Tycoon 2FA: an in-depth analysis of the latest version of the AiTM phishing kit

By Sekoia TDR and Quentin Bourgue

Published: 2024-03-25 · Archived: 2026-04-05 17:13:49 UTC

Table of contents

Introduction

To enhance our threat intelligence, improve detection and identify new threats, Sekoia analysts engage in continuous hunting to address the main threats affecting our customers. For this, we proactively search and identify emerging threats, using our telemetry data, internal tools and external services.

In October 2023, our daily threat hunting routine led us to **uncover a new Adversary-in-The-Middle (AiTM) phishing kit** allegedly used by multiple threat actors to carry out widespread and effective attacks. Our investigation revealed that this kit was associated with the **Tycoon 2FA Phishing-as-a-Service (PhaaS) platform**, which had been active since at least August 2023.

At this time, the Sekoia Threat Detection & Research (TDR) team conducted an in-depth analysis of the Tycoon 2FA PhaaS kit and shared[1] some of our findings with the cybersecurity community on Twitter. Since then, we have been actively monitoring the infrastructure of Tycoon 2FA phishing pages, campaigns leveraging the kit, source code updates, and activities of the alleged developer.

Our monitoring of the prominent PhaaS kit revealed that Tycoon 2FA has become **one of the most widespread AiTM phishing kits over the last few months**, with more than 1,100 domain names detected between late October 2023 and late February 2024.

In mid-February 2024, we identified **a new emerging version of the Tycoon 2FA** that was widely distributed in the wild. This new version enhances its obfuscation and anti-detection capabilities and changes network traffic patterns. In response to these developments, Sekoia analysed the changes and highlighted the new infrastructure.

This blog post aims to present **an in-depth analysis of Tycoon 2FA and the recent developments** we spotted in the phishing kit. Additionally, this report provides **tracking opportunities to actively monitor the infrastructure** and mitigate risks associated with Tycoon 2FA.

Context

Uncovering of Tycoon 2FA

In October 2023, our threat hunting for evasive phishing campaigns identified the massive use of QR codes redirecting to several AiTM phishing kits. While some of them were already known and monitored by us, such as Caffeine, Dadsec, EvilProxy and NakedPages, others were unfamiliar to us. Analysing unknown phishing pages led us to identify a growing infrastructure of hundreds of similar AiTM phishing pages.

These similarities included:

- A small HTML page containing a script that deobfuscates an additional script using base64 and XOR operations, and executes it;

- Requests to the same obfuscated JavaScript code, named "*myscr[0-9]{6}.js*"
- Usage of a custom CloudFlare Turnstile page, the Cloudflare CAPTCHA alternative, to protect the phishing page;
- Requests to specific Cascading Style Sheets (*CSS*) resources, named "*pages-godaddy.css*" and "*pages-okta.css*";
- Usage of WebSocket to exfiltrate the user input data.

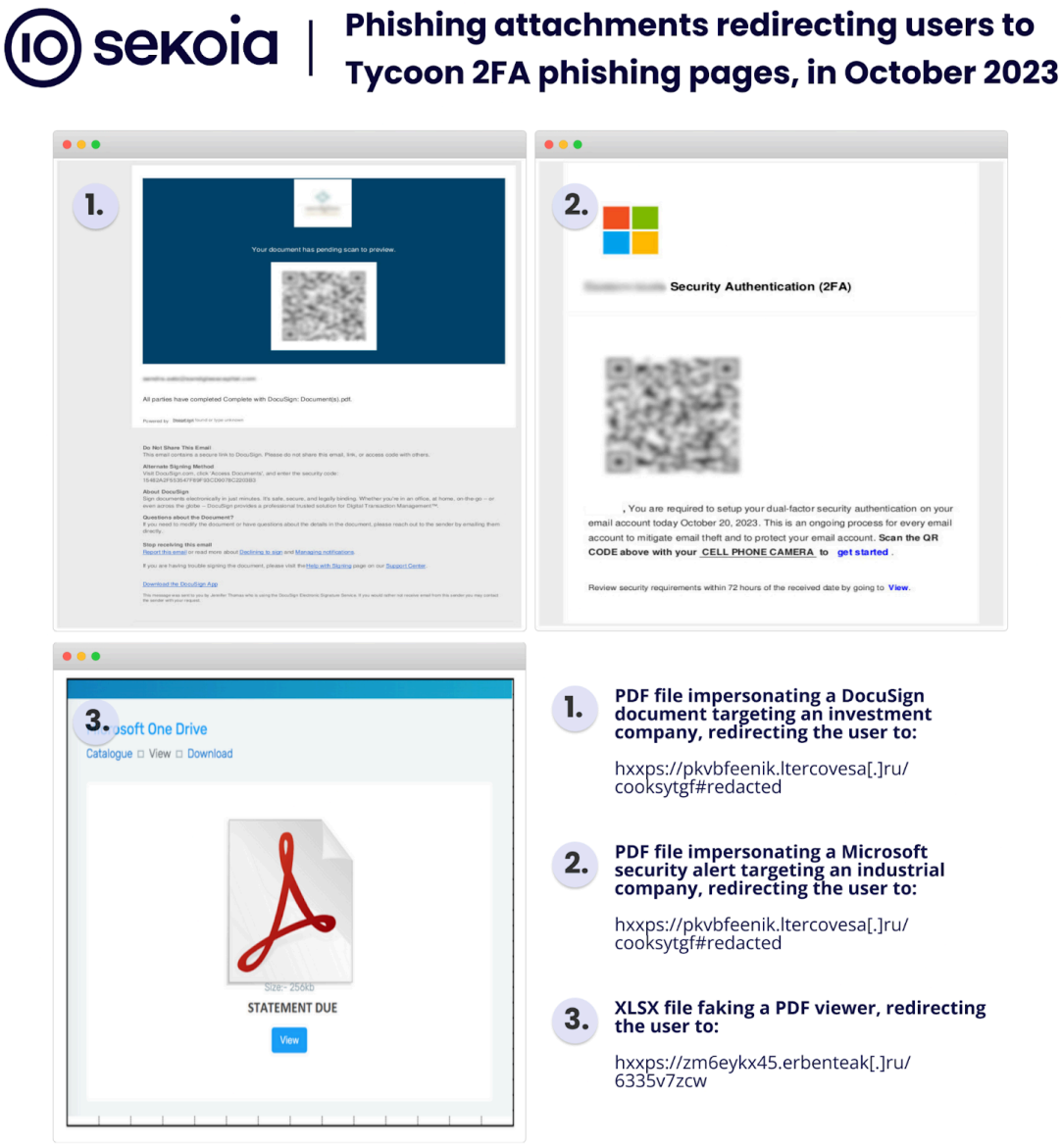

Figure 1. Email attachments redirecting users to Tycoon 2FA phishing pages, distributed in October 2023

By pivoting on these similarities using urlscan.io, we therefore listed hundreds of phishing pages of this previously unknown cluster. In October 2023, we shared the following urlscan.io's query to track the similar phishing pages using the specific resource filenames:

filename:("pages-godaddy.css" AND "pages-okta.css")

The oldest phishing pages returned by this heuristic retrieved their resources from the same domain "*codecrafterspro[.]com*", which appeared to be a central server of this cluster.

