Las herramientas de análisis de Blockchain ofrecen nuevas formas de "seguir el dinero" en casos de ransomware



**La evolución de los modelos de negocio y el rápido cambio global hacia el trabajo remoto, combinados con el creciente uso de criptomonedas, están creando nuevas amenazas de ransomware para las empresas de todo el mundo. Sin embargo, si bien las amenazas están en aumento, también lo está el uso de nuevas y poderosas capacidades en forma de herramientas de análisis de blockchain para combatir la costosa tendencia actual.**

Un tipo de software malicioso que puede bloquear el acceso a sistemas informáticos o datos valiosos, generalmente paralizando los procesos críticos para el negocio, el ransomware está permitiendo a los ciberdelincuentes sacar provecho como nunca antes al extorsionar a empresas grandes o pequeñas por pagos de criptomonedas. Pero los expertos en análisis de blockchain de hoy en día están tomando cada vez más el camino para "seguir el dinero", rastreando el movimiento de fondos ilícitos para proporcionar soluciones y nuevas defensas. Los investigadores estadounidenses hicieron un avance alentador en mayo, por ejemplo, aprovechando el poder del análisis de blockchain y recuperando rápidamente US $ 2.3 millones de los US $ 4.4 millones pagados en un ataque bien publicitado contra el gigante energético estadounidense Colonial Pipeline Co.1

Según la firma de análisis de blockchain Chainalysis,2 Las direcciones vinculadas al ransomware extorsionaron al menos US $ 81 millones en criptomonedas a partir del 10 de mayo de 2021, después de acumular un récord de US $ 406 millones en 2020. Chainalysis señala que el verdadero costo es probablemente mucho mayor, ya que las corporaciones a menudo no informan sobre costosos ataques de ransomware que están en aumento.

Se estima que el 41 por ciento de las organizaciones han informado haber experimentado un aumento de los incidentes de delitos cibernéticos, incluidos los ataques de rescate, mientras que los empleados han estado trabajando desde casa.3 Los casos siguen aumentando. Colonial Pipeline, operador del oleoducto de combustible más grande de Estados Unidos, sufrió un ataque de ransomware en mayo de 2021 que interrumpió los suministros de petróleo y gas en los Estados Unidos, y la empresa pagó US $ 4.4 millones en bitcoin para desbloquear su red.4

Datos recientes indican que la mayoría de las víctimas de ransomware están pagando para limitar la interrupción y el daño del negocio. La firma de seguros global Hiscox Group, en su Informe de Preparación Cibernética 2021, coloca la cifra en aproximadamente el 60 por ciento para los clientes afectados.5 Y pagar no garantiza nada cercano a la recuperación completa.

En promedio, los pagadores de rescate han recuperado solo el 65 por ciento de sus datos cifrados, mientras que el 29 por ciento recuperó solo la mitad de sus datos, según un informe reciente de la firma de seguridad cibernética Sophos, The State of Ransomware 2021, después de una encuesta global de más de 5,000 organizaciones.6 Sophos señala que el 37 por ciento de las empresas encuestadas informaron haber sido golpeadas en el último año por el ransomware, que Sophos llama una "gran amenaza" para las empresas de hoy.

El crimen organizado está sacando provecho

Los ataques de ransomware también están aumentando en sofisticación. Más allá de cifrar datos para paralizar las empresas, los hackers de hoy en día a menudo "exfiltran" o roban datos confidenciales o críticos para el negocio para obtener un rescate. Si no se realiza ningún pago, los datos se filtran públicamente. El llamado 'malware básico', por su parte, puede aparecer en los sistemas empresariales como malware de bajo nivel, pero está diseñado para acceder a un objetivo, recopilar datos valiosos y compartirlos con los atacantes para lanzar sus intentos de extorsión.

Además, la combinación de criptomonedas y ransomware ha creado una poderosa herramienta para los grupos del crimen organizado. La realidad es que el ransomware está proporcionando un alto retorno de la inversión para los delincuentes, y el rápido crecimiento de la liquidez en los mercados de criptomonedas está creando más oportunidades para ataques lucrativos contra las empresas.

Uso de análisis de blockchain para "seguir el dinero"

Afortunadamente, las herramientas de análisis de blockchain están siendo utilizadas cada vez más por las autoridades y los proveedores de servicios de activos virtuales (VASP), las empresas que brindan servicios relacionados con los criptoactivos y los intercambios de criptoactivos como Coinbase, para monitorear transacciones y detectar patrones cuestionables o reveladores relacionados con ataques de rescate. Los profesionales de KPMG también están implementando herramientas de análisis de blockchain hoy para ayudar a los clientes a "seguir el dinero".

