Mayorista de Valor Agregado

Malware o la sofisticación de los riesgos

Cómo prevenir y combatir la nueva generación de amenazas

Presentado por:
Juan Francisco Torres

SurfControl®

Contenido de la charla

- Conceptos básicos y terminología
- Problemática
- Impacto en las empresas
- Impacto en el modelo de seguridad
- Tecnologías existentes
- Solución propuesta
- Conclusiones y recomendaciones

Mayorista de Valor Agregado

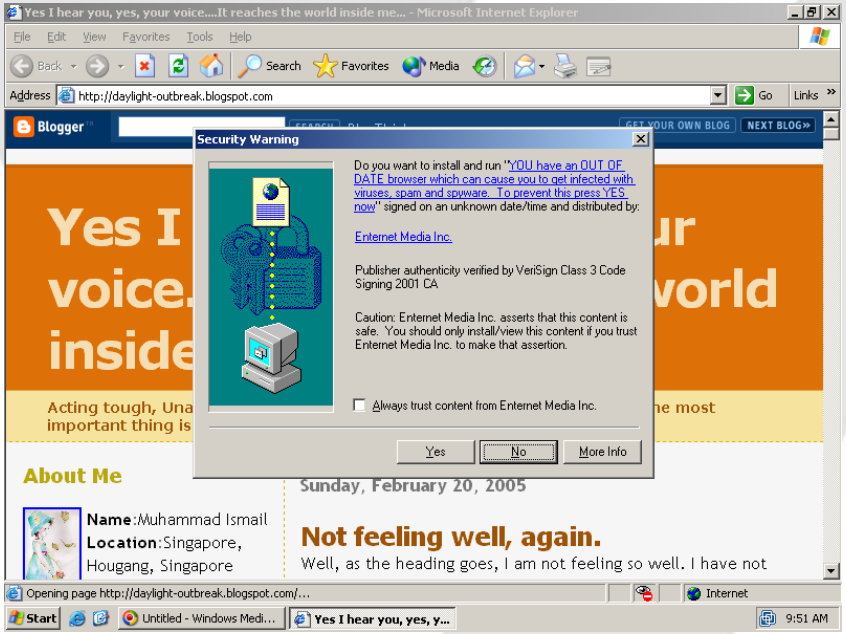
Conceptos básicos y terminología

Malware

- Software diseñado para infiltrar o dañar un sistema de cómputo, sin el consentimiento informado del usuario.
- Hace referencia a la intención de su creador, más que a una característica particular del software.
- Esto incluye software malicioso y no deseado, como:
  - Infeccioso: Virus y gusanos
  - Encubierto: Troyanos, rootkits y puertas traseras (backdoors)
  - Para beneficio económico: spyware, botnets, loggers, dialers

Spyware

- Amplia categoría de software malicioso, diseñado para interceptar o tomar el control parcial de la operación de un computador.
- Esto sucede sin el consentimiento informado del propietario del equipo o de su usuario legítimo.
- Generalmente la información es almacenada y enviada a través de la red.
- Enfocado a beneficio económico.



P2P: Peer-to-Peer

- Término usado para las redes que utilizan el poder de cómputo y ancho de banda de los participantes.
- Utilizadas principalmente para compartir archivos (audio, video y datos).
- Utilizadas para transmisión en tiempo real de datos como telefonía.

