Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Como defenderse del virus NIMDA/Red Code/Sircam ... (31924 lectures)

Per **Carlos Cortes Cortes**, ***carcoco*** (http://bulma.net/~carcoco/)

Creado el 21/09/2001 17:54 modificado el 21/09/2001 17:54

El virus **NIMDA** es un virus/troyano de los de ultima hornada, que utiliza varias tecnicas diferentes para atacar: Correo Electronico (gracias al OutLook), al visualizar pagina web (gracias al IE y puede que a otros navegadores), red local de Windows (gracias a Microsoft) y **atacando servidores web** (gracias al ISS de Microsoft).
Pero que tiene todo esto que ver con Linux ? ...
[NUEVO]: Correccion de errores, multiples enlaces nuevos y nueva seccion sobre el **Sircam**.
[ACTUALIZACION]: Ejecucion del virus Sircam en Linux usando Wine.

Voy a centrarme en el ultimo de los metodos de ataque: infeccion de servidores web (se basa en aprovechar un error relacionado con la escalada de directorios a traves de caracteres Unicode en la URL), en servidores Internet Information Server:

El ataque lo que hace es mandar una peticion **GET** que busca el **cmd.exe** de los windows o el **root.exe** de otros troyanos como el **Code Red II**, de forma que si el ISS es vulnerable conseguira infectalo y este ordenador pasara a buscar nuevas victimas.
El virus scanea direcciones **IP** por Internet, atacando a **todo tipo de maquinas**.
Si tenemos activado el servidor **Apache** en nuestro Linux, quedaran registrados en sus log's todos estos ataques a nuestra maquina. Pudiendo conocer quien nos esta atacando y desde que IP concretamente de una forma muy sencilla:

Aqui podemos ver las peticiones que esta haciendo el **nimda** y otros troyanos como el **CodeRed II**:

```
egrep "cmd\.exe|root\.exe|\.ida" /var/log/httpd/access_log
```

Y esta nos devuelve el numero de ip's diferentes desde las que nos han atacado:

```
egrep "cmd\.exe|root\.exe|\.ida" /var/log/httpd/access_log | \
        awk '{print $1}' | sort | uniq | wc -l
```

Aqui tenemos *firmas* de ataques de otros gusanos:

```
egrep "scripts|_vti_bin|_mem_bin" /var/log/httpd/access_log | \
        cut -f1 -d" " | sort | uniq | wc -l
```

(Nota: La ubicacion del fichero de lods puede ser diferente, se puede averiguar tecleando *locate access_log*. La contrabarra "\" indica que el comando sigue en la linea siguiente)

Ahora podemos saber la direccion y el dominio madre de esa IP, utilizando el comando **whois**
http://bulma.net/body.phtml?nIdNoticia=380[1]

Posibles **medias a tomar**:
- Programas que detectan y manda correo a los administradores de las maquinas y/o listas especiales de maquinas infectadas:
codeblue-v4:
Este programa escrito en C, recorre un fichero de log's buscando ataques por virus del tipo Code-Red y similares, una vez encontrada la direccion IP, intenta establecer una conexion con dicha maquina, para enviarle un correo avisando al Administrador de la infeccion.

http://www.tenebrous.com/files/codeblue-v4.tar.gz[2]

wormreport-1.2
Este programa tambien recorre los logs, generando un informe con el numero de accesos, el nombre, la IP e intenta averiguar el domino. Luego este log se manda a una direccion para coordinar y corregir el problema.
http://tuxzone.net/scripts/wormreport-1.2.tar.gz[3]

Nimda Notifyer:
Similar a los anteriores manda al coordinador de netblock un correo informado de las maquinas infectadas.
http://www.digitalcon.ca/nimda/nimda-notify.pl[4]

CNimda de Felix-Gabriel Gangu
Este programa en PHP, que muestra los intentos del **NIMDA** de infectar tu servidor.
http://phpclasses.upperdesign.com/browse.html/package/335[5]

Snort[6] es un NIDS, Network Intruction Detection System; en este articulo nos dan las claves para configurarlo de forma que nos detecte los ataques del nimda.
http://www.snort.org/article.html?id=31[7]
http://lizard.drsuse.org/snort/snort18.html[8]

- **LaBrea**:
La idea detras del programa **LaBrea**, es crear unas maquinas virtuales usando direcciones IP de nuestra propia red no utilizadas, de forma que aunque no detienen al virus/gusano/troyano, *lo mantienen entretenido*, aligerando notablemente el impacto de los mismo en nuestras redes.
http://www.hackbusters.net/LaBrea/[9]

- **Samba, nmap**: Conociendo la ip de la maquina que nos esta atacando, y sabiendo que tendra compartida una carpeta con el usuario administrador y sin permisos, podemos usar los comandos del **samba**: **nmblookup, smbclient y smbmount**, para acceder a la misma y dejarle una mensaje al administrador del sistema, o incluso podriamos detener el ataque. Seria un especie de autodefensa ;-)
Aunque no se las implicaciones legales de esta opcion, puesto que incluso nos podrian acusar de acceso ilegar a sus maquinas :-(. Cuidado!.
http://www.samba.org[10]
http://www.insecure.org/nmap/[11]

