Cinco pasos para la protección contra malware avanzado: una realidad de Cisco

Lo que aprenderá

El panorama de amenazas ha evolucionado drásticamente en los últimos cinco años y las defensas existentes ya no son adecuadas para enfrentar las capacidades y los recursos de los atacantes.

En este informe aprenda los pasos necesarios para defenderse contra el malware avanzado:

1. Cómo detectarlo y bloquearlo en el perímetro
2. Cómo proteger el interior de la red
3. Cómo evaluar y proteger terminales
4. Cómo analizar las amenazas
5. Cómo eliminar el malware e impedir la reinfección

Introducción

Hace cinco años, los profesionales de la seguridad podían enfocarse en el cumplimiento e implementar controles profundos, como programas de firewalls o de antivirus, para defenderse de atacantes que en su mayoría eran poco sofisticados. A menudo ocurrían ataques de gusanos y troyanos, pero las organizaciones que contaban con revisiones y procesos de administración de configuración aceptables se mantenían protegidas en gran medida. Sin embargo, los atacantes continuaron buscando la ruta de menor resistencia y los cambios subsiguientes en el entorno afectaron significativamente la función de la seguridad de la información en la protección de los activos corporativos.

Ahora los profesionales de seguridad enfrentan adversarios mucho más sofisticados. Este nuevo tipo de atacantes ya no está interesado en operaciones de tipo robo relámpago. En cambio, para penetrar los dispositivos de la red de una organización prefieren adoptar un enfoque lento y metódico. Los atacantes se enfocan en mantener un punto de apoyo persistente y extraer propiedad intelectual y datos importantes del cliente. Esta nueva misión requiere un aumento drástico en las capacidades operativas y en la sofisticación de los ataques.

En la actualidad, el sector enfrenta atacantes profesionales bien financiados que invierten en investigación de seguridad para rivalizar con los proveedores más grandes de seguridad y generar un suministro aparentemente interminable de ataques de día cero. A menos que sea necesario, los atacantes no malgastan ni un día, sino que optan por el ataque más simple y necesario. Es por eso que se pueden observar toda clase de ataques: desde sencillos y simples hasta complejos e innovadores.

El instrumento preferido de los atacantes sigue siendo el malware. Sus métodos evolucionaron desde afectar las operaciones hasta mantener presencia en las redes objetivo para robar tanto datos financieros como propiedad intelectual mientras evaden la detección de manera permanente. Esta misión ampliada (y mucho más estratégica) requiere el uso de malware avanzado. El malware avanzado es mucho más difícil de detectar que los virus y los gusanos típicos porque es:

- **Dirigido:** la detección genérica antivirus tradicional ya no es eficaz.
- **Adaptable:** tácticas evasivas innovadoras permiten a los atacantes reasignar los dispositivos comprometidos y evitar la detección.

- **Eficaz:** las técnicas comprobadas de desarrollo de software se utilizan para refinar el malware y garantizar la eficiencia de los ataques.
- **Oculto:** el bloqueo de comunicaciones entre el dispositivo y las redes de comando y control aísla los dispositivos comprometidos y oculta la causa de los ataques de malware.

La eliminación del malware avanzado una vez que se ha logrado identificar no es sencilla. Es fundamental contar con visibilidad en el linaje del archivo de malware: procesos primarios y secundarios para erradicar definitivamente los archivos que introducen el malware y para detectar amenazas polimórficas. Después de generar el perfil del ataque, si no se encuentra y se realiza limpieza del punto de origen del malware (paciente cero), así como en todos los demás dispositivos que poseen código de malware inactivo, las organizaciones sufren constantes reinfecciones. Es la versión moderna del Día de la Marmota.

Insuficientes defensas

Hace pocos años, la detección y la limpieza del malware eran simples. El malware no era evasivo ni estaba dirigido a un dispositivo o a una persona en particular. Generalmente el malware apuntaba a una vulnerabilidad conocida, lo que aumentaba la probabilidad de detección. Como resultado, las defensas usadas por las empresas eran bastante simples. Con los años, los atacantes han cambiado sus tácticas significativamente y aunque las defensas han mejorado, no ha sucedido lo suficientemente rápido como para mantenerse al ritmo de los ataques.

