El Negocio de los Falsos Antivirus

Análisis del Nuevo Estilo de Fraude Online

PandaLabs – Julio 2009

Sean Paul Correll -Luis Corrons

Resumen ejecutivo

La proliferación del malware se ha extendido en los últimos años y el número de amenazas ha alcanzado proporciones asombrosas. Por desgracia, el crimen informático se ha convertido en un peligro oculto dentro de nuestra sociedad, y detrás de esta tendencia creciente se encuentra un tipo de malware llamado 'rogueware' o falsos antivirus: una variedad mucho más omnipresente y peligrosa que las amenazas anteriormente observadas por los investigadores de seguridad. El rogueware consiste en falsas soluciones de software diseñadas para robar dinero a los usuarios de ordenadores, cobrándoles por eliminar amenazas que en realidad no existen.

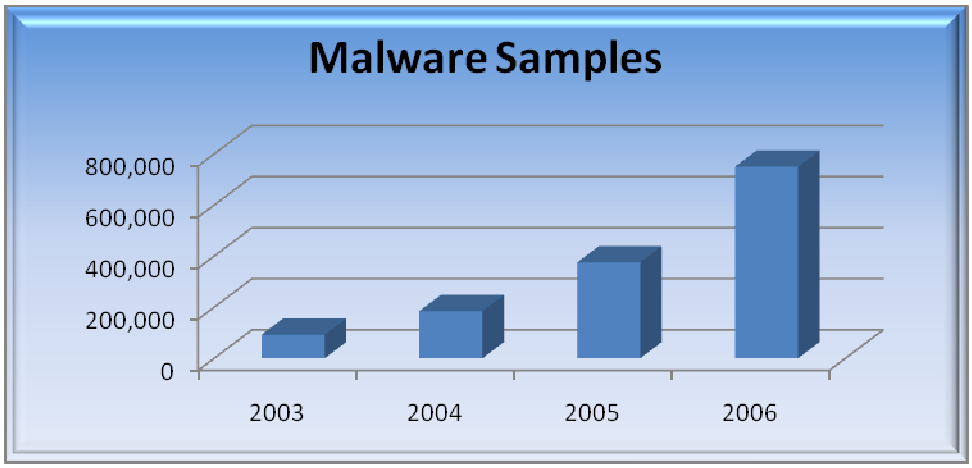
A finales del año 2008 PandaLabs detectó casi 55.000 ejemplares de rogueware. El objetivo de este estudio es investigar la economía creciente de los falsos antivirus, su asombrosa proliferación y los efectos que han tenido hasta ahora.

El estudio ha tenido resultados sorprendentes:

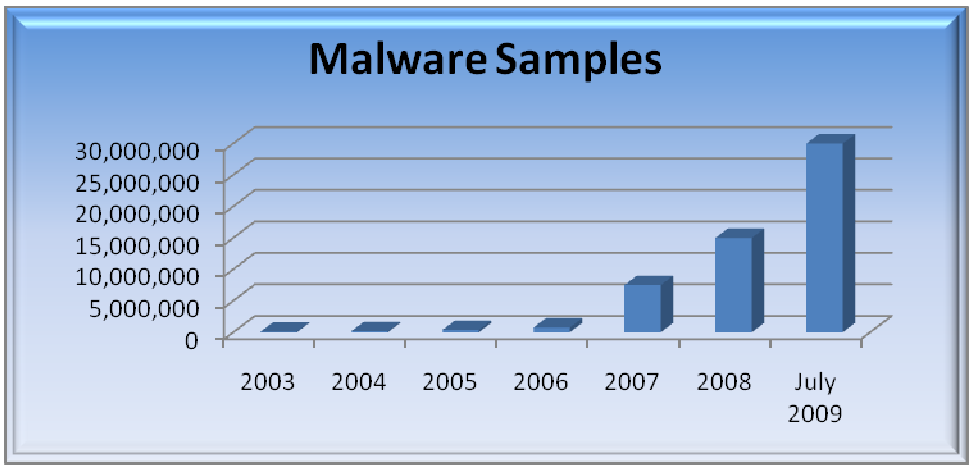
- Estimamos que para finales del 3er trimestre de 2009 detectaremos más de 637.000 nuevos ejemplares de rogueware (un incremento de diez veces en menos de un año).
- El rogueware infecta aproximadamente 35 millones de nuevos ordenadores cada mes (alrededor de un 3,50 por ciento de todos los ordenadores).
- Los ciber-delicuentes están ganando unos 34 millones de dólares al mes gracias a los ataques de rogueware.

Historia de la proliferación del malware

En los últimos años, el malware ha crecido muy velozmente tanto en volumen como en sofisticación. La gráfica inferior muestra la situación del malware entre los años 2003 y 2006, un período de tiempo en el que la cantidad de ejemplares en circulación se duplicaba cada año:

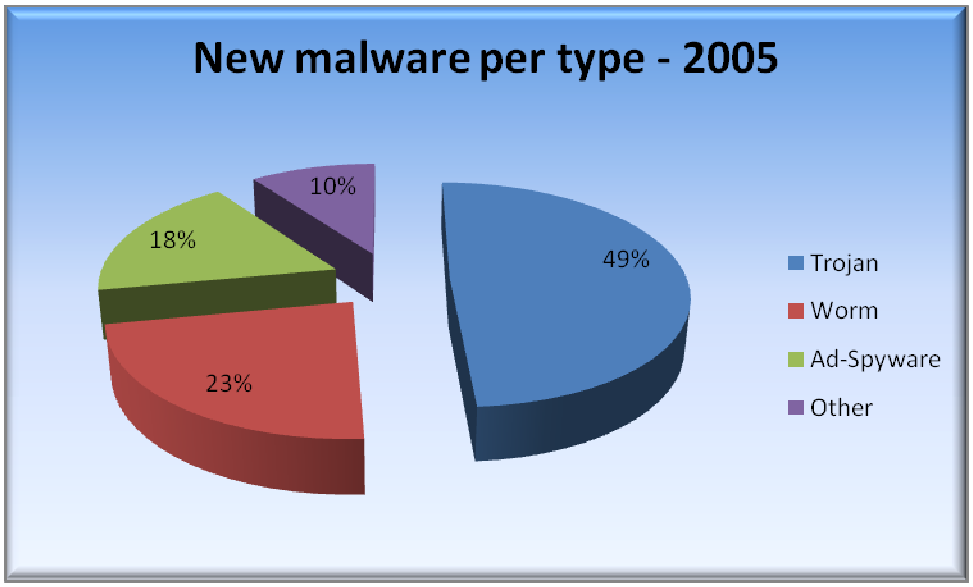


Hace aproximadamente cinco años sólo existían 92.000 ejemplares, mientras que a finales del 2008 había unos 15 millones. Al finalizar este estudio en julio del 2009, PandaLabs había detectado más de **30 millones de ejemplares de malware**.

