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

El síndrome de Estocolmo (15006 lectures)

Per **Ricardo Galli Granada**, ***gallir*** (http://mnm.uib.es/gallir/)

Creado el 24/12/2001 03:49 modificado el 24/12/2001 03:49

*El **FBI tuvo que intervenir y amenazar a Microsoft**. ¿Porque? Quizás os suene el último: vulnerabilidad del UPnP en el Windows XP descubierto menos de una semana después de su lanzamiento... O quizás os suene más el Sircam, Melissa, Anna Kournikova, IloveYou, Happy99, CodeRed, Goner, BadTrans... Esos virus han ocasionado pérdidas monumentales[1], aún así las empresas e instituciones públicas siguen comprando productos Microsoft. ¿Que otra cosa puede ser sino el síndrome de los secuestrados?. Estoy alucinado, tanto que me salió un rant en toda regla...*

FBI y XP

Al final el FBI tuvo que intervenir[2] para expresar a Microsoft su preocupación por los bugs del software de la compañía. Sobre todo después de descubrirse el último bug peligrosísimo del Windows XP (CERT[3], The Register[4]). El bug fue descubierto por la empresa eEYe[5] menos de una semana después de haberse lanzado el XP.

Aunque el bug fue anunciado casi inmediatamente a Microsoft, y viendo que este no respondía con un parche de seguridad, la empresa se decidió a divulgarlo después de un tiempo más que prudencial. El bug es tan peligroso que salió hasta en los medios generalistas más importantes (Yahoo[6], Los Angeles Times[7], Washington Post[8]).

El bug está relacionado en el Universal Plug and Play[9] (¿otro mas?) que viene instalado y habilitado por defecto en Windows. Ahora no sólo podrían borrar todos los ficheros de tu ordenador, sino que hasta podrían poner el aire acondicionado de tu casa a -10 grados en pleno invierno.

Todo esto ocurre, curiosamente, después que Jim Allchin, vicepresidente de Microsoft (Platforms Group) dijese que el XP[10] es, de lejos, el sistema más seguro de toda la gama Windows (aún así nosotros le creemos...). Tampoco debemos olvidar el fiasco de seguridad[11] del sistema Passport, la base de su nueva plataforma HailStorm.

Aún hay más... el problema de seguridad del Internet Explorer[12] que permite ejecutar casi cualquier fichero por no respetar las cabeceras MIME de los emails.

¿Primer bug...?

Pero ahora viene lo cómico, o penoso, depende del punto de vista, que demuestra la falta de memoria o responsabilidad de los responsables de Microsoft. De acuerdo a Scott Culp, la última vulnerabilidad del XP es el primero[13] relacionado con ataque remotos que afecta a sistemas de escritorio.

Que morro!!! ¿ya se olvidó por ejemplo del Back Orifice?

¿o del SECHOLE.EXE[14]?

¿o de la vulnerabilidad del IE con el javascript y frames[15]?

¿o del buffer oveflow del Clip Art del Office[16]?

¿o del Teardrop y Land[17]?

¿o del muy antiguo, 1995, de la vulnerabilidad de las carpetas e impresoras compartidas[18]?

Y por si eso no es suficiente, les podemos recordar algunos de las vulnerabilidades más famosas de los últimos tiempos y que ocasionaron grandes daños y pérdidas a las empresas afectadas:

- Sircam[19]
- Code Red[20]
- Goner[21]
- BadTrans[22]
- Vulnerabilidad de cache del Outlook y Outlook Express[23].
- Kaiten, Voyager, Voyager Alpha Force, y CBlade.worm[24] del SQL Server.
- Nimda[25]
- Buffer Overflow en Microsoft IIS 5.0[26]
- Anna Kournikova[27]
- Buffer overflow en SQL Server 7.0 y SQL Server 2000[28]
- Vulnerabilidad del Outlook View Control[29]
- ILoveYou[30]
- Happy99[31]
- Troyano ExploreZip[32]
- Melissa[33]
- Vulnerabilidad de nombres largos en IIS[34]
- Remote Explorer o RICHS[35]

La lista es impresionante, y eso que sólo mencionamos los más conocidos o dañinos. De todos las vulnerabilidades enumeradas, sólo hay unos tres o cuatro tipos distintos, lo que demuestra de alguna manera la seriedad con que se están tomando en cuestiones de seguridad en Microsoft.

¿Que medidas toma Microsoft para solucionar esos problemas? ¿hacer parches inmediatamente para remediar los bugs? No, intenta encubrir los problemas[36] echando la culpa de los ataques a la divulgación de las vulnerabilidades.

El váter en la cocina

¿Porque está ocurriendo todo esto con Microsoft? Difícil de explicar, hay varios factores, pero está claro que las decisiones de diseño no la están tomando los técnicos, sino más bien parece que las toman los comerciales de la empresa. **Microsoft necesita vender**, y como ya le queda poco que pueda vender con argumentos técnicos, y porque necesitan estar obligatoriamente, aunque de forma ficticia, por delante su gran competidor: el *Open Source*.

¿Como lo hace? **Inventándose nuevos requerimientos de usuario**. Así llegaron a la conclusión que los usuarios necesitan **ejecutar código dentro de un procesador de texto o en el cliente de correo**. ¿A quién se le ocurrió eso?

