

Tycoon 2FA Takedown | Cloudflare

 cloudflare.com/en-au/threat-intelligence/research/report/tycoon-2fa-takedown

Cloudflare participates in global operation to disrupt Tycoon 2FA



Overview

Cloudforce One has successfully disrupted the Phishing-as-a-Service (PhaaS) criminal enterprise known as Tycoon 2FA. First appearing in August 2023 and widely believed to be a fork of the earlier “Dadsec” phishing kit, Tycoon 2FA has a history of enabling cybercriminals to bypass multi-factor authentication (MFA) and steal session cookies.

After gaining full access to a victim’s authenticated session, subscribers to the Tycoon 2FA kit often launch Business Email Compromise (BEC) attacks using criminal-controlled “mule” accounts. Leading up to the disruption, Tycoon 2FA was one of the most popular kits for facilitating BEC attacks. In an attempt to prevent detection of their phishing kits, Tycoon 2FA group abused Cloudflare services and other legitimate infrastructure providers.

This report details Cloudforce One’s identification and tracking of Tycoon 2FA operations along with details of the coordinated disruption actions taken against this criminal enterprise in partnership with Microsoft. Central to this effort was understanding the capabilities of the PhaaS platform and its use by cybercriminals. To help others protect themselves from similar threats, this report also provides analysis of recent campaigns observed by Cloudforce One, highlighting some of the tactics, techniques, and procedures (TTPs) that define Tycoon 2FA operations.

Executive summary

- Cloudflare, in partnership with Microsoft, has taken action against Tycoon 2FA, a PhaaS platform designed to bypass MFA. It was also one of the most popular kits for facilitating BEC attacks.
- The kits abused Cloudflare Workers to host malicious logic that redirected security researchers to benign sites like Amazon to evade detection while harvesting live session tokens from targeted users.
- In March 2026, in a coordinated effort to disrupt this cybercriminal ecosystem, Cloudflare executed a technical takedown of the Workers projects and infrastructure supporting the kit. This action was coordinated with a civil legal process initiated by Microsoft's Digital Crimes Unit (DCU) to seize associated domains from registrars worldwide.
- This report provides technical details of the actor's TTPs, our disruption strategy, and how others can protect themselves from similar threats.

What is Tycoon 2FA?

Tycoon 2FA surfaced in August 2023 as a specialized evolution of earlier phishing frameworks designed to defeat MFA. The service was sold via private Telegram channels to a diverse, global customer base, with our internal telemetry confirming widespread adoption by cybercriminals across multiple regions. For a starting price of roughly \$120, these subscribers gained access to a turnkey ecosystem capable of bypassing the MFA that organizations rely on for security.

The platform functioned as a transparent reverse proxy that sits between a victim and a legitimate service like Microsoft 365 or Gmail. Unlike traditional phishing kits that simply steal static passwords, Tycoon 2FA relayed authentication prompts in real-time to capture live session tokens and cookies. This technical maneuver allowed attackers to inherit a fully authenticated session, effectively rendering SMS codes, authenticator apps, and push notifications useless.

Below is a high-level description of Tycoon 2FA functionality:

- Instead of showing you a fake static page, Tycoon proxies the real Microsoft 365 or Google login page to the victim.
- When you enter your credentials and your MFA code, Tycoon passes them to the legitimate service in real-time.
- Once the service says "Identity Confirmed," it sends back a session token. Tycoon grabs this token before it ever reaches your browser.

- The attacker imports that token into their own browser. Since the session is already "authenticated," the platform never asks them for a code.

To try to maintain the longevity of their infrastructure, Tycoon 2FA developers integrated advanced evasion techniques including the abuse of Cloudflare Workers and multi-stage redirection flows. These scripts performed rigorous anti-analysis checks to detect security researchers or automated scanners, redirecting unwanted connection attempts to benign sites like Amazon or Tesla to mask the underlying malicious intent.

Tycoon 2FA campaigns frequently extended beyond simple account access into [BEC](#) attacks. By leveraging hijacked session tokens, attackers embedded themselves within corporate email environments to monitor internal communications and financial workflows. From here, attackers could send legitimate-looking invoices from the compromised account to a third-party partner or vendor. Because the fraudulent request originated from a trusted, authenticated account, this multi-stage fraud model bypassed traditional email security filters. This allowed attackers to successfully divert payments to criminal-controlled mule accounts, resulting in significant financial losses.

Campaign analysis & threat breakdown

Tycoon 2FA campaigns leveraged diverse lures and technical vectors to compromise various industries. Detections were particularly frequent among real estate and firms specializing in AEC (Architecture, Engineering, and Construction), where attackers utilized "Payoff Letters" or "Mortgage Statements" as primary bait.

