GUÍA PRÁCTICA PARA COMBATIR EL MALWARE AVANZADO

Todo lo que deben saber las empresas descentralizadas y las pequeñas y medianas empresas acerca de las amenazas de la red de próxima generación

PUBLICADO EN SEPTIEMBRE DE 2014

DÍA CERO ES EL NUEVO TERRENO DE COMBATE

En el campo de la biomedicina, los investigadores y médicos ya comprendieron hace tiempo que los microbios y las bacterias evolucionan y son cada vez más resistentes a los antibióticos. Necesitan desarrollar nuevos medicamentos más fuertes para mantenerse actualizados. Del mismo modo, en el mundo de la seguridad de la información, surgieron nuevas razas de malware que son más avanzadas y resistentes a las defensas convencionales. Los atacantes han evolucionado con el tiempo y son cada vez más inteligentes.

En este eBook, explicaremos cómo esto ocurrió– y más importante aún, qué puede hacer usted al respecto.

PARCHES, FIRMAS Y MÁS

DEFENSAS QUE NO LLEGAN LO SUFICIENTEMENTE LEJOS

En 2003, el gusano "SQL Slammer" paralizó el tráfico de Internet en diversas partes del mundo durante varias horas. Este tristemente célebre gusano apuntó a una conocida vulnerabilidad en la base de datos SQL de Microsoft para la cual había un parche disponible seis meses antes. Las claves de su éxito y proliferación fueron su pequeño tamaño y la forma en que se replicó rápidamente y buscaba al azar nuevos objetivos para infectar.

Durante los años siguientes, los proveedores de TI respondieron a amenazas como esta. Cada mes, Microsoft lanza al mercado una serie de actualizaciones para abordar las vulnerabilidades que se encontraron en su software. Adobe lo sigue y lanza hotfixes (parches) de seguridad en el mismo "Patch Tuesday" [N. del T.: se utiliza este término no oficial para hacer referencia al momento en que Microsoft publica en forma regular los parches de seguridad]. Cisco también proporciona un gran conjunto de soluciones relacionadas con la seguridad una vez por trimestre. Se recomienda a los administradores de TI parchear sus sistemas con frecuencia para mantenerse al día.

Otras defensas incluyen a los Sistemas de Prevención de Intrusiones (IPS, por sus siglas en inglés) que utilizan una profunda inspección de paquetes para buscar patrones conocidos de ataques a la vulnerabilidad.

Los sistemas de antivirus bloquean y envían el malware a cuarentena.

Las normas como PCI DSS (Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago) establecen que las compañías deben mantener su software de antivirus actualizado según las últimas marcas.

Se utilizan soluciones de gestión central para asegurar que todos los usuarios estén ejecutando las últimas soluciones AV en sus desktops, laptops y ahora hasta en sus dispositivos móviles con Android.

Pero no es suficiente.

¿EN QUÉ CONSISTE UNA AMENAZA PERSISTENTE AVANZADA?

Para comprender por qué las tecnologías actuales no son suficientes para proteger a la red de hoy, debemos comprender qué tienen de diferente las **Amenazas Persistentes Avanzadas** (APT, por sus siglas en inglés).

El malware moderno utiliza técnicas **avanzadas** tales como canales de comunicación encriptados, rootkits a nivel núcleo y sofisticadas capacidades de evasión para superar las defensas de la red. Más importante aún, por lo general aprovechan las vulnerabilidades del tipo día cero – fallas para las cuales aún no existen parches y aún no se escribió el código del virus. En 2012, el equipo de WatchGuard LiveSecurity® informó acerca de cuatro vulnerabilidades del tipo día cero que estaban siendo atacadas libremente. En 2013, escribimos alertas acerca de trece amenazas del tipo día cero que se estaban utilizando activa y libremente.

Por lo general, el malware moderno es **persistente** y está diseñado para permanecer. Es furtivo y oculta cuidadosamente sus comunicaciones, y "vive" la mayor cantidad de tiempo posible en una red víctima, por lo general luego limpiándose a sí mismo (eliminando registros, utilizando un fuerte encriptado y solo reportando a su controlador en pequeñas ráfagas confusas de comunicación).