Leveraging DNS, registrar and WHOIS records, we pivoted on domain names that we identify as belonging to the same threat actor:

Domain Name	***First seen***
tycoongroup[.]ws *codecrafters[.]su*	*2023-07-29* *2023-08-09*

codecrafterspro[.]com	*2023-08-17*
devcraftingsolutions[.]com	*2023-09-07*

In October 2023, "*codecrafters[.]su*" and "*devcraftingsolutions[.]com*" also hosted resources for the phishing pages we analysed. Of note, the same login panel "Powered by TycoonGroup" was found on both domains (see Figure 2), confirming that the domain "*tycoongroup[.]ws*" belongs to this infrastructure. At this time, the domain hosted a website that promoted Tycoon as the "best 2FA bypass phishing platform" (see Figure 2).

This tangible evidence allowed Sekoia to **associate this growing infrastructure of hundreds of phishing pages with the Tycoon 2FA phishing platform**.

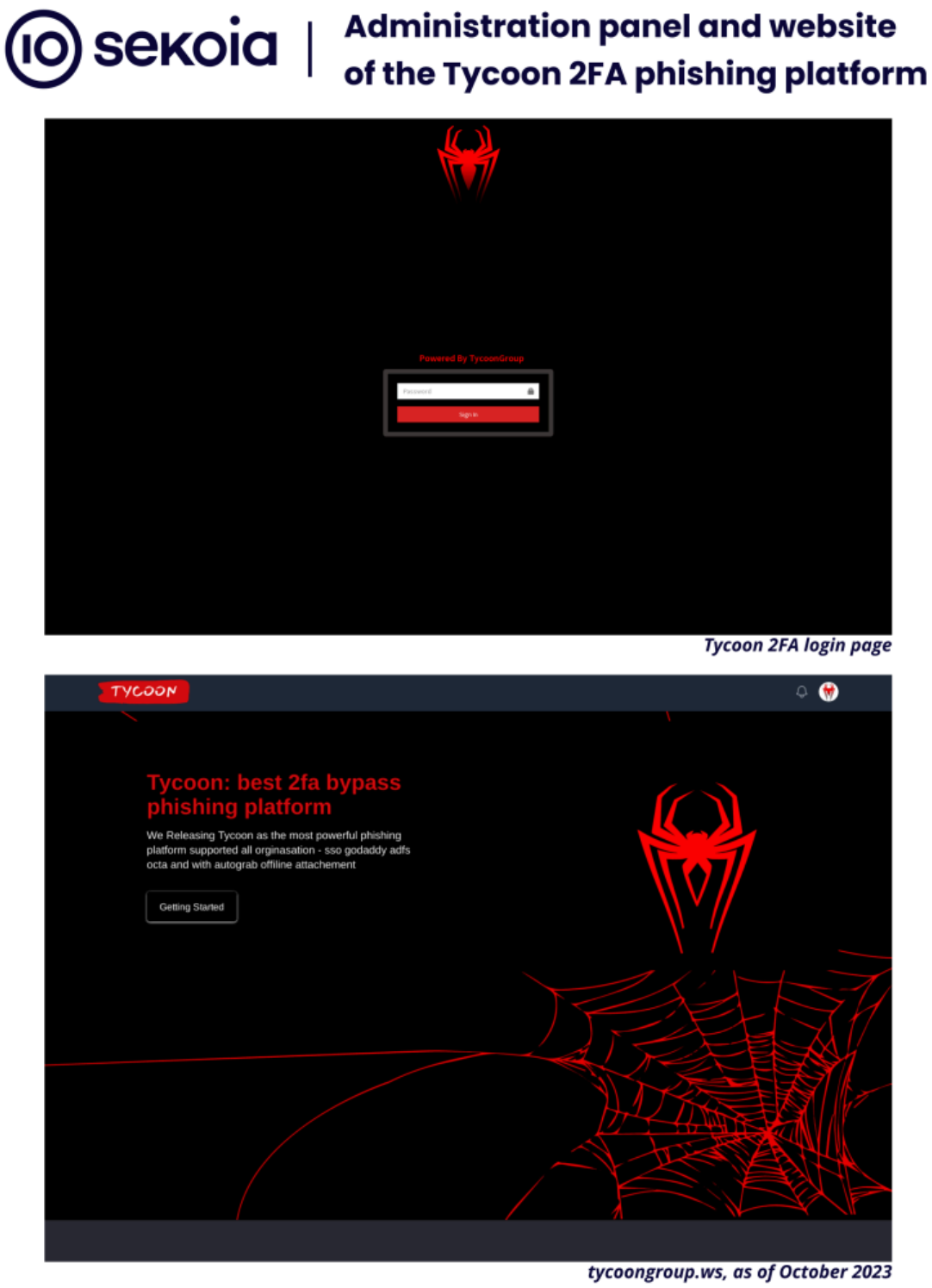

Figure 2. Login page of Tycoon 2FA administration panel and Tycoon 2FA website (tycoongroup[.]ws), as of October 2023

Background of Tycoon 2FA

In addition to a dedicated website, the Tycoon 2FA operator also advertised its PhaaS using Telegram since October 2023. This threat actor goes under the handles *Tycoon Group*, *SaaadFridi* and *Mr_XaaD* and regularly publishes changelogs about the latest updates of Tycoon 2FA in the Telegram channel "*hxxps://t.me/tycoon_2fa_Link*".

The threat actor, who is also the alleged developer of the phishing kit, sells ready-to-use Microsoft 365 and Gmail phishing pages, as well as attachment templates, starting at $120 for 10 days, with prices increasing depending on the TLD. In March 2023, the phishing service provided several domain name extensions, including .ru, .su, .fr, .com, .net and .org.

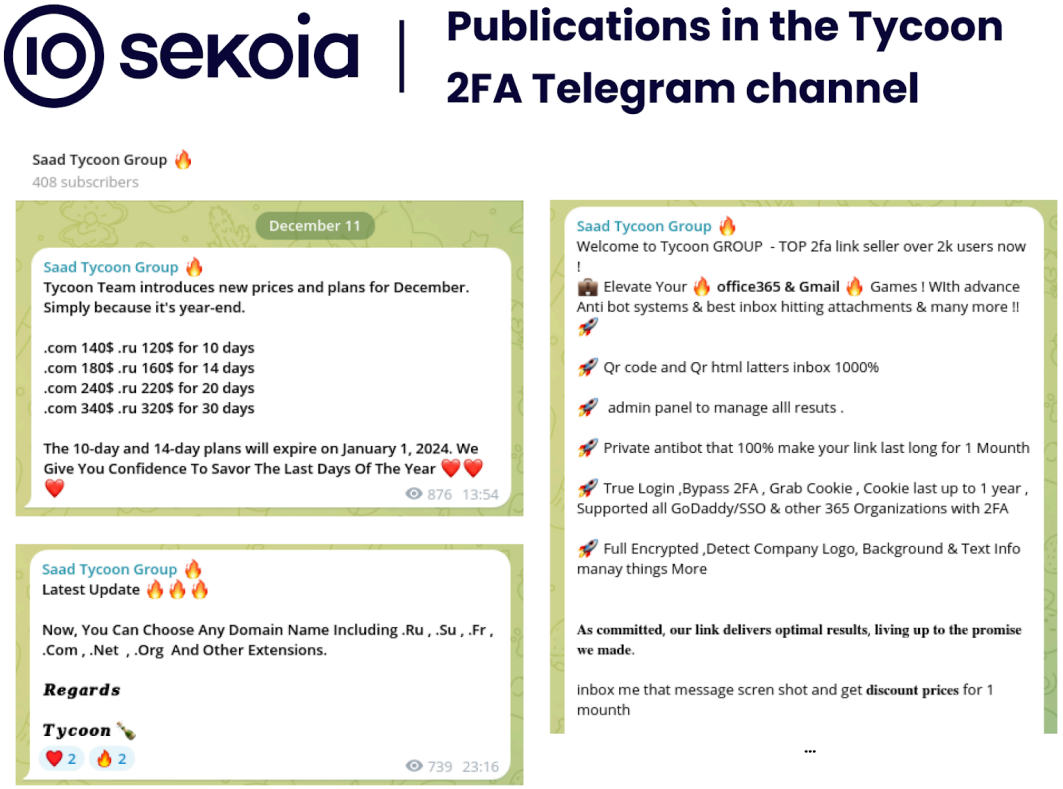

Figure 3. Publications in the Tycoon 2FA Telegram channel named "Saad Tycoon Group", advertising the Tycoon 2FA PhaaS

