TLP:WHITE

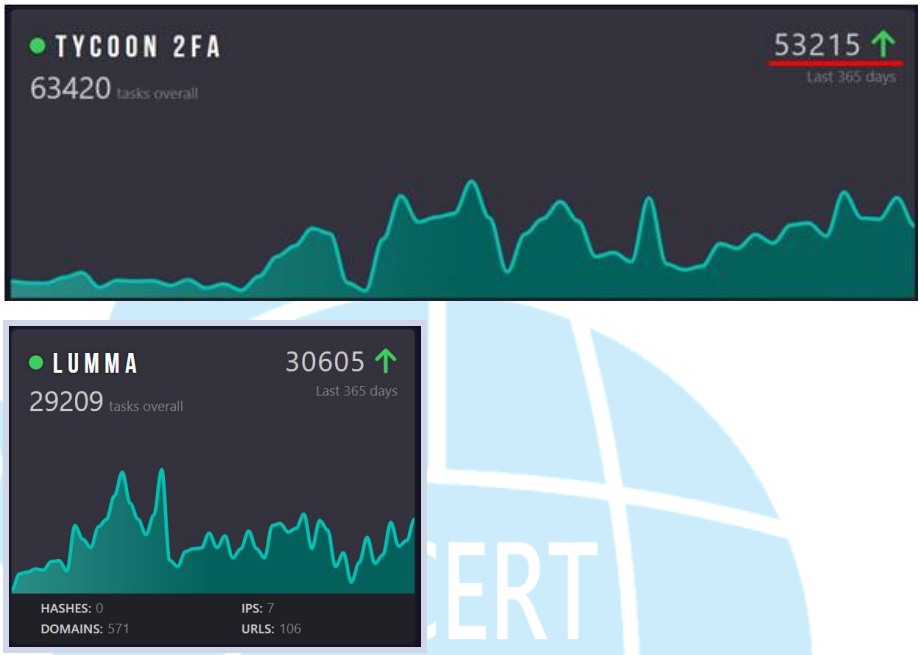
新型態網路釣魚工具包
Tycoon 2FA 分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2025 年 08 月

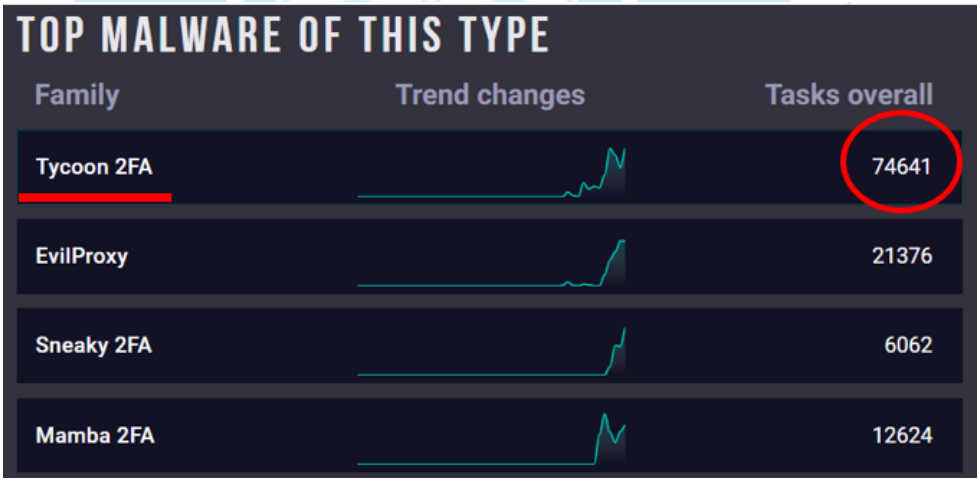
一、事件簡介

1. 2025/8 從 ANYRUN 沙箱檢測平台上的上傳樣本統計資料發現，在過去一年 TYCOON 2FA 被上傳檢測的樣本數為第一名，而且其數量為第二名 LUMMA 之兩倍。



