PANDA
CLOUDINTERNETPROTECTION

Simply... Evolution

CÓMO LOS HACKERS ATACAN A LAS EMPRESAS DESDE DENTRO DE LA RED

PANDA CLOUD
OFFICE PROTECTION

PANDA CLOUD
EMAIL PROTECTION

PANDA CLOUD
INTERNET PROTECTION

PANDA SECURITY

INTRODUCCIÓN

A medida que las defensas de las empresas evolucionan, también lo hacen los métodos de ataque empleados por aquellos que intentan superarlas. Estamos entrando en una época en la que los atacantes han dejado de asaltar las fortalezas empresariales desde fuera. No les hace falta, ya están dentro. Gracias al incremento meteórico del flujo de tráfico Web y a la lista impresionante de vulnerabilidades presentes en las aplicaciones Web que residen en las máquinas de los usuarios, éstos se han convertido en agentes que facilitan los ataques a las empresas. Basta con convencer a un empleado confiado de que visite una página Web, para que un hacker pueda conseguir acceso a datos valiosos en el corazón de una red supuestamente segura.

Durante demasiado tiempo, las empresas han enfocado la mayoría de sus recursos de seguridad en la protección de los servidores corporativos, ignorando los riesgos inherentes a los PCs de los empleados. En la medida en que los controles de seguridad para los servidores con conexión a nternet han mejorado –gracias a los esfuerzos de las empresas de software y a los equipos de seguridad de las compañías– los atacantes han empezado a buscar blancos más fáciles: PCs con poca seguridad y usuarios con pocos conocimientos.

Proteger cientos de servidores con un equipo de administradores expertos resulta sencillo comparado con la tarea de ofrecer seguridad a miles de PCs y formar a los empleados que los utilizan. Y este reto va a ser cada vez más complicado dado que los usuarios tienen cada vez más movilidad, situándose fuera del alcance de la protección de la red local. Los hackers, además, de ser conscientes de esto, disponen de recursos, la motivación económica necesaria y un verdadero ejército de atacantes. A medida que los ataques evolucionan, también debe hacerlo la seguridad de las empresas, adoptando soluciones que proporcionen una protección uniforme a todos los usuarios, ya sean PCs dentro de la sede central de la compañía o el portátil de un empleado navegando por la Web desde su café preferido.

Las redes corporativas se describen a menudo como si fuesen un caramelo – duro y crujiente por fuera, blando y masticable por dentro. Construimos fosos y muros impenetrables alrededor de la red de la empresa, la fortaleza que guarda nuestros preciados tesoros digitales. Los atacantes lo saben, y al igual que con el Caballo de Troya de la mitología griega, saben que es mucho más fácil atacar dicha estructura desde dentro que atravesar múltiples capas de seguridad hasta llegar al oro. A diferencia, sin embargo, de los astutos griegos que entraron en Troya escondidos en el gigantesco caballo de madera, los hackers de nuestra época tienen ya su ejército dentro de nuestras fortificaciones, esperando la orden de atacar. Y seguramente, usted conoce ya esta brigada virtual por su nombre más común: los empleados.

Es difícil encontrar hoy en día una oficina donde Internet no sea el recurso más apreciado por los empleados. Internet es un bien imprescindible, ya sea para enviar correo o navegar por la Web.Sin embargo, también resulta un campo de minas lleno de riesgos de seguridad. Hay sitios de phishing que parecen de la nada y se esfuman con la misma velocidad. Las redes sociales se han convertido en un caldo de cultivo para los hackers, con ataques llegando cada día en forma de spam a los buzones de los usuarios o en los

comentarios de sus blogs. Y en la era de la Web 2.0, dónde prima el contenido generado por los usuarios, los sitios legítimos se han convertido en tablones de anuncios virtuales para ataques de contenido activo y binarios maliciosos.

Lejos quedan los días en los que los atacantes golpeaban tenazmente contra los recursos perimetrales –servidores Web y de correo-, con la esperanza de encontrar un servidor desactualizado, sin los últimos parches y actualizaciones. Cada vez es más difícil encontrar un servidor con agujeros de seguridad, gracias a que los administradores de redes y proveedores de software son cada vez más conscientes de los peligros existentes, y son más diligentes a la hora de implementar buenas prácticas de codificación. Esto se debe en gran parte a las duras lecciones aprendidas en el pasado. Pero, ¿por qué perder tiempo buscando servidores vulnerables en una empresa, cuando en la misma compañía existen miles de usuarios vulnerables?

Durante años, las empresas han invertido gran parte de su presupuesto de seguridad en proteger sus joyas de la corona, es decir, los servidores corporativos. Después de todo, allí es donde residen los datos más importantes. Han comprado firewalls y sistemas de detección de intrusos (IDS). Han blindado los servidores y optimizado los ciclos de parches para asegurarse de que los recursos con conexión al exterior estén a prueba de todo. Mientras tanto, la seguridad del usuario final ha quedado en gran parte olvidada.

Es cierto que cada PC tiene su antivirus y que los usuarios tienen que leer y firmar una política de seguridad, pero en el mundo Web 2.0 en el que se puede infectar un PC simplemente con abrir una página Web, estas medidas son de poca utilidad. Proteger una red ya no sólo implica proteger un puñado de servidores en la zona desmilitarizada. Eso es fácil. Lo difícil es proteger a miles de usuarios itinerantes contra ataques cada vez más dinámicos, y para los cuales quizás no existan parches.

ANTECEDENTES

Tanto las técnicas empleadas por los hackers, como las medidas protectoras diseñadas por los expertos de seguridad han evolucionado a lo largo de los años. Podemos hablar de distintas épocas en la historia de la seguridad informática, cada una de ellas marcada por diferentes formas de ataque. Se ha dicho, y es cierto, que la batalla entre los atacantes de redes y sus defensores es como un interminable juego del gato y ratón; pero las reglas no dejan de cambiar. Es importante, sin embargo, mirar hacía atrás para aprender del pasado y a la vez mirar a la bola de cristal para anticiparse a lo que se nos viene encima.

El gusano "I Love You", identificado por primera vez el 4 de mayo de 2000, era simplemente un archivo de VBScript adjunto a un mensaje con el asunto "I Love You". 1 Los receptores de este correo estaban tan ansiosos por averiguar quien era su admirador secreto que cientos de miles de máquinas se infectaron en unas pocas horas, mientras que los administradores tuvieron que dedicar largas jornadas a reparar el daño.

La motivación principal de los atacantes en esta época era conseguir fama y notoriedad. En el caso del gusano "I Love You", salvo la

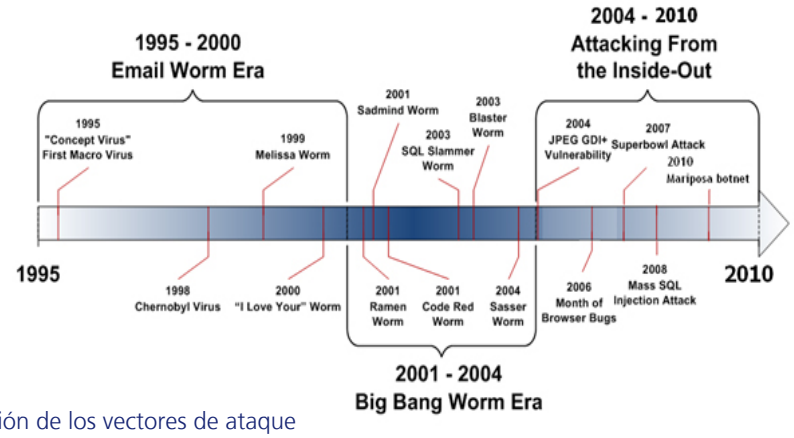

Figura 1 – Evolución de los vectores de ataque

1995-2000 – Atacando al cliente:

La era de los gusanos de correo electrónico

Hacia finales del milenio pasado, los atacantes aprovecharon la explosión de la popularidad del correo electrónico combinándola con la ingeniería social para empezar una nueva era: la era de los gusanos de correo electrónico. El correo electrónico resultaba el medio ideal para los ataques. Mediante el email, un hacker podía enviar archivos adjuntos a miles de usuarios –específicos o escogidos al azar– con un mínimo esfuerzo y coste. El único desafío consistía en convencer al usuario final de que abriese el adjunto, y en este sentido fuimos testigos de un gran despliegue de creatividad por parte de los 'malos'.

sobreescritura de ciertos archivos para propagarse, el daño en sí mismo era relativamente pequeño, y quedaba claro que el gusano no había sido diseñado con fines económicos. David L. Smith, el autor del gusano 'Melissa' admitió durante su juicio que bautizó el malware con el nombre de una stripper que había conocido en Florida. Smith tuvo el dudoso honor de ser la primera persona en los Estados Unidos en ser condenada por crear un programa malicioso.2 Los creadores de estos gusanos, así como los autores de la mayoría de las amenazas de esta época, estaban motivados por la curiosidad o incluso por su propio ego, pero no por el dinero.

