Cronología de un ataque en Skype

La propagación del gusano Rodpicom

ESET Latinoamérica | *info@eset-la.com* | *www.eset-la.com*

Indice

Autor:

Pablo Ramos – Security Researcher de ESET Latinoamérica

Co-autores:

Juan Forgia – Malware Analystis de ESET Latinoamérica

Matías Porolli – Especialista de Awareness & Research de ESET Latinoamérica

André Goujon – Especialista de Awareness & Research de ESET Latinoamérica

Joaquin Rodriguez Varela – Malware Lab Coordinator de ESET Latinoamérica

Sebastian Bortnik – Gerente de Educación y Servicios

Cronología de un ataque masivo en Skype

Introducción

Los ataques masivos de códigos maliciosos generan un gran impacto en los usuarios. En primera instancia los dejan vulnerables, desprotegidos, y en segundo lugar, demuestran cómo los cibercriminales pueden reutilizar técnicas antiguas para seguir afectando a miles y miles de usuarios. A mediados del mes de mayo, usuarios de todo el mundo comenzaron a recibir mensajes de sus contactos a través de distintos programas de mensajería instantánea como **Skype** y **Gtalk,** entre otros. Estos mensajes propagaban una nueva variante del gusano Rodpicom, detectada por los productos de ESET como *Win32/Rodpicom.C*, y en pocas horas este incidente se convirtió en una nueva epidemia de malware que, como manifiesta el presente artículo, no fue casualidad y continuó su actividad durante semanas, con varias decenas de actualizaciones, mensajes en distintos idiomas y la utilización de técnicas de evasión de detecciones e infección con un alto nivel de complejidad.

A lo largo del presente artículo, se repasarán cada una de las etapas de este ataque tratando de entender cuáles fueron las características que lograron saltar las barreras de protección de empresas, y remarcar una vez más que la combinación de técnicas de Ingeniería Social y códigos maliciosos pueden dejar vulnerables a los usuarios.

Entendiendo el ataque

En relación a la propagación de códigos maliciosos, existe un ciclo de vida entre cada campaña que realiza el atacante. Durante este período variable de tiempo, la efectividad del ataque puede cambiar, llegando por momentos a un valor máximo de efectividad ya sea por la cantidad de víctimas que infecta o usuarios que reciben la amenaza. Durante estos intervalos de tiempo, la probabilidad de que un usuario reciba algún mensaje, correo y/o vea algún tipo de propagación de una amenaza es mayor.

Cuando la cantidad de usuarios que reciben la misma amenaza, a través del mismo canal de propagación y en un corto período de tiempo supera cierto límite, se ven reacciones en cadena que sobrepasan los objetivos del atacante y comienza a caer fuera del grupo de usuarios que se eligieron como posibles víctimas.

En gran parte, todo este conjunto de situaciones convergieron el 20 de mayo, momento en el cuál además de las notificaciones del Sistema de Alerta temprana de ESET, llegaron consultas de usuarios afectados, e incluso comenzaron a llegar mensajes hasta de contactos que miembros del Laboratorio de ESET Latinoamérica tenían en sus cuentas de Skype. Este comportamiento fue uno de los primeros disparadores hacia el análisis y alerta a usuarios de la región sobre la aparición de un nuevo gusano, que se propagaba de manera masiva a través de toda la región y, seguramente, el resto del mundo.

La primera oleada: confusiones y proactividad

Durante el 20 de mayo, se propagaron en Internet mensajes a través de Skype que invitaban a los usuarios a ver una foto que había sido subida a distintas redes sociales[1]. Los enlaces que redirigían al usuario hacia la amenaza estaban acortados con el acortador de direcciones URL de Google que descargaban un archivo comprimido que contenía el código malicioso.

Esta amenaza era detectada por ESET Smart Security como una varitante de *Win32/Kryptik.BBKB*, y logró que más de 300 mil usuarios hicieran clic en los mensajes y descargaran la amenaza; el 67% de las detecciones provinieron de Latinoamérica. Tal magnitud indicaba que se trataría de un ataqué orientado pura y exclusivamente para usuarios que hablaran español, sin embargo, finalmente se descubrió que no era así.

Esta primera hipótesis surgió de la evolucíon en torno al origen de los clics. Si bien durante la primera etapa, Latinoamérica parecía ser la región más afectada, las campañas posteriores demostraron lo contrario: los horarios de creación y propagación de los mensajes coincidían con las primeras horas de la mañana de Europa.

El efecto de las primeras horas del ataque y las grandes cantidades de usuarios engañados por el uso de Ingeniería Social se vieron reflejados en los sistemas de acortadores de direcciones URL, como se puede observar en la siguiente imagen:

[1] Alerta, gusano se propaga velozmente vía Skype, más de 300 mil afectados http://blogs.eset-la.com/laboratorio/2013/05/21/alerta-gusano-propaga-velozmente-skype-100-mil-afectados/

