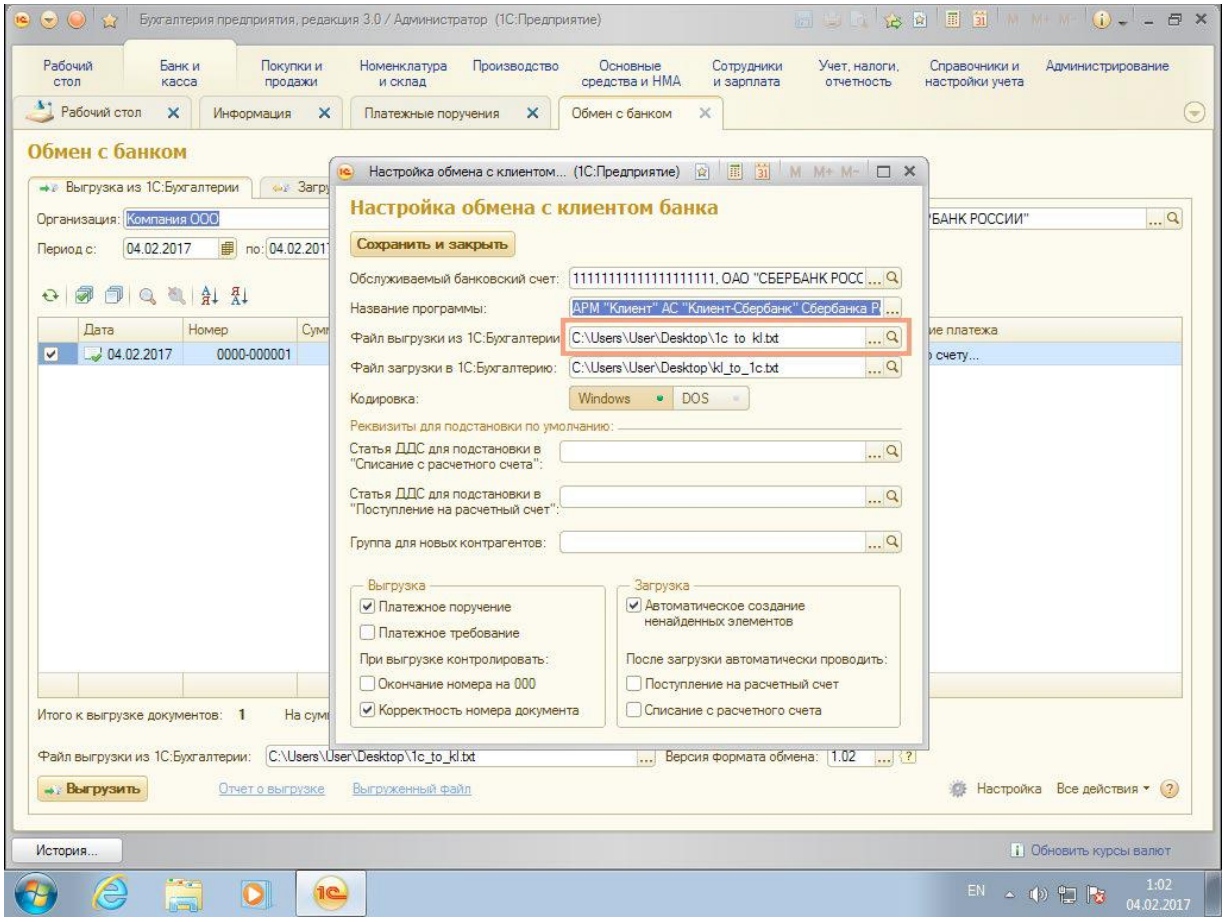
АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# Кибергруппа RTM специализируется на краже средств у российских компаний

*27 февраля 2017 года*

Известно несколько кибергрупп, специализирующихся на краже средств у российских компаний. Мы наблюдали атаки с применением лазеек в системах безопасности, открывающих доступ в сети целевых объектов. Получив доступ, атакующие изучают структуру сети организации и развертывают собственные инструменты для кражи средств. Классический пример этого тренда – хакерские группировки Buhtrap, Cobalt и Corkow.




Группа RTM, которой посвящен этот отчет, является частью данного тренда. Она использует специально разработанные вредоносные программы, написанные на Delphi, которые мы рассмотрим подробнее в следующих разделах. Первые следы этих инструментов в системе телеметрии ESET обнаружены в конце 2015 года. По мере необходимости группа загружает в зараженные системы различные новые модули. Атаки нацелены на пользователей систем ДБО в России и некоторых соседних странах.

