Seguridad intrínseca

Cómo unificar y acelerar la seguridad de los terminales en la empresa

vmware® Carbon Black

Índice

Introducción

Ahora más que nunca, la nube es fundamental para todas las organizaciones del mundo.

Prácticamente toda nuestra atención colectiva está puesta en adaptarnos al COVID-19. Sin embargo, incluso antes de enfrentarse a esta crisis actual, los líderes del sector público y privado ya buscaban formas de expandir las operaciones globales mientras conducían a sus equipos a través de una transformación digital.

Como ya advirtieron muchos ejecutivos, la nube es la manera (en verdad, la única manera viable) en que pueden prosperar los negocios. De hecho, sin importar cuál sea el centro de atención hoy o el próximo año, el futuro alberga la promesa de la nube.

No obstante, toda oportunidad supone un riesgo. En especial cuando se realizan acciones sin tener en cuenta las posibles consecuencias para la seguridad (p. ej., errores de configuración de la nube, contenedores de Amazon S3 sin protección, etc). A menos que la seguridad esté incorporada desde el comienzo, cada paso de la transformación digital correrá riesgo.

Este documento le brinda un plan de desarrollo para implementar su programa de ciberseguridad sobre una base sólida. Al implementar la seguridad unificada en las capas de control básicas (terminales, redes, sistemas de identidad, nubes y las cargas de trabajo en las que se ejecutan), los equipos empresariales pueden disminuir el riesgo y los costos y, a su vez, cumplir con los objetivos de la empresa. A eso se refiere la seguridad intrínseca.

Breve historia de la ciberseguridad

A finales de la década de 1980, se creó, por accidente, el primer gusano informático como parte de un proyecto de investigación que buscaba descifrar el tamaño de la Internet.[1] Desde entonces, aunque no contamos con cifras exactas, determinamos que, cada dos años, la Internet crece a casi dos veces su tamaño.[2]

Por desgracia, los gusanos y virus se siguen autopropagando en la actualidad. La industria de la ciberseguridad respondió a estos (y a otros) riesgos centrándose en las capas, las vías y los vectores específicos que se ven afectados por estos ataques. En lugar de observar estos riesgos en contexto y abordarlos de manera holística, la mayoría de las empresas y los proveedores de seguridad que las respaldan adoptaron un enfoque por vectores.

Con el crecimiento de la industria de la ciberseguridad desde sus inicios, cada proveedor que ingresa al mercado se centra en un aspecto del riesgo cibernético, presente ya sea en los terminales, las aplicaciones o las transacciones y los sistemas de autenticación. Este enfoque de los mejores productos de su tipo fomenta una defensa vulnerable e inconexa, en la que cada equipo se centra en un tipo de producto o aspecto de la infraestructura de TI. Al crear silos de seguridad y operaciones de TI, las empresas incrementan la complejidad y sacrifican la visibilidad unificada.

Además, este enfoque convencional se presta a una respuesta reaccionaria. Los equipos de seguridad de TI se centran demasiado en amenazas puntuales porque no pueden visualizar cada amenaza dentro de un contexto más amplio. Y cuando los equipos perciben la necesidad de mitigar las amenazas, a menudo se ven obligados a descubrir cómo añadir seguridad a los procesos y sistemas, en lugar de abordar el tema de la seguridad desde el inicio.

Independientemente de la industria o de la ubicación geográfica, todas las empresas deben considerar los desafíos que plantea un enfoque de seguridad aislado, adicional y centrado en las amenazas. Por fortuna, existe una solución. Y ahora es el momento oportuno. Si tenemos en cuenta que más del 50 % de los equipos de seguridad y TI manifiestan tener poco personal[3], es fundamental buscar la manera de avanzar para maximizar la efectividad.

1. Forbes. "This Week In Tech History: The Birth Of The Cybersecurity And Computer Industries" (Esta semana en la historia tecnológica: el nacimiento de las industrias de la computación y la ciberseguridad). Gil Press. 1 de noviembre de 2015.
2. Live-Counter.com. "How Big Is The Internet?" (¿Qué tamaño tiene Internet?).
3. VMware Carbon Black. "Informe del panorama de la seguridad 2020". Marzo de 2020.

La seguridad intrínseca representa la visión de VMware de revolucionar la ciberseguridad **integrando** la visibilidad unificada y el control en cada aspecto de la infraestructura de una empresa: redes, cargas de trabajo, nube, espacio de trabajo/terminal e identidad.

REFUERCE SU EQUIPO DE CAZADORES DE AMENAZAS

Una de las principales lecciones que aprendemos de las empresas con una seguridad sólida es que los programas de persecución de amenazas funcionan. En la encuesta SANS 2019, el 36 % de los encuestados informó una mejora notable en las detecciones sólidas y una mejor cobertura tras la implementación de programas de persecución de amenazas.[4] Al igual que un sistema de alarma temprana, los cazadores de amenazas descubren ataques ocultos que pueden haber burlado el radar de los sistemas de seguridad tradicionales, como las herramientas antivirus, las soluciones de administración de eventos e información de seguridad (Security Information and Event Management, SIEM) y los sistemas de detección de intrusiones (Intrusion Detection Systems, IDS). Gracias al descubrimiento proactivo de estos sigilosos indicadores de compromiso de la seguridad, los cazadores de amenazas pueden interrumpirlos antes de que causen estragos importantes. Para obtener información sobre cómo VMware Carbon Black Cloud™ puede potenciar su programa de persecución de amenazas, inscríbase a nuestro *taller virtual "Conviértase en un cazador de amenazas"*.

Componentes de la seguridad intrínseca

Evitar las ciberamenazas requiere de la colaboración de todos. La defensa contra estos ataques constantes nunca ha sido tan difícil si tenemos en cuenta que los equipos de TI tienen a su cargo actualmente cada vez más dispositivos, aplicaciones y datos. Necesitamos con urgencia adoptar un nuevo enfoque que pueda ampliarse para adaptarse a un área de riesgos cada vez mayor. Y eso es lo que ofrece la seguridad intrínseca. De hecho, es la única forma de lograr un avance real en la lucha contra los ciberataques.