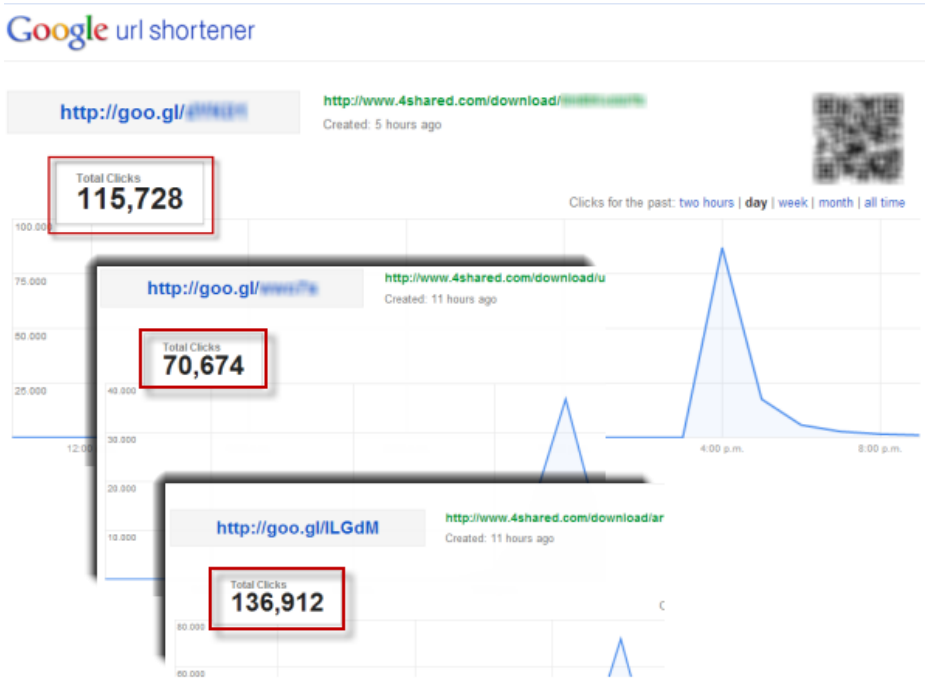

Imagen 1 – Propagación de enlaces maliciosos durante el 20 de mayo.

Asimismo, lo que en un inicio se detectó gracias a la Heurística Avanzada de los productos de ESET, luego de un primer análisis del Laboratorio se identificó como una variante de *Win32/Gapz*, un poderoso bootkit analizado por los laboratorios de ESET y capaz de inyectarse dentro del proceso *explorer.exe* con el objetivo de tomar control del sistema[2]. Luego de un análisis más minucioso, se pudo determinar que en realidad la amenaza era el ***dropper* PowerLoader**.

El fin principal de este **dropper** consta en evadir las protecciones del sistema, infectarlo e inyectar código malicioso dentro de los procesos. Entre sus actividades, descargaba otra variante de un código malicioso que era el encargado de propagarse a través de los mensajeros instantáneos. Esta amenaza fue detectada por ESET Smart Security como el gusano ***Win32/Rodpicom.C***[3], una amenaza normalmente utilizada en conjunto con otros códigos maliciosos para la propagación de malware a través de mensajeros instantáneos, y que todavía es altamente riesgosa.

Mensajeros y mensajes: las estadísticas del ataque

Hasta las primeras horas del 21 de mayo, todos los mensajes que se habían propagado desde los sistemas infectados utilizaban el acortador de direcciones URL de Google, sin embargo, esto cambió radicalmente a partir del segundo día de actividad. Las estadísticas que recolectó el Laboratorio durante el primer día de actividad, permitieron identificar cinco direcciones URL acortadas con ***goo.gl*** que en su totalidad generaron más de 495 mil clics durante toda la campaña.

Del total de los clics, **el 27% provino de algún país de América Latina:** entre los primeros tres se encuentran **México (27.023), Brasil (37.757)** y **Colombia (54.524).** En referencia a otros países afectados, podemos resaltar el caso de Rusia con un total de 41.107 y Alemania en el primer puesto global con 84.817 clics durante esta primera oleada.

Además, un dato relevante es que el 85% de los clics provinieron de alguna versión de Windows, por lo que 8 de cada 10 usuarios que cayeron en el engaño utilizaban algún sistema operativo de Microsoft:

[2] Is Gapz the most complex bootkit yet?: http://www.welivesecurity.com/2013/04/08/is-gapz-the-most-complex-bootkit-yet/ http://www.welivesecurity.com/wp-content/uploads/2013/04/gapz-bootkit-whitepaper.pdf
[3] *Win32/Rodpicom*: http://www.virusradar.com/en/Win32_Rodpicom.A/description

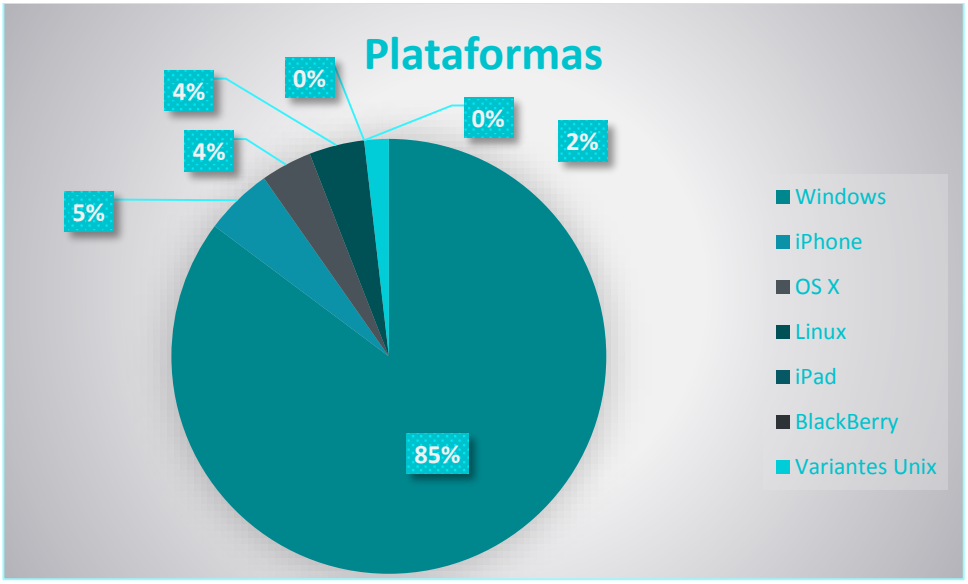

Imagen 2- Distribución de plataformas afectadas por el ataque en Skype durante el primer día.

La distribución por sobre los sistemas operativos utilizados por los usuarios es lógica en relación a la distribución del mercado, pero no representa ningún valor específico sobre la cantidad de infecciones reales del ataque. El valor real de infectados es muy dificil de determinar, pero claramente la técnica de Ingeniería Social utilizada ha probado una vez más ser altamente efectiva.

