Microsoft echa el cierre a 1.400 cuentas proveedoras de ransomware

Según ha informado la multinacional estadounidense en su informe "Cyber Signals", estas cuentas proveedoras de ?ransomware? se dedicaban a la recopilación de credenciales de clientes robadas.

Fuente: CSO COMPUTER HOY

Esta proliferación explica que la Unidad de Crímenes Digitales de Microsoft eliminase más de 531.000 URLs y 5.400 kits de phishing entre julio de 2021 y junio de 2022, lo que llevó a la clausura de más de 1.400 cuentas de correo electrónico maliciosas. El escaso tiempo que los ciberdelincuentes emplean para acceder a los datos personales de un usuario engañado a través de correo electrónico (phishing) también es preocupante, puesto que tardan alrededor de una hora y doce minutos en entrar en sus sistemas. En el caso de las amenazas a los dispositivos informáticos remotos que se comunican a través de endpoints, el tiempo medio que requiere un atacante para comenzar a moverse dentro de una red corporativa es de una hora y cuarenta minutos.

Un hecho relacionado directamente con una de las principales conclusiones del estudio: las compañías han experimentado un aumento del volumen y la sofisticación de los ataques. En esta misma línea, el Informe de Delitos en Internet 2021 impulsado por la Oficina Federal de Investigación de Estados Unidos, avanzaba que el coste de la ciberdelincuencia alcanzó más de 6.900 millones de dólares. Unos datos en consonancia con los ofrecidos por la Agencia de Ciberseguridad de la Unión Europea (ENISA): entre mayo de 2021 y junio de 2022, los ciberdelincuentes, a través del ransomware, robaron unos 10 terabytes (TB) de datos al mes. Además, cabe mencionar que el 58,2% de los archivos robados incluían información personal de los empleados.

Sofisticación de los ataques

En este análisis, la compañía destaca que la especialización y consolidación del cibercrimen han impulsado el ransomware como servicio (RaaS), que se ha convertido en un modelo de negocio dominante. Los programas RaaS, entre los que se encuentran Conti o REvil, ofrecen a los ciberdelincuentes la oportunidad de comprar el acceso tanto a las cargas útiles o del ransomware como a la fuga de datos y a la infraestructura de pago. Estos son utilizados por diferentes actores maliciosos para comercializar con la posibilidad de acceder a las redes y su experiencia. Así, aquellos ciberdelincuentes que no dispongan de los conocimientos necesarios para ejecutar sus ataques, pueden pagar por dichas técnicas y utilizar, entre otras, aplicaciones de pruebas de intrusión y de sistemas.

Ransomware como servicio (RaaS)

La compañía estadounidense con sede en Redmond, Microsoft, ha cerrado un total de 1.400 cuentas de correo maliciosas

utilizadas por los ciberdelincuentes para recopilar las contraseñas robadas de sus clientes a través de ransomware en el último año. Así se desprende de la segunda edición del informe Cyber Signals, un documento desarrollado periódicamente que versa sobre ciberamenazas y que muestra las tendencias en seguridad y ciberdelincuencia. En esta edición, el pliego ofrece una visión sobre la evolución de la extorsión en el cibercrimen.

Irene Iglesias Álvarez

FUENTE: CSO COMPUTER HOY