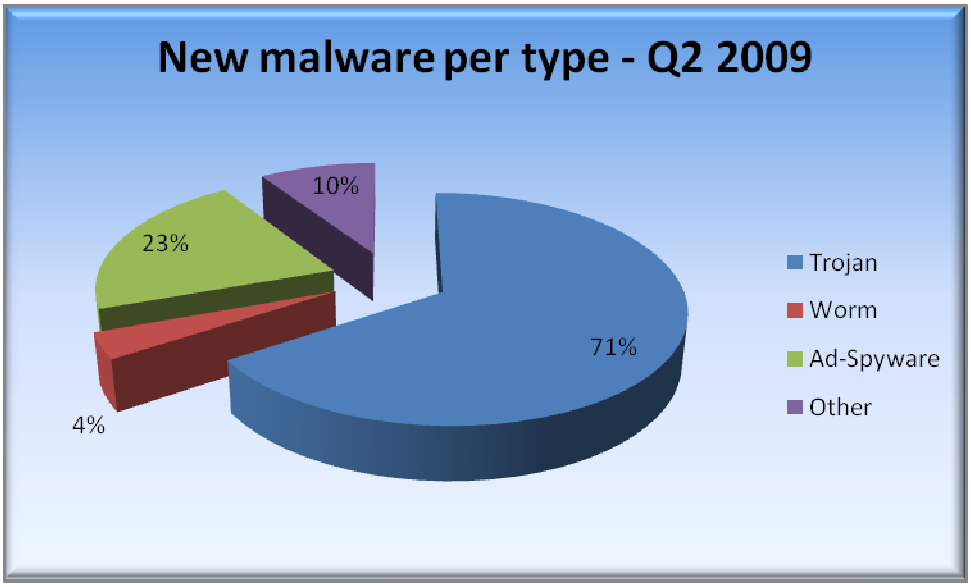


El motivo de este espectacular aumento está claro: el dinero. El año 2003 supuso el nacimiento de los troyanos bancarios. Desde entonces, estos códigos maliciosos, diseñados para robar las credenciales de acceso a servicios de banca online, se han convertido en la actualidad en una de las formas más habituales de malware. Cada día salen a la luz nuevas variantes que han evolucionado tecnológicamente para esquivar las medidas de seguridad de los bancos. Varias organizaciones, como el Anti-Phishing Working Group (www.antiphishing.org) han intentado unir a los diversos miembros de la industria de seguridad informática para contrarrestar los esfuerzos de los ciber-criminales. Sin embargo, se trata de una batalla larga y dura, y ni siquiera está claro si podremos ganarla alguna vez.

En general, el motivo de que se creen más troyanos, keyloggers y bots que ningún otro tipo de malware es porque resultan los más útiles para el robo de identidad. En el año 2005, casi la mitad de los nuevos códigos maliciosos eran troyanos:



En la actualidad, en el segundo trimestre de 2009, la situación es mucho peor, ya que los troyanos suponen el 71 por ciento del nuevo malware:



Al igual que en cualquier otro negocio, los delincuentes informáticos buscan operar de la forma más eficaz posible. A la hora de desarrollar un troyano, deben decidir qué plataformas soportará y el número de victimas potenciales. Windows es la plataforma atacada en más del 99 por ciento de los casos, siendo también la que más usuarios tiene hasta la fecha.

El objetivo final de los delincuentes es obtener beneficio económico del malware. Los troyanos resultan la herramienta perfecta para robar información. Sin embargo, dicha información debe convertirse en dinero contante y sonante, y los criminales deben buscar métodos innovadores para conseguirlo.

Aquí es donde entran los falsos antivirus. Estas aplicaciones se hacen pasar por soluciones antivirus que detectan cientos de amenazas en los ordenadores de sus víctimas. Sin embargo, cuando los usuarios tratan de eliminar dichas amenazas utilizando la aplicación, se les pide que compren la correspondiente licencia. A menudo, los usuarios, preocupados por la supuesta infección, acaban adquiriendo la licencia. Una vez pagan la licencia, no vuelven a saber nada más del supuesto "vendedor" y siguen teniendo el falso antivirus en su ordenador.

A pesar de que estas aplicaciones llevan ya varios años en circulación, no fue hasta principios del año 2008 que comenzaron a ser empleadas de forma masiva.

Rogueware

Los efectos de los falsos antivirus

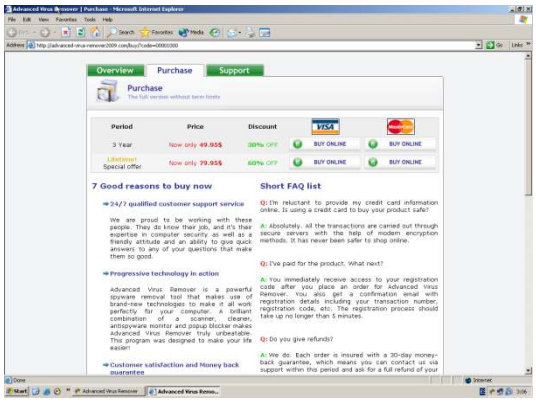
Síntomas del rogueware

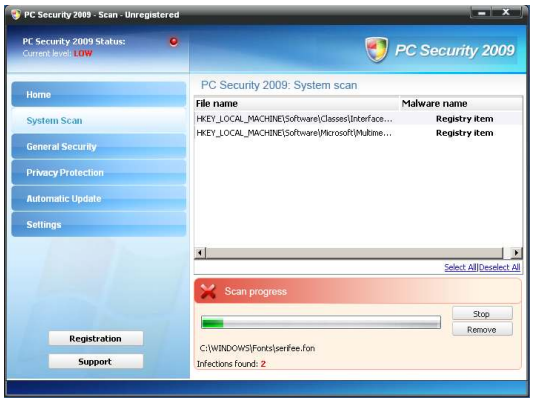
Además de quedarse con el dinero de los consumidores y ofrecer justamente lo contrario a proteger la seguridad, muchos falsos antivirus comparten las siguientes características:

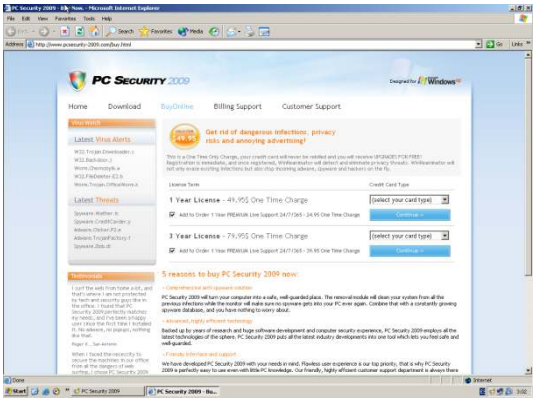
- Muestran falsos avisos emergentes, lanzan mensajes desde la barra de tareas y modifican el salvapantallas y el escritorio
- Su diseño es parecido al de un antivirus real
- Completan un análisis del sistema con gran rapidez
- Las “infecciones” detectadas hacen referencia a distintos archivos en cada análisis.
-

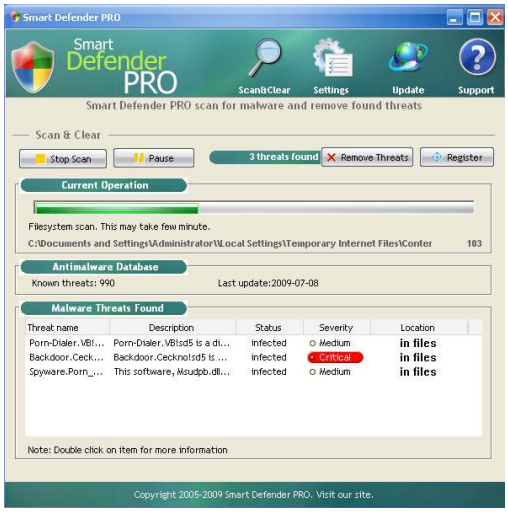
Por otro lado, los falsos antivirus modifican el sistema operativo para evitar que se eliminen los falsos avisos que muestran. Estas acciones incluyen ocultar las pestañas Escritorio y Protector de pantalla de la sección Pantalla del Panel de Control del ordenador. Esto impide a los usuarios restaurar su fondo de escritorio y su salvapantallas. El objetivo de estas técnicas es acabar con la paciencia de los usuarios para que finalmente registren el producto y paguen la cuota correspondiente.

