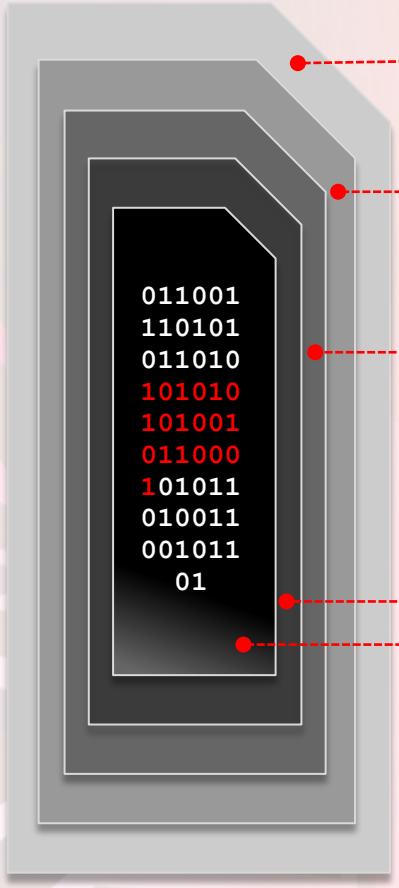
PROPUESTA ANTIMALWARE

SentinelOne

PARA

GRUPO IMAGEN

LAS AMENAZAS DE HOY EVANDEN FACILMENTE LOS AV TRADICIONALES, SE NECESITA UN NUEVO ENFOQUE



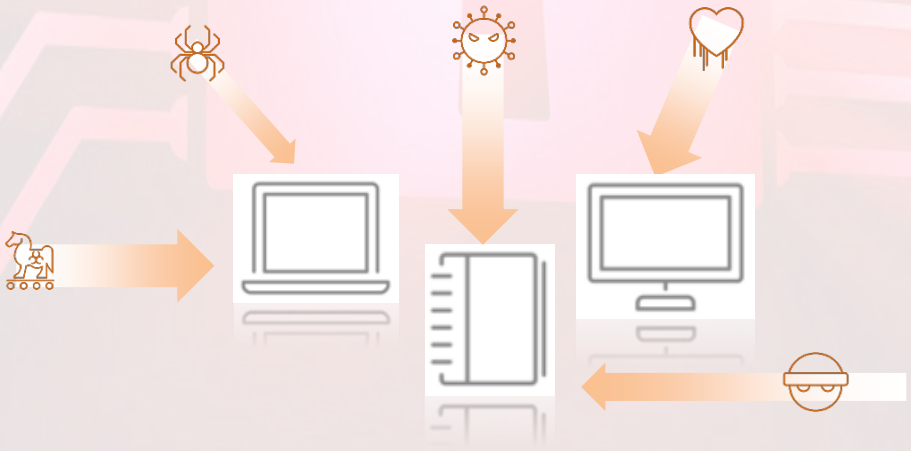
Wrappers
Designado para transformar código en binario

Variations / Obfuscators
Designado para alterar levemene el código para que código conocido parezca nuevo

Packers
Designado para asegurar que el código corra en una computadora real (anti-VM, sleepers, interactions, anti-debug, anti-sandbox)

Targeting
Designado para permitir que el código corra solamente en una determinada configuración

Malicious Code
Código de ataque que corre con el objetivo de espiar, robar o exfiltrar datos de manera persistente



DYNAMIC BEHAVIOUR TRACKING: UN ENFOQUE SOBRE MACHINE LEARNING.

Tener la capacidad de ver lo que se está ejecutando en un punto final y cómo cada aplicación o proceso se está comportando, fue la mayor pieza que faltaba en la solución del problema de amenazas avanzadas.

El agente de SentinelOne "interviene" en cada proceso y thread del sistema extrayendo todos los datos de operaciones relevantes, incluyendo llamadas al sistema, red, IO, registro (en Windows) y más, para que pueda supervisar el comportamiento de cada proceso que se ejecuta en el sistema. El módulo de análisis está trabajando constantemente en segundo plano y ejecuta sofisticados algoritmos de correspondencia de patrones para detectar comportamientos maliciosos en operaciones de proceso de contexto completo – cubriendo el sistema de manera amplia en sus operaciones como en la información histórica. Los “patrones” – técnicas y comportamiento del malware – son investigados diariamente en los laboratorios de SentinelOne mediante técnicas de reverse engineering en miles de muestras de malware, agrupándolas y deduciendo comportamientos para investigar y calificarlas.

México CDMX. 3 de febrero de 2021

PROPUESTA SENTINELONE

La defensa definitiva contra el ransomware y otras amenazas

SentinelOne, compañía fundada en 2013 por un equipo de élite de ingenieros en ciberseguridad y posicionada en el Cuadrante Mágico de Gartner de Plataformas de Protección de Endpoints, ofrece una solución unificada para el puesto final de trabajo y servidores ya que proporciona detección, protección, remediación en tiempo real y análisis forense ante amenazas avanzadas de nueva generación.

Para ello se basa en análisis y seguimiento dinámico de comportamientos en los endpoints para así poder proteger de los distintos vectores de ataque con automatismos inteligentes. Es la única compañía de endpoint de nueva generación que ha sido certificada por el AVTest, capaz de sustituir a un Antivirus tradicional en una instalación, manteniendo sus requisitos de compliance, como HIPAA y PCI DSS.

