Alerta

Técnica

Campaña de Kits de Phishing en Colombia

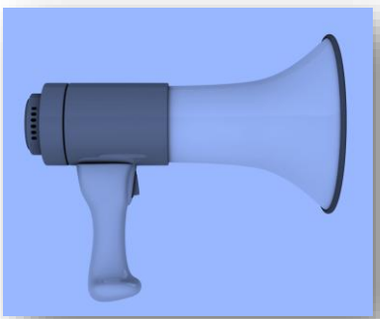
COLCERT AL-20251215 - 088

TLP:CLEAR

Resumen ejecutivo

En Colombia se identificó actividad relacionada con los kits de phishing Tycoon 2FA, EvilProxy y Mamba, empleando infraestructura distribuida para capturar credenciales corporativas mediante técnicas de proxy inverso y suplantación de servicios legítimos.

Durante el análisis realizado se identificaron campañas de suplantación digital dirigida a colaboradores de empresas del país, cuyo objetivo principal es obtener credenciales corporativas de correo electrónico mediante técnicas avanzadas de *phishing*. Los ataques emplearon tres kits ampliamente usados a nivel internacional: **Tycoon 2FA**, **EvilProxy** y **Mamba**, herramientas diseñadas para burlar mecanismos de seguridad como la autenticación multifactor y replicar interfaces legítimas de servicios como Outlook, Gmail o portales protegidos por Cloudflare.



NIVEL DE RIESGO

ALTO

A través de la revisión de los enlaces maliciosos y la infraestructura asociada, se detectó un volumen importante de dominios y subdominios utilizados para redirigir a las víctimas hacia páginas fraudulentas que imitaban con alto nivel de detalle los servicios originales. Estos kits funcionan como proxy inverso, capturando en tiempo real las credenciales ingresadas por el usuario y, en algunos casos, incluso interceptando códigos de autenticación de un solo uso.

El análisis permitió documentar los métodos utilizados, los patrones de comportamiento malicioso, las TTP vinculadas con el marco MITRE ATT&CK y la infraestructura utilizada por los ciberdelincuentes. Esto ofrece a las organizaciones colombianas una base sólida para fortalecer su vigilancia, mejorar sus políticas de autenticación y aumentar la concienciación del personal frente a este tipo de engaños.

Kits De Phishing Identificados

Tycoon 2FA

Es un kit de phishing diseñado para capturar credenciales corporativas y, especialmente, códigos de autenticación multifactor (2FA). Este tipo de herramientas se ha vuelto popular porque permite a los ciberdelincuentes vulnerar inclusive cuentas protegidas con doble verificación. El kit de phishing se encuentra alojado en la página web maliciosa a la que el usuario es redirigido.

¿Cómo opera?

- ❑ Presenta a la víctima una página idéntica a servicios como Outlook o Gmail.
- ❑ Cuando la persona ingresa su usuario y contraseña, el kit captura esa información en segundo plano.
- ❑ Luego solicita el código de verificación (OTP), haciéndolo pasar por un proceso de seguridad legítimo.
- ❑ El ciberdelincuente recibe ambos datos en tiempo real y puede iniciar sesión de inmediato antes de que el código expire.

Elementos técnicos observados:

- Dominios con terminaciones poco comunes (.icu, .biz.id, .ai.in, .in.net), usados para reducir costos y evitar bloqueos. Subdominios que imitan servicios empresariales: opentelemetry, callback, powerbi, expressvpn, keepachangelog.
- Enlaces ocultos mediante abreviadores o redireccionamientos múltiples.
- Interacción en tiempo real con el servidor del atacante, lo que facilita la captura instantánea del OTP.

Imagen 1. Suplantación de un captcha de sitio web de Tycoon 2FA.

Imagen 2. Código QR que redirecciona a sitio web de Tycoon.

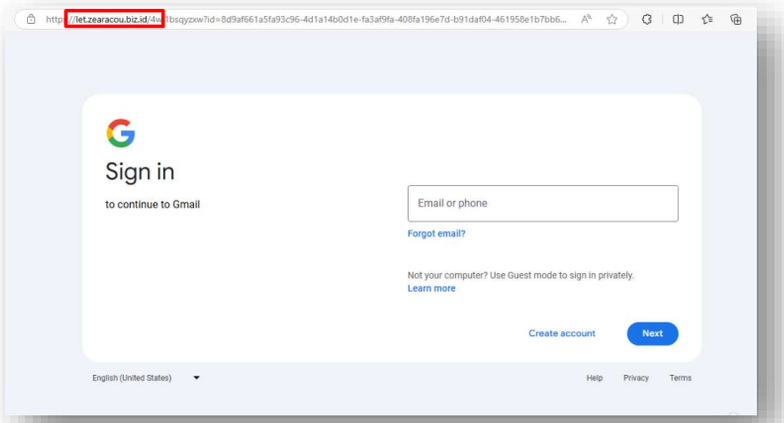


Imagen 3. Sitio web de Tycoon suplantando a Gmail.