1 http://www.pandasecurity.com/homeusers/security-info/about-malware/encyclopedia/overview.aspx?idvirus=28492
2 http://news.zdnet.com/2100-9595_22-517177.html

1995-2000 – Atacando al cliente:

La era de los gusanos de correo electrónico

Hacia finales del milenio pasado, los atacantes aprovecharon la explosión de la popularidad del correo electrónico combinándola con la ingeniería social para empezar una nueva era: la era de los gusanos de correo electrónico. El correo electrónico resultaba el medio ideal para los ataques. Mediante el email, un hacker podía enviar archivos adjuntos a miles de usuarios –específicos o escogidos al azar– con un mínimo esfuerzo y coste. El único desafío consistía en convencer al usuario final de que abriese el adjunto, y en este sentido fuimos testigos de un gran despliegue de creatividad por parte de los 'malos'. El gusano "I Love You", identificado por primera vez el 4 de mayo de 2000, era simplemente un archivo de VBScript adjunto a un mensaje con el asunto "I Love You". 1
Los receptores de este correo estaban tan ansiosos por averiguar quien era su admirador secreto que cientos de miles de máquinas se infectaron en unas pocas horas, mientras que los administradores tuvieron que dedicar largas jornadas a reparar el daño.
La motivación principal de los atacantes en esta época era conseguir fama y notoriedad. En el caso del gusano "I Love You", salvo la sobreescritura de ciertos archivos para propagarse, el daño en sí mismo era relativamente pequeño, y quedaba claro que el gusano no había sido diseñado con fines económicos. David L. Smith, el autor del gusano 'Melissa' admitió durante su juicio que bautizó el malware con el nombre de una stripper que había conocido en Florida. Smith tuvo el dudoso honor de ser la primera persona en los Estados Unidos en ser condenada por crear un programa malicioso. 2 Los creadores de estos gusanos, así como los autores de la mayoría de las amenazas de esta época, estaban motivados por la curiosidad o incluso por su propio ego, pero no por el dinero.

2001-2004 – Atacando al servidor:

El 'Big Bang' de los gusanos

La creación de un gusano que se aprovechase de la ingenuidad humana para propagarse no suponía un gran reto. Los atacantes se limitaban a crear aplicaciones, ya fuesen código compilado o scripts interpretados, y las enviaban por correo a las víctimas con la esperanza de que -con la ayuda de algún truco de ingeniería social- se ejecutasen. Durante la siguiente época (el 'Big Bang' de los gusanos), los atacantes se mostraron mucho más hábiles, aprovechando vulnerabilidades existentes en las aplicaciones más populares de los servidores. Afortunadamente para los atacantes, nunca faltaban agujeros de seguridad en la infraestructura de Internet que explotar, y las empresas facilitaban el proceso con ciclos de parches muy lentos.

El gusano SQL Slammer, que empezó a propagarse el 25 de enero de 2003, es un ejemplo perfecto de cómo se aprovechaban las vulnerabilidades durante esta época. El gusano se difundió con tanta rapidez que paralizó zonas enteras de la Web. Gracias en parte a la capacidad de Slammer de propagarse a través de paquetes individuales UDP, en las fases iniciales de la infección el número de sistemas infectados se duplicaba cada 8,5 segundos. 3 Pese a que Microsoft publicó el parche para reparar el agujero de seguridad que explotaba SQL Slammer el 24 de julio de 2002, 4 numerosos sistemas seguían siendo vulnerables unos seis meses después de la aparición del gusano. Y eso a pesar de que el investigador David Litchfield había publicado una prueba de concepto del exploit durante el congreso BlackHat Briefings de 2002 (concretamente, el 1 de agosto de 2002). 5

3 http://www.wired.com/wired/archive/11.07/slammer.html
4 http://www.microsoft.com/technet/security/bulletin/Ms02-039.mspx

Año 2004 y siguientes – Atacando desde dentro:

La era de la 'motivación económica'

A partir del año 2004, los gusanos de propagación rápida han dejado de ser noticia de forma gradual. ¿Significa esto que los buenos han ganado la batalla? ¿Es la Web, de repente, más segura? No, todo lo contrario, los atacantes no han abandonado la lucha; simplemente han adoptado tácticas mas adecuadas en un escenario muy dinámico. Aunque este escenario ha cambiado en parte debido a una mejor protección de los recursos que dan acceso a Internet, también ha cambiado por la entrada en escena del crimen organizado. Los atacantes ya no lanzan ataques llamativos.

En su lugar, ya sea aprovechando vulnerabilidades o lanzando ataques de ingeniería social, intentan pasar desapercibidos, multiplicando así el valor que obtienen de sus ataques.

En enero de 2008 fuimos testigos de un ejemplo claro de este nuevo tipo de ataque. Mediante ataques SQL automatizados se inyectó codigo malicioso en al menos 70.000 sitios Web públicos. Los servidores no eran el objetivo final; simplemente ofrecían una plataforma para el ataque. El código inyectado en estos sitios explotaba numerosas vulnerabilidades conocidas, instalando keyloggers en los ordenadores de las víctimas que visitaban las páginas Web usando navegadores vulnerables. Con keyloggers instalados en miles de PCs, los atacantes tenían acceso a gran cantidad de datos confidenciales: nombres de usuario, contraseñas de acceso y números de tarjetas de crédito.

Este ataque aprovechaba vulnerabilidades comunes de los servidores Web para infectar a aquellos que visitaban los sitios comprometidos. Sin embargo, no siempre resulta necesario identificar sitios vulnerables, como se demostró cuando MySpace se las vio con el gusano Samy. Samy era un ataque no malicioso de cross site scripting (XSS) que automatizaba el proceso de añadir amigos al perfil de Samy Kamkar. [6] El gusano fue lanzado como un experimento por parte del chico de 19 años, y acabó por afectar a mas de un millón de usuarios de MySpace. Samy Kamkar salió con libertad condicional y tuvo que realizar servicios a la comunidad por haber llevado a cabo su 'ataque.' [7]
Este ataque fue posible gracias a que MySpace, como muchos otros sitios Web 2.0, permite a los usuarios añadir su propio contenido HTML. Como medida de seguridad, y para prevenir usos maliciosos, se identifica y bloquea el contenido no deseado, como JavaScript.

A este proceso se le llama 'blacklisting' o listado en lista negra. Sin embargo, resulta muy difícil bloquear todo el contenido malicioso ya que existen numerosos trucos de codificación que pueden emplearse para evitar las restricciones de seguridad; una lección que MySpace aprendió de la forma más dura. Ambos ataques aprovechaban debilidades en el servidor para llegar a su objetivo final: el navegador Web de una victima confiada. Esto muestra una tendencia cada vez más popular entre los atacantes, y que debe su éxito a la falta de énfasis en la importancia de proteger los navegadores, así como a los beneficios económicos que ofrece a los hackers. Esta tendencia requiere además de un cambio en el enfoque tradicional de seguridad si se quiere combatir la amenaza de forma efectiva.