Para adaptarse a un área de riesgos cada vez mayor, los equipos de las empresas deben:

- **Ampliar sus defensas:** ir más allá de los silos; implementar una seguridad unificada en los terminales, las cargas de trabajo, las nubes, las redes y las identidades.
- **Profundizar sus análisis:** captar y analizar la actividad conforme a diversos métodos (aprendizaje automático, firmas, análisis del comportamiento, etc.) y a partir de amplios conjuntos de datos (basado en la nube y en los terminales).
- **Expandir su alcance:** integrarse fácilmente con otras tecnologías de seguridad para las cargas de trabajo organizadas y automatizadas.

Este es el marco básico de la seguridad intrínseca. Amplitud. Profundidad. Extensibilidad.

Los tres atributos distintivos en los que se basa la seguridad intrínseca brindan la amplitud, la profundidad y la extensibilidad que necesitan las empresas globales en la actualidad:

- La seguridad se unifica a través de las herramientas y los equipos.
- La seguridad está centrada en el contexto conforme a lo que se pretende proteger.
- La seguridad se incorpora a la infraestructura.

FIGURA 1: Atributos de la seguridad intrínseca.

4. Instituto SANS. "SANS 2019 Threat Hunting Survey: The Differing Needs of New and Experienced Hunters" (Encuesta sobre la caza de amenazas SANS 2019: las diversas necesidades de los cazadores nuevos y existentes). Mathias Fuchs y Joshua Lemon. 25 de octubre de 2019.

Los aspectos fundamentales: cinco puntos de control

Cinco componentes arquitectónicos sirven de sostén a las aplicaciones y los datos que impulsan los negocios empresariales: terminales, cargas de trabajo, nubes, redes y sistemas de identidad. Si se incorpora la seguridad en cada uno de estos puntos de control y se unifican los controles de seguridad a través de un mismo enfoque de administración, los equipos pueden mejorar la seguridad, eliminar la complejidad y obtener eficiencia.

En primer lugar, es fundamental que todos los equipos encargados de administrar los principales puntos de control puedan ver cómo se accede a los datos y a las aplicaciones empresariales. En la tabla 1 se describen los puntos de control y las principales preguntas que enfrentan los equipos que los administran.

PUNTO DE CONTROL	EJEMPLOS	¿QUIÉN ES RESPONSABLE?	¿QUÉ ES NECESARIO SABER?
Terminales	Computadoras portátiles, servidores, sistemas de punto de venta (point-of-sales, POS), etc.	TI o seguridad	• ¿Reforcé mis dispositivos? • ¿Mis terminales son seguros? • ¿Puedo confiar en este dispositivo y permitir la conexión?
Cargas de trabajo	Infraestructura como servicio (IaaS), plataforma como servicio (PaaS), software como servicio (SaaS), nubes múltiples/ híbridas	CloudOps/ Infraestructura/ DevOps/ SecDevOps	• ¿Mis cargas de trabajo tienen la configuración correcta? • ¿Reduje la superficie de ataques en mis cargas de trabajo? • ¿Cómo puedo detectar los problemas que surgen y solucionarlos?
Nubes	Híbridas, perimetrales, públicas, de telecomunicaciones	Equipo de la nube/ proveedor de servicios	• ¿Mis nubes públicas tienen una configuración segura?
Redes	LAN, VLAN, WAN, zona desmilitarizada (DMZ), etc.	Operaciones de red	• ¿Mis redes confiables son seguras? • ¿Microsegmenté mis recursos esenciales? • ¿Tengo tráfico malicioso interno? • ¿Segmenté mi red para limitar el desplazamiento lateral?
Identidades y sistemas de identidad	Active Directory, inicio de sesión único (SSO), administradores de contraseñas, etc.	Propietarios de aplicaciones de seguridad de la información y de TI	• ¿El usuario es quien dice ser? • ¿Puedo confiar en este proceso de autenticación o autorización (p. ej., es previsible este comportamiento)? • ¿Qué credenciales pueden estar vulneradas?

TABLA 1: Puntos de control que impulsan los negocios empresariales.

Para responder estas preguntas de manera rápida y precisa, los equipos deben saber qué ocurre con estos puntos de control y si estos patrones de actividad son normales, inusuales o el indicio de un posible ataque o intrusión.

En la actualidad, la mayoría de los equipos empresariales utilizan múltiples tecnologías a las que acceden mediante diversas consolas para trabajar a diario. La tarea no es menor, como tampoco lo son los intentos de descifrar todos los datos. Por consiguiente, los equipos presentan una limitación en relación con la comprensión que tienen de las amenazas y su capacidad para priorizar las iniciativas de respuesta a incidentes. Y dado que la mayoría de las amenazas guardan relación con más de un punto de control, sigue siendo difícil reconocer el contexto por completo.

Con nuestro enfoque de seguridad intrínseca, se implementa un monitoreo profundo y un análisis del comportamiento en cada punto de control, que luego se unifican para poder reconocer el contexto por completo. De la misma forma que una videocámara registra todos los movimientos de cada punto de control, la seguridad intrínseca permite reconocer el contexto de manera íntegra. Aunque no es necesario recomponer manualmente la telemetría desde distintos puntos de control, los equipos están capacitados para rastrear amenazas desde el punto de entrada y en cada paso intermedio.

Los ataques unificados requieren defensas unificadas

Los atacantes no limitan su actividad nefasta a un solo punto de control. De hecho, los más sofisticados son capaces de permanecer ocultos. La actividad de los atacantes en cualquier punto de control individual puede parecer inofensiva en la superficie. Sin embargo, cuando unificamos todo, estamos mejor preparados para defendernos.

Después de todo, los delincuentes cibernéticos ingeniosos pueden abrirse paso entre las brechas operativas ocultas que se forman cuando los equipos realizan sus actividades en flujos de trabajo aislados. El enfoque de la seguridad intrínseca divide estos silos en puntos de control críticos para que los equipos puedan colaborar con mayor rapidez y coherencia. El contexto completo de la amenaza se comparte entre los equipos para que puedan ser proactivos, se prioricen las amenazas con mayor impacto y se organicen respuestas coordinadas con el fin de obtener mejores resultados.

