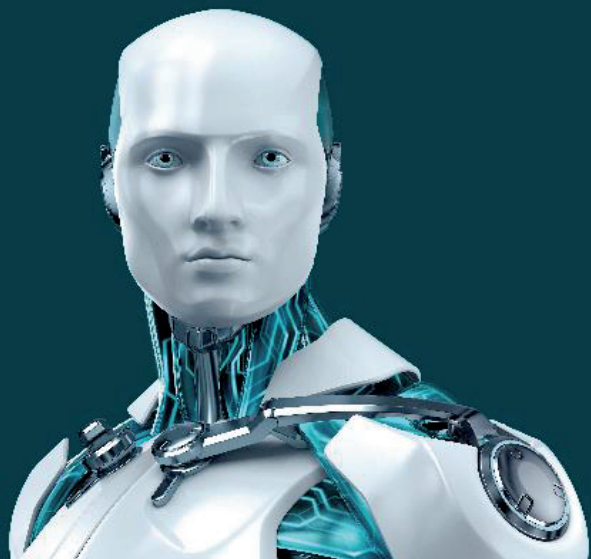
ENJOY SAFER TECHNOLOGY™

Operación Groundbait:

Análisis de un kit de herramientas para espionaje cibernético

Anton Cherepanov, ESET

Mayo 2016



Contenido

Resumen ejecutivo

La Operación Groundbait (en ruso: *Прикормка*, *Prikormka*) es una operación activa de espionaje cibernético dirigida a ciudadanos ucranianos. El grupo detrás de ella ha estado lanzando ataques dirigidos para espiar individuos específicos, posiblemente con motivos políticos.

Este paper presenta los descubrimientos de ESET con respecto a la Operación Groundbait basados en nuestra investigación de la familia de malware Prikormka. Ofrece un análisis técnico detallado de la familia de malware Prikormka y sus mecanismos de propagación, así como una descripción de las campañas de ataque más destacadas.

Descubrimientos principales:

- El país donde más se encontró este malware es Ucrania. Ha estado activo desde al menos el año 2008.
- Los objetivos principales de la Operación Groundbait son los separatistas que operan contra el gobierno, ubicados en las repúblicas populares autodeclaradas de Donetsk y Lugansk en el este de Ucrania.
- También hubo un gran número de otros objetivos ucranianos, entre los que se incluyen funcionarios públicos, políticos y periodistas, entre otros.
- Lo más probable es que los ataques se conduzcan desde Ucrania.

El descubrimiento

En el tercer trimestre de 2015, ESET identificó una familia de malware modular hasta entonces desconocida: Prikormka. La investigación subsiguiente reveló que este malware ha estado activo desde al menos el año 2008, y el país donde más se detectó es Ucrania. La razón por la que había pasado desapercibido durante tanto tiempo es el índice relativamente bajo de infección antes de 2015. Pero en ese año, la cantidad de infecciones aumentó significativamente.

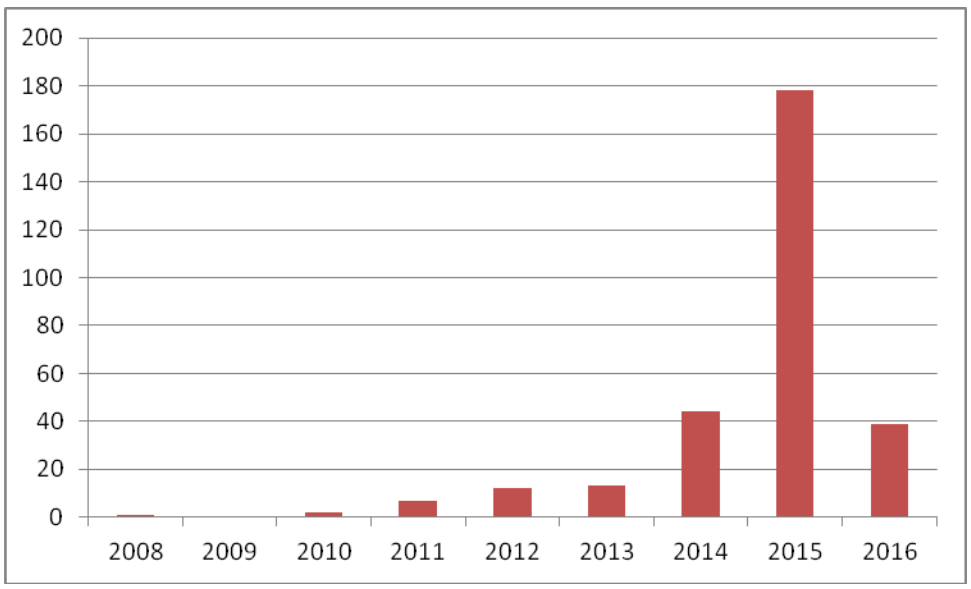


Imagen 1: Cantidad de muestras únicas recopiladas por ESET, por año, según sus marcas de fecha y hora.

La Imagen 1 muestra el número de muestras únicas de Prikormka compiladas cada año desde 2008, de acuerdo con las marcas de fecha y hora de su encabezado PE. Aunque las marcas de fecha y hora

por sí solas generalmente no son un indicador fiable, en este caso, el sistema telemétrico LiveGrid® de ESET confirmó que los datos eran precisos.

Uno de los primeros casos de este malware analizado en nuestro laboratorio llevaba el nombre `prikormka.exe`. La palabra rusa y ucraniana "prikormka" ("*Прикормка",* en inglés, "*groundbait"*), es un tipo de cebo o carnada de pesca que se arroja al agua para atraer a los peces. Elegimos usar este nombre durante nuestra investigación y luego decidimos mantenerlo, por lo que el malware lleva los nombres `Win32/Prikormka` y `Win64/Prikormka` respectivamente.

Su baja tasa de detección y su capacidad de pasar desapercibido durante años son características muy comunes de los ataques dirigidos (APT). La investigación de las campañas y la actividad de Prikormka han confirmado nuestra sospecha de que este malware se usa en ataques de este tipo.

Los ataques dirigidos en general tienen diversos fines, tales como operaciones de reconocimiento, el robo de propiedad intelectual, el sabotaje y el espionaje. Después de analizar las tácticas, técnicas y procedimientos empleados por este grupo de malware en particular, llegamos a la conclusión de que los objetivos de ataque son personas en lugar de empresas. Incluso cuando detectamos el malware Prikormka en un entorno corporativo, no vimos ninguna clase de movimiento lateral (una técnica muy utilizada por los adversarios avanzados en sus ataques cibernéticos).

Sospechamos que este grupo opera en Ucrania, país donde se encuentra la mayoría de sus víctimas. Por esa razón y debido a la naturaleza de los ataques, los clasificamos como operaciones de espionaje cibernético.

Las campañas

En esta sección mostraremos las campañas más importantes y prominentes, junto con sus documentos señuelo asociados.

En primer lugar examinaremos las estadísticas de detección por país según los datos de ESET LiveGrid®:

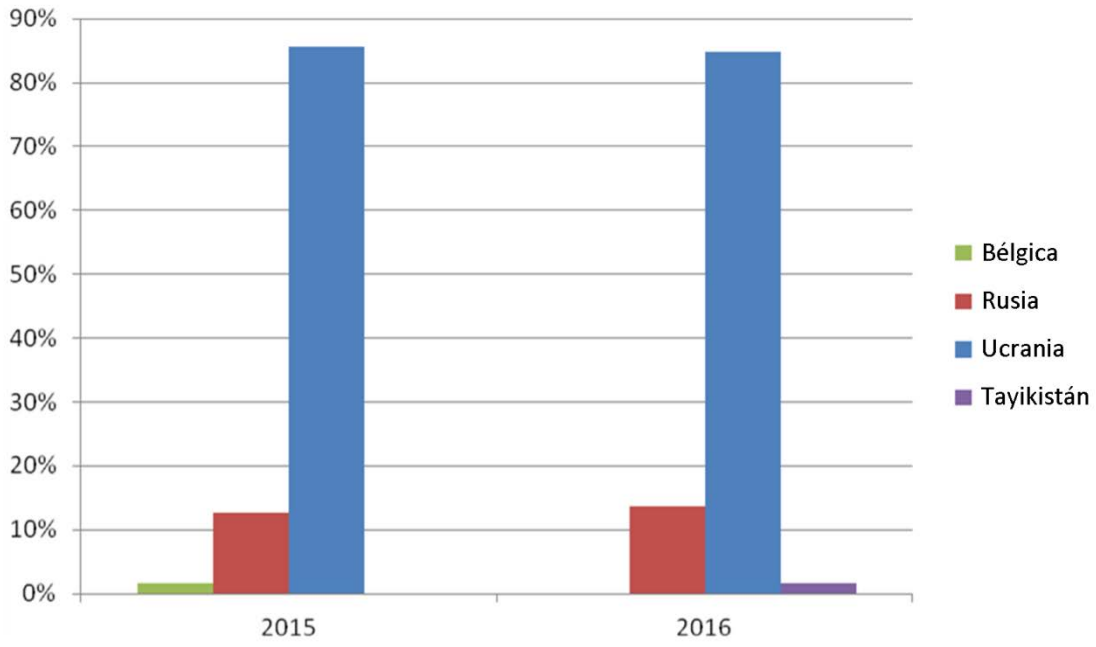


Imagen 2: Estadísticas de detección del malware Prikormka según ESET LiveGrid®.

De acuerdo con nuestros datos telemétricos, Ucrania es el país donde se detectó la mayor parte de infecciones. Nuestra investigación reveló también que los responsables del malware demuestran una fluidez nativa en el uso del ucraniano y el ruso, además de comprender plenamente la situación política actual en Ucrania.

Para responder la pregunta de qué tipo de víctimas fueron atacadas en los países mencionados, analizamos los documentos señuelo usados para engañarlas.

El vector de infección principal que identificamos durante nuestra investigación consiste en enviar correos electrónicos dirigidos de phishing con adjuntos maliciosos ejecutables, o con un enlace de descarga a un archivo malicioso alojado en un servidor remoto. Cuando el usuario hace clic en un adjunto malicioso que se hace pasar por un documento inofensivo, el dropper Prikormka muestra un documento señuelo con el fin de engañar a las víctimas y distraer su atención, ya que van a estar esperando que se abra un documento al hacer clic. Esta técnica funciona con usuarios que no conocen mucho sobre tecnología; sin embargo, el éxito de la infección depende más que nada de la calidad de los correos electrónicos dirigidos de phishing.

El atacante tiene una mayor probabilidad de infectar el sistema si el documento señuelo es relevante para la víctima: en otras palabras, cuando la víctima no se sorprende al recibir un mensaje de este tipo. Por lo tanto, el análisis de los documentos señuelo puede revelar información acerca de los objetivos deseados de estos ataques cibernéticos.

En segundo lugar, hay otro elemento presente en todas las muestras del malware Prikormka, al que llamamos ID de campaña. El ID de campaña es una cadena de texto única que sirve para identificar infecciones específicas o intentos de infección llevados a cabo por los operadores del malware Prikormka. Las combinaciones de letras y números utilizadas a veces revelan información sobre los objetivos de ataque.

Hasta el momento, identificamos más de 80 ID de campaña diferentes e incluso una cantidad mayor de documentos señuelo vinculados a estos ID. Se observó que por lo general un ID de campaña se usa contra un tipo de objetivo, que puede ser un individuo, una entidad o un grupo de personas. Esto significa que se puede encontrar un mismo ID en equipos diferentes.

También proporcionamos un listado completo de las campañas más representativas con su marca de fecha y hora de compilación, y el ID único de cada campaña en el Apéndice A.

Vale la pena mencionar que en algunos casos es difícil identificar cuáles son las víctimas objetivo, especialmente cuando las infecciones de Prikormka son descubiertas cuando el malware ya está instalado y activo. Sin embargo, notamos algunas infecciones de Prikormka activas en redes de equipos pertenecientes a objetivos de alto valor, incluyendo el gobierno ucraniano. En las siguientes descripciones de las campañas de Groundbait mencionamos otros de los objetivos más significativos.

Campañas contra separatistas

Entre los objetivos principales de Prikormka se encuentran los separatistas en el este de Ucrania. Desde 2014, esta región está sumida en un conflicto armado militar.

En abril de 2014, un grupo de personas proclamó unilateralmente la independencia de dos regiones de Ucrania oriental: Donetsk y Lugansk. En respuesta, el gobierno ucraniano clasificó estas dos entidades como organizaciones terroristas y, por lo tanto, el territorio de estas regiones se ha declarado Zona de operaciones antiterroristas (del inglés ATO). El 11 de mayo de 2014, las

autoridades de dichas repúblicas autoproclamadas llevaron a cabo un referéndum con el fin de legitimar el establecimiento de las repúblicas.

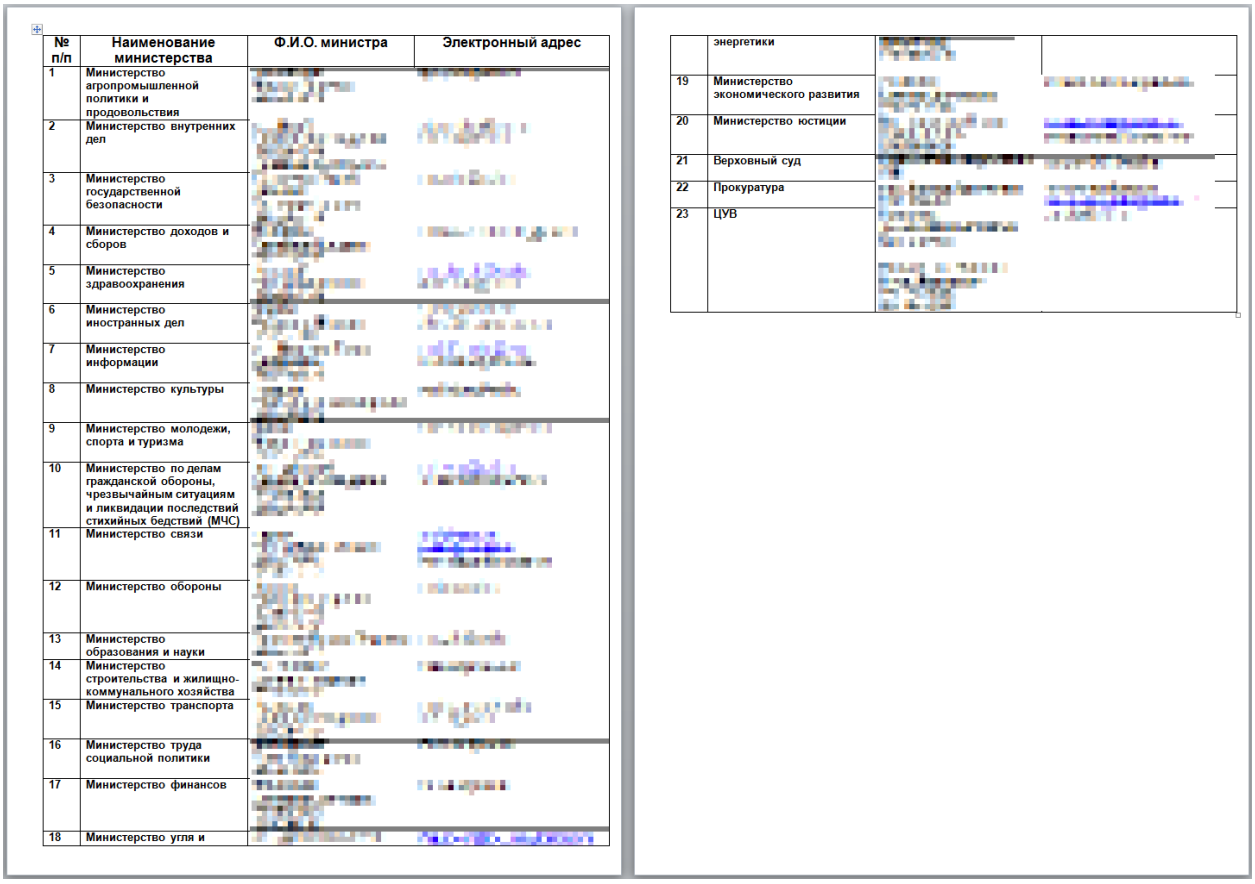
Un número significativo de los documentos señuelo utilizados en los ataques de Prikormka aprovecharon numerosos temas relacionados con los estados autoproclamados de la República Popular de Donetsk (DPR) y la República Popular de Lugansk (LPR). Por otra parte, una serie de documentos señuelo también contiene información privada, que incluye estadísticas y documentos aparentemente utilizados en el flujo de trabajo interno de dichos estados autoproclamados. Esto nos lleva a pensar que los operadores están apuntando intencionadamente a personas ubicadas en estas dos regiones. Nuestras sospechas quedan confirmadas por la telemetría de ESET LiveGrid®: Donetsk y Lugansk son las dos regiones ucranianas con más cantidad de infecciones del malware Prikormka.

Los atacantes utilizan tácticas de Ingeniería Social para convencer a la víctima de que abra el archivo adjunto malicioso. Éstas incluyen el uso de nombres provocativos o atractivos para los archivos adjuntos del correo electrónico. Algunos ejemplos son los siguientes:

- `Нацгвардейцы со шприцами сделали из донецкого мальчика мишень для ракет.exe` (del ruso: La guardia nacional ucraniana dirigió cohetes contra un niño de Donetsk). Fecha de la compilación: 5 de noviembre de 2014
- `Последнее обращение командира бригады 'Призрак' Мозгового Алексея Борисовича к солдатам и офицерам ДНР и ЛНР.scr` (del ruso: El líder de la brigada Prizrak Aleksey Borisovich Mozgovoy hace un último llamamiento a los soldados y al oficial de la DPR y la LPR). Fecha de la compilación: 24 de mayo de 2015
- `Места дислокации ВСУ в зоне проведения АТО.scr` (del ruso: Desarticulación de las fuerzas armadas de Ucrania en la zona ATO). Fecha de la compilación: 15 de diciembre de 2015

Los siguientes son ejemplos de documentos señuelo utilizados en ataques contra los separatistas en las regiones de Donetsk y Lugansk.