Muchos ataques son ahora una mezcla combinada de diferentes técnicas. Los grupos de atacantes muy capacitados, motivados y con respaldo financiero representan **Amenazas** significativas porque tienen metas y objetivos muy específicos en mente – por lo general, una ganancia financiera a causa del robo de tarjetas de crédito y otra valiosa información sobre cuentas.

CARACTERÍSTICAS DE UNA AMENAZA PERSISTENTE AVANZADA

Con un Objetivo

El foco es una organización individual, un estado-nación o incluso una tecnología específica.

Avanzada

Un ataque desconocido del tipo día cero que tiene cargas útiles de malware y utiliza rootkits a nivel núcleo y tecnologías de detección de evasión.

Persistente

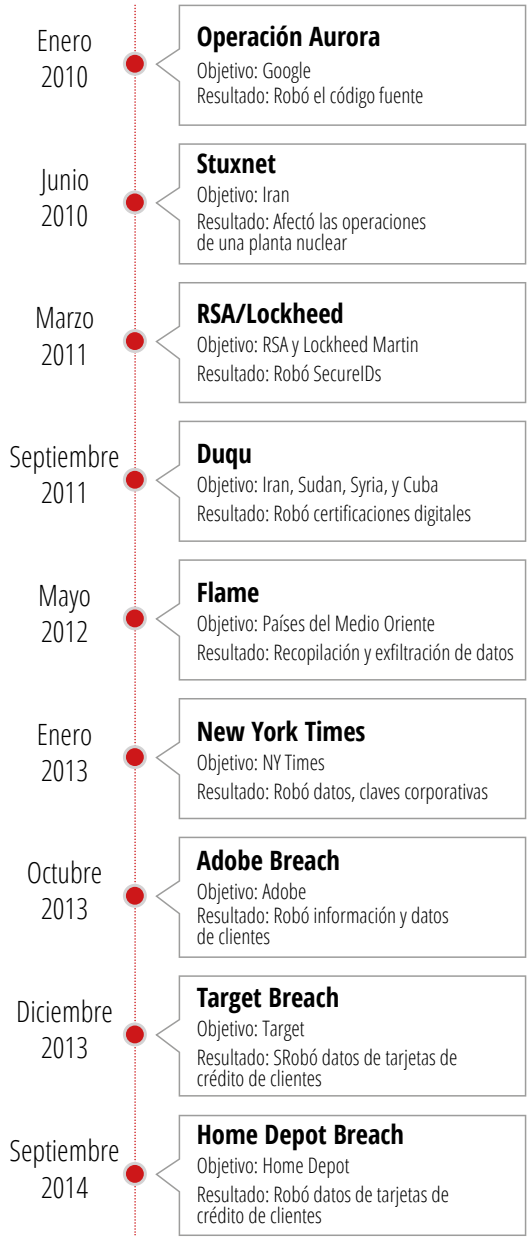
No se detiene. Continúa con la suplantación de identidades (phishing), conectándose y explorando hasta que encuentra la forma de satisfacer al malware.

LA EVOLUCIÓN DE LAS AMENAZAS PERSISTENTES AVANZADAS

TÉCNICAS ESTADO-NACIÓN AHORA UTILIZADAS PARA UNA GANANCIA FINANCIERA

Las consecuencias de las fallas son significativas para cualquier compañía. Forbes informó que las utilidades del gran minorista de los Estados Unidos, Target, tuvieron una caída del 50% en el 4° trimestre de 2013 y la razón principal fue la publicidad negativa en torno a su mayor falla de seguridad de datos en la época de las fiestas de 2013. El precio de las acciones cayó un 9%.

