La Agencia de Seguridad e Infraestructura y Ciberseguridad de Estados Unidos (CISA) y la Oficina Federal de Investigaciones (FBI), emitieron este miércoles una advertencia conjunta sobre la explotación activa de vulnerabilidades en los productos locales de Microsoft Exchange por parte de actores estatales y ciberdelincuentes.

> *«El CISA y el FBI evalúan que los adversarios podrían explotar estas vulnerabilidades para comprometer redes, robar información, cifrar datos para obtener un rescate o incluso ejecutar un ataque destructivo. Los adversarios también pueden vender acceso a redes comprometidas en la web oscura»,* dijeron las agencias.

Los ataques se han dirigido principalmente a gobiernos locales, instituciones académicas, organizaciones no gubernamentales y entidades comerciales en varios sectores de la industria, incluida la agricultura, la biotecnología, la industria aeroespacial, la defensa, los servidores legales, los servicios públicos de energía y la farmacéutica, que las agencias dicen que están en línea con actividad previa realizada por ciber actores chinos.

Se cree que decenas de miles de entidades, incluyendo la Autoridad Bancaria Europea y el Parlamento Noruego, han sido violadas para instalar una puerta trasera basada en la web llamada China Chopper web shell, que brinda a los atacantes la capacidad de robar las bandejas de entrada de correo electrónico y acceder remotamente a los sistemas objetivos.

El desarrollo se produce conforme a la rápida expansión de los ataques dirigidos a servidores Exchange vulnerables, con múltiples actores de amenazas explotando las vulnerabilidades desde el 27 de febrero antes de que finalmente fueran parcheados por Microsoft la semana pasada, convirtiendo rápidamente lo que se etiquetó como *«limitado y dirigido»* en una campaña de explotación masiva indiscriminada.

Aunque no existe una explicación concreta para la explotación generalizada por parte de tantos grupos diferentes, se especula que los adversarios compartieron o vendieron código de explotación, lo que provocó que otros grupos pudieran abusar de las vulnerabilidades, o

que los grupos obtuvieron la explotación de un vendedor común.

El 2 de marzo de 2021, Volexity reveló públicamente la detección de múltiples exploits de día cero utilizados para detectar fallas en las versiones locales de los servidores Microsoft Exchange, al mismo tiempo que registró la primera actividad de explotación en estado salvaje el 3 de enero de 2021.

Al utilizar exitosamente las vulnerabilidades, llamando al ataque conjunto como ProxyLogon, permite que un atacante acceda a los servidores Exchange de las víctimas, lo que les permite obtener acceso persistente al sistema y control de una red empresarial.

Aunque Microsoft inicialmente atribuyó las intrusiones a Hafnium, un grupo de amenazas que se considera patrocinado por el estado y que opera fuera de China, la compañía eslovaca de seguridad cibernética ESET dijo el miércoles que identificó no menos de 10 actores de amenazas distintos, que probablemente se aprovecharon de las fallas de ejecución remota de código para instalar implantes maliciosos en los servidores de correo electrónico de las víctimas.

Además de Hafnium, los cinco grupos detectados que explotan las vulnerabilidades antes del lanzamiento del parche son Tick, LuckyMouse, Calypso, Websiic y Winnti (también conocido como APT41 o Barium), con otros cinco (Tonto Team, ShadowPad, Opera Cobalt Strike, Mikroceen y DLTMiner) escaneando y comprometiendo los servidores de Exchange en los días inmediatamente posteriores al lanzamiento de las correcciones.

Hasta ahora no existe evidencia concluyente que conecte la campaña con China, pero el investigador de seguridad senior de Domain Tools, Joe Slowik, dijo que varios de los grupos mencionados anteriormente han estado vinculados a actividades patrocinadas por China, incluyendo Tick, LuckyMouse, Calypso, Tonto Team, Mikroceen y Winnti, lo que indica que las entidades chinas distintas de Hafnium están vinculadas a la actividad de explotación de

Exchange.

> *«Parece claro que hay numerosos grupos que aprovechan las vulnerabilidades, los grupos están utilizando escaneo masivo o servicios que les permiten apuntar de forma independiente a los mismos sistemas y, finalmente, existen múltiples variaciones del código que se descartan, lo que puede ser indicativo de iteraciones del ataque»,* dijo el equipo de inteligencia de amenazas de la Unidad 42 de Palo Alto Networks.