Other variants focused on HR-themed subjects like "Compensation Review" or "Payroll Benefits," often delivered via PDF attachments that impersonated local housing authorities. In some instances, the campaigns pivoted toward IT impersonation, creating urgency with notifications about blocked inbox messages.

HR-themed PDF lure, impersonating a housing authority, that embeds a QR code to redirect victims to a Tycoon 2FA phishing link.

Lure impersonating a housing authority to target employees regarding "updated compensation information".

"New Voicemail Notification" prompt to trick the user into opening a malicious HTML attachment.

Lure impersonating IT services with a French-language interface notifying targets of "blocked messages".

Tycoon 2FA abused Cloudflare Workers to act as a sophisticated proxy for login and 2FA requests. These Workers were observed proxying traffic through malicious domains like chiohe[.]biz[.]id to steal credentials and MFA codes for high-value platforms such as Microsoft,

GoDaddy, and Okta. When a victim interacted with the campaign, the Worker returned obfuscated HTML, which then loaded a heavily obfuscated script that provided the core proxy functionality.

The scripts embedded in these pages were engineered with rigorous anti-analysis protections designed to terminate the session if they detected automation markers such as navigator.webdriver, PhantomJS, or the presence of Burp Suite. To prevent manual inspection, the actors implemented defensive lockdowns that disabled right-click context menus and common keyboard shortcuts like “F12” and “Ctrl+U”. They further employed an anti-debugger loop that used “debugger” statements to measure processing lag; if a delay of more than 100ms was detected—typically signifying that browser Developer Tools were open—the script would immediately redirect the visitor to a benign site like Overstock or Amazon.

Sandbox [analysis](#) confirms that, if anti-analysis measures were passed, the final payload was often a Microsoft 365 or Gmail credential harvesting page. From here, the phishing kit would fingerprint the victim's browser and geolocation, capture their credentials, encrypt the data with AES using the CryptoJS library, and exfiltrate it to a remote command-and-control server. As highlighted earlier, these credentials were often subsequently leveraged to facilitate BEC.

Disruption

On March 4th, 2026, Cloudforce One joined Microsoft in a massive, multi-partner operation designed to dismantle Tycoon 2FA's infrastructure across both the legal and technical fronts. Microsoft initiated the process by identifying and analyzing domains specifically used in attacks against its global customer base.

Microsoft shared these findings with a network of strategic partners, including Cloudflare, to expand the scope of the investigation and synchronize a global disruption operation aimed at dismantling the Tycoon 2FA infrastructure. Through extensive research and analysis of the infrastructure, Cloudflare was able to identify the broader footprint of the actor, uncovering thousands of related domains—including several that were staged but not yet active in live campaigns.

The operation proceeded through several concurrent but coordinated layers of enforcement:

- Microsoft’s civil action: Microsoft filed a civil action in a U.S. court to legally compel international domain registrars to suspend malicious domains and transfer control to Microsoft’s Digital Crimes Unit.
- Mass infrastructure purge: Cloudflare separately executed a comprehensive sweep to clear out all zones associated with the threat, resulting in the banning of thousands of domains and Workers projects.

- Killing Worker scripts and suspending accounts: Beyond taking action against Tycoon 2FA domains, Cloudflare suspended the related threat actor accounts and killed all associated Workers scripts to block the kit's proxy functionality at the edge.
- Law enforcement coordination: Europol played a central role in the operation, coordinating law enforcement actions across various national agencies in countries where Tycoon 2FA victims were identified.

Because the registrars for some of these 24,000 domains are located in non-cooperative jurisdictions, technical intervention remained a critical failsafe. For any infrastructure that could not be legally seized, Cloudflare deployed interstitial warning pages. This ensures that any victim attempting to access a Tycoon 2FA link is blocked by a high-visibility security alert, effectively neutralizing the phishing kit even if the underlying domain remains technically active on the internet.

Mitigation and detection

Effective defense against Tycoon 2FA and similar PhaaS platforms requires email security solutions that rely on proactive identification of delivery infrastructure and advanced behavioral detection models. Cloudflare Email Security maintains this defensive posture through the use of Email Detection Fingerprints (EDF) alongside continuous refinement of specialized detection logic designed to adapt to the actor's shifting tactics. Tailored detections like those provided below identify and neutralize these campaigns at the ingestion point:

- RVT.CSRF.HTML_Base64_Ratio_Compression.JS_DOM_SCRIPT.Phishing
- Tycoon2FA.Downloader.Link
- Tycoon2FA.Downloader.Link.2
- Tycoon2fa_Bing_Redirect
- Tycoon2fa_Campaign.Recipient_Email_On_Parent_Url.Decode_Diagnostic
- Tycoon2fa_Campaign.Parameters_Farnlly
- Tycoon2fa_Campaign.ClientDomain_Subject.Recipient_Email_On_Parent_Url
- Tycoon2fa_Campaign.Email_Address_On_Url.Encoded.Phishing
- Tycoon2fa_Mixpanel_Phishing_Campaign

These detections evaluate domain reputation, alongside capabilities to identify suspicious sentiment and branding within the messages. We combine these high-confidence detections in our production environment along with proactive threat hunting techniques to identify emerging

email-based threats. Additionally, these detections leverage our machine learning models, which analyze email content, sentiment and metadata to detect and flag malicious messages.

