Technical report

TLP:CLEAR

Global analysis of Adversary-in-the-Middle phishing threats

Quentin Bourgue, Grégoire Clermont and TDR team, June 2025

sekoia

Table of contents

Introduction

In recent years, organisations have increasingly encountered **massive and more sophisticated phishing attacks** that primarily target Microsoft 365 and Google accounts **using Adversary-in-the-Middle (AitM) technique**. This growing trend has been amplified by the **proliferation of Phishing-as-a-Service (PhaaS) offerings in the cybercrime ecosystem.** These services provide access to advanced phishing kits for a wide range of cybercriminals, including those with limited technical skills, at a lower cost.

AitM phishing kits mainly aim to **harvest session cookies** from targeted services to **bypass the Multi Factor Authentication (MFA) process during subsequent logins**. To achieve this, AitM phishing servers relay user inputs, including usernames, passwords and MFA codes, to the legitimate authentication API while intercepting the returned session cookie. With that cookie, an attacker can replay the session, and access the victim's account without needing to perform any further authentication. Such compromises frequently lead to **significant financial losses via Business Email Compromise (BEC) operations**, financial fraud, or even Big Game Hunting ransomware attacks.

The Sekoia Threat Detection & Research (TDR) team closely monitors the AitM phishing attacks and regularly provides technical reports on emerging kits that we uncover through our daily threat hunting routine. This **global report delves into the threat posed by AitM phishing**, offering both contextual and operational insights. Using our telemetry data and research findings, this report explores current trends in the AitM phishing landscape and the prevalence of leading kits.

Additionally, the report delivers valuable and actionable intelligence to help analysts detect, identify and investigate the AitM phishing threat. It highlights detection opportunities and includes concise sheets for the eleven most widespread AitM phishing kits as of Q1 2025.

Key takeaways

> Since 2023, the TDR team has actively monitored Adversary-in-the-Middle (AitM) phishing threats by developing detection rules, uncovering adversary infrastructure, and tracking prevalent tactics, techniques, and procedures (TTPs).

> Sekoia's TDR team has developed a methodology based on telemetry, adversaries' infrastructure tracking, and campaigns monitoring to rank the most active AitM phishing threats from January to April 2025.

> According to this methodology, the most widespread phishing kits are Tycoon 2FA, Storm-1167, NakedPages, Sneaky 2FA, EvilProxy, and Evilginx.

> Over the past months, threat actors have rapidly adopted new TTPs in high volume AitM phishing campaigns, transitioning from QR codes to HTML attachments and more recently to SVG files for link distribution.

> Numerous fully-featured and turnkey AitM phishing kits are readily available within the cybercrime ecosystem, offered at low cost and requiring minimal technical expertise.

> The cybercrime ecosystem specialising in AitM phishing and Business Email Compromise (BEC) attacks is becoming increasingly professional, providing a broader suite of products and services.

> This report includes an overview sheet for 11 relevant AitM phishing kits, providing analysts with technical details, tracking and detection opportunities.

Glossary of AitM terminology

Understanding Adversary-in-the-Middle (AitM) phishing involves grasping several technical concepts. To facilitate this comprehension, we have compiled a glossary of key terms associated with this threat.

- **Phishing-as-a-Service (PhaaS)**
  Phishing-as-a-Service is a subscription-based model that provides cybercriminals with access to phishing kits and associated services. Most PhaaS platforms also offer additional features, such as anti-bot webpages, HTML and SVG attachment templates, and data forwarding to Telegram bots.

- **Operator**
  In the PhaaS model, the operators are responsible for managing the entire service. This includes maintaining the kit's source code, operating the shared infrastructure, advertising and selling the service, and providing customer support.

- **Affiliate**
  Affiliates are cybercriminals who subscribe to PhaaS service. They usually pay a licence fee to access either a version of the kit's source code or a web-based platform for managing phishing pages. Affiliates' activities involve building target lists, conducting email campaigns, and monetising successful phishing attacks through Business Email Compromise (BEC).

- **Reverse proxy**
  A reverse proxy server acts as an intermediary between the user's device and the legitimate authentication service, relaying traffic and capturing sensitive user data in the process. This AitM method enables attackers to replicate authentication pages and intercept user requests. Phishing kits such as Evilginx, EvilProxy, and NakedPages use reverse proxy servers.

- **Synchronous relay**
  The synchronous relay method involves phishing kits cloning legitimate authentication webpages to harvest user data, which is then forwarded to the legitimate authentication service in real time. Synchronous relay servers enable attackers to customise phishing pages. PhaaS platforms like Tycoon 2FA, Sneaky 2FA and Mamba 2FA employ synchronous relay servers.

- **Centralised infrastructure**
  Within the PhaaS model, phishing kits generally rely on two types of infrastructure: servers that host phishing pages and servers that manage centralised functions such as licence verification and authenticating interactions with the legitimate services. While phishing pages are primarily hosted on servers controlled by affiliates, operators manage the centralised infrastructure.

- **Anti-bot capabilities**
  Most phishing kits are equipped with anti-bot capabilities to prevent their pages from being detected by automatic scanners. These capabilities include CAPTCHA pages requiring human interaction, traffic filtering based on device fingerprinting (such as operating system, browser, IP address), code obfuscation, and URL randomisation.

Adversary-in-the-Middle (AitM) phishing attacks

Threat actors increasingly conduct AitM phishing attacks, employing continuously evolving spearphishing techniques and leveraging a variety of kits available within the cybercrime ecosystem. Our analysis, along with open-source reporting, indicates that most AitM attacks rely on a common set of tactics, techniques, and procedures (TTPs).

AitM phishing pages predominantly target Microsoft 365 and, to a lesser extent, Google accounts - platforms that are prevalent in professional environments. Compromising these cloud accounts allows attackers to steal operational information from email inboxes, calendars, document storage, as well as to impersonate their victims.

The following section outlines the typical approaches used by attackers, from social engineering lures to Business Email Compromise (BEC) attacks.

Social engineering lures

AitM phishing campaigns primarily target employees in finance, sales, human resources, and executive roles, capitalising on their connection to financial operations to facilitate BEC and other fraud. These large-scale campaigns now hit organisations worldwide.

The lures used in email phishing campaigns typically involve corporate matters, such as:

- **Financial**: bonus distribution, invoice queries, benefits enrollments, compensation adjustment, tax reviews, contract renewals.

- **Human resources**: vacations, salaries, payrolls notification, policy agreements, employee handbooks.

- **IT and security**: policy updates, secured documents, messages, signature reviews.

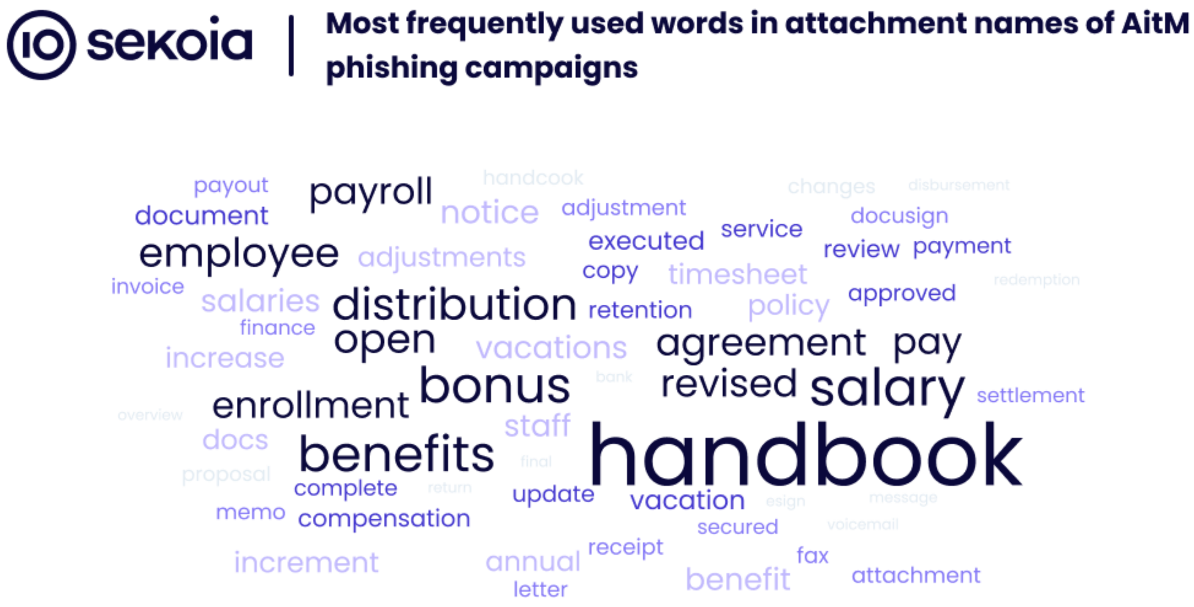


Figure 1. Most frequently used words in attachment names of AitM phishing campaigns, as observed by Sekoia (January-April 2022)

These phishing emails often use either attachments, such as PDF, SVG and HTML documents, or embed links in the email body that redirect users to malicious websites.

To trick victims, attackers commonly rely on the following social engineering strategies:

- **Impersonation of trusted entities**
  To establish trust, attackers spoof the sender's display name or email address to pose as legitimate services such as Microsoft, Google, Adobe and DocuSign, or to impersonate organisation's departments, or executives.

- **Urgency**
  To prompt immediate action and defeat potential scepticism, the content of the phishing email highlights the urgency of the required action, often using a deadline or a potential restriction.

- **Confidentiality requirement**
  To prevent internal communication about the phishing email and isolate the victim, the message may invoke a privacy policy or claim that a personal document should not be shared.

- **Security guarantee**
  To gain confidence, the email may include a footer indicating a security scan that supposedly certified the email is safe, creating a false sense of confidence.

Many AitM phishing emails combine one or more of these strategies to maximise effectiveness.

Common TTPs

As with other social engineering lures, most attackers follow similar TTPs during the stages leading up to a fake authentication page, including the initial malicious email, incorporating one or more redirection steps, and deploying anti-bot features.

In 2023, Sekoia analysts identified that adversaries had largely adopted the tactic of embedding **QR codes within documents** to redirect users to AitM phishing pages. By mid-2025, this technique remained widespread, even as security products became more effective at detecting phishing links distributed through QR codes.

Since 2024, we have seen a rise in the **use of HTML attachments** that directly execute JavaScript to render phishing pages. Two factors contribute to the emergence of this trend: these attachments are potentially less detectable by email security tools, resulting in higher success rate for email spamming campaigns. Additionally, several PhaaS providers, such as Mamba 2FA, Tycoon 2FA and Greatness, now offer ready-to-use HTML phishing templates to their customers, accelerating the adoption of this technique.

In early 2025, we noted a significant surge in the use of **malicious SVG attachments** leveraged to redirect victims to AitM phishing pages. First observed at the end of 2024, this technique involves SVG files that contain either JavaScript or an `xlink:href` attribute[1]. By April 2025, we observe that cybercriminals are making extensive use of malicious SVG attachments for both phishing and malware distribution, likely reflecting improved distribution and compromise rates.

Regardless of whether attackers begin with QR code, HTML attachments, or documents-embedded links, the final stage is to redirect users to a final phishing page. To evade email filters and prevent scanners from accessing malicious domains, adversaries frequently insert one or more redirection steps. These steps often make use of legitimate domain names to build user trust and avoid detection by automated scanning tools. Attackers commonly exploit the **"open redirect" vulnerabilities**, injecting malicious URL into user-controlled parameters within legitimate applications to redirect visitors to arbitrary websites. In specific terms, open redirects rely on a URL parameter that specifies the destination link for the user.

Redirection pages controlled by adversaries often incorporate **traffic filtering mechanisms**, ensuring that the phishing page is displayed only to likely targets. This filtering may rely on either custom or commercialised traffic distribution systems (TDS) or on checks of users' device characteristics. Typically, these mechanisms verify that the user's IP address originates from a residential internet service provider (ISP), and that the operating system and web browser are consistent with those used in corporate environments. For example, the Tycoon 2FA PhaaS integrates the BlackTDS service to prevent distributing phishing pages from being served to bots and analysis environments[2], while Mamba 2FA uses Adspect TDS[3] for similar purposes.

[1] https://developer.mozilla.org/en-US/docs/Web/SVG/Reference/Attribute/xlink:href
[2] https://rmceoin.github.io/malware-analysis/2024/12/26/antibot2.html
[3] https://rmceoin.github.io/malware-analysis/2024/12/21/antibot1.html

Finally, in most AitM phishing campaigns, the malicious page is protected by a **CAPTCHA requiring human interaction**. These anti-bot webpages are usually provided by the PhaaS and integrate legitimate services (such as Cloudflare Turnstile, reCAPTCHA, hCaptcha), open-source solutions (like IconCaptcha), or custom CAPTCHAs.

Only after successfully navigating all these steps, users land on the AitM phishing page, which typically mimics either a Microsoft 365 or a Google authentication portal.

Business Email Compromise (BEC) attacks

Upon compromising cloud accounts, attackers use gained access to conduct further BEC attacks, mainly focused on financial fraud, including:

- **Internal and external spearphishing**: using a compromised employee account to impersonate them in a follow-up phishing campaign.
- **Data exfiltration**: extracting documents from email inboxes and cloud storage.
- **Various fraudulent transactions**: modifying banking details, issuing fake invoices, or instructing employees to transfer funds.

Successful financial fraud demands a comprehensive understanding of the victim's role, the organisation's workflow, and both internal and external people interactions. Adversaries may spend days or weeks on reconnaissance.

To maintain access, attackers often add their own 2FA method after compromising the account, ensuring they can still access it even if session cookies are revoked. They may also create email forwarding rules that automatically redirect incoming messages to an attacker controlled email address, enabling continued information gathering even after the victim resets their account.

It is essential to note AitM phishing is also leveraged by espionage groups, such as the Russian state-sponsored intrusion set Calisto[4], as well as various Chinese groups[5]. Their motivations, goals and TTPs differ from those of financially motivated intrusion sets and are not detailed in this report.