El mensaje utilizado por los equipos infectados variaba de un momento a otro, pero todos los contactos de la víctima recibían un mensaje similar al que se observa en la siguiente imagen:

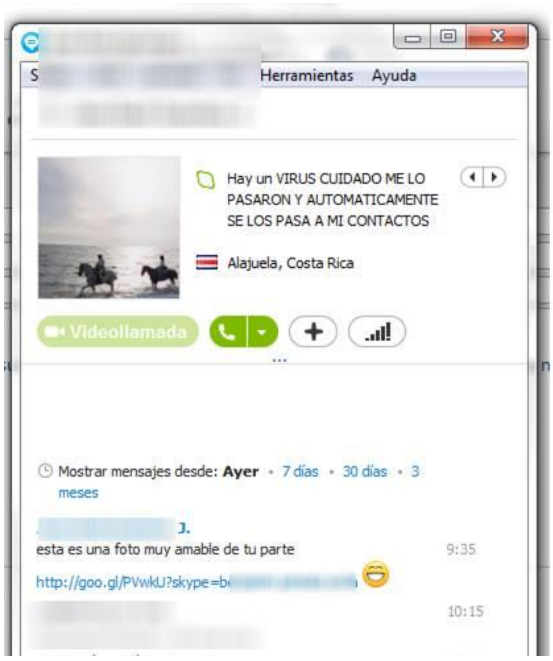

Imagen 3 - Mensaje de propagación de un usuario infectado con Win32/Rodpicom.

Esta misma imagen se reprodujo en miles de casos en los cuales usuarios desprotegidos eran engañados e infectaban sus sistemas con este pack de códigos maliciosos. Los cinco enlaces utilizados y registrados durante las primeras veinticuatro horas del ataque redirigían a los usuarios a tres archivos diferentes con los nombre del tipo:

- Fotos91-lol.zip
- Fotos92-lol.zip
- Fotos93-lol.zip

Todos los enlaces que estaban acortados con el acortador de URL de Google redigirían a los usuarios a 4shared[4], un servicio de hosting de archivos, a excepción de uno que utilizaba otro servicio. Nuevamente, ninguna de estas combinaciones es novedosa, hecho que llama la atención y plantea dudas sobre por qué los niveles de efectividad y repercusión han sido tan elevados. Con los datos que presentamos hasta el momento, es posible asegurar que esta es una de las campañas más grandes que se ha propagado a través de Skype.

La segunda oleada y la periodicidad: repitiendo la fórmula de éxito

En los días posteriores a la primera oleada de mensajes, los cibercriminales responsables de este ataque continuaron utilizando distintos mensajes y nuevas variantes de sus códigos maliciosos. Esto no incrementó, como era de esperar, la cantidad de usuarios que cayeron víctimas del engaño, pero sí generó nuevos y distintos mensajes.

En este contexto, el impacto y la sorpresa que generaban los mensajes no fueron tan efectivos como en el inicio, sin embargo, esto no desanimó a los cibercriminales, quienes comenzaron a utilizar distinos servicios de acortadores de URL para lograr que los usuarios descarguen sus códigos maliciosos:

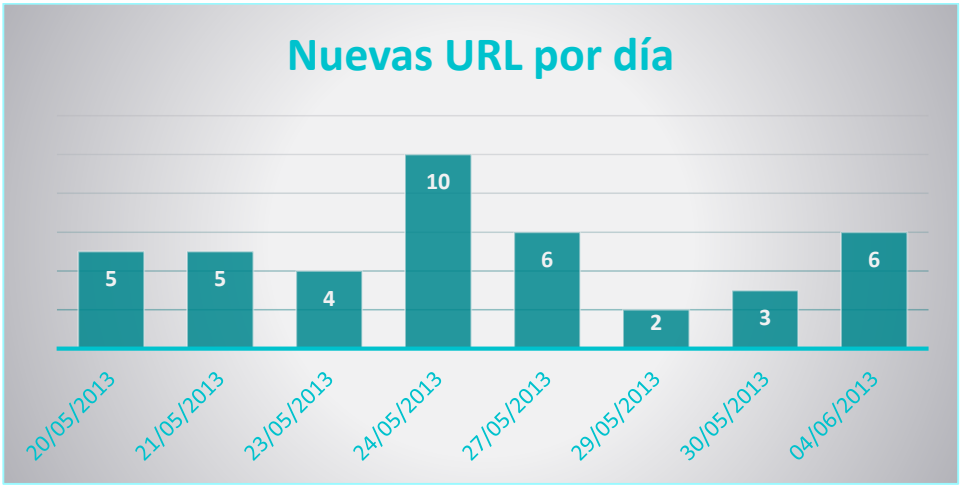

Imagen 4 - Cantidad de enlaces utilizados por día en campañas de propagacíon de malware.

Durante un período de dos semanas, se observaron un total de **cuarenta y un enlaces diferentes** redirigiendo a los usuarios a distintos códigos maliciosos. Además, se usaron diferentes servicios de acortadores de URL, entre los que podemos destacar:

- Goo.gl
- bit.ly
- ow.ly
- urlq.d
- is.gd
- fur.ly

No todos los servicios de acortadores de URL proveen de información acerca de los clics y otros datos como sistemas operativos, referrers, etc, sin embargo de los que sí fue posible recuperar información se contabilizó un total de 766.957 clics.