Pero los problemas vienen de antes, cuando decidieron incorporar primero la parte gráfica dentro del núcleo del sistema operativo (NT), teóricamente muy estable. Luego han empeorado la situación, cuando todo está de alguna forma integrada como parte esencial del sistema, desde visualizar una página web hasta leer un correo electrónico con macros Visual Basic.

Han cometido el peor error que podían haber hecho, como necesitaban vender productos nuevos y con el argumento de mejorar la experiencia del usuario, **han metido el váter en la cocina**. Vale que con eso nos ahorramos el camino desde el baño a la comida, pero todos sabemos que **donde se come no se caga**. Y además sabemos que la *cocina* de los sistemas operativos está muy caliente últimamente.

Los periodistas

Pero esto no es el mayor problema, al fin y al cabo Microsoft es una empresa y la única obligación que tiene es **maximizar beneficios para sus accionistas**. Los problemas mayores, además del monopolio demostrado, es que la gente todavía se cree el marketing de Microsoft, **inclusive los *periodistas informáticos***.

Cada vez que sale una versión nueva de Windows **festejan que el váter está cada vez más cerca de la cocina**, tan cerca que hasta se puede cagar mientras se come. Así nos ahorramos tiempo y energía dicen. Además ya casi

desaparece el váter, la cocina de encarga de todo.

Aún así, lo anterior es relativamente comprensible, los periodistas trabajan para revistas, cobran poco y no pueden hacer enfadar a los anunciantes, que en su gran mayoría son de Microsoft o de empresas que desarrollan software sobre esa plataforma. *Show must go on*.

Los *IT managers*

Lo peor es que los directivos de tecnologías de las empresas o de las administraciones, que sólo se deben a sus empresas, siguen como borregos las directivas de Microsoft (¡por supuesto que hay excepciones!, pero son eso, excepciones), y se gastan millones en licencias y contratos de mantenimiento, **a pesar de las lista abrumadora de vulnerabilidades que tiene**.

Hasta el FBI tiene que intervenir. ¿Tu comprarías una casa si la Policía Nacional le está diciendo al dueño que tiene que arreglarla porque en cualquier momento se cae?. Eso es lo que está haciendo esta gente, comprando e hipotecándose por casas **de una sola empresa** que en cualquier momento se caen.... a pesar de que la policía les está avisando del peligro.

¿Que les o nos pasa? ¿No hay alternativas? Sí que la hay, en Bulma ya se han publicado artículos y enlaces de empresas que han implementado Linux y/o Open Source como alternativa y les funciona perfectamente, como servidores o escritorio[37]. Ese no es el problema, sino que sufren el Síndrome de Estocolmo y no se dan cuenta. Están aterrorizados de alejarse de su secuestrador, **creen que el mundo exterior, sea Open Source, Unix o Apple, es muy duro** y no merece la pena el esfuerzo...

Pero algún día se percatarán que **los únicos lugares donde se duerme, se come y se caga en la misma habitación son los zulos...**

Lista de enlaces de este artículo:

1. http://www.elpais.es/articulo.html?d_date=20011224&xref=20011224elpepisoc_3&type
2. http://www.theregister.co.uk/content/4/23495.html
3. http://www.cert.org/advisories/CA-2001-37.html
4. http://www.theregister.co.uk/content/4/23480.html
5. http://www.eeye.com/html/press/PR20011220.html
6. http://dailynews.yahoo.com/h/ap/20011221/ts/microsoft_hackers_10.html
7. http://bulma.net/link/?l79
8. http://www.washingtonpost.com/wp-dyn/articles/A10033-2001Dec20.html
9. http://www.upnp.org
10. http://bulma.net/link/?l80
11. http://www.theregister.co.uk/content/4/22655.html
12. http://www.cert.org/advisories/CA-2001-36.html
13. http://www.washingtonpost.com/wp-dyn/articles/A7050-2001Dec20.html
14. http://www.wired.com/news/technology/0,1282,14044,00.html
15. http://news.cnet.com/news/0,10000,0-1003-200-332965,00.html
16. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bull
17. http://www.cert.org/advisories/CA-1997-28.html
18. http://www.ciac.org/ciac/bulletins/g-06a.shtml
19. http://www.cert.org/advisories/CA-2001-22.html
20. http://www.cert.org/advisories/CA-2001-19.html
21. http://www.cert.org/incident_notes/IN-2001-15.html
22. http://www.cert.org/incident_notes/IN-2001-14.html
23. http://www.cert.org/advisories/CA-2000-14.html
24. http://www.cert.org/incident_notes/IN-2001-13.html
25. http://www.cert.org/body/advisories/CA200126_FA200126.html
26. http://www.cert.org/advisories/CA-2001-10.html
27. http://www.cert.org/advisories/CA-2001-03.html
28. http://www.kb.cert.org/vuls/id/700575
29. http://cert-nl.surfnet.nl/s/2001/S-01-83.htm

30. http://www.cert.org/advisories/CA-2000-04.html
31. http://www.cert.org/incident_notes/IN-99-02.html
32. http://www.cert.org/advisories/CA-1999-06.html
33. http://www.cert.org/advisories/CA-1999-04.html
34. http://www.cert.org/advisories/CA-1998-04.html
35. http://www.cert.org/incident_notes/IN-98-07.html
36. http://www.theregister.co.uk/content/archive/22740.html
37. http://www.crn.com/Sections/CoverStory/CoverStory.asp?ArticleID=31793

E-mail del autor: gallir _ARROBA_ uib.es