Los dispositivos VPN de Fortinet sin parches han sido objetivo de una serie de ataques contra empresas industriales en Europa, con el fin de implementar una nueva cepa de ransomware llamada Cring, dentro de las redes corporativas.

Por lo menos uno de los incidentes de piratería provocó el cierre temporal de un sitio de producción, dijo la compañía de ciberseguridad Kaspersky en un informe publicado el miércoles, sin nombrar públicamente a la víctima.

Los ataques cibernéticos ocurrieron en el primer trimestre de 2021, entre enero y marzo.

> *«Varios detalles del ataque indican que los atacantes analizaron cuidadosamente la infraestructura de la organización objetivo y prepararon su propia infraestructura y conjunto de herramientas basándose en la información recopilada en la etapa de reconocimiento»,* dijo Vyacheslav Kopeytsev, investigador de seguridad de Kaspersky ICS CERT.

La divulgación se produce días después de que la Oficina Federal de Investigaciones (FBI) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), advirtieran sobre los actores de amenazas persistentes avanzadas (APT) que escanean activamente dispositivos VPN de Fortinet SSL vulnerables a CVE-2018-13379, entre otras.

> *«Los actores de APT pueden usar estas vulnerabilidades u otras técnicas de explotación comunes para obtener acceso inicial a múltiples servicios gubernamentales, comerciales y tecnológicos. El acceso inicial posiciona a los actores de APT para llevar a cabo ataques futuros»*, dijo la agencia.

CVE-2018-13379 se refiere a una vulnerabilidad de recorrido de ruta en el portal web FortiOS

SSL VPN, que permite a atacantes no autenticados leer archivos de sistema arbitrarios, incluido el archivo de sesión, que contiene nombres de usuario y contraseñas almacenados en texto sin formato.

Aunque los parches para la vulnerabilidad se lanzaron en mayo de 2019, Fortinet dijo en noviembre pasado que identificó una «*gran cantidad*» de dispositivos VPN que permanecían sin parche, al mismo tiempo que advirtió que las direcciones IP de esos dispositivos vulnerables conectados a Internet se estaban vendiendo en la web oscura.

Los ataques dirigidos a empresas europeas no fueron diferentes, según la respuesta a incidentes de Kaspersky, que descubrió que el despliegue del ransomware Cring implicaba la explotación de CVE-2018-13379 para obtener acceso a las redes objetivo.

> *«Algún tiempo antes de la fase principal de la operación, los atacantes realizaron conexiones de prueba a la puerta de enlace VPN, aparentemente para asegurarse de que las credenciales de usuario robadas para la VPN todavía fueran válidas»,* dijeron los investigadores de Kaspersky.

Al obtener acceso, se dice que los adversarios utilizaron la utilidad Mimikatz para desviar las credenciales de la cuenta de los usuarios de Windows que habían iniciado sesión previamente en el sistema comprometido, luego utilizarlas para ingresar a la cuenta del administrador del dominio, moverse lateralmente a través de la red, y finalmente, implementar el ransomware Cring en cada máquina remotamente utilizando el marco Cobalt Strike.

Cring, una cepa incipiente que fue observada por primera vez en enero de 2021 por el proveedor de telecomunicaciones Swisscom, cifra archivos específicos en los dispositivos utilizando algoritmos de cifrado fuertes después de eliminar los rastros de todos los archivos de respaldo y finalizar los procesos de Microsoft Office y Oracle Database. Después del cifrado exitoso, suelta una nota de rescate exigiendo el pago de dos bitcoins.

Además, los hackers responsables de la amenaza tuvieron cuidad de ocultar su actividad al disfrazar los scripts de PowerShell maliciosos con el nombre de «kaspersky» para evadir la detección y se aseguró de que el servidor que alojaba la carga útil del ransomware solo respondiera a las solicitudes provenientes de países europeos.

> *«Un análisis de la actividad de los atacantes demuestra que, basándose en los resultados del reconocimiento realizado en la red de la organización atacada, optaron por cifrar los servidores que los atacantes creían que causarían el mayor daño a las operaciones de las empresas si se perdían»*, dijo Kopeytsev.

Actualización

Fortinet se comunicó con Masterhacks para ofrecer su versión sobre el tema y mencionar las formas de mitigación para los usuarios que aún no aplican parches:

"La seguridad de nuestros clientes es nuestra prioridad. CVE-2018-13379 es una vulnerabilidad antigua resuelta en mayo de 2019. Al conocerse, Fortinet emitió de forma inmediata un aviso PSIRT, se comunicó directamente a los clientes y se publicó en el blog corporativo en múltiples ocasiones – agosto de 2019, julio de 2020 y de nuevo en abril de 2021 – recomendando encarecidamente realizar la actualización correspondiente. Tras su resolución, hemos mantenido informados a nuestros clientes hasta abril de 2021. CVE-2019-5591 fue solucionado en julio de 2019 y CVE-2020-12812 en julio de 2020. Instamos a aquellos clientes no lo han hecho todavía a implementar de forma inmediata la actualización y las mitigaciones. Para obtener más información, visite nuestro blog y consulte inmediatamente el aviso de mayo de 2019"