El primer ejemplo es un archivo ejecutable con el nombre `СПРАВОЧНИК по МИНИСТЕРСТВАМ обновленный.exe` (del ruso: Directorio de Ministerios - actualizado), cuyo documento señuelo es una lista de los Ministerios de la república autoproclamada. El ID de campaña para este archivo ejecutable es `D_xxx`.



№ п/п	Наименование министерства	Ф.И.О. министра	Электронный адрес
1	Министерство агропромышленной политики и продовольствия		
2	Министерство внутренних дел		
3	Министерство государственной безопасности		
4	Министерство доходов и сборов		
5	Министерство здравоохранения		
6	Министерство иностранных дел		
7	Министерство информации		
8	Министерство культуры		
9	Министерство молодежи, спорта и туризма		
10	Министерство по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (МЧС)		
11	Министерство связи		
12	Министерство обороны		
13	Министерство образования и науки		
14	Министерство строительства и жилищно-коммунального хозяйства		
15	Министерство транспорта		
16	Министерство труда социальной политики		
17	Министерство финансов		
18	Министерство угля и		

	энергетики		
19	Министерство экономического развития		
20	Министерство юстиции		
21	Верховный суд		
22	Прокуратура		
23	ЦУВ		

Imagen 3: Documento señuelo con la lista de Ministerios de la DPR. (En esta imagen y en las siguientes, ESET alteró los datos potencialmente confidenciales).

Este es otro ejemplo de un documento señuelo, dejado por un archivo ejecutable llamado `материалы к зачету по законодательству.exe` (del ruso: Materiales para el examen de leyes). Este ejecutable deja varios documentos, entre ellos la constitución temporal de la LPR así como otros documentos legales y políticos. El ID de campaña es `L_ment`; la palabra "ment" es policía en la jerga popular rusa. Por lo tanto, los atacantes demuestran tener un profundo conocimiento de esta lengua.

ЛУГАНСКАЯ НАРОДНАЯ РЕСПУБЛИКА

ЗАКОН

Об оперативно-розыскной деятельности

Настоящий Закон определяет содержание оперативно-розыскной деятельности, осуществляемой на территории Луганской Народной Республики, и закрепляет систему гарантий законности при проведении оперативно-розыскных мероприятий.

Глава I. Общие положения

Статья 1. Оперативно-розыскная деятельность

Оперативно-розыскная деятельность - вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим Законом (далее - органы, осуществляющие оперативно-розыскную деятельность), в пределах их полномочий посредством проведения оперативно-розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств.

Статья 2. Задачи оперативно-розыскной деятельности

Задачами оперативно-розыскной деятельности являются:

Imagen 4: Documento señuelo con la Ley, que describe las reglas para actividades especiales de investigación del crimen.

Algunos de los documentos señuelo usan como tema el Acuerdo de Minsk. Éste es un ejemplo de uno de estos documentos, que proviene de un dropper con el nombre `Схема демилитаризованной зоны в районе Шиокино.exe` (del ruso: Esquema de la zona desmilitarizada en Shyrokyne, aunque Shyrokyne está escrito con un error tipográfico en ruso). El ID de campaña es `Lminfin`.

ДОНЕЦКАЯ НАРОДНАЯ РЕСПУБЛИКА

Рабочая группа по реализации
Комплекса мер по выполнению
Минских соглашений

DONETSK PEOPLE'S REPUBLIC

Working Grouponthe
implementation of set of measures
on the execution of Minsk Agreements

Исх. [illegible] от 04 июля 2015 г

[illegible]

копия:

[illegible]

Направляю в Ваш адрес схему демилитаризованной зоны в районе н.п. Широкино и отвода вооруженных формирований Донецкой Народной Республики в одностороннем порядке.

Полномочный представитель
Донецкой Народной Республики
на переговорах Контактной
группы в Минске

Д.В. Пушилин

ПОЛНОМОЧНЫЙ ПРЕДСТАВИТЕЛЬ ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ НА ПЕРЕГОВОРАХ КОНТАКТНОЙ ГРУППЫ В МИНСКЕ

Imagen 5: Documento señuelo que utiliza el tema del Acuerdo de Minsk.

Otro de los documentos señuelo también incluye un mapa de la zona de seguridad establecida por el Protocolo de Minsk. El siguiente es un ejemplo proveniente de un dropper cuyo nombre de archivo es `Отвод с 4 участками по сост на 14.08.exe` (del ruso: Retirada [de armamento pesado] el 14/08). El ID de campaña es BUR.

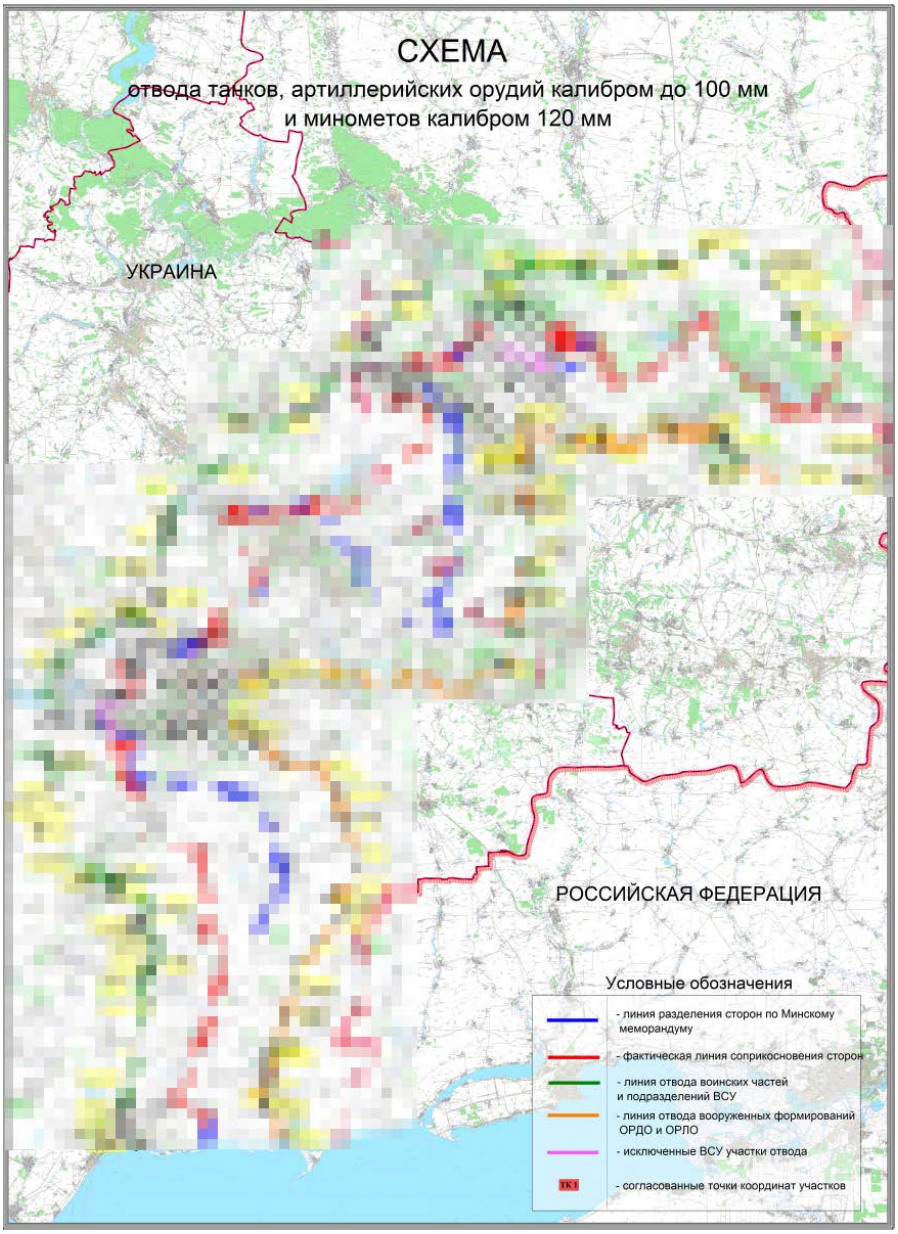


Imagen 6: Documento señuelo con mapa de la zona de seguridad.

Nota importante: la mayor parte de los archivos binarios Prikormka que parecen haber sido destinados a atacar a los separatistas tienen un ID de campaña que comienzan con la letra D o L. Es posible que signifiquen la República Popular de Donetsk y la República Popular de Lugansk respectivamente. También observamos un archivo ejecutable llamado `Заявление Эдуарда Басаргина 13 октября 2015 года в 15 часов.exe` (del ruso: Declaración de Eduard Basargin el 13 de octubre de 2015 a las 3 pm), cuyo ID de campaña es `RF_lgm`. Como las detecciones identificadas tuvieron lugar en Rusia, el prefijo RF podría referirse a la Federación Rusa.

Campaña contra el partido político nacionalista ucraniano

Todos los documentos señuelo mencionados anteriormente fueron extraídos de archivos ejecutables cuyos nombres estaban en ruso. Aunque el ucraniano es el idioma oficial del estado, los pueblos del este de Ucrania tienden a utilizar el ruso, a diferencia de las regiones occidentales de Ucrania, donde se utiliza el ucraniano.

Algunos de los archivos binarios de Prikormka tienen nombres en ucraniano. Por ejemplo, encontramos el nombre de archivo `План ДНР на 21 липня, щодо відводу військ.exe` (del ucraniano: El plan de la DPR para retirar las tropas el 21 de julio). El hecho de que los nombres de los archivos adjuntos estén en idioma ucraniano sugiere que el receptor deseado de estos mensajes fraudulentos prefiere usar este idioma por sobre el ruso. Esta hipótesis parecería correcta, ya que el malware Prikormka fue detectado en las regiones occidentales de Ucrania.

El ID de campaña de este archivo ejecutable en particular es `Psek`, lo que nos hace suponer con alto grado de certeza que los miembros del partido nacionalista ucraniano Sector de Derecha (en ucraniano: Pravyi Sektor) fueron los objetivos del malware Prikormka.

ДОНЕЦКАЯ НАРОДНАЯ РЕСПУБЛИКА
Рабочая группа по реализации Комплекса мер по выполнению Минских соглашений

DONETSK PEOPLE'S REPUBLIC
Working Grouponthe implementation of set of measures on the execution of Minsk Agreements

Исх. от 20 июля 2015 г

Представителям СММ ОБСЕ в Донецкой Народной Республике

Сообщаем Вам, что руководством ДНР принято решение об одностороннем отводе вооружений калибром менее 100 мм и танков от линии соприкосновения сторон в соответствии с Минскими договоренностями.

21 июля 2015 г. В 11.00 (по мск) под контролем СММ ОБСЕ планируется отвести восемь единиц техники:

№ п/п	наименование вооружения	бортовой номер	номер корпуса/КПП (башня)
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

Полномочный представитель Донецкой Народной Республики на переговорах Контактной группы в Минске

Д.В. Пушилин

Imagen 7: Documento señuelo posiblemente utilizado contra los miembros del partido nacionalista ucraniano.

Otras campañas

Los objetivos de la Operación Groundbait no fueron únicamente los separatistas en Donetsk y Lugansk y las víctimas de alto perfil. Hemos encontrado otras campañas con documentos señuelo interesantes, pero no podemos identificar a las víctimas previstas basándonos únicamente en esos documentos.

El siguiente es un ejemplo de un documento señuelo que posiblemente fue utilizado contra una institución religiosa. Proviene del dropper con nombre de archivo `Новое слово жизни.exe` (del

ruso: Nuevo mundo de vida). El ID de campaña es `medium` y la elección de este nombre podría referirse a médiums y espiritismo.

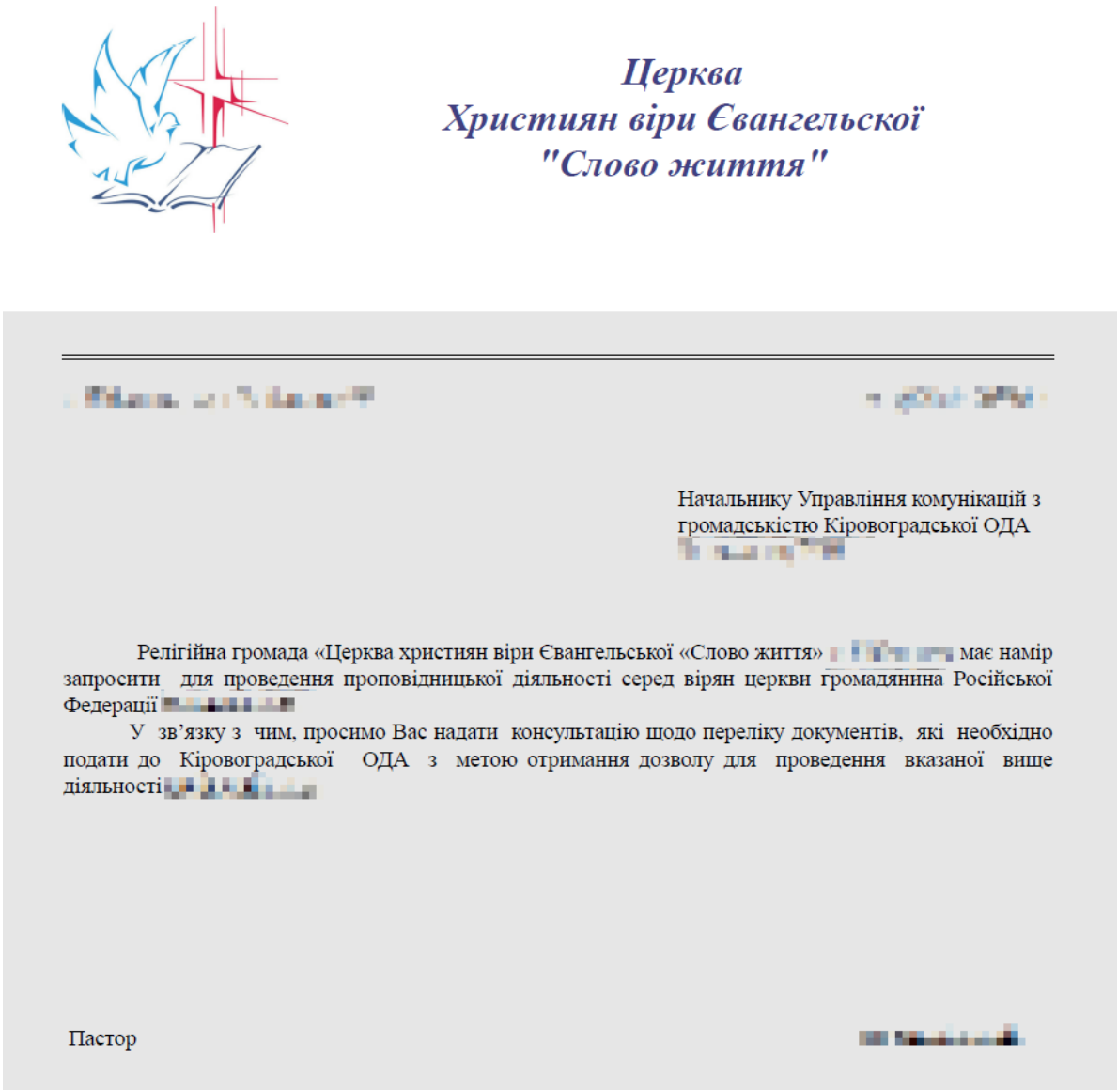


Imagen 8: Documento señuelo posiblemente utilizado contra organizaciones religiosas.

En marzo de 2016 se descubrió otra campaña religiosa. En esta ocasión, el nombre del archivo malicioso estaba en húngaro: `fizikai munka 2.pdf.scr`, que significa "CV para trabajo físico". El documento señuelo colocado por este archivo es el CV (currículum vitae) de una persona, escrito en húngaro.

El archivo malicioso `.SCR` se enviaba comprimido en un solo archivo junto con otros dos documentos: el CV de la misma persona en ucraniano y un certificado en húngaro que confirma que dicha persona está capacitada para realizar el trabajo físico. Si solo nos basamos en esta información, es difícil decir quién podría ser el objetivo deseado, pero el hecho de que el receptor posiblemente sepa húngaro y ucraniano hace que sea interesante mencionar esta campaña. Su ID es `F_ego`.

Szám: Som/2013/1/23

TANÚSÍTVÁNY

[redacted]

[redacted] - Kabinet mint vizsgaszervező előtt az egyes rendészeti feladatokat ellátó személyek tevékenységéről, valamint egyes törvényeknek az iskolakerülés elleni fellépést biztosító módosításáról szóló 2012. évi CXX. törvény 23. §-ában meghatározottak alapján a személy- és vagyonőrök képzését követően

megfelelt minősítéssel

VIZSGÁT

tett.

Kelt: Kaposvár (7400), Somssich P. u. 15., MÁV Kollégium, 2013. év 06. hó 10. nap

P.H.

