UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Microsoft Corporation, a Washington Corporation and Health-ISAC, INC., a Florida Corporation,

Plaintiff,

v.

Saad Fridi,

and

John Does 1-4, Controlling A Computer Network and Thereby Injuring Plaintiffs and Their Customers,

Defendants.

Civil Action No.

FILED UNDER SEAL PURSUANT TO LOCAL RULE 5

DECLARATION OF SELENA LARSON IN SUPPORT OF PLAINTIFFS' *EX PARTE* APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER

I, Selena Larson, declare as follows:

1. I am a Staff Threat Researcher at Proofpoint, a cybersecurity company that detects and blocks email-based threats at scale. We protect 2.7 million customers and have broad visibility into cybercrime activity that uses email to distribute malicious links and attachments. A current version of my curriculum vitae is attached to this declaration as Exhibit 1.

2. I make this declaration in support of Plaintiffs' *Ex Parte* Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted. If called as a witness, I could and would testify to the truth of the matters set forth herein.

3. My team of researchers identifies and investigates advanced threats and develops actionable threat intelligence that we use to secure our customers. Our team focuses on both

espionage and cybercriminal activities, including credential phishing operations like Tycoon 2FA.

Overview of Tycoon 2FA Phishing Campaigns

4. My declaration focuses on the Tycoon 2FA phishing kit and associated activities. Tycoon 2FA operates as an adversary-in-the-middle (AitM)[1] phishing kit. Its primary function is to harvest usernames, passwords, and Microsoft 365 and Gmail session cookies. Attackers use these cookies to circumvent multifactor authentication (MFA)[2] access controls during subsequent authentication. That allows them to achieve full account takeover (ATO) and gain unauthorized access to a user's accounts, systems and cloud services—even those that have MFA as an additional security measure.

5. According to our internal threat data, in 2025, 99% of organizations experienced account takeover attempts, and 67% experienced a successful account takeover as a result of phishing activity. Of these, 59% of taken over accounts had MFA enabled. While not all MFA bypassing ATO campaigns are attributable to Tycoon 2FA, the Tycoon 2FA Defendants are responsible for the highest volume AiTM phishing threat in Proofpoint visibility. Tycoon 2FA message volumes vary based on threat actor activity, and in February 2026, Proofpoint has observed over 3 million messages associated with Tycoon 2FA.

---

[1] AiTM, which is a form of cyberattack where the malicious actor intercepts communications between two parties without their knowledge. It is particularly common for AiTM attacks to leverage PhaaS platforms given the high volume of phishing emails that these phishing kits make possible. This enables these criminals to then enter the system using these purloined credentials and remain undetected.

[2] MFA or multi factor authentication is a security process requiring users to provide two or more different types of factors to verify their identify to reduce the risk of unauthorized access. Tycoon 2FA Defendants are so deadly because their kits allow threat actors to collect not only the password but the MFA token as well.

6. Tycoon 2FA Defendants rely on attacker-controlled infrastructure to host the phishing webpage. Using the AiTM attack methodology, the platform allows the interception of victims' entered credentials. The credentials are then relayed to the legitimate service for a transparent, successful login, prompting MFA requests (this step ensures that the victim does not suspect cybercriminal activity). The resulting session cookies are relayed back to the threat actors.

7. Tycoon 2FA is sold as a phishing-as-a-service (PhaaS) kit, meaning that threat actors purchase access to the phishing tool and then they can customize it to suit their specific needs. The kit can be used multiple times through the duration of the subscription. Tycoon 2FA is used by multiple different threat actors, and sold by one main individual. It has been sold on Telegram since 2023 and was initially distributed via the "Saad Tycoon Group" Telegram channel.[3]

8. Some Tycoon 2FA users (cybercriminals who purchase the kit) are leveraging "ATO Jumping" whereby the actor compromises an initial email account, uses the compromised sender to broadly distribute Tycoon 2FA URLs, and attempts further account takeover (ATO) activities. Using this technique enables the phishing emails to look like they are authentically coming from a victim's trusted contact, increasing the likelihood of a successful compromise.

9. Tycoon 2FA infections can lead to a variety of malicious activities including theft of private data including financial information, personally identifiable information, proprietary business information; full account takeover and access to M365 hosts that can be sold to

---

[3] *See* Sekoia TDR and Quentin Bourge, Quentin Bourge, *Tycoon 2FA: an in-depth analysis of the latest version of the AiTM phishing kit*, Sekoia, available at https://blog.sekoia.io/tycoon-2fa-an-in-depth-analysis-of-the-latest-version-of-the-aitm-phishing-kit/#88b42268-54a7-49a0-9ff6-3f3d363c41ea (Mar. 25, 2024).

additional threat actors; and potentially lead to follow-on malware compromises including ransomware attacks.