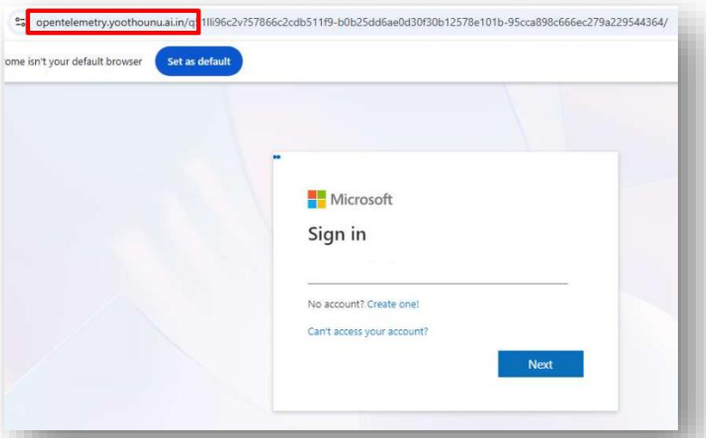


Imagen 4. Sitio web de Tycoon suplantando a Outlook.

EvilProxy

EvilProxy es uno de los kits de *phishing* más avanzados actualmente. Funciona como una plataforma de "*phishing* como servicio" (PhaaS), lo que significa que los ciberdelincuentes no necesitan grandes conocimientos técnicos, solo necesitan pagar por el servicio y reciben campañas listas para usar.

¿Cómo opera?

- Usa un servidor proxy inverso para colocarse entre la víctima y el servicio legítimo.
- La víctima ve la página real de Outlook, Gmail o Microsoft 365, pero todas sus acciones pasan primero por el servidor controlado por los atacantes.
- El kit captura credenciales, *cookies* de sesión y tokens de autenticación, permitiendo que el atacante entre a la cuenta sin necesidad de contraseñas adicionales o códigos 2FA.

Elementos técnicos observados:

- Infraestructura escalable y modular, con panel de control para los atacantes.
- Uso extensivo de workers[.]dev, un servicio legítimo de Cloudflare que permite ejecutar código en la nube.
- Alta capacidad para evadir detecciones tradicionales de correo.
- Recolección de tokens de sesión, lo que permite iniciar sesión sin generar alertas adicionales.
- Redireccionamientos encadenados y uso de certificados SSL válidos para parecer legítimos.

Elementos técnicos observados:

- Infraestructura escalable y modular, con panel de control para los atacantes.
- Uso extensivo de workers[.]dev, un servicio legítimo de Cloudflare que permite ejecutar código en la nube.
- Alta capacidad para evadir detecciones tradicionales de correo.
- Recolección de tokens de sesión, lo que permite iniciar sesión sin generar alertas adicionales.
- Redireccionamientos encadenados y uso de certificados SSL válidos para parecer legítimos.

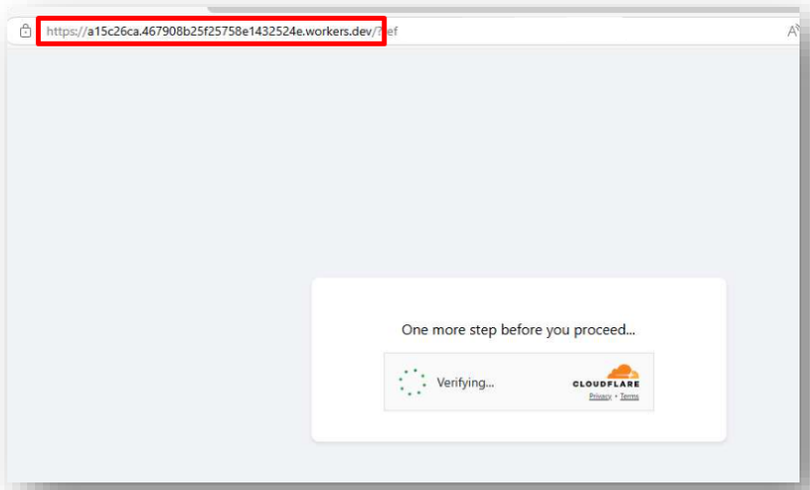


Imagen 5. Suplantación de un captcha de sitio web de EvilProxy.

