PRESIDENCIA DEL CONSEJO DE MINISTROS

Oficina Nacional de GOBIERNOELECTRÓNICO e INFORMÁTICA

BOLETÍN DE ALERTA ANTIVIRUS

Centro de Consulta e Investigación sobre Seguridad de la Información

Edición Nº 147/ 28 Noviembre de 2008

Visite el Portal del Estado Peruano: www.peru.gob.pe

INDICE

MICROSOFT INFORMA SOBRE DOS NUEVOS VIRUS

Microsoft informó que el virus tipo gusano llamado Win32/Conficker.A se esta extendiendo rápidamente, infectando a las computadoras a través de las redes. Además, existe un troyano llamado Win32/IRCbot.BH, que provoca daños propagándose a través de un servidor de mensajería.

El virus se está extendido rápidamente entre las empresas y PCs particulares. La vulnerabilidad de Windows afecta de manera crítica a sistemas Windows 2000, XP y 2003.

En el primer caso el atacante puede tomar control del equipo cuando se habilite el modo de compartir archivos. Este gusano afecta de manera menor a Windows Vista y Windows Server 2008, y todas sus ediciones soportadas.

Ambos virus utilizan un agujero de seguridad que Microsoft solucionó el mes pasado con el parche **MS08-067,** pero en los últimos días los equipos que no han aplicado el parche se están infectando velozmente.

La infección se ha propagado sobre todo por Estados Unidos, aunque también por varios países europeos y de Sudamérica.

MAS INFORMACION:

- **Microsoft**
  http://www.microsoft.com/latam/technet/seguridad/boletines/2008/ms08-067.mspx
- **RevistaInfo**
  http://www.revistainfotigre.com.ar/2008/11/27/microsoft-advierte-sobre-2-nuevos-virus/

CLASIFICACIÓN DE LOS PROGRAMAS MALICIOSOS, NOVIEMBRE DE 2008

En noviembre de 2008; Viruslist ha realizado con los resultados de Kaspersky Security Network (KSN) la siguiente estadística de virus.

La primera tabla contiene los datos recogidos por Kaspersky Security antivirus versión 2009. En esta tabla se presentan los programas nocivos, publicitarios y potencialmente peligrosos detectados en los equipos de los usuarios.

Posición	Cambios en la posición	Programma nocivo
1	▲3	Virus.Win32.Sality.aa
2	▮▮0	Packed.Win32.Krap.b

FUENTES

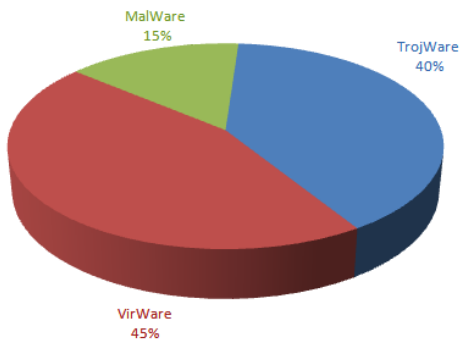
- Alerta Antivirus
- Microsoft
- RevistaInfo
- VirusList
- Kaspersky

3	New	Trojan-Downloader.WMA.GetCodec.c
4	-1	Worm.Win32.AutoRun.dui
5	3	Trojan-Downloader.Win32.VB.eql
6	New	Worm.Win32.AutoRun.rja
7	0	Packed.Win32.Black.a
8	New	Exploit.JS.RealPlr.nn
9	New	Trojan-Downloader.JS.Tabletka.a
10	-5	Trojan-Downloader.JS.IstBar.cx
11	-1	Trojan.Win32.Agent.abt
12	New	Trojan-Downloader.Win32.Agent.anje
13	2	Virus.Win32.VB.bu
14	New	Worm.Win32.Mabezat.b
15	New	Worm.Win32.AutoRun.eee
16	0	Email-Worm.Win32.Brontok.q
17	-8	Virus.Win32.Alman.b
18	-7	Worm.VBS.Autorun.r
19	New	Trojan-Downloader.JS.Iframe.yp
20	New	Trojan.Win32.Autoit.ci

En noviembre el virus Sality.aa se convirtió en el líder. La cantidad de equipos que ha infectado ha crecido bruscamente en los últimos dos meses.

En la lista de los 20 han aparecido dos nuevos cargadores de scripts, Trojan-Downloader.JS.Tabletka.a y Trojan-Downloader.JS.Iframe.ypy tres gusanos, dos de los cuales son representantes de una de las familias de crecimiento más dinámico: Worm.Win32.Autorun. Tomando en cuenta el simple pero efectivo método de reproducción de los gusanos Autorun, la cantidad de equipos infectados seguirá creciendo. En lo que concierne al tercer nuevo gusano Mabezat.b, es ahora el líder de nuestra segunda lista de los 20.

Todos los programas nocivos, presentes en esta lista se pueden agrupar según la clase de amenaza que representan. El porcentaje de programas troyanos ha bajada un 10% más, pero el porcentaje de programas capaces de reproducirse por sí mismos ha crecido al 45%, lo que constituye un hecho muy preocupante.



La segunda tabla del informe son los datos acerca de qué programas nocivos son los que con más frecuencia infectan los equipos de los usuarios. Aquí dominan los diferentes programas nocivos capaces de infectar ficheros.

Posición	Cambios en la posición	Programma nocivo
1	0	Worm.Win32.Mabezat.b
2	1	Virus.Win32.Sality.aa
3	1	Net-Worm.Win32.Nimda
4	-2	Virus.Win32.Xorer.du
5	1	Virus.Win32.Parite.b
6	1	Virus.Win32.Virut.n
7	-2	Virus.Win32.Alman.b
8	0	Virus.Win32.Sality.z
9	1	Virus.Win32.Small.l
10	2	Email-Worm.Win32.Runouce.b
11	-2	Virus.Win32.Virut.q
12	3	Virus.Win32.Parite.a
13	4	Worm.Win32.Fujack.k
14	-1	Worm.Win32.Otwycal.g
15	-1	Virus.Win32.Hidrag.a
16	New	P2P-Worm.Win32.Bacteraloh.h
17	Return	Worm.VBS.Headtail.a
18	-2	Trojan.Win32.Obfuscated.gen
19	1	Virus.Win32.Neshta.a
20	-2	Trojan-Downloader.WMA.GetCodec.b

Este mes los cambios son mínimos en la lista, hay sólo un nuevo programa malicioso y uno que ha regresado a la lista de los 20.

MAS INFORMACION:

- **VirusList**
  http://www.viruslist.com/sp/analysis?pubid=207271011

- **Kaspersky**
  http://latam.kaspersky.com/

CUALQUIER CONSULTA ENVIAR UN CORREO AL
CENTRO DE CONSULTA E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION - CCISI

ccisi@pcm.gob.pe
Teléfono : 2744356 – 106