Proofpoint's Investigation into Tycoon 2FA

10. My team has regularly tracked actors using the Tycoon 2FA phishing kit since 2024, and we have observed over 250 campaigns impacting our customers.

11. We observe Tycoon 2FA distributed via email campaigns. A campaign is a time-bound set of related activity that is clustered by indicators of compromise (IOCs) such as senders, URLs, attachments, Tycoon 2FA configuration, etc. Tycoon 2FA campaigns vary in terms of scale; some include just a handful of messages; some include millions of messages. Campaign timelines can range from one day to one week.

12. Tycoon 2FA kits allow distribution of the phishing emails based on the criminals' preferred method of email spam. Emails may contain malicious links, QR codes, SVGs, or attachments with URLs. In all cases, a user is redirected to an actor-controlled URL that displays a unique CAPTCHA resolution that, if solved, will direct to an attacker-controlled site impersonating a Microsoft or Google login portal. In many cases, the threat actor will display a target organization's Azure Active Directory branding to further the social engineering component and trick a user into thinking they are entering their credentials into a real corporate site.

13. Tycoon 2FA campaigns are typically opportunistic and target a broad range of organizations and leverage compromised accounts to spread their phishing kits. Proofpoint has observed Tycoon 2FA launching its phishing attacks via compromised accounts from various industries including legal, real estate, healthcare, government, education, construction, and technology, as well as personal emails such as Gmail addresses. **Figure 1** is an example of a

phishing email that is attributed to Tycoon 2FA. As shown in the screenshot, the threat actor invites review of a document and encourages the recipient to click on the link. If the recipient clicks on the lick they will be taken to a Tycoon 2FA-controlled page. **Figures 2-3** shows the sign on process that the victim is redirected to, where they are showed a fake login screen that is controlled by Tycoon 2FA.

