Dorkbot: conquistando Latinoamérica

ESET Latinoamérica: Av. Del Libertador 6250, 6to. Piso - Buenos Aires, C1428ARS, Argentina. Tel. +54 (11) 4788 9213 - Fax. +54 (11) 4788 9629 - info@eset-la.com, www.eset-la.com

Autor:
Pablo Ramos
Especialista de Awareness & Research

Fecha:
Enero de 2012

Índice

Introducción

Desde el Laboratorio de Análisis de malware de ESET Latinoamérica investigamos y analizamos diariamente cuáles son las tendencias en relación al desarrollo de amenazas y códigos maliciosos en la región. Como resultado de este trabajo se realizó la investigación de **Dorkbot,** un código malicioso que en el último tiempo ha alcanzado el mayor índice de detección en Latinoamérica.

Su consolidación dentro del Top 10 del Ranking de Amenazas para Latinoamérica demuestra claras diferencias entre la región y el resto del mundo, lo cual motivó la presente investigación. Esta amenaza, marca una tendencia en relación a las técnicas de propagación utilizadas ya que Dorkbot logra propagarse explotando vulnerabilidades conocidas en los sistemas operativos para luego robar información y convertir al equipo infectado en parte de una red botnet.

A través de una investigación de esta familia de malware, se detallarán sus puntos fuertes y los motivos por los cuales ha tenido tan alto impacto durante la última mitad del 2011. En primer lugar, se presentan las variantes de esta familia de códigos maliciosos con el objetivo de conocer sus diferencias y cualidades técnicas como así también las metodologías de propagación y evolución.

En la segunda parte del artículo se analiza la propagación de esta amenaza en Latinoamérica y en los distintos países de la región, además de realizarse una comparación con el resto del mundo. Asimismo, se remarcan las diferencias entre las tendencias en la región y los índices de detección que registra este gusano, además de analizar una campaña de propagación puntual realizada para Latinoamérica. Para concluir, se verán las diferencias y el análisis de los motivos que llevaron a esta amenaza a posicionarse como el **código malicioso más importante de la región durante el 2011**.

Sus variantes

Dorkbot es un código malicioso que se propaga a través de enlaces en Internet y, luego de comprometer el sistema, infecta los dispositivos de almacenamiento extraíbles que se conecten a éste. Entre sus principales funcionalidades, cuenta con características que le permiten convertir el equipo infectado en parte de una red de equipos zombis (botnet). Una vez que el sistema está bajo el control del atacante éste puede realizar acciones como:

- Robo de credenciales de sitios web como **Gmail** y **Hotmail.**
- Ataques de denegación de servicio
- Bloqueo de direcciones IP
- Descarga y ejecución de otros códigos maliciosos
- Inyección de código en páginas web
- Propagación a través de redes sociales y mensajeros instantáneos, por ejemplo el chat de **Facebook** y **Windows Live Messenger**.
- Redirección de tráfico web para la realización de ataques de phishing.

Dorkbot es parte de una suite de herramientas, denominadas *crimepacks*, las cuales son utilizadas para crear malware y obtener beneficios de él. Los *crimepacks* pueden ser adquiridos por los cibercriminales con el objetivo de realizar ataques para el robo de información. Esto significa que una vez que cuentan con el paquete de construcción pueden realizar distintas campañas de propagación de códigos maliciosos a lo largo de la región.

Como parte del *crimepack*, el atacante obtiene un constructor (conocido como **NgrBot**) con el que puede indicar las configuraciones del código malicioso para cada caso en particular, como comandos personalizados, dirección del servidor, entre otros:

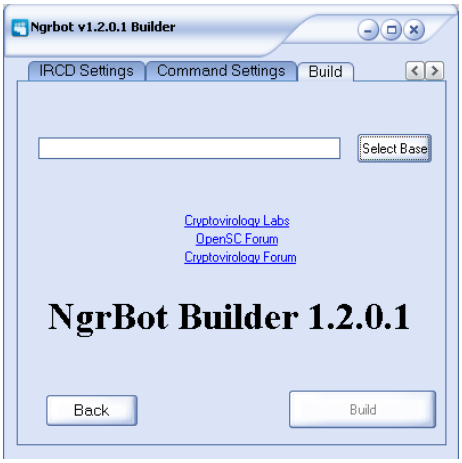

Imagen 1- NgrBot, constructor de Win32/Dorkbot.

Debido a las características mencionadas anteriormente, en conjunto con otras que serán presentadas a continuación, Dorkbot se ha convertido en uno de los códigos maliciosos más utilizados por los cibercriminales en Latinoamérica.

Para el análisis del mismo nos basaremos en las firmas creadas por ESET para la detección de esta familia de malware como así también en sus principales vectores de propagación. Las amenazas detectadas por ESET NOD32 Antivirus como *Win32/Dorkbot.A* y *Win32/Dorkbot.B* son dos variantes del código malicioso en sí. Por otro lado, las firmas *Win32/Dorkbot.C*, *Win32/Dorkbot.D* y *Win32/Dorkbot.E* son técnicas de propagación de este malware.

Dorkbot.A: el inicio

La primera variante del gusano fue detectada en abril del 2011 y recopila una serie de técnicas utilizadas por distintas amenazas para propagarse a través de los sistemas infectando dispositivos de almacenamiento masivo, tales como las memorias USB. Según ESET Live Grid, el sistema estadístico de ESET, el **16,20%** de todas las detecciones de Dorkbot en Latinoamérica pertenecen a esta variante.

Cuando el código malicioso se ejecuta por primera vez en un sistema crea una entrada en el registro de Windows:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

De esta forma, en el próximo inicio del equipo se ejecutará una copia del código malicioso que se almacena en **%appdata%\<nombre_malware>.exe**. Esta técnica ya es ampliamente utilizada y, de no existir protección antivirus, la amenaza se ejecuta al inicio del sistema.