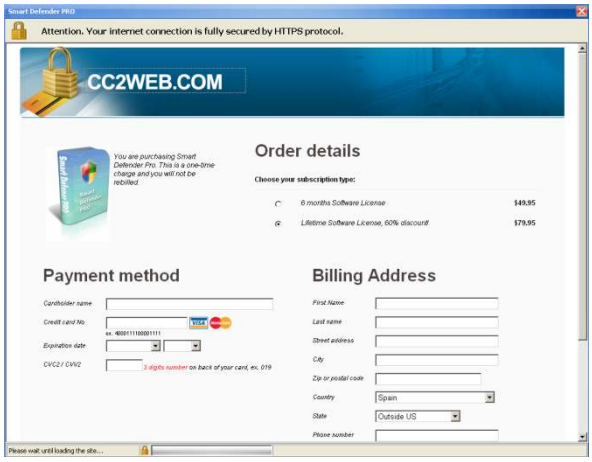
A continuación se muestran varios ejemplos de rogueware y las plataformas de pago a las que redirigen a los usuarios cuando intentan “desinfectar” sus sistemas:

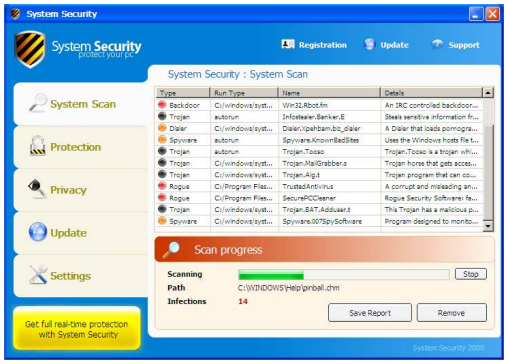


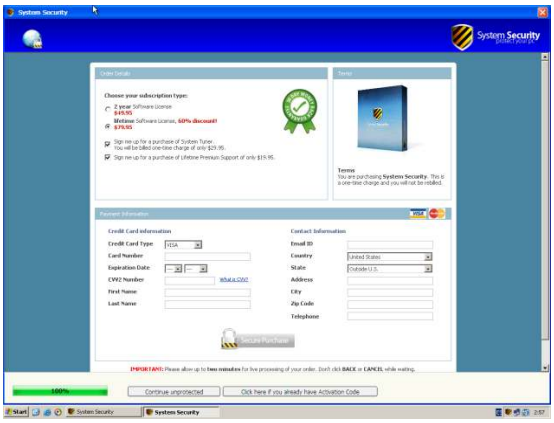








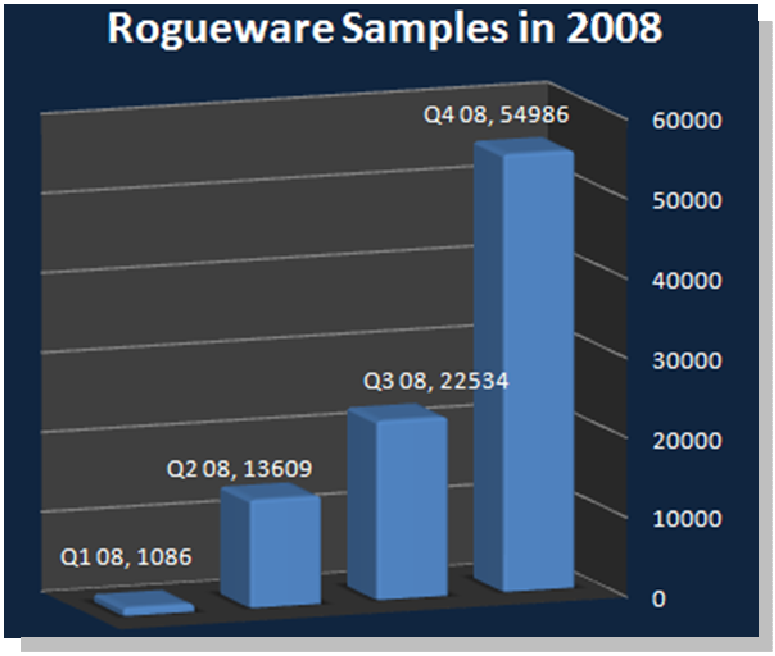




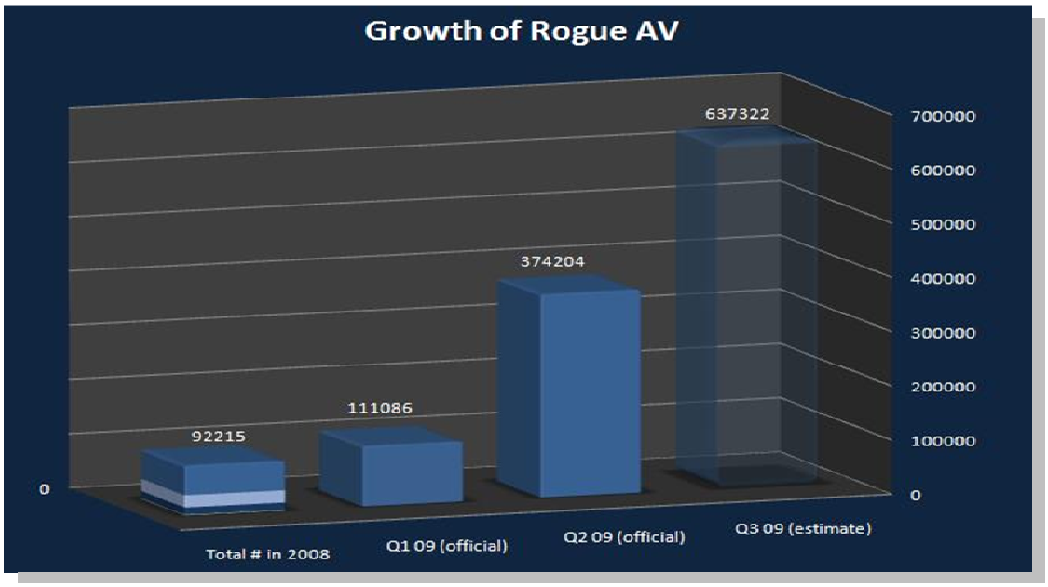
Los delincuentes ya no necesitan robar información a los usuarios para ganar dinero; simplemente hacer que los usuarios se desprendan voluntariamente del mismo. Tal y como se muestra anteriormente, la interfaz de los falsos antivirus está diseñada muy cuidadosamente y resulta extremadamente convincente, lo que indica que los criminales están invirtiendo mucho dinero y esfuerzo en desarrollar y distribuir estos programas. Además, utilizan técnicas agresivas para asustar a los usuarios y hacer que compren la licencia.

Evolución de los falsos antivirus desde el año 2008 al 2º trimestre de 2009, y predicciones para el futuro

Los falsos antivirus están experimentando un crecimiento exponencial. En el 2º trimestre del año 2008 PandaLabs creó un equipo especializado en la detección y eliminación de este tipo de malware. La gráfica que aparece a continuación muestra el crecimiento de los falsos antivirus durante el año 2008:



El número de ejemplares creció de forma exponencial, y la evolución de los mismos durante el año 2009 muestra una curva de crecimiento aún mayor:

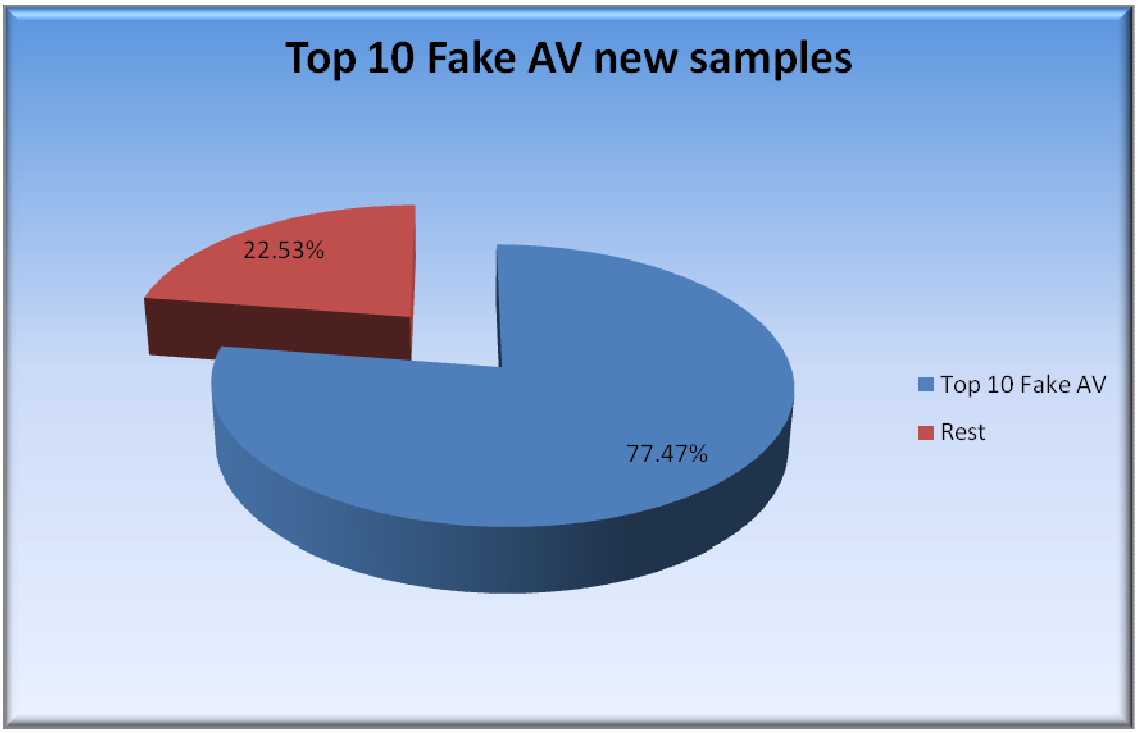


Solamente en el 1er trimestre de 2009 se crearon más ejemplares que durante todo el año 2008. El 2º trimestre fue aún peor, ya que surgieron cuatro veces más ejemplares que en el año 2008. PandaLabs calcula que en el 3er trimestre de este año el número total de ejemplares de malware superará la cifra surgida en los 18 meses anteriores.

El motivo principal para la creación de tantas variantes es evitar la detección basada en firmas de los programas antivirus reales. El uso de técnicas de análisis de comportamiento, tan eficaz con los gusanos y troyanos, tiene poco éxito con este tipo de malware, ya que estos programas en sí no actúan de forma maliciosa en los ordenadores, si no que únicamente se limitan a mostrar información falsa.

Los delincuentes emplean varios métodos para crear las diversas variantes. Una de las técnicas más utilizadas es el polimorfismo del lado del servidor, que significa que cada vez que se descarga el falso antivirus se trata de un archivo binario distinto.

A pesar de que existen aproximadamente 200 familias distintas de rogueware, al extrapolar los datos del 2º trimestre de 2009, se ha descubierto que 10 de estas familias son responsables del 77.47 por ciento de todas las variantes:



Si se echa un vistazo a las 20 familias que más rogueware pusieron en circulación en el último semestre, éstas suponen aproximadamente el 90 por ciento de todos los ejemplares de malware:

Falsos antivirus	Número de ejemplares	%
SystemSecurity	70883	18,94%
SystemGuard2009	38927	10,40%
Xpantivirus2008	33233	8,88%
WinPcDefender	32749	8,75%
Antivirus2009	29666	7,93%
SpywareGuard2008	24323	6,50%

XPPolice	20151	5,39%
AntivirusXPPro	19536	5,22%
SystemSecurity2009	10265	2,74%
MSAntiSpyware2009	10191	2,72%
SecuritySystem	9512	2,54%
ProAntispyware2009	8628	2,31%
RogueAntimalware2009	7382	1,97%
MalwareDefender2009	6120	1,64%
PCProtectionCenter2008	4949	1,32%
VirusResponseLab2009	4409	1,18%
VirusShield2009	4218	1,13%
WinDefender2009	4038	1,08%
VirusRemover2008	3242	0,87%
AdvancedVirusRemover	2931	0,78%

Infecciones por falsos antivirus en el primer semestre de 2009

El número de variantes no tiene por qué coincidir necesariamente con la proporción de ordenadores infectados por los falsos antivirus. Para comprobar el grado de distribución de los falsos antivirus, PandaLabs generó ratios de infección a partir de sus servidores de estadísticas, y descubrió que aproximadamente el 98 por ciento de todos los ordenadores analizados estaban infectados.

A continuación, PandaLabs recogió datos de los ordenadores infectados por los falsos antivirus y descubrió que el 3,50 por ciento de los ordenadores analizados cada mes estaba infectado con rogueware. Como hemos explicado anteriormente, la masiva creación de nuevas variantes tiene como objetivo evitar su detección por parte de los antivirus, por lo que las familias más infecciosas no tienen por qué ser las más prolíficas.

La siguiente tabla muestra una clasificación de las 20 familias de falsos antivirus que más infecciones han causado en el último semestre. Estas familias representan el 81,67 por ciento de todas las infecciones detectadas por PandaLabs relacionadas con el rogueware. Las familias marcadas en rojo aparecen también en la lista de las 20 familias con el mayor número de ejemplares en circulación:

1	**Antivirus2009**	**15,89 %**
2	**VirusRemover2008**	**9,90%**
3	**Xpantivirus2008**	**8,52%**
4	**XPAntiSpyware2009**	**6,13%**
5	**SystemGuard2009**	**5,26%**
6	**SpywareRemover2009**	**4,34%**
7	**Antivirus360**	**3,88%**

8	**RealAntivirus**	**3,57%**
9	**RogueAntimalware2008**	**3,45%**
10	**SystemSecurity**	**3,42%**
11	**SpywareGuard2008**	**2,67%**
12	**AntivirusPro2009**	**2,39%**
13	**AntivirusXP2008**	**2,04%**
14	**MSAntiSpyware2009**	**1,87%**
15	**RogueAntimalware2009**	**1,69%**
16	**AntivirusXPPro**	**1,67%**
17	**ProAntispyware2009**	**1,57%**
18	**SecurityCenter**	**1,38%**
19	**AntiMalwareSuite**	**1,02%**
20	**Antispy2008**	**1,00%**

Implicaciones económicas

Debido al rápido crecimiento del rogueware y a su único objetivo de obtener beneficios financieros, PandaLabs ha querido cuantificar el efecto económico de este tipo de malware en la economía global. Basándose en estimaciones existentes dentro de la industria informática, PandaLabs ha extrapolado información y calculado una serie de cifras para demostrar las consecuencias económicas del rogueware. Según la consultora Forrester Research, existen aproximadamente mil millones de ordenadores en todo el mundo. Basándose en esta cifra, PandaLabs calcula que aproximadamente 35 millones de ordenadores (el 3,5 por ciento del total) se infectan con rogueware cada mes. Esto no quiere decir que 35 millones de personas se infectan cada mes, ya que hay personas que utilizan un ordenador distinto en casa y en el trabajo. Teniendo esto en cuenta, consideraremos que la mitad de dicha cifra corresponde a usuarios reales: 17,500,000.

Otra empresa consultora dentro del sector informático, el grupo Gartner, ha estimado que el 3,30 por ciento de las personas pierden dinero debido al phishing, ya que envían sus datos bancarios a phishers. El rogueware es mucho más agresivo y tiene mayor poder de engaño que el phishing. Sin embargo, no existe ninguna investigación hasta la fecha que cuantifique el número de personas que han sido engañadas y han comprado falso software antivirus para eliminar infecciones inexistentes. Por ello, y basándose en la cifra de Gartner de que el 3,30 por ciento de los usuarios pierde dinero debido al phishing, PandaLabs calcula que 557.500 usuarios compran rogueware cada mes. Es importante tener en cuenta que las técnicas utilizadas por el rogueware son mucho más agresivas que las del phishing, por lo que es probable que esta cifra sea en realidad más alta.