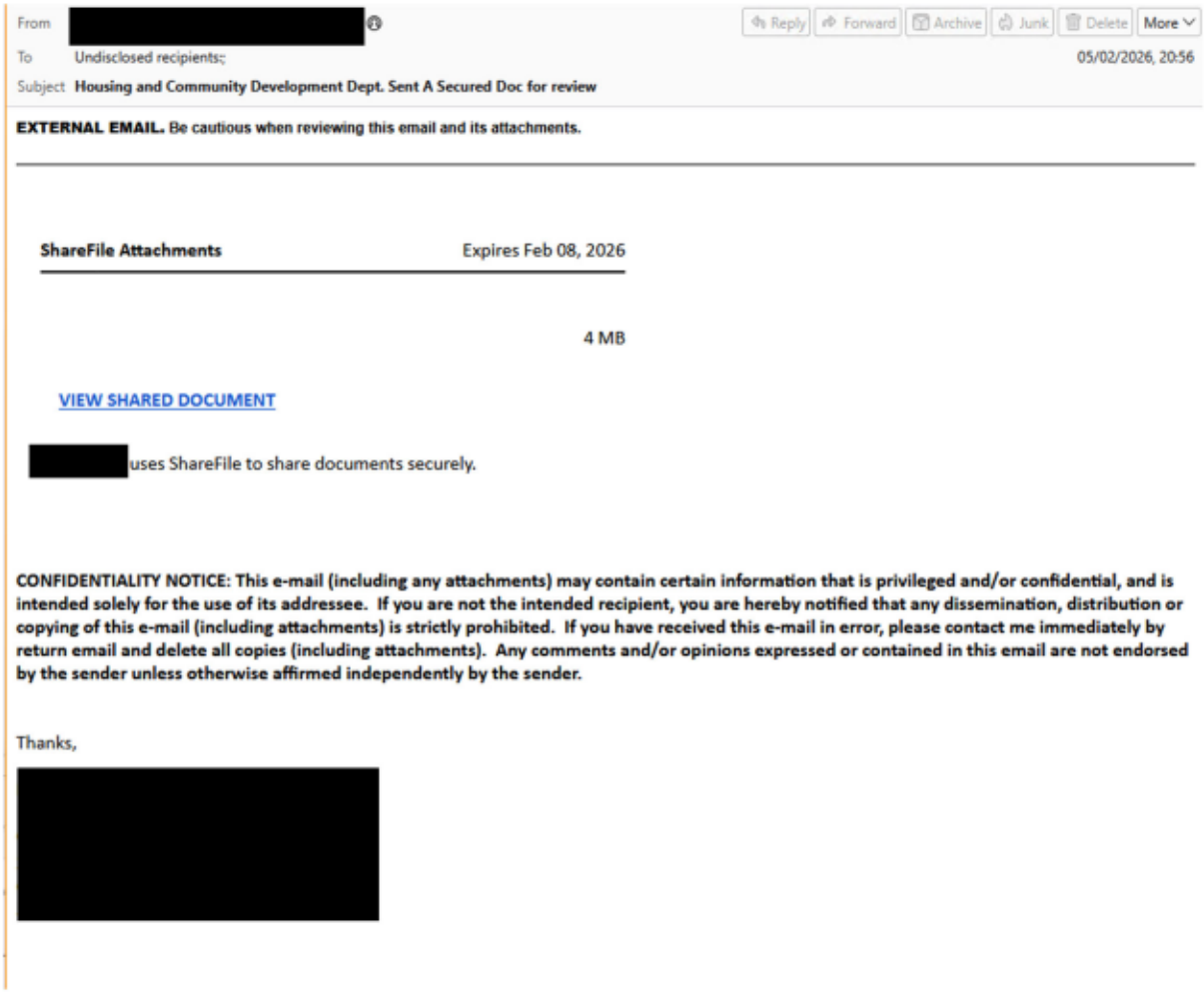

Figure 1: Tycoon 2FA phishing email containing a Defendant-controlled URL.

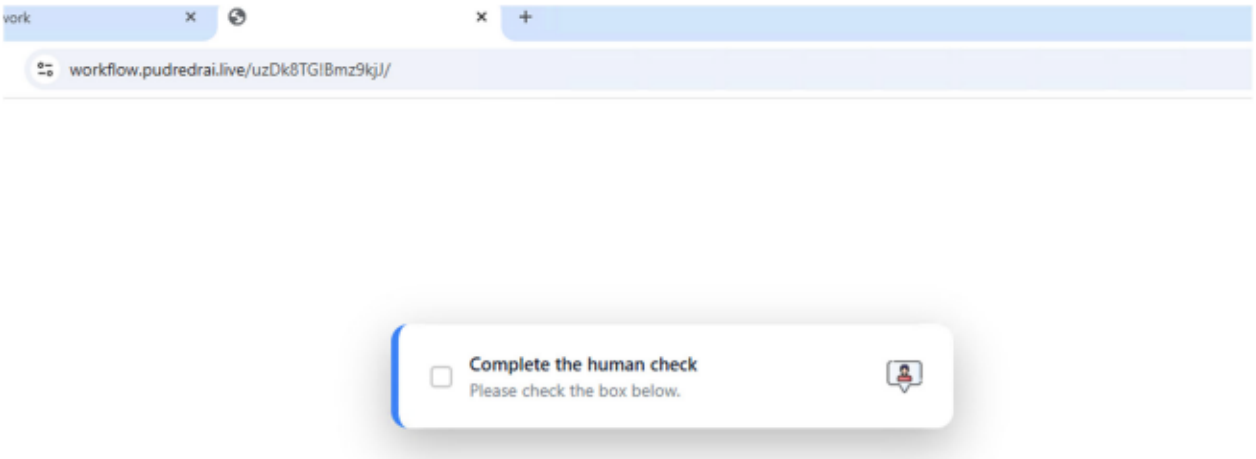

Figure 2: Tycoon 2FA CAPTCHA.