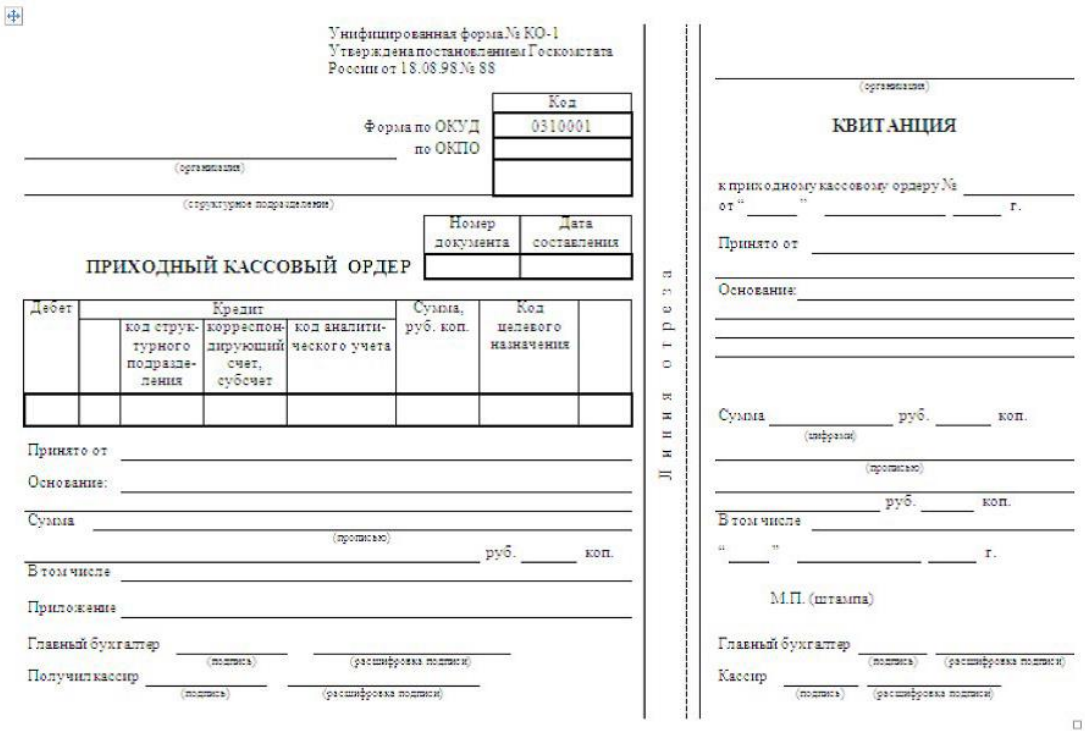
## 1. Цели

Кампания RTM ориентирована на корпоративных пользователей – это очевидно из процессов, которые атакующие пытаются обнаружить в скомпрометированной системе. В фокусе бухгалтерское ПО для работы с системами дистанционного банкинга.

Список процессов, интересующих RTM, напоминает соответствующий список группы Buhtrap, но при этом у группировок различаются векторы заражения. Если Buhtrap чаще использовала поддельные страницы, то RTM – атаки drive-by download (атаки на браузер или его компоненты) и рассылку спама по электронной почте. По данным телеметрии, угроза нацелена на Россию и несколько ближайших стран (Украину, Казахстан, Чехию, Германию). Тем не менее, в связи с использованием механизмов массового распространения, обнаружение вредоносного ПО за пределами целевых регионов не удивляет.

Общее число обнаружений вредоносного ПО сравнительно невелико. С другой стороны, в кампании RTM используются сложные программы, что свидетельствует о высокой таргетированности атак.

Мы обнаружили несколько документов-приманок, используемых RTM, включая несуществующие контракты, счет-фактуры или документы налогового учета. Характер приманок в сочетании с типом программного обеспечения, на которое нацелена атака, указывает на то, что атакующие «заходят» в сети российских компаний через бухгалтерию. По той же схеме действовала группа Buhtrap в 2014-2015 гг.



Унифицированная форма № КО-1
Утверждена постановлением Госкомстата России от 18.08.98 № 88

Код
Форма по ОКУД 0310001
по ОКПО

(организация)

(структурное подразделение)

Номер документа | Дата составления

ПРИХОДНЫЙ КАССОВЫЙ ОРДЕР

| Дебет | Кредит | | | | Сумма, руб. коп. | Код целевого назначения | |
|---|---|---|---|---|---|---|---|
| | | код структурного подразделения | корреспондирующий счет, субсчет | код аналитического учета | | | |
| | | | | | | | |

Принято от
Основание:
Сумма
(прописью)
руб. коп.
В том числе
Приложение
Главный бухгалтер (подпись) (расшифровка подписи)
Получил кассир (подпись) (расшифровка подписи)

Линия отреза

(организация)

КВИТАНЦИЯ

к приходному кассовому ордеру № от "" г.
Принято от
Основание:
Сумма руб. коп.
(цифрами)
(прописью)
руб. коп.
В том числе
"" г.
М.П. (штампа)
Главный бухгалтер (подпись) (расшифровка подписи)
Кассир (подпись) (расшифровка подписи)