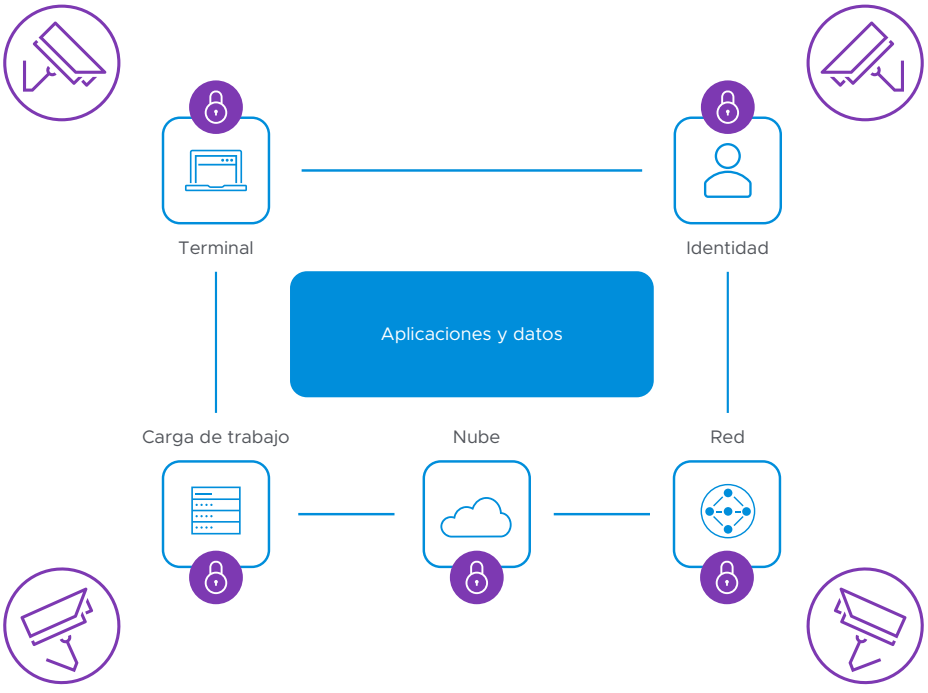

FIGURA 2: Los cinco puntos de control de la seguridad intrínseca.

Este enfoque disminuye los riesgos y los costos. Reforzar los terminales y mejorar la higiene cibernética contribuye en gran medida a la prevención de ataques, incluso antes de que sucedan. Además, nuestro enfoque combina varias capacidades de prevención en lugar de basarse en un solo método, como el aprendizaje automático, las firmas o el análisis de comportamiento. Por este motivo detectamos ataques que pueden pasar desapercibidos para otros proveedores.

Si tiene información clara y exhaustiva sobre lo que ocurre en cada terminal, puede responder con mayor rapidez y precisión. Cuanto antes detecte una amenaza, más probable será que pueda interrumpirla y obtener un mejor resultado.

En la siguiente sección, demostraremos cómo nuestro enfoque le permite ampliar, profundizar y extender sus defensas en algunos escenarios de riesgo comunes.

Ejemplos de escenarios de riesgo

Si bien los equipos de seguridad y de TI deben defenderse de una amplia variedad de ataques, se pueden reconocer ciertos patrones de ataques estándares. Después de todo, saber cómo ocurren los ataques permite que los equipos puedan prepararse mejor, establecer órdenes de prioridad y desarrollar defensas estandarizadas.

Describiremos los pasos típicos que dan los atacantes cuando escogen una víctima y explicaremos cómo las empresas pueden implementar contramedidas de seguridad intrínseca.

Paso 1: Reconocimiento e infiltración

Se emplean distintas tácticas como el análisis de puertos, las sondas de red y la ingeniería social para obtener información sobre la víctima y determinar la mejor manera de infiltrarse en la red. Durante este paso, el objetivo es obtener acceso inicial sin encender las alarmas. Algunos ejemplos de tácticas de infiltración son el compromiso no autorizado (secuestro de sesión de navegador); la explotación de una aplicación pública; el compromiso de un servicio remoto externo (p. ej., VPN); el robo o la reutilización de credenciales y la suplantación de identidad mediante vínculos o archivos adjuntos.

Contramedidas eficaces: Refuerzo y prevención

Las empresas que piensan a futuro disminuyen exponencialmente el área general de riesgos a través de medidas de higiene cibernética sencillas. Con acciones tales como la aplicación de parches en las vulnerabilidades o la ejecución de análisis proactivos y continuos en sus redes, las empresas pueden reducir los problemas a los que deben responder y aumentar así su adaptabilidad y eficiencia en general. Además, cuando implementan una autenticación sólida y protegen el acceso de los trabajadores remotos, las empresas fomentan la productividad de los empleados y evitan que los atacantes pongan en peligro los datos y las comunicaciones empresariales.

Paso 2: Persistencia y manipulación

Cuando el atacante obtiene acceso, su siguiente objetivo es mantenerlo la mayor cantidad de tiempo posible sin ser detectado. La persistencia se logra por medio de distintos métodos, como la manipulación de cuentas válidas y funciones de accesibilidad de los SO; la creación de cuentas nuevas; el acceso a archivos y carpetas ocultos; el uso indebido de perfiles de PowerShell; la modificación de configuraciones de registro y claves de ejecución, y las modificaciones de accesos directos.

Contramedidas eficaces: Monitoreo y detección

El contexto necesario para identificar un ciberataque se obtiene a través del registro de actividad detallada entre terminales y la correlación de estos datos con el tráfico de red y los procesos de autenticación. El enfoque de la seguridad intrínseca permite unificar las pistas que deja un atacante. Dado que VMware Carbon Black Cloud monitorea y analiza constantemente los patrones de comportamiento de cada punto de control, puede descubrir la actividad sigilosa de atacantes que haya pasado desapercibida fuera de un contexto unificado.

Paso 3: Ejecución y exfiltración

No siempre se conoce la intención de los atacantes, aunque es común que roben datos que puedan revender en la Internet oscura. Ya sea con la información privada de un cliente (p. ej., el historial médico) o con los secretos de una empresa (p. ej., el robo de propiedad intelectual o espionaje empresarial), el objetivo de los atacantes es exfiltrar los datos sin encender las alarmas y eliminar todos los rastros de su presencia. Durante ese proceso, los atacantes también pueden desplazarse lateralmente por una red y elevar su privilegio a una instancia superior para encontrar lo que buscan. Una vez que lo logran, suelen cifrar y comprimir los datos para que sean indetectables y se puedan transferir con mayor rapidez (ya sea mediante un canal de comando y control, un protocolo alternativo, otro medio de la red o directamente a la nube).