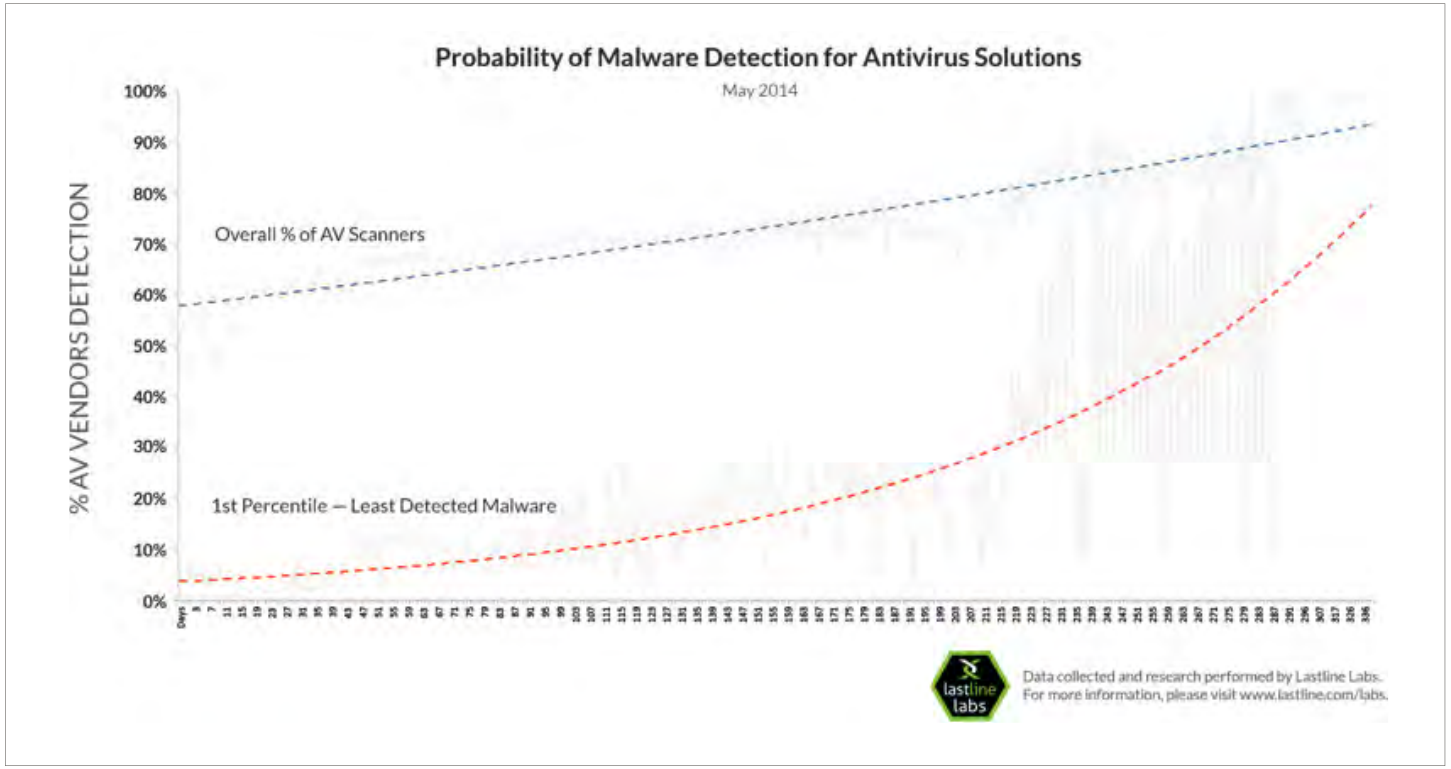
El CIO ya no es parte de la compañía y el 5-10% de los compradores de Target informó que no volverá a hacer compras en la tienda.
En los meses siguientes a la falla que sufrió Target, muchos otros grandes minoristas informaron episodios de pérdida de datos. Hacia fines de julio de 2014, el Departamento de Seguridad Nacional de los Estados Unidos emitió una advertencia en la que comunicaba que el malware en puntos de venta Backoff y sus variantes habían comprometido a más de 1.000 redes. Instaron a las compañías a que buscaran a Backoff en sus redes.



