	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 075	**Fecha: 28-03-2023**
		Página 8 de 20

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Extensión maliciosa de Chrome roba cuentas de correos Gmail		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código Malicioso		

Descripción

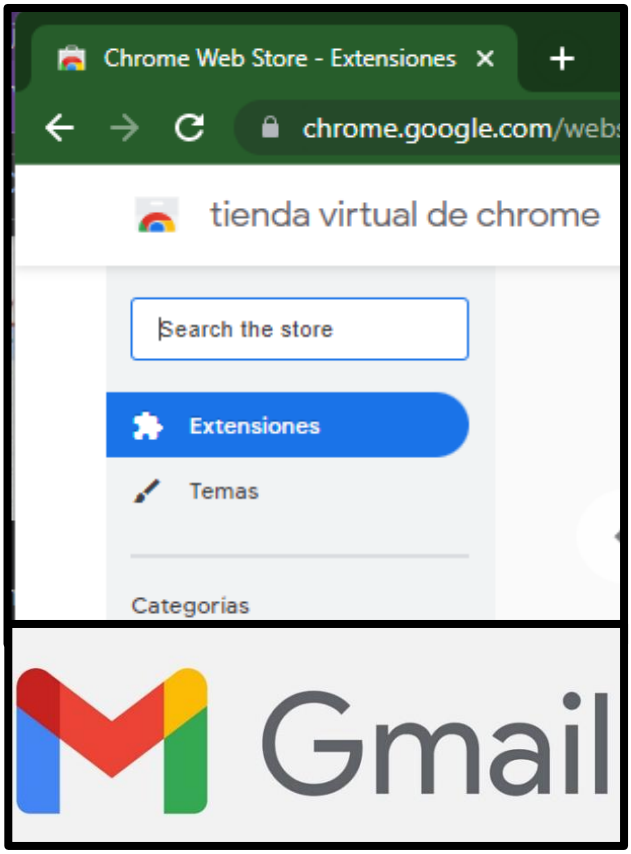
ANTECEDENTES:

El 24 de marzo del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se ha encontrado información sobre una extensión maliciosa de Chrome que roba cuentas de correo Gmail, mediante el empleo de phishing como primer vector de ataque.

DETALLES:

El Servicio Nacional de Inteligencia (NIS) de República de Corea y la Oficina Federal para la Protección de la Constitucional (BfV) de Alemania han lanzado un aviso sobre una campaña de ataques de ciberdelincuentes norcoreanos que utilizan extensiones de Chrome infectadas para robar correos electrónicos de Gmail.

Estos ciberdelincuentes son conocidos como Kimsuky, pero también tienen otros nombres como Thallium y Velvet Chollima. Se trata de un grupo de actores maliciosos de Corea del Norte que utiliza el phishing se hacen pasar por una fuente legítima para realizar ciberespionaje dirigido a diplomáticos, políticos, periodistas, agencias gubernamentales e incluso profesores universitarios.



Kimsuky utiliza una extensión maliciosa de Google Chrome que se propaga a través de un correo electrónico fraudulento enviado a la potencial víctima. En él, se le anima a instalar dicha extensión en Chrome, aunque también puede instalarse en navegadores basados en Chromium, como son Microsoft Edge o Brave.

Una vez instalada, la extensión, que aparece bajo el nombre "AF", se activa cuando el usuario abre su cuenta de Gmail, sin que se dé cuenta. Es en este momento cuando el malware comienza a interceptar todo el contenido de los mensajes, aunque también se han alertado que tiene acceso a los datos almacenados en servicios en la nube.

Para robar la información, la extensión "AF" utiliza la API Devtools, un conjunto de herramientas para desarrolladores web integrado en el navegador de Google Chrome. Con ello, los actores maliciosos enviaban los datos robados a su servidor de retransmisión. Así, conseguían todos los datos en secreto, sin pasar por la configuración de seguridad del correo electrónico.

También se ha hecho evidente que los piratas informáticos abusan de la función de Google Play que sincroniza la información de la web con el teléfono. La función permite a los usuarios instalar aplicaciones en sus dispositivos vinculados directamente desde sus computadoras, lo que brinda una vía para instalar malware en estos dispositivos.

Los atacantes envían la aplicación maliciosa al sitio para desarrolladores de la consola Google Play con el pretexto de "solo pruebas internas". Luego agregan el dispositivo de la víctima como objetivo de prueba y solicitan a Google Play que instale la aplicación maliciosa en el dispositivo de la víctima.

También han registrado una campaña Kimsuky en la que utiliza una aplicación fraudulenta alojada en Google Play Store, que se conoce desde octubre del pasado año 2022 como FastViewer, Fastfire o Fastspy DEX. Dado que los investigadores ya revelaron públicamente los hashes de FastViewer, los actores de amenazas actualizan periódicamente FastViewer para seguir usándolo.

RECOMENDACIONES:

- Mantener actualizado tu navegador de Chrome. De esta manera se asegura tener instalados todos los parches de seguridad del navegador, antes de instalar una extensión.
- Instalar extensiones de Chrome de forma segura, únicamente desde la tienda oficial Chrome Web Store. Google revisa todas las extensiones que se ofrecen en su tienda. Aunque a veces pasan algunas extensiones con comportamientos maliciosos, pero no tardan mucho en descubrirlo.
- No instalar extensiones de Chrome que provienen de webs, foros, u otros lugares no oficiales. Cualquiera puede escribir una extensión de Chrome con capacidad para tomar el control del ordenador, si no ha sido revisada y no ha pasado los controles de seguridad básicos que lleva a cabo Google.
- Revisar su equipo y verificar las extensiones instaladas, procure quitar las extensiones que no usa habitualmente.
- No instalar extensiones que han aparecido recientemente al mercado.

Fuentes de información	▪ hxxps://gbhackers.com/malicious-chrome-extensions-2/amp/ ▪ hxxps://www.20minutos.es/tecnologia/ciberseguridad/hackeo-extensiones-chrome-robarte-correos-gmail-5112774/