Rafael Pagan Colon <rafael.pagan@upr.edu>

Alerta sobre el programa malicioso "Conflicker Worm"

7 messages

cartero.AC@upr.edu <cartero.AC@upr.edu> **Tue, Mar 31, 2009 at 3:10 PM**
To: rafael.pagan@upr.edu, rafael.pagan@upr.edu

A todos los usuarios:

Recientemente, los medios noticieros en EEUU han estado avisando del virus “Conflicker Worm”; el cual alegadamente se propagará el miércoles, 1 de abril. También conocido como “Downadup” o “Kido”, el mismo ha logrado infectar gran número de computadoras en el pasado. La compañía Symantec indica que quienes utilizan versiones actualizadas de sus productos están protegidos de este programa malicioso (en la industria se le conoce a este tipo de programa como “malware”).

Los administradores de servidores y redes Windows deben cerciorarse de que a sus servidores se les ha aplicado el parche de seguridad Núm. MS08-067 emitido por Microsoft.

Aunque no se tiene seguridad de la intención específica del virus (particularmente de su variante “C”), se entiende que Conflicker se propaga a través de las redes, una vez identifica alguna computadora que encuentre vulnerable a su ataque. El “malware” desactiva el servicio de resguardo automático, elimina puntos de restauración que se hayan configurado, inhibe los servicios de seguridad (tales como en el caso de programados anti-virus que no estén actualizados) y prohíbe el acceso a las páginas Web de los programas de Seguridad tales como Symantec. De hecho, el síntoma principal de que una computadora está infectada es la incapacidad para acceder alguna de las siguientes páginas Web, según quien sea su proveedor de programa de antivirus.

- http://www.symantec.com/norton/theme.jsp?themeid=conficker_worm&inid=us_ghp_link_conficker_worm
- http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx
- http://www.mcafee.com

Además, expone la computadora infectada a recibir programas adicionales de “malware”. De ahí, el programa intenta replicarse a otras computadoras en la red.
Se entiende que los usuarios en mayor riesgo de que se les infecte sus computadoras son aquellos cuyas computadoras no están configuradas para recibir parches de seguridad y actualizaciones de Microsoft (en los casos donde el sistema operativo es Windows XP) y cuyos programas de antivirus no se hayan actualizado. Quienes no tengan copias legítimas instaladas del sistema operativo Windows también se encuentran en riesgo.

A continuación se le enumeran algunas recomendaciones para mitigar la posibilidad de que su computadora sufra un ataque:
1. Si no tiene un programa antivirus, procure e instale uno.
2. Si tiene un programa antivirus instalado, confirme que el mismo está actualizado. Como regla general, al levantar la ventana del programa en ejecución, acceda la opción de Help del menú principal; e identifique el renglón de “About [nombre del programa]”. Este le mostrará la fecha de la última actualización.
3. Mantenga su computadora actualizada con los parches de seguridad más recientes de Microsoft. En caso de dudas, contacte la Oficina de Sistemas de Información de su unidad o recinto.
4. Evite utilizar programas “gratis” de seguridad. En ocasiones, son engañosos por cuanto representan tácticas de intimidación para que los usuarios tenga que comprar un producto completo; o peor, un web site de malware que aprovechará para bajar programación ilícita.
5. Valide que la construcción de sus contraseñas (“passwords”) sea fuerte y difícil de decifrar. Siga las guías establecidas institucionalmente e incluidas en el Procedimiento de Administración y Uso de Tecnología Informática; el cual está disponible a través del enlace http://acweb.upr.edu/docs/osi/Procedimiento_de_Administración_de_Tecnología_1.6.pdf.

