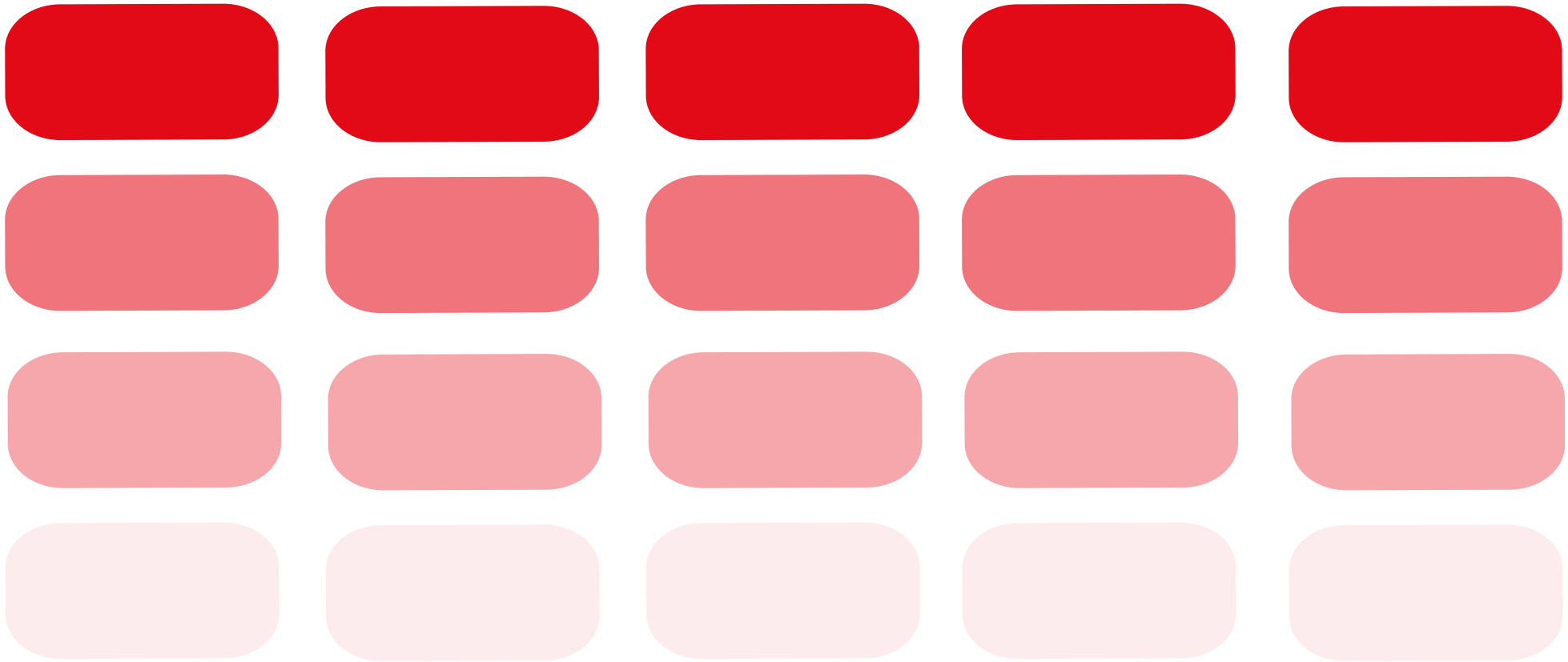


Informe cibercrimen 2008

S21sec e-crime

* [Sobre S21sec]

S21sec, compañía española especializada en servicios de seguridad digital y líder en el sector, fue fundada en el año 2000 y cuenta con más de 250 expertos certificados. La investigación y desarrollo han constituido un objetivo prioritario en la estrategia de S21sec desde sus inicios. Esto le ha llevado a crear el primer centro de I+D+i especializado en seguridad digital de toda Europa. S21sec opera con el 90% de las entidades financieras y 26 de las grandes empresas que cotizan en el IBEX 35. Con oficinas en Pamplona, San Sebastián, Madrid, Barcelona, Sevilla, León, Murcia, Londres, México D.F. y Monterrey, S21sec ofrece servicios integrales de seguridad digital a nivel mundial las 24 horas del día.

Más información en www.s21sec.com.

* [Índice]

* [Prólogo]

2008: El cibercrimen como fuente de beneficio

Desde que S21sec empezó a ofrecer su servicio de lucha contra el fraude, en el año 2004, tanto las amenazas existentes como el servicio de lucha contra el fraude han ido evolucionando vertiginosamente, de tal forma que las amenazas a las que nos enfrentamos hoy poco tienen que ver con aquellas de 2004.

Una de las peores consecuencias de la profesionalización del fraude en Internet ha sido la implicación de las bandas organizadas de crimen tradicional en todos los delitos de Internet en los que se pueda sacar algún beneficio económico. Este desembarco de organizaciones perfectamente jerarquizadas y estructuradas (en contraposición con los atacantes de principios del siglo XXI) ha supuesto un cambio fulgurante en la manera en que nos tenemos que enfrentar a estas nuevas amenazas. Hoy en día, la eterna carrera del gato y el ratón es más real que nunca, con el agravante de que ambos cuentan con todos los recursos y la tecnología necesaria para hacer cada vez más difícil el transcurso de la carrera.

El grado de especialización y los recursos empleados son tan avanzados, que ya hoy en día nadie duda de la existencia de redes botnets formadas por miles (a veces cientos de miles) de ordenadores controlados por todo el mundo, amparados muchas veces por proveedores de servicio (ISP) legales (incluso en países como EEUU, como el caso de McColo), que son usados para la consecución de cualquier tipo de delito: fraude, extorsión, chantajes, espionaje industrial… todo vale hoy en día, y lo más preocupante, todo está en alquiler o venta. Los tiempos donde había que ser un experto para poder infectar, controlar o robar información de una máquina han pasado a la historia. Si además sumamos la presente situación económica mundial, donde parte de la población necesita dinero de forma urgente, ello propicia la incursión de muchas personas y grupos, totalmente ajenos a Internet, al mundo de los delitos de Internet.

Toda esta avalancha de incidentes y nuevas formas de fraude nos ha obligado a crear y lanzar nuevos servicios a nuestros clientes, además de analizar concienzudamente los problemas del pasado para ayudar a nuestros clientes a frenar cualquier intento de ataque las 24 horas del día (sean un ejemplo las 6 horas de media de cierre de sitios fraudulentos a finales de 2008, los informes especializados o los análisis remotos).

La evolución de cibercrimen:

Época Romántica (1996-2000)

- Virus destructivos
- Carácter local, sin propagación
- Creación de Virus
- Personas solitarias, muy localizadas

MOTIVACIONES:
Superación personal
Conocimientos técnicos

Origen:
Personas individuales o grupos muy pequeños

A destacar:
Alta calidad técnica
No hay programación

Edad Media (2001-2004)

- Primeros phishing (11S)
- Gusanos
- Botnets 1.0 (IRC)

MOTIVACIONES:
Dinero rápido
Infecciones masivas

Origen:
Personas individuales o grupos muy pequeños

A destacar:
Baja calidad técnica
No hay programación

Fraude (2005-2006)

- Milicias cibernéticas
- Múltiples objetivos
- Control del 50% de los ordenadores

MOTIVACIONES:
Dinero de cualquier forma
Extorsiones

Origen:
Personas individuales o grupos muy medianos

A destacar:
Phishing y malware
100% fraude bancario

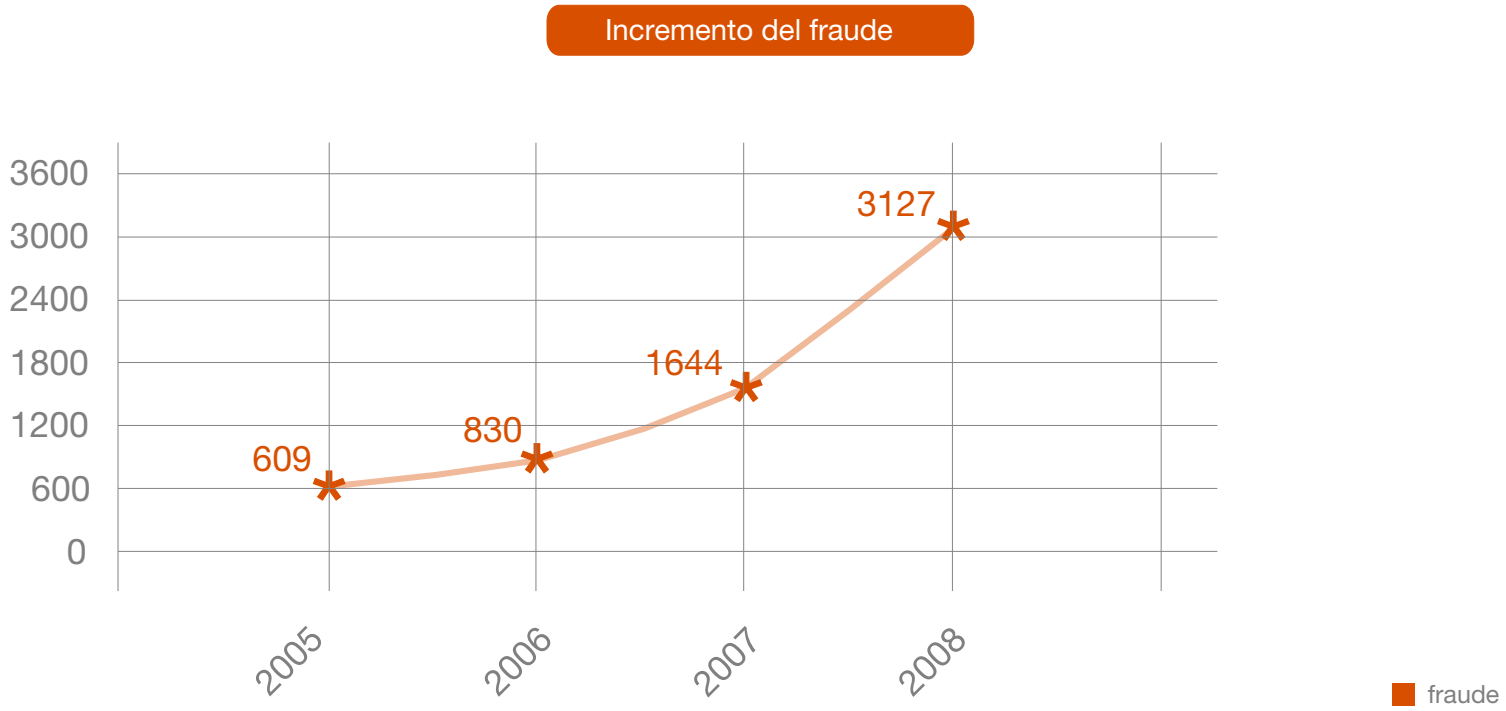
e-crime (2007-2009)

- Ataques geopolíticos
- Botnets 2.0
- ISP a prueba de balas
- Infraestructura en venta
- Iframe businesss, pay per install, clickfraud, botnets, DDoS, infection kits, C&C, cyberwarfare, espionaje industrial…

MOTIVACIONES:
Controlar Internet
Dominación total

Origen:
Grupos de crimen organizado

A destacar:
Target: gobiernos, empresas
Amenazas políticas



Las amenazas geopolíticas han sido durante 2008 una preocupación creciente por parte de todos los países debido al incremento de la tensión y actividades militares y políticas en Internet (cyberwarfare). Los incidentes más comentados han tenido lugar en diferentes zonas calientes del planeta: Georgia, Estonia, Israel, Palestina, Corea del Norte, India, Pakistán, China, Estados Unidos, … y son muchas veces la punta del iceberg de las actividades de Inteligencia de muchos países que han visto Internet como un nuevo campo de batalla, el único que el hombre ha creado, y el que implica tener unidades muy especializadas con conocimientos que muchas veces rompen los esquemas de la doctrina militar clásica. Es hora de aprender a anticipar (prevenir), proteger la información y nuestro patrimonio y saber gestionar correctamente cualquier tipo de crisis o incidente.

También durante 2008 han aparecido viejos fantasmas del pasado con la aparición del gusano Conficker (recuerden Blaster, Sasser…), gusano que muchas empresas de seguridad declaraban que era imposible que hoy en día tuviera un grado de éxito tan elevado. La realidad es que Conficker ha afectado negativamente a muchas pequeñas, medianas y grandes empresas dejando en evidencia lo vulnerables que hoy en día seguimos siendo a este tipo de amenazas, con la particularidad de que hoy somos mucho más dependientes de Internet y las tecnologías relacionadas, con lo que el daño afligido es aún mucho mayor.