Protección de terminales

Los conjuntos de aplicaciones para protección de terminales que se implementan en la actualidad comenzaron a utilizarse a principios de los años noventa como productos antivirus basados en firmas. Las empresas de antivirus analizaban las nuevas muestras de malware, desarrollaban firmas para la detección e implementaban esas nuevas firmas en todos los terminales protegidos. Ese modelo proporcionó una eficacia razonable durante casi una década antes de que sucedieran tres hechos que rompieron con el modelo basado en firmas:

1. **Los volúmenes de software se disparan:** cada día surgen decenas de miles de nuevos ejemplos de malware. Hace pocos años, los proveedores de antivirus no podían analizar y generar el perfil de todo el malware y mucho menos distribuir las firmas subsiguientes.
2. **Polimorfismo:** los atacantes avanzados hacen que los atributos del archivo de malware se transformen. Estos virus que cambian de manera aleatoria hacen imposible su detección mediante el tradicional enfoque basado en firmas.
3. **Pruebas:** con servicios de prueba basados en Internet, los atacantes pueden evaluar el malware antes de iniciar un ataque. Estos “sandboxes” virtuales ejecutan una muestra de malware contra todas las tecnologías antivirus disponibles.

Aunque el sector ha reconocido los límites del modelo de antivirus tradicional, en este momento abandonarlo no sería práctico. Casi todas las obligaciones de cumplimiento requieren la protección de terminales. Aunque las aplicaciones de antivirus tradicionales todavía agregan valor porque bloquean malware no sofisticado, la protección de terminales no es suficiente como mecanismo de detección principal para el malware avanzado.

Reputación

Para cerrar la brecha de detección, los proveedores de protección de terminales introdujeron la reputación. Los proveedores de seguridad utilizan técnicas sofisticadas de recopilación y minería de datos para determinar si ya se ha detectado una dirección IP o un archivo específico, evaluar su conducta y decidir si se lo bloquea. La idea de la reputación es muy potente. Permite predecir el comportamiento malicioso, que proporciona los medios para prevenir un ataque generalizado. Sin embargo, tal como se utiliza hoy en día, la reputación tiene una aplicabilidad limitada como defensa primaria contra el malware avanzado.

Los atacantes pueden simular ser una dirección IP con una buena reputación y así obtener un pase libre para atacar. Las organizaciones podrían adoptar un enfoque del tipo “culpable hasta que se demuestre lo contrario” y bloquear todas las direcciones IP o los archivos que tengan reputaciones desconocidas, pero esto genera falsos positivos y afecta la capacidad de los empleados para realizar su trabajo.

Del mismo modo, la reputación de archivos tiene límites similares. Las firmas de archivo que se utilizan para identificar el malware se pueden evadir con los ataques polimórficos descritos anteriormente. Cualquier enfoque basado en la reputación depende de ya haber visto el ataque en otro lugar. Es necesaria una amplia distribución de agentes y un análisis escalable de datos para ver un ataque antes de que se difunda.

Lista blanca de aplicaciones

Casi todos los tipos de malware se basan en algún tipo de archivo ejecutable e introducen código en la memoria del dispositivo comprometido. Si una organización puede definir una lista de aplicaciones específicas autorizadas para ejecutarse en un dispositivo y bloquear todas las demás aplicaciones, es mucho más difícil que el dispositivo se infecte. Este concepto se ha convertido en una categoría de soluciones conocidas como lista blanca de aplicaciones (AWL), que puede ser muy eficaz en el bloqueo de malware y en la protección de los dispositivos.

Desafortunadamente, la lista blanca de aplicaciones afecta de manera espectacular la experiencia del usuario. Si una aplicación específica no está en la lista blanca, un empleado no podrá ejecutarla. Mantener actualizada la lista blanca se vuelve rápidamente inviable y deja a los empleados sin el software que necesitan para realizar su trabajo. A veces se les da a los empleados un período de gracia para ejecutar aplicaciones no autorizadas, pero esto da lugar a rupturas en el modelo de seguridad.

La lista blanca de aplicaciones ofrece una protección sólida para dispositivos de función fija (kioscos, sistemas de control, cajeros automáticos, etc.). A pesar de que no es aplicable para un dispositivo de computación de propósito general, la lista blanca de aplicaciones funciona de manera eficaz en los terminales que solo utilizan una pequeña cantidad de aplicaciones.

Detección de malware basado en la red

Dado el polimorfismo agresivo que se puede observar en el actual malware avanzado, la detección de malware ya no funciona mediante firmas en base a la apariencia del archivo. La detección requiere un perfil integral que detalle qué es lo que hace el malware. Un enfoque popular implica ejecutar cada archivo potencial de malware dentro de un sistema operativo para determinar qué le puede hacer el archivo al dispositivo. Este cuasi sandbox se puede ejecutar en varias ubicaciones, incluso en un terminal, un dispositivo independiente basado en red o un servicio de la nube.