A pesar de que el precio de cada aplicación de rogueware varía, en general existen dos tipos de licencias:

- Las más baratas cuestan 49,95 dólares
- Las más caras cuestan 79,95 dólares

Utilizando estos datos y suponiendo que 2/3 partes de las personas compran la aplicación más barata, y que el precio medio es de 59,95 dólares. PandaLabs ha calculado que los delincuentes están ganando más de 34 millones de dólares al mes gracias al rogueware.

59.95$ * 557.000 = 34.621.125$ ◄—— AL MES

34 millones de dólares mensuales suponen más de 415 millones de pérdidas económicas al año.

Una mirada al negocio del rogueware

En septiembre del año 2008 un hacker conocido como “NeoN” fue capaz de infiltrarse en Bakasoftware (uno de los mayores fabricantes de rogueware) explotando vulnerabilidades de inyección SQL en su página web. Este hacker reveló información clave sobre la forma en que Bakasoftware llevaba a cabo su negocio, y, por primera vez, fue posible ver el daño real que estaba causando el negocio del rogueware.

									Сумма, USD		
Страна	Сабаккаунт	Дата	Продукт	Uniq	Raw	Loader	Сетапы	Покупки	Покупки	Возвраты	Рефералы
Все	Все	2008-08-28	Все продукты	508	508	7	8	198	6989.13	-886.34	0.00
Все	Все	2008-08-27	Все продукты	1023	1023	8	6	848	31686.52	-4068.87	0.00
Все	Все	2008-08-26	Все продукты	1019	1020	8	8	795	28659.07	-2970.27	0.00
Все	Все	2008-08-25	Все продукты	1061	1061	10	7	243	8640.59	-105.13	0.00
Все	Все	2008-08-24	Все продукты	1072	1073	6	5	82	2898.02	-373.11	0.00
Все	Все	2008-08-23	Все продукты	772	775	9	7	71	2515.28	-511.60	0.00
Итого				5455	5460	48	41	2237	81388.61	-8915.32	0.00

El análisis de la las ventas conseguidas por uno de los mayores afiliados de Baka mostró unas beneficios de 81.388,61 dólares en 6 días, lo que significa que, si esta tendencia se mantuviese lo largo de varias semanas, las ganancias totales rondarían los 400.000 dólares mensuales. Eso supone casi 5.000.000 de dólares al año. La cifra resulta realmente astronómica si tenemos en cuenta que este cálculo proviene sólo de uno de los múltiples afiliados de Baka, por no mencionar que el negocio del rogueware se ha cuadruplicado desde el año 2008 (en términos del número de ejemplares).

Sistema de afiliados

El modelo de negocio de los falsos antivirus tiene dos componentes principales: los creadores de los programas y los distribuidores. Los creadores se encargan de crear las falsas aplicaciones, proporcionar las plataformas de distribución, las pasarelas de pago y otros servicios de back office. Los afiliados se encargan de distribuir el rogueware al mayor número de personas de la forma más rápida posible.

E-мейл	ICQ	Payment method	Payment details				
[redacted]	[redacted]	Webmoney	[redacted]				Domains
[redacted]	[redacted]	Webmoney	[redacted]				Domains
[redacted]	[redacted]	Webmoney	[redacted]				Domains
[redacted]	[redacted]	Epassporte	[redacted]				Domains
[redacted]	[redacted]	Webmoney	[redacted]				Domains
[redacted]	[redacted]	Webmoney	[redacted]				Domains
[redacted]	[redacted]	Webmoney	[redacted]				Domains
[redacted]	404799881	Webmoney	[redacted]				Domains
[redacted]	[redacted]	Epassporte	[redacted]				Domains

Normalmente estos afiliados provienen de Europa del Este y son captados en foros de hacking. Ganan una cantidad variable por cada instalación y una comisión del 50 al 90 por ciento por las ventas completadas. El método de recaudación más utilizado parece ser Webmoney, aunque también se utiliza Epassporte. Tras ser reclutado, el afiliado proporciona el método de pago que prefiere, así como sus datos de contacto (correo electrónico y número de ICQ). Una vez se introduce al afiliado en el sistema, se le asigna un identificador único que se añade al final de cada dominio de distribución de malware, para así poder hacer un seguimiento de las ventas. (Ej. http://www.rogueware.com/index.php?aid=1200)

TransactionType	Settled	Merchant	FirstName	LastName	Email	CreditCard	Merchant Amou	Total Amoun	IP	TID	AffiliateI
AUTH_ONLY_CAPTURED	Settled	Spyaway	michelle	[redacted]	[redacted]92@comcast.net	3713...1003	$48.95	$49.95	[redacted].157.186	46916819	396123
AUTH_ONLY_CAPTURED	Settled	Spyaway	Juana	[redacted]	[redacted]_06@hotmail.com	5121...3350	$48.95	$49.95	[redacted].10.22	46917674	396126
AUTH_ONLY_CAPTURED	Settled	Spyaway	Peter	[redacted]	[redacted]1982@gmail.com	4063...9884	$48.95	$49.95	[redacted].125.107	46921375	396130
AUTH_ONLY_CAPTURED	Settled	Spyaway	Steve	[redacted]	[redacted]@verizon.net	4264...9385	$48.95	$49.95	[redacted]220.233	46923594	396133
AUTH_ONLY_CAPTURED	Settled	Spyaway	rosemarie	[redacted]	[redacted]tarrs01@aol.com	4744...9411	$48.95	$49.95	[redacted].16.165	46973570	396166
AUTH_ONLY_CAPTURED	Settled	Spyaway	Robin	[redacted]	[redacted]aol.com	4790...0892	$48.95	$49.95	[redacted].200.203	46976483	396170
AUTH_ONLY_CAPTURED	Settled	Spyaway	Zachary	[redacted]	[redacted]er@yahoo.com	4862...8716	$48.95	$49.95	[redacted].92.96	46989064	396183
AUTH_ONLY_CAPTURED	Settled	Spyaway	Kimberly	[redacted]	[redacted]@earthlink.net	4060...1468	$48.95	$49.95	[redacted].63.87	46990599	396184
AUTH_ONLY_CAPTURED	Settled	Spyaway	Kristin	[redacted]	[redacted]erstone@netzero.net	4640...1583	$48.95	$49.95	[redacted]06.80	46991211	396185
AUTH_ONLY_CAPTURED	Settled	Spyaway	Toni	[redacted]	[redacted]cox.net	4147...0461	$48.95	$49.95	[redacted]108.193	46998371	396187
AUTH_ONLY_CAPTURED	Settled	Spyaway	Aad	[redacted]	[redacted]connet.nl	5413...5594	$48.95	$49.95	[redacted].191.79	46998627	396188
AUTH_ONLY_CAPTURED	Settled	Spyaway	stefano	[redacted]	[redacted]lo@tiscali.it	3752...1005	$48.95	$49.95	[redacted].35.61	47003256	396190
AUTH_ONLY_CAPTURED	Settled	Spyaway	WALTER	[redacted]	[redacted]@msn.com	5401...1019	$48.95	$49.95	[redacted].126.200	47008022	396191
AUTH_ONLY_CAPTURED	Settled	Spyaway	nicole	[redacted]	[redacted]p@navy.mil	5155...5443	$48.95	$49.95	[redacted].245.64	47008636	396192
AUTH_ONLY_CAPTURED	Settled	Spyaway	Aram	[redacted]	[redacted]@optonline.net	5466...5712	$48.95	$49.95	[redacted].143.26	47011793	396196
AUTH_ONLY_CAPTURED	Settled	Spyaway	Timothy	[redacted]	[redacted]@iw.net	3732...1003	$48.95	$49.95	[redacted].87.99	47013819	396197
AUTH_ONLY_CAPTURED	Settled	Spyaway	albert	[redacted]	[redacted]orris@comcast.net	5491...3835	$48.95	$49.95	[redacted].75.110	47018075	396198
DECLINED	Pending	Spyaway	jeff	[redacted]	[redacted]e@mchsi.com	4121...2422	$48.95	$49.95	[redacted].154.210		396200
DECLINED	Pending	Spyaway	jeff	[redacted]	[redacted]e@mchsi.com	4121...2422	$48.95	$49.95	[redacted].154.210		396202

PandaLabs ha descubierto también logs de ventas que contenían datos personales de las víctimas engañadas por el rogueware. Se pudieron obtener datos como el nombre completo, datos financieros, direcciones de correo electrónico y direcciones IP de los servidores de las pasarelas de pago. Parece claro que los criminales no sólo buscar beneficiarse de las ventas del rogueware, sino también generar ingresos adicionales vendiendo los logs con los datos extraídos de los pagos.