Para mayor información, se les suministra algunas fuentes adicionales de información:
US-CERT
Technical Cyber Security Alert TA09-088A
http://www.us-cert.gov/cas/techalerts/TA09-088A.html

SANS Internet Storm Center
Third party information on conficker (Removal instructions, tools, etc)
http://isc.sans.org/diary.html?storyid=5860

SANS Internet Storm Center

Locate Conficker infected hosts with a network scan!
http://isc.sans.org/diary.html?storyid=6097

Conficker Working Group
Conficker Information Sheet for Network Providers
http://www.confickerworkinggroup.org/wiki/pmwiki.php?n=SP.ServiceProviders

---

cartero.AC@upr.edu <cartero.AC@upr.edu> **Tue, Mar 31, 2009 at 3:12 PM**
To: rafael.pagan@upr.edu, rafael.pagan@upr.edu

[Quoted text hidden]

---

cartero.AC@upr.edu <cartero.AC@upr.edu> **Tue, Mar 31, 2009 at 3:17 PM**
To: rafael.pagan@upr.edu, rafael.pagan@upr.edu

[Quoted text hidden]

---

cartero.AC@upr.edu <cartero.AC@upr.edu> **Tue, Mar 31, 2009 at 3:28 PM**
To: rafael.pagan@upr.edu, rafael.pagan@upr.edu

[Quoted text hidden]

---

cartero.AC@upr.edu <cartero.AC@upr.edu> **Tue, Mar 31, 2009 at 3:28 PM**
To: rafael.pagan@upr.edu, rafael.pagan@upr.edu

[Quoted text hidden]

Rafael Pagan Colon <rafael.pagan@upr.edu> **Thu, Apr 2, 2009 at 11:57 AM**
To: cordero.ingrid@gmail.com

Ingrid

Este es el correo que emití ayer; y del cual te hablé anoche. Espero que te sea de utilidad.

RPC

[Quoted text hidden]

Ingrid Cordero <icordero@rocpr.net> **Thu, Apr 2, 2009 at 3:13 PM**
To: Rafael Pagan Colon <rafael.pagan@upr.edu>

Muchas gracias! No te había podido enviar un email como me pediste porque he estado sin Internet todo el día. Gracias por acordarte!

Ingrid M. Cordero
RSM ROC & Company
Management Consulting Division

From: Rafael Pagan Colon [rafael.pagan@upr.edu]
Sent: Thursday, April 02, 2009 11:57 AM
To: cordero.ingrid@gmail.com
Subject: Fwd: Alerta sobre el programa malicioso "Conflicker Worm"

[Quoted text hidden]

BusinessWeek.com -- - A Lost Decade for Job Growth - 7 hours ago

Web Clip < >

« Back to Search Results | Archive | Report spam | Delete | Move to Inbox | Labels | More actions

1 of **41** **Older ›**

New window
Print all
Collapse all
Forward all
Turn off highlighting

ALERTA contra intento de acceso no autorizado "PHISHING"

Appn GAE X Ofic. OSI X Service Bulk Mail X Service IT Security PHISHING X

cartero.ac@upr.edu to me, me show details Sep 3 (3 days ago) Reply

Recientemente, se está recibiendo un correo electrónico titulado "WEBMAIL MANTENIMIENTO!" de parte de un tal "Administrador de la UPR". El correo contiene una petición para que cada usuario suministre su correo electrónico en Google Apps junto a la contraseña de su cuenta.

DICHO MENSAJE DE CORREO NO ES REAL NI LEGÍTIMO. Constituye lo que se conoce como "phishing"; lo cual es un intento por obtener las credenciales de su cuenta; y así acceder de forma no autorizada a la misma. SE RECOMIENDA QUE EL MENSAJE SE ELIMINE O MARQUE COMO SPAM.

En el evento de un mantenimiento legítimo, el personal universitario responsable por la administración de la tecnología institucional jamás haría una solicitud en masa de cuentas de correo y contraseñas.