En el sector hay mucha publicidad sobre el equipo independiente de detección de malware basado en red y por una buena razón. La identificación de malware en el momento en que ingresa a la red es una alternativa mucho mejor que apostar a que solo un agente de terminal lo detecte o arregle el daño generado después de que la infección se ha difundido. Sin embargo, estos dispositivos de detección de malware basados en red no son una panacea.

Por ejemplo, el malware avanzado generalmente puede determinar si esto sucede en un sandbox, por lo que permanece inactivo e inadvertido. De manera similar, algunos tipos de malware no hacen nada durante horas (o días); esperan que un sandbox no disminuya los recursos mediante la ejecución constante del archivo. Los dispositivos del perímetro de la red de una organización no verán todo el tráfico destinado a los dispositivos terminales. Un dispositivo móvil que esté conectado a una red pública de Wi-Fi no estará protegido por la gateway de malware basado en red porque el tráfico no pasa a través de la red corporativa.

La incapacidad de gestionar todos los dispositivos al mismo tiempo no es el único problema con los dispositivos de malware independientes, basados en red. Si el dispositivo no está en línea ni bloqueando el malware conocido, las amenazas pueden ingresar a la red. Además, las infecciones requieren corrección y las soluciones de detección basadas en red frecuentemente carecen de un componente de terminal para corregir o bloquear el ataque directamente en el dispositivo.

La detección independiente basada en red no proporciona visibilidad a los ataques que se consideren de malware recién hasta después del hecho. Por ejemplo, el malware sensible al sandbox ingresa a la red y compromete un dispositivo terminal. En ese momento, usted debe ver dónde más aparece el archivo en la red para garantizar que se limpien todos los dispositivos. La falta de contexto que se crea al realizar el seguimiento de lo que sucede después de que un archivo atraviesa el perímetro e ingresa en la red principal o en una oficina remota genera un punto ciego. La única manera de proporcionar ese contexto es tener presencia en el terminal y ejecutar el análisis de datos masivos para determinar esos patrones.

Proceso de prevención de malware avanzado

Claramente, las soluciones actuales para detectar malware avanzado no están completamente a la altura de la tarea. Los límites de las tecnologías existentes demuestran que no hay una manera estructurada de detectar y corregir ataques de malware avanzado. Si el sector ha aprendido algo en la última década es que no hay una tecnología milagrosa que pueda resolver cualquier problema de seguridad. Las organizaciones deben considerar la detección avanzada de malware dentro de un ciclo de vida de prevención más amplio.

Esta sección presenta y explica el proceso recomendado de cinco pasos de Cisco para tratar con malware avanzado:

1. Cómo detectarlo y bloquearlo en el perímetro
2. Cómo proteger el interior de la red
3. Cómo evaluar y proteger terminales
4. Cómo analizar las amenazas
5. Cómo eliminar el malware e impedir la reinfección

Cómo detectarlo y bloquearlo en el perímetro

Administrar las amenazas tan cerca del perímetro como sea posible para evitar que el malware ingrese a la red y potencialmente infecte los dispositivos terminales. Un dispositivo de detección de malware es una estrategia importante de seguridad perimetral. Estos dispositivos aprovechan los servicios en la nube o utilizan sandbox incorporados para evaluar no solo a qué se parece el malware sino qué hace. Con la búsqueda de malware conocido, el dispositivo basado en red para la detección de malware debería funcionar en línea para bloquear el ataque sin influir en el rendimiento de la red ni agregar latencia.

Cómo proteger el interior de la red

Busque el malware (y otros ataques) en los segmentos protegidos de la red que contienen activos de tecnología sensibles, si se supone que ningún ataque se origina desde un elemento interno de confianza. Los atacantes avanzados adoptan un enfoque sistemático para obtener acceso a las redes de las organizaciones. Comienzan comprometiendo cualquier dispositivo para obtener un punto de apoyo dentro de la organización. Después de integrarse en la red, los atacantes penetran cada vez más profundo y comprometen dispositivos adicionales hasta alcanzar su objetivo.

Cómo evaluar y proteger los terminales

Es poco aconsejable suponer que cualquier dispositivo de seguridad perimetral será un 100% eficaz para bloquear todas las amenazas. Las defensas sofisticadas contra el malware avanzado en cada terminal son otra capa fundamental de la defensa contra ataques. Debido a que muchos dispositivos no siempre están conectados a una red corporativa y no siempre tienen las protecciones de malware basado en red, esos terminales necesitan protección en sí mismos. Dado que a los empleados no les agrada ver comprometida su experiencia como usuarios, cualquier agente de terminal que se instale debe ser ligero y no dificultar el rendimiento.