The publications also include screenshots of the administration panel accessible to the customers. This enabled us to identify links between Tycoon 2FA and another known phishing platform.

As mentioned[2] on Twitter in October 2023, the Tycoon 2FA phishing platform shares several similarities with the Dadsec OTT phishing kit, which we analysed in-depth in the "*FLINT 2023-043 – Dadsec OTT: a new prevalent PhaaS using AitM phishing*" sent to our clients in November 2023.

First, the Dadsec OTT and Tycoon 2FA administration panels are almost identical in content and design, as shown in Figure 4. On both platforms, we find the logo of the PhaaS in the top right-hand corner, the same statistical data categories (*Bots Blocked*, *Total Visits*, *Valid Login*, *SSO Login* and *Invalid Login*), similar main tabs (*Settings* and *Clear Logs*), and an almost identical UI design, with the same table, buttons, font, *etc.*

Second, the Dadsec OTT and Tycoon 2FA phishing kits operate in a similar way. To protect from bot traffic, both phishing pages first challenge the user with a test using Cloudflare Turnstile. Both of them use custom HTML pages to embed the Cloudflare CAPTCHA alternative (see Figure 5):

- Dadsec OTT pages contain the text "*While we are checking your browser…*" above the Cloudflare Turnstile test.
- Tycoon 2FA pages contain the same text as Dadsec in its previous version. In 2024, the pages include the text "*this page is running browser checks to ensure your security*" below the Cloudflare Turnstile test.

Once the challenge is passed, the two phishing pages display a page mimicking Microsoft authentication. The workflow to retrieve, deobfuscate and process the fake authentication page differ between both phishing kits.

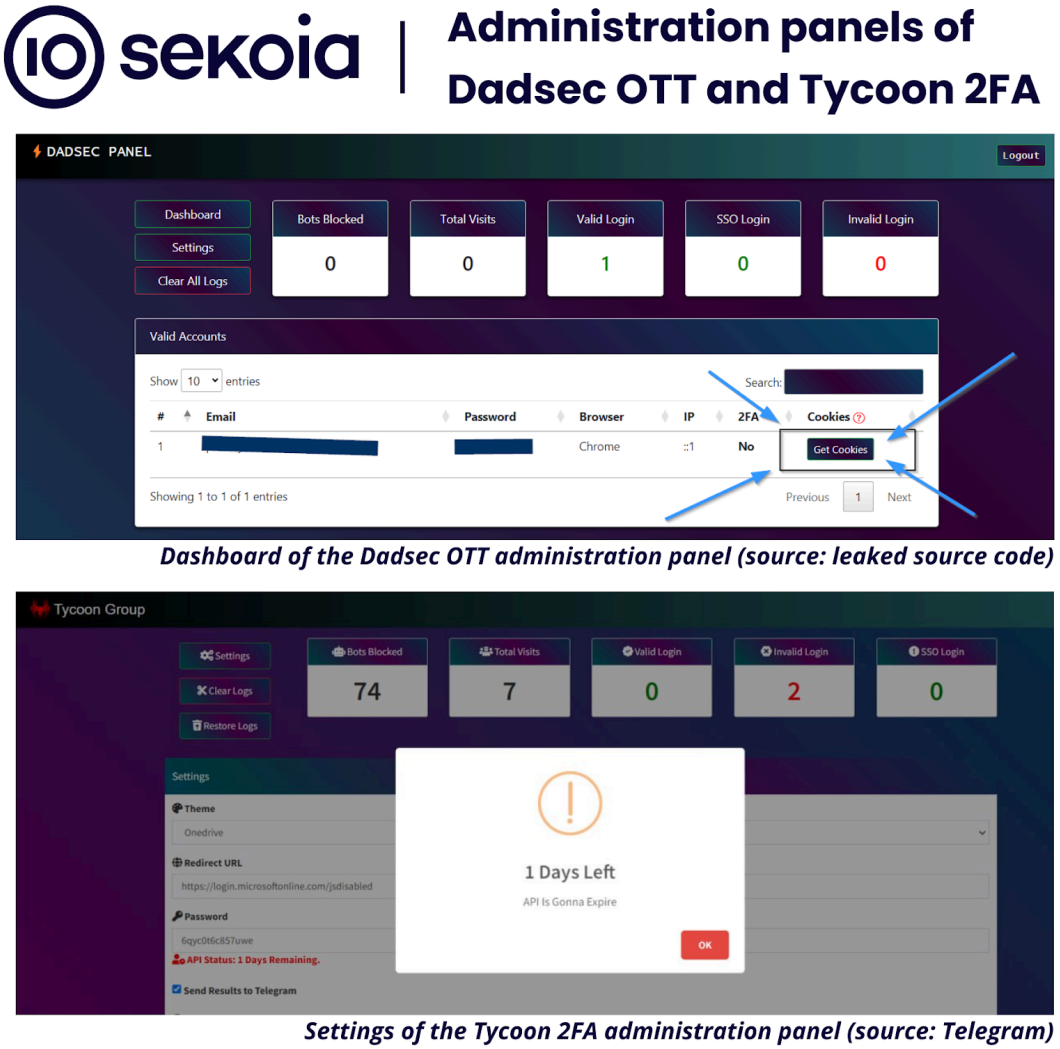

Figure 4. Comparison of Dadsec OTT and Tycoon 2FA administration panel dashboards (source: Telegram)

