Alerta ID:	102
Fecha del reporte:	19/05/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Tycoon 2fa secuestra cuentas de Microsoft 365 vía device code phishing
Herramienta de detección	N/A
Activo involucrado:	sistemas expuestos a internet
Tipo de alerta:	Boletín informativo
Nivel de riesgo:	Alta

Resumen ejecutivo

Informar a las entidades sobre una campaña activa y en evolución protagonizada por el kit de Phishing-as-a-Service (PhaaS) conocido como Tycoon 2FA.

Dicha campaña ha adoptado una nueva técnica de compromiso basada en el flujo OAuth 2.0 Device Authorization Grant para secuestrar cuentas de Microsoft 365 sin necesidad de capturar credenciales y eludiendo la autenticación multifactor (MFA).

Descripción:

Tycoon 2FA es una plataforma de Phishing-as-a-Service activa desde agosto de 2023, comercializada en Telegram y Signal con precios que comenzaban en $120 USD por 10 días de acceso. En su apogeo (mediados de 2025) fue responsable del 62% de los intentos de phishing bloqueados por Microsoft, con más de 30 millones de correos mensuales y aproximadamente 96.000 víctimas identificadas en más de 500.000 organizaciones globales.

La variante documentada en abril de 2026 por el equipo eSentire Threat Response Unit (TRU) representa una evolución significativa: en lugar de robar credenciales mediante un proxy adversario-en-el-medio (AiTM), los atacantes ahora abusan del flujo de autorización de

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

dispositivos OAuth 2.0 para obtener tokens de acceso y de actualización directamente de Microsoft, sin que la víctima ingrese su contraseña en ningún sitio malicioso.

Modo de explotación detallado.

El ataque combina una cadena de entrega de cuatro capas en el navegador con el abuso del flujo OAuth 2.0 Device Authorization Grant. A continuación se describe cada fase en detalle:

Paso 1 — Correo de señuelo con URL de Trustifi
La víctima recibe un correo con temática de factura de proveedor o aviso de buzón de voz. El enlace embebido es una URL de click-tracking legítima de Trustifi (plataforma real de seguridad de correo), lo que permite evadir los filtros de seguridad basados en reputación de dominio. La apariencia del correo es profesional y convincente.

Paso 2 — Redirección en cadena: Trustifi → Cloudflare Workers (Capas 1 y 2)
Capa 1: El Worker de Cloudflare descifra en el navegador un payload oculto mediante AES-GCM y JavaScript ofuscado. La misma clave AES del kit de 2025 sigue activa, evidenciando que los operadores respaldaron su codebase antes del takedown.

Capa 2: Un script controlador realiza verificaciones anti-análisis exhaustivas: detecta Selenium, Puppeteer, Playwright y Burp Suite; aplica un blocklist hardcodeado de 230 proveedores de seguridad, VPNs, sandboxes y crawlers de IA con anti-debug timing traps. Las solicitudes desde entornos de análisis son redirigidas automáticamente a una página legítima de Microsoft.

Paso 3 — Obtención del Device Code desde el backend del atacante (Capa 3)
Una vez validado el entorno de la víctima, la Capa 3 contacta el backend del atacante alojado en Alibaba Cloud (AS45102). El backend solicita a Microsoft un código de autorización de dispositivo OAuth 2.0 (device_code + user_code), impersonando la aplicación Microsoft Authentication Broker (AppId: 29d9ed98-a469-4536-ade2-f981bc1d605e). Simultáneamente inicia un bucle de polling a login.microsoftonline.com/token esperando la autorización de la víctima.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Paso 4 — Presentación del user_code a la víctima (Capa 4)

La víctima ve una página que simula un portal Microsoft 365 con una notificación de buzón de voz. Se le presenta un user_code corto y se le instruye a copiarlo y pegarlo en microsoft.com/devicelogin, que es la página REAL de Microsoft. Esto genera confianza en la víctima, ya que interactúa directamente con infraestructura genuina.

Paso 5 — Autenticación legítima + MFA en microsoft.com/devicelogin

La víctima ingresa el código en la página real de Microsoft, introduce sus credenciales y completa su MFA normalmente. Microsoft autentica exitosamente al usuario. Lo que la víctima no percibe es que está autorizando acceso al dispositivo controlado por el atacante, no al suyo propio.

