VECTRA
SECURITY THAT THINKS

LIBRO ELECTRÓNICO

Cómo detener el ransomware: mensajes desde la primera línea

Resumen

Ninguna empresa quiere descubrir que se está desplegando un ataque de ransomware en su entorno, pero si puede identificar rápidamente las señales, tendrá muchas opciones de conseguir detenerlo. Pero, ¿cómo lo hacemos? Eso es precisamente lo que vamos a tratar en este documento y lo ilustraremos con ejemplos reales de cómo nuestros principales clientes trabajan junto con el equipo de Sidekick de Vectra para responder a los ataques de RansomOps, con el fin de evitar interrupciones de negocio de consecuencias desastrosas antes de que se despliegue el ransomware.

En este libro electrónico realizamos un análisis en profundidad de las razones por la que la detección de la actividad de los ciberdelincuentes y de las tareas de reconocimiento conocidas como RansomOps son fundamentales para detener el ransomware. Además, incluimos muchas de las medidas que los profesionales de seguridad están adoptando para neutralizar las tácticas de ransomware actuales. Contaremos cómo nuestros clientes de los servicios Sidekick de Vectra son capaces de detectar los ataques activos prácticamente de manera inmediata, así como algunos de los desafíos, observaciones y recomendaciones que todas las empresas deberían conocer.

Una cosa es segura, la diferencia entre éxito y fracaso a la hora de detener el ransomware radica en la velocidad de respuesta y la intervención rápida; ¡cortemos el paso al ransomware!

Servicio Sidekick MDR de Vectra

Sidekick MDR de Vectra es un servicio transparente y permanente (24/7/365) que investiga de forma proactiva la actividad maliciosa que identifica Vectra Detect.

Sidekick MDR actúa como potente refuerzo del equipo de seguridad desplegando a analistas de seguridad experimentados para ayudarle a sacar el máximo partido de la inteligencia artificial de Vectra para detectar de manera temprana y detener las violaciones de seguridad. Con Sidekick MDR sobre la plataforma Vectra, obtiene:

Un refuerzo definitivo para su equipo de seguridad gracias al acceso a analistas de seguridad experimentados que ayudan a expulsar a sofisticados ciberdelincuentes y operadores de ransomware.

Experiencia, contexto y claridad en relación con los signos reveladores tempranos de un ataque, amenaza o ransomware detectados por Vectra Detect con analistas que ayudan de manera proactiva a dar una respuesta rápida.

Supervisión proactiva y permanente para que sepa cuándo la detección de una amenaza o ransomware requiere una acción y respuesta inmediatas.

Personalización de su despliegue de Vectra adaptado específicamente a su entorno, sus objetivos empresariales y los riesgos de su sector. Esto incluye personalizar los controles, ofrecer recomendaciones de expertos, detectar las tendencias y métricas del entorno y acelerar las investigaciones.

El ransomware es un negocio

Por muy detestables que puedan parecernos, la bandas de ransomware y sus afiliados dirigen un negocio, y como cualquier otro negocio, su objetivo principal es ganar dinero. Tiene motivaciones económicas y sacan provecho de su capacidad para llegar hasta los sistemas y los datos para apoderarse de ellos lo más rápido posible, para después cobrar una suma considerable a sus propietarios para devolverles el control.

Esta mentalidad es la que impulsa muchas de las reflexiones que se debaten en este libro electrónico, mientras que conocer las motivaciones que mueven a los ciberdelincuentes es un elemento fundamental de cualquier estrategia de seguridad. Una vez disponga de esta información y sea capaz de identificar claramente los sistemas y datos de un entorno susceptibles de provocar una interrupción en caso de compromiso, su empresa estará en mejor posición para impedir que se despliegue un ataque.

Veamos por qué los ejercicios de simulación pueden contribuir a ayudar a poner esto de relieve y cómo los equipos de seguridad ofensiva (red team) pueden ofrecer una evaluación objetiva del nivel de preparación actual.

Empiece por lo básico

Por supuesto que el mejor resultado es impedir que las bandas de ransomware consigan acceder a su entorno. Y si bien la prevención no es infalible, la motivación económica puede jugar a su favor. De hecho, puede reducir drásticamente sus riesgos a través de una higiene de autenticación básica y una aplicación de parches adecuada.