Személy- vagyonvédelmi és Magánnyomozói Szakmai Kamara Somogy Megyei Szervezete

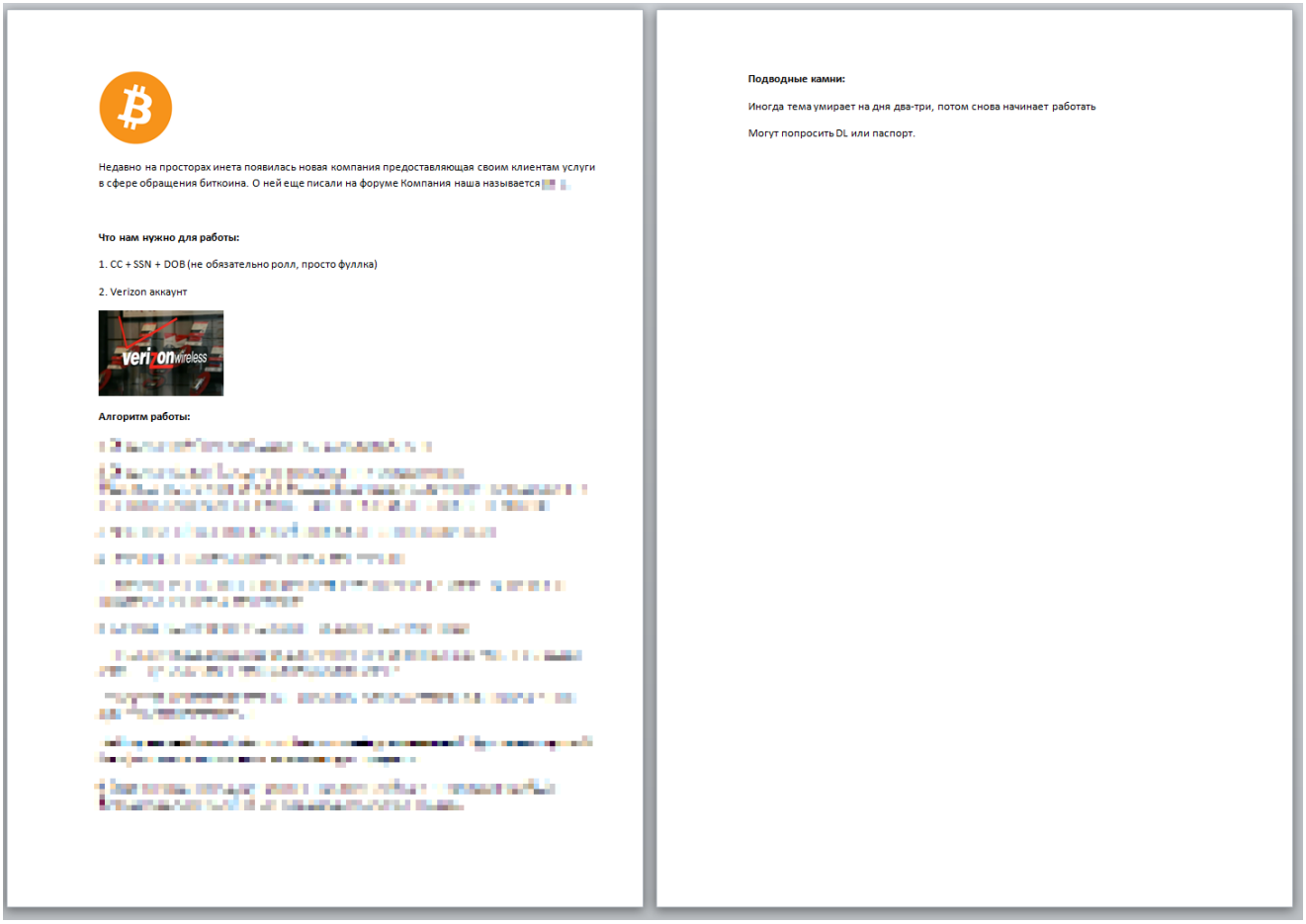
vizsgaszervező vezetője

vizsgabizottság elnöke

13

Imagen 9: El documento en húngaro se enviaba a la víctima en un único archivo comprimido con el malware Prikormka.

El siguiente es un ejemplo de un documento señuelo, colocado por un archivo con nombre `bitcoin.exe`. El ID de campaña en este caso es `hmod`.



Недавно на просторах инета появилась новая компания предоставляющая своим клиентам услуги в сфере обращения биткоина. О ней еще писали на форуме Компания наша называется

Что нам нужно для работы:

1. CC + SSN + DOB (не обязательно ролл, просто фуллка)

2. Verizon аккаунт

Алгоритм работы:

Подводные камни:

Иногда тема умирает на дня два-три, потом снова начинает работать

Могут попросить DL или паспорт.

Imagen 10: Documento señuelo que explica cómo cometer un fraude de tarjeta de crédito.

El texto en ruso explica detalladamente los pasos a seguir para comprar bitcoins usando tarjetas de crédito robadas. El documento está repleto de palabras en la jerga popular, utilizadas frecuentemente por los *carders* rusoparlantes. [1]

Otro ejemplo es un documento señuelo misterioso extraído de un dropper cuyo nombre es `prikormka.exe`. El ID de campaña es `30K_alfa`.

[1] Ciberdelincuentes que se dedican a usar tarjetas de crédito robadas.

Официальный представитель "FIN" в Украине

Прикормка содержит натуральный БЕТАИН!!!

Наименование		ВЕС	В пачке			Цена ОПТ без НДС			
						От 1000 уе	от 300 уе	От пачки	Розница
Прикормка FIN «Лещ»		0,7 кг	15	Цвет: Натуральный	без НДС	0,75 $	0,85 $	0,95 $	1,5 $
				Цвет: Натуральный + мотыль		0,78 $	0,88 $	1 $	1,6 $
ЛЕТНЯЯ				Цвет: Крашенная		0,8 $	0,9 $	1 $	1,6 $
				Цвет: Крашенная + мотыль		0,85 $	0,95 $	1 $	1,6 $
Прикормка FIN "ФИДЕР"		0,7 кг	15	Цвет: Натуральный	без НДС	0,75 $	0,85 $	0,95 $	1,5 $
				Цвет: Натуральный + мотыль		0,78 $	0,88 $	1 $	1,6 $
ЛЕТНЯЯ				Цвет: Крашенная		0,8 $	0,9 $	1 $	1,6 $
				Цвет: Крашенная + мотыль		0,85 $	0,95 $	1 $	1,6 $
Прикормка FIN «Универсальная»		0,7 кг	15	Цвет: Натуральный	без НДС	0,75 $	0,85 $	0,95 $	1,5 $
				Цвет: Натуральный + мотыль		0,78 $	0,88 $	1 $	1,6 $
ЛЕТНЯЯ				Цвет: Крашенная		0,8 $	0,9 $	1 $	1,6 $
				Цвет: Крашенная + мотыль		0,85 $	0,95 $	1 $	1,6 $
Прикормка FIN «Карп Карась Линь»		0,7 кг	15	Цвет: Натуральный	без НДС	0,75 $	0,85 $	0,95 $	1,5 $
				Цвет: Натуральный + мотыль		0,78 $	0,88 $	1 $	1,6 $
ЛЕТНЯЯ				Цвет: Крашенная		0,8 $	0,9 $	1 $	1,6 $
				Цвет: Крашенная + мотыль		0,85 $	0,95 $	1 $	1,6 $

Imagen 11: Documento señuelo misterioso colocado por el archivo `prikormka.exe`.

Este documento señuelo contiene una lista de precios de una tienda ucraniana que vende diversos tipos de cebo de pesca.

Detalles técnicos

En esta sección se describen los aspectos técnicos del malware Prikormka, incluyendo la arquitectura del software malicioso, la comunicación con los servidores de C&C y el análisis detallado de los módulos utilizados.

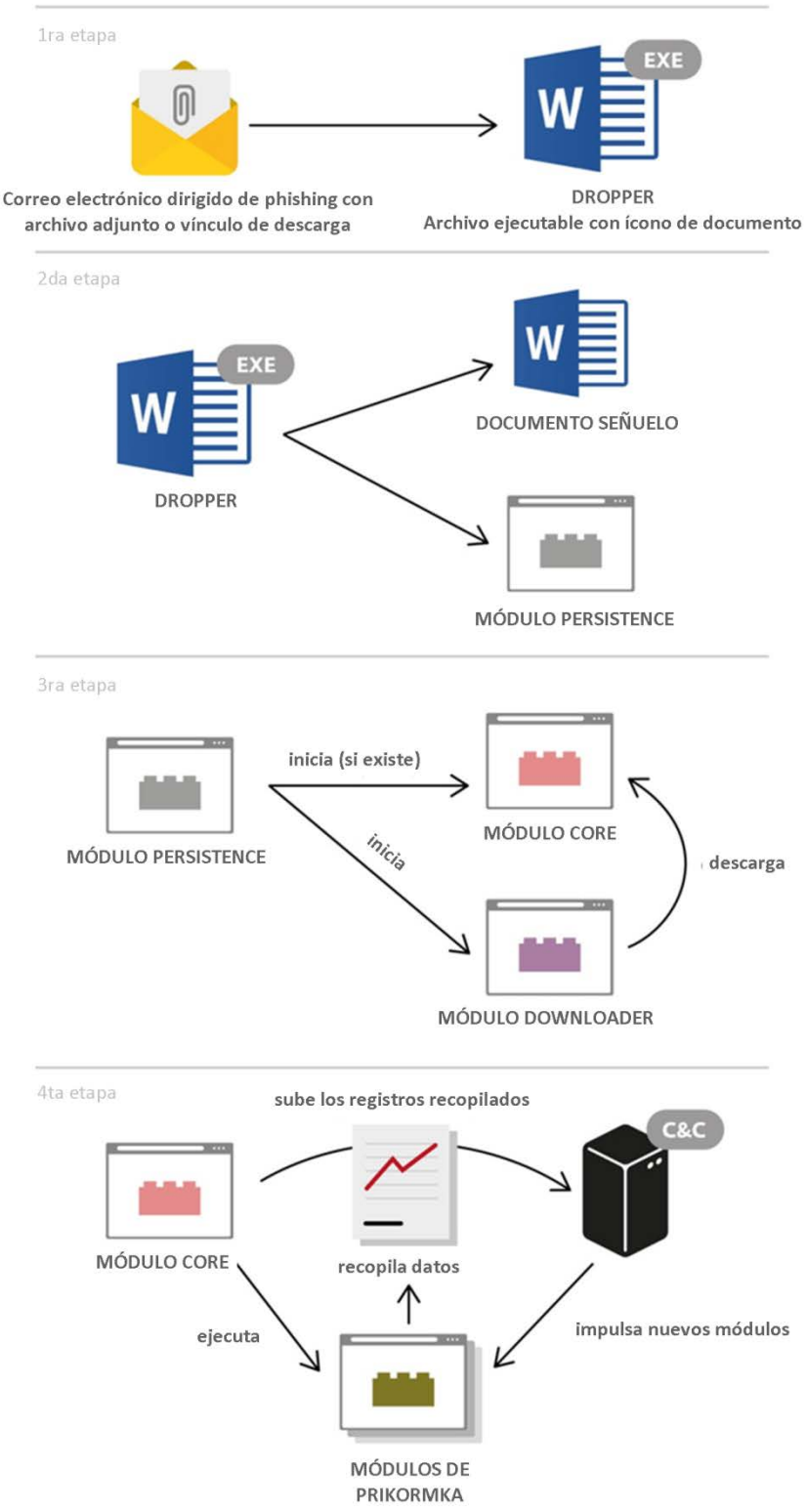


Imagen 12: Esquema simplificado de la arquitectura del malware Prikormka.

El dropper

El componente inicial de este malware es un archivo dropper, que normalmente se envía como adjunto en un correo electrónico. Por lo general, tiene la extensión .SCR o .EXE y se entrega en un archivo comprimido. Con el fin de engañar a la víctima, el dropper Prikormka se hace pasar por diversos tipos de documentos o archivos comprimidos de autoextracción.

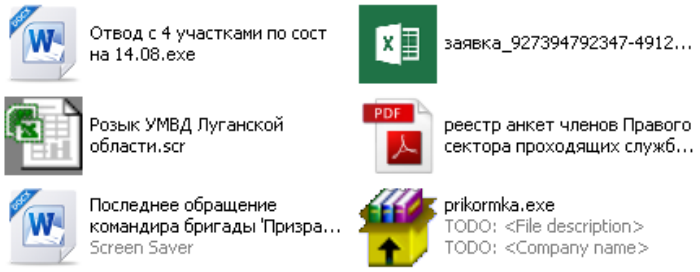


Imagen 13: Íconos utilizados por el malware Prikormka.

Cuando se ejecuta, infecta el equipo y al mismo tiempo muestra uno o más documentos señuelo. Para ello, el malware abre una ventana de WinRAR para abrir archivos comprimidos de autoextracción (SFX). En algunos casos, crea un archivo SFX ejecutable legítimo no malicioso en el disco y luego lo inicia. Curiosamente, ese archivo comprimido SFX siempre incluye una interfaz gráfica del usuario localizada en idioma ruso, incluso en los casos en que el nombre de archivo dropper está en ucraniano. En cambio, el dropper cuyo nombre de archivo está en húngaro no muestra esta ventana.

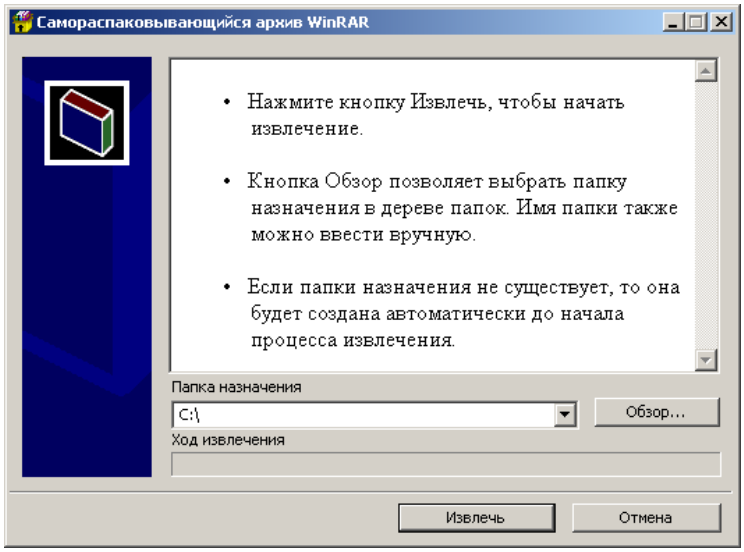


Imagen 14: Interfaz rusa del archivo comprimido SFX.

El archivo SFX ejecutable contiene uno o más documentos señuelo. Por ejemplo, un archivo SFX colocado por Prikormka contenía 24 documentos. Por supuesto, el número y el tamaño de los documentos señuelo afecta el tamaño de los droppers. El tamaño de archivo del dropper más grande identificado fue de 25 MB.

La mayoría de los dropper ejecutables tienen un archivo integrado a la aplicación, donde se especifica que requiere privilegios de administrador para ejecutarse en el sistema. Si el usuario no tiene privilegios de administrador, el sistema le pedirá las credenciales.

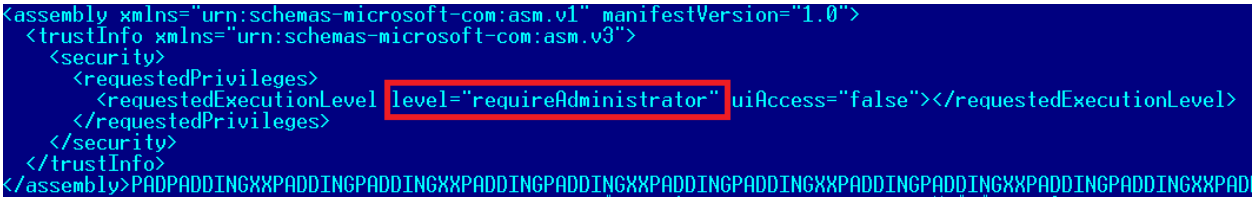


Imagen 15: Documento integrado en el dropper Prikormka.

El dropper necesita privilegios de administrador debido a la técnica utilizada por el malware para lograr ser persistente en el sistema infectado. En concreto, el malware secuestra la orden de carga del archivo DLL para que se inicie automáticamente en cada arranque del sistema. El dropper guarda uno de los módulos DLL de Prikormka en el directorio de Windows bajo el nombre `ntshrui.dll`.

Como este archivo DLL se almacena en el directorio de Windows, el proceso `explorer.exe` lo cargará con cada arranque del sistema en lugar del archivo legítimo `ntshrui.dll`, que se almacena en el subdirectorio `C:\Windows\System32`. De este modo, el módulo Prikormka secuestra la orden de carga de los archivos DLL. Este método de persistencia no es nuevo; la comunidad antimalware ya lo ha analizado públicamente varias veces.

También hay otra técnica interesante utilizada por el malware Prikormka, más específicamente, por sus archivos dropper con extensión `.SCR`. La extensión de archivo `.SCR` significa protector de pantalla y representa un archivo ejecutable de Windows estándar. La diferencia principal entre un archivo `.EXE` y uno `.SCR` es que el protector de pantalla se ejecuta con argumentos especiales de línea de comandos.

Por lo general, los ciberdelincuentes simplemente reemplazan el nombre de un archivo ejecutable por la extensión `.SCR` para evadir varias medidas de seguridad que se basan en las extensiones de los archivos. Los autores de Prikormka implementaron una verificación de tales argumentos de línea de comandos, por lo que, cuando el binario se ejecuta como un ejecutable estándar (sin los argumentos necesarios), no infecta el sistema. En consecuencia, esta sencilla verificación permite que el malware logre eludir algunas técnicas de detección en modo sandbox utilizadas para procesar muestras automáticamente.

En el caso de que la infección comience con un archivo `.SCR`, el troyano emplea métodos estándar para cargar su DLL mediante `rundll32.exe` y mantiene su persistencia en el sistema mediante la configuración de una entrada con el nombre `guidVGA` o `guidVSA` en la clave de registro Run:

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

Para que tanto las versiones de Windows Explorer de 32 bits como la de 64 bits puedan cargar el malware, éste contiene archivos binarios para ambas plataformas. La mayoría de los módulos están escritos en el lenguaje de programación C y compilados con Microsoft Visual Studio.

El dropper almacena módulos en sus recursos; algunos de estos recursos se cifran con una operación XOR simple.