En definitiva, el programa de afiliados funciona igual que un negocio normal. Uno de los sistemas de afiliados más conocido es el que dirige KlikVIP, que ofrece comisiones a cualquiera que instale sus aplicaciones de rogueware, y de vez en cuando organiza fiestas con sus "distribuidores". Estas fotos son de la última fiesta que celebraron en Montenegro en marzo del 2008:

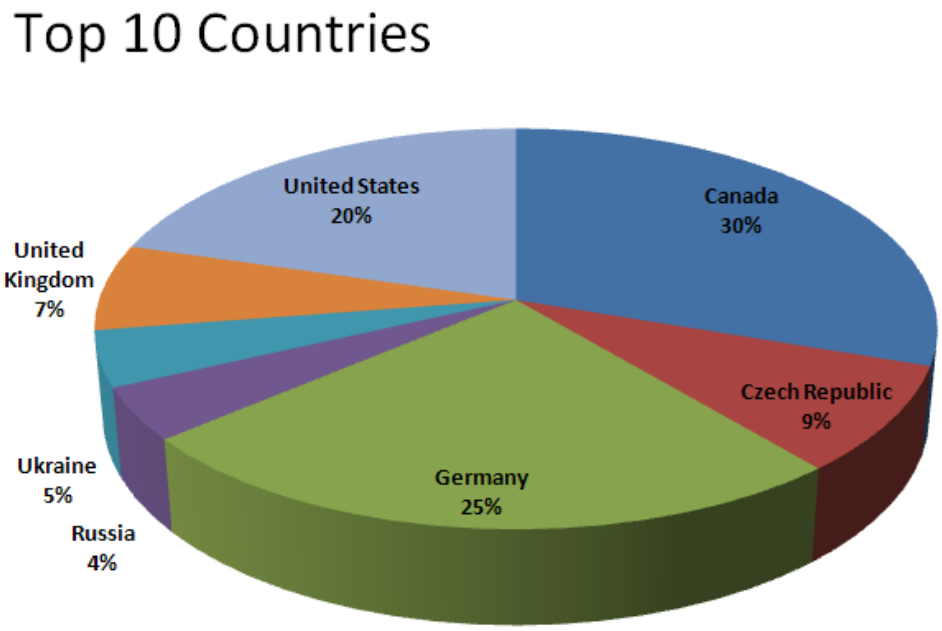
Estudiando las estadísticas de Alexa -de KlikVIP- del último trimestre, fuimos capaces de identificar el origen de los distribuidores:

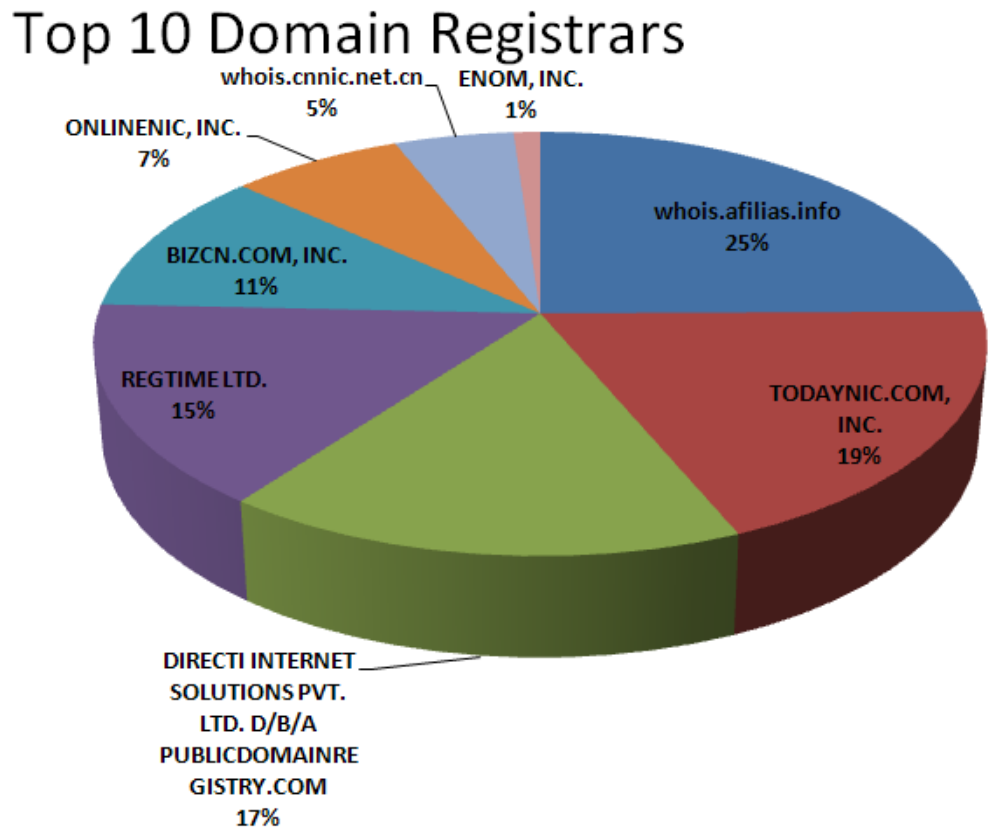
Estos distribuidores utilizan normalmente un sistema de pago-por-instalación. Los datos siguientes corresponden a la lista de precios de uno de uno de los sitios afiliados:

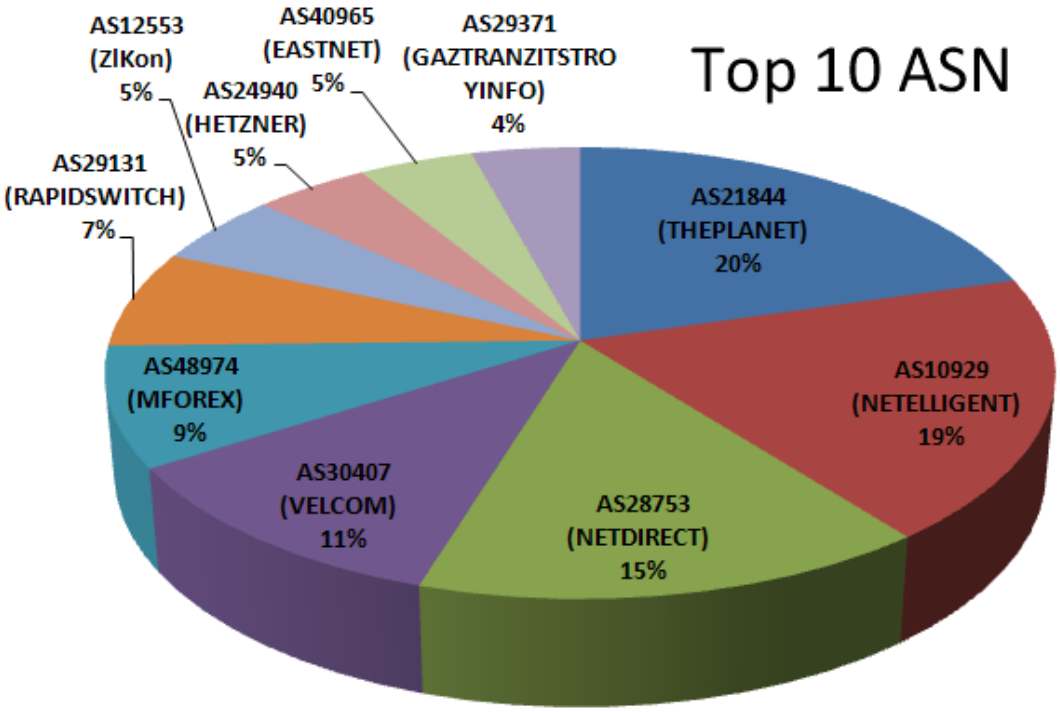
USA	$0.30
Canada & United Kingdom	$0.10
Western Europe	$0.03
Other countries	$0.02

¿De dónde proviene todo esto?