[4] https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-war-support/

[5] https://www.justice.gov/opa/media/1391896/dl

Phishing-as-a-Service ecosystem

The PhaaS model lowers the entry barrier for threat actors by providing AitM phishing capabilities without requiring significant technical expertise or resources. This enables cybercriminals to achieve a quick return on investment.

The following section provides an overview of the current PhaaS ecosystem, highlighting the primary strategies employed by the PhaaS operators.

Typology of PhaaS offerings

AitM phishing kits are typically **sold via monthly subscription plans**, ranging from $100 to $1,000. PhaaS platforms offer a **variety of features**, including email and **attachment templates**, **anti-bot capabilities**, an administration panel for managing campaigns and harvested data, and data forwarding to Telegram. The quality and completeness of these offerings enable cybercriminal services to differentiate themselves from competitors.

While most PhaaS providers offer customers source code that partially or fully implements AitM capabilities, requiring deployment on the client's own infrastructure, other PhaaS operators host fully operational phishing pages on behalf of their clients. This type of service makes AitM phishing kits even more accessible to cybercriminals with limited technical skills.

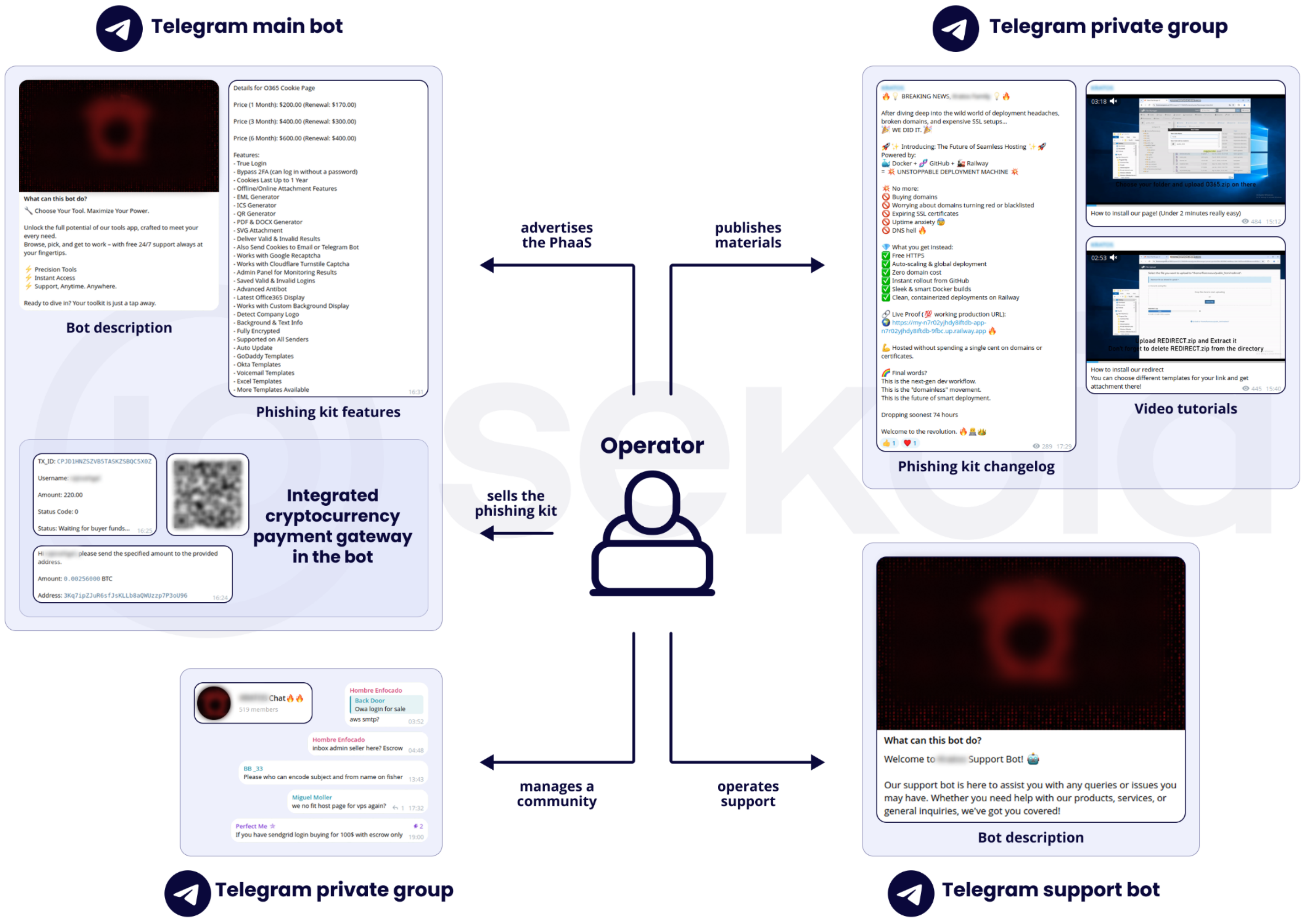
Sales and distribution of PhaaS offerings typically **occur via Telegram channels** and private groups. These cybercrime services frequently use Telegram bots integrated with cryptocurrency payment gateways to streamline transactions and manage affiliate licences. PhaaS operators also use these channels to publish product changelogs and provide tutorials or videos that guide affiliates through onboarding and adopting new platform features.

Some PhaaS operators organise Telegram groups to foster a community where affiliates can seek help, discuss their operations, and trade data or services.

Additionally, we observed the use of secured messaging applications like Signal, Session, SimpleX, and Tox for similar purposes, although far less popular.

To illustrate the PhaaS model described above, the following figure examines the main operations conducted by the operator of Sneaky 2FA through Telegram.

Typical Phishing-as-a-Service (PhaaS) model for AitM phishing kits



What can this bot do?

🔧 Choose Your Tool. Maximize Your Power.

Unlock the full potential of our tools app, crafted to meet your every need.
Browse, pick, and get to work – with free 24/7 support always at your fingertips.

⚡ Precision Tools
⚡ Instant Access
⚡ Support, Anytime. Anywhere.

Ready to dive in? Your toolkit is just a tap away.

Details for O365 Cookie Page

Price (1 Month): $200.00 (Renewal: $170.00)

Price (3 Month): $400.00 (Renewal: $300.00)

Price (6 Month): $600.00 (Renewal: $400.00)

Features:
- True Login
- Bypass 2FA (can log in without a password)
- Cookies Last Up to 1 Year
- Offline/Online Attachment Features
- EML Generator
- ICS Generator
- QR Generator
- PDF & DOCX Generator
- SVG Attachment
- Deliver Valid & Invalid Results
- Also Send Cookies to Email or Telegram Bot
- Works with Google Recaptcha
- Works with Cloudflare Turnstile Captcha
- Admin Panel for Monitoring Results
- Saved Valid & Invalid Logins
- Advanced Antibot
- Latest Office365 Display
- Works with Custom Background Display
- Detect Company Logo
- Background & Text Info
- Fully Encrypted
- Supported on All Senders
- Auto Update
- GoDaddy Templates
- Okta Templates
- Voicemail Templates
- Excel Templates
- More Templates Available

16:31

TX_ID: CPJD1HNZSZVB5TASKZSBQC5X0Z

Username: [redacted]

Amount: 220.00

Status Code: 0

Status: Waiting for buyer funds... 16:25

Hi [redacted] please send the specified amount to the provided address.

Amount: 0.00256000 BTC

Address: 3Kq7ipZJuR6sfJsKLLb8aQWUzzp7P3oU96 16:24

[redacted] Chat🔥🔥
519 members

Hombre Enfocado
Back Door
Owa login for sale
aws smtp? 03:52

Hombre Enfocado
inbox admin seller here? Escrow 04:48

BB _33
Please who can encode subject and from name on fisher 13:43

Miguel Moller
we no fit host page for vps again? 1 17:32

Perfect Me ☆ 2
If you have sendgrid login buying for 100$ with escrow only 19:00

[redacted]
🔥💡 BREAKING NEWS, [redacted] 💡🔥

After diving deep into the wild world of deployment headaches, broken domains, and expensive SSL setups...
🎉 WE DID IT. 🎉

🚀✨ Introducing: The Future of Seamless Hosting ✨🚀
Powered by:
🐳 Docker + 🧬 GitHub + 🚂 Railway
= 💥 UNSTOPPABLE DEPLOYMENT MACHINE 💥

💥 No more:
🚫 Buying domains
🚫 Worrying about domains turning red or blacklisted
🚫 Expiring SSL certificates
🚫 Uptime anxiety 😰
🚫 DNS hell 🔥

💎 What you get instead:
✅ Free HTTPS
✅ Auto-scaling & global deployment
✅ Zero domain cost
✅ Instant rollout from GitHub
✅ Sleek & smart Docker builds
✅ Clean, containerized deployments on Railway

🔗 Live Proof (💯 working production URL):
🌍 https://my-n7r02yjhdy8iftdb-app-n7r02yjhdy8iftdb-9fbc.up.railway.app 🔥

💪 Hosted without spending a single cent on domains or certificates.

🌈 Final words?
This is the next-gen dev workflow.
This is the "domainless" movement.
This is the future of smart deployment.

Dropping soonest 74 hours

Welcome to the revolution. 🔥🧑‍💻👑
👍 1 ❤️ 1 289 17:29

[redacted]
How to install our page! (Under 2 minutes really easy)
484 15:12

[redacted]
How to install our redirect
You can choose different templates for your link and get attachment there!
445 15:40

What can this bot do?

Welcome to [redacted] Support Bot! 🤖

Our support bot is here to assist you with any queries or issues you may have. Whether you need help with our products, services, or general inquiries, we've got you covered!

Figure 2. Typical Phishing-as-a-Service (PhaaS) operations for AitM phishing kits

Timeline of prominent PhaaS

Over the past few years, we have witnessed the emergence and widespread adoption of multiple PhaaS platforms. The following section presents a graphical overview of their evolution, along with relevant background information.

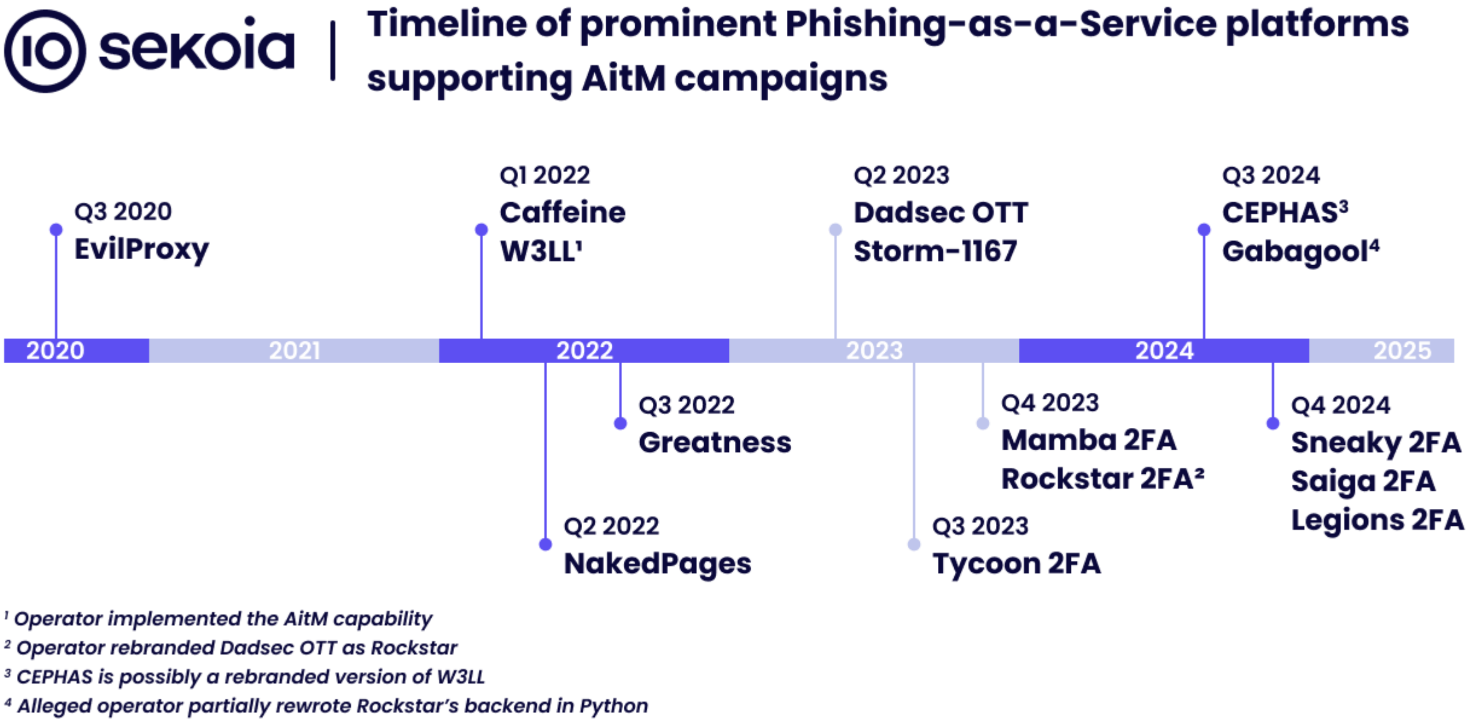

sekoia
Timeline of prominent Phishing-as-a-Service platforms supporting AitM campaigns
Q3 2020
EvilProxy
Q1 2022
Caffeine
W3LL¹
Q2 2023
Dadsec OTT
Storm-1167
Q3 2024
CEPHAS³
Gabagool⁴
2020
2021
2022
2023
2024
2025
Q3 2022
Greatness
Q2 2022
NakedPages
Q4 2023
Mamba 2FA
Rockstar 2FA²
Q3 2023
Tycoon 2FA
Q4 2024
Sneaky 2FA
Saiga 2FA
Legions 2FA
¹ Operator implemented the AitM capability
² Operator rebranded Dadsec OTT as Rockstar
³ CEPHAS is possibly a rebranded version of W3LL
⁴ Alleged operator partially rewrote Rockstar's backend in Python

Figure 3. Timeline of prominent Phishing-as-a-Service offering AitM phishing kits, between 2020 and 2025 as monitored by Sekoia

EvilProxy has been offered as-a-service on the *Exploit* cybercrime forum since August 2020, later expanding to the *XSS* forum (July 2022), as well as on Telegram. The operator promoted the kit using terms such as "Phishing-as-a-Service" and "reverse proxy".

