Servicios de asesoramiento sobre amenazas
INFORMACIÓN GENERAL SOBRE EL SERVICIO DE ANÁLISIS DE MALWARE

Introducción

La escalada de ataques de malware es una amenaza importante para las organizaciones de todos los tamaños. Su capacidad para infiltrarse en los sistemas, robar datos confidenciales, interrumpir las operaciones y dañar irrevocablemente la reputación de la marca plantea un serio desafío que debe abordarse. Sin embargo, los equipos de seguridad internos sobrecargados a menudo carecen del tiempo, los recursos y la experiencia necesarios para un análisis de malware enfocado para adelantarse de manera efectiva a las campañas y ataques maliciosos.

Al externalizar el análisis de malware a un proveedor de servicios de confianza, las organizaciones pueden:

- **Optimice la asignación de recursos:** Asigne recursos estratégicamente, asegurándose de que las inversiones en herramientas, personal e infraestructura se alineen con las prioridades de la organización.
- **Mejore las inversiones existentes:** recopile e implemente indicadores de compromiso (IOC) en toda la infraestructura de seguridad existente para identificar y mitigar mejor las vulnerabilidades de malware.
- **Optimice las operaciones de seguridad:** implemente procesos y herramientas para reducir la complejidad y mejorar la eficiencia en todos los marcos de ciberseguridad.
- **Obtenga acceso a conocimientos especializados:** aproveche un equipo dedicado de analistas para llevar a cabo investigaciones en profundidad que identifiquen software, hashes y URL potencialmente maliciosos.

SERVICIO DE ANÁLISIS DE MALWARE

El Servicio de Análisis de Malware de Appgate, dirigido por nuestro experimentado Equipo de Análisis e Investigación de Malware (MART), cuenta con dos ofertas de servicios que los equipos de seguridad pueden utilizar para enviar archivos, hashes y URL potencialmente maliciosos para su investigación. El análisis rápido utiliza procesos, herramientas y sistemas automatizados para extraer datos y crear un informe oportuno e informado. Deep Analysis aprovecha las fuentes de datos líderes de la industria aumentadas por metodologías internas y evaluaciones prácticas de ingeniería inversa para ofrecer información detallada sobre cepas de malware más oscuras y emergentes.

Ambos servicios incluyen IOC procesables, información y recomendaciones con niveles de alerta para que los equipos de seguridad puedan mitigar los riesgos de manera efectiva. Las organizaciones también pueden obtener una rica inteligencia contextual sobre amenazas para cualquier indicador sospechoso derivado de las muestras enviadas para mejorar de forma proactiva la eficacia de la respuesta a incidentes.

SUSCRIPCIONES AL SERVICIO DE ANÁLISIS DE MALWARE

Análisis rápido: este servicio analiza automáticamente los envíos de muestras de malware conocidos. El informe incluirá una sección dedicada con información como nombre de archivo, hashes, marcas de tiempo, tipo de archivo, servidores de comando y control (C2), cadenas útiles, imágenes y más. Los informes de análisis rápido para la mayoría de las muestras de malware se entregan en 30 minutos.

Se recomienda el análisis rápido como primer paso inicial para una prestación de servicios más rápida y un análisis acelerado que incluya:

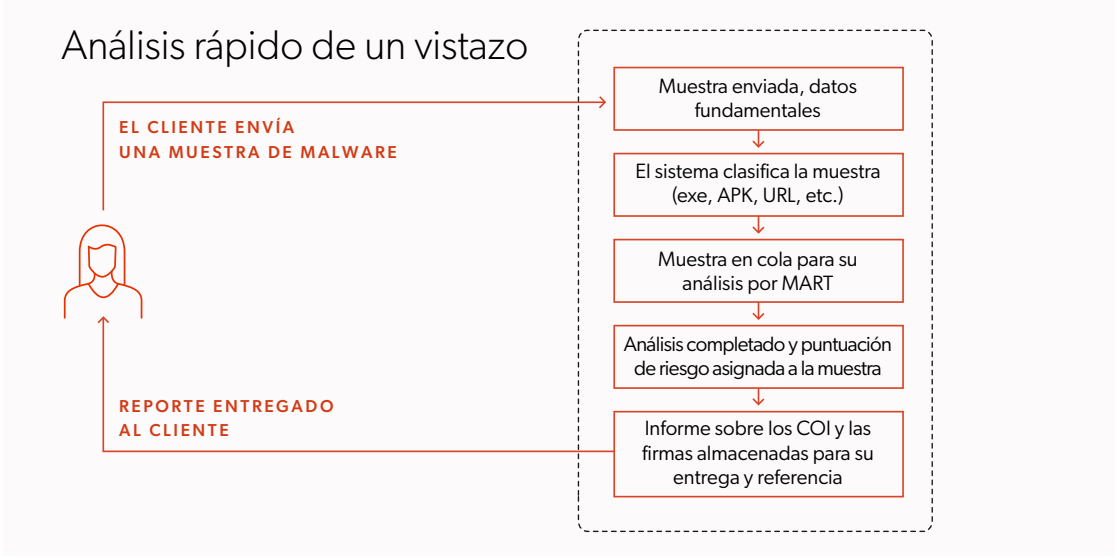
- Ingesta de archivos a través de la interfaz de usuario o la API
- Análisis estático y dinámico
- Identificación basada en reglas y firmas
- Inteligencia de amenazas e informes del COI
- Detección de marcas objetivo