Mayorista de Valor Agregado

IM: Mensajería instantánea

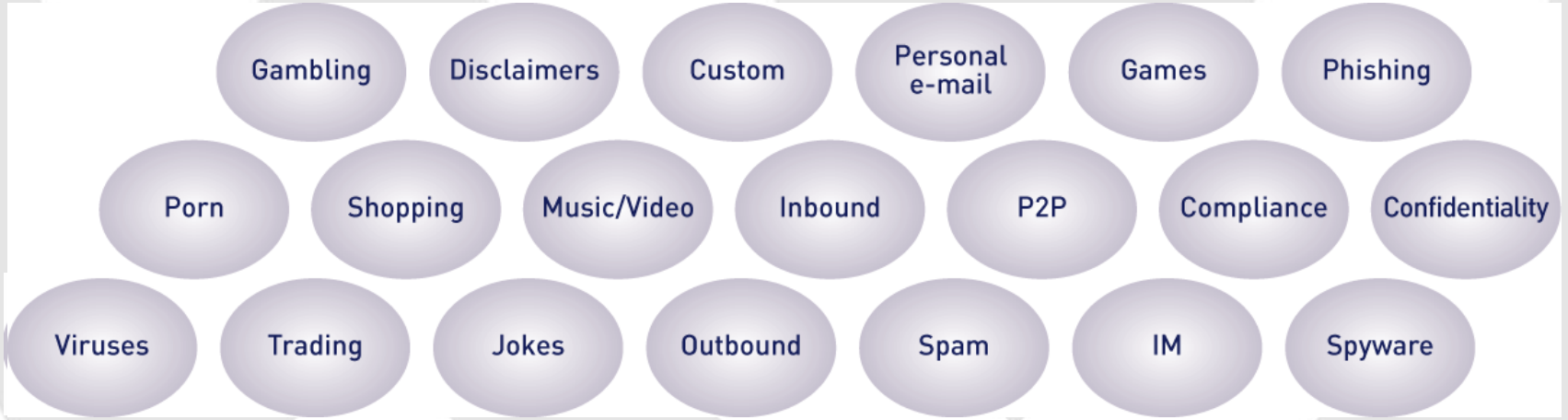
- Forma de comunicación en tiempo real entre dos o más personas, basada en texto digitado.
- Requiere de un programa “cliente” que se conecta al servicio a través de la red.
- Ofrecen servicio de “presencia” de personas.