Los registros de cada uno de los enlaces y la cantidad de clics de los usuarios permiten observar que a medida que avanzaron las horas, el flujo de usuarios continuaba hacia las diferentes variantes de este código malicioso. Durante la propagación, desde el Laboratorio de Análisis e Investigación de ESET Latinoamérica se realizó un seguimiento detallado sobre la efectividad de cada variante permitiendo ver qué enlace fuemás eficaz, y los horarios y picos de propagación:

[4] Servicio para compartir archivos: http://www.4shared.com/

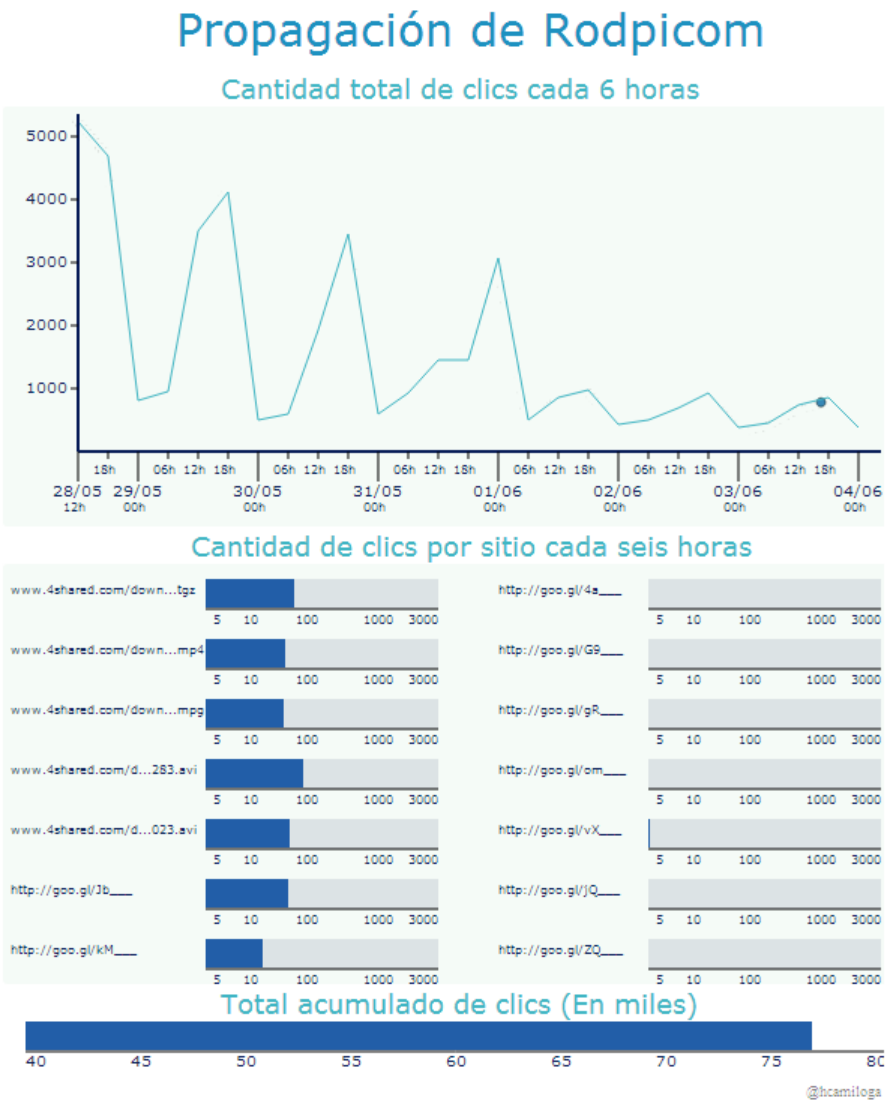

Imagen 5- Propagación de Rodpicom en función del tiempo.

El resultado del análisis evidencia una baja en las infecciones a medida que avanzó el tiempo, y que la misma técnica dejó de ser efectiva a medida que los usuarios fueron alertados y se enteraron de la situación. Tal información permite ver de qué manera un cibercriminal aprovecha el desconocimiento y la falta de protección del usuario. [5]

De Internet para el mundo

A medida que el número de clics y la cantidad de mensajes aumentaba, el proceso de obtención de información y distribución de los usuarios afectados se hizo más claro y las secuelas de algunos sistemas utilizados para el seguimiento dejaron muchos datos para analizar.

Observando los gráficos y estadísticas de propagación, quedó casi comprobado que **los países más afectados no son de Latinoamérica**[6], sin embargo, miles de usuarios fueron engañados por mensajes que ni siquiera estaban dirigidos hacia ellos, y al hacer clic, se infectaron y de esta manera, la propagación se extendió a todos sus contactos. Además, como se podrá observar posteriormente, los mensajes ni siquiera estaban escritos en español.

[5] Visualizando la propagación del gusano Rodpicom en Skype: http://blogs.eset-la.com/laboratorio/2013/06/07/visualizando-propagacion-gusano-rodpicom-skype/

[6] Gusano en Skype: Rodpicom acumula más de 700 mil clics y se confirman nuevos medios de propagación: http://blogs.eset-la.com/laboratorio/2013/05/28/gusano-skype-rodpicom-700-mil-mensajeros/

Lo sucedido con el „**Gusano de Skype“** demostró tener un alto grado de propagación, casi a niveles exponenciales durante los primeros días de funcionamiento, logrando que por cada nueva víctima todos sus contactos de **Skype**, **Gtalk** y otros sistemas de mensajería instantánea recibieran estos enlaces maliciosos.