Según nuestros datos de amenazas, los ataques de ransomware contra las empresas de servicios financieros aumentaron más del 900 % en el corto período desde febrero a abril de 2020.[5]

Contramedidas eficaces: Respuesta y recuperación

Bloquee los desplazamientos laterales no autorizados mediante una microsegmentación para proteger las aplicaciones, los datos y las cargas de trabajo importantes. Establezca protocolos de monitoreo para las cuentas privilegiadas y comunicaciones salientes a servidores de comando y control conocidos. Además, recuerde la importancia de los datos y artefactos forenses detallados. Sin estas pruebas, los líderes no pueden tomar las decisiones correctas sobre cómo procesar la infracción o cómo fortalecer los controles y actualizar las políticas de seguridad.

En los siguientes escenarios de riesgo, describiremos cómo VMware Carbon Black Cloud amplía, profundiza y extiende las defensas de su empresa.

Ransomware

El ransomware es uno de los tipos de malware más disruptivos y costosos. Dado que deja inutilizables los datos y sistemas de la víctima hasta que se paga un rescate, las amenazas de ransomware obligan a las empresas a tomar una decisión intolerable: pagarle al delincuente y hacerlo rápido, o arriesgarse a perder más dinero, mientras ponen en riesgo sus operaciones, su marca y la confianza de sus clientes.

Si bien ninguna industria está a salvo de estos ataques, cada vez hay más ataques de ransomware contra el sector financiero, lo que probablemente se deba a la crisis económica y de salud pública actual. Según nuestros datos de amenazas, los ataques de ransomware contra las empresas de servicios financieros aumentaron más del 900 % en el corto período desde febrero a abril de 2020.[5]

Los costos del ransomware van más allá de pagar el rescate real (si es que se paga) y pueden provocar la pérdida de datos, tiempo fuera de servicio, pérdida de productividad y deterioro de la reputación, sin mencionar todos los costos relacionados con la recuperación: la restauración de los sistemas, los procesos y la reputación de la marca; la formación de los empleados y la realización de investigaciones forenses completas.

¿Cómo funciona?

La punta del iceberg en los ataques de ransomware suele ser un correo electrónico de suplantación de identidad u otra táctica de ingeniería social que engaña a los usuarios para que compartan sus credenciales o descarguen directamente el malware. Dicho esto, en uno de los ataques de ransomware más devastadores, NotPetya, los atacantes explotaron una vulnerabilidad común para infectar los sistemas de las víctimas, sin la necesidad de engañar a los usuarios.

Las últimas innovaciones de ransomware utilizan PowerShell, scripts, macros y ataques basados en la memoria para eludir los antivirus tradicionales basados en firmas. Cuando aprovechan estas tecnologías nativas, los atacantes evitan ser detectados durante las fases de distribución e instalación de un ataque.

Una vez instalado, el ransomware cifra de inmediato algunos o todos los archivos del usuario. Los archivos y el sistema de archivos permanecen cifrados hasta que la víctima sigue las indicaciones del atacante y paga el rescate, momento en el que obtiene una clave de descifrado para restaurar el acceso a sus datos y sistema.

El ransomware es un gran negocio que sigue aumentando exponencialmente. En los foros clandestinos, las publicidades de ransomware como servicio apuntan a atacantes cibernéticos inexpertos que poseen los medios, la orientación y la infraestructura para comenzar su propio negocio con tan solo USD 10 como capital inicial.[6]

Lo que usted puede hacer

A pesar del panorama sombrío, existen medidas concretas que puede tomar para no convertirse en la próxima víctima del ransomware. En concreto, las soluciones de VMware Carbon Black evitan los ataques de ransomware con tres mecanismos de protección específicos. Le explicaremos cómo funciona.

Conozca el estado de seguridad en tiempo real de todos sus terminales. Este es el primer paso fundamental para evitar el ransomware y otros brotes de malware. Con nuestra plataforma, los equipos de seguridad y de TI pueden comprender el estado actual de más de 1.500 artefactos en cualquier terminal y ejecutar evaluaciones

5. VMware Carbon Black. "Atracos modernos a bancos 3.0". Tom Kellermann y Ryan Murphy. Mayo de 2020.

6. Recorded Future. "5 Ransomware Trends to Watch in 2020" (Cinco tendencias de ransomware para observar en 2020). Allan Liska. 13 de febrero de 2020.

continuas para hacer un seguimiento de la higiene de TI. Además, pueden actuar de inmediato y de manera remota con Secure Shell en cualquier terminal dentro o fuera de la red, llevar a cabo investigaciones completas y solucionar las exposiciones que sirven como punto de apoyo para los atacantes de ransomware.

Sugerencia de expertos: Con VMware Carbon Black® Cloud Enterprise EDR™, sus equipos de persecución de amenazas pueden explorar el entorno de manera proactiva y buscar vulnerabilidades que puedan ponerlo en riesgo de sufrir ataques de ransomware.

Combinando un antivirus de próxima generación (NGAV) con la detección y respuesta de terminales (EDR) de comportamiento, VMware Carbon Black Cloud ofrece múltiples capas de capacidades de prevención para identificar y deshabilitar el ransomware y otros tipos de malware. En lugar de basarse solo en firmas o aprendizaje automático, nuestra solución utiliza estos y otros métodos. Nuestra plataforma se actualiza constantemente con inteligencia dinámica de detección de amenazas, lo que incluye las actualizaciones de firmas más recientes, puntajes de reputación y más de 110 comportamientos básicos de atacantes, tales como los TID de MITRE ATT&CK. De esta manera, podemos identificar mejor los ataques de ransomware conocidos antes de que se ejecuten.

Bloquee el acceso a los bienes, identifique variantes y atrápelos. En el caso de que el ataque de ransomware pueda traspasar la primera serie de medidas de prevención y comience la ejecución inicial, nuestro motor de análisis del comportamiento identificará la actividad resultante y la bloqueará antes de que cause daños. En concreto, VMware Carbon Black Cloud monitorea y bloquea los intentos de acceso y modificación con los que se pretende controlar los registros de arranque y las instantáneas. Además, utiliza archivos falsos, que son archivos inofensivos que se alojan en los terminales, para engañar, atrapar y exponer las variantes de ransomware evasivas.

Este enfoque permite que VMware siga mejorando nuestra capacidad de detectar nuevas variantes de ransomware y mejorar nuestras tácticas para interrumpirlas.

