

Seguridad y Privacidad en Redes

SNIFFERS



¿Qué son los sniffers?

- ✓ Un sniffer es un “capturador” de tráfico de red.
- ✓ Pueden utilizarse:
 - ✓ Como una herramienta que facilita el mantenimiento de las redes (analizador de protocolos).
 - ✓ Con fines de “espionaje”
- ✓ Aprovechan:
 - ✓ Que las redes de área local utilizan medios compartidos
 - ✓ El comportamiento de algunos protocolos de red



Sniffers -Conceptos

- ✓ Modo promiscuo:
 - ✓ Es un modo de recepción especial que implica que el adaptador recibirá todas las tramas que viajen por el medio y no sólo las que van dirigidas a ese adaptador.
 - ✓ Esta funcionalidad es usada por los agentes de monitoreo de tráfico o sniffers.



Conceptos relacionados (cont)

- ✓ Modo promiscuo:
 - ✓ Algunos drivers permiten habilitar este modo.
- ✓ ¿Cómo detectarlo?
 - ✓ En algunos SO UNIX-like (Ifconfig)
 - ✓ En un SO Windows (Antisniffers)



Sniffers en redes switcheadas

- ✓ En un ambiente no switcheadado, cuando un nodo transmite, las tramas viajan por el medio compartido y son “vistas” por todos los nodos que forman parte del segmento
- ✓ Un switch divide dominios de colisión: un segmento está conformado por el nodo y el puerto del switch al que dicho nodo está conectado.



¿Es posible sniffear una red switchcada?



Sniffers en redes switcheadas

- ✓ Algunas técnicas usadas en redes con switches:
 - ✓ Switch Jamming
 - ✓ ICMP Redirect
 - ✓ ICMP Router Advertisements
 - ✓ ARP Spoofing al switch
 - ✓ ARP Redirect o Spoofing al cliente
 - ✓ Aprovechar el puerto de monitoreo en el switch
 - ✓ Cable-taps/Hubs
 - ✓ DHCP spoofing



Ejemplos de herramientas

- ✓ Algunas herramientas que implementan sniffers:
 - ✓ Etherpeek
 - ✓ Wireshark (nuevo nombre del proyecto Ethereal)
 - ✓ Tcpdump
 - ✓ Ettercap



Sniffers-Etherpeek

- ✓ Analizador de protocolos que constituye una poderosa herramienta de monitoreo y permite decodificar tramas en tiempo real, durante la captura.
- ✓ Algunas de las funcionalidades que el mismo provee:
 - ✓ Permite realizar y guardar capturas en distintos formatos.
 - ✓ Muestra el contenido de los paquetes de forma tal que resulta sencillo interpretar la información que los mismos transportan
 - ✓ Permite definir filtros para realizar la captura.
 - ✓ Permite simular el envío de paquetes cuyo contenido puede modificarse.

<http://www.wildpackets.com/>





Sniffers-Etherpeek

Interfaz de la herramienta

EtherPeek Demo - [Capture 1]

File Edit View Capture Send Monitor Tools Window Help

Packets received: 19 Memory usage: 0% Filter state: Accept all packets Start Capture