La razón está en que habitualmente los ciberdelincuentes consiguen el acceso inicial a través de una vulnerabilidad sin parche y expuesta a una zona desmilitarizada (DMZ), una cuenta sin autenticación de doble factor o alguna debilidad similar. Básicamente, si las empresas pasan por alto alguno de los métodos de prevención básicos, no hace falta que los ciberdelincuentes utilicen sofisticadas y laboriosas tácticas para conseguir el acceso.

> El mejor resultado es impedir que las bandas de ransomware consigan acceder a su entorno.

Afortunadamente, basta con activar la autenticación multifactor (MFA) en su VPN, IDP u otros puntos de entrada para complicar un poco el trabajo de los ciberdelincuentes, que tal vez decidan intentarlo con otra víctima que se lo ponga más fácil. Lo mismo ocurre con la gestión de parches. Si se emplean prácticas adecuadas de aplicación de parches en toda su zona DMZ, también contribuirá a alejar los ataques. Aunque ninguna estrategia preventiva es infalible, una inversión inteligente en soluciones de prevención complicará a los ciberdelincuentes el acceso a su entorno.

Prepárese para responder rápido...Día y noche

Apuntalar las medidas básicas mejorará la exposición a riesgos, pero no los eliminará por completo. Las razones son muchas, pero lo cierto es que solo hace falta un error en la configuración de una cuenta, un parche sin aplicar, un usuario que haga clic en el enlace equivocado...o una nueva vulnerabilidad de día cero en su VPN (financiadas por las enormes cantidades de dinero vertidas en el ecosistema de ransomware) para abrirse paso. Hemos visto de todo.

Y cuando un operador de ransomware se infiltra en su entorno, tenga la seguridad de que se moverá RÁPIDO. Ciertamente hemos respondido a ataques que avanzaban lentamente durante varios días. Sin embargo, es habitual que la mayor parte del ataque se produzca en una sola noche y fuera del horario laboral. Recuerde que el tiempo es dinero para ciberdelincuentes con motivaciones económicas. Ya sea dando a los responsables de la defensa la menor cantidad de tiempo o por una cuestión de números, son pocos los ciberdelincuentes que se ven obligados a pasar desapercibidos. De hecho, el tiempo de permanencia global de los ataques de ransomware ha descendido de manera importante en los últimos años.

La parte positiva para los responsables de la protección es que esa velocidad hace evidente el ataque si se dispone de la tecnología de protección adecuada. Utilizando Vectra, por ejemplo, hemos observado hosts críticos a los dos minutos del acceso inicial. Sin embargo, debido a la velocidad de avance del ataque, esto convierte en esencial la capacidad de respuesta rápida y decisiva para detener la amenazas antes del despliegue del ransomware.

Desafortunadamente, esta capacidad de respuesta rápida no se limita a las horas de oficina. Hemos observado actividad de reconocimiento de primera fase y movimiento lateral a todas horas, es decir, básicamente cuando el operador de ransomware tenía tiempo para sus actividades. Unas veces en mitad del día, otras durante la noche, los fines de semana o incluso durante un día festivo. Sin embargo, según nuestras observaciones, el esfuerzo final de filtración y cifrado es más probable que se realice en mitad de la noche, durante el fin de semana o en un festivo, cuando la capacidad de respuesta a incidentes está en su momento más bajo.

En la práctica, esto significa que es necesario realizar una supervisión permanente (24 horas al días, 7 días a la semana).

Disponga de una estrategia de respuesta

El primer paso para responder a una amenaza de ransomware es detectar al adversario en su entorno. Resulta igualmente importante saber lo que hará en los distintos escenarios para detener el ataque. ¿Hasta dónde está dispuesto a llegar? En una de nuestras intervenciones, el agresor llegó a conseguir acceso de administrador de dominios del controlador de dominios, donde el equipo de seguridad en acción tuvo que tomar una decisión instantánea para desconectar completamente sus sistemas de Internet, a fin de ganar algo de tiempo para poder responder. Afortunadamente, la cosa salió bien.