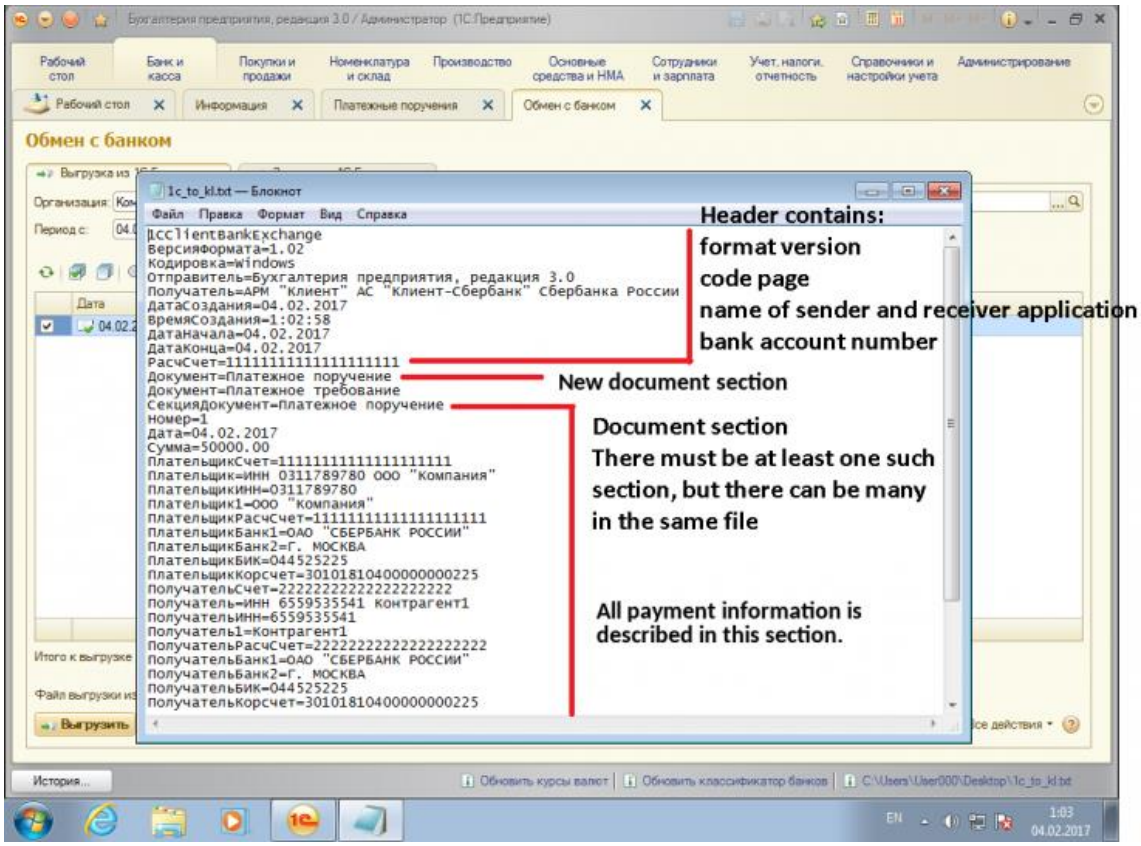
В ходе исследования нам удалось взаимодействовать с несколькими C&C-серверами. Полный список команд перечислим в следующих разделах, а пока можем сказать, что клиент передает

данные с кейлоггера напрямую на сервер атакующих, с которого затем поступают дополнительные команды.

Тем не менее, дни, когда вы могли просто подключиться к командному серверу и собрать все интересующие данные, прошли. Мы воссоздали реалистичные файлы журналов, чтобы получить несколько релевантных команд от сервера.

Первая из них – запрос боту для передачи файла 1c_to_kl.txt – транспортного файла программы «1С: Предприятие 8», появление которого активно отслеживает RTM. 1С взаимодействует с системами ДБО путем выгрузки данных об исходящих платежах в текстовый файл. Далее файл направляется в систему ДБО для автоматизации и исполнения платежного поручения.

Файл содержит платежные реквизиты. Если злоумышленники изменят данные об исходящих платежах, перевод уйдет по подложным реквизитам на счета атакующих.




Примерно через месяц после запроса этих файлов с командного сервера мы наблюдали загрузку в скомпрометированную систему нового плагина 1c_2_kl.dll. Модуль (библиотека DLL) предназначен для автоматического анализа файла выгрузки путем проникновения в процессы бухгалтерского ПО. Мы подробно опишем его в следующих разделах.

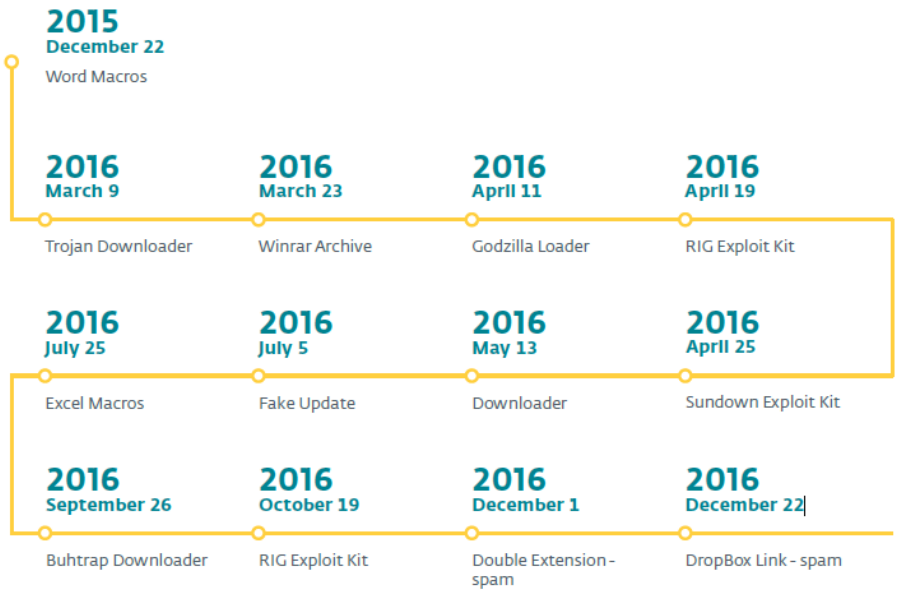
Интересно, что «ФинЦЕРТ» Банка России в конце 2016 года выпустил бюллетень с предупреждением о киберпреступниках, использующих файлы выгрузки 1c_to_kl.txt. Разработчики из 1С также знают об этой схеме, они уже выступили с официальным заявлением и перечислили меры предосторожности.

С командного сервера загружались и другие модули, в частности, VNC (его 32 и 64-битные версии). Он напоминает модуль VNC, который ранее использовался в атаках с трояном Dridex.

Данный модуль предположительно используется для удаленного подключения к зараженному компьютеру и детальному изучению системы. Далее атакующие пытаются перемещаться в сети, извлекая пароли пользователей, собирать информацию и обеспечивать постоянное присутствие вредоносного ПО.

