Ransomware:
la bolsa o la vida (digital)

Nicasio de Tomas
Channel Manager Dell Security Iberia
Alex Vazquez
Ingeniero Preventa Dell Security

Agenda

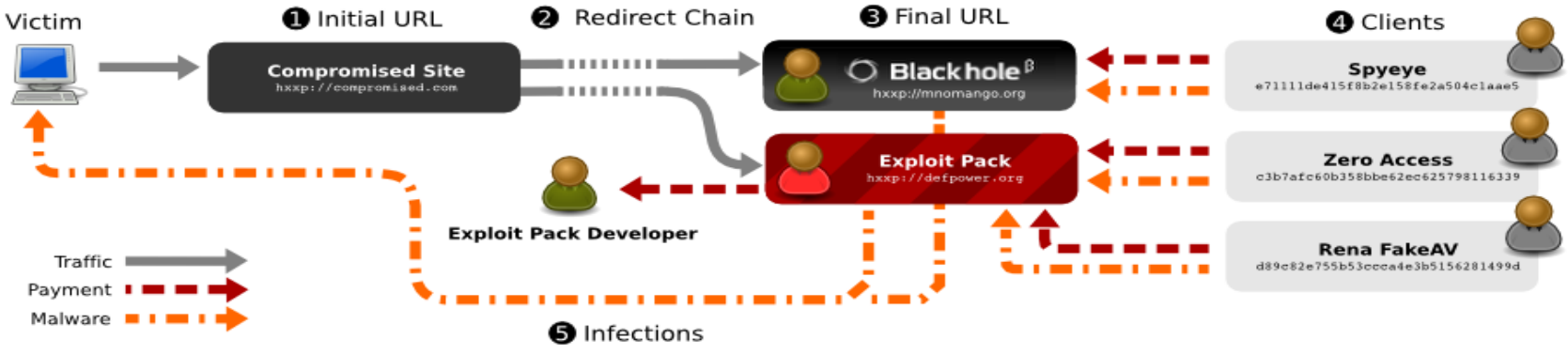
- Algunas definiciones
- Tipos de Ransomware
- Breve historia del Ransomware
- Canales de Propagación
- Como protegernos contra el Ransonware
- Seguridad basada en capas
- Sonicwall NGFW – Configuración y buenas prácticas
- Conclusiones y Referencias

Algunas definiciones

- **Ransomware** (del inglés *ransom* (rescate) y *ware* (software))**:** es un tipo de malware que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.[1] Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

(Source: https://es.wikipedia.org/wiki/Ransomware

Algunas definiciones(cont.)



- **Exploit Kit:** Un exploit kit es un kit de software diseñado para ejecutarse en servidores web, con el fin de identificar las vulnerabilidades de software en los equipos cliente que se comunican con él, para explotarlas y poder transferir y ejecutar código malicioso.

(Source: https://en.wikipedia.org/wiki/Exploit_kit)

Algunas definiciones(cont.)

- **Spear phishing:** Intentos de phishing dirigidos a particulares o empresas específicas. Los atacantes pueden recopilar información personal acerca de su objetivo y aumentar su probabilidad de éxito. Esta técnica es, con diferencia, la más exitosa en Internet hoy en día, representa el 91% de los ataques.

(fuente: https://en.wikipedia.org/wiki/Spear-phishing)

- **Drive-by download** significa dos cosas, ambas relacionadas con la descarga involuntaria de software a través de Internet:

  1) Descargas autorizadas por el usuario, pero sin entender las consecuencias (por ejemplo descargas que instalan un programa desconocido, un ejecutable falsificado,componentes ActiveX o Java applet).

  2) Cualquier descarga que ocurre sin el conocimiento de una persona, a menudo un virus informático, software espía,malware, o software de actividades ilegales.

(fuente: https://en.wikipedia.org/wiki/Drive-by_download)

Tipos de Ransomware

Locker Ransomware

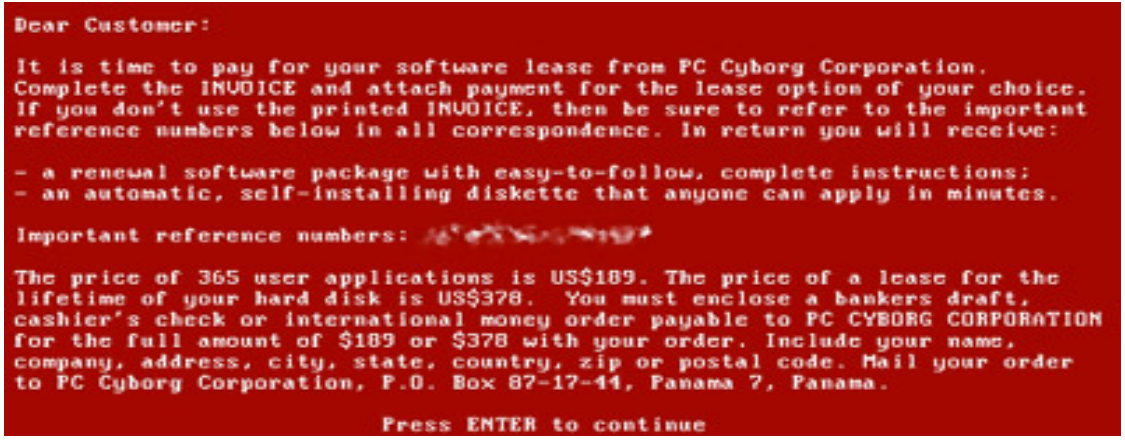
- Restringe el acceso del usuario al interfaz de su dispositivo.
- Normalmente se propaga a través de ingeniería social, campañas de phishing y sitios web legítimos comprometidos.
- Por lo general, no afecta a los documentos o ficheros de sistema; en su lugar, sólo se restringe el acceso a la interfaz.
- A menudo puede ser eliminado fácilmente mediante la restauración del sistema a la última copia o mediante la implementación de una herramienta de eliminación comercial.
- Algunas variantes más sofisticadas incorporan ingeniería social en la estafa para presionar al usuario a pagar el rescate (Ej.: disclaimer del FBI o Policía).

Crypto Ransomware

- Crypto ransomware tiene como objetivo los datos y el sistema de ficheros del dispositivo.
- La funcionalidad del sistema y los archivos críticos normalmente no quedan afectados.
- A menudo incluye un tiempo límite, después del cuál la clave de descifrado podría (o no) ser eliminada de forma permanente si la víctima no paga el rescate a tiempo.
- Antes de 2013, las implementaciones existentes eran mucho más simples y fáciles de descifrar (clave de descifrado común, claves de descifrado almacenadas en el dispositivo o en el código, etc.).
- A partir de 2013, hubo una evolución hacia implementaciones más complejas y el uso de algoritmos de cifrado asimétrico fuerte, como RSA, 3DES, AES, etc.
- La mayoría usan Tor, proxies, y cripto-monedas, como bitcoins para permanecer en el anonimato.

Breve historia del Ransomware

Ransomware no es una nueva amenaza!



Nombre: AIDS Trojan

Fecha: 1989

Creador: Dr. Joseph Popp (Biologist)

Propagacion: Floppy disks

Rescate: $189 o $378

- Este fue el primer ransomware conocido
- Ocultaba carpetas y encriptaba ficheros
- Se ejectutaba despues de 90 reinicios del ordenador
- Pedía un rescate (enmascarado como licencia de software) para ser pagado en una cuenta de Panama

Archiveus Trojan & GPCode (PGPCoder)

- **Nombre:** Archiveus Trojan
- **Fecha:** 2006
- **Creador:** desconocido
- Primer ransomware que usó encriptación RSA.
- Exigía a las victimas comprar artículos de farmacia on-line.
- Encriptaba toda la carpeta de Mis documentos.