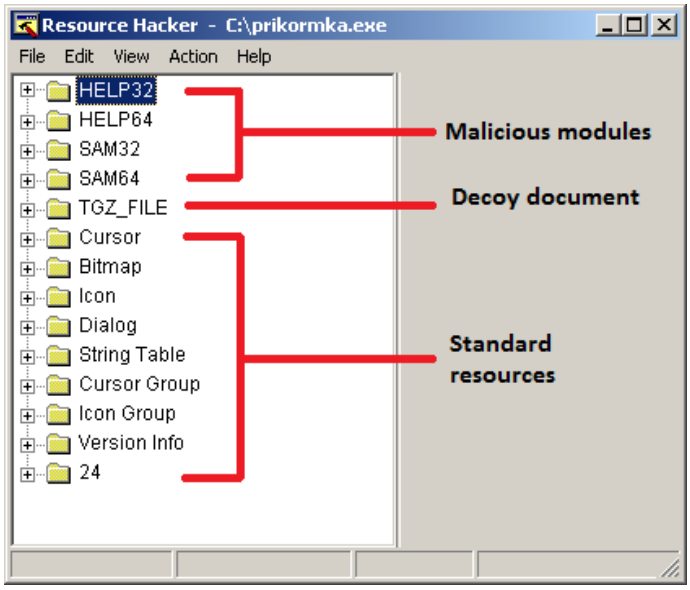


Imagen 16: Recursos ubicados dentro del dropper binario Prikormka.

El dropper es responsable de la creación del archivo `rbcon.ini`, utilizado por el malware para almacenar el ID de campaña y otros valores.

Las versiones anteriores de Prikormka utilizan una técnica diferente: el ID de la campaña estaba incorporado en el archivo binario de uno de los módulos:

Imagen 17: ID de la campaña con el valor `hmyr32` incorporado en el archivo binario.

El valor del ID de campaña se codificó en forma rígida dentro del binario Prikormka en el momento de su compilación; por otra parte, el ID de campaña en la versión de 32 bits de los binarios termina con 2, mientras que el ID en la versión de 64 bits de los binarios termina con 4.

Esta técnica probablemente resulta eficaz para un pequeño número de víctimas, pero es de suponer que crea problemas para los atacantes cuando la cantidad de víctimas comienza a aumentar. Quizá la tarea de volver a compilar y empaquetar las partes principales del conjunto de herramientas para cada nueva víctima empezó a consumir demasiado tiempo, por lo que, hacia mediados de 2015, los atacantes cambiaron su esquema. A partir de junio de 2015, el ID de campaña se comenzó a almacenar en un archivo aparte llamado `rbcon.ini`, que los atacantes denominan `objectset`. Los autores del malware también incorporaron un nuevo valor llamado `roboconid`, que representa el ID del operador.

Nuestra investigación nos permitió confirmar que este ID es un número único para el operador de software malicioso, que realiza operaciones cibernéticas y tiene la tarea asignada de infectar, espiar y seguir un objetivo en particular.

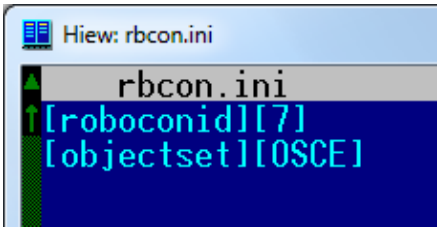


Imagen 18: El archivo `rbcon.ini` contiene tanto el ID de campaña como el ID del operador.

Algunos de los binarios del dropper incluyen una ruta a un archivo PDB, que puede revelar la estructura de directorios utilizado por los atacantes.

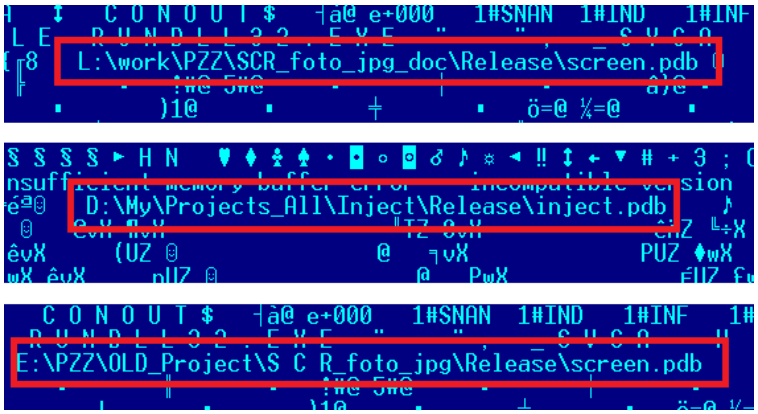


Imagen 19: Algunas de las rutas a archivos PDB descubiertas dentro del malware Prikormka.

Los escritores de malware llaman internamente a este troyano PZZ; contamos con más evidencia que apoya esta teoría.

La familia de Prikormka es un troyano típico de espionaje cibernético con una arquitectura modular. La funcionalidad del troyano les permite a los atacantes robar información confidencial de la computadoras infectadas y subirla a servidores de comando y control (C&C).

Módulos de Prikormka

Los módulos Prikormka se almacenan en el disco del sistema infectado en forma de archivos DLL. Hay módulos para diversos fines, tales como la comunicación con los servidores de C&C, propósitos auxiliares (por ejemplo, la persistencia en el sistema), y la extracción de diferentes tipos de información confidencial desde el equipo infectado. Como ya mencionamos, los módulos de Prikormka están compilados tanto para plataformas Windows de 32 como de 64 bits.

Hay un conjunto estándar de módulos descargables con nombres predefinidos, que se describirán en detalle en las siguientes secciones de este documento. Para poder ejecutarse, el módulo (archivo DLL) debe almacenarse en el disco con un nombre de archivo específico y debe tener una de las siguientes funciones de exportación: `Starting`, `KickInPoint`, `Cycle`. No obstante, los atacantes son capaces de impulsar el envío de cualquier módulo personalizado a una víctima en particular. En concreto, observamos que los módulos personalizados generalmente llevan el nombre `mp.dll`.

Debe tenerse en cuenta que los operadores de malware son los responsables de decidir qué módulos impulsarán a la computadora infectada.

Prikormka a veces almacena módulos con funcionalidades diferentes bajo un mismo nombre o, por el contrario, también puede almacenar módulos con funcionalidades similares bajo nombres

distintos. Algunas versiones del malware almacenan los módulos con un nombre de archivo que solo incluye la fecha y la hora actuales. Por eso, en este documento nos referimos a los complementos (plugins) por su código.

Código del módulo	Nombre interno del módulo	Nombre del archivo	Propósito
PERSISTENCE	samlib.dll	samlib.dll, ntshrui.dll	Usado para ser persistente en el sistema
DOWNLOADER	helpldr.dll	helpldr.dll, _wshdmi.dll	Descarga el módulo CORE
CORE	hauthuid.dll	hauthuid.dll, _svga.dll, _wshdmi.dll	Carga todos los demás módulos, se comunica con los servidores de C&C, carga registros
DOCS_STEALER	iomus.dll	iomus.dll	Recopila documentos
KEYLOGGER	kl.dll, hlpuctf.dll	hlpuctf.dll	Registra las pulsaciones de teclado
SCREENSHOTS	scrsh.dll	scrsh.dll	Extrae capturas de pantalla del escritorio
MICROPHONE	snm.dll	snm.dll	Captura audio con el micrófono
SKYPE	swma.dll	swma.dll	Graba las llamadas de audio realizadas por Skype
LOGS_ENCRYPTER	atiml.dll	atiml.dll	Comprime y cifra los registros recopilados
GEOLOCATION	geo.exe	Inv.exe	Determina la ubicación geográfica del equipo infectado
OS_INFO	InfoOS	mp.dll	Recopila información sobre el equipo infectado
PASSWORDS	Brother	mp.dll	Recopila las contraseñas guardadas en el equipo para diversas aplicaciones instaladas
FILE_TREE	mpTREE	mp.dll	Recopila el árbol de archivos del disco rígido del equipo infectado

Tabla 1: Lista de módulos de Prikormka identificados durante nuestra investigación.

La siguiente lista contiene los nombres de archivo de los módulos a los que se hace referencia en el código del malware, pero que no hemos encontrado durante nuestra investigación, y por lo tanto no fue posible evaluar su funcionalidad:

- `miron.dll`
- `meta.dll`
- `hmuid.dll`
- `sh.exe`
- `mupdate.exe`

Es importante tener en cuenta que los componentes de Prikormka creados en la primera etapa del malware (entre 2008 y 2010) utilizaban un esquema de nombres completamente diferente. A continuación mostramos algunos ejemplos de este tipo de nombres de archivo:

- `smdhostn.dll`
- `heading.dll`
- `lgs.dll`
- `la.dll`
- `lh.exe`
- `lp.exe`
- `inl.exe`

Módulo PERSISTENCE

Como se describió anteriormente, este módulo secuestra la orden de carga del archivo DLL para mantener su persistencia en el sistema.

Cuando se inicia, el módulo crea la carpeta `%USERPROFILE%\AppData\Local\MMC` y copia allí los siguientes archivos desde el directorio `%WINDIR%`:

- `hauthuid.dll (CORE)`
- `hlpuctf.dll (KEYLOGGER)`
- `atiml.dll (LOGS_ENCRYPTER)`
- `iomus.dll (DOCS_STEALER)`
- `swma.dll (SKYPE)`
- `helpldr.dll (DOWNLOADER)`
- `rbcon.ini`

A continuación, este componente se carga y ejecuta el módulo CORE (o, si el módulo CORE no se encuentra disponible, ejecuta el módulo DOWNLOADER).

Si existe el archivo `%USERPROFILE%\AppData\Local\MMC\nullstate.cfg`, el componente elimina del directorio MMC todos los nombres de archivo enumerados arriba y se cierra, por lo tanto, queda desactivado.

Algunos de los binarios del módulo PERSISTENCE incluyen una ruta a un archivo PDB, que revela la estructura de directorios utilizada por los autores del malware durante la compilación. Tres de estas rutas contienen una marca de fecha y hora, posiblemente correspondiente al momento en que se creó o modificó el proyecto. Una de estas rutas contiene la cadena rusa `Раб. программы`, que se traduce como "programas informáticos para el trabajo".

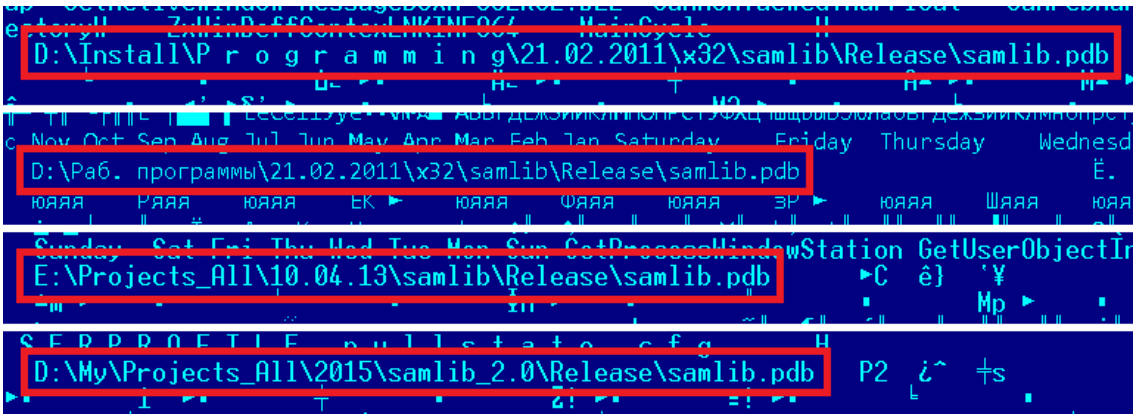


Imagen 20: Algunas de las rutas a archivos PDB descubiertas dentro del módulo PERSISTENCE de Prikormka.

Módulo DOWNLOADER

El propósito principal de este componente es descargar el módulo CORE y ejecutarlo.

El módulo DOWNLOADER realiza una petición HTTP a uno de sus servidores de C&C, recibe datos, los descifra, los almacena con el nombre `hauthuid.dll` y luego carga el archivo DLL. La comunicación se cifra con el algoritmo Blowfish y luego con Base64.

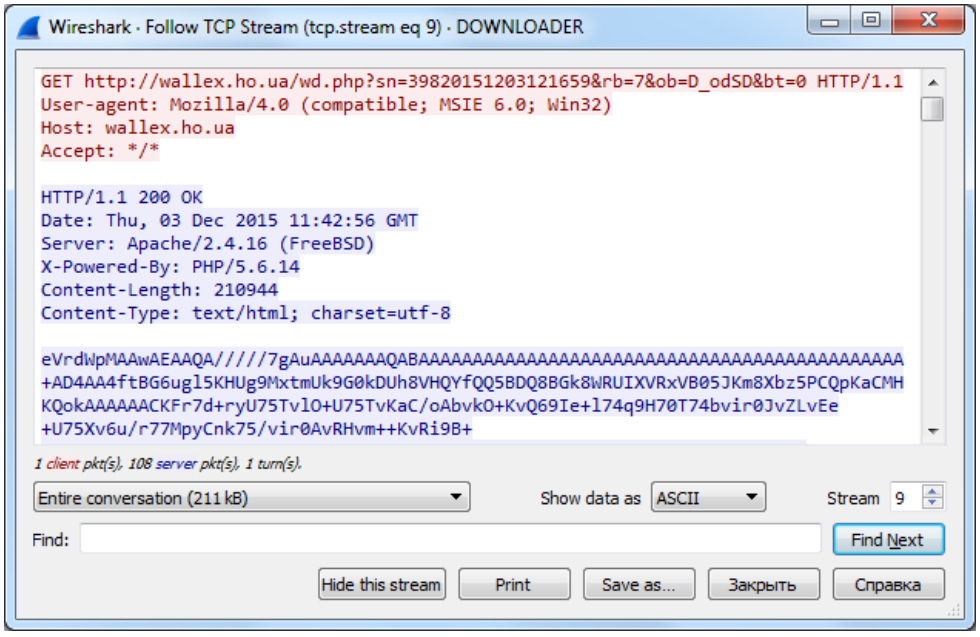


Imagen 21: Tráfico capturado desde el módulo DOWNLOADER del malware Prikormka.

Además del ID de campaña y el ID del operador, el módulo incluye en la solicitud la fecha y hora en que se produjo la infección y si la plataforma Windows es de 32 o 64 bits.

Algunos de los binarios del módulo DOWNLOADER contienen rutas a archivos PDB, lo que indica que internamente llaman a este módulo `Loader` o `helpldr`:

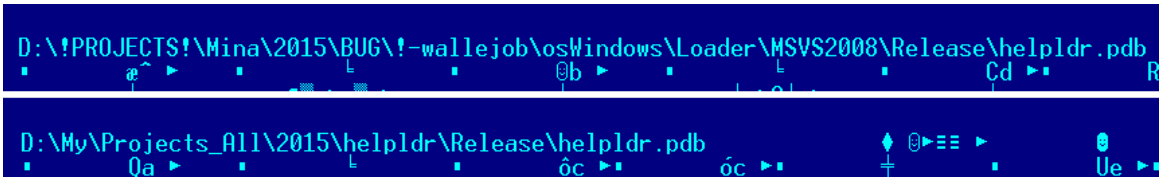


Imagen 22: Rutas de PDB descubiertas dentro del módulo DOWNLOADER de Prikormka.

Módulo CORE

El módulo CORE es el responsable de establecer las comunicaciones con los servidores de C&C, entre otras tareas, las cuales incluyen descargar módulos adicionales, cargarlos y subir los datos robados al servidor remoto.

Como este malware (y específicamente el módulo CORE) existe desde hace varios años, los detalles de su implementación varían; sin embargo, el concepto principal del módulo CORE se ha mantenido sin cambios a través de los años. Descarga componentes adicionales que sirven para recopilar diversos tipos de datos. Cuando se carga un componente de este tipo, extrae información confidencial y la guarda en un archivo de registro específico. Este último almacena los datos recopilados como texto sin formato o los cifra. El módulo CORE hace verificaciones periódicas de tales archivos de registro y, cuando encuentra que uno de ellos está disponible, lo sube al servidor remoto. Sin embargo, no sube ningún archivo de registro que supere los 500MB de tamaño.

Para almacenar los módulos descargables y los archivos de registro recopilados, crea dos directorios:

- `%USERPROFILE%\AppData\Local\MMC\`
- `%USERPROFILE%\AppData\Local\SKC\`

La carpeta MMC se utiliza principalmente para los componentes de malware descargables adicionales, mientras que la carpeta SKC se utiliza para almacenar los archivos de registro recopilados. De aquí en más utilizaremos el término "carpeta de registro" para referirnos al directorio SKC.

Los módulos descargables no son capaces de subir los datos recopilados. De hecho, solo los módulos CORE y DOWNLOADER se comunican con los servidores de C&C. El protocolo de comunicación del módulo CORE es muy similar al del módulo DOWNLOADER.

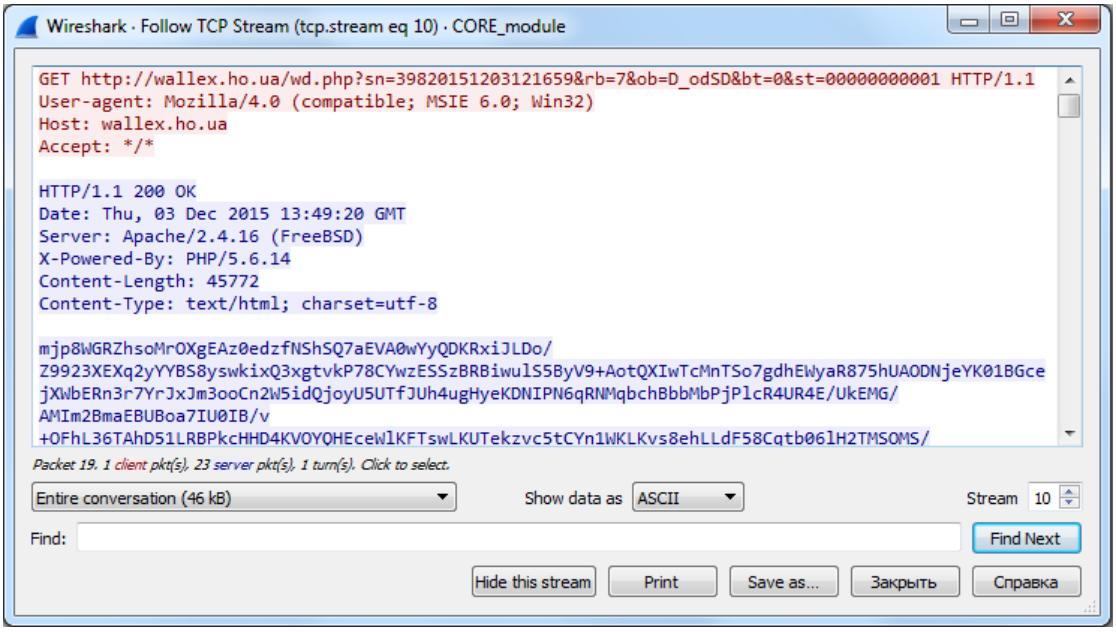


Imagen 23: Tráfico capturado del módulo CORE del malware Prikormka.