Packets filtered: 19

Packet	Source	Destination	Flags	Size	Delta Time	Protocol	Summary
1	Compaq:01:0F:70	Ethernet Broadcast		64		ARP Request	163.10.10.13 = ?
2	3com:A0:4F:8C	Ethernet Broadcast		64	4,058012	ARP Request	163.10.10.30 = ?
3	Kingston Tech:6A:E...	Ethernet Broadcast		64	0,594186	ARP Request	163.10.10.14 = ?
4	Asiarockorporation:...	Kingston Tech:6A:E...		64	0,000139	ARP Response	Asiarockorporation:39:7E:79 = 16...
5	IP-163.10.10.3	IP-163.10.10.14		78	0,000017	PING Req	Echo: 163.10.10.14
6	IP-163.10.10.14	IP-163.10.10.3		78	0,000139	PING Reply	Echo Reply: 163.10.10.3
7	3com:A0:4F:8C	Ethernet Broadcast		64	0,397401	ARP Request	163.10.10.30 = ?
8	IP-163.10.10.3	IP-163.10.10.14		78	0,596639	PING Req	Echo: 163.10.10.14
9	IP-163.10.10.14	IP-163.10.10.3		78	0,000128	PING Reply	Echo Reply: 163.10.10.3
10	Cisco:AF:4B:EE	01:00:0C:CC:CC:CC	*	328	0,224673	Discovery	
11	Cisco:AF:4B:EF	01:00:0C:CC:CC:CC	*	328	0,001380	Discovery	
12	3com:A0:4F:8C	Ethernet Broadcast		64	0,177191	ARP Request	163.10.10.30 = ?
13	IP-163.10.10.58	IP-163.10.10.63		96	0,394281	NB Name Svc	C QUERY NAME=NEPTUNO.LINTI <20> ...
14	Asustek Computer:7...	Ethernet Broadcast		64	0,001238	ARP Request	163.10.10.2 = ?
15	IP-163.10.10.3	IP-163.10.10.14		78	0,208688	PING Req	Echo: 163.10.10.14
16	IP-163.10.10.14	IP-163.10.10.3		78	0,000124	PING Reply	Echo Reply: 163.10.10.3
17	IP-163.10.10.58	IP-163.10.10.63		96	0,539051	NB Name Svc	C QUERY NAME=NEPTUNO.LINTI <20> ...
18	IP-163.10.10.3	IP-163.10.10.14		78	0,456172	PING Req	Echo: 163.10.10.14
19	IP-163.10.10.14	IP-163.10.10.3		78	0,000131	PING Reply	Echo Reply: 163.10.10.3

Packets / Nodes / Protocols / Summary / Graphs / Conversations / Log / Filters

Idle Conexión de área local Packets: 19 Duration: 00:00:10

Network Statistics

Gauge Value

utilization 60 70 80 90 100

packets/s 1K 10K 100K

errors/s 10 100 1000

Messages: 61 60 0 1 0

Date	Time	Message
13/09/2004	18:35:40	http://www.ossim.net/images/es/ossim.6.jpg from 163.10.10.3
13/09/2004	18:35:41	http://www.ossim.net/images/es/ossim.7.jpg from 163.10.10.3
13/09/2004	18:37:19	EtherPeek Demo quit
15/09/2004	17:29:56	EtherPeek Demo started
15/09/2004	17:32:03	New capture

For Help, press F1

Conexión de área local

Paquetes capturados



Sniffers-Etherpeek

Capture 1 - Packet #15

Packet: 15 [X]

Info: F=0x00000000 S=0x00000000 L=78 T=17:32:17.846101600 09/15/2004

- Ethernet Header**
 - Destination: 00:0B:6A:39:7E:79 *Asiarockorporation:39:7E:79*
 - Source: 00:C0:F0:6A:E0:A4 *Kingston Tech:6A:E0:A4*
 - Protocol Type: 0x0800 *IP*
- IP Header - Internet Protocol Datagram**
 - Version: 4
 - Header Length: 5 (20 bytes)
 - Differentiated Services=00000000
 - Total Length: 60
 - Identifier: 33658
 - Fragmentation Flags=000
 - Fragment Offset: 0 (0 bytes)
 - Time To Live: 128
 - Protocol: 1 *ICMP - Internet Control Message Protocol*
 - Header Checksum: 0x5D21
 - Source IP Address: 163.10.10.3
 - Dest. IP Address: 163.10.10.14
- ICMP - Internet Control Messages Protocol**
 - ICMP Type: 8 *Echo Request*
 - ICMP Code: 0
 - ICMP Checksum: 0x3A5C
 - Identifier: 0x0200
 - Sequence Number: 0x0011
 - ICMP Data Area: (32 bytes)
- FCS - Frame Check Sequence**
 - FCS: 0x0B52AE24 *Calculated*

0000:	00 0B 6A 39 7E 79 00 C0 F0 6A E0 A4 08 00 45 00 00 3C 83 7A 00 00 01 5D 21 A3 0A 0A	..j9~y...j....E...<.z....}!...
0029:	03 A3 0A 0A 0E 08 00 3A 5C 02 00 11 00 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70\....abcdefghijklmnopqrstuvwxyz
0058:	71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 00 00 00 00	qrstuvwabcdefghi....

