| Centro Nacional de Seguridad Digital | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°203 | Fecha: 29-08-2023 |
|---|---|---|
| | | Página: 4 de 6 |

| | | | |
|---|---|---|---|
| Componente que reporta | **CENTRO NACIONAL DE SEGURIDAD DIGITAL** | | |
| Nombre de la alerta | El phishing como servicio se vuelve más inteligente: Microsoft hace sonar la alarma ante los ataques AiTM | | |
| Tipo de Ataque | Phishing | Abreviatura | Phishing |
| Medios de propagación | Redes sociales, SMS, correo electrónico, videos de internet, entre otros | | |
| Código de familia | G | Código de Sub familia | G01 |
| Clasificación temática familia | Fraude | | |

Descripción

1. **ANTECEDENTES:**

   Microsoft advierte sobre un aumento en las técnicas de phishing de adversario en el medio ( AiTM ), que se están propagando como parte del modelo de cibercrimen de phishing como servicio (PhaaS).

   Además de un aumento en las plataformas PhaaS con capacidad AiTM, el gigante tecnológico señaló que los servicios de phishing existentes como PerSwaysion están incorporando capacidades AiTM.

2. **DETALLES:**

   "Este desarrollo en el ecosistema PhaaS permite a los atacantes llevar a cabo campañas de phishing de gran volumen que intentan eludir las protecciones MFA a escala", dijo el equipo de Microsoft Threat Intelligence en una serie de publicaciones en X (anteriormente Twitter).

   Los kits de phishing con capacidades AiTM funcionan de dos maneras, una de las cuales se refiere al uso de servidores proxy inversos (es decir, la página de phishing) para transmitir tráfico hacia y desde el cliente y el sitio web legítimo y capturar sigilosamente las credenciales del usuario, códigos de autenticación de dos factores, y cookies de sesión.

   Un segundo método implica servidores de retransmisión sincrónicos.

   "En AiTM, a través de servidores de retransmisión sincrónicos, se presenta al objetivo una copia o una imitación de una página de inicio de sesión, como los ataques de phishing tradicionales", dijo Microsoft. "Storm-1295, el grupo de actores detrás de la plataforma Greatness PhaaS, ofrece servicios de retransmisión sincrónica a otros atacantes".

   Greatness fue documentada por primera vez por Cisco Talos en mayo de 2023 como un servicio que permite a los ciberdelincuentes atacar a los usuarios comerciales del servicio en la nube Microsoft 365 utilizando señuelos convincentes y páginas de inicio de sesión. Se dice que ha estado activo desde al menos mediados de 2022.

   El objetivo final de estos ataques es desviar cookies de sesión, lo que permite a los actores de amenazas acceder a sistemas privilegiados sin necesidad de volver a autenticarse.

   "Eludir MFA es el objetivo que motivó a los atacantes a desarrollar técnicas de robo de cookies de sesión AiTM", señaló el gigante tecnológico. "A diferencia de los ataques de phishing tradicionales, los procedimientos de respuesta a incidentes para AiTM requieren la revocación de las cookies de sesión robadas".

3. **RECOMENDACIONES:**

   - Configurar el doble factor de autentificación.
   - Realizar el monitoreo de cualquier anomalía del posible recurso afectado.
   - Reducir el periodo máximo de cambio de contraseña a 30 o 45 días.
   - Desactivar las listas de correo que no se usan para evitar que atacantes futuros puedan usarlas y solo activarlas cuando sea necesario.
   - Evaluar el uso de una red privada virtual (VPN) para prevenir la vulnerabilidad de servicios expuestos.
   - Limitar el acceso con listas blancas. Generar una lista de IP públicas permitidas y/o lista de países permitidos y/o usuarios y/o horarios permitidos.

| | |
|---|---|
| Fuente de Información: | hxxps://thehackernews.com/2023/08/phishing-as-service-gets-smarter.html |