BOLETÍN DE ALERTA

Boletín Nro.: 2020-26

Fecha de publicación: 10/09/2020

Tema: Ransomware como servicio “REvil” y otras variantes

Sistemas afectados:

- Microsoft Windows, en todas sus versiones

Descripción:

Se ha observado en los últimos tiempos nuevas víctimas del Ramsonware Revil en países latinoamericanos, dejando paralizadas las operaciones de importantes organizaciones, causando millonarias pérdidas, daños a la imagen, entre otros.

Es importante conocer detalladamente el funcionamiento de esta infección maliciosa, de modo a tomar las medidas de precaución necesarias, a fin de evitar su replicación.

Recordemos que el ransomware es un **malware** o **código malicioso** que tiene como objetivo cifrar los datos de la computadora de la víctima impidiendo el acceso y solicitando un pago de “**rescate**” generalmente en **bitcoins**.

Casos recientes en donde se puede ver aparición de los **ransomware como servicio** o **RaaS (Ransomware as a Service)**, “servicios” que permiten a cualquier persona u organización con intenciones maliciosas, adquirir un ransomware a través de medios ilícitos. Esto con el objetivo de realizar ataques de encriptación y robo de archivos contra los objetivos de su elección.

Ransomware REvil

REvil o también conocido como **Sodinokibi** es un ransomware que sigue el **modelo RaaS,** reconocido como la evolución del **malware GandCrab** y detectado por primera vez en el año 2019 (según: infradata.com). Este malware, primeramente intenta

obtener privilegios en el sistema mediante la explotación de vulnerabilidades conocidas, seguidamente recopila datos confidenciales del sistema y de la sesión del usuario para finalmente realizar el cifrado de los datos.

Además, este ransomware recurre a diferentes técnicas de ofuscación de código, esto para dificultar su análisis e identificación por parte de los programas de antivirus o sistemas de detección de intrusos, volviéndolo una gran amenaza, ya que podría pasar desapercibido ante dichos controles.

Principales técnicas empleadas para la distribución de este ransomware y/o variantes son:

- Envío de correos electrónicos con archivos maliciosos adjuntos (archivos como ZIP, RAR, Javascript, PDF, ejecutables .exe, entre otros) mediante campañas de phishing;
- Por medio de **publicidad maliciosa** o **malvertising**, es decir, código malicioso presente en anuncios que aparecen durante la navegación web, ejecutados directamente en la computadora para redirigir a servidores donde serán descargados otros ejecutables;
- Ataques de fuerza bruta al protocolo **RDP (Remote Desktop Protocol)**;
- La explotación de la vulnerabilidad identificada con el **CVE-2019-2725**, la cual afecta a **Oracle Weblogic Server** en sus versiones 10.3.6.0 y 12.1.3.0 (en el caso específico del ransomware REvil).

Las campañas de distribución detectadas recientemente han sido dirigidas a la búsqueda de software de tarjetas de crédito o puntos de venta (PoS), todo esto utilizando herramientas legítimas, aprovechando **puertas traseras** o **backdoors** de la infraestructura de los servicios como CloudFront, Amazon, Pastebin con el fin de alojar payloads y crear una estructura de servidor **Command & Control (C&C)**, permitiendo que no sean detectados y el tráfico no sea bloqueado por actividad sospechosa.

¿Cómo funciona REvil?

- El archivo ejecutable, es empaquetado de forma personalizada, es decir, todas las cadenas de texto, librerías y **archivos DLL** (librería de enlace dinámico) son empaquetados con el **algoritmo criptográfico RC4** con una clave aleatoria diferente y de longitud variable para cada uno de los elementos.

- Toda esta información anteriormente mencionada, es completamente cifrada en tiempo de ejecución utilizando el **hash** de la cadena, en lugar de la propia cadena para dificultar aún más la detección, a todo esto se le suma también que en la estructura de datos no es posible reconocer el tamaño de las claves ni de los datos, haciendo que programas de descifrados por medios automatizados no se puedan o resulten difíciles de ser utilizados.