La única diferencia entre las peticiones HTTP del módulo DOWNLOADER y del módulo CORE es el parámetro `st` de la URL. Este parámetro indica cuál de los módulos descargables está activo y fue cargado por Prikormka. En la implementación actual, hay espacio para 11 módulos adicionales. El servidor responde ya sea con el contenido del módulo que se debe ejecutar o con contenido falso.

Los registros se cargan durante una petición POST a una URL similar:

- `hxxp:/server.ua/wd.php?sn=%DATE_TIME_OF_INFECTION%`

Vale la pena mencionar que las primeras versiones de Prikormka almacenaban las direcciones de los servidores de C&C en texto sin formato; más tarde, los atacantes comenzaron a utilizar el algoritmo Base64 para ocultar las direcciones de los servidores. Finalmente, las últimas versiones de los módulos CORE usan cifrado simple: para descifrarlo, el investigador debe añadir el valor hexadecimal 0x17 a cada byte cifrado.

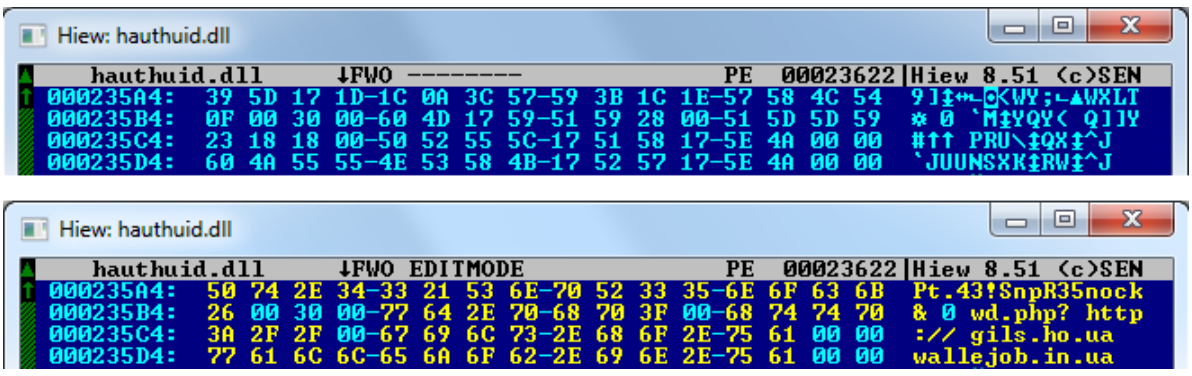


Imagen 24: Ejemplo de cifrado simple utilizado por Prikormka para ocultar las direcciones de sus servidores de C&C.

Módulo DOCS_STEALER

Este módulo se encarga de recopilar documentos de medios extraíbles o discos rígidos, conectándose a través de una interfaz USB.

El módulo se concentra en buscar archivos con las siguientes extensiones: .DOC, .XLS, .DOCX, .XLSX, .PPT, .PPTX, .PPS, .PPSX, .PDF, .RTF, .TXT, .ODT. De todas formas, no recoge todos los archivos que lleven estas extensiones, sino solo aquellos que fueron modificados en los últimos 7 días (o 14, o 30, dependiendo de la versión del módulo).

Los archivos recopilados luego se comprimen, se cifran con Blowfish y se almacenan según el siguiente esquema:

- `%USERPROFILE%\AppData\Local\ioctl\%DISK_ID%\%DATE%_%TIME%.kf`

Módulo KEYLOGGER

Este módulo se encarga de registrar las pulsaciones del teclado y los títulos de las ventanas en primer plano.

La información recopilada se guarda en la carpeta de registro con los siguientes nombres:

- `%DATE%_%TIME%_fix.lg`
- `lgfix`
- `lpl`
- `fplid`
- `fmmlg`

Si el archivo de registro excede los 10 MB, el módulo elimina el registro y comienza desde cero. Algunas versiones del módulo cifran el archivo de registro con Blowfish.

Módulo SCREENSHOTS

Este módulo se encarga de tomar capturas de pantalla del escritorio de la víctima.

Por defecto, el módulo captura una imagen cada 15 minutos. Sin embargo, si la víctima abre una aplicación de VoIP como Skype o Viber, el período entre las capturas se reduce drásticamente a 5 segundos. La imagen tomada se guarda en formato JPEG.

La información recopilada se guarda en la carpeta de registro con los nombres de archivo `%DATE%_%TIME%.tgz.scrsh` o `%DATE%_%TIME%.stgz`.

Módulo MICROPHONE

Este módulo es el responsable de grabar sonido con un micrófono.

El módulo registra archivos de audio de 10 minutos de duración. Detiene la grabación bajo un comando, o cuando no queda más espacio disponible en disco. El audio grabado se codifica con el codificador LAME para MP3.

La información recopilada se guarda en la carpeta de registro con el nombre de archivo `%DATE%_%TIME%.snm`.

Módulo SKYPE

Este módulo es el responsable de grabar las conversaciones de audio de Skype.

Para poder grabar las llamadas de Skype, el módulo utiliza una interfaz legítima: la API de escritorio de Skype. Cuando una aplicación de terceros está por comenzar a utilizar esta API, el messenger de Skype muestra una advertencia y le pide al usuario que permita el acceso. Para evadir esta función de seguridad de Skype, el módulo de Prikormka crea un subproceso que busca la ventana y hace clic en el botón "Permitir acceso" mediante programación, sin intervención humana.

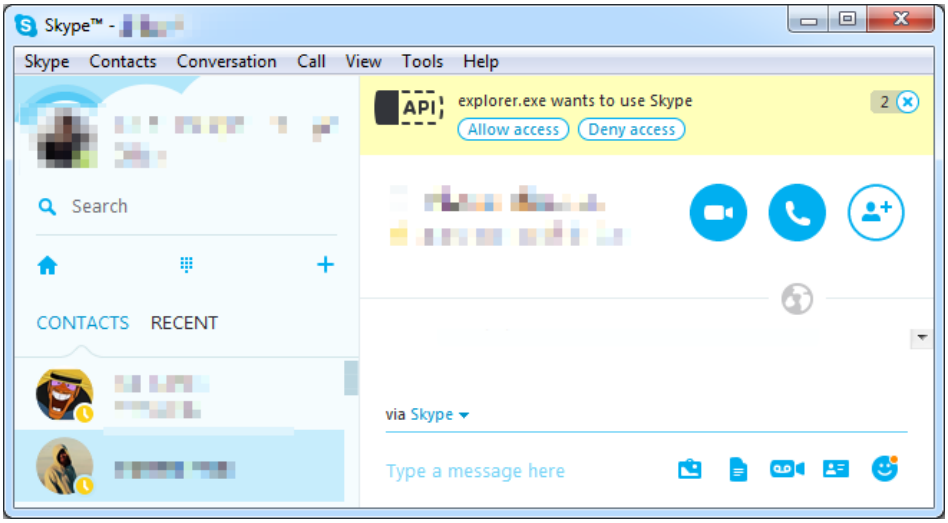


Imagen 25: Advertencia mostrada por Skype.

Algunos fragmentos del código de este módulo de Prikormka sugieren que una parte fue copiada del código publicado en el sitio web openrce.org en 2006.

```
.data:1001D0EC ; char str_MINISHELL[]
.data:1001D0EC str_MINISHELL    db 'CREATE APPLICATION minishell',0
.data:1001D0EC                                          ; DATA XREF: ProcessMessage+67↑o
.data:1001D0EC                                          ; SkypeAPI_Windows_WindowProc+3F↑o
.data:1001D109                  align 4
.data:1001D10C ; char str_CALL[]
.data:1001D10C str_CALL         db 'CALL %d',0          ; DATA XREF: get_CALL_ID+C↑o
.data:1001D114 ; char str_ALTER_CALL[]
.data:1001D114 str_ALTER_CALL   db 'ALTER CALL %d',0    ; DATA XREF: get_CALL_ID+26↑o
.data:1001D122                  align 4
.data:1001D124 ; char str_GET_CALL[]
.data:1001D124 str_GET_CALL     db 'GET CALL %d PARTNER_DISPNAME',0
.data:1001D124                                          ; DATA XREF: ProcessMessage+161↑o
```

Imagen 26: La cadena de texto `CREATE APPLICATION minishell` sugiere que una parte del código fue copiada y pegada.

La información recopilada se guarda en la carpeta de registro con los nombres de archivo `%DATE%_%TIME%.skw` y `_skype.log`.

Módulo LOGS_ENCRYPTER

Este módulo es el responsable de cifrar los registros.

El módulo comprime los datos a través del algoritmo LZSS y cifra los siguientes archivos de registro con Blowfish:

- `%USERPROFILE%\AppData\Local\MMC\inf`
- `%USERPROFILE%\AppData\Local\MMC\fsh`

- `%USERPROFILE%\AppData\Local\SKC\*.scrsh`
- `%USERPROFILE%\AppData\Local\SKC\*.snm`
- `%USERPROFILE%\AppData\Local\SKC\*.skw`
- Los archivos listados en `%USERPROFILE%\AppData\Local\MMC\ierdir.dat`

El módulo CORE crea el archivo `ierdir.dat`, que contiene una lista cifrada de los archivos que los atacantes desean subir desde el equipo de la víctima.

Luego del cifrado, se eliminan los archivos originales (pero no los cifrados). Los resultados del cifrado se almacenan en los siguientes archivos:

- `%USERPROFILE%\AppData\Local\MMC\ipl`
- `%USERPROFILE%\AppData\Local\MMC\kpl`

Además, el contenido cifrado se codifica con el algoritmo Base64. Cabe notar que, antes de que se inicie el contenido, el módulo agrega una firma más:

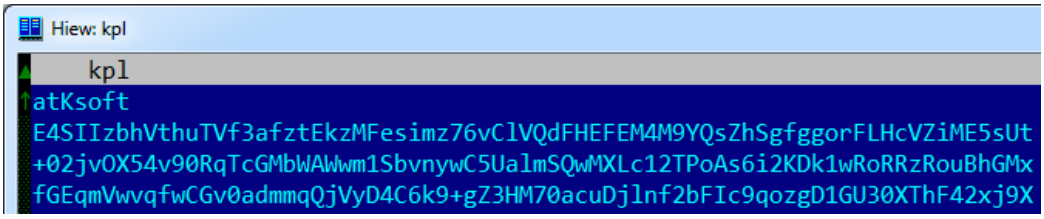


Imagen 27: Firma "atKsoft" al comienzo de los archivos de registro cifrados.

Aún no encontramos ninguna aplicación legítima capaz de leer estos archivos ni sabemos a qué se refiere el nombre de la misteriosa firma "atKsoft".

Módulo GEOLOCATION

Este módulo es el responsable de localizar geográficamente el equipo infectado.

A diferencia de otros módulos, éste está escrito en el lenguaje de programación C#. Recopila información acerca de las redes Wi-Fi disponibles en el momento, incluyendo el identificador de grupo de servicios (SSID) y la dirección MAC. A continuación, el módulo hace una solicitud al servicio de Google, suministrando la información recopilada como parámetros. La respuesta del servicio de Google contiene la ubicación posible basándose en la información suministrada.

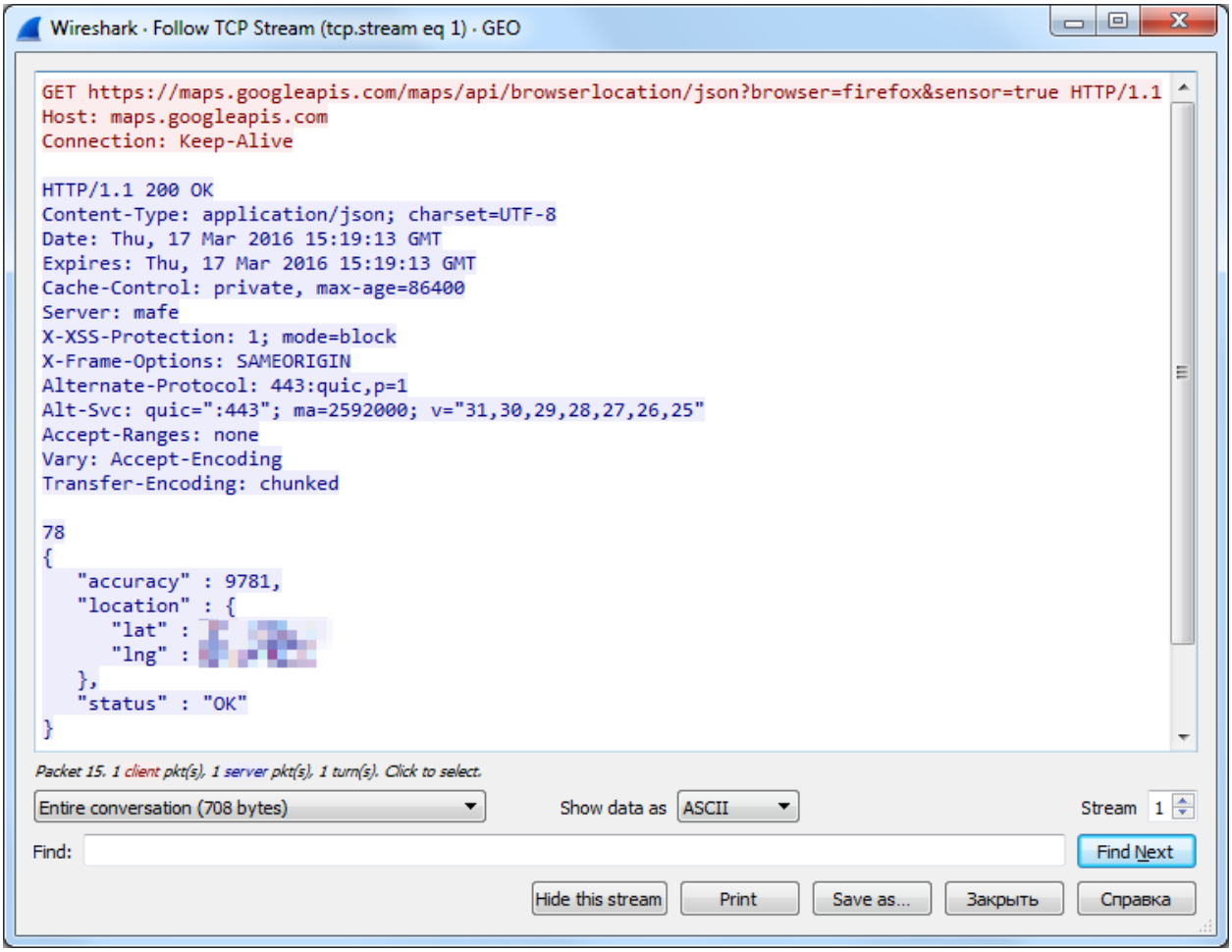


Imagen 28: Tráfico capturado del módulo GEOLOCATION del malware Prikormka.

La información recopilada se guarda en la carpeta de registro bajo el nombre de archivo `geo%DATE%.inf`.

El archivo binario del módulo GEOLOCATION tiene una ruta de PDB; la estructura de esta ruta es similar a la ruta de PDB del módulo DOWNLOADER:

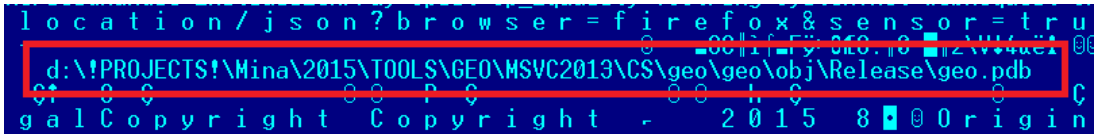


Imagen 29: Ruta de PDB descubierta dentro del módulo GEOLOCATION.

Módulo OS_INFO

Este módulo es el responsable de recopilar información sobre el equipo infectado.

Entre la información recopilada se encuentra:

- Información sobre la batería para equipos portátiles
- Versión del sistema operativo de Windows
- Nombre del equipo y nombre del usuario
- Direcciones IP y direcciones MAC
- Memoria física
- Unidades de disco disponibles

- Impresoras disponibles
- Resolución del escritorio
- Software antivirus instalado

Para recopilar esta información, el módulo usa las funciones de API de Windows.

La información recopilada se guarda en la carpeta de registro con el nombre de archivo `%DATE%_%TIME%.inf`.

Módulo PASSWORDS

Este módulo es el responsable de recopilar las contraseñas almacenadas en las aplicaciones instaladas en el equipo infectado.

El módulo recopila la versión de la aplicación, los nombres de inicio de sesión y las contraseñas almacenados en las siguientes aplicaciones:

- Google Chrome
- Navegador Opera
- Navegador Yandex
- Navegador de Internet Comodo Dragon
- Navegador Rambler (Nichrome)
- Mozilla Firefox
- Mozilla Thunderbird

Por alguna razón, este módulo no recopila las contraseñas de los navegadores Microsoft Internet Explorer y Microsoft Edge. Como los navegadores Yandex y Rambler son muy populares en países de habla rusa, creemos que este módulo ha sido diseñado para utilizarse en ataques contra usuarios en dichos países.