Lamentablemente, no podemos decir que 2008 haya sido el año en que se haya organizado un espíritu de colaboración para frenar cualquier tipo de amenazas. Los intereses de cada país (y de cada empresa) son tan grandes que es muy difícil establecer un marco de colaboración internacional. Existen múltiples iniciativas de colaboración, no sólo a nivel de Fuerzas del Orden, sino también a nivel privado, pero todas ellas se han quedado en propósitos, y nunca realmente son operativas. A día de hoy, cualquier incidente en el que varios países estén involucrados resulta una pesadilla, en términos de investigación, causando muchas veces vagos resultados debido a la lentitud de las acciones. S21sec está presente en múltiples de esas iniciativas, pero a la hora de la verdad lo que realmente funciona son las relaciones personales, aunque es cierto que paulatinamente algún órgano empieza a tomarse en serio sus actividades (como ICANN).

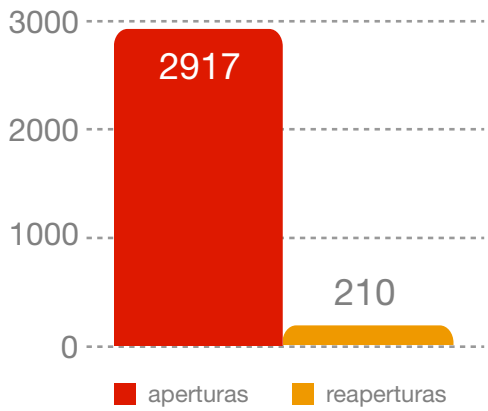
En resumen, 2008 ha sido un año apasionante desde el punto de vista de la investigación, pero a la vez preocupante debido a que las amenazas existentes han dejado de estar en su época de la infancia y se están haciendo mayores. Realmente es difícil hoy en día (a principios de 2009) hablar de un tema que no sea el económico, pero es necesaria una iniciativa a nivel internacional para organizar la lucha de las amenazas en Internet; esta lucha no sólo es responsabilidad de las Fuerzas del Orden, sino de todos los usuarios de Internet, cuestión clave para que durante el año 2009 podamos hacer frente a todos los incidentes que nos afecten.

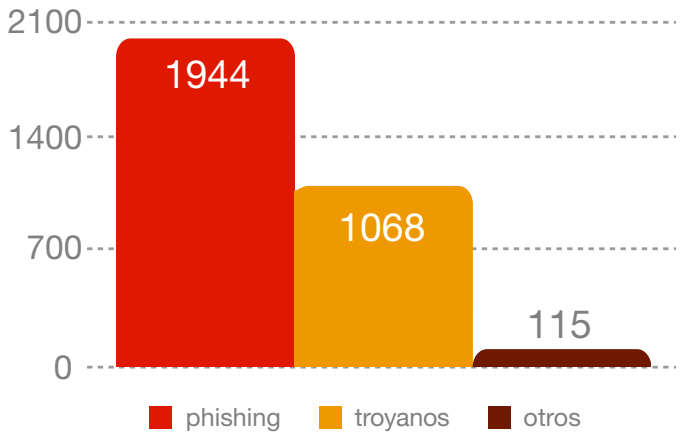
David Barroso
Director S21sec e-crime

* [Resumen: incidentes de fraude]

Al igual que en los informes mensuales, en este apartado se muestra un resumen de las estadísticas registradas por el servicio de antifraude de S21sec e-crime.

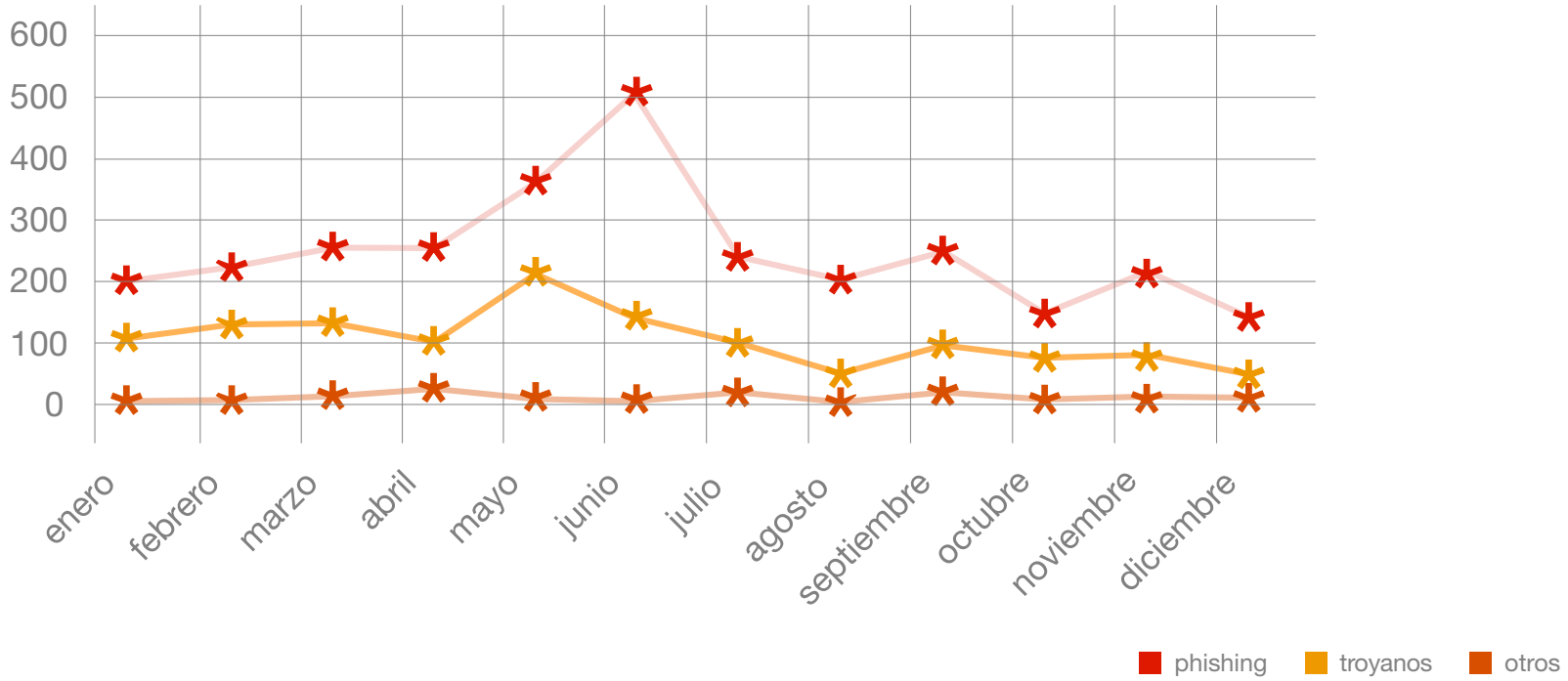
• Número total de incidentes dividido por tipos





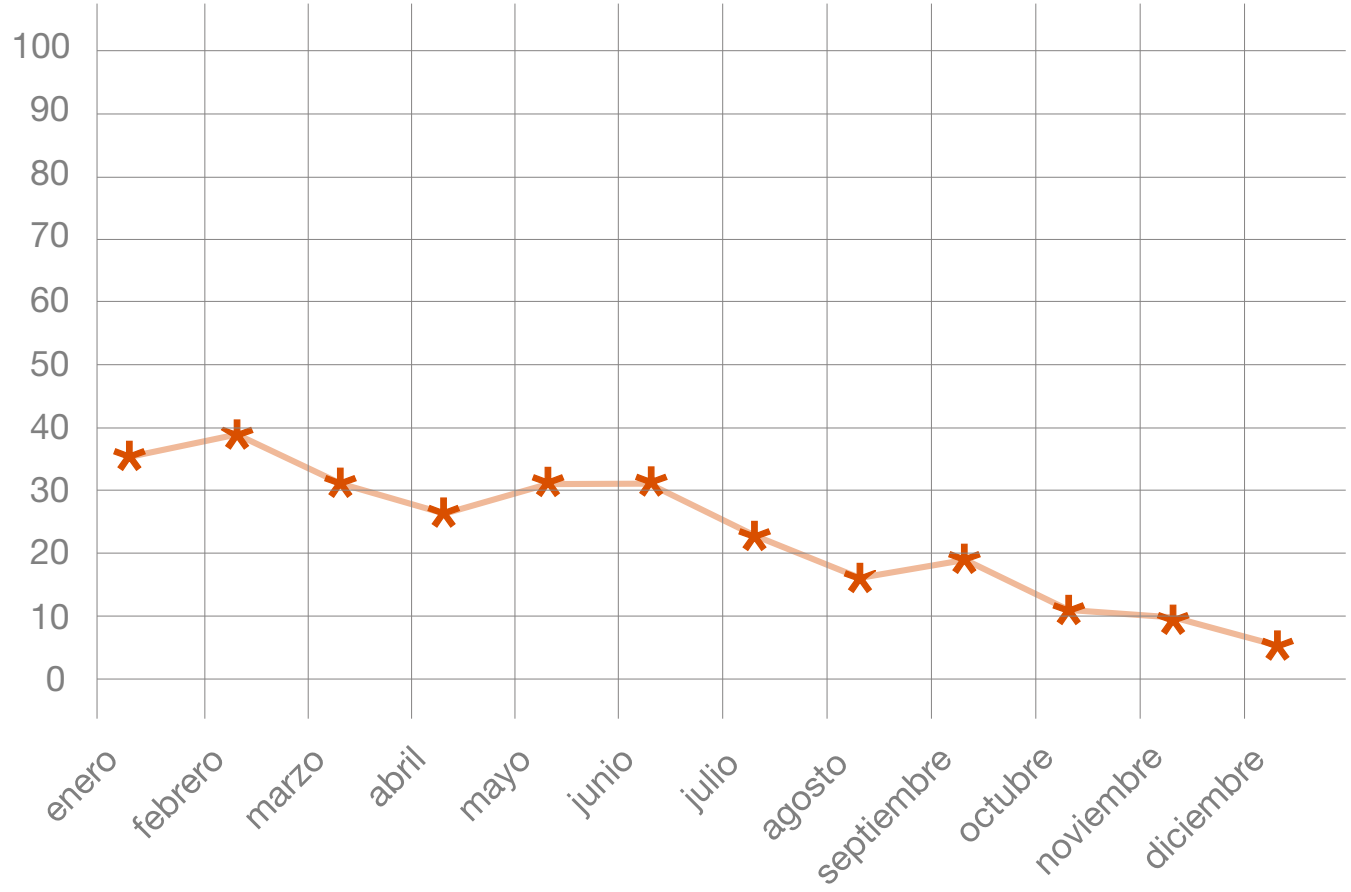
Es importante observar que los incidentes de troyanos se han incrementado hasta suponer el 34,15 % del número total de incidentes del año.