Obviamente lo mejor es evitar que se produzca el ataque de ransomware, ya que la recuperación es difícil. SentinelOne es el único software de seguridad de endpoints que protege frente a tipos de ransomware desconocido. EPP de SentinelOne utiliza un novedoso motor de inspección de ejecución predictiva que va más allá del análisis de archivos (incluso el análisis de algoritmos matemáticos) que observa la ejecución real de cada proceso o hilo del sistema en tiempo real. Al comprender el comportamiento de ejecución de todas las aplicaciones, programas y procesos en tiempo real, SentinelOne EPP ofrece la defensa definitiva frente al ransomware.

¿ Cómo nos protege ?

SentinelOne se centra en la ejecución de código en tiempo real en lugar de marcadores estáticos para la detección de amenazas. Este motor de ejecución es capaz de monitorear todos los procesos de los endpoints, añadir un contexto completo para cada proceso y predecir ataques de ransomware ocultos avanzados basándose en el comportamiento de ejecución del software sospechoso. El enfoque en la ejecución de procesos permite encontrar y evitar que el ransomware eluda las técnicas de detección estáticas, y que permanezca oculto a la mayoría de productos de seguridad.

Inspección de ejecución predictiva

Al contrario de los filtros estáticos que analizan los archivos y elementos persistentes del ransomware, el motor de inspección de ejecución de SentinelOne permite monitorear la ejecución restringida de todo el software sospechoso, incluyendo el ransomware basado en la memoria y scripts para comprender su comportamiento. Somos capaces de detectar y dar respuesta a lo que está sucediendo en el endpoint en el momento en que sucede. Esto permite a SentinelOne encontrar ransomware muy avanzado que no produce actividad alguna en disco o archivos, que no deja ningún indicador de puesta en compromiso de los sistemas, y que utiliza técnicas sofisticadas de incrustación para enmascarar su actividad.

Funcionamiento en el espacio del núcleo (kernel)

El agente de SentinelOne opera en el espacio del núcleo. Esto permite a SentinelOne llevar a cabo la protección, detección y respuesta con un impacto mínimo comparado con otros productos. Además de lograr ventajas claras de rendimiento, el agente de SentinelOne proporciona protección frente a todos los vectores de ataque, siendo a la vez altamente resistente a los intentos que pueda llevar a cabo el ransomware para eludir o desactivar el agente..

Roll-Back (retorno a un punto anterior)

El ransomware, junto con otras formas de malware se basa específicamente en cifrar u ocultar los archivos de datos y del sistema como un vector de ataque. Muchas de las variantes más sofisticadas del ransomware que se usan hoy en día van un paso más allá y eliminan la capacidad de la víctima para recuperar los datos cifrados destruyendo las "copias shadow" (copias ocultas de seguridad o puntos de restauración) creadas por el sistema operativo. Estas copias las utilizan los profesionales de TI en las operaciones de recuperación además de el propio SO, por ejemplo cuando se recupera de un fallo crítico del sistema. SentinelOne es la única solución que guarda y protege las copias shadow de los archivos de datos, por lo que es el único capaz de ayudar a las víctimas a recuperar sus archivos tras una infección de ransomware.

Respuesta y mitigación automáticas

SentinelOne es la única solución que ofrece protección completa de endpoints además de Endpoint Detection and Response (EDR - Detección y Respuesta de Endpoints) en una plataforma unificada. Nuestra capacidad para proporcionar un solo producto que se ocupa de la detección, prevención y respuesta es única. Hemos recibido la certificación de AV-TEST y constituimos una sustitución verdadera para todos los productos de seguridad, incluyendo los antivirus tradicionales y los productos de seguridad más novedosos.

Para diferentes sistemas operativos

Aunque el ransomware a día de hoy se dirige más a endpoints Windows, otras plataformas como Mac OS X y los SO móviles se están convirtiendo en objetivos cada vez más frecuentes. Además de Windows, SentinelOne EPP es compatible con Mac OS X, ofreciendo una cobertura del dispositivo en toda la superficie de ataque del endpoint. SentinelOne EPP es también compatible con diversos entornos virtuales y además soporta Linux, un sistema operativo cada vez más importante debido al aumento de las implementaciones de servidores Linux..

CANTIDAD	DESCRIPCIÓN	COSTO POR LICENCIA	DESCUENTO %	PRECIO CON DESCUENTO	SUBTOTAL US$
900	SentinelOne Enpoint + Consola en la nube + Entrenamiento - SUSCRIPCIÓN 1 AÑO	65.00	70.80	19.00	17,100.00
	TOTAL				**17,100.00**

OFERTA COMERCIAL Y CONDICIONES DE PAGO

CONDICIONES DE VENTA

**Vigencia de la Oferta: 19 de febrero de 2021.*

** Precios cotizados en dólares americanos.*

**** Los precios no incluyen el 16% de IVA***

MMTEC.BIZ S.A. DE C.V.
Lago Onega 431 – Interior 504
Colonia Granada – Miguel Hidalgo
CDMX - 11520

Marcelo Musacchio

Representante Legal

Tel: 556788 5237

Email: m@mmtec.biz