La información recopilada se guarda en la carpeta de registro con el nombre de archivo `%DATE%_%TIME%.inf`.

Módulo FILE_TREE

Este módulo se encarga de recoger información sobre el sistema de archivos de los discos rígidos de la computadora, incluyendo las rutas de archivos con extensiones específicas, su tamaño y fecha de creación. El módulo no recopila el contenido real del archivo.

Los atacantes están interesados en las siguientes extensiones de archivo:

- Documentos: TXT, DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF
- Archivos comprimidos: ZIP, RAR
- Bases de datos: DB, SQLITE
- El cliente de correo electrónico The Bat!: TBB, CFG, CFN, TBN, TBB
- Microsoft Outlook: OST, PST
- Otros: DAT, WAV, EXE

Como el cliente de correo electrónico The Bat! es muy popular en los países de habla rusa, el hecho de que el malware se centra en las extensiones de archivo asociadas a este cliente de correo electrónico es otro indicador más de que se diseñó con la intención de usarlo contra usuarios de habla rusa.

Cabe señalar que no aparecen todas estas extensiones de archivo juntas en cada muestra individual del malware. Esta lista completa incluye todas las extensiones de archivo posibles que fuimos observando en distintas versiones del módulo FILE_TREE. Los atacantes pueden crear una versión personalizada de este módulo para una víctima específica.

La información recopilada se guarda en la carpeta de registro con el nombre de archivo `%DATE%_%TIME%_tree.inf`.

Algunos de los archivos binarios del módulo FILE_TREE tienen rutas a archivos PDB; una de estas rutas revela el nombre de usuario del creador del malware.

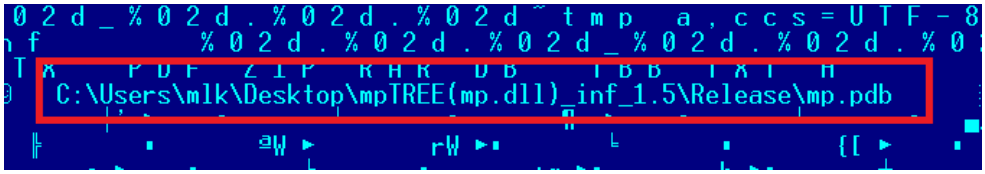


Imagen 30: Ruta a un archivo PDB descubierta dentro de un módulo FILE_TREE.

Servidores de C&C

Durante nuestra investigación sobre la Operación Groundbait, observamos una serie de nombres de dominio de servidores de C&C y de direcciones IP. La mayoría de ellos están ubicados en Ucrania y utilizan proveedores de hosting ucranianos. En el Apéndice B se muestra un listado más completo.

Según los datos proporcionados por la empresa de servicios de hosting, uno de los servidores de C&C, `gils.ho[.]ua`, ha estado funcionando desde el año 2008. Para ocultar su actividad ilegal, los atacantes crearon un sitio web falso que contiene información sobre la capital de Ucrania: Kiev.

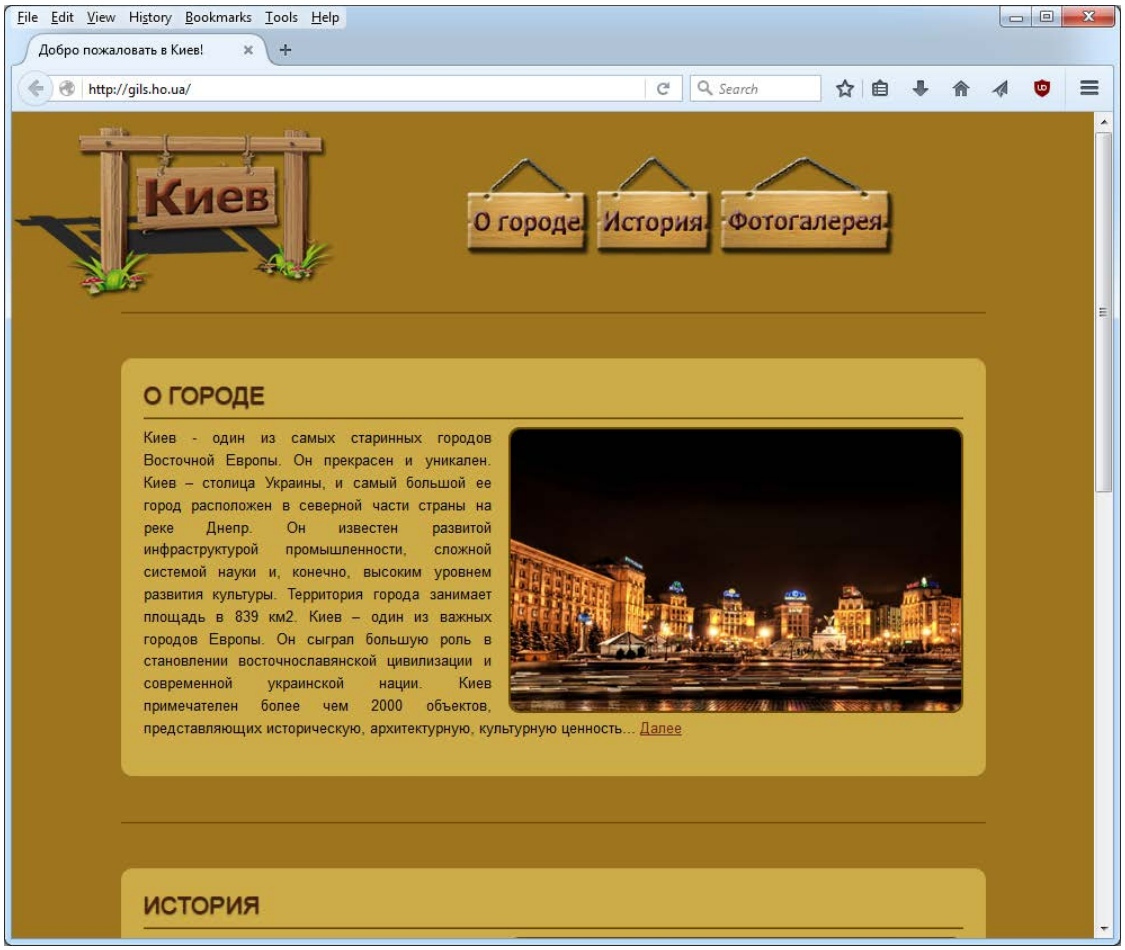


Imagen 31: Sitio web falso creado por los atacantes.

Durante nuestra investigación, obtuvimos acceso a un servidor de C&C de la Operación Groundbait mal configurado y logramos obtener un listado de directorios.

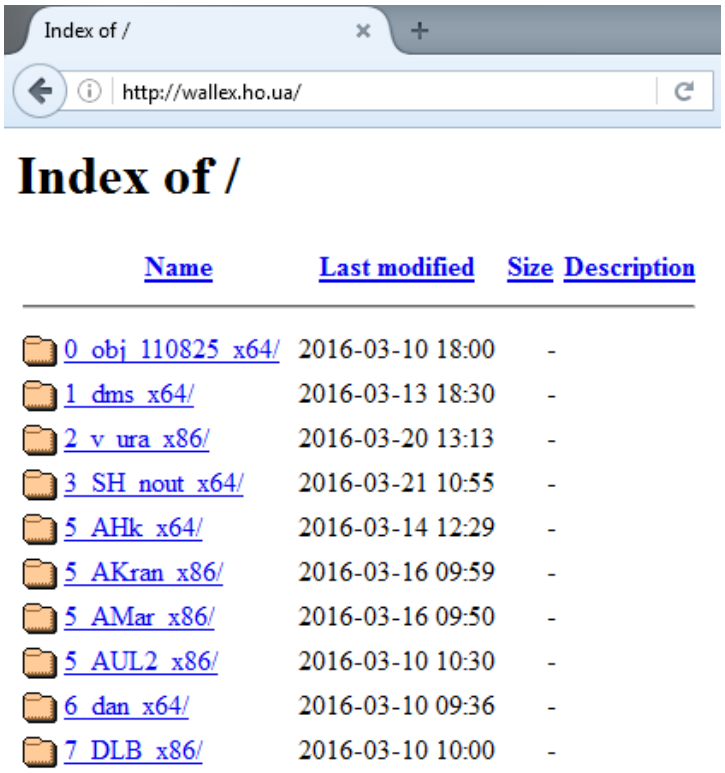


Imagen 32: Listado de directorios de los servidores de C&C de la Operación Groundbait.

En un momento dado, el directorio raíz contenía 33 subdirectorios, con una carpeta individual para cada víctima. Esto significa que el servidor se utilizaba para controlar 33 equipos infectados con Prikormka. El nombre de cada subcarpeta contiene el ID del operador, el ID de campaña y la arquitectura del dispositivo infectado.

Cada carpeta contiene dos subcarpetas con los siguientes nombres: `data` y `util`. La primera carpeta contiene los datos extraídos cifrados y la segunda carpeta tiene los módulos de Prikormka cifrados.

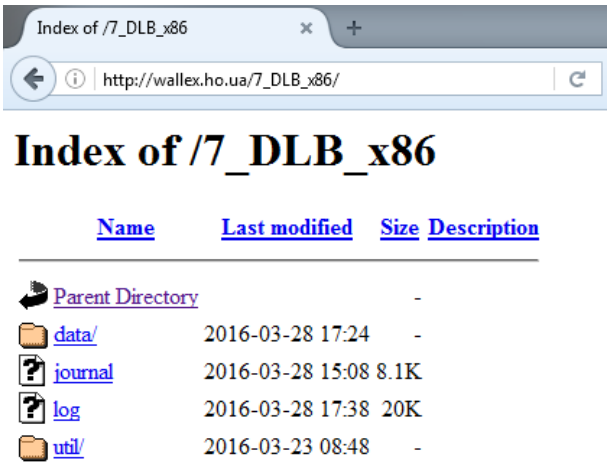


Imagen 33: Estructura interna de directorios de una subcarpeta.

Además de las carpetas `data` y `util`, cada subcarpeta de una víctima específica contenía dos archivos de registro en texto sin formato: `journal` y `log`, que revelaban datos interesantes sobre los operadores del malware y sus víctimas.

El archivo `log` incluye el registro de las comunicaciones entre el servidor y el equipo infectado: en concreto, la dirección IP del equipo infectado, la fecha y hora, el tipo de petición (GET o POST), el tamaño de la solicitud, y el estado de los módulos de Prikormka (en los casos en que se trata de una petición GET).

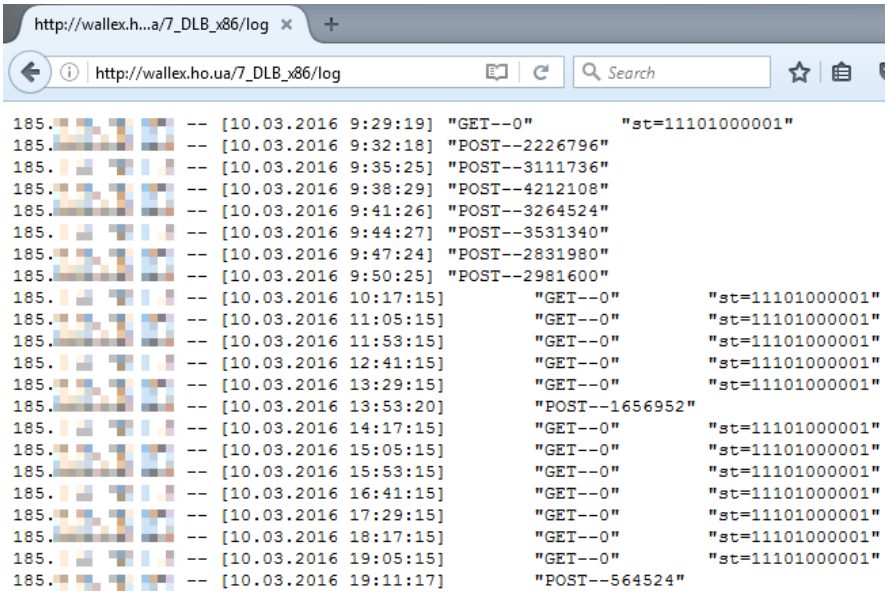


Imagen 34: El contenido del archivo `log` se guarda en el servidor de C&C de la Operación Groundbait.

El archivo `journal` contiene el registro de las comunicaciones entre el servidor y el operador de malware. El registro de comunicación incluye la dirección IP del operador, la fecha y hora, y el tipo de petición. Cabe señalar que, una vez que el operador de malware descarga el archivo con los datos extraídos, éste se elimina del servidor.

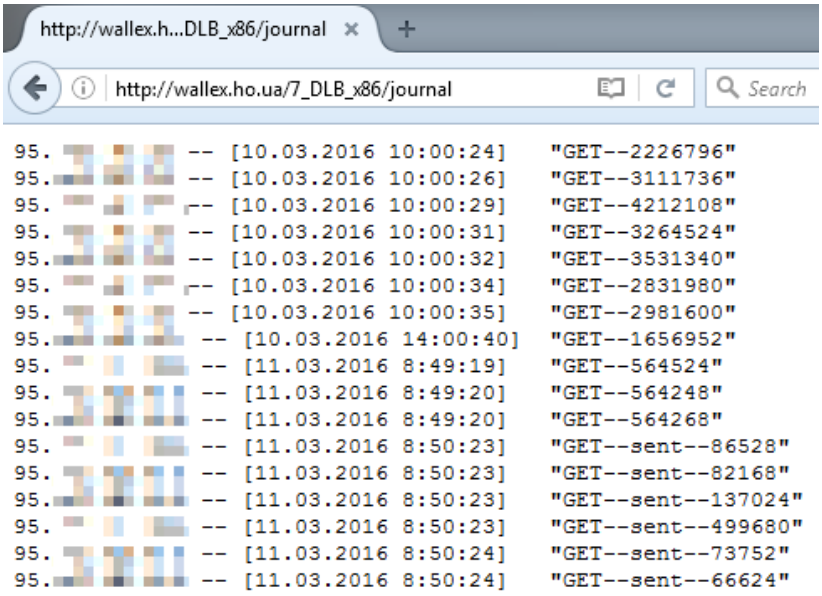


Imagen 35: Contenido del archivo `journal` encontrado en uno de los servidores de C&C de la Operación Groundbait.

De acuerdo con nuestro análisis de los registros de comunicaciones obtenidos de un servidor, hubo 33 víctimas, localizadas principalmente en el este de Ucrania. Además de ellas, había algunas víctimas más de Rusia y de Kiev, Ucrania.

El análisis de los registros reveló que varios operadores de malware se conectaban al servidor utilizando varios proveedores de servicios de Internet en Kiev y Mariúpol. Algunos de ellos accedían al servidor de C&C a través de la red Tor.

Atribución

En esta sección intentaremos identificar el origen de la amenaza sobre la base de los indicios dejados por los atacantes, ya sea en forma intencional o no:

- La mayoría de los servidores de C&C de Prikormka están ubicados en Ucrania y usan servicios de hosting ucranianos
- El grupo tras esta amenaza usa los idiomas ruso y ucraniano con fluidez, como lo demuestran el texto de los documentos señuelo y los archivos binarios del malware
- Algunas de las rutas a archivos PDB revelaron que los atacantes utilizaban directorios con nombres en ruso
- Todos los droppers de Prikormka analizados contenían códigos de idioma que corresponden al ucraniano (código hexadecimal 0x0422) o al ruso (0x0419) en sus recursos de archivos PE (Imagen 37)
- Las marcas de tiempo correspondientes a la compilación de los archivos binarios de Prikormka sugieren que los autores del malware trabajan en la zona horaria de Europa del Este
- De acuerdo con los registros de los servidores de C&C, varios operadores de malware que participaban en la Operación Groundbait se estuvieron conectando a través de diversos proveedores de Internet en dos ciudades ucranianas: Kiev y Mariúpol.

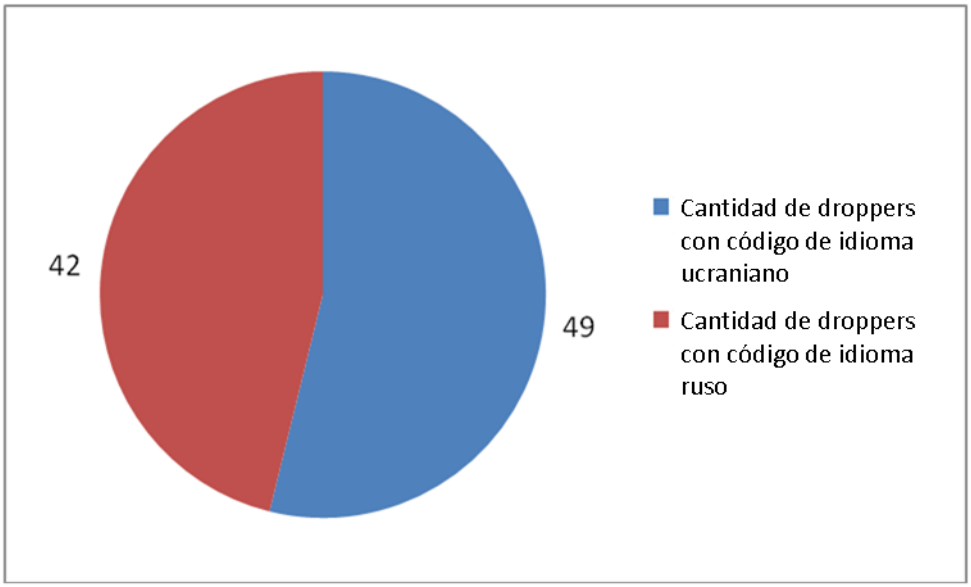


Imagen 36: Distribución de los códigos de idioma entre droppers.