CASOS DE USO

- **Defensa rápida, contención proactiva:** implemente rápidamente los IOC identificados en la arquitectura de seguridad para contener las amenazas de forma proactiva y minimizar el radio de explosión.
- **Operaciones de seguridad:** integre el servicio en los flujos de trabajo de operaciones de seguridad existentes para mejorar las capacidades de detección y respuesta a amenazas.
- **Investigación de malware:** realice análisis en profundidad de muestras de malware nuevas y emergentes para comprender su comportamiento y su impacto potencial.
- **Búsqueda de amenazas:** busque de forma proactiva signos de compromiso o amenazas emergentes dentro de las redes o sistemas empresariales.

CAPACIDADES CRÍTICAS

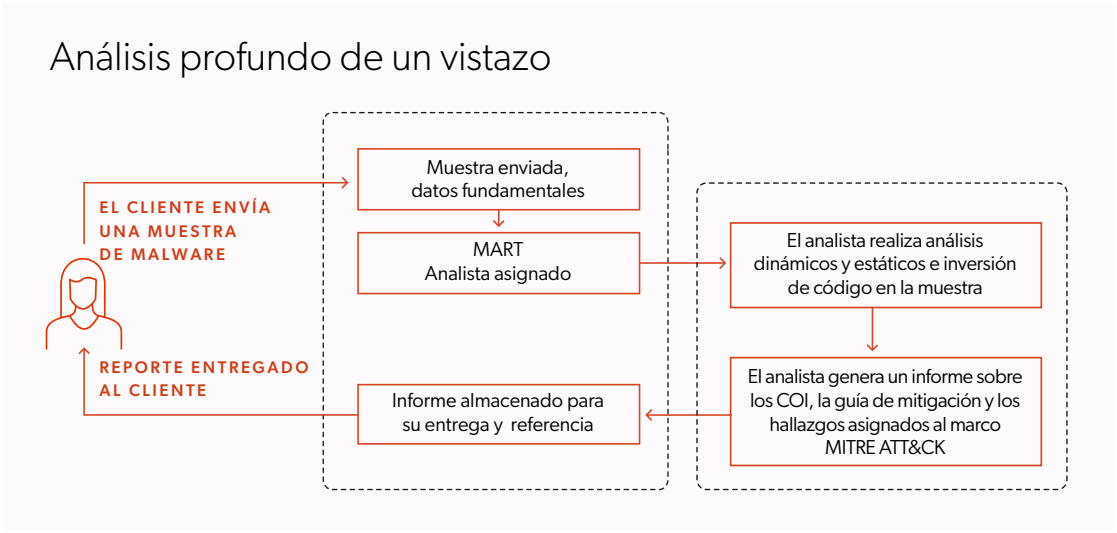
- **Inteligencia contextual sobre amenazas:** aproveche las metodologías avanzadas de ingeniería inversa y los análisis de archivos y URL para identificar cepas y familias de malware y su posible impacto.
- **Informes completos:** genere informes personalizados de acuerdo con los requisitos específicos de la organización (disponibles en formatos PDF o JSON).
- **Mapeo MITRE ATT&CK:** Asigne los hallazgos a tácticas, técnicas y procedimientos (TTP) comunes utilizados en amenazas persistentes avanzadas para desarrollar estrategias de defensa más efectivas.
- **Implementación práctica:** Obtener informes fáciles de usar y recomendaciones prácticas para la implementación en las herramientas de seguridad empresarial existentes y tecnologías.
- **Soporte de cumplimiento:** Mantenga las estrictas políticas internas y los requisitos de cumplimiento normativo que implican el análisis de malware y la respuesta a incidentes.