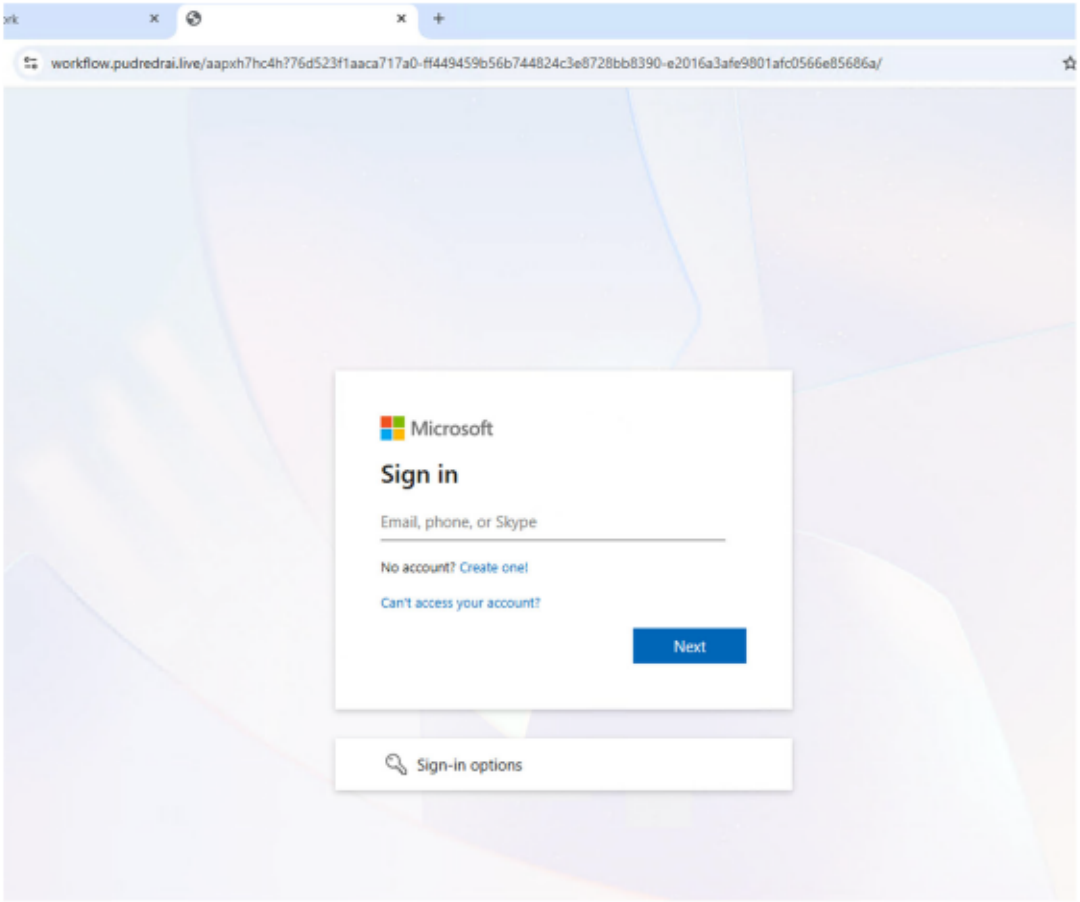

Figure 3: Tycoon 2FA login page impersonating a legitimate Microsoft sign in page.

Attribution of 2FA Tycoon Defendants

14. Proofpoint is able to attribute campaigns to Tycoon 2FA Defendants phishing based on a variety of factors including the panel used by customers to manage campaigns, CAPTCHA landing pages used by the threat actors, and artifacts in the credential receiver webpages.

15. Tycoon 2FA customers manage their campaigns via a control panel provided and administered by the Defendant Fridi. The panel landing pages have changed slightly since 2023, but overall, the general URL structure and landing page functionality has remained the same. These similarities have allowed me to investigate Tycoon 2FA behavior and develop signatures that allow me to attribute phishing activity to Tycoon 2FA Defendants.

16. Tycoon 2FA provides purchasers with a control panel, or dashboard, that the purchasers of the kit can use to create phishing templates, launch their phishing activity, and track metrics of their phishing campaigns. It is possible to access the control panel login page by taking a Tycoon 2FA-controlled domain (for example a domain that is embedded in the phishing email) and replacing the hostname with either “pannal” or “panel” and entering /sp/ in the URI.

17. For instance, in October 2024, one of the Tycoon 2FA-controlled domains was jlzq[.]riandleas[.]com, and the associated control panel was accessible through the URL https[:]//panel[.]riandleas[.]com/sp/login. *See* **Figure 4.**