Contenido de uno de los paquetes capturados

Muestra el contenido en ASCII





Sniffers – Wireshark

- ✓ Es una herramienta similar al Etherpeek, que corre en plataformas Unix y Windows.
- ✓ Es opensource. Conocido anteriormente como Ethereal.
- ✓ Difiere en la interfaz que provee y en algunos aspectos relacionados con la funcionalidad de la herramienta.

<http://www.wireshark.org>



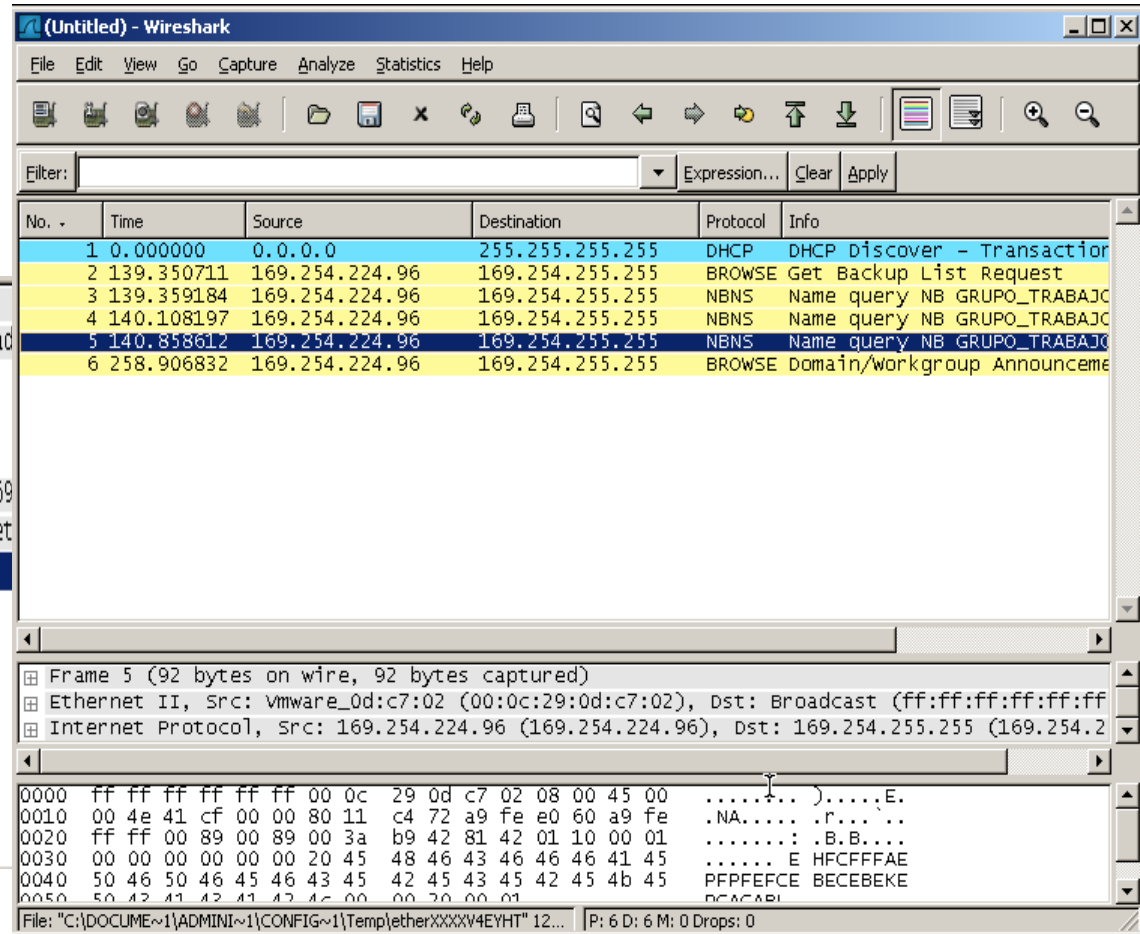


Sniffers – Wireshark

Interfaz de la herramienta

Contenido de uno de los paquetes capturados

Frame 5 (92 bytes on wire, 92 bytes captured)
 Ethernet II, Src: Vmware_0d:c7:02 (00:0c:29:0d:c7:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 Source: Vmware_0d:c7:02 (00:0c:29:0d:c7:02)
 Type: IP (0x0800)
 Internet Protocol, Src: 169.254.224.96 (169.254.224.96), Dst: 169.254.255.255 (169.254.255.255)
 User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
 NetBIOS Name Service
 Transaction ID: 0x8142
 Flags: 0x0110 (Name query)
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries



Sniffers – Wireshark

¿Vemos una DEMO?



Sniffers – Tcpdump

- ✓ Es una herramienta de monitoreo de tráfico orientada a comandos que permite especificar expresiones regulares para definir el tráfico a capturar
- ✓ Ej: `tcpdump -X host 163.10.5.66`
`tcpdump -i eth0 port 80`

<http://www.tcpdump.org>



Sniffers – Ettercap

- ✓ Es un sniffer multipropósito que permite realizar ataques de “man in the middle” (Mitm).
- ✓ Es opensource.
- ✓ Corre sobre plataformas Windows y Linux.
- ✓ Permite sniffear en redes switcheadas.

