Investigadores de ciberseguridad han detectado una campaña activa de publicidad maliciosa que explota la plataforma publicitaria de Meta y cuentas de Facebook comprometidas para difundir un malware conocido como SYS01stealer.

> *«Los ciberdelincuentes responsables de la campaña utilizan marcas de confianza para ampliar su alcance»,* comentó Bitdefender Labs en un informe.
>
> *«La campaña de malvertising emplea casi cien dominios maliciosos, utilizados no solo para distribuir el malware, sino también para operaciones de comando y control (C2) en tiempo real, permitiendo a los atacantes gestionar la operación de forma continua.»*

SYS01stealer fue registrado por primera vez por Morphisec a principios de 2023, en el contexto de campañas que atacan cuentas empresariales de Facebook mediante anuncios de Google y perfiles de Facebook falsos que promocionan juegos, contenido para adultos y software pirateado.

Al igual que otros programas maliciosos de robo de información, el objetivo principal es sustraer credenciales de inicio de sesión, historial de navegación y cookies. Sin embargo, SYS01stealer también se enfoca en acceder a datos de cuentas y anuncios de negocios en Facebook, los cuales son reutilizados para distribuir más malware mediante anuncios falsos.

> *«Las cuentas de Facebook comprometidas permiten que toda la operación se amplifique. Cada cuenta hackeada puede reutilizarse para promover más anuncios maliciosos, incrementando el alcance de la campaña sin que los atacantes tengan que crear cuentas nuevas»,* agregó Bitdefender.

El malware SYS01stealer se distribuye principalmente a través de publicidad maliciosa en

plataformas como Facebook, YouTube y LinkedIn, con anuncios que promueven temas para Windows, juegos, software de inteligencia artificial, editores de fotos, VPNs y servicios de streaming de películas. La mayoría de estos anuncios en Facebook están dirigidos a hombres de 45 años o más.

> *«Esto logra atraer a las víctimas a hacer clic en estos anuncios, exponiéndolos al robo de sus datos de navegación»,* explicó Trustwave en un análisis del malware en julio de 2024.
>
> *«Si en los datos obtenidos se incluye información relacionada con Facebook, existe la posibilidad de que no solo se roben los datos del navegador, sino que los atacantes también puedan controlar las cuentas de Facebook para distribuir más anuncios maliciosos y mantener el ciclo de infección.»*

Los usuarios que interactúan con estos anuncios son redirigidos a sitios falsos alojados en Google Sites o True Hosting, los cuales imitan marcas y aplicaciones legítimas para iniciar la infección. Además, se sabe que los atacantes utilizan cuentas de Facebook comprometidas para publicar anuncios fraudulentos.

La carga inicial descargada desde estos sitios es un archivo ZIP que contiene un ejecutable benigno, utilizado para cargar de manera indirecta una DLL maliciosa que desencadena un proceso de múltiples etapas.

Este proceso incluye la ejecución de comandos de PowerShell para evitar que el malware funcione en un entorno de prueba, modificar la configuración de Microsoft Defender Antivirus para excluir ciertos archivos y rutas, y configurar el entorno operativo para ejecutar el malware basado en PHP.

En las últimas cadenas de ataque observadas por la empresa rumana de ciberseguridad, los archivos ZIP incluyen una aplicación Electron, lo que indica que los atacantes están

adaptando y refinando sus estrategias continuamente.

También se encuentra en el Archivo de Shell de Átomo (ASAR) un archivo JavaScript («main.js») que ahora ejecuta comandos de PowerShell para realizar verificaciones en sandbox y llevar a cabo el stealer. La persistencia en el sistema se logra configurando tareas programadas.

> *«La capacidad de adaptación de los cibercriminales detrás de estas campañas hace que la campaña infostealer SYS01 sea especialmente amenazante. El malware utiliza detección de sandbox, interrumpiendo sus funciones si detecta que se está ejecutando en un entorno controlado, frecuentemente utilizado por analistas para examinar malware. Esto le permite permanecer indetectado en muchas ocasiones»,* indicó Bitdefender.
>
> *«Cuando las empresas de ciberseguridad comienzan a señalar y bloquear una versión concreta del cargador, los hackers responden rápidamente al actualizar el código. Luego lanzan nuevos anuncios con malware actualizado que elude las últimas medidas de seguridad.»*

Campañas de Phishing que Abusan de Eventbrite

Este desarrollo ocurre mientras Perception Point informa sobre campañas de phishing que mal utilizan la plataforma de eventos y venta de entradas Eventbrite para robar información financiera o personal.

Los correos electrónicos, enviados desde noreply@events.eventbrite[.]com, incitan a los usuarios a hacer clic en un enlace para pagar una factura pendiente o confirmar su dirección de entrega, tras lo cual se les solicita ingresar sus datos de acceso y detalles de la tarjeta de crédito.

El ataque se hace posible porque los actores de amenazas crean cuentas legítimas en el servicio y organizan eventos falsos, aprovechando la reputación de una marca reconocida y escondiendo el enlace de phishing en la descripción del evento o como un archivo adjunto. La invitación a estos eventos se envía luego a sus objetivos.

> *«Como el correo electrónico se envía desde el dominio y la dirección IP verificados de Eventbrite, es más probable que evite los filtros de correo electrónico, logrando llegar a la bandeja de entrada del destinatario»*, comentó Perception Point.
>
> *«El dominio del remitente de Eventbrite también aumenta la probabilidad de que los destinatarios abran el correo y hagan clic en el enlace de phishing. Este abuso de la plataforma Eventbrite permite a los atacantes eludir la detección, asegurando mayores tasas de entrega y apertura.»*

Un Tipo Diferente de «Estafa de Pig Butchering»

Los investigadores de amenazas también están señalando un incremento en el fraude relacionado con criptomonedas que finge representar a diversas organizaciones, dirigido a usuarios mediante ofertas laborales falsas que supuestamente les permiten ganar dinero desde casa. Los mensajes no solicitados también afirman representar marcas legítimas como Spotify, TikTok y Temu.

La actividad comienza a través de redes sociales, mensajes de texto y aplicaciones de mensajería como WhatsApp y Telegram. Los usuarios que aceptan los trabajos son instruidos por los estafadores a registrarse en un sitio web malicioso usando un código de referencia, tras lo cual se les pide completar diversas tareas: enviar reseñas falsas, realizar pedidos de productos, reproducir canciones específicas en Spotify o reservar hoteles.

La estafa se desarrolla cuando el saldo de la cuenta de comisiones ficticias de las víctimas se vuelve negativo, y se les presiona a recargar invirtiendo su propia criptomoneda para

obtener bonificaciones por las tareas.

> *«Este ciclo dañino continuará mientras los estafadores piensen que la víctima seguirá aportando dinero al sistema. Si sospechan que su víctima se ha dado cuenta de la estafa, bloquearán su cuenta y la ignorarán»,* afirmaron los investigadores de Proofpoint.

Este esquema ilegal ha sido atribuido con alta certeza a actores de amenazas que también realizan «pig butchering», conocido también como fraude de inversión en criptomonedas basado en el romance.

> *«El fraude laboral ofrece retornos más pequeños pero más frecuentes para los estafadores en comparación con el 'pig butchering'. Esta actividad aprovecha el reconocimiento de marcas populares en lugar de una larga estafa de confianza basada en el romance»,* explicaron desde Proofpoint.