Reply Forward

cartero.ac@upr.edu to me, me show details Sep 3 (3 days ago) Reply

- Show quoted text -

Reply Forward

cartero.ac@upr.edu to me, me show details Sep 3 (3 days ago) Reply

- Show quoted text -

Reply Forward

cartero.ac@upr.edu to me, me show details Sep 3 (3 days ago) Reply

- Show quoted text -

Reply Forward

« Back to Search Results | Archive | Report spam | Delete | Move to Inbox | Labels | More actions

1 of **41** **Older ›**

Seminario en Línea sobre la Seguridad en la Utilización de los Sistemas de Información

Vicepresidencia de Investigación y Tecnología

Oficina del Principal Oficial de Informática

Oficina Central de Sistemas de Información

Próximo Final

Seguridad en la Utilización de los Sistemas de Información - Agenda

- Seguridad Física
- Seguridad Lógica
- Utilización de la Información
- Resguardar la Información
- Eliminación Segura de la Información

Seguridad Física

Seguridad Física

Cuido del Equipo en el Área de Trabajo

- Proteja el equipo de riesgos ambientales: polvo, fuego y agua
- Suministre ventilación adecuada al equipo
- Regulador de voltaje y fuente de carga ininterrumpidas (UPS) extienden la vida útil del equipo
- Desactive y apague el equipo al concluir el día
- Al levantarse de su área de trabajo, desactive su sesión (logoff) o tranque la pantalla (“Lock Computer”)
- Notifique de inmediato cualquier falla con la computadora o con su acceso a la red

Seguridad Física

Cuido del Equipo en el Área de Trabajo

- Coordine de antemano con la OSI la instalación de cualquier programa (“software”)
- No fume o ingiera alimentos o bebidas mientras utiliza la computadora
- No modifique la configuración de su equipo o de la programación
- No deje su computadora desprotegida, a la vista y acceso de todos
- Informe de inmediato la pérdida o robo de su equipo
- No utilice equipo módem o de conectividad inalámbrica independiente de la red de comunicaciones

Seguridad Física

Cuido del Equipo Fuera del Área de Trabajo

- Además de los Cuidados anteriores…
  - Nunca deje su computadora portátil desatendida; particularmente en sitios públicos.
  - No deje su computadora portátil a plena vista.
  - Guarde el equipo bajo llave o asegúrelo al escritorio mediante cable con candado.
  - No deje su computadora portátil en el auto.
  - Si va de viaje, utilice un bulto no descriptivo para guardar su computadora.

UNIVERSIDAD DE PUERTO RICO

Seguridad Lógica

Comienzo Anterior Próximo Final

Seguridad Lógica

- Utilización de clave de usuario y contraseña
- Contraseñas fuertes v. Contraseñas débiles
- Protección contra amenazas externas
  - Código malicioso
  - Protección contra una Infección

Seguridad Lógica

Utilización de Clave de Usuario

- El acceso a un sistema requiere una clave de usuario (cuenta)
- Toda cuenta de usuario requiere una contraseña
- La combinación de clave de acceso y contraseña es única y exclusiva para cada usuario
- No comparta su cuentas y contraseña
- Cada usuario es responsable de las consecuencias de cualquier acción tomada con su clave de usuario
- El proceso de registrar la clave de usuario y contraseña se conoce como “autenticación”

Seguridad Lógica

Utilización de Clave de Usuario

- No escriba la contraseña
- Al cambiar su contraseña, no re-utilice contraseñas pasadas
- Tranque preventivo: Tres fallas consecutivas en el proceso de autenticación desactiva la cuenta temporalmente
- Se suspende la cuenta inactiva por 30 días o más
- Se suspende la cuenta de un empleado que dimite, se retira, es trasladado fuera del área o es despedido
- Se elimina la cuenta inactiva por 1 año o más

Seguridad Lógica

Utilización de Contraseña

- Cambie su contraseña de ocurrir una de las siguientes:
  - Luego que brinde la contraseña a terceros para recibir mantenimiento o reparar su equipo
  - Cuando personal de administración de redes o sistemas dimite, se retira, es despedido o transferido fuera de sus responsabilidades de administración de la red o de los sistemas
  - Cuando la confiabilidad o confidencialidad de la contraseña quede en entredicho