Mayorista de Valor Agregado

Problemática

Mayorista de Valor Agregado

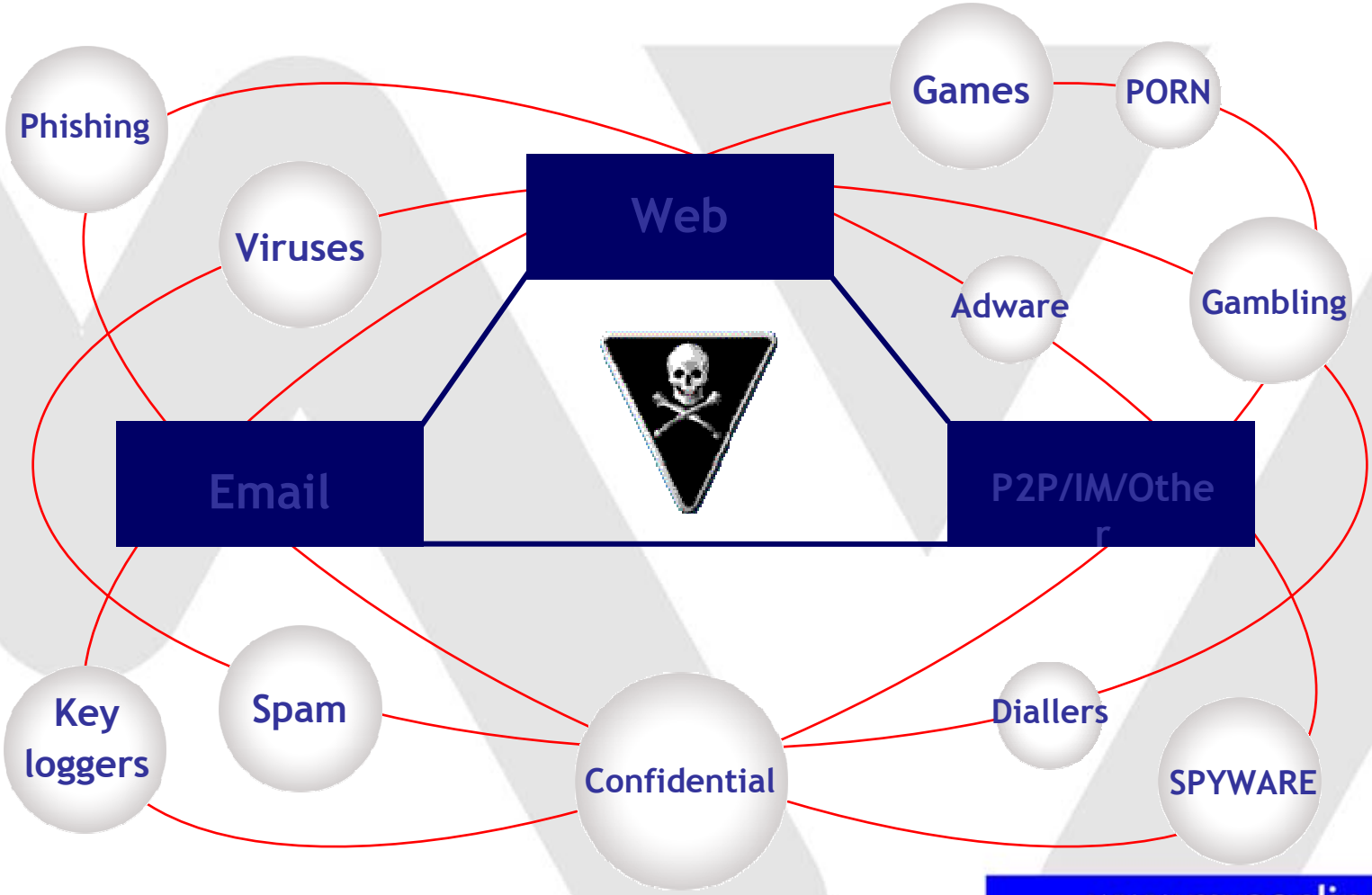
Riesgos de Seguridad en Internet



Pre 1995 · 1995 · 1996 · 1997 · 1998 → 2002 · 2003 · 2004 · 2005

Mayorista de Valor Agregado

El reto de la amenaza compuesta



Cuáles son las debilidades?

- Las amenazas toman ventaja del comportamiento de los usuarios:
  - Juegos en línea
  - Descargas gratis de videos y música
  - Uso de mensajería no estándar con amigos y/o familiares
  - Almacenamiento de archivos en máquina local o en la red
  - Instalación de programas freeware o shareware
- Las amenazas afectan a los usuarios directamente, y a la empresa indirectamente

Datos sobre IM, P2P y juegos

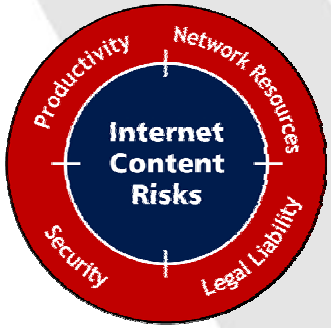
- Aumento de uso de estos programas como método para propagar spyware y/o ataques de phishing (captura de información en sitios web falsos).
- Reportado como el problema #5 en el Top 10 del 2005 de la revista “CIO Insight”
- Permiten traspaso de la seguridad del perímetro o son ingresados por los usuarios móviles.
- 87% de PCs corporativos con algún tipo de programa no deseado (55% sin incluir cookies) - Webroot, Q1 2005

Mayorista de Valor Agregado

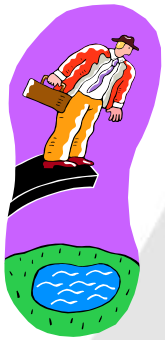
Impacto en las empresas

El riesgo para el negocio

- Riesgos de productividad
  - Pérdida de productividad por uso de juegos y mensajería.
- Riesgos de seguridad
  - Código malicioso (spyware, loggers, etc.) y otras descargas provenientes de la red, programas P2P, IM y correo electrónico.
  - Pérdida de información confidencial a través de IM, P2P, spyware
- Riesgos legales
  - Uso ilegal y/o copia de música, archivos, programas o juegos con derechos de autor.
- Riesgos de red
  - Desempeño de la red disminuido o anulado debido a uso de juegos y/o programas P2P



Cómo entran las amenazas a la red?