• Evolución de los incidentes por meses

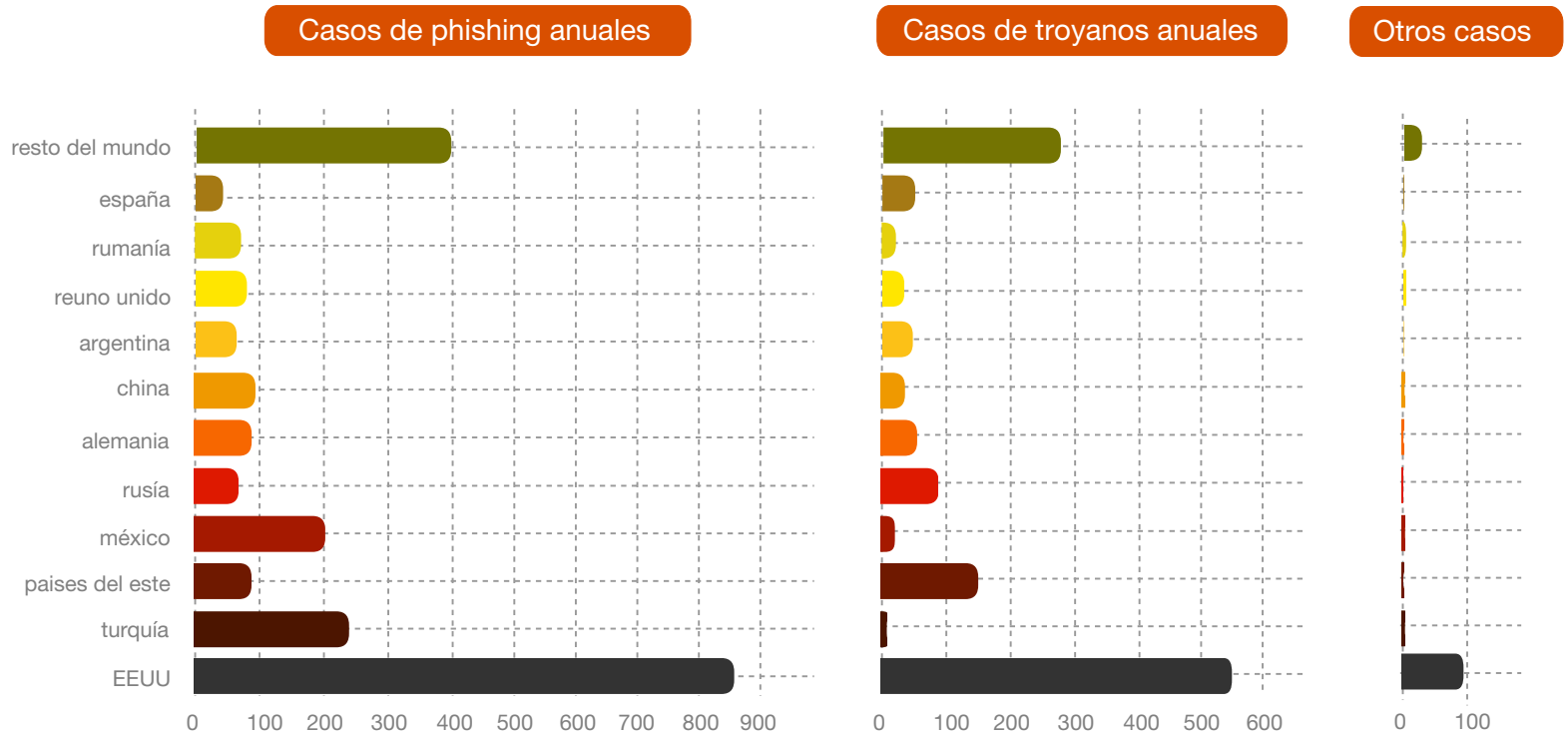


De manera similar a lo ocurrido en el año anterior, hubo un periodo de aproximadamente tres meses (Mayo, Junio y Julio) donde se produjo un incremento de los ataques, que acabó en un descenso de incidentes en los últimos meses del año.

• Tiempo medio de cierre en horas



• Origen de los ataques



Siguiendo la casuística de años precedentes, es EEUU el principal origen de los incidentes gestionados en el año 2008; la única noticia relevante es el aumento de incidentes con ISPs en Turquía así como la disminución en China y Rusia.

* [Visión global del cibercrimen]

La consciencia en cuanto a amenazas en Internet y ciberdelincuencia ha ido cobrando importancia gradualmente a lo largo del tiempo para llegar a su máximo exponente durante el año 2008. Las noticias relacionadas con ciberataques de todo tipo y fraude han traspasado las barreras de círculos especializados para aparecer en grandes medios de comunicación, ayudando a crear una conciencia de seguridad entre el gran público. Posiblemente en esta coyuntura se ha creado el caldo de cultivo adecuado para comenzar a aunar fuerzas y arrancar una serie de medidas concretas dedicadas a erradicar amenazas que hasta ahora gozaban de cierta impunidad.

Lucha internacional contra el cibercrimen

El segundo semestre del año 2008 ha sido bastante fructífero en cuanto a la lucha contra el cibercrimen se refiere. La comunidad de Internet (hablando de expertos en seguridad informática, ISPs, periodistas, etc) ha iniciado lo que se puede considerar como un paso lógico en esta guerra: eliminar muchos de los servidores clave en la infraestructura criminal.

Internet es una red de subredes comunicadas entre ellas y cuya administración depende de los proveedores de Internet (ISP). Estas subredes, llamadas Sistemas Autónomos (AS), se conectan a través del protocolo BGP y, básicamente, representan el núcleo de Internet.

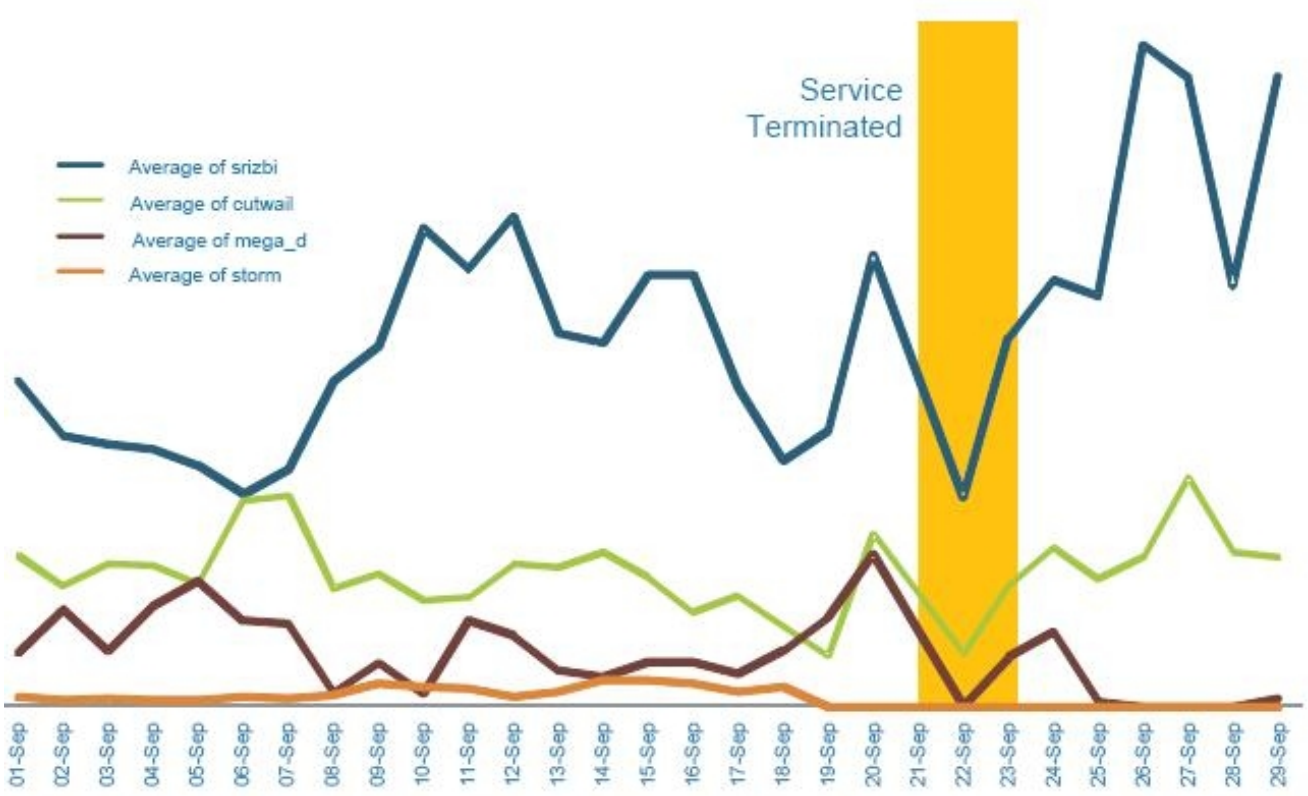
Existen algunos ISPs conocidos por mantener algunos de los servidores más importantes de la infraestructura criminal. Estos servidores se consideran como puntos negros de la infraestructura, por lo que era cuestión de tiempo que se eliminaran. Ya que los ISPs que mantienen estas máquinas no responden a los avisos de abuso, la única forma de actuar contra ellos era que su propio proveedor de servicios los desconectara.

1. Atrivo / Interchange

Esta desconexión fue la que sufrió un ISP llamado **Atrivo/Interchange** en agosto de este año. Atrivo era un ISP que mantenía diferentes ciberdelincuentes y que había ignorado los avisos de abuso durante al menos tres años. Pacific Internet Exchange fue el proveedor de servicios que dejó a éste otro sin salida a Internet el 30 de agosto de este año, dejando sin conexión a todos los servidores dependientes de Atrivo. Temporalmente, el ISP malicioso encontró otros proveedores, hasta que finalmente desapareció totalmente el 25 de septiembre.
El resultado de esta desconexión fue que varias botnets se vieron afectadas, ya que sus paneles de control dejaron de estar activos. Éste fue también el final de la botnet Storm, puesto que sus últimos tres paneles de control estaban localizados en los dominios de Atrivo. El siguiente gráfico muestra el impacto de la desconexión del ISP en la actividad de diferentes botnets.

2. McColo

El segundo ISP en ser desconectado, gracias a la acción del periodista del WashingtonPost Bryan Krebs, fue McColo. **McColo** parecía ser el ISP preferido por los ciberdelincuentes últimamente, y también la nueva casa de algunos de los anteriormente mantenidos por Atrivo. Debido al esfuerzo de Brian Krebs, McColo fue desconectado el martes 11 de septiembre de 2008. Tras ello lograron encontrar un proveedor alternativo y eligieron un sábado a la tarde para volver a conectar su infraestructura. Supuestamente eligieron ese tramo horario con la intención de evitar la detección y reacción de los administradores del nuevo ISP, pero esta reconexión únicamente estuvo activa durante un corto periodo de tiempo antes de ser desconectados de nuevo. Aún así, este pequeño lapso de tiempo fue suficiente para trasladar su infraestructura, colocando nuevos paneles de control en ISPs ajenos a Atrivo y McColo.



Ilustration of activity from major bot nets and impact of Intercage ISP disconnection

Gráfico: Actividad botnets. Fuente: Washingtonpost

Referencias:
http://www.spamhaus.org/news.lasso?article=636
http://asert.arbornetworks.com/2008/10/timeline-atrivointercage-depeering-dissolution/
http://voices.washingtonpost.com/securityfix/2008/10/atrivo_shutdown_hastened_demis.html
http://voices.washingtonpost.com/securityfix/2008/10/spam_volumes_plummet_after_atr.html

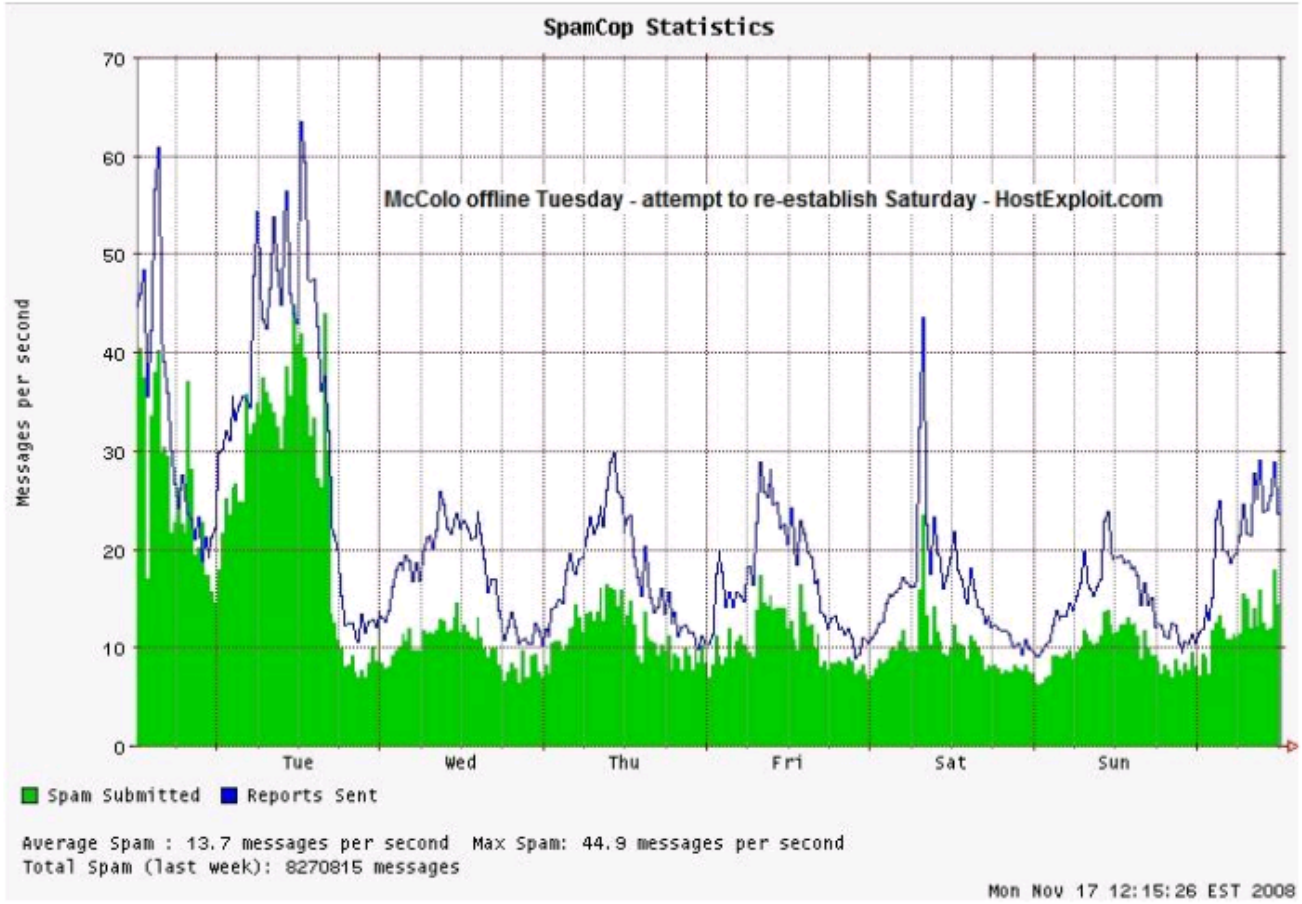


Gráfico: Actividad spam. Fuente: hostexploit

Referencias:
http://www.secureworks.com/research/threats/warezov/
http://hostexploit.com/downloads/Hostexploit%20Cyber%20Crime%20USA%20v%202.0%201108.pdf

La desconexión de McColo redujo el envío de spam global a casi la mitad.

