohibit the launch of system utilities such as mshta.exe, powershell.exe, and wscript.exe from untrusted directories using AppLocker or WDAC.
- Configure detection rules inside EDR/SIEM to monitor anomalous execution chains, especially with explorer.exe as a parent process.
- Check email attachments and downloads using LNK parsers, for example, using YARA rules to check for anomalous long arguments, keywords like bypass, hidden, Invoke-Expression/IEX, and URLs.

See also

Client-Side Exploitation: Abusing WebDAV+URL+LNK to Deliver Malicious Payloads

Explore how attackers abuse WebDAV, URL, and LNK files for malware delivery, along with practical YARA, SIGMA detection rules.

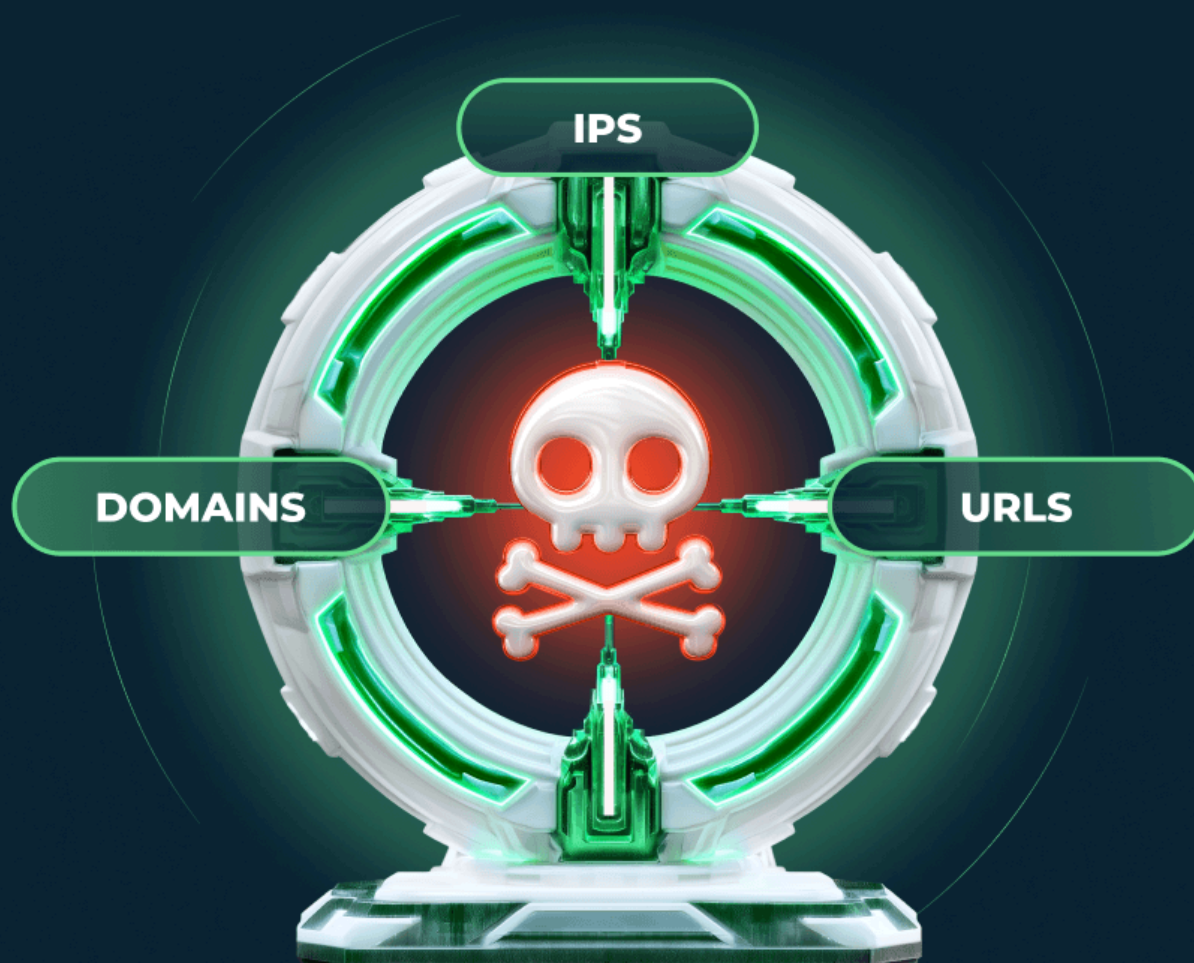
[Read article](#)