Cómo analizar las amenazas

Mantenga la visibilidad de toda la actividad de archivos y realice el seguimiento del tráfico de salida para detectar la potencial exportación no autorizada de datos críticos e identificar el tráfico de comando y control para indicaciones de dispositivos comprometidos. A pesar de los grandes esfuerzos realizados a través de los controles de protección en las redes y en los terminales, todavía es necesario analizar y evaluar los ataques de malware a fin de determinar su grado de amenaza para las organizaciones.

Cómo eliminar el malware e impedir la reinfección

Ponga en cuarentena y limpie el dispositivo infectado a fin de minimizar el riesgo para otros dispositivos de la red. Sin embargo, eso no es suficiente para realmente eliminar el malware o evitar la reinfección. El análisis de datos masivos para realizar un seguimiento de cada archivo de cada dispositivo (de dónde provino y qué ocasionó su ejecución) ofrece visibilidad en toda la empresa e identifica todas las instancias del archivo de malware. Esto garantiza que se encuentre al paciente cero (el primer dispositivo víctima de malware) y que se controle cualquier infección subsiguiente. La protección eficaz contra el malware avanzado también requiere la capacidad de etiquetar los archivos que más adelante se identifiquen como malware. Esto permite identificar los objetivos de ataques para la corrección específica. Después de la corrección, las organizaciones deben implementar normas integradas en la gateway del perímetro de seguridad, dentro de los dispositivos que protegen redes internas y en los terminales para eliminar el riesgo de reinfección.

Superioridad de información: defensa contra malware avanzado

Cisco introdujo un completo conjunto integrado de capacidades de defensa contra malware avanzado. Cisco® Advanced Malware Protection (AMP) ofrece una visión única e inteligente de las amenazas avanzadas que enfrentan las organizaciones e incluye inteligencia colectiva que realiza un seguimiento de los patrones de tráfico de los atacantes; los analiza y los bloquea tanto en la red como en el terminal. También tiene el respaldo del análisis de datos masivos a fin de abordar el malware antes, durante y después del ataque.

Inteligencia de seguridad colectiva

Cisco recopila y analiza millones de muestras de malware por mes y evalúa el impacto del malware en una variedad de dispositivos. Este análisis se realiza en la nube de Cisco Collective Security Intelligence (CSI) y no ejecuta el malware en las instalaciones del cliente, donde el ataque podría escaparse de los límites del dispositivo y posiblemente infectar otros. Cisco AMP realiza el análisis del archivo, brinda información detallada sobre el comportamiento del malware, el nombre de archivo original, capturas de pantalla de la ejecución del malware y capturas de paquetes de muestra. Descubrimos los ataques emergentes de malware antes de que sucedan infecciones generalizadas mediante el análisis de los archivos de malware de más de 10 000 organizaciones de todo el mundo.

Cisco FireSIGHT Management Center: Inteligencia desde la red

Realice el seguimiento del tráfico de red con Cisco FireSIGHT™ Management Center con la seguimiento de CSI para identificar los dispositivos comprometidos. Cisco FireSIGHT Management Center desarrolla una línea de base de tráfico de red normal y, luego, busca anomalías de red, que pueden indicar un ataque de malware. Mediante la búsqueda del tráfico de comando y control o la actividad de exportación no autorizada, y la correlación de esas amenazas con las aplicaciones y los sistemas operativos objetivo, las organizaciones obtienen una perspectiva más amplia de lo que sucede en sus redes y, por lo tanto, tienen otros medios para identificar los ataques de malware avanzado.

Después de que Talos Security Intelligence and Research Group haya identificado los ataques y haya generado sus perfiles, estos patrones de ataque se pueden implementar en los puntos de aplicación, tanto en el perímetro como dentro de la red, en el firewall de próxima generación (NGFW) Cisco FirePOWER™ y en los dispositivos de sistemas de prevención de intrusiones de próxima generación (NGIPS). Evalúe y priorice el impacto de las amenazas con una perspectiva en tiempo real del entorno de infraestructura de TI dinámico, que supervisa y analiza el tráfico de red de su organización con Cisco FireSIGHT Management Center.

Protección contra malware avanzado de Cisco FirePOWER

Detecta el malware a medida que ingresa con Cisco AMP para FirePOWER en los dispositivos Cisco FirePOWER. FirePOWER, configurado como NGIPS o NGFW, determina la huella digital del archivo y la reenvía a Cisco FireSIGHT Management Center, que la revisa con la nube de Cisco CSI (o, en el caso de archivos vistos con frecuencia, con el caché local) para determinar rápidamente si conoce el archivo. Esta búsqueda ligera de los archivos ya analizados ofrece un enfoque más escalable que la ejecución de cada archivo en el dispositivo.

