Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°025	Fecha: 29-01-2024
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Otra variante de Phobos Ransomware lanza ataque – FAUST		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES**:

   La familia de ransomware Phobos es un grupo notorio de software malicioso diseñado para cifrar archivos en la computadora de una víctima. Surgió en 2019 y desde entonces ha estado involucrado en numerosos ciberataques.

   Los atacantes utilizaron el servicio Gitea para almacenar varios archivos codificados en Base64, cada uno de los cuales llevaba un binario malicioso. Cuando estos archivos se inyectan en la memoria de un sistema, inician un ataque de cifrado de archivos.

2. **DETALLES:**

   La versión FAUST, una variante de Phobos, puede mantener la persistencia en un entorno determinado y genera múltiples subprocesos para una ejecución eficiente.

   El documento de Microsoft Excel (.XLAM) que descubrimos contiene un script VBA integrado. Al abrir el documento, el script activa PowerShell para la siguiente etapa usando la función “Workbook_Open()”. Luego descarga datos codificados en Base64 de Gitea, que se pueden decodificar en un archivo XLSX limpio. Luego, este archivo se guarda en la carpeta TEMP y se abre automáticamente, lo que induce a error a los usuarios al pensar que el proceso se ha completado y no supone ningún daño, ya que también se recupera sigilosamente un ejecutable que se hace pasar por un actualizador del software AVG AntiVirus ("AVG Updater. exe").

   El archivo ejecutable “AVG update.exe” funciona como descargador. Incorpora una gran cantidad de código extraño para evadir la detección y complicar el análisis. Al emplear una técnica de inyección de procesos, asigna memoria de lectura, escritura y ejecución (RWE) para inyectar el código malicioso en un proceso recién generado. Este binario busca e inicia otro ejecutable llamado "SmartScreen Defender Windows.exe" para iniciar su proceso de cifrado empleando un ataque sin archivos para implementar el código shell malicioso.

   La variante Faust exhibe la capacidad de mantener la persistencia en un entorno y crea múltiples subprocesos para una ejecución eficiente.

   El ransomware FAUST crea archivos info.txt e info.hta dentro de los directorios que contienen los archivos cifrados y agrega la extensión ".faust" a cada archivo cifrado. Estos archivos se utilizan como una forma de ponerse en contacto con los atacantes para iniciar negociaciones de rescate.

   “También inicia múltiples subprocesos para realizar diversas tareas. Estas tareas incluyen implementar cifrado, escanear unidades lógicas, buscar recursos de red/compartir, escanear archivos individualmente y buscar explícitamente archivos relacionados con bases de datos”, compartió Fortinet con Cyber Security News.

3. **RECOMENDACIONES:**

   - Abstenerse de abrir archivos de documentos de fuentes no confiables.
   - Normalizar la gestión de copias de seguridad.
   - Mantener siempre actualizado los programas, tanto en los dispositivos como en los servidores.
   - Procurar la gestión de un plan que incluya detección, investigación y respuesta a amenazas 24/7.
   - En caso de infección, no pagar el rescate ni contactar con los ciberdelincuentes, ya que no hay garantía de que cumplan sus promesas. En su lugar, buscar ayuda profesional para eliminar el ransomware y restaurar los archivos cifrados.

Fuente de Información:	• hxxps://www.fortinet.com/blog/threat-research/phobos-ransomware-variant-launches-attack-faust • hxxps://gbhackers.com/phobos-ransomware-office-document/ • hxxps://thehackernews.com/2024/01/albabat-kasseika-kuiper-new-ransomware.html