Cyber Threat Intelligence

CRITICALSTART® Security Advisory:

TLP AMBER // [CS-SA-26-0101] Strategic Phishing Campaigns Leverage CAPTCHA and Email Routing Misconfiguration

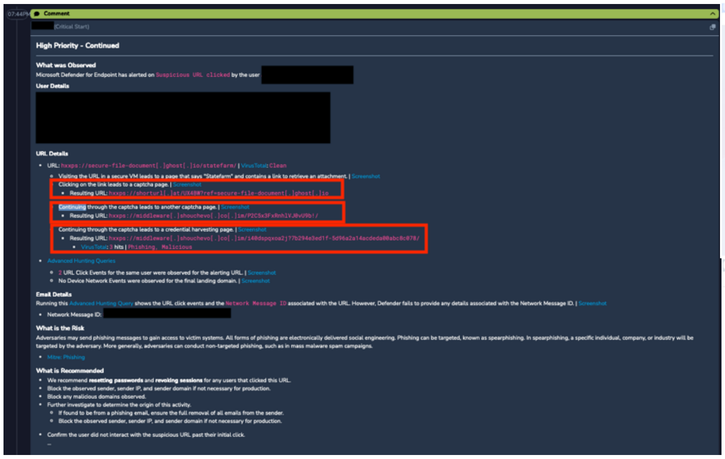
Executive Summary

Critical Start is tracking an increase in advanced phishing attacks that move beyond simple links and attachments delivered via email. These campaigns rely on layered social engineering and alternative delivery techniques to gain initial access, with primary activity centered on fake CAPTCHA pages, phishing messages that appear to originate from inside the organization, among others. These tactics are designed to reduce user suspicion, evade automated detection, and increase the likelihood of credential theft and follow-on compromise. Per activity being observed in the wild across both Windows and macOS environments, reports note there has been consequent credential theft, session token compromise, and persistent access.

Findings

Fake CAPTCHA Pages as a Trust Mechanism

Attackers are using fake CAPTCHA pages to establish legitimacy and control user interaction after initial engagement. These pages are hosted on malicious or compromised sites and are designed to appear routine and familiar. In some cases, the CAPTCHA is used as a gating step before redirecting victims to credential harvesting portals that collect usernames, passwords, and multi factor authentication codes. In a recent investigation, Critical Start's Security Operation Center (SOC) analysts observed multiple fake CAPTCHA pages deployed, which eventually redirected the user to a credential harvesting page impersonation a Microsoft login page.



[redacted] (Critical Start)

High Priority - Continued

What was Observed

Microsoft Defender for Endpoint has alerted on Suspicious URL clicked by the user [redacted]

User Details

[redacted]

URL Details

- URL: hxxps://secure-file-document[.]ghost[.]io/statefarm/ | VirusTotal: Clean
  - Visiting the URL in a secure VM leads to a page that says "Statefarm" and contains a link to retrieve an attachment. | Screenshot
  - Clicking on the link leads to a captcha page. | Screenshot
    - Resulting URL: hxxps://shorturl[.]at/UX4BW?ref=secure-file-document[.]ghost[.]io
  - Continuing through the captcha leads to another captcha page. | Screenshot
    - Resulting URL: hxxps://middleware[.]shouchevo[.]co[.]im/P2C5x3FxRnhlVJ0vU9b!/
  - Continuing through the captcha leads to a credential harvesting page. | Screenshot
    - Resulting URL: hxxps://middleware[.]shouchevo[.]co[.]im/i40dspqxoa2j77b294e3ed1f-5d96a2a14acdeda00abc8c078/
      - VirusTotal: 3 hits | Phishing, Malicious
- Advanced Hunting Queries
  - 2 URL Click Events for the same user were observed for the alerting URL. | Screenshot
  - No Device Network Events were observed for the final landing domain. | Screenshot

Email Details

Running this Advanced Hunting Query shows the URL click events and the Network Message ID associated with the URL. However, Defender fails to provide any details associated with the Network Message ID. | Screenshot

- Network Message ID: [redacted]

What is the Risk

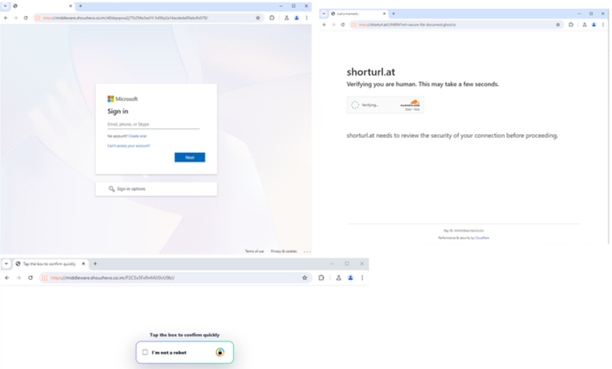
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

- Mitre: Phishing

What is Recommended

- We recommend **resetting passwords** and **revoking sessions** for any users that clicked this URL.
- Block the observed sender, sender IP, and sender domain if not necessary for production.
- Block any malicious domains observed.
- Further investigate to determine the origin of this activity.
  - If found to be from a phishing email, ensure the full removal of all emails from the sender.
  - Block the observed sender, sender IP, and sender domain if not necessary for production.
- Confirm the user did not interact with the suspicious URL past their initial click.

--



https://middleware.shouchevo.co.im/i40dspqxoa2j77b294e3ed1f-5d96a2a14acdeda00abc8c078/

https://shorturl.at/UX4BW?ref=secure-file-document.ghost.io

shorturl.at

Verifying you are human. This may take a few seconds.