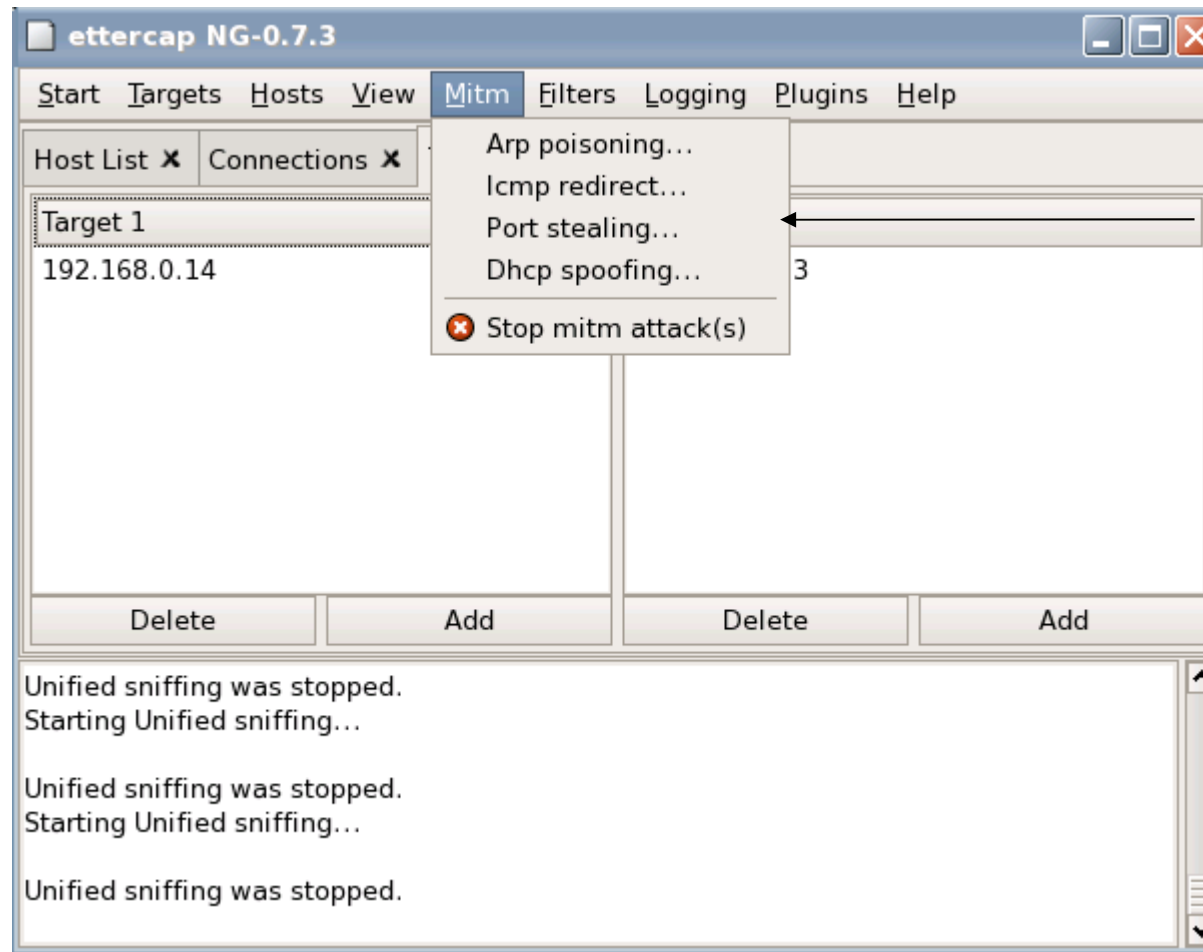
<http://ettercap.sourceforge.net/>



Sniffers – Ettercap

Interfaz de la herramienta

Hosts a sniffear →



Técnicas para sniffear en redes switcheadas

Sniffers – Ettercap

¿Vemos una DEMO?



Sniffers de propósitos específicos

- ✓ Para snifear mensajería instantánea:
 - ✓ Aimsniff [<http://www.aimsniiff.com/>]
 - ✓ Imsniff []
- ✓ Para snifear imágenes
 - Driftnet [<http://sourceforge.net/projects/im-sniif/>]
- ✓ Tráfico SSL:
 - ✓ SSLSniff
[<http://www.thoughtcrime.org/software/sslsniff/>]
- ✓ Tráfico Wireless:
 - ✓ Kismet [<http://www.kismetwireless.net>]
 - ✓ AirPcap [<http://www.wireshark.org>]



Sniffers – Más herramientas y urls

Otras herramientas

- ✓ Cain and Abel [<http://www.oxidit.it/cain.html>]
- ✓ Dsniff [<http://www.monkey.org/~dugsong/dsniff/>]
- ✓ Ngrep [<http://www.packetfactory.net/projects/ngrep/>]