- Una vez ejecutado en el sistema lo primero que realiza es generar un **identificador** o **mutex** que sirve para evitar que múltiples procesos ingresen a la vez en la sección crítica, previniendo así posibles fallas.

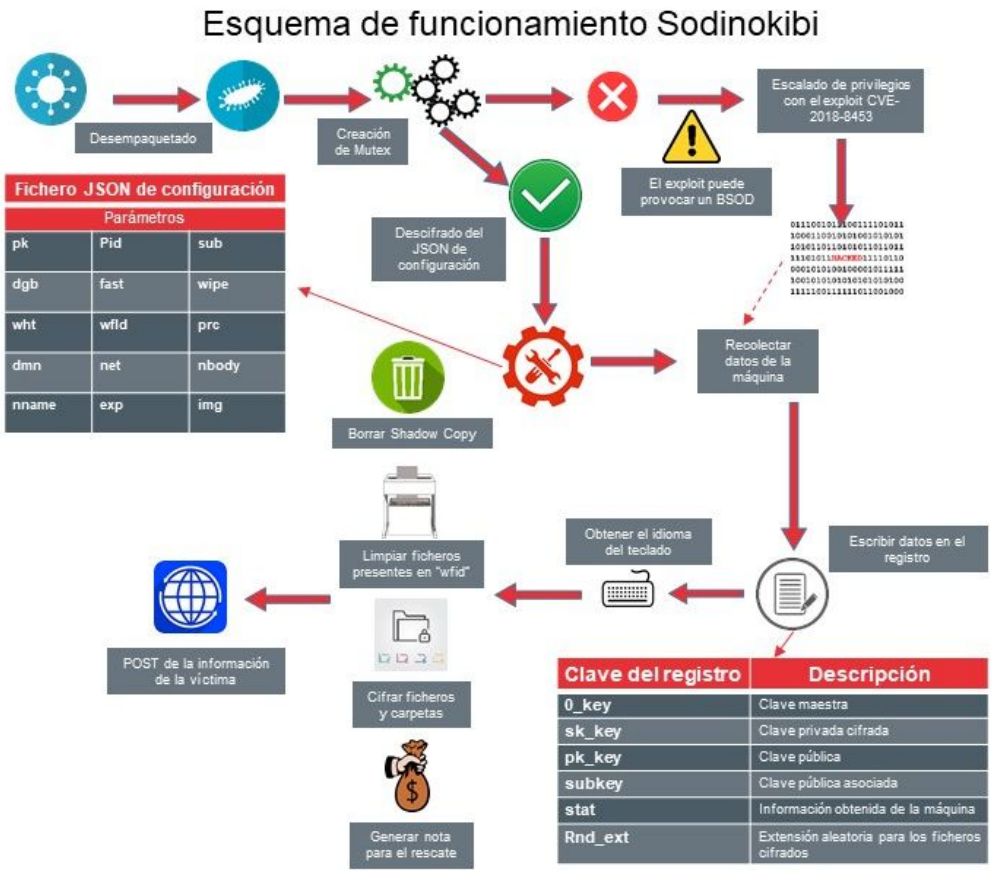
- Lo siguiente es, descifrar la **configuración personalizada** la cual se encuentra en **formato JSON**, esto servirá para dictar las operaciones a realizar, las cuales fueron solicitadas por el "**suscriptor**" o "**comprador**" del servicio.
- Posteriormente, el malware intenta **escalar privilegios** comprobando si el **sistema Windows** es vulnerable al fallo identificado con el **CVE-2018-8453** que afecta al **componente Win32k** de los sistemas Windows 10, Windows 8, Windows 7 y Windows Server 2008, 2012, 2016 y 2019 (con parche de seguridad ya publicado). En caso de que el sistema en cuestión se encuentre parcheado, lo vuelve a intentar mediante la función **RunAS**, esto con el fin de forzar la elevación de privilegios y evitar el **control de cuentas de usuario (UAC)** encargado de prevenir los cambios no autorizados en los sistemas Windows.