5 http://www.blackhat.com/presentations/bh-asia-02/bh-asia-02-litchfield.pdf
6 http://blogoscoped.com/archive/2005-10-14-n81.html
7 http://it.slashdot.org/article.pl?sid=07/02/04/1439222

LOS PROTAGONISTAS

Fabricantes de software

Durante el 'Big Bang' de los gusanos, ninguna empresa, distribuidor de código abierto ni comercial se libró del mal trago de tener que explicar a sus clientes que la existencia de un agujero de seguridad en sus soluciones para empresas había comprometido la seguridad de miles de servidores. La mayoría de las veces el daño era importante y fulgurante, llegando en forma de gusano de rápida propagación que atacaba de forma indiscriminada. Sin embargo, las empresas que sufrían los ataques estaban lejos de ser víctimas inocentes. En cada uno de los ejemplos tratados anteriormente existían parches disponibles para las vulnerabilidades explotadas. Se atacaban vulnerabilidades conocidas, pero pese a ello, dichos ataques eran extraordinariamente exitosos gracias a que los ciclos de parches de las empresas eran demasiado largos.

En algunos casos se argumentaba que eran necesarios largos periodos de testeo antes de poder implementar los parches, mientras que en otros casos, las empresas responsables simplemente no entendían los riesgos que suponía no aplicar los parches necesarios. En muchos aspectos, estos fueron los buenos tiempos – cuando el daño era visible. Aunque costoso, estaba claro cuando comenzaba y terminada un ataque y también quedaba claro qué era lo que había que limpiar. Según se avanza hacia la era en la que los ataques se dirigen a usuarios finales específicos y los atacantes son extremadamente cuidadosos en mantenerse por debajo del radar, los gusanos que hacían mucho 'ruido' parecen un auténtico lujo.

Los gusanos de la época del Big Bang fueron directamente responsables de los cambios en las prácticas de desarrollo. Las empresas de software se dieron cuenta de que, a menos que se produjera un cambio radical en su forma de desarrollar software, producir software vulnerable era inevitable. En ningún sitio tuvo más impacto esta nueva realidad que en Microsoft. Después del descubrimiento de embarazosas vulnerabilidades en prácticamente todos sus servicios de Internet más importantes - explotadas por gusanos como Code Red, SQL Slammer y Passer-, Bill Gates emitió un famoso comunicado explicando la necesidad de dar más importancia a la seguridad, disponibilidad y privacidad de todos los productos de software. [8] Este comunicado supuso el comienzo de la iniciativa 'Trustworthy Computing'. Microsoft se dio cuenta de que si seguía ignorando los aspectos de seguridad tras estos hechos iría directa al fracaso.

La seguridad debía ser tenida en cuenta desde el primer día. Eso significaba que todas las personas involucradas en el ciclo de desarrollo del software debían ser responsables de la seguridad de un producto – no sólo el equipo de seguridad. Esta filosofía llevó a la creación del Security Development Lifecycle de Microsoft, con la arquitectura de Michael Howard y Steve Lipner. Este ciclo ha tenido como resultado una disminución significativa de las vulnerabilidades críticas en las aplicaciones para servidores de las empresas. Microsoft fue líder también de otro cambio importante en esta época. Desde octubre de 2003, la compañía pasó de lanzar parches de seguridad en intervalos impredecibles a hacerlo de forma regular cada mes. [9]

En la actualidad, Microsoft publica sus parches el segundo martes de cada mes a la 1 PM EST. Aunque las empresas no sepan exactamente qué es lo que se va a publicar, al menos pueden estar seguras de que existe personal adecuado trabajando en el testeo y desarrollo de los parches publicados.

Otra iniciativa fundamental que ahora es común entre las empresas de software es la creación de equipos de respuesta. A finales de los años 90, si se descubría una vulnerabilidad de seguridad en una aplicación comercial, era realmente complicado notificárselo a la empresa afectada para que pudiese publicar el parche correspondiente. Como mucho, se podía llegar a rastrear el punto adecuado de contacto, pero en ese caso no era nada raro encontrarse con prácticas intimidatorias o presiones legales para que el asunto no saliese a la luz. Sin embargo y una vez más, las empresas aprendieron de sus errores. Se dieron cuenta de que los investigadores independientes podían ser una valiosa prolongación de sus equipos internos de seguridad e implementaron los recursos necesarios para promover y facilitar la comunicación entre ellos. Hoy día, toda empresa importante de seguridad dispone de un equipo responsable de responder a los informes sobre vulnerabilidades y de asegurarse de que son atendidos.

8 http://news.cnet.com/2009-1001-817210.html
9 http://news.cnet.com/Microsoft-releases-monthly-security-fixes/2100-7355_3-5091835.html

Empresas

Las empresas han aprendido las lecciones de la época del 'Big Bang' de los gusanos. Mientras que, anteriormente, los ciclos de parches de las empresas duraban semanas, e incluso meses, la mayoría de compañías se dan cuenta ahora de que no proteger las vulnerabilidades conocidas mientras los hackers se afanan en crear código para explotarlas es peor que la posibilidad de que surjan problemas de incompatibilidad. Además, los equipos de seguridad de las empresas son cada vez más diligentes a la hora de reforzar los servidores antes del despliegue y de realizar exámenes de seguridad tanto internos como por parte de terceros a intervalos regulares.

En lo que respecta a los gastos de seguridad informática, históricamente la mayoría de fondos se dedicaban a los servidores de seguridad. En los primeros años 90, las empresas invertían mucho en firewalls para mantener a los 'malos' fuera. Sin embargo, en el momento en que fue necesaria una seguridad más granular, el gasto pasó a sistemas de prevención y detección de intrusiones basados en red. Según avanzamos por la pila de protocolos, las empresas han optado por firewalls para las aplicaciones Web y pasarelas de seguridad para el correo electrónico. Mientras que, en la última década, las empresas han blindado los servidores con acceso a Internet, el acceso a los equipos de sobremesa se ha movido en la dirección contraria.

Las máquinas de sobremesa han pasado de albergar un único y básico navegador Web capaz de digerir HTML, a disponer de cientos de aplicaciones que se benefician de contenido dinámico Web, actualizaciones, archivos de ayuda y comunicaciones. De hecho, hoy en día sería realmente difícil encontrar una aplicación moderna que no interactúe con recursos Web. Al mismo tiempo, los empleados demandan cada vez más tener acceso a la Web ya que hace tiempo que Internet se ha convertido en un recurso crítico para su trabajo. Sin embargo y pese a todo ello, los gastos informáticos aún no están en consonancia con este cambio. Más allá de la protección antivirus para equipos de sobremesa y quizá de los esfuerzos para blindar dichos ordenadores, poco más se ha hecho para proteger a los usuarios finales de las amenazas externas. Los atacantes son muy conscientes de esta incoherencia en los gastos de seguridad y sus ataques han evolucionado para centrarse en las máquinas vulnerables y fácilmente accesibles de los usuarios finales.

Atacantes

La fama y notoriedad que una vez inspiraron a los atacantes han sido reemplazados por una nueva motivación: el beneficio económico. En los últimos años se han realizado un gran número de estudios para tratar de cuantificar el daño ocasionado por las epidemias de códigos peligrosos. En el año 2001, NewsFactor calculó que el gusano provocó tales ataques, hay otro factor que ha jugado un papel importante. Los atacantes están hoy mejor organizados y están motivados por la oportunidad de beneficiarse económicamente de sus creaciones. Ya no les interesa aparecer en la portada del Wall Street Journal por haber creado un gusano que haya hecho mucho ruido. Cuando uno es consciente de un ataque, puede prevenirlo.