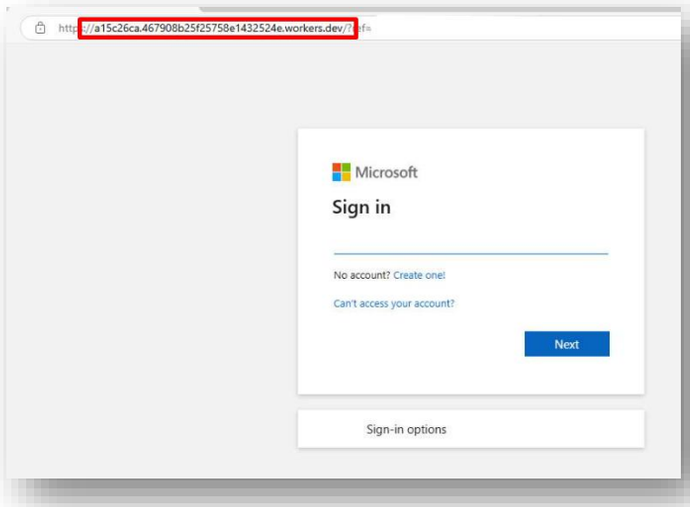


Imagen 6. Sitio web de EvilProxy suplantando a Outlook.

Mamba

Mamba es un kit de *phishing* más reciente pero cada vez más utilizado para campañas dirigidas a usuarios de Microsoft 365. Su principal ventaja para los atacantes es que permite desplegar rápidamente páginas de inicio de sesión falsas con apariencia altamente convincente.

¿Cómo opera?

- Imita interfaces de servicios corporativos, principalmente Outlook y Microsoft 365, replicando logos, tipografías y validaciones básicas.
- Cuando el usuario ingresa su correo, el kit realiza una verificación falsa para hacerlo parecer legítimo.
- Posteriormente captura la contraseña y la envía al servidor del ciberdelincuente.
- En algunos casos integra módulos para rastrear la ubicación de la víctima y validar el navegador.

Elementos técnicos observados:

- Plantillas HTML muy similares a las oficiales.
- Integración con CAPTCHA falsos (en ocasiones imitando Cloudflare) para generar confianza.
- Registro de información adicional como User-Agent, dirección IP y geolocalización aproximada.
- Infraestructura ligera que permite campañas masivas de bajo costo.

Mamba

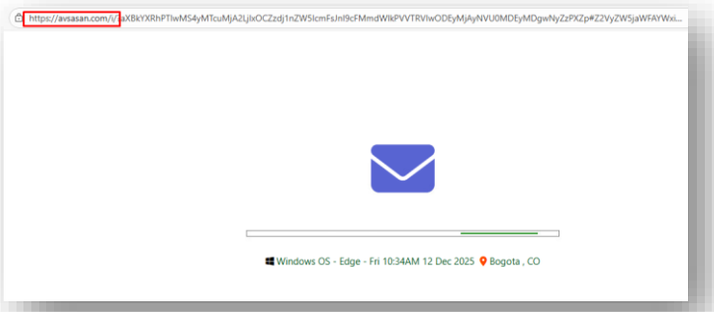


Imagen 7. Previa identificación de datos del equipo.

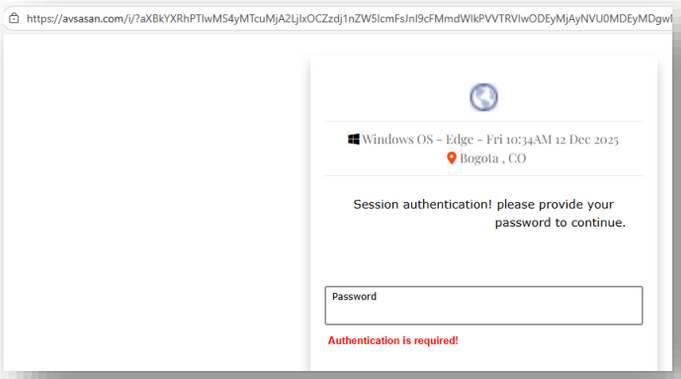


Imagen 8. Suplantación de portal de inicio de sesión de una empresa.