Sugerencia de expertos: Con Carbon Black Cloud Enterprise EDR, puede personalizar las detecciones conforme a sus propios datos o aprovechar automáticamente los indicadores de compromiso (indicators of compromise, IoC) nuevos desde VMware Carbon Black Cloud y otros proveedores de inteligencia de detección de amenazas.

Interrumpa los intentos de comunicaciones, repare las brechas y verifique las correcciones. VMware Carbon Black Cloud puede identificar las nuevas variantes de ransomware, incluso para los terminales sin conexión. Por ejemplo, supongamos que el ransomware en cuestión implica un ataque de día cero y no tiene un indicador de reputación registrado. En este escenario, VMware Carbon Black Cloud bloquea la ejecución binaria maliciosa basándose en su comportamiento nefasto. Ningún archivo ejecutable es inofensivo si inserta un código en procesos de ejecución legítimos o inicia nuevos procesos secundarios desde búferes de memoria en paquetes.

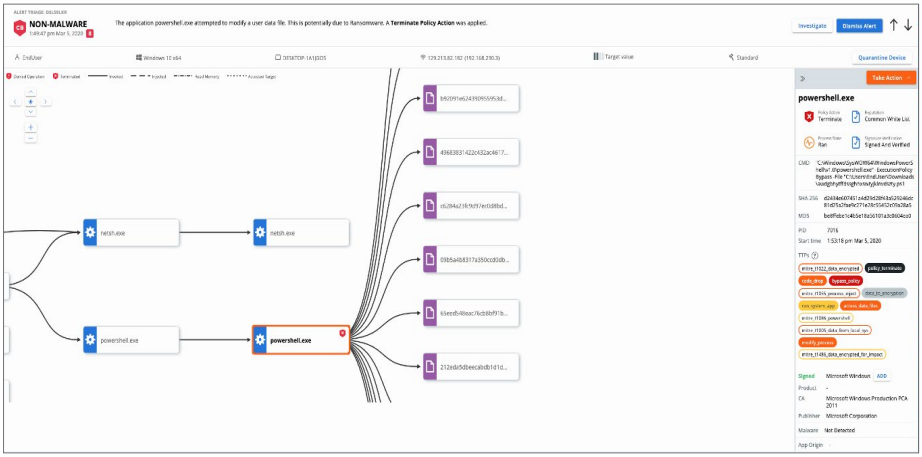

FIGURA 3: Observe todos los procesos y cómo se inician.

Dado que nuestra solución se basa en patrones de ataque en lugar de IoC sin contexto del comportamiento, tiene la inteligencia necesaria para evitar de forma confiable que los archivos ejecutables intenten comunicarse con el servidor de comando y control. Además, ofrece una visibilidad plena de cómo ocurrió el ataque. Con esta información, los equipos de TI y SecOps pueden reparar proactivamente las vulnerabilidades importantes y utilizar nuestra serie de herramientas de corrección para colocar máquinas en cuarentena, bloquear software y eliminar los elementos no deseados.

Sugerencia de expertos: Con VMware Carbon Black® Cloud Audit and Remediation™, los equipos de TI y escritorio pueden realizar consultas en vivo en toda su red de terminales para verificar que se haya reducido eficazmente el brote de ransomware.

Robo y uso indebido de credenciales

Con un conjunto de credenciales válido, los atacantes pueden realizar más actividades maliciosas sin encender ninguna alarma. Por este motivo, las credenciales suelen ser un blanco popular, en especial durante la primera etapa de un ataque. En el último informe Verizon Data Breach Investigation Report (Informe de investigación sobre infracciones de datos de Verizon), se indicó que el 29 % de las infracciones de datos involucraron el uso de credenciales robadas.[7]

Según el informe Cost of a Data Breach (Informe sobre el costo de las filtraciones de datos) 2019 de IBM Security y Ponemon Institute, el costo promedio total de una infracción de datos es de USD 3,92 millones.[8] Con este precio tan elevado, es increíble que algo tan simple como un nombre de usuario y una contraseña de tipo administrativo sirvan de resguardo contra lo que podría ser una amenaza existencial para muchas empresas.

Las cuentas privilegiadas son los recursos más valiosos para un atacante. Con una cuenta privilegiada, los atacantes prácticamente tienen las llaves de toda la empresa. Pueden crear nuevas cuentas, modificar las existentes para otorgar privilegios excesivos y eliminar los rastros de su trabajo poniendo a cero los archivos de registro que dejan constancia de su actividad.

Si su objetivo es robar los datos de una empresa o de un cliente, los atacantes pueden vender las credenciales robadas en el mercado negro a alguien que desee realizar espionaje corporativo o algún ciberdelito.

¿Cómo funciona?

Por lo general, los atacantes obtienen acceso a las credenciales a través de la suplantación de identidad o la suplantación de identidad dirigida. Otros métodos comprenden robar credenciales mediante ataques de inyección SQL, desarrollar scripts entre sitios (XSS), realizar secuestros de sesiones o realizar ataques de tipo "man in the middle" contra los sitios web. Algunos de los ataques más insidiosos a credenciales utilizan herramientas nativas autorizadas, como PowerShell, para que la actividad parezca legítima a primera vista y evitar que se enciendan las alarmas.

Cuando los atacantes tienen credenciales en un terminal, el siguiente objetivo es expandir ese privilegio y desplazarse lateralmente en la red para buscar datos valiosos, como datos confidenciales de clientes o datos de la propiedad empresarial. Además, buscan ampliar sus privilegios comprometiendo el controlador de dominios y la base de datos de Active Directory.

Lo que usted puede hacer

Otorgue facultades y formación. Cada empleado de una empresa es un administrador clave de la seguridad cibernética. Asegúrese de que sus empleados comprendan su rol y facilíteles la protección de sus credenciales con un software de administración de contraseñas, o bien oculte por completo las credenciales con un inicio de sesión único (SSO). La autenticación de factores múltiples es otro elemento imprescindible para las empresas globales, en particular para aquellas con empleados que se conectan desde cualquier parte del mundo.

Revise periódicamente las cuentas de dominio con privilegios y su acceso a las cuentas de dominio VIP para evaluar si son necesarias y si tienen un propósito legítimo en las operaciones empresariales. Dado que estas credenciales son los principales objetivos de los atacantes, vigílelas de cerca y limítelas a la menor cantidad de personas posible.