No cabe duda de que los mayores distribuidores de rogueware se encuentran en Europa del Este. No obstante, resulta interesante conocer también la localización de los dominios, los servidores y los países utilizados para realizar estos ataques:







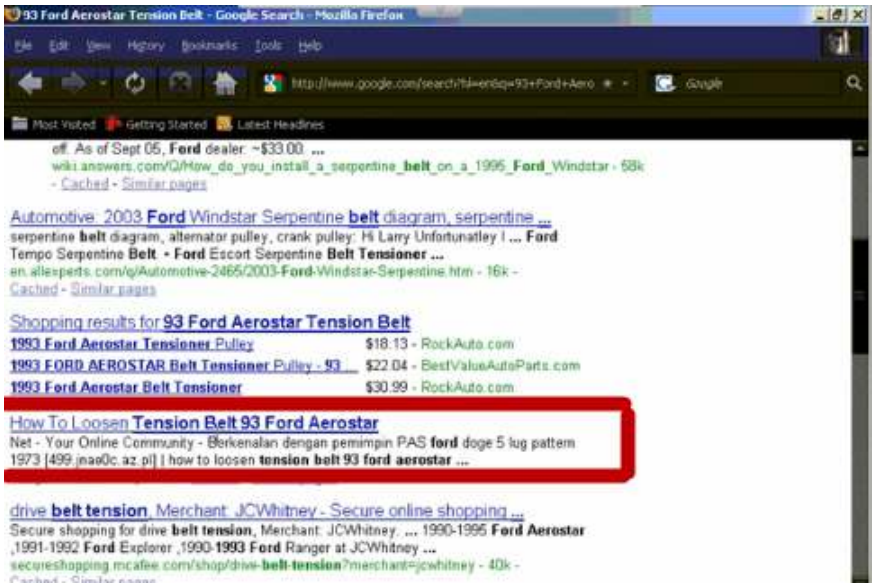
Distribución del rogueware

La naturaleza tan lucrativa del negocio del rogueware causó una avalancha de ataques a finales del año 2008 y durante el año 2009. Por primera vez, páginas de medios sociales como Facebook, MySpace, Twitter y Digg se convirtieron en objetivo de los distribuidores. Sin embargo, a pesar de este interés en los medios sociales, el mayor intento de distribución se realizó mediante técnicas de Blackhat SEO contra la empresa automovilística Ford en abril de 2009. Más de tres millones de términos de búsqueda fueron secuestrados, lo que motivó que los primeros resultados de prácticamente toda búsqueda que hicieran los usuarios sobre coches, repuestos o servicios de Ford llevasen a páginas de distribución de rogueware. Una vez Ford dio a conocer esta situación de forma pública, los criminales centraron sus objetivos en otras compañías como Nissan y Volkswagen.

Los 5 ataques más importantes a medios sociales

A continuación detallamos los cinco ataques más importantes de rogueware sobre medios sociales:

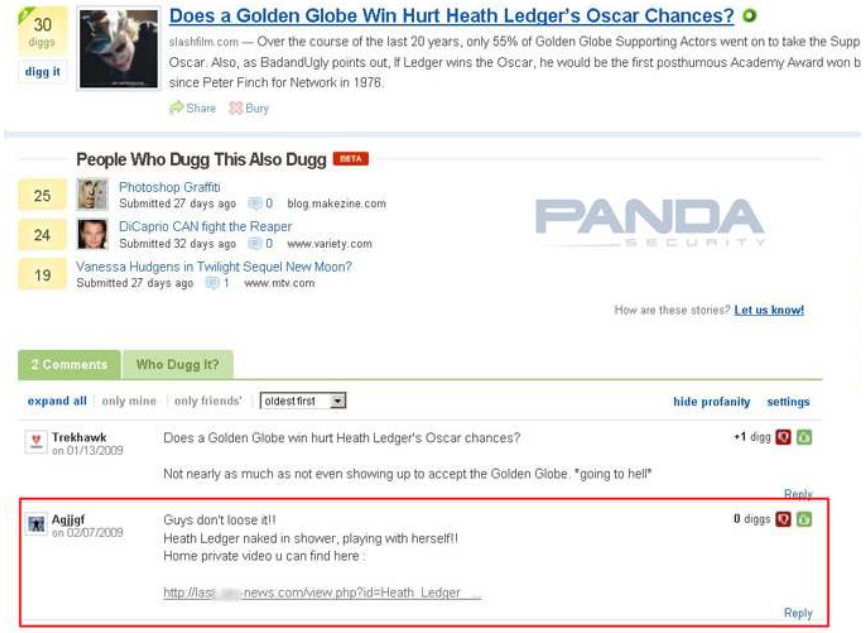
1. Ataque SEO contra la compañía de automóviles Ford



El ataque:

- 1.000.000 enlaces maliciosos indexados por Google
- 3.000.000 de términos de búsqueda legítimos secuestrados
- Las víctimas buscaban instrucciones (ej. Cómo aflojar un cinturón de seguridad)
- Se sirvieron 100 nuevos binarios de MSAntiSpyware2009 en 24 horas

2. Comentarios en Digg.com que dirigen a páginas de falsos antivirus



El ataque:

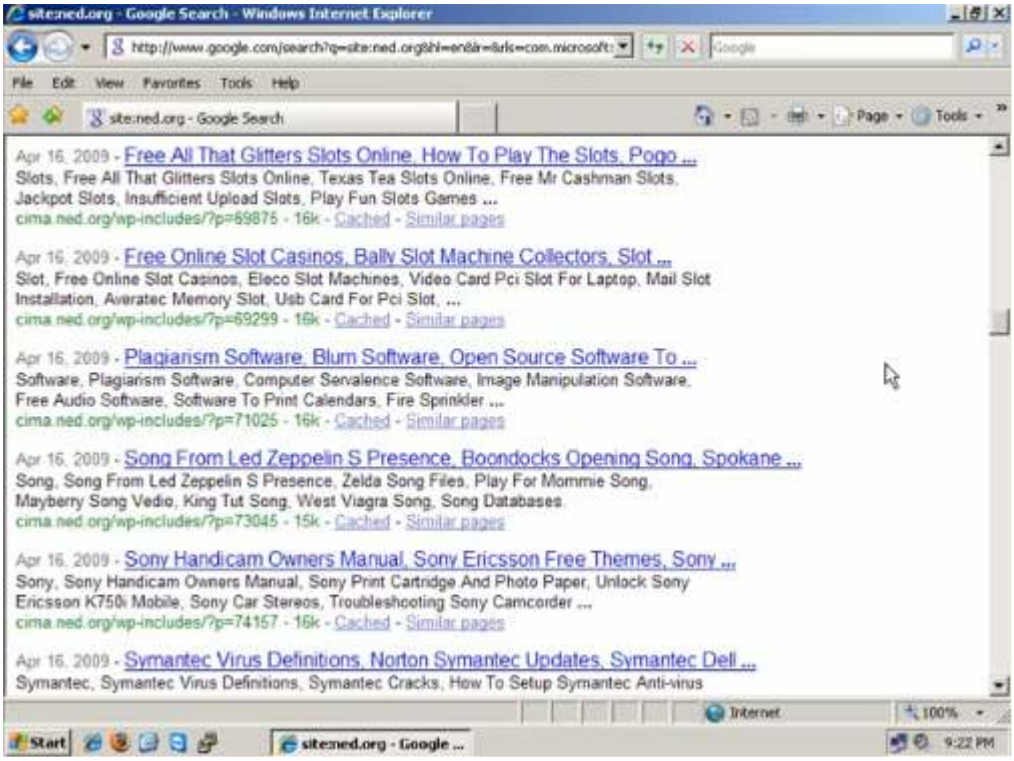
- Más de 500.000 comentarios que llevaban a paginas de falsos antivirus
- Los comentarios tenían como objetivo el título y contenido de las nuevas entradas