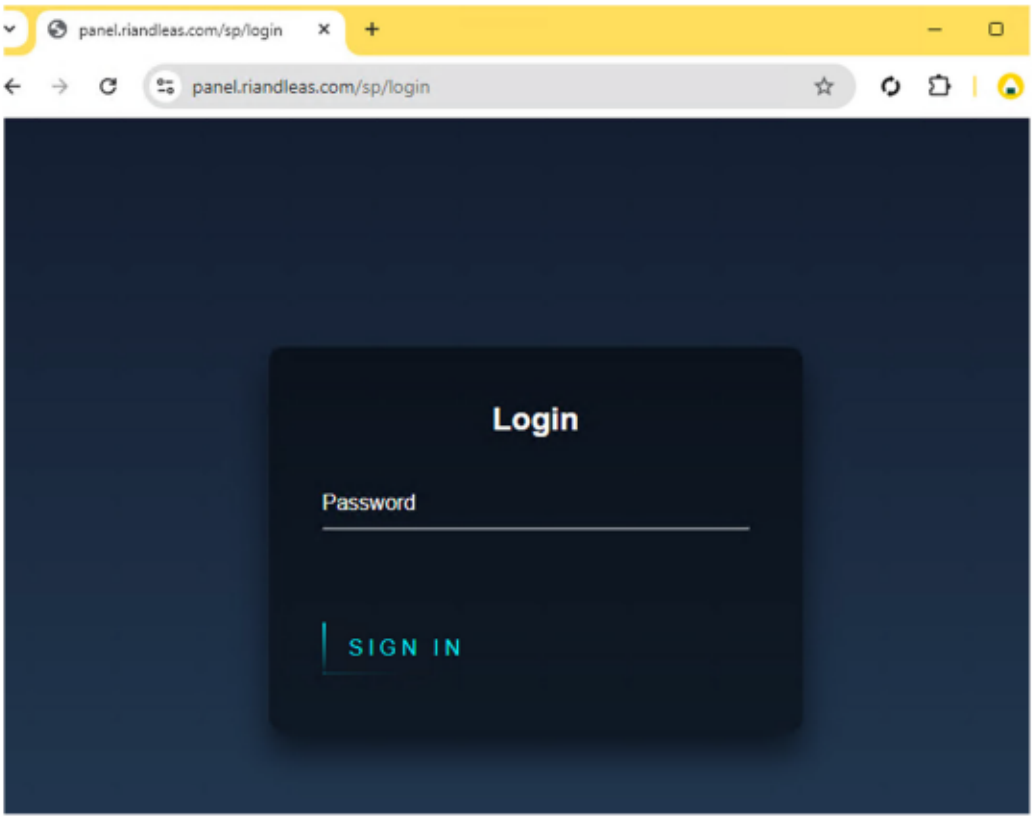

Figure 4: Panel screenshot for Tycoon 2FA login panel.

18. As another example, cd[.]frafiomai[.]co[.]za is another Tycoon 2FA-controlled domain. The associated control panel was accessible through the following URL: https[:]//pannal[.]frafiomai[.]co[.]za/sp/login. *See* **Figure 5**. When a purchaser of the phishing kit log into their control panel, they have to complete a CAPTCHA to verify that they are not a bot or automated scanner. *See* **Figure 6** By requiring a CAPTCHA during the login sequence, Tycoon 2FA adds a heighted level of security to control panel access. This makes this phishing kit particularly attractive for cybercriminals because it prevents automated analysis and access to the panel, adding an extra layer of security for threat actors. **Figures 5 and 6** represent what the control panel login page and CAPTCHA process looked like in 2025. In 2026, Tycoon 2FA has changed the appearance of the control panel login page and CAPTCHA process (*see* **Figure 7-8**) but the infrastructure and process remain the same.