7. Verizon. "2020 Data Breach Investigations Report" (Informe de investigación sobre infracciones de datos 2020).
8. IBM Security y Ponemon Institute. "Cost of a Data Breach Report" (Informe sobre el costo de las filtraciones de datos). 2019.

Sugerencia de expertos: Carbon Black Cloud Audit and Remediation permite que los equipos realicen evaluaciones de configuración de seguridad de cualquier aspecto de la configuración de un terminal, con el fin de verificar si los empleados cumplen con las políticas de uso corporativas (p. ej., el uso de un software de administración de contraseñas). Lo mismo ocurre con la configuración del controlador de dominio, ya que dificulta que los atacantes roben las credenciales.

Detecte un ataque sigiloso, bloquéelo automáticamente y enfréntelo. Proteger y monitorear los controladores de dominio y las cuentas administrativas que tienen acceso directo a Active Directory es un paso fundamental para detener un ataque antes que de comience.

VMware Carbon Black Cloud detecta los ataques orientados al robo de credenciales que se ocultan detrás de aplicaciones nativas autorizadas como PowerShell. Nuestra herramienta de procesamiento de flujo de eventos detecta cualquier comportamiento inusual en un terminal, incluso si el proceso está autorizado. En este ejemplo, vemos que PowerShell inicia lsass.exe. Una vez que se compromete la seguridad, los atacantes tienen acceso pleno a las credenciales de la cuenta de dominio gracias a este archivo ejecutable. Como este comportamiento es inusual y muy sospechoso, VMware Carbon Black Cloud bloquea la acción de inmediato y de manera local en el terminal y envía una alerta.

Recopile datos forenses y actualice automáticamente las políticas de seguridad. Aunque es posible frustrar el ataque de robo de credenciales, sigue valiendo la pena conectarse al terminal para investigar si existe una exposición adicional o alguna otra actividad de atacantes. Utilice VMware Carbon Black Cloud para aislar los sistemas afectados y acceder a ellos de forma remota a través de Secure Shell para realizar una evaluación más minuciosa e implementar pasos de corrección adicionales.

VMware Carbon Black Cloud recopila y almacena automáticamente datos forenses detallados para que pueda investigar el intento de infracción y utilizar estos datos para actualizar las políticas de seguridad de los terminales en conjunto. Por ejemplo, si descubrió que el uso indebido de las credenciales involucraba el acceso remoto a una cuenta administrativa, puede agregar una regla que permita el acceso remoto a cuentas administrativas únicamente desde una lista aprobada de direcciones IP o rango de direcciones.

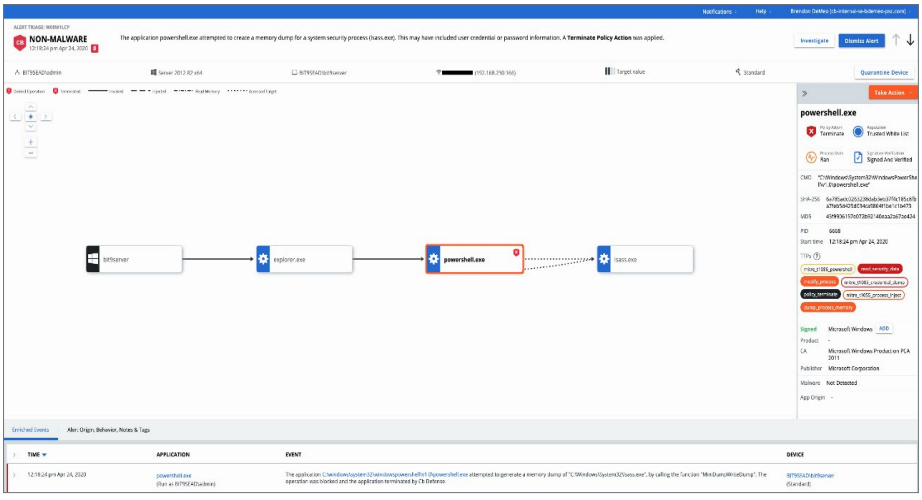

FIGURA 4: Evalúe el proceso de manera detallada.

Revisar minuciosamente los datos forenses cuando se investiga un incidente brinda detalles importantes y precisos sobre lo que ocurrió en el sistema. Los equipos de seguridad pueden aprovechar los registros de auditoría externos de esta actividad, para así tener toda la información necesaria para tomar una decisión precisa e inmediata sobre lo que ocurrió exactamente y el alcance del incidente. Sin este nivel de registro de auditoría de actividades independiente, uno asumiría que el alcance es mayor, lo que generaría una cantidad excesiva de informes.

Por otra parte, los análisis forenses pueden aprovecharse para validar lo ocurrido con la mayor precisión posible. Sin embargo, esto es muy costoso y engorroso, requiere mucho tiempo y es necesario contar con excelentes conocimientos sobre el tema. Aun así, el análisis forense a veces solo ofrece la mejor conjetura basada en las pruebas que quedan en el host.

Suplantación de identidad, suplantación de identidad dirigida y otros ataques por correo electrónico

Los delincuentes cibernéticos se parecen mucho a otros estafadores o timadores. Aprovechan las crisis, como la pandemia de COVID-19, para lograr mediante engaños que sus víctimas actúen, y la suplantación de identidad es la manera perfecta de hacerlo. Según el informe 2020 Verizon Data Breach Investigation Report (Informe de investigación sobre infracciones de datos 2020 de Verizon)[9], se utilizaron tácticas de suplantación de identidad en el 32 % de las infracciones de datos. Sin embargo, es probable que esa cifra aumente en el informe de 2021.

Incluso antes del brote de COVID-19, los ataques de suplantación de identidad ya estaban en aumento y a punto de alcanzar su mayor nivel en los últimos tres años.[10] Por lo general, una campaña de suplantación de identidad tiene como objetivo robar credenciales, por lo que los atacantes engañan a los empleados para que visiten páginas falsas de inicio de sesión con el fin de robar sus credenciales. Sin embargo, los atacantes están reforzando sus técnicas y añadiendo trampas más sofisticadas orientadas a empleados que trabajan desde casa, con aplicaciones móviles, mapas sobre el COVID-19 y software de red privada virtual (VPN) falsos.

La suplantación de identidad dirigida es un es un tipo de suplantación con objetivos muy concretos. A menudo, atacan a personas importantes, como ejecutivos o miembros de juntas directivas, utilizando información que obtienen a partir de datos disponibles públicamente (p. ej., sitios de redes sociales, artículos periodísticos, etc.) para que sus mensajes sean más creíbles.