LOS ANTIVIRUS NO PUEDEN SEGUIR EL RITMO

La lucha contra el código malicioso es una carrera armamentista. Cuando los defensores presentan nuevas técnicas de detección, los atacantes tratan de encontrar nuevas maneras de superarlas. Las compañías de antivirus (AV) tradicionales emplean ingenieros y escritores de códigos de virus para analizar los archivos. Controlar la ejecución de programas desconocidos en un entorno instrumentado. O pueden enviar archivos a herramientas como Anubis, que ejecutan un archivo e informan acerca de cualquier actividad o conducta sospechosa que indique la presencia de un virus. Pero escribir códigos de virus está perdiendo propósito porque hay un 88% de probabilidad de que se haya creado un nuevo malware como variante del malware existente para evitar la detección mediante las técnicas clásicas.

Lastline Labs publicó una investigación basada en cientos de miles de piezas de malware que detectaron en un año, desde mayo de 2013 a mayo de 2014. Se probó cada muestra de malware contra los 47 proveedores de antivirus que ofrece VirusTotal, un sitio de terceros que reúne y compara diferentes soluciones de AV. La meta consistía en determinar cuán efectivo es el AV, qué motores detectaron a las muestras de malware y cuán rápido detectaron nuevo malware. Los resultados fueron increíbles.



- **El Día O, solo 51%** de los escáneres de AV detectaron nuevas muestras de malware.
- **Luego de 2 semanas, hubo un salto notable** en las tasas de detección (hasta del 61%), lo que demostró el clásico retraso de los proveedores de AV.
- **El malware en la categoría "con menor probabilidad de ser detectada" de un percentil** (línea roja) no fue detectado por la mayoría de los escáneres de AV durante meses y, en algunos casos, nunca fue detectado.

LA EVOLUCIÓN DE LAS DEFENSAS

PASO 1: MÁS ALLA DEL ENTORNO DE PRUEBAS (SANDBOX)

Actualmente, se utilizan soluciones de entorno de pruebas en forma automática como parte del proceso de detección. Se ejecuta y analiza el código en forma dinámica en el entorno de pruebas sin ningún tipo de revisión humana. Pero los autores de malware ahora utilizan técnicas evasivas para asegurar que sus programas no revelen ninguna actividad maliciosa al ejecutarlos en dicho entorno de análisis automatizado.

Algunas de las técnicas comunes utilizadas por el malware incluyen:

- **Verificar la presencia** de una máquina virtual
- **Buscar conocidas claves de registro** de Windows que indiquen un entorno de pruebas en particular
- **Esperar** a que el entorno de pruebas finalice el análisis

Los proveedores de seguridad reaccionaron agregando cierta contrainteligencia de sus propios sistemas. Verifican búsquedas de malware para claves reconocidas y fuerzan a que un programa se despierte luego de hibernar. Pero este enfoque es aún reactivo. Los sistemas de análisis de malware deben actualizarse manualmente para abordar cada nuevo truco evasivo. Los autores de malware que crean evasiones del tipo día cero pueden sortear la detección hasta tanto se actualice el entorno de pruebas.

LIMITACIONES DE LOS ENTORNOS DE PRUEBAS EN BASE A LA VIRTUALIZACIÓN

Hoy en día, las implementaciones más comunes de entornos de pruebas por lo general dependen de un entorno virtual que contiene el sistema operativo huésped. En ciertas ocasiones un entorno de pruebas ejecuta el sistema operativo directamente en una máquina real. El problema clave, y la limitación fundamental de los entornos de pruebas modernos basados en la virtualización, es su falta de visibilidad y conocimiento sobre la ejecución de un programa de malware. El entorno de pruebas necesita ver la mayor cantidad posible de conductas del malware, pero lo hace a escondidas del malware. Si el malware pudiera detectar la presencia de un entorno de pruebas alterará su conducta.

Por ejemplo, en lugar de simplemente hibernar, los programas sofisticados realizan algún tipo de computación (inútil) que da la apariencia de una actividad. De tal manera, no hay forma de que el entorno de pruebas despierte al programa. El programa simplemente ejecuta, y desde el punto de vista del sistema de análisis de malware, todo es normal.