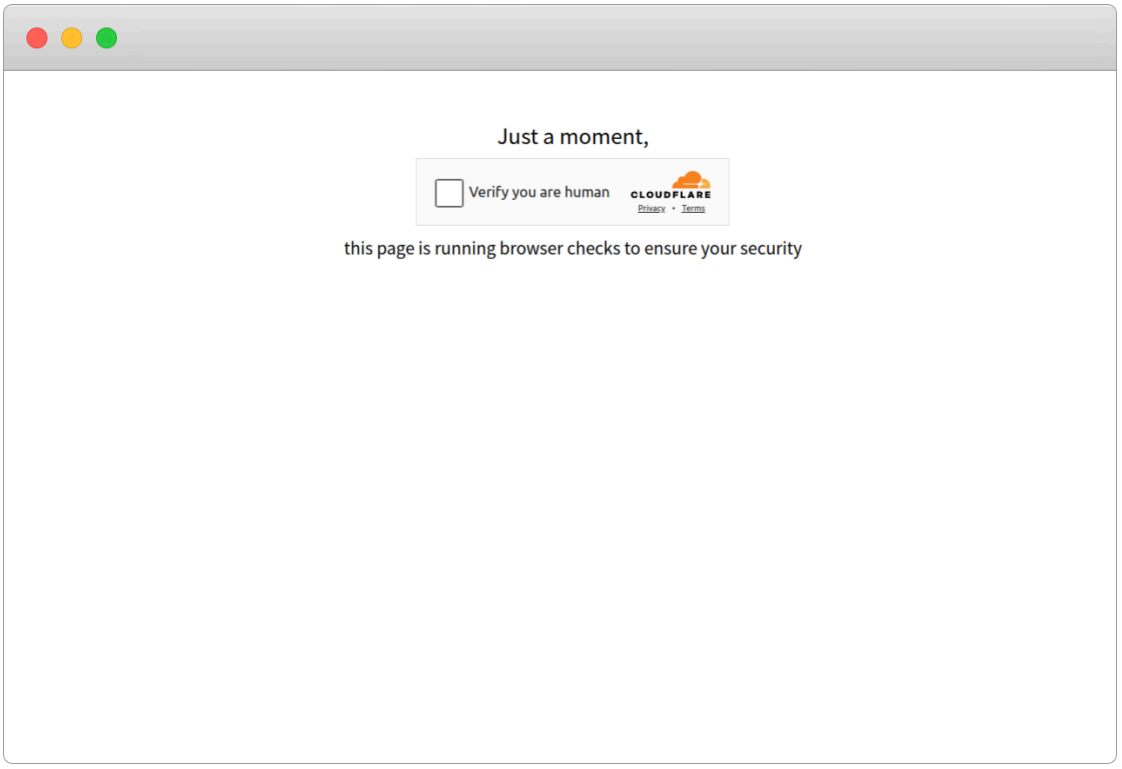

Figure 5. Custom page embedding a Cloudflare Turnstile challenge used by the Tycoon 2FA phishing kit

Sekoia analysts assess with high confidence that **the alleged developer of the Tycoon 2FA PhaaS had access to and partially reused the source code of the Dadsec OTT phishing kit**. It is plausible that the Tycoon 2FA developer forked the code of the Dadsec OTT administration panel and developed the core functions of the new AiTM phishing kit, including the front-end HTML code of the phishing pages and the back-end code for the authentication process.

The leak of Dadsec's source code that we analysed in October 2023 supports this hypothesis, since the Tycoon 2FA developer could have obtained this leak to initiate its new PhaaS project. Another possibility is that the developer of Tycoon 2FA was a customer of Dadsec OTT and had access to the front-end code. Further gathering of additional evidence, such as the source code of Tycoon 2FA, may help to confirm or refute these hypotheses.

Technical analysis

The technical analysis provided in this report is based on the new version of Tycoon 2FA released in mid-February 2024. According to Sekoia's tracking of Tycoon 2FA phishing pages, the earliest page corresponding to this new version was observed in the wild on 12 February 2024. An example of this version can be found at "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/*", which was scanned using urlscan[.]io at https://urlscan.io/result/1876f332-e54f-4d24-9a42-d703e80cc9ec/.

Our analysis is mainly based on the "victim-facing" interactions. We do not have access to the source code of the Tycoon 2FA phishing kit, meaning we cannot study the back-end of the adversary infrastructure.

The phishing kit **relies on the AiTM technique** and involves an attacker server (also known as reverse proxy server) hosting the phishing web page, intercepting victims' inputs and relaying them to the legitimate service, and prompting the MFA request. Once the user completes the MFA challenge, and the authentication is successful, the server in the middle captures session cookies. Stolen cookies allow attackers to replay a session and therefore bypass the MFA, even if credentials have been changed in between.

The following is a comprehensive overview of the main operations specific to the Tycoon 2FA phishing kit:

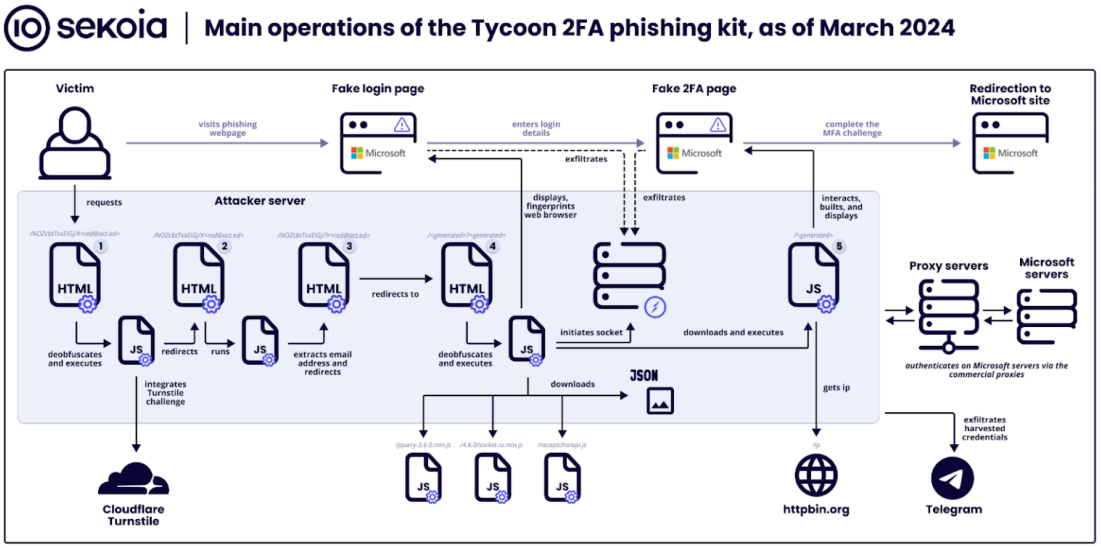

Figure 6. Overview of the main operations specific to the Tycoon 2FA phishing kit, as of March 2024

Stage 0 – Spreading phishing pages

The customers of the Tycoon 2FA PhaaS mainly distribute their phishing pages using redirections from URLs and QR code, which are embedded in email attachments or email bodies. The Tycoon 2FA service provides their clients with templates of phishing attachments (HTML pages), aiming at offering ready-to-use decoy documents, and making it easier for cybercriminals to carry out their campaigns.

For example, some PDFs use human resources, financial, or security-themed lures to convince the target into following the next steps up to sharing their credentials and resolving the MFA challenge. Sekoia observed decoys impersonating DocuSign, Microsoft, Adobe, among others (see Figure 1).

Most of the phishing campaigns carried out by the Tycoon 2FA customers seem to target organisations worldwide, by sending large volumes of phishing emails. Some of the customers focus on identifying and targeting employees in the financial, accounting, or executive departments to take advantage of their access through fraud or use of privileged information.

Stage 1 – Cloudflare Turnstile challenge

When a user clicks on the phishing URL, it is redirected to a page embedding a Cloudflare Turnstile challenge (see Annex 1) to prevent unwanted traffic.