Propagación en dispositivos de almacenamiento masivo

Para propagarse a través de dispositivos de almacenamiento masivo *Win32/Dorkbot.A* guarda una copia de sí mismo en ***%removabledrive%\RECYCLER%\<nombre_malware>.exe***. Luego, con el objetivo de asegurarse la ejecución de la amenaza al conectar el dispositivo USB en otro sistema, utiliza dos técnicas diferentes.

La primera, es una de las técnicas de propagación más conocidas y con mayor índice de detección: la creación del archivo ***autorun.inf***. Este archivo contiene la dirección en la cual se almacenó el gusano y hace uso del inicio automático de los sistemas de Microsoft hasta la llegada de Windows 7. La explotación de esta funcionalidad es detectada por ESET NOD32 Antivirus como *INF/Autorun*.

Por otro lado, la segunda técnica de propagación hace uso de la vulnerabilidad MS10-046 que afecta desde **Windows XP** hasta **Windows 7**. Este *exploit* utilizado inicialmente por el gusano Stuxnet, permitió infectar una gran cantidad de sistemas demostrando que, aún con el parche disponible, los usuarios siguen siendo vulnerables.

Para engañar al usuario, se modifican los atributos de las carpetas existentes como archivos del sistema, para ocultarlos, y se crean accesos directos de los mismos. Finalmente, cuando el usuario hace doble clic en el acceso directo de una carpeta para acceder a su contenido, se ejecuta la amenaza:

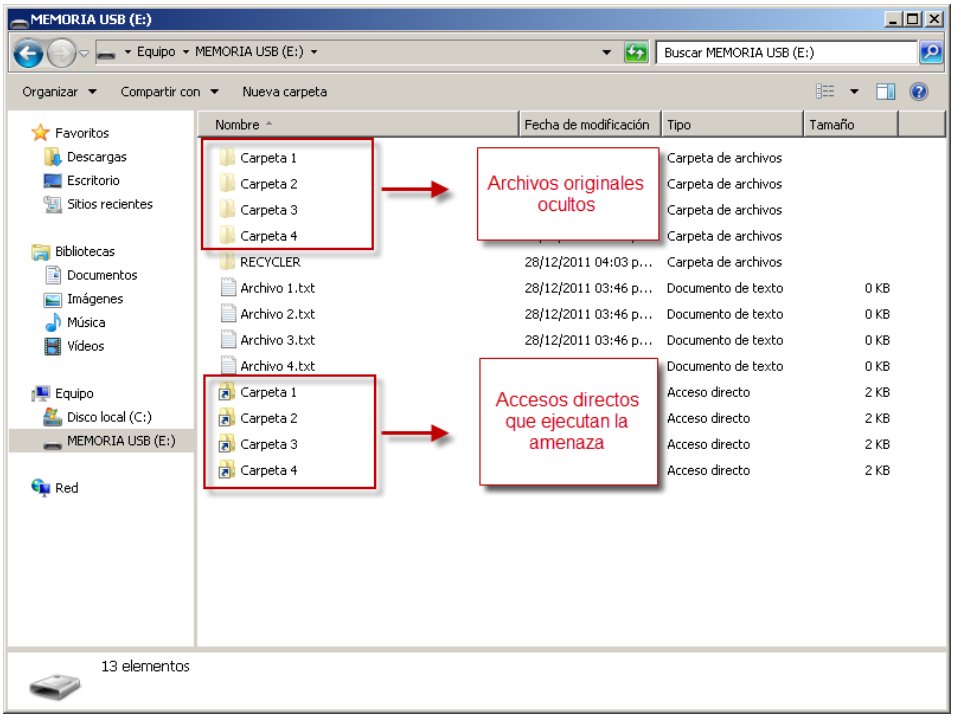

Imagen 2- Memoria USB infectada con Dorkbot

En la imagen anterior puede observarse el estado de una memoria USB conectada a un equipo infectado con una variante de Dorkbot. Este método ha resultado extremadamente efectivo y es una de las principales herramientas que le permitió a esta amenaza un alto índice de propagación.

Control remoto y robo de información

Una de las principales características de esta familia de códigos maliciosos es la capacidad de controlar un equipo de manera remota. A través del protocolo de comunicación **IRC** (*Internet Relay Chat*), Dorkbot recibe comandos que le permiten robar información de un equipo

infectado como por ejemplo las credenciales de acceso a **Hotmail**, **Facebook**, **Gmail**, entre otros servicios en línea.

Otra de las funcionalidades con las que cuenta este gusano es la habilidad de propagarse a través de servicios de mensajería instantánea. Mediante comandos remotos (también enviados desde el administrador de la botnet a los equipos zombis), esta amenaza se propaga utilizando **Windows Live Messenger**, el mensajero instantáneo de Microsoft.

Dorkbot.B: adiós Autorun

La segunda variante de esta familia de códigos maliciosos aparece a mediados del mes de mayo de 2011. Los cambios en relación a la primera versión de este código malicioso remarcan algunas tendencias en cuanto a los métodos de propagación utilizados.

En primera instancia, se dejó de utilizar la propagación a través de dispositivos de almacenamiento masivo mediante el **autorun.inf**. A partir de esta variante la infección de dispositivos USB se hace solo a través de la ejecución del código desde los accesos directos. Este cambio se relaciona directamente con: los sistemas operativos más utilizados por los usuarios en toda Latinoamérica (según el sistema estadístico online StatCounter, para la región, Windows 7 es el sistema operativo más utilizado con el 47,82%, dejando en segundo lugar a Windows XP con el 44,53%) y con la efectividad de esta técnica de propagación.

