Centro Nacional de Seguridad Digital	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 136**	**Fecha: 10-06-2023**
		Página 4 de 21

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Los hackers filtran credenciales de administrador de i2VPN en Telegram		
Tipo de ataque	Captura de información confidencial	Abreviatura	CIC
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	K	Código de subfamilia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES

Los usuarios de i2VPN corren el riesgo de una violación masiva de seguridad y privacidad si las supuestas credenciales de inicio de sesión son auténticas.

La aplicación I2VPN cuenta con una base significativa de usuarios y con más de 500 000 descargas solo en Google Play Store.

2. DETALLES:

- I2VPN es una popular aplicación de servidor proxy VPN freemium disponible para descargarse en Google Play y App Store. Recientemente hubo un incidente de ciberseguridad, hackers ciberdelincuentes afirmaron haber violado con éxito las credenciales de administrador de i2VPN.
- El incidente de ciberseguridad genero la publicidad de la información confidencial de i2VPN en Telegram, los ciberdelincuentes obtuvieron acceso al panel de administración principal de i2VPN y toda la información privada de los usuarios.
- Los datos filtrados incluían dirección de correo electrónico, ID de usuario, nombres de cuenta, métodos de pago, fechas de vencimiento y contraseña del administrador, capturas de pantalla del panel donde se encuentra los centros de datos y los detalles de suscripción de usuarios.
- A pesar que los ciberdelincuentes no divulgaron los datos de los usuarios, las credenciales obtenidas por los ciberdelincuentes proporcionan acceso a una cantidad sustancial de información personal y centros de datos. Incluso pueden emplear información de las cuentas comprometidas para iniciar ataques de phising haciéndose pasar por personas y engañarlas para que divulguen información confidencial.
- Las compañías VPN son un objetivo para estos ciberdelincuentes, hace unos días SuperVPN también fue víctima exponiéndose 360 millones de registros de usuarios al público.
- Los usuarios de estas compañías VPN pueden tomar precauciones, tales como: evaluar si continuaran empleando i2VPN, cambiar sus credenciales de inicio de sesión, revisar los sitios web que se conectó mientras utilizaba el servicio VPN, eliminar o transferir sus archivos o comunicaciones confidenciales para evitar mayor compromiso.

3. RECOMENDACIONES:

- A los usuarios, estar atentos ante cualquier actualización oficial o notificación de i2VPN con respecto a la violación y medidas de seguridad.
- Tener cuidado al compartir información personal en línea.

Fuentes de información	▪ hxxps://www.hackread.com/hackers-i2vpn-admin-credentials-telegram-leak/ ▪ hxxps://www.safetydetectives.com/news/i2vpn-exposed-telegram/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 136	**Fecha: 10-06-2023**
		Página 5 de 21

Componente que reporta	**COMANDO OPERACIONAL DE CIBERDEFENSA DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS**		
Nombre de la alerta	Nueva campaña de Magecart secuestra sitios legítimos para alojar scripts con skimmers de tarjetas de crédito.		
Tipo de ataque	Pishing	Abreviatura	Pishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G01
Clasificación temática familia	Código Malicioso		

Descripción

1. Una nueva campaña de robo de tarjetas de crédito de Magecart secuestra sitios legítimos para actuar como servidores de comando y control "improvisados" y para inyectar y ocultar los skimmers en sitios de comercio electrónico específicos.

   Un ataque de Magecart es cuando los delincuentes informáticos ingresan a las tiendas en línea para inyectar scripts maliciosos que roban las tarjetas de crédito y la información personal de los clientes durante el pago. Según los investigadores de Akamai que monitorean esta campaña, ha comprometido a organizaciones en los Estados Unidos, el Reino Unido, Australia, Brasil, Perú y Estonia.

   La firma de ciberseguridad también señala que muchas de las víctimas no se han dado cuenta de que fueron violadas durante más de un mes, lo que es un testimonio del sigilo de estos ataques.

   El primer paso de los atacantes es identificar sitios legítimos vulnerables y hackearlos para alojar su código malicioso, usándolos como servidores C2 para sus ataques, al distribuir los skimmers de tarjetas de crédito utilizando sitios web legítimos con buena reputación, los actores de amenazas evaden la detección y los bloqueos se liberan de la necesidad de configurar su propia infraestructura.

   Para aumentar el sigilo del ataque, los actores de amenazas ofuscan el skimmer en Base64, que también oculta la URL del host, y construyeron su estructura de una manera que se asemeja a Google Tag Manager o Facebook Pixel, que son servicios populares de terceros y poco probable que levanten sospechas.

   Akamai informa haber visto dos variantes del skimmer utilizadas en esta campaña en particular. La primera es una versión muy ofuscada que contiene una lista de selectores de CSS que apuntan a la PII del cliente y los detalles de la tarjeta de crédito. Los selectores de CSS eran diferentes para cada sitio objetivo, hechos a la medida para coincidir con cada víctima.

   La segunda variante de skimmer no estaba tan bien protegida, exponiendo indicadores en el código que ayudaron a Akamai a mapear el alcance de la campaña e identificar víctimas adicionales.

   Después de que los skimmers roban los detalles de los clientes, los datos se configuran en el servidor del atacante a través de una solicitud HTTP creada como una etiqueta IMG dentro del skimmer, se aplica una capa de codificación Base64 a los datos para ofuscar la transmisión y minimizar la probabilidad de que la víctima descubra la infracción.

   Se ha identificado que estas aplicaciones maliciosas han estado implantando en secreto hardware en dispositivos móviles desprevenidos sin detección, al utilizar una función de detección de anomalías integrada en su software Bitdefender Mobile Security hace apenas un mes, Bitdefender identificó de manera efectiva las aplicaciones maliciosas.

   Los propietarios de sitios web pueden defenderse contra las infecciones de Magecart protegiendo adecuadamente las cuentas de administrador del sitio web y aplicando actualizaciones de seguridad para su CMS y complementos.

Los clientes de tiendas en línea pueden minimizar el riesgo de exposición de datos utilizando métodos de pago electrónicos, tarjetas virtuales o estableciendo límites de cargo en sus tarjetas de crédito.

2. RECOMENDACIONES:

- Aprende a identificar claramente los correos electrónicos sospechosos de ser 'phishing'.
- Verifica la fuente de información de tus correos entrantes.
- Nunca entres en la web de tu banco pulsando en links incluidos en correos electrónicos.
- Refuerza la seguridad de tu ordenador.
- Introduce tus datos confidenciales únicamente en webs seguras.
- Revisa periódicamente tus cuentas.
- No sólo de banca online vive el phishing.
- El phishing sabe idiomas.
- Ante la mínima duda se prudente y no te arriesgues.
- Infórmate periódicamente sobre la evolución del malware.

Fuentes de información	hxxps://blog.segu-info.com.ar/2023/06/nueva-campana-de-magecart-secuestra.html