Proofpoint Threat Response Auto-Pull

Cuarentena automática del correo electrónico malicioso tras la entrega

VENTAJAS PRINCIPALES

- Cuarentena automática de los mensajes de correo electrónico maliciosos que consiguen superar las soluciones de seguridad perimetrales
- Reducción exponencial del tiempo que necesitan los equipos de seguridad y mensajería cuando revisan la organización y la respuesta de seguridad del correo
- Empleo de la inteligencia de amenazas de Proofpoint para la clasificación de los mensajes
- Monitorización automática de los buzones de correo malicioso para detectar amenazas
- Cuarentena de los mensajes reenviados a individuos o listas de distribución
- Seguimiento de las campañas de phishing con algunas denuncias y eliminación de la pérdida de tiempo derivado de mensajes denunciados por error

Proofpoint Threat Response Auto-Pull (TRAP) permite a sus administradores de mensajería y seguridad simplificar el proceso de respuesta a los incidentes relacionados con el correo electrónico. Cuando se detecta un mensaje malicioso, TRAP analiza automáticamente el correo electrónico y elimina los mensajes maliciosos. Además, coloca en cuarentena los mensajes no deseados que han llegado a las bandejas de entrada de los usuarios. Con TRAP, dispone de una potente solución que reduce significativamente el tiempo que necesitan sus equipos de seguridad y mensajería para limpiar el correo electrónico.

Más del 90 % de las violaciones de seguridad comienzan por un mensaje de correo electrónico, que es el principal vector de ataque. Las amenazas por correo electrónico siguen evolucionando, por lo que las organizaciones estarán expuestas a más mensajes maliciosos. Los mensajes de correo electrónico maliciosos pueden contener enlaces que se hacen infecciosos una vez entregados o bien utilizar técnicas de evasión, lo que genera falsos negativos y permite la entrega de mensajes de correo electrónico maliciosos a los usuarios. Los equipos de seguridad del correo electrónico deben ocuparse con frecuencia del análisis y la limpieza del correo electrónico para reducir la exposición a amenazas y limitar los daños potenciales. Si bien poner en cuarentena un mensaje puede ser una tarea sencilla, que solamente requiere entre 10 y 15 minutos, cuando se trata de diez mensajes o más, la tarea puede complicarse y necesitar más tiempo.

Compartir inteligencia de distintos vectores con el gráfico de amenazas Nexus de Proofpoint

El gráfico de amenazas Nexus de Proofpoint facilita la agregación y la correlación de datos de amenazas en el correo electrónico, la nube, la red y las redes sociales. Favorece la protección y respuesta para amenazas en tiempo real para todos sus productos de Proofpoint. El gráfico forma parte de la plataforma de Proofpoint, por lo que no hay nada que instalar, desplegar o administrar. Al pertenecer a esta red y poder adelantarse a las amenazas en continua evolución, disfrutará de las ventajas siguientes:

- Inteligencia en tiempo real sobre amenazas obtenida de una comunidad formada por más de 115 000 clientes.
- Visibilidad multivectorial desde el correo electrónico, la nube, la red y las redes sociales.
- Seguimiento de más de 100 ciberdelincuentes para conocer las motivaciones y tácticas empleadas con el fin de mejorar la protección.

TRAP también aprovecha la inteligencia del gráfico de amenazas Nexus de Proofpoint para crear asociaciones entre los destinatarios y las identidades de los usuarios, con el fin de revelar posibles campañas asociadas, e incluso identificar las direcciones IP y dominios del ataque. A continuación, realiza acciones automatizadas en función de si se trata de usuarios atacados que pertenecen a departamentos o de grupos específicos con permisos especiales.

Además, si detectamos un mensaje de correo electrónico que contiene enlaces o adjuntos maliciosos, o direcciones IP sospechosas en el sitio de un cliente, compartimos esta información en la base completa de clientes para que puedan protegerse antes de la entrega del mensaje. Suprimimos y ponemos en cuarentena los mensajes que se han entregado en la bandeja de entrada de los usuarios.

Identificación y reducción del riesgo de phishing con CLEAR

Un empleado informado puede ser su última línea de defensa frente a un ciberataque. Con Closed-Loop Email Analysis and Response (CLEAR), el ciclo de denuncia, análisis y corrección de mensajes potencialmente maliciosos pasa de durar días a completarse en solo unos minutos. CLEAR, enriquecido con la inteligencia de amenazas de Proofpoint, detiene de raíz los ataques activos con solo un clic. Y su equipo de seguridad puede ahorrar tiempo y esfuerzo, ya que los mensajes maliciosos se ponen en cuarentena automáticamente.

Con CLEAR, dispone de una solución completa que combina las funciones de PhishAlarm, el botón de denuncia del correo electrónico, PhishAlarm Analyzer, que clasifica por categorías y prioridades mediante la inteligencia de amenazas de Proofpoint, y TRAP, para el enriquecimiento de los mensajes y la corrección automática de los mensajes maliciosos.

Los mensajes denunciados se envían a un buzón de correo malicioso para utilizar CLEAR y se supervisan y procesan con TRAP de la misma forma. A continuación, se analizan comparándolos con la inteligencia de amenazas de Proofpoint y otras obtenidas de terceros, con el fin de determinar si hay algo en el contenido que coincida con marcadores maliciosos. Los mensajes se retiran automáticamente de la bandeja de entrada del destinatario.

Administración del correo electrónico fuera de banda

TRAP también emplea archivos CSV y Proofpoint SmartSearch. Se pueden cargar los resultados de SmartSearch o archivos CSV, o utilizar incidentes manuales con algunos datos clave para iniciar una acción de cuarentena para uno o miles de mensajes de correo electrónico. Las amenazas de seguridad, así como los mensajes que infringen las directivas, pueden retirarse de los buzones de correo rápidamente. Además, se muestra una lista de actividades que indica quién ha leído los mensajes y si el intento de retirada del mensaje de correo electrónico ha funcionado.

Cuarentena automática de mensajes reenviados

Los mensajes de correo electrónico maliciosos y no deseados pueden reenviarse a otras personas, departamentos o listas de distribución. Intentar retirar estos mensajes tras la entrega es siempre una tarea complicada para muchos administradores. TRAP soluciona esta situación con lógica e inteligencia empresarial incorporada que reconoce cuándo se reenvían o envían los mensajes a listas de distribución. A continuación, examina automáticamente y sigue el rastro de los destinatarios para localizar y retirar dichos mensajes. Todo esto le ahorra tiempo y frustración.

Clasificación mejorada

TRAP proporciona a los analistas de los SOC un proceso de clasificación mejorada de los mensajes que contienen URL. Las URL pueden investigarse con seguridad, gracias a la tecnología Proofpoint Browser Isolation. De esta forma, los analistas pueden evaluar su contenido para evitar riesgos en la organización.

MÁS INFORMACIÓN

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

ACERCA DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) es una compañía líder en ciberseguridad 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**.

©Proofpoint, Inc. Proofpoint es una marca comercial de Proofpoint, Inc. en Estados Unidos y en otros países. Todas las marcas comerciales mencionadas en este documento son propiedad exclusiva de sus respectivos propietarios.