Paso 6 — Emisión de tokens OAuth al dispositivo del atacante

Microsoft emite un access token y un refresh token al cliente del atacante (el polling iniciado en el Paso 3). Con el refresh token, el atacante puede obtener nuevos access tokens indefinidamente sin requerir interacción adicional del usuario. Los tokens son válidos para Exchange Online, Microsoft Graph y OneDrive for Business, comprometiendo la totalidad del entorno M365.

Indicadores de compromiso

Los siguientes indicadores fueron publicados por eSentire TRU para la campaña de abril de 2026. El repositorio completo actualizado se mantiene en:

https://github.com/eSentire/iocs/tree/main/Tycoon2FA

TIPO DE IOC	INDICADOR / VALOR	DESCRIPCIÓN
User-Agent (device-code)	node, undici	Agentes Node.js usados en polling del atacante; visibles en Entra sign-in logs
User-Agent (variante anterior)	axios/1.x	Variante credential-relay; útil para detección de campañas previas
ASN / Hosting	AS45102 — Alibaba Cloud	Infraestructura de polling del atacante; nuevo proveedor post-takedown marzo 2026

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

TIPO DE IOC	INDICADOR / VALOR	DESCRIPCIÓN
OAuth App ID	29d9ed98-a469-4536-ade2-f981bc1d605e	Microsoft Authentication Broker suplantado para obtener tokens M365
Dominio Check Domain	shivacrio[.]com/bytecore~tx1j8	Patrón de Check Domain URL confirmado en campaña abril 2026
Plataforma abusada	Trustifi click-tracking URLs	URLs de seguimiento legítimas de Trustifi usadas como vector de redirección inicial
Plataforma abusada	Cloudflare Workers	Capas 1 y 2 de la cadena de entrega en el navegador
Cifrado	AES-GCM (misma clave de 2025)	Clave de cifrado AES-GCM preservada intacta del kit original post-takedown
Blocklist	230 ASN/vendors en Layer 2	Lista de bloqueo de proveedores de seguridad, VPNs, sandbox y crawlers de IA
Cebo (lure)	Factura proveedor / aviso buzón de voz	Plantillas de señuelo usadas para engañar a la víctima
Hosting anterior	Global Connectivity Solutions, M247, Hivelocity	Proveedores de infraestructura pre-takedown (marzo 2026)

Vulnerabilidades.

Este ataque no explota una vulnerabilidad de software con CVE asignado, sino que abusa de características de diseño legítimas del ecosistema de autenticación moderno. Las debilidades son de naturaleza lógica y de configuración:

FLAW #1 — Abuso del flujo OAuth 2.0 Device Authorization Grant (RFC 8628)
Descripción: El flujo fue diseñado para dispositivos con capacidades de entrada limitadas (smart TVs, CLI tools). Permite que un usuario autorice a un dispositivo ingresando un código corto en una URL de verificación. El problema: no existe mecanismo que confirme que el dispositivo que inició la solicitud pertenece al usuario que la está autorizando.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Impacto: Un atacante genera un device_code válido, presenta el user_code a la víctima y, una vez que esta lo ingresa en la página legítima de Microsoft, recibe tokens OAuth plenos en su propio dispositivo. La MFA se completa correctamente para la sesión equivocada.

FLAW #2 — Suplantación del Microsoft Authentication Broker
Descripción: Los atacantes impersonan el AppId 29d9ed98-a469-4536-ade2-f981bc1d605e (Microsoft Authentication Broker), aplicación de primera parte de Microsoft que intermedia tokens para Exchange Online, Graph y OneDrive.
Impacto: El consentimiento aparece en logs de Entra ID como actividad normal de una aplicación Microsoft, un único consentimiento otorga acceso a todo el ecosistema M365, dificultando la detección temprana por parte del equipo de seguridad.

FLAW #3 — Abuso de plataformas legítimas para evasión de controles
Descripción: El ataque encadena múltiples servicios confiables: Trustifi (click-tracking), Cloudflare Workers (hosting de capas de redirección) y la propia infraestructura de autenticación de Microsoft. Al usar servicios de alta reputación, los controles basados en listas de bloqueo de dominios fallan.
Impacto: Los controles de seguridad de correo y proxy no identifican el ataque porque cada paso individual utiliza una plataforma de confianza reconocida.