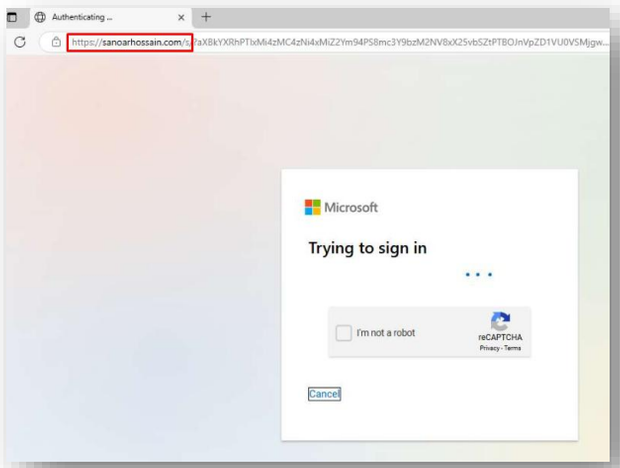


Imagen 9. Suplantación de un captcha de sitio web de Mamba.

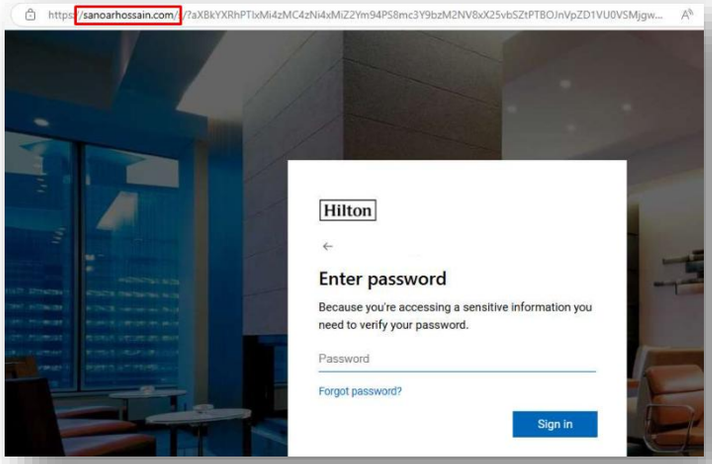
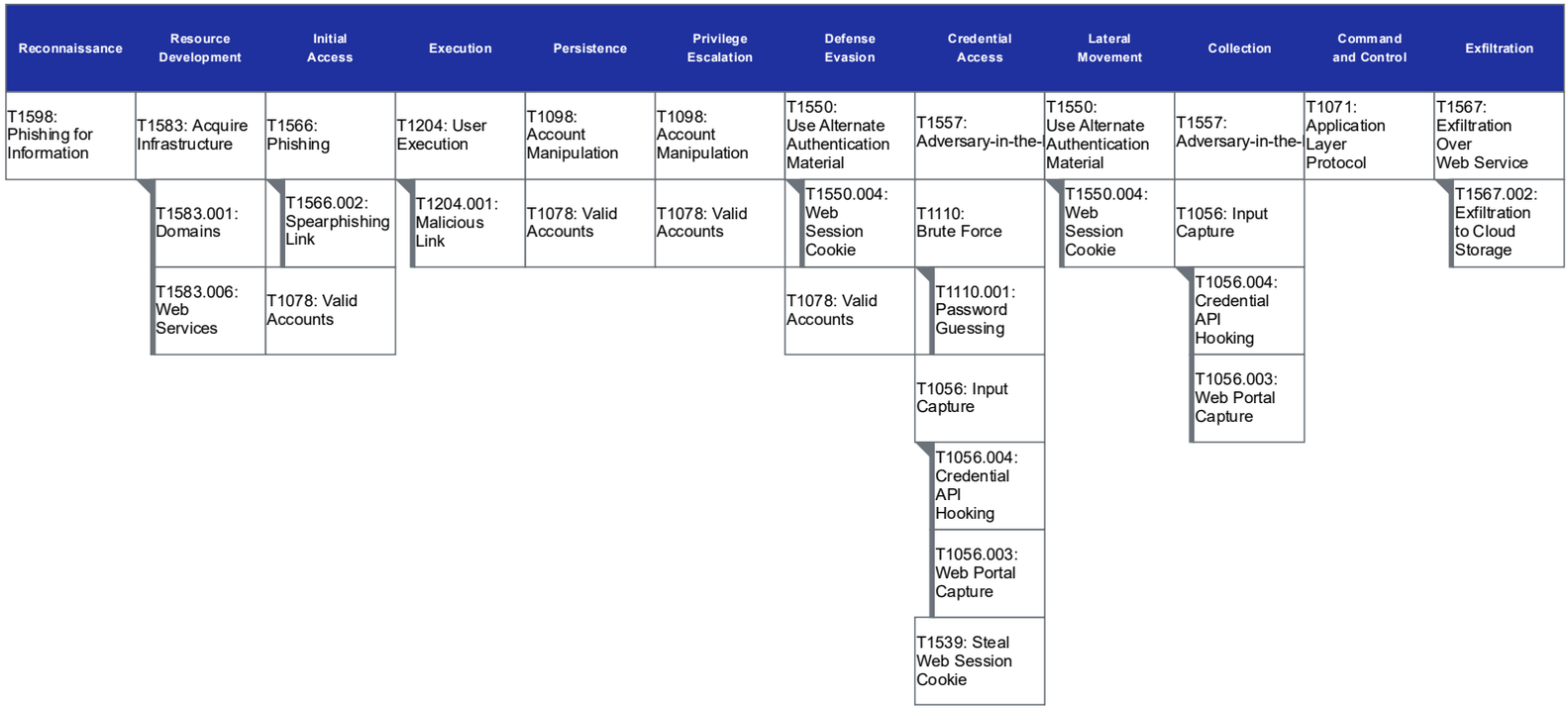