## 2. Векторы заражения

На следующем рисунке представлены векторы заражения, обнаруженные в период изучения кампании. Группа использует широкий спектр векторов, но преимущественно атаки drive-by download и спам. Эти инструменты удобны для таргетированных атак, поскольку в первом случае атакующие могут выбирать сайты, посещаемые потенциальными жертвами, во втором – отправлять электронную почту с вложениями напрямую нужным сотрудникам компаний.



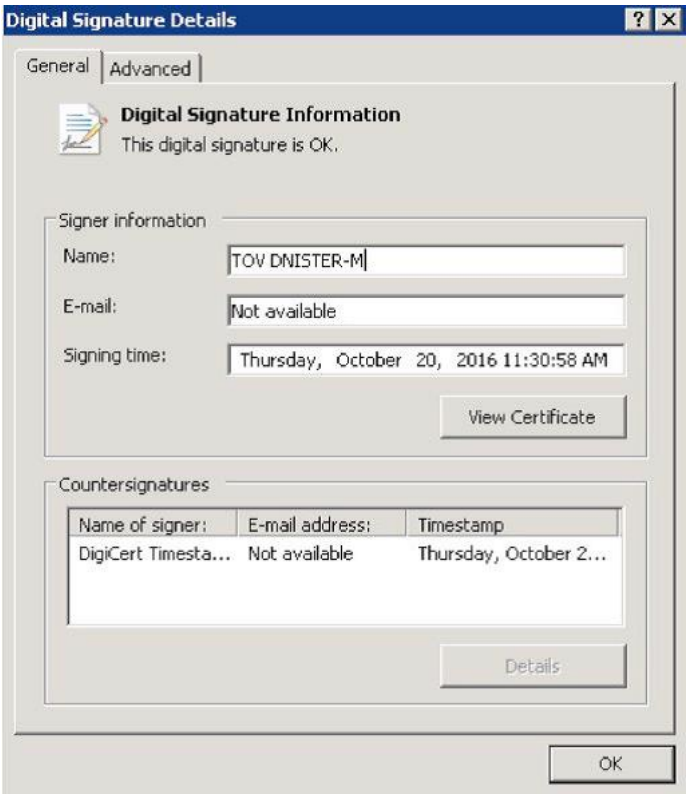

Вредоносное ПО распространяется в нескольких каналах, включая наборы эксплойтов RIG и Sundown или спам-рассылки, что указывает на связи атакующих с другими киберзлоумышленниками, предлагающими эти сервисы.

## 2.1. Как связанны RTM и Buhtrap?

Кампания RTM очень похожа на компанию Buhtrap. Закономерный вопрос: как они связаны друг с другом?

В сентябре 2016 года мы наблюдали распространение образца RTM при помощи загрузчика Buhtrap. Кроме того, мы нашли два цифровых сертификата, используемых как в Buhtrap, так и RTM.

Первый, якобы выданный компании DNISTER-M, использовался для цифровой подписи второй формы Delphi (SHA-1: 025C718BA31E43DB1B87DC13F94A61A9338C11CE) и DLL Buhtrap (SHA-1: 1E2642B454A2C889B6D41116CCDBA83F6F2D4890).




Второй, выданный компании Bit-Tredj, использовался для подписи загрузчиков Buhtrap (SHA-1: 7C1B6B1713BD923FC243DFEC80002FE9B93EB292 и B74F71560E48488D2153AE2FB51207A0AC206E2B), а также выгрузки и инсталляции компонентов RTM.

| Company Name | Validity Period | Thumbprint & Serial |
|---|---|---|
| Bit-Tredj | 29/05/2016 – 30/05/2017 | Thumbprint<br>2c14b428c4f5e260db13cff1b6b28d22beb59d7f<br>Serial<br>54460e1fcd612cd3377ac2cd76e4240f |
| TOV DNISTER-M | 19/04/2016 – 20/04/2017 | Thumbprint<br>457880da8899679870ad5b87312d882c006c9559<br>Serial<br>2567a463a84bb9d4207a11ec979205ac |
| Kit-SD, OOO | 21/06/2016 – 22/06/2017 | Thumbprint<br>b79d75191b3c0e3742b42c82e0a40dff9976708a<br>Serial<br>1e21a4adcda618adc7b53193ef4aaf62 |

Операторы RTM используют сертификаты, общие с другими семействами вредоносного ПО, но у них есть и уникальный сертификат. По данным системы телеметрии ESET, он выдан компании Kit-SD и использовался только для подписи некоторых вредоносных программ RTM (SHA-1: 42A4B04446A20993DDAE98B2BE6D5A797376D4B6).

RTM использует такой же, как и у Buhtrap загрузчик, компоненты RTM загружается из инфраструктуры Buhtrap, поэтому у групп похожие сетевые индикаторы. Тем не менее, по нашим оценкам, RTM и Buhtrap – разные группировки, как минимум, потому что RTM распространяется разными способами (не только при помощи «чужого» загрузчика).

Несмотря на это, хакерские группировки используют схожие принципы работы. Они нацелены на предприятия, использующие бухгалтерское ПО, схожим образом собирают информацию о системе, ищут устройства чтения смарт-карт и разворачивают массив вредоносных инструментов для слежки за жертвами.

## 3. Эволюция

В этом разделе мы рассмотрим разные версии вредоносного ПО, обнаруженные в ходе исследования.