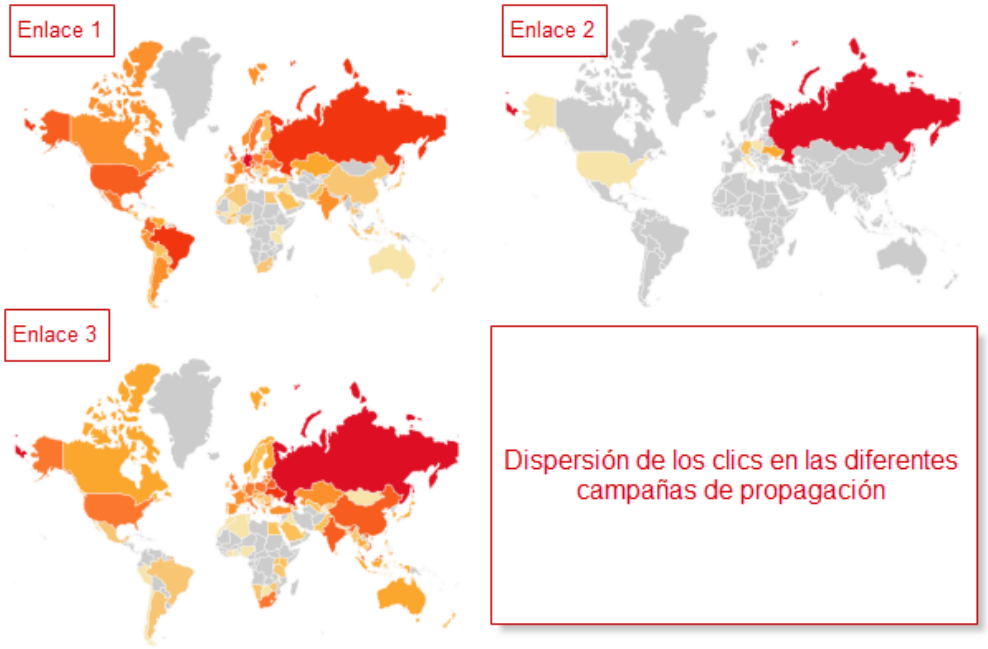

Imagen 6- Dispersión geográfica de los clics en enlaces de bit.ly.

La dispersión de clics a lo largo del mundo varía según el enlace, sin embargo, se puede ver el alcance que estos cibercriminales han obtenido, sin siquiera ser concientes de la cantidad de infecciones que esto puede significar o los objetivos que estaban persiguiendo.

Una vez que cesó la distribución de mensajes y campañas de propagación, el funcionamiento de los equipos infectados era aparentemente normal, pasando inadvertido ante los ojos de los usuarios que, sin saberlo, continuaban utilizando equipos infectados. En algunos casos, se han encontrado más de 30 actualizaciones del código malicioso alojados carpetas del sistema.

Explicando los ataques

Luego de dos semanas de actividad y seguimiento, mucha información quedó disponible para analizar, no solo en relación a la amenaza y cómo se propagaba, sino también a la cantidad de códigos maliciosos y versiones de archivos utilizados durante el ataque. Varias familias de malware se vieron involucradas a medida que los días avanzaron, lo que indica que los cibercriminales tomaron distintas acciones según el caso.

Las armas de los cibercriminales

Dentro de las distintas familias de códigos maliciosos existentes, es posible encontrar amenazas que cumplen funciones determinadas, como *droppers*, *downloaders*, *information hijackers*, *rootkits* y hasta incluso códigos maliciosos que se encargan de explotar vulnerabilidades de los sistemas operativos para robar información el usuario. En el ataque que involucró al "gusano de Skype", el equipo de investigación de ESET detectó más de veinticuatro ***hashes*** diferentes entre más de 130 archivos.

Las dos principales amenazas involucradas correspondían a variantes de Win32/PowerLoader, como el encargado de infectar al sistema y reportar al C&C (Panel de Comando y Control) y Win32/Rodpicom, un gusano capaz de propagarse a través de distintos mensajeros instantáneos.

Power Loader, un dropper problemático

Lo que durante el primer momento del ataque parecía ser una variante del código malicioso *Win32/Gapz* terminó con la identificación y detección específica del ***dropper*** utilizado en otros ataques: ***Win32/PowerLoader***. Tal como lo aclara Aleksandr Matrosov[7], miembro del Laboratorio de Investigación de ESET, Power Loader es un constructor de ***bots*** para la creación de amenazas conocidas como "*downloaders*" y un claro ejemplo de la especialización y modularidad del mundo del cibercrimen.

El constructor de Power Loader se filtró en la red a principios de año y además también se ha encontrado en variantes de otro código malicioso con mucho impacto en la región: ***Win32/Dorkbot***. Esta herramienta del cibercrimen le permite a los atacantes especificar hasta tres direcciones URL a las cuales se contactará el equipo infectado para descargar un malware y ejecutarlo en el sistema.

En relación al archivo malicioso involucrado en este ataque, la configuración contenía los siguientes datos:

```
[main]
srvurls=hxxp://r.gigaionjumbie.biz/images/gx.php;hxxp://x.dailyradio.su/images/gx.php;hxxp://w.kei.su/images/gx.p
srvdelay=15
srvretry=2
buildid=REE
```

En otras palabras, se identificaron tres direcciones URL correspondientes a los C&C de la *botnet*, como así también otros datos de la configuración, como cantidad de reintentos y el temporizador. Una vez que el equipo está infectado, se contactará cada 15 minutos con el panel de control para descargar distintas variantes de la amenaza u otros archivos ejecutables que podrán ser utilizados por los atacantes para diversas actividades. Esta acción de configuración es la principal causante de que los sistemas infectados con este código malicioso propagaran los mensajes cada 15 minutos.

Más allá de la complejidad técnica de *Power Loader* para ocultar su comportamiento, su objetivo es claro: infectar al sistema y descargar una muestra desde algún sitio en Internet. Esta acción permite que los cibercriminales puedan conocer con detalle qué sistemas han sido infectados, ya que una vez que se ejecuta el código este reportará al C&C dónde envía algunos datos del equipo a través de una comunicación cifrada:

[7] Gapz and Redyms droppers based on PowerLoader Code: http://www.welivesecurity.com/2013/03/19/gapz-and-redyms-droppers-based-on-power-loader-code/