Bitcoin es ahora la criptomoneda más utilizada en ataques y considerada la más detectable de las criptomonedas, lo que en última instancia facilita que las herramientas de análisis de blockchain rastreen los pasos dados por los actores maliciosos.

Los expertos pueden aprovechar el hecho de que bitcoin no es completamente anónimo, sino "pseudo-anónimo". Cada transacción es visible en la cadena de bloques pública de bitcoin, y aunque los datos de la transacción no contienen información sobre la verdadera identidad de un remitente o receptor, las direcciones de bitcoin pueden proporcionar pistas sobre las identidades.

Los proveedores de análisis de blockchain agregan información fuera de la cadena de bloques, conocida como "datos fuera de la cadena", para identificar a los remitentes y receptores de fondos. Para lograr esto, los análisis analizan los datos históricos de blockchain, combinados con el conocimiento de los buenos y malos actores y técnicas, para detectar patrones de transacción. Esto permite identificar las direcciones de blockchain de los actores ilícitos y brinda una oportunidad crítica para rastrear los fondos ilícitos.

La criptomoneda lavada generalmente se abre camino, a través de intercambios de criptomonedas, a los bancos a medida que los delincuentes convierten la criptomoneda en moneda fiduciaria. En su viaje, los delincuentes pueden usar 'mezcladores' o intercambios no conformes para cubrir sus huellas, mezclando sus bitcoins con otros usuarios para dificultar la detección. Los hackers también pueden ir a plataformas peer-to-peer (P2P) e intercambiar criptomonedas con otros para evitar a las autoridades. Los atacantes también usan un patrón de "cadena de pelar" para ofuscar los fondos ilícitos, básicamente una cadena de múltiples billeteras de bitcoin por las que pasan los fondos de rescate para ocultar el rastro de la criptomoneda obtenida ilegalmente.

Avanzar en la lucha contra los costosos ataques

Afortunadamente, como se está viendo, las herramientas de análisis de blockchain, que son distintas de las técnicas y sistemas típicos contra el lavado de dinero, pueden ayudar a los VASP y las autoridades a examinar las billeteras criptográficas y las transacciones en busca de conexiones con actividades ilícitas. También proporcionan puntajes de riesgo para las direcciones con las que los usuarios están interactuando, lo que idealmente les permite identificar, administrar y mitigar el riesgo. Esto está ayudando a las empresas a evitar que se laven fondos ilícitos a través de sus sistemas, o a detectar dicha actividad y denunciarla a las autoridades.

Como se está viendo, las herramientas de blockchain impulsan el progreso para hacer que los ataques de ransomware sean menos atractivos. Los investigadores estadounidenses lograron recuperar millones pagados en el ataque de mayo mencionado anteriormente en colonial Pipeline. A los pocos días del pago del rescate, la firma de análisis de blockchain Elliptic identificó la billetera bitcoin que recibió el pago y observó que había recibido pagos de bitcoin desde marzo y, aunque la mayoría de los pagos se trasladaron, alrededor de US $ 2 millones permanecieron en la misma cuenta y fueron incautados por el FBI.7

Los profesionales de KPMG están aprovechando las herramientas de análisis de blockchain para ayudar a los clientes a identificar el "dinero sucio" relacionado con un ataque de rescate. Están trabajando desde diferentes ángulos para ayudar a los clientes en este contexto:

* Ayudar a los VASP y a las instituciones financieras expuestas a diseñar modelos contra el lavado de dinero (AML) y el financiamiento del terrorismo (CTF) que permitan la identificación, detección y mitigación de riesgos asociados con la entrada de fondos ilícitos.
* Integración de la funcionalidad de las herramientas de análisis de blockchain dentro de la función de monitoreo operativo.
* Diseñar escenarios que permitan la detección de patrones de riesgo potenciales en el comportamiento de los clientes, e identificar los enlaces utilizados para permitir la recepción de fondos relacionados con un ataque de ransomware.
* Realizar informes de diligencia debida sobre el origen de los fondos ilícitos para evaluar su conexión con ataques de ransomware o la web oscura.

Abordar la amenaza y las crecientes amenazas de hoy

La investigación de Verizon indica que hasta el 90 por ciento de las campañas de ransomware funcionan dirigiéndose a vulnerabilidades conocidas para obtener acceso inicial.8

También es importante tener en cuenta cómo el riesgo de terceros se está volviendo significativo. El cambio de proveedor en caso de un ataque, o durante la interrupción de la cadena de suministro relacionada con la pandemia, a menudo se está acelerando sin el rigor adecuado, creando nuevas amenazas.