- **Nombre:** GPCode Trojan
- **Fecha:** 2006
- **Creador:** Programador Ruso (desconocido)
- **Propagacion:** Correo spam con fichero Word adjunto.
- **Rescate:** 100 – 200 $
- La versión inicial usaba un algoritmo de encriptación propietario. En 2010 se lanzo una versión mejorada con encriptación avanzada (RSA/AES)

Reveton

- **Nombre:** Reveton (Virus de la Policia)
- **Fecha:** 2012
- **Creador:** Desconocido
- **Propagacion:** Correo spam, Drive-by-Download, botnets…
- **Rescate:** 200 $
- Se conecta a la botnet ZeuS/Citadel
- Muestra dirección IP, webcam,
- Usa Geolocalización para personalizar el mensaje.

Cryptolocker

- **Nombre:** Cryptolocker
- **Fecha:** Septiembre 2013
- **Creador:** Desconocido
- **Propagacion:** Correo phishing (ZIP adjunto con ejecutable disfrazado de PDF)
- **Encriptacion:** RSA 2048
- **Rescate:** 0.3 – 2 Bitcoins en 72 - 100 horas

- Las máquinas infectadas se conectaban a la botnet Gameover ZeuS.
- La clave privada necesaria para desencriptar los ficheros se almacenaba en los servidores C&C.
- Cryptolocker y la botnet ZeuS se cerraron en Mayo del 2014 tras la Operacion Tovar. Las claves privadas se usaron para crear una herramienta online de recuperación de ficheros cifrados.

Cryptowall

- **Nombre:** Cryptowall
- **Fecha:** Principios de 2014
- **Creador:** Desconocido
- **Propagacion:** Exploit kits y correo spam (adjunto RAR con fichero CHM)
- **Encriptacion:** AES-256
- **Rescate:** 1 Bitcoin
- Usa Geolocalización para personalizar los mensajes.

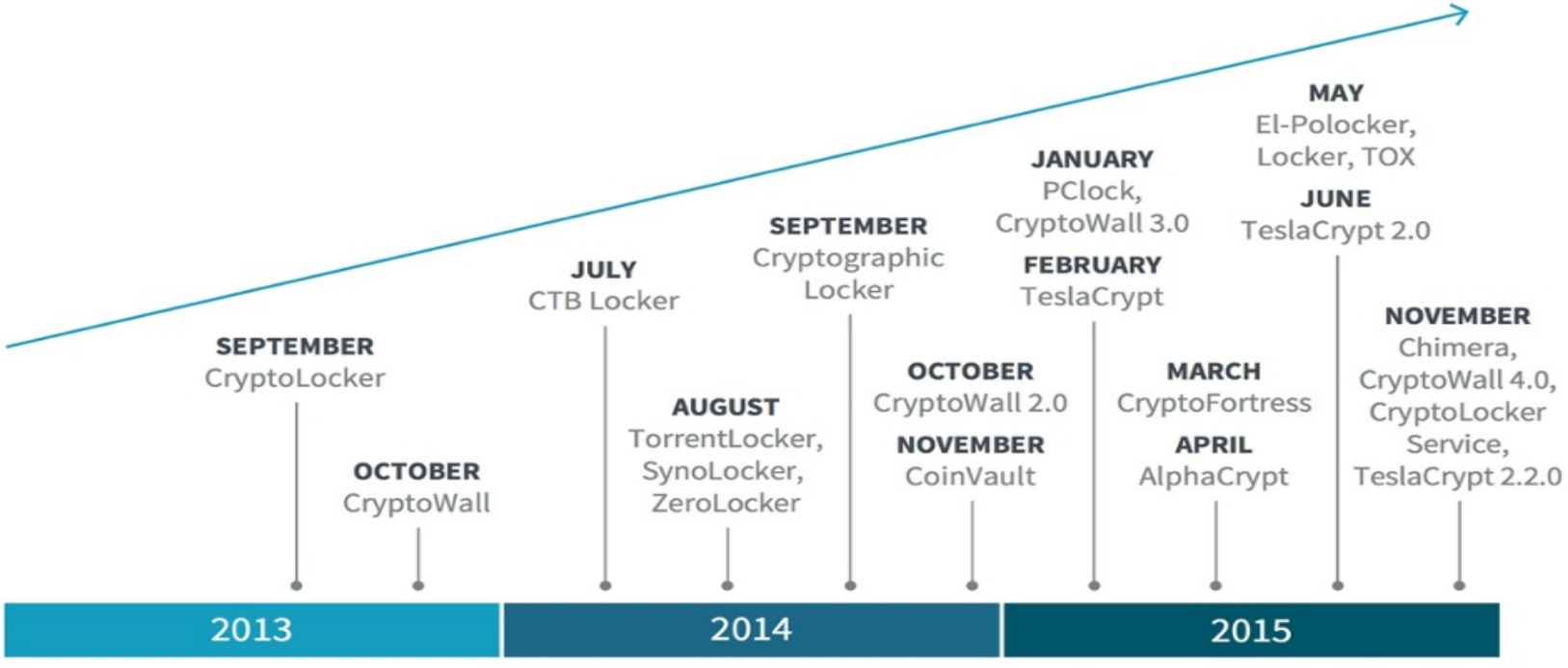
- Usa la red I2P para la conexión con el servidor C&C que almacena las claves privadas, y la red Tor para el pago del rescate.
- Dado el éxito de Cryptolocker, aparece como un clon mejorado después de la Operacion Tovar.

Locky

- **Nombre:** Locky
- **Fecha:** Febrero 2016
- **Creador:** Dridex (grupo criminal)
- **Propagacion:** Spam con adjunto (Word con macros)
- **Encriptacion:** RSA 2048 y AES-128
- **Rescate:** 0,5 – 1 bitcoin
- Más de 90.000 equipos infectados cada día.
- Se hizo popular tras la infección de equipos en varios hospitales norteamericanos.