圖片來源:AnyRun 沙箱檢測平台

2. 在網路釣魚工具包(Phishing kit)類別中，該程式排名第一。

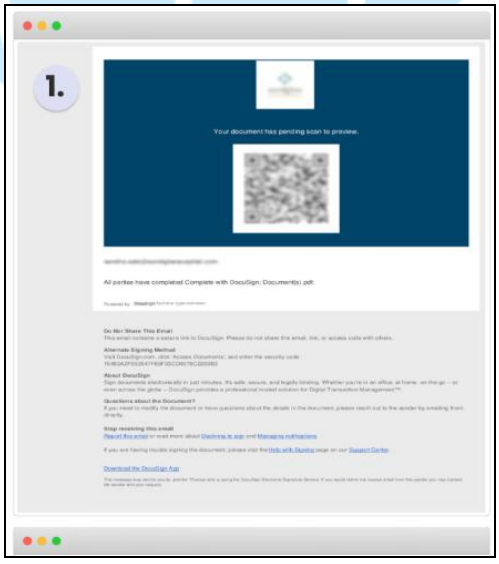


圖片來源:AnyRun 沙箱檢測平台

3. 為了解該惡意程式 TYCOON 2FA 之行為特徵，故進行分析。

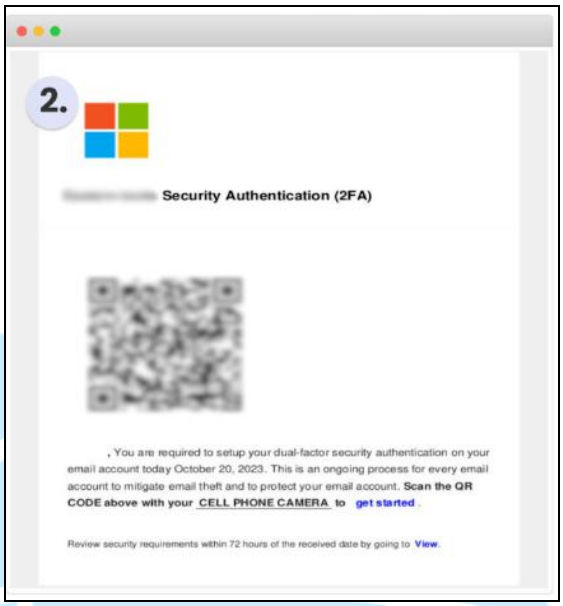
二、 Tycoon 2FA

1. Tycoon 2FA 是一個網路釣魚即服務 (PhaaS) 平台，於 2023 年被發現，並在 2025 年出現重大更新。它主要在繞過多因素身份驗證 (MFA) 的保護，特別是針對 Microsoft 365 和 Gmail 帳戶。
2. 資安業者 Sekoia 揭露 Tycoon 2FA 的開發者以租用的型式提供買家使用，專門用於竊取微軟 365 及 Google 的帳密資料。駭客迄今濫用超過 1,200 個網域名稱，現在它是受到廣泛利用的中間人攻擊網路釣魚工具包之一。
3. Tycoon 2FA 可以攔截使用者憑證和會話 Cookie，從而繞過 MFA，即使採取了額外的安全措施，也能實現未經授權的帳戶存取，而使用雲端服務的組織面臨的風險將最大。
4. Tycoon 2FA 透過社交工程進行多階段攻擊，包括網路釣魚電子郵件和二維碼，進而重新導向到虛假登錄頁面。
5. Tycoon 2FA 在 2023 年 10 月散播的方式是透過電子郵件附件將使用者重新導向至 Tycoon 2FA 釣魚頁面，例如下列各範例。
   (1) PDF 檔案內容冒充針對一家投資公司的 DocuSign 文件檔，將使用者重新導向至 Tycoon 2FA 釣魚頁面。



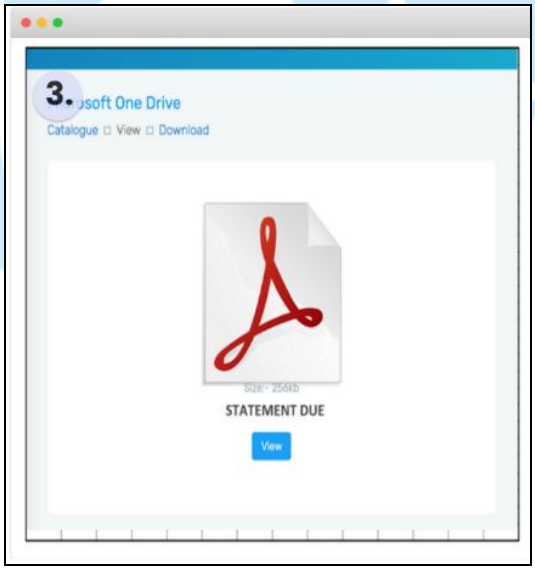
圖片來源:sekoia 之 blog

(2) PDF 檔案內容冒充針對某工業公司的 Microsoft 安全警報，將使用者重新導向至 Tycoon 2FA 釣魚頁面。



圖片來源:sekoia 之 blog

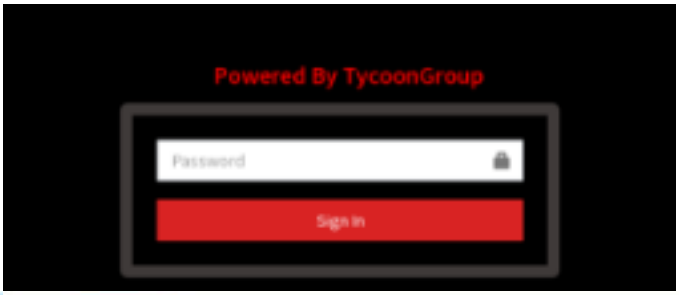
(3) XLSX 檔案偽裝成 PDF 檔案，將使用者重新導向到 Tycoon 2FA 釣魚頁面。

