Protección frente al ransomware con Proofpoint

Cómo evitar que el ransomware arraigue y se propague por su organización

Productos

- Proofpoint Advanced Threat Protection
- Proofpoint Cloud Security

Ventajas principales

- Prevención de riesgos iniciales
- Prevención del descubrimiento, del movimiento lateral y la persistencia
- Prevención de la filtración de datos

El ransomware es una de las formas de ciberataque más destructivas. Arruina a empresas, obliga a hospitales a rechazar a pacientes y paraliza gobiernos. Se ha convertido en la actualidad en una de las ciberamenazas más peligrosas. Solo el año pasado, Estados Unidos sufrió más de 65 000 ataques de ransomware. Esta amenaza es una preocupación para la mayoría de los CISO y se ha convertido en un problema de seguridad nacional. Y lo que es todavía más alarmante, muchas organizaciones se encuentran totalmente desarmadas para hacer frente a un ataque de ransomware. Solo el 13 % de los expertos de TI entrevistados por el Ponemon Institute afirmaron que su empresa es capaz de prevenir un ataque de ransomware. Y más del 68 % se consideran "vulnerables" o "muy vulnerables" [1].

Los mensajes de correo electrónico y la web son los principales vectores de ataque del ransomware. Actualmente, la mayoría de esos ataques se llevan a cabo en varias fases. El correo electrónico o los sitios web comprometidos juegan un papel fundamental en las primeras fases de la cadena de ataque. A menudo, distribuyen una payload (carga útil) en forma de descargador de malware. Esta carga está diseñada para penetrar en el sistema de un usuario, con el fin de robar credenciales de conexión y acceder a la red del usuario. Los operadores de ransomware también practican el robo de credenciales de conexión para acceder a servicios expuestos a Internet. Las tácticas más comunes incluyen los mensajes de correo electrónico de phishing, los ataques por fuerza bruta de contraseñas y los compromisos por descarga desapercibida.

Una vez conseguido el acceso inicial, los responsables del ransomware establecen la persistencia, realizan una misión de reconocimiento y se mueven lateralmente. Desde dentro, los ciberdelincuentes no solo pueden cifrar archivos confidenciales, sino que también pueden filtrar información sensible para utilizar en tácticas de doble extorsión.

En paralelo a la mejora de la capacidad de las soluciones de copia de seguridad y recuperación a la hora de frustrar los ataques de ransomware, se ha producido una evolución de las tácticas de los ciberdelincuentes para superarlas. En la actualidad se utiliza el conocido como ransomware de doble extorsión. Esta táctica consiste en filtrar datos confidenciales y, a continuación, cifrar los archivos. Si la empresa víctima del

1 The Ponemon Institute. "The Rise of Ransomware" (El aumento del ransomware) enero de 2017.

ataque se niega a pagar por del descifrado de los archivos, el ciberdelincuente dispone de tres opciones para reclamar el pago:

- Amenazar a la víctima con divulgar datos en línea.
- Vender los datos al mejor postor.
- Enviar mensajes de correo electrónico a los clientes y partners de la víctima amenazándoles con divulgar sus datos.

El correo electrónico es el principal vector de infección y por esa razón un gran porcentaje de los ataques de ransomware empiezan, directa o indirectamente, por un mensaje de phishing. Estos mensajes incitan a los usuarios a abrir un adjunto malicioso o a hacer clic en una URL maliciosa. Solamente las soluciones avanzadas le permiten detectar y bloquear este tipo de amenaza antes de que comprometan las credenciales de conexión de un usuario. Como consecuencia de la migración a gran escala de datos empresariales a la nube, cada vez son más los archivos de contraseñas y datos sensibles que se almacenan en ella. Es importante limitar la exposición de datos en la nube para reducir el volumen de datos susceptibles de ser compartidos con los ciberdelincuentes.

Proofpoint ha observado que los ataques de ransomware son cada vez más dirigidos, más devastadores y más perturbadores para las actividades de las empresas. Proofpoint Advanced Threat Protection y Proofpoint Cloud Security pueden ayudarle a prevenirlos. Nuestras plataformas completas e integradas reducen el riesgo de ataque de ransomware gracias a varios niveles de controles que permiten:

- Prevenir las infecciones iniciales.
- Detectar el acceso inicial e impedir el descubrimiento, el movimiento lateral y la persistencia.
- Prevenir la filtración de datos.

Prevenir las infecciones iniciales

Proofpoint Advanced Threat Protection y Proofpoint Cloud Security previenen las infecciones iniciales gracias a que:

- Detectan y bloquean el ransomware y los descargadores de malware que originan la distribución de ransomware.
- Previenen los compromisos de credenciales.
- Ofrecen visibilidad de los riesgos de ataque de ransomware.
- Aíslan los clics en una URL en función del riesgo.
- Forman a los usuarios para que sean capaces de identificar y denunciar los mensajes de correo electrónico maliciosos.
- Automatizan la corrección de las amenazas por correo electrónico.

