Resumen de la solución

Protección frente al malware evasivo

Como ya indicamos en el Informe de McAfee Labs sobre amenazas: junio de 2017, para evitar ser detectado, el malware evasivo se camufla, se anexa a aplicaciones legítimas o hace un uso ilegítimo de ellas. Este malware reconoce cuando está siendo analizado en un entorno aislado y retrasa su ejecución, pudiendo esperar días, semanas o incluso meses hasta encontrar la oportunidad adecuada para atacar.

El desarrollo de un programa de seguridad para proteger frente a malware evasivo debe basarse en tres pilares.

- **Personas**: es necesario ofrecer la formación necesaria a los profesionales de la seguridad de manera que respondan de forma adecuada a los incidentes de seguridad y gestionen correctamente la tecnología de seguridad actual. Los ciberdelincuentes utilizan habitualmente la ingeniería social para infectar a los usuarios. Si no se les avisa e instruye, los usuarios dejarán alguna ventana abierta a los agresores.
- **Procesos**: deben implementarse estructuras y procesos internos claros para que los profesionales de la seguridad sean eficaces. Las mejores prácticas de la seguridad (actualizaciones, copias de seguridad, administración, inteligencia, planes de respuesta a incidentes, entre otras) son la clave para un equipo de seguridad eficaz.
- **Tecnologías**: la tecnología da soporte a los equipos y los procesos. Debe completarse y ampliarse para que pueda adaptarse a las nuevas amenazas.

Prácticas y procedimientos recomendados para protegerse frente al malware evasivo

- La defensa más importante contra las infecciones por malware son los usuarios. Los usuarios deben ser conscientes del riesgo de la descarga e instalación de aplicaciones que proceden de fuentes potencialmente peligrosas. Además, deben saber que se puede descargar malware de manera inadvertida mientras se navega.
- Tenga siempre actualizados los navegadores web y los complementos, así como el antimalware en los endpoints, y los gateways de la red con las últimas versiones.
- No permita que accedan a la red de confianza sistemas que no hayan sido distribuidos y certificados por el grupo de seguridad de TI de la empresa. El malware evasivo se puede propagar fácilmente por sistemas no protegidos conectados a la red de confianza.

McAfee™
Together is power.

- El malware evasivo se oculta en el interior de software legítimo que ha sido previamente "troyanizado" por un agresor. Para evitar ataques de este tipo, recomendamos que se refuerce la protección de los mecanismos de distribución y entrega del software. Es siempre aconsejable tener un repositorio central de aplicaciones corporativas del que los usuarios pueden descargar el software aprobado.
- En los casos en los que los usuarios están autorizados a instalar aplicaciones que no han sido validadas previamente por el grupo de seguridad de TI, se les debe informar de que únicamente deben instalar aplicaciones con firmas de confianza procedentes de proveedores conocidos. Es muy habitual que aplicaciones que se ofrecen online supuestamente "inofensivas" contengan malware evasivo.
- Evite descargas de aplicaciones de fuentes distintas de la Web. Son muy elevadas las probabilidades de descargar malware de grupos USENET, canales IRC, clientes de mensajería instantánea o sistemas P2P. Los enlaces a sitios web vistos en IRC y la mensajería instantánea suelen apuntar a descargas infectadas.
- Ponga en práctica programas educativos para prevenir los ataques de phishing. El malware se suele distribuir a través de ataques de phishing.
- Utilice la inteligencia sobre amenazas en combinación con la tecnología antimalware. Esta combinación ayudará a agilizar la detección de amenazas.

Cómo pueden protegerle los productos de McAfee frente al malware evasivo

McAfee ofrece una nueva generación de funciones de seguridad destinadas a combatir las amenazas modernas más evasivas. Gracias al uso de potentes herramientas de análisis con aprendizaje automático y de contención de aplicaciones, las empresas pueden descubrir las amenazas ocultas y atajarlas de raíz mucho más rápidamente y con mucho menos esfuerzo.

Estas funciones están disponibles a través de los siguientes productos de McAfee:

Real Protect

Real Protect, que forma parte de la solución McAfee Endpoint Protection, combina el análisis estático antes de la ejecución y el análisis de comportamientos posterior a la ejecución con el fin de detener más malware que ninguna otra solución basada en firmas o meramente estática, todo ello integrado en el ecosistema de McAfee. Esta solución aplica avanzadas técnicas de aprendizaje automático para identificar el código malicioso mediante la evaluación en profundidad de sus funciones estáticas (análisis antes de la ejecución) y de lo que hace realmente (análisis dinámico de comportamientos), todo sin el empleo de firmas. La herramienta desvela las últimas técnicas de ocultación con el fin de descubrir las amenazas ocultas de manera que el malware zero-day no tenga donde esconderse.

Contención dinámica de aplicaciones

Contención dinámica de aplicaciones (DAC, Dynamic Application Containment), también parte de la solución McAfee Endpoint Protection, facilita la protección de endpoints "paciente cero" frente a nuevas infecciones de malware de tipo zero-day. Cuando un endpoint detecta un archivo sospechoso, la función DAC bloquea inmediatamente los comportamientos habituales de dicho malware (como cambiar el registro, escribir en un directorio temporal o eliminar archivos). A diferencia de las técnicas que retienen el archivo (y al usuario) durante unos minutos, la función DAC permite que el archivo sospechoso se cargue en la memoria sin que pueda realizar determinados cambios en el endpoint ni infectar a otros sistemas mientras esté bajo sospecha.

Resumen de la solución

Real Protect y DAC están integradas —entre ellas, con otras soluciones de seguridad de terceros, como SPLUNK, Avecto y ForeScout, y con McAfee Endpoint Protection— con el fin de proporcionar una defensa en varios niveles frente a las amenazas más evasivas. De esta forma, permiten a su equipo de seguridad abordar todas las fases del ciclo de vida de defensa de amenazas —la detección, corrección y protección proactiva— de forma automática y rápida.

