Unas horas después de las noticias enviadas por agencias de inteligencia e investigadores de seguridad cibernética acerca de los servidores Exchange sin parches podrían abrir el camino para infecciones de ransomware a raíz de la rápida escalada de ataques desde la semana pasada, los hackers se han puesto al día.

Según los últimos informes, los hackers están aprovechando las fallas de ProxyLogon Exchange Server, bastante explotadas, para instalar una nueva variedad de ransomware denominada DearCry.

> *«Microsoft observó una nueva familia de clientes de ataques de ransomware operados por humanos, detectados como Ransom: Win32/DoejoCrypt.A». Los ataques de ransomware operados por humanos están utilizando las vulnerabilidades de Microsoft Exchange para explotar a los clientes»,* dijo el investigador de Microsoft, Phillip Misner.

El equipo de inteligencia de seguridad de Microsoft, confirmó en Twitter por separado que comenzó a *«bloquear una nueva familia de ransomware que se utiliza después de un compromiso inicial de los servidores Exchange locales sin parches».*

La compañía de seguridad Kryptos Logic dijo que identificó alrededor de 6970 web shells expuestos, algunos de los cuales se utilizaron para infectar los servidores comprometidos con el ransomware DearCry, lo que sugiere que otros grupos de ciberdelincuentes están aprovechando la puerta trasera de la web shell de primera etapa que el actor de amenazas de Hafnium instaló para agregar malware de su elección.

Al llamar a DearCry un ransomware de «copia», el director de Sophos, Mark Loman, dijo que la cepa crea copias cifradas de los archivos atacados utilizando una clave de cifrado incrustada en el binario del ransomware y elimina las versiones originales, lo que permite a las víctimas *«potencialmente recuperar algunos datos»* debido a este comportamiento de cifrado.

> *«Los defensores deben tomar medidas urgentes para instalar los parches de Microsoft para evitar la explotación de sus parches de Microsoft Exchange. Si esto no es posible, el servidor deben desconectarse de Internet o ser monitoreado de cerca por un equipo de respuesta a amenazas»,* dijo Loman.

En un aviso conjunto publicado por la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) y la Oficina Federal de Investigaciones (FBI), las agencias advirtieron que *«los adversarios podrían explotar estas vulnerabilidades para comprometer redes, robar información, cifrar datos para pedir un rescate o ejecutar un ataque destructivo».*

El armamento exitoso de las vulnerabilidades permite a un hacker acceder a los servidores Exchange de las víctimas, lo que les permite obtener acceso persistente al sistema y control de una red empresarial. Con la nueva amenaza de ransomware, los servidores no parcheados no solo corren el riesgo de un posible robo de datos, sino que también se cifran potencialmente, lo que impide el acceso a los buzones de correo de una organización.

Eliminan PoC de GitHub

Mientras tanto, conforme los hackers y los ciberdelincuentes del estado nacional se acumulan para aprovechar las vulnerabilidades de ProxyLogon, la compañía ha eliminado un código de prueba de concepto (PoC) compartido en GitHub, propiedad de Microsoft, por un investigador de seguridad, citando que el exploit está bajo ataque activo.

En una declaración a Vice, la compañía dijo: *«De acuerdo con nuestras políticas de uso aceptable, desactivamos la esencia después de los informes de que contiene un código de prueba de concepto para una vulnerabilidad recientemente revelada que se está explotando activamente».*

La medida también provocó un debate propio, con investigadores que argumentan que Microsoft está *«silenciando a los investigadores de seguridad»* al eliminar las PoC

compartidas en GitHub.

> *«Esto es enorme, eliminar un código de investigadores de seguridad de GitHub contra su propio producto y que ya ha sido parcheado. Fue un PoC, no un exploit funcional, ninguno de los PoC ha tenido el RCE. Incluso si lo tuviera, ese no es un llamado cuando es el momento apropiado para el lanzamiento. Es un problema en su propio producto, y están silenciando investigadores de seguridad en eso»,* dijo Dave Kennedy de TrustedSec.

> *«Si la política desde el principio no fuera PoC/Metasploit/etc, eso sería una mierda, pero es un servicio. En cambio, dijeron que estaba bien, y ahora que se ha convertido en el estándar para que los profesionales de la seguridad compartan el código, se han elegido a sí mismos como árbitros de lo es que 'responsable'. Qué conveniente»,* dijo Tavis Normandy, de Google Project Zero.

Un portavoz de Masterhacks está contactando a Microsoft para más noticias acerca de lo sucedido con la eliminación de la PoC en GitHub, por lo que esta noticia se actualizará al tener más detalles.