Nuevas funcionalidades

Entre los cambios más importantes que se agregaron a esta segunda variante de Dorkbot se incluye la **propagación a través del chat de Facebook**. La utilización de las **redes sociales** para la distribución de códigos maliciosos mediante técnicas de **Ingeniería Social** aumentó considerablemente el alcance del ataque.

Además, *Win32/Dorkbot.B* cuenta con la posibilidad de inyectar código de manera dinámica en páginas web cuando se accede desde un sistema infectado. Esto se hace por medio de *iframes*, un recurso del lenguaje HTML que permite referenciar un sitio externo dentro de la página actual. En otras palabras: cuando el usuario accede a una página web, el contenido puede ser modificado por el atacante. Un ejemplo asociado al robo de información es ingresar un campo más dentro de una página falsa que intenta replicar el sitio web de un banco, que solicite el PIN bancario al acceder al *home banking*.

Otra de las funcionalidades a remarcar de esta nueva variante se asocia con la posibilidad de redireccionar el tráfico de red. Los ataques de **phishing** son ampliamente utilizados en Latinoamérica con el objetivo de robar las credenciales de acceso al *home banking*. Es decir, que

cada vez que el usuario se conecta a un sitio web de este tipo, su usuario y contraseña serán enviadas al delincuente.

Las distintas campañas de propagación de esta amenaza la posicionan como la segunda variante de Dorkbot más utilizada en toda Latinoamérica con el 28,18% del total de detecciones. Uno de los principales motivos del porcentaje de detecciones para esta amenaza se basa en sus capacidades para el robo de información y propagación.

Dorkbot.C

La tercera variante de esta familia de gusanos centra sus actividades en la explotación de otra vulnerabilidad de Windows publicada en el boletín de seguridad MS04-011. Dado el éxito de las variantes anteriores, no ha sido muy propagada en la región.

Dorkbot.D: detección de enlaces directos

La utilización de accesos directos para engañar a los usuarios es uno de los métodos más eficaces para infectar un sistema desprotegido. Es por ello que la firma de esta variante detecta directamente los archivos LNK que contienen en su interior otras variantes de Dorkbot (mayoritariamente B). Se trata de una detección genérica y proactiva de la misma amenaza. La detección de esta variante representa el **55,58% del total de las detecciones de Dorkbot en la región**, confirmando este método de propagación como primario.

Cuando se intenta acceder al contenido dispositivo USB los archivos se encuentran ocultos. Por este motivo, una posible víctima solo puede hacer clic en los accesos directos y, sin saberlo, infectar el equipo. Esta acción es utilizada para la propagación de *Win32/Dorkbot.A* y *Win32/Dorkbot.B*.

Al analizar más en detalle este método de propagación, se puede observar que dentro de los accesos directos se oculta una cadena de texto. Cuando el usuario hace doble clic en él, se ejecuta el código malicioso.

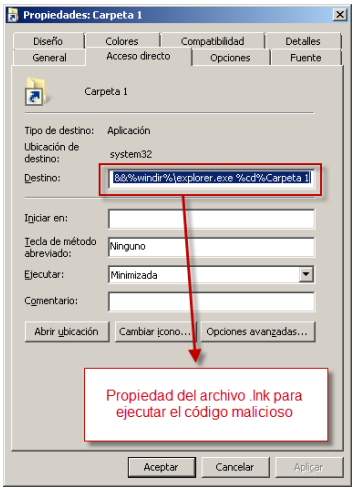

Imagen 3 - Propagación mediante accesos directos

Dentro del campo "Destino" que contiene la ruta a la que apunta el acceso directo, se almacena una cadena que contiene:

> *%windir%\system32\cmd.exe /c "start %cd%RECYCLER\<nombre_malware>.exe &&%windir%\explorer.exe %cd%Carpeta 1*

Cuando el usuario hace doble clic sobre el acceso directo para abrir la carpeta, se ejecuta el código malicioso y luego se abre una nueva sesión del Explorador de Windows en donde se muestra su contenido. De esta manera, Dorkbot intenta pasar desapercibido y, si el equipo no está protegido eficientemente por un antivirus, el mismo será infectado.

El nivel de detecciones de esta amenaza a nivel regional refleja la importancia de analizar los dispositivos USB con un *software* de seguridad cuando se conectan al equipo.

Dorkbot.E: inyector

La última firma correspondiente a esta familia de códigos maliciosos se refiere a distintas técnicas utilizadas por los cibercriminales para ocultar sus amenazas. La utilización de compresores o la ofuscación de código son detectadas proactivamente de esta manera, e internamente ocultan una variante de *Win32/Dorkbot.A* o *Win32/Dorkbot.B*.

Cronología en Latinoamérica

Desde la aparición de este código malicioso solo fueron necesarios unos pocos meses para que se consolide como una de las **amenazas con mayor índice de detección en la región**. La masificación de Dorkbot en Latinoamérica se ha diferenciado de lo que indican las estadísticas para el resto del mundo.

Durante el mes de diciembre de 2011, el porcentaje de propagación de esta amenaza en la región fue del 8%, mientras que en Europa fue del 0,8% y en Norteamérica fue de apenas del 0,26%. Desde el Laboratorio de Análisis e Investigación de ESET Latinoamérica se realizó el seguimiento de este crecimiento en los países de la región.