- ✓ Snoop [<http://www.spitzner.net/snoop.html>]



DETECCIÓN DE SNIFFERS



¿Cómo se detectan los Sniffers?

- ✓ Si bien en teoría se dice que es imposible detectarlos, debido a que son pasivos (sólo monitorean el tráfico, no transmiten nada), a veces en la práctica es posible detectarlos.
- ✓ Existe una serie de métodos que hacen posible la detección de los sniffers.



Métodos de detección de sniffers

- ✓ Ping method
- ✓ ARP method
- ✓ DNS method
- ✓ Decoy method
- ✓ Host method
- ✓ Latency method



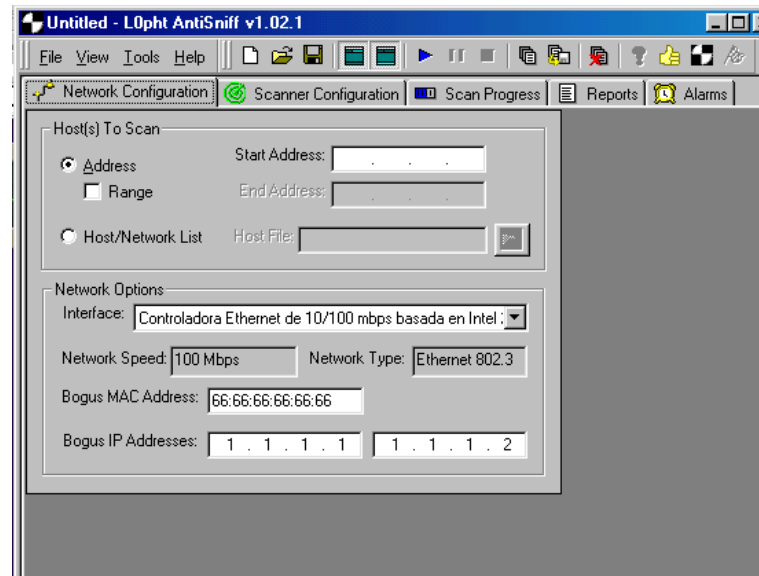
Métodos de detección de sniffers

- ✓ Existen herramientas que realizan esta tarea basándose en los métodos anteriormente mencionados.
- ✓ Otras herramientas permiten generar paquetes de modo tal de permitirnos poner en marcha alguno de los métodos en cuestión.



