Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°017	Fecha: 19-01-2024
		Página: 4 de 13

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Se abusa de Teamviewer para violar redes en nuevos ataques de Ransomware		
Tipo de Ataque	Ransonware	Abreviatura	Ransonware
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**:

Los actores de ransomware están utilizando nuevamente TeamViewer para obtener acceso inicial a los puntos finales de la organización e intentar implementar cifradores basados en el creador de ransomware LockBit filtrado.

TeamViewer es una herramienta legítima de acceso remoto utilizada ampliamente en el mundo empresarial, valorada por su simplicidad y capacidades.

La herramienta también es apreciada por estafadores e incluso actores de ransomware, que la utilizan para obtener acceso a escritorios remotos, descargando y ejecutando archivos maliciosos sin obstáculos.

Un caso similar se informó por primera vez en marzo de 2016, cuando numerosas víctimas confirmaron que sus dispositivos habían sido vulnerados utilizando TeamViewer para cifrar archivos con el ransomware Surprise.

2. **DETALLES:**

En ese momento, la explicación de TeamViewer para el acceso no autorizado fue el relleno de credenciales, lo que significa que los atacantes no explotaron una vulnerabilidad de día cero en el software, sino que utilizaron las credenciales filtradas de los usuarios.

«Como TeamViewer es un software muy extendido, muchos delincuentes online intentan iniciar sesión con los datos de las cuentas comprometidas para averiguar si existe una cuenta de TeamViewer correspondiente con las mismas credenciales«, explicó entonces el proveedor del software.

«Si este es el caso, es probable que puedan acceder a todos los dispositivos asignados para instalar malware o ransomware«.

Un nuevo informe de Huntress muestra que los ciberdelincuentes no han abandonado estas viejas técnicas y aún se apoderan de los dispositivos a través de TeamViewer para intentar implementar ransomware.

Los archivos de registro analizados (connections_incoming.txt) mostraron conexiones de la misma fuente en ambos casos, lo que indica un atacante común.

En el primer punto final comprometido, Huntress vio en los registros múltiples accesos por parte de los empleados, lo que indica que el personal utilizaba activamente el software para tareas administrativas legítimas.

En el segundo punto final visto por Huntress, que ha estado funcionando desde 2018, no había habido actividad en los registros durante los últimos tres meses, lo que indica que se monitoreaba con menos frecuencia, lo que posiblemente lo hacía más atractivo para los atacantes.

En ambos casos, los atacantes intentaron implementar la carga útil del ransomware utilizando un archivo por lotes de DOS (PP.bat) colocado en el escritorio, que ejecutaba un archivo DLL (carga útil) mediante un comando rundll32.exe.

El ataque al primer punto final tuvo éxito, pero fue contenido. En el segundo, el producto antivirus detuvo el esfuerzo, forzando repetidos intentos de ejecución de la carga útil sin éxito.

Si bien Huntress no ha podido atribuir los ataques con certeza a ninguna banda de ransomware conocida, señalan que es similar a los cifradores LockBit creados utilizando un constructor LockBit Black filtrado.

En 2022, se filtró el creador de ransomware para LockBit 3.0, y las bandas Bl00dy y Buhti lanzaron rápidamente sus propias campañas utilizando el creador.

El constructor filtrado le permite crear diferentes versiones del cifrador, incluido un ejecutable, una DLL y una DLL cifrada que requiere una contraseña para iniciarse correctamente.

Según los IOC proporcionados por Huntress, los ataques a través de TeamViewer parecen estar utilizando la DLL LockBit 3 protegida por contraseña.

Si bien BleepingComputer no pudo encontrar la muestra específica vista por Huntress, encontramos una muestra diferente cargada en VirusTotal la semana pasada.

Esta muestra se detecta como LockBit Black, pero no utiliza la nota de ransomware LockBit 3.0 estándar, lo que indica que fue creada por otra banda de ransomware que utiliza el generador filtrado.

Si bien no está claro cómo los actores de amenazas están tomando el control de las instancias de TeamViewer, la compañía compartió la siguiente declaración BleepingComputer sobre los ataques y la seguridad de las instalaciones.

«En TeamViewer, nos tomamos muy en serio la seguridad y la integridad de nuestra plataforma y condenamos inequívocamente cualquier forma de uso malicioso de nuestro software.

Nuestro análisis muestra que la mayoría de los casos de acceso no autorizado implican un debilitamiento de la configuración de seguridad predeterminada de TeamViewer. Esto a menudo incluye el uso de contraseñas fáciles de adivinar, lo cual sólo es posible utilizando una versión desactualizada de nuestro producto. Enfatizamos constantemente la importancia de mantener prácticas de seguridad sólidas, como el uso de contraseñas complejas, autenticación de dos factores, listas de permitidos y actualizaciones periódicas de las últimas versiones de software. Estos pasos son fundamentales para protegerse contra el acceso no autorizado.

3. RECOMENDACIONES:

- Practicar una higiene estricta de las contraseñas. Utilizar contraseñas únicas y complejas para todas las cuentas y cambiarlas periódicamente.
- Habilitar la autenticación de dos factores cuando esté disponible.
- No hacer clic en enlaces sospechosos ni descargue archivos adjuntos de fuentes desconocidas.
- Ejecutar la estrategia 3-2-1 de copias de seguridad, que consiste en realizar tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Mantener siempre actualizado los programas, tanto en los dispositivos como en los servidores, para evitar que los atacantes aprovechen las vulnerabilidades y se infiltren en su red.
- Utilizar un software antivirus confiable y mantenerlo activo y actualizado.
- Centrar la estrategia de defensa en la detección de movimientos laterales y el bloqueo de actividades fraudulentas de transferencia de datos confidenciales a Internet (fuga de informaciones). Es importante prestar especial atención al tráfico saliente para detectar las conexiones de los ciberdelincuentes en su red.
- Procurar la gestión de un plan que incluya detección, investigación y respuesta a amenazas 24/7, ya sea internamente o en asociación con un proveedor especializado de servicios de detección y respuesta gestionadas.
- 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://blog.ehcgroup.io/2024/01/19/14/45/32/16505/se-abusa-de-teamviewer-para-violar-redes-en-nuevos-ataques-de-ransomware/seguridad-informatica/ransonware/ehacking/ • https://www.bleepingcomputer.com/news/security/teamviewer-abused-to-breach-networks-in-new-ransomware-attacks/#google_vignette