Es interesante notar que los droppers usados en la primera etapa del malware (de 2012 a 2015) contienen recursos con códigos de idioma en ruso. Los autores del malware fueron cambiando gradualmente del ruso al ucraniano hacia mediados de 2015.

La Imagen 38 muestra la distribución de las horas de compilación para las muestras de Prikormka.

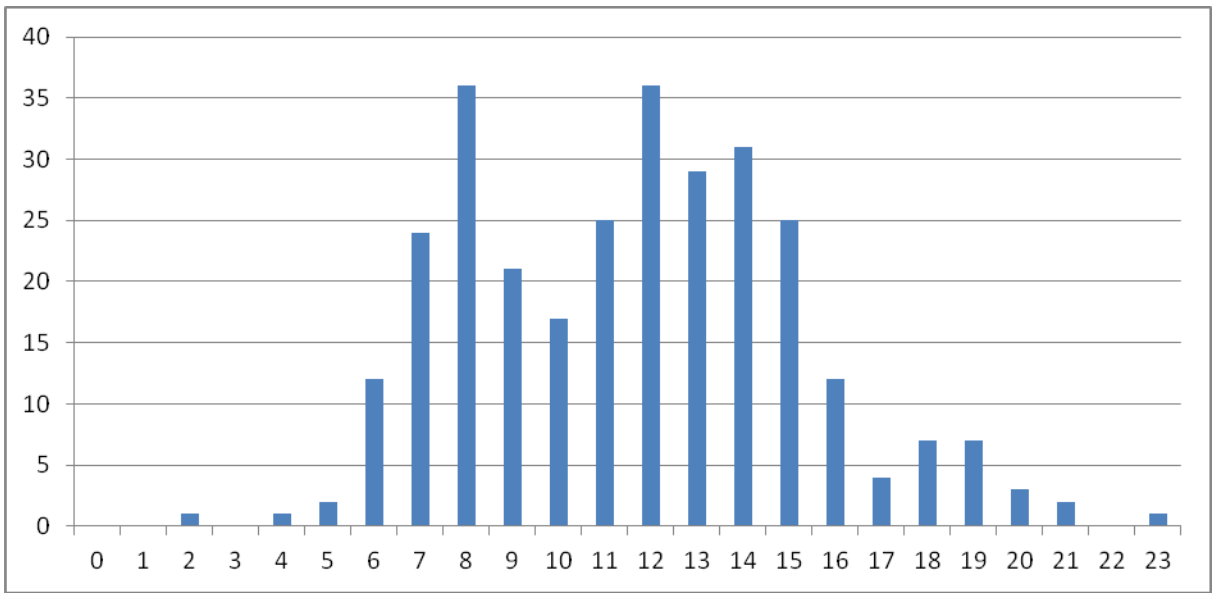


Imagen 37: Muestras ordenadas por hora (UTC).

De estos datos podemos deducir que los autores del malware trabajan desde las 6:00 hasta las 16:00 horas (UTC), y a veces se quedan trabajando hasta tarde por la noche. Estos horarios corresponden a la franja horaria de 8:00 a 18:00 horas en Europa del Este, que es el horario de la jornada laboral estándar en Ucrania.

De acuerdo con los resultados de nuestra investigación y los hechos mencionados en este documento, llegamos a la conclusión de que los atacantes detrás de la Operación Groundbait están interesados en el seguimiento o el espionaje de los separatistas en las regiones de Donetsk y Lugansk, así como algunos objetivos específicos de alto perfil, entre los que se incluyen políticos ucranianos. Los operadores y/o los autores del malware conocen muy bien los idiomas ucraniano y ruso, y es probable que operen desde dentro de las fronteras de Ucrania.

Conclusión

Nuestra investigación de estas campañas de ataques maliciosos y del malware Prikormka sugiere que es la primera amenaza ucraniana conocida utilizada en ataques dirigidos.

En cuanto a los avances técnicos, los atacantes no utilizaron ningún método sofisticado ni técnicas novedosas. No obstante, no importa si el atacante utiliza métodos sofisticados o no siempre y cuando alcance su objetivo principal: en este caso, robar la información confidencial que necesitan de sus víctimas.

El logro más notable de los atacantes responsables de la Operación Groundbait es haber pasado desapercibidos durante más de 7 años. El malware ha estado activo por lo menos desde el año 2008. Este hallazgo queda confirmado por las marcas de tiempo y hora de los archivos binarios, la telemetría de ESET y los proveedores de servicios de hosting utilizados.

Después de BlackEnergy y la Operación Potao Express, la Operación Groundbait es una demostración más de que el uso de malware altamente dirigido para el espionaje en un conflicto armado es una realidad corriente.

Los Indicadores de sistemas comprometidos (IOC) que se pueden utilizar para identificar una infección están disponibles en GitHub.

Ante cualquier duda o para enviar muestras relacionadas con este tema, escríbenos a: threatintel@eset.com

Créditos

Un agradecimiento especial a @TheEnergyStory

APÉNDICE A: DETALLES DE LAS CAMPAÑAS DE PRIKORMKA

Fecha y hora del archivo PE (UTC)	ID de campaña	ID del operador del malware
19 de abril de 2012 09:11:27	N/D (dañado)	N/D
25 de julio de 2012 8:31:32	SKt	N/D
13 de septiembre de 2013 08:21:54	MNa	N/D
12 de marzo de 2014 15:17:23	Pgks	N/D
15 de julio de 2014 12:18:51	Abk	N/D
03 de octubre de 2014 8:57:13	W_zp7a	N/D
05 de noviembre de 2014 7:56:00	zma	N/D
05 de noviembre de 2014 19:30:35	Psep	N/D
13 de noviembre de 2014 10:20:10	hmod	N/D
25 de noviembre de 2014 15:12:31	1ff	N/D
01 de diciembre de 2014 8:07:07	hmyr3	N/D
05 de diciembre de 2014 13:11:35	1ii	N/D
31 de enero de 2015 13:19:22	1vo	N/D
10 de febrero de 2015 18:31:49	Pgad5	N/D
19 de febrero de 2015 15:51:33	Pkof	N/D
02 de marzo de 2015 16:23:42	Ptrop	N/D
11 de marzo de 2015 8:43:12	l01u001	N/D
23 de marzo de 2015 12:46:24	Asap	N/D
23 de marzo de 2015 16:03:19	P647	N/D
10 de abril de 2015 12:26:20	Plg8_	N/D
06 de mayo de 2015 6:08:52	W_cu6a	N/D
24 de mayo de 2015 8:46:38	Pod13_	N/D
11 de junio de 2015 14:59:45	Aste	N/D
21 de junio de 2015 15:36:24	MVD_LNR_kontakt	7
26 de junio de 2015 13:25:22	r03u0002	N/D
29 de junio de 2015 6:19:36	Dmindoh_zb	7
01 de julio de 2015 12:42:04	r03u0002	N/D
05 de julio de 2015 6:21:49	Lminfin	7
09 de julio de 2015 14:48:56	gm	1
16 de julio de 2015 14:29:29	Lmgb	7
16 de julio de 2015 14:55:50	Lrod	7
16 de julio de 2015 15:03:59	Dmo	7
18 de julio de 2015 4:35:41	Lsck3	7
18 de julio de 2015 5:07:50	Dmo	7
19 de julio de 2015 7:41:54	PMil_6	N/D
19 de julio de 2015 8:11:26	PLmgb2	N/D
20 de julio de 2015 17:51:04	Psek	7
21 de julio de 2015 6:08:53	medium	3
26 de julio de 2015 19:17:52	MDLV2	7
26 de julio de 2015 19:22:27	OSCE	7
07 de agosto de 2015 9:23:57	BOY_D	12
14 de agosto de 2015 6:11:43	BUR	7
17 de agosto de 2015 17:58:58	RBx	7
17 de agosto de 2015 18:32:51	MRV1	N/D
22 de agosto de 2015 11:35:37	D_00732	7
28 de agosto de 2015 13:42:34	D_xxx	7
03 de septiembre de 2015 12:02:35	zkonv	N/D
24 de septiembre de 2015 16:39:43	L_mgb	7
13 de octubre de 2015 10:52:47	R_pol_x	7

13 de octubre de 2015 11:54:58	RF_lgm	7
14 de octubre de 2015 6:55:23	LKos_xx	7
21 de octubre de 2015 12:56:05	K83_mo	10
21 de octubre de 2015 19:33:21	DLB3	7
22 de octubre de 2015 8:48:26	DLB_sgrish	7
29 de octubre de 2015 14:00:05	FSfarm	11
30 de octubre de 2015 7:40:28	piter	8
11 de noviembre de 2015 8:57:44	45K_perev	10
20 de noviembre de 2015 16:43:20	30K_alfa	10
26 de noviembre de 2015 12:54:58	REP_L	12
28 de noviembre de 2015 7:39:26	L_K_geniy	7
03 de diciembre de 2015 7:21:31	D_odSD	7
03 de diciembre de 2015 9:40:43	L_min1	7
03 de diciembre de 2015 10:33:27	D_newsG	7
15 de diciembre de 2015 11:48:39	M_raz_	N/D
18 de diciembre de 2015 9:12:40	7_L_xxx	7
18 de diciembre de 2015 12:12:10	33K_pushkin	10
28 de diciembre de 2015 13:57:12	38K_135_vnos	10
29 de diciembre de 2015 14:58:11	Kvk_ham	7
12 de enero de 2016 11:44:22	38K_83_parf	10
14 de enero de 2016 9:14:22	L_ssa	7
19 de enero de 2016 15:30:41	shubin	35
19 de enero de 2016 15:31:31	shubin	35
19 de enero de 2016 15:33:35	shubin	35
22 de enero de 2016 10:04:27	34_Ffot	11
30 de enero de 2016 6:38:17	MM_mmh	7
30 de enero de 2016 7:56:11	L_m3	7
01 de febrero de 2016 9:46:49	38_Faro	11
05 de febrero de 2016 8:00:05	MM_1eco	7
05 de febrero de 2016 8:20:01	MM_1kur	7
05 de febrero de 2016 8:51:46	L_1m1	7
08 de febrero de 2016 14:49:52	L_ment	7
17 de febrero de 2016 15:06:39	sdd1	12
22 de febrero de 2016 14:25:18	L_rozysk	7
22 de febrero de 2016 14:29:36	L_rozyskR	7
25 de febrero de 2016 10:26:58	33K_037	10
25 de febrero de 2016 14:18:30	F_ego	11
22 de marzo de 2016 15:25:59	sgukiev	11
08 de abril de 2016 12:13:20	avl	6
18 de abril de 2016 11:10:21	L_ukrB	7
27 de abril de 2016 12:40:46	puh	6
05 de mayo de 2016 11:42:54	L_gp	7

APÉNDICE B: INDICADORES DE SISTEMAS COMPROMETIDOS

Los usuarios del software de seguridad de ESET están totalmente protegidos ante el malware Prikormka descrito en el presente paper. Además, ESET le suministrará información adicional sobre esta amenaza a cualquier persona u organización que se infecte o se haya infectado en el pasado.

Correo electrónico de contacto: threatintel@eset.com

Detecciones de ESET

```
Troyano Win32/Agent.UIG
Troyano Win32/Agent.XOR
Troyano Win64/Agent.XOR
Troyano Win32/Agent.XQX
Troyano Win32/Agent.XRA
Troyano Win32/Agent.XRB
Troyano Win32/Agent.XRC
Troyano Win64/Agent.DX
Troyano Win32/TrojanDropper.Agent.RGH
Troyano Win32/TrojanDropper.Agent.RHN
Troyano Win32/Prikormka
Troyano Win64/Prikormka
Troyano MSIL/Prikormka
```

Basado en el host

```
%PROGRAMFILES%\IntelRestore\
%USERPROFILE%\Resent\roaming\ocp8.1\
%USERPROFILE%\AppData\Local\MMC\
%USERPROFILE%\AppData\Local\PMG\
%USERPROFILE%\AppData\Local\SKC\
%USERPROFILE%\AppData\Local\CMS\
%USERPROFILE%\AppData\Local\VRT\
%USERPROFILE%\AppData\Local\ioctl\
%WINDIR%\ntshrui.dll
%WINDIR%\hauthuid.dll
%WINDIR%\hlpuctf.dll
%WINDIR%\atiml.dll
%WINDIR%\iomus.dll
%WINDIR%\swma.dll
%WINDIR%\helpldr.dll
%WINDIR%\rbcon.ini
%USERPROFILE%\AppData\Local\CMS\krman.ini
%USERPROFILE%\AppData\Local\VRT\_wputproc.dll
```

Mutexes

```
ZxWinDeffContexLNKINFO64
Zw_&one@ldrContext43
Paramore756Contex43
ZxWinDeffContexSMD64
ZxWinDeffContexWriteUSBIO64x
ZxWinDeffContexRNDRV45scr
ZxWinDeffContexRNDRV45snd
ZxWinDeffContexSkSwmA
ZxWinDeffContexKINP64
ZxWinDeffContexRNDRV65
ZxWinDeffContexRNDRV65new
ZxWinDeffContexRNDRV65xyz
ZxWinDeffContexRNDRV65xy
ZxWinDeffContexRNDRV64
Client67workProc98List3To
```

Servidores de C&C

```
disk-fulldatabase.rhcloud.com (IP: 54.175.208.187, 23.22.38.222)
wallejob.in.ua (IP: 185.68.16.35)
wallex.ho.ua (IP: 91.228.146.13)
gils.ho.ua (IP: 91.228.146.12)
literat.ho.ua (IP: 91.228.146.13)
lefting.org (IP: 91.228.146.11)
celebrat.net (IP: 91.228.146.11)
```

bolepaund.com (IP: 91.228.146.12)

Servidores utilizados para enviar correos electrónicos dirigidos de phishing

server-eacloud.rhcloud.com (IP: 54.152.171.48, 54.163.210.39)
easerver-fulldatabase.rhcloud.com (IP: 52.23.164.7, 23.22.221.237)

Hashes SHA-1

Droppers de Prikormka:
42041871308B5711041B7AF69B78F45DF642546C
37F75844C0D0F7F80A699153AF131984D2CE2B6D
029F054A52FE93B0CD6C4D1D815A795EAE9CAAB4
66C143D7C33666903B174F4B94D609BE8791914D
60351035ECDEED071E3FB80AFFE08872A0B582C9
0296191B323900B2BC014E2ACB5E0614C679B682
1BF0E90027EF798727A4496B1928F1FA79146051
76CAE58E4DF4D029155BF2E44BA0F8075DC99020
C0FBE31F1E6E56E93932076BA55A5229E22B5C4A
CF09B0CD03C9D0553F0B82827C989D04F1A1FAF1
7C28B907E1053F825478A74FDC1090FBF71DD878
D7F35B66C554EE1076279DF54C4E931651A7A211
2B0FB236DDC0098ADDF051531912FC2601FFCCDC
EAB122E5857DF838469B5B00DA0A3BD06DF8DA05
00BCCEBB7614BA270CA2908EE5711F25D3740E7E
F908824DB35EFD589449D04E41F8BCEA057F6E52
A8CED2FF8F3D4B77160CB81843652D971469A30B
6002357FB96A786401BAA40A89A85DBA3A7D7AD4
E3E9CA2AC83CFADD80FECD002B377B6B41AC5250
EAFC458AAC3F1564E940BAC7D45C1E659636CC86
FCBC8C75246511F9E4D49FE501F956A857FACE84
803C48A93785581AA89422B6B1E73677BF8DC749
87C34623EBEC481FD430F6CE26849220C641742C
A1EE4E4BA27B4035F29FA6AB943AE072D42E65B8
19AAB5FAE0809F87EF27A18208A3C0C52DEA182A
C88218C2C23555D5E39596B2110BDA54A7AD50DB
EC16141D6C0399B74A26B7B572580B3AC4CBC811
76B77E40182DA242307272B9F77132ABB0B46515
7AB44936E5545C5778C697ABCC20FD8955E35F36
86DD049877B564158020AB9B1A6CA3C30371979D
8665C7A753BA5F619FE79D52DC49724F17D81DAC
8839ED42EC1440CBF30CC345F11B88450EA8FE46
4D2C8CD6C514202CBC133347E2C35F63F03A77BF
CDF0734730EA786AD2D3B0E9D0D82F85D3C4AD07
99345C5E6FC6901B630C044DD5C6A5015A94B046
93FE501BCDF62060798E35643B7E5F4E3FFF05A6
1287205FE5B83583CB28D39D965D182EA1DFCFDB
C0C4DB689F393A26611B7F8FE08F38B456A173DA
3F867CF4AE4B1232B08E40ADABE7BC21EF856FE2
E9A2B1611EDC105FBA65AFFCDAB062D6FA5C67B0
ADDF8193442D145C6BCB4C54B95A5CFE759C6436
CD5AA66AD7C8D418F19B486211591E31B5B74AB6
8A01C06DF6E59F1513146DFE07936E4ACA59B152
E35081B99C5445952AD4E204A4C42F06D7C3707D
A6D8431EFBA501864C4646A63071D28B30EEBF99
613F631D0E384954D2FEA5BE39124AD821C8E5D6
D45CECD9DDD79259C6518300ED77257A9ABBDF92
642033A50EF2C51E1F391D85ED870B09A308469A
FD95C6B33AF4B29EFBD26D388C50164C3167CB68
9A578C7C305BE62167EF87AB52E59A12F336186A
FE9F5018198567F3D3FB3AA09279C65DBE981171