Imagen 10. Sitio web de Mamba suplantando a Microsoft 365.

Tácticas, técnicas y Procedimientos (TTP) identificadas



Mitigaciones de MITRE ATT&CK

MITIGACIÓN	ID MITIGACIÓN	RELEVANCIA
Formación y concienciación de usuarios	**M1017**	Reduce la probabilidad de que empleados hagan clic en enlaces phishing y entreguen credenciales. Programas regulares de simulación y reporte aceleran la detección y frenan campañas basadas en ingeniería social.
Autenticación multifactor	**M1032**	Implementar MFA fuerte disminuye el impacto de la captura de credenciales. Un doble factor de autenticación bien implementado y con controles condicionales complica el uso de credenciales y tokens comprometidas.
Restringir contenido web	**M1021**	El filtrado de URL, bloqueo de Tiendas de dominios sospechosas (TLD), bloqueo de redirecciones y control de ejecución de scripts en navegadores ayuda a impedir el acceso a las páginas donde viven los kits y a detectar redirecciones a Cloudflare Workers usadas por EvilProxy. También reduce la superficie donde se alojan plantillas y formularios falsos.
Auditoría y monitoreo	**M1047**	Registro y análisis de eventos de autenticación, alertas por uso de tokens/session cookies anómalas permiten identificar accesos derivados de robo de sesiones o uso de sesiones capturadas por AiTM. Es clave para respuesta temprana tras la suplantación.

Recomendaciones

- De ser posible **implementar mecanismos de autenticación robusta** basados en FIDO2 o llaves de seguridad hardware, evitando MFA por SMS o TOTP cuando sea posible, ya que kits como **EvilProxy** pueden interceptar códigos de un solo uso mediante ataques AiTM. El uso de autenticación resistente al *phishing* reduce drásticamente la posibilidad de que un adversario reutilice credenciales robadas o secuestre sesiones activas.

- **Configurar políticas de acceso condicional que validen ubicación, tipo de dispositivo** y riesgo de sesión antes de permitir el inicio de sesión en cuentas corporativas. Estas políticas añaden capas de verificación que bloquean accesos provenientes de infraestructura usada en *phishing*, incluso si el ciberdelincuente posee credenciales válidas.

- **Bloquear dominios recién creados (DGA/NRD), TLD sospechosos** y servicios usados recurrentemente por kits de *phishing* (, dominios .biz.id, .sa.com, etc.), mediante filtros DNS corporativos y soluciones CASB. Este bloqueo preventivo reduce la exposición de los usuarios a páginas donde se alojan estos kits.

- Reforzar la integridad de las sesiones mediante el **uso de tokens con tiempos de vida más cortos**, detección de anomalías en cookies y revocación inmediata de sesiones ante comportamientos atípicos. Esto ayuda a mitigar el impacto de técnicas de secuestro de sesión que kits como EvilProxy pueden explotar.

- **Actualizar continuamente los indicadores de compromiso** (IOC) en firewalls, WAF, SIEM y herramientas de filtrado de correo, asegurando que la infraestructura maliciosa descubierta se bloquee de forma inmediata. La rápida propagación de dominios en estos kits hace necesario un ciclo de actualización constante.