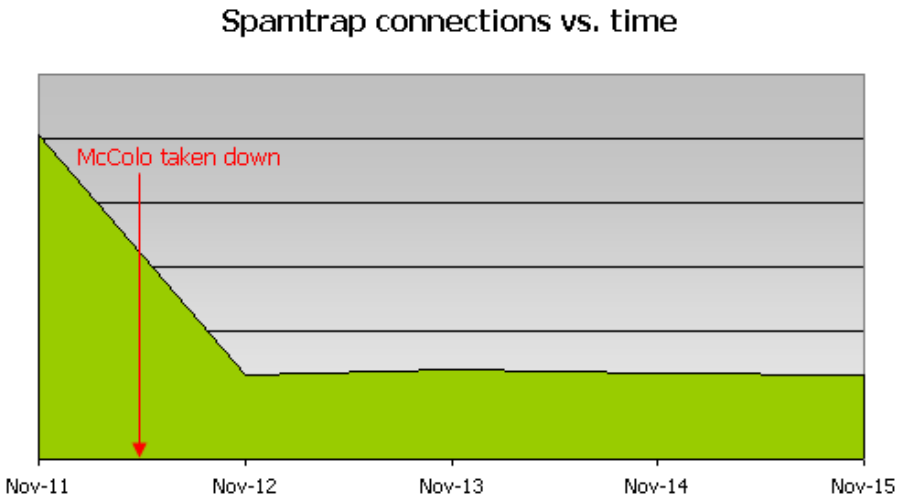


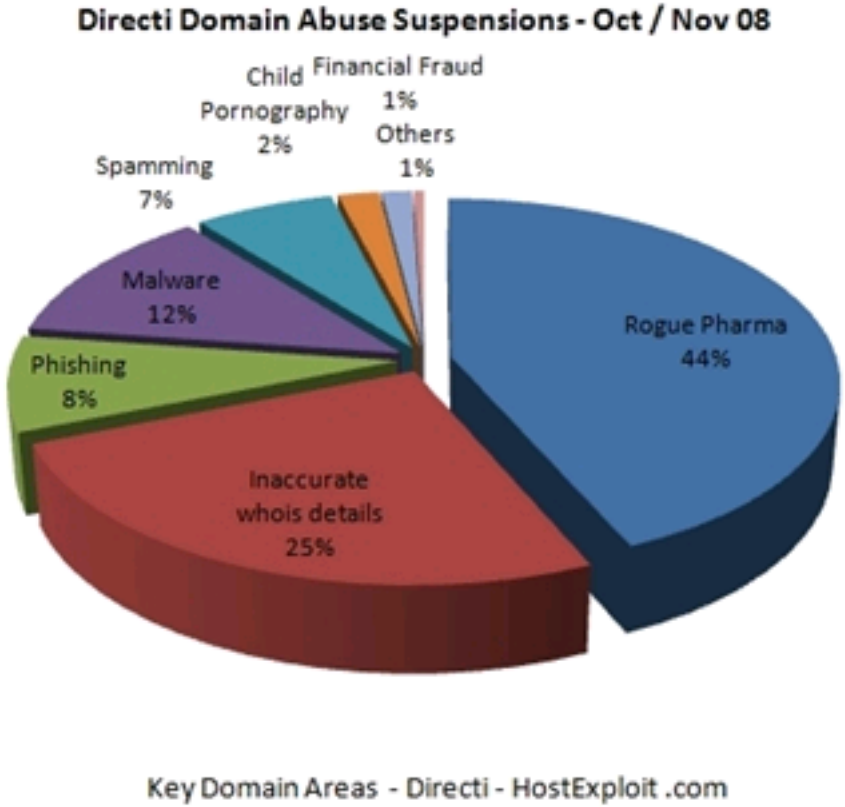
Gráfico: Actividad spam. . Fuente: sophos

3. EstDomains

Pero no sólo los ISPs han estado en el punto de mira en la lucha contra el cibercrimen, los registradores de dominios no se libraron de la quema. Especialmente **EstDomains**, que tenía registrados cientos de miles de dominios en su mayoría fraudulentos. La ICANN rescindió el 28 de octubre su acuerdo de acreditación (Registrar Accreditation Agreement), dejando sin validez la licencia para continuar con su actividad.

Referencias:
http://www.f-secure.com/weblog/archives/00001522.html
http://www.sophos.com/security/blog/2008/11/1995.html

Directi, un registrador de dominios supuestamente ajeno al mundo del cibercrimen, acogió el 1 de diciembre a más de 280.000 dominios que habían quedado en el aire tras la suspensión de EstDomains. **Directi** ha publicado recientemente unas estadísticas de los dominios que han sido suspendidos en octubre y noviembre gracias a los avisos de abuso recibidos, dejando ver que no siguen para nada las pautas de EstDomains.



Referencias:
http://www.directi.com/estbulktransfer/

4. Ecatel

El 28 de noviembre apareció el primer mensaje que hablaba de que algunos de los clientes de McColo habían aparecido en el ISP Ecatel. Después de constatarse que **Ecatel** se había convertido en la nueva "casa" de algunos ciberdelincuentes, varios de sus proveedores, como Hurrican, Tiscali, HEnet o GBLX, aparentemente dejaron de prestarle servicios. A día de hoy este ISP es enrutado a través de JointTransit, en Amsterdam, como muestra el siguiente histórico del esquema de enrutado BGP:

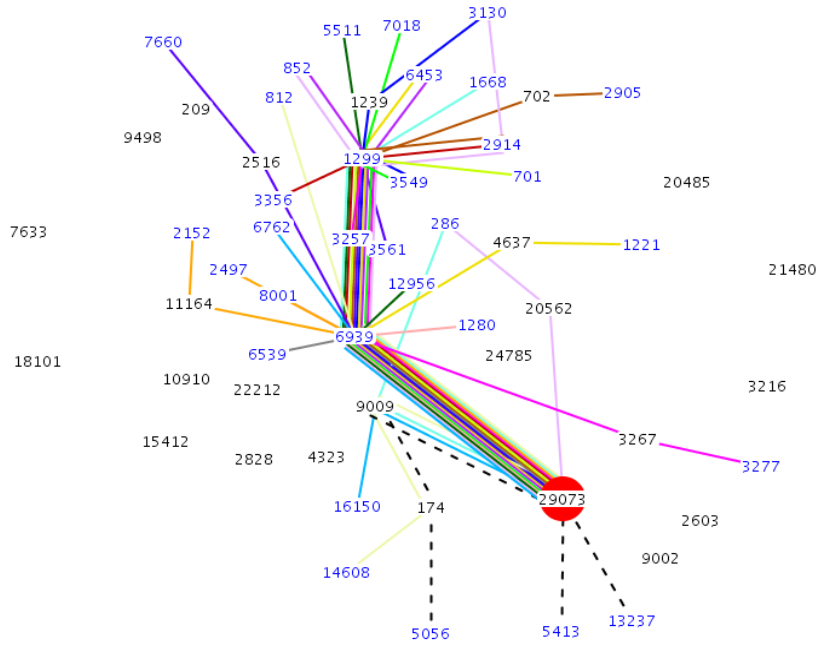


Gráfico: Ecatel enrutado todavía a través de Hurrican, AS 6939

Referencias:
http://www.matchent.com/wpress/?q=node/421

La desconexión por parte de su anterior proveedor, Hurrican (AS6939), uno de los mejores en los rankings de calidad de servicio, seguramente les hizo más conscientes de los posibles fraudes. De esta forma, y si no quieren acabar como Atrivo y McColo, desde ahora se supone que intentarán mantener su red limpia de delincuentes.

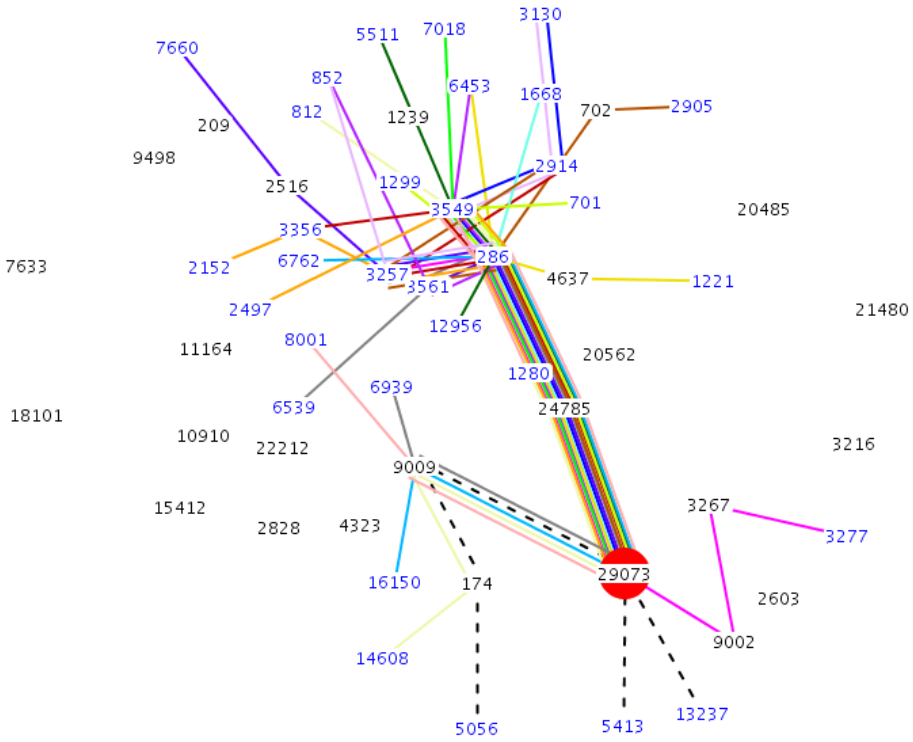


Gráfico: Ecatel enrutado a través de JointTransit Amsterdam

Referencias:
http://www.netconfigs.com/general/ranks.htm

Estadísticas generales de Spam

Como se puede ver a continuación, el volumen de spam enviado en 2008 se ha reducido drásticamente. Esto es debido al esfuerzo en contra del cibercrimen realizado por parte de la comunidad internacional.

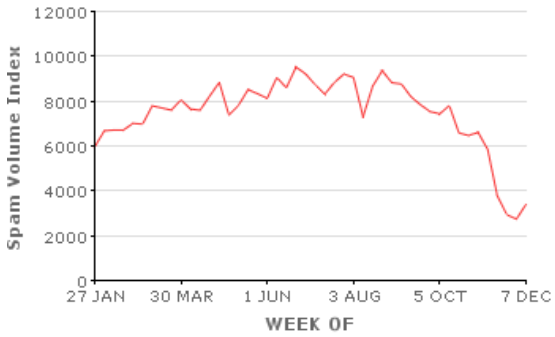


Gráfico: Volumen envío spam. Fuente: Marshal.com

En el siguiente gráfico se puede ver qué botnets son las más activas en cuanto al envío global de spam. Es interesante remarcar que la botnet Storm, que jugó un papel importante en el envío mundial de spam, ha desaparecido completamente de la lista.