- Malware es un síntoma de otras amenazas:
  - Juegos: muchos juegos gratis contienen adware
  - Redes P2P como Kazaa
  - IM: transferencia de archivos
  - Programas gratis: Frecuentemente contienen agentes de seguimiento o análisis (spyware) que reportan a sitios externos

- La presencia de estos programas indica uso inadecuado de la red por parte de los usuarios en una o varias máquinas.

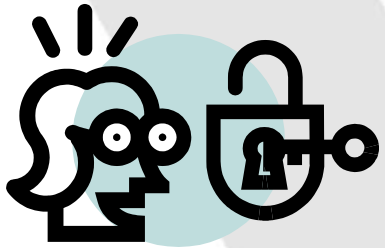
Mayorista de Valor Agregado

Impacto en el modelo de seguridad

Mayorista de Valor Agregado

Propiedades del modelo de seguridad

- **Confidencialidad**: Los recursos del sistema solo pueden ser accedidos por los elementos autorizados.
- **Integridad**: Los recursos del sistema solo pueden ser modificados o alterados por los elementos autorizados.
- **Disponibilidad**: Los recursos del sistema deben permanecer accesibles a los elementos autorizados.

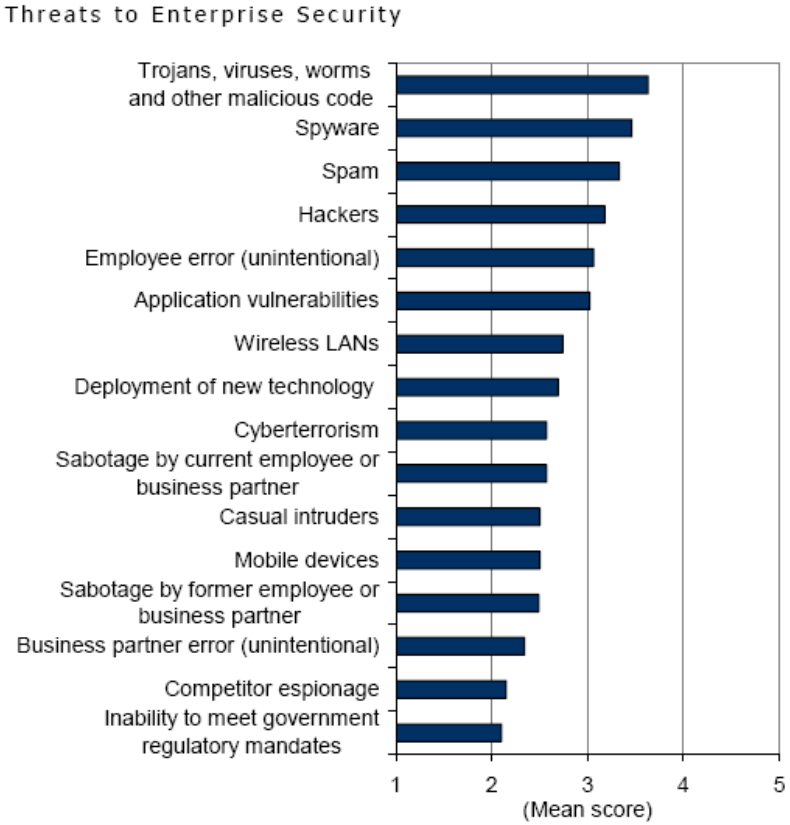


Variables afectadas

- **Confidencialidad**: Los programas instalados tienen acceso a la información del usuario, y la transmiten a terceros.
- **Integridad**: El código externo altera el funcionamiento del sistema operativo y de la red donde se encuentra.
- **Disponibilidad**: El uso no autorizado de los recursos limita la productividad y el acceso a la información y a los sistemas