Análisis profundo: Para este servicio, nuestro equipo de análisis e investigación de malware realiza ingeniería inversa de malware para descubrir detalles de ataque específicos del cliente. El equipo analiza meticulosamente la comunicación con los servidores C2 e identifica funciones de malware como la inyección de procesos, las inyecciones web y la criptografía. Un informe detallado de análisis profundo proporciona información completa, incluido el comportamiento de las amenazas y las TTP, y normalmente se entrega en uno a tres días en función de la complejidad de la muestra enviada.

El análisis profundo es óptimo para tipos de malware oscuros y emergentes que requieren un escrutinio más profundo e incluye:

- Alcance del malware, su impacto y familia asociada
- Permisos solicitados
- Análisis de comportamiento de la muestra, scripts inyectados y funciones
- Ejecución de comandos personalizados
- Investigación C2
- Lista completa de cadenas descifradas y relevantes para denotar las capacidades del malware
- Abordar los requisitos y especificaciones específicos del cliente



Las cuatro etapas del análisis profundo de MART

Appgate navega por el intrincado panorama del análisis de malware a través de cuatro etapas fundamentales:

Etapa 1: Análisis estático: abarca la revisión de cadenas de código, hashes, detalles de encabezado y metadatos dentro de los archivos de malware enviados. El análisis de las propiedades estáticas ofrece información rápida sobre la reducción de riesgos para evitar la ejecución de código potencialmente dañino.

Fase 2: Análisis dinámico: aprovecha el entorno de espacio aislado para ejecutar código malintencionado sospechoso. Los resultados permiten a su equipo de seguridad observar de cerca los comportamientos de malware y recopilar datos sin arriesgarse a infectar el sistema o la red.

Etapa 3: Inversión de código: si es necesario, un analista especializado investiga el funcionamiento interno del malware descubierto, incluida la inversión de código para descubrir funcionalidades ocultas, técnicas de cifrado y estrategias antianálisis.

Etapa 4: Informes: un informe completo sobre las capacidades y los posibles efectos del malware. Incluye detalles técnicos, indicadores de compromiso (IOC), recomendaciones de detección y mitigación, y mapeo de los hallazgos con el marco MITRE ATT&CK.

Beneficios

- **Aproveche nuestra experiencia:** Obtenga acceso al equipo de análisis e investigación de malware de Appgate para mantenerse a la vanguardia de las últimas tendencias de fraude y amenazas cibernéticas.
- **Mejore la eficiencia de las operaciones de seguridad:** optimice las operaciones de seguridad y optimice la asignación de recursos para centrarse en tareas de alta prioridad e iniciativas estratégicas.
- **Mejore la respuesta a incidentes:** enriquezca los datos de telemetría de seguridad con inteligencia de amenazas para permitir una mitigación más rápida y eficaz de los incidentes de seguridad.
- **Mejore la postura de seguridad:** mitigue la amenaza de cepas nuevas y emergentes de malware y sitios sospechosos con una amplia cobertura de plataforma en Windows, Linux, MacOS y Android.
- **Fuerte retorno de la inversión:** elimine la necesidad de dedicar recursos internos al análisis manual y minimice los riesgos asociados con posibles violaciones de datos e interrupciones operativas.

Conclusión

El servicio de análisis de malware de Appgate proporciona una guía de mitigación completa, personalizada y práctica para hacer frente a las amenazas de malware en evolución. Al aprovechar la experiencia especializada y las técnicas de análisis de vanguardia, las organizaciones pueden optimizar las operaciones de seguridad, optimizar la asignación de recursos, aumentar las herramientas y tecnologías existentes y garantizar una protección continua contra las amenazas cibernéticas en evolución.

Acerca de Appgate

Appgate es la empresa de acceso seguro. Potenciamos la forma en que las personas trabajan y se conectan al proporcionar soluciones diseñadas específicamente sobre los principios de seguridad Zero Trust. Este enfoque de seguridad definido por las personas permite conexiones rápidas, sencillas y seguras desde cualquier dispositivo y ubicación a cargas de trabajo en cualquier infraestructura de TI en entornos en la nube, locales e híbridos. Appgate ayuda a las organizaciones y agencias gubernamentales de todo el mundo a comenzar donde están, acelerar su viaje hacia Zero Trust y planificar su futuro. Más información en appgate.com.

appgate