

# Dominios .com.ar utilizados por Conficker

**Autor:** Raúl Batista

**Edición y Corrección:** Lic. Cristian Borghello, CISSP

**Fecha Publicación:** 06 de abril de 2009

**Publicado en** [Segu-Info](#)

## Introducción

Aparecido en octubre de 2008, el malware [Conficker](#) [1] (conocido también como Downadup o Kido) se aprovechaba de una vulnerabilidad de Windows parcheada a poco de ser explotada, el 23 de octubre de 2008 con el boletín de seguridad MS08-067.

Este malware se propagó (y aún lo hace) por sistemas Windows, debido a la demora de millones de usuarios en actualizar su sistema operativo e introdujo una novedad en su capacidad de auto-actualización: cada día genera distintos nombres de dominio de donde actualizarse.

## El problema

Estos dominios pueden ser previamente registrados por sus autores para que se descarguen de allí las actualizaciones correspondientes del malware, conformando una Botnet (y un problema de seguridad) de tamaño sin precedentes.

Recientemente se conoció una modificación en el gusano conocido como Conficker (variante C) mediante el cual genera 50.000 nombres de dominios pseudo-aleatoriamente en 116 [TLD](#) [2] diferentes, de los cuales intentará descargar actualizaciones generadas por sus autores. Con este diseño pretende sortear las dificultades anteriores, cuando sólo eran 250 dominios distintos por día y, los investigadores y organizaciones coordinados lograban bloquear muchos de esos dominios al registrarlos con anticipación.

*“Un dominio de nivel superior (TLD) es la parte final de un dominio de Internet; esto es, las letras que siguen al punto final de cualquier nombre de dominio”. Leer completo en [Wikipedia](#) [2]*

Distintos investigadores de seguridad, fabricantes de antivirus, empresas de seguridad, universidades y otros organismos gubernamentales y privados han reunido y organizado sus esfuerzos y hallazgos de una manera sin precedentes.

## Trabajo internacional

El grupo conformado se conoce como [Conficker Working Group \(CWG\)](#) [3] y, podría decirse que esta vez se **está a la altura de los acontecimientos**, para detener de cualquier forma posible esta amenaza.

Estudiando los recursos y recomendaciones dadas por CWG, se observa una que se dirige específicamente a los [operadores de los TLD](#) [4]; o sea los organismos responsables de registrar los dominios para un determinado país o tipo. Por ejemplo para los dominios de Argentina, terminados en **.com.ar**, el organismo responsable de administrar el registro de nombres en el DNS autoritativo para este TLD es **NIC.ar**.

CWG dice textualmente (traducido desde el inglés):

*“Como operador mundial de registro de dominios su organización está en una posición única de tomar medidas contra el Conficker. No solo pueden Uds, preservar e incrementar el prestigio de su marca internacionalmente, sino también la reputación de sus países”*

Con lo cual cada registro debe demostrar si también está a la altura de las circunstancias. Y continúa el CWG:

*“Los individuos tras esta amenaza sin duda se están apoyando en la probabilidad que los TLD elegidos no tendrán la motivación o recursos para tomar medidas contra la amenaza que han creado. Con su participación en este esfuerzo serán capaces de promover públicamente como se han involucrado en la mitigación de esta amenaza potencialmente desastrosa. En la medida que esta amenaza sigue evolucionando y creciendo en severidad, cada industria involucrada juega un papel importante en su mitigación. Nuestro éxito depende de la cooperación y colaboración a través de las industrias”*

El NIC local de cada país en particular tiene un compromiso ético, moral y profesional de colaborar para mitigar este problema.