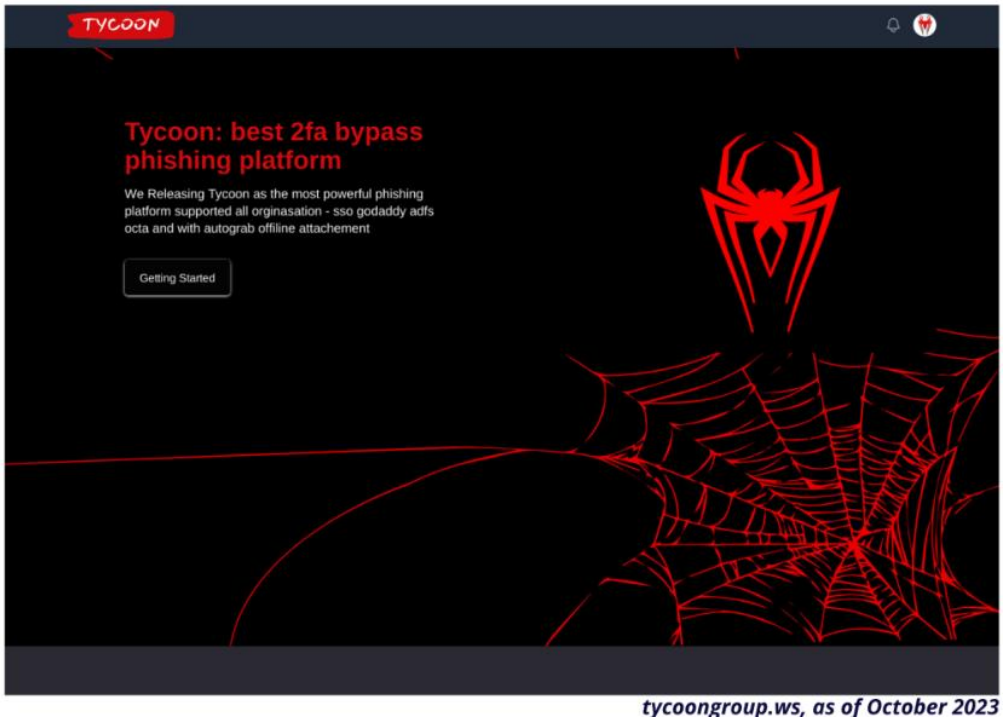


圖片來源:sekoia 之 blog

6. 不斷增長的數百個網路釣魚頁面基礎設施與 Tycoon 2FA 網路釣魚平台聯繫起來。

(1) 2023 年 10 月「codecrafters[.]su」和「devcraftingsolutions[.]com」這兩個網域上都發現相同的登入面板「Powered by TycoonGroup」，這證實網域名稱「tycoongroup[.]ws」屬於該基礎設施。當時，該網域委託管理一個網站，將 Tycoon 宣傳為「最佳 2FA 繞過釣魚平台」。下列圖片為截至 2023 年 10 月 Tycoon 2FA 管理面板和 Tycoon 2FA 網站 (tycoongroup[.]ws) 的登入頁面。



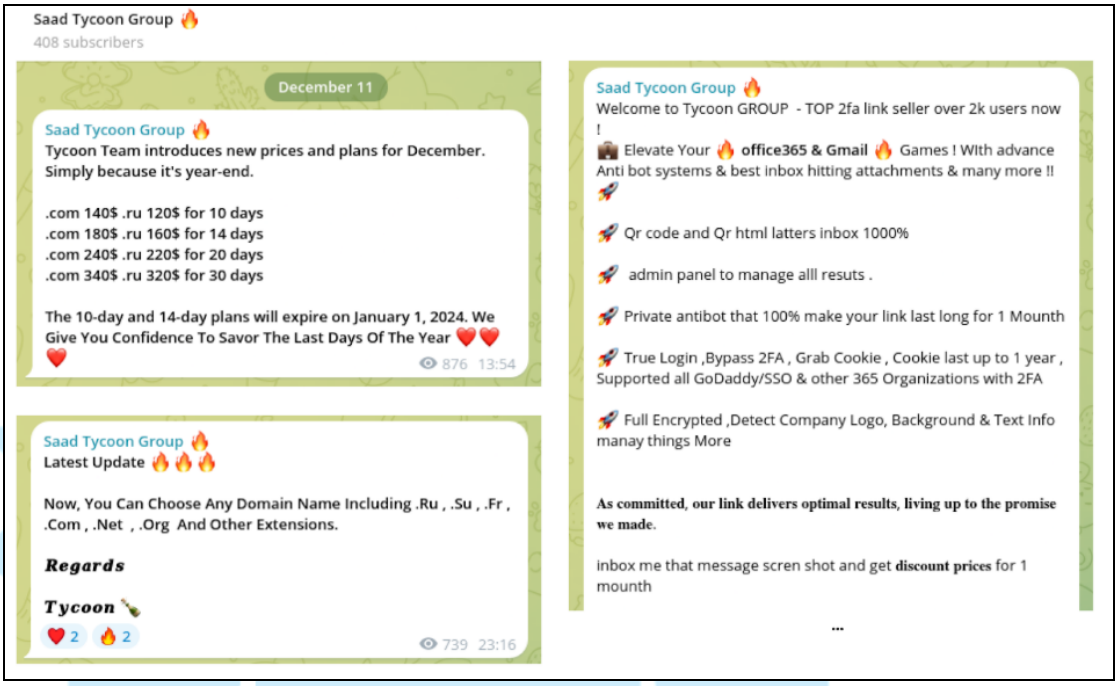


圖片來源:sekoia 之 blog

(2) 在 2023 年 10 月下旬至 2024 年 2 月下旬期間檢測到了超過 1,100 個網域。

7. Tycoon 2FA 開發者自 2023 年 10 月起使用 Telegram 宣傳其 PhaaS，而且使用 Tycoon Group、SaaadFridi 和 Mr_XaaD 等帳號，定期在 Telegram 頻道「hxxps://t.me/tycoon_2fa_Link」上發布 Tycoon 2FA 最新

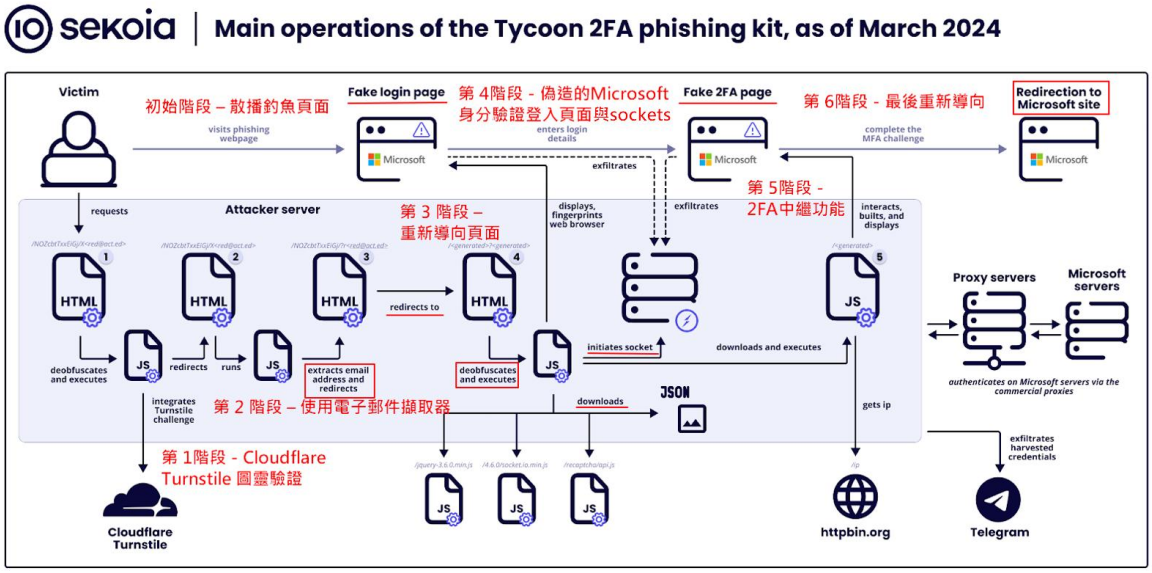
更新的變更日誌。該開發者出售即用型 Microsoft 365 和 Gmail 釣魚頁面以及附件模板，10 天起價 120 美元，價格因網域擴展名（.ru、.su、.fr、.com、.net、.org 等）而異。下列圖片為在 Tycoon 2FA Telegram 頻道「Saad Tycoon Group」上發布文章，宣傳 Tycoon 2FA PhaaS。



