Eliminar el virus nimbda del servidor apache

Por Paco Aldarias Raya

Impreso: 3 de mayo de 2004

Email: pacolinux arroba inicia punto es
Web: `http://pagina.de/pacodebian`
Con Linux Debian. En Valencia (España)
Este documento es de libre reproducción siempre que se cite su fuente.
Realizado con: LaTeX

Índice

1. Introducción

El virus nimba intenta propagarse por la red. Infecta los servidores web de mocosoft, el llamado Internet Information Server (IIS)

2. Como se propaga

Veamos un trozo del log de apache: /var/log/http/access

```
217-127-85-207.uc.nombres.ttd.es - - [02/Jun/2002:06:28:15 +0200] "GET /scripts/

217-127-85-207.uc.nombres.ttd.es - - [02/Jun/2002:06:28:19 +0200] \
"GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 6

217-127-250-172.uc.nombres.ttd.es - - [02/Jun/2002:17:51:59 +0200] \
"GET /scripts/root.exe?/c+dir HTTP/1.0" 404 6

217-127-250-172.uc.nombres.ttd.es - - [02/Jun/2002:17:52:09 +0200] \
"GET /MSADC/root.exe?/c+dir HTTP/1.0" 404 6

217-127-250-172.uc.nombres.ttd.es - - [02/Jun/2002:17:52:19 +0200] \
"GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 6

217-127-250-172.uc.nombres.ttd.es - - [02/Jun/2002:17:52:29 +0200] \
"GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 6

217-127-250-172.uc.nombres.ttd.es - - [02/Jun/2002:17:52:37 +0200] \
"GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 6

217-127-250-172.uc.nombres.ttd.es - - [02/Jun/2002:17:52:45 +0200] \
"GET  /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP

217-127-250-172.uc.nombres.ttd.es - - [02/Jun/2002:17:52:54 +0200] "GET /_mem_bi

217-127-250-172.uc.nombres.ttd.es - - [02/Jun/2002:17:53:02 +0200] "GET /msadc/.
 HTTP/1.0" 404 6

217-127-250-172.uc.nombres.ttd.es - - [02/Jun/2002:17:53:11 +0200] "GET /scripts
```

3. Como solucionarlo

Revisando este fichero y filtrando estas maquinas con el cortafuegos.

4. Como se filtran las ips

Haciendo este script q lo q hace es revisar el log de apache /var/log/httpd/access_log buscando las cadenas q lo identifican y generar un fichero llamado /etc/nat/intrusos.txt

```
++++++Inicio script ++++++++++++++++++++++++++++++++
echo [*] Elimnado Nimbda
echo [+] Por Paco Aldarias
echo [+] Realizado el 8.6.02
echo [+] /etc/nat/nimba.txt

fl=/var/log/httpd/access_log
fi=/etc/nat/intrusos.txt

for i in `grep msadc $fl | cut -f1 -d' ' | sort | uniq | xargs echo`; do
        echo $i >> $fi
        echo [+] Pasado $i a $fi
done

for i in `grep default.ida $fl | cut -f1 -d' ' | sort | uniq | xargs echo`; do
        echo $i >> etc/nat/intrusos.txt
        echo [+] Pasado $i a $fi
done

ft=/etc/nat/temp.txt
echo [*] Quitando repetidos de $fl
for i in `cat $fi | sort | uniq | cut -f12 -d ',' |  xargs echo`; do
        echo $i >> $ft
        echo [+] Pasando $i a $ft
done
cp $ft $fi
cat $fi
rm $ft
++++++++++++++++++++ fin script ++++++++++++++++++++
```

5. Como hacer q el cortafuegos cierre el paso a esas maquinas

Añadiendo al cortafuegos este script:

```
++++++++++++++++++++++ inicio parte del script /etc/rc.d/nit.d/nat *************
fich=/etc/nat/intrusos.txt
cf=/sbin/iptables
idsl=eth0
echo [*] Bloqueando maquina no confiables fichero $fich

for linea in $(cat $fich); do
        echo [-] $cf -A INPUT -i $iadsl -s $linea -j DROP;
        $cf -A INPUT -i $iadsl -s $linea -j DROP;
done
++++++++++++++++++++++++ fin script ++++++++++++++++++++++++++++++++++++++++++
```

6. Text del virus nimba

http://www.securityspace.com/smysecure/w32_nmda_amm.html

Nota: Se pueden añadir al ficheros intrusos txt, las ips molestas, q las bloqueara tambien.