Algunos ejemplos

✓ Antisniff



- ✓ PMD: promiscuous mode detector
- ✓ Etherpeek, Nemesis u otra herramienta para generar paquetes
- ✓ Sniffdet [<http://sniffdet.sourceforge.net/index.html>]

Otras formas de obtener Información

Keyloggers

Registran las pulsaciones de teclado realizadas por un usuario, guardándolas en un archivo o enviándolas a través de Internet, por ejemplo por email.

Pueden ser:

- ✓ De software (PC Spy Keylogger, Pykeylogger, etc)

- ✓ De hardware



Otras formas de obtener Información

Keyloggers de software:

Extienden el concepto, permiten no sólo almacenar las teclas pulsadas por el usuario, sino también tomar imágenes de pantallas, eventos del mouse, etc.

¿Cómo se distribuyen?

- ✓ A través de un **troyano** o como parte de un **virus informático** o **gusano informático**.
- ✓ En general se puede decir que pueden adjuntarse a un archivo cualquiera.

¿Cómo se evitan o previenen?

- ✓ Antivirus actualizados constantemente
- ✓ Firewalls personales configurados advirtiendo tráfico saliente



Keyloggers

¿Vemos una DEMO?



Otras formas de obtener Información

Mucho más importante que antivirus y firewalls



Concientización del Usuario

- Evitar abrir sobre adjuntos u archivos no solicitados o esperados, sobre todo nunca utilizando usuarios permisos de administrador o super usuario.
- Evitar utilizar el equipo como super usuario, restringirlo a los casos necesarios únicamente .

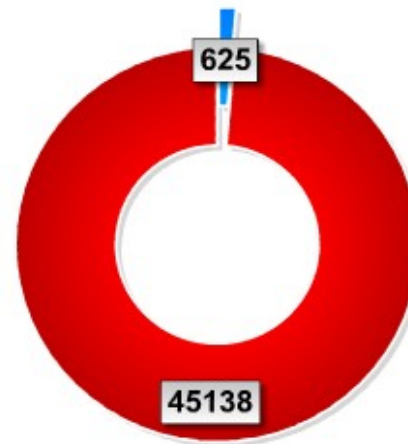


Otras formas de obtener Información

¿Porqué no confiar plenamente en mi antivirus?

Según Virus Total el 24/10/08 a las 00:40 hs :

Failures in Detection (Last 24 Hours)



Red: Infected files which one or more antivirus engines failed to detect as a threat.

Blue: Infected files detected by all antivirus engines.

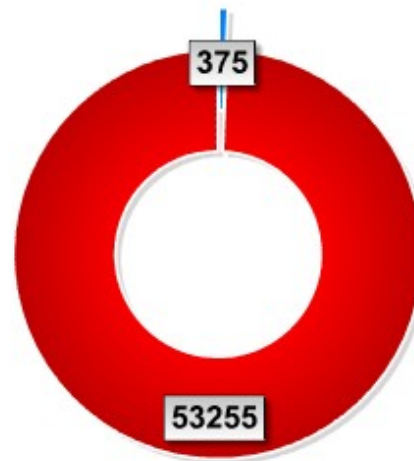


Otras formas de obtener Información

Datos publicados al 20-10-09...