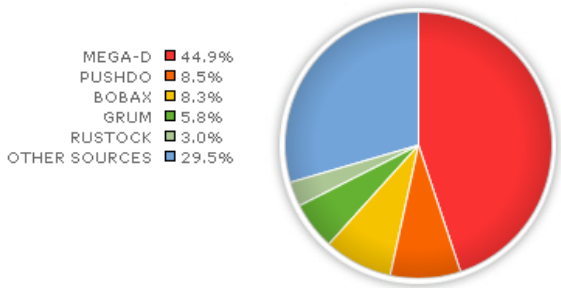


Gráfico: Envío spam de botnets. Fuente: Marshall.com

Referencias:
http://www.marshal.com/trace/spam_statistics.asp

Mecanismos para asegurar la existencia de una botnet

La mayoría de las botnets, tal y como las conocemos hoy en día, siguen el paradigma cliente-servidor, alojándose los paneles de control en servidores dedicados, desde donde se mantiene la infraestructura y se almacenan los datos recolectados. Por ello, éstos juegan un rol muy importante, siendo piezas clave de la infraestructura. Como se ha comentado anteriormente, estos paneles de control son el punto débil y la primera elección a la hora de atacar la infraestructura de los delincuentes. Esto se ha visto varias veces este año: al hacer desaparecer estos servidores, las máquinas infectadas (bots) no pueden enviar los datos recogidos ni generar spam, resultando una pérdida de beneficios para los criminales.

Con el objetivo de evitar la pérdida de conexión con sus paneles de control, cada vez más troyanos están implementando un método para tener siempre un "plan B", normalmente basado en la fecha actual. La combinación de la fecha actual y un algoritmo secreto es la clave de la reconexión con un nuevo servidor de la botnet. Cuando un panel de control deja de estar activo, los cibercriminales generan a partir de ciertas fechas y de su algoritmo varios nombres de dominio que registran. Como el código malicioso alojado en las máquinas infectadas dispone del mismo algoritmo, llegada la fecha seleccionada éste realizará una petición a ese nombre de dominio "secreto", recuperando la comunicación perdida. De esta forma, los delincuentes pueden volver a tomar el control de la botnet y seguir recibiendo datos de sus bots a pesar de los cierres puntuales de los paneles de control.

La compañía FireEye averiguó, por ejemplo, el algoritmo de generación de nombres de dominio para la botnet Srizbi y registró los dominios para fechas futuras, haciendo imposible para los criminales la recuperación de su botnet durante ese periodo de tiempo.

1. Algoritmo de generación de dominios de Sinowal

Otro ejemplo de este método es el usado por el conocido Sinowal. En los siguientes párrafos se detalla una parte de su algoritmo de generación de dominios.

Referencias:
http://blog.fireeye.com/research/2008/11/its-srizbi-trun-now.html

Existen dos tipos de dominios generados por el troyano dependiendo de la fecha actual: el principal y el secundario. El principal se genera semanalmente, concretamente cada domingo, mientras que el secundario se genera diariamente. Ambos poseen siempre siete letras y siguen el mismo método para las cuatro últimas letras del dominio siendo diferente para las tres primeras, aunque todavía se está investigando este asunto. Las tres últimas letras dependen del mes en el que se generan, modificando el orden de las letras de las abreviaturas de los meses en inglés:

Mes	Tres últimas letras
Enero	ANJ
Febrero	EBF
Marzo	ARM
Abril	PRA
Mayo	AYM
Junio	UNJ
Julio	ULJ
Agosto	UAG
Septiembre	ESP
Octubre	OKT
Noviembre	ONV
Diciembre	EDC

La cuarta letra depende del día del mes en que se genera, siguiendo un ciclo mensual, que, salvo excepciones, sigue el patrón letra+2:

Día	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Letra	c	e	g	i	k	m	o	q	s	u	w	y	b	d	f

Día	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Letra	h	j	l	i	k	m	o	q	s	u	w	y	b	d	f

Esta generación de dominios permite a los delincuentes asegurar la comunicación de su troyano con los servidores. Mientras que ellos se encarguen de registrar los futuros dominios y apunten a los servidores todo irá bien para ellos, ya que desde éstos se descargarán los archivos de configuración actualizados, donde se encontrará el nuevo Servidor Inyector.

Tanto para el dominio primario como el secundario se usan tres TLDs (Top Level Domains) diferentes. Primero se usa .com, si no responde se usa .net y por último .biz.

DarkMarket

Los cibercriminales tienen foros en Internet dedicados especialmente a la compra/venta de datos robados, como números de tarjetas de crédito y otros elementos relacionados con el fraude. La mayoría de los sitios underground serios son bastante herméticos y en su comunidad se conocen muy bien los unos a los otros. Esto también quiere decir que ningún miembro (supuestamente, puesto que muchas veces se demuestra lo contrario) robaría dinero a los demás.

DarkMarket era uno de estos sitios, que se colocaba entre los punteros de habla inglesa. Corrían rumores de que el sitio entero fue montado por gente del FBI, aunque la versión oficial es que infiltraron a un agente como administrador del sitio con alias “Master Splynter” a finales de 2006, operando éste desde la oficina de la NCFTA (National Cyber-Forensics & Training Alliance) en Pittsburgh. El FBI usó DarkMarket para construir perfiles de sus miembros, recogiendo información sobre sus direcciones IP, así como de sus actividades en el sitio.

Referencias:
http://www.fbi.gov/page2/oct08/darkmarket_102008.html

La operación secreta del FBI se puso en peligro cuando “Max Ray Butler”, otro miembro de DarkMarket, realizó una intrusión en el servidor del sitio y anunció a la comunidad underground de que “Master Splynter” había accedido desde la oficina de la NCFTA en Pittsburgh. Pero al ser miembro de otro foro que hacía la competencia a DarkMarket no se le hizo demasiado caso, alegando rivalidades entre los dos sitios.

En octubre de 2008 el foro fue cerrado por el FBI y la operación terminó con varios arrestos a lo largo de todo el mundo.

Referencias:
http://blog.wired.com/27bstroke6/2008/10/darkmarket-post.html
http://news.bbc.co.uk/2/hi/uk_news/7675191.stm

Ciberguerra (cyberwarfare)

En la actualidad, el objetivo principal de la ciber delincuencia es el dinero. Tal y como se ha mencionado con anterioridad, ya no se busca prestigio ni publicidad por parte de los atacantes, básicamente todo se basa en conseguir beneficios económicos. Sin embargo, últimamente empiezan a aparecer nuevos ataques con fines políticos, o incluso dirigidos a nivel estatal contra otros países con los que se mantienen conflictos. Durante el 2008 este tipo de ataques han empezado a aparecer con cierta frecuencia en los medios de comunicación.

1. Rusia – Georgia

Durante el verano de 2008, el conflicto entre Rusia y Georgia tuvo su eco también mediante una serie de actividades acaecidas en la red. Los ataques contra Georgia tuvieron como consecuencia que distintas páginas web gubernamental es se viesen comprometidas, con continuos ataques de denegación de servicio distribuidos contra otras páginas del gobierno, teniendo como consecuencia la migración de ciertos sitios a servicios de hosting de Estados Unidos. Un grupo de ciber activistas pro Ruso incluso proporcionaba ayuda en su página oficial para promocionar este tipo de actividades (stopgeorgia.ru/stopgeorgia.info):

- Potenciar a los usuarios de Internet con herramientas para realizar ataques distribuidos de denegación de servicio.
- Proporcionando una lista de páginas georgianas vulnerables a inyección SQL.
- Publicando una lista de direcciones de correo de políticos georgianos para ataques dirigidos y spam.

Referencias:
http://blogs.zdnet.com/security/?p=1670
http://ddanchev.blogspot.com/2008/11/ddos-attack-against-bobbearcouk.html

2. Israel – Gaza

Otro ejemplo más reciente es el conflicto entre Israel y Gaza, donde una guerra real da lugar a un escenario en el que distintos activistas apoyan a uno de los bandos implicados.

Por ejemplo, hay algunos activistas pro Israel que han preparado una página web (http://help-israel-win.tk) para reclutar personas con la misma opinión. Para ello ofrecen una herramienta llamada “Patriot” que básicamente es una herramienta de denegación de servicio distribuida controlada remotamente y diseñada para atacar a ciertas páginas web. Unas 8.500 personas ya forman parte de este proyecto mediante la descarga de esta “arma-cibernética”.

Desde hace algunas semanas, un buen número de páginas se han visto afectadas por diversos ataques, dejando mensajes a favor de uno u otro bando en las mismas.

“Este es el último indicador de un nuevo tipo de conflicto en el que se combinan balas y bombas con bits y bytes”.

Referencias:
[20] http://www.defensetech.org/archives/004630.html

* [Las vulnerabilidades más explotadas]

Las vulnerabilidades más explotadas por el cibercrimen en 2008

En 2008 también han aparecido varias vulnerabilidades muy notables, algunas de ellas creando una gran expectativa, más que justificada en algunos casos. Las noticias en cuanto a vulnerabilidades han abundado en todo tipo de medios de comunicación, en general confundiendo bastante al gran público. No obstante muchas de las vulnerabilidades han sido muy reales y aprovechadas con gran rapidez para la difusión de troyanos y creación de botnets, otras han sido más teóricas que prácticas y algunas se han podido solucionar antes de ser aprovechadas por los atacantes. En este apartado se resumen las más importantes registradas por nuestro **servicio Vulnera** de alerta, información y gestión de vulnerabilidades.

1. Ataque masivo de inyección SQL

El ataque inicial se realizó de forma totalmente indiscriminada contra una serie de objetivos a nivel mundial aproximadamente en abril de 2008. Desde entonces, se siguieron registrando casos en distintos rango de red y países, de modo que el problema siguió extendiéndose usando la misma técnica de ataque.

En este caso no se trataba de un troyano específico ni de la explotación de una vulnerabilidad conocida o 0-day, sino del intento masivo de explotación de un problema habitual en muchos aplicativos web debido a la falta de medidas de seguridad y de programación segura, como es la inyección SQL.

A partir de dicha inyección, era posible llegar a insertar código malicioso en la base de datos de la entidad afectada. En este caso, el ataque intentaba inyectar código de scripting, codificado en hexadecimal, en la base de datos con la esperanza de hacerlo en las tablas de las que se alimenta el aplicativo para mostrar el código HTML del mismo.
De este modo se lograba insertar un script o un iframe en el código HTML que redirigía al site malicioso.

La unidad de e-crime de S21sec pudo localizar la herramienta utilizada en estos ataques a gran escala, siendo esta una aplicación para Win32 desarrollada en Delphi y con la información en chino.

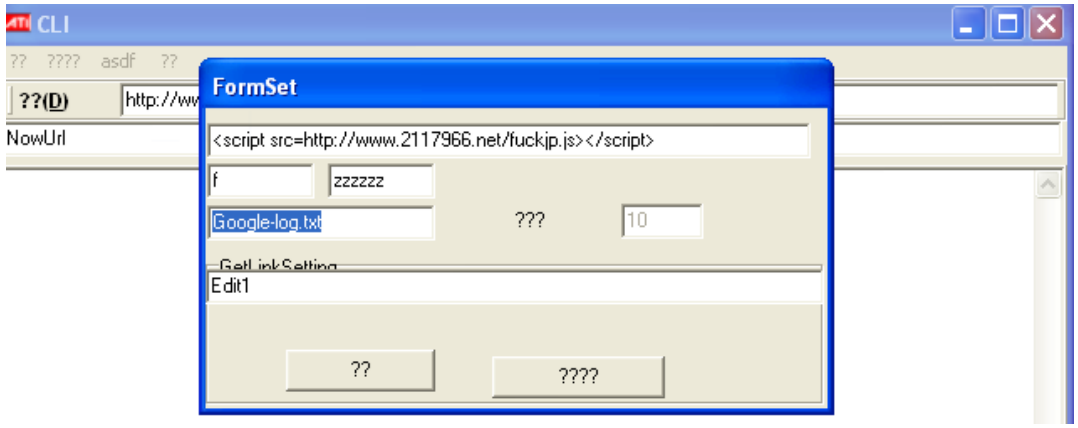


Imagen: Herramienta usada para el ataque masivo

El ataque se realizaba buscando en google aplicativos que tuvieran la extensión asp o aspx, ya que el código que se trataba de inyectar estaba hecho en sql script de SQL Server y optimizado para el mismo. No se trataba de explotar ninguna vulnerabilidad de ninguna tecnología, simplemente era un tipo de ataque conocido optimizado para una plataforma que, presumiblemente, utilizaba una buena parte del mercado.

Una vez obtenidos los aplicativos potencialmente vulnerables, se buscaban parámetros tipo id, a, b, c, etc., para intentar la inyección. No se realizaba ninguna comprobación de si existían o no, simplemente se intentaba inyectar de forma indiscriminada con la esperanza que una buena parte de los intentos tuvieran éxito. Al realizar el ataque sobre un número tan alto de aplicativos, era plausible que se lograra una alta cantidad de éxitos en términos absolutos.