The Microsoft Threat Intelligence team reported[6] that phishing campaigns employing AitM capabilities have significantly increased since mid-2021, possibly using the EvilProxy service and the open-source tool Evilginx.

In 2022, the services **Caffeine**, **NakedPages** and **Greatness** were released and sold on Telegram. The same year, W3LL integrated AitM capabilities into its phishing kit to target Microsoft 365 accounts. Although all three AitM phishing kits have been used for several years, NakedPage and Greatness remain among the most prevalent in 2024 and early 2025.

[6] https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

In a June 2023 report on AitM phishing and BEC attacks[7], Microsoft Threat Intelligence mentioned a new synchronous AitM phishing kit operated by a threat actor tracked as **Storm-1167**. TDR has been monitoring the related adversary infrastructure and assess with high confidence that the Storm-1167 phishing kit is part of a PhaaS offering with hundreds of customers as of April 2025.

In October 2023, we analysed the new **Dadsec OTT** phishing kit sold as-a-service[8], which emerged in May 2023 and was quickly adopted by threat actors. By the end of that year, it became one of the most popular phishing pages platforms. We believe this PhaaS was rebranded as **Rockstar 2FA** around December 2023.

Later in 2023, while analysing the trendy QR code phishing campaigns, TDR analysts uncovered the new **Tycoon 2FA** phishing pages operated by the Tycoon Group's PhaaS[9], which partially reused the Dadsec OTT source code. Since then, Tycoon 2FA has become the most widely used PhaaS.

We also published findings on another new AitM phishing kit, dubbed **Mamba 2FA**[10], which has been in use since at least November 2023. Following our in-depth analysis, we concluded that Mamba 2FA was sold as-a-service to dozens of affiliates.

In 2024, several new AitM phishing kits, including **Sneaky 2FA**, **CEPHAS**, **Gabagool**, **Saiga 2FA** and **Legions 2FA** entered the market, allegedly under the PhaaS model. Although phishing pages associated with these emerging services are not as widespread as those of established players, they are gradually gaining ground. For instance, our SOC platform recorded a surge in Sneaky 2FA detections during Q1 2025, nearing those of the top 5 AitM phishing threats.

Tools and services to set up phishing attacks

In addition to PhaaS offerings, various **tools and services are available in the cybercrime ecosystem to facilitate the set up of phishing attacks**. These resources support AitM techniques, as well as more generic phishing activities.

To operate their spamming email campaigns, threat actors use email sending software, often referred to as "sender" or "mailer", or delivery services that bundle multiple capabilities. These capabilities include generating email content, attachments, and headers, but also sending bulk emails and managing SMTP configurations. Cybercriminals use both legitimate email sending tools or services, such as SendGrid, Mailgun, and Mailchimp, and custom tools that offer features better suited for phishing activities. These features may include proxy servers rotation, obfuscation of attachments, and email spoofing.

[7] https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/

[8] https://app.sekoia.io/intelligence/objects/report--2f39b32d-42e8-4453-9ca7-9cd1954991e4

[9] https://x.com/sekoia_io/status/1717891843105366409

[10] https://blog.sekoia.io/mamba-2fa-a-new-contender-in-the-aitm-phishing-ecosystem/

To maximise deliverability, cybercriminals might purchase services to “warm up” SMTP domains and servers for weeks or months before launching their spamming campaigns. This warming service involves SMTP infrastructure for benign activities initially, helping them build reputation and prevent their phishing traffic from being flagged or blocked by security solutions.

Additionally, adversaries can purchase the following from specialised threat actors:

- Mailing list data, also known as “leads”
- “SMTP checkers” to verify and parse lists of email addresses
- Access to compromised email address within specific domain names
- Pre-configured or compromised SMTP servers
- Attachment templates or code for anti-bot or redirection infrastructure
- Traffic Distribution System (TDS) services

Investigating AitM phishing threats: methods and findings

Since 2023, the TDR team has actively monitored AitM phishing threats by developing detection rules, creating tracking heuristics, uncovering phishing infrastructures, and unveiling campaigns using malicious attachments, URLs, or redirection steps.

The following section outlines the monitoring techniques we employ, discussing their advantages and limitations, and provides an overview of prominent phishing kits as of early 2025.

TDR monitoring of AitM phishing threats

Detection and CTI production

To ensure broad coverage of AitM phishing threats, the TDR team primarily focuses on writing detection rules and tracking the adversaries' infrastructure.

Our detection efforts concentrate on anomalies and characteristic patterns in Microsoft Entra ID authentication logs to identify successful AitM phishing attempts. Synchronous phishing kits often contain inconsistencies in User-Agent and Application ID values during authentication, which we correlate using Sigma detection rules. Further details on detection opportunities can be found in the section titled "Detection opportunities".

Additionally, some detection strategies are based on the URL and subdomain patterns used by certain AitM phishing kits.

Adversary infrastructures Indicators of Compromise (IoCs) collected by TDR include domain names and servers hosting anti-bot and phishing pages, those involved in exfiltration of harvested data, and IP addresses communicating with legitimate authentication services, notably the Microsoft API.

Our methodology involves proactive heuristics to identify active servers by analysing HTTP responses, HTML pages, and URL patterns. To achieve this, we rely on both scanning search engines like Censys, urlscan.io, Virus Total, or conducting targeted scanning campaigns on phishing endpoints.

Sekoia.io telemetry

By analysing telemetry data from our detection rules alongside actionable CTI on the Sekoia SOC platform, we gain valuable insights into the most widespread kits. Before presenting the results, we outline some strengths and limitations of Sekoia.io telemetry.

- **CTI-based telemetry**
  The Sekoia SOC platform records hits of Indicators of Compromise (IoCs) derived from our tracking heuristics. This metric measures phishing kits' prevalence by observing network logs in environments monitored by Sekoia.io. The main advantage is the proactive monitoring of adversary infrastructures, such as anti-bot and phishing domains and exfiltration servers, detected through network monitoring.

  For self-hosted phishing kits, monitoring the number of active servers gives a good insight into how many affiliates are using a given PhaaS offering.

  However, coverage bias can arise due to different levels of complexity in tracking the servers for different phishing kits. Additionally, this telemetry relies on scans which may be delayed by a few days compared to the actual infrastructure deployment.

- **Pattern-based telemetry**
  Detections generated by our rules on customer logs, primarily leveraging anomalies in Microsoft Entra ID audit logs. This real-time detection approach relies on unique rules, often resilient over time with low false positive rates, that catch most AitM phishing attacks for a given kit.

  The main limitation is the reliance on identifiable anomalies specific to the phishing kit, that are mostly introduced by the developer for synchronous AitM phishing kits.

General biases of our telemetry include the predominance of data from European-based organisations with a certain cybersecurity maturity to collect Entra ID logs and ingest them into the SOC platform.

The figure below presents insights from for both CTI and detection-based telemetry in the Sekoia SOC platform.

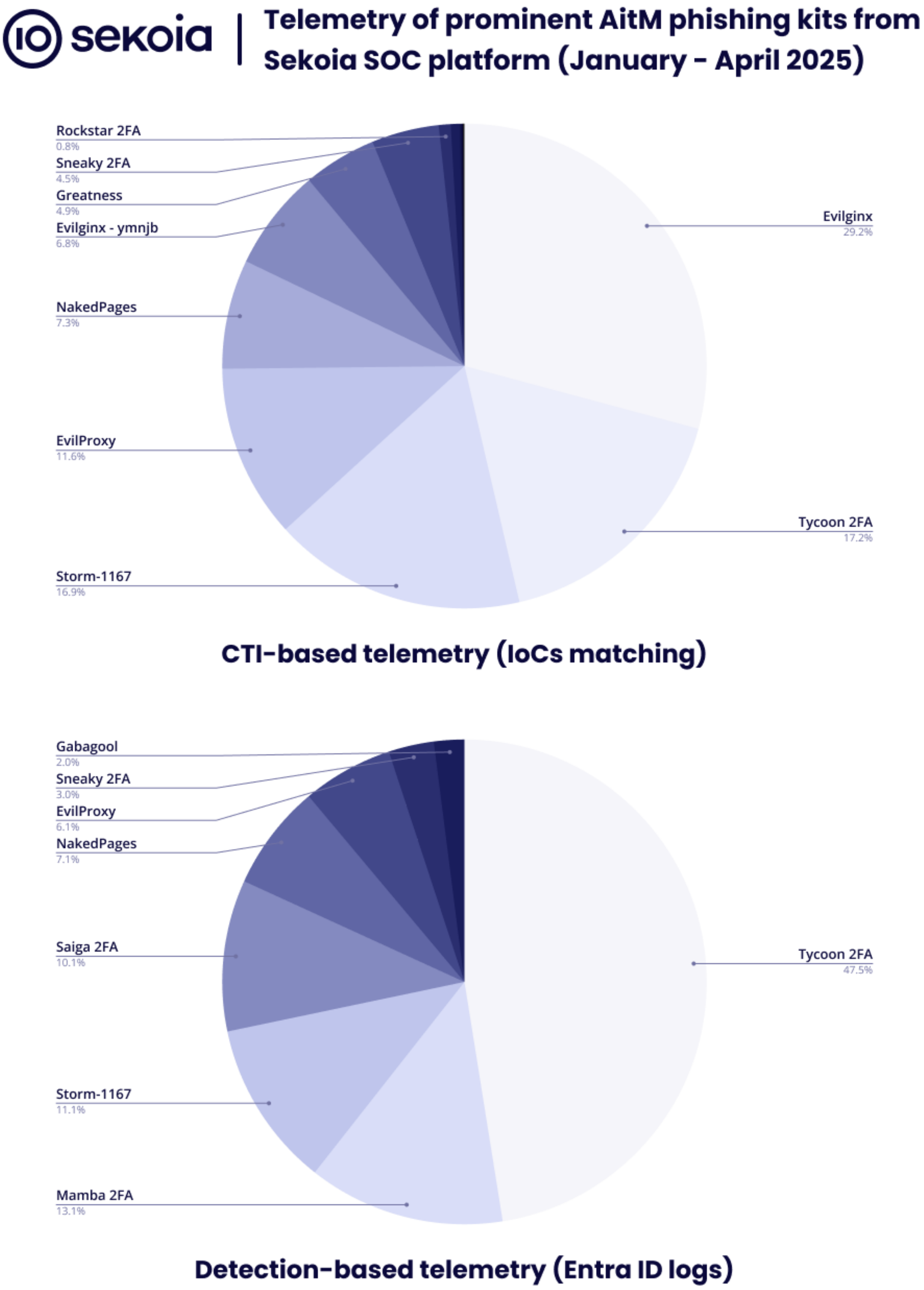


Figure 4. Telemetry of prominent AitM phishing kits from Sekoia SOC platform

Hunting AitM phishing campaigns in the wild

To offset biases in our telemetry, we engage threat hunting by employing multiple tracking strategies across various services to monitor AitM phishing campaigns in the wild.

Since the widespread adoption of QR codes redirecting to AitM phishing pages in 2023, we have been actively monitoring attachments embedding these QR codes. By searching for documents (PDF, HTML, DOC, *etc.*) that embed QR codes redirecting to CAPTCHA services like Cloudflare Turnstile, hCaptcha or reCAPTCHA we can identify numerous attachments used in AitM phishing campaigns. These documents typically redirect users to anti-bot webpages. By analysing the resulting URLs, we can identify which phishing kits are being used and to map prevailing trends. Moreover, this proactive approach helps uncover emerging phishing kits.

While most PhaaS implementations rely on anti-bot webpages using CAPTCHA services with human interaction checks, some - like Mamba 2FA or Greatness - do not use them. Therefore, this approach does not cover all AitM phishing kits.

We also use signatures to detect malicious SVG and HTML files, which are widely used in early 2025, as well as anti-bot and lure webpage templates, that are commonly employed by various cybercriminals.

This proactive threat hunting provides a comprehensive overview of various phishing campaigns targeting organisations worldwide, and supplements our insights obtained with Sekoia.io CTI and detection telemetry.

Most relevant phishing kits

By using the methodologies described above, our monitoring of AitM phishing threats from January to April 2025 resulted in the following prevalence table.

For each AitM phishing kit, we assigned a score (out of 5) to assess its prominence based on observations from our telemetry, adversary infrastructure monitoring, and threat hunting activities.

AitM phishing kit	CTI telemetry	Detection telemetry	Number of servers	Number of domains	Threat hunting	Global
Tycoon 2FA	*5*	*5*	*4*	*5*	*5*	**4.8**
Storm-1167	*5*	*3*	*4*	*5*	*4*	**4.2**
NakedPages	*4*	*2*	*5*	*5*	*4*	**4**
Sneaky 2FA	*4*	*2*	*5*	*4*	*3*	**3.6**
EvilProxy	*5*	*2*	*5*	*4*	*0*	**3.2**
Evilginx - ywnjb	*4*	*2*	*4*	*5*	*1*	**3.2**
Saiga 2FA	*4*	*3*	*NA*	*3*	*1*	**2**
Greatness	*4*	*0*	*3*	*3*	*0*	**2**
Mamba 2FA	*2*	*3*	*NA*	*1*	*0*	**1.75**
Gabagool	*1*	*1*	*3*	*2*	*0*	**1.6**
CEPHAS	*0*	*0*	*NA*	*2*	*1*	**0.6**

** Scores are out of 5.*

Table 1. Prominence of AitM phishing kits according to Sekoia observations from January to April 2025

We assess with high confidence that this **ranking accurately represents the most active AitM phishing threats in early 2025**.

In the first months of 2025, the **Tycoon PhaaS** has shown significant activity, with dozens of new domain names being registered daily and protected behind Cloudflare. Additionally, the service updates the Tycoon 2FA source code and anti-bot pages weekly. We believe the frequent rotation of new anti-bot pages is intended to evade detection based on the HTML, potentially extending the time a domain can be used before being flagged as phishing by Cloudflare.