Usando **Iptables** y el script **ipblock** podemos bloquear las direcciones IP que esten infectadas y que nos estan saturando nuestras redes:
http://bulma.net/body.phtml?nIdNoticia=861[12]

Deteccion de virus con tcpdump:
http://bulma.net/body.phtml?nIdNoticia=843[13]

He realizado una **selecion** de **documentacion** y **programas/scripts** sobre estos virus/gusanos/troyanos, seguro que aqui puedes encontrar informacion complementaria y muy valiosa; como la que explica como configurar el apache, de forma que cuando le llegue algun intento de infeccion, responda mandado una paguina web, al servidor infectado, usando la misma vulnerabilidad que explota el troyano:

- http://www.dasbistro.com/default_ida_info.html[14]
- http://salfter.dyndns.org/codered.shtml[15]
- http://ogg.2y.net/default.txt[16]
- http://www.beezhive.com/~mike/nimda.phps[17]
- http://michel.arboi.free.fr/UKUSA/couic.html[18]
- http://www.incidents.org/react/nimda.php[19]
- http://woodynet.siscom.net/Apache-CodeRed-1.08.tar.gz[20]
- http://www.everydns.net/~davidu/Apache-Nimba-0.1.tar.gz[21]
- http://www.incidents.org/react/nimda.php[19]

Otro de los virus que todavia se mantiene vivo y en su dia causo bastantes problemas, al colapsar los buzones de correo, de miles de usuarios en todo el mundo, es el **Sircam**. Este virus se autoreplica, usando una vulnerabilidad del

OutLook, mandando correos con ficheros adjuntos de considerable tamaño y con mensajes tan sugerentes como *Te mando este fichero para que me des tu opinion*, siendo el origen del mensaje alguien conocido por el destinatario. Aqui el problema radica en poder borrar de nuestros buzones, los enormes correos (que ademas llevaban el virus):

Os presento tres posibles alternativas, **Mailfilter**, **AniMail** y **PopMail**, pero existen muchas mas alternativas y posibilidades:
- Mailfilter o cómo remediar un ataque del Sircam:
http://barrapunto.com/article.pl?sid=01/08/08/0633233&mode=thread&threshold=[22]
http://www.planetalinux.com.ar/article.php?aid=52[23]
http://mailfilter.sourceforge.net/[24]
- Animail:
href="http://www.escomposlinux.org/fer_y_juanjo/linux.php?pag=animail.html[25]
- PopMail:
http://www.escomposlinux.org/sromero/prog/popmail.html[26]

Ejecucion del **virus Sircam** en **Linux** usando **Wine**.
Parece ser que usando el wine[27] (**Wine** Is Not an Emulator - **Wine** no es un emulador, sino realmente es una capa de abstraccion que permite ejecutar binarios de windows en Linux), se ha conseguido ejecutar el virus Sircam en sistemas Linux, pudiendo estudiarlo internamente de una forma totalmente controlada e inofesiva:
http://www.vnunet.com/News/1125594[28] | http://appdb.codeweavers.com/appview.php?appId=277[29]

--
Carlos (aka carcoco)
http://bulma.net/todos.phtml?id_autor=132 [30]

Lista de enlaces de este artículo:

1. http://bulma.net/body.phtml?nIdNoticia=380
2. http://www.tenebrous.com/files/codeblue-v4.tar.gz
3. http://tuxzone.net/scripts/wormreport-1.2.tar.gz
4. http://www.digitalcon.ca/nimda/nimda-notify.pl
5. http://phpclasses.upperdesign.com/browse.html/package/335
6. http://www.snort.org
7. http://www.snort.org/article.html?id=31
8. http://lizard.drsuse.org/snort/snort18.html
9. http://www.hackbusters.net/LaBrea/
10. http://www.samba.org
11. http://www.insecure.org/nmap/
12. http://bulma.net/body.phtml?nIdNoticia=861
13. http://bulma.net/body.phtml?nIdNoticia=843
14. http://www.dasbistro.com/default_ida_info.html
15. http://salfter.dyndns.org/codered.shtml
16. http://ogg.2y.net/default.txt
17. http://www.beezhive.com/~mike/nimda.phps
18. http://michel.arboi.free.fr/UKUSA/couic.html
19. http://www.incidents.org/react/nimda.php
20. http://woodynet.siscom.net/Apache-CodeRed-1.08.tar.gz
21. http://www.everydns.net/~davidu/Apache-Nimba-0.1.tar.gz
22. http://barrapunto.com/article.pl?sid=01/08/08/0633233&mode=thread&threshold=
23. http://www.planetalinux.com.ar/article.php?aid=52
24. http://mailfilter.sourceforge.net/
25. http://www.escomposlinux.org/fer_y_juanjo/linux.php?pag=animail.html
26. http://www.escomposlinux.org/sromero/prog/popmail.html
27. http://www.winehq.org/
28. http://www.vnunet.com/News/1125594
29. http://appdb.codeweavers.com/appview.php?appId=277
30. http://bulma.net/todos.phtml?id_autor=132

E-mail del autor: carcoco _ARROBA_ gmail.com