

HP distribuye por error controladores infectados por el virus FunLove.

HP ha hospedado en su página web, durante un tiempo indefinido, uno de sus controladores de impresora infectado por FunLove, un virus de hace casi seis años. BitDefender alertó de la situación y el archivo que contenía el virus fue retirado de los repositorios de la compañía.

HP se ha visto obligada a retirar de sus servidores un controlador para la impresora de HP "Officejet g85 All-in-One" en su versión coreana para Windows 95/98 por contener el virus FunLove. BitDefender, la conocida empresa antivirus, se percató de que esos drivers en concreto contenían un virus descubierto a finales de 1999 que tuvo una importante capacidad de infección, con posteriores versiones de malware basadas en él.

Al parecer HP tropieza en la misma piedra, pues ya sufrió la embestida de este virus anteriormente, y fue distribuido también con una versión japonesa de uno de sus controladores. Un año después (en 2002), a Microsoft le pasó exactamente lo mismo... incluso con el mismo virus FunLove.

La posible repercusión del hecho a nivel de infección es mínima. HP ya no comercializa la impresora en concreto, y el hecho de que la amenaza estuviese limitada a una versión de un lenguaje concreto y unos sistemas operativos obsoletos hacen que el impacto potencial de infección sea muy pequeño. Además, se trata de un "viejo conocido" de los antivirus, por lo que todos lo pueden detectar hoy en día.

Lo llamativo del hecho es que el espécimen sobreviviese tanto tiempo anclado a unos controladores de impresora. Este incidente pone en evidencia una pobre política de seguridad de HP, en la que un simple escaneo preventivo de sus ficheros hubiese detectado el problema. Unas firmas MD5 o SHA-1 de los controladores en cuestión hubiesen igualmente ayudado a detectar la anomalía mucho antes de que BitDefender tuviera que avisarles y su imagen se viese dañada. Otra solución hubiese sido el análisis en tiempo real de tráfico saliente... Es en estos casos, a veces inimaginables, cuando las medidas preventivas demuestran su verdadero valor.

Este curioso caso, además, puede justificar en cierta medida la acumulación de firmas que pueden considerarse obsoletas en las bases de datos de antivirus. Esta práctica la realizan las casas como estrategia comercial basada en números de detecciones (el problema que Bernardo Quintero denominó "efecto zoo") y se basa en incluir en sus bases de datos firmas (poco "prácticas") para virus antiguos, obsoletos o considerados pruebas de concepto.

Aunque por ahora es viable mantener todo tipo de firmas conocidas en los antivirus llegará un momento, teniendo en cuenta el ritmo de crecimiento actual, en que la situación se vuelva insostenible y se deba modificar la estrategia en favor de firmas genéricas, mejores heurísticas o aliviar la carga de virus considerados obsoletos... pero entonces, amenazas como la de FunLove, oculto en servidores de prestigiosas compañías, se convertirían en riesgos reales (aunque mínimo, riesgo al fin y al cabo). Si BitDefender no se hubiese percatado de este problema, el virus podría haber dormitado en los servidores públicos de HP indefinidamente ¿Qué hubiese pasado, si para entonces, los antivirus no lo reconocieran?

En cualquier caso, el hipotético problema de una resurrección vírica no supera a la amenaza real y

tangible que hoy por hoy supone el preocupante crecimiento de malware no detectado que aparece cada día. En la ventana de tiempo que ocurre entre que el virus es detectado y su firma es incluida en la base de datos de antivirus, las posibilidades de infección se multiplican. Esto en el mejor de los casos, pues según se desprende de Virustotal.com, los virus no son siempre reconocidos y aunque se detecten las firmas de ejemplares de hace varios años, otros muchos troyanos actuales y considerablemente más peligrosos quedan, por siempre, sin identificar.

Más información:

More HP printer drivers infected News - PC Advisor
www.pcadvisor.co.uk/news/index.cfm?newsid=6295

Un error de Microsoft infecta los sistemas de 26 clientes con el virus FunLove
<http://www.idg.es/pcworld/noticia.asp?idn=15665>

Sergio de los Santos
ssantos@hispasec.com

Fuente:
<http://www.hispasec.com/unaaldia/2781>

Fecha artículo: 2006-06-06 21:02:47 - url artículo: <http://www.internautas.org/html/783.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org