The alleged PhaaS offering the **Storm-1167** phishing kit also provides cybercriminals with a comparable service, featuring a large centralised and frequently renewed infrastructure along with regular updates to anti-bot pages. We estimate that the PhaaS has several hundred active affiliates, inferred from the domain names registered, which are likely associated with unique affiliates.

NakedPages and **EvilProxy** are both long-standing PhaaS that have maintained approximately 220 and 280 distinct active servers on average, from January 2024 to April 2025. Although this number fluctuates slightly month to month, we believe it accurately reflects a consistent affiliate base. Both services operate with decentralised infrastructure, allowing each affiliate to install the kit on their own server. Consequently, we estimate that each could have between 150 and 250 customers.

Emerging at the end of 2024, **Sneaky 2FA** and **Saiga 2FA**, both fully-featured PhaaS offerings, have since been widely adopted by threat actors, as evidenced by Sekoia.io's CTI and signature-based telemetry.

The open-source AitM phishing kit **Evilginx** remains one of the most prevalent as of early 2025. Notably, we identified a Evilginx configuration, also known as "phishlet", that is likely shared or sold within cybercrime communities and is widely used by threat actors. TDR analysts are tracking the associated infrastructure cluster as "Evilginx - ywnjb" based on the subdomain "*ywnjb.**" used as a reverse proxy for the legitimate Microsoft FQDN *login.live[.]com*. Of note, *YWNjb* is "*acc*" encoded in base64, likely corresponding to the term "*account*".

The **Mamba 2FA** PhaaS ranks 9th in our list of the most prevalent phishing kits in early 2025. We estimate this ranking may be underestimated because our metrics consider the number of active servers and phishing domain names. In contrast, Mamba 2FA employs a decentralised infrastructure with fewer domains compared to other kits. Sekoia.io telemetry indicates that compromises via Mamba 2FA occur fairly frequently.

While the ranking of the most prevalent AitM phishing kits offers valuable insights into prominent threats, it is important to acknowledge that our findings are influenced by our monitoring methodologies, which primarily focus on French and European organisations. Despite this inherent bias, the ranking remains informative and helps prioritise detection and monitoring efforts on the most significant threats.

Sheets for phishing kits

This section provides an overview sheet for each prominent AitM phishing, designed to help analysts understand and address the threat. These sheets aim to assist SOC analysts in detecting and investigating AitM phishing compromises, enable detection engineers to write detection patterns, support CTI analysts in capitalising on each threat, and aid DFIR analysts in attributing and contextualising phishing-related incidents.

Each sheet includes:

- **Context** about the phishing kit: this covers aliases, initial emergence, business model, background, and major updates to the kit.
- **Technical details** of the kit's operations: this details the implementation of anti-bot pages and the main steps of user interaction, including redirections, anti-bot checks, fake authentication steps, and the final redirection.
- **Infrastructure overview**: this section describes various components of the phishing kit infrastructure, including those managed by the operator and affiliates.
- **Detection and tracking opportunities**: it outlines details such as URL patterns, authentication with Microsoft services (including Application ID and User-Agent values), and indicators in the phishing code.
- Short **bibliography**: it lists the main reports describing the threat.

TDR analysts conducted an in-depth analysis of all the kits listed in the "Most relevant phishing kits" section and summarised their findings in this document.

Tycoon 2FA

PREVALENCE	IMPLEMENTATION
High	Synchronous relay

ALIASES Storm-1747

LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365, Google
FIRST SEEN	August 2023

CONTEXT

- PhaaS since at least August 2023, sold on Telegram
- Major AitM PhaaS in 2024 and early 2025
- Includes source code from Dadsec at the origin

ANTI-BOT PAGES

- Custom CAPTCHA pages
- Fake Cloudflare Turnstile pages
- Fake hCaptcha pages
- Fake reCAPTCHA pages

INFRASTRUCTURE

Operator's infrastructure

- Phishing domain names
- Central servers:
  - Verification domain names (returning 1 or 0)
  - Exfiltration domain names

URL PATTERNS

- Domain names, mostly matching this pattern `[a-z0-9]{2,6}\.[a-z]{5,15}\.(ru|com|es)` (also .cc, .info, .su, .vip and other TLDs)
- Autograb URL mostly matching these patterns:
  - `https://<domain>/[a-zA-Z0-9@!]{4,15}/($|*|?em=|)<email-address>`
  - `https://<domain>/[a-zA-Z0-9]{0,15}@[a-zA-Z0-9]{0,15}/`
  - `https://<domain>/[a-zA-Z0-9]{0,15}@[a-zA-Z0-9]{0,15}/($|*)<username-email-address>`
- Others URLs (resources, exfiltration, check): pseudo-randomly generated

MAIN STEPS	
HTML pages (Anti-bot, redirection, and fake Microsoft authentication pages) • HTML page loading a custom CATCHA challenge • Obfuscated JavaScript code using AES encryption and base64 encoding (crypto-js library)	Phishing domain
Check with central server • Receive 1 or 0 from central server, likely to continue or not	Verification domain
JavaScript code implementing authentication steps • Obfuscated JavaScript code using AES encryption and base64 encoding(crypto-js library) • JavaScript implementing user's browser fingerprint and anti-debugging functions and all the variations in a Microsoft 365 authentication	Phishing domain
Fingerprinting • Send obfuscated information on the host and the authentication	Phishing domain
Exfiltration • Send obfuscated data	Exfiltration domain

AUTHENTICATION WITH MICROSOFT SERVICES	TOP ASNS
APP ID 4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)	AS9009 AS29802

OTHER CHARACTERISTICS

- Unwanted traffic redirection to various eCommerce websites

INDICATORS IN CODE

- Code deobfuscation by using libraries fetched from:
  - `https://code.jquery.com/jquery-3.6.0.min.js`
  - `https://cdnjs.cloudflare.com/ajax/libs/crypto-js/4.1.1/crypto-js.min.js`
- Invisible character (unicode U+200B) in HTML title

Sekoia.io	@sekoia_io analysts uncovered a new emerging Adversary-in-the-Middle (AiTM) Phishing-...	Oct 2023
Sekoia.io	Tycoon 2FA: an in-depth analysis of the latest version of the AiTM phishing kit	Mar 2024
Randy McEoin	Tycoon2FA Deobfuscation	Nov 2024
Randy McEoin	Anti-bot services used by PhaaS - Part 2	Dec 2024

Storm-1167

PREVALENCE	IMPLEMENTATION
High	Synchronous relay

ALIASES FlowerStorm

LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365
FIRST SEEN	April 2023

CONTEXT

- Major AitM PhaaS since
- Similarities with Rockstar 2FA, which disappeared in Q4 of 2024

ANTI-BOT PAGES

- Custom Cloudflare Turnstile with Microsoft logo

INFRASTRUCTURE

Operator's infrastructure

- Phishing domain: mostly `.it.com` FQDNs since mid-February 2025, and `.com` or `.de` domain names related to business, technology, finance or legal themes
- FQDN from Tencent cloud platform - hosting the main JavaScript code
- Exfiltration domain: most likely a single `.cfd`, `.sbs`, or `.xyz` domain name per affiliate until mid-March 2025, since FQDNs of the phishing domain

URL PATTERNS

FQDN from Tencent cloud platform:

- Pattern of Tecent domain names: `<BucketName-APPID>.cos.ap-<REGION>.myqcloud.com`, *e.g.* `5425043750-1317754460.cos.ap-tokyo.myqcloud[.]com`

Exfiltration domain:

- URL: `/google.php`
- Domain name: `[0-9]{9,10}\.(cfd|my\.id|sbs|xyz)`, *e.g.* `5425043750[.]sbs`

MAIN STEPS

Cloudflare Turnstile page Two templates: • White page embedding the Turnstile challenge with instructions generated randomly • Dark page embedding the Turnstile challenge, a Microsoft logo and fake Microsoft instructions	Phishing domain
JavaScript code implementing authentication steps • Obfuscated JavaScript • JavaScript code implementing all the variations in a Microsoft 365 authentication, and rendering fake Microsoft pages	FQDN from Tencent cloud platform
Exfiltration • Send data to "/google.php" into POST parameters using the "do" field to indicate the step	Exfiltration domain
Redirection • Redirection to a legitimate Office365 URL	Microsoft domain

AUTHENTICATION WITH MICROSOFT SERVICES		TOP ASNS
APP ID	4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)	AS132203 AS19871

INDICATORS IN CODE

- Pseudo-randomly generated HTML title for anti-bot and phishing pages (lowercase)
- HTML comments in various languages (English, French, German, Arabic, Spanish), formerly using nature theme (flowers or fruits)

Microsoft TI	Detecting and mitigating a multi-stage AiTM phishing and BEC campaign	Jun 2023
Sophos X-Ops	Phishing platform Rockstar 2FA trips, and "FlowerStorm" picks up the pieces	Dec 2024

NakedPages

PREVALENCE	High
IMPLEMENTATION	Reverse proxy
ALIASES	Storm-1101, SakaiPages, ironsentry
LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365, allegedly 5+ others
FIRST SEEN	May 2022

CONTEXT

- Major AitM PhaaS between 2023 and 2025
- Rebranded multiple time (NakedPages, SakaiPages, IronSentry) and remains widespread

ANTI-BOT PAGES

- Custom Cloudflare Turnstile with black footer
- Default Cloudflare Turnstile webpage, with or without custom text

INFRASTRUCTURE

- Initial domain:
  - either Cloudflare Workers, subdomains from `workers.dev`
  - affiliate-controlled domain names
- Phishing domain:
  - affiliate-controlled domain names

URL PATTERNS

Initial Clouflare Turnstile and redirection URLs:

- mostly `https://<initial-domain>/?(qrc|email)=<email-address>`
- or `https://<initial-domain>/?(qrc|email)=<base64(email-address)>`
- sometimes additional query fields, such as `?cfg`

Additional redirection steps:

- `https://<phishing-domain>/?dataXX0=.*`
- `https://<phishing-domain>/owa/?login_hint=<email-address>`

Default Microsoft endpoints (reverse proxy), *e.g.*:

- `https://<phishing-domain>/aadcdn.msftauth.net/~/shared/1.0/content/.*`

Final redirection step:

- `https://<phishing-domain>/ping/v5767687`

MAIN STEPS

Cloudflare Turnstile webpage

Initial domain

- Cloudflare Turnstile HTML page displaying the malicious domain name

Previous versions used a custom page to hide the malicious domain, which contained a typo: "We needs to review…".

Anti-bot checks and redirection step

Initial domain

- Anti-bot checks performed on server-side
- HTML page embedding JavaScript to redirect to the phishing domain including the victim's email address in the phishing URL and using an iframe

Fake Microsoft authentication page

Phishing domain

- Phishing server operating as a reverse proxy, relaying all requests to Microsoft API

Redirection

Mosty Microsoft domain

- Redirection to another URL using the HTTP Location returned by the server

AUTHENTICATION WITH MICROSOFT SERVICES		TOP ASNS
APP ID	• 00000002-0000-0ff1-ce00-000000000000 (Office 365 Exchange Online) • 72782ba9-4490-4f03-8d82-562370ea3566 (Office365) • 4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)	AS36352 AS215540 AS401120 AS149440 AS14061

INDICATORS IN CODE

For previous versions of custom Cloudflare Turnstile webpages:

- `We needs to review the security of your connection before proceeding.`
- `We need to review the security of your connection before proceeding.`

Microsoft login page:

- `rickorigin=`

CloudSEK	Sophisticated Phishing Toolkit Dubbed "NakedPages" for Sale on Cybercrime Forums	Jun 2022
Microsoft	DEV-1101 enables high-volume AiTM campaigns with open-source phishing kit	Mar 2023

Sneaky 2FA

PREVALENCE	IMPLEMENTATION
Medium	Synchronous relay

ALIASES Sneaky Log, WikiKit

LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365
FIRST SEEN	September 2024

CONTEXT

- PhaaS since at least October 2024, sold on Telegram
- Quickly emerged at the end of 2024 and the beginning of 2025

ANTI-BOT PAGES

- Cloudflare Turnstile challenge impersonating Microsoft
- Cloudflare Turnstile with a blurred background

INFRASTRUCTURE

- Affiliate's infrastructure:
  - Phishing domain

URL PATTERNS

- Autograb URL:
  - `https://<domain>/<uri>/#<email-address>` or `https://<domain>/<uri>/?a=<base64(email-address)>`
- Phishing pages:
  - `https://<domain>/<uri>/[a-zA-Z0-9]{120,170}/(index|verify|validate)`

MAIN STEPS

Benign HTML page — Phishing domain

- HTML page with food-related content not visible to user
- Loading the next-stage using `window.location.reload()`
- Obfuscated using HTML tags

Cloudflare Turnstile page — Phishing domain

- HTML page with food-related content not visible to user
- Embed JavaScript code loading the Turnstile challenge

Redirection steps — Phishing domain

- HTML page with food-related content not visible to user
- Loading the next-stage using window.location.reload()
- Obfuscated JavaScript code managing the redirection

Fake Microsoft authentication page — Phishing domain

- HTML page embedding all the Microsoft authentication pages
- Base64-encoded images and obfuscation using HTML tags
- Obfuscated JavaScript code managing the authentication process

Redirection — Microsoft domain

- Redirection to a legitimate Office365 URL

AUTHENTICATION WITH MICROSOFT SERVICES

APP ID 4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)

TOP ASNS

AS14061
AS14956
AS36352
AS58329
AS39378

OTHER CHARACTERISTICS

Redirection to Wikipedia webpages (Microsoft themed) using href links, *e.g.* `https://href[.]li/?https://en.wikipedia[.]org/wiki/`

INDICATORS IN CODE

- HTML tags, such as `<!-- Food Section -->`
- HTML title, *e.g.* "Verify your account", "Verify your identity", "Confirm your login", "Signin to your account", etc.