Por lo general, el malware se ejecuta en modo usuario (ya sea como usuario regular o administrador). Los entornos de pruebas basados en la virtualización observan las llamadas del sistema y las llamadas API de Windows desde los programas en modo usuario. Las llamadas del sistema o las llamadas de función capturan todas las interacciones entre un programa y su entorno (por ejemplo, cuando se leen los archivos, se escriben las claves de registro y se produce tráfico de red). Pero el entorno de pruebas es ciego a todo lo que ocurre entre las llamadas de sistema. Los autores de malware pueden apuntar a este punto ciego. En nuestro ejemplo, el código dilatorio es un código que se ejecuta entre las llamadas de sistema.

PASO 2: EMULACIÓN TOTAL DEL SISTEMA

Se requiere un enfoque más inteligente. Un emulador es un programa de software que simula la funcionalidad de otro programa o de una pieza de hardware. Un emulador brinda mayor flexibilidad porque implementa funcionalidad en el software. La emulación OS del sistema operativo proporciona un alto nivel de visibilidad en torno a las conductas del malware. Pero los emuladores de nivel OS no pueden replicar cada llamada en un sistema operativo. Por lo general, se enfocan en un subconjunto popular de funcionalidades. Desafortunadamente, este enfoque es el más fácil de detectar y evadir por parte del malware.

La emulación total del sistema, donde el emulador simula el hardware físico (incluyendo CPU y memoria), brinda el nivel más profundo de visibilidad de la conducta del malware, y es el más difícil de detectar por parte del malware avanzado.

APT BLOCKER DE WATCHGUARD

APT Blocker, un nuevo servicio disponible para todos los dispositivos UTM y NGFW de WatchGuard, utiliza la emulación total del sistema (CPU y memoria) para obtener vistas detalladas de la ejecución de un programa de malware. Luego de ejecutarse primero a través de otros servicios de seguridad, se deja una impresión de los archivos en la memoria y se comparan con una base de datos existente – primero en el dispositivo y luego en la nube. Si nunca antes se vio el archivo, se analiza utilizando el emulador de sistema, que monitorea la ejecución de todas las instrucciones. Puede identificar las técnicas de evasión que otros entornos de pruebas no logran hacerlo.

Al detectar malware se lo puede bloquear inmediatamente en el firewall. En ciertas ocasiones, un archivo realmente del tipo día cero puede pasar mientras se realiza el análisis en la nube. En tales casos, el sistema WatchGuard puede proporcionar alertas inmediatas avisando que un código sospechoso se encuentra en la red a fin de que TI pueda hacer el correspondiente seguimiento en forma inmediata.

TIPOS DE ARCHIVOS ANALIZADOS POR APT BLOCKER

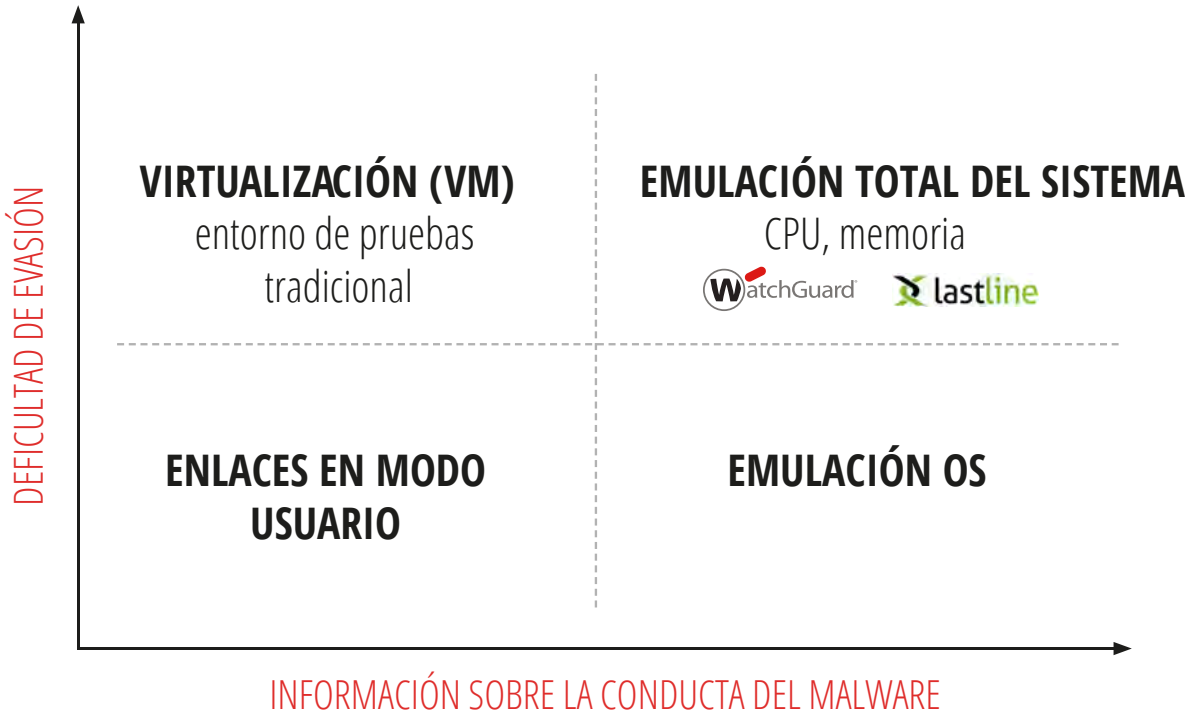
- Todos los archivos ejecutables de Windows
- Adobe PDF
- Microsoft Office
- Archivos del Instalador de Aplicaciones para Android (.apk)
- Se descomprimen los archivos comprimidos como archivos .zip de Windows