圖片來源:sekoia 之 blog

三、 Tycoon 2FA 的運作原理

Tycoon 2FA 這個網路釣魚工具包依賴中間人攻擊(AiTM)技術，涉及託管網路釣魚網頁的攻擊者伺服器（也稱為反向代理伺服器），攔截受害者的輸入並將其轉發到合法服務，以及提示多因素身份驗證(MFA)請求。一旦使用者完成 MFA 質詢，並且身份驗證成功，中間伺服器就會捕獲會話 Cookie。即使在此期間憑證已更改，竊取的 Cookie 允許攻擊者重播會話，從而繞過 MFA。以下是針對 Tycoon 2FA 網路釣魚工具包的主要操作說明。



圖片來源:sekoia 之 blog

初始階段 – 散播釣魚頁面

Tycoon 2FA 服務為其客戶提供網路釣魚附件（HTML 頁面）模板，主要在提供可立即使用的誘餌文檔。Tycoon 2FA PhaaS 的客戶主要使用嵌入在電子郵件附件或電子郵件正文中的 URL 和 QR Code 的重新導向，來散播其釣魚頁面。藉由內含 URL 或 QR Code 的釣魚郵件引誘收信人上當。

第 1 階段－Cloudflare Turnstile 圖靈驗證

當使用者點擊釣魚 URL 時，它會被重新導向到嵌入 Cloudflare Turnstile 圖靈驗證的頁面，以防止不必要的流量，並且透過圖靈驗證系統 Cloudflare Turnstile 排除機器人。

以下是一些 URL 範例:

- "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/*" (如果 URL 未指定電子郵件信箱);
- "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/X<red@act.ed>*";
- "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/X<base64(red@act.ed)>*";

該 URL 頁面的 HTML 程式碼包含下列內容:

1. 實作無限載入的 CSS 程式碼的樣式屬性。
2. 請求 C2 伺服器，並接收「0」或「1」的腳本屬性。
   (1) 如果請求傳回「0」，則腳本進行反混淆並寫入第二個 HTML 程式碼，即嵌入 Cloudflare Turnstile 圖靈驗證的頁面。
   (2) 如果請求返回「1」，則腳本進入下一步，即偽造的微軟釣魚頁面，提示輸入電子郵件信箱。
3. base64 和 XOR 混淆的 HTML 程式碼匯入 Cloudflare Turnstile 圖靈驗證，並顯示自訂文字「此頁面正在執行瀏覽器檢查，以確保您的安全」。該程式碼包含一個腳本，用於執行以下操作：
   (1) 執行 Cloudflare Turnstile 圖靈驗證。
   (2) 將資訊外洩到可能專用於 Tycoon 2FA 客戶的網路釣魚網域。POST 要求發送以下資料:「pagelink」、「bltdip」（使用者的 IP 位址）、「bltdref」（釣魚頁面的 URL）、「bltdua」（User-Agent）和「bltddata」。C2 伺服器會回應「成功」或「錯誤」。
   (3) 當從 C2 伺服器收到「成功」時重新載入頁面。
   (4) 當收到「錯誤」時重新導向到另一個頁面。

第 2 階段－使用電子郵件擷取器

使用者無法發現此階段的執行，因為它在背景執行 JavaScript 程式碼，然後根據電子郵件地址的存在將使用者重新導向到另一個頁面。過程中駭客收集受害者的電子郵件信箱、密碼，並透過 WebSocket 外流。

在這個階段，由於頁面重新下載，URL 與前一個 URL 相同。因此，它可能是：

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

此頁面的 HTML 程式碼包含一個 JavaScript 程式碼，該程式碼使用正規表示式從 URL（如果包含）中提取電子郵件地址。它涵蓋使用 base64 編碼的電子郵件地址和明文編碼的電子郵件地址。然後，它會重新導向到相同的 URL，但分隔符號「？」後面的字元不同，取決於電子郵件地址的存在和格式。

下一階段 URL 的範例如下，分隔符號「？」和電子郵件信箱之間的字元據稱是由 C2 伺服器隨機產生的。

- "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/?r*" (如果沒有電子郵件信箱提取);
- "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/?r<red@act.ed>*" (如果電子郵件信箱被提取);
- "*hxxps://i9152.cisele0[.]com/NOZcbtTxxEiGj/?rr<red@act.ed>*" (如果提取了 base64 編碼的電子郵件信箱).