Para comprobar si un aplicativo se había visto afectado, la mejor opción era buscar cualquier modificación no controlada en el HTML que se cargaba en el mismo. Se podían buscar las cadenas de los sites maliciosos o buscar inyecciones en los logs de peticiones realizadas contra el mismo.

2. Ejecución remota de código en Adobe Flash Player

En abril de este año se publicó una vulnerabilidad de Adobe Flash, identificada como CVE-2007-0071, que fue utilizada en el mes de mayo en forma de 0-day y propagada a través de un ataque masivo de inyección SQL. Varios sitios legítimos fueron objeto de estas inyecciones, llevando de forma silenciosa al navegador hasta servidores donde se explotaba esta vulnerabilidad. Este ataque parecía provenir de China, y los delincuentes usaban este exploit para infectar las máquinas con troyanos, con el objetivo de robar las credenciales de sus usuarios.

La vulnerabilidad consistía en un integer overflow en las versiones 9.0.115.0, 8.0.39.0 y anteriores de Adobe Flash Player, y permitía a un atacante remoto la ejecución de código arbitrario en el sistema tras el envío de un archivo SWF con una valor negativo del parámetro Scene Count, que, tras pasar por una comparación con signo, se usaba como offset de un puntero nulo, derivando en un buffer overflow.

3. Ataques a routers

Los primeros ataques a routers se usaron activamente con propósitos fundamentalmente maliciosos. Estos ataques se basan en la idea de cambiar la configuración del router de la víctima, añadiendo, por ejemplo, un nuevo servidor DNS o deshabilitando el filtrado de paquetes. Para lograr su cometido un atacante debía modificar una página web y colocar en ella un iframe o un link como el siguiente:

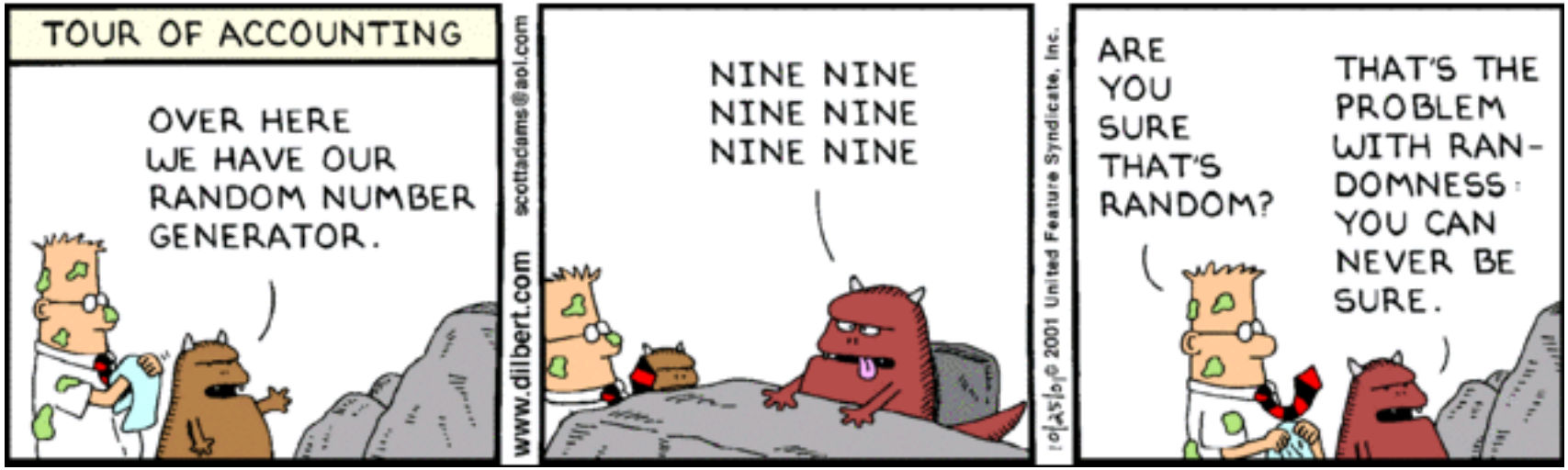
https://192.168.0.1/apply.cgi?submit_button=Firewall&change_action=&action=Apply&block_wan=1&block_loopback=0&multicast_pass=0&ident_pass=0&block_cookie=0&block_java=0&block_proxy=0&block_activex=0&filter=off&_block_wan=1&_block_multicast=0&_ident_pass=1

Este ejemplo deshabilita la configuración del cortafuegos de un router Linksys WRT54 GL y puede incluso ser realizado sin necesidad de autenticación (CSRF).

Brian Krebs también escribió sobre una variante de la familia Zlob que hacía uso de esta vulnerabilidad para cambiar la configuración de los servidores DNS de su víctima.

4. Bug Openssl en Debian

Una vulnerabilidad que afectaba a las distribuciones basadas en Debian salió a la luz en mayo. El problema estaba relacionado con un fallo de diseño en el sistema criptográfico de SSL, en concreto se trataba de una debilidad en el algoritmo de generación de números aleatorios de la librería libssl.



Referencias:
http://packetstormsecurity.org/0801-exploits/TISA2008-01.txt

Este grave fallo tuvo su origen en la eliminación de algunas líneas de código que al depurar provocaban avisos de variables no inicializadas en todos los archivos que hacían uso de la librería libssl. El borrar esta parte de código tuvo un efecto paralelo oculto, dejando sin efectividad el proceso de seeding del PRNG de libssl. En concreto, en lugar de incluir datos aleatorios en la semilla inicial, únicamente se incluía el identificador del proceso con ese fin. En estas distribuciones el valor máximo de un identificador de proceso es 32.768, siendo este número realmente pequeño para su uso como semilla, por el reducido rango de variación. Sabiendo esto, era una tarea más o menos sencilla la generación de todas la claves públicas y privadas posibles, pudiendo comprometer las conexiones seguras establecidas mediante la librería afectada. Además, este fallo también se trasladaba a los sistemas que no hacían uso de esta librería desde el momento que realizaban una conexión con un equipo vulnerable. Es por ello que diferentes paquetes y programas se vieron salpicados por este bug: OpenVPN, OpenSSH, Web, Mail, DNSSEC, etc.

5. Vulnerabilidad en el protocolo DNS

Dan Kaminsky descubrió y publicó una vulnerabilidad del protocolo DNS que afectaba de manera global a todo Internet. Esto hizo necesario que todos los elementos de la red que se comunicaran a través de este protocolo tuvieran que ser actualizados para evitar posibles ataques.

Se trataba de un ataque de envenenamiento de la caché (cache-poisoning), es decir, la cache DNS es modificada con el objetivo de que una petición legítima de un dominio concreto resuelva hacia una IP de la elección del atacante. Por la recursividad de las peticiones DNS, las consultas se hacen de arriba hacia abajo: cuando un usuario quiere visitar una URL, primero el servidor DNS de su proveedor mira si tiene esa información en caché, si no es así pregunta a un servidor raíz si sabe quién controla ese dominio en concreto, después pregunta al servidor autorizado por ese dominio cuál es la IP de ese subdominio, y por último el usuario recibe esa IP del servidor de nombres de su proveedor.

En todos los niveles de esta jerarquía existe el concepto de caché, que sirve para responder de forma más eficiente a consultas muy comunes, quedando almacenada la información de resolución de dominios de forma temporal. Hasta entonces era más o menos sencillo mediante prueba y error el envenenar la caché de un servidor para que cierto subdominio resolviera a la IP elegida, gracias a la debilidad del protocolo UDP ante el spoofing y que el identificador usado por el protocolo DNS para dotar de unicidad a las peticiones es de sólo 16 bits. Pero lo que Dan Kaminsky descubrió fue la forma de que todas las peticiones de subdominios de un dominio elegido fueran redirigidas a un falso servidor autorizado de ese dominio, que él mismo controlaba. Este falso servidor se introducía como autorizado mediante el envenenamiento de la caché del servidor intermedio: primero el atacante hace una petición de un subdominio falso, el servidor víctima pregunta por ese subdominio, y el atacante responde antes que nadie a esta pregunta diciéndole que para ese dominio debe preguntar al servidor malicioso, controlado por él, y quedando registrado en caché. Desde ese momento todas las peticiones a ese dominio serán enviadas al falso servidor.

La solución al problema pasa por el uso de DNSSEC, que introduce respuestas autorizadas criptográficamente a las peticiones DNS, que pueden ser verificadas también. Ya que esto es un tanto utópico por la necesidad de consenso mundial, otra solución es el intentar dotar de más aleatoriedad a las peticiones DNS, dificultando así la suplantación de las respuestas. De momento se ha usado como medida “temporal” la modificación del puerto origen para dotar de más aleatoriedad al sistema, ya que el atacante se ve obligado a adivinar también este puerto. No obstante no debería ser una solución definitiva.

Referencias:
http://blog.s21sec.com/2008/08/blackhat-las-vegas-2008.html
http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
http://www.heise-online.co.uk/news/DNS-security-problem-details-released--/111145

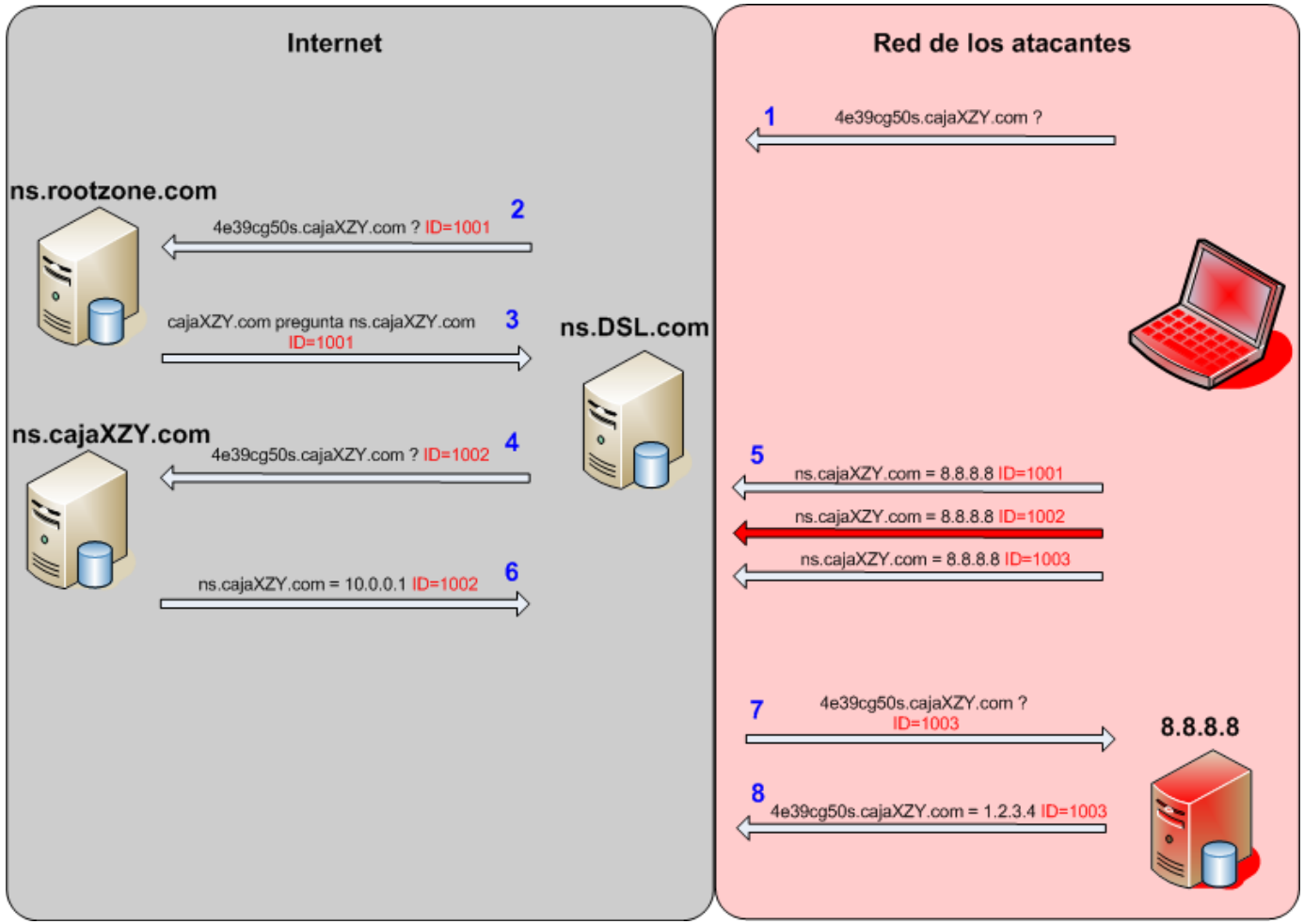


Imagen: Esquema del ataque al protocolo DNS

Referencias:
http://blog.s21sec.com/2008/08/blackhat-las-vegas-2008.html
http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
http://www.heise-online.co.uk/news/DNS-security-problem-details-released--/111145

6. ClickJacking

Clickjacking es la “extensión” de una vulnerabilidad de la que se tiene constancia hace años (en parte se considera una extensión de Cross Site Request Forgery , aunque no todas las técnicas de clickjacking impliquen el uso de CSRF) y que recientemente ha emergido de la mano de dos ingenieros de seguridad: Jeremiah Grossman y Robert Hansen.