Recommendations

Cloudflare recommends the following steps to mitigate threats from PhaaS operations like Tycoon 2FA.

Upgrade to phishing-resistant MFA

- Adopt FIDO2/WebAuthn: Use hardware keys (YubiKeys) or Passkeys. They use a cryptographic handshake that fails if the URL is even slightly off.
- Deploy Certificate-Based Auth (CBA): Restrict access to devices with unique, pre-installed digital certificates to ensure only trusted hardware can connect.

Implement strict conditional access

- Require managed devices: Block any login attempt not coming from a corporate-enrolled device (via Intune/Jamf).
- Enforce geofencing: Block traffic from high-risk regions or countries outside your operational footprint.
- Flag impossible travel: Trigger immediate alerts for sessions that jump vast distances faster than a plane can fly.

Harden session integrity

- Enable token binding: Lock session tokens to the specific TLS connection; stolen cookies become useless on an attacker's machine.
- Shorten session lifespans: Force frequent re-authentication to shrink the "window of opportunity" for stolen tokens.
- Use Continuous Access Evaluation (CAE): Kill active sessions instantly if a user's IP changes or risk levels spike.

Strengthen network & email defenses

- DNS filtering: Automatically block "newly registered domains" to stop fresh phishing links in their tracks.
- AI-driven email security: Use tools like Cloudflare to identify real-time infrastructure fingerprints used by platforms like Tycoon.

- Sandboxing & deep inspection: Detonate links in isolated environments to expose hidden redirects before they reach the user.
- Strict DMARC/SPF/DKIM: Move to a "Reject" policy to prevent brand spoofing and unauthorized sender impersonation.

In addition, we provide all organizations (whether a Cloudflare customer or not) with free access to our email Retro Scan tool, allowing them to use our predictive AI models to scan existing inbox messages. Retro Scan will detect and highlight any threats found, enabling organizations to remediate them directly in their email accounts. With these insights, organizations can implement further controls, either using Cloudflare Email Security or their preferred solution, to prevent similar threats from reaching their inboxes in the future.

Indicators of compromise

The domains listed below represent a small snapshot of the more recent infrastructure associated with the Tycoon 2FA enterprise. The table constitutes only a fraction of the extensive indicators tracked by Cloudforce One. Cloudforce One customers can access the complete list of indicators and associated analytical context via the [Threat Events platform](#). To support global mitigation efforts, the disruption operation involved disseminating the IOCs to participating national CERTs, government agencies, and strategic industry partners.

Malicious Domains

serviciosdrc[.]com

agousa[.]org

hpcbjoukzdlx[.]es

wvhjkdig[.]ru

hrcbods[.]es

qkmuadvkc[.]es

rkbfoavkwgn[.]es

djxrc[.]ru

Malicious Domains

kfrutc[.]ru

uywwpjlanfv[.]ru

nwd[.]hpcbjoukzdlx[.]es

x5l4l[.]wvhjkdig[.]ru

xiuwx[.]hpcbjoukzdlx[.]es

y9oln[.]wvhjkdig[.]ru

Email Detection Fingerprints (EDF)

2b8e9ee98cc7addb50f3b101f78157ad0a9f:f64406156750c40cbdedcd9bec33

f747790170959f314805d60a8a128bbd4a20:d1319d8cfc9d439493bded0d3c86

e8a50f92ea2215ea8d19772c549555ca423a:5b3569164caed5175d0746b9f657

79bd63a413f63b37cfba99975b1403d2d0e6:4455c9d316072f822988e6bc12cb

HTML Structure Hashes (SHA256)

c46289f3f7c486d684783ec50a01a437252eabd0159e7efd7594afcaf242c7bb

9f6d91dda0a3c4d5054e78e90f30d2f0c98c79a03cb16d58819f0cb58d9c3abb

66a5b9c0d963dd910a502749eec42d6660b27aafa09b9ce01d73e3f73754b707

0499fdfcb2fddfd2e5d3f3eab2910ff2854208a8140e514cf5f1f39e12b7c55b