Akamai

WHITE PAPER

Cómo acabar con la cadena de exterminio del ransomware con el conjunto de soluciones de seguridad empresarial de Akamai

Tabla de contenido

Introducción

Acabe con el ransomware en las distintas fases de la cadena de exterminio con las soluciones de seguridad empresarial de Akamai

Una de las amenazas de seguridad más importantes a las que se enfrentan las organizaciones actualmente es el ransomware, un método de malware que tiene como objetivo cifrar los archivos importantes de un dispositivo y dejarlos inutilizables. A continuación, los operadores de malware exigen un rescate a cambio de una clave de descifrado o de un software que permita restaurar los archivos a su estado original. En los últimos años, los grupos de delincuencia relacionada con el ransomware han perfeccionado sus tácticas y han comenzado a exfiltrar los datos de sus víctimas para ejercer una mayor presión, amenazando con filtrarlos públicamente o venderlos en la Dark Web.

Para poder defenderse de este tipo de ataque, es importante que los defensores sepan cómo trabajan los grupos de ransomware con el fin de lograr sus objetivos. Este documento le ayudará a hacer exactamente eso.

Comprensión de la cadena de exterminio del ransomware

Los ataques de ransomware son complejos: infiltrarse en el sistema es solo el principio. Para maximizar el daño, un atacante también debe distribuir su carga maliciosa por la red antes de empezar el proceso de cifrado. Si solo se cifra un equipo, el atacante no habrá alcanzado el impacto necesario para exigir un rescate. Para que el ataque de ransomware dé sus frutos, el atacante debe seguir varios pasos: detectar los activos de red, moverse lateralmente, entre otros. Este proceso a menudo se conoce como cadena de exterminio del ransomware.

Cada uno de los pasos de esta cadena abre nuevas oportunidades para la detección y mitigación. La preparación previa de su red con el conjunto de soluciones de seguridad empresarial de Akamai puede permitirle reducir su superficie de ataque, además de ayudarle a mitigar y contener cualquier posible daño causado por el ransomware antes incluso de que se dé cuenta de que ha sido víctima de este. En este documento se explica cómo puede utilizar Akamai Guardicore Segmentation, Enterprise Application Access y Secure Internet Access para detectar y bloquear la actividad de ransomware en los diferentes pasos de la cadena de exterminio:

Acceso inicial

Primera fase del ataque, en la que los atacantes vulneran la red interna desde el exterior

Detección

Métodos de detección que utilizan los atacantes para identificar activos importantes de la red

Movimiento lateral

Fase en la que los atacantes se propagan por la red y vulneran otros activos

Mando y control

Diferentes métodos mediante los que los atacantes mantienen un canal de comunicación en la red para enviar información y comandos a los activos comprometidos

Exfiltración

Métodos que usan los atacantes para exfiltrar datos confidenciales robados de forma encubierta

Acceso inicial

Cada organización tiene infinidad de interfaces con Internet, que los atacantes tendrán como objetivo para obtener acceso a la red. Akamai le permite proteger totalmente esas interfaces y mantener a los atacantes fuera de su red.

Protección de los servidores web

> Utilice las funciones de análisis de carga de Secure Internet Access para proteger los servidores web frente a ataques

Según Kaspersky, el método que más suelen utilizar los atacantes para obtener el acceso inicial es el ataque a las aplicaciones orientadas a Internet, a menudo aprovechando las vulnerabilidades de primer día en sistemas que no cuentan con los parches necesarios. Vulnerabilidades como Log4Shell (CVE-2021-44228) y ProxyLogon (CVE-2021-26855) se siguen explotando activamente en la actualidad para atacar las redes y distribuir el ransomware.

Enterprise Threat Protector se puede configurar para supervisar todo el tráfico web entrante en los servidores orientados a Internet; a continuación, se analiza ese tráfico para poder identificar y bloquear cualquier actividad maliciosa o anómala.

Bloqueo de las URL de phishing

> Utilice las funciones de inspección de URL de Enterprise Threat Protector para detectar y bloquear los intentos de phishing

El phishing es un método muy habitual de ataque a las redes. Los atacantes suelen enviar correos electrónicos con enlaces a archivos adjuntos maliciosos o páginas de inicio de sesión falsas diseñadas para robar credenciales. Con el cliente de Enterprise Threat Protector en sus terminales podrá analizar en tiempo real cada una de las URL en las que hagan clic los usuarios, identificar enlaces maliciosos o anómalos y bloquearlos.