- En caso de que no se obtengan los privilegios el programa finaliza y el ataque fracasa, caso contrario, recopila datos sobre la configuración del sistema y de sesión, además de comprobar el idioma del sistema (si coincide con alguno incluido de los excluidos en la configuración JSON, finaliza)

- Seguidamente y si el lenguaje del sistema no coincide con los excluidos, se inutilizan las funciones de restauración del sistema "**Shadow Copy**", desactivando el proceso **vssadmin** y con el comando **bcdedit** se desactivan las copias de seguridad, para luego eliminar todas aquellas que se encuentran almacenadas en el sistema.

- Finalmente, se procede al cifrado de los archivos del sistema añadiendo a los mismos una extensión personalizada asignada durante la compilación del código. Así como también se genera la "**nota de rescate**" en cada directorio donde fueron cifrados los archivos, con el nombre "**[Extensión]-how-to-decrypt.txt**". En este archivo de texto se detallan todas las instrucciones que debe seguir la víctima para descifrar sus archivos, los mensajes conducen a un sitio web (accesible mediante el navegador Tor) en donde se proporciona un descifrador de prueba gratuito para hasta 3 archivos, esto como una "garantía" antes de que se realice el supuesto "pago de rescate", mediante bitcoins.

- Además, durante la ejecución del malware, este realiza la exfiltración de los datos de la víctima. Datos a ser utilizados por los ciberdelincuentes, como un método de extorsión adicional para las víctimas que no acceden al **"pago del rescate"**, con amenazas de que serán puestos en venta a potenciales competidores o publicados directamente en internet.



Fuente: INCIBE-CERT

Con ello, el daño de un ransomware puede ir más allá del cifrado de los archivos, lo cual de por sí resulta algo crítico y en especial para una empresa, sino que también existe la posibilidad de que dichos datos potencialmente confidenciales sean revelados al público.

Cabe recalcar que, existen otras familias de ransomware que implementan técnicas similares a la descrita, pero con diferencias en los algoritmos de encriptado u otro aspecto interno del código fuente, ransomwares como **Maze**, **Clop**, **DoppelPaymer, Nefilim, Sekhmet, Robin Hood y Nemty**.

Maze, fue el primero que implementó la metodología de exfiltración de datos en el año 2019, dando hincapié a otras familias de ransomware a aplicar el mismo **modus**

operandi. Hoy en día, afectan a empresas alrededor del mundo ya que el daño no solo se reduce a la pérdida de los archivos almacenados, sino que también a la pérdida de la confidencialidad, reputación y en la mayoría de los casos se interrumpe la actividad normal de la organización.

Sin embargo, lo que resulta preocupante es que, como se trata de un **"servicio"**, muchos de estos malwares cuentan con grupos de ciberdelincuentes que se encargan de administrar, arreglar y mejorar cada vez más la eficacia de los programas, con el dinero recaudado de las **"suscripciones"** y ventas de los datos robados de las víctimas.

Casos recientes

El caso más reciente de infección con el ransomware REvil fue el del **Banco Estado de Chile**, en donde a través de un comunicado de prensa informó que todas las sucursales se encontrarán inoperativas y cerradas mientras solucionan el problema ocurrido y que **"no hubo afectación alguna a los fondos del banco"**.

Además, la empresa de telecomunicaciones **Telecom Argentina** fue también víctima de este ransomware el pasado 18 de julio, en donde los ciberdelincuentes solicitaron un total de **7,5 millones de dólares** en criptomonedas para la recuperación de los archivos extraídos.

El pasado 22 de julio, la **empresa pública Adif**, encargada de la construcción y gestión de líneas de ferrocarril en España sufrió un ciberataque con el ransomware REvil. Los ciberdelincuentes obtuvieron un estimado de **800 GB de información confidencial** de la compañía, además los ciberdelincuentes compartieron parte de la información obtenida en la web oscura o dark web. Entre estos datos se encontraban contratos, facturas, correspondencia privada, números de teléfono y datos de clientes.

Impacto:

El **ransomware REvil**, debido a sus características de cifrado robustas no cuenta con ninguna utilidad o método de solución para descifrar los archivos (hasta el momento). Esto podría generar daños como:

- Pérdida total de datos confidenciales almacenados en el disco duro;
- Interrupción de las actividades regulares, principalmente en negocios o empresas;
- Potenciales pérdidas financieras para volver a restaurar los sistemas afectados y archivos;
- Daño potencial a la reputación de una organización.