Detección y bloqueo de ransomware y descargadores de malware

La plataforma Proofpoint Advanced Threat Protection detecta y bloquea el ransomware como payload inicial. También bloquea el malware que origina el ransomware. Contamos con varios motores basados en el aprendizaje automático que permiten detectar el malware, el código malicioso y las técnicas de detección de la evasión. Esto protege a los usuarios de los sitios web maliciosos o de los archivos infectados con ransomware.

La plataforma realiza un análisis de la reputación y del contenido. Asimismo, ejecuta un análisis en entorno aislado (sandbox) en profundidad de las amenazas ocultas en URL o archivos adjuntos. Empleamos análisis predictivo que identifica y aísla las URL sospechosas en función de las tácticas de los atacantes. Por ejemplo, la plataforma analiza en entorno aislado todas las URL de sitios web legítimos para compartir archivos debido a su uso cada vez mayor para alojar malware. Las soluciones que dependen de un análisis de reputación no podrían detectar estos ataques.

Prevención de los compromisos de credenciales.

Los ciberdelincuentes utilizan distintas tácticas para robar las credenciales de un usuario: phishing, ataques por fuerza bruta, la web oscura (Dark Web) e información expuesta en el almacenamiento en la nube de un usuario. Una vez que han conseguido las credenciales, ya no es necesario enviar un descargador. Basta con que el ciberdelincuente utilice sus credenciales para conectarse a su VPN o a los servicios web. A partir de ahí solo tienen que robar los datos confidenciales o cifrar los archivos. La adopción cada vez mayor de servicios cloud expone a las empresas a usuarios negligentes que transfieran archivos de contraseñas y otros datos sensibles en la nube.

Proofpoint Advanced Threat Protection detecta y bloquea los mensajes de phishing mediante varios motores de detección, incluidos clasificadores de aprendizaje automático que realizan la inspección de las URL. Proofpoint Cloud Security permite identificar la información sensible expuesta en cuentas cloud que pueden aprovechar los ciberdelincuentes.

Visibilidad del riesgo de ataque de ransomware

Proofpoint le permite identificar a sus VAP (Very Attacked People™ o personas muy atacadas), que son las personas de su empresa más expuestas a ataques. También puede saber quiénes son los empleados más atacados y qué amenazas reciben. Estos datos le permiten ajustar su estrategia de defensa a las amenazas específicas a las que se enfrentan sus VAP.

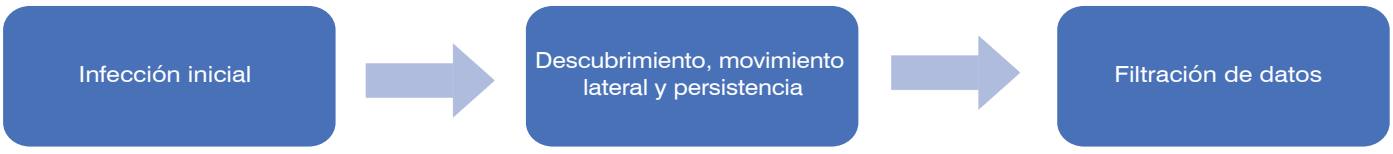

Figura 1: Tres niveles de protección.