Reducción de la superficie de ataque de la VPN

Utilice Enterprise Application Access para posibilitar un acceso a la VPN seguro y específico de la aplicación y reducir la superficie de ataque externa

En el entorno de trabajo híbrido actual, que suele incluir teletrabajo, es cada vez más habitual permitir a los usuarios utilizar una VPN para iniciar sesión en la red corporativa. A menudo atacan los ordenadores personales de los empleados para hacerse con las credenciales de sus VPN, que utilizan para acceder a la red interna. A menudo atacan los ordenadores personales de los empleados, poniendo en peligro las credenciales de sus VPN y utilizándolas para acceder a la red interna. En algunos casos, los atacantes también tendrán como objetivo los servidores vulnerables para filtrar las credenciales. En noviembre de 2022, los atacantes aprovecharon una vulnerabilidad en los servidores VPN de Fortinet para obtener el acceso inicial y, a continuación, propagar programas de ramsonware en toda la red.

Enterprise Application Access le permite reducir en gran medida este riesgo, al permitir el acceso a la red basado en roles y específico de cada aplicación. No concede a los usuarios acceso completo a toda la red, como ocurre con las VPN tradicionales, sino que solo permite el acceso limitado a las aplicaciones especificadas. De esta forma, si un atacante consiguiera obtener las credenciales del usuario y eludir la protección de autenticación multifactorial (MFA), no podrá obtener acceso a toda la red y solo tendrá acceso a un conjunto limitado de aplicaciones.

Mando y control

Bloqueo de servidores de mando y control (C2)

Utilice Akamai Secure Internet Access para bloquear los servidores de mando y control de malware conocidos

El malware en general, y el ransomware en particular, necesitan comunicarse con servidores C2 externos para enviar comandos y obtener información de los activos infectados. Mediante el análisis del amplio conjunto de datos de comunicación de Akamai, podemos supervisar los dominios de C2 de ransomware y malware, así como realizar un seguimiento de las campañas nuevas y en evolución. El cliente de Enterprise Threat Protector nos permite supervisar todas sus comunicaciones de DNS en tiempo real y bloquear la comunicación con dominios maliciosos, lo que evita que el malware se ejecute según lo previsto y logre sus objetivos.

Detección

Una vez que los atacantes logran infiltrarse, intentan identificar otros activos para comprender mejor la estructura de la red antes de comenzar a moverse lateralmente. Esto suele generar una comunicación interna, que Guardicore Segmentation de Akamai puede detectar.

