Los pagos de ransomware alcanzarán un récord de 1.100 millones de dólares en 2023

Después de una desaceleración en los pagos a bandas de ransomware en 2022, el año pasado los pagos totales de rescates aumentaron a su nivel más alto hasta el momento, según un nuevo informe de la empresa de rastreo de cifrado Chainalysis.

Pila de billetes de dólares estadounidenses

FOTOGRAFÍA: DAVID MUIR/GETTY IMAGES

Hace un año, parecía haber un rayo de esperanza en la larga guerra de desgaste de la industria de la ciberseguridad contra las bandas de ransomware. Al parecer, menos víctimas corporativas de esos piratas informáticos habían pagado rescates en 2022, y los ciberdelincuentes ganaban menos con sus despiadados ataques. Quizás el cóctel de medidas de seguridad mejoradas, una mayor atención por parte de las fuerzas del orden, sanciones internacionales a los operadores de ransomware y el escrutinio de la industria de las criptomonedas podría en realidad vencer el flagelo del ransomware.

Bueno no. Ese respiro parece haber sido un simple contratiempo en la trayectoria del ransomware para convertirse en una de las formas de ciberdelito más rentables y quizás la más disruptiva del mundo. De hecho, 2023 fue el peor año de su historia.

El miércoles, la empresa de seguimiento de criptomonedas Chainalysis publicó nuevas cifras de su informe anual sobre delitos que muestran que los pagos de ransomware superaron los 1.100 millones de dólares en 2023, según su seguimiento de esos pagos en cadenas de bloques. Ese es el número más alto que Chainalysis ha medido en un solo año, y casi el doble que el año anterior. De hecho, la compañía ahora describe los pagos de rescate relativamente bajos de 567 millones de dólares de 2022 como una “anomalía”, ya que las transacciones totales de extorsión han crecido constantemente desde 2020 hasta su récord actual de 10 cifras.

"Es como si hubiéramos retomado justo donde lo dejamos, el verdadero ataque durante Covid en 2020 y 2021", dice Jackie Burns Koven, jefa de inteligencia de amenazas en Chainalysis. "Se siente muy sin guantes".

Ese récord de más de mil millones de dólares en pagos de extorsión fue el resultado, en parte, de la gran cantidad de ataques de ransomware en 2023. La empresa de ciberseguridad Record Future contabilizó 4.399 ataques de ransomware el año pasado, basándose en informes de noticias y listados públicos de bandas de ransomware. víctimas en sus sitios de la web oscura, una táctica que los grupos suelen utilizar para presionar a las víctimas mientras amenazan con revelar sus datos robados. Eso se compara con solo 2.581 ataques totales en 2022 y 2.866 en 2021.

El aumento en el número de ataques parece haber contrarrestado una tendencia más positiva: según algunos cálculos, menos víctimas de ransomware están pagando los rescates que exigen los piratas informáticos. Según datos de la empresa de respuesta a incidentes Coveware, que frecuentemente negocia con bandas de ransomware en nombre de las víctimas, solo el 29 por ciento de las víctimas de ransomware pagaron un rescate en el cuarto trimestre de 2023, una caída dramática de las tasas de pago entre el 70 y el 80 por ciento para la mayor parte de 2019 y 2020.

Sin embargo, aunque cada vez menos víctimas pagan, la suma total recaudada por las bandas de ransomware sigue creciendo a medida que más ciberdelincuentes se sienten atraídos por una industria lucrativa y llevan a cabo más ataques. Allan Liska, analista de inteligencia de amenazas de Recorded Future, sostiene que la naturaleza altamente pública del ransomware sirve como una especie de publicidad, que atrae constantemente a piratas informáticos más oportunistas, como tiburones que huelen la sangre en el agua. "Todo el mundo ve todos estos ataques de ransomware", afirma Liska. "Los delincuentes tienden a acudir en masa a donde ven que se está ganando dinero".

Grafico

Pagos totales anuales de ransomware a lo largo del tiempo. CORTESÍA DE CHAINALYSIS

Cómo ver el Super Bowl 2024 (y el espectáculo de medio tiempo)

CULTURA

Cómo ver el Super Bowl 2024 (y el espectáculo de medio tiempo)

REECE ROGERS

Las mejores ofertas de juguetes sexuales para el día de San Valentín

ENGRANAJE

Las mejores ofertas de juguetes sexuales para el día de San Valentín

JAINA GRIS

Chainalysis señala que el récord de 1.100 millones de dólares en rescates pagados en 2023 también fue impulsado por piratas informáticos de ransomware que exigían sumas mayores a las víctimas, muchas de las cuales fueron cuidadosamente elegidas tanto por su incapacidad para tolerar un ataque devastador como por su capacidad de pago, lo que Burns Koven de Chainalysis llama “caza mayor”. Esto resultó en que cerca del 75 por ciento del valor total de los pagos de ransomware proviniera de transacciones que superaron la marca del millón de dólares en 2023, en comparación con solo el 60 por ciento en 2021.