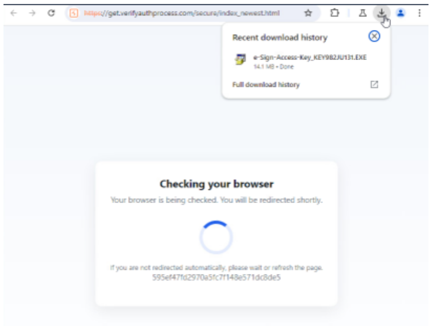
shorturl.at needs to review the security of your connection before proceeding.

https://middleware.shouchevo.co.im/P2C5x3FxRnhlVJ0vU9b!/

Tap the box to confirm quickly

□ I'm not a robot

In more advanced attempts, the CAPTCHA page instructs users to perform additional actions under the guise of verification, including copying and pasting commands into PowerShell, Command Prompt, Run, or Terminal, enabling browser permissions, or downloading small "verification" files. These actions result in the execution of malware, installation of infostealers, or theft of browser session cookies and authentication tokens.



https://get.verifyauthprocess.com/secure/index_newest.html

Checking your browser

Your browser is being checked. You will be redirected shortly.

If you are not redirected automatically, please wait or refresh the page.
595ef471d2970a5fc7f148e571dc8de5

Email Routing Misconfiguration and Internal Spoofed Phishing

Cyber threat actors are exploiting misconfigured email routing and weak spoofing protections to deliver phishing messages that appear to originate from within the target organization. These messages originate from spoofed organizations' domain and may use the same address in both the "From" and "To" fields to reinforce legitimacy. Reports note indicators such as SPF or DMARC failures, missing or improperly validated DKIM signatures, and message headers showing external delivery despite internal appearance. Lure themes include voicemail notifications, shared document alerts, HR related communications, and password reset or expiration notices. In observed campaigns, messages route users through legitimate looking intermediary links, including Google Maps URLs, before redirecting to phishing infrastructure. These campaigns have been associated with phishing as a service platforms such as Tycoon2FA, enabling credential theft and session token compromise while evading common email filtering and user scrutiny. Notably, Microsoft has warned about this vulnerability.

Effectiveness of Advanced Phishing Strategies for Enterprise Compromise

Advanced phishing campaigns exploit trust in familiar workflows, infrastructure, and visual cues while reducing the visibility of malicious activity to security controls. Fake CAPTCHA pages take advantage of user conditioning to treat verification steps as routine and low risk, leading victims to follow instructions quickly without evaluating legitimacy. When CAPTCHA workflows prompt actions such as credential entry, command execution, browser permission changes, or file downloads, attackers gain the ability to deploy malware, install infostealers, harvest session tokens, and establish persistent access under the appearance of normal user behavior.

Internal spoofed phishing is effective because messages appear to originate from within the organization. Misconfigured email routing and spoof protections allow attackers to bypass external sender warnings, while the use of identical "From" and "To" addresses reinforces legitimacy. Business relevant lure themes align with expected operational activity, and routing through legitimate looking intermediary links further lowers suspicion. User interaction enables attackers to collect credentials, capture multi factor authentication tokens, pivot into mailboxes and cloud services, and deliver follow on payloads while evading common email filtering and user scrutiny.

Combined, these techniques shift execution and trust decisions to the user, enable credential and session compromise as an initial foothold, and provide a reliable path to malware deployment, lateral movement, and broader enterprise compromise while bypassing traditional link analysis and perimeter based defenses.

Mitigation Recommendations

To mitigate the risks posed by CAPTCHA-based phishing and internal spoofed email campaigns, we recommend the following:

User Guidance

- Do not run commands or paste text into PowerShell, Command Prompt, Terminal, or Run dialogs in response to any website instructions.
- Do not install software or browser extensions as part of a verification step.
- Treat any unexpected credential or multi-factor authentication requests as suspicious, even if the message appears internal.
- Verify emails requesting account actions, document access, or password resets through a secondary channel (phone, chat, or official portal).

Organizational Guidance

- Reinforce user awareness with clear examples of fake CAPTCHA pages and internal-looking phishing messages.
- Monitor for suspicious command execution originating from browsers or triggered by user interaction with web pages.
- Harden email authentication by enforcing DMARC reject policies, SPF hard fail, and validated DKIM.
- Review mail routing and connector configurations to prevent internal spoofing and external messages appearing as internal.
- Monitor for unusual login activity, new device registrations, or anomalous session tokens that could indicate stolen credentials or infostealer activity.
- If compromise is suspected, immediately reset credentials, invalidate active sessions, and review authentication and mailbox logs for follow-on activity.

Conclusion

The threat activity outlined in this advisory reflects a continued evolution in phishing tradecraft, where attackers prioritize trust abuse and user-driven actions over exploit-based intrusion. Fake CAPTCHA workflows, internal-looking email delivery enabled by routing misconfigurations enable threat actors to bypass common detection controls and reliably obtain credentials, session tokens, and initial access. These campaigns demonstrate that phishing is no longer limited to simple credential harvesting and is increasingly used as a launch point for malware deployment, persistence, and follow-on compromise across cloud and endpoint environments. Organizations should treat user interaction with deceptive verification workflows or internal-originating messages as a high-risk event and respond accordingly by strengthening email authentication, improving visibility into user-initiated execution, and treating credential exposure as an enterprise-wide security issue rather than an isolated incident.

Further Reading

1. https://www.microsoft.com/en-us/security/blog/2026/01/06/phishing-actors-exploit-complex-routing-and-misconfigurations-to-spoof-domains/
2. https://any.run/cybersecurity-blog/click-fix-attacks-eric-parker-analysis/

The CRITICAL**START**® Cyber Research Unit will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. For future updates the CTI team will post updates via Cyber Operations Risk & Response™ Bulletins and on the CRITICAL**START**® Intelligence Hub.