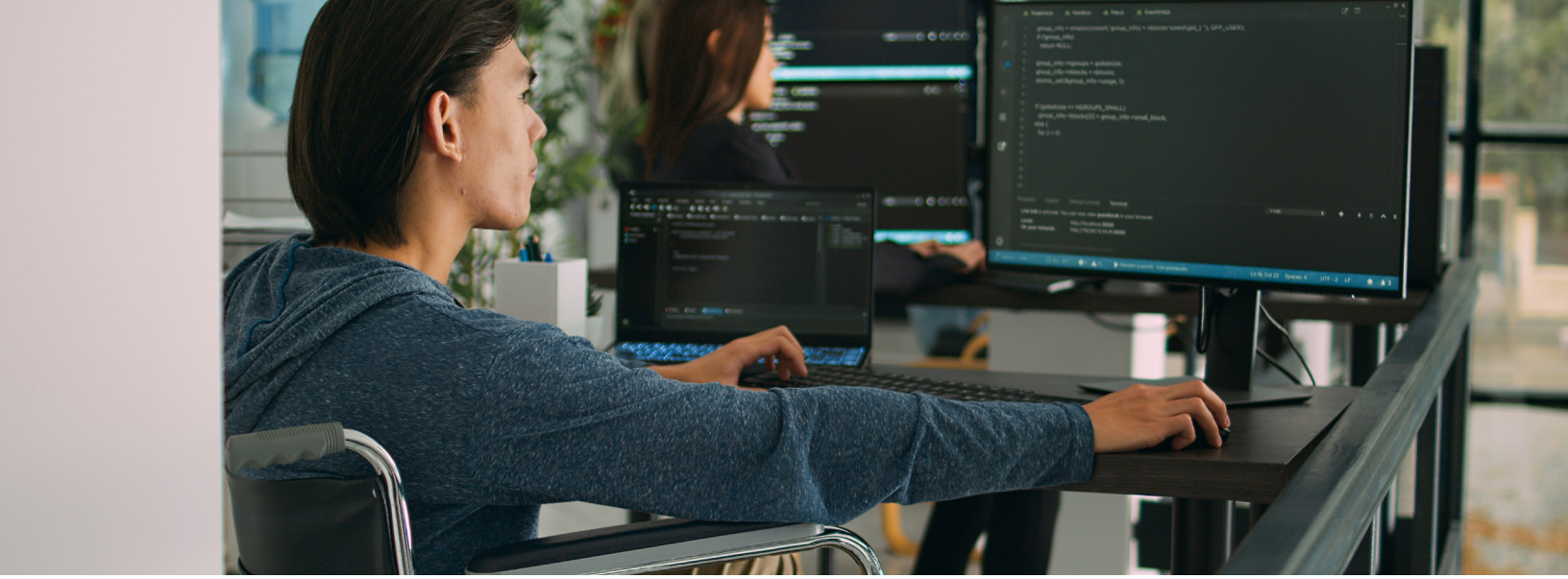
Identificación de los análisis de red

> Utilice los detectores de Akamai Guardicore Segmentation para identificar análisis de red sospechosos

Uno de los métodos más habituales que utilizan los atacantes para detectar redes es el análisis de puertos para identificar servicios de red. Muchos grupos de ransomware usan escáneres de red de código abierto. En un reciente informe de la CISA sobre el ransomware LockBit 3.0, se observó que el grupo usaba "SoftPerfect Network Scanner" para llevar a cabo el análisis de los puertos. Otro ejemplo es el grupo de ransomware Nokoyawa, que se observó que analizaba las redes para detectar servidores SQL con el fin de acceder a datos confidenciales incluidos en ellos.

Guardicore Segmentation de Akamai supervisa todas las comunicaciones de la red y cuenta con detectores integrados que identifican y alertan sobre dichos análisis, lo que le permite detener la propagación del malware antes de que comience.

Fig. 1: Incidentes de análisis de red en Guardicore Segmentation de Akamai



Engaño frente a detección

Utilice Guardicore Segmentation de Akamai para identificar los intentos de detección

Cuando los atacantes entran en una red, no conocen de antemano su estructura ni los diferentes activos que contiene. Para resolver este problema, tendrán que "explorar en la oscuridad" e intentar orientarse manualmente. Guardicore Segmentation de Akamai le permite aprovechar esto gracias al servicio de engaño, que atrae a los atacantes a servidores que se usan de cebo, supervisa sus actividades y le avisa cuando se detecten anomalías.

Por ejemplo, un atacante accede a la red e intenta usar la fuerza bruta para obtener las credenciales SSH de un servidor Linux. Guardicore Segmentation de Akamai identificará esta anomalía y reenviará al atacante a un cebo generado de forma dinámica. Una vez en el cebo, se registrarán todas las acciones que lleve a cabo el atacante y se generará una alerta.

A continuación, se muestra un ejemplo de una de estas alertas:

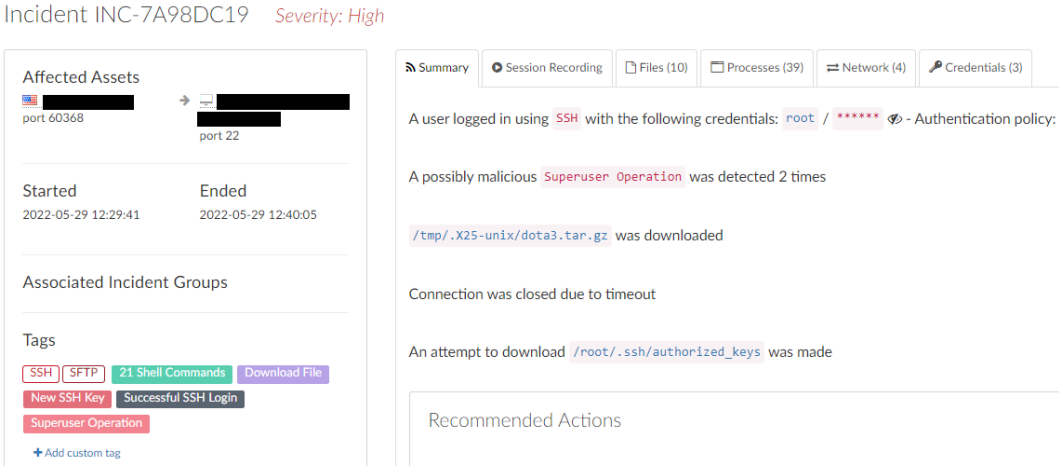


Fig. 2: Incidente de engaño en Guardicore Segmentation de Akamai

Movimiento lateral

Una vez que un atacante obtiene acceso a la red y se familiariza con su topología, querrá utilizarla para moverse lateralmente. Los grupos de ransomware modernos vulnerarán una red y, a continuación, se moverán lateralmente para comprometer el mayor número posible de activos, cifrándolos todos. Los productos de seguridad empresarial de Akamai le permiten limitar las posibilidades de movimiento lateral y minimizar el alcance de la filtración.

Identificación de indicadores de hosts sospechosos

> Utilice el módulo Insight de Akamai Guardicore Segmentation para identificar aquellos indicadores de host sospechosos de varias formas

Los atacantes utilizan herramientas de PowerShell para lograr distintos objetivos, uno de ellos es moverse lateralmente. Los droppers de PowerShell están muy extendidos y los atacantes suelen utilizarlos como primer elemento de código que ejecutan en un activo comprometido. Se ha demostrado que las infecciones recientes del ransomware Quantum están haciendo exactamente eso: ejecutar código de PowerShell en Windows Management Instrumentation (WMI).

Mediante el módulo Insight de Akamai Guardicore Segmentation, puede ejecutar consultas programadas para analizar el registro de eventos de PowerShell en todos sus activos, etiquetarlos con indicadores maliciosos y ponerlos en cuarentena.

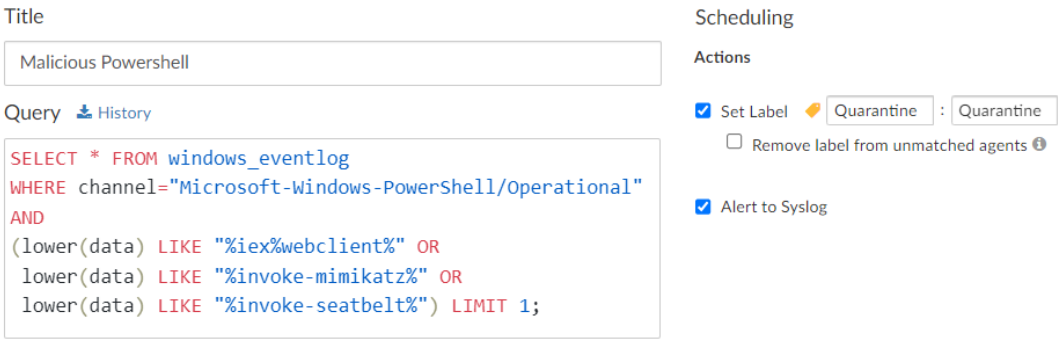


Fig. 3: Creación de una consulta de Insight programada para detectar PowerShell malicioso

Sin embargo, PowerShell es solo uno de los ejemplos. Insight se puede usar para analizar una amplia gama de indicadores de movimiento lateral, con cualquiera de las tablas de osquery existentes, por ejemplo:

- Utilice la tabla file para detectar archivos de malware basándose en nombres o hashes
- Utilice la tabla startup_items para detectar entradas de ejecución automática sospechosas en sus activos
- Utilice la tabla yara para analizar los archivos de sus activos con las reglas de yara con el fin de detectar cepas del malware

Bloqueo de los ataques a las LAN

Utilice Guardicore Segmentation de Akamai para bloquear y detectar ataques en los protocolos de la red local

Después de atacar al paciente cero de la red, los atacantes aprovechan las vulnerabilidades de los protocolos LAN, como ARP, para infectar otros activos. Con un firewall tradicional, esos ataques pueden pasar desapercibidos, ya que se realizan en la capa 2, y este tipo de comunicación no llega al firewall.