A solo a cuatro meses de su primera aparición, este código malicioso se consolidó dentro de las primeras 10 amenazas de la región. En el siguiente gráfico se puede observar la variación en las detecciones de Dorkbot en Latinoamérica:

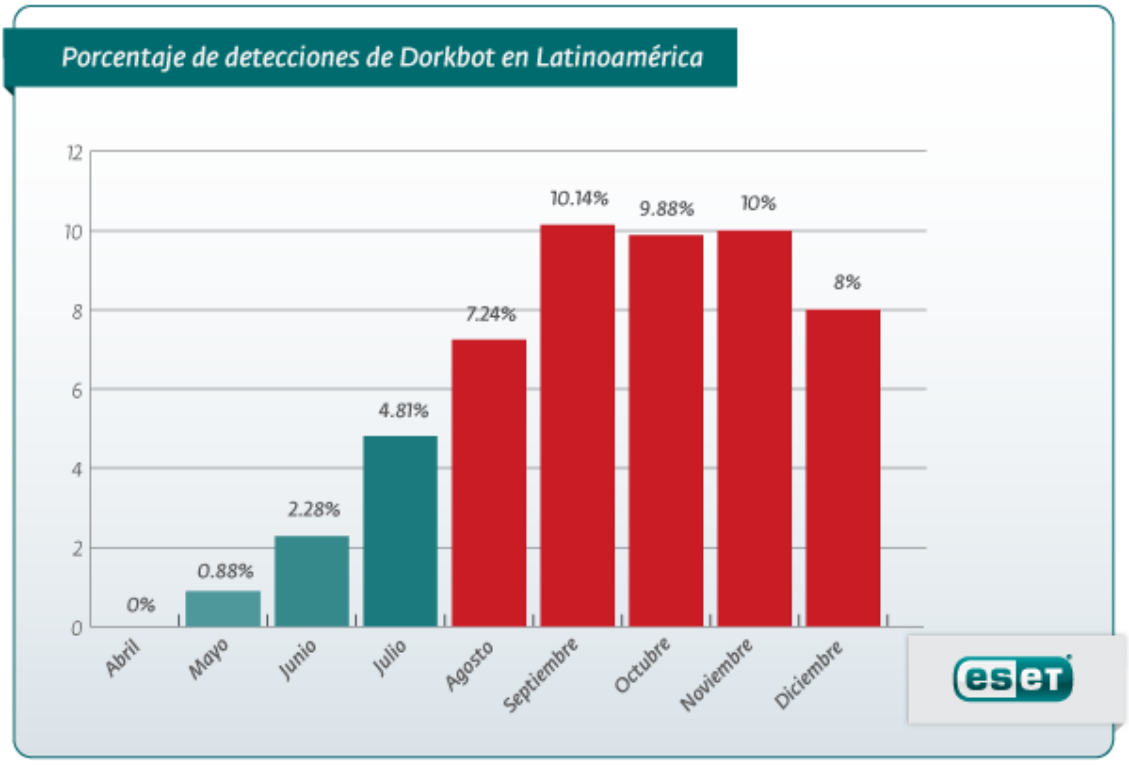

Imagen 4 - Detecciones por mes en Latinoamérica

Durante el último semestre del año el crecimiento de esta amenaza fue más que considerable: Dorkbot se ubicó entre los tres códigos maliciosos más detectados en Latinoamérica durante los últimos meses.

Análisis por país

La cantidad de detecciones de malware en Latinoamérica ha ido creciendo a lo largo de los años y han comenzado a observarse ataques dirigidos a usuarios de cada uno de los países y tal como se observará, Dorkbot tiene una distribución bastante marcada en distintos países de la región.

Sobre el total de detecciones para la región, el primer puesto lo tiene México, con el 38,86% del total, lo que significa que el código ha sido detectado en 4 de cada 10 equipos durante el 2011 en ese país. En segundo lugar se ubica Perú, con el 16,33%, y el podio lo completa Colombia con el 12,40%. A continuación se muestra el Top 10 de países donde más se propagó Dorkbot en Latinoamérica:

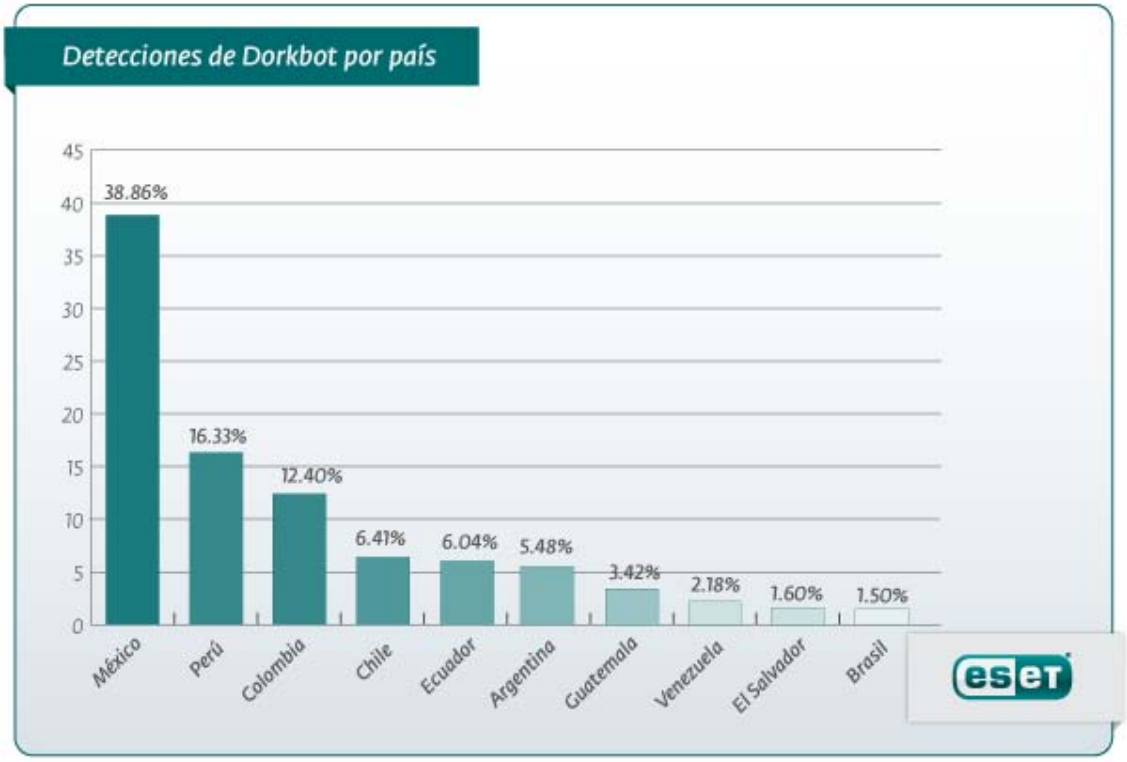

Imagen 5 - Ranking de detección por país

La distribución a lo largo de Latinoamérica en lo que respecta a la utilización de este código malicioso también difiere con el resto del mundo. Más del 65% de las detecciones se encuentran concentradas entre México, Perú y Colombia.

México es el país con mayor cantidad de detecciones: Durante el mes de diciembre, el 12% de las amenazas fue alguna variante de Dorkbot. Por otro lado, en Perú uno de cada diez equipos ha recibido esta amenaza durante el 2011. Finalmente, si bien Colombia está en el tercer puesto del ranking, la proporción de equipos que recibieron esta amenaza es aún mayor ya que casi el 15% del total de detecciones pertenece a la familia de esta amenaza.

La amenaza en el resto del mundo

Al comparar las estadísticas de Dorkbot a nivel mundial se puede diferenciar cómo esta amenaza está siendo propagada en Latinoamérica más que en el resto del mundo. Según cifras del sistema estadístico ESET Live Grid, es posible observar la distribución de las detecciones de esta familia de códigos maliciosos, indicándose en color rojo aquellos países con mayor porcentaje de propagación de Dorkbot respecto al total de detecciones de malware en dicho país:

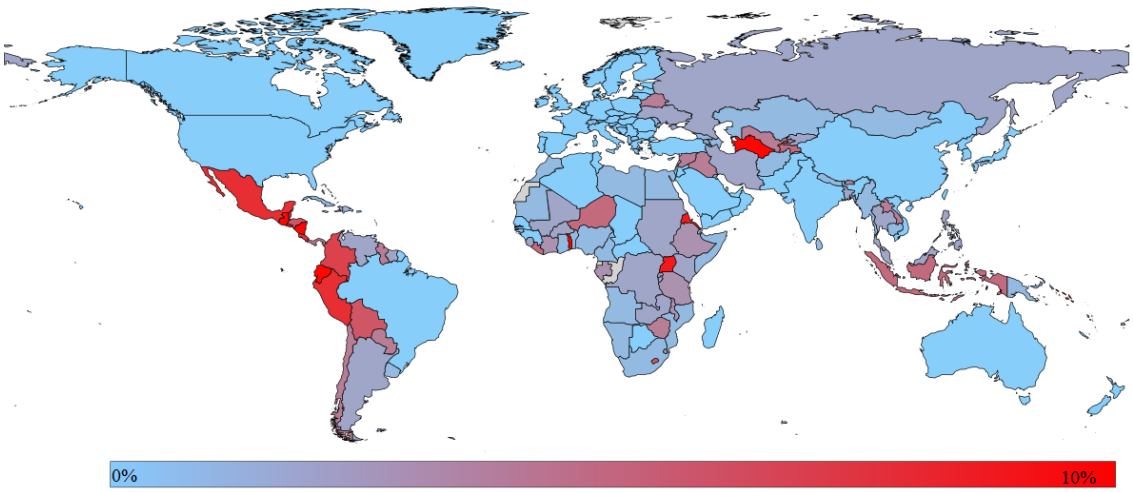

Imagen 6 – Dorkbot en el mundo

Al observar el gráfico también se observa la amplia utilización de esta amenaza en Centroamérica en donde, como se presentó anteriormente, se encuentran los países con mayor índice de detección de la región. Para los cibercriminales latinoamericanos, Dorkbot está teniendo un alto índice de efectividad, lo que se ve reflejado en las detecciones. La propagación

de esta amenaza en América Latina durante el segundo semestre del 2011, ubicándose en los primeros puestos del ranking, refleja las tendencias reportadas por ESET Latinoamérica para el 2012: robo de información y redes sociales.

Por otro lado, si se analizan los datos en cuanto a cantidad de detecciones, México y Perú lideran el ranking, ambos con la mayor cantidad de detecciones de Dorkbot durante el 2011, incluso más que en países como Rusia y Estados Unidos que cuentan con un gran número de usuarios:

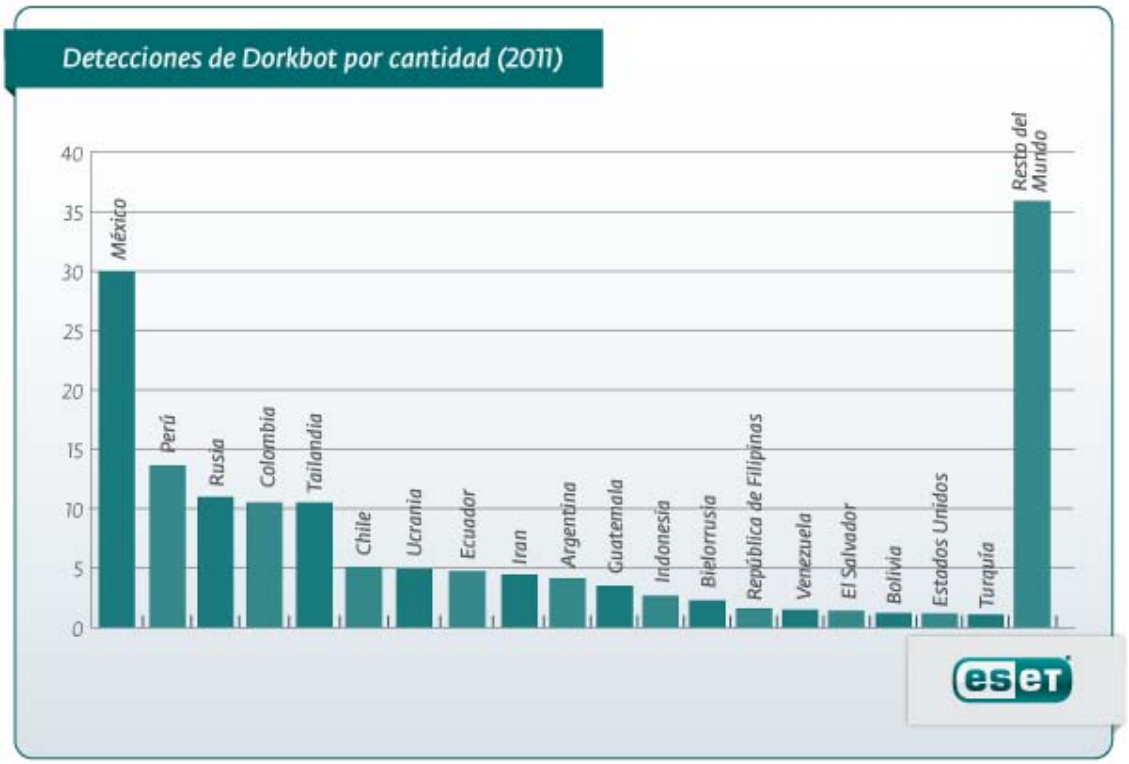

Imagen 7- Detecciones de Dorkbot por cantidad

Dentro de los **20 países con más detecciones de Dorkbot en el mundo, la mitad de ellos son latinoamericanos**: además de los ya mencionados México y Perú, aparecen Colombia (4º), Chile(6º), Ecuador (8º), Argentina (10º), Guatemala (11º), Venezuela (15º), El Salvador (16º) y Bolivia (17º).

Análisis de un caso en Latinoamérica

Como parte del trabajo de investigación del Laboratorio de ESET Latinoamérica, se realizó el seguimiento de un caso en la región, en el cual se recapitularán las capacidades de este código malicioso. La información capturada durante el análisis permite conocer los comportamientos de los cibercriminales en la región y cómo utilizan los sistemas infectados para el **robo de información**.

El siguiente análisis corresponde a una variante de *Win32/Dorkbot.B* que se propagó mayoritariamente en **Perú** con la finalidad de realizar **ataques de phishing**. Los objetivos de este ataque son bancos de ese país y de **Chile**.

Campaña de propagación

Originalmente el ataque se propagó como una supuesta recarga gratuita de una reconocida compañía de teléfonos celulares. Los usuarios que quisieran obtener este falso beneficio descargaban el código malicioso y al ejecutarlo infectaban su sistema.

Propagación en redes sociales y mensajeros instantáneos

Una de las acciones que se detectó durante en el seguimiento de este ataque es que los equipos infectados **utilizaban las redes sociales y los mensajeros instantáneos para continuar propagando la amenaza**. Desde el Centro de Comando y Control se envían mensajes para actualizar los mensajes de propagación y el intervalo con el que serán enviados.

En la siguiente imagen, se puede observar cómo el equipo zombi recibe las órdenes para comenzar a propagar por el chat de **Facebook** (comando *http.set*) y por **Windows Live Messenger** (*msn.set*) el siguiente mensaje: "*esta foto de hugo chavez agonizando es realmente impactante http://[ELIMINADO]/IMG00359268.JPG XD*".

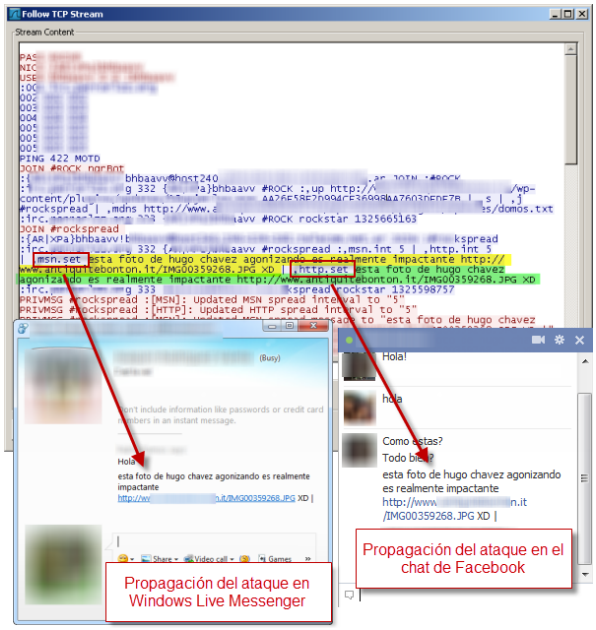

Imagen 8 - Propagación automática

Infección

La primera acción del código malicioso después de ser ejecutado es agregar una entrada al registro de Windows para iniciarse automáticamente la próxima vez que arranque el sistema.