Mayorista de Valor Agregado

Cuáles son las amenazas?:



n = 435

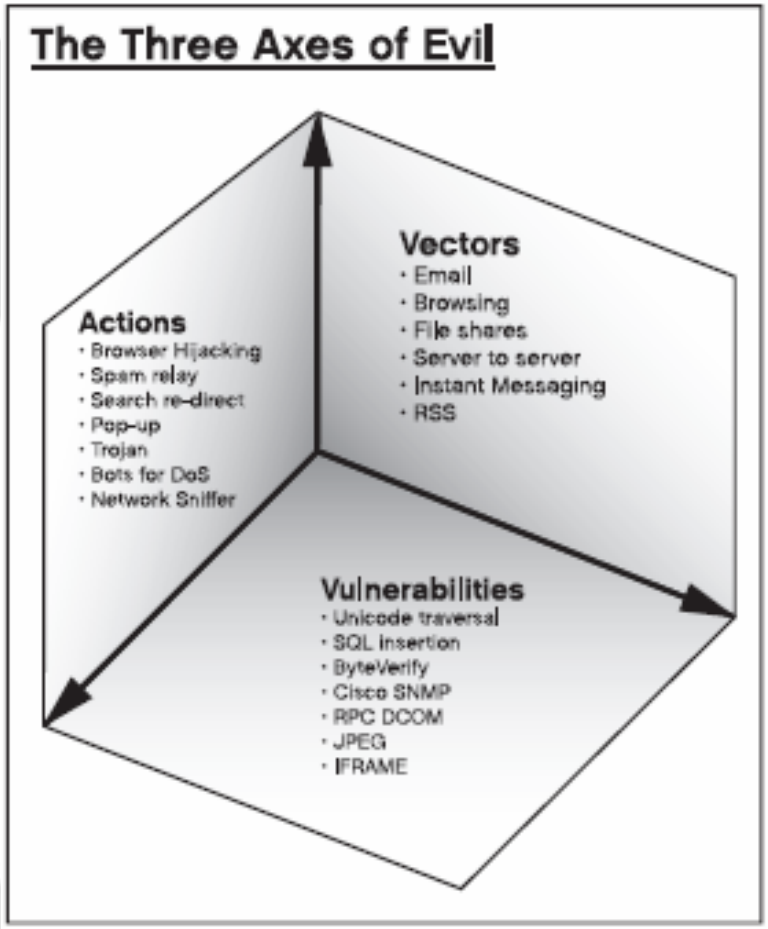
Note: Scores are based on a scale from 1 to 5, with 1 being no threat and 5 being a significant threat.

Source: IDC's *Enterprise Security Survey*, 2005

Mayorista de Valor Agregado

Se asume que:

- El tráfico es pequeño y limitado a pocos usuarios.
- Los usuarios son capacitados e instruidos sobre estos riesgos.
- Se cuenta con soluciones perimetrales de seguridad que son suficientes y cubren todos los factores.



Mayorista de Valor Agregado

Tecnología existente

Mayorista de Valor Agregado

Programas antivirus

- Enfocados exclusivamente a virus y gusanos.
- Requiere adiciones para revisar archivos y programas especiales (IM, P2P).
- Velocidad de las actualizaciones es muy variada de acuerdo al tipo de solución implementada.

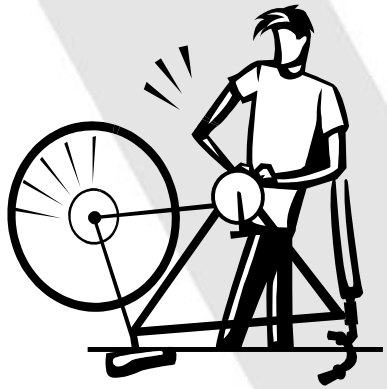
Mayorista de Valor Agregado

Programas anti-spyware

- Enfocados exclusivamente a programas reconocidos como spyware.
- Realizan tareas correctivas (reactivas) para eliminar el software.
- Baja centralización de despliegue, control, actualización y recolección de información.