Seguridad Lógica

Contraseñas Fuertes

- Tamaño idóneo de una contraseña: 6 caracteres o más
- Algunas técnicas para seleccionar una contraseña fuerte:
  - Escribir la palabra seleccionada en reverso. Por ejemplo, “anesartnoc” en lugar de “contrasena”.
  - Utilizar anagramas (una palabra con dos o más letras transpuestas). Por ejemplo, “trauqne” en lugar de “tranque”.
  - Sustituir letras por números, caracteres especiales u otras letras. Por ejemplo, “c3kur_1d@t” en lugar de “seguridad”
  - Alternar letras mayúsculas y minúsculas. Por ejemplo, “pROTexIOn”

Seguridad Lógica

CONTRASEÑAS DÉBILES

- Las contraseñas débiles son fáciles de romper
- Algunos ejemplos de contraseñas débiles son
  - Fechas (aniversarios, cumpleaños)
  - Nombres de parientes, amigos y mascotas
  - Números de teléfono o Tablilla del vehículo
- Nunca utilice su clave de acceso como contraseña
- No utilice información confidencial, tal como su número de seguro social o pasaporte, o algún componente de ellos, como clave de acceso o como contraseña

Seguridad Lógica

Protección contra Amenazas Externas

- Riesgo de Infección por Código Malicioso
  - Código malicioso: ¿Qué es?
  - Categorías del código malicioso
  - Efectos de un código malicioso
- Protección contra Infección
  - Parches de seguridad
  - Programas antivirus
  - Instalación y actualización de programas antivirus
  - ¿Cómo resolver una infección?

Seguridad Lógica

¿Qué es un Código Malicioso?

- ✓ Programa de intención maliciosa
- ✓ Representa un riesgo sustantivo a la Universidad por su potencial de pérdida de dinero, tiempo y datos
- ✓ Se conoce en inglés como “malware”
- ✓ Se instalan en las computadoras de manera intencional o accidental
- ✓ Su existencia puede ser desconocida por un usuario por tiempo indefinido
- ✓ A través del tiempo, el nivel de sofisticación, velocidad de propagación y magnitud del daño de este tipo de programa ha incrementado

Seguridad Lógica

Categorías de Código Malicioso

- ✓ Virus

  Programa que se replica de computadora en computadora

- ✓ Caballos de Troya

  Programa que se esconde en un archivo o programa válido para acceder a una computadora; luego procede a infectar la misma o dañar archivos que residen allí

- ✓ Gusanos (“worms”)

  Se propaga y replica similar a los virus y caballos de Troya. Se distingue de ambos en que su propósito final es destruir datos o sectores de un disco duro, de modo que la computadora se vuelva inservible

Seguridad Lógica

Fuentes de Código Malicioso

- Acceder a una computadora infectada
- Utilizar diskettes, discos compactos o “pen drives” infectados
- Bajar archivos de una página web de origen dudoso
- Ejecutar un programa infectado; particularmente los que llegan como anejos (“attachments”) en correos electrónicos desconocidos
- Por acciones maliciosas intencionales de individuos que buscan acceder remotamente una computadora

Seguridad Lógica

Efectos del Código Malicioso

- El comportamiento de la computadora o de una de sus aplicaciones cambia.
- Aumenta el tamaño de los archivos, sin explicación aparente
- Cambia la fecha de actualización de un programa o archivo
- Disminuye el espacio disponible de disco o de memoria después de correr un programa gratis (“Freeware”) o compartible (“Shareware”)
- Refleja múltiples accesos inesperados al disco duro

Seguridad Lógica

Protección Contra una Infección

- Minimice el compartir programas y archivos a través de diskettes, discos compactos o “pen drives” de fuentes exteriores
- Resguarde periódica y consistentemente sus datos y documentos (“backups”); por lo menos a nivel semanal
- Parche de seguridad
  - Programa correctivo suministrado por el suplidor para proteger sus sistemas y los datos que éstos acceden

Seguridad Lógica

Protección Contra una Infección

- Programas antivirus
  - Programa diseñado para proteger una computadora de la posibilidad de infección por código malicioso
  - Toda computadora que se conecte a la red de comunicaciones de la Universidad tiene que utilizar un programas antivirus

Seguridad Lógica

¿Cómo Resolver una Infección?