Below are some examples of URLs:

- “*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/*” if not email address specified in the URL;
- “*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/X<red@act.ed>*”;
- “*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/X<base64(red@act.ed)>*”;

The HTML code of this page contains:

- A style attribute with CSS code that implements an infinite load;
- A script attribute that requests an alleged central Command & Control (C2) server and receives either a “*0*” or a “*1*”:

    - If the request returns "*0*", the script deobfuscates and writes a second HTML code, which is the page embedding the Cloudflare Turnstile challenge;
    - If the request returns "*1*", the script proceeds to the next step, which is the fake Microsoft phishing page prompting for email address;
- A base64 and XOR obfuscated HTML code imports the Cloudflare Turnstile challenge and displays the custom text "*this page is running browser checks to ensure your security*". It contains a script that performs the following actions:
    - Runs the Cloudflare Turnstile challenge;
    - Exfiltrates information to the phishing domain likely dedicated to the Tycoon 2FA customer. The POST request sends the following data: "*pagelink*", "*bltdip*" (the user's IP address), "*bltdref*" (the URL of the phishing page), "*bltdua*" (the User-Agent) and "*bltddata*". The C2 server responds either with "*success*" or "*error*";
    - Reloads the page when it receives a "*success*" from the C2 server;
    - Redirects to another page when it receives an "*error*".

Interestingly, the custom text displayed below the challenge is specific to the Tycoon 2FA phishing kit and enables us to recognise the phishing pages of this PhaaS quickly.

The next steps correspond to the common scenario when the user proceeds to the validation of the Cloudflare Turnstile challenge and receives a "*success*" from the C2 server.

This stage is not visible to the user, as it executes a JavaScript code in the background and then redirects the user to another page depending on the presence of an email address.

For this stage, the URL is identical to the previous one, as the page is reloaded. Therefore, it could be:

- "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/*";
- "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/X<red@act.ed>*";
- "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/X<base64(red@act.ed)>*".

The HTML code of this page contains a JavaScript code that extracts the email address from the URL (if it contains one), using regular expressions. It covers email addresses encoded using base64 and those in clear. It then redirects to the same URL, but with different characters after the separator "*?*", depending on the presence and the format of the email address.

Examples of the next-stage URL are:

- "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/?r*" if no email address extraction;
- "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/?r<red@act.ed>*" if an email address is extracted;
- "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/?rr<red@act.ed>*" if a base64-encoded email address is extracted.

Of note, the characters between the separators "*?*" and the email addresses are allegedly randomly generated by the C2 server.

Stage 3 – Redirection page

Once again, this stage is not visible to the user, as it redirects to another web page of the phishing domain.

The HTML code only contains the text "*Redirecting to*" and the next-stage URL, both in the HTML title and body.

An example of the next-stage URL is:

- "h*xxps://i9152.cisele0[.]com/lbuakdidnqmytlcBiVbomCGYTSPFFZAABOLJGWUCZHXZKPGZOQRAVFAAF?317727838333203306556902opEXJOOmXGJPZNFTJIXPAAFUILTKKRQQEFFSNIABRZNUPXEUOAKDATDS*"

Stage 4 – Fake Microsoft authentication login page and sockets

The HTML code is a script attribute that embeds a deobfuscation function and obfuscated HTML code, which is the fake Microsoft authentication page, and its grabbing features.

The deobfuscation function takes the obfuscation payload and a XOR key as arguments, decodes the base64-encoded payload, and XORs it.

The decoded HTML embeds the source code of the fake Microsoft authentication page, which downloads resources including:

- JavaScript files:
  - "*hxxps://www.google[.]com/recaptcha/api.js*"
  - "*hxxps://cdn.socket[.]io/4.6.0/socket.io.min.js*"
  - "*hxxps://code.jquery[.]com/jquery-3.6.0.min.js*"
- Images for the background and the icons of the phishing page;
- The redirection URL, if the authentication process succeeds.

It also contains over 260 lines of JavaScript code aiming to:

- Fingerprint the user's web browser using the User-Agent;
- Initiate a WebSocket with the C2 server (same domain as the phishing page), using the downloaded library "*socket.io.min.js*";
- Implement socket communications;
- Capture and exfiltrate the user inputs;
- Retrieve the final redirection URL.

At the end of the JavaScript code, it downloads and executes an additional highly obfuscated JavaScript, which implements the two-factor authentication (2FA) challenge.

An example of the JavaScript code URL is:

- "h*xxps://i9152.cisele0[.]com/34S7EHRE0DB8QrFfvijoRMsX632e0GRF8rZ89110*"

Stage 5 – 2FA relaying

The JavaScript code interacts with the HTML of the previous stage to build and display the Microsoft 2FA page.

The code is obfuscated using numerous variable renaming with hexadecimal patterns (*e.g.* "*_0x40e211*", "*_0x2db5*", "*_0x5e1add*"), string manipulation (*e.g.* split, extraction, concatenation), functions overlay, and other code transformations. TDR analysts assess that the Tycoon 2FA developer likely used the open-source tool javascript-obfuscator available[3] on GitHub to obfuscate this stage.

If the first step of the authentication using the email address and password succeeds, the JavaScript code is then responsible for handling user interactions and form validation of the phishing page. It also updates the HTML page with the fake Microsoft page implementing the 2FA method. For this, it implements numerous conditional statements depending on the user inputs and responses of the Microsoft server. Some elements to be displayed on the phishing page are also received by the WebSockets, including the final redirection page, or the message error if the Microsoft API denies the 2FA challenge.

Based on the JavaScript code received by the user web browser, Tycoon 2FA implements the following 2FA methods:

- Microsoft Authenticator (push notifications)

- One-time password (OTP) code, delivered by:
  - Applications
  - SMS
- Phone call verification

Using commercial proxy servers, the Tycoon 2FA phishing pages relay the user inputs, including the email address, the password, and the 2FA code, to the legitimate Microsoft authentication API. The response to the Microsoft API traffic returns the appropriate pages and information to the user.

Due to its position in the middle of the authentication process, the C2 server captures all relevant data and notably the session cookies, allowing the cybercriminals to replay a session and therefore bypass the MFA.

This **2FA relaying capability is the core feature of an AiTM phishing kit, aiming at intercepting login details** during a legitimate session-based authentication between the victim and the legitimate service. From the perspective of the victim's web browser, the Tycoon 2FA relaying capability consists of a JavaScript code implementing all the variations in a successful or failed Microsoft 365 authentication.

Stage 6 – Final redirection

The final stage of the Tycoon 2FA phishing kit involves redirecting the user to a URL specified by the cybercriminal.

The JavaScript code of the stage 4 embeds an endpoint URL in the variable "*urlo*" aimed at returning the final redirection URL. When the authentication is successful, the phishing page sends a POST request to this endpoint with a session identifier (argument "*pagelink*") set during the WebSocket communications and other information. Then, the C2 server responds with the redirection URL.

Most customers of the Tycoon 2FA PhaaS use the default redirection URL, which is "*hxxps://login.microsoftonline[.]com/common/SAS/ProcessAuth*". Subsequently, we observed a threat actor who used a non-existent WeTransfer URL "*hxxps://wetransfer[.]com/invoicedocument*" (see Annex 2). This use is possibly related to a phishing email pretending that the user must authenticate on Microsoft 365 to access a document. Once authenticated through the Tycoon 2FA phishing page, the user is redirected to this legitimate "not found" webpage, which could lead them not to suspect that the previous page was malicious. The same goes for the default redirection URL, which redirects the user to an error page of the legitimate Microsoft website.