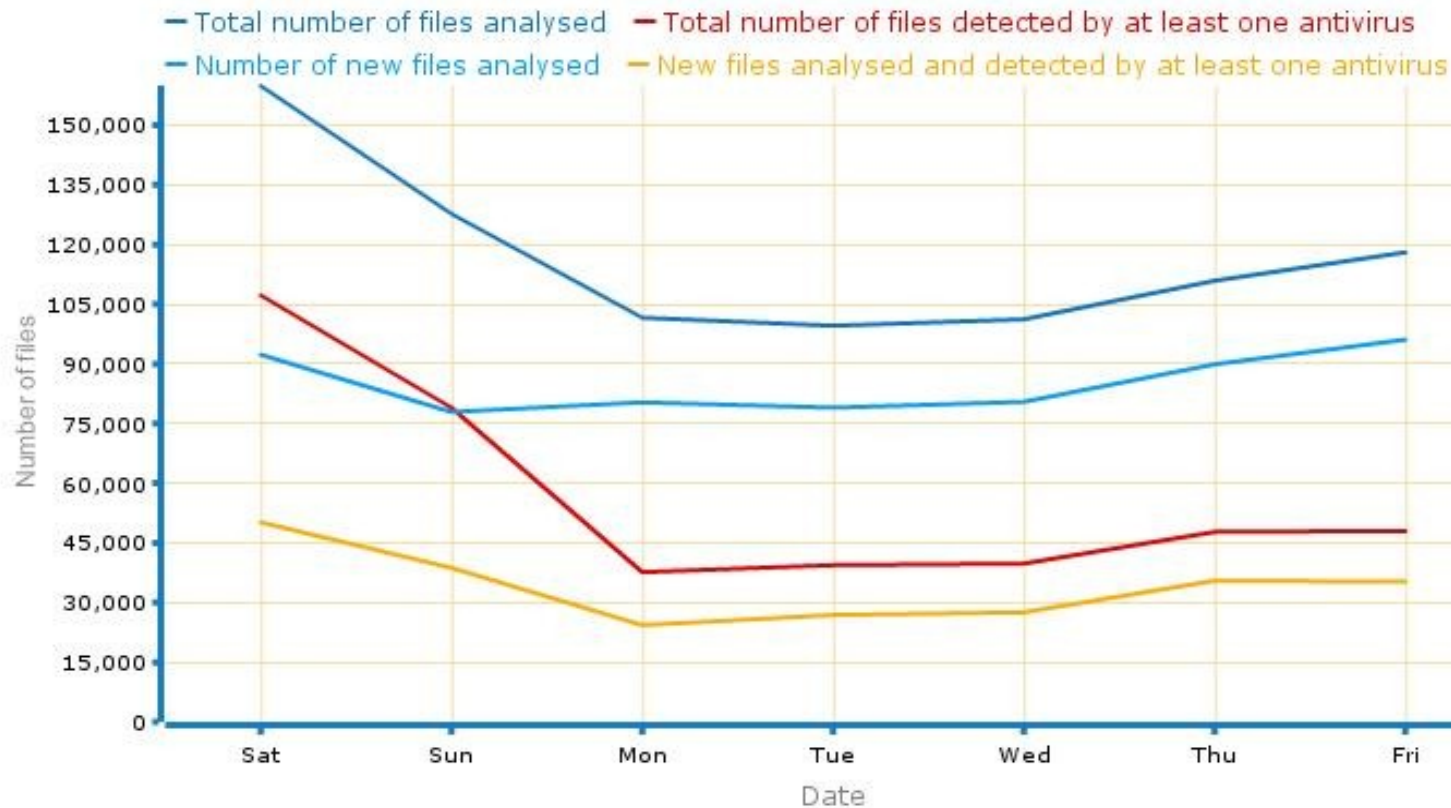
Red: Infected files which one or more antivirus engines failed to detect as a threat.

Blue: Infected files detected by all antivirus engines.