TRAC Labs	WikiKit AiTM Phishing Kit: Where Links Tell Lies	Dec 2024
Sekoia.io	Sneaky 2FA: exposing a new AiTM Phishing-as-a-Service	Jan 2025

EvilProxy

PREVALENCE	IMPLEMENTATION
Medium	Reverse proxy

ALIASES Storm-0835

LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365, Google, allegedly 20+ others
FIRST SEEN	August 2020

CONTEXT

- Phishing kit sold on cybercrime forums (Exploit and XSS) since at least August 2020, as well as on Telegram
- Major AitM PhaaS from 2020 to early 2025
- Reverse proxy

ANTI-BOT PAGES

- Custom reCAPTCHA pages

INFRASTRUCTURE

Affiliate's infrastructure

URL PATTERNS

- Initial URLs:
  - `https://<phishing-subdomain-1>/?[a-zA-Z0-9]{2,6}=[a-zA-Z0-9]{2,6}`
  - `https://<phishing-subdomain-1>/?username=<email-address>`
- Authentication URL:
  - `https://[a-f0-9]{32}\.<phishing-domain>/.*`
- Authentication URL (older versions):
  - `https://[a-f0-9]{8}-[a-f0-9]{8}\.<phishing-domain>/.*`
  - `https://(accounts|0ffice|0nline1|l1ve)\.<phishing-domain>/.*`

MAIN STEPS		
reCAPTCHA webpage (optional)	Phishing subdomain 1	HTML page containing a reCAPTCHA challenge and obfuscated JavaScript code
Fake Microsoft authentication page	Phishing subdomain 1	HTML page containing the fake Microsoft authentication page and obfuscated heavy JavaScript code
Authentication steps	Phishing subdomains 2 and 3	Phishing server operating as reverse proxy, relaying all requests to the Microsoft API
Redirection	Phishing subdomains 2 and 3	Redirection to a Microsoft URL fetched using a WebSocket

AUTHENTICATION WITH MICROSOFT SERVICES		TOP ASNS
APP ID	72782ba9-4490-4f03-8d82-562370ea3566 (Office365)	AS14061 AS63949 AS14956 AS401120 AS399629

OTHER CHARACTERISTICS

- WebSockets communicating ping-pong, command and redirection URL data
- Automatically authorise the KMSI (Keep me signed in)
- Authentication request every 6 hours to keep the compromised session active (`RequestType=OrgIdWsFederation:federation`)

INDICATORS IN CODE

- HTML title of the reCAPTCHA webpage: `reCAPTCHA: Click Allow to verify that you are not a robot`

Resecurity	EvilProxy Phishing-as-a-Service with MFA Bypass Emerged in Dark Web	Sep 2022

Evilginx – ywnjb

PREVALENCE	IMPLEMENTATION
Medium	Reverse proxy

ALIASES

LICENSING	Open source
TARGET	Microsoft 365
FIRST SEEN	December 2022

CONTEXT

- Open-source AitM phishing kit maintained by *kgretzky*, available on GitHub since 2017
- Configuration file (phishlet) required for the phishing kit, most attackers use a variant of the phishlet named "o365" with the configured subdomain "YWNjb" to harvest Microsoft 365 credentials. This phishlet was first observed in December 2022.

ANTI-BOT PAGES

Not provided by Evilginx
Custom pages used by attackers

INFRASTRUCTURE

Clustering:

- Phishing clusters based on the subdomains used by the kit, which depend on the phishlet (configuration)
- Main phishing cluster "YWNjb" uses the characteristic subdomain "YWNjb"

URL PATTERNS

Identical to Microsoft ones, but using a malicious domain names, *e.g.*:

- `<phishing-domain>/common/oauth2/v2.0/authorize`
- `<phishing-domain>/common/GetCredentialType`
- `<phishing-domain>/common/SAS/BeginAuth`

MAIN STEPS (FOR YWNJB PHISHLETS)

Fake Microsoft authentication page — Phishing subdomain "office." or "login."

- HTML page containing the fake Microsoft authentication page and obfuscated heavy JavaScript code

Script handling authentication steps — Phishing subdomain "ywnjb."

- Legitimate Microsoft code injected with the phishing subdomain

Exfiltration — Phishing subdomain "office." or "login."

- Phishing server operating as a reverse proxy, relaying all requests to Microsoft API

Redirection — Microsoft domain

- Redirection to a Microsoft URL using the HTTP Location header from the request to the subdomain "react."

AUTHENTICATION WITH MICROSOFT SERVICES

APP ID 4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)

TOP ASNS

AS16509
AS14061
AS22612
AS47583
AS14956

OTHER CHARACTERISTICS

Unwanted traffic (incorrect path, or else) redirecting to Rick Astley song on YouTube

INDICATORS IN CODE

Malicious URLs included in legitimate Microsoft code

Kuba Gretzky	*evilginx2* repository on GitHub	Jul 2018
Microsoft	From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fr...	Jul 2022

Saiga 2FA

PREVALENCE	IMPLEMENTATION
Low	Synchronous relay

ALIASES SAIGA Page

LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365
FIRST SEEN	November 2024

CONTEXT

- Phishing kit used by the threat group "SAIGA Group", allegedly offered as-a-service
- Actively used in the wild in early 2025, and discovered by Sekoia in February 2025
- Relative low level of sophistication

ANTI-BOT PAGES

- Custom Cloudflare Turnstile pages, possibly not used by default by the kit

INFRASTRUCTURE

- Affiliate's infrastructure:
  - Phishing domain names

URL PATTERNS

- Autograb URL:
  - `https://<domain>/?S=<email-address>`
- Exfiltration endpoints:
  - `/api/(config|check-bot|check-ip|deets|email|login|notice|auth|poll|process|kmsi)/`

MAIN STEPS

JavaScript pages implementing phishing functions — Phishing domain

- Initial HTML page fetching several JavaScript scripts
- Obfuscated JavaScript of a Next.js application
- JavaScript code communicating with the phishing server, parsing data, and dynamically displaying fake Microsoft authentication pages

Exfiltration — Phishing domain

- POST requests to multiple endpoints exfiltrating victim's data and fetching server's data

Redirection — Custom domain

- Redirection to a URL received by the phishing server

AUTHENTICATION WITH MICROSOFT SERVICES		TOP ASNS
APP ID	4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)	AS36352 AS9009 AS47583 AS23470 AS16276

OTHER CHARACTERISTICS

- Design of the fake Microsoft authentication pages does not exactly copy the legitimate ones (different font, different boxes)

INDICATORS IN CODE

- Next.js JavaScript code
- HTML title using Latin words, *e.g.* `Dolor et culpa ut culpa nulla occaecat esse eiusmod velit nisi aliquip irure eu ad.`
- Characteristic JSON files received from `/api/` endpoints containing configuration settings

Sekoia.io	Saiga 2FA malware object in Sekoia.io CTI (Customer access only)	Feb 2025
Red Piranha	Suspected SAIGA Threat Actors Exploit Australian Legal Sector with EDR Bypass	Mar 2025

Greatness

PREVALENCE	IMPLEMENTATION
Low	Synchronous relay

ALIASES Storm-1295

LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365
FIRST SEEN	June 2022

CONTEXT

- PhaaS since June 2022
- Significant threat since 2023
- New major version in February 2025, with backend source code rewrite in Python

ANTI-BOT PAGES

- Custom CAPTCHA pages impersonating Microsoft

INFRASTRUCTURE

Operator's infrastructure

- Phishing domain names
- Central server hosted on Amazon AWS (AS16509)

Affiliate's infrastructure (optional)

- Cloud services (Cloudflare R2 or Workers, Linode Object Storage)
- or attacker-controlled domains

URL PATTERNS

- Malicious JavaScript:
  - `https://<phishing-domain>/s/[a-f0-9]{7,12}?[a-f0-9]{7,12}=<email-address>`
  - `https://<phishing-domain>/s/[a-f0-9]{7,12}?[a-f0-9]{7,12}=<base64(email-address)>`
- FingerprintJS library: `https://<phishing-domain>/s/[0-9]{2}?0`
- HTML code: `https://<phishing-domain>/r/[0-9]{2}?session=[a-f0-9]{64}`
- WebSockets: `ws://<phishing-domain>/p/[0-9]{3}?session=[a-f0-9]{64}`

MAIN STEPS

HTML attachment fetching JavaScript — Attachment

- Benign HTML code embedding a JavaScript fetching an external script
- Can also be hosted by the affiliate (cloud service or attacker-controlled domain)

JavaScript and HTML codes — Phishing domain

- JavaScript codes implementing custom CAPTCHA and authentication steps, FingerprintJS library
- HTML code of the fake authentication steps

Exfiltration through WebSockets — Phishing domain

- Encoded data using three XOR keys
- Harvested data in JSON format

Redirection — Microsoft or Google domain

- Redirection to a legitimate domain

AUTHENTICATION WITH MICROSOFT SERVICES

APP ID 4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)

TOP ASNS

PacketStream residential proxy

AS16509

OTHER CHARACTERISTICS

- Resources fetched from `upload.wikimedia[.]org` (Microsoft logo), `encrypted-tbn0.gstatic[.]com` (refresh image), `cdn2.iconfinder[.]com` (mail image) and `static.vecteezy[.]com` (CAPTCHA background) by the custom CAPTCHA page
- Some of the authentication requests performed from the central server (AS16509)

INDICATORS IN CODE

- HTML attachment containing such following JavaScript code:
  - `<script> b8527f88086 = ''.replace.call("<obfuscated-url>",/(a2ec21|edd117f1)/g,""); $.getScript(b8527f88086);</script>`
- Malicious JavaScript code containing characteristic variables and function, *e.g.* `var loader`, `var def_end`, `function docWriter`, `const botdPromise`, `const fpPromise`, *etc.*

Cisco Talos	New phishing-as-a-service tool "Greatness" already seen in the wild	May 2023
Vade	Phishing as a Service: Analyzing "Greatness"	Jun 2023

Mamba 2FA

PREVALENCE	IMPLEMENTATION
Medium	Synchronous relay

ALIASES

LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365
FIRST SEEN	November 2023

CONTEXT

- PhaaS since at least November 2023, sold on Telegram

ANTI-BOT PAGES

Blank page

Use of Adspect anti-bot service

INFRASTRUCTURE

Operator's infrastructure

- Phishing domain names
  - three groups: `/o/`, `/r/` or `/s/` phishing URLs
  - including some compromised legitimate domains (*e.g.* WordPress)
- Exfiltration domain names
  - usually 3 active at a time (one for each of the groups of phishing URLs)
  - behind Cloudflare
  - hosting Node.js code (Express, Socket.IO)

URL PATTERNS

- Autograb URL:
  - `https?://<phishing-domain>/(o|r|s)/?(c3Y9bzM2NV|aXBkYXRhP)<base64>N0123N<email>`
- Exfiltration URL:
  - `(https|wss)://<exfiltration-domain>/socket.io/?EIO=4&transport=...`

MAIN STEPS

Anti-bot check • Obfuscated HTML and JavaScript • JavaScript fingerprinting of the web browser	Phishing domain
Fake Microsoft authentication page • Obfuscated JavaScript code implementing all the variations in a Microsoft 365 authentication	Phishing domain
Exfiltration • Send data using Socket[.]IO JavaScript library (WebSocket with HTTP fallback)	Exfiltration domain
Redirection • Redirection to a legitimate Office URL	Microsoft domain

AUTHENTICATION WITH MICROSOFT SERVICES

APP ID 4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)

TOP ASNS

IPRoyal proxies in ASs Simoresta UAB and Karolio IT

OTHER CHARACTERISTICS

- Anti-bot check redirection to `https://google.com/404/`
- Final redirection to `https://outlook.office365.com/error/`

INDICATORS IN CODE

- Anti-bot page:
  - `<img src="/files/images/Logo.png" data-digest="<base64>" onerror="(new Function(atob(this.dataset.digest)))();" style="visibility: hidden;">`
- Phishing page:
  - `<html id='html' sti='<base64>' vic='<autograb>' lang='en'>`
  - `const pointLink = "<base64>";`

AnyRun	Analysis of the Phishing Campaign: Behind the Incident	Jun 2024
Sekoia.io	Mamba 2FA: A new contender in the AiTM phishing ecosystem	Oct 2024
Randy McEoin	Anti-bot services used by PhaaS - Part 1	Dec 2024

Gabagool

PREVALENCE	IMPLEMENTATION
Low	Synchronous relay

ALIASES Skyw4lker

LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365
FIRST SEEN	October 2024

CONTEXT

- Highly likely a PhaaS, active since at least the end of October 2024
- Possibly the successor of Rockstar 2FA with the backend re-written in Python instead of PHP, based on several technical similarities

ANTI-BOT PAGES

- Custom Cloudflare Turnstile page, containing the text "Browser security check in progress."