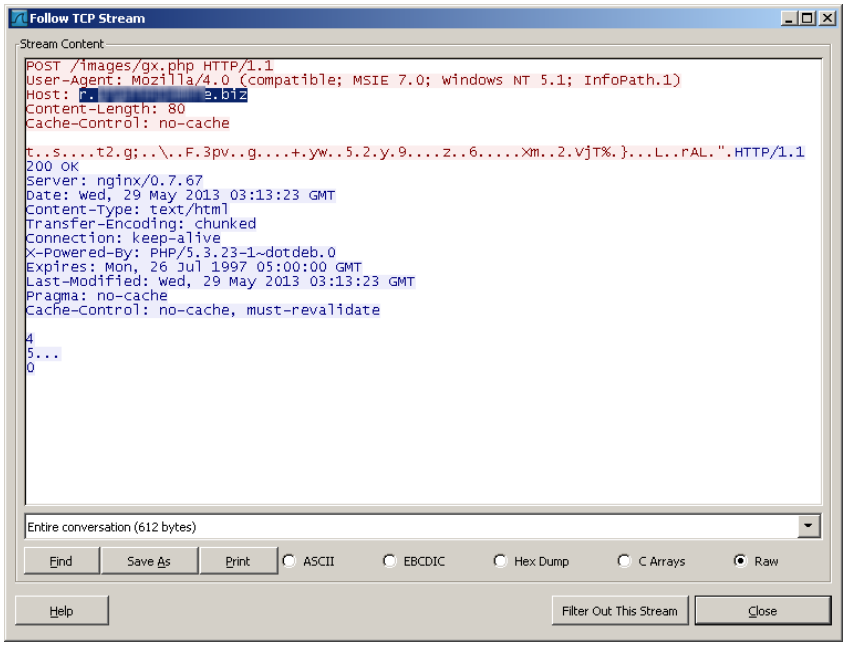

Imagen 7- Captura de tráfico del reporte de un bot.

Todos los otros códigos maliciosos descargados por el ***dropper***, son almacenados en el directorio "C:\ProgramData" y durante los días de actividad se registraron **más de 50 archivos en un solo equipo**:

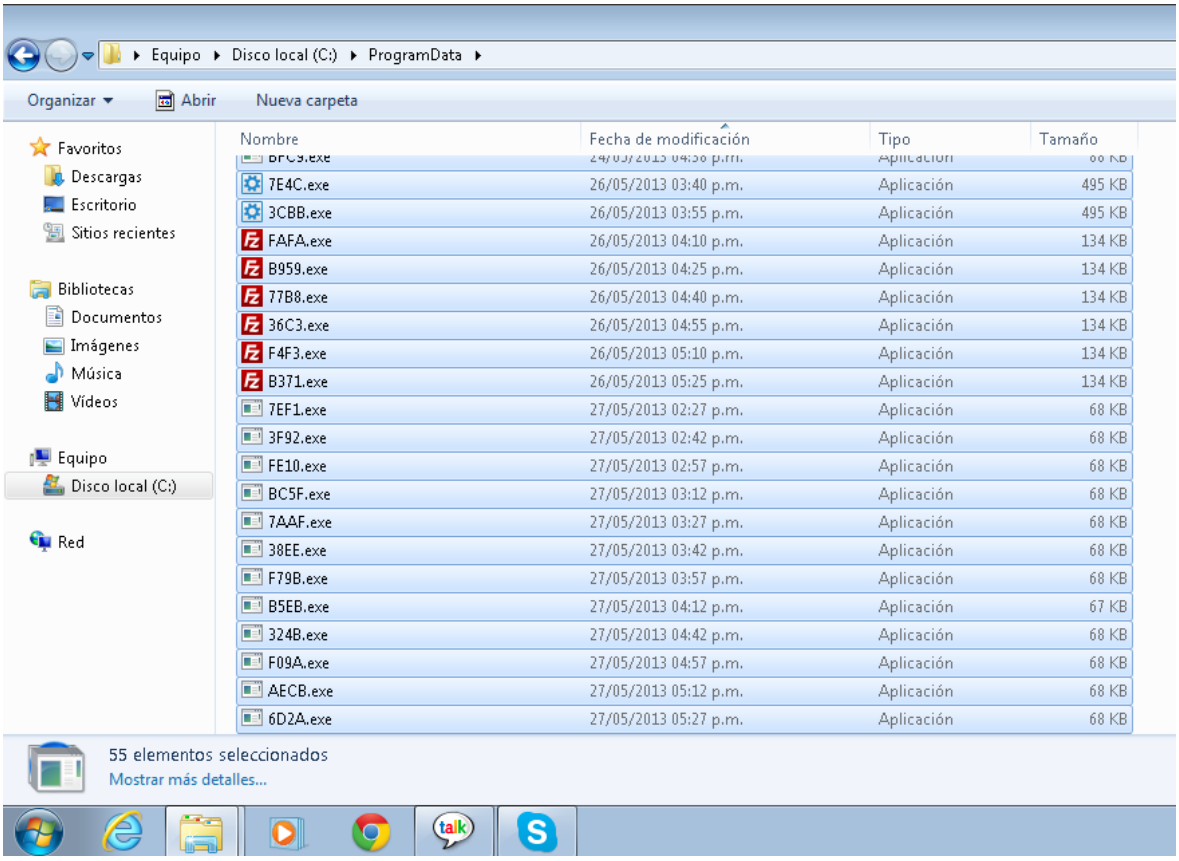

Imagen 8 - Actualización de archivos descargados por el dropper Win32/PowerLoader en un sistema infectado.

Tal como se puede corroborar, se descargaban múltiples archivos diariamente y se almacenaban en el mismo directorio, una acción que demuestra cierta desprolijidad y que se suele ver frecuentemente en el mundo del cibercrimen. En caso de que el usuario no se haya percatado de la infección, los ciberdelincuentes podrían continuar actuando en su sistema y tener acceso a su información.

Entre los códigos maliciosos involucrados en la segunda etapa del ataque, se encuentran las siguientes familias:

- Win32/Injector[8]: normalmente, esta familia de malware se inyecta dentro de otros procesos y puede capturar contraseñas y nombres de usuarios de entidades financieras y otros servicios en línea, como por ejemplo credenciales de redes sociales. Existen determinadas variantes que les permiten a los atacantes conectarse remotamente al sistema infectado.
- Win32/Agent[9]: una familia de códigos maliciosos que suele recolectar información del usuario y enviarla hacia un sitio externo.
- Win32/Rodpicom: este gusano normalmente se utiliza en conjunto con otras amenazas y su función principal es la de propagar enlaces maliciosos a través de aplicaciones de mensajería instantánea.