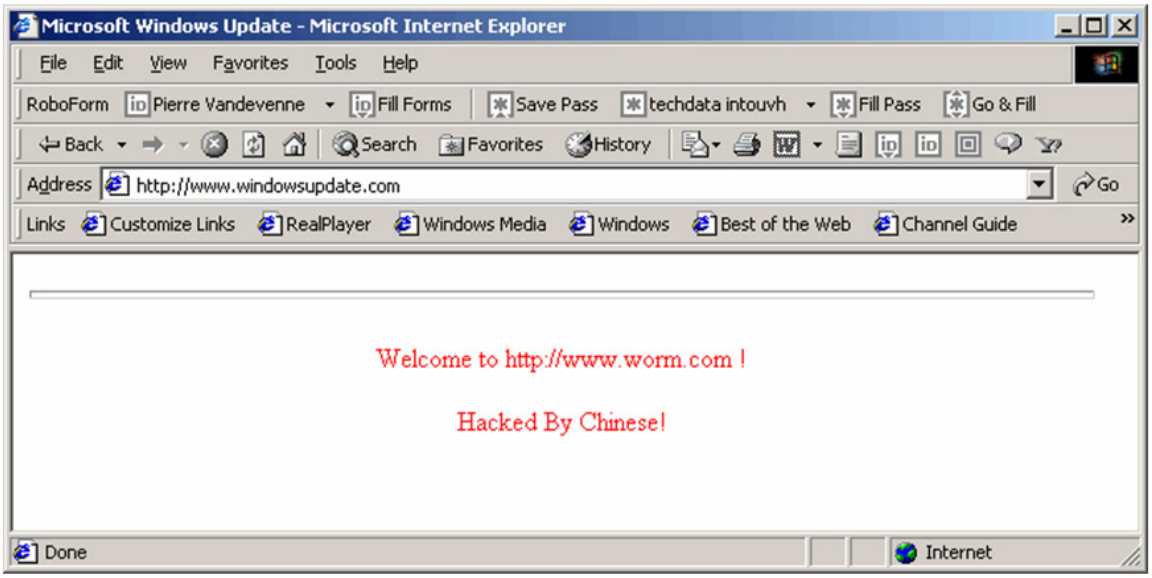

Figura 2 - Irónicamente, el sitio de Windows Update fue uno de los muchos afectados por Code Red 11

Code Red había causado daños valoradosen más de 2 mil millones de dólares y lo declaró "el más caro en la historia de Internet". 10
Este coste correspondía principalmente a las horas dedicadas a parchear e inocularde limpiar los daños, el mundo debería haber soltado una expresión colectiva de alivio ante el hecho de que los daños fuesen relativamente menores.

Hoy en día, la mayor parte de protagonistas de la era del 'Big Bang' de los gusanos ha desaparecido. Mientras que las empresas y fabricantes de software pueden reclamar una cierta cantidad de crédito por mejorar el pobre nivel de seguridad que

El objetivo hoy día es permanecer bajo el radar, explotar las vulnerabilidades técnicas o sociales durante el mayor tiempo posible y hacer la mayor cantidad de dinero posible. En muchos aspectos, los gusanos como Code Red eran un lujo: sabíamos en qué momentos comenzaban y terminaban los daños, y cuando finalmente se posaba el polvo, era evidente donde limpiar. Hoy en día los ataques son mucho más difíciles de identificar. Esto es especialmente cierto cuando los ataques se centran en un usuario final concreto, máquinas sin protección o con controles mínimos para detectar los ataques.

10 http://www.newsfactor.com/perl/story/12668.html
11 http://www.theregister.co.uk/2001/07/20/code_red_bug_hits_microsoft

VECTORES DE ATAQUE

Al igual que el objetivo de los atacantes ha pasado de los servidores de Internet a los equipos de sobremesa, portátiles y dispositivos móviles, también su estrategia ha cambiado.

Ingeniería social

Como se ha dicho muchas veces, la seguridad es tan fuerte como el más débil de los eslabones de la cadena que la compone. Generalmente, el eslabón más débil es el elemento humano. La ingeniería social, en este contexto, implica intentar obtener información confidencial de los usuarios intentado que hagan cosas que sus políticas de seguridad deberían impedirles hacer. Es la combinación perfecta: Un cebo cuidadosamente seleccionado que emplee la ingeniería social puede convencer a los usuarios de que entreguen sus datos o instalen un programa malicioso que capture información y se la envíe a los hackers. Los 10 exploits más importantes del año 2007 tuvieron como objetivo sitios Web y servicios con un gran volumen de tráfico para llevar a cabo ataques de ingeniería social.

El único obstáculo que un atacante debe superar para que triunfe un ataque de este tipo es convencer al usuario de que acceda a un recurso Web. Históricamente esto se realizaba mediante correos de spam que inundaban los buzones de entrada de los usuarios con URLs, esperando que un cierto número de ellos hiciesen clic en las mismas. Sin embargo, los atacantes están refinando estas tácticas. Se han dado cuenta de que pueden evitar la necesidad de generar tráfico de usuarios incorporando un sitio Web popular al ataque. Están empleando técnicas de ataque consistentes en infectar sitios Web populares con contenido malicioso, añadir contenido proporcionado por usuarios maliciosos a sitios Web 2.0, o incluso comprar espacio publicitario. En muchos casos el objetivo no es el propio sitio; el sitio es simplemente el mecanismo de propagación del ataque, que tiene como objetivo al usuario final.

En muchos casos estos ataques no implican una explotación de tipo técnico. Simplemente se trata de convencer al usuario de que ejecute código malicioso para que el ataque tenga éxito. Se podría pensar que a medida que las tecnologías de seguridad evolucionan y las empresas invierten en educar a los usuarios finales sobre las amenazas de seguridad, el éxito de este tipo de ataque disminuiría con el tiempo. Sin embargo y tristemente, los ataques de ingeniería social siguen teniendo mucho éxito y son relativamente fáciles de realizar por los atacantes, sobre todo si se tiene en cuenta el paradigma de la Web 2.0: “

No construyas un site para tus usuarios, deja que los usuarios construyan un site para ellos mismos”. Los usuarios finales se han convertido en desarrolladores Web, y si no se establecen unas restricciones granulares al contenido que pueden añadir, esta misma filosofía, que ha llevado a la explosión del contenido creado por el propio usuario, puede ser utilizada también como un vector de ataque muy eficaz.

Vulnerabilidades del navegador Web

En julio de 2006, el afamado investigador de seguridad HD Moore lanzó un controvertido proyecto conocido como el Mes de los Fallos de los Navegadores.[13] Cada día, a lo largo del mes, Moore revelaba detalles de una nueva vulnerabilidad en un navegador Web. Moore no tenía como objetivo ninguna empresa en particular; de hecho, publicó información sobre vulnerabilidades en Internet Explorer, Mozilla, Safari, Opera y Konqueror. Aunque sus métodos pudieran ser cuestionables, resulta difícil no estar de acuerdo en que alcanzó su objetivo de llamar la atención sobre el pobre estado de la seguridad de los navegadores de Internet.

Los navegadores Web se han convertido en una especie de navaja suiza virtual, ofreciendo funcionalidades que van mucho más allá de simplemente visualizar páginas Web. Pueden asimilar fuentes de noticias, llamar a otras aplicaciones, manejar tecnologías propietarias, etc. De hecho, con plug-ins de terceros, la capacidad de los navegadores Web es prácticamente ilimitada. A medida que ha aumentado la funcionalidad de los navegadores, también lo ha hecho la complejidad de las aplicaciones y ha surgido una cantidad ingente de vulnerabilidades, muchas de las cuales son de naturaleza crítica y pueden llegar a comprometer por completo la seguridad de la máquina host. Incluso las vulnerabilidades que no tienen como resultado la ejecución de código pueden tener implicaciones graves. Normalmente los phishers explotan agujeros en los navegadores para mejorar la efectividad de sus ataques. Aunque los navegadores disponen de controles integrados que muestran a los usuarios los recursos a los que están accediendo – la barra de direcciones, barra de estado, certificados SSL, etc.- dichos controles dejan de ser de confianza en el momento en el que las vulnerabilidades permiten manipular dicha información. Los phishers son muy conscientes de esto.

Vulnerabilidades de ActiveX

ActiveX es una tecnología propietaria de Microsoft que permite crear componentes reutilizables de software. Los controles ActiveX pueden ser marcados como 'safe for scripting', lo que permite llamarles desde el navegador Web Internet Explorer (IE). Esta técnica, aunque no ofrece compatibilidad multiplataforma debido a la naturaleza propietaria de la tecnología, es una forma habitual de ampliar la funcionalidad de IE. Sin embargo, en caso de que dichos controles fuesen vulnerables, esto proporcionaría a los atacantes un vector excepcional para acceder a la máquina local. Se han descubierto un gran número de desbordamientos de buffer en los controles ActiveX, que permiten que un atacante ejecute código arbitrario en una máquina local simplemente convenciendo a la víctima de que navegue hasta una página Web que contenga el código malicioso.