62487DD8EC172462F9B4CBB790EF6F7878D20352
E397F1D784B4A9EEE7EEAC427C549A301DEC0C7C
E8A2734C3FFECB76DD4D1C28D646EE59188BE7BF
8DF79B2734BCD83B3D55FF99521D10E550DFCFF3
64D31BBCF8E224E06BB5F1B350D2F18BFDD78A8E
D5B785F8F92C7588CFAD7A1A21DAFFA6EB9CFA5C
8327A743756FA1B051725BF8EC3FDD9B9E844E9A
98440EC18A7E78925CB760F5016111115C89F1F8
6E56BC6023085D6E88668D1C66B91AB5AA92F294
160CF2ABB25495188A0ACB523BD201B0369CFFD2
6E5A098A3EDDEEC2E4986DE84FB00D7EA7EE26B8
8358EA16A0DE64994FBECE1AAC69E847F91BB1B3
3A6C8CB6688E2A56057BA9B3680E5911D96B2C8C
AB011CD03B3F211F43930AABD909B5611A829D9D
279711B6828B6CF642C0DAB4D16411C87956F566
2BF9CA8B16BCD679AFB6E9E53C3BB0B04E65044A
9551C390B2DF178DED895D531F440FDDBAE122AA
BB8D93A4049968C6D5A243DCFB65A6F4B4DE22A2
80CB14652E8251C79187DF8A01D29ABD46A3118C
6E24C2403DAFAE05C351C5A0A16E2B6403E0F398
09EA7B2F67797915BBFED16F0B21E4E31F4980A3
0AA48DEE8F528B037D8D72AAD039BB2759F362E3
40D7D09053BF60925CBB820417A42DBC6293E017
A6600BD9752E041ED7EE026123A60B19C96259AB
506CCEBDAC5754D1E20D9C3FB280CEC7782EEA6E
40F33CD2AD98FE1E6BF4AB199021498F9E3125A1
9F03A4E0ACD38635104292B8054485E6BF898C48
B373BF4B3AA28FF6D373DA5EAA848AF9772F6454
FD83C2484E2986F22B09623E5971AA54FBD8BCD3
065B075293968732F2BE433B7B492869E4260EE5
B358687593FEBDFD0E1858726098DCFD61D9F8B5
FD2FBB8E4676673A35276B46F2C74562703BCF39
CCD19FD4A1408FCD855B7909578340846904E707
9D84665C00F81C2835E2A41711A139547351D850
69536CAF0522C1A915D6AC4C65177A26EFA7944B
243421FE7C1FC007EFA0C9CCAB6F6E2A0C94FCC2
5B7D6D7C3C4AD74A7F1E32B780776DB41FF18DDD
4418A32BBD215F5DE7B0063B91731B71804E7225
EE1E5D95FCAD429126944804D80D7C2412AF492E
E494328255EF2B9ED9B332EE845513A93339217F
6B53A3A3CB9D87D5925C82839015DAD16042C2FF

Primeras versiones de Prikormka:
1B8BC6924F4CFC641032578622BA8C7B4A92F65E
B5F1B3BD6AD281C8EB9D633A37E0BE63B97A8BEB
BCEDAB81CC5F4D2EA1DA8A71F91DF6E16362723B
DC52EE62B94DC38790C3EF855CE5773E48D6CD55
44B6B8375CF788076C0DD64A93E27F69A01F5DFD
539033DE14539D485481549EF84C9E49D743FC4C

Módulos PERSISTENCE de Prikormka:
AD9A6F7BA895769844663B4936E776239D3A3D17
E1B5CD1978F6C6D72AA6B07ADD1EE83E9BB8480D
6E312A999EE7DCD9EC8EB4F0A216F50F50EB09F6
8F8BD3C4CE2F932ABFB31B9F586C40D1E22EE210
3F8D8B20B8FCC200939BBB92FB3B93BB3B4ECD24
756730D1C542B57792F68F0C3BC9BCDE149CF7C6
4F1441F16E80272F488BB114DB6508F0BB9B9E1B
2E1C7FFAB7B1047E3438E6BA920D0914F8CC4E35
3C9990B5D66F3AE9AD9A39A10AC6D291DD86A8F9
CC7091228C1B5A0DAF39ECDA570F75F122BE8A16
26FAEAAE2C042C0A416287A7C54D63D5B4C781B3
854F7CB3A436721F445E0D13FB3BEFF11BF4153D
0596EFE47D6C143BE21294EB4E631A4892A0651A

7DAE2A15E364EE06C9301236AE8FC140884CEA95
C2F720DEF2264F08E5211671D46E73311DC6C473
36215D9A691D826E6CEBC65925BFA6B579675158
0354A768508F6B9D88588641397B76A0CBB10BF2
1790B3D73A5DD676D17B39C01A079DEBD6D9F5C5
2F1E4AF1A5A95B3483E901ABDD96454C57419BA4
53174F09C4EDB68ED7D9028B86154B9C7F321A30
FCD81737FF261A84B9899CB713933AA795279364

Módulos DOWNLOADER de Prikormka:
D12CD6C4CA3388B68FCF3E46E206064CAA75F893
C2EA09D162BDAD2541C97D30A4E171F267305671
C10D6E4ADB3B29C968D7F3086C8E7005DD1E36F4
CE4605994E514086ADA5A767296DB66D7EA84175
148218ECDDE9ECC19B1343080884EB819783D9B2
5B256971F332498ACC833B36CBE9AD0CEC71384C
4A8452575FF69BDD0806AA8915E459E8ADC66DF1
04DFC621649511E1AB6CB800124DD5E2874A1629
D51863CBC1AC4BFC2B87F247DC75975E2A9CD992
C8AF6A8270CBD030F09C24888480AEF093ACCF48
EF127184967BE14A3719978E0236FFF5C0AF811B
2FF9E3AB4912A4AEA3C511D9355B8EDD13888E2A
40B163E8E74397E69F18805BD7DAB67F06D3D9E2
A8DFCD6CDB0755966F3D6766B94989CDAA0C35F9
6D4A80FE57D57B43DAF85401DFDD2CDA48D1F023
7844678942383F8116BAC656BC56D4B230FF62E8
8B9460431296DAF13BBE8D0F81EBFC19A84BB741
995EE9772DDDF2D6B4A55ACF26FA41F40786532D
ED7B147766C1370367D277F7BA7E354DBDDE5E09
37316B972F5C22D069764800475EED7CD3279802
1DF0B7239E48CF8E7391085BE5B835C892A5B3E8
0323D1C5D565627C32FF08780A59EB45D6C0C7C3
4673475BD3307FE8869ACA0402B861DDE5EC43AC
F38CFC487481D2B0167E5B76F06500BC312081B6
35159C96F695B96773C5C1DCF8206DBE75A83D86

Módulos CORE de Prikormka:
2A64606DB1DB872E7176F0C6C3FF932E2146BFC9
328DE44A4B6140EF49CE1465482EFE0E4C195399
520AA689066D0C69F6FD9C623E263211022CCF21
790367A2032951488FC6F56DCF12062AE56CAA61
551CD9D950A9C610E12451550BD6A3FBF5B00B77
EF3244AB1DF7D74F1FC1D8C3AF26A3D3EA4364A5
1636112D8441A6616B68CBE9DC32DDB5D836BBA1
8A57E5EED18A6DB6F221B1B9E8831FE4A9CAD08C
DCB813E5D2A1C63027AADC7197FD91505FD13380
A360EAC305946FF468E1A33E84ED38176D95CAC9
8F67C4BD2EE7C68249DCD49AD7A3924D3EC6810C
C020EFFD3C7AD06907ECFEA424BE1DCB60C7447D
D2A98115DF0C17648CCB653AF649D24B528B471D
D7EEB8DB22AAD913B38E695A470E8B2F1440D4D3
154AA820D552ABD65C028DED7E970C8DEFA8C237
83B492A2905CE6ACFADE43AB52BF52E6F02FDCD5
4F945A3B3EB058668C3DFC0A8469B42E16C277A7
963963004E4CA0D966D84324EC8ED3694F6A7F5B
9DE8860AD499E64F8BDCFC800DDAFF49D4F948E5
C9C2510654081D621A5B1768520D7D7C04219FCB
9D025A015FDB720C0FDEBCFE54661F3ACED94E3E
D09B6194453BFC59EB438E455D14621B280DF4A6
1A865E934EFF339A826979C70A2FC055E3C9D12F
4C5F412C915FB3F178A81BC4FBDA336F69A22086
7372639A9E5C274DFFAA35ABF4C8E7A0BEBD4305
311672ECB756E52AD396227DD884D1C47234961A
7A22E549BE02F7F4753BB9CBA34079CEB15CA381

6AB00FCABC6BC06586F749F54C4955592285608C
66248AE0A3D6B5091C629343CC535F98E08A2947
0DD8E1922CEB96061C9F6678728DD45CBDC6F675
A093993B9488A9427300B2AC41460BE8164A0F9A
6D861826206D834A224583898BE6AF1A3D46E7CF
64679BDB8A65D278CDA0975F279D8881E1ABD40A
92476C6AE5F976C58D11BDD956878451F361776D
202637EF3C9B236D62BE627C6E1A8C779EB2976B
C41BB97C203D6221FB494D732CB905FF37376622
986E739948E3B5C303F7766F9F9AF3D2E1A5BCA7
3AB61FEC417686AFC1AC430AAF5A17254D05A14A
0D7785E53AB1A7F43902AFF50E7A722C0E0B428F
B5EEAE045F1082438E4C7B7F12F7F4630043A48E
57E345893F508F390F2947E83092A47D845EA445
C9756E95679EAD052D53ADCFA39BB4B1402C9126
D864067BFA52383BC012BA1AAF8FFB893D419C07
CDD58347F873EB7E0BC602DA9930A519683C67C7
DFABE31E58334C873AEDD361D69D5C80016F9F42
625D822EE0D95C6E581B929C6C4E4B44D749D2BB
A224A76DABE62BD7CA055CA1119108AD5812AF06
E4C56D11E84497EEC3E275043E36845EB2F3F57E
B43713CBD307BC12AD7BA61C87975F74221A3439
AED9C3BCA2B42889A9110B92D3D31B5FD3324BDF
6AE2C768D932EDA538983DD7A50CF7DE14BF54D2
BE73A2C17AAE689BC1A20761850374636B67BF0F
80FFA899CB3A6595FAFA66421BCCD6E5AAAD8552
7C5F7296DDDA9B188B572DF348843F822BD6ED21
F9EB705D8A1EDC7FF9B93D9CF9211840C4482865
7979BEC789770860A6F12B7A7D41470DE4AFC873
6DF75137E8966537BB921EAB30DF4F7BC2C6FEB4
2115C50CAF8D1B365D78818DF84A8CE29F7FD9E8
AFDAD724A2C351C750DB43688D107B1300B1D1D4
64002D2C4C6678776C64BB018736C9B0745F47F4
7843CB7DE03C8B564FD72D923B4BD6D28A466A3C
EB4647CA60FEA9049A34EC59D9658946A2C26D9D
ED3D4EEF28174F60F1653F35000B871F6E023D21
860D0CDFC065E91083979DD50A72251C26A638A4
FC2C689C507FED54432AD1726E524B38F52B187A
D219640BA205A7013A23BA19CD6C2B32439F105E
DE60C2A81AE2F3E5DBD2B2D0DBEBDB56FED62F7C
D38FDAE48EABF2642F3327FAC865B079233CC7C6
B23995462751EDFAD19B72BEA4A047CC89533A59
88ED6686CF59F12AA984216EC60097C4BD319007
DEF9B207BFD7C6D4B216DF2B37C33CD851DC7FE1
8D49305FD140B179D2293FBAFF6E7CE46A03AF16
F35B1D2165EC00A56EE6DE89D09963DD3FD02744
B42234F5A5EFB6423E9D4904BA282127F1282C8E
326ADEA3AC1F8FAC3B522E6B47941263DA110A42
3E023A83EAA85A77B935B2D3A00AEB5B1ADCD9CC
129B852E62CB7BF487D5F37E17F6E3CC9A838DB8
F030559F81B8DC3CC0DED6C46C6D1BBB67A2CA65
3C904AFB938EFCF210F388E5AA46379AEADBCD50
D8921385ADAFF131C9D452A4D9BBA2C7D755880E
915F7F5471A94A6E095EE8D90FCFE84E7A5FE1D5
0DB71AA8B51FAACEA7D4C5819EC6AF9C342D02FD
A4847B06E603E90640051FCDD5D1515F007F7BD5
7C9E4CC3F5B260439D69E93376AA668BF32123D0
3246B5F43756DC8DC4438933005DF66A3C8CE25F
E97B383E3CF55D0792F22D57273C18848B849C6E
7C6FA82657B291FAFE423B7B45D0ED732F4D5352
4595EAB593594860985F5FB501B85386F1F1A5B8
45F1F06C3A27CE8329E2BDCDEEA3C530711B5B72
476DCA86DE7AF1F15327084021A3BB7F42818248
70A362985D5237ACD6282E16A238B0FDB1002A1F

73596D1587549DC234588FCB5666BEEFD7C90D81
97958B3124EC5DCAB64DD88A1E97E6B585B04628
B47640C4952ACC2705F7EAD9E8EAA163059FD659
596F945AB52AE0E780905E150ACD2017AB2ECDFC
5CEFFF9C7D016364D40F841CB74D65BB478BA0C6
424DD485FA8572DB84CF6845C27C1F8679A61AEC
099C5611F3BDBB8D453DFBF7967F30891906FF2C
7C2587B85178AD89389D957F11AF1065C46F66DB
840AFB728FDA57195E53F225CB3F6E788B96A579
12ACC64605D4FE2F3CEEEFBD0A7C4FD655E6AEAA

Módulos DOCS_STEALER de Prikormka:
BA434FB6169E8A1785E353EEBF9B907505759A07
A34BD2A059F57FB1FE281A2BD7247A9A72A467B8
04DEB60B6A1D53448EFFB34EA7C55E6916FE32B1
C75D8850273431A41F0EFCF8F74E86BCFE1DFA5A
7C9CB1619FFCF36B32273E1A78A58D817D2B7C8C
A580856FA6AC3159F0A7E91D5992810B953A36A1
5C82CA8B2E8320E6B6C071CCB0D4EF9B03001CAA
7275A6ED8EE314600A9B93038876F853B957B316
9286B96452C519D5E1E74D1CDDBDD76B51F4FBAA
FAB3B3371AA5878B6508DA487735E3A674A9F61B
0D4839F99C30AD76E082851A214A32116CE932A7
652B012E0ACACB78221CAA7A3C3EE461F07264EA

Módulos KEYLOGGER de Prikormka:
BFDCD0A3F7495C43D8D42B4272BDC90695DC44D7
CC42C6BEEB70D3A9BC7E1159C644E54DE2BE5CBC
6A4F24665569DD61FD29AF8FDCB3E2C90961DFF0
D1DA3076830813EC6FFF0B0DE3462BB5B713A090
E6D92C025CF726B08288B6798AEEFCF550D51C31
0B81BA761C6BA88C0AFC682693D99355E55F5A76
0CDC66ACBB5B7D6FAA85F7DF8D747A96CED7A9BD
194316ADC74AEDED98EE2696B4AB54900A6EDF15
45959818DBA4924E129E22CF1B0BDF02C2DD7B49
820EAC424FC27296FE725E1C5DAA8F6C53E104A7
25D6F1EFD758AACE399C6D62A89BE039281CFF69
722E1CDA3C516D43F17A6D4F5F1390D16113BC30
DE966273DD5AD4DAA01562109932EBD39A13A5A2

Módulos SCREENSHOTS de Prikormka:
645DFA35E41F6442793CF7647A75956E05563DE8
AD74ABEA34A20D0196A152E6668E3C29135B22D4

Módulos MICROPHONE de Prikormka:
FCE83DF7018A49072F9A28A8E135EB00C011D9EB
2C76974722287C7CDB0FCA2BC6CCEDEE62E77D24

Módulos SKYPE de Prikormka:
C3AA3DBD33751F85002F2F65562098F516737435
2A0EA9E0F3F8E6507D212640594ACF52910275E9
1BB3BBCA79BA45E4215DFC2A6960E03BA60A2B71
0CB528C69706A6513A0E70D3A07A75822F79E6EC
423BCEFC82A14258BDC2CD9740454D28F894DC06
FEAB6E92B905114980B5633F8742E4A7DCD0B4FA
BB6CE0957F7E8430007FA4DE1E47C190E1C97AC5
658DF9B4BB13459A9507466BB7D22B723C85D1C5
6C24E244A0DDA2CADED4D1B5CC8B820A46DC19F4

Módulos LOGS_ENCRYPTER de Prikormka:
D5C2C7C3D670D63AD6998848747A0418665EA2CB
352C36ED1BF7EB74C9649615F9A40C13D80EE55D
6740A385AB33B9CC3EC22FB7971F93538BE44997

22F10F17AB9F18D9BF1FE9EEEA413A9787B29D4C
E95458CA9663E4FAB94DD232121D5E994A76015D
2BD3FE012486BD89C87858CC4C3DC9D86742738C

Módulos GEOLOCATION de Prikormka:
50CCCD576A815AC8EFFB160A628646C876DF8CB0

Módulos OS_INFO de Prikormka:
4B8EE967F44ECA2EEB3B8420A858CECFE0231208
72C17994336FE4E1B3CF0D7A6CBC45AA43A8DDF0
824F0E198A8A6E08FB95920AEF06870A6305FE3F
6C902496AC1FEF60D343B03822F49DB5F66BE038

Módulos PASSWORDS de Prikormka:
B986114C5173052FCB9583A55D5099D99B709352
17F5E1FC52D6C617CD81B0983B70FAC7A60F528C

Módulos FILE_TREE de Prikormka:
3EDD14E6FA0297ED3162D7F119D8D126662ED28B
2A5AF8E43887051C1F1B488756AAC204B95561CE
4E40286676FCBAC48070BA86B72761A21AC2466C
3E4BE58421DBAEA7651DA13B16CB900DB82A7DEF
D1396938E981DD807103B7B9F9442B99952C21AA
74CDA4D4C776CA2A661AC49B6D0E0F0560380A04
8EFDC716FDFD704EC0296860E61AFF9C952946D4
93E196B59771647828BBC3C3B61831150FE1FE02
8384ED4EA9E299306F15A1082231C427A8742271
6E70BE32954E41FAFFC496EAF890B279832B4530
8EA98A8D3D8F62C4543B3DD36E6D6F79F1ACB9E7