## 3.1. Версионность

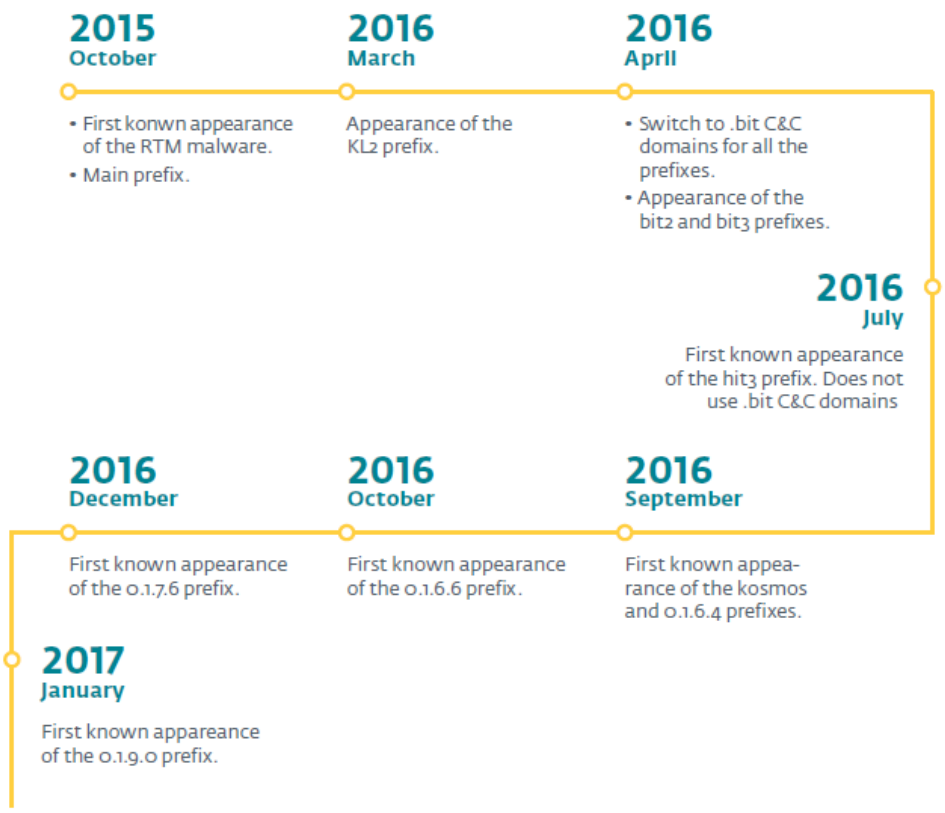
RTM хранит конфигурационные данные в разделе реестра, наиболее интересна часть botnet-prefix. Список всех значений, которые мы видели в изученных образцах, представлена в таблице ниже.

| 0.1.6.4 | 0.1.6.6 | 0.1.7.6 | 0.1.9.0 |
|---|---|---|---|
| bit | bit2 | bit3 | hit3 |
| mtr | KL2 | kosmos | main |

Возможно, значения могут быть использованы для записи версий вредоносной программы. Тем не менее, мы не заметили особых различий между версиями, такими как bit2 и bit3, 0.1.6.4 и 0.1.6.6. Более того, один из префиксов существует с самого начала и превратился из типичного домена C&C в .bit домен, как будет показано далее.

## 3.2. График

Используя данные телеметрии, мы создали график появления образцов.



## 4. Технический анализ

В этом разделе мы опишем главные функции банковского трояна RTM, включая механизмы устойчивости, собственную версию алгоритма RC4, сетевой протокол, шпионский функционал и некоторые другие возможности. В частности, мы сосредоточимся на образцах SHA-1 AA0FA4584768CE9E16D67D8C529233E99FF1BBF0 и 48BC113EC8BA20B8B80CD5D4DA92051A19D1032B.

## 4.1. Установка и сохранение

### 4.1.1. Реализация

Ядро RTM – DLL, библиотека загружается на диск при помощи .EXE. Исполняемый файл, как правило, упакован и содержит код DLL. После запуска он извлекает DLL и запускает ее, используя следующую команду:

```
rundll32.exe "%PROGRAMDATA%\Winlogon\winlogon.lnk",DllGetClassObject
```

```
host
```

### 4.1.2. DLL

Основная DLL всегда загружается на диск как winlogon.lnk в папке %PROGRAMDATA%\Winlogon. Это расширение файла как правило связано с ярлыком, но файл на самом деле является DLL-библиотекой, написанной на Delphi, названной разработчиком core.dll, как указано на рисунке ниже.


Пример названия DLL F4C746696B0F5BB565D445EC49DD912993DE6361

После запуска троян активирует механизм устойчивости. Это можно реализовать двумя разными способами – в зависимости от привилегий жертвы в системе. При наличии прав администратора, троян добавляет запись Windows Update в реестр HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Команды, содержащиеся в Windows Update, будут выполняться в начале сеанса пользователя.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Windows Update [REG_SZ] = rundll32.exe "%PROGRAMDATA%\winlogon.lnk",DllGetClassObject host

Троян также пытается добавить задачу в Планировщик заданий Windows. Задача запустит DLL-библиотеку winlogon.lnk с теми же параметрами, как указано выше. Права обычного пользователя позволяют трояну добавить запись Windows Update с теми же данными в реестр HKCU\Software\Microsoft\Windows\CurrentVersion\Run\:

```
rundll32.exe "%PROGRAMDATA%\winlogon.lnk",DllGetClassObject host
```

## 4.2. Модифицированный алгоритм RC4

Несмотря на известные недостатки, алгоритм RC4 регулярно используется авторами вредоносных программ. Тем не менее, создатели RTM немного видоизменили его – вероятно, чтобы усложнить задачу вирусных аналитиков. Модифицированная версия RC4 широко используется во вредоносных инструментах RTM для шифрования строк, сетевых данных, конфигурации и модулей.