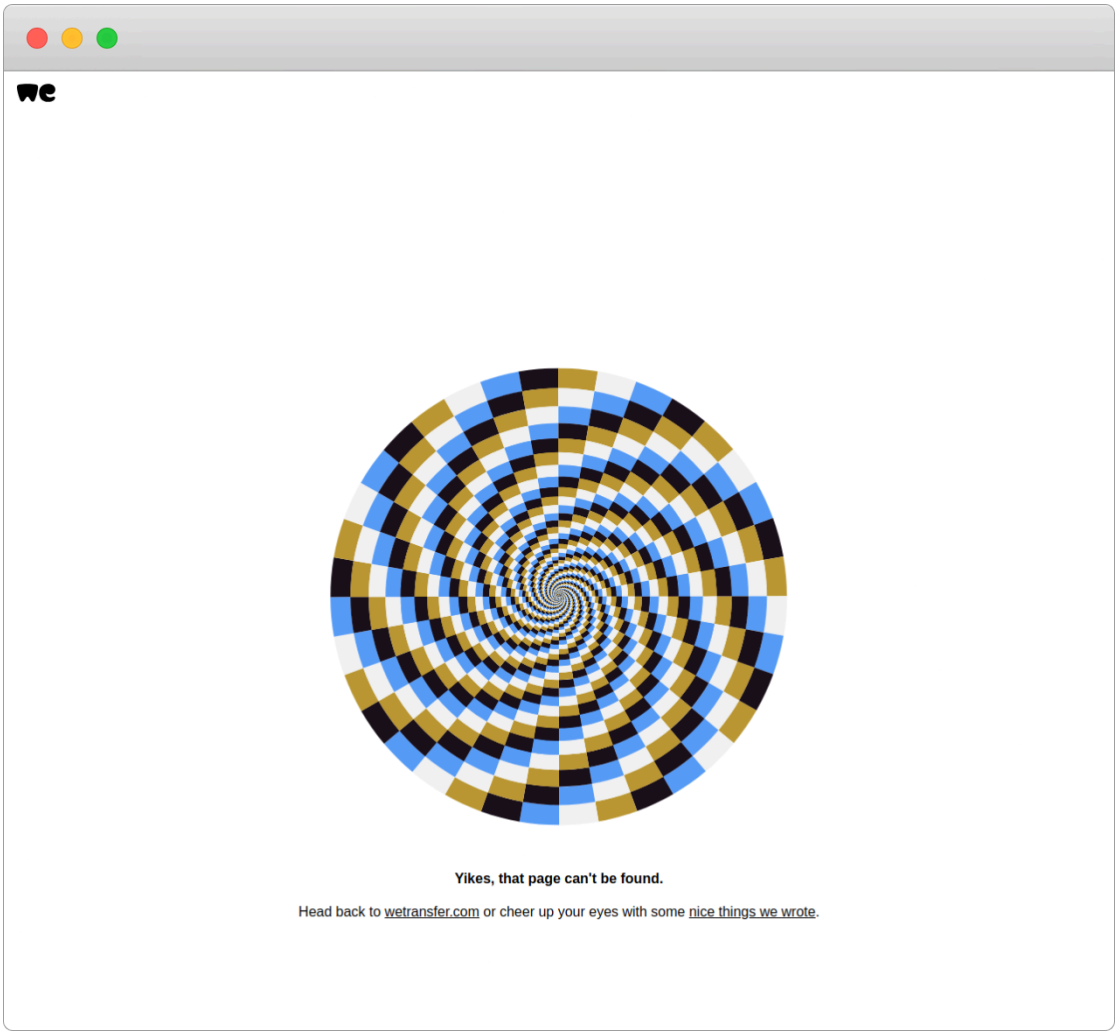

Figure 7. Final redirection to a non-existent WeTransfer webpage, after a successful authentication on the Tycoon 2FA phishing page

Finally, the phishing page once again exfiltrates some victim details to the C2 server using a HTTP POST request. The sent data include the session identifier (argument "*pagelink*"), the IP address obtained from the "*httpbin[.]org*" API, the User-Agent and other information.

Regarding the redundancy of this communication, Sekoia analysts believe that **the developer did not invest significant effort in optimising the code of the phishing kit, revealing that this phishing kit is not as sophisticated as some other PhaaS competitors such as Caffeine**.

Exfiltration through WebSockets

From the rendering of the fake Microsoft page to the closure of the phishing page by the user, the **C2 server collects harvested data and status of the operations using WebSockets**. It also communicates to the user web browser some elements to build the following phishing pages.

An example of URL initiating the WebSockets communications is:

- "h*xxps://i9152.cisele0[.]com/web6socket/socket.io/?type=User&appnum=1&EIO=4&transport=websocket*"

The following is the main steps of the Tycoon 2FA WebSocket communications for a successful authentication using the Microsoft Authenticator as 2FA (the client being the user web browser):

← Initiation of the WebSocket (server to client)	{“sid”:”4KP6W7ZLo_GpdtK9AF6E”,”upgrades”:[],”pingInterval”:1000,”pingTimeout”:60000,”maxPayload”:1000000}
→ Exfiltration of the user details (client to server)	[“send_to_browser”,{“route”:”enteremail”,”arguments”:[“<EMAIL ADDRESS”,”<SESSION ID>”,”chrome”,”<IP ADDRESS>”],”getresponse”:1}]
→ Update of the status (client to server)	[“browser_connected”,”4572″]
← Response of the server (server to client)	[“response_from_browser”,{“message”:”correct email”,”bottomsection”:[{“a_text”:”Forgot my password”,”a_id”:”idA_PWD_ForgotPassword”,”type”:”link”}],”backbutton”:1}]
→ Exfiltration of the user password (client to server)	[“send_to_browser”,{“route”:”enterpassword”,”arguments”:[“<PASSWORD>”],”getresponse”:1}]
← Response of the server (server to client)	[“response_from_browser”,{“message”:”approve auth request auth app”,”bottomsection”:[{“a_text”:”I can’t use my Microsoft Authenticator app right now”,”a_id”:”signInAnotherWay”,”type”:”link”},{“a_text”:”More information”,”a_id”:”moreInfoUrl”,”type”:”link”}],”backbutton”:0,”authappcode”:”39″,”description”:{“type”:”text”,”text”:”Open your Authenticator app, and enter the number shown to sign in. ”},”image_src”:”<ICON_LINK>”}]
→ Acknowledge of the client (client to server)	[“send_to_browser”,{“route”:”responserecieved”,”arguments”:[],”getresponse”:0}]

→ Waiting for 2FA validation (Microsoft Authenticator) (client to server)	[“send_to_browser”,{“route”:”waitauth”,”arguments”:[“app”],”getresponse”:1}]

The WebSocket communications exfiltrating harvested credentials remain unchanged in the latest version of the Tycoon 2FA phishing kit.

Main changes in the latest version

The latest version of Tycoon 2FA introduced changes to the JavaScript and HTML codes responsible for its main phishing capabilities. Additionally, the phishing page retrieves its various resources in a different order and filters unwanted traffic more widely to reject those from bots or analysis.

To identify the main changes introduced by the latest version, here is an overview of how the previous version worked and a comparison with our analysis of the new version:

1. The first HTML page contains a JavaScript code that fingerprints the web browser, deobfuscates the next-stage URL, and redirects to the next-stage.

→ This stage is similar to the stage 1 of the new version, but does not embed the Cloudflare Turnstile challenge.