- Procure su resguardo más reciente
- Ubique *todos* los medios que hayan sido insertados en su computadora en el transcurso de los últimos seis (6) meses previo a la restauración.
  - Estos medios deberán ser desinfectados.
  - Si no pueden ser desinfectados, deberán destruirse para evitar una nueva infección. Previo a su destrucción, coordine con la OSI para respaldar los datos contenidos en estos medios para los cuales no tenga otro respaldo, desde una computadora aislada de la red.
- Coordine con la OSI para que se restauren los programados en la computadora afectada y se recuperen los datos y documentos utilizando su último resguardo.

Seguridad Lógica

¿Cómo Resolver una Infección?

- La OSI llevará a cabo las siguientes tareas:
  - Desconectará la computadora de la red
  - Analizará la gravedad de la infección, previo a apagar la computadora
  - Reactivará la computadora, subiendo el sistema operativo desde un medio alterno (disco compacto o CD)
  - Cotejará que el sistema sube de manera estable

Seguridad Lógica

¿Cómo Resolver una Infección?

- Resguardará ("backup") los archivos no ejecutables (documentos, imágenes, hojas de cálculo, presentaciones, bases de datos, etc.) a un nuevo medio recién formateado (diskette, "pen drive", CD o DVD nuevo)
- Hará limpieza ("low level format") del disco infectado
- Reformateará el disco, luego procederá a restaurar el sistema operativo y reestructurará los directorios
- Restaurará los programados oficialmente asignados al usuario utilizando los medios originales del producto; tal y como si fuera una nueva instalación de los programados
- Restaurará los archivos a los que previamente se les hizo resguardo

Utilización y Protección de la Información

Utilización de la Información

- Información
  - Conjunto de datos que describen de manera colectiva a una persona, entidad, lugar, cosa o concepto; con utilidad para la Universidad en sus gestiones académicas, docentes, investigativas y administrativas
- Categorías
  - Confidencial
  - Privada
  - De directorio

Categorías de la Información

EJEMPLOS

- Confidencial
  - Número de seguro social
  - Fecha de nacimiento
  - Datos sobre la salud
  - Credo religioso o político
- Privada
  - Dirección residencial
  - Calificaciones académicas
  - Ayuda médica o de consejería recibida
- De directorio (pública)
  - Nombre y apellidos
  - Género (femenino o masculino)

Protección de la Información

- Mantenga actualizada su información personal
- Acceda sólo aquellas cuentas, archivos y datos que
  - Les pertenece
  - Sobre los cuales se le haya brindado autorización de acceso
  - Estén disponibles públicamente
- Utilice la información de la Universidad sólo para tareas asociadas a su responsabilidad hacia la Universidad; no para asuntos personales

Protección de la Información

- Asegure la información que está bajo su custodia
- Mantenga confidencial la información clasificada como privada o confidencial, o que esté asociada a personas ya fallecidas
- No divulgue jamás información alguna a la cual tenga acceso, pero sobre la cual no tiene propiedad, autorización o permiso para divulgar
- En caso de dudas, trate la información de manera confidencial hasta que confirme el grado de sensibilidad y confidencialidad

Compartir la Información

- Compartir información es una parte intrínseca de la filosofía de la Universidad
- Al compartir información, el usuario debe cumplir con
  - Leyes federales y locales aplicables
  - Política , Estándares y Procedimientos vigentes
- La instalación de programas para compartir archivos de tipo "Peer-to-Peer" (P2P) no está explícitamente prohibido, *PERO…*

Compartir la Información

- Cuando un programa P2P se instala, activa por defecto la funcionalidad de compartir archivos.
  - Representa un riesgo serio de seguridad
  - Expone a la Universidad a posibles violaciones de derechos de autor, aunque no se esté consciente de ello
  - Cualquier computadora que tenga instalado un programa P2P, irrespectivo de si le pertenece o no a la Universidad, deberá desactivar la funcionalidad de compartir archivos mientras esté conectada a la red de comunicaciones de la Universidad

Compartir la Información

- Consulte con la OSI previo a instalar y utilizar programas P2P , para validar que el tráfico en la red y la seguridad de la red no se vean impactadas
- La OSI asignará prioridad a las aplicaciones legítimas de la Universidad, segmentando la red en particiones a las que le asignará el ancho de banda correspondiente

Resguarde la Información

Resguardar la Información

¿Qué es un Resguardo?