"Locky" sets your wallpaper to make sure you know what to do next

Summary

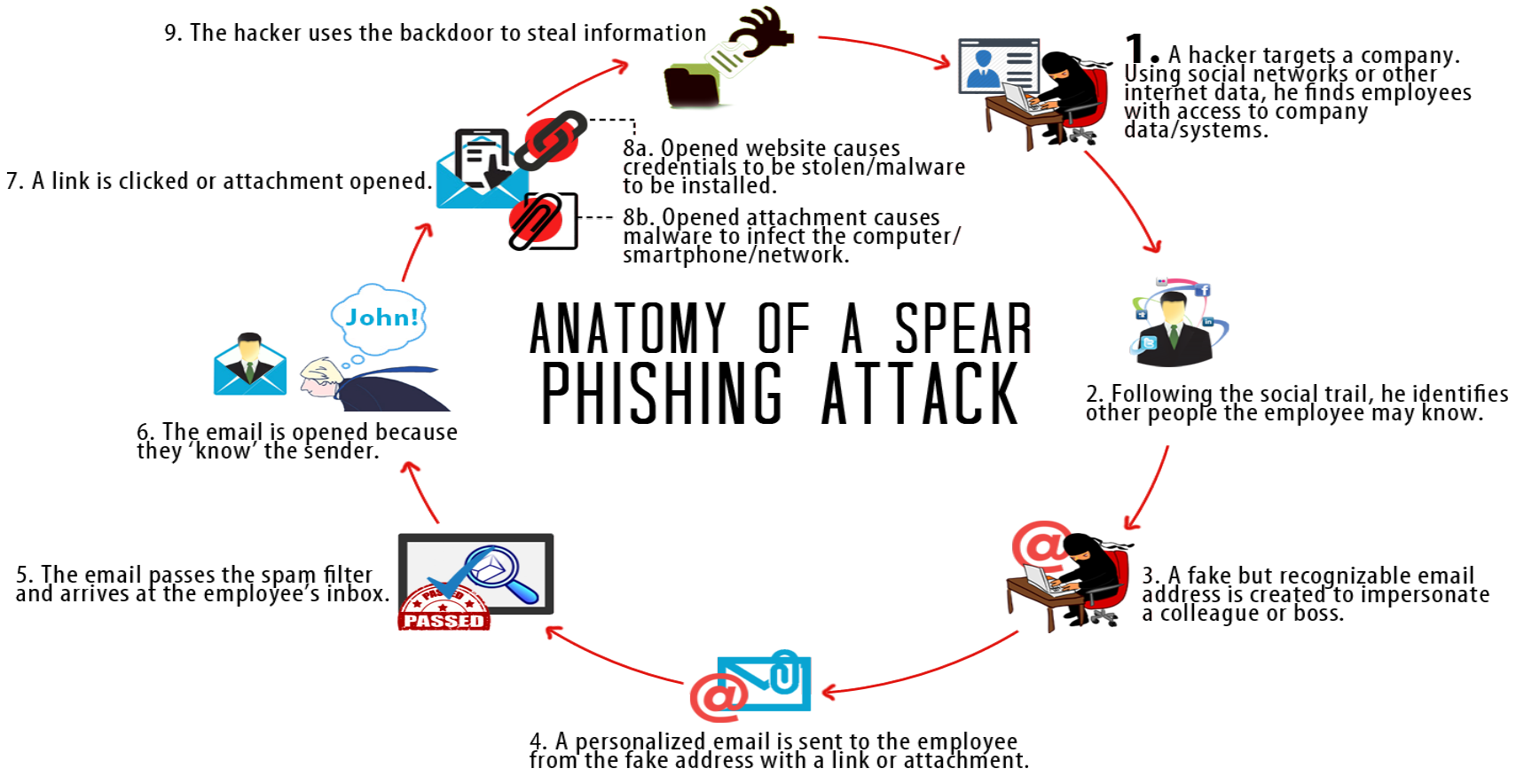

SEPTEMBER
CryptoLocker
OCTOBER
CryptoWall
JULY
CTB Locker
AUGUST
TorrentLocker,
SynoLocker,
ZeroLocker
SEPTEMBER
Cryptographic
Locker
OCTOBER
CryptoWall 2.0
NOVEMBER
CoinVault
JANUARY
PClock,
CryptoWall 3.0
FEBRUARY
TeslaCrypt
MARCH
CryptoFortress
APRIL
AlphaCrypt
MAY
El-Polocker,
Locker, TOX
JUNE
TeslaCrypt 2.0
NOVEMBER
Chimera,
CryptoWall 4.0,
CryptoLocker
Service,
TeslaCrypt 2.2.0
2013
2014
2015

Canales de propagación

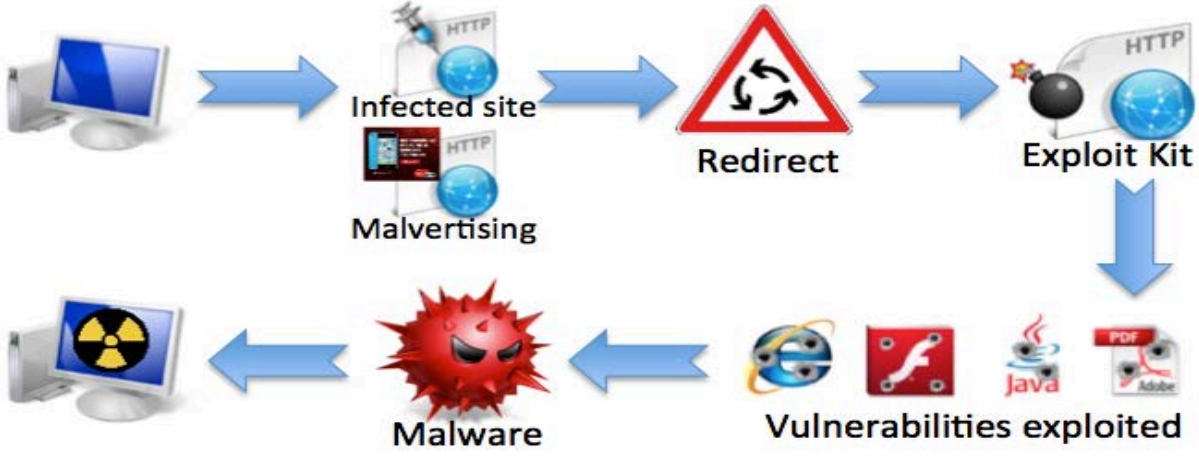
Spear-Phishing

- Durante muchos años, el correo spam utilizando técnicas de ingeniería social ha sido el método preferido para la distribución de todo tipo de malware, incluyendo ransomware.
- Los ciber-delincuentes usan una botnet para el envío de spam.
- El spam por lo general viene en forma de correo electrónico que contiene un archivo adjunto malicioso o un enlace que lleva a un sitio web con Exploit Kits.
- Los correos spam encarnan toda una gama técnicas de ingeniería social y elementos psicológicos para engañar a los usuarios y que instalen el ransomware. Algunos de los temas más comunes son:
  - Notificación de entrega
  - Factura de energia
  - Curriculums de personas buscando empleo
  - Devolución de impuestos y/o Facturas
  - Notificaciones de multas
  - Correos de amigos de redes sociales

Anatomia de un ataque Spear-Phishing



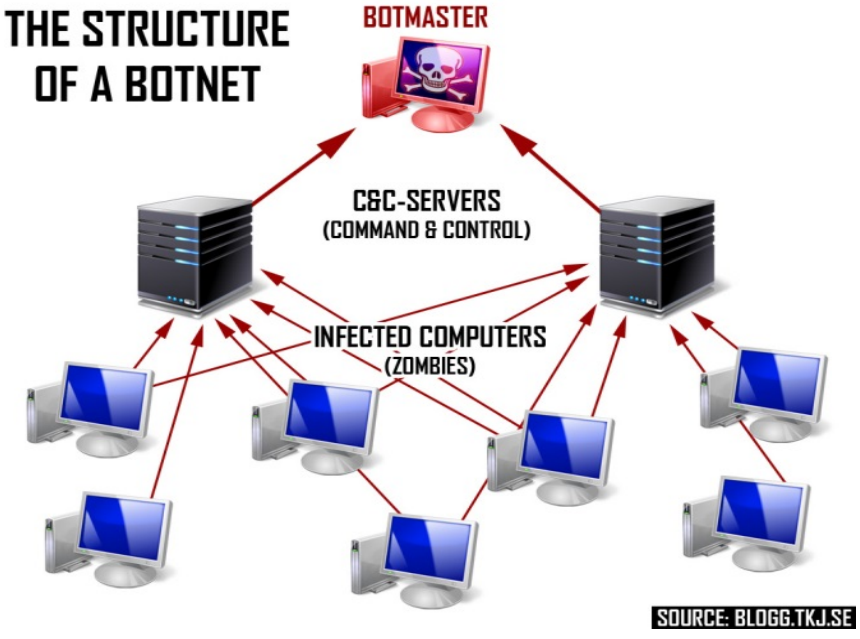
Drive-by Download



- Las páginas que usan drive-by-download normalmente se encuentran alojadas en sitios web legítimos en los que un atacante ha publicado algún código de explotación (p.ej.: iframes invisibles).
- El usuario es redirigido al servidor malicioso, que contiene un exploit kit que tratará de explotar vulnerabilidades en el navegador en sí, o en algunos plugins del navegador como Java, Adobe Reader o Flash
- Si el host es vulnerable al exploit kit, entonces el malware se descargará en el sistema y lo infectará.