第 3 階段 – 重新導向頁面

此階段對使用者是不可見的，因為它會將收信人導向冒牌微軟登入網頁及偽造的雙因素驗證流程。

HTML 程式碼僅包含文字「重新導向到」和下一階段的 URL，包括 HTML 標題和正文。

下一階段 URL 的範例如下：

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

LJGWUCZHXZKPGZOQRAVFAAF?3177278383332033065569 02opEXJOOmXGJPZNFTJIXPAAFUILTKKRQQEFFSNIABRZNUPXEUOAKDATDS”

第 4 階段－偽造的 Microsoft 身分驗證登入頁面與 sockets

此處的 HTML 程式碼是一個腳本屬性，嵌入了反混淆函數和混淆後的 HTML 程式碼，也就是偽造的微軟身分驗證頁面及其抓取功能。

反混淆函數以混淆 payload 和 XOR 金鑰作為參數，對 base64 編碼的 payload 進行解碼，並對其進行 XOR 運算。解碼後的 HTML 嵌入了偽造的 Microsoft 驗證頁面的原始程式碼，該頁面下載的資源包括：

(a.) JavaScript 檔案。

- “*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*”

(b.) 釣魚頁面的背景圖片和圖示。

(c.) 如果身份驗證過程成功，則為重新導向 URL。

它還包含超過 260 行 JavaScript 程式碼，旨在:

(a.) 使用用戶代理程式對使用者的網頁瀏覽器進行指紋辨識。

(b.) 使用下載的 library「socket.io.min.js」與 C2 伺服器（與釣魚頁面相同的網域）發起 WebSocket。

(c.) 實現 socket 通訊。

(d.) 捕獲並竊取使用者輸入。

(e.) 檢索最終重新導向 URL。

在 JavaScript 程式碼的末尾，它會下載並執行一個額外的高度混淆的 JavaScript，該 JavaScript 實現了雙重認證 (2FA) 的圖靈驗證。

JavaScript 程式碼 URL 的範例如下:

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

第 5 階段－ 2FA 中繼功能

JavaScript 程式碼與上一階段的 HTML 互動以建立和顯示 Microsoft 2FA 頁面。程式碼使用大量具有十六進位模式的變數重新命名（例如: "_0x40e211"、"_0x2db5"、"_0x5e1add"）、字串操作（例如:拆分、提取、併列）、函數覆蓋和其他程式碼轉換進行混淆。

如果使用電子郵件地址和密碼進行身份驗證的第一步成功，則 JavaScript 程式碼負責處理使用者互動和釣魚頁面的表單驗證。它還會使用實施了 2FA 方法的偽造 Microsoft 頁面來更新 HTML 頁面。為此，它會根據使用者輸入和 Microsoft 伺服器的回應執行許多條件語句。 WebSocket 也會接收釣魚頁面上顯示的一些元素，包括最終的重新導向頁面，或當 Microsoft API 拒絕 2FA 驗證時顯示的錯誤訊息。

根據使用者 Web 瀏覽器收到的 JavaScript 程式碼，Tycoon 2FA 實作了以下雙重認證方法: Microsoft Authenticator（推播通知）、一次性密碼 (OTP) 代碼(由應用程式或簡訊傳送)、電話驗證。Tycoon 2FA 網路釣魚頁面使用商業代理伺服器將使用者輸入（包括電子郵件地址、密碼和 2FA 代碼）轉送到合法的 Microsoft 驗證 API。對 Microsoft API 流量的回應會向使用者傳回適當的頁面和資訊。由於 C2 伺服器處於身份驗證過程的中間位置，它會捕獲所有相關資料，尤其是會話 cookie，從而使網路犯罪分子能夠重播會話，從而繞過 MFA。

此 2FA 中繼功能是 AiTM 網路釣魚工具包的核心功能，主要在受害者和合法服務之間的合法會話身份驗證期間攔截登入詳細資訊。從受害者的 Web 瀏覽器的角度來看，Tycoon 2FA 中繼功能包含一段 JavaScript 程式碼，該程式碼實現了 Microsoft 365 身份驗證成功或失敗的所有變化。

第 6 階段－最後重新導向

Tycoon 2FA 網路釣魚工具包的最後階段涉及將使用者重新導向到駭客指定的 URL。階段 4 的 JavaScript 程式碼在變數「urlo」中嵌入端點 URL，旨在傳回最終的重新導向 URL。當認證成功後，釣魚頁面會向該端點發送 POST 請求，其中包含在 WebSocket 通訊期間設定的會話識別碼（參數「pagelink」）和其他資訊。然後，C2 伺服器使用重新導向 URL 進行回應。

Tycoon 2FA PhaaS 的大多數客戶使用預設重新導向 URL，即「hxxps://login.microsoftonline[.]com/common/SAS/ProcessAuth」。隨後，觀察到一個攻擊者使用了不存在的 WeTransfer URL「hxxps://wetransfer[.]com/invoicedocument」。這種使用可能與網路釣魚電子郵件有關，該電子郵件假裝使用者必須在 Microsoft 365 上進行身份驗證才能存取文件。一旦透過 Tycoon 2FA 網路釣魚頁面進行身份驗證，用戶就會被重新導向到這個合法的「未找到」網頁，這可能會導致他們不會懷疑上一個頁面是惡意的。預設重新導向 URL 也是如此，它會將使用者重新導向到合法 Microsoft 網站的錯誤頁面。

最後，釣魚頁面再次使用 HTTP POST 請求將一些受害者詳細資訊洩

露給 C2 伺服器。傳送的資料包括會話識別碼（參數「pagelink」）、從「httpbin[.]org」 API 取得的 IP 位址、User-Agent 以及其他資訊。

透過 WebSocket 進行滲透

在整個 Tycoon 2FA 網路釣魚工具包的運作過程中，WebSocket 扮演著重要角色。從偽造的 Microsoft 頁面呈現到使用者關閉釣魚頁面，C2 伺服器使用 WebSocket 收集收集到的資料和操作狀態。它還會向使用者 Web 瀏覽器傳遞一些元素，以建立後續的釣魚頁面。