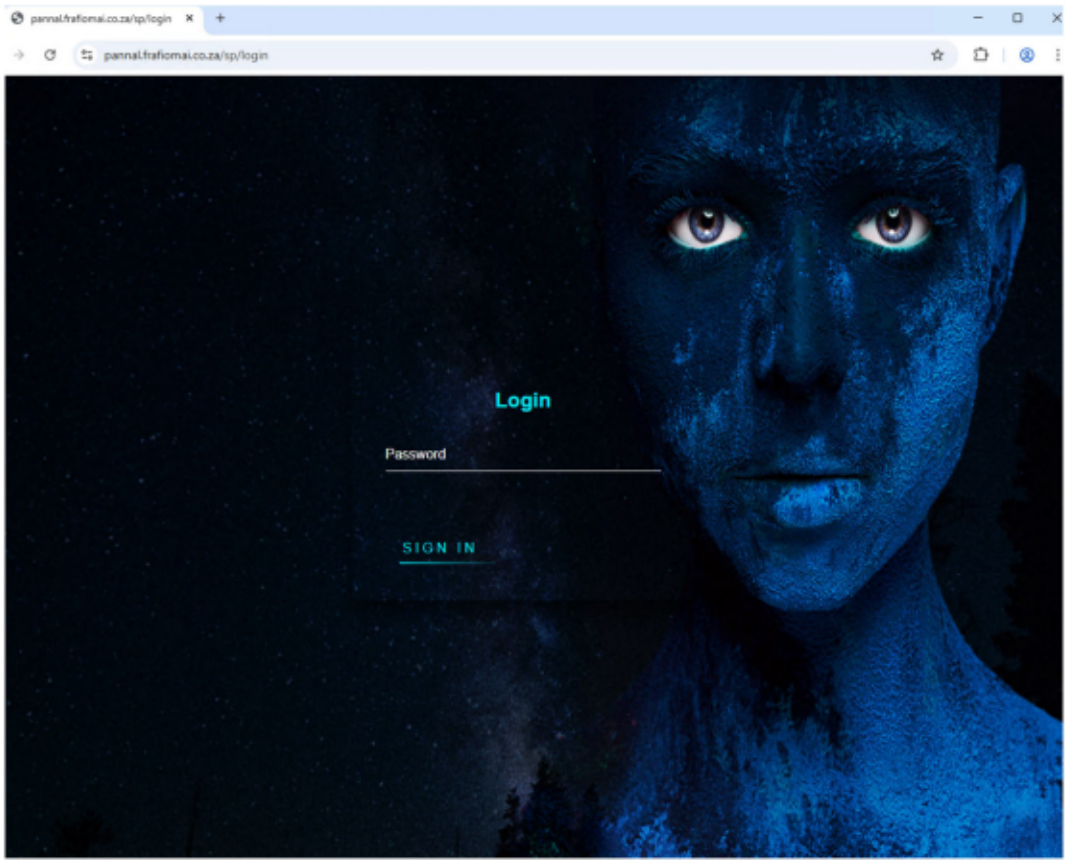

Figure 5: Panel landing page (2025)

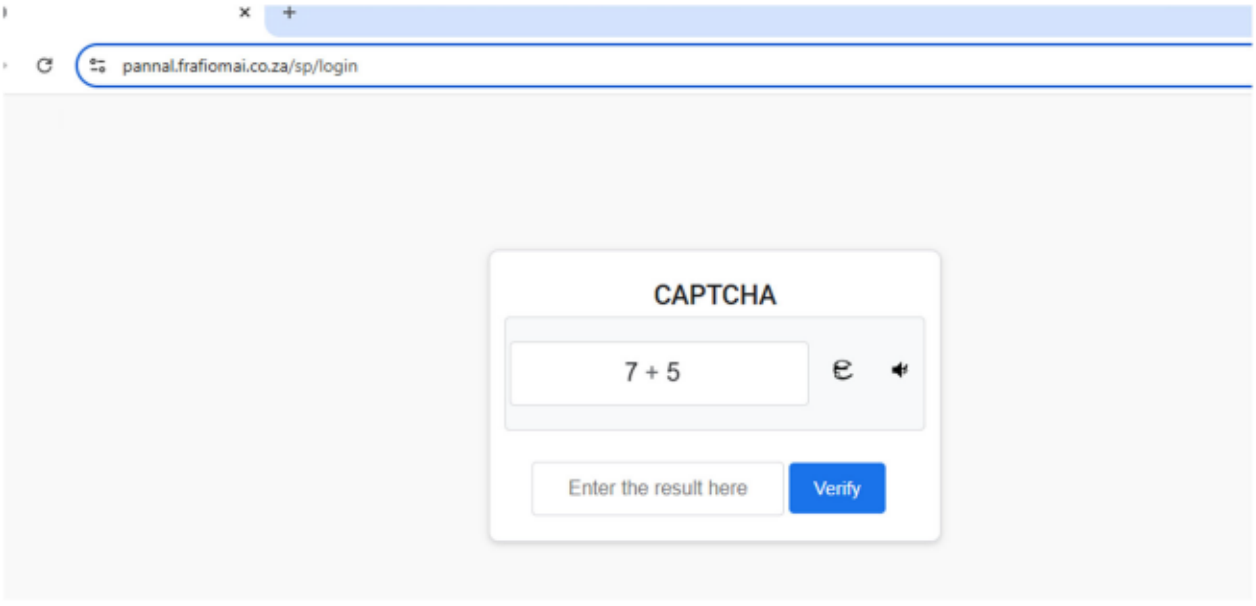

Figure 6: CAPTCHA required to access the Tycoon 2FA panel (2025)

