Después de que la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) lanzara un descifrador para que las víctimas afectadas se recuperaran de los ataques del ransomware ESXiArgs, los hackers vuelven con una versión actualizada que logra cifrar más datos.

Un administrador de sistemas informó sobre la aparición de la nueva variante en un foro en línea, donde otro participante afirmó que los archivos de más de 128 MB tendrán el 50% de sus datos encriptados, lo que hace que el proceso de recuperación sea más desafiante.

Otro cambio notable es la eliminación de la dirección de Bitcoin de la nota de rescate, y los atacantes ahora instan a las víctimas a contactarlos en Tox para obtener la información de la billetera.

Los hackers *«se dieron cuenta de que los investigadores estaban rastreando sus pagos, y es posible que incluso supieran antes de lanzar el ransomware que el proceso de cifrado en la variante original era relativamente fácil de eludir»,* dijo Censys.

Las estadísticas compartidas por la plataforma de colaboración abierta de Ransomwhere revelaron que hasta 1252 servidores fueron infectados por la nueva versión de ESCiArgs hasta el 9 de febrero de 2023, de los cuales 1168 son reinfecciones.

Desde el comienzo del brote de ransomware a inicios de febrero, más de 3800 hosts únicos se han visto comprometidos. La mayoría de las infecciones se encuentran en Francia, Estados Unidos, Alemania, Canadá, Reino Unido, Países Bajos, Finlandia, Turquía, Polonia y Taiwán.

ESXiArgs, como Cheerscrypt y PrideLocker, se basa en el casillero Babuk, cuyo código fuente se filtró en septiembre de 2021. Pero un aspecto crucial que lo diferencia de otras familias de ransomware es la ausencia de un sitio de fuga de datos, lo que indica que no se está ejecutando en un modelo de ransomware como servicio (RaaS).

> *«Los rescates se fijan en poco más de dos bitcoins (47,000 dólares estadounidenses en este momento) y las víctimas tienen tres días para pagar»,* dijo la compañía de seguridad cibernética Intel471.

Aunque inicialmente se sospechó que las intrusiones involucraban el abuso de un error de OpenSLP de dos años y ahora parcheado en VMware ESXi (CVE-2021-21974), se informaron compromisos en dispositivos que tienen el protocolo de descubrimiento de red deshabilitado.

Desde entonces, VMware ha dicho que no ha encontrado evidencia que sugiera que se esté usando una vulnerabilidad de día cero en su software para propagar el ransomware.

Esto indica que los hackers detrás de la actividad pueden estar aprovechando varias vulnerabilidades conocidas en ESXi para su beneficio, por lo que es imperativo que los usuarios se muevan rápidamente para actualizar a la última versión. Los ataques aún no se han atribuido a un actor o grupo de amenazas conocido.

> *«Según la nota de rescate, la campaña está vinculada a un único actor o grupo de amenazas. Los grupos de ransomware más establecidas suelen realizar OSINT en víctimas potenciales antes de realizar una intrusión y establecen el pago del rescate en función del valor percibido»*, dijo Arctic Wolf.

La compañía de seguridad cibernética Rapid7 dijo que encontró 18,581 servidores ESXi con acceso a Internet que son vulnerables a CVE-2021-21974, y agregó que también observó que los atacantes de RansomExx2 apuntan de forma oportunista a los servidores ESXi susceptibles.

> *«Si bien el impacto económico de esta brecha en particular puede parecer bajo, los atacantes cibernéticos siguen afectando a las organizaciones mediante la muerte por miles de cortes»,* dijo Tony Lauro, director de tecnología y estrategia de

> seguridad de Akamai.

> *«El ransomware ESXiArgs es un excelente ejemplo de por qué los administradores de sistemas necesitan implementar parches rápidamente después de que se publiquen, así como de lo lejos que llegarán los atacantes para que sus ataques sean exitosos. Sin embargo, los parches son solo una línea de defensa dependiente».*