RevBits®

FICHA TÉCNICA

Deception Technology

La única tecnología de engaño disponible que implementa señuelos reales, deseables y atractivos basados en servidores para atrapar a los actores maliciosos con una virtualización de doble capa.

A medida que los actores malintencionados se han vuelto más sofisticados, ha aumentado la necesidad de una seguridad inteligente. Una vez que el actor malicioso está dentro y es capaz de moverse lateralmente, el uso de trampas puede ser la última línea de defensa contra la pérdida catastrófica de datos.

Funcionalidades la Solución

Monitoreo robusto
La tecnología de engaño de RevBits proporciona información sobre los ataques actuales para detectar, rastrear y responder a amenazas sofisticadas en tiempo real.

Cárcel fortificada
La virtualización de doble capa del señuelo garantiza que sea casi imposible que los actores malintencionados escapen.

Implemente servidores populares y aplicaciones
La tecnología de engaño de RevBits utiliza los servidores de bases de datos más comunes, los servicios de intercambio de archivos y muchos otros.

Listo para la nube
Imágenes en la nube disponibles para Amazon, Google y Azure para su uso con la tecnología de engaño implementada.

Cebo atractivo
La tecnología de engaño de RevBits aprovecha dos métodos para implantar cebos atractivos. Los administradores del sistema tienen la opción de implantar migas de pan manualmente en los archivos de configuración de la aplicación o implementar automáticamente las credenciales (gotas de miel) en la sestaciones de trabajo de la red. Tanto las migas de pan como las gotas de miel llevarán a los atacantes a los señuelos y revelarán su fuente.

Despliegue simple y rápido
Instale la tecnología de engaño de RevBits en cualquier servidor dentro de la red.

El objetivo es atraer la amenaza con servidores reales y una vez allí, atrapar la amenaza y evitar el escape.

Bajo consumo de recursos
Se pueden lanzar numerosos señuelos dentro de cada MV, minimizando los recursos del sistema y maximizando la eficiencia operativa.

Acceso inmediato a la imagen
RevBits mantiene todas las imágenes del señuelo y las extrae e implementa automáticamente en la red del cliente a pedido.

Informes e integración avanzados
La tecnología de engaño de RevBits se integra con los productos SIEM para ofrecer alertas en tiempo real. Se envían alertas por SMS y correo electrónico a los administradores del sistema sobre incidentes. Detecte y bloquee ataques diseñados para hacerse pasar por remitentes de confianza. Los ataques sin malware se frustran mediante el análisis en tiempo real de los correos electrónicos, la detección de anomalías en los encabezados, los dominios similares y la suplantación de identidad del remitente.

Requerimientos de Software

Servidor: Alojado en la red del cliente y esta basado en Linux

Imágenes en la nube disponibles para implementación: Amazon, Google, Azure

Funcionalidades Adicionales de la Solución

Administre actores maliciosos y amenazas internas – La tecnología de engaño de RevBits está diseñada para enfrentarse al actor malicioso que ha obtenido acceso no autorizado en la red, así como la amenaza interna que compromete la red para acceder a activos valiosos. En ambos casos, el objetivo es atraer la amenaza con servidores reales y, una vez allí, atrapar la amenaza y evitar que escape. La tecnología de engaño de RevBits está diseñada para cumplir con estos dos requisitos vitales en la tecnología de engaño.

Fácil de implementar, fácil de administrar – Con la tecnología de engaño de RevBits, servidores de bases de datos trampa reales (MySQL, PostgreSQL, MSSQL, etc.), servidores de archivos (FTP, SMB, etc.), dispositivos de red (enrutadores, firewalls, etc.) y todos los protocolos de red comunes (SSH, RDP, VNC, etc.) se pueden iniciar con un solo clic. Un tablero central permite a los administradores de red administrar, configurar y monitorear todos los señuelos en toda su empresa.

Diseño único – La arquitectura de virtualización de doble capa de la tecnología de engaño de RevBits proporciona un encapsulado superior de los atacantes en los señuelos. Además de los beneficios de seguridad, la tecnología de engaño de RevBits permite una fácil implementación, una gestión eficiente y un bajo consumo de recursos.

Beneficios de Deception Technology

Implementación asequible – A través de un diseño único, la tecnología de engaño de RevBits permite una implementación extensa de señuelos sin aumentar el uso de recursos. Un servidor RevBits puede albergar múltiples señuelos en la red.

Aumente el valor de la implementación a través de una búsqueda de amenazas exitosa – El valor de implementar la tecnología de engaño de RevBits aumenta debido al uso de trampas reales basadas en servidores. El uso de señuelos reales basados en servidores aumenta la probabilidad de capturar al actor malicioso y evitar que acceda a otros activos importantes en la red.

Construido con la seguridad en mente – La tecnología de engaño de RevBits utiliza virtualización de dos capas para garantizar la captura del actor malicioso o la amenaza interna. Esta virtualización de doble capa garantiza que la inversión en el producto sea rentable: una vez atrapado en un señuelo de la tecnología de engaño de RevBits, la probabilidad de que el actor malicioso pueda escapar se reduce significativamente.

Implementación simple – La tecnología de engaño de RevBits es fácil de implementar: no se requiere software especializado para la implementación, múltiples imágenes listas para usar en la nube.

Mantenga su empresa protegida. Obtenga una demostración o evaluación gratuita.
Para obtener más información, visite www.revbits.com

34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248) • www.revbits.com