Investigadores en ciberseguridad han emitido una alerta sobre campañas de correos electrónicos maliciosos que utilizan una herramienta de *phishing-as-a-service* (PhaaS) conocida como Rockstar 2FA, diseñada para robar credenciales de cuentas de Microsoft 365.

> *«Esta operación implementa un ataque de tipo adversario en el medio (AitM), lo que permite a los atacantes capturar tanto las credenciales de acceso como las cookies de sesión. Esto implica que incluso las cuentas protegidas con autenticación multifactor (MFA) no están completamente seguras»,* explicaron Diana Solomon y John Kevin Adriano, expertos de Trustwave.

Rockstar 2FA se identifica como una evolución del kit de *phishing* DadSec, también llamado Phoenix. Microsoft está siguiendo las actividades de los responsables de esta plataforma PhaaS bajo el nombre en clave Storm-1575.

Este kit, al igual que versiones anteriores, se promociona en plataformas como ICQ, Telegram y Mail.ru mediante un modelo de suscripción, ofreciendo sus servicios por $200 durante dos semanas o $350 al mes. Esto permite que ciberdelincuentes con poca experiencia técnica realicen campañas masivas con facilidad.

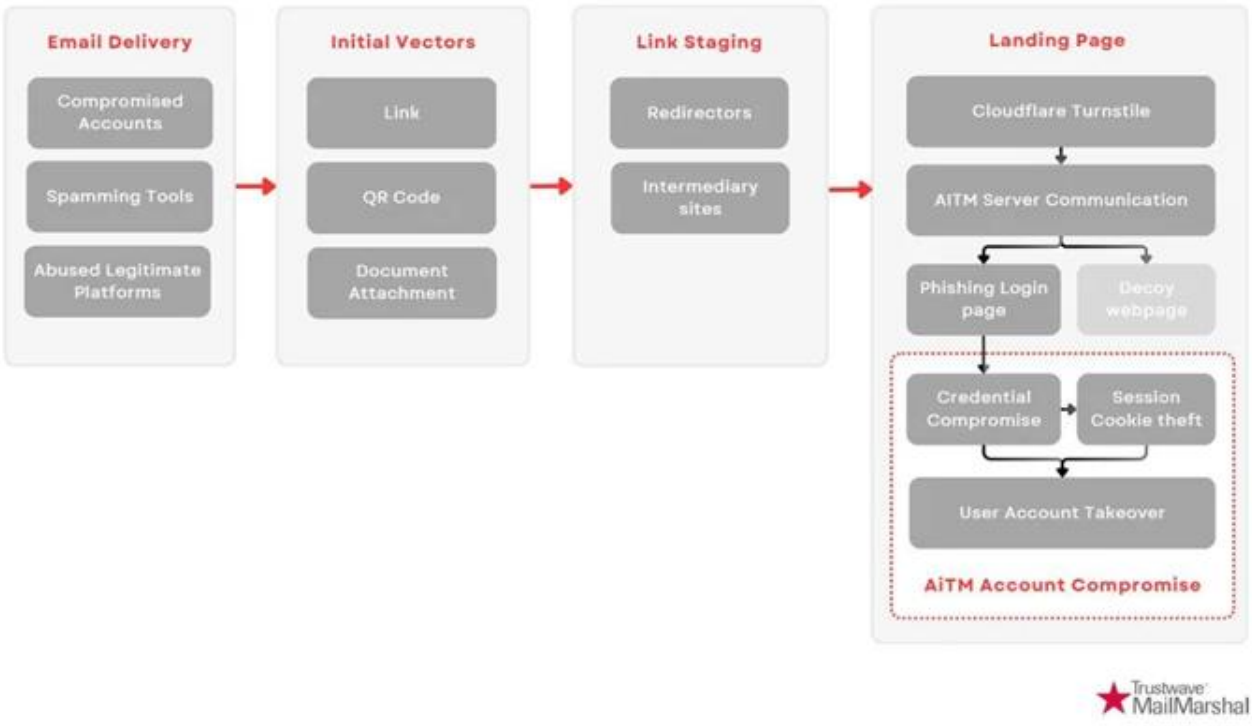
Funcionalidades clave de Rockstar 2FA:

- Capacidad para evadir autenticación de dos factores (2FA).
- Recolección de cookies asociadas al 2FA.
- Protección contra análisis automatizados (antibot).
- Temas de inicio de sesión que replican servicios conocidos.
- Enlaces diseñados para evitar detecciones (FUD).
- Integración con bots de Telegram.

El kit también incluye un *«panel de administración moderno e intuitivo»* que facilita a los usuarios monitorear el progreso de sus campañas, generar enlaces y archivos adjuntos, así como personalizar las plantillas aplicadas a los enlaces.

Según Trustwave, las campañas detectadas emplean diversos métodos de acceso inicial, como enlaces directos, códigos QR y documentos adjuntos, que son distribuidos a través de cuentas comprometidas o herramientas de spam. Los correos suelen utilizar tácticas engañosas, como notificaciones de intercambio de archivos o solicitudes para firmar documentos electrónicamente.

Para evitar los sistemas de detección antispam, los atacantes recurren a redireccionadores legítimos, como enlaces acortados o servicios de reescritura de URLs. Además, el kit incorpora herramientas como Cloudflare Turnstile para bloquear análisis automatizados en las páginas de *phishing*.



Trustwave destacó que esta plataforma utiliza servicios legítimos como Atlassian Confluence, Google Docs Viewer y herramientas de Microsoft, como OneDrive, OneNote y Dynamics 365 Customer Voice, para alojar los enlaces fraudulentos. Esto demuestra cómo los atacantes se

aprovechan de la confianza que inspiran estas plataformas.

> *«El diseño de las páginas de phishing imita casi a la perfección las páginas de inicio de sesión oficiales de las marcas atacadas, a pesar de que el código HTML ha sido ampliamente ofuscado. Toda la información proporcionada por el usuario en estas páginas es enviada directamente al servidor AitM. Los atacantes luego utilizan las credenciales robadas para extraer la cookie de sesión asociada a la cuenta comprometida»,* señalaron los investigadores.

Paralelamente, Malwarebytes ha informado sobre otra campaña de *phishing* conocida como Beluga, que utiliza archivos adjuntos en formato .HTM para engañar a los destinatarios y hacerlos ingresar sus credenciales de Microsoft OneDrive en una página falsa. Estas credenciales son enviadas a un bot de Telegram.

Además, se han identificado enlaces de *phishing* y anuncios engañosos en redes sociales que promueven aplicaciones fraudulentas, como el adware MobiDash, y aplicaciones financieras falsas diseñadas para robar dinero e información personal, prometiendo ganancias rápidas.

> *«Los juegos de apuestas anunciados parecen ser oportunidades legítimas para ganar dinero, pero están diseñados para engañar a las personas y hacer que depositen fondos, los cuales nunca podrán recuperar»*, explicó Mahmoud Mosaad, analista del CERT de Group-IB.
>
> *«Por medio de estas aplicaciones y sitios web fraudulentos, los atacantes recopilan datos personales y financieros durante el registro. Algunas víctimas han reportado pérdidas superiores a los $10,000 debido a estas estafas»,* agregó.