Un típico equipo con Windows tiene cientos, si no miles, de controles ActiveX instalados. Dichos controles pueden haber sido generados por desarrolladores de terceros sin prácticas seguras de testeo. Los investigadores se centran en estas debilidades y desarrollan herramientas que automatizan el proceso de descubrimiento de vulnerabilidades en los controles ActiveX. Estas herramientas están diseñadas par

mutar los datos estándar de entrada de las aplicaciones y monitorizar la aplicación de destino para determinar si consigue procesar los datos mutados o fracasa y queda en un estado vulnerable. La aparición de herramientas fáciles de utilizar como COMRaider [14] y AxMan [15], ha llevado al descubrimiento de un gran número de vulnerabilidades de ActiveX, muchas de las cuales son accesibles para atacantes remotos vía IE.

Vulnerabilidades de formato de archivo

Los formatos de los archivos, como los protocolos de red, son reglas predefinidas para la comunicación. Estas reglas definen la estructura de los datos a enviar entre los ordenadores y siempre que tanto el emisor como el receptor se adhieran a la estructura definida, se podrá crear archivos en una máquina y leerlos en otra. Sin embargo, ¿qué pasa cuando el emisor se aleja de dicho formato? ¿Qué sucede si se cambian bits aquí y allí? ¿Puede la máquina receptora interpretar el archivo? ¿Descartará el archivo, o dará lugar a una vulnerabilidad en sus esfuerzos por leerlo?

Las vulnerabilidades de formato de archivo son una clase única de vulnerabilidad ya que los archivos no son código ejecutable y normalmente no se les considera una amenaza. Sin embargo, se ha descubierto que los archivos mal formados pueden dar lugar a vulnerabilidades en las aplicaciones empleadas para interpretarlos. Esto supone un importante desafío para aquellos que tienen la tarea de proteger las redes. Mientras que las aplicaciones antivirus contienen normalmente identificadores para detectar formatos conocidos de archivos malformados, se han producido numerosas situaciones en las que se han explotado vulnerabilidades de día 0, o vulnerabilidades desconocidas de formato de archivo, para llevar a cavo ataques dirigidos.

En estos ataques, el atacante envía un archivo malicioso a la víctima bien como adjunto a un mensaje de correo electrónico o publicándolo en un sitio web. En el momento en que la aplicación vulnerable que debe interpretarlo abre dicho archivo, normalmente al hacer doble clic sobre el mismo, se explota el fallo de seguridad. Bloquear todos los tipos de archivos que resultan potencialmente vulnerables no es una solución realista contra este tipo de ataque ya que se ha descubierto este tipo de vulnerabilidad en todos los tipos de archivos más utilizados, incluyendo formatos de audio, vídeo y documentos. Estos ataques han supuesto un importante desafío para Microsoft ya que se han descubierto vulnerabilidades en formatos de archivos utilizados por las aplicaciones de Microsoft Office. Dada la popularidad de aplicaciones como Word, Excel, y PowerPoint en los entornos corporativos, este tipo de archivos supone uno de los vectores de ataque más útiles sobre los individuos de una empresa.

Ataques Web 2.0

El término Web 2.0 no describe una tecnología en concreto; se refiere a la evolución en el desarrollo de recursos Web por motivos técnicos y sociales. Una nueva variedad de tecnologías como AJAX y Rich Internet Applications (p. ej. Adobe Flash y Microsoft SilverLight) está haciendo que las aplicaciones Web sean mucho más interactivas y amigables. Poco a poco, esta transición está borrando las líneas que separan las funcionalidades de las aplicaciones Web y de las aplicaciones tradicionales de sobremesa.

Aunque las tecnologías Web 2.0 no han generado nuevos tipos de ataques, estamos viendo una aparición de vulnerabilidades típicas de las aplicaciones Web tradicionales en aplicaciones Web 2.0. Esto sucede por los siguientes motivos:

A menudo no aprendemos de nuestros propios errores. En muchas ocasiones las empresas se precipitan en adoptar nuevas tecnologías sin tener en cuenta las consecuencias que esto puede tener desde el punto de vista de la seguridad. Aunque las aplicaciones Web 2.0 pueden y deben ser seguras, son nuevas para un gran número de desarrolladores que deben aprender rápidamente a desarrollar proyectos con las mismas sin detenerse en su seguridad. Además, estas tecnologías son nuevas para los propios profesionales de la seguridad, cuyos conocimientos y herramientas pueden no ser suficientes aún para la tarea de descubrir vulnerabilidades tradicionales en un nuevo entorno.

Otro aspecto a tener en cuenta con los sitios Web 2.0 es que suponen un cambio con respecto a la dinámica tradicional de dónde transcurren los procesos. En una aplicación Web tradicional, todos los procesos tienen lugar en la nube (aplicación y servidores de bases de datos), mientras que los resultados se muestran en el navegador Web.

Las tecnologías RIA y AJAX producen aplicaciones con mayor capacidad de respuesta principalmente porque liberan al navegador de las tareas de procesamiento. Al hacerlo, la lógica de la aplicación, que antes no quedaba expuesta al usuario final, queda ahora disponible a aquellos que quieran investigar el código de la parte cliente. Esto en sí no tiene por que ser un problema, siempre que los desarrolladores conozcan las consecuencias de dicha estructura. Mientras que en el pasado los desarrolladores no tenían que preocuparse por el hecho de exponer datos o una lógica sensible ya que nunca salía del servidor, ahora ya no disponen de ese lujo. La seguridad que procedía de mantener datos en la oscuridad ya no es posible.

TENDENCIAS

Sofisticación de los ataques

La batalla entre los atacantes y los que nos defienden de ellos es una lucha sin fin. A medida que las empresas de seguridad desarrollan tecnologías innovadoras para identificar y evitar los ataques, aquellos que los llevan a cabo buscan métodos igualmente innovadores de evadirlas. Muchos de los ataques Web que más éxito han tenido hasta el día de hoy han sido relativamente poco sofisticados, aprovechándose de técnicas de ingeniería social. De hecho, ciertamente da miedo pensar en la gran cantidad de ataques que han tenido éxito sin necesidad de utilizar técnicas sofisticadas. Sin embargo, a medida que mejoran las defensas y los usuarios finales están cada vez más informados sobre temas de seguridad, los atacantes se están dando cuenta de que deben subir el nivel de sofisticación.

En los últimos años hemos visto la aparición de una serie de tendencias relacionadas con las ofisticación de los ataques. Los atacantes cada vez utilizan más las vulnerabilidades de día 0. Dichos ataques se basan en vulnerabilidades que han sido descubiertas recientemente a veces por los propios atacantes o bien adquiridas en mercados ilegales. De cualquiera de las formas, las defensas basadas en identificadores resultan inútiles ante dichos ataques, ya que sólo es posible generar identificadores en respuesta a un vector de ataque conocido.

Las redes de bots también se han convertido en una de las armas favoritas de los hackers. Las redes de bots están formadas por cientos de miles de hosts infectados conocidos como 'zombies', que reciben instrucciones de servidores de control. Las redes de bots se han convertido en una amenaza muy poderosa debido a su resistencia y flexibilidad. Son extremadamente difíciles de neutralizar en su totalidad debido a su naturaleza descentralizada y pueden ser utilizadas para prácticamente todo tipo de ataque. En el momento en que un equipo comprometido se convierte en un 'zombie', los atacantes dejan de estar interesados en su contenido. En su lugar, se interesan por sus ciclos de CPU, ciclos que utilizan como les viene en gana para enviar spam, llevar a cabo ataques de denegación de servicio, fraudes de tipo click-thru o cualquier otra acción maliciosa que el 'pastor de bots' desee realizar.

Aspecto económico

Atacar y controlar recursos informáticos se ha convertido en una actividad creciente y económicamente rentable y que, al igual que cualquier otro negocio, da cabida a un gran número de individuos, cada uno de ellos esperando obtener su parte del pastel. Por ello, se ha producido una evolución de las economías estructuradas 'underground' que cobijan a este tipo de sujetos. En la actualidad, existe una cantidad relativamente pequeña de personas en este mundillo clandestino que dispongan de los conocimientos necesarios para descubrir vulnerabilidades que puedan ser explotadas. Tales conocimientos no son necesarios siempre y cuando se esté dispuesto a pagar por ellos. El 5 de enero de 2006 Microsoft publicó de forma precipitada un parche fuera de su ciclo habitual de publicación de parches de seguridad. [16] ¿La razón? En los días anteriores a dicha publicación, se había descubierto que una vulnerabilidad muy extendida de formato de archivo en las aplicaciones de Microsoft que mostraban imágenes WMF no sólo se estaba explotando de forma activa, sino que el código que permitía explotarla se estaba vendiendo en el mercado negro por 4.000 [17] dólares aproximadamente. Este hecho fue una señal clara del crecimiento de tales mercados.