2. The next-stage payload is an obfuscated JavaScript code, named with the characteristic pattern “/myscr[0-9]{6}.js”, which corresponds to the fake Microsoft authentication page and also embeds the Cloudflare Turnstile challenge. The HTML code of the fake Microsoft login page is encoded as unicode in a large array of integers. Mathematical operations whose results do not influence deobfuscate are performed.

→ This stage includes a part of stage 4 (the fake login page) and stage 1 of the new version (CloudFlare Turnstile challenge). The deobfuscation method embedding unnecessary mathematical operations disappeared in the latest version.

3. The old version downloads the three following JavaScript codes:

- “*/web6/assets/js/pages-head-top-web.min.js*”, which downloads the WebSocket JavaScript library and the second JavaScript code;
- “*/web6/assets/js/pages-head-web.min.js*”, which implements the 2FA relying using the WebSocket and downloads the third JavaScript code;
- “*/web6/assets/js/pages.min.js*”, that builds the 2FA challenge webpages.

→ This stage is now part of stage 4 and 5.

4. It sends data to “*/web6/info*” using several POST requests and retrieves the HTML code to build the 2FA challenge webpages.

→ This stage is now part of stage 4 and 5.

By comparing two versions of the Tycoon 2FA phishing kit, we identified similar deobfuscation functions and core functionalities. However, notable changes were made to the structure of the different stages.

Notably, there was an enhancement in stealth tactics by providing the malicious resources once the user resolved the CloudFlare Turnstile challenge. And URLs are now set using pseudorandom names.

Moreover, it appears that the phishing kit developer **extended the kit's capabilities to identify and evade more traffic patterns associated with analysis or scan environments**. This includes IP addresses hosted in datacenters or associated with the Tor network, as well as specific User-Agent strings of bots and some versions of Linux web browsers.

These changes suggest a **deliberate effort to improve the phishing kit's stealth and evasion techniques, to strengthen its resilience against detection and analysis**.

Tracking opportunities

Sekoia analysts actively monitor the Tycoon 2FA phishing infrastructure by tracking phishing URLs.

In response to the changes made to the phishing kit in mid-February 2024, we updated our tracking heuristics to illuminate the infrastructure hosting the new version of Tycoon 2024.

Previous resources-based heuristics

As mentioned above, the older versions of Tycoon 2FA used JavaScript files with characteristic patterns or hardcoded names.

Some of our basic heuristics based on the URL pattern stem from the Tycoon 2FA requests. Sekoia analysts used queries similar to the following one on urlscan[.]io:

- Heuristic valid since August 2023:

filename:("pages-godaddy.css" AND "pages-okta.css")

This query relied on the specific names of two CSS files used by the phishing kit to replicate login pages. By March 2024, this heuristic yielded over 3,000 results on urlscan, all associated with high confidence with Tycoon 2FA phishing pages.

- Heuristic valid since August 2023:

filename.keyword:/.*\/myscr[0-9]{6}\.js/ filename:"turnstile/v0/api.js"

This query is based on the specific generated name of the JavaScript code embedding the fake Microsoft login page and the Cloudflare Turnstile challenge. By March 2024, this heuristic yielded over 4000 results on urlscan, all strongly associated with Tycoon 2FA phishing pages.

- Heuristic valid since November 2023:

filename:("/web6/assets/js/pages-head-top-web.min.js" OR "/web6/assets/js/pages-head-web.min.js")

This query is based on the specific names of JavaScript code implementing core capabilities of the Tycoon 2FA phishing kit, such as exfiltration using WebSockets, and dynamically building the 2FA relaying pages. By March 2024, this heuristic yielded around 3,000 results on urlscan, associated with high confidence with Tycoon 2FA phishing pages.

However, recent changes in Tycoon 2FA led to the renaming and modification of these specific resources. Also, they are not loaded until the Cloudflare Turnstile challenge is resolved. Therefore, the phishing pages of the latest version no longer load these specific resources when analysed by URL scanning services.

Resources-based heuristics for the latest version

When scanning a Tycoon 2FA phishing page using the latest version, only requests of stages 0 and 1 are sent, as the Turnstile challenge must then be solved first. If no redirection steps precede the URL of the phishing page, the scan results in 5 requests, *e.g.*:

Requests for stage 0 and 1	**Details**	**Size**
GET hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/	Tycoon 2FA phishing page	7 KB
GET hxxps://7374.ginvet9[.]com/	Central server to approve the Turnstile challenge	1 B
GET hxxps://code.jquery[.]com/jquery-3.6.0.min.js	Jquery library	87 KB
GET hxxps://challenges.cloudflare[.]com/turnstile/v0/api.js?render=explicit	Cloudflare Turnstile challenge	38 KB
GET hxxps://challenges.cloudflare[.]com/cdn-cgi/challenge-platform/h/g/turnstile/if/ov2/av0/rcv0/0/8jtx6/0x4AAAAAAAS4S8P1a9d4qbbW/auto/	Cloudflare Turnstile challenge	0 B

To find a heuristic to list Tycoon 2FA phishing pages using the latest version, we can use the following elements on urlscan[.]io:

- The hash of the response from the central C2 server, mostly returning "*0*" to approve the challenge display (SHA256: *5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9*);
- The resources requested by the phishing page before the Turnstile challenge;
- A limited number of requests are sent (5 if no redirection steps), and the total of data received does not exceed 150 KB

Sekoia analysts use similar queries on urlscan:

- Heuristic valid since mid-February 2024:

filename:("code.jquery.com/jquery-3.6.0.min.js" AND "challenges.cloudflare.com/turnstile/v0/api.js")
hash:5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9

This query uses the hash of the response of the central C2 server. In March 2024, this heuristic yielded over 500 results on urlscan, associated with high confidence with Tycoon 2FA phishing pages.

- Heuristic valid since August 2023:

filename:("code.jquery.com/jquery-3.6.0.min.js" AND "challenges.cloudflare.com/turnstile/v0/api.js") stats.requests:<7 stats.dataLength:<150000

This query uses the number of requests and the data size of all resources. In March 2024, this heuristic yielded over 700 results on urlscan that we associated with medium confidence with Tycoon 2FA phishing pages.

Tracking Tycoon 2FA is more complex since the developer enhanced the stealth capabilities of the phishing kit. Even though we cannot use characteristic filenames to continue tracking the phishing pages, **Sekoia found heuristics by correlating the legitimate resource names with the response of the central C2 server, or the length of the data as well as the size of the resources**.

HTML page embedding the Cloudflare Turnstile challenge

As already mentioned, the HTML page importing the Cloudflare Turnstile challenge displays the text "*this page is running browser checks to ensure your security*".

Given that the urlscan Pro service allows to search for the visible text context, we can use the following query to list the Tycoon 2FA phishing pages:

text.content:"this page is running browser checks to ensure your security"

Cryptocurrency asset

On 28 November 2023, a screenshot was published in the "*Saad Tycoon Group*" Telegram channel, illustrating a private discussion with a Tycoon 2FA customer sharing feedback about the service. The discussion mentioned a Bitcoin address (19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx), that we assess with high confidence to belong to "*Saad Tycoon Group*", the operator and alleged developer of the PhaaS.

