Microsoft lanzó parches de emergencia para corregir cuatro vulnerabilidades no reveladas anteriormente en Exchange Server, que según la compañía, están siendo explotadas activamente por un nuevo actor de amenazas patrocinado por el estado chino con el objetivo de robar datos.

El Centro de Inteligencia de Amenazas de Microsoft (MSTIC), describió los ataques cibernéticos como *«limitados y dirigidos»,* agregando que el adversario utilizó estas vulnerabilidades para acceder a los servidores de Exchange locales, lo que a su vez otorgó acceso a cuentas de correo electrónico y allanó el camino para la instalación de malware adicional para facilitar el acceso a largo plazo a los entornos de las víctimas.

La compañía atribuyó principalmente la campaña a un actor de amenazas llamado HAFNIUM, un colectivo de hackers patrocinado por el estado que opera desde China, aunque sospecha que otros grupos también pueden estar involucrados.

Al discutir las tácticas, técnicas y procedimientos (TTP) del grupo por primera vez, Microsoft describió a HAFNIUM como un *«actor altamente calificado y sofisticado»,* que destaca principalmente a entidades en Estados Unidos por exfiltrar información confidencial de una variedad de sectores de la industria, incluyendo investigadores de enfermedades infecciosas, bufetes de abogados, instituciones de educación superior, contratistas de defensa, grupos de expertos en políticas y ONG.

Se cree que HAFNIUM organiza sus ataques al aprovechar los servidores privados virtuales alquilados en Estados Unidos, como un intento por encubrir su actividad maliciosa.

El ataque de tres etapas implica obtener acceso a un servidor Exchange, ya sea con contraseñas robadas o mediante el uso de vulnerabilidades no descubiertas previamente, seguido de la implementación de un shell web para controlar el servidor comprometido de forma remota.

El último eslabón de la cadena de ataque utiliza el acceso remoto para robar los buzones de correo de la red de una organización y exportar los datos recopilados a sitios para compartir

archivos, como MEGA o Mediafire.

Para poder lograrlo, se utilizan hasta cuatro vulnerabilidades de día cero, descubiertas por investigadores de Volexity y Dubex, como parte de la cadena de ataque:

- CVE-2021-26855: Vulnerabilidad de falsificación de solicitud del lado del servidor (SSRF) en Exchange Server.
- CVE-2021-26857: Vulnerabilidad de deserialización insegura en el servicio de mensajería unificada.
- CVE-2021-26858: Vulnerabilidad de escritura de archivo arbitrario posterior a la autenticación en Exchange.
- CVE-2021-27065: Vulnerabilidad de escritura de archivo arbitrario posterior a la autenticación en Exchange.

Aunque las vulnerabilidades afectan a Microsoft Exchange Server 2013, 2016 y 2019, Microsoft afirmó que está actualizando Exchange Server 2010 para fines de *«Defensa en profundidad».*

Además, debido a que el ataque inicial requiere una conexión no confiable al puerto 443 del servidor Exchange, la compañía señala que las organizaciones pueden mitigar el problema restringiendo las conexiones no confiables o utilizando una VPN para separar el servidor Exchange del acceso externo.

Microsoft enfatizó que los exploits no están relacionados con las vulnerabilidades de SolarWinds, pero dijo que informó a las agencias gubernamentales apropiadas de Estados Unidos sobre la nueva ola de ataques, pero la compañía no brindó más detalles sobre cuántas organizaciones fueron atacadas.

Al afirmar que las campañas de intrusión parecían haber comenzado alrededor del 6 de enero de 2021, Volexity advirtió que detectó una explotación activa de múltiples vulnerabilidades de Microsoft Exchange utilizadas para robar correo electrónico y comprometer redes.

> *«Mientras que los atacantes parecen haber volado inicialmente en gran parte bajo el radar con el simple robo de correos electrónicos, recientemente giran a lanzar exploits para hacerse un hueco»,* dijeron los investigadores de Volexity, Josh Grünzweig, Matthew Meltzer, Sean Koessel, Steven Adair y Thomas Lancaster.
>
> *«Desde la perspectiva de Volexity, esta explotación parece involucrar a múltiples operadores que utilizan una amplia variedad de herramientas y métodos para descargar credenciales, moverse lateralmente y otros sistemas de puerta trasera»,* agregaron.

Aparte de los parches, el analista senior de inteligencia de amenazas de Microsoft, Kevin Beaumont, también creó un complemento nmap que se puede utilizar para escanear una red en busca de servidores de Microsoft Exchange potencialmente vulnerables.

Debido a la gravedad de las vulnerables, los parches se implementaron hasta una semana antes de la programación del martes de parches de la compañía, que generalmente se reserva para el segundo martes de cada mes. Se recomienda a los clientes que utilicen una versión vulnerable de Exchange Server que instalen las actualizaciones inmediatamente.

> *«Aunque hemos trabajado rápidamente para implementar una actualización para las vulnerabilidades de HAFNIUM, sabemos que muchos actores estatales y grupos criminales se moverán rápidamente para aprovechar cualquier sistema sin parches. La aplicación inmediata de los parches actuales es la mejor protección contra el ataque»,* dijo Tom Burt, vicepresidente corporativo de seguridad del cliente de Microsoft.