Downloaders & Botnets

- El malware se distribuye en varias fases a través de downloaders, para minimizar la probabilidad de detección basada en firmas.
- Una vez que el downloader infecta un ordenador, su trabajo consiste en descargar malware adicional en el sistema comprometido.
- Se sabe que algunas botnets infectan con ransomware algunas de las máquinas comprometidas. Esto se hace generalmente por los ciberdelincuentes para obtener un rendimiento económico de parte de los ordenadores que controlan.



Ingeniería Social y Auto-Propagación

- Algunos ransomware también tienen la capacidad de propagarse. Por ejemplo, en Android, hay algunas variantes de ransomware que no sólo bloquean el dispositivo o cifran archivos, sino que emplean técnicas similares a las que usan los gusanos para propagarse a todos los contactos de la agenda, mediante el envío de mensajes SMS con ingeniería social.
- Potencialmente, la auto-propagación es una forma de propagación efectiva para el ransomware, pero causa problemas a los delincuentes que esperan un pago del rescate. Nadie estará dispuesto a pagar si se sigue exigiendo un nuevo pago de rescate después de cada pago.

Como protegernos frente al Ransomware

Usuarios Educación y formación

- **Los usuarios son normalmente el eslabón más débil.**
- La gran mayoría de las infracciones y los incidentes de ciberseguridad están directamente correlacionados con las acciones inocuas o maliciosas del personal.
- A menudo, los cibercriminales tratan de dirigirse a ellos utilizando técnicas de ingeniería social. Los empleados deberían de estar formados para reconocer un enlace o un archivo adjunto malicioso.
- La mejor arma para defenderse contra este tipo de ataques es la **educación y formaciones básicas en materia de seguridad** (Ej.: Sonicwall Phishing IQ Test - http://www.sonicwall.com/phishing/).
- Algunos sitios útiles para los usuarios para verificar archivos adjuntos de correo o enlaces en caso de duda:
  - https://www.virustotal.com
  - https://malwr.com/submission/

Mantener acualizados SO y Aplicaciones

- La mejor defensa contra una infección basada en exploits es **asegurarse de que su sistema operativo y las aplicaciones están actualizadas con los últimos parches de seguridad.**
- Algunas de las aplicaciones mas comunes son también las más atacadas por los Exploit kits. **Si utiliza cualquiera de las siguientes aplicaciones, se recomienda que utilice las actualizaciones automáticas si es posible.**
- **Adobe**: Usuarios de Adobe Acrobat/Reader, Flash Player, and Shockwave Player **deberían de asegurarse de estar al día en cuanto a los parches.**
- **Adobe publica actualizaciones el segundo martes de cada mes.**
- Este enlace proporciona más información y detalles sobre parches: https://helpx.adobe.com/security.html

Mantener acualizados SO y Aplicaciones(cont.)

- **Microsoft**: Los usuarios de productos de Microsoft tales como Windows, Office e Internet Explorer **son a menudo objetivo de los Exploit Kits**. Microsoft normalmente publica actualizaciones de software el segundo martes de cada mes. El siguiente enlace proporciona más información y detalles sobre parches: https://technet.microsoft.com/en-us/security/bulletin/
- **Oracle**: Oracle Java es con frecuencia objetivo de los Exploit Kits. Oracle normalmente publica parches de software una vez al trimestre. Puede encontrar más información acerca de las actualizaciones de software de Oracle en la siguiente ubicación: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Estrategia de Backup

- **Hacer copias de seguridad es siempre una buena idea**, incluso sin las amenazas del ransomware.
- Las copias de seguridad son también una parte esencial del **plan de continuidad de negocio y recuperación ante desastres**, que todas las empresas deberían tener.
- Las copias de seguridad de los archivos importantes deben hacerse con regularidad.
- **La frecuencia de las copias de seguridad** y la solución de almacenamie enerse en cuenta, **en fu**

Securidad basada en Capas

- **El mejor enfoque es utilizar una defensa de múltiples capas:**
  - Antispam
  - Antivirus
  - IDS/IPS
  - Web Filtering
  - Anti-Botnet
  - DPI-SSL Inspection
  - Application Control
  - Sandboxing

- **Cada capa actúa en una fase diferente del ataque.**
- **Todas las capas deben ser traspasadas para que el ataque tenga éxito.**

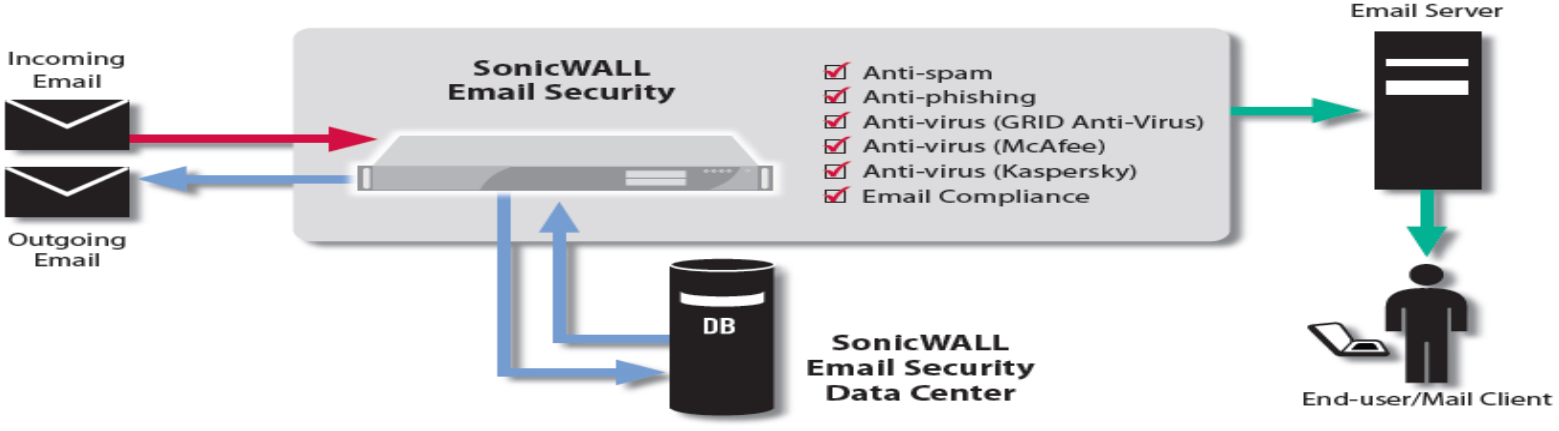
RESUMEN

- Educación y formación de los usuarios
- Mantener actualizados SO, Aplicaciones y Plug-ins
- Tener una estrategia de Backup
- **Seguridad basada en capas**