### 4.2.1. Различия

Оригинальный алгоритм RC4 включает два этапа: инициализацию s-блока (она же KSA – Key-Scheduling Algorithm) и генерацию псевдослучайной последовательности (PRGA – Pseudo-Random Generation Algorithm). Первый этап предполагает инициализацию s-блока с использованием ключа, на втором этапе исходный текст обрабатывается при помощи s-блока для шифрования.

Авторы RTM добавили промежуточный этап между инициализацией s-блока и шифрованием. Дополнительный ключ является переменной и задается в то же время, что и данные для шифрования и дешифрования. Функция, выполняющая этот дополнительный шаг, представлена на рисунке ниже.

```
unsigned int __fastcall TCrypt_RC4_variant_xor_stable(int a1, char *s_table, char
*xored_s_table, int iv)
{
  unsigned int i; // eax@1
  unsigned int v5; // eax@2
  i = 0;
  do
  {
    *&xored_s_table[i] = iv ^ *&s_table[i];
    v5 = i + 4;
    *&xored_s_table[v5] = iv ^ *&s_table[v5];
    v5 += 4;
    *&xored_s_table[v5] = iv ^ *&s_table[v5];
    v5 += 4;
    *&xored_s_table[v5] = iv ^ *&s_table[v5];
    v5 += 4;
    *&xored_s_table[v5] = iv ^ *&s_table[v5];
    v5 += 4;
    *&xored_s_table[v5] = iv ^ *&s_table[v5];
    v5 += 4;
    *&xored_s_table[v5] = iv ^ *&s_table[v5];
    v5 += 4;
    *&xored_s_table[v5] = iv ^ *&s_table[v5];
    v5 += 4;
    *&xored_s_table[v5] = iv ^ *&s_table[v5];
    i = v5 + 4;
  }
  while ( i < 255 );
  return i;
}
```

### 4.2.2. Шифрование строк

На первый взгляд, в основной DLL библиотеке есть несколько доступных для чтения строк. Остальные зашифрованы с использованием описанного выше алгоритма, структура которого показана на следующем рисунке. Мы нашли больше 25 различных ключей RC4 для шифрования строк в проанализированных образцах. Ключ XOR различается для каждой строки. Значение цифрового поля, разделяющего строки, всегда 0xFFFFFFFF.

В начале исполнения RTM расшифровывает строки в глобальную переменную. Когда это необходимо для доступа к строке, троян динамически вычисляет адрес расшифрованных строк на основе базового адреса и смещения.

Строки содержат интересную информацию о функциях вредоносного ПО. Некоторые примеры строк представлены в разделе 6.8.

```
struct struct_encrypted_string
{
        int separator; //constant - 0xFFFFFFFF

        int size;

        int xor_key[4];

        char encrypted_data[size];

};
```

## 4.3. Сеть

Способ контакта вредоносного ПО RTM с командным сервером меняется от версии к версии. Первые модификации (октябрь 2015 – апрель 2016) использовали для обновления списка команд традиционные доменные имена вместе с каналом RSS на livejournal.com.

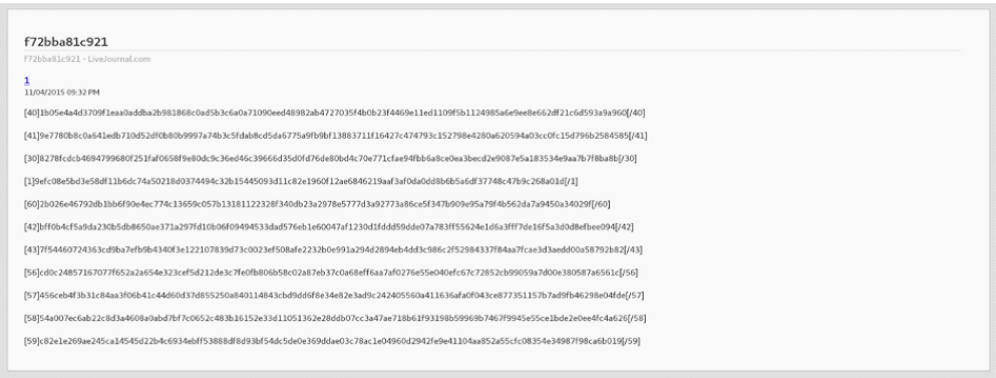
С апреля 2016 года мы наблюдали в данных телеметрии переход на домены .bit. Это подтверждает дата регистрации доменов – первый домен RTM fde05d0573da.bit был зарегистрирован 13 марта 2016 года.

Все URL адреса, которые мы видели во время наблюдения за кампанией, имели общий путь: /r/z.php. Он довольно необычен, и это поможет определить запросы RTM в сетевых потоках.

### 4.3.1. Канал для команд и управления

Старые образцы использовали этот канал для обновления своего списка командных серверов. Хостинг находится на livejournal.com, на момент подготовки отчета он оставался на URL hxxp://f72bba81c921(.)livejournal(.)com/ data/rss.

Livejournal – российско-американская компания, предоставляющая платформу для блогов. Операторы RTM создают ЖЖ-блог, в котором размещают статью с кодированными командами – см. скриншот.




Строки команд и управления кодируются с помощью модифицированного алгоритма RC4 (раздел 4.2). Текущая версия (ноябрь 2016 года) канала содержит следующие адреса сервера команд и управления:

- hxxp://cainmoon(.)net/r/z.php

- hxxp://rtm(.)dev/0-3/z.php
- hxxp://vpntap(.)top/r/z.php

### 4.3.2. Домены .bit

В большинстве свежих образцов RTM авторы подключаются к C&C доменам, использующим домен верхнего уровня TLD .bit. Его нет в списке доменов верхнего уровня ICANN (Корпорации по управлению доменными именами и IP-адресами). Вместо этого, он использует систему Namecoin, построенную на основе технологии Bitcoin. Авторы вредоносного ПО не часто используют TLD .bit для своих доменов, хотя пример такого использования ранее наблюдался в версии бот-сети Necurs.