LASTLINE TECHNOLOGY

WatchGuard eligió un socio líder en el mercado para el desarrollo del servicio APT Blocker. Lastline Technology fue fundada por el equipo técnico que desarrolló Anubis, la herramienta que ha sido utilizada durante los últimos ocho años por investigadores alrededor del mundo para analizar archivos en búsqueda de malware potencial.

DIFICULTAD DE EVASIÓN PARA DETECTAR MALWARE

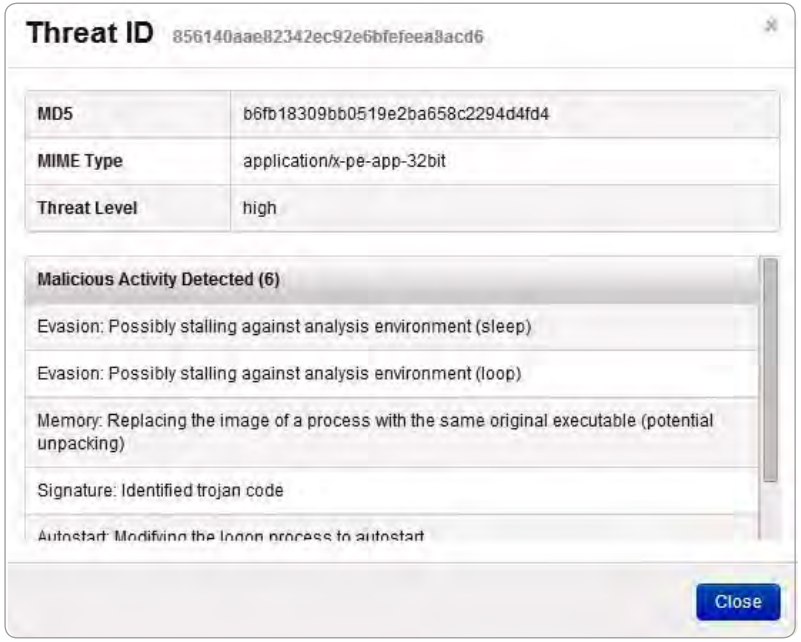
La emulación total del sistema es la más fuerte detección de malware.



