MCAFEE: ADVANCED THREAT DEFENSE: DETECCIÓN DE AMENAZAS AVANZADAS

Revolucionando el ámbito de la detección al conectar las funciones de análisis del malware avanzado con las defensas existentes

Hoy en día las organizaciones se enfrentan a ataques avanzados y a malware evasivo, lo cual, demanda una protección inmediata para poder revelar las amenazas evasivas.

La solución de McAfee “Advanced Threat Defense”: detección de amenazas avanzadas ha revolucionado el ámbito de la detección al conectar las funciones de análisis del malware avanzado con las defensas existentes, desde el perímetro de la red hasta los endpoints y compartir información con todo el entorno. Al compartir esta información, las soluciones colaboran para cerrar inmediatamente las comunicaciones de comando y control (C&C), poniendo en cuarentena los sistemas en peligro, bloquean otras instancias de la misma amenaza o similares, evalúan el daño y permiten iniciar las acciones pertinentes.

La solución detecta el malware más sigiloso, de tipo zero-day. Combina motores de análisis que no requieren intervención, como las firmas antivirus, los basados en la reputación y la emulación en tiempo real, con análisis dinámicos (en entornos aislados) con el fin de examinar el comportamiento real. La investigación sigue con un análisis detallado dl código estático que examina los atributos del archivo y los grupos de instrucciones con el fin de descubrir el comportamiento previsto o evasivo y evaluar así, las semejanzas con familias de malware conocido. El último paso del análisis busca específicamente identificadores de actividad maliciosa identificados a través de aprendizaje automático mediante una red neuronal.

Los creadores de malware utilizan la compresión para modificar la composición del código u ocultarlo a fin de eludir la detección. La mayoría de los productos no pueden descomprimir correctamente el código ejecutable original (fuente) para su análisis. McAfee Advanced Threat Defense incluye numerosas funciones de descompresión que dejan al descubierto el código ejecutable original. De esta forma, el análisis en profundidad de código estático no se limita a examinar los atributos de archivo de primer nivel, sino que detecta anomalías analizando los atributos y conjuntos de instrucciones para averiguar el comportamiento previsto

McAfee Advanced Threat Defense se integra de distintas formas: directamente con soluciones de seguridad concretas, a través de McAfee Threat Intelligence Exchange o mediante McAfee Advanced Threat Defense Email Connector. La integración directa permite que las soluciones de seguridad tomen medidas con los archivos que McAfee Advanced Threat Defense identifica como maliciosos, como incorporar al instante la información sobre la amenaza en los procesos existentes de implementación de directivas y bloquear las demás instancias de esos archivos o archivos similares para que no entren en la red.

Los endpoints que tienen McAfee Threat Intelligence Exchange activado pueden bloquear la instalación del malware, lo que evita que se conviertan en el "paciente cero", y ofrecen protección proactiva si el archivo aparece en el futuro. Por su parte, los gateways que funcionan con McAfee Threat Intelligence Exchange pueden evitar que el archivo entre en la organización. Además, los endpoints siguen recibiendo información sobre archivos sospechosos aun estando desconectados de la red, lo que elimina los ángulos muertos cuando la carga útil se distribuye fuera de banda.

McAfee Advanced Threat Defense Email Connector permite a McAfee Advanced Threat Defense recibir adjuntos de correo electrónico para su análisis desde un gateway de correo electrónico. McAfee Advanced Threat Defense analiza los archivos de los adjuntos y devuelve un veredicto a todos los gateways de correo electrónico activos incluido en el encabezado del mensaje. A continuación, el gateway de correo electrónico puede realizar una acción basada en las directivas, como eliminar o poner en cuarentena el adjunto, para evitar que el malware infecte y se propague por la red interna. Un modo offline permite la entrega al usuario final del correo con adjuntos, mientras se analiza en McAfee Advanced Threat Defense.

Despliegue de McAfee Advanced Threat Defense

Opciones flexibles de despliegue de análisis de amenazas avanzadas para todas las redes. McAfee Advanced Threat Defense está disponible como dispositivo in situ o en formato virtual, con compatibilidad para la nube pública y privada, y está disponible en Azure Marketplace.