3. Las palabras más buscadas en Twitter llevan a páginas de falsos antivirus

El ataque:

- Los mensajes (tweets) tenían como objetivo las palabras más buscadas en Twitter.com
- 27.000 tweets cada 24 horas
- 60 ejemplares únicos detectados durante un periodo de 72 horas

4. Falsos antivirus que explotan la vulnerabilidad de Wordpress para facilitar los ataques de Blackhat SEO

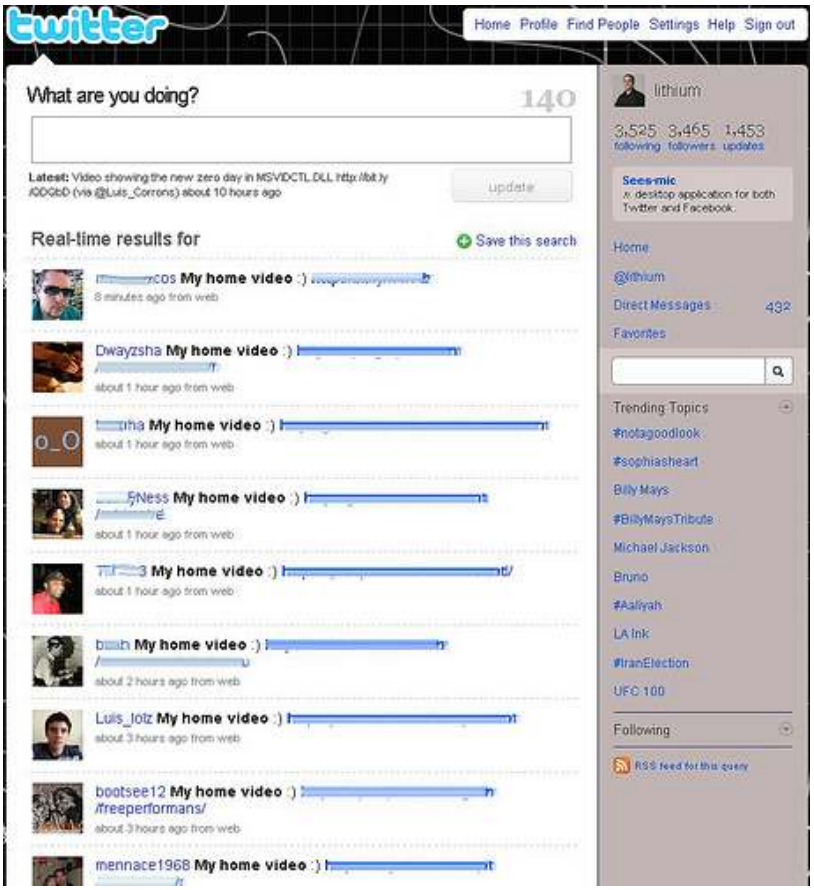


El ataque:

- Sitios afectados: Ned.org y TheWorkBuzz.com

- El objetivo era una vulnerabilidad de seguridad en una versión antigua de Wordpress
- Redirigía todos los enlaces a servidores de rogueware
- Facilitaba un ataque Blackhat SEO contra 13.000 términos de búsqueda

5. Koobface llega a Twitter



El ataque:

- Mensajes (tweets) redirigidos a 20 páginas de rogueware.
- El gusano se propagaba a través de Twitter tras la infección
- La página maliciosa mostraba un aviso emergente para una actualización de Flash que parecía real

Conclusión

Como hemos mostrado en este informe, la situación del rogueware es grave y empeora cada día, ya que los criminales siguen creando nuevos métodos para desarrollar y distribuir el malware. Se trata de un negocio altamente lucrativo para los delincuentes, por lo que se trata de infectar al mayor número de personas posible. Por este motivo, las redes sociales se han convertido en una forma muy efectiva de infectar a los usuarios, y, según PandaLabs, es probable que esta tendencia siga extendiéndose.

Los criminales saben cómo evitar que sus creaciones sean detectadas por los antivirus. La mayoría de ellas no muestra comportamientos sospechosos, por lo que las empresas antivirus tienen que centrarse en la detección por firmas (específicas o genéricas) para neutralizar dichos programas. Esta es la razón principal por la que los delincuentes están creando tantos ejemplares nuevos. Por otra parte, PandaLabs ha empezado a detectar variantes más avanzadas de malware que utilizan características de troyanos, además de rootkits y otras técnicas, para evitar las tecnologías de protección antivirus.

Durante muchos años tanto los consumidores como las empresas se han tenido que enfrentar a nuevas amenazas, desde virus y spam, hasta phishing. Para poder luchar contra el crimen informático seguirá siendo muy importante concienciar al público sobre las raíces del problema, buscar medios legales y fomentar la educación individual de los usuarios. Las empresas antivirus deben jugar un papel fundamental en esta labor, exponiendo el problema casi en tiempo real y presentando soluciones.

Por último, las empresas antivirus deben admitir que la industria de la seguridad informática se encuentra aún lejos de ganar esta batalla. Ésta es precisamente la razón por la que Panda comenzó a desarrollar las tecnologías basadas en la nube en el año 2006. La empresa necesitaba poder analizar de forma rápida cada nuevo ejemplar, y compararlo en tiempo real con la información de malware recopilada en sus 20 años de existencia, con el fin de proporcionar protección en minutos en lugar de en días. Afortunadamente, hoy día existen otras empresas antivirus que están siguiendo esta tendencia. No obstante, seguro que los delincuentes empiezan pronto a buscar nuevos canales para sacar rendimiento económico a sus creaciones de malware.

Autores

Sean-Paul Correll

Sean-Paul se incorporó a Panda Security en el año 2005 en el área de soporte técnico. Desde entonces ha ocupado varios puestos dentro de la organización, manteniéndose fiel a su verdadera pasión, la seguridad. Sean está especializado en la vigilancia de amenazas, con un énfasis especial en las amenazas emergentes. Es un miembro activo de la comunidad de la seguridad y frecuentemente se presta voluntario a dedicar su tiempo a ayudar a personas con infecciones de malware.

Luis Corrons

Luis lleva trabajando en Panda Security desde 1999. Empezó en el departamento de soporte técnico, ayudando a los usuarios domésticos y corporativos a resolver sus incidencias de virus. Un año más tarde se incorporó al equipo de soporte técnico internacional, ayudando a los departamentos de soporte técnico de las Organizaciones Nacionales en más 50 países. En el año 2002 fue nombrado director de PandaLabs y coordinador de las alertas de malware a nivel mundial, neutralizando gusanos como Klez, SQLSlammer, Sobig, Blaster, Sasser, Mydoom, etc. Durante este tiempo ha coordinado varios proyectos de automatización relacionados con el malware (p. ej. sistema automático de análisis y respuesta, y sistema automático de información sobre malware).

Su primer contacto con los ordenadores se produjo a la edad de 4 años (con un Sharp MZ-80K) con el que empezó a programar en lenguaje Basic. Entre sus mayores aficiones se encuentran disfrutar de la compañía de su mujer Nerea, su perro Robin y su trabajo, así como el ajedrez y los videojuegos.