Real Protect y DAC permiten:

- Desenmascarar ataques descubriendo las técnicas de ocultación para revelar más amenazas de malware.
- Limitar el impacto de un ataque: contenga, blinde y evite daños en los sistemas, antes de que se produzca un ataque o antes de que los daños sean irreversibles.
- Realizar el seguimiento y la adaptación: utilice defensas automatizadas e integradas para llevar a cabo operaciones de seguridad más variadas sin tener que diseñarlas o activarlas de manera manual.

Vea la demostración en vídeo de la contención de malware evasivo mediante Real Protect y DAC.

Recomendaciones para la configuración de Contención dinámica de aplicaciones (DAC)
Las reglas de DAC en la directiva McAfee Default están definidas únicamente para informar, por lo que reducen los falsos positivos. La función Protección contra amenazas adaptable proporciona otras dos directivas de DAC predefinidas: McAfee Default Balanced y McAfee Default Security. Estas directivas definen las reglas recomendadas para bloquear, en función del perfil de seguridad:

- McAfee Default Balanced proporciona un nivel básico de protección al tiempo que minimiza los falsos positivos de muchos instaladores y aplicaciones populares que no están firmados.
- McAfee Default Security ofrece una protección agresiva, pero podría generar falsos positivos con más frecuencia para instaladores y aplicaciones sin firmar.

Evalúe el impacto de las reglas de DAC mediante el uso de la directiva McAfee Default con reglas definidas para informar. Para determinar si conviene definir las reglas para bloquear, supervise los registros e informes. Tras obtener eventos de infracción de DAC permitida (ID de evento 37280), defina las reputaciones a nivel de empresa o las exclusiones de DAC antes de implementar la directiva McAfee Default Balanced.

La función DAC puede excluir procesos en función del nombre, código hash MD5, datos de firma y ruta. Si su empresa firma herramientas que se despliegan de forma interna, añada estas firmas como exclusiones para reducir los falsos positivos.

Las reglas de DAC tienen control de flujo, lo que limita el número de eventos que se generan a una vez por hora, por regla y por proceso. El control de flujo de DAC rastrea los procesos por ID. Cuando se reinicia un proceso, el sistema operativo le asigna un nuevo ID, que restablece el control de flujo aunque el nombre de proceso sea el mismo. Por ejemplo, si el proceso A infringe la regla A de DAC 100 veces cada hora, recibirá un evento por hora. Si el proceso A se reinicia durante esa hora, el control de flujo se restablece para el proceso A y recibe otro evento si sigue infringiendo la regla A de DAC. Si el proceso B infringe la misma regla A de DAC, recibe un segundo evento (con los detalles del proceso B). Haga clic aquí para obtener más información sobre las mejores prácticas específicas sobre las reglas de DAC definidas de McAfee.

Ejecute la herramienta GetClean de McAfee en las imágenes base del despliegue para sistemas de producción a fin de garantizar que se envíen los archivos limpios a McAfee Global Threat Intelligence (GTI) para su clasificación. Esta herramienta garantiza que McAfee GTI no proporcione un valor de reputación incorrecto para sus archivos. Para obtener más información, consulte la guía GetClean Product Guide (PD23191).

McAfee Cloud Threat Detection

Mejore fácilmente las protecciones de McAfee para neutralizar el malware avanzado y descubrir las amenazas evasivas gracias a la ayuda de McAfee Cloud Threat Detection (CTD). Consiga acceso a McAfee ePO Cloud, active McAfee Cloud Threat Detection (CTD) e intégrela con sus productos de McAfee.

Para utilizar McAfee Cloud Threat Detection con sus productos de seguridad de McAfee, haga lo siguiente:

- Active McAfee CTD en McAfee ePO Cloud.
- Active McAfee CTD en la interfaz de su producto de seguridad de McAfee y obtenga la clave de aprovisionamiento.
- Utilice esta clave para generar una clave de activación en la interfaz de McAfee ePO Cloud.
- Utilice la clave de activación para activar su producto de seguridad de McAfee.

Las instrucciones detalladas varían para obtener la clave de aprovisionamiento y activar un producto. Consulte la guía del producto para obtener información detallada sobre la integración de McAfee CTD con su producto de McAfee.

Cuando los productos integrados empiezan a enviar archivos para su análisis a McAfee CTD, la información de uso aparece en la página Subscriptions (Suscripciones) de McAfee ePO Cloud.

McAfee Active Response

- McAfee Active Response es una solución expresamente diseñada para buscar y responder a las amenazas avanzadas. Cuando se utiliza junto a fuentes de información sobre amenazas, como McAfee GTI, Dell SecureWorks o ThreatConnect, permite identificar y eliminar las amenazas evasivas antes de que puedan propagarse.
- Los recopiladores personalizados permiten crear herramientas específicas para buscar e identificar indicadores de peligro asociados a las aplicaciones troyanizadas.
- El usuario crea desencadenadores y reacciones para definir acciones cuando se cumplen determinadas condiciones. Por ejemplo, cuando se encuentran hashes o nombres de archivo específicos, puede emprenderse automáticamente una acción de eliminación.

Otros documentos para ampliar la información

Neutralize Advanced Threats: Adapt Layered Defenses for Comprehensive Malware Protection (Neutralice las amenazas avanzadas: adapte las defensas por capas para disfrutar de una protección integral frente al malware)

McAfee Security Advice Center: Diez formas principales de defenderse frente al malware y los troyanos

McAfee Endpoint Security: preguntas frecuentes

McAfee
Together is power.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/es