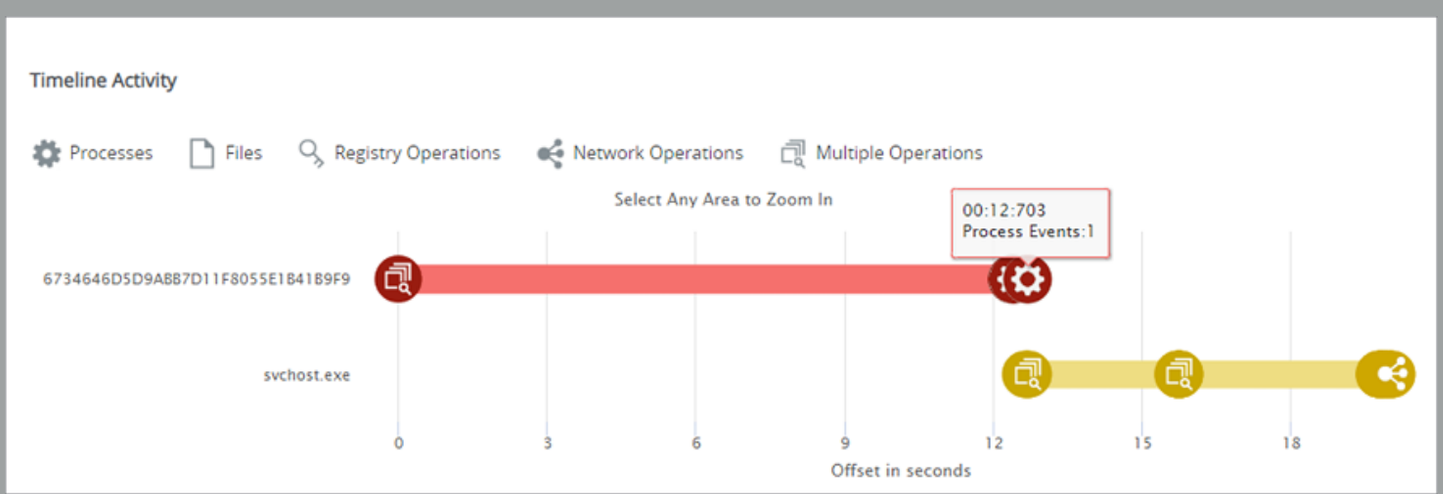

Figura 1. La actividad de línea de tiempo muestra los pasos de ejecución de la amenaza analizada.