- Copia que se hace de los archivos, datos y documentos electrónicos de una computadora
- Su propósito es poder recuperar cualquiera de ellos, en caso de que la versión con la que se trabaja se dañe o se pierda debido a algún caso fortuito
- La copia se hace generalmente a un medio de almacenaje portátil, tal como un disco compacto (CD), disco digital (DVD) cartucho de cinta magnética, diskette o dispositivo "pen drive" (también conocido como USB)
- Se recomienda almacenar el resguardo fuera del área de trabajo

Resguardar la Información

¿Quién Resguarda?

- Cada usuario es responsable por resguardar los datos y archivos que mantenga en su computadora o en algún otro dispositivo fuera de algún servidor bajo la administración de la OSI.

- Los pasos para crear un resguardo de su computadora se halla en el ***Procedimiento para Utilizar y Administrar la Tecnología Informática***

Resguardar la Información

¿Quién Resguarda?

- De suceder alguna interrupción o fallo en una aplicación o servicio electrónico, la Universidad no se hace responsable por el daño o pérdida de datos que ocurra, ni por las complicaciones que se puedan derivar como resultado del incidente

- Si la computadora se conecta a una red local, ausculte con la OSI la posibilidad de almacenar los archivos y documentos en el servidor; de modo que se incluyan en los resguardos periódicos del servidor

Resguardar la Información

Frecuencia Recomendada

- Se recomienda un resguardo semanal para documentos y archivos que cambian con poca frecuencia
- Se recomienda un resguardo diario para documentos y archivos que cambian con mucha frecuencia
- Para archivos y documentos críticos, se recomienda hacer un resguardo al final del día en que se cambian

UNIVERSIDAD DE PUERTO RICO

Eliminación Segura de la Información

Comienzo Anterior Próximo Final

Eliminar Información de Manera Segura

CONCEPTO GENERAL

- Los datos privados en computadoras y otros dispositivos electrónicos representan un riesgo sustancial al momento de disponer o transferir dicho equipo
- Previo a transferir o disponer del equipo, debe eliminarse dicha información de manera segura
- Eliminación segura de datos

  Proceso de erradicar los datos almacenados en una computadora o en medios electrónicos de almacenaje, de modo que estos datos ya no se puedan recuperar.

Eliminar Información de Manera Segura

¿Qué se Debe Eliminar?

- Los datos en una computadora, antes de transferir hacia un destino desconocido o hacia una persona u oficina que no está autorizada para acceder la información
- Medios externos utilizados para almacenar datos (discos externos, diskettes, CD's, DVD's o "pen drives") previo a disponer de ellos
- Eliminar documentos o archivos por métodos convencionales (por ejemplo, pulsando la tecla de "Delete") no elimina totalmente los mismos. Quedan remanentes sustanciales en el disco físico de la computadora, lo cual representa un riesgo para la Universidad.
- Las técnicas de eliminación segura son necesarias para proteger los datos y programas licenciados por la Universidad.

Eliminar Información de Manera Segura

Formas de Eliminar

- Reformatear el disco duro de la computadora
- Utilizar un programa especializado de eliminación segura para escribir caracteres aleatorios en múltiples pases sobre los datos
- Sustituir el contenido actual del disco duro con una imagen que no contiene datos privados
- Destruir el disco duro físicamente

Eliminar Información de Manera Segura

Apoyo del Personal de la OSI

- El personal departamental responsable por los datos privados en sus sistemas electrónicos deberán asegurarse que los datos y programas han sido removidos de los equipos que han de transferir fuera del departamento.
- Podrá solicitar apoyo de la OSI para cumplir con esta responsabilidad.
- OSI debe recomendar el programa de eliminación segura que se habrá de utilizar. Existen varias versiones libres de costo, disponibles a través del Internet.

Comienzo Anterior