INFRASTRUCTURE

Affiliate's infrastructure

- Initial domain name (optional)
- Phishing domain names

Operator's infrastructure

- Central servers: exfiltration domain names

URL PATTERNS

- Credentials exfiltration: `POST <phishing-domain>/<folder>/assets/php/endpoints/accounts.php`

MAIN STEPS	
HTML page loading a JavaScript (optional) • HTML page containing a base64-encoded JavaScript fetching and executing an external JavaScript code	Initial domain
HTML loading fake Microsoft authentication pages • JavaScript performing AES decryption of a base64-encoded HTML • JavaScript downloading additional code • HTML document displaying fake authentication pages	Phishing domain
Fake Microsoft authentication page • AES-encrypted HTML • HTML code of the fake authentication pages • JavaScript code implementing authentication steps	Exfiltration domain
Victim IP address • Gather the victim IP address using an external service	api.ipify[.]org or ipapi[.]co
Exfiltration • Send harvested data	Exfiltration domain, Phishing domain
Redirection • Redirection to another URL set in the JavaScript file	Microsoft domain

AUTHENTICATION WITH MICROSOFT SERVICES		TOP ASNS
APP ID	4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)	AS174

OTHER CHARACTERISTICS

- Use of landing pages impersonating Sharepoint, and possibly other Microsoft services, in addition to the fake Microsoft authentication page
- Credentials exfiltrated twice: to the operator's central exfiltration domain that implements the AiTM capability, as well as to the affiliate-controlled phishing domain

INDICATORS IN CODE

- Custom Cloudflare Turnstile page and HTML loader containing:
  - CSS comment `/* Your CSS styles */` and car-related HTML comments
  - Characteristic strings, *e.g.* variable `usuuid`, functions `decstr`, `querulous` and `sendMouseData`
- AES-encryption using variables `a`, `b` and `c`, and the JavaScript library `crypto-js.min.js`
- Exfiltration of harvested data using the field `do` (values: `GURI`, `check`, `le`, `ver`, `cV`), `em`, `psk`, and others

TRAC Labs	AiTM Phishing, Hold the Gabagool: Analyzing the Gabagool Phishing Kit	Nov 2024

CEPHAS

PREVALENCE	IMPLEMENTATION
Low	Synchronous relay

ALIASES W3LL Panel, OV6

LICENSING	Phishing-as-a-Service
TARGET	Microsoft 365
FIRST SEEN	August 2024

CONTEXT

- PhaaS used since August 2024
- Kit formerly known as W3LL Panel since at least February 2019
- W3LL Panel has AitM capabilities since March 2022

ANTI-BOT PAGES

- Custom Cloudflare Turnstile (optional)

INFRASTRUCTURE

Affiliate-controlled:

- Initial domain, can be object storage service
- Phishing domain

Operator's infrastructure:

- Central server interacting with Microsoft API (AS202015)

URL PATTERNS

- Phishing page: `https://<phishing-server>/<UUID>/`
- Encoded phishing page content: `GET <folder>/p5Qw9X8rN3.php`
- Turnstile verification: `POST <folder>/bR7sD9kJ2m.php`
- Credentials exfiltration: `POST <folder>/khL9kO2fV1.php`

MAIN STEPS

Static HTML document — Local file or attachment URL

- Obfuscated HTML and JavaScript
- Optional Cloudflare Turnstile
- JavaScript fetching, decoding and rendering the fake Microsoft page from the phishing server

Anti-bot checks — Phishing domain

- The fake Microsoft page is not returned (404) if checks on the source IP and User-Agent suggest automated scanning

JavaScript code implementing authentication steps — Phishing domain

- Sending user inputs to the phishing server and updating the fake Microsoft page for each authentication step

Exfiltration — Phishing domain

- Send data in HTTP POST parameters

Redirection — Often Microsoft domain

- Redirection to a configurable decoy URL

AUTHENTICATION WITH MICROSOFT SERVICES		TOP ASNS
APP ID	4765445b-32c6-49b0-83e6-1d93765276ca (OfficeHome)	AS202015
		AS14061
		AS399629
		AS36352
		AS20473
		AS14956

INDICATORS IN CODE

- Default Turnstile text: `Online safety check underway.`
- Hard-coded HTML element ids: `JKDfIUfjdsnf`, `KlwiHWjdk`, `UuejjerBHDdhEHE`
- Attachment / Landing page :
  - long comments about events happening at specific locations (*e.g.* "wine tasting on Riverside Avenue …", "Anime Convention at the golf course …")
  - `class="cloudflare_security_text"`
- Phishing page
  - two-words comments about astronomy concepts (*e.g.* "Stellar Vortex", "Spectral Quasar")
  - `localStorage.getItem('ov-cf')`

Group-IB	W3LL done: uncovering hidden phishing ecosystem driving BEC attacks	Sep 2023
Group-IB	W3LL phishing kit – the tools, the criminal ecosystem, and the market impact	Oct 2023

TLP:CLEAR

Detection opportunities

Detecting AitM phishing attacks requires a multi-faceted approach leveraging various log sources and monitoring techniques. This section outlines detection strategies based on authentication logs analysis and network traffic monitoring, highlighting unique characteristics and anomalies associated with different phishing kits.

Our analysis focuses specifically on detection methods for AitM attacks targeting Microsoft Entra environments, as our team has conducted extensive research on Entra detection opportunities. Google Workspace detection remains an area for future exploration.

Authentication logs analysis

Microsoft Entra authentication logs provide valuable insights for detecting AitM phishing attacks. Two primary log sources contain similar content but differ in format and collection method:

- **Microsoft Entra sign-in logs**
  Detailed authentication events recorded directly by Microsoft Entra ID.
- **Microsoft 365 Audit Logs**
  Authentication events collected via Purview, Unified Audit Logs (UAL), or Office 365 Management API.

Several log fields can be leveraged to identify unique characteristics of authentications performed via specific PhaaS offerings.

User-Agent anomalies

Many synchronous relay kits use hardcoded User-Agent header values instead of forwarding the actual web browser value from the victim. These anomalies include:

- **Missing User-Agent values**
- **Library-specific User-Agent strings**
- **Invalid or fabricated User-Agent strings**
- **Outdated or rare User-Agent values**

Application ID and Resource ID

The Application ID and Resource ID fields indicate which application requests the login and which resource the user attempts to access. While these indicators alone are insufficient to definitively identify AitM phishing, they add specificity to detection rules since **a given kit typically targets the same Application and Resource consistently**.

Most PhaaS kits target *OfficeHome*, the homepage of Microsoft 365 Copilot (formerly Office 365), which is the default application used by the Microsoft Entra sign-in page when no specific application is selected. The most notable exceptions are EvilProxy, which targets the *Office365* application, and NakedPages which offers multiple Microsoft phishing templates, including one targeting *Office 365 Exchange Online*.

ASN and country of source IP

AitM phishing kits typically operate from rented web servers with **IP addresses belonging to hosting provider Autonomous Systems** (AS), contrasting with legitimate users whose connections usually originate from Internet Service Provider ASes. This distinction can be incorporated into detection logic, although users of personal VPN services may generate false positives as these services also operate from hosting providers.

For phishing services using centralised infrastructure, operators often consistently employ a single hosting provider with servers in the same geographic region. For instance, authentications relayed by Storm-1167 phishing pages always originate from AS19871 (Network Solutions) servers located in the United States, or AS132203 (Tencent) servers located either in the US or in Germany.

Self-hosted phishing kits show different patterns based on affiliate preferences or operator recommendations. Sneaky 2FA kits predominantly use DigitalOcean (AS14061), while NakedPages instances more frequently appear on bulletproof hosting provider Global Connectivity Solutions (AS215540) or HostPapa (AS36352).

Some phishing services employ commercial proxy services to obscure their infrastructure's IP addresses or evade ASN/country-based detections. A notable example was Caffeine (also known as ONNX, taken down in November 2024), which used a residential proxy service, causing authentication attempts to appear as originating from ISP networks rather than hosting providers. As of early 2025, Greatness uses a proxy pool (possibly PacketStream) composed of a mix of hosting and residential IP addresses, and Mamba 2FA uses IPRoyal datacenter proxies.

Correlation ID reuse

A user's journey through the Microsoft Entra authentication flow typically comprises multiple steps, each generating a distinct event in authentication logs. To indicate events related to the same authentication attempt, logs include a Correlation ID field, intended to be a unique identifier common across all steps of the authentication process.

Crucially, this identifier's value is based on parameters passed by the client. **Some AitM kits fail to generate new unique correlation IDs for each sign-in**, instead reusing the same UUID across multiple authentication attempts.

Incoherences across authentication steps

Several synchronous relay kits contain implementation bugs causing **variations in User-Agent strings or source ASN/country** between successive events of the same authentication attempt. These inconsistencies offer significant detection opportunities.

Network traffic monitoring

Beyond authentication logs, network traffic provides additional detection opportunities for AitM phishing campaigns.

Domain name patterns in DNS logs

AitM phishing kits using reverse proxy implementations often map distinct subdomains of the phishing domain to corresponding FQDNs of the impersonated authentication service. Certain **subdomain names or patterns serve as high-fidelity indicators** that a domain hosts a specific phishing kit.

For example, the `ywnjb.` subdomain pattern is consistently used in a popular Evilginx phishlet (configuration file), making it a reliable indicator of this particular phishing kit.

URL patterns in web navigation logs

Reverse proxy AitM kits typically reproduce the exact URL paths of the authentication services they impersonate.
For instance, the legitimate URL `hxxps://login.microsoftonline[.]com/common/SAS/BeginAuth` would be relayed by the phishing kit as `hxxps://<phishing-domain>/common/SAS/BeginAuth`.

This behaviour enables the creation of detection rules identifying **characteristic URL paths of legitimate authentication services associated with unexpected domain names**. Such detection requires logging of complete URLs from web traffic, achieved through web proxies with HTTPS decryption capabilities or browser extensions.

Conclusion

In recent years, **Adversary-in-the-Middle (AitM) phishing** has emerged as a **major cyber threat to organisations**. These campaigns primarily target employees in finance, sales, human resources, and executive roles through diverse social engineering schemes and techniques, tactics, and procedures (TTPs). Phishing operations often serve as the initial phase of cyberattacks, leading to financial fraud and substantial losses.

The rise in AitM phishing attacks is largely driven by the **professionalisation of the cybercrime ecosystem**, especially through the **Phishing-as-a-Service (PhaaS) model**. Over the past years, multiple PhaaS platforms have entered the cybercrime market, offering turnkey AitM phishing kits at lower costs and requiring minimal technical expertise.

Sekoia's continuous monitoring and detailed analysis of prominent kits provide valuable insights into the AitM phishing threat and its associated cybercrime ecosystem. Our proactive efforts to **identify emerging trends, TTPs, and new PhaaS** provide a global overview and help assess the prevalence of each kit, allowing for better prioritisation and contextualisation of the AitM phishing threat.

The Sekoia TDR team actively produces actionable cyber threat intelligence (CTI) with exclusive Indicators of Compromise (IoCs) and detection strategies using Sigma rules. This strengthens the defenses of our customers and partners against AitM phishing threats.

Perspective

In this section, we take a step back to assess the future evolution of the AitM phishing threat and to anticipate emerging trends.

A review of current developments suggests that AitM phishing threats will continue to evolve, with attackers frequently adapting their initial access TTPs and social engineering strategies to increase the effectiveness of email-based campaigns. The recent shift to distributing phishing links via QR codes, HTML attachments, and SVG files demonstrates the adaptability of these threat actors. It is highly likely that **additional techniques will emerge and become widespread** within the cybercrime ecosystem.

Anti-bot features, such as human interaction verification, are increasingly differentiating PhaaS offerings. The **expanded use of Traffic Distribution Systems (TDS)** and the **continuing advancement of anti-bot mechanisms** are expected to further enhance these services, potentially increasing customer retention among cybercriminals.

To date, large-scale AitM phishing campaigns have predominantly targeted Microsoft 365 and Google accounts. Sekoia analysts anticipate that, in the medium term, **targeting** will likely **diversify** to include platforms that facilitate document signatures, identity and access management, financial transactions, and the storage of sensitive information. For example, AitM phishing campaigns using NakedPages have already been observed targeting Docusign accounts.

While not a prediction, potential **takedown operations** against major PhaaS such as Tycoon 2FA, Storm-1187, and NakedPages **could significantly hinder the threat** by disrupting cybercriminal activity and deterring market entry. Repeated law enforcement actions in 2023 and 2024, including takedowns of ONNX (Caffeine)[11] and BulletProftLink[12] infrastructures, illustrate the potential impact of such operations. However, as new platforms continue to emerge, ongoing and coordinated efforts will remain essential to reducing the organisational risk posed by AitM phishing.

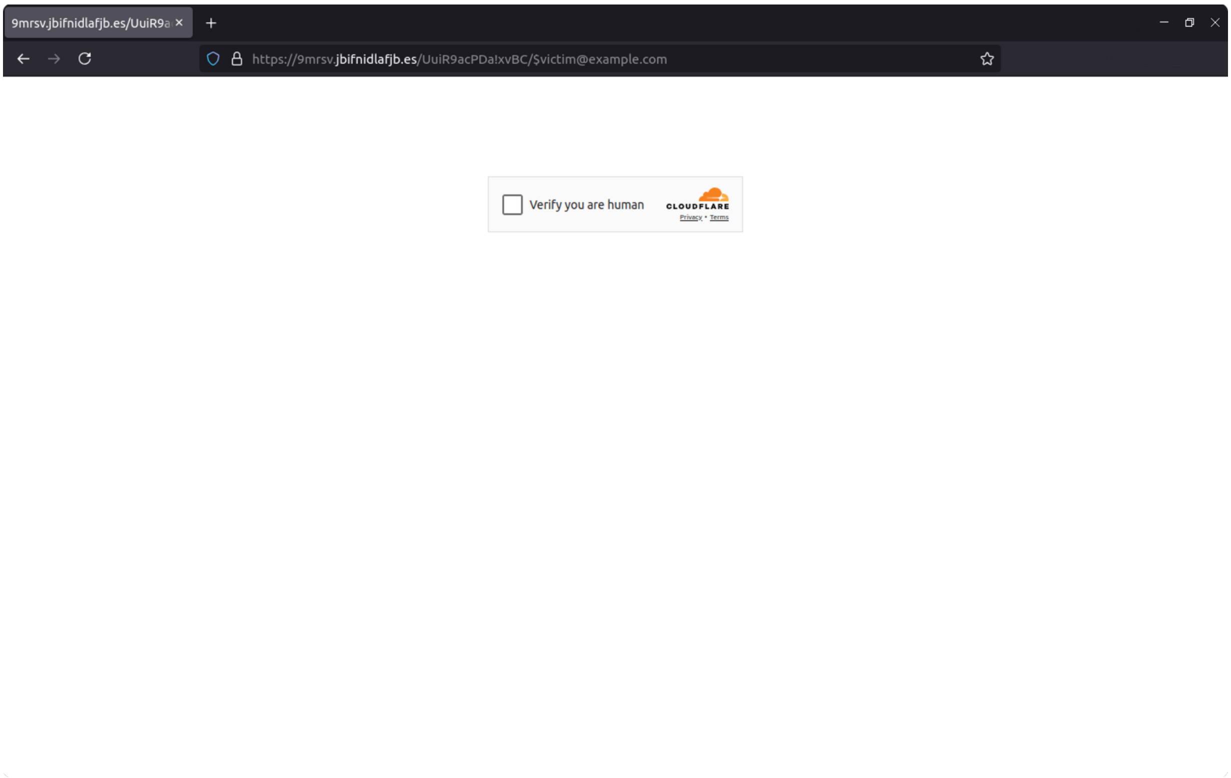
[11] https://blogs.microsoft.com/on-the-issues/2024/11/21/targeting-the-cybercrime-supply-chain/