A continuación, se presenta un análisis más profundo de la variante encontrada durante el caso de Skype.

Rodpicom, el gusano de los mensajes

Hasta el momento, la parte más visible del ataque fue el gusano Rodpicom[10]. Este código malicioso busca en la memoria del sistema los procesos correspondientes a los programas de mensajería instantánea, accede a ellos y reenvía a todos los contactos de la víctima distintos mensajes de propagación que contienen malware o cualquier otra amenaza informática.

Rodpicom no actúa solo y es común que sea utilizado por otras amenazas como un vector de propagación. Cabe destacar que, este gusano elegirá el idioma del sistema para propagarse. En otras palabras, las personas detrás de este ataque no diseminaron su ataque a través de todo el mundo, sino que como el gusano envía mensajes a todos los contactos de la víctima, esto generó que los niveles de propagación llegarán a casi 750 mil usuarios a hacer clics al recibir tales mensajes.

En las dos semanas de propagación de este ataque, se han identificado un total de 69 archivos detectados por los productos de ESET como variantes de Win32/Rodpicom.C, correspondientes a 5 *hashes* diferentes:

SHA 1	Cantidad de veces que se propagó
19474f2e66ac366e89dc788d2292b35534bb2345	3
357b9a728da740f587e04daf1a8ad2603daf924e	12
381d82f5b5349e2a67f28f41dac9a306a8c5a604	9
c178a3c73dd711ffb920747bd44ae61fdc30aebd	1
e2d3634b1ea861e1b6d271fd3ffdcfaa1e79f1d5	44

Una vez que el código malicioso se activa, lista todos los procesos en ejecución y los recorre buscando algún programa de mensajería instantánea a través del cual se pueda propagar, como lo que se enumera a continuación:

- Skype
- Windows Messenger
- Quite Internet Pager
- GoogleTalk
- Digsby

Particularmente, Digsby permite configurar muchos clientes de mensajería instantánea, incluso a Facebook Messenger. Esto demuestra una vez más que, un código malicioso técnicamente sencillo es capaz de generar un impacto muy importante entre los usuarios, las empresas y organismos que utilizan sin protección distintas aplicaciones de mensajería instantánea.

El impacto que generó este gusano fue significativo, por lo menos en Latinoamérica. Esto se puede comprobar por la cantidad de clics que los usuarios de la región hicieron sobre los enlaces y las alertas y solicitudes de ayuda que ESET Latinoamérica recibió durante las primeras horas de propagación.

---

[8] Descripción de una variante de Win32/Injector: http://www.virusradar.com/en/Win32_Injector/description
[9] Descripción de una variante de Win32/Agent: http://www.virusradar.com/en/Win32_Agent.ODG/description
[10] Descripción de Win32/Rodpicom: http://www.virusradar.com/en/Win32_Rodpicom.A/description

Un solo ataque, muchas armas

A modo general, es importante entender que se trata de una ataque planificado, que los cibercriminales querían lograr grandes tasas de infectados y una propagación masiva. Además, no debemos dejar de lado que muchas de las actualizaciones y cambios en los mensajes recibidos o ejecuciones de nuevas campañas comenzaban alrededor de las 9:00 AM del horario europeo. Este hecho coinicide con los ingresos laborales, donde el tráfico de comunicación a través de las redes sociales y sistemas de mensajería instantánea es mayor.

Un conjunto de cuatro códigos maliciosos diferentes fueron suficientes para poner en alerta a miles de usuarios y organizaciones, que vieron sus defensas vulnerables a técnicas que se creían olvidadas y estaban asociadas a aplicaciones ya en desuso, como el Windows Live Messenger.

La combinación de múltiples amenazas en un solo ataque no es una novedad, pero nuevamente demostró ser extremadamente efectiva. Además, cada una de las características de los códigos maliciosos involucrados cumplieron una función específica. **Power Loader** se utilizó como un *dropper* práctico y eficiente, capaz de **saltar las protecciones de seguridad, infectar el sistema** descargando distintas amenazas y ejecutándolas en el sistema. ***Rodpicom*** logró proporciones de propagación altísimas durante las primeras horas de actividad y luego, al modificar los enlaces con nuevas variantes, logró afectar a más usuarios. Finalmente, las dos familias de códigos maliciosos restantes son utilizadas en el mundo del cibercrimen para extraer información de los sistemas infectados incluyendo contraseñas, nombres de usuarios, archivos y distintos tipos de información sensible.

Lecciones aprendidas

Los sucesos comprendidos entre el 20 de mayo y los primeros días de junio dejaron al descubierto que técnicas con años de antigüedad tienen niveles de efectividad lo suficientemente buenos para causar daños. Distintas organizaciones vieron sus soluciones de seguridad vulneradas, alertas al por mayor sin entender qué era lo que pasaba hasta que paulatinamente se aclaró el panorama y se identificaron las amenazas.

Toda una red de una empresa puede verse afectada por cada usuario corporativo que caiga en un engaño de este tipo, y no por la complejidad de la amenaza, sino por el impacto que esto podría tener en caso de propagarse a clientes, proveedores y otros contactos importantes que hoy en día se suelen administrar desde distintas aplicaciones.

Para los usuarios hogareños, el impacto puede parecer menor, sin embargo, tienen una mayor exposición a este tipo de riesgos ya que las temáticas utilizadas están mayoritariamente relacionadas a las redes sociales, como por ejemplo fotos o comentarios en **Facebook**.

Otro factor que salió a la luz con toda la actividad que generó el gusano Rodpicom, está relacionado con las tecnologías que utilizan los usuarios para conectarse a Internet. En este caso en particular, los cibercriminales buscaban atacar a usuarios que utilizarán alguna versión de Microsoft Windows.