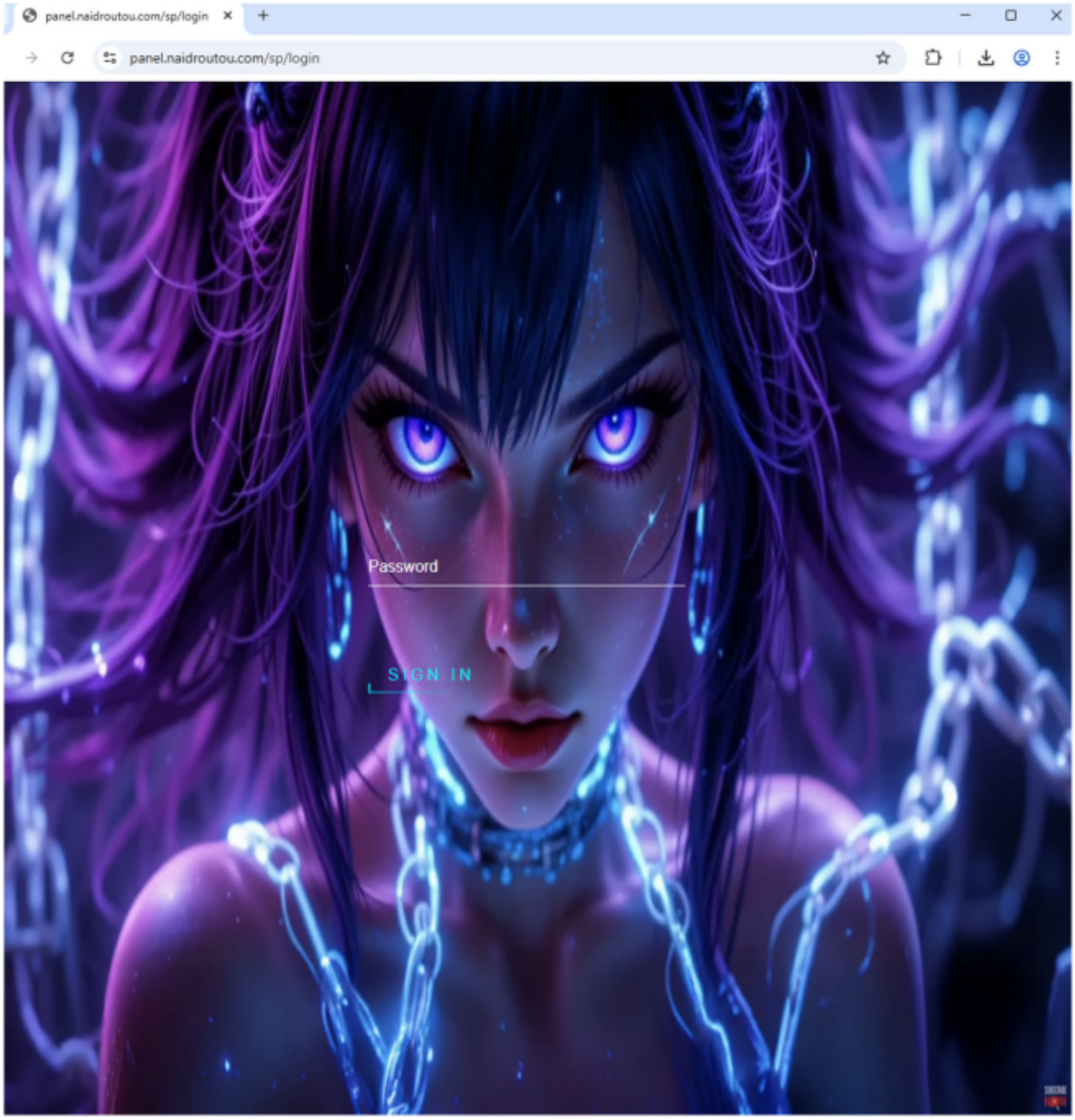

Figure 7: Tycoon 2FA panel login screen, February 2026.