El *Conficker Working Group* dice haber notificado con 3 semanas de anticipación a cada responsable de los TLD involucrados. Para el caso de Argentina, **NIC.ar** recibió este pedido:

*“Se requiere que actúe inmediatamente - faltan solo tres semanas para el 1° de abril, la fecha proyectada en la que los administradores de la red bot retomaran el control de la botnet - y le estamos pidiendo a todos los registrantes que actúen al menos, sino con más, de una semana antes en que los dominios vayan a ser registrados”*

Resumiendo, **NIC.ar** debe estar al tanto de este importante problema y sería bueno que comuniquen a los medios y a la comunidad sobre las actividades que se están llevando a cabo en este sentido, sobre todo con la gran cantidad de infecciones que se han reportado en Argentina.

## Estudio local

Desde [Segu-Info](#), se analizaron las predicciones realizadas por la *Universidad de Bonn* a través de ingeniería reversa del malware (el código fue publicado por dicha Universidad) y, de los 50.000 dominios diarios, se extrajeron los correspondientes a Argentina. El resultado muestra que aproximadamente 410 dominios diarios son .com.ar, es decir **12.982 para todo abril**. [Ver listado I](#) [5].

Se realizó también la consulta DNS de cada uno de esos dominios. El resultado obtenido es que ya se encuentran registrados 102 dominios, lo que generaría lo que se denomina **colisión**. [Ver listado II](#) [6].

Como la actualización de Conficker solo puede hacer uso de dominios registrados previamente, en el caso de los .com.ar podría obtener un registro nuevo pero dentro de los nombres ya previstos en la lista mencionada. Asumimos que estos dominios ya son conocidos y analizados por **NIC.ar** y razonablemente esperamos que estén bloqueando o investigando una nueva solicitud en caso de producirse alguna.

Pero, en el caso de los dominios en **colisión**, ¿qué pasa si están en uso y el servidor es vulnerable al punto de permitir que, en forma inadvertida por su propietario, un atacante logre dejar una actualización de Conficker?

**NIC.ar** está en posición única de comunicarse con los propietarios de esos 102 dominios ya existentes y advertirles para que tomen medidas preventivas, así como realizar el trabajo para los meses venideros.

**Nota:** no cualquier persona puede registrar y utilizar estos dominios para propagar otra amenaza, ya que Conficker, antes de actualizar su código, verifica que la nueva variante haya sido firmada digitalmente por sus creadores.

## Esperanzas

Algo que está públicamente claro es el esfuerzo y recursos conseguidos por el CWG y sus miembros y, es este esfuerzo el que debe ser imitado en el resto del mundo.

Falta saber si los NIC regionales están actuando, pues no conocemos de sus acciones o al menos no las han dado a conocer aún. **¿Estarán los NIC latinoamericanos a la altura de las circunstancias?**

Por lo pronto [NIC Chile el 31 de marzo](#) [7] ya se ha unido a un grupo de trabajo internacional, con quienes ha coordinado el bloqueo de todos los nombres de dominio en .cl que podría utilizar este gusano. De esta manera, se intercepta su operación y se evita su activación.

Mientras tanto en Argentina resulta difícil ser optimista viendo cuantos **domainers** ocupan espacios en rangos de dominios consecutivos tal como se ha visto recientemente a partir de la publicación de una lista de [dominios con caracteres multilingües](#) [8].

Esperamos que los hechos cambien y se prevean las posibles consecuencias, aunque por ahora no tenemos respuesta oficial en que basar esa esperanza.

**Más información:**

- [1] <http://www.segu-info.com.ar/conficker/>
- [2] [http://es.wikipedia.org/wiki/Dominio\\_de\\_nivel\\_superior](http://es.wikipedia.org/wiki/Dominio_de_nivel_superior)
- [3] <http://www.confickerworkinggroup.org/>
- [4] <http://www.confickerworkinggroup.org/wiki/pmwiki.php/TLD/TLDOperators>
- [5] <http://www.segu-info.com.ar/conficker/conficker-dominios.pdf>
- [6] <http://www.segu-info.com.ar/conficker/conficker-colisiones-registradas.pdf>
- [7] <http://www.nic.cl/anuncios/2009-03-31.html>
- [8] <http://www.segu-info.com.ar/articulos/94-nic-ar-habilita-uso-multilingue.htm>