PASO 3: VISIBILIDAD DEL SISTEMA

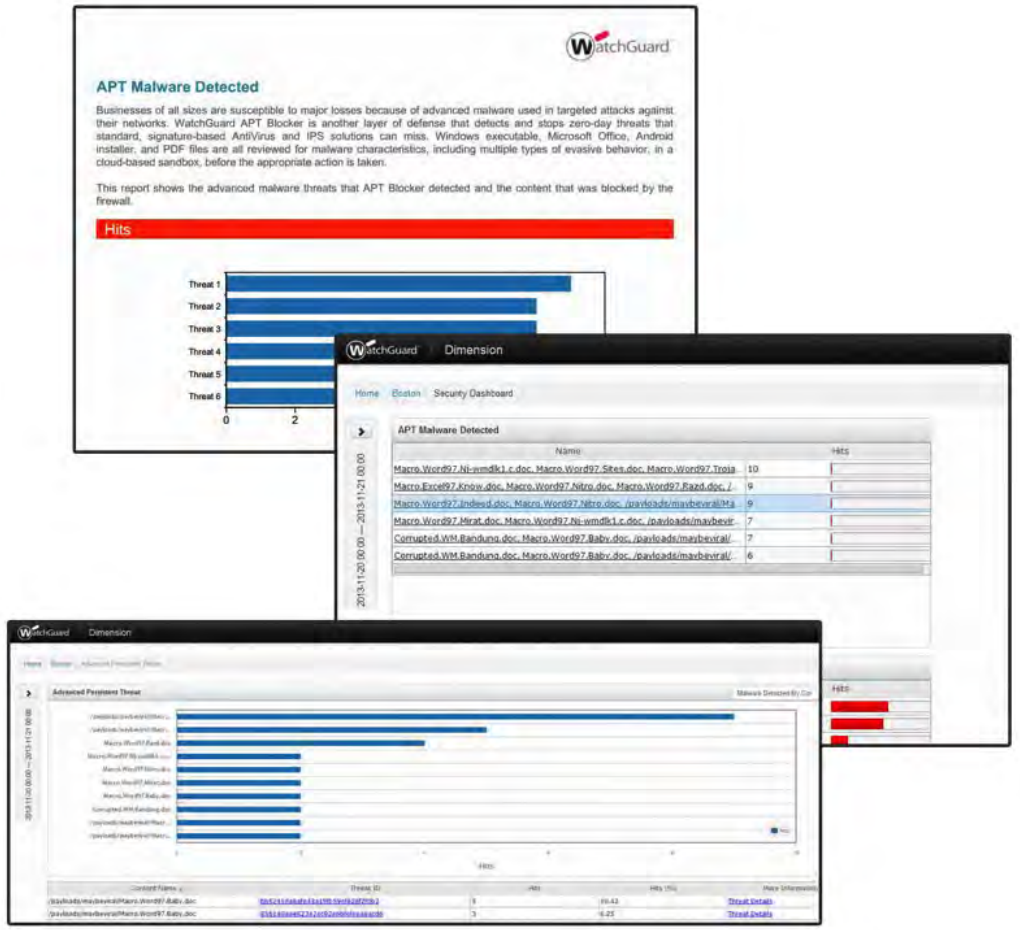
WatchGuard Dimension™ también incluye actividad APT en los paneles de seguridad de nivel superior, junto con informes detallados de todos los otros servicios de seguridad. Los breves informes ejecutivos de nivel superior incluyen la actividad de APT, y existen diez diferentes informes predefinidos para que elija el administrador.

EL INFORME DE APT MUESTRA LA ACTIVIDAD MALICIOSA



El ejemplo anterior muestra diversas características típicas del malware. Las dos evasiones de arriba demuestran cómo la solución pudo detectar la actividad maliciosa que puede haber engañado a otras soluciones de entorno de pruebas.

ACTIVIDADES DE APT BLOCKER VISTAS A TRAVÉS DE LA DIMENSIÓN DE WATCHGUARD



PASO 4: INFORMACIÓN ACCIONABLE

La detección de malware no es suficiente. El personal de TI debe obtener información clara y accionable que no se pierda en un mar de datos de registros. Los departamentos de TI deben mantener el negocio funcionando y ayudar al balance final. A pesar del tremendo impacto que pueden tener los incidentes de seguridad en un negocio, muchos departamentos de TI desconfían de las presuntas alertas de seguridad. Neiman Marcus tuvo más de 60.000 incidentes de registros que demostraban que su red tenía malware. Target tenía archivos de registro un par de días después de la primera falla indicando que existía un problema pero dichos archivos de registro fueron ignorados.