Aunque ese equipo estuvo muy cerca de que se desencadenara un ataque de ransomware, este escenario es poco habitual. Podría merecer la pena preguntarse: ¿qué haría si su empresa estuviera en la misma situación? ¿Sería aceptable este nivel de alteración para el negocio? ¿Sería capaz de responder de forma eficaz sin que su equipo de seguridad remoto tuviera acceso a Internet? ¿Existen otras opciones de respuesta a las que debería recurrir?

Hemos visto que la toma de decisiones rápida y decisiva bajo presión es un ingrediente clave de una respuesta eficaz. Conocer y practicar su estrategia antes de que la necesite podría marcar la diferencia.

Para detener el ransomware, no busque el ransomware

Los ataques modernos de ransomware (en realidad, RansomOps), no despliegan el código binario de ransomware hasta el final. Esto significa que si llega a ver el propio ransomware, lo más probable es que sea demasiado tarde.

Se trata de un error común ya que para detener los ataques en marcha, necesitará detectar y responder a las etapas PREVIAS al despliegue del ransomware.
La realidad es que lo más probable es que trabajará sin tener un conocimiento pleno del adversario ni de su objetivo final. En muchos casos, observará un ataque que progresa rápidamente, y puede que algunos signos reveladores de las herramientas o de la infraestructura de mando y control que le permitan hacer una conjetura fundamentada de lo que está ocurriendo.

En este punto sus planes de respuesta tendrán que centrarse en una clase más general de intrusión y progresión de ataques para, entonces, darse cuenta de que el objetivo es solo una probabilidad y no una certeza.

Las cuentas y las herramientas de administración son fundamentales

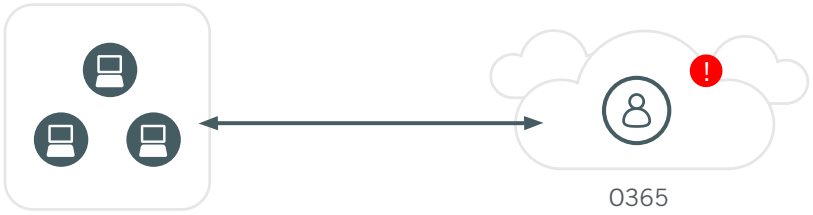
Hemos observado exploits utilizados para conseguir acceso inicial, e incluso en ocasiones para el movimiento lateral. Sin embargo, como en la mayoría de los ataques modernos, el principal interés está en las credenciales (cuentas administrativas y de servicio). Junto con los protocolos de administración, estas son las tácticas favoritas de prácticamente todos los afiliados de ransomware.

La intención, como en muchos ataques, es conseguir acceso de administrador de dominio del controlador de dominios para lanzar la fase final del ataque. Desde esta posición estratégica, es muy fácil conseguir acceso a la mayoría de los datos de valor. También es posible desplegar ransomware de una forma increíblemente rápida, mediante herramientas de administración que tengan GPO (objeto de directiva de grupo).

Debido al interés por las credenciales, resulta absolutamente fundamental supervisar el uso de todas las cuentas con privilegios, ya que hemos observado que esta es con seguridad una de las señales de detección de ataques más valiosas.

Temas comunes

Los analistas de Vectra compilaron desafíos de seguridad, de usuarios y de procesos comunes en las distintas interacciones con clientes.



Acceso inicial:

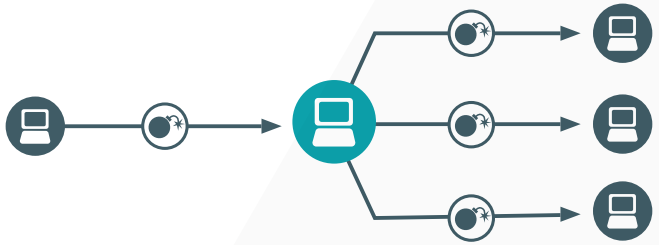
- Los ciberdelincuentes no cesan en la búsqueda de vulnerabilidades en sistemas y servicios públicos accesibles a través de Internet.
- Los servidores con RDP, FTP o VPN son objetivos habituales, y permiten el acceso inicial a empresas y a la nube.
- La falta de autenticación multifactor es una debilidad que suelen aprovechar.
- En algunos casos, el ataque tardó horas en desarrollarse desde el acceso inicial y en otros, se necesitaron días o incluso semanas. Hay tiempo para que los equipos de seguridad detecten y respondan rápido, pero se requiere una vigilancia permanente.

Mando y control (C2):

- Cobalt Strike destaca como la herramienta favorita actualmente.
- Algunas herramientas de acceso remoto populares, tanto autorizadas como no autorizadas, también se han utilizado para controlar sistemas. En un caso, detectamos el uso de software Cisco AnyConnect para controlar máquinas dentro de la empresa, por una persona ubicada fuera de ella.

Reconocimiento y movimiento lateral

- En la mayoría de los casos, la búsqueda fue agresiva e incluyó el mapeo de red, consultas rDNS y enumeración de recursos compartidos. En general, las búsquedas rápidas permitieron detectar los ataques en cuestión de minutos desde el acceso inicial.
- El reconocimiento relacionado con credenciales, como consultas LDAP y llamadas RPC para localizar ubicaciones de credenciales, también fue muy habitual.
- El movimiento lateral en las primeras fases incluía exploits comunes. En las etapas posteriores se utilizaban principalmente credenciales y protocolos de administración.



Filtración

- El uso sitios para compartir archivos gratuitos para cargar información de reconocimiento para el análisis fue muy habitual. Por ejemplo, Mega Upload (mega.com) y temp.sh.

Recomendaciones

Nuestros equipos trabajan estrechamente a diario con los equipos de seguridad, para responder a las alertas críticas que generan las soluciones de detección y respuesta frente a amenazas basadas en inteligencia artificial de Vectra. En nuestro primer contacto con los clientes, no está claro si una amenaza es ransomware. A medida que aumenta la gravedad de la amenaza, vamos consiguiendo datos y contexto sobre el ataque que nos permiten determinar si efectivamente se trata de ransomware. Hemos descubierto una amplia variedad de herramientas y prácticas de seguridad que dificultan a los ciberdelincuentes la ejecución de las campañas de ransomware y que, en última instancia, consiguen detenerlos con garantías. Concretamente:

Prevención

- Evalúe periódicamente su nivel de seguridad externa e implemente las correcciones de mayor prioridad. Preste especial atención a la infraestructura de acceso remoto y a los servicios más vulnerables, como RDP y FTP, que se ha demostrado que son objetivos frecuentes.
- Active la autenticación multifactor siempre que sea posible en proveedores de identidad o infraestructuras de acceso remoto.
- En general, la implementación de controles, reglas y políticas de prevención robustas dificulta la elevación de privilegios, incluso después del acceso, lo que permite ganar tiempo para responder.
- Las cuentas con privilegios requieren atención especial. Aunque puede resultar difícil desde el punto de vista operativo, cuanto más se haga para fomentar el uso de servidores puente y sistemas de administración de cuentas con privilegios, más complicada será la ruta de elevación.

Detección

- Hay tiempo para parar un ataque una vez que el operador del ransomware ha conseguido acceso y antes de que se filtren los datos o se despliegue el ransomware.
- Invierta en detección y respuesta frente a amenazas en toda la red, la infraestructura de identidades, la nube y los endpoints para maximizar las posibilidades de una detección temprana.

Investigación y respuesta

- Los ataques de ransomware pueden avanzar rápidamente, a cualquier hora del día o de la noche. Es fundamental supervisar las alertas críticas de manera permanente, ya sea reforzando los equipos internos o mediante soluciones de detección y respuesta gestionadas (MDR) o proveedores de servicios de seguridad gestionados (MSSP).
- La integración de telemetría de registros de red, los endpoints y la nube proporciona el mejor contexto, claridad y detalle para la investigación de las amenazas llegar hasta la causa principal definitiva.
- La búsqueda de un incremento de la actividad de búsqueda de su zona DMZ antes del acceso inicial, junto con inteligencia de fuentes abiertas (OSINT), pueden ofrecer una evaluación temprana de un posible ciberdelincuente, así como datos más claros para la respuesta.

Para obtener más información, póngase en contacto con nosotros en info@vectra.ai.

Correo electrónico info@vectra.ai vectra.ai