

El Ransomware Report del 3º trimestre del 2022, revela que este delito informático aumentó un 466% desde 2019, y que está empezando a ser utilizado como precursor de la guerra física

El informe desvela también que una mayoría de equipos de TI y de ciberseguridad no disponen de una visión global de todas las vulnerabilidades de su organización, ni tampoco de un contexto de amenaza suficiente en torno a las que representan un mayor riesgo

Ivanti, el proveedor de la plataforma de automatización Ivanti Neurons, que descubre, gestiona, asegura y da servicio a los activos de TI desde la nube hasta el dispositivo, ha anunciado hoy los resultados del informe Ransomware Report del 3º trimestre del 2022, realizado en colaboración con Cyber Security Works, una autoridad en numeración certificada (CNA) y Cyware, el proveedor líder de Cyber Fusion, SOAR de última generación y soluciones de inteligencia de amenazas. El informe ha revelado que el ransomware aumentó un 466 % desde 2019 y que cada vez se utiliza más como precursor de la guerra física, como se ha puesto de manifiesto en el conflicto de Rusia en Ucrania y en la ciberguerra de Irán y Albania.

Los grupos de ransomware siguen creciendo en volumen y sofisticación, con 35 vulnerabilidades asociadas a este tipo de malware en los tres primeros trimestres de 2022, y 159 explotaciones activas. Para complicar más las cosas, la escasez de datos y el contexto actual de las amenazas está dificultando que las organizaciones parcheen eficazmente sus sistemas informáticos y mitiguen la exposición a la vulnerabilidad.

El informe identificó 10 nuevas familias de ransomware (Black Basta, Hive, BianLian, BlueSky, Play, Deadbolt, H0lyGh0st, Lorenz, Maui y NamPoHyu), lo que representa un total de 170. Con 101 CVEs (Common Vulnerabilities and Exposures, por su siglas en inglés) para el phishing, los atacantes de ransomware confían cada vez más en las técnicas de spear phishing o estafa dirigida a personas, empresas o entidades específicas. Pegasus es un claro ejemplo, en el que bastó un simple mensaje, típico de una ciberestafa, para crear un acceso inicial de backdoor que, unido a las vulnerabilidades del iPhone, provocó la infiltración y la exposición de numerosas personalidades en todo el mundo.

El ransomware necesita de la interacción humana, y es un mito pensar que el phishing es el único vector de ataque. Para conocer con exactitud las tácticas, técnicas y procedimientos que pueden utilizarse para comprometer a una organización, en el marco MITRE ATT&CK se analizaron y mapearon 323 vulnerabilidades de ransomware. El resultado fue que 57 de ellas originaron una toma de control completa del sistema, desde el acceso inicial a la exfiltración.

El estudio desveló también la existencia de dos nuevas vulnerabilidades de ransomware (CVE-2021-40539 y CVE-2022-26134), ambas explotadas por prolíficas familias de este malware como

AvosLocker y Cerber, bien sea antes o el mismo día en que fueron incorporadas a la Base Nacional de Vulnerabilidades (NVD) de Estados Unidos. La investigación incide en que si las organizaciones confían únicamente en la información de la NVD para parchear sus vulnerabilidades, serán susceptibles de sufrir ataques.

Srinivas Mukkamala, director de Producto de Ivanti, afirmó que "Los equipos de TI y de ciberseguridad deben adoptar urgentemente una estrategia basada en el riesgo para la gestión de las vulnerabilidades, con el fin de defenderse mejor contra el ransomware y otras amenazas. Esto pasa por la utilización de tecnologías de automatización, que pueden correlacionar datos de diversas fuentes (es decir, escáneres de red, bases de datos de vulnerabilidad internas y externas, y pruebas de penetración), medir el riesgo, proporcionar alertas tempranas, predecir los ataques y priorizar las actividades de remediación. Las organizaciones que continúen confiando en prácticas tradicionales de gestión de vulnerabilidades, como aprovechar únicamente el NVD y otras bases de datos públicas para priorizar y parchear vulnerabilidades, seguirán corriendo un alto riesgo de ataque cibernético".

El hecho de que los escáneres más conocidos no detecten la totalidad de las vulnerabilidades, es un claro ejemplo de que su gestión debe evolucionar e ir más allá de las prácticas tradicionales. El informe destaca que 18 vulnerabilidades relacionadas con el ransomware no son detectadas por los escáneres más populares.

Aaron Sandeen, director general de Cyber Security Works, lamentó que "produce terror pensar que los escáneres no identifican todas las vulnerabilidades expuestas. Las organizaciones necesitan adoptar una solución de gestión de la superficie de ataque, capaz de descubrir las exposiciones en todos los activos de la organización".