La vulnerabilidad se anunció el 16 de sSeptiembre del presente año y los detalles iban a ser divulgados en la conferencia sobre seguridad web OWASP de Nueva York el 22 de septiembre. Finalmente bajo petición de diversas compañías, entre las que destacan Microsoft y Adobe, dicha presentación se anuló (con el beneplácito de los descubridores) con el objetivo de dar más tiempo a los desarrolladores para tomar medidas contra la vulnerabilidad (a pesar de no ser una vulnerabilidad exclusiva de un determinado producto). Los detalles fueron publicados oficialmente el día 7 de octubre en el blog de Robert Hansen.

Básicamente consiste en un ataque en el que un usuario web hace click en un elemento de una página para realizar una determinada acción, a priori legítima para él (acceder a algún sitio restringido, enviar un formulario, etc.), pero en vez de ejecutar una operación “legal”, el atacante “secuestra” dicho elemento para efectuar cualquier otra acción, es decir, el click es secuestrado por el atacante.

Este vector de ataque, no sólo es un problema que afecte a los distintos navegadores o a determinados productos sino que es un problema con muchas más implicaciones de lo que puede parecer a priori.

El ataque se ejecuta mediante una página web maliciosa con objetos incrustados normalmente desde otro domino (ya sea mediante iframes, modificación de contenidos, flash, java, etc), mediante el uso de HTML dinámico u hojas de estilo en cascada el atacante puede esconder el destino de la ejecución del click al usuario.

En este contexto, el uso de Javascript incrementa la efectividad del ataque ya que permitiría monitorizar el puntero del ratón en todo momento. Existen multitud de técnicas que hacen que la vulnerabilidad sea explotable en entornos muy diversos sin la necesidad de recaer en Javascript, por ejemplo mediante el uso de iframes.

Las posibilidades del ataque son múltiples: como ha podido demostrarse en alguna prueba de concepto, es posible, mediante el uso de la técnica de clickjacking, hacer que un usuario haga click en una web legítima a simple vista, activando, de forma oculta, el envío de audio/video desde su webcam hacia el destino seleccionado por el atacante.

Desde su aparición se han comentado diversas estrategias para reaccionar contra este bug: modificación de código por parte de los webmasters para que impidan el uso de iframes, redefinir el estándar HTML para conseguir un mayor control de los enlaces y referencias de una página web (medida efectiva pero poco realista), volver a los navegadores de solo texto como Lynx (sin comentarios), etc. La conclusión que prevalece es que la manera más efectiva y escalable de tomar medidas, recae en los desarrolladores de navegadores.

Actualmente, la solución “temporal” más efectiva es utilizar el navegador Firefox con el complemento NoScript, que desde su versión 1.8.2.1 lleva implementadas medidas específicas contra esta vulnerabilidad.

7. MS08-067

El pasado día 23 de oOctubre Microsoft lanzó una actualización crítica fuera de su ciclo habitual (Boletín MS08-067) para parchear una vulnerabilidad que permite ejecutar código de manera remota si el sistema afectado recibe una petición RPC especialmente diseñada.

Referencias:
http://www.youtube.com/watch?v=gxyLbpldmuU
http://ha.ckers.org/blog/20081007/clickjacking-details/
http://en.wikipedia.org/wiki/Cross-site_request_forgery
http://blogs.adobe.com/psirt/2008/09/thanks_to_jeremiah_grossman_an.html
http://ha.ckers.org/blog/20080915/clickjacking/

La clasificación es crítica para sistemas Windows XP, versiones inferiores a éste y para la familia de servidores 2003. En cambio, para las nuevas versiones de Windows (Vista y Server 2008), ha sido clasificada de importante, ya que para una correcta explotación el usuario debe estar autenticado previamente.

Dicha vulnerabilidad explota un desbordamiento de buffer a través de la función NetPathCanonicalize() residente en la librería netapi32.dll. De este modo, el atacante puede realizar una escalada de privilegios usando la pipe \\pipe\srvsvc para acceder a otras máquinas de la red.

Al poco tiempo de hacerse público el fallo, se detectaron los primeros exploits, así como diversos ejemplos de código malicioso que ya se aprovechaban de dicha vulnerabilidad, entre ellos destacan principalmente los siguientes:

• Win32/Gimmiv.A :

Troyano que roba información sensible de la máquina infectada y a su vez intenta infectar otras máquinas (características de gusano). Hay dos componentes principales de este espécimen, un dropper y una DLL, que una vez instalada en %System%\wbem\sysmgr.dll, efectúa el payload correspondiente.

Se crean las siguientes entradas en el registro para ejecutarse como servicio del sistema:

HKLM\SYSTEM\CurrentControlSet\Services\sysmgr
HKLM\SYSTEM\CurrentControlSet\Services\sysmgr\Parameters\ServiceDll ="%System%\wbem\sysmgr.dll"
HKLM\SYSTEM\CurrentControlSet\Services\sysmgr\Parameters\ServiceMain= "ServiceMainFunc"
HKLM\SYSTEM\CurrentControlSet\Services\sysmgr\DisplayName = "System Maintenance Service"
HKLM\SYSTEM\CurrentControlSet\Services\sysmgr\ImagePath = "%SystemRoot%\System32\svchost.exe -k sysmgr"

Referencias:
http://www.milw0rm.com/exploits/6824
http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

Seguidamente, la DLL se elimina del sistema mediante la ejecución de:

"%Temp%\<random name >.bat".

Una vez infectado el sistema, el troyano roba información confidencial (versión del sistema operativo, usuarios y contraseñas almacenados en el equipo, información sobre los antivirus instalados en el equipo, etc) y envía los datos recopilados hacia la IP 59.106.145.58 mediante el protocolo HTTP.

Gimmiv.A también se conecta a la IP mencionada para descargar un archivo .cab en %System%\initproc02x.cab, que contendrá los componentes necesarios para cargar el gusano, que utilizará la vulnerabilidad MS08-067 para infectar otras máquinas escaneando el puerto TCP 139 en busca de otros hosts vulnerables. Una vez localizados nuevos objetivos, envía una petición de conexión RPC para conectarse a ese host usando el UUID (Identificador Universal Único) 4b324fc8-1670-01d3-1278-5a47bf6ee188. Una vez explotada la vulnerabilidad, ejecuta la rutina de descarga del troyano en la nueva máquina infectada.

- W32-Downadup o Win32/Conficker.A :

Gusano que inyecta su código en el proceso services.exe para permanecer residente en memoria y dificultar la desinfección. También crea un nuevo servicio en el equipo infectado denominado netsvcs y añade las siguientes claves en el registro:

"%Temp%\<random name >.bat".
*HKLM\SYSTEM\CurrentControlSet\Services\<random filename>**\Parameters\ServiceDll** =*
"%System%\<random filename>"

Referencis:
http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
http://community.ca.com/blogs/securityadvisor/default.aspx

Una vez infectada la máquina, comprueba la fecha actual, si esta es inferior o igual al 1 de diciembre, intenta descargase el archivo loadadv.exe desde la dirección *hxxp://trafficconverter.biz/4vir/antispyware/loadadv.exe.*

Este archivo es un falso Anti-Spyware que, tras realizar falsos escaneos, proporcionará ciertos resultados indicando que es necesaria una limpieza del equipo, invitando al usuario a comprar la versión completa del producto. Si la fecha del sistema está entre el 25 y el 30 de noviembre, intenta conectarse a otros dominios diferentes pertenecientes a la infraestructura delictiva. Además, realiza más peticiones HTTP, una de ellas intentando descargarse una base de datos de geolocalización de IPs desde: *http://www.maxmind.com/download/geoip/database/GeoIP.dat.gz*

Conficker.A ejecuta un servidor HTTP en el equipo infectado utilizando un puerto aleatorio, lo que permitirá que otros sistemas víctimas descarguen el gusano. También intenta averiguar la dirección IP del equipo infectado mediante los siguientes servidores: *www.getmyip.org; getmyip.co.uk; checkip.dyndns.org*

Mantiene el control de infección por equipo (sólo se permite una copia del código malicioso corriendo en el sistema). A tal efecto, el gusano crea una exclusión mutua con el formato Global\<números aleatorios>-<números aleatorios>.

8. Vulnerabilidad Collab.collectEmailInfo() en Adobe Acrobat Reader

Tal y como se vio durante el mes de noviembre del presente año, se registraron diversos incidentes en el que nuevamente se utilizaron archivos PDF como origen de diversas infecciones. Uno de los factores que aumentan la peligrosidad de este tipo de infecciones, es la percepción de que son documentos estáticos e inofensivos desde el punto de vista de la seguridad. Nada más alejado de la realidad. Desde la versión 1.4 de dicho formato se permite la inclusión de scripts, objetos incrustados, etc., lo que permite a los cibercriminales un importante y nuevo punto de infección.

Referencis:
http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
http://community.ca.com/blogs/securityadvisor/default.aspx

Esta nueva oleada de infecciones se valía de una nueva vulnerabilidad crítica en el programa Adobe Acrobat Reader (en sus versiones anteriores a la 8.2.1), que permitía la ejecución de código arbitrario en el sistema infectado. La vulnerabilidad residía en la función Collab.collectEmailInfo(), que al no comprobar correctamente los argumentos de entrada, concretamente en el argumento msg, permitía explotar dicha función y ejecutar el código especialmente creado por el atacante.

En este caso, el departamento de e-crime de S21sec detectó infraestructuras de código malicioso que sacaban provecho de dicha vulnerabilidad. En primera instancia, los atacantes debían engañar al usuario para que éste abriera el PDF especialmente creado, mediante técnicas de ingeniería social o mediante la inclusión de iframes en sitios web legítimos vulnerables. Una vez abierto, las acciones llevadas a cabo por el exploit son las siguientes:

1) Comprobar versión del programa de Adobe.
2) Relleno en memoria de un array (incluye la shellcode a ejecutar).
3) Segunda comprobación de versión.
4) Creación de un string (que se pasa como argumento a la función vulnerable).
5) Explotación de la función vulnerable (Collab.collectEmailInfo).
6) Ejecución del shellcode.

Los shellcodes detectados en aquel entonces se limitaban a actuar como downloaders, esto es, procedían a descargar y ejecutar un archivo (malicioso).

Debido a la poca documentación existente sobre la capacidad de utilizar lenguajes de scripting en algunos programas, se prevé que durante el año 2009, aparecerán nuevos ataques que utilizarán estas técnicas como origen de infecciones.

Como era de esperar, los exploits relacionados con PDFs se han añadido a los exploits packs más comunes (fiesta, zopack, addpack, etc).

Referencias:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2007-5659

Como solución evidente del problema se recomendó la actualización de los programas implicados hasta su última versión, así como la aplicación de los parches pertinentes.

9. Vulnerabilidad crítica de Internet Explorer 7

El 9 de diciembre, curiosamente a la vez que Microsoft realizaba su actualización mensual de los martes, salió a la luz una vulnerabilidad que afectaba al Internet Explorer 7 en las versiones de Windows XP y 2003, aunque posteriormente se vio que también podía encontrarse en Windows Vista. El problema se encontraba en el parseo de documentos XML por parte de la librería mshtml.dll, que permitía la carga controlada del contenido del registro EAX, desembocando en la ejecución de código arbitrario en la máquina afectada.

Esta vulnerabilidad ha podido localizarse debido a su explotación activa en los sistemas en forma de 0-day. El departamento de e-crime siguió de cerca esta nueva oleada de ataques, descubriendo una campaña de infección masiva mediante la técnica de inyección SQL que a su vez servía para lograr más usuarios infectados.

Se trataba de un escenario parecido a la primera oleada de inyecciones SQL, ya comentada anteriormente, realizada durante la pasada primavera y proveniente de China. En esta ocasión el objetivo era el mismo, pero el ataque se realizaba mediante los usuarios infectados en lugar de realizarse desde una serie de servidores dedicados, dificultando su erradicación.