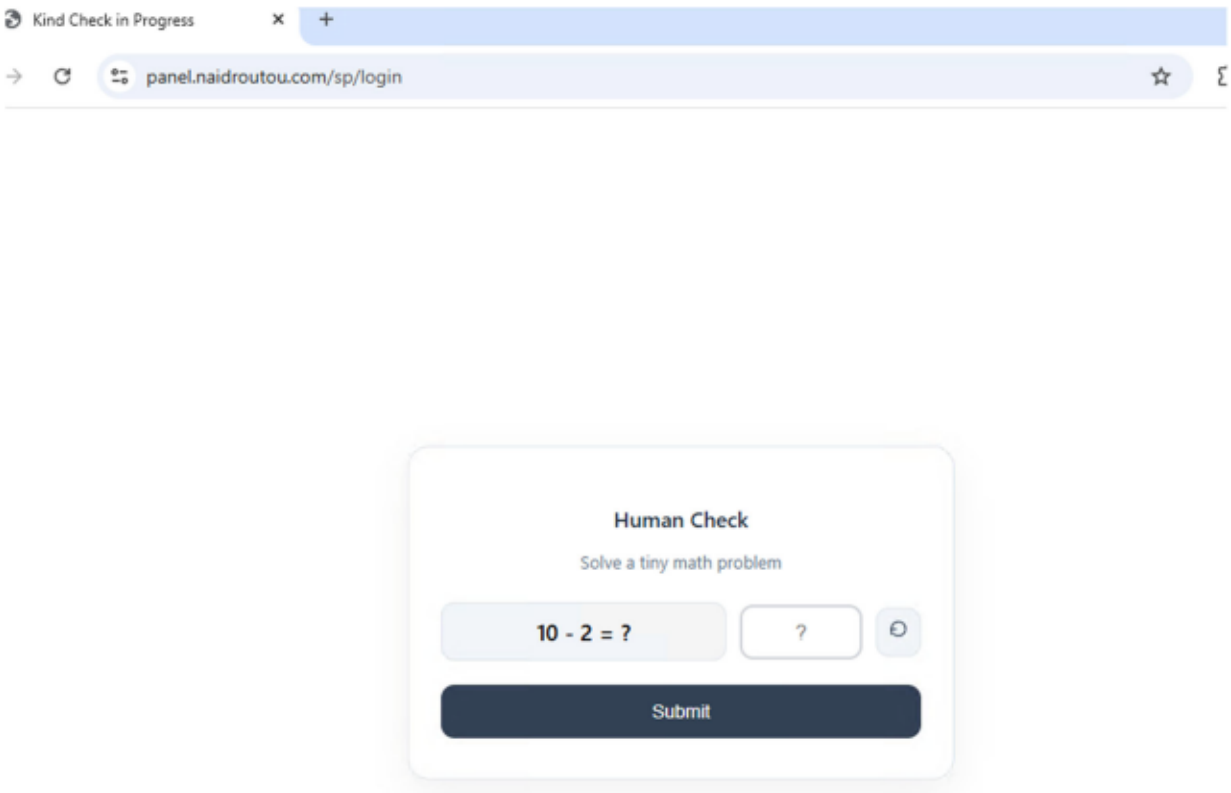

Figure 7: February 2026 Tycoon 2FA panel CAPTCHA.

18. Attribution to Tycoon 2FA phishing can also be made based on artifacts in the code on the CAPTCHA and credential receiver pages. The threat actor regularly changes its CAPTCHA pages, which are the landing pages that require human interaction in order to get to the credential receiver page. However, some artifacts remain unique and consistent enough to be able to identify as Tycoon 2FA. In this current example from a recent campaign (February 2026), the JavaScript observed in the CAPTCHA, contains a unique and consistent form ID structure and although the actor was trying to obfuscate the POST traffic, the form ID pattern and subsequent script are unique to only the Tycoon 2FA phishing kit. As shown in **Figure 9**, this code renders what the victim sees when they click on a Tycoon 2FA-controlled domain. Although Tycoon 2FA frequently updates this code, there are certain attributes and patterns that remain consistent, and that allows me to confirm that even when the code is updated, the activity

is still attributable to Tycoon 2FA. Additionally this code allows me to see how Tycoon 2FA attempts to obfuscate their cybercriminal activity; another signature of Tycoon 2FA is that they use the same scripts across campaigns to obfuscate their tracks.

Figure 9: CAPTCHA JavaScript.

19. The current campaigns also have trackable artifacts in the API logs, or the records of communications between the Tycoon 2FA application and Tycoon 2FA servers. *See* **Figure 10**. The "var" and "fetch" will contain the same patterns of data in every Tycoon 2FA API call (the way that the server communicates with the webpage).

Figure 10: Tycoon 2FA API call JavaScript.

20. Researchers can further identify and attribute Tycoon 2FA domains based off infrastructure identified in a single campaign. Looking at a domain used by a Tycoon 2FA

customer, investigating registrant details including hostname and nameserver, and pivoting on those characteristics, can provide additional domains used by the Tycoon 2FA threat actors. As part of my investigation and in collaboration with Microsoft, I provided a list of domains that Proofpoint assessed with high confidence are related to Tycoon 2FA infrastructure. Microsoft, in connection with their *Ex Parte* Application for Temporary Restraining Order is seeking seizure of these domains.

Impact of Tycoon 2FA Phishing Activity

21. The majority of tracked Tycoon 2FA campaigns impact North America, mainly the U.S. and Canada, with additional activities targeting many European countries including Germany, Spain, France, and the UK.

22. Tycoon 2FA campaigns are opportunistically targeted but regularly include targets that align with Critical Infrastructure Sectors as designated by the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Based on Proofpoint's visibility, the following is an example of industries that were targeted in observed Tycoon 2FA campaigns in our threat data, and the percent of campaigns in which they appeared (a single campaign can include targets in multiple industries):

Industry	**Percent of Tycoon 2FA Campaigns**
Defense	64%
Aerospace	73%
Education	75%
Hospitality	76%
Utilities	76%
Real Estate	77%
Energy	78%
Government	79%
Business Services	82%
Healthcare	83%
Manufacturing	83%
Financial Services	84%
Technology	85%

23. Successful account takeovers can cause significant harm to compromised organizations including financial and reputational damage, loss of proprietary data, and potentially lead to follow-on attacks like ransomware that can have destructive and potentially organizational damaging consequences.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 24th day of February, 2026, in New York, New York.

Selena Larson