Triage and Hunt Threats Faster with TI Lookup

Accelerate alert validation and threat hunting by enriching indicators with real attack context, including related infrastructure, campaigns, malware families, and historical activity.

With TI Lookup, analysts can access up to 24x more IOCs per incident across ANY.RUN's TI solutions, giving teams broader context for prioritizing alerts and developing high-confidence hunting hypotheses.

The result is faster investigation, stronger threat coverage, and more consistent decisions across SOC shifts and analyst tiers.



Integrate ANY.RUN in your SOC →

Trend 5: Trusted, legitimate platforms as the entryway

ANY.RUN's data shows a growth in the popularity of hiding malware delivery infrastructures inside trusted channels.

This includes SEO poisoning, malvertising, codesigning, and npm package compromise across common services like Visual Studio Code extensions, WhatsApp, and PDFtools.

+90.7%

Attacks using Adobe infrastructure from H2 2025 to H1 2026

SOC & Business Impact

Trusted Chains Reduce Suspicion

These attack chains appear normal before execution, making them easy to trust and harder to stop with simple mitigation methods.

Investigation Starts Too Late

In many cases, analysis begins only after the payload has been delivered and credential theft has already occurred.

Risk Mitigation Playbook

Strategic Focus

Expand detection beyond file reputation and malware hashes. Treat trust abuse as a separate risk category during detection and triage.

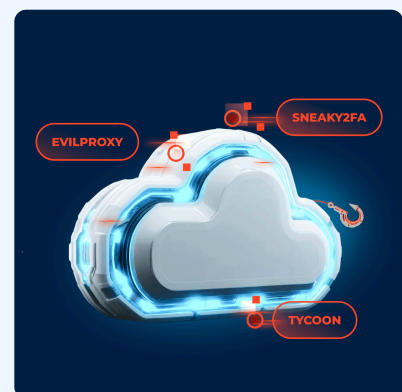
Operational Steps

- Configure alerts for newly registered domains that utilize legitimate software keywords (e.g., VPN, PDF-tools, or specific corporate utility names) to identify potential SEO poisoning or malvertising sites.
- Monitor for unexpected code-signing chains and the installation of IDE or browser extensions from non-standard or newly appeared sources.
- In developer and CI/CD environments, implement telemetry to detect drastic changes in package maintainer ownership.

See also

Enterprise Phishing via Microsoft & Google Cloud Platforms

Explore how enterprise phishing campaigns abuse trusted Microsoft and Google platforms to hide malicious activity from detection.

[Read article](#)

Trend 6: Cross-platform attacks target Windows, Linux, and macOS

Malicious activity is becoming less tied to a single operating system. Threat actors increasingly use portable payloads and adaptable languages such as Python to target different environments faster, while some malware families are built to support multiple platforms from the start.

+5.1%

**Python-based attacks
from Q1 to Q2 2026**

SOC & Business Impact

Platform-Specific Rules Create False Coverage

Detection rules built for only one platform can make teams overestimate their visibility across the environment.

Sandbox Assumptions Break Down

Cross-platform payloads challenge analysis setups that are designed around one operating system or execution path.

The Same Campaign Spreads Across Environments

Attackers can move across developer workstations, Linux servers, and other environments without being detected as part of one campaign.

Risk Mitigation Playbook

Strategic Focus

Build a unified correlation model across macOS, Windows, and Linux to ensure cross-platform visibility.

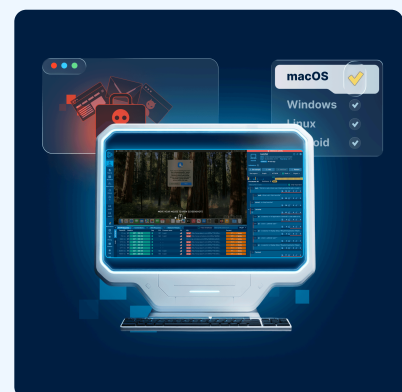
Operational Steps

- Establish monitoring for shared domains and similar lures (e.g., the same phishing themes or ClickFix prompts) across the entire fleet. Detection logic should hunt for repetitive RMM and remote access tools, archive or installer abuse, and cross-OS exfiltration patterns.
- Strengthen control over developer endpoints, Linux servers, and mixed-fleet environments, where the same campaign may leave various artifacts depending on the OS.
- If a suspicious DMG is found on macOS, the investigation must immediately check Windows and Linux endpoints for related infrastructure connections or similar file names.

See also

Expanding Your SOC's Cross-Platform Analysis with ANY.RUN's Interactive Sandbox

Explore how cross-platform sandbox analysis helps SOC teams investigate threats across Windows, Linux, Android, and macOS.

[Read article](#)

Trend 7: Calendar event files are becoming more common in phishing

According to **ANY.RUN's** H1 2026 statistics, .ics and calendar invite attachments are on the rise. Phishing lures, malicious URLs, or QR codes can appear not only in emails, but also inside calendar event files.

Although this method is not new, it is becoming more popular as an additional way to interact with the victim.

**Over 400
cases**

**of .ics use in phishing
attacks in H1 2026**

SOC & Business Impact

Calendar Events Add Another Attack Surface

Event files create an additional contact point with the victim and blur the line between email security and calendar-related infrastructure.

Related Artifacts May Be Investigated Separately

The email, attachment, and calendar event may be handled as separate objects, even when they belong to the same attack.

Visibility Breaks Across the Investigation

When these artifacts are not connected, SOC teams lose continuity during analysis, which can slow down investigation and response.

Risk Mitigation Playbook

Strategic Focus

Treat calendar invites as part of the phishing attack surface, especially when they come from external senders or contain links, QR codes, or unexpected attachments.

Operational Steps

- Establish detection rules to track .ics files and text/calendar MIME types across all incoming emails, file archives, and web downloads.
- Proactively correlate calendar-event artifacts with other common phishing components. This includes identifying links to QR codes, HTML/PDF attachments, and impersonation lures targeting Microsoft, DocuSign, or SharePoint.
- Within Microsoft 365 and Google Workspace environments, implement strict governance over external invitations and auto-add functionalities.

See also

Stay updated on the latest attacks using .ics files

Use the query **commandLine:".ics" AND threatLevel:"malicious"** in Threat Intelligence Lookup to uncover recent threats associated with calendar event files.

[Search in TI Lookup](#)

Expand Threat Coverage with TI Feeds

Strengthen monitoring with verified threat indicators generated from live malware and phishing investigations, delivered directly into SIEM, SOAR, TIP, and detection pipelines.

ANY.RUN Threat Intelligence Feeds provide 99% unique IOCs compared with other TI sources, extending detection coverage with malicious infrastructure that may not appear in existing feeds.

For SOC and MSSP operations, this supports earlier detection at scale while reducing the workload required to continuously identify, validate, and distribute new indicators.



Integrate ANY.RUN in your SOC →

Trend 8: Supply chain attacks via open-source software are rising

Instead of directly hitting the final victim, threat actors increasingly target software delivery channels like npm packages, PyPI, Crates.io, and CI/CD publications.

The methods include malicious package publishing, self-propagating worms, and the compromise of official distributors.

SOC & Business Impact

Trust in Official Packages Breaks Down

Compromise at upstream layers undermines trust in official packages and updates, making malicious activity harder for SOC teams to investigate.

One Attack Can Reach Many Organizations

This method can affect multiple downstream organizations at the same time, expanding the impact beyond a single compromised environment.

Some Campaigns Self-Propagate

Campaigns such as Mini Shai-Hulud do not only infect packages, but can also spread further by abusing victim tokens and pipelines.

Risk Mitigation Playbook

Strategic Focus

Regular download alerts are delivered too late and don't represent the real impact scope. This is why there's a need to track more specific incident categories and suspicious indicators.

Operational Steps

- Actively monitor the publication of new package versions and alert on drastic or rapid changes in maintainer ownership.
- Implement automated checks for suspicious preinstall and postinstall hooks within package manifests.
- Track anomalies in GitHub Actions and OIDC (OpenID Connect) authentication flows to detect pipeline hijackings. Monitoring should identify mass changes across namespaces.

See also

Expert-curated reports on emerging attacks for your SOC/MSSP team

ANY.RUN's TI Reports deliver insights into active malware & phishing campaigns, providing actionable indicators, TTPs, and other detection artifacts for your proactive defense.

[Read TI Reports](#)



Trend 9: Linux privilege escalation is becoming more reliable after compromise

A growing number of reliable Linux local privilege escalation (LPE) exploits are appearing in the wild.

They point to a broader shift toward more stable post-compromise root escalation across Linux environments, including major distributions and cloud Linux workloads.

SOC & Business Impact

One Exploit Can Expand Cloud Impact

In cloud- and container-first environments, a successful Linux LPE can give attackers root access on the host, enable container escape, expose secrets, and support lateral movement across clusters or CI/CD environments.

Detection Leaves Fewer Artifacts

Linux LPE is harder to fight than regular malware detection because exploitation is local and may leave only minimal artifacts.

Public PoCs Accelerate Risk

Public PoCs and writeups can quickly make new kernel flaws widespread, especially when they apply to many modern enterprise distributions.

Risk Mitigation Playbook

Strategic Focus

Expand Linux security coverage beyond CVE tracking and patch status. Focus on how privilege escalation can increase the impact of an initial compromise across cloud, container, and CI/CD environments.

Operational Steps

- Pay attention to not only CVEs but also post-exploitation escalation, e.g., the launch of su/sudo right after a suspicious activity, unusual calls to kernel networking/page-cache paths, and drastic changes in privilege boundary at Linux hosts.
- During triage, mark kernel LPE, container escape, public PoC, active exploitation, and so on as separate incident categories.
- For hardening, defenders need to deploy new kernel updates, live patching, minimal local attack surface, and separate rights in container and CI/CD environments.

See also

How to Hunt and Investigate Linux Malware

Explore techniques for hunting and investigating Linux malware, analyzing threats like botnets and stealers, and leveraging **Threat Intelligence Lookup** to strengthen security.

[Read article](#)

Trend 10: OAuth device code compromise is growing in phishing attacks

Threat actors are increasingly abusing the legitimate Microsoft OAuth Device Code flow to compromise Microsoft 365 accounts.

Instead of regular credential harvesting, they redirect the user from the phishing page to the legitimate Microsoft page, and once their credentials are confirmed, the OAuth tokens are delivered to the attacker.

+483.7%

Device code phishing attacks from Q1 to Q2 2026

SOC & Business Impact

Legitimate Login Pages Hide the Attack

Users enter credentials on a real Microsoft page, so the usual visual indicators of phishing may be missing or less obvious.

Risk Shifts from Password Theft to Token Abuse

Even if the password is not exposed, attackers can still gain access to Microsoft 365 through OAuth tokens.

Standard Web Monitoring Sees Less

The activity runs through legitimate authentication flows and HTTPS, making triage harder and requiring more precise signal correlation.

Risk Mitigation Playbook

Strategic Focus

Treat suspicious authentication flows as a compromise signal pay attention to abnormal device-code authentication patterns, even when the user entered credentials on a legitimate Microsoft page.

Operational Steps

- Monitor anomalous OAuth and device-code authentication events in Microsoft Entra ID and Microsoft 365, including successful device-code authentications for users who do not normally need this flow.
- Track follow-up calls to M365 resources after device login, suspicious phishing pages that display verification codes, and HTTP requests to suspicious hosts with paths such as `/api/device/start`, `/api/device/status/`, and `/api/status/init`.
- In **ANY.RUN's Interactive Sandbox**, check suspicious URLs and monitor activity tagged as `oauth-ms-phish`, `eviltokens`, or `kali365`.

See also

EvilTokens Phishing as a Service: Attackers Breach M365 Accounts with OAuth Device Codes

Explore how EvilTokens abuses Microsoft OAuth Device Code flow to compromise M365 accounts without direct credential theft.

[Read article](#)

Trend 11: Attackers are using legitimate RMM tools to breach companies

Attackers increasingly use phishing pages not to deliver an obviously malicious payload, but to push the installation of legitimate RMM or remote access tools.

The initial access model shifts from malware-first to phishing-first, where the final tool may look trusted in an enterprise environment.

+26.5%

RMM attacks from H2 2025 to H1 2026

SOC & Business Impact

Legitimate Tools Reduce Detection Confidence

RMM phishing is high-risk because attackers abuse tools that may already be allowed or trusted inside the organization.

Triage Must Separate Admin Activity from Intrusion

SOC teams need to distinguish legitimate remote administration from unauthorized remote access, which complicates detection, triage, and response.

Trusted Context Extends Dwell Time

When malicious intent is harder to prove, attacks may stay unnoticed longer and give attackers extended access to the infrastructure.

Risk Mitigation Playbook

Strategic Focus

Treat unexpected RMM activity as a context-driven access risk, not as automatically benign software.

Legitimate or signed RMM tools should still be validated against the delivery path, approved admin workflows, and expected usage.

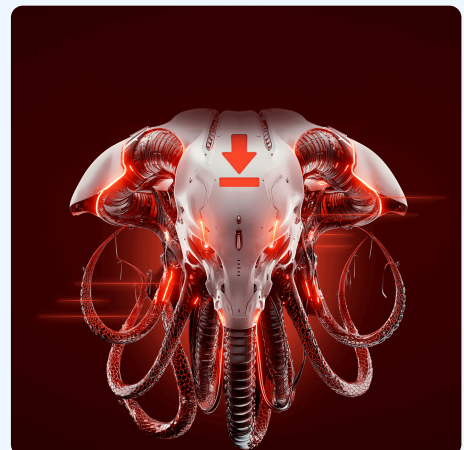
Operational Steps

- Maintain a strict, centralized allowlist of approved RMM tools, including specific authorized tenants, accounts, admin hosts, and sanctioned workflow.
- Security systems must be configured to track the full attack chain: from the initial visit to a phishing page to the subsequent installer or script download, culminating in RMM execution and outbound connections to remote infrastructure.
- During incident triage, analysts must verify the download source and parent process; RMM tools launched from user directories (e.g., %TEMP%, Downloads, AppData).

See also

Phishing-to-RMM Attacks: The Remote Access Blind Spot CISOs Can't Ignore

Explore how phishing-to-RMM attacks turn trusted remote access tools into an initial access path.

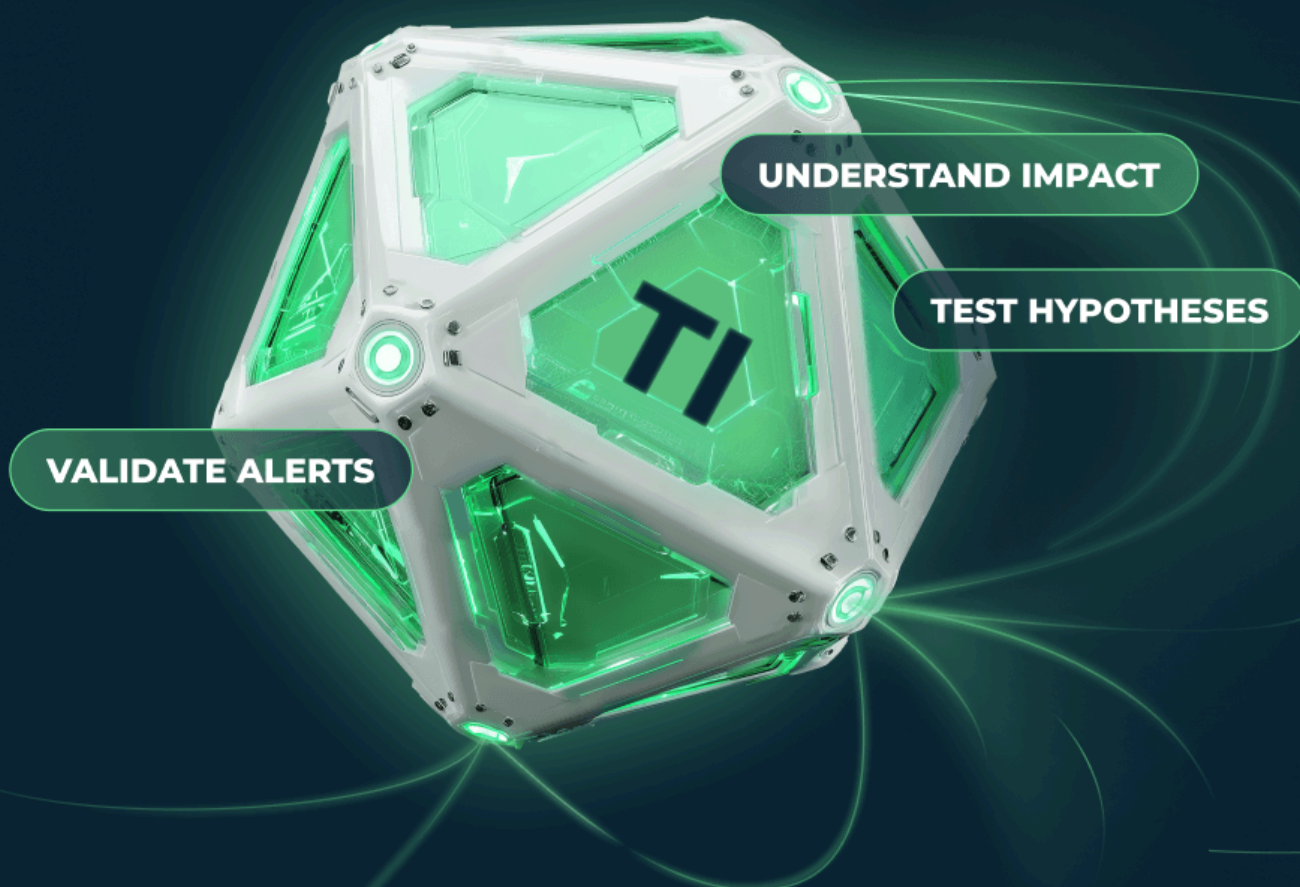
[Read article](#)

Stay Updated on the Latest Threats with TI Reports

Track emerging malware, phishing campaigns, APT activity, and cybercriminal operations through analyst-researched reports focused on the threats shaping current attack activity.

Each report combines expert analysis with embedded TI Lookup queries, allowing SOC and threat intelligence teams to move directly from campaign-level findings to relevant indicators, infrastructure, and investigative context.

This gives SOC leadership a practical way to turn current threat research into hunting priorities, detection opportunities, and faster response.



Enrich investigations with TI Reports →

Trend 12: Legitimate website abuse is growing in ClickFix campaigns

Instead of creating dedicated phishing domains, threat actors increasingly spread ClickFix campaigns through compromised legitimate websites.

They inject code into real websites to display fake messages that urge users to run malicious commands in PowerShell or CMD.

+104.7%

ClickFix attacks from H2 2025 to H1 2026

SOC & Business Impact

Clean Domains Pass Reputation Checks

Attackers abuse legitimate websites with clean history, so the domains may not be identified as suspicious during early detection.

Standard Detection Coverage Misses the Setup

Many security tools focus on newly registered domains or known phishing pages, while ClickFix can start from a trusted website.

Manual Execution Hides the Malicious Step

The malicious logic may be hidden in injected JavaScript, while the user is pushed to run the command manually. This makes detection and triage harder and requires deeper browser and webpage analysis.

Risk Mitigation Playbook

Strategic Focus

Don't consider domain reputation as sufficient proof of safety. Legitimate and long-standing websites can still become the first stage of an attack, so SOC teams should assess the full user interaction flow, not only the domain or URL.

Operational Steps

- During triage, analysts must perform a **deep-dive into webpage content and JavaScript**, rather than focusing solely on the domain or URL.
- Monitoring must be tuned to alert on pages that urge users to execute PowerShell or CMD commands to resolve browser or document errors.
- Establish specialized monitoring for suspicious URI patterns associated with ClickFix infrastructure, including calls to `/jsrepo?rnd=`.

See also

Stay updated on the latest ClickFix attacks

Use queries like: **threatName:"clickfix" AND submissionCountry:"de"** in Threat Intelligence Lookup to uncover threats in your industry and region.

[Search in TI Lookup](#)

Trend 13: Discord, Telegram, and GoFile are used as exfiltration channels

In stealer attacks, exfiltration increasingly relies on legitimate public services such as Discord, Telegram, and GoFile instead of attacker-owned infrastructure.

These services are often available from corporate networks and allow attackers to transfer stolen data without maintaining their own C2 infrastructure.

+11.1%

**Attacks using Discord
from H2 2025 to H1 2026**

SOC & Business Impact

Legitimate Services Hide Exfiltration

Traffic to Discord, Telegram, or GoFile may look legitimate, but in stealer activity it can represent the final stage of the attack: sending stolen data to the operator.

Blocking Entire Services Is Not Practical

Because these services can have legitimate use, blocking them altogether may not be a reasonable option for many organizations.

Context Determines Malicious Intent

SOC teams need process, activity, and data-collection context to understand whether a connection to these services was normal traffic or actual exfiltration.

Strategic Focus

Monitor activity related to legitimate services like Discord, Telegram, and GoFile. It's key to assess the context: which process connected to the service, what happened before the connection, and whether data collection or archive creation occurred.

Operational Steps

- Monitor Discord webhook activity, especially requests to **discord.com/api/webhooks/**, **discordapp.com/api/webhooks/**, and related endpoints. Focus on POST requests, **multipart/form-data**, archive uploads, and unusual process origins. Prioritize detections where webhook URLs, IDs, or tokens appear in malware configs, memory, files, or command-line artifacts.
- For Telegram, track Bot API usage via **api.telegram.org/bot**, including **/sendMessage**, **/sendDocument**, and **/sendPhoto**. Watch for bot tokens, **chat_id**, and file transfers using POST with **multipart/form-data**. Flag cases where tokens or chat IDs are embedded in malware artifacts or processes send data to Telegram.
- For GoFile, monitor **gofile.io** and related upload endpoints like **api.gofile.io** and **/uploadFile**. Focus on POST uploads, archive creation (.zip, .rar, .7z), and generated download links. Prioritize cases where uploaded archives are later shared via Telegram or Discord.

See also

How to Intercept Data Exfiltrated by Malware via Telegram and Discord

Explore how malware uses Telegram and Discord APIs to send stolen data through legitimate public services.

[Read article](#)

Trend 14: Phishing imitates payment and government services to target employees

This trend is built around phishing, payment data theft, and business process abuse. Phishing campaigns increasingly imitate not only fine-payment and government-fee services, but also banks, tax authorities, municipal portals, and other official payment services.

