



Acerca del Informe de Amenazas de Seguridad en Internet de Symantec

El *Informe de Amenazas de Seguridad de Internet de Symantec*, proporciona una actualización de seis meses de la actividad de amenazas de Internet, la cual incluye un análisis de ataques basados en las redes, un repaso de las vulnerabilidades conocidas y destaca los códigos maliciosos de mayor importancia y los riesgos de seguridad adicionales. Este resumen del *Informe de Amenazas de Seguridad en Internet*, puede alertar a los lectores de las amenazas inminentes y las tendencias actuales. El informe también presenta recomendaciones para la protección y mitigación de estas inquietudes. Este volumen cubre un período de seis meses comprendido entre el 1° de Julio y el 31 de Diciembre de 2004.

Con más de 20.000 sensores monitoreando la actividad de las redes en más de 180 países, por medio del sistema de gestión de amenazas Symantec DeepSight™ Threat Management System y por los servicios de seguridad administrada de Symantec llamado Symantec™ Managed Security Services, Symantec ha establecido uno de los más amplios recursos de información sobre seguridad de Internet en el mundo. Symantec recopila la información de los códigos malignos, así como también los informes de spyware y adware de más de 120 millones de clientes, servidores y sistemas de portales que han desplegado productos antivirus de Symantec. Symantec también posee una de las bases de datos más completas del mundo sobre vulnerabilidades de seguridad, que cubre más de 11.000 vulnerabilidades que afectan a más de 20.000 tecnologías de más de 2.000 vendedores. Además de estas bases de datos de vulnerabilidades, Symantec opera BugTraq, uno de los foros más comunes para el descubrimiento y la discusión de vulnerabilidades en Internet. Finalmente, la Sonda de Red Symantec “Symantec Probe Network”, un sistema de más de dos millones de cuentas “señuelo” atrae mensajes de correos electrónicos de 20 países diferentes en todo el mundo, lo que permite que Symantec pueda medir la actividad global spam y phishing. Estos recursos proporcionan a los analistas de Symantec fuentes de datos incomparables, con las cuales pueden identificar las tendencias emergentes en los ataques y la actividad de códigos malignos.

El *Informe de Amenazas de Seguridad en Internet de Symantec*, se afianza principalmente en el análisis experto de datos reales. Con base en la destreza y experiencia de Symantec, el *Informe de Amenazas de Seguridad*, rinde un comentario muy completo sobre la actividad actual de amenazas en Internet. Al publicar el análisis de la discusión de la actividad de seguridad en Internet, en el *Informe de Amenazas de Seguridad en Internet*, Symantec espera proporcionar a la comunidad de seguridad de información, toda la información necesaria para ayudar a eficazmente proteger sus sistemas ahora y en el futuro.

Mensaje Principal

Como se anotó en el *Informe de Amenazas de Seguridad* anterior, las vulnerabilidades de las aplicaciones Web, continúan planteando amenazas serias. Las aplicaciones Web son blancos comunes porque éstas disfrutan de amplio despliegue y pueden permitir a los atacantes evadir las medidas tradicionales de seguridad, como las firewalls. Esto es una preocupación de seguridad seria porque las vulnerabilidades de las aplicaciones Web pueden permitir a los atacantes el acceso a información confidencial, sin necesidad de comprometer los servidores individuales. Cerca del 48% de las vulnerabilidades documentadas entre el 1° de Julio y el 31 de Diciembre de 2004, fueron vulnerabilidades de aplicaciones Web.

Entre el 1° de Julio y el 31 de Diciembre de 2004, Symantec documentó más de 1.403 nuevas vulnerabilidades, lo que se traduce en más de 58 nuevas vulnerabilidades por semana, o casi 10 nuevas vulnerabilidades diarias en promedio sobre las del año pasado. De estas vulnerabilidades, 97% fueron consideradas como moderadas o altamente severas, lo que significa que la explotación exitosa de vulnerabilidades podría resultar en un compromiso total o parcial del sistema que se pretende atacar. Además, 70% fueron consideradas como de fácil explotación, lo que podría significar, o bien que no se requiere de un código para explotar exitosamente las vulnerabilidades, o que dicho código está disponible públicamente. Combinado con este problema, es que casi el 80% de todas las vulnerabilidades documentadas durante el período de este informe, son remotamente explotables, lo que muy posiblemente aumenta el número de posibles atacantes.