Control directo sobre el sistema operativo

- Sistemas operativos como MS Windows XP cuentan con controles muy restringidos y locales (registro)
- No se encuentra integrado al software de control y administración de dominios.
- No permite manejo granular por usuarios, máquinas o aplicaciones



Mayorista de Valor Agregado

Soluciones de software existentes

- Interacción con usuario final confusa (resultados poco claros)
- Solamente abarcan un tipo de amenaza (spyware o P2P o IM)
- Requiere una administración de seguridad perimetral muy pesada, pues depende del tipo de programa utilizado (puertos variables)
- Poca integración con herramientas centralizadas como Active Directory
- Escaneo de archivos de audio/video limitado a extensiones de archivos (no por firma digital)

Mayorista de Valor Agregado

Solución propuesta

Mayorista de Valor Agregado

Qué es SurfControl Enterprise Threat Shield?

Un producto que:

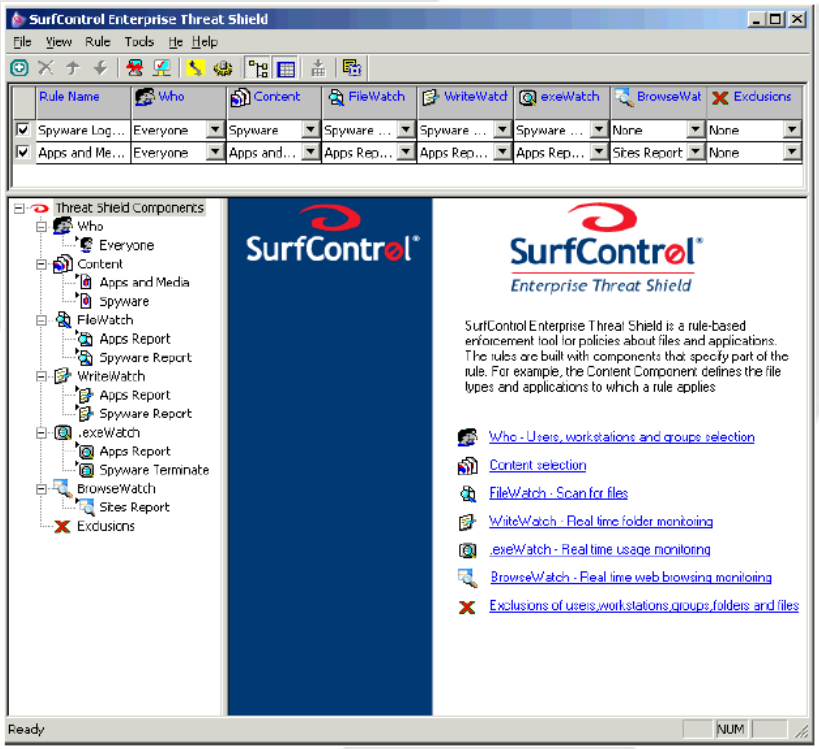
- Permite al negocio tener control sobre una amplia gama de programas en permanente evolución
  - Bases de datos dinámicamente actualizadas
  - Políticas granulares
- Protección completa contra programas que ponen en riesgo su red
  - Revisión continua
  - Remueve
  - Finaliza
- Diseñado para la empresa
  - Manejo centralizado
  - Reportes completos

Enterprise
Threat Shield

Mayorista de Valor Agregado

Amplio control de amenazas

- Control completo de amenazas
  - Bases de datos extensas de firmas, dinámicamente actualizadas, que controlan aplicaciones de spyware, keyloggers, IM, P2P y juegos.
  - Bloqueo por firmas de protocolos y por características de archivos.
  - Permite crear bases de datos de firmas personalizadas según la empresa.
- Políticas de seguridad flexibles
  - Administrador de políticas permite control granular por usuario, tiempo, y tipo de aplicación, que permite definir y asegurar el uso de las políticas de seguridad.



Mayorista de Valor Agregado

Protección completa

- Protegido contra alteración
- Residente en memoria – poco espacio
- Cuatro tecnologías de escaneo
  - FileWatch – revisa almacenamiento local/red en busca de amenazas
  - WriteWatch – revisa escritura local/red en medios de almacenamiento
  - .exeWatch – revisa los programas que son ejecutados para garantizar uso aplicación de políticas
  - BrowseWatch – registra tiempo exacto de navegación
- Bloquea, Reporta, Remueve, Monitorea

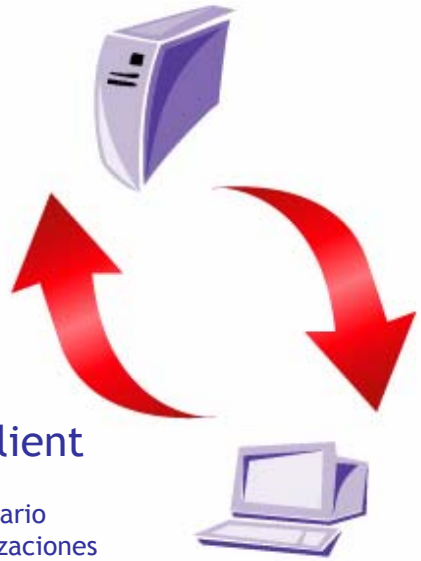
Mayorista de Valor Agregado

Para la empresa: Máximo control

- Despliegue centralizado
- Fácil integración con servicios de directorio (Active Directory, Novell eDirectory)
- Reportes y administración centralizados
- Impacto mínimo en los usuarios – no requiere de su intervención
- Impacto mínimo en rendimiento de las máquinas de usuarios

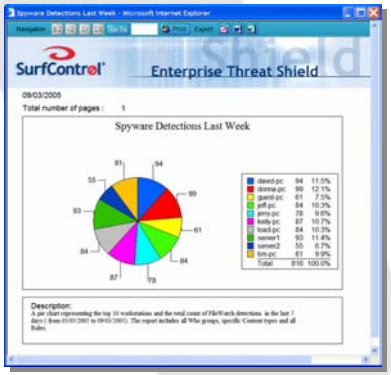
Threat Shield Server

Bases de datos Threat Shield
Reglas
Actualizaciones
Unido al directorio



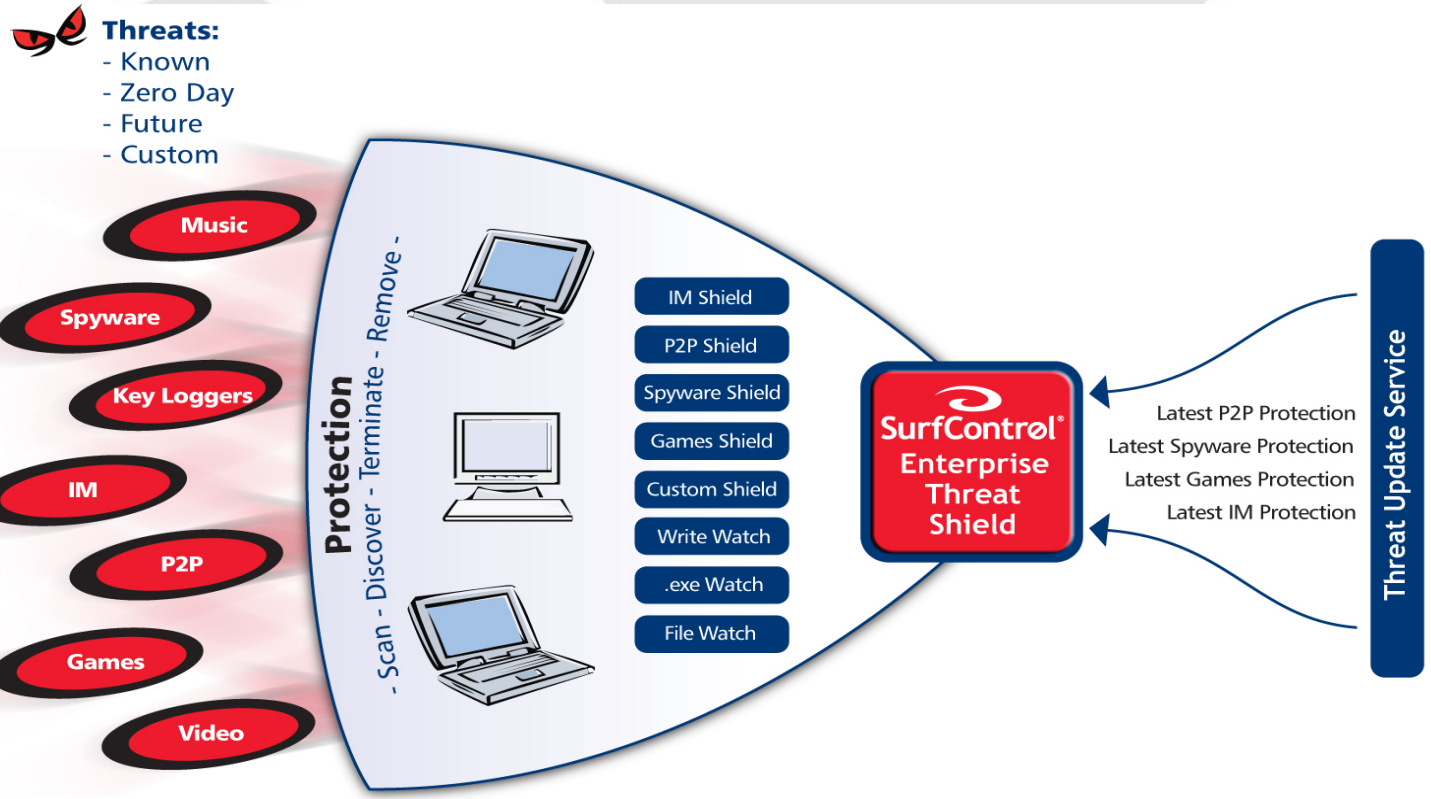
Threat Shield Client

Residente en memoria
No es detectable por usuario
Verifica cambios/actualizaciones en las bases de datos



Mayorista de Valor Agregado

Más que descubrir y remover: Prevención total



Mayorista de Valor Agregado

Conclusiones y recomendaciones

Mayorista de Valor Agregado

Para tener en cuenta…

- Realizar un análisis detallado del estado de los equipos de la empresa, en relación a software, archivos de audio/video y aplicaciones de uso particular como IM, juegos, etc (evaluación de riesgos – ISO 17799)
- Contar con una política de uso aceptable que tenga en cuenta el uso de programas en las estaciones de trabajo, la copia de archivos de audio/video y el uso de programas de mensajería, y alineada con la política de la compañía. (ISO 17799)
- Contar con herramientas que permitan realizar el monitoreo y control, y reporte de este tipo de software, y planes de acción de mantenimiento y reparación. (implementar administración – ISO 17799)

Mayorista de Valor Agregado

Recomendaciones

- Herramientas usadas:
  - Deben ser efectivas, que hagas clara diferencia entre programas legítimos y programas no deseados.
  - Evaluar el costo de la prevención comparado con el costo de tener programas en la red (tiempo usuarios, organización, hardware y software)
  - Deben ser proactivas, no reactivas
  - Deben proporcionar registros de funcionamiento
  - Tener en cuenta una arquitectura multicapas (en el perímetro y en los PCs) para mayor control (complementarias entre ellas)
- Características
  - Manejo centralizado, escalable, protección para usuarios remotos, cuarentena y borrado, reportes y alertas, actualizaciones y bases de datos

Mayorista de Valor Agregado

Bibliografía

- http://news.zdnet.co.uk/0,39020330,39197141,00.htm
- www.wikipedia.org
- http://www.antispywarecoalition.org
- www.surfcontrol.com

Mayorista de Valor Agregado

Gracias por su atención

Más información en www.mvaonline.com
Email: info@mvaonline.com

Lo esperamos en el área de Exhibición a las 6:00 PM