El informe analizó también el impacto del ransomware en las infraestructuras críticas, resultando la sanidad, la energía y la fabricación crítica los tres sectores más afectados. Y reveló que el 47,4 % de las vulnerabilidades del ransomware afectan a los sistemas sanitarios, el 31,6 % a los sistemas energéticos y el 21,1 % a la fabricación crítica.

Anuj Goel, cofundador y CEO de Cyware, explicó que "aunque las estrategias de recuperación tras un incidente han ido mejorando con el tiempo, el viejo dicho de que 'más vale prevenir que curar' sigue siendo válido. Para analizar correctamente el contexto de la amenaza y priorizar eficazmente las acciones de mitigación proactiva, la inteligencia de vulnerabilidad debe llevarse a cabo a través de la orquestación resistente de los procesos de seguridad, con el fin de garantizar la integridad de los activos vulnerables".

El informe ofrece también información sobre las tendencias actuales y futuras del ransomware. Por ejemplo, que el malware con capacidades multiplataforma aumentó su demanda, ya que los operadores de ransomware podían dirigirse fácilmente a varios sistemas operativos a través de una única base de código. Además, identificó un número importante de ataques a terceros, proveedores de soluciones de seguridad y librerías de código de software, lo que supone un número ingente de posibles víctimas. De cara al futuro, y a medida que desaparecen destacados grupos como Conti y DarkSide, las organizaciones verán cómo van surgiendo nuevas bandas de ransomware, que

probablemente reutilizarán o modificarán el código fuente y los métodos de explotación adoptados por los grupos de ransomware desaparecidos.

El Informe se basa en información recogida de diversas fuentes, incluyendo datos propios de Ivanti y CSW, bases de datos de amenazas e investigadores de amenazas y equipos de pruebas de penetración. [Hacer clic aquí para acceder al informe completo.](#)

Sobre Ivanti

Con Ivanti, el trabajo 'desde cualquier lugar es posible. En el teletrabajo, los empleados utilizan un sinfín de dispositivos para acceder a las aplicaciones de TI y a los datos a través de diferentes redes para seguir siendo productivos mientras trabajan desde cualquier lugar. La plataforma de automatización Ivanti Neurons conecta las soluciones líderes del sector de gestión unificada de dispositivos, ciberseguridad y gestión de servicios empresariales, ofreciendo una plataforma de TI unificada que permite a los dispositivos autocurarse y autoprotegerse, capacitando a los usuarios para el autoservicio. Más de 45.000 empresas, entre las que se encuentra 96 de la lista Fortune 100, han confiado en Ivanti para descubrir, gestionar, asegurar y dar servicio a sus activos de TI desde la nube hasta el terminal, ofreciendo excelentes experiencias de usuario final a los empleados, dondequiera y comoquiera que trabajen. Para más información, accede a www.ivanti.com y sigue a @Golvanti.

Sobre Cyware

Cyware ayuda a los equipos de ciberseguridad de las empresas a crear centros de fusión cibernética independientes de la plataforma, ofreciendo soluciones de inteligencia sobre ciberamenazas y SOAR (orquestación, automatización y respuesta de seguridad) de última generación. Como resultado, las empresas pueden aumentar su velocidad y la precisión, al tiempo que reducen los costes y el agotamiento de los analistas. Las soluciones Cyber Fusion de Cyware hacen que la colaboración segura, el intercambio de información y la visibilidad mejorada de las amenazas sean una realidad para los MSSP, las empresas, las agencias gubernamentales y las comunidades de intercambio (ISAC/ISAO/CERTs, entre otros) de todos los tamaños y necesidades. Para más información, accede a www.cyware.com y síguenos LinkedIn y Twitter.

Sobre CSW

CSW es una empresa de servicios de ciberseguridad centrada en la gestión de la superficie de ataque y las pruebas de penetración como servicio. Nuestra innovación en la investigación de vulnerabilidades y exploits nos llevó a descubrir más de 45 días cero en productos tan conocidos como Oracle, D-Link, WSO2, Thembay, Zoho, etc., entre otros. Nos convertimos en una Autoridad de Numeración CVE para permitir la intervención de miles de cazadores de errores y desempeñar un papel fundamental en el esfuerzo global de gestión de vulnerabilidades. Como líder reconocido en la investigación y el análisis de la vulnerabilidad, CSW está a la vanguardia de la ayuda a las empresas de todo el mundo para proteger su negocio de las amenazas en constante evolución. Para más información visite www.cybersecurityworks.com o síganos en LinkedIn y Twitter.

Datos de contacto:

Amparo Torres
AT&A Comunicación
669840176

Nota de prensa publicada en: [Madrid](#)

Categorías: [Comunicación E-Commerce](#) [Ciberseguridad](#)

NotasdePrensa

<https://www.notasdeprensa.es>