El enfoque basado en software que usa Guardicore Segmentation le permite supervisar y bloquear todo el tráfico que entra o sale de un activo, incluso el tráfico local que normalmente no llegaría al firewall de aplicación.

Restricción de los puertos de gestión

Utilice Guardicore Segmentation de Akamai para crear políticas en el nivel de proceso que reduzcan la superficie de ataque en los puertos confidenciales

Una vez dentro de la red, los atacantes suelen realizar una escalada de privilegios en aquellos activos comprometidos para robar credenciales. Cuando las han obtenido, los atacantes utilizan a menudo protocolos de gestión como RDP, RPC, SMB y WinRM para ejecutar una carga de ransomware en todos los activos de la red. Sin embargo, bloquear estos puertos por completo no suele ser posible, ya que los administradores los necesitan para las operaciones habituales.

Guardicore Segmentation de Akamai le permite aplicar políticas en el nivel de proceso para, de esta forma, poder decidir qué procesos deben comunicarse a través de puertos de gestión confidenciales. Examinemos el caso de WinRM. Lo utilizan muchos programas de administración, entre ellos Ansible. Sin embargo, los atacantes también suelen tenerlo como objetivo con herramientas como Evil-WinRM para moverse lateralmente. Con Guardicore Segmentation, podemos crear una política para permitir conexiones WinRM entrantes solo desde procesos Ansible y bloquear otros procesos que se ejecuten a través del mismo puerto:

Section	Source	Destination	Ports/Protocols	Action
Allow	ansible-operator	Windows Any	5985 TCP | UDP	Allow
Block	Any	Windows Any	5985 TCP | UDP	Block

Fig. 4: Ejemplo de la política de Guardicore Segmentation de Akamai para limitar la comunicación de WinRM

Exfiltración

En los últimos años, los atacantes han adaptado sus tácticas de extorsión y empezado a filtrar archivos confidenciales de sus víctimas para presionarlos aún más. Los atacantes intentarán pasar desapercibidos entre el ruido de la red a medida que exfiltran los datos de la organización, si bien normalmente pueden detectarse y bloquearse durante esta fase.

Bloqueo de los dominios de exfiltración

> Utilice Guardicore Segmentation de Akamai para limitar el acceso a los servicios que pueden sufrir ataques para obtener sus datos

Los atacantes utilizan con frecuencia herramientas públicas para filtrar datos de la red, una opción muy habitual son los servicios de alojamiento público como MEGA, Dropbox y Google Drive. El desafío a la hora de supervisar estos dominios radica en que se suelen utilizar con fines legítimos en la red. Por ejemplo, acceder al dominio MEGA a través de un navegador podría considerarse un proceso legítimo, pero hacerlo mediante la utilidad rclone, que utilizan activamente varios grupos de ataque para exfiltrar datos, se consideraría un proceso malicioso.

Gracias a Guardicore Segmentation de Akamai, podemos minimizar el riesgo de dichas herramientas al bloquear sus dominios en todos los terminales que no necesiten acceder a ellos y permitiendo el acceso únicamente a través de aplicaciones aprobadas, como los navegadores.

Defensa multicapa

Para lograr su objetivo más codiciado, los atacantes tienen que pasar por varias fases de ataque distintas. Cada paso ofrece a los equipos de seguridad la oportunidad de bloquear y detectar la actividad maliciosa asociada. Con ayuda de los diferentes productos de Akamai, los equipos de seguridad pueden usar medidas de mitigación en cada uno de los pasos de la cadena de exterminio del ransomware para detener a los atacantes y detectar cualquier comportamiento anómalo.

Para obtener más información sobre Guardicore Segmentation de Akamai o para solicitar una demostración personalizada del producto, visite akamai.com/guardicore.

Akamai protege la experiencia de sus clientes, su personal, sus sistemas y sus datos, ayudándole a integrar la seguridad en todo lo que crea, dondequiera que lo cree o distribuya. La visibilidad de las amenazas globales que ofrece nuestra plataforma nos permite adaptar y desarrollar su estrategia de seguridad para integrar el enfoque Zero Trust, detener el ransomware, proteger las aplicaciones y las API o combatir los ataques DDoS, y le proporciona la confianza necesaria para innovar, crecer y transformar todo su entorno. Para obtener más información acerca de las soluciones de seguridad, informática y distribución de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado en septiembre de 2023.