¿Cómo funciona?

El enmascaramiento es un elemento fundamental de los ataques de suplantación de identidad y suplantación de identidad dirigida. Ocurre cuando se manipula el nombre y la ubicación de un archivo ejecutable (legítimo o malicioso) para evadir las defensas y la detección. Ya sea a través de un adjunto de correo electrónico malicioso enmascarado como uno benigno o de una página de inicio de Office 365 con estructura incorrecta que se haga pasar como legítima, el objetivo es siempre engañar al usuario para que haga clic en el elemento. Cuando el usuario lo hace, el atacante tiene la oportunidad de obtener un acceso inicial.

Por lo general, se utilizan archivos adjuntos en los correos electrónicos para llevar a cabo una infección inicial. Algunos de los tipos de archivos adjuntos que se utilizan tienen las siguientes extensiones: ZIP, 7Z, TAR, RAR, JAR, VBS, IMG, GZ, EXE, ISO, SCR, RTF, PDF, DOC, XLS. Los correos electrónicos de suplantación de identidad suelen contener encabezados falsos y mensajes auténticos para engañar a la víctima con un sentido de seguridad falso. Además, los estafadores utilizan nombres atractivos en los archivos adjuntos para hacer que los usuarios los abran.

Cuando se abre el archivo adjunto, se ejecuta el malware incorporado al documento (p. ej., una macro maliciosa de Microsoft Office que utiliza un código VBA). La unidad de análisis de amenazas de VMware Carbon Black también observó recientemente el uso de un archivo adjunto ISO que contenía un archivo PE enmascarado como archivo SCR. Cuando se ejecuta, el archivo PE implementa RemCos. RemCos es una herramienta comercializada de administración remota (remote administration tool, RAT) que suele ofrecerse mucho en la Internet oscura.[11]

Con acceso remoto y un conjunto válido de credenciales, los atacantes pueden causar mucho daño dentro de una organización, por lo que es fundamental que las empresas detecten los accesos iniciales y frustren las ejecuciones.

Lo que usted puede hacer

Instruya a sus empleados. Como con cualquier ataque de ingeniería social, los estafadores se aprovechan de la naturaleza humana: nuestra curiosidad y nuestra capacidad única de distraernos fácilmente. Instruya a sus empleados para que puedan advertir una posible suplantación de identidad, aliéntelos a que sean

9. Verizon. "2020 Data Breach Investigations Report" (Informe de investigación sobre infracciones de datos 2020).

10. Comparitech. "Phishing statistics and facts for 2019–2020" (Datos y estadísticas de suplantación de identidad del período 2019-2020). Sam Cook. 7 de febrero de 2020.

11. VMware Carbon Black. "Análisis técnico: Hackers que sacan provecho de la pandemia de COVID-19 para lanzar ataques de suplantación de identidad, aplicaciones/mapas falsos, troyanos, puertas traseras, criptomineros, redes de robots y ransomware". Jared Myers y Ed Murphy. 19 de marzo de 2020.

escépticos y enséñeles a detectar las estafas. Por ejemplo, recuérdeles que nunca es aceptable realizar solicitudes de información personal, nombres de usuario y contraseñas por correo electrónico.

Aliéntelos a desconfiar de los errores gramaticales y ortográficos, las imágenes y los enlaces rotos y otras características que parezcan extrañas en un correo electrónico. O mejor aún, configure una dirección de correo electrónico a la que puedan enviar los correos sospechosos con el fin de realizar una investigación exhaustiva **antes** de abrir algún archivo adjunto o hacer clic en un enlace. Considere implementar simulaciones seguras de suplantación de identidad y programas de capacitación que evalúen y aumenten el reconocimiento de los intentos de suplantación de identidad y suplantación de identidad dirigida (p. ej., Gophish) por parte de sus empleados.

Desenmascare la actividad maliciosa. Aunque un usuario cometa el error de abrir un archivo adjunto malicioso o haga clic en una página de inicio de sesión falsa y ponga en marcha el acceso inicial de un atacante, no todo está perdido. Por ejemplo, VMware Carbon Black Cloud identificará el proceso malicioso que se haga pasar por uno legítimo según el comportamiento. Nuestra plataforma capta y recopila detalles sobre qué procesos primarios se inician con qué procesos secundarios, lo que nos permite detectar los comportamientos inusuales y detener un ataque de suplantación de identidad en curso.

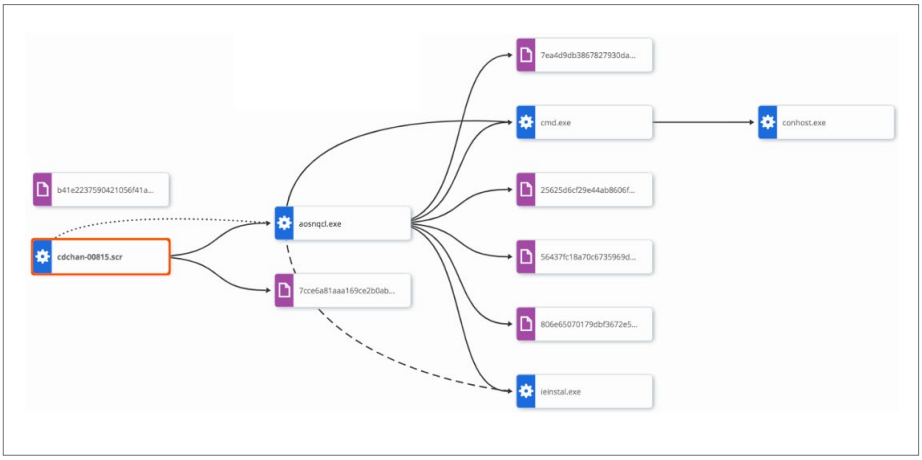

FIGURA 5: Descubra los comportamientos maliciosos.

Sugerencia de expertos: VMware Carbon Black® Cloud Managed Detection™ amplía los equipos de seguridad empresarial ofreciendo un monitoreo avanzado de alertas y una clasificación de amenazas para notificar las amenazas que podrían exponer a su empresa a los riesgos de suplantación de identidad o suplantación de identidad dirigida.