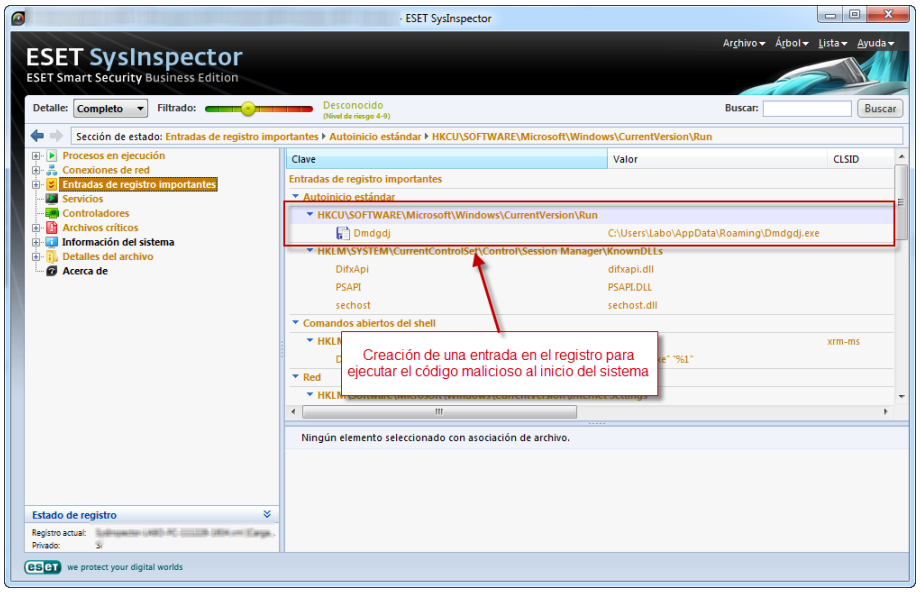

Imagen 9 - Inicio automático de Dorkbot

En la imagen se puede observar cómo ESET SysInspector, herramienta de diagnóstico desarrollada por ESET que permite ver los cambios en el sistema y el listado de archivos críticos, muestra la creación de una llave en el registro de Windows para ejecutar el archivo "Dmdgdj.exe" alojado en el disco C al iniciar el sistema. De esta manera, el atacante se asegura que siempre se ejecute su amenaza.

Otra de las acciones realizadas por Dorkbot es el contacto con el **Centro de Comando y Control** para registrar un nuevo bot (o equipo zombi) y comenzar a recibir órdenes. El **protocolo de comunicación** utilizado por esta familia de gusanos es **IRC** como se puede corroborar en la siguiente imagen:

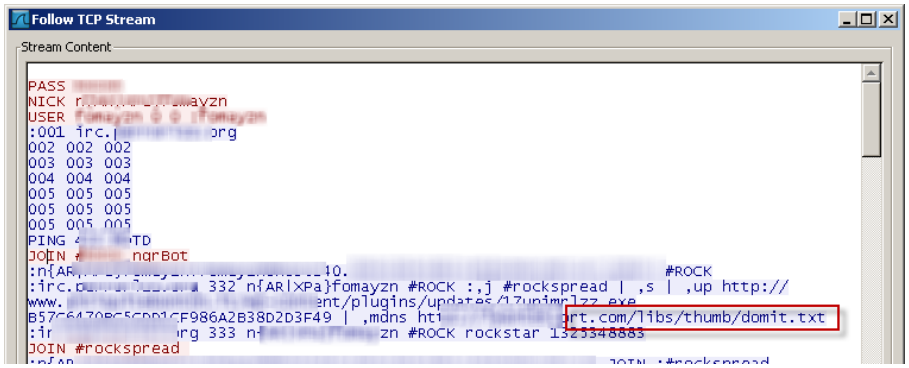

Imagen 10 - Conexión al servidor IRC

Cuando un nuevo equipo zombi se reporta recibe órdenes para actualizar el código remoto (comando *up*) y descargar el listado de direcciones URL (comando *mdns*). El contenido en el archivo **domit.txt** indica el listado de bancos de Perú y Chile en donde se realizará phishing al usuario infectado.

La información descargada será utilizada para modificar el archivo hosts del sistema operativo y redirigir al usuario a servidores falsos. Cuando el usuario intenta acceder a cualquiera de estas direcciones URL cae en una página falsa diseñada por el atacante. Cada vez que el usuario se conecte a estos dominios, también serán enviadas las credenciales de acceso del *home banking* al atacante.

Robo de información

Además del ataque de phishing y la propagación a través de las redes sociales, Dorkbot cuenta con un módulo de robo de información. Cuando el usuario se conecta a servicios como **Gmail**, **Facebook**, **Hotmail** o **Twitter,** las credenciales de acceso se envían al atacante. Este proceso se ejecuta cada vez que el usuario intenta iniciar sesión en alguno de estos servicios. La sustracción de datos personales le permite al atacante volver a propagar la amenaza con las credenciales obtenidas de los equipos zombis.

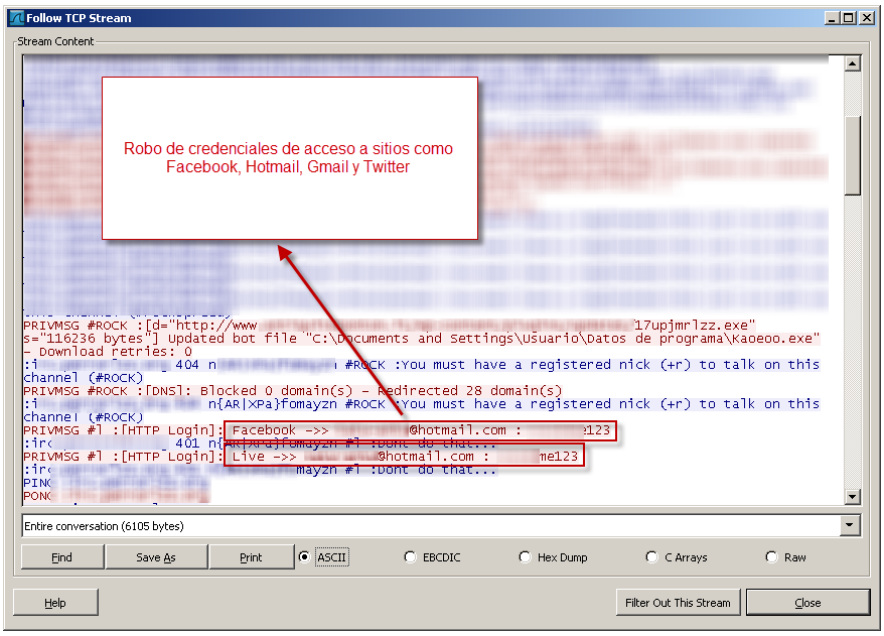

Imagen 11 - Robo de credenciales

Como pueden observar, se trata de un ataque complejo en el cual un equipo infectado queda bajo el control del atacante. De esta manera, todas las acciones que se realicen en el equipo y toda la información enviada puede ser monitoreada por el cibercriminal.

