Se ha descubierto una nueva variante de la familia de ransomware Vega, denominada Zeppelin, explotada en la naturaleza y en las compañías de atención médica en Europa, Estados Unidos y Canadá.

Sin embargo, lugares como Rusia, Ucrania, Bielorrusia y Kazajistán, no se ven afectados, ya que el ransomware termina sus operaciones si se encuentra en máquinas ubicadas en esos lugares.

Esto hay llamado la atención, ya que todas las variantes anteriores de la familia Vega, también conocida como VegaLocker, apuntaban principalmente a usuarios rusos, lo que indica que Zeppelin no es el trabajo del mismo grupo de pirateo detrás de los ataques anteriores.

Debido a que el ransomware Vega y sus variantes anteriores se ofrecieron como un servicio en foros subterráneos, los investigadores de BlackBerry Cylance creen que Zeppelin *«terminó en manos de diferentes actores de amenazas o reconstruido de fuentes compradas, robadas o filtradas».*

Según un informe de BlackBerry Cylance, Zeppelin es un ransomware altamente configurable basado en Delphi, que se puede personalizar fácilmente para habilitar o deshabilitar distintas funciones, según las víctimas o los requisitos de los atacantes.

Zeppelin puede implementarse como un EXE, DLL o incluirse en un cargador de PowerShell e incluye las siguientes características:

- IP Logger: Rastrea las direcciones IP y la ubicación de las víctimas
- Inicio: Para ganar persistencia
- Eliminar copias de seguridad: Para detener ciertos servicios, deshabilitar la recuperación de archivos, eliminar copias de seguridad e instantáneas, etc.
- Task Killer: Elimina los procesos especificados por el atacante
- Desbloqueo automático: Para desbloquear archivos que parecen bloqueados durante el cifrado

- Melt: Para inyectar subproceso de eliminación automática en notepad.exe
- Mensaje de UAC: Intenta ejecutar el ransomware con privilegios elevados

Basado en las configuraciones establecidas por los atacantes desde la interfaz de usuario del constructor Zeppelin durante la generación del binario ransomware, el malware enumera los archivos en todas las unidades y los recursos compartidos de red y los cifra con el mismo algoritmo utilizado por las otras variantes de Vega.

> *«Zeppelin emplea una combinación estándar de cifrado simétrico de archivos con claves generadas aleatoriamente para cada archivo (AES-256 en modo CBC), y cifrado asimétrico utilizado para proteger la clave de sesión (utilizando una implementación RSA personalizada, posiblemente desarrollada internamente)»,* dijeron los investigadores.
>
> *«Curiosamente, algunas de las muestras cifrarán solo los primeros 0x1000 bytes (4KB), en lugar de 0x10000 (65KB). Puede ser un error no intencionado o una elección consciente para acelerar el proceso de cifrado mientras que la mayoría de los archivos quedan inutilizables»*, agregaron.

Además de las características que se habilitarán y los archivos que se cifrarán, el constructor Zeppelin también permite a los atacantes configurar el contenido del archivo de texto de la nota de rescate, que se coloca en el sistema y se muestra a la víctima luego de cifrar los archivos.

> *«Los investigadores de BlackBerry Cylance descubrieron varias versiones diferentes, que van desde mensajes breves y genéricos hasta notas de rescate más elaboradas y adaptadas a organizaciones individuales»*, dicen los investigadores.

> *«Todos los mensajes indican a la víctima que se comunique con el atacante por medio de una dirección de correo electrónico proporcionada y que indique su número de identificación personal»,* agregaron.

Para evadir la detección, el ransomware Zeppelin se basa en distintas capas de ofuscación, incluido el uso de claves pseudoaleatorias, cadenas encriptadas, que utilizan códigos de diferentes tamaños, así como retrasos en la ejecución para escapar de las sandbox y engañar a los mecanismos heurísticos.

Zeppelin fue descubierto por primera vez hace casi un mes, cuando se distribuyó a través de sitios web con agujeros de agua con sus cargas útiles PowerShell alojadas en el sitio web de Pastebin.

Los investigadores creen que al menos algunos de los ataques de Zeppelin se llevaron a cabo por medio de MSSP, que tendrían similitudes con otra campaña reciente altamente dirigida que utilizó el ransomware llamado Sodinokibi, también conocido como Sodin o REvil.

Los investigadores también compartieron indicadores de compromiso (IoC) en su publicación de blog. Hasta ahora, casi el 30% de las soluciones antivirus no pueden detectar esta amenaza particular de ransomware.