Hoy día, disponer del dinero y de las conexiones adecuadas puede dar acceso a códigos maliciosos, números de tarjeta de crédito, o herramientas para la realización de ataques. Sin embargo, la preocupación más importante es el aumento y popularidad del uso de las redes de bots. Más que adquirir los productos necesarios para llevar a cabo sus propios ataques, los criminales está recurriendo a los pastores de redes de bots para acceder a ciertos servicios (infraestructuras potentes y establecidas de redes de bots empleadas para realizar una gran variedad de ataques). Los pastores de las redes de bots se dedican a alquilar los ciclos de CPU creados por ellos mismos, a precios reducidos que van desde los $10/hora. [18]

Web 2.0

Además de los cambios técnicos, las influencias sociales también están contribuyendo a la llamada revolución Web 2.0. Mientras que la Web 1.0 se centraba en la transferencia de negocios tradicionales a Internet, la Web 2.0 está generando modelos de negocio completamente nuevos. Los sitios Web 2.0 se centran en conectar a los usuarios entre sí (p.ej. Facebook y MySpace) y promover el contenido creado por los propios usuarios (p.ej. YouTube y Flickr). Desde el punto de vista de la seguridad, esta transición ha aumentando en gran medida la complejidad de las aplicaciones Web y ha incrementado la superficie total de ataque, ya que los usuarios han pasado de ser meros observadores a participantes en el proceso de construcción de los sitios Web.

Los sitios Web 2.0 se basan en la misma estructura subyacente de las páginas Web anteriores, aunque añaden capas de complejidad y llevan gran parte de la lógica de las aplicaciones al navegador Web. Como resultado, las vulnerabilidades de las aplicaciones Web tradicionales son más difíciles de identificar. Dada la naturaleza interconectada de la Red, los servidores Web vulnerables sirven a menudo para atacar a los usuarios que visitan dichos sitios. Tomemos el ejemplo de los ataques de Cross Site Scripting, una de las vulnerabilidades más

presentes en los sitios Web actuales. Si los sitios son capaces de aceptar datos introducidos por los usuarios pero no desinfectan adecuadamente dichos contenidos, los hackers pueden utilizar lenguajes como JavaScript para ejecutar código en el navegador Web de las víctimas. Una vez un atacante consigue forzar la ejecución de código de script, puede controlar el navegador de la víctima. Esto puede llevar al robo de información confidencial, la realización de acciones no deseadas o incluso al uso del navegador de la víctima como herramienta para lanzar ataques contra otros sistemas de la red interna.

Movilidad

Mientras que las advertencias de ataques a teléfonos móviles no han pasado nunca de ser sólo eso, advertencias, la verdad es que la situación está cambiando. Los teléfonos móviles nunca han sido objetivos atractivos debido a la gran cantidad de sistemas operativos que existen y a su limitada funcionalidad. Así como un atacante podía invertir dinero en desarrollar un código malicioso para una máquina de Windows y tener al instante un objetivo consistente en millones de ordenadores con conexiones continúas a Internet, la situación era bien distinta en el caso de los móviles.

A medida que la industria se ha concentrado en un puñado de plataformas (Symbian, RIM, Windows Mobile y OS X iPhone), la perspectiva de desarrollar códigos para las mismas empieza a ser más atractiva. Por otro lado, las aplicaciones para móviles han dejado de ser versiones 'lite' y simplificadas con funcionalidades mínimas. Mobile Safari, por ejemplo, el navegador integrado por defecto en el iPhone, es un completo navegador AJAX capaz de procesar las mismas páginas Web que los equipos de sobremesa. Es más, comparte parte del código utilizado por sus hermanos mayores. Por lo tanto, desde el punto de vista de un atacante, el mismo exploit que utiliza una vulnerabilidad de AJAX en un sitio Web para infectar el navegador Safari, puede convertirse en un código malicioso multi-plataforma que ataque también a los usuarios de móviles. Esta tendencia sólo será mayoritaria cuando las plataformas móviles sean más sofisticadas y comiencen a almacenar más y más datos. Los teléfonos móviles ya no son sólo teléfonos móviles – son pequeños portátiles.

DESAFÍOS

El tráfico Web se ha convertido en el principal medio de acceder a los recursos de Internet debido al hecho de que prácticamente todas las redes corporativas permiten el tráfico de salida por los puertos TCP 80 (HTTP) y 443 (HTTPS). Aplicaciones que en el pasado se beneficiaban de otros protocolos emplean en la actualidad el protocolo HTTP(S) exclusivamente o al menos tienen la capacidad de cambiar a HTTP(S) en caso de que las rutas alternativas estén bloqueadas por los firewalls de la empresa. A medida que el tráfico Web ha ganado en importancia en la red corporativa, también lo ha hecho la necesidad de protegerlo. En redes grandes y distribuidas, la monitorización y protección de dicho tráfico entraña muchos desafíos.

empresas. Dada la naturaleza propietaria de tales tecnologías y la falta de soluciones de alta gama de un único fabricante, las empresas se ven obligadas a administrar cada vez más aplicaciones de software y appliances de hardware para asegurar la seguridad Web de su red. Tal y como se ve en la figura 3, una única solicitud o respuesta Web debe atravesar media docena de soluciones de seguridad independientes antes de entrar o salir de la red de la empresa. A esto se une el hecho de que las empresas disponen de múltiples pasarelas de Internet. Por otro lado, dichas pasarelas pueden estar bajo un control descentralizado o haber sido añadidas a la infraestructura general mediante adquisiciones, por lo que no es sorprendente que se den situaciones en las que una empresa trabaje con múltiples

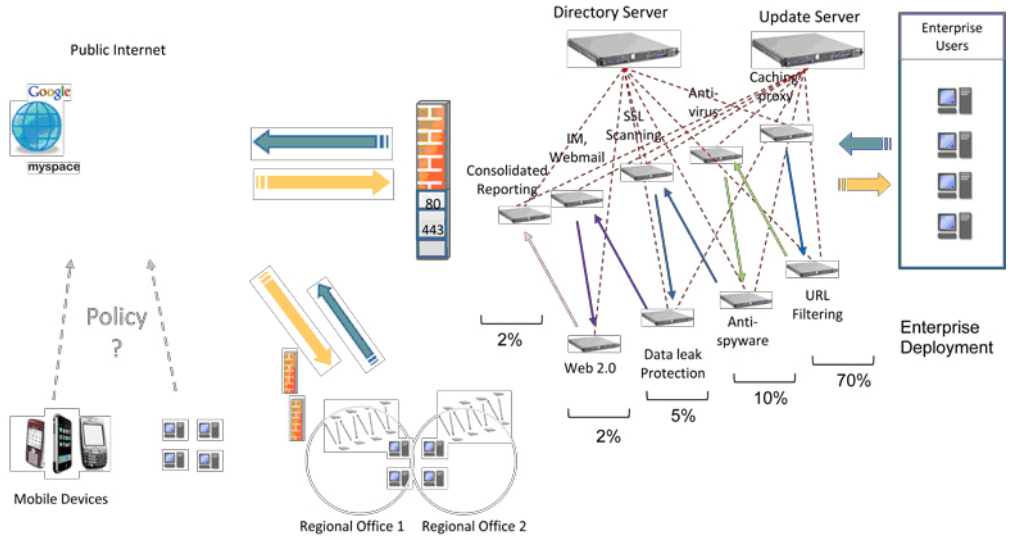

Figura 3 – Infraestructura típica de la seguridad Web

Protección uniforme

La seguridad Web sigue siendo una industria en permanente evolución, y como tal, hay un gran número de soluciones 'standalone' en el mercado desarrolladas por una gran cantidad de

tecnologías de seguridad Web de varias empresas, desplegadas en varias ubicaciones. En tales circunstancias es difícil, pero no imposible, ofrecer protección uniforme en todas las ubicaciones.