[12] https://www.nst.com.my/news/crime-courts/2023/11/976212/igp-police-arrest-eight-people-international-syndicate-which

Annexes

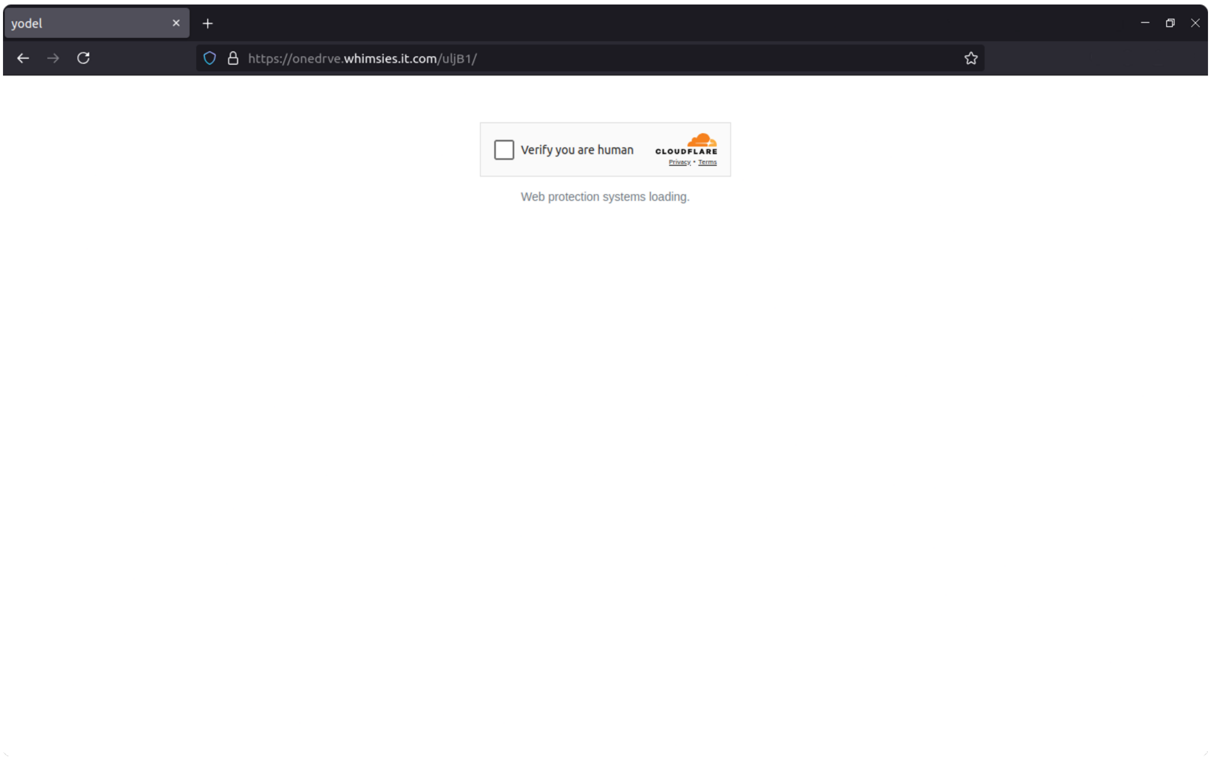
Anti-bot pages

Tycoon 2FA anti-bot page:



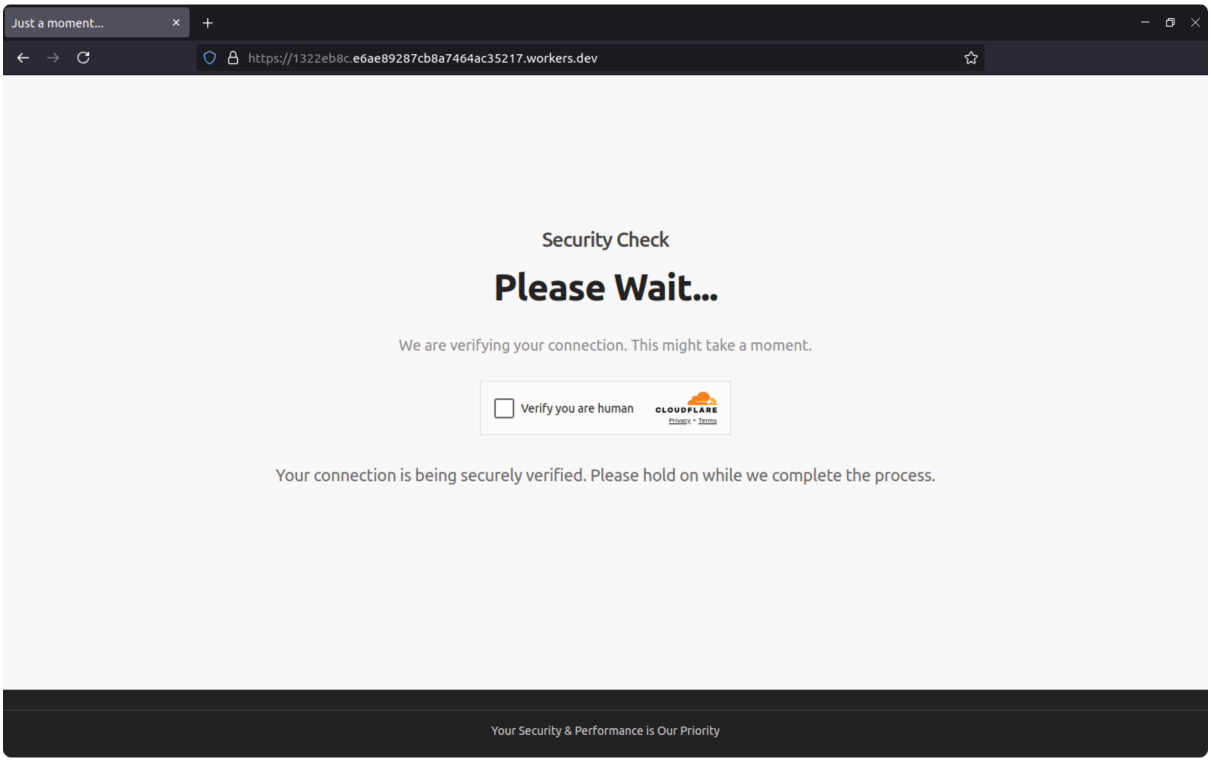
9mrsv.jbifnidlafjb.es/UuiR9a ×
+
https://9mrsv.jbifnidlafjb.es/UuiR9acPDa!xvBC/$victim@example.com
□ Verify you are human
CLOUDFLARE
Privacy • Terms

Storm-1167 anti-bot page:



Web protection systems loading.

NakedPages anti-bot page:



https://1322eb8c.e6ae89287cb8a7464ac35217.workers.dev

Security Check

Please Wait...

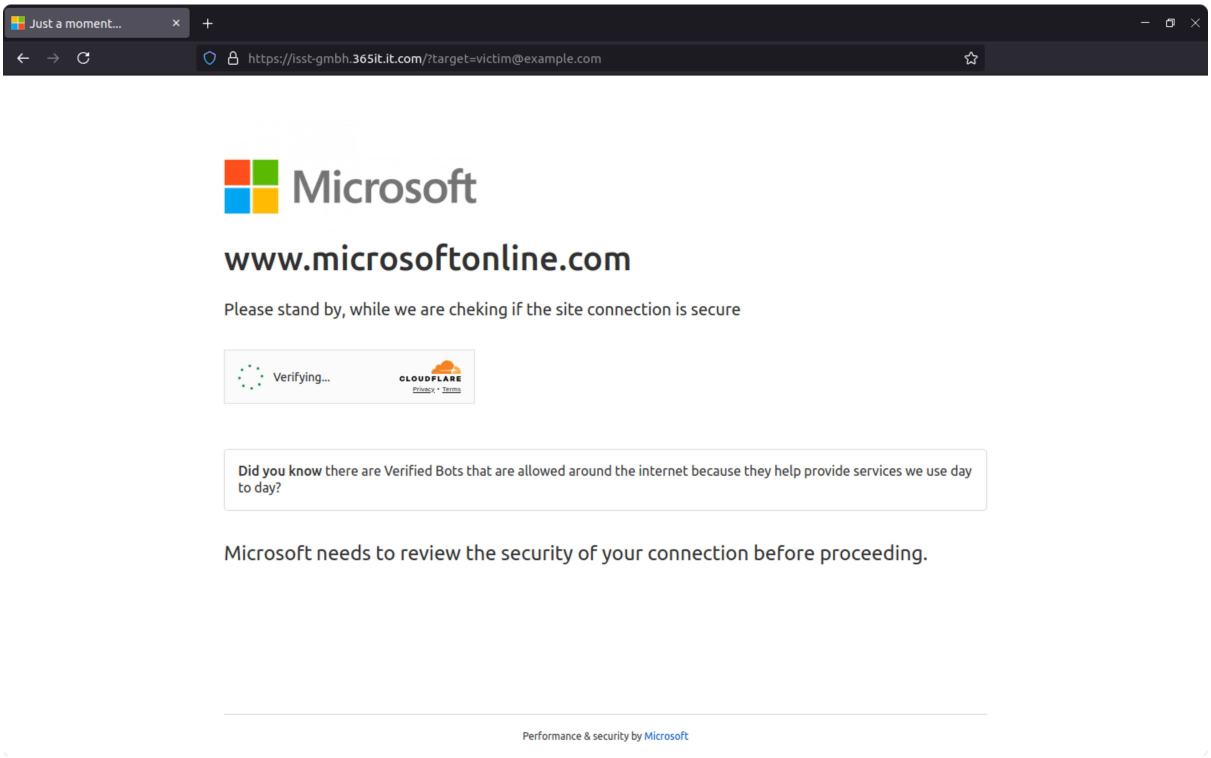
We are verifying your connection. This might take a moment.

□ Verify you are human

Your connection is being securely verified. Please hold on while we complete the process.

Your Security & Performance is Our Priority

Sneaky 2FA anti-bot page:



https://isst-gmbh.365it.it.com/?target=victim@example.com

www.microsoftonline.com

Please stand by, while we are cheking if the site connection is secure

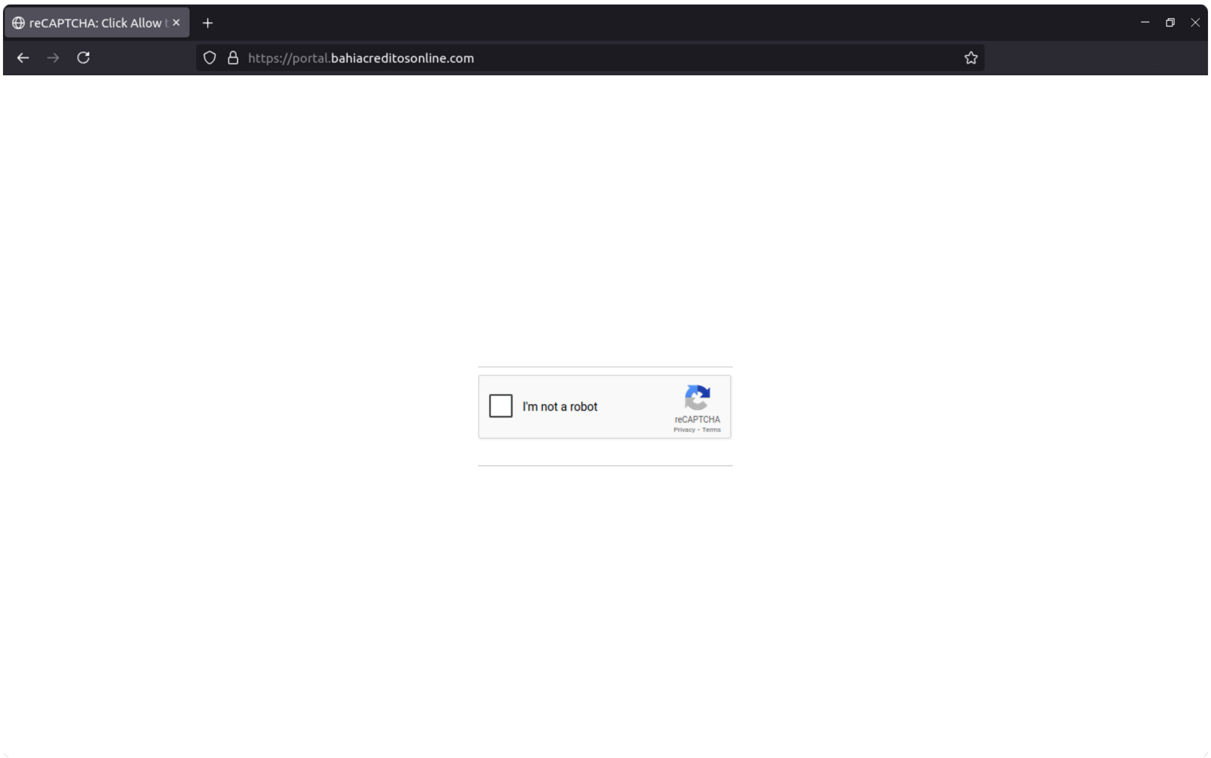
Verifying...

Did you know there are Verified Bots that are allowed around the internet because they help provide services we use day to day?