Attackers target employees involved in finance, accounting, legal, procurement, fleet management, and decision-making processes by using themes such as taxes, fines, debts, refunds, and mandatory payments.

SOC & Business Impact

Attacks Blend into Business Workflows

These attacks look like normal financial or administrative tasks, such as checking a fine, paying a fee, confirming a debt, or processing a tax notice.

Employees May Complete the Scenario Manually

Because the request appears relevant to their work, employees may follow the steps themselves and enter sensitive data into a fake form.

No Malware Means Lower Detection Confidence

There may be no malware, exploit, or obvious payload. Without context around the user, department, domain, and page content, the incident may look like a low-priority suspicious URL rather than business process abuse.

Risk Mitigation Playbook

Strategic Focus

Treat payment- and government-themed phishing as business process abuse, not just generic phishing. SOC teams should prioritize the incident based on the user's role, department, and potential financial exposure.

Operational Steps

- Monitoring must prioritize combinations of high-risk indicators: newly registered or low-reputation domains combined with service impersonation, clear payment intent, and access by a corporate user.
- Track themes related to debts, payment checks, and official notices where the sender's display name imitates a municipal body or bank but the underlying link points to a non-official domain.
- Detection rules should flag POST requests occurring after page visits to uncategorized domains, as this indicates data submission into a form.

See also

Cyber Attacks on Government Agencies: Detect and Investigate with ANY.RUN for Fast Response

Explore case studies on detecting and investigating cyber attacks targeting government agencies, using ANY.RUN's Sandbox and Threat Intelligence solutions for rapid response.

[Read article](#)

Trend 15: Dead Drop Resolvers are being used to hide C2 and delivery chains

Malware actors increasingly use Dead Drop Resolvers (DDR) as an infrastructure layer. Instead of storing the final C2 URL, configuration, or delivery-chain elements directly in the sample, malware retrieves them from external sources during execution.

These sources can include smart contracts and blockchain infrastructure, as seen in EtherHiding, Steam profiles, or other legitimate and out-of-band resources where attackers can hide C2 configuration.

SOC & Business Impact

Static IOCs Lose Value

DDR makes malware infrastructure more resilient because the final C2 may be absent from the sample and only appear during execution.

Legitimate Sources Hide C2 Resolution

The DDR source may look legitimate, such as a blockchain RPC endpoint or a Steam profile, making detection and triage harder.

Attack Context Can Be Missed

If teams only see the final C2 connection or only the DDR request, they may miss how the malware resolved infrastructure and continued the attack chain.

Risk Mitigation Playbook

Strategic Focus

Shift detection from isolated IOCs to the full behavioral chain of C2 resolution. SOC and MSSP teams should treat DDR activity as a separate detection category, even in cases when C2 infrastructure appears only during execution.

Operational Steps

- Actively track indicators of blockchain-based DDR (EtherHiding), including eth_call, eth_getStorageAt, and generic JSON-RPC requests.
- Flag requests to steamcommunity.com/profiles/ that originate from non-browser or non-Steam processes, particularly when these requests are followed by connections to unknown or rare external hosts.
- Proactively correlate all DDR requests with subsequent C2 connections, payload execution, or exfiltration activity.

See also

Kamasers: A Multi-Vector DDoS Botnet Targeting Organizations Worldwide

Explore how Kamasers uses Dead Drop Resolver mechanisms and legitimate public services to retrieve active C2 infrastructure.

[Read article](#)

Power Your Business Security with ANY.RUN



ANY.RUN's solutions are used by more than 16,000 businesses across multiple industries, such as finance, manufacturing, healthcare, and technology, including 74 of Fortune 100 companies.

Interactive Sandbox helps SOC & MSSP teams identify malware & phishing targeting Windows, Linux, macOS, and Android systems. It provides capabilities for fast, hands-on investigations for streamlined triage and informed response.

ANY.RUN's Threat Intelligence delivers rich, real-time info on active cyber attacks, to expand threat coverage, accelerate alert validation, and power proactive defense.

Integrate ANY.RUN in your SOC →