Cualquier solución de malware avanzado debe proporcionar lo siguiente:

- Alertas por correo electrónico cuando se detecta un archivo dañino
- Capacidades de registro e informe que se integren con otras capacidades de seguridad en la red
- Una clara indicación del motivo por el cual se identificó a un archivo como malware para que no sea rechazado en forma inmediata como un potencial falso positivo

La solución APT BLOCKER DE WATCHGUARD

cumple con todos los requisitos de visibilidad con alertas por correo electrónico, análisis de registros en tiempo real y la capacidad de investigar con mayor profundidad para buscar más información.
El servicio está totalmente integrado con WatchGuard Dimension, la galardonada solución de visibilidad e inteligencia de seguridad que se incluye sin cargo en todas las soluciones UTM y NGFW de WatchGuard. Va más allá de una simple alerta indicando que se trata de un archivo sospechoso.
Se proporciona un detallado informe de actividad maliciosa para cada archivo clasificado como malware.

MANTENGA SUS DATOS SEGUROS CON LA DETECCIÓN DE MALWARE AVANZADO

Las amenazas han evolucionado. Los hackers de hoy en día utilizan las mismas técnicas avanzadas que se utilizaron previamente en ataques a estados-naciones en los últimos años.

Las soluciones de seguridad deben evolucionar para mantenerse un paso adelante de dichas amenazas y para mantener a su red segura. La detección de malware basado en códigos de virus ya no es suficiente. Los servicios de prevención de intrusiones y antivirus son aún una parte necesaria de la defensa de cualquier compañía pero deben complementarse con nuevas capacidades de detección avanzada con cuatro características clave:

1. **Un entorno de pruebas en la nube** con emulación total del sistema – con la capacidad de analizar múltiples tipos de archivos
2. **La capacidad de ir más allá** del entorno de pruebas para detectar diferentes formas de evasiones avanzadas
3. **Visibilidad con alertas claras** de todo el malware detectado y explicaciones con los motivos por los cuales se considera que un archivo es malicioso
4. **La capacidad de responder en forma proactiva** y bloquear archivos maliciosos

APT Blocker de WatchGuard trasciende la detección de antivirus basada en códigos de virus, utilizando un entorno de pruebas basado en la nube con emulación total del sistema para detectar y bloquear ataques del tipo día cero y malware avanzado.

Para mayor información acerca de APT Blocker de WatchGuard y otros servicios de seguridad líderes en el mercado ofrecidos por WatchGuard en sus plataformas UTM y NGFW, visite www.watchguard.com/apt.

DOMICILIO:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Sitio Web:
www.watchguard.com

VENTAS EN AMÉRICA DEL NORTE: +1.800.734.9905

VENTAS INTERNACIONALES:
+1.206.613.0895

ACERCA DE WATCHGUARD

WatchGuard® Technologies, es líder global de soluciones de seguridad integradas y multifunción para empresas que combinan de forma inteligente el hardware estándar de la industria, las mejores funciones de seguridad y herramientas de gestión basadas en políticas. WatchGuard proporciona una forma fácil y poderosa de protección a cientos de miles de empresas de todo el mundo. Los productos WatchGuard están respaldados por WatchGuard LiveSecurity® Service, un innovador programa de soporte. WatchGuard tiene su sede en Seattle, Washington y oficinas en toda América del Norte, Europa, Asia-Pacífico y América Latina. Para mayor información, visite WatchGuard.com

NOTAS FINALES

i http://en.wikipedia.org/wiki/SQL_Slammer
ii http://watchguardsecuritycenter.com
iii http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/
iv http://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059/
v http://bits.blogs.nytimes.com/2014/08/22/secret-service-warns-1000-businesses-on-hack-that-affected-target/?_php=true&_type=blogs&_r=0]
vi http://info.lastline.com/blog/next-generation-sandbox-offers-comprehensive-detection-of-advanced-malware
vii http://info.lastline.com/blog/different-sandboxing-techniques-to-detect-advanced-malware
viii http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data
ix http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p1
x http://www.watchguard.com/news/press-releases/network-computing-awards-names-watchguard-dimension-best-new-product-of-the-year.asp