Dada la feroz evolución del ransomware, la caída de los pagos totales en 2022 ahora parece representar una rara aberración. Chainalysis y otras empresas de seguridad explican ese mal año señalando la guerra en Ucrania, que interrumpió a los operadores de ransomware ucranianos, distrajo a los rusos y los llevó a la piratería política y causó conflictos dentro de grupos de ransomware con lealtades mixtas, así como las sanciones internacionales que disuadieron a las víctimas de pago de rescates e importantes medidas represivas por parte de las fuerzas del orden.

En un caso, para Por ejemplo, el prolífico grupo de ransomware conocido como Conti se disolvió después de que uno de sus líderes publicara una declaración en apoyo de la guerra de Rusia en Ucrania y otro discrepara al filtrar una gran cantidad de comunicaciones internas del grupo. Muchos de los miembros de Conti luego se reformaron bajo la marca de la operación ransomware Hive, que resultó haber sido infiltrada durante meses por el FBI y otras agencias que robaban silenciosamente las claves de descifrado del grupo para frustrar cientos de sus intentos de extorsión. Chainalysis estima que esa picadura por sí sola probablemente evitó más de 200 millones de dólares en pagos de ransomware. "La disolución de Conti fue casi una tormenta perfecta", afirma Burns Koven.

El año pasado, por el contrario, se produjo una tormenta de rendimiento de un tipo muy diferente: el grupo de ransomware Cl0p aprovechó una vulnerabilidad en la aplicación de transferencia de archivos MOVEit para comprometer a miles de víctimas, buscándolas en busca de los objetivos de mayor valor. Varios de ellos eran empresas médicas y agencias gubernamentales que poseían millones de registros confidenciales. En total, al menos 62 millones de personas se vieron afectadas, y Cl0p cosechó más de 100 millones de dólares de esa explotación masiva, lo que representa el 45 por ciento de todos los pagos de rescate en junio de 2023 y el 39 por ciento en julio según el recuento de Chainalysis.

El crecimiento continuo del negocio del ransomware, cuya interrupción para las víctimas, cabe señalar, cuesta mucho más de los 1.100 millones de dólares que algunos de ellos pagaron en 2023, puede parecer una señal de fracaso de la continua represión contra los delitos relacionados con las criptomonedas: desde el principio En lo que va de la década, los reguladores y las fuerzas del orden han estado persiguiendo no sólo a los grupos de ransomware, sino también a los intercambios y “mezcladores” deshonestos que a menudo sirven como herramientas de lavado de dinero que permiten a los ciberdelincuentes retirar sus ganancias criptográficas.

Burns Koven sostiene, sin embargo, que incluso el total récord del rescate de 2023 no significa que la represión contra las criptomonedas no esté funcionando. De hecho, dice, ha llevado a los grupos de ransomware a buscar constantemente nuevos métodos de lavado y, en algunos casos, los ha obligado a retener los pagos de rescate durante años antes de intentar retirar esa criptomoneda sucia, por temor a que sea congelada o apoderado. Añade que una notificación más rápida a las autoridades por parte de las víctimas que pagan rescates (incluso más rápido de lo que Chainalysis u otras empresas de rastreo de criptomonedas pueden detectar esos pagos en blockchains) podría ayudar aún más a perseguir esos fondos y evitar que sean liquidados.

"La mejor manera de reducir estas cifras es impactar el proceso de lavado y cobro", dice Burns Koven. Más allá incluso de operaciones llamativas de aplicación de la ley como la adquisición de Hive, dice que "también hay fricciones y parálisis operativas que contribuyen a estancar algunas de sus operaciones y su capacidad de obtener ganancias".

Por ahora, sin embargo, el ransomware no parece estar estancado. Y si apretar los tornillos a los blanqueadores de dinero (o a las víctimas que pagan rescates, o a los propios hackers) tiene alguna posibilidad de resolver el problema, esos tornillos aún no están lo suficientemente apretados.