啟動 WebSocket 連線的 URL 範例如下：

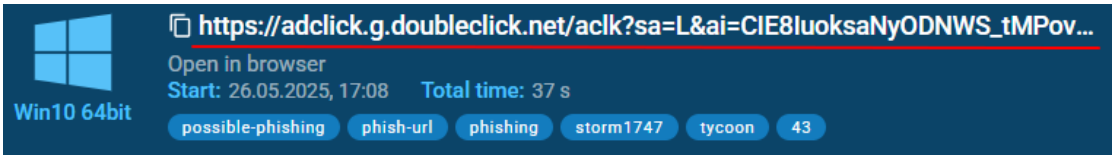
- "h*xxps://i9152.cisele0[.]com/web6socket/socket.io/?type=User&appnum=1&EIO=4&transport=websocket*"

以下是使用 Microsoft Authenticator 作為 2FA（Client 端是使用者 Web 瀏覽器）成功進行身份驗證的 Tycoon 2FA WebSocket 連線的主要步驟圖示。在最新版本的 Tycoon 2FA 網路釣魚工具包中，WebSocket 連線竊取的憑證保持不變。

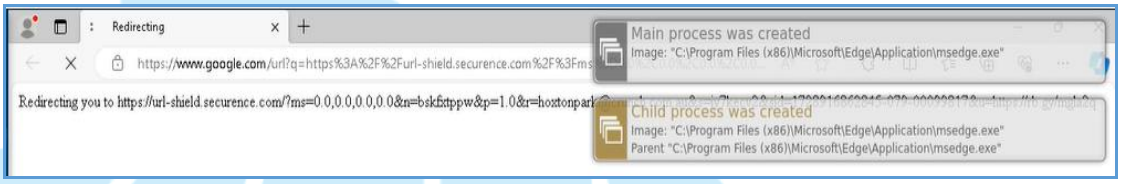


四、 Tycoon 2FA 樣本的檢測

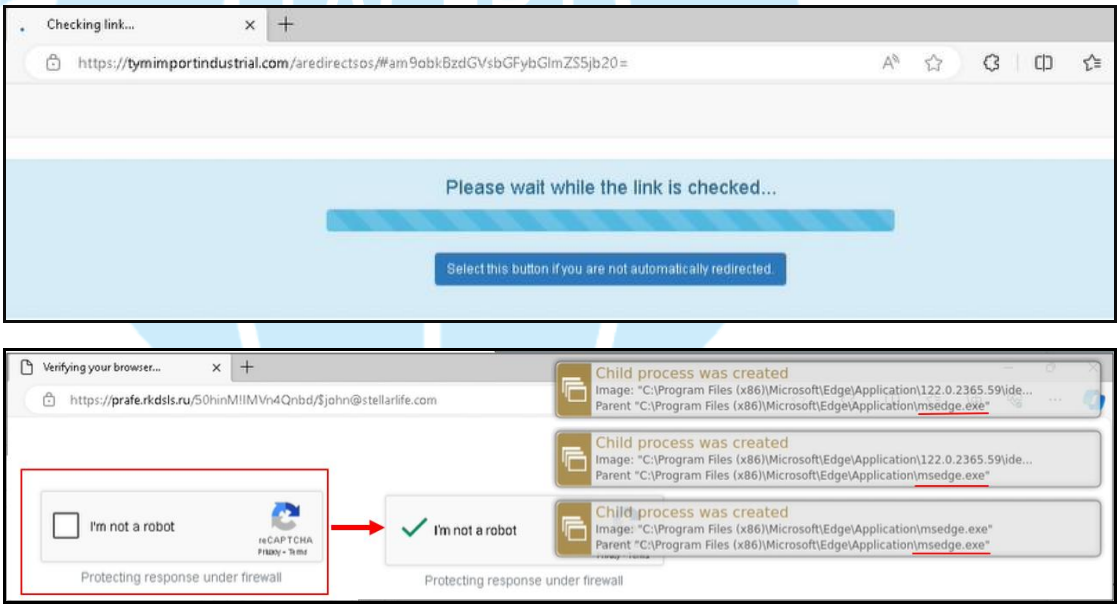
1. 在 AnyRun 沙箱檢測一個 Tycoon 2FA 樣本，觀察其特徵行為。攻擊行為從對下圖中的 URL 的請求開始。



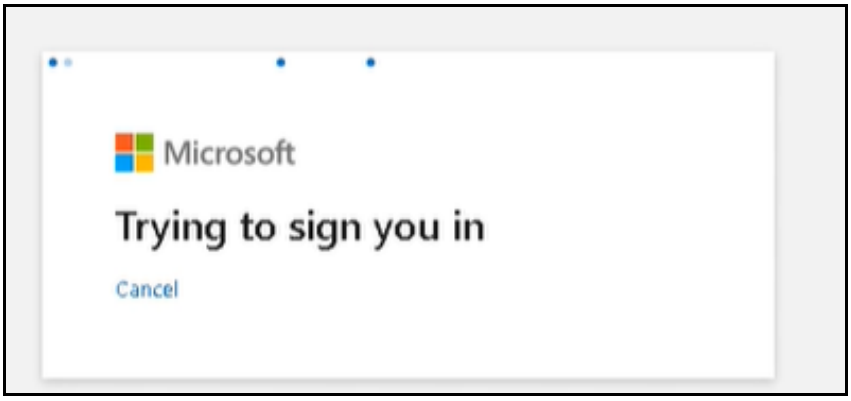
2. 在點選惡意網址後，發現被重新導向某個網址，並且在背景產生兩個程序來執行 msedge.exe。