Es necesario remarcar que las posibles actividades que el botmaster puede realizar con un equipo zombi incluyen ataques de denegación de servicio o la inyección de código en páginas web.

Conclusión: de Autorun a LNK

La consolidación de Dorkbot como el código malicioso con mayor índice de detección de Latinoamérica refleja un cambio en las técnicas de propagación de amenazas de la región. En primera instancia, se observa cómo la masificación de las botnet se desarrolla a lo largo de todo el continente y la ejecución de ataques locales está en aumento.

Otro de los puntos a tener en cuenta en lo que respecta a las técnicas de propagación, es la utilización de los accesos directos para la infección de un sistema. Desde la aparición de Dorkbot, el índice de detección para otras familias de códigos maliciosos como *INF/Autorun* o *Win32/Autorun* ha disminuido considerablemente:

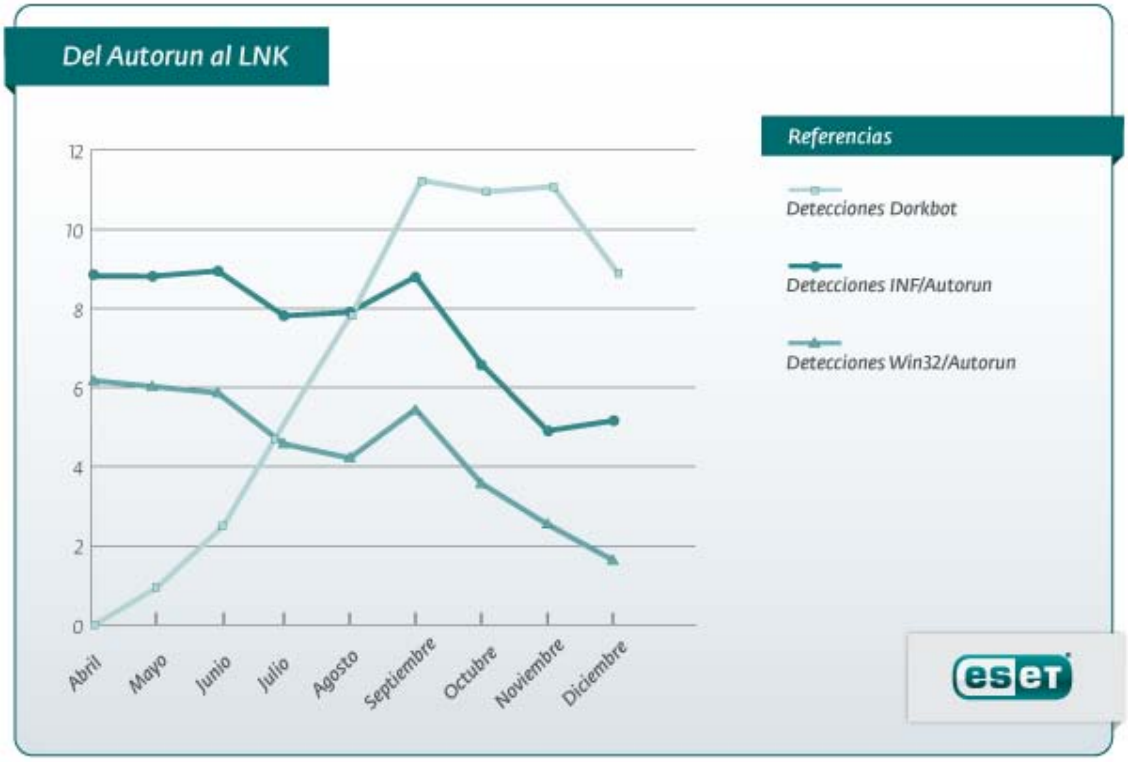

Imagen 10 – Relación entre detecciones de Dorkbot y Autorun

Uno de los principales motivos para este cambio en las técnicas de propagación utilizadas, está acompañado de la evolución de los sistemas operativos. En las últimas versiones de los productos de Microsoft, la ejecución automática de medios de almacenamiento extraíble se encuentra desactivada. Esta modificación lleva a los desarrolladores de códigos maliciosos a implementar nuevas técnicas de propagación y, en el caso particular de Dorkbot, han sido

efectivas y se ven reflejadas en las estadísticas de toda la región: **en 6 meses se consolidó como el código malicioso con mayor índice de detección para Latinoamérica**.

Dorkbot es el código malicioso con mayor crecimiento para Latinoamérica en el 2011, se ha propagado a través de dispositivos de almacenamiento masivo, redes sociales y mensajeros instantáneos con el objetivo de robar información. Sin embargo, el impacto que tuvo en Latinoamérica, a diferencia del resto del mundo, remarca la falta de conciencia en lo que respecta a la utilización de software licenciado y la instalación de los parches de seguridad. Además, es importante tener en cuenta que la educación es un factor muy importante en lo que respecta a la seguridad informática, ya que ayuda a mitigar los incidentes tanto para entornos hogareños como empresariales.