FLAW #4 — Persistencia ilimitada mediante refresh tokens
Descripción: Los refresh tokens OAuth tienen vida útil extendida y no se invalidan automáticamente al cambiar la contraseña del usuario. Una vez obtenido, el atacante puede renovar el access token indefinidamente.
Impacto: El acceso persiste hasta que el administrador revoca explícitamente los tokens desde Microsoft Entra ID, acción que usualmente no se realiza de forma proactiva ante un compromiso no detectado.

Principales activos afectados.

Este ataque no depende de una versión específica de software vulnerable, sino de la configuración del entorno de identidad. Los siguientes servicios y contextos están en riesgo:

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

ACTIVO / COMPONENTE	DESCRIPCIÓN DEL RIESGO
Microsoft 365 (todas las suscripciones)	Business Basic/Standard/Premium; Enterprise E1/E3/E5. Cualquier tenant con Device Code Flow habilitado.
Microsoft Entra ID (Azure AD)	Tenants donde el flujo OAuth Device Authorization Grant no ha sido restringido mediante Conditional Access.
Exchange Online	Accesible mediante tokens obtenidos vía Microsoft Authentication Broker (AppId suplantado).
Microsoft Graph API	Permite lectura de correo, archivos, calendarios, contactos y directorios del usuario comprometido.
OneDrive for Business	Acceso completo a archivos almacenados; vector principal de exfiltración de documentos confidenciales.
SharePoint Online / Microsoft Teams	Accesibles a través de los mismos tokens OAuth emitidos por Microsoft Authentication Broker.
Usuarios sin formación en ciberseguridad	Usuarios que no reconocen el riesgo de ingresar device codes recibidos por correo o páginas no solicitadas.
Orgs. sin Conditional Access configurado	Organizaciones que no han implementado políticas que bloqueen el Device Code Flow o restrinjan clientes públicos OAuth.

Recomendaciones

- Monitorear accesos al endpoint /devicelogin desde fuentes inusuales o no registradas.
- Revisar en Entra logs: Device Code flows exitosos seguidos de accesos desde nuevas IPs geográficas.
- Habilitar Microsoft Sentinel con reglas específicas para Device Code Phishing.
- Configurar Microsoft Defender for Office 365 con políticas de Safe Links para inspeccionar URLs de redirección.
- Bloquear o alertar correos con click-tracking de plataformas externas que redirijan a dominios sospechosos.
- Implementar DMARC, DKIM y SPF en todos los dominios corporativos.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Establecer procedimiento de reporte rápido ante cualquier solicitud de código de dispositivo sospechosa.

Fuentes:

- Tycoon2FA hijacks Microsoft 365 accounts via device-code phishing (Mayo 2026) Https://www.bleepingcomputer.com/news/security/tycoon2fa-hijacks-microsoft-365-accounts-via-device-code-phishing/
- Tycoon 2FA Operators Adopt OAuth Device Code Phishing (Mayo 2026) https://www.esentire.com/blog/tycoon-2fa-operators-adopt-oauth-device-code-phishing
- Repositorio de IoCs Tycoon 2FA — actualizado continuamente https://github.com/eSentire/iocs/tree/main/Tycoon2FA
- Europol-coordinated action disrupts Tycoon2FA phishing platform (Marzo 2026) https://www.bleepingcomputer.com/news/security/europol-coordinated-action-disrupts-tycoon2fa-phishing-platform/
- Tycoon 2FA Operators Adopt OAuth Device Code Phishing to Bypass MFA (Mayo 2026) https://cybersecuritynews.com/tycoon-2fa-operators-adopt-oauth-device-code/
- Tycoon 2FA Phishing Actors Disperse, Adopt Device Code Phishing (Mayo 2026) https://www.okta.com/blog/threat-intelligence/tycoon_2fa_phishing_actors_scatter/
- OAuth Device Code Phishing Campaigns Surge Targeting Microsoft 365 (Dic. 2025) https://www.infosecurity-magazine.com/news/oauth-phishing-campaigns/
- Microsoft leads takedown of Tycoon2FA phishing service infrastructure (Marzo 2026) https://www.csoonline.com/article/4140890/microsoft-leads-takedown-of-tycoon2fa-phishing-service-infrastructure.html
- Enterprise Techniques Matrix — técnicas referenciadas en este boletín https://attack.mitre.org/
- OAuth 2.0 Device Authorization Grant — especificación técnica del flujo abusado https://datatracker.ietf.org/doc/html/rfc8628

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

telefónicas (+57) 3168931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570