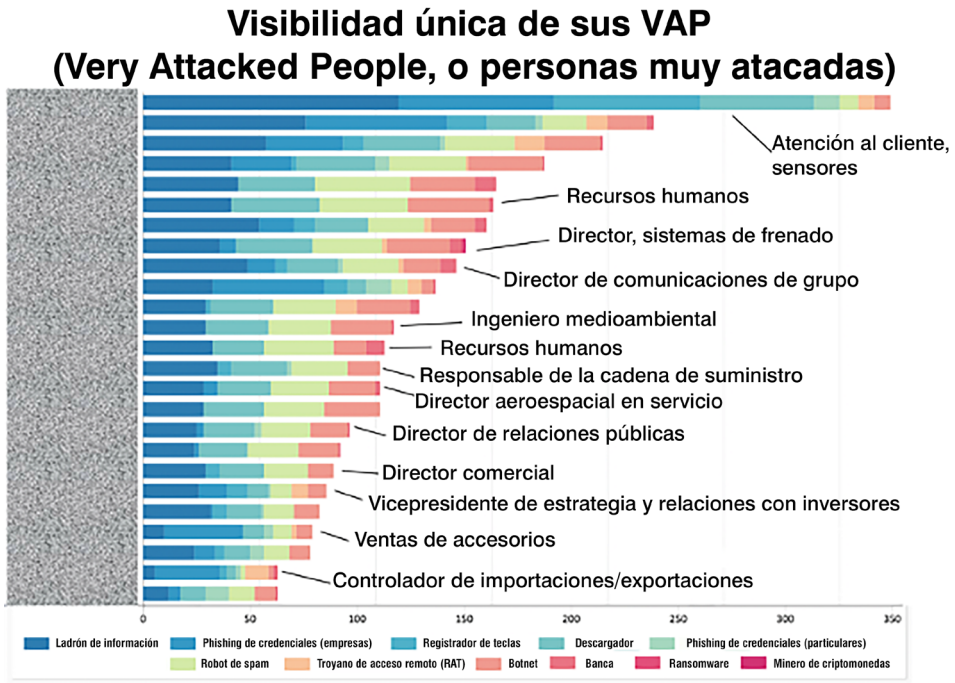

Figura 2: Proofpoint le permite identificar a sus VAP (Very Attacked People o personas muy atacadas).

Proofpoint también proporciona información detallada sobre las amenazas y las campañas. El panel Threat Insight muestra los datos forenses detallados sobre los ciberdelincuentes, las formas de propagación, ejemplos de mensajes, los destinatarios previstos, la progresión del ataque, etc.

Reducción del impacto gracias al aislamiento integrado del correo electrónico

Los ciberdelincuentes pueden añadir carga maliciosa a las URL tras su entrega. Esta estrategia permite evadir la detección inicial. Proofpoint Browser Isolation reduce el impacto de la activación de URL maliciosas por los usuarios. Ofrece una protección en tiempo real durante el clic en las URL de los mensajes de correo electrónico corporativos y aísla la actividad de navegación en un contenedor seguro que muestra exclusivamente una versión protegida a los usuarios. Asimismo, previene los descargadores iniciales y el robo de credenciales, lo que permite interrumpir la cadena de ataque.

Puede implementar un aislamiento basado en los riesgos según la política y la información sobre sus VAP, enviar las URL de mayor riesgo en sesiones de navegación aisladas, definir reglas más estrictas para las personas objetivo aislando todos sus clics e incluso adaptar la política de aislamiento en función del riesgo del usuario y de la URL en la que hace clic.

Concienciación de los usuarios sobre la seguridad

La prevención de los ataques de ransomware pasa inevitablemente por la formación de sus empleados. Ellos constituyen la última línea de defensa de la empresa.

Para que una ataque de ransomware tenga éxito, es necesario que un usuario haga clic en un enlace o descargue un archivo adjunto. Según el informe DBIR 2021 de Verizon, en el 85 % de los incidentes del año pasado intervino el factor humano[2].

La plataforma Threat Protection incluye formación para concienciar en materia de seguridad destinada a sensibilizar a los usuarios sobre los ataques de ransomware y a formarlos para que no hagan clic en los mensajes sospechosos. Puede reforzar la formación de los usuarios más atacados y de los que ya han sido víctimas de un ataque real. Para consolidar la formación de los usuarios, puede utilizar los recursos de nuestra biblioteca de contenidos en sus comunicaciones internas y alertas de seguridad. También puede ejecutar simulaciones de ataques con plantillas basadas en señuelos reales observados en los miles de millones de mensajes que analiza Proofpoint. La plataforma proporciona mecanismos simples para denunciar los mensajes sospechosos, como el botón PhishAlarm y las etiquetas de advertencia en el correo electrónico.

Automatización de la corrección de mensajes maliciosos

Los equipos de seguridad a menudo sufren carencias de personal y se ven inundados de alertas que deben filtrar y analizar rápidamente. La plataforma Threat Protection garantiza la orquestación, automatización y respuesta a incidentes de seguridad contra el correo electrónico (mSOAR). Automatiza la investigación corrección de los mensajes maliciosos o no deseados denunciados por los usuarios.

2 Verizon. "DBIR: Data Breach Incidentes Report" (Informe sobre las investigaciones de fugas de datos) 2021.

Las credenciales de las cuentas de los usuarios son las llaves de acceso a su empresa. Basta con un nombre de usuario y una contraseña para que un operador de ransomware lance ataques dentro y fuera de su empresa.

Estos mensajes se analizan automáticamente y se completan con múltiples sistemas de inteligencia de amenazas y de reputación. Si el mensaje es malicioso, puede ponerse en cuarentena automáticamente, junto con todos los mensajes relacionados. Elimina la necesidad de investigar cada alerta y de corregir manualmente los mensajes maliciosos. Esto permitirá a su equipo de seguridad ahorrar una enorme cantidad de tiempo y esfuerzo. Para cerrar el círculo, los usuarios reciben un mensaje personalizado que confirma la naturaleza maliciosa del mensaje, lo que sirve para reforzar los buenos comportamientos.

La plataforma Threat Protection analiza los mensajes incluso una vez entregados. Si identifica un elemento sospechoso después de la entrega, el mensaje se extrae automáticamente de la bandeja de entrada del usuario, incluso si los mensajes se han reenviado a otros usuarios o se enviado a través de listas de distribución.