Informes unificados

Junto al desafío de administrar tecnologías descentralizadas en distintas ubicaciones, se añade la complicación de no disponer de informes unificados. Resulta muy complicado gestionar riesgos cuando no se dispone de una visión completa del entorno. Aunque un gran número de empresas de Gestión de Información de Seguridad (SIM) han dado el paso de unificar los informes de sus aplicaciones de seguridad individuales, con cada empresa empleando sus propios estándares de generación de informes, sólo son capaces de unificar aquellos datos que sean consistentes entre las distintas empresas.

Los enormes archivos de log que el tráfico Web puede generar aumentan la dificultad de generar enormes unificados. Un usuario individual puede registrar fácilmente decenas de miles de transacciones Web en un solo día. Así que, en el caso de las grandes empresas, incluso los archivos de log diarios se vuelven inmanejables. Además, hay que combinar dichos informes en un sistema centralizado de información, punto en el cual incluso la prospección básica de datos se vuelve una imposibilidad. ¿De qué sirve una función de generación de informes que tarde 10 horas en ejecutar las consultas a bases de datos relacionales necesarias para un único informe?

Aplicación consistente de las políticas

Los informes recogen los resultados del sistema de seguridad. Los datos de entrada de dicho sistema son las políticas, que definen la postura de la empresa en cuanto a la seguridad. Al igual que ocurre con los informes, cuando se trabaja con una variedad de soluciones de múltiples empresas en ubicaciones dispersas, puede que no sea posible aplicar las políticas de un modo consistente.

Si las distintas delegaciones de una empresa emplean soluciones de distintos proveedores, al final la empresa se verá obligada a aplicar una 'política de compromiso' debido a las distintas funcionalidades. La presencia de funciones de seguridad descentralizas también complica las cosas y hace que al final cada oficina aplique las políticas que considera oportunas. Incluso en el caso de los departamentos de seguridad que puedan disfrutar del lujo de tener un control centralizado sobre las políticas, así como de appliances de seguridad consistentes en toda la empresa, puede resultar muy complicado asegurar que todos los cambios se aplican de forma consistente en todas las ubicaciones.

Fuga de datos

Gracias en parte al poder cada vez mayor de iniciativas de carácter normativo como HIPPA o GLBA, la detección y neutralización de las pérdidas de datos se está convirtiendo en una de las prioridades principales de los Responsables de Seguridad de las empresas. Aparte del cumplimiento normativo, el problema se complica aún más por la facilidad con las que se puede transferir información sensible más allá de las fronteras de la red interna de la empresa. Ya sea de forma intencionada o no, resulta muy sencillo transferir datos mediante la Web, el correo electrónico, la mensajería instantánea o los clientes P2P. Las empresas necesitan soluciones unificadas que puedan asegurar el cumplimiento y aplicación de políticas de Protección de las Fugas de Datos (DLP) en todas las tecnologías y pasarelas de Internet de la empresa.

Amenaza[1]s desconocidas

A menudo se dice que no se puede evitar aquello que no se conoce. Esto no es del todo cierto, aunque siempre que los atacantes dispongan de la ventaja de tener conocimiento propietario sobre un ataque, las reglas del juego cambian. Muchas de las tecnologías de seguridad actuales se basan solamente en identificadores – en cuyo caso es necesario conocer un ataque para generar un identificador que lo detecte. Hoy día se descubren y negocia con vulnerabilidades de día 0 en el mercado negro mucho antes de que se creen y distribuyan los identificadores y parches correspondientes. Las medidas de seguridad deben ir más allá de los identificadores para analizar los comportamientos de las redes y poder diferenciar entre tráfico 'bueno' y 'malo'. En un mundo en el que surgen amenazas mixtas todos los días, las soluciones basadas en identificadores proporcionan una protección limitada.

También es posible combatir las amenazas desconocidas mediante el 'principio de privilegio mínimo o más restrictivo': una antigua regla del mundo de la seguridad que a menudo se ignora para apaciguar a los usuarios finales. ¿Es razonable que un usuario final solicite acceso a su cliente favorito de mensajería instantánea (MI)? Probablemente no. Puede que dicha petición tenga un propósito profesional totalmente legítimo e incluso aunque no fuese así, no hay que desdeñar el hecho de mantener felices a los empleados. Sin embargo, ¿puede aumentar un elemento adicional de software el peligro al que se expone la empresa? Por supuesto.

Cada elemento tecnológico adicional que se añade a una red aumenta la probabilidad de heredar código vulnerable. Resulta necesario alcanzar un equilibrio. Un modo de alcanzar dicho compromiso consiste en permitir acceso a aplicaciones adicionales, pero controlando su funcionalidad. Por ejemplo, sería posible desplegar ese mismo cliente de mensajería instantánea pero de forma controlada. Las empresas necesitan soluciones que, por ejemplo, permitan conversaciones de texto mediante mensajería instantánea pero restrinjan la descarga de archivos. De esta forma se protegería contra los ataques de ingeniería social que intentan convencer a los usuarios de que descarguen y ejecuten archivos. El control granular de las aplicaciones Web y aplicaciones de sobremesa ofrece opciones que van más allá del simple permitir / denegar.

Coste

A medida que Internet se vuelve más compleja y surgen nuevos vectores de ataque, también aparecen nuevos costes asociados con la implementación de un sistema robusto de seguridad. Hace tiempo que pasaron los días en los que un firewall y algún software antivirus de sobremesa eran protección suficiente. Hoy día, las empresas adquieren appliances para el análisis antivirus online, la protección contra fugas, el filtrado de URLS, la inspección SSL, la generación de informes, etc. Cada nuevo appliance requiere de una inversión adicional de capital que hay que duplicar en cada pasarela de Internet, y este coste no contempla las horas necesarias para desplegar y mantener la solución. Las empresas buscan convertir los gastos fijos y a menudo inesperados en costes variables y predecibles.

SOLUCIONES

La protección y control del tráfico Web generado por los usuarios ha dejado de ser una opción para las empresas, es una necesidad. La cuestión, por tanto, es saber cómo afrontar este desafío de forma que proporcione el mayor control de la forma más económica.

Defensas basadas en el cliente

Este término se refiere a soluciones de software que residen directamente en la máquina cliente, de diversas maneras. Por ejemplo, es poco probable encontrar hoy día un equipo de sobremesa en una empresa que no disponga de un motor antivirus instalado. Además de esto, cada vez son más populares los sistemas anti-spyware e incluso los firewalls y sistema de detección de intrusiones en el host (HIPS), con ciertas funcionalidades embebidas directamente en el sistema operativo sin que sean necesarias soluciones de terceros. Sin embargo, la mayor parte de estas protecciones están diseñadas para proteger a las propias máquinas de ataques externos directos. No están diseñadas para detectar o evitar ataques Web provocados por las acciones de los propios usuarios. Tomemos, por ejemplo, un ataque de cross-site scripting (XSS) que envíe las credenciales de autenticación del usuario a un servidor controlado por un atacante cuando la víctima acceda a un sitio Web vulnerable. En un caso como éste, la vulnerabilidad existe en el servidor Web, no en la máquina cliente. Sin embargo, es el usuario el que se ve afectado. En un caso así, ninguna de las tecnologías de seguridad del lado del cliente que hemos mencionado anteriormente hubiera sido capaz de evitar el ataque.

Las dos desventajas inmediatas que presenta cualquier protección instalada en el lado del cliente son la instalación y mantenimiento de la solución y la falta de control sobre su uso. En las grandes empresas, la instalación manual de las aplicaciones cliente resulta inviable debido al esfuerzo y coste que conlleva. Esto es particularmente evidente en el caso de los empleados remotos que nunca se desplazan físicamente a la empresa. Además esta el caso de los usuarios que quieren evitar la acción de las soluciones del lado del cliente, no por razones maliciosas, sino para escapar de la acción de un motor antivirus demasiado agresivo que les impide realizar su trabajo.