Seguridad basada en capas

Solución Antispam completa

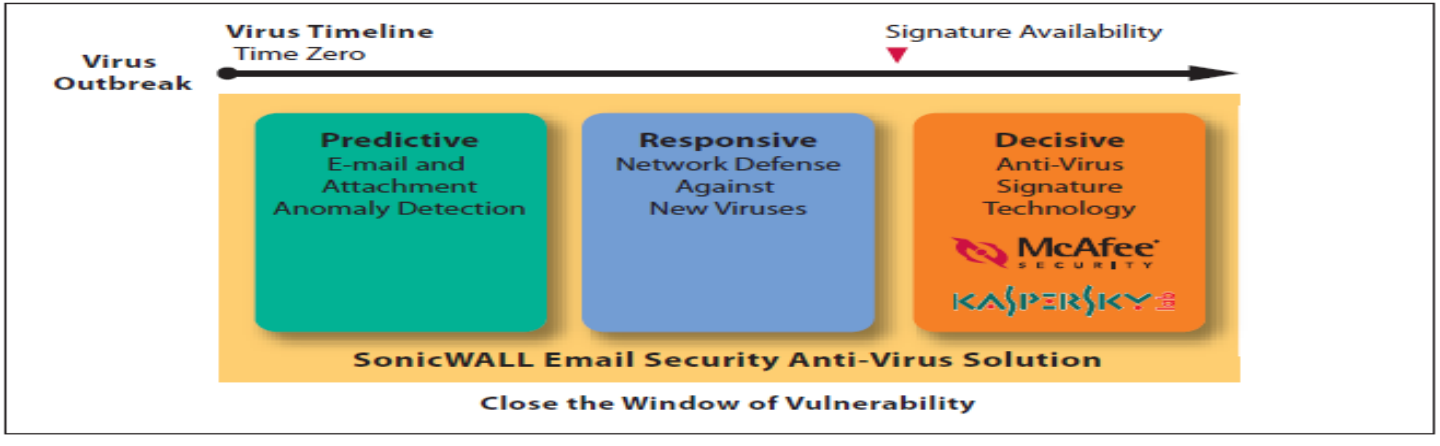
- Las técnicas de escaneo múltiples ofrecen una gran protección
- La tecnología de seguridad de Dell SonicWALL utiliza una combinación de diferentes técnicas para el análisis de correo orientadas a identificar las amenazas potenciales y ofrecer una protección mas robusta en tiempo real ante los ataques de **spam, malware, phishing, spoofing y zombi.**



Solución Antispam completa(cont.)

- Dell SonicWALL Email Security es la única solución de seguridad de correo electrónico **que integra múltiples tecnologías anti-virus**, como **Dell SonicWALL GRID Anti-Virus**, **McAfee, Kaspersky y Cyren**, proporcionando una protección superior a la de aquellas soluciones que se basan en una única tecnología antivirus.

- **La solución protege no sólo contra los virus conocidos, sino también de virus sospechosos.**



Sistema prevención intrusiones (IPS)

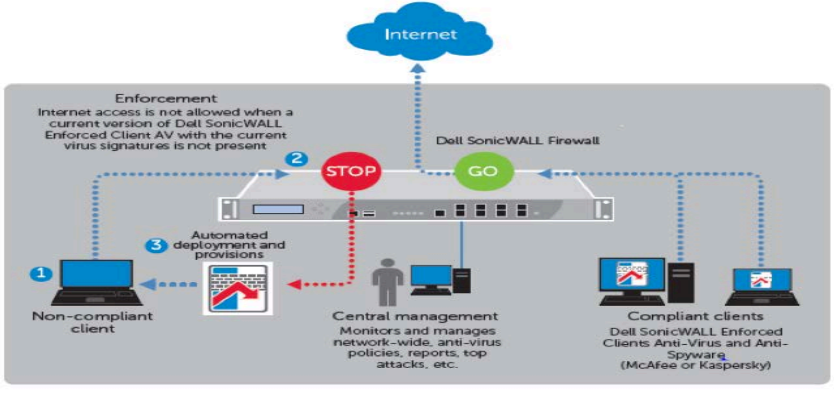
- **Capa Efectiva contra Drive-by-Downloads y Exploit Kits**.
- Es capaz de detectar exploits contra vulnerabilidades del sistema operativo, navegador y plugins del navegador.
- Algunas categorias de IPS relativas al ransomware son:
  - ActiveX
  - Backdoor
  - Bad-Files
  - Exploit
  - Exploit kits
  - Java
  - Virus
  - Web-Client
  - XSS

AntiVirus en el Gateway y en la nube

- El servicio **Cloud AV** nos permite aumentar el tamaño de la base de datos de malware (**casi 40 millones de firmas AV actualmente).**
- Cloud AV mejora los tiempos de respuesta. Las firmas basadas en la nube se generan tan pronto como se recibe una muestra maliciosa.
- Tenemos **nuestro propio equipo de investigación de amenazas.** Desarrollamos nuestras propias firmas basadas en nuestra propia investigación, no hay dependencias con terceras partes.
- Nuestro equipo de investigación de amenazas es activo en la comunidad de investigación de amenazas y colabora con los equipos de investigación líderes en el mundo.
- Recibimos **100.000 nuevas muestras de malware al día** y tenemos nuestra propia colección de muestras de malware.
- Las firmas se despliegan todos los días y **los firewalls actualizan la base de datos de firmas cada hora.**
- En el año **2015 se detectaron y bloquearon 8.190 millones de casos de propagación de malware y 2.070 millones prevenciones/día.**

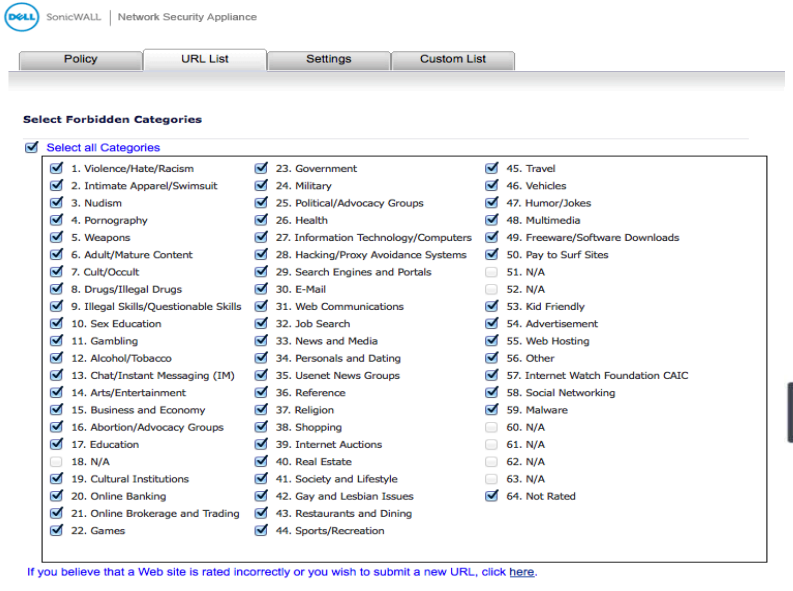
Antivirus Enforcement (Cliente)

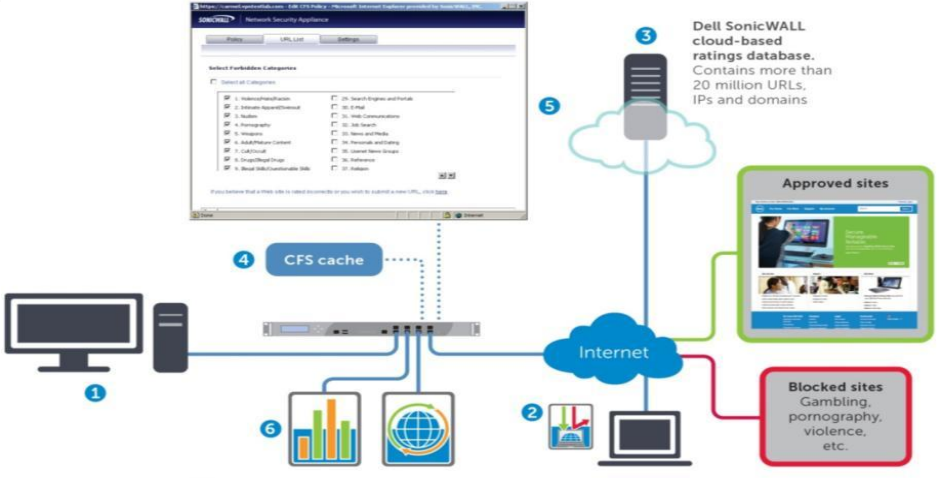
- **Verdadera segunda capa de protección AV** en el punto final (la puerta de enlace utiliza GRID AV).
- Dos sabores disponibles: **Kaspersky y/o McAfee**.
- **Gestión centralizada desde el Firewall**. Para navegar los clientes tienen que tener el Antivirus instalado y actualizado.
- **DDP/E (nuevo concepto revolucionario para protección AV del Endpoint)**



Content Filtering Service (CFS) y Client (CFC)

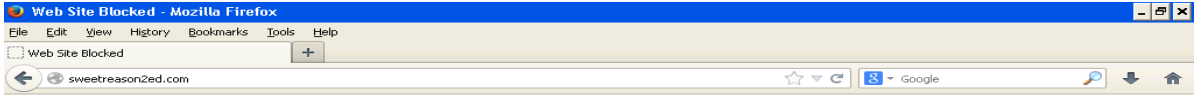
- **Capacidad de bloquear los sitios web peligrosos o de mala reputación, no sólo para los dispositivos detrás del firewall, sino también cuando están fuera del perímetro de la red.**

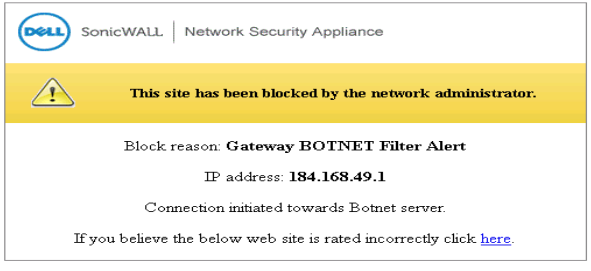




Anti-Botnet

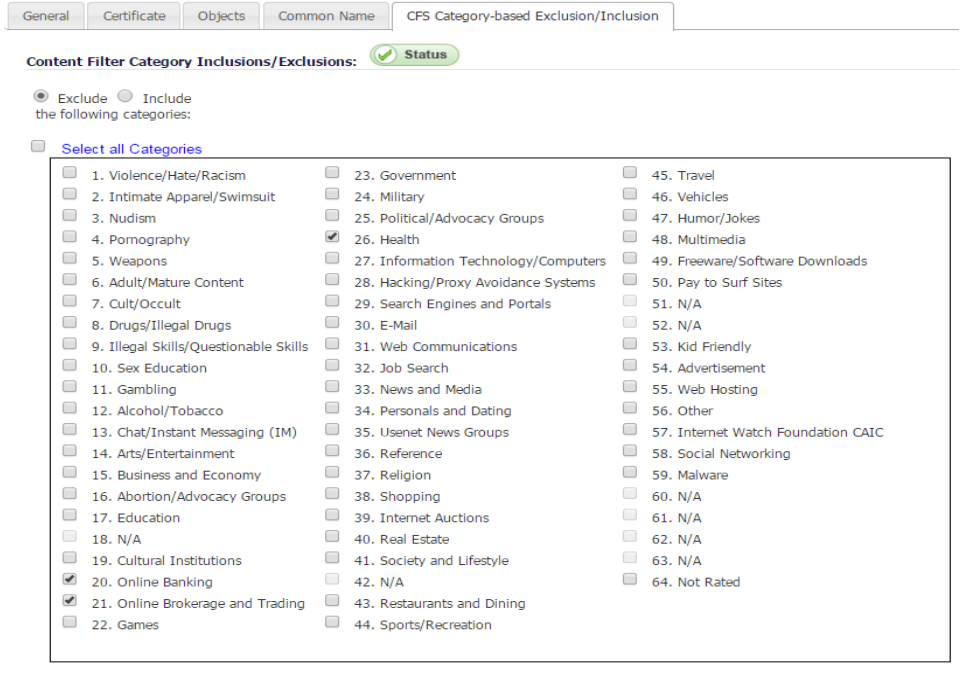
- Las botnets son difíciles de identificar y de controlar debido a la naturaleza transitoria de sus orígenes.
- El servicio Anti-Botnet proporciona una **defensa anti-evasiva y robusta** frente a la actividad maliciosa de las botnets, utilizando una **base de datos actualizada dinámicamente** para bloquear las conexiones a/desde servidores de C&C conocidos.





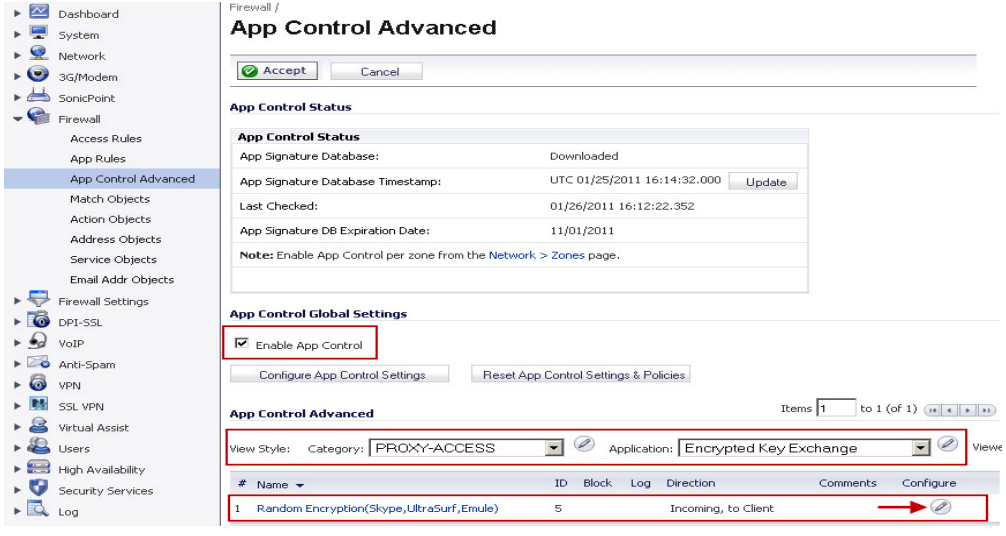
DPI-SSL

- Proporciona la capacidad de **inspecionar el tráfico cifrado con SSL** para detectar contenido malicioso o fugas de información.
- Mayor control granular y flexibilidad.



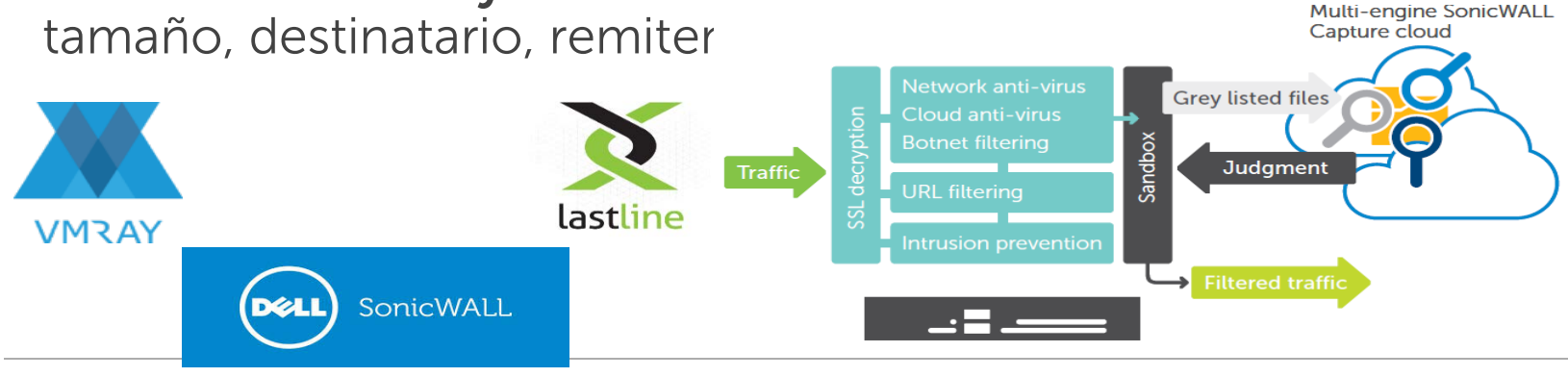
Control de Aplicaciones

- El servicio de Control de Aplicaciones proporciona una solución para la configuración de **políticas basadas en firmas de aplicación**.
- La función principal de esta herramienta de control de acceso en la capa de aplicación es la de **controlar la navegación, la transferencia de ficheros, correos, y adjuntos de correo**.



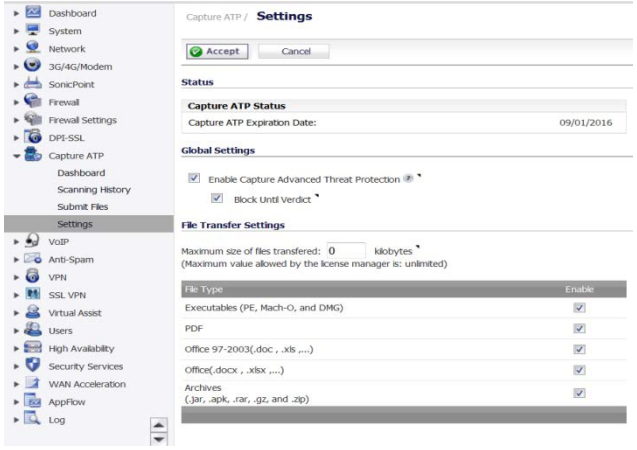
CAPTure - capa de seguridad adicional

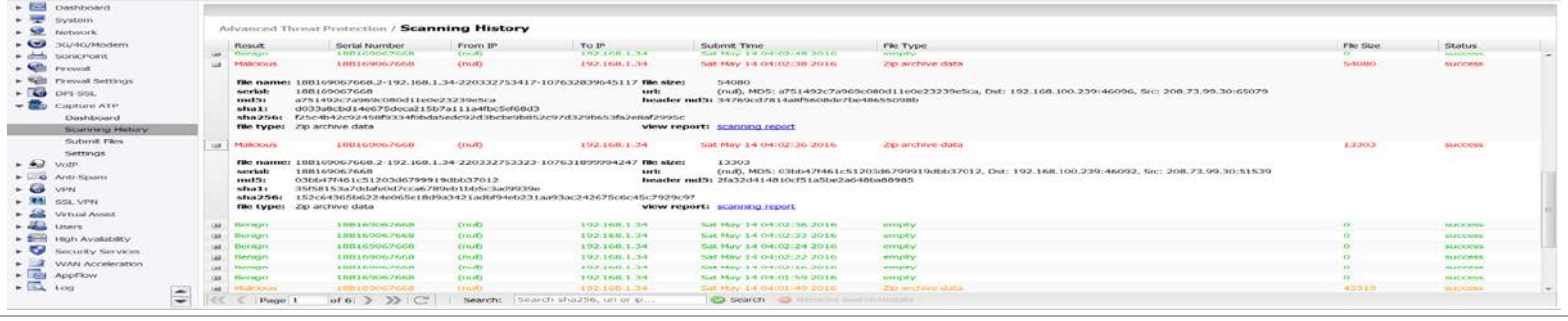
- **Análisis de amenazas avanzadas multi-motor**:
  - Sandbox Virtualizado (Dell Sonicwall).
  - Emulación completa del sistema (Lastline).
  - Análisis a nivel de Hypervisor (VMRay).
- **Amplio número de tipos de ficheros y entornos** que puede analizar:
  - PE, MS Office, PDF, JAR, APK.
  - Windows, Android y Mac OS.
  - Entornos multi-navegador.
- **Envío automático y manual de archivos** basado en tipos de fichero, tamaño, destinatario, remiter



CAPTure (cont.)

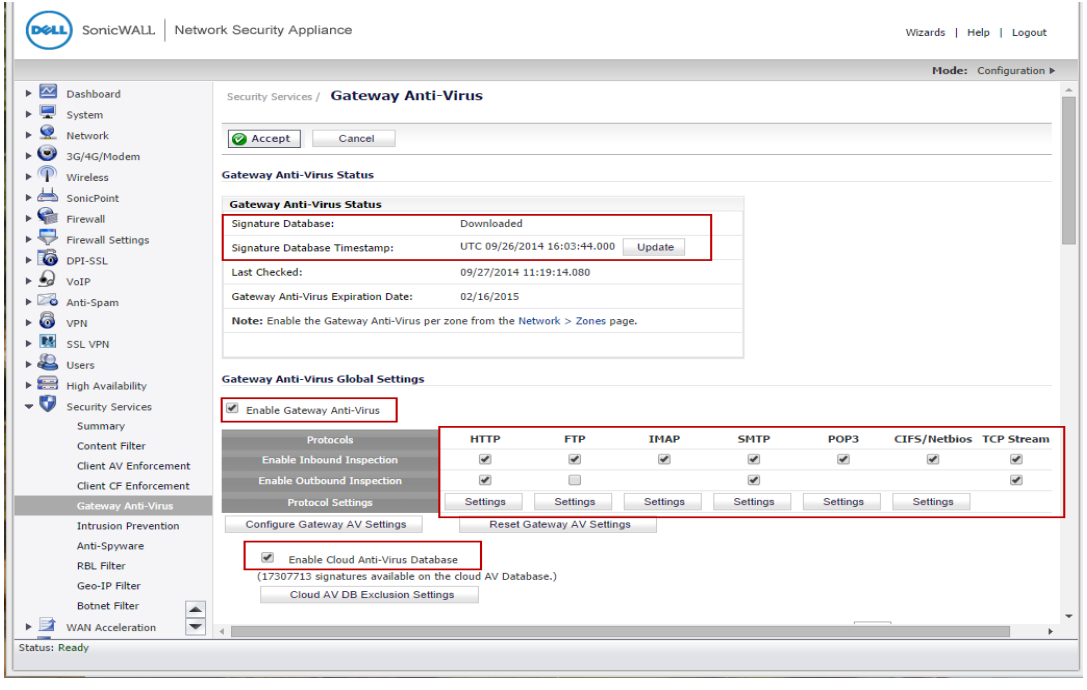
- **Bloquear hasta veredicto**
  - Retiene los ficheros en el gateway hasta que haya un veredicto para prevenir que los ficheros maliciosos entren en la red (parámetro configurable)
- **Rápido despliegue de nuevas firmas**
  - Firmas desplegadas inmediatamente a los dispositivos con el servicio SonicWALL Capture habilitado.
  - Firmas e información de las amenazas disponible a todos los firewalls en 48 hours





NGFW - Configuracion y Buenas Prácticas

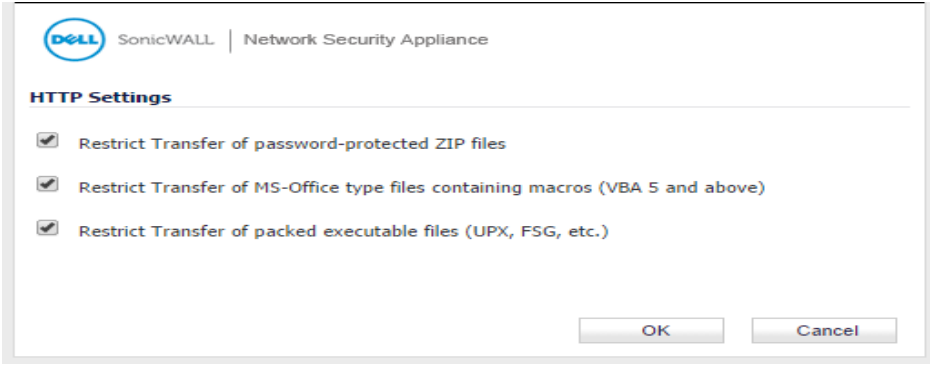
Recomendaciones para GAV



- **Asegúrate de que el servicio GAV está actualizado con las últimas firmas.**
- **Habilita GAV && Cloud AV**
- **Habilita la inspección Entrante y Saliente de HTTP, FTP, IMAP, SMTP, POP3, CIFS/Netbios y TCP Stream.**

Recomendaciones para GAV (cont.)

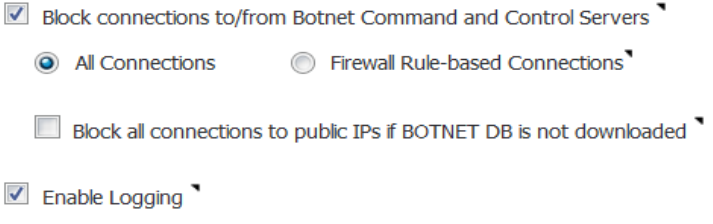
- Habilita GAV en todas las zonas internas y externas (**Network → Zones**)
- Bajo la configuración de cada protocolo (HTTP, etc.), habilita las siguientes opciones:
  - Restrict Transfer of password-protected ZIP files
  - Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)
  - Restrict Transfer of packed executable files (UPX, FSG, etc.)



Recomendaciones para IPS && Anti-Botnet

- **Intrusion Prevention Service (IPS):**
  - Asegúrate de que el IPS está actualizado con las últimas firmas.
  - Habilita la prevención de los ataques de riesgo Alto y Medio. Esto incluirá automáticamente las firmas contra este tipo de malware
  - **Habilita IPS en todas las zonas internas y externas**.

- **Botnet Filter:**
  - En la página Security Services → Botnet Filter, habilita la opción **"Block connections to/from Botnet** Command and Control Servers"
  - Habilita la opción de "**Enable Logging**"

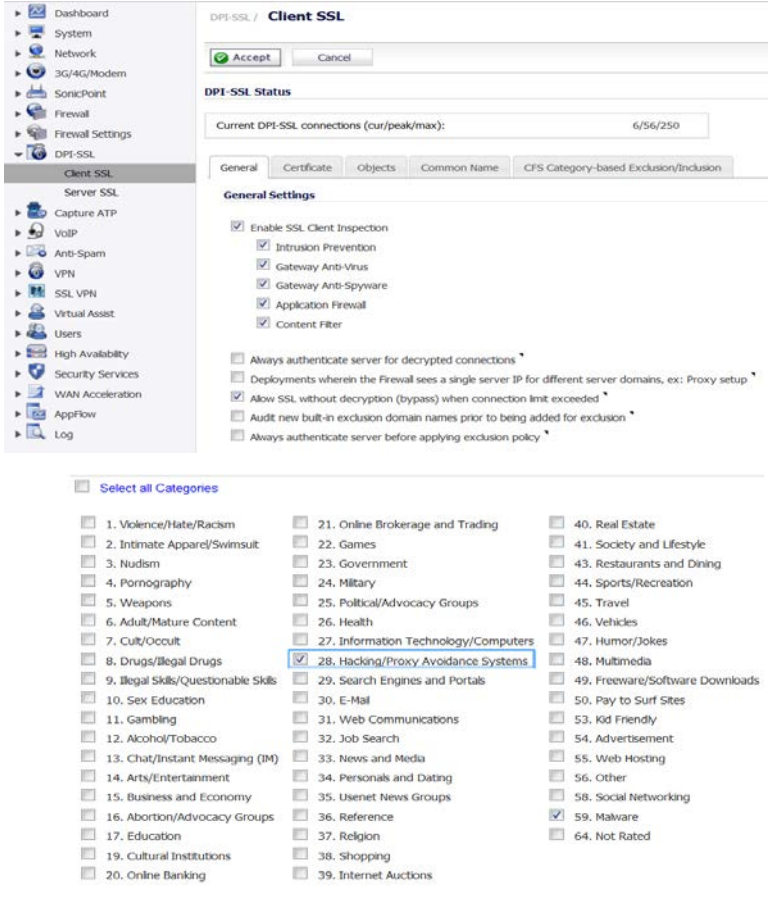


Recomendaciones para App Control

- Habilita las opciones de **Block y Log para las aplicaciones TOR e I2P** (Firewall → App Control Advanced, Categoría PROXY-ACCESS).
- Algunas firmas de TOR/I2P requerirán que se **bloquee también las firmas Encrypted Key Exchange (SIDs 5 & 7).**
  - Encrypted Key Exchange (SID 5) -- Random Encryption (Skype,UltraSurf,Emule)
  - Encrypted Key Exchange (SID 7) -- UDP Random Encryption(UltraSurf)
  - Tor (SID 3154) -- Client Activity 1
  - Tor (SID 3155) -- Client Activity 2
  - Tor (SID 7344) -- Client Activity 3
  - Tor (SID 8617) -- Client Activity 4
  - Tor (SID 3584) -- Client Activity 5
  - Tor (SID 10318) -- Client Activity 6
  - Tor (SID 10443) -- Client Activity 7
  - Tor (SID 3156) -- Inbound Activity
  - I2P (SID 10817) -- HTTP Proxy Access 1 [Reqs SID 5 & 7]
  - I2P (SID 10820) -- HTTP Proxy Access 2 [Reqs SID 5 & 7]
  - I2P (SID 10821) -- HTTP Proxy Access 3 [Reqs SID 5 & 7]

Recomendaciones para DPI-SSL && CFS

- En el menú DPI-SSL → Client SSL, habilita la opción de "**Enable SSL Client Inspection**", y también los servicios Gateway Anti-virus, Intrusion Prevention, AntiSpyware, App Firewall y Content Filtering.
- Habilita el servicio CFS y configúralo para bloquear las categorías **"Malware" y "Hacking/Proxy Avoidance Systems".**



Conclusiones

Conclusiones Finales

- **Estar protegido con garantias al 100% es una utopia.**
- Las recomendaciones de seguridad y las buenas prácticas **minimizan las posibilidades de sufrir un incidente de seguridad** y los problemas asociados con ella.
- Incluso aplicando todas las recomendaciones de seguridad y buenas prácticas, no estarás completamente protegido .... Pero en realidad nunca lo has estado.
- La seguridad ofensiva siempre va un paso por delante de la seguridad defensiva.
- Los cibercriminales normalmente tratan de explotar el eslabón más débil, por lo que es fundamental educar y formar a los usuarios, ya que son normalmente el principal objetivo.
- **No confíe en los que afirman que pueden lograr una protección del 100%, están mintiendo**.
- Los clientes normalmente son conscientes sólo del ransomware que ha comprometido sus sistemas, **pero no de todos los intentos anteriores que fueron bloqueados con éxito**.

Referencias

Referencias

- https://www.sonicwall.com/whitepaper/2016-dell-security-annual-threat-report8107907
- http://www.icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report.pdf
- https://blog.knowbe4.com/a-short-history-evolution-of-ransomware
- https://support.software.dell.com/kb/sw12434