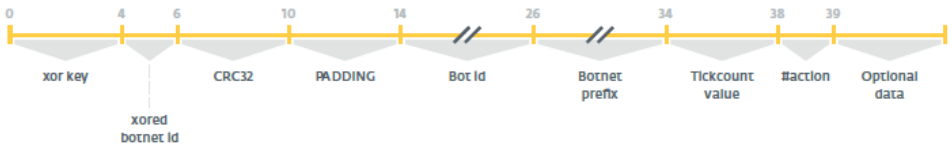
В отличие от Bitcoin, пользователи распределенной базы Namecoin имеют возможность сохранять данные. Основное применение этой особенности – домен верхнего уровня .bit. Можно регистрировать домены, которые будут храниться в распределенной базе данных. Соответствующие записи в базе содержат IP-адреса, разрешенные доменом. Данный TLD «устойчив к цензуре», поскольку только регистрирующее лицо может изменить разрешение домена .bit. Это означает, что прекратить работу вредоносного домена при использовании этого вида TLD намного труднее.

Троян RTM не встраивает ПО, необходимое для прочтения распределенной базы Namecoin. Он использует центральные серверы DNS, такие как dns.dot-bit.org или серверы OpenNic, для разрешения доменов .bit. Следовательно, он имеет ту же устойчивость, что и у серверов DNS. Мы наблюдали, что некоторые командные домены перестали определяться после упоминания в записи блога.

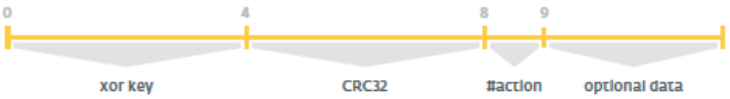
Другое преимущество TLD .bit для хакеров – стоимость. Чтобы зарегистрировать домен, операторам нужно заплатить всего 0,01 НК, что соответствует 0,00185 долларов (на 5 декабря 2016 года). Для сравнения: домен.com стоит как минимум 10 долларов.

### 4.3.3. Протокол

Для связи с командным сервером RTM использует запросы HTTP POST с данными, форматированными при помощи пользовательского протокола. Значение пути всегда /r/z.php; пользовательский агент Mozilla/5.0 (совместимый; MSIE 9.0; Windows NT 6.1; Trident/5.0). В запросах на сервер данные форматируются, как следует далее, где значения смещения выражаются в байтах:




Байты с 0 до 6 не кодируются; байты, начиная с 6, кодируются при помощи модифицированного алгоритма RC4. Структура пакета ответов командного сервера проще. Кодируются байты с 4 до размера пакета.



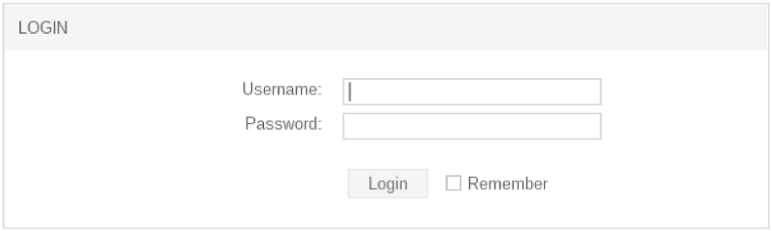
Список возможных значений байтов действия представлен в таблице ниже:

| Значение | Действие |
|---|---|
| **0** | OK (ACK) |
| **1** | Основной компонент. Опционально: строка содержит команду |
| **3** | Неопознанный тип запроса |
| **4** | Непредвиденный тип запроса |
| **5** | Установить модуль |
| **6** | Выполнить загруженный исполняемый модуль |
| **7** | Выполнить загруженный исполняемый модуль. В отсутствии прав администратора малварь попытается повысить привилегии, используя метод, описанный в разделе 4.8.2 |
| **8** | Загрузить DLL |
| **9** | Загрузить и выполнить исполняемый модуль MZ в памяти без использования файла |
| **10** | Добавить сертификат в Windows Store |
| **11** | Самообновление |
| **12** | Записать файл в папку приложений (как правило C:\ProgramData) |

Вредоносная программа всегда вычисляет CRC32 расшифрованных данных и сравнивает полученное с тем, что представлено в пакете. Если они отличаются, троян сбрасывает пакет. Дополнительные данные могут содержать различные объекты, включая файл PE, файл для поиска в файловой системе или новые командные URL.

### 4.3.4. Панель

Мы заметили, что RTM использует панель на командных серверах. Скриншот ниже:




## 4.4. Характерный признак

RTM – типичный банковский троян. Неудивительно, что операторам нужна информация о системе жертвы. С одной стороны, бот собирает общие сведения об ОС. С другой – выясняет, содержит ли скомпрометированная система атрибуты, связанные с российскими системами ДБО.

### 4.4.1. Общая информация

Когда вредоносное ПО установлено или запущено после перезагрузки, на командный сервер уходит отчет, содержащий общую информацию, включая:

- часовой пояс;
- язык системы по умолчанию;
- полномочия авторизованного пользователя;
- уровень целостности процесса;
- имя пользователя;
- имя компьютера;
- версию ОС;
- дополнительные установленные модули;
- установленную антивирусную программу;
- список считывателей смарт-карт.

## 4.4.2. Система дистанционного банковского обслуживания

Типичная цель трояна – система ДБО, и RTM – не исключение. Один из модулей программы называется TBdo, он выполняет разные задачи, включая сканирование дисков и истории посещений.