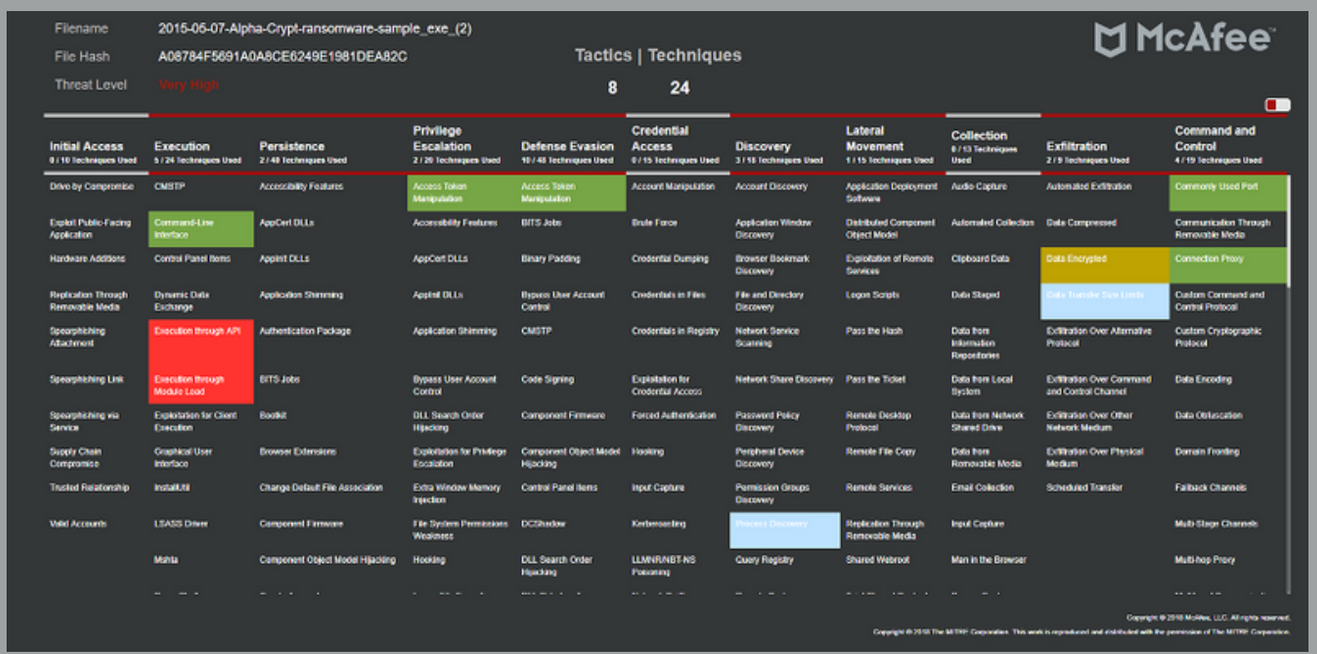

Figura 2. Los detallados informes ofrecen información esencial para las investigaciones, tal como la asignación del marco MITRE ATT&CK™.

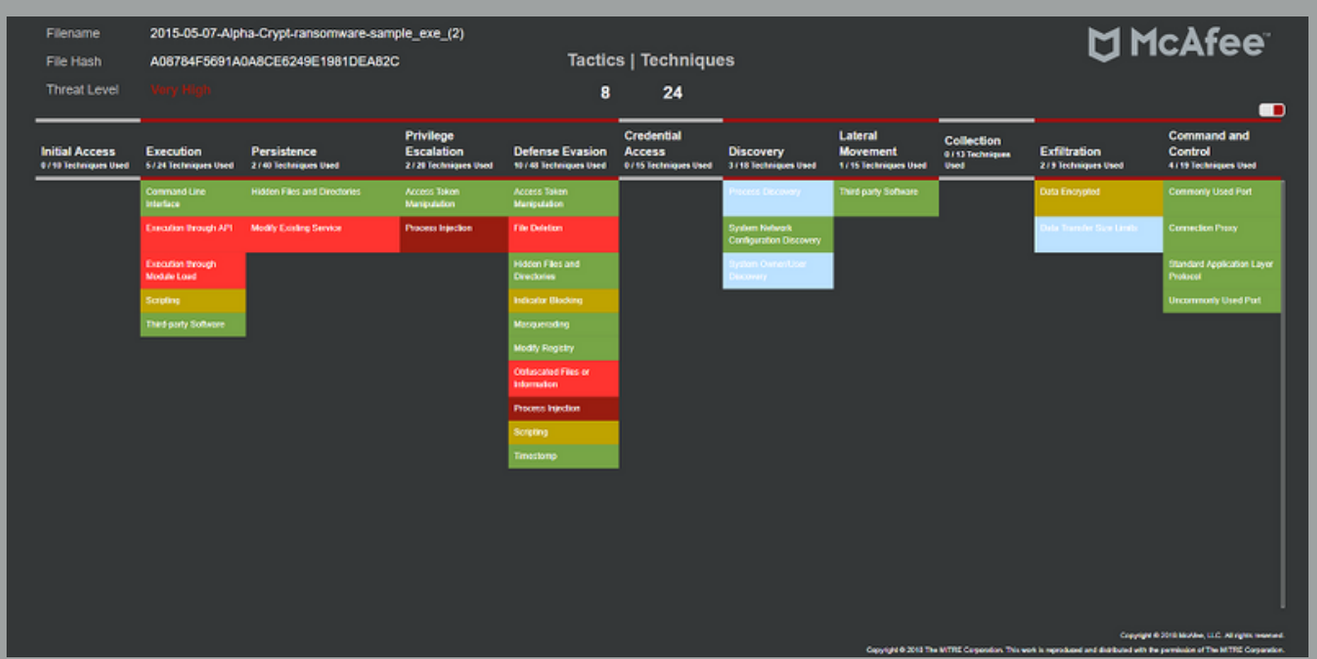

Figura 3. La vista filtrada del informe de MITRE ATT&CK™ (figura 2) se centra en las técnicas identificadas.

Conozca como Apollocom puede ayudar a integrar esta y otras soluciones de McAfee a su organización y contribuir en su ecosistema de ciberseguridad.


Apollocom
Tecnología conectada con la inteligencia
@apollocommx