Sin embargo, al analizar las estadísticas de los acortadores de direcciones URL, es posible identificar las diferentes plataformas que los usuarios utilizaron para seguir los enlaces maliciosos y cómo se podrían exponer a otros tipos de amenazas. Tal como se mencionó anteriormente, más del 80% de los usuarios que siguieron los enlaces propagados utilizaban alguna variante de Microsoft Windows y, además, es posible identificar los navegadores utilizados por las posibles víctimas:

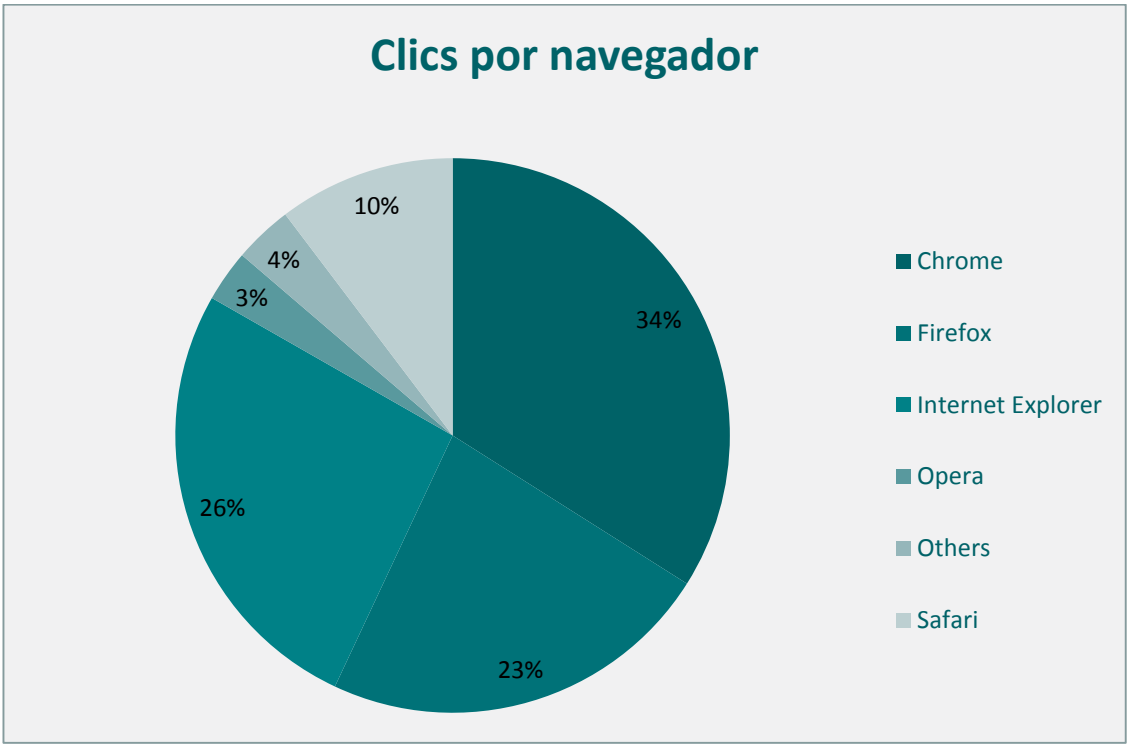

Imagen 9 - Navegadores utilizados por las posibles víctimas.

Esto corresponde con datos ya conocidos acerca de cuáles son navegadores preferidos por los usuarios al momento de navegar en Internet y, además, que la identificación de los mismos por parte de los atacantes les puede permitir distintos tipos de ataques.

Conclusión

El 85% de los usuarios que cayeron en el engaño de los mensajes estaban ejecutando alguna versión de Microsoft Windows, lo que significaría que sobre un aproximado de 590 mil posibles afectados, 501.500 fueron expuestos a infecciones del gusano Rodpicom. Afortunadamente, los valores y reportes de infecciones no han demostrado tales niveles de efectividad, pero simplemente suponiendo la hipótesis de que uno de cada cuatro usuarios que descargó la amenaza por seguir los enlaces se infectó, serían más de 14 mil infectados.

En diferentes ocasiones, se ha observado que los cibercriminales han utilizado herramientas para explotar vulnerabilidades en los sistemas operativos de las víctimas, en donde las funciones de identificación de los sistemas operativos juegan un rol vital y ***crimepacks,*** como ***Blackhole*** o similares, pueden ser utilizados para burlar las protecciones del sistema, aprovecharse de una falla de seguridad en el navegador y lograr comprometer la seguridad del sistema.

Las técnicas de propagación de códigos maliciosos se basan en factores que involucran la creatividad de los cibercriminales, la explotación de vulnerabilidades y otros procesos para evadir las herramientas de protección. Por otro lado, en lo que refiere a sistemas de protección, una falla, una mala configuración, o la ausencia de concientización en relación a técnicas de propagación, pueden generar un impacto importante ya sea nivel corporativo u hogareño.

El alcance del gusano Rodpicom puso de nuevo en tela de juicio cómo nos estamos protegiendo ante este tipo de amenazas. En este sentido, la heurística implementada en las soluciones antivirus juega un papel imporante en la detección de estas amenazas antes de que infecten los sistemas, pero también es necesario apoyarse en la educación como una técnica proactiva de protección.

Existen múltiples herramientas de defensa que se pueden implementar a nivel hogareño ucorporativo, y cada una de ellas se debe ajustar a las necesidades de cada caso en particular. Pensar en una protección por capas para garantizar la seguridad de un entorno corporativo, es una regla de oro en el mundo de la seguridad, asignando a cada capa una tarea diferente, pero con la premisa de minimizar el impacto en la operabilidad y usabilidad de los recursos.

Para contrarrestar los ataques de **Ingeniería Social,** la educación de los usuarios es un factor tan importante como lo son las actualizaciones de seguridad para los sistemas operativos y las aplicaciones. Ambos deben ser realizados como una tarea conjunta entre los departamentos de seguridad, IT y recursos humanos.