Bichos ..

IRIS-CERT, Depto RedIRIS . Red.es

Grupos de Trabajo . Logroño, 24/10/2005

La idea de mwcollect cambia de nombre.....

BICHOS

BICHOS

Puede ser: “Basic Information Collector of Harmful ObjectS”, o bien “Backbone Information Collector of Harmful Objects”, se admiten sugerencias ;-)

En pocas palabras: Capturar los “bichos” antes de que infecten equipos de la red académica y coordinar a nivel internacional la eliminación de estos bichos.

- Mejorar la detección de bots y gusanos sabiendo cuales son los más difundidos.
- Detección de direcciones IP externas que se encuentren realizando ataques a sistemas internos.
- Poder analizar los bots de forma rápida para determinar las características más importantes de estos.
  - Servidor, puerto, claves de control, ...
  - Desactivación de las botnets y detección del origen del ataque

La “B” por Backbone

En el Troncal de RedIRIS se están aplicando una serie de filtros:

- Puertos de MS-DS (445/TCP)
- NetBIOS Tradicional (139/TCP), 138/TCP, etc...

En vez de ser filtrado (basura) el tráfico es reenviado a un equipo central que:

- Contabiliza el número de intentos de conexión
- Dispone de un sistema trampa de baja interacción (mwcollect) para cargar simular un sistema vulnerable.
- Se procesa y descargar el gusano/bots

Estadísticas sobre el número de conexiones que se rechazan en el backbone.

La "I" por Información

La información recopilada permite:

- Conocer cuales son los espécimenes que están "en estado salvaje" en estos momentos atacando nuestras redes.
- Promediar el número de nuevos "bichos" que aparecen.
- Detectar cuales son los ataques concretos que más se están realizando en un momento dado.
- Responder ante el ataque, contacto con las redes origen de los escaneos

La “C” por colector

Desde Marzo de esta año han empezado a desarrollarse “máquinas trampas de baja interacción”.

- No simulan un sistema Operativo, sino solamente un servicio.
- Responden ante ataques automáticos, no ante intrusiones “humanas”
- Ideales para la captura de “gusanos y bots”

Tres programas:

- Mwcollect, www.mwcollect.org El primero que surgio, C++ , Linux/ Windows
- Multipot, http://www.idefense.com/iia/labs-software.php?show=9 , Windows
- Nepenthes, www.nephentes.org , Más completo, C++ .

La "H", dañinos ...

No se procesan las conexiones "por error"

Solo procesan conexiones a nivel de protocolo malformadas que tengan como objetivo un buffer overflow o exploit

- Permiten detectar conexiones "no reconocidos", nuevos vectores de exploit y shellcodes

Analizan el código inyectado por el atacante para determinar si se esta forzando la descarga o ejecución de un fichero

- Igualmente permite detectar nuevos shellcodes que no sean los habituales.

Descargan el fichero, pero no lo analizan.

La "O", programas

Los programas descargados suelen ser los ejecutables que después podemos encontrar en máquinas infectadas.

Gran parte de estos ejecutables no se pueden analizar directamente:

- Cifrados con dos o más "empaquetadores" distintos para reducir su tamaño y reducir la probabilidad de detección por antivirus.
- Muchas veces el algoritmo de cifrado ha sido modificado para evitar su detección por el motor de antivirus.

Se pueden emplear técnicas de análisis de binarios para detectar la información más importante:

- Equipo de control
- Opciones que llevan incorporado, ataques, etc.

La “S” por Plural

Al recibir todo el tráfico del Troncal el número de conexiones es demasiado elevado, para que la aplicación pueda procesar todas las conexiones.

- Todos los paquetes TCP/SYN de inicio son recibidos por el equipo y enviados a syslog.
- Limitado el número de paquetes TCP/SYN que se aceptan y que vía NAT Inverso llegan a la aplicación. (200 pqts/min)
- La aplicación solo procesa aquellos ataques ante los cuales tiene un analizador reconocido, descartando el resto.

Los binarios serán distribuidos a grupos de seguridad, firmas antivirus, etc para su análisis.

Resultados hasta ahora

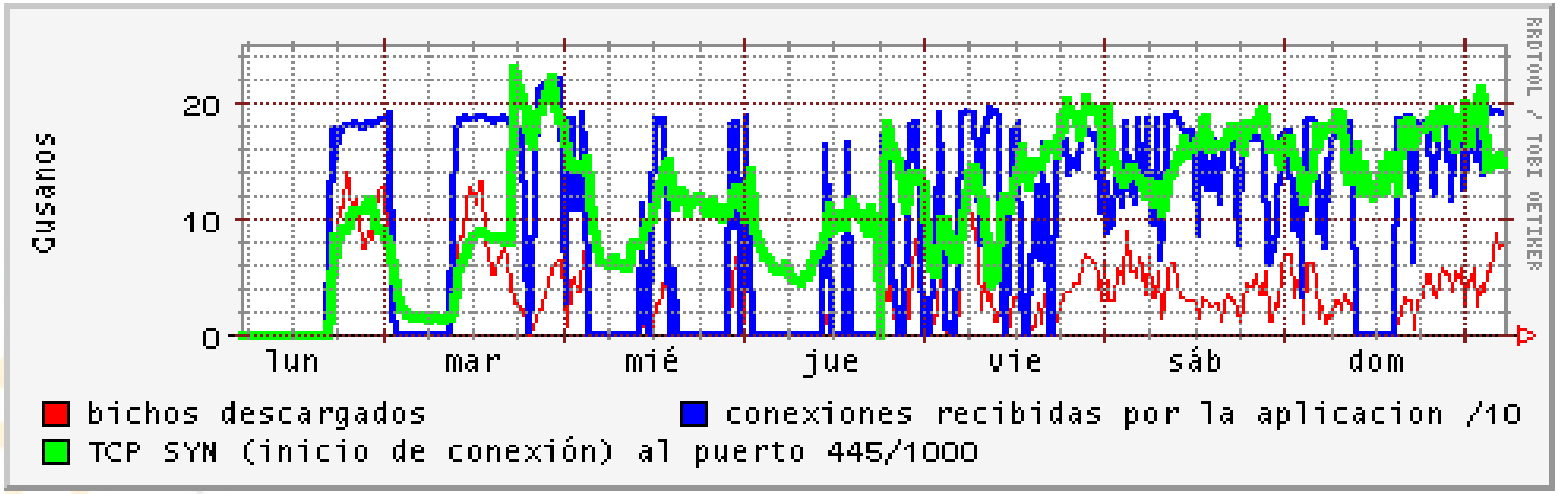
Pruebas de los tres colectores:

- **Mwcollect: realizado un paquete rpm de instalación, en la instalación inicial "muere" algunas veces por exceso de tráfico, pocos patrones de ataques reconocidos.**

- **Multipot: Escrito en Visual Basic, no funciona fuera de Windows, en pruebas en una conexión domestica presenta problemas en algunos ataques, incorpora algunos ataques no NetBIOS/Microsoft, como Veritas**

- **Nepenthes: Parece ser el más activo últimamente, incorporar vulnerabilidades de diversos servicios, requiere una versión actualizada de Linux , probado solamente en conexión domestica.**

Tráfico detectado por minutos



Las lineas no están a escala:

- Las conexiones están en escala 1:1000
- La linea azul indica la “estabilidad” de la aplicación sometida a un tráfico de 200 conexiones /min
- La linea roja indica la efectividad “bichos” descargados.

Trabajo en progreso

Trafico detectado:

- Procesamiento del tráfico para comprobar las direcciones origen de los ataques.
- Envío a sistemas automáticos para la distribución a los ISP
- Estadísticas de efectividad de estas medidas.

Recolección de malware:

- Scripts de procesamiento de logs y envío de nuevos especimenes para su estudio.
  - Uso de PGP para el envío cifrado y evitar así los antivirus.
  - Procesamiento automático de los mensajes para su almacenaje y estadísticas.

Trabajo en Progreso (II)

Documentación de las técnicas de análisis de binarios para el estudio de los nuevos espécimenes.

- Colaboración entre diversos grupos de seguridad.
- Material práctico “Hand-on”
- Prevista una versión preliminar para los próximos grupos de trabajo.

Recolectores de binarios.

- Finalizar el empaquetamiento (rpm) de los programas
- Documentar su uso y configuración
- Colaboración en el análisis de nuevos ataques y su integración en estos recolectores

Vias Futuras

Migración del sistema:

- Pentium Celerom 600Mz 256 Mb RAM.
- Sistema operativo Antiguo
- Prueba de nepenthes en el troncal

Colaboración con otras iniciativas:

- Pruebas de porcentajes de detección con diversos antivirus.
- Envío de las muestras a otros equipos para su análisis

Vias Futuras

Captura de otros tráficos dañinos.

- Resto de puertos NetBIOS filtrados
- Puertos que se indiquen.
- Posibilidad de instalación de colectores en Universidades para la captura de ataques de protocolos no filtrados en el troncal.
  - HTTP
  - SMPT
  - SSH
- Captura de tráfico en direccionamiento sin uso para simular servicios los servicios en general.

Vias Futuras

Passive DNS Replication

http://www.enyo.de/fw/software/dnslogger/

- Base de datos con información sobre como varían los dominios a lo largo del tiempo.
- Permite detectar los ataques de phising y otros tipos de cambios “no autorizados” de DNS

Se clonaría el tráfico de DNS que sería procesado de forma independiente por el replicador, guardando información sobre como ha variado un dominio a lo largo del tiempo.

red.es

Red IRIS

¿ Preguntas ?

red.es