En un grupo rastreado como «*Paloma Zafiro*«, por investigadores de Red Canary, los atacantes lanzaron múltiples proyectiles web sobre algunas víctimas en diferentes momentos, algunos de los cuales se desplegaron días antes de realizar la actividad de seguimiento.

Según el análisis de telemetría de ESET, se dice que más de 5000 servidores de correo electrónico pertenecientes a empresas y gobiernos de más de 115 países se han visto afectados por actividades maliciosas relacionadas con el incidente.

Por su parte, el Instituto Holandés de Divulgación de Vulnerabilidades (DIVD), informó el martes que encontró 46,000 servidores de 260,000 en todo el mundo que no estaban parcheados contra las vulnerabilidades de ProxyLogon.

Algo que resulta muy preocupante, es que la evidencia apunta al hecho de que el despliegue de los shells web aumentó después de la disponibilidad del parche el 2 de marzo, lo que aumenta la posibilidad de que entidades adicionales hayan intervenido de forma oportunista para crear exploits mediante la ingeniería inversa de actualizaciones de Microsoft como parte de múltiples campañas independientes.

> *«El día después del lanzamiento de los parches, comenzamos a observar a muchos más actores de amenazas escaneando y comprometiendo servidores Exchange en*

> *masa. Curiosamente, todos ellos son grupos APT centrados en el espionaje, excepto uno atípico que parece estar relacionado con una conocida campaña de minería de monedas (DLTminer). Aún no está claro cómo ocurrió la distribución del exploit, pero es inevitable que cada vez más los actores de amenazas, incluidos los operadores de ransomware, tendrán acceso tarde o temprano»*, dijo Matthieu Faou, investigador de ESET.

Además de instalar el shell web, otros comportamientos relacionados o inspirados en la actividad de Hafnium incluyen la realización de reconocimientos en entornos de víctimas mediante la implementación de scripts por lotes que automatizan varias funciones como la enumeración de cuentas, la recolección de credenciales y el descubrimiento de redes.

PoC pública disponible

Para complicar aún más las cosas, está disponible lo que parece ser el primer exploit público funcional de prueba de concepto (PoC) para las vulnerabilidades de ProxyLogon a pesar de los intentos de Microsoft de eliminar los exploits publicados en GitHub durante los últimos días.

> *«He confirmado que existe una PoC pública flotando alrededor de la RCE plena explotación de la cadena. Tiene un par de errores, pero con algunas correcciones pude instalar el shell en mi caja de prueba»,* dijo el investigador de seguridad Marcus Hutchins.

Junto con el lanzamiento de la PoC también se encuentra una descripción técnica detallada de los investigadores de Praetorian, quienes realizaron ingeniería inversa de CVE-2021-26855 para construir un exploit de extremo a extremo completamente funcional identificando las diferencias entre las versiones vulnerables y parcheadas.

Aunque los investigadores decidieron deliberadamente omitir los componentes críticos de

PoC, el desarrollo también generó preocupaciones de que la información técnica podría acelerar más el desarrollo de un exploit funcional, lo que a su vez desencadenó más actores de amenazas para lanzar sus propios ataques.

A medida que la línea de tiempo del hackeo en expansión cristaliza lentamente, lo que está claro es que la oleada de infracciones contra Exchange Server parece haber ocurrido en dos fases, con Hafnium utilizando la cadena de vulnerabilidades para atacar a los objetivos de forma sigilosa ilimitadamente, antes de que otros hackers comenzaran a impulsar la actividad de escaneo a partir del 27 de febrero.

El periodista de seguridad cibernética Brian Krebs, atribuyó esto a la perspectiva de que *«diferentes grupos de ciberdelincuentes se enteraron de algún modo de los planes de Microsoft de enviar soluciones para las fallas de Exchange una semana antes de lo que esperaban».*

> *«El mejor consejo para mitigar las vulnerabilidades reveladas por Microsoft es aplicar los parches relevantes. Sin embargo, dada la velocidad con la que los adversarios utilizaron estas vulnerabilidades como armas y el extenso período de tiempo previo a la divulgación cuando se explotaron activamente, es probable que muchas organizaciones necesiten realizar actividades de respuesta y reparación para contrarrestar las intrusiones existentes»,* dijo Slowik.

Actualización

Microsoft elimina la PoC de GitHub creando controversia entre los investigadores de seguridad cibernética, al mismo tiempo que los hackers están propagando ransomware al explotar las vulnerabilidades de ProxyLogon.