Para los archivos maliciosos, la nube de Cisco CSI devuelve la huella digital del archivo y el informe del centro de administración de la IP de destino, lo que permite la corrección inmediata del dispositivo comprometido. Cisco AMP para FirePOWER va más allá y protege las organizaciones incluso cuando se determina que un archivo es malicioso después del hecho. La nube de Cisco CSI actualiza Cisco FireSIGHT Management Center cuando se reclasifica un archivo malicioso. Los tableros e informes de eventos subsiguientes se actualizan automáticamente y pueden identificar el dispositivo infectado. Esta capacidad continua para detectar malware avanzado persiste aún después de que el archivo ha atravesado el perímetro.

La evaluación de cada archivo que atraviesa el perímetro requiere la ampliación de los recursos hasta abarcar todo rango de la amenaza de malware. El rendimiento líder en el sector de los dispositivos Cisco FirePOWER garantiza que la detección de malware basada en la red no afecte el rendimiento ni agregue latencia a las aplicaciones críticas.

Bloquee el tráfico saliente basado en la reputación IP para garantizar que los terminales no se comuniquen con los sitios conocidos de distribución de malware mediante dispositivos de Cisco FirePOWER respaldados por la inteligencia de Cisco FireSIGHT Management Center a través de la nube de Cisco CSI.

Cisco AMP for Endpoint: Protección integral de terminales

Cisco AMP for Endpoint es el producto completo de Cisco para protección de terminales, para PC, dispositivos móviles y sistemas virtuales. Protege dispositivos, estén o no conectados a la red. Cisco AMP for Endpoints, implementado como agente que se conecta a nuestro sofisticado análisis de datos masivos, examina toda la actividad de archivos en un dispositivo para garantizar que se identifique el malware antes de la infección. Similar a la solución Cisco AMP for FirePOWER en el caso de que el malware se identifique después de la infección, Cisco AMP for Endpoints sabe qué dispositivos han estado en contacto con el malware y puede marcar esos dispositivos para la corrección específica.

Las potentes innovaciones como el análisis de archivos y trayectoria de archivos de Cisco AMP for Endpoints muestran qué sistema se infectó primero con el malware y también el alcance del ataque a través de la red. Esto permite que las organizaciones identifiquen el vector inicial del ataque para el brote de malware, así como la profundidad y el alcance de la infección. Identifique y limpie todas las instancias de la infección de malware, lo que brinda una visibilidad inigualable con Cisco AMP for Endpoints.

Conclusión

Somos la única empresa que ofrece una solución integral que apunta a las amenazas en todo el ciclo de vida del malware avanzado. Hacemos posible que las organizaciones detecten y combatan el malware avanzado, ya que reunimos soluciones basadas en red y en dispositivos, con el análisis de datos masivos y la inteligencia de seguridad colectiva. Ya que ofrece una solución integrada para ejecutarse en el ciclo de vida de Cisco AMP, Cisco garantiza que las organizaciones estén protegidas antes, durante y después del ataque.

Identifique y bloquee el malware conocido en el perímetro y dentro de la red con Cisco AMP for FirePOWER, tanto en los firewalls de próxima generación como en los dispositivos de IPS de última generación. Proteja los dispositivos estén o no conectados a la red corporativa, con las protecciones combinadas de capa de red de Cisco FirePOWER y el agente basado en dispositivo de Cisco AMP for Endpoints. Todas las ofertas de Cisco AMP aprovechan la nube de Cisco CSI para asegurarse de que el malware identificado después del hecho se detecte y se elimine de manera rápida y eficaz.

Acerca de Cisco

Cisco es el líder mundial en TI. Ayudamos a las empresas a aprovechar las oportunidades del futuro, ya que demostramos que pueden suceder cosas increíbles cuando conectamos lo que antes estaba desconectado.

Brindamos una de los portafolios más completos del sector para protección contra amenazas avanzadas, además de un amplio conjunto de opciones de aplicación y de corrección integradas, ubicuas, continuas y abiertas. Con este modelo de seguridad centrado en las amenazas, los defensores pueden abordar la totalidad de la duración del ataque, en todos los vectores: antes, durante y después del mismo.

Sede central en América
Cisco Systems, Inc.
San José CA

Sede Central en Asia-Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede central en Europa
Cisco Systems International BV Amsterdam.
Holanda

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones y los números de teléfono y fax están disponibles en el sitio web de Cisco en **www.cisco.com/go/offices**.

Impreso en EE. UU. C11-733367-00 14/11