En el volumen anterior del *Informe de Amenazas de Seguridad en Internet*, Symantec anticipó que el phishing emergería como una preocupación seria de seguridad. Durante los últimos seis meses, esta preocupación se ha confirmado. Phishing es un método para robar información confidencial, como por ejemplo claves, números de

tarjetas de crédito y otra información financiera. Esto es una amenaza seria para los consumidores y para las empresas. Mediante el uso de métodos sofisticados de ingeniería social, los atacantes engañan a los usuarios finales para que estos revelen su información más sensible. Desde Mayo de 2003 y hasta Mayo de 2004, las pérdidas en que incurrieron los usuarios de bancos y tarjetas de crédito de los estados Unidos, han sido estimadas en 1.2 billones de dólares. Entre el 1° de Julio y el 31 de Diciembre de 2004, Symantec detectó 10.310 nuevos ataques phishing. Además, para finales de Diciembre, los filtros antifraude Symantec Brightmail™ AntiSpam bloquearon un promedio de más de 33 millones de atentados phishing por semana, de aproximadamente 9 millones por semana a comienzos de Julio. Phishing no es la única amenaza para la información confidencial. Algunos códigos malignos son creados con la intención de robar intencionalmente la información confidencial de un computador comprometido. Entre el 1° de Julio y el 31 de Diciembre de 2004, estas amenazas representaron un 54% de los 50 más altos códigos malignos reportados a Symantec, por encima del 44% en el primer semestre de 2004, y 36% en el segundo semestre de 2003. Esto se debe parcialmente al uso continuo de los Troyanos, una amenaza particular a la exposición confidencial. Entre el 1° de Julio y el 31 de Diciembre de 2004, los Troyanos representaron el 33% de los 50 códigos malignos principales reportados a Symantec.

Durante este período del informe, hubo un aumento importante en el número de variantes de virus y gusanos basados en Windows. Desde el 1° de Julio hasta el 31 de Diciembre de 2004, Symantec documentó más de 7.360 variantes de gusanos y virus. Este representa un aumento del 64%, sobre el período anterior de seis meses. A 31 de Diciembre de 2004, el número total de amenazas de documento Win32 y sus variantes estuvo cerca de 17.500. Esto fuerza a las organizaciones a actualizar sus soluciones de antivirus con una mayor frecuencia que nunca, lo que a su vez, coloca mayor presión sobre los recursos corrientes.

En una comparación de distintos Web browsers, el descubrimiento de vulnerabilidades que afectan los Web browsers, está en aumento con más vulnerabilidades Mozilla documentadas en este periodo que aquellas que afectan al Windows Internet Explorer. Esto es contrario a la tendencia observada en períodos anteriores, en los cuales todas las vulnerabilidades afectaban exclusivamente el Windows Internet Explorer. Entre el 1° de Julio y el 31 de Diciembre de 2004, Symantec documentó 21 vulnerabilidades que afectaban los browsers Mozilla (Firefox and Mozilla) siendo más de 50% de esas vulnerabilidades consideradas como Altamente Severas. El de Windows Internet Explorer tenía 13 vulnerabilidades en este período del informe, siendo más del 26% de éstas clasificadas como de Alta Severidad. Sobre todo, mientras que existe una mayor proporción de vulnerabilidades que afectan los Browsers Mozilla, aún hay una alta proporción de vulnerabilidades de Alta Severidad que afectan el Windows Internet Explorer. Esto podría conducir a un compromiso total del sistema.

Con el fin de proporcionar una visión anticipada de los tipos de visión incluidos en el informe, el resto de este documento destaca un pequeño sub-juego de hallazgos preliminares, que serán discutidos en mayor profundidad en la publicación de Marzo de 2005.

