UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2009−006

Proteja a sus equipos Windows del gusano Conficker

En los últimos días el UNAM−CERT ha recibido diversos reportes que advierten de un incremento en la actividad del gusano Conficker. Se sugiere a los usuarios en general tomar las medidas necesarias descritas en la presente nota y documentos anexos a fin de evitar que sus equipos sean infectados por este gusano malicioso.

Fecha de Liberación:	27 de Marzo de 2009
Ultima Revisión:	29 de Marzo de 2009
Fuente:	Conficker Working Group, Microsoft Corp, UNAM−CERT y otros equipos de respuesta a incidentes.

Riesgo

Alto

I. Sistemas Afectados

- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003
- Microsoft Windows Vista
- Microsoft Windows Server 2008

II. Descripción

El gusano Conficker es un código malicioso que explota una vulnerabilidad en los sistemas operativos Windows que no han instalado la actualización KB958644 descrita en el boletín MS−067 de Microsoft Corp. Este código malicioso puede propagarse mediante la red o a través de dispositivos extraíbles como memorias USB, diskettes, entre otros.

Algunos reportes indican que una nueva variante entrará en operación el 1 de abril de 2009, por lo que se recomienda a los administradores y usuarios de sistemas Windows instalar la actualización de seguridad a la brevedad posible.

Para los usuarios que han sido infectados por el código malicioso se sugiere utilizar una herramienta automatizada para la eliminación del gusano.

Notas:

- Los métodos de prevención y erradicación del código malicioso están descritos en la sección Solución del presente boletín.
- Si desea conocer más información del gusano Conficker, UNAM−CERT ha desarrollado un documento no técnico que describe la evolución y comportamiento del gusano Conficker, el cual se encuentra disponible en:
  - El gusano Conficker − http://www.seguridad.unam.mx/doc/?ap=articulo/ul>

III. Impacto

Un atacante remoto podría ejecutar código arbitrario y tomar control total del sistema afectado.

IV. Solución

- Para prevenir una infección del gusano se recomienda instalar la actualización de Seguridad de Microsoft Corp.
  - Vulnerabilidad en el servicio Server podría permitir la ejecución remota de código (958644) − http://www.seguridad.unam.mx/vulnerabilidadesDB/?vulne=5666
- Actualice su software antivirus
- Para la erradicar al gusano de un sistema Windows se recomienda hacer uso de una herramienta automatizada.
- Los usuarios avanzados podrían hacer una eliminación manual del código malicioso.
  - Eliminación del Gusano Conficker de equipos Windows − http://www.seguridad.unam.mx/doc/?ap=articulo

V. Preguntas frecuentes acerca del gusano Conficker

- ¿Cómo se propaga el gusano Conficker?

  Este gusano Conficker principalmente se propaga mediante la red enviando paquetes RPC malintencionados a los sistemas Windows; pero también puede propagarse mediante dispositivos extraíbles como memorias USB, Diskettes, entre otros.

- ¿Qué acciones realiza Conficker en los equipos infectados?

  En general, se puede detectar la infección de Conficker si se presentan los siguientes síntomas:

  - Desactivación de los servicios de actualizaciones automáticas, Windows Defender, Background Inteligent Transfer Service (BITS) y el servicio de reportes de Windows.
  - Modificación en las directivas de cuenta, por ejemplo si existían políticas para el bloqueo de cuentas, estas directivas son desactivadas.
  - Congestionamiento en la red. En especial puede identificarse tráfico dirigido al puerto 445 de TCP.
  - Restricción de acceso a sitios Web relacionados con antivirus, actualizaciones de Windows y antispyware.
  - El rendimiento de las aplicaciones es deficiente.
- ¿Qué impacto ha tenido Conficker?

  Conficker ha tenido un gran impacto alrededor del mundo, pues se estima que existen más de 10 millones de equipos infectados con alguna de las variantes. En México, el UNAM−CERT ha identificado al 26 de marzo de 2009 un número aproximado de 71 mil equipos comprometidos que afectan el dominio .mx con éste código malicioso y no se descarta que las infecciones continúen.

- ¿Debo estar preocupado por el 1 de abril?

  Algunos reportes indican que una nueva variante entrará en operación el 1 de abril de 2009, sin embargo los usuarios que han instalado la actualización descrita en el boletín MS−067 y que utilizan algún software de seguridad como antivirus o antispyware no deberían preocuparse por las nuevas variantes.

- Si mi organización ha sido afectada por Conficker, ¿qué puedo hacer?

  Recomendamos utilizar algún método automatizado para la erradicación, estas herramientas pueden encontrarse en la sección "¿Cómo erradicar la infección?" del presente documento. Si se trabaja en un entorno administrado como Active Directory podría implementarse la instalación de la herramienta automatizada mediante el uso de las Directivas de Grupo (GPO).

VI. Referencias

- El gusano Conficker − http://www.seguridad.unam.mx/doc/?ap=articulo
- Proyecto Seguridad en Windows − http://www.seguridad.unam.mx/windows
- Vulnerabilidad en el servicio Server de Microsoft podría permitir la ejecución remota de código − http://www.cert.org.mx/boletin/?vulne=5667
- Help Protect Windows from Conficker − http://technet.microsoft.com/en−us/security/dd452420.aspx
- Centralized Information About The Conficker Worm − http://blogs.technet.com/mmpc/archive/2009/01/22/centralized−information−about−the−conficker−wo
- Keep the latest worm infestation off your PC − http://www.windowssecrets.com/2009/01/22/02−Keep−the−latest−worm−infestation−off−your−PC
- Implantación de la Herramienta de eliminación de software malintencionado de Microsoft Windows en un entorno empresarial − http://support.microsoft.com/kb/891716/
- Conficker – Seminarios de Seguridad Informática UNAM−Microsoft (Video) http://podcast.unam.mx/wp−content/uploads/podcastunam−2009−02−19−22222.m4v
- Conficker – Seminarios de Seguridad Informática UNAM−Microsoft (pdf) http://seminarios.seguridad.unam.mx

---

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Oscar Raúl Ortega Pacheco (oortega at seguridad dot unam dot mx)
- Juan Carlos Guel Lopez (cguel at seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)
- Jesús Mauricio Andrade Guzmán (mandrade at seguridad dot unam dot mx)

UNAM−CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47