



AVANCES DEL BANCO MUNDIAL EN DEFENSAS CONTRA MALWARE CON APPGATE

SERVICIOS DE ASESORAMIENTO SOBRE AMENAZAS

Una institución financiera líder mejora la postura de seguridad al mitigar las amenazas de malware y otras vulnerabilidades avanzadas con el servicio de análisis de malware de Appgate

Historia

Es una institución financiera líder, una de las más grandes de América Latina y clasificada entre los 50 bancos más valiosos del mundo, que opera en varios segmentos, incluyendo banca, seguros y servicios financieros. Esta institución atiende a millones de clientes con una amplia gama de productos y servicios diseñados para mejorar la seguridad financiera y el bienestar.

Desafíos y requisitos

Debido a sus grandes participaciones y a su alto perfil, el banco se ha enfrentado a un flujo incesante de amenazas de malware en evolución, lo que compromete su capacidad para proporcionar soluciones financieras de alta calidad a los clientes. Esta escalada significó que el ocupado equipo de seguridad del banco se encargó de analizar cada nueva cepa y variación de malware. Necesitaban una solución que pudiera realizar investigaciones avanzadas y proporcionar rápidamente un análisis en profundidad de las amenazas para determinar el alcance, impacto e indicadores de compromiso (IOC) para cada incidente. El banco también buscó agilizar las operaciones de seguridad, optimizar la asignación de recursos, mitigar los riesgos de malware y garantizar operaciones comerciales ininterrumpidas.

Solución

Para hacer frente a estos desafíos, se asociaron con los servicios de asesoramiento sobre amenazas de Appgate para aprovechar la información de análisis de malware automatizado y manual sobre archivos, hashes y URL maliciosos. El banco obtuvo acceso a la experiencia experta de Appgate y a las herramientas y técnicas avanzadas necesarias para identificar, analizar y mitigar las amenazas relacionadas con el malware. Los informes detallados de Malware Analysis Service incluían inteligencia contextual avanzada sobre amenazas e IOC que el banco podía integrar en su arquitectura de seguridad empresarial existente. Además, al mapear los hallazgos relevantes para el marco de MITRE ATT&CK, los informes integrales permitieron al equipo desarrollar estrategias efectivas para defenderse contra las amenazas actuales y futuras.

“El equipo y los servicios de análisis de malware de Appgate realmente han mejorado nuestras capacidades de operaciones de seguridad. Los recursos de Appgate agregaron escaneos de malware de alta calidad, agregaron inmediatamente sus indicadores a nuestras herramientas de seguridad y utilizaron IOC para ayudar a buscar más infecciones en todo el ambiente. El contexto nos ayudó a prevenir varios ataques de malware relacionados con el malware que Appgate había analizado. Esto nos ayudó a centrarnos en los nuevos ataques en lugar de abordar continuamente las variaciones del mismo malware. La información que identificaron sobre el impacto potencial fue procesable para las amenazas presentes y futuras”.

— Analista Líder de Seguridad de la Información

El servicio de análisis de malware de Appgate proporcionó una solución completa y práctica para hacer frente a las amenazas de malware persistentes. Al aprovechar la experiencia experta de Appgate, las técnicas de análisis avanzadas y la inteligencia de amenazas procesable, el banco ha mejorado significativamente su postura de seguridad y ha obtenido una protección continua contra las amenazas cibernéticas en evolución.

CASOS DE USO

Respuesta a incidentes

Malware research

Extracción de indicadores de compromiso

Threat hunting

Contención proactiva de amenazas

RESULTADOS

Aumento de la velocidad de descubrimiento de indicadores significativos

Menor tiempo de respuesta y fácil inclusión de indicadores en la barandilla

Reducción drástica del tiempo de análisis para cambiar el enfoque a la corrección de archivos, URL y hashes potencialmente maliciosos

Identificación oportuna de amenazas de alta prioridad

Acerca de Appgate

Appgate es la empresa de acceso seguro. Potenciamos la forma en que las personas trabajan y se conectan proporcionando soluciones basadas en 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 para cargas de trabajo en cualquier infraestructura de TI en entornos híbridos, locales y en la nube. Appgate ayuda a las organizaciones y agencias gubernamentales de todo el mundo a comenzar donde están, acelerar su viaje hacia Zero Trust y su plan para el futuro. Más información en [appgate.com](https://www.appgate.com).