Tales desafíos se han acelerado en medio del aumento masivo en la adopción de servicios en la nube que acompaña la tendencia actual de trabajo desde casa. La tecnología y las herramientas en la nube que proporcionan acceso instantáneo a las redes empresariales han sido muy convenientes para las empresas, pero también para los posibles atacantes.

Para empeorar las cosas, el ransomware como servicio está aumentando la eficiencia de los actores maliciosos. Esencialmente, alguien empaqueta un conjunto de herramientas utilizadas en un ataque, lo que permite a los ciberdelincuentes cifrar subrepticiamente los datos dentro de la organización comprometida y retenerlos en un rescate.

En última instancia, las empresas deben abordar, después del ataque, precisamente cómo ocurrió un ataque. Pero las empresas con demasiada frecuencia asumen que una vez que se paga un rescate, el problema se resuelve, cuando en realidad los atacantes a menudo regresan con nuevas demandas de extorsión.

También existe la necesidad de que los intercambios de criptomonedas implementen controles adecuados. Si los bitcoins obtenidos por los piratas informáticos van a un intercambio, el intercambio debe tener controles y medidas contra el lavado de dinero para rastrear e idealmente identificar bitcoins adquiridos ilegalmente u otros activos criptográficos. Los bancos y los VASP también deben aumentar las defensas y sus capacidades para evitar que el dinero de los ataques de ransomware ingrese a sus plataformas.

Idealmente, las empresas necesitan mejorar todas las defensas a través de los diversos vectores de ataque que están surgiendo en las empresas remodeladas de hoy en día para detectar problemas y evitar el riesgo de que el ransomware prolifere a través de las redes comerciales. Los profesionales cibernéticos de KPMG están trabajando con éxito con clientes en una variedad de sectores para combatir las amenazas actuales. Aquí hay algunas acciones que recomendamos que las empresas tomen ahora y en el futuro para ayudar a mejorar la seguridad cibernética, la gestión de riesgos cibernéticos y la resiliencia cibernética:

Acciones de seguridad para hoy

* Las empresas, los intercambios y los bancos deben implementar herramientas de análisis de blockchain y controles AML adaptados a la gestión de los servicios y riesgos de criptomonedas específicos de hoy.
* Evalúe los impactos potenciales de la pérdida de sistemas y datos en su negocio y prepare un plan de acción de respuesta y pruébelo.
* Actualizar la capacitación y los recursos de concientización sobre seguridad para el trabajo post-COVID.
* Compruebe la identidad, la autenticación y el acceso a los sistemas de TI. Compruebe las capacidades de endpoint Detection and Response (EDR) y lo que puede registrar y supervisar.
* Verifique su capacidad de respuesta a incidentes y copias de seguridad y sea pirateado por un hacker ético para probar completamente su respuesta.

Acciones de seguridad en el futuro

* Priorizar el desarrollo continuo de defensas y contramedidas para abordar los riesgos a medida que los costosos ataques evolucionan y proliferan. Los bancos se enfrentan a la exposición a medida que los clientes reciben moneda ilegal relacionada con ataques de rescate.
* Evalúe todos los cambios tecnológicos en busca de posibles errores y examine los entornos de trabajo remoto en busca de nuevas vulnerabilidades. Examine cómo los cambios en los procesos o las innovaciones tecnológicas pueden aumentar el riesgo de una "amenaza interna". Integre la seguridad en todos los procesos de entrega de TI para ayudar a garantizar que los errores y las vulnerabilidades se aborden lo antes posible.
* Ejecute un ejercicio basado en un escenario que tendrá el mayor impacto en su organización. Implemente un programa de evaluaciones precisas e integrales que pondrán a prueba regularmente sus defensas y capacidades de respuesta contra amenazas y vectores relevantes.
* Comprenda exactamente lo que significa la adopción y expansión de los servicios en la nube con respecto a las responsabilidades de seguridad compartidas.

Responder de manera inteligente y proactiva a la creciente amenaza del ransomware se ha vuelto crítico para la continuidad del negocio y hay poco tiempo que perder para que las empresas mejoren sus defensas y estrategias de respuesta a medida que continúa esta tendencia costosa y potencialmente destructiva.

NOTAS

1bbc.com/news/business-57394041

2 blog.chainalysis.com/reports/ransomware-update-may-2021

3Encuesta de CIO de Harvey Nash/KPMG, 2020

4 Fuente: bbc.com/news/business-57394041

5Informe de preparación cibernética de Hiscox, hiscoxgroup.com/cyber-readiness

6Sophos El estado del ransomware 2021, secure2.sº phos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

7https://www.elliptic.co/blog/elliptic-follows-bitcoin-ransoms-paid-by-darkside-ransomware-victims

8Informe de investigaciones de violación de datos de Verizon 2020