Puedes engañarme una vez, pero no siempre. Una vez que se frustra el ataque de suplantación de identidad o suplantación de identidad dirigida, es fundamental reconocerlo (o reconocer otros semejantes) en el futuro.
Carbon Black Cloud Enterprise EDR recopila y visualiza información detallada sobre los ataques a los terminales y facilita los análisis de la causa principal.
El motor de análisis del comportamiento de VMware Carbon Black Cloud analiza automáticamente el comportamiento del ataque y garantiza que los terminales de todos los clientes a nivel mundial queden protegidos en el futuro contra este tipo de comportamiento. Este perfil de protección es sumamente eficaz porque, como previene los ataques conforme al comportamiento, los atacantes deben elaborar nuevas técnicas de ataque para su próximo intento. Otros métodos de prevención suelen basarse en indicadores de compromiso muy frágiles que pueden modificarse con mucha facilidad, como hashes de archivos maliciosos, nombres de hosts, direcciones IP y claves de registro. Además, VMware Carbon Black Cloud le permite crear fácilmente listas de vigilancia personalizadas que lo alerten cada vez que se lance un ataque similar.

Por ejemplo, si vimos que un RAT como RemCos puede instalarse e iniciar una conexión a una dirección IP en Irán, podemos crear una lista de vigilancia que nos alerte para bloquearla si vuelve a ocurrir.

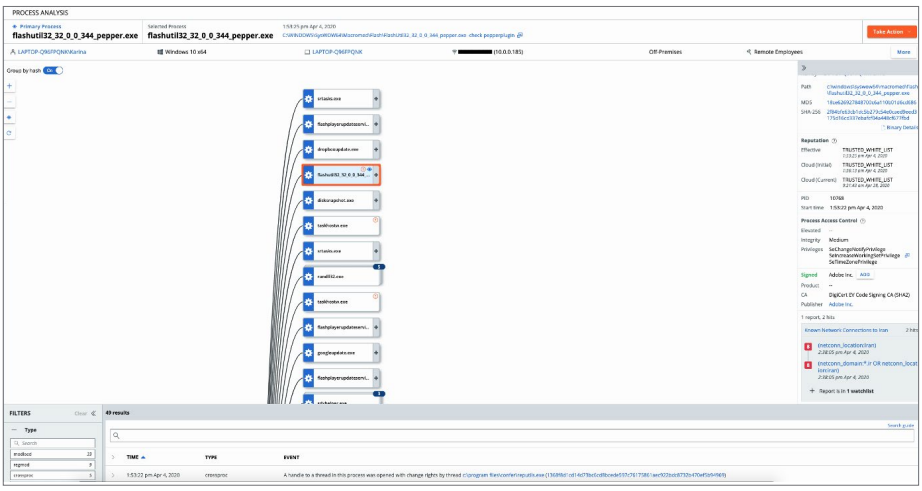

FIGURA 6: Los datos pormenorizados respaldan las investigaciones.

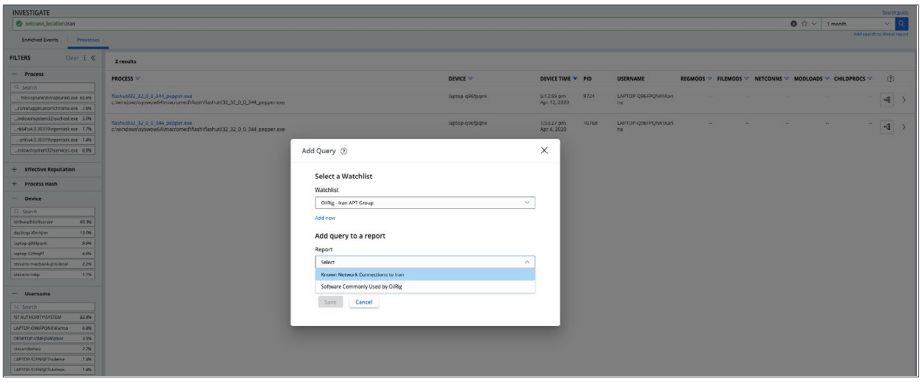

FIGURA 7: Configuración de listas de vigilancia personalizadas.

MÁS INFORMACIÓN

Para solicitar una demostración personalizada o probar el producto gratis en su organización, visite *carbonblack.com/trial.*

Para obtener más información o para comprar los productos de VMware Carbon Black, llámenos al 855-525-2489 en los Estados Unidos o al +44-118-908-2374 en Europa, Medio Oriente y África (EMEA).

Para obtener más información, escriba a *contact@carbonblack.com* o visite *carbonblack.com/epp-cloud.*

Resumen

Las empresas enfrentan una lucha cuesta arriba contra los delincuentes cibernéticos. Con el lastre de tecnologías obsoletas y complejas que no mitigan los ataques sofisticados y las amenazas mixtas, los equipos necesitan una nueva forma de avanzar. Una forma que aproveche al máximo los equipos y los presupuestos reducidos, que se integre fácilmente a las tecnologías y flujos de trabajo existentes, y que proporcione una seguridad confiable en todos los puntos de control de una empresa.

La seguridad intrínseca de VMware Carbon Black se encarga precisamente de ello.

Como uno de los líderes en protección de terminales nativos de la nube, nos dedicamos a proteger al mundo de los ataques cibernéticos. VMware Carbon Black Cloud es una plataforma de protección de terminales (EPP) nativos de la nube que combina el fortalecimiento de los sistemas inteligentes y la prevención de comportamientos, necesarios para mantener alejadas las amenazas emergentes, con un solo agente ligero y una consola fácil de usar.

Mientras que otros productos de seguridad de terminales solo recopilan un conjunto de datos relacionados con lo que ya se sabe que es malo, VMware Carbon Black Cloud recopila datos exhaustivos de actividad de terminales de manera continua y analiza los patrones de comportamiento de los atacantes para detener proactivamente los ataques cibernéticos antes de que desaten el caos.

Cuando detienen estas anomalías rápidamente, los equipos de seguridad obtienen visibilidad, descubren las causas principales de los ataques con prontitud y toman medidas.

Con una comunidad de usuarios activa y una amplia red de integración, que incluye API abiertas, documentación y herramientas para desarrolladores, estará bien protegido cuando establezca nuestra plataforma en su entorno.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 EE. UU. Tel.: 877-486-9273 Fax: 650-427-5001 www.vmware.com