Todas las páginas que quedaban afectadas redirigían a los usuarios legítimos a páginas que intentaban la infección mediante la explotación de diferentes vulnerabilidades, incluyendo la mencionada. En caso de lograr su objetivo, se instalaba un downloader en la máquina del usuario que descargaba más binarios desde el servidor malicioso, así como un troyano para robo de credenciales de juegos on-line, y el binario para realizar las infecciones masivas de SQL. De este modo, la máquina infectada quedaba preparada para potencialmente descargar más binarios en el futuro, y lista para formar parte de una botnet.

Debido a la criticidad de la vulnerabilidad Microsoft proporcionó el 17 de diciembre un parche para solventar este problema.

10. Colisiones MD5

En la edición 25c3 del “Chaos Computer Club” se realizó una presentación donde se demostró que es posible llevar a cabo un ataque basado en la debilidad del MD5 y sus colisiones. Se ha conseguido suplantar una AC intermedia de tal manera que se pueden firmar todos los certificados que se deseen. Y sí, el coste computacional es elevado (se ha utilizado una granja de 200 PlayStation 3), pero factible, por ejemplo con una buena red distribuida o una buena botnet. Los 7 investigadores involucrados son Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik y Benne de Wege.

Una vez vistas las orejas al lobo, ¿se dejará de utilizar definitivamente MD5? ¿Se pasará a SHA? La gente pulsa Aceptar aunque el certificado no sea válido, pero ahora no hace falta ni eso.

¿Seguimos necesitando de una prueba real para creer que un ataque teórico es serio? Esto es una prueba de que no debería ser así. Realmente no se ha presentado ninguna novedad técnica aunque, como bien decían en la charla, las colisiones MD5 se presentaron hace años, pero parece que mientras no se publique una utilidad que permita hallar una colisión con dos clicks y tarde 5 minutos no es un descubrimiento importante. La teoría bien fundamentada es tan importante como la práctica.

Referencias:
http://www.phreedom.org/research/rogue-ca/md5-collisions-1.0.ppt
http://www.win.tue.nl/hashclash/rogue-ca/
https://i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org/

Tendencias y predicciones 2009

En la línea de lo comentado en este estudio, el fraude on-line sigue en constante crecimiento tal y como se desprende de las diferentes estadísticas recopiladas.Teniendo en cuenta este hecho y el aumento en el número de casos atendidos en estos primeros meses de 2009, podemos prever un elevado incremento para el 2009.

Uno de los factores que sin duda incrementará la proliferación de nuevos esquemas de fraude es la continuidad del estancamiento económico mundial durante todo el año 2009, que será aprovechado por los delincuentes en mayor medida para conseguir elevar su número de víctimas.

El hecho de engañar a usuarios mediante falsas promesas de trabajos, loterías, premios y en general cualquier argumento que pueda suponer un ingreso de dinero fácil se seguirá produciendo de manera cada vez más acentuada durante este año 2009, optimizando progresivamente las técnicas utilizadas hasta llegar a un grado de sofisticación que supondrá un aumento en el número de **ataques "personalizados"** (spear phishing) orientados hacia diferentes perfiles de usuario, incluso logrando cierta individualización en los mensajes destinados a captar la atención de los usuarios.

Este hecho se verá sin duda facilitado en gran medida por la ya comentada proliferación del uso de **redes sociales** y por el aprovechamiento por parte de los "atacantes" de todas aquellas fuentes que puedan contener información que facilite el proceso de ganarse la confianza de la víctima ya sea para conseguir una nueva infección o para utilizarla en algún esquema de blanqueo de dinero una vez acometido el fraude.

El uso de técnicas de **ingeniería social** no es nada nuevo, pero el hecho de que este tipo de ataques estén "respaldados" por un factor externo que afecta a prácticamente a la totalidad del mundo: la crisis económica, hará que mucha gente sea más receptiva (consciente o inconscientemente) a este tipo de engaños.

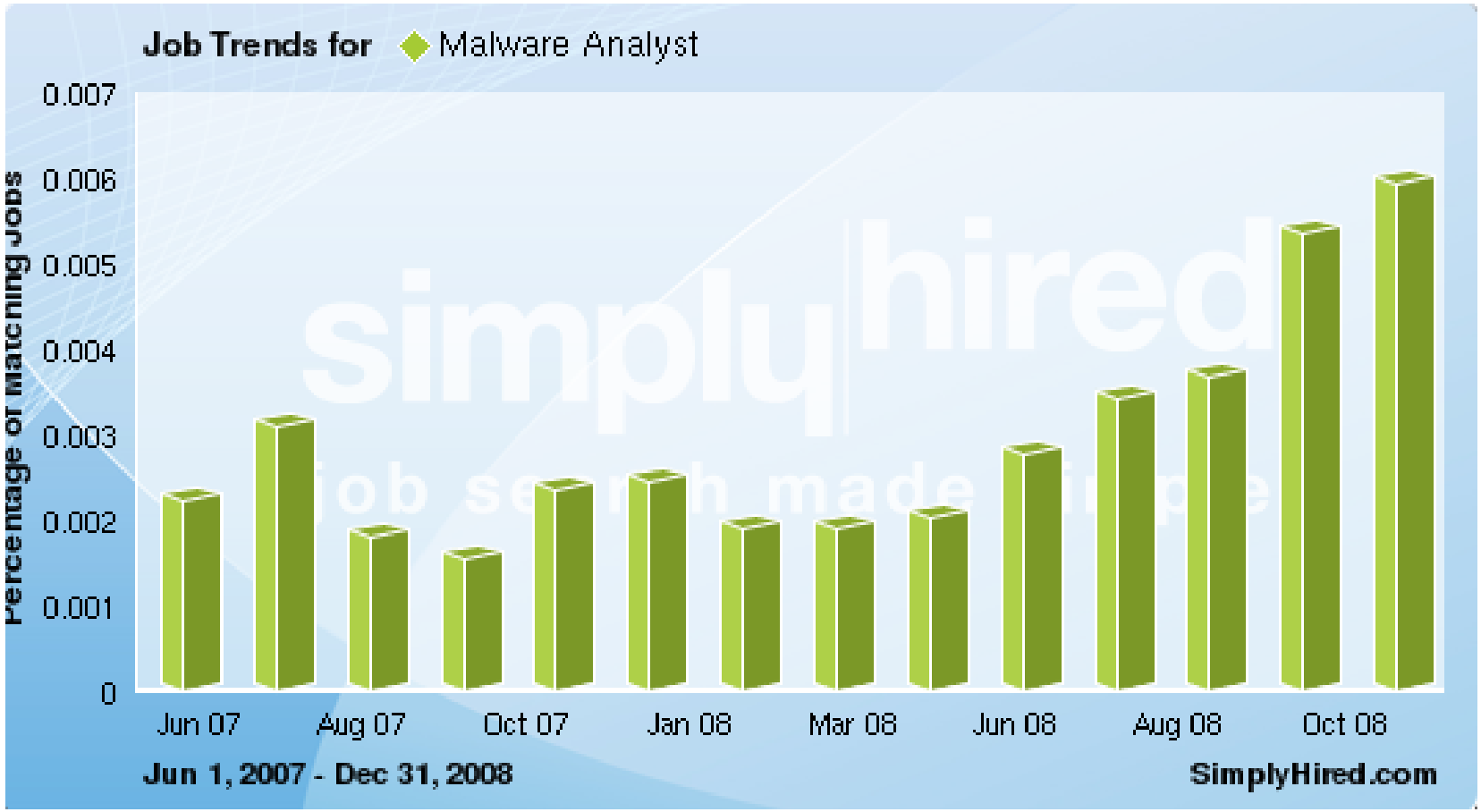
Otro de los puntos a tener en cuenta, es la continua profesionalización del cibercrimen con la imparable irrupción de **bandas organizadas**, dotando a sus infraestructuras de más recursos operativos para lograr sus objetivos.

Probablemente se acentúe esta profesionalización y su consiguiente enfoque hacia un modelo de empresa "legítima". De este modo es de esperar que los esfuerzos de estas organizaciones se oriente cada vez más al robo de **datos corporativos**, dado que con la misma inversión conseguirán datos mucho más valiosos para su posterior venta y utilización. Esta suposición puede respaldarse al comprobar las diferencias de precios en el mercado negro de información perteneciente a particulares (tarjetas de crédito, contraseñas, etc.) en contraposición al mayor valor que representa información financiera de grupos empresariales o financieros.

Por otro lado, los recursos de la industria de la seguridad (especialmente la lucha contra el fraude) muestran también una tendencia al aumento (al menos su solicitud en el mercado laboral).

La solicitud de perfiles técnicos relacionados con la investigación y desarrollo de estrategias y tecnologías contra todo tipo de código malicioso seguirá en aumento durante este año, aunque es probable que no se llegue a equilibrar la balanza entre los recursos utilizados en ambos lados del juego aunque se produzca una mayor inversión por parte de todos los actores participantes en el mundo del fraude on-line.

Durante el año 2009, posiblemente se asista a una mayor concienciación sobre la realidad del cibercrimen por parte del espectro político a nivel mundial, lo que se traducirá en nuevas regulaciones, leyes y propuestas. Quedará por ver la efectividad real de estas medidas.



Fuente: www.simplyhired.com

Siguiendo con la vertiente política, hay que tener en cuenta la posibilidad de que la difusión de código malicioso vía **p2p** disminuya en algunos países, con la entrada en vigor del endurecimiento de la ley antipiratería. Francia, Reino Unido, Italia o Irlanda son ejemplos de países en los que las medias antipiratería entraran en vigor recientemente. Otros países como Alemania, han decidido no extrapolar estas leyes a su régimen jurídico. La situación en España en este sentido, indica que es probable que se produzcan cambios respecto a la legislación sobre este tipo de redes, aunque no está demasiado claro cómo evolucionará el panorama.

El hecho que disminuya la posibilidad de infecciones vía p2p, no significa que el fraude on-line no siga creciendo mediante el uso de otras vía de infección, destacando claramente la **WWW** como método principal de propagación.

Uno de los aspectos más positivos a los que asistiremos durante este año, será el incremento por parte de los sectores tanto públicos como privados del uso de Inteligencia basada en la recogida y análisis de información obtenida mediante fuentes públicas: **OSINT (Open Source Intelligence)**, y será bajo estas directrices de compartir información de manera responsable y controlada cuando se obtengan mejores y más efectivos resultados contra la lucha contra el fraude tecnológico consiguiendo acortar los tiempos de cierre de infraestructuras criminales.

Otro hecho a destacar será la continuidad y optimización de los ataques utilizando diferentes tecnologías (ya se han visto ejemplos durante el año pasado de técnicas de infección mediante el uso de Flash o documentos pdf). En este sentido se percibirá un incremento en el uso de banners publicitarios propagados por los cibercriminales con contenido malicioso en forma de campañas publicitarias difíciles de resistir, ya sea creando una nueva red de anuncios on-line, o utilizando vulnerabilidades en las redes de anuncios existentes. En definitiva, el código malicioso será el protagonista de la mayoría de casos de fraude on-line en detrimento de otro tipo de esquemas como el phishing.

La proliferación de la telefonía móvil y la evolución de las tecnologías necesarias para implementar todo tipo de aplicaciones en este tipo de dispositivos acentuará el uso de este recurso por parte de los ciberdelincuentes. Probablemente se empiecen a ver implicados **smartphones** ya sea como método de propagación, o como método para optimizar todo el proceso de ocultamiento de la comunicación del código malicioso con su respectivo panel de control (**mymobilesite** para nokia o **Freebit** para Iphone podrían ser utilizados a tal efecto).

En ambos métodos se agudizará el uso de técnicas de evasión de filtrados de URLs, la mayoría de binarios maliciosos pasaran a usar redirectores para traspasar mecanismos como el **Safebrowsing** de Google, y proliferará el uso de servicios como **Tinyurl** y similares para ofuscar la dirección de destino.

También es importante destacar que es muy probable que se creen nuevas familias de troyanos cuyo objetivo será atacar a empleados de sectores muy concretos (banca, sanidad, financiero). Ya se pudo ver a finales de 2008 un fichero de configuración de una muestra de código malicioso en la que claramente destacaba como objetivo el robo de credenciales a dispositivos que normalmente se utilizan como **gateway** para conectar a los empleados con su red interna (sistemas VPNSSL y similares).

Colabore en la prevención del cibercrimen, su participación es importante. Si lo detectas contacte con nuestro servicio de alerta en el correo de ecrime@s21sec.com o a través de nuestra web www.s21sec.com .

*[Barcelona . León . Madrid . Pamplona
San Sebastián . Sevilla . Londres . México DF . Monterrey]