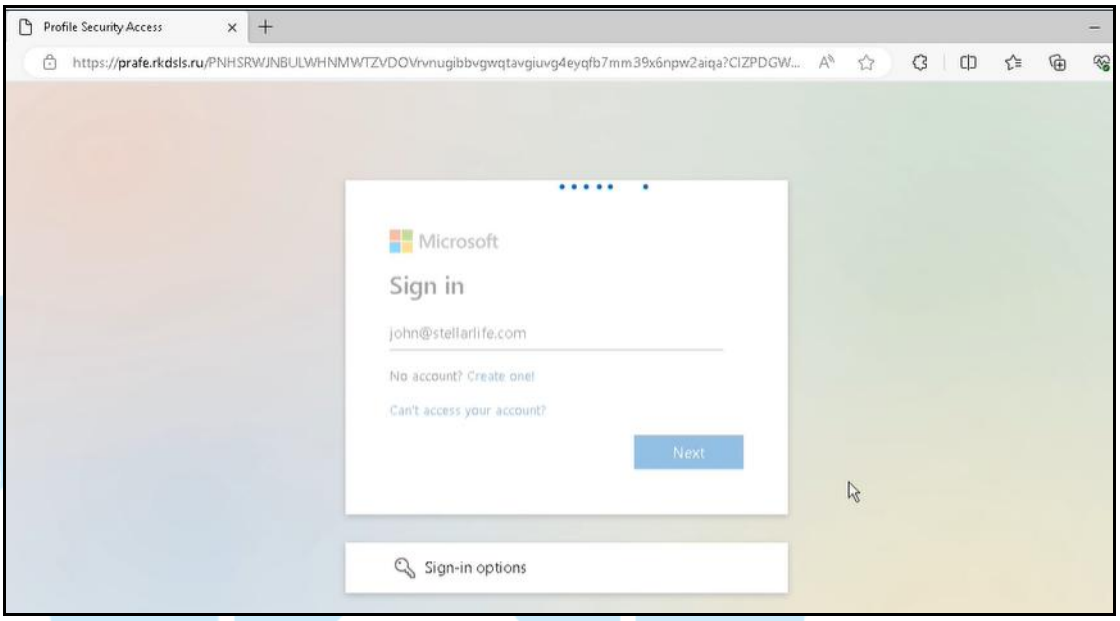


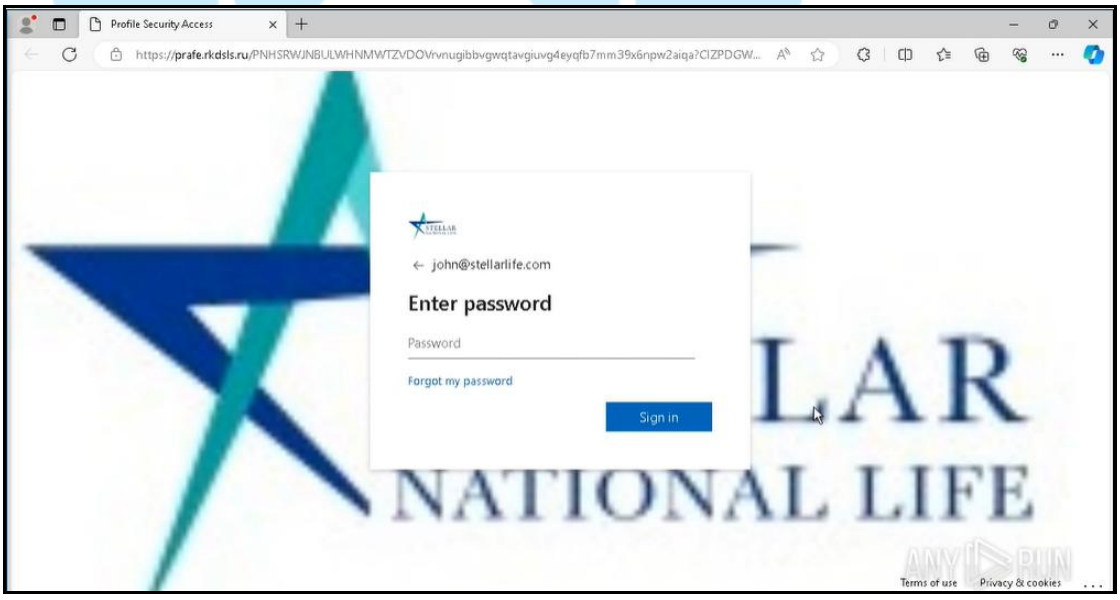
3. 接著出現檢查連結的視窗，最後導向「我不是機器人」的驗證頁面。勾選「我不是機器人」後會在背景中執行三個 msedge.exe 程序。



4. 最後可看到嘗試登入 john@stellarlife.com 電子郵件信箱的頁面在執行中，其中有經過微軟驗證程序，但是最後沒有登入成功，出現重新登入 stellarlife 公司的電子郵件信箱 john@stellarlife.com 的畫面。







5. Tycoon 2FA IoCs

下面的 IoC 清單可在 Sekoia.io GitHub 儲存庫中找到。從清單中可以

發現這些網址的結尾都使用特定頂級網域名稱 (TLD)，例如:ru 或 com。

0q5e0.nemen9[.]com	fisaca.trodeckh[.]com	tnyr.moporins[.]com
25rw2.canweal[.]com	galume.aricente[.]com	wasogo.shantowd[.]com
35fu2.ouchar[.]ru	gz238.uatimin[.]com	x12y.restrice[.]ru
4343w.jgu0[.]com	horizon.sologerg[.]com	xrs.chenebystie[.]com
43rw98nop8.m1p8z[.]com	jp1y36.it2ua[.]com	xva.tjlpkcia[.]com
4m2swl.7e2r[.]com	k348d.venti71[.]com	zaqaxu.dthiterp[.]ru
5me78.methw[.]ru	kjlvo.ningeona[.]com	zekal6.tnjxb[.]com
6j312.rchan0[.]com	kjsdflwe.nitertym[.]ru	zemj4f.ymarir[.]ru
77p3e.rimesh3[.]com	l846d.ferver8[.]com	
8000n.uqin[.]ru	libudi.oreversa[.]com	
8uecv.gnornamb[.]com	n29k4.ilert[.]ru	
98q5e.ructin[.]com	n9zph.lw8opi[.]com	
9c43r.theq0[.]com	o6t94g.3tdx2r[.]com	
9oc0y2isa27.demur3[.]com	oo99v.coqqwx[.]ru	
beacon.diremsto[.]com	p1v12.17nor[.]com	
bloggcenter[.]com	pmd8ot6xhw.3qjpc[.]com	
buneji.fiernmar[.]com	q908q.refec7[.]com	
e85t8.nechsha[.]com	r298y.sem01[.]com	
ex1uo.rhknt[.]ru	rlpq.tk9u[.]com	
explore.atlester[.]ru	roriku.orankfix[.]com	
fiq75d.rexj[.]ru	tlger-surveillance[.]com	