Detectar el acceso inicial e impedir el descubrimiento, el movimiento lateral y la persistencia

Proofpoint Cloud Security detecta las amenazas de ransomware gracias a que:

- Supervisa y detecta las cuentas cloud comprometidas.
- Supervisa las subidas de archivos maliciosos a cuentas cloud.
- Protege de payloads de mando y control con Web Security.

Detección de la usurpación de cuentas cloud

Las credenciales de las cuentas de los usuarios son las llaves de acceso a su empresa. Basta con un nombre de usuario y una contraseña, sobre todo en el caso de aplicaciones cloud como Microsoft 365 o Google Workplace, para que un operador de ransomware lance ataques dentro y fuera de su empresa. La solución CASB de Proofpoint Cloud Security ofrece controles adaptables de acceso en tiempo real basados en el riesgo, el contexto y la función. Bloquea automáticamente los intentos de acceso a apps cloud desde ubicaciones peligrosas o por parte de ciberdelincuentes conocidos. Proofpoint CASB también utiliza datos contextuales para confirmar la identidad de un usuario e impedir el acceso de riesgo, como la ubicación del usuario, el dispositivo, la red y el momento de la conexión. Puede definir políticas de acceso, como la aplicación de identificación multifactor y la restricción del acceso desde dispositivos no gestionados para proteger frente a los operadores de ransomware.

Proofpoint le ofrece una visibilidad inigualable para identificar la propagación lateral o los riesgos a los que se exponen los datos de una cuenta comprometida. También puede determinar si una conexión sospechosa está asociada a una cuenta que envía mensajes de correo electrónico maliciosos, así como si un ciberdelincuente intentó instalar un acceso persistente mediante la definición de reglas de reenvío o de delegación de mensajes de correo electrónico mediante tokens OAuth. Asimismo, le permite conocer el tipo de actividad de los archivos sospechosos.

Prevención de la distribución de ransomware desde aplicaciones cloud

El ransomware puede propagarse al compartir archivos infectados y mediante la sincronización automática. Puede tener repercusiones graves para su organización, sus partners y sus clientes. Proofpoint Cloud Security supervisa activamente los recursos compartidos de archivos en la nube y sus alertas en caso de archivos sospechosos. Gracias al uso de análisis en entorno aislado (sandbox) de los archivos de las apps cloud, puede contener estos archivos maliciosos en la nube a través de una cuarentena automatizada y otros medidas de mitigación.

Protección frente a payloads de mando y control con Web Security

Una vez comprometido, el dispositivo envía una señal a los servidores del ciberdelincuente. El ciberdelincuente envía entonces el siguiente conjunto de instrucciones. Gracias al control del dispositivo, el operador de ransomware puede llevar a cabo una serie de acciones, como la distribución de ransomware o la filtración de datos.

Las funciones Web Security y Browser Isolation de Proofpoint Web Security bloquean las conexiones a sitios web comprometidos. De esta forma impiden que el operador de ransomware controle el dispositivo y cause más daño. La inteligencia sobre amenazas está optimizada por Proofpoint Nexus Threat Graph, que combina billones de puntos de datos en tiempo real de múltiples vectores de amenazas de todo el mundo, tecnologías avanzadas de inteligencia artificial y aprendizaje automático, así como un equipo internacional de investigadores que permite ir un paso por delante de las ciberamenazas más peligrosas.

Prevenir la filtración de datos

Proofpoint Advanced Threat Protection y Proofpoint Cloud Security previenen la filtración de datos gracias a que:

- Supervisan los primeros signos de filtración de datos.
- Detectan e impiden todo movimiento de datos no autorizado.

Las funciones Web Security y Browser Isolation de Proofpoint Cloud Security ofrecen una seguridad de datos con reconocimiento de riesgos que permite prevenir la pérdida de datos en tiempo real. Junto con Browser Isolation, Web Security permite aplicar controles de acceso granulares, como el acceso de solo lectura y permitir o bloquear las aplicaciones cloud y la web. Browser Isolation protege el acceso de los usuarios a los datos y las aplicaciones aislando las sesiones del navegador en un contenedor seguro.

Además, Proofpoint CASB le ayuda a conseguir visibilidad instantánea de la actividad de los archivos sospechosos, que puede relacionarse con inicios de sesión sospechosos. Los equipos de seguridad pueden diferenciar rápidamente una actividad de archivo iniciada por un ciberdelincuente de una iniciada por un usuario, e intervenir a tiempo.

Proofpoint no solo protege los datos sensibles de las aplicaciones cloud, puede bloquear la filtración de contenido sensible a través de payloads de mando y control, su descarga a dispositivos no gestionados (del operador de ransomware) y su envío por correo electrónico.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad del Fortune 1000, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.