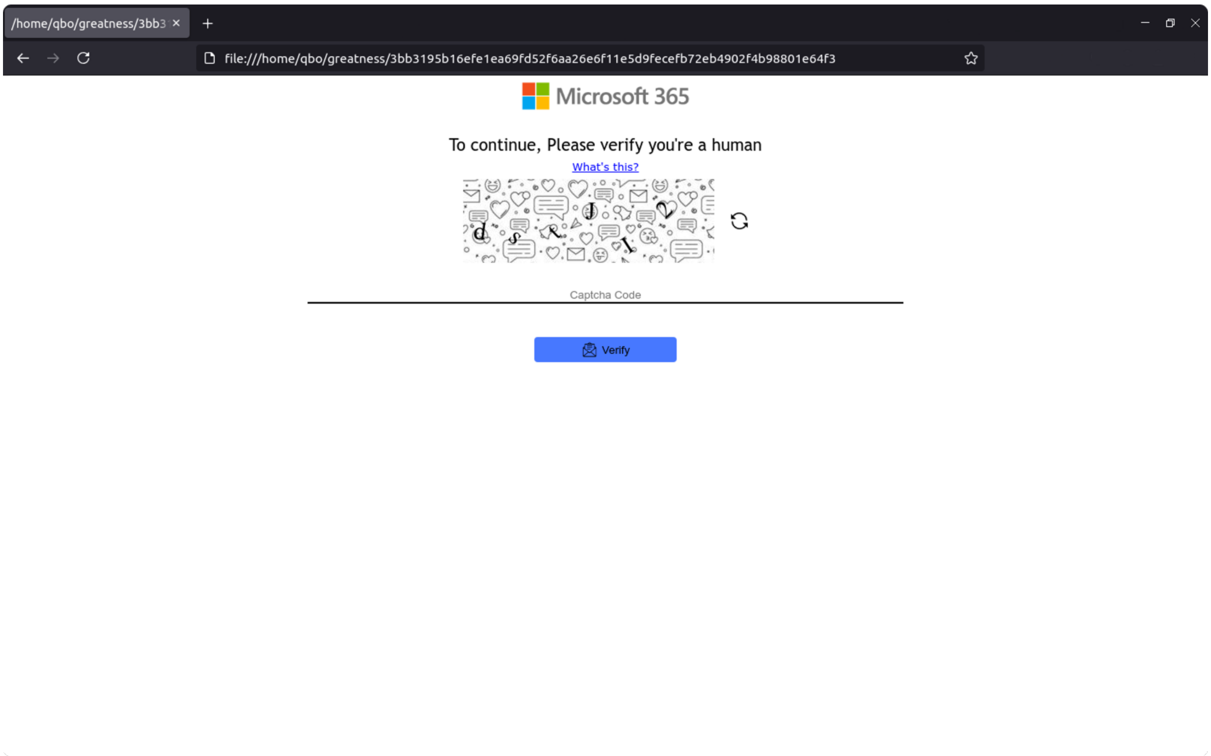
Microsoft needs to review the security of your connection before proceeding.

Performance & security by Microsoft

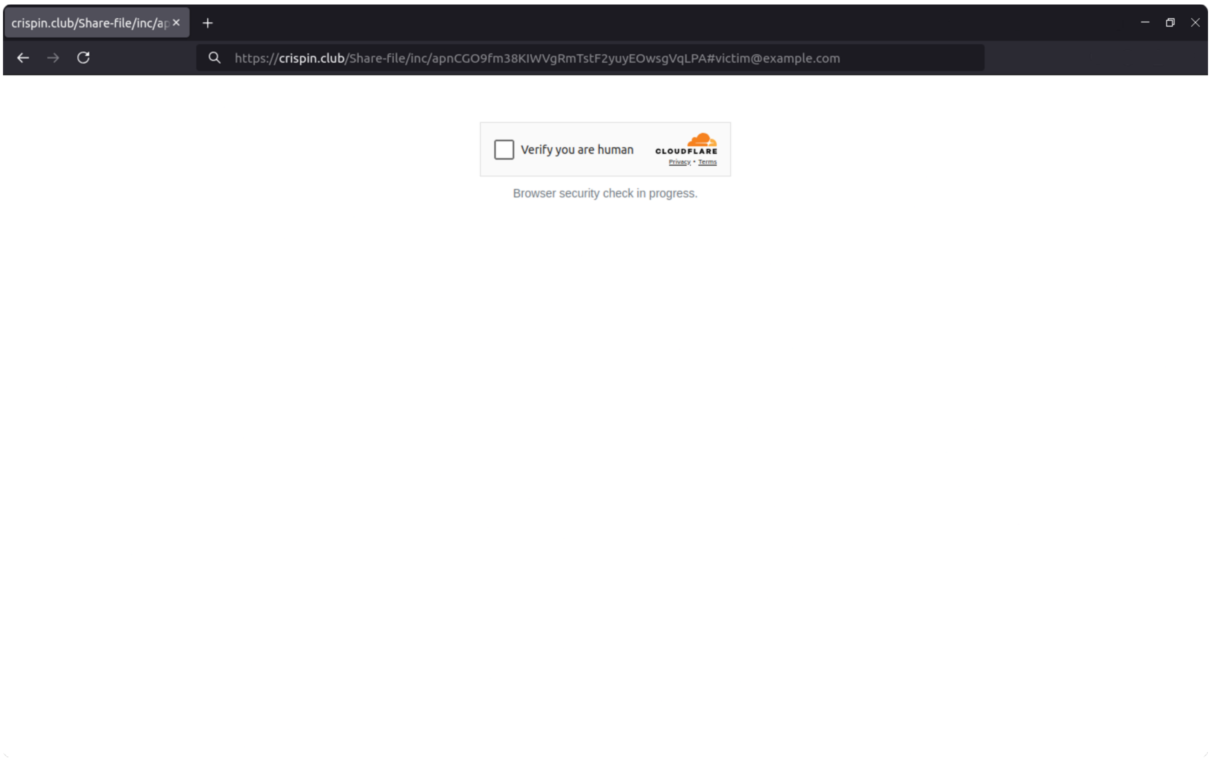
EvilProxy anti-bot page:



Greatness anti-bot page:


/home/qbo/greatness/3bb3
file:///home/qbo/greatness/3bb3195b16efe1ea69fd52f6aa26e6f11e5d9fecefb72eb4902f4b98801e64f3
Microsoft 365
To continue, Please verify you're a human
What's this?
Captcha Code
Verify

Gabagool anti-bot page:



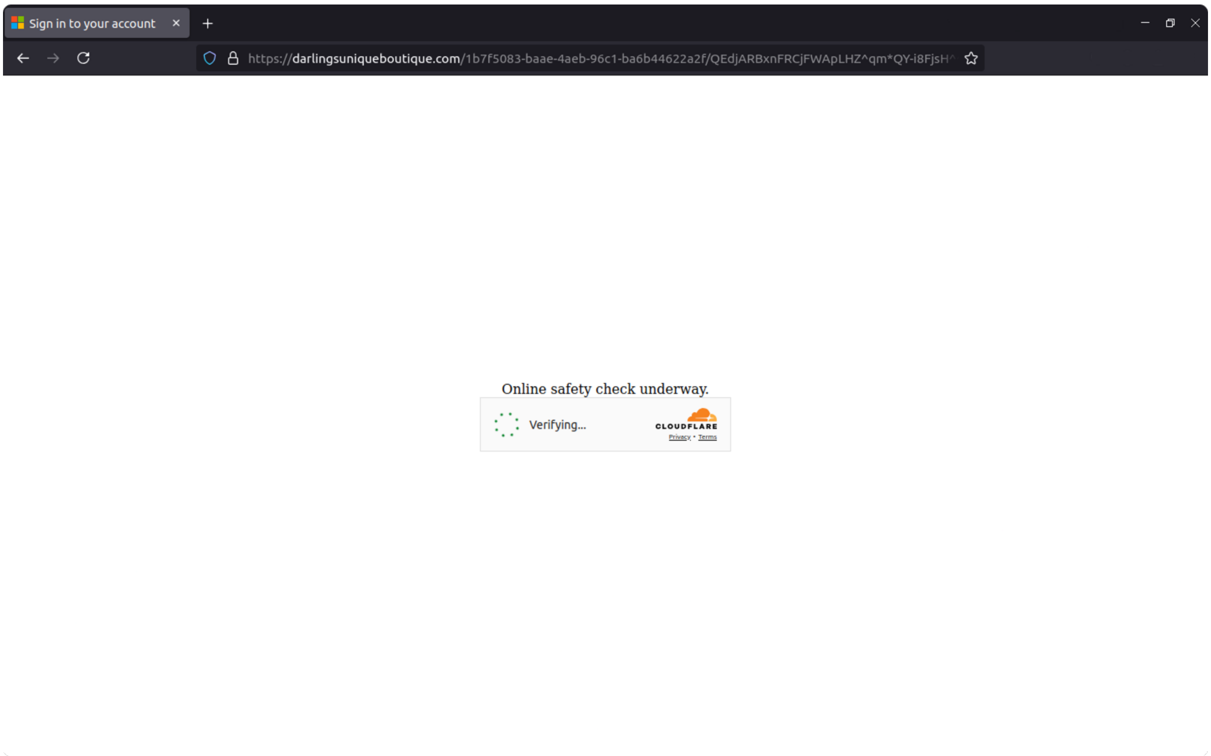
crispin.club/Share-file/inc/ap

https://crispin.club/Share-file/inc/apnCGO9fm38KIWVgRmTstF2yuyEOwsgVqLPA#victim@example.com

□ Verify you are human

Browser security check in progress.

CEPHAS anti-bot page:



Sign in to your account

https://darlingsuniqueboutique.com/1b7f5083-baae-4aeb-96c1-ba6b44622a2f/QEdjARBxnFRCjFWApLHZ^qm*QY-i8FjsH^

Online safety check underway.

Verifying...

Microsoft logs fields reference

The following table summarises the key log fields across different platforms that can be leveraged for AitM phishing detection:

Field	Microsoft Entra sign-in log	Microsoft 365 Audit Log
User-Agent	userAgent	ExtendedProperties[Name=UserAgent].Value
Application ID	appId	ApplicationId
Resource ID	resourceId	ObjectId
Source IP ASN	autonomousSystemNumber	Not included (derivable from ClientIP)
Source IP country	location.countryOrRegion	Not included (derivable from ClientIP)
Correlation ID	correlationId	InterSystemsId

External references

[Mozilla] xlink:href - SVG: Scalable Vector Graphics | MDN
[Randy McEoin] Anti-bot services used by PhaaS - Part 2
[Randy McEoin] Anti-bot services used by PhaaS - Part 1
[Sekoia.io] Calisto show interests into entities involved in Ukraine war support
[U.S. Department of Justice] Case 25-sz-13 Seizure Warrant
[Microsoft] Microsoft Digital Defense Report 2023
[Microsoft] Detecting and mitigating a multi-stage AiTM phishing and BEC campaign
[Sekoia.io] FLINT 2023-043 - Dadsec OTT: a new prevalent PhaaS using AitM phishing
[Sekoia.io] Phishing attachments redirecting users to Tycoon 2FA phishing pages
[Sekoia.io] Mamba 2FA: A new contender in the AiTM phishing ecosystem
[Sekoia.io] Tycoon 2FA: an in-depth analysis of the latest version of the AiTM phishing kit
[Randy McEoin] Tycoon2FA Deobfuscation
[Sophos] Phishing platform Rockstar 2FA trips, and "FlowerStorm" picks up the pieces
[CloudSEK] Sophisticated Phishing Toolkit Dubbed "NakedPages" for Sale on Cybercrime Forums
[Microsoft] DEV-1101 enables high-volume AiTM campaigns with open-source phishing kit
[TRAC Labs] WikiKit AiTM Phishing Kit: Where Links Tell Lies
[Sekoia.io] Sneaky 2FA: exposing a new AiTM Phishing-as-a-Service
[Resecurity] EvilProxy Phishing-as-a-Service with MFA Bypass Emerged in Dark Web
[Kuba Gretzky] Evilginx source code on GitHub
[Microsoft] From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud
[Sekoia.io] Saiga 2FA malware object in Sekoia.io CTI (Customer access only)
[Red Piranha] Suspected SAIGA Threat Actors Exploit Australian Legal Sector with EDR Bypass
[Cisco Talos] New phishing-as-a-service tool "Greatness" already seen in the wild
[Vade] Phishing as a Service: Analyzing "Greatness"
[ANY.RUN] Analysis of the Phishing Campaign: Behind the Incident
[TRAC Labs] AiTM Phishing, Hold the Gabagool: Analyzing the Gabagool Phishing Kit
[Group-IB] W3LL done: hidden phishing ecosystem driving BEC attacks
[Group-IB] W3LL phishing kit – the tools, the criminal ecosystem, and the market impact
[Microsoft] Targeting the cybercrime supply chain
[New Straits Times] IGP: Police arrest eight people in international syndicate which developed phishing templates to dupe victims

About Sekoia.io TDR team

TDR is the Sekoia Threat Detection & Research team. Created in 2020, TDR provides exclusive Threat Intelligence, including fresh and contextualised IOCs and threat reports for the Sekoia SOC Platform. TDR is also responsible for producing detection materials through a built-in Sigma, Sigma Correlation and Anomaly rules catalogue.

TDR is a team of multidisciplinary and passionate cybersecurity experts, including security researchers, detection engineers, reverse engineers, and technical and strategic threat intelligence analysts.

Threat Intelligence analysts and researchers are looking at state-sponsored & cybercrime threats from a strategic to a technical perspective to track, hunt and detect adversaries. Detection engineers focus on creating and maintaining high-quality detection rules to detect the TTPs most widely exploited by adversaries.

About Sekoia.io

Sekoia.io is the European cybertech, leading provider of Extended Detection and Response (XDR) solutions based on Cyber Threat Intelligence (CTI). Its mission is to provide businesses and public organizations with the best protection technologies against cyber attacks.

By combining threat anticipation through knowledge of attackers (Sekoia Intelligence) with automation of detection and response, the Sekoia SOC platform (Sekoia Defend – XDR) provides security teams a unified view and total control over their information systems. Its interoperability with third-party solutions and compliance with international technical standards enable organizations to take full advantage of their existing technologies.

Sekoia.io gives its customers the means to focus their human resources on high value-added missions, optimize their cyber-defense strategy and regain the advantage against advanced cyber threats.

Find more publications on blog.sekoia.io

Please don't hesitate to provide your feedback on our publications by clicking here.
You can also contact us at tdr@sekoia.io for further discussions.