Solución y prevención:

- Es importante realizar **copias de seguridad (backup)** de toda información importante personal o laboral en forma periódica. Mantenga las copias en un dispositivo independiente (disco duro externo, o servicios en la nube). Esto posibilita la recuperación de toda la información de forma rápida y segura ante una infección. Algunas consideraciones para asegurar los backups:
    - Cifrar las copias de seguridad,
    - Comprobar que las copias de seguridad realizadas funcionen.
    - Realizar pruebas de restauración,
    - Contar con diferentes soportes de las copias de seguridad (por ejemplo: un servidor NAS y un disco duro externo),
    - Asegurarse que la ubicación física donde serán almacenadas las copias de seguridad sea confiable y segura, es recomendable el almacenamiento de las mismas en un centro de datos externo.
- Instale soluciones de **antivirus/firewall** y manténgalo actualizado.

- Mantenga el sistema operativo, sistemas o aplicaciones utilizadas con los últimos parches de seguridad aplicados.
- Evite abrir correos electrónicos sospechosos o con archivos adjuntos, tanto si vienen de remitentes conocidos como desconocidos. Antes, asegúrese de que el remitente le está enviando un adjunto, además no ingrese a enlaces dudosos que le son enviados a través de correo electrónico, servicios de mensajería, redes sociales, etc.
- Configurar la conexión al **Escritorio remoto (RDP), SMB o SSH** para que sea accesible sólo desde **Redes Privadas Virtuales** (Virtual Private Network o VPNs), es recomendable también configurar reglas del firewall en el equipo, para que sólo acepte conexiones de los recursos que realmente necesitan conectarse al servicio. Además, configure una contraseña **robusta** para el acceso al recurso, la misma debe contener al menos 10 caracteres, números, letras (minúsculas y mayúsculas) y caracteres especiales.
- Capacitar a los usuarios para que estos puedan conocer las amenazas y las técnicas utilizadas por los ciberdelincuentes, así también cómo protegerse de ellas.
- En caso de una **infección con ransomware**, se recomienda:
    - Desconectar el dispositivo de la **red**, para evitar la propagación.
    - Identificar el tipo y la **familia** del ransomware mediante la extensión de los archivos encriptados o la “nota de rescate”, a modo de buscar alguna posible solución (en caso de que exista) en sitios como **No More Ransom**.
    - **No pagar** el rescate. Nada le asegura que los archivos serán devueltos por los delincuentes, esto podría ocasionar que los ciberdelincuentes ejecuten ataques adicionales al dispositivo y continuar con la extorsión, además estaría financiando a estos ciberdelincuentes con el pago del **“rescate”**.

- Evite descargar **desencriptadores** de páginas no oficiales o no confiables, ya que existen familias de ransomware que se distribuyen a través de desencriptadores falsos.
- En caso de ser víctima de ransomware, puede reportar el incidente al CERT-PY, enviando un correo a abuse@cert.gov.py para recibir ayuda adicional.

Información adicional:

- https://www.incibe-cert.es/blog/sodinokibi-caracteristicas-y-funcionamiento
- https://www.incibe-cert.es/blog/sodinokibi-prevencion-identificacion-y-respuesta
- https://www.infradata.com/resources/what-is-revil-ransomware/
- https://www.proficio.com/doppelpaymer-ransomware/
- https://blog.malwarebytes.com/threat-spotlight/2020/05/maze-the-ransomware-that-introduced-an-extra-twist/
- https://www.pcrisk.es/guias-de-desinfeccion/9153-sodinokibi-ransomware
- https://www.trendtic.cl/2020/09/banco-estado-ransomware-sodinokibi-seria-el-responsable-del-cierre-de-sucursales-y-csirt-del-gobierno-mantiene-alerta-cibernetica-alta/
- https://www.welivesecurity.com/la-es/2020/05/29/ransomware-filtracion-informacion-tendencia-consolido-2020/
- https://unaaldia.hispasec.com/2020/07/ciberataque-a-telecom-argentina.html