Eventos Destacados

Tendencias de los Ataques

- Por la tercera vez consecutiva del periodo del informe, el Ataque Microsoft SQL Server Resolution Service Stack Overflow (anteriormente conocido como el Ataque Slammer), fue el ataque más común, utilizado por el 22% de los atacantes.
- Las organizaciones recibieron 13.6 ataques diarios, por encima de los 10.6 registrados en los seis meses anteriores.
- Computadores bot conocidos, declinaron de más de 30.000 por día a finales de Julio, a un promedio de menos de 5.000 diarios para finales del año.
- El Reino Unido tuvo un porcentaje mayor de computadores bot infectados, que cualquier otro país.
- Estados Unidos continúa siendo el país con mayor número de ataques de origen, seguido por la China y Alemania.
- El sector de servicios financieros experimentó 16 eventos severos por cada 10.000 eventos de seguridad, el mayor porcentaje de cualquier industria.

Tendencias de Vulnerabilidad

- El tiempo entre la divulgación de una vulnerabilidad y la liberación del código de explotación relacionado, aumentó de 5.8 a 6.4 días.

- Symantec documentó 1.403 nuevas vulnerabilidades, un aumento del 13% sobre el período anterior de seis meses.
- Las vulnerabilidades de aplicaciones Web representó el 48% de todas las vulnerabilidades divulgadas, un aumento del 39% de las vulnerabilidades del primer semestre de 2004.
- 97% de las vulnerabilidades divulgadas, fueron clasificadas como moderada o altamente severas.
- 21 vulnerabilidades que afectaron los browsers Mozilla fueron divulgadas durante los últimos seis meses, comparado con 13 vulnerabilidades que afectaron el Windows Internet Explorer.
- 70% de las vulnerabilidades reportadas fueron consideradas como fáciles de explotar.

Tendencias de Códigos Malignos

- Las variantes de Netsky, MyDoom, Beagle, dominaron los 10 ejemplos de códigos malignos durante el segundo semestre de 2004.
- Symantec documentó más de 7.360 nuevos virus y gusanos Win32, un aumento del 6.4% sobre el primer semestre del año.
- Códigos malignos que expusieron la información confidencial representaron el 54% de los 50 ejemplos principales de códigos malignos.
- A finales del período de este informe, había 21 ejemplos conocidos de códigos malignos para aplicaciones móviles, por encima de uno en Junio de 2004.
- Había dos bot presentes en los ejemplos de códigos maliciosos principales, comparados con solamente uno durante el período de informe anterior.
- 4.300 nuevas variantes distintas del Spybot fueron reportadas, lo que representa un aumento del 180% sobre los seis meses anteriores.

Riesgos de Seguridad Adicional

- Durante los últimos seis meses de 2004, los programas adware representaron un 5% de los 50 reportes de clientes Symantec principales, un aumento del 4% del reporte anterior.
- El programa Iefeats, fue el programa adware más reportado, representando un 36% de los 10 reportes superiores.
- Webhancer fue el programa spyware reportado más frecuentemente durante el segundo semestre de 2004, representando un 38% de los 10 spyware superiores reportados.
- Cinco de los 10 superiores ejemplos reportados, fueron instalados a través del Web browser. Nueve de los 10 programas de spyware superiores reportados fueron empaquetados con otro software.
- Entre el 1° de Julio y el 31 de Diciembre de 2004, Symantec detectó 10.310 nuevos ataques phishing.
- Hacia fines de Diciembre, los filtros antifraude de Symantec bloquearon más de 33 millones de atentados phishing por semana en promedio, un aumento de aproximadamente 9 millones por semana a comienzos de Julio.
- Symantec reportó un crecimiento del 77% en spam para empresas cuyos sistemas fueron monitoreados.

Mirando Hacia el Futuro

- Symantec considera que aumentará el uso de bots y redes bot, para ganancia financiera.
- Se espera un aumento, tanto en su número como en su intensidad, de códigos malignos enfocados a los dispositivos móviles.
- Symantec considera que habrá un aumento en ataques a clientes, utilizando gusanos y virus como medio de propagación.
- Symantec espera un aumento en los ataques escondidos en contenidos incrustados de audio y en imágenes de video.
- Symantec espera que los investigadores de vulnerabilidades intensifiquen su enfoque en Mac Os.
- Symantec espera que los riesgos de seguridad relacionados con adware y spyware se intensificarán. No se espera que la legislación inminente para refrenar estos riesgos sea un disuasivo eficaz o suficiente por si mismo.