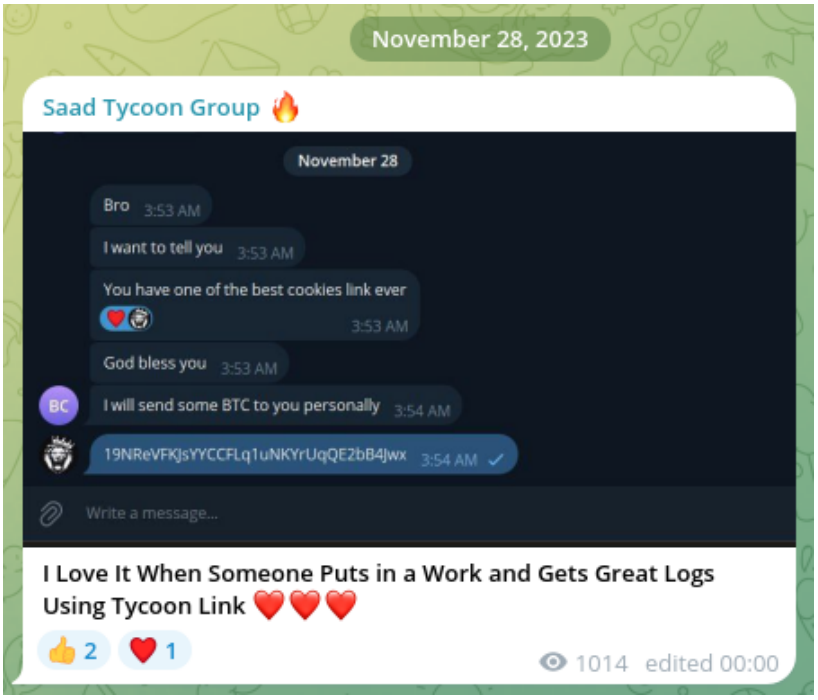

Figure 8. Publication in the Tycoon 2FA Telegram channel mentioning a Bitcoin address, allegedly belonging to "Saad Tycoon Group"

Investigation of the cryptocurrency wallet led us to make the following observations, as of mid-March 2024:

- Since October 2019, the Bitcoin wallet has recorded more than 1,800 transactions including 1117 inputs and 1088 outputs;
- According to BlockExplorer[4], the total amount of Bitcoin as of 12 March 2024:
  - Sent is 5.46848394 BTC (around $391,644 at the time of writing)
  - Received is 5.50159883 BTC (around $394,015 at the time of writing)
- Since August 2023, the potential beginning of Tycoon 2FA's activities:
  - The wallet has recorded around 700 incoming transactions with an average value of $366;
  - Approximately 90% of their values were between $25 and $720;
  - The total value of transactions exceeded $250,000;
  - More than 530 transactions were over $120, which is the entry price of the PhaaS for a 10 days .ru link.

Over the last few months, **the wallet dynamics (incoming transactions and associated amounts) align with the observed Tycoon 2FA PhaaS activities**. Indeed, the prices publicly announced by the service range between $120 and $320. Additionally, the operator of the PhaaS mentioned that the customers have to pay an extra charge for any domain change, which could explain transactions of a few dozen dollars.

Assuming that the wallet is mainly used for the Tycoon 2FA PhaaS operations since August 2023, **the total amount of transactions suggests that several hundred Tycoon 2FA kits were sold as-a-service over half a year**. These alleged sales figures are consistent with the thousands of phishing pages that were collected in the wild since August 2023 and associated with high confidence with Tycoon 2FA.

The total amount of transactions on the *Saad Tycoon Group*'s Bitcoin wallet indicates that **the fraudulent service generates a significant amount of money**. The financial cost of the phishing infrastructure is substantial for this service, encompassing domain registration, server hosting, possibly phishing page protection using Cloudflare (hosting and Cloudflare Turnstile) and commercial proxy services. Conversely, the development and maintenance of the kit likely rely on one individual, given the relatively low sophistication and limited improvements over time.

Conclusion

First seen in the wild in August 2023, **Tycoon 2FA is an Adversary-in-The-Middle phishing kit, distributed under the Phishing-as-a-Service model**. It mainly aims to harvest Microsoft 365 session cookies to bypass the MFA process during subsequent authentication. Tycoon 2FA became widespread in the months following its release and is currently massively used in numerous phishing campaigns.

Our analysis of the main operations of Tycoon 2FA revealed that **the developer enhanced stealth capabilities in the most recent version of the phishing kit**. The recent updates could reduce the detection rate by security products of the Tycoon 2FA phishing pages and the infrastructure. Additionally, its ease of use and its relatively low price make it quite popular among threat actors.

Sekoia actively monitors the Tycoon 2FA phishing infrastructure and has identified over 1,200 domain names since August 2023. Using the tracking heuristics shared above, we will continue to actively monitor the infrastructure.

Through studying the Bitcoin transactions allegedly attributed to *Saad Tycoon Group*, Sekoia analysts believe that **the Tycoon Group operations are highly lucrative**, and we expect the Tycoon 2FA PhaaS to remain a prominent threat within the AiTM phishing market in 2024.

To provide our customers with actionable intelligence, TDR analysts will continue to monitor the prevalent PhaaS and proactively search for the associated infrastructures.

IoCs & Technical details

Tycoon 2FA IoCs

The list of IoCs is available on Sekoia.io GitHub repository.

0q5e0.nemen9[.]com
25rw2.canweal[.]com
35fu2.ouchar[.]ru
4343w.jgu0[.]com
43rw98nop8.m1p8z[.]com
4m2swl.7e2r[.]com
5me78.methw[.]ru
6j312.rchan0[.]com
77p3e.rimesh3[.]com
8000n.uqin[.]ru
8uecv.gnornamb[.]com
98q5e.ructin[.]com
9c43r.theq0[.]com
9oc0y2isa27.demur3[.]com
beacon.diremsto[.]com
bloggcenter[.]com
buneji.fiernmar[.]com
e85t8.nechsha[.]com
ex1uo.rhknt[.]ru
explore.atlester[.]ru
fiq75d.rexj[.]ru
fisaca.trodeckh[.]com
galume.aricente[.]com
gz238.uatimin[.]com
horizon.sologerg[.]com
jp1y36.it2ua[.]com
k348d.venti71[.]com
kjlvo.ningeona[.]com
kjsdflwe.nitertym[.]ru
l846d.ferver8[.]com
libudi.oreversa[.]com
n29k4.ilert[.]ru
n9zph.lw8opi[.]com
o6t94g.3tdx2r[.]com
oo99v.coqqwx[.]ru
p1v12.17nor[.]com
pmd8ot6xhw.3qjpc[.]com
q908q.refec7[.]com
r298y.sem01[.]com
rlpq.tk9u[.]com
roriku.orankfix[.]com
tlger-surveillance[.]com
tnyr.moporins[.]com
wasogo.shantowd[.]com

x12y.restrice[.]ru
xrs.chenebystie[.]com
xva.tjlpkcia[.]com
zaqaxu.dthiterp[.]ru
zekal6.tnjxb[.]com
zemj4f.ymarir[.]ru

Cryptocurrency wallet address

19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx used by Saad Tycoon Group

External references

1. https://twitter.com/sekoia_io/status/1717891843105366409 ↩
2. https://twitter.com/sekoia_io/status/1717891849153610153 ↩
3. https://github.com/javascript-obfuscator/javascript-obfuscator/ ↩
4. https://blockexplorer.one/bitcoin/mainnet/address/19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx ↩

Feel free to read other Sekoia TDR (Threat Detection & Research) analysis here :

CTI Cybercrime Infrastructure

Share this post:
