Cómo se desarrolla el ransomware con y sin Respuesta Autónoma

Índice

Introducción

En una era de ataques rápidos y en constante cambio, con tiempos de espera cada vez más reducidos y equipos de seguridad cada vez más sobrecargados, la detección por sí sola no es suficiente y la tecnología que puede responder a los ataques emergentes se ha convertido en una necesidad para detener la ciberinterrupción.

Darktrace Antigena utiliza su comprensión evolutiva acerca de la 'forma de ser' de todos y todo en el negocio para tomar decisiones en una fracción de segundo y realizar acciones dirigidas, interrumpiendo los ataques en curso sin afectar las operaciones normales del negocio.

A continuación, analizamos cómo se desarrolla el ransomware **con y sin Respuesta Autónoma.**

En los primeros cuatro escenarios, las empresas estaban haciendo una prueba de valor con Darktrace, por lo que Darktrace Antigena no estaba configurado en Modo Activo, en cuyo modo puede actuar de forma autónoma. En estos casos, el ataque continuó y se detuvo solamente gracias a la intervención humana temprana. Los dos últimos escenarios demuestran lo que ocurre cuando se configura Antigena para que responda de forma autónoma contra un ataque emergente.

Sin Respuesta Autónoma

Las primeras señales del ransomware: un ataque sorpresa

En un contratista de defensa canadiense, un atacante obtuvo acceso a un servidor consiguiendo las credenciales de un administrador y comenzó a propagarse lateralmente utilizando comandos WMI. Sin embargo, la cadena de eventos inusual y sospechosa fue detectada inmediatamente por la IA de Darktrace y, en el Modo Activo, la Respuesta Autónoma habría interrumpido el ataque inmediatamente.

En este caso, el ataque avanzó y la IA de Darktrace detectó las 5 etapas del ataque que continuaron durante las siguientes 48 horas, incluyendo C2 y más movimiento lateral. Cuando el atacante implementó el ransomware, los pocos dispositivos en los que Darktrace Antigena estaba activo quedaron aislados del ataque, mientras que los dispositivos desprotegidos finalmente fueron víctimas del cifrado. Con una implementación completa de la Respuesta Autónoma, este ataque habría terminado en el primer inicio de sesión.

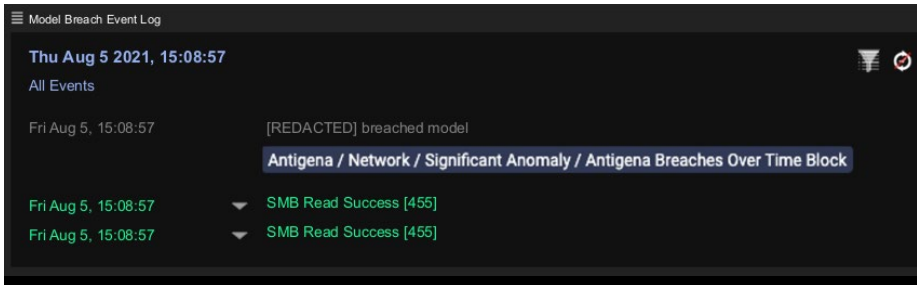


Figura 1: un modelo de Antigena se activa cuando se detectan múltiples anomalías en un período de tiempo

> «El ransomware al que nos enfrentamos actualmente se mueve demasiado rápido como para que los humanos puedan enfrentarse a él solos, la forma en la que nos mantenemos por delante es haciendo que la IA de Darktrace luche por nosotros de manera precisa y proporcional».
>
> Leon Shepherd, CIO, Ted Baker

Cómo la IA detuvo una intrusión de WastedLocker

En una organización agrícola de los EE.UU., Darktrace detectó un ataque de ransomware WastedLocker después de que un empleado fuera engañado para que descargara una actualización del navegador falsa. Podemos ver cómo Antigena habría bloqueado al instante el tráfico C2 en este y otros canales a medida que ocurrieran.

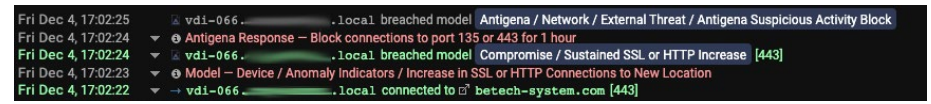


Figura 2: incumplimientos del patrón y la acción que habría tomado Antigena para solucionarlos

A medida que el atacante cambiaba de táctica e intentaba transmitir más, Antigena intensificó su respuesta. En ningún momento, sugirió interferir con actividades no relacionadas con el ataque.

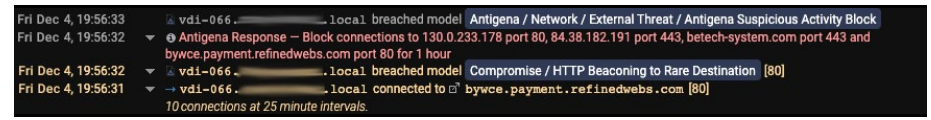


Figura 3: La posible respuesta de Antigena se intensifica

Afortunadamente, el equipo de seguridad reaccionó a tiempo a las alertas de Darktrace y, con el Cyber AI Analyst generando automáticamente un reporte de incidentes conciso y procesable, pudieron detener el ataque antes de que provocara graves daños.

Este rápido tiempo de reacción fue crucial para detener un incidente de seguridad extremadamente costoso y dañino. Depender únicamente de la respuesta humana es arriesgado: si el equipo no hubiera estado en alerta máxima y sin las detecciones de alta confianza de Darktrace, el ataque habría evolucionado a las etapas de cifrado.

Cyber AI Analyst investiga el ransomware Sodinokibi (REvil)

Después de que se utilizaran las credenciales de un miembro del equipo de TI de una organización minorista para atacar a un controlador de dominio, la IA de Darktrace detectó que el atacante escribía archivos sospechosos y después eliminaba batch script y ficheros log en el directorio raíz para borrar sus huellas. Luego, el controlador de dominio estableció conexiones con varios endpoints externos inusuales, y Darktrace presenció una carga de 28 MB que probablemente era una exfiltración de datos de reconocimiento inicial.

En el transcurso de dos semanas, Darktrace fue testigo de cómo un servidor SQL realizaba un escaneo de red, conexiones RDP internas inusuales que utilizaban credenciales de administrador y cargas de datos a varios endpoints de almacenamiento en la nube. PsExec se utilizó para implementar el ransomware, lo que provocó un cifrado de archivos.

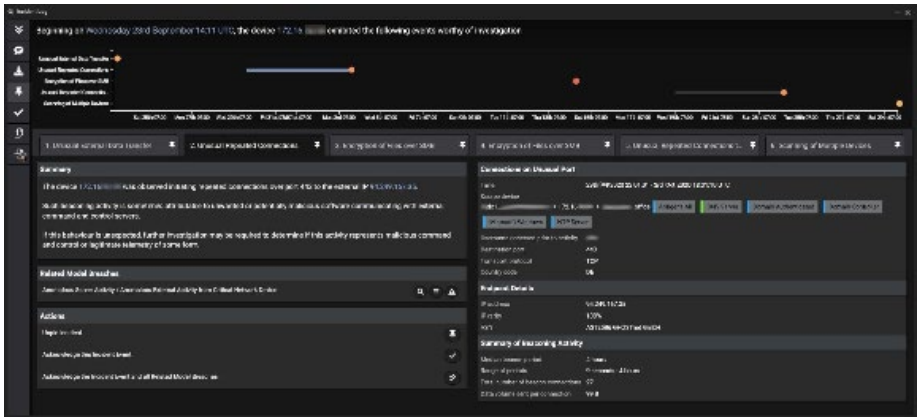
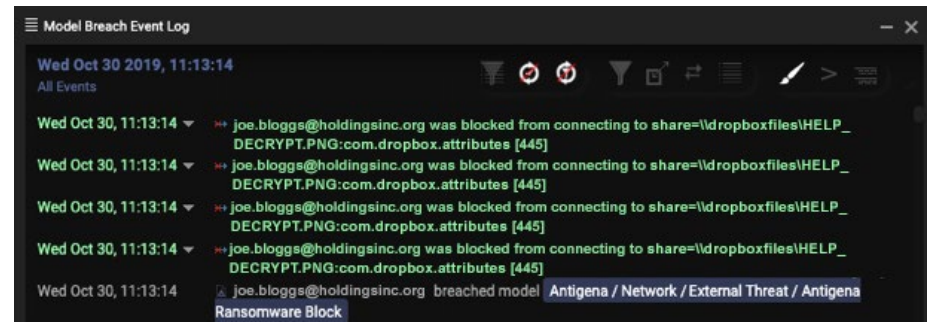


Figura 4: Cyber AI Analyst investiga

A pesar de los hallazgos claros presentados por el Cyber AI Analyst en 15 informes de incidentes, Darktrace estaba en modo de prueba y nadie estaba monitoreando la tecnología. En ausencia de la Respuesta Autónoma, se permitió que el ataque del ransomware Sodinokibi tuviera éxito, mientras que Antigena lo habría detenido en sus primeras etapas.

Ransomware de doble extorsión

La velocidad de propagación de un ransomware se evidenció en este incidente que afectó a una empresa energética canadiense, en la que el cifrado comenzó poco más de 12 horas después del reconocimiento inicial. Cada etapa del ataque fue detectada y alertada por Darktrace, incluyendo el escaneo de red, el movimiento RDP y las conexiones maliciosas de TeamViewer. Estas actividades, junto con una descarga de datos posterior de 1,95 TB y el inicio del cifrado, se realizaron sobre todo fuera del horario laboral, pero Darktrace las identificó como evidencias de que se estaba produciendo un ataque. Con la Respuesta Autónoma, este ataque habría finalizado en las etapas iniciales de reconocimiento y movimiento lateral.



```
Wed Oct 30 2019, 11:13:14
All Events

Wed Oct 30, 11:13:14   joe.bloggs@holdingsinc.org was blocked from connecting to share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes [445]
Wed Oct 30, 11:13:14   joe.bloggs@holdingsinc.org was blocked from connecting to share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes [445]
Wed Oct 30, 11:13:14   joe.bloggs@holdingsinc.org was blocked from connecting to share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes [445]
Wed Oct 30, 11:13:14   joe.bloggs@holdingsinc.org was blocked from connecting to share=\\dropboxfiles\HELP_
                       DECRYPT.PNG:com.dropbox.attributes [445]
Wed Oct 30, 11:13:14   joe.bloggs@holdingsinc.org breached model Antigena / Network / External Threat / Antigena
                       Ransomware Block
```

Figura 5: Antigena evita que el dispositivo infectado realice actividades de rescate y movimiento lateral

> «La Respuesta Autónoma combate los ataques de ransomware más sofisticados y lo hace a los pocos segundos de que surja la amenaza».
>
> Abhay Raman, CSO, Sun Life

Con Respuesta Autónoma

Minimizar el impacto de REvil transmitido a través de los servidores de Kaseya

Mientras EE.UU. se preparaba para un fin de semana festivo antes del 4 de julio, el grupo de ransomware REvil aprovechó una vulnerabilidad en el software de Kaseya para atacar a más de 1.500 empresas.

Una empresa con la Respuesta Autónoma implementada fue protegida de este ataque cuando la IA de Darktrace detectó un tráfico de SMB inusual e impuso el 'patrón de vida' del ordenador portátil, evitando así que se establecieran más conexiones inusuales.

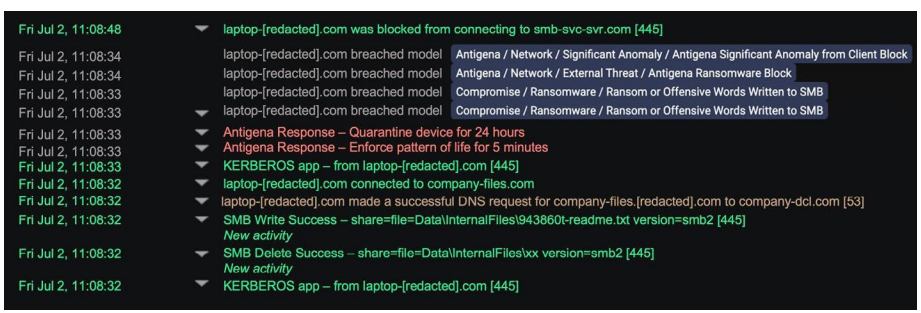


Figura 6: Darktrace detecta el intento de cifrado desde el dispositivo infectado y entra en acción

Se detuvieron los intentos posteriores realizados por el dispositivo infectado para conectarse a otros dispositivos, lo que evitó que el ataque se propagara. Los archivos de la red se salvaron del cifrado solamente porque estas acciones se realizaron inmediatamente y siguieron el ritmo de la velocidad del ataque, gracias a la Respuesta Autónoma.

Darktrace Antigena responde al ransomware en un menos de 1 segundo.

Antigena neutraliza un ransomware de día cero

En este ejemplo, la IA de Darktrace detectó un pico en el patrón de conexiones habituales realizadas por un dispositivo, así como una actividad de SMB sospechosa y búsquedas DNS inversas inusuales, una táctica que se utiliza a menudo durante el reconocimiento.

Una investigación adicional sobre la actividad de SMB reveló que se había accedido a cientos de archivos relacionados con Dropbox en recursos compartidos de SMB a los que el dispositivo no había accedido antes. Además, varios de estos archivos empezaron a cifrarse, añadiéndoles la extensión [HELP_DECRYPT].

Figura 7: Darktrace detecta una actividad de SMB relacionada con archivos de Dropbox

Afortunadamente, Antigena estaba en el Modo Activo y contraatacó al segundo, imponiendo el patrón de vida normal al bloquear las conexiones anómalas durante cinco minutos, lo que detuvo inmediatamente el cifrado. Cuando la IA de Darktrace entró en acción, solamente cuatro de estos archivos se habían cifrado con éxito.

Figura 8: Darktrace Antigena responde 1 segundo después de detectar el ransomware

A continuación, Antigena realizó una segunda acción para evitar que el ransomware se propagara a otros dispositivos. La combinación de varias actividades anómalas fue una evidencia suficiente para que la Respuesta Autónoma neutralizara la amenaza: el paciente cero estuvo en cuarentena durante 24 horas, sin poder conectarse al servidor ni a ningún otro dispositivo de la red. Por lo tanto, Antigena no solo detuvo la actividad de cifrado en su avance, sino que además evitó que los atacantes se movieran lateralmente por toda la red sin obstáculos, ya sea escaneando, utilizando credenciales de administrador recopiladas o realizando un reconocimiento interno.

Conclusión

A medida que el ransomware se vuelve cada vez más rápido y los atacantes continúan experimentando con nuevas técnicas, la Respuesta Autónoma se ha convertido en un componente vital de la estructura de seguridad. Al conocer perfectamente su empresa digital, puede responder a los ataques emergentes con precisión quirúrgica, conteniendo la amenaza sin interrumpir su negocio.

Los ejemplos anteriores demuestran que, incluso con los mecanismos de detección más avanzados, sin un mecanismo de respuesta proporcionado y a la velocidad de la máquina, el ransomware puede seguir causando importantes y costosos trastornos cibernéticos. El ransomware sigue siendo capaz de provocar una ciberinterrupción significativa y costosa.

La Respuesta Autónoma protege sus datos críticos, dondequiera que se encuentren, ya sea en las aplicaciones y la infraestructura en la Nube, el correo electrónico, la red corporativa o en los dispositivos de endpoint.

Acerca de Darktrace

Darktrace (DARK: L), líder global en inteligencia artificial de seguridad cibernética, ofrece tecnología de clase mundial que protege a más de 6,500 clientes alrededor del mundo de amenazas avanzadas, incluyendo ransomware y ataques a la nube y SaaS. El enfoque fundamentalmente diferente de la empresa aplica la IA de autoaprendizaje para permitir que las máquinas comprendan y logren defender el negocio de forma autónoma. Con sede en Cambridge, Reino Unido, la empresa cuenta con 1.700 empleados y más de 30 oficinas a nivel global. Darktrace fue nombrada una de las "empresas más influyentes" de la revista TIME para 2021.

Para más información

Visite darktrace.com
info@darktrace.com
Síganos en Twitter