- Fortalecer la seguridad del correo corporativo mediante **políticas avanzadas de detección** de *phishing*, análisis de enlaces en modo “sandbox”, protección de URL en tiempo real y autenticación de mensajes con SPF, DKIM y DMARC en modo estricto. Estas medidas reducen la probabilidad de que los usuarios reciban los enlaces maliciosos.

- **Educar de manera continua a los colaboradores** sobre señales de suplantación, comportamiento típico de páginas AiTM, importancia de no ingresar credenciales en enlaces recibidos por correo y cómo reportar incidentes sospechosos. Aunque es una medida no técnica, es esencial para reducir el éxito de campañas como las observadas.

FUENTES:

Barracuda Networks Blog (es.blog.barracuda.com), 22 ene 2025, 12 dic 2025, Threat Spotlight: kit de phishing Tycoon 2FA actualizado para evadir la inspección, Blog corporativo / fuente técnica.
https://es.blog.barracuda.com/2025/01/22/threat-spotlight-tycoon-2fa-phishing-kit

Barracuda Networks Blog (es.blog.barracuda.com), 19 mar 2025, 12 dic 2025, Threat Spotlight: Un millón de ataques Phishingcomo servicio en dos meses ponen de manifiesto una amenaza en rápida evolución, Blog corporativo / fuente técnica.
https://es.blog.barracuda.com/2025/03/19/threat-spotlight-phishing-as-a-service-fast-evolving-threat

Indicadores de compromiso

Tipo de IOC	Valor	Amenaza
Dominio	keepachangelog[.]chooviotrikougoo[.]me[.]uk	**Tycoon 2FA**
Dominio	mobile[.]vaichuthe[.]ai[.]in	**Tycoon 2FA**
Dominio	ticket[.]traistaibu[.]sa[.]com	**Tycoon 2FA**
Dominio	metric[.]bavitu[.]pro	**Tycoon 2FA**
Dominio	seo[.]pechaifa[.]biz[.]id	**Tycoon 2FA**
Dominio	engineering[.]grozzly[.]sa[.]com	**Tycoon 2FA**
Dominio	opentelemetry[.]yoothounu[.]ai[.]in	**Tycoon 2FA**
Dominio	zizuhey[.]anglosamerican[.]com	**Tycoon 2FA**
Dominio	row[.]veashogu[.]us	**Tycoon 2FA**
Dominio	actividadlineaww[.]webcindario[.]com	**Tycoon 2FA**
Dominio	equity[.]pechaifa[.]biz[.]id	**Tycoon 2FA**
Dominio	drddevelopments[.]com	**Tycoon 2FA**
Dominio	poustewou[.]vahelai[.]my[.]id	**Tycoon 2FA**
Dominio	asw[.]mafairoo[.]sa[.]com	**Tycoon 2FA**
Dominio	callback[.]lintora[.]digital	**Tycoon 2FA**
Dominio	bundle[.]olivegreens[.]icu	**Tycoon 2FA**
Dominio	subscription[.]vaichuthe[.]ai[.]in	**Tycoon 2FA**
Dominio	mvp[.]bouvitoo[.]biz[.]id	**Tycoon 2FA**
Dominio	expressvpn[.]thoodeazo[.]sa[.]com	**Tycoon 2FA**
Dominio	powerbi[.]dioyilio[.]ru[.]com	**Tycoon 2FA**
Dominio	cariagehealthcare[.]com	**Tycoon 2FA**
Dominio	siri[.]veranto[.]digital	**Tycoon 2FA**
Dominio	mdrive-reauthy[.]com	**Tycoon 2FA**
Dominio	emtech[.]sbs	**Tycoon 2FA**
Dominio	noscript[.]lootouboo[.]in[.]net	**Tycoon 2FA**
Dominio	a15c26ca[.]467908b25f25758e1432524e[.]workers[.]dev	**EvilProxy**
Dominio	27904837[.]152678eb54a422d76c34631f[.]workers[.]dev	**EvilProxy**
Dominio	18a8e07d[.]6b89aa11ed3d17b4418ae790[.]workers[.]dev	**EvilProxy**
Dominio	aabf8f25[.]bdeaa88df36aa196d31d7d70[.]workers[.]dev	**EvilProxy**
Dominio	sub[.]intelisgtm[.]xyz	**EvilProxy**
Dominio	avsasan[.]com	**Mamba**