Сканируя диск, троян проверяет, установлено ли на машине банковское ПО. Полный список целевых программ – в таблице ниже. Обнаружив интересующий файл, программа отправляет информацию на командный сервер. Следующие действия зависит от логики, заданной алгоритмами командного центра (C&C).

| | | | | | |
|---|---|---|---|---|---|
| _ftcgpk.exe | 1cv8s.exe | CLBANK.EXE | iscc.exe | sbis.dll | wclnt.exe |
| 1cv7.exe | bicrypt | client.jks | ISClient.exe | sbis.exe | webmoney.exe |
| 1cv7l.exe | bssax.ocx | faktura | maratl.exe | SGBClient.exe | winpost.exe |
| 1cv7s.exe | cbmain.ex | ifobsclient.exe | npbssplugin.dll | SGBClient.exe | |
| 1cv8.exe | cbsmain.dll | internetbanktools.exe | qiwicashier.exe | transaq.exe | |
| 1cv8c.exe | cft - bank client | intpro.exe | rclient.exe | wallet.dat | |

RTM ищет также шаблоны URL адресов в истории посещений браузера и в открытых вкладках. Кроме того, программа изучает использование функций FindNextUrlCacheEntryA и FindFirstUrlCacheEntryA, а также проверяет каждый вход на соответствие URL адресам одному из нижеперечисленных шаблонов:

| | | |
|---|---|---|
| bsi.dll? | faktura.ru | elba.raiffeisen |
| online.payment.ru | /iclient/ | handybank. |
| bankline.ru | ibank2 | wupos.westernunion |
| /ic/login.zhtml | bco.vtb24.ru | online.sberbank |
| /servlets/ibc | elbrus.raiffeisen | |

Обнаружив открытые вкладки, троян обращается к Internet Explorer или Firefox через механизм динамического обмена данными (DDE), чтобы проверить, соответствует ли вкладка шаблону.

Проверка истории посещений и открытых вкладок выполняется в цикле WHILE (цикле с предусловием) с перерывом в 1 секунду между проверками. Другие данные, которые отслеживаются в режиме реального времени, рассмотрим в разделе 4.5.

Если шаблон найден, программа сообщает об этом на командный сервер при помощи списка строк из следующей таблицы:

| | | | | |
|---|---|---|---|---|
| BSS | RosBank | BiCrypt | SberBank_Fiz | ISCC |
| BSS_PC | SberBank_BO | VTB24 | CFT | WebMoney |
| iBank2_PC | INIST | SGB | WinPost | XTC |
| Faktura | Inversion | Raiffeisen | SBIS | iFOBS |
| PCB | Interbank | HandyBank | CIBank | TRANSAQ |
| InterPro | iBank2 | WU | QiwiCashier | OSMP |

## 4.5. Мониторинг

Во время работы трояна информация о характерных особенностях зараженной системы (включая данные о наличии банковского ПО) отправляется на командный сервер. Снятие цифровых отпечатков происходит, когда RTM впервые запускает систему мониторинга сразу после исходного сканирования ОС.

### 4.5.1. Дистанционное банковское обслуживание

Модуль TBdo также отвечает за мониторинг процессов, связанных с банкингом. Он использует динамический обмен данными, чтобы в момент первоначального сканирования проверить вкладки в Firefox и Internet Explorer. Другой модуль TShell используется для мониторинга командных окон (Internet Explorer или проводника).

Модуль использует интерфейсы COM IShellWindows, iWebBrowser, DWebBrowserEvents2 и IConnectionPointContainer для мониторинга окон. Когда пользователь переходит на новую веб-страницу, вредоносная программа отмечает это. Затем она сравнивает URL адрес страницы с вышеперечисленными шаблонами. Обнаружив совпадение, троян делает шесть последовательных скриншотов с интервалом в 5 секунд и отправляет их на командный сервер C&C. Программа также проверяет некоторые названия окон, относящихся к банковскому ПО – полный список ниже:

| Window name | Class name |
|---|---|
| CIBank | SunAwtFrame |
| CIBank | SunAwtDialog |
| Логин (Login) | TLoginWindow |
| Null | TfmISClient |
| Ключ электронной подписи (Key Electronic Signature) | TInitialForm |

### 4.5.2. Смарт-карта

RTM позволяет мониторить считыватели смарт-карт, соединенных с зараженными компьютерами. Эти устройства используются в некоторых странах для сверки платежных поручений. Если устройства этого типа присоединяются к компьютеру, для трояна это может указывать на использование машины для банковских транзакций.

В отличие от других банковских троянов, RTM не может взаимодействовать с такими смарт-картами. Возможно, этот функционал входит в дополнительный модуль, который мы пока не видели.

### 4.5.3. Клавиатурный шпион

Важная часть мониторинга зараженного ПК – перехват нажатия клавиш. Создается впечатление, что разработчики RTM не пропускают никакой информации, поскольку отслеживают не только обычные клавиши, но и виртуальную клавиатуру и буфер обмена.

Для этого используется функция SetWindowsHookExA. Атакующие регистрируют нажатые клавиши или клавиши, соответствующие виртуальной клавиатуре, вместе с именем и датой программы. Затем буфер направляется на командный C&C сервер.

Для перехвата буфера обмена используется функция SetClipboardViewer. Хакеры регистрируют содержимое буфера обмена, когда данные представляют собой текст. Перед отправкой буфера на сервер также регистрируется имя и дата.

### 4.5.4. Скриншоты

Еще одна функция RTM – перехват скриншотов. Возможность применяется, когда модуль мониторинга окон обнаруживает интересующий сайт или банковское ПО. Скриншоты выполняются