五、 總結與建議

1. Tycoon 2FA 採用中間人攻擊 (AiTM) 方法，攻擊者透過反向代理伺服器設定釣魚頁面。使用者輸入憑證並完成 2FA 流程後，伺服器會擷取會話 Cookie，從而使攻擊者能夠重複使用會話並繞過安全措施。

2. 目前 Tycoon 2FA 非常流行，並被包括 Saad Tycoon 團體在內的網路犯罪者廣泛使用。該平台提供現成的釣魚頁面和易於使用的管理面板，即使是技術水平較低的攻擊者也能輕鬆上手。

3. 檢測 Tycoon 2FA 的建議

鑑於 Tycoon 2FA 釣魚頁面原始碼不斷變化，因此，行為分析對於可靠檢測至關重要。為了檢測 Tycoon 2FA，可以觀察是否有以下行為，若有那麼該行為很有可能涉及 Tycoon 2FA 網路釣魚。

(1) C2 Domain Triangle:是否有與來自特定頂級網域名稱 (TLD) 網域

池中的一組網域進行連線，包括 .ru、.es、.su、.com、.net 和 .org。

(2) 資源載入：檢索是否應用特定的 JavaScript 函式庫、CSS 樣式表或 Web 內容。例如: https://code.jquery.com/jquery-3.6.0.min.js 。

(3) 會話重新導向：會話結束時重新導向到 Microsoft 官方身份驗證頁面。

4. 在預防 Tycoon 2FA 網路釣魚工具包的攻擊方面，有下列防護建議提供參考。

(1) 採用抗網路釣魚的多重驗證方式（Phishing-Resistant MFA）

Tycoon 2FA 常透過竊取 session cookie 來繞過傳統 MFA（如 SMS 或 TOTP 應用），因此應該使用硬體安全金鑰（如 FIDO2 / WebAuthn U2F），它們與網域綁定，不易被中間人攻擊所欺騙。避免使用 SMS 或一般 OTP 應用程式（如 Google Authenticator），因為這些方式容易被惡意頁面中轉或竊取。

(2) 強化電子郵件過濾與網域封鎖機制

Tycoon 2FA 常使用合法或被入侵的郵件帳號（如 Amazon SES）發送釣魚郵件。防護建議如下:

(a)啟用 SPF(寄件人授權驗證機制)、DKIM(郵件簽章驗證機制)、DMARC(綜合驗證與報告機制)等認證機制，以降低假冒郵件成功送達率。

(b)部署進階網域過濾：利用 DNSFilter 建議，封鎖其 65 個已知 root domains，並監控子網域模式（如短暫 FQDN、.es 等新域名）。

(3) 建立行為式偵測與威脅情報系統

Tycoon 2FA 的偽裝能力強，傳統簽名防禦可能不足。防護建議如下：

(a)採用具行為偵測（behavioral analysis）的安全系統，比如監控異常 CAPTCHA 模式、資源載入方式、重新導向行為等。

(b) 整合 IoC（Indicators of Compromise） 與動態阻擋策略，堵截根域與子域惡意流量。

(4) 教育使用者與進行模擬演練

因 Tycoon 2FA 擅長偽裝 Microsoft/Gmail 登入頁面與 QR-phishing（quishing）投餌，使用者需具備識別能力。

(a) 定期進行模擬釣魚演練，提升識別釣魚 QR code 和畸形 URL 的能力。

(b) 培訓單位人員確認網址是否為單位官方域名，避免透過郵件或 QR code 快速登入。

(5) 強化終端偵測與沙箱分析

Tycoon 2FA 力圖阻止分析工具與沙箱，它會偵測 DevTools、Burp Suite、Selenium 等工具並導向空白頁，甚至覆寫剪貼簿內容。因此，應使用 整合 EDR/XDR 平台，並建立可疑活動的行為指紋庫，如異常 clipboard 操作、不可點擊右鍵、重新導向行為等。

彙整前述建議為下列「防禦建議總覽表」。

防禦方向	建議措施
MFA 強化	使用 FIDO2/WebAuthn 硬體金鑰。
郵件過濾	啟用 SPF/DKIM/DMARC 認證機制，封鎖已知 Tycoon 根域(root domain)。
行為偵測	部署行為分析系統，監控異常 CAPTCHA/重新導向行為。
使用者教育	進行模擬釣魚演練，教導辨識假登入頁。
終端防護	使用 EDR/XDR，檢測剪貼簿/右鍵/DevTools 干擾行為。
威脅情報整合	導入 IoC、動態封鎖 Tycoon 的 domain patterns。

5. 在防護上建議除了關注 Microsoft Outlook 身份驗證網路釣魚之外，還需觀察到針對 Google 帳戶身份驗證的 Tycoon 2FA 變種。對於該類型的偵測和應對需要結合行為監控、進階威脅情報、預防網路釣魚 MFA 與加強使用者對這類攻擊的認知。

參考資料

1. **Tycoon 2FA: an in-depth analysis of the latest version of the AiTM phishing kit**
   https://blog.sekoia.io/tycoon-2fa-an-in-depth-analysis-of-the-latest-version-of-the-aitm-phishing-kit/
2. **AnyRun 沙箱檢測 tycoon**
   https://any.run/malware-trends/tycoon/
3. **Evolution of Tycoon 2FA Defense Evasion Mechanisms: Analysis and Timeline**
   https://any.run/cybersecurity-blog/tycoon2fa-evasion-analysis/