Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°168	Fecha: 17-07-2023
		Página: 4 de 9

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Los ciberdelincuentes explotan las vulnerabilidades de Microsoft Word para implementar malware LokiBot		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Lokibot, también conocido como Loki PWS, es un malware perteneciente a la familia de troyanos que está activo desde 2015 y es utilizado en campañas a nivel global. Lokibot fue diseñado para robar credenciales de navegadores, clientes FTP/ SSH, sistemas de mensajería, y hasta incluso de billeteras de criptomonedas.

Originalmente fue desarrollado en lenguaje C y distribuido en foros clandestinos y mercados en la dark web. Las primeras versiones apuntaban al robo de billeteras de criptomonedas y contraseñas de aplicaciones utilizadas por la víctima, así como las almacenadas en Windows. Se puede definir a Lokibot como un Malware-as-a-Service (MaaS); es decir, un malware que se ofrece como servicio para que terceros lo puedan utilizar. Por esta razón es una herramienta atractiva para los atacantes, porque les permite desarrollar sus propias versiones de Lokibot. Es importante mencionar que existen variantes de Lokibot dirigidas al sistema operativo Android que funcionan como troyano bancario. En 2017 se encontró una variante que, al detectar que era eliminada, se activaba un módulo para el cifrado de archivos en el dispositivo móvil infectado.

Los atacantes generalmente utilizan Lokibot para apuntar a dispositivos con el sistema operativo Windows. Principalmente, se propaga por medio de campañas de phishing que incluyen archivos adjuntos maliciosos o URL embebidas. Estos adjuntos pueden ser archivos Word, Excel o PDF, u otro tipo de extensiones, como .gz o .zip que simulan ser archivos PDF o .txt.

2. DETALLES:

El malware Loki PWS se enfoca en recopilar información confidencial de las máquinas que operan con sistemas Windows infectados. Los atacantes están aprovechando las vulnerabilidades de Microsoft Word para distribuir el malware LokiBot.

Los ataques se basan en dos vulnerabilidades conocidas como: CVE-2021-40444 y CVE-2022-30190 (también conocido como Follina). El archivo de Word que explota CVE-2021-40444 contiene un enlace GoFile externo incrustado dentro de un archivo XML que conduce a la descarga de un archivo HTML. Este archivo HTML emplea la vulnerabilidad Follina para descargar una carga útil adicional, un módulo inyector escrito en Visual Basic que descifra y lanza LokiBot. El inyector también incluye técnicas de evasión para detectar depuradores y entornos virtualizados.

Otra variante de la cadena de ataque descubierta utiliza un documento de Word con script VBA que ejecuta una macro al abrir el documento utilizando las funciones "Auto Open" y "Document_Open". Este Script actúa como un conducto para descargar una carga útil provisional desde un servidor remoto, que también funciona como un inyector para cargar LokiBot y conectarse a un servidor de comando y control (C2). Ver figura.

LokiBot tiene muchas capacidades, como el registro de pulsaciones de teclas, la captura de pantallas y la recopilación de información de inicio de sesión de navegadores web y desviar datos de una variedad de billeteras de criptomonedas. Los atacantes que emplean LokiBot continuan actualizando sus métodos de acceso inicial para propagar e infectar sistemas de manera eficiente.

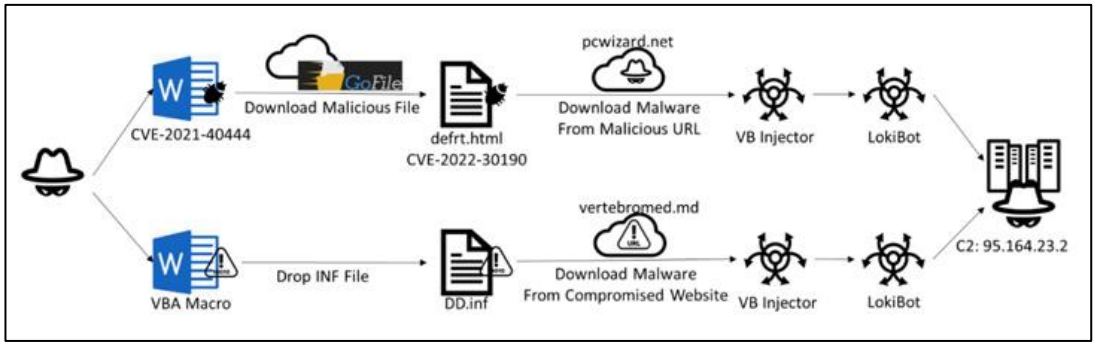

Figura Cadenas de Ataque de Lokibot

A. **Plataformas afectadas**: Microsoft Windows.

B. **Impacto:** Controlar y recopilar información confidencial del dispositivo de la víctima.

C. **Nivel de gravedad:** Crítico.

3. RECOMENDACIONES:

- Tener cuidado al tratar con documentos de Office o archivos desconocidos, en especial si contienen enlaces a sitios web externos.
- Evitar hacer clic en enlaces sospechosos o abrir archivos adjuntos de fuentes no confiables.
- Mantener el software y los sistemas operativos actualizados con los últimos parches de seguridad.
- Aplicar las actualizaciones KB5005565 y KB5003637, lanzadas para corregir las vulnerabilidades CVE-2021-40444 y CVE-2022-30190, respectivamente.

Fuente de Información:	• hxxps://thehackernews.com/2023/07/cybercriminals-exploit-microsoft-word.html • hxxps://www.fortinet.com/blog/threat-research/lokibot-targets-microsoft-office-document-using-vulnerabilities-and-macros • hxxps://www.welivesecurity.com/la-es/2021/09/30/lokibot-principales-caracteristicas-malware-roba-credenciales/ • hxxps://blog.segu-info.com.ar/2021/09/microsoft-publica-el-parche-para-el-0.html?m=0 • hxxps://www.genbeta.com/windows/puedes-actualizar-tu-windows-10-patch-tuesday-junio-solventa-50-vulnerabilidades-cinco-ellas-zero-day