Pasarelas de seguridad Web

El mercado actual de las pasarelas de seguridad Web (WSG) consiste principalmente en fabricantes de appliances que construyen soluciones basadas en proxies de alto rendimiento diseñadas para inspeccionar el tráfico de entrada y salida. Los appliances WSG residen en una o más pasarelas de Internet a lo largo de la empresa y presentan una clara ventaja sobre las defensas basadas en el cliente: los usuarios finales no pueden desactivarlas. Aunque siempre se las ha considerado como una protección complementaria más que una alternativa a las defensas en el cliente como los motores AV de sobremesa en los HIPS, las WSGs ofrecen a las empresas más control sobre el tráfico Web y mejoran por tanto la seguridad de la red ante la cada vez mayor cantidad de amenazas de Internet.

Las WSGs no están sin embargo libres de desventajas. Se trata de un appliance adicional que desplegar y administrar. Es necesario desplegar una appliance individual en cada una de las pasarelas de Internet, lo que no sólo aumenta los gastos globales sino que, en el caso de las grandes empresas, puede llevar a una falta de informes unificados. Incluso aunque resultara posible la unificación de los informes, el volumen ingente de entradas de logs haría imposible la prospección de datos.

Seguridad en la nube

Los desarrollos basados en la nube o las soluciones SaaS para la seguridad de los navegadores Web ofrecen algunas ventajas únicas. Los sectores de CRM (p.ej. Salesforce) y ERP (p.ej. NetSuite) han comenzado a evolucionar hacia modelos de computación en la nube para beneficiarse de ventajas tales como la facilidad de uso y un menor coste total de propiedad. Las soluciones SaaS se están beneficiando de estas mismas ventajas para la seguridad Web en el lado del cliente.

Protección uniforme

Los appliances especificados en la Figura 3 son ofrecidos por una gran cantidad de empresas de seguridad. No existe un único fabricante que sea líder en todas las áreas del mercado WSG. Por tanto, las empresas se enfrentan a una difícil elección: optar por un proveedor único y aceptar soluciones con funcionalidades de segundo nivel, o elegir la mejor solución en cada categoría y lidiar con las posibles incompatibilidades entre las soluciones. Al final, las empresas se ven forzadas a elegir

entre el menor de dos males. Sin embargo, en la actualidad están surgiendo soluciones SaaS que ofrecen más funcionalidades en todas las áreas indicadas en la Figura 3, y gestionadas desde un único interfaz Web.

Informes unificados

Gracias a que todo el tráfico pasa por la misma infraestructura gestionada, el proveedor de la solución SaaS puede resolver el problema de la unificación de logs. Desde el punto de vista del usuario final, es posible visualizar los logs de todas las pasarelas y usuarios móviles de la empresa y realizar tareas de prospección de datos desde el frontal de una aplicación Web.

Aplicación consistente de las políticas

Las soluciones SaaS no sufren los problemas derivados de desplegar políticas a una multitud de dispositivos responsables de su cumplimiento. Todo el tráfico Web de la empresa es redireccionado a través de pasarelas geográficamente dispersas que aplican las políticas consolidadas definidas por la empresa. De este modo, se aplica una protección uniforme a todo el tráfico Web independientemente de su origen. Todos los cambios que se realizan sobre las políticas de seguridad se realizan en una única ubicación, a través de una interfaz Web. Por tanto, no se requiere de un software propietario para administrar el sistema.

Fuga de datos

Las fugas de datos plantean riesgos en cuanto a la confidencialidad y cumplimiento normativo. Aunque las soluciones DLP basadas en appliances ofrecen un nivel de protección razonable contra dichos riesgos, presentan problemas a la hora de aplicar una política uniforme en todas las pasarelas, y en cuanto a la unificación de informes. Estos desafíos son particularmente exigentes en el área de la fuga de datos, donde la falta de cumplimiento normativo puede tener importantes consecuencias. Las soluciones basadas en SaaS, en las que toda la información fluye a través de una infraestructura centralizada, resuelven estas cuestiones.

Coste

Al trasladar la tecnología desde la red interna de la empresa a la nube, una parte importante del gasto de capital se convierte en un gasto variable por usuario. Por lo tanto, además de pasar de unos costes fijos a unos variables, las soluciones basadas en la nube ofrecen un coste total de propiedad menor, debido en gran parte a la eliminación de las tareas de despliegue y mantenimiento de los appliances adquiridos.

CONCLUSIÓN

A medida que los atacantes cambian sus objetivos, también lo hacen aquellos cuya tarea consiste en defender los activos de la red. La red de la empresa ya no se concibe como una fortaleza solitaria e impenetrable. Ha evolucionado hasta convertirse en una infraestructura distribuida no sólo en términos de oficinas remotas, sino también con la existencia de un mayor número de empleados móviles poseedores de valiosos activos digitales. La meta ya no es únicamente mantener alejados a los 'malos'. Las empresas necesitan administrar el acceso Web de los usuarios finales a fin de evitar que los atacantes puedan reclutar a sus empleados sin que se de cuenta para que les hagan el trabajo sucio. Todo esto, sin imponer controles demasiado restrictivos sobre empleados cada vez más autosuficientes, y buscando mantener un equilibrio entre una plantilla segura y a la vez productiva.

Como todo el tráfico Web pasa por los puertos 80 (HTTP) y 443 (HTTPS), las empresas no pueden permitirse el lujo de dejar desprotegidas estas puertas de entrada. El desafío al que se enfrentan consiste en identificar soluciones económicas que den respuesta a la multitud de amenazas que rodean al tráfico Web de los usuarios. Aunque las defensas basadas en el cliente como los antivirus y anti-spyware de sobremesa y los sistemas HIPS seguirán siendo controles importantes para la seguridad de las empresas, nunca serán soluciones adecuadas para ofrecer una protección completa. Está claro que las empresas deben ser capaces también de administrar todo su tráfico Web. Esto no sólo incluye el tráfico que entra y sale de la LAN de la empresa, sino también el tráfico hacia y de portátiles y usuarios móviles, así como cualquier dispositivo móvil que tenga acceso a los activos de la compañía.

Aunque la industria de las pasarelas de seguridad de Internet (WSG) ha surgido para dar respuesta a este desafío, las soluciones basadas en appliances seguirán enfrentándose a las limitaciones impuestas por unos empleados cada vez más distribuidos. Lograr una protección uniforme, con informes unificados y que permita la aplicación de políticas de forma consistente puede ser complicado cuando se gestionan múltiples pasarelas. Además de esto, resulta imposible proteger a los usuarios remotos que acceden a Internet de forma directa, sin utilizar la VPN de la empresa. A medida que las comunicaciones corporativas siguen avanzando hacia las soluciones Web, la importancia de administrar el tráfico de Internet ya no sólo afecta al campo de la seguridad sino también a la protección contra las fugas de datos y al control del ancho de banda. La gestión de este tráfico se ha convertido en una tarea difícil y costosa. Aunque las soluciones basadas en appliances han abierto el camino en el mercado de las WSGs, las empresas se están dando cuenta de las ventajas que supone pasarse a una proveedor que ofrezca una solución única con protección y control uniforme de todo el tráfico Web independientemente de la ubicación o el dispositivo. Así como las soluciones en la nube y SaaS se están convirtiendo en líderes del mercado en otras industrias, está claro que las ventajas de este modelo se están haciendo evidentes también en el mercado WSG.

SUITE PANDA CLOUD PROTECTION

Panda Cloud Internet Protection es parte de la suite Panda Cloud Protection, una completa solución de seguridad SaaS que protege los principales puntos de entrada de amenazas -endpoints, correo electrónico y tráfico Web- contra el malware, spam, cross-site scripting y otros ataques avanzados Web 2.0, mediante una solución ligera, segura y sencilla.

Esta suite de seguridad está basada en la nube, ofreciendo máxima protección, reduciendo el gasto y aumentando la productividad. La solución se despliega en cuestión de minutos y se gestiona de forma sencilla gracias a la intuitiva Consola de Administración en la Nube única de Panda.

La suite Panda Cloud Protection se beneficia de la gran capacidad de la Inteligencia Colectiva: un sistema basado en la nube que almacena 21 terabytes de conocimiento y experiencia obtenido directamente de millones de usuarios. Panda Cloud Protection ofrece protección completa para el mundo real, no intrusiva e instantánea contra el malware conocido y desconocido.

Panda Cloud Protection se beneficia del poder de la nube para proporcionar protección en tiempo real contra las amenazas conocidas y desconocidas en cualquier momento y en cualquier lugar, gracias al poder de la Consola de Administración en la Nube.