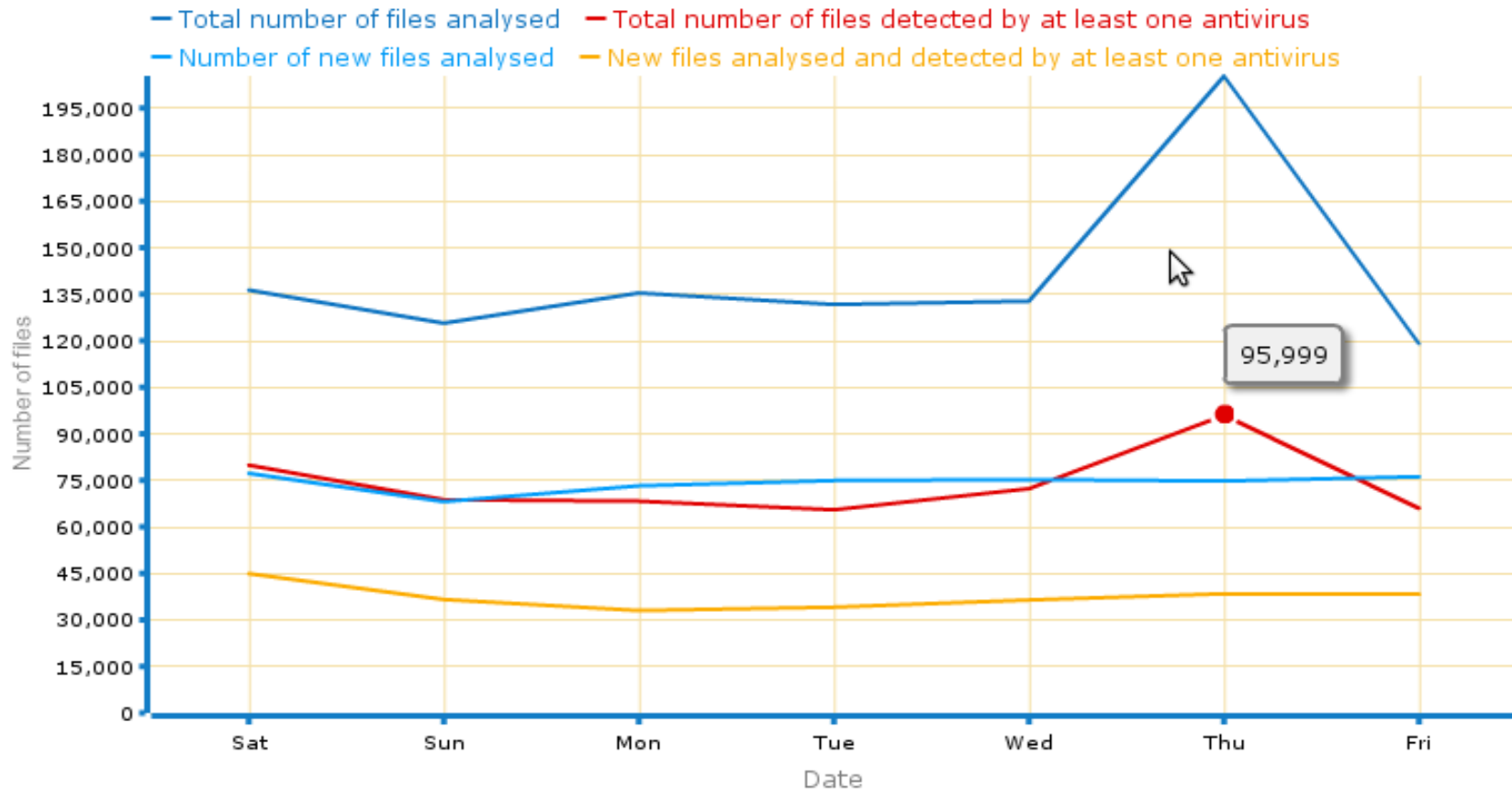
Otras formas de obtener Información

En octubre del 2010



Otras formas de obtener Información

En la actualidad.....el 1-10-2011...



Otras formas de obtener Información

¿Quiero ver un adjunto pero dudo de mi software antivirus?

- Virus total: <http://www.virustotal.com>
- No Virus Thanks: <http://www.novirusthanks.org>
- Scanner-virus: <http://www.scanner.virus.org>



Otras formas de obtener Información

Keyloggers

¿Cómo se evitan o previenen a nivel de red?

- ✓ Instalando filtros de spyware a nivel de host
- ✓ Instalar un aplicación de gateway con filtro de contenidos.
- ✓ Monitoreando los logs del sistema de detección de intruso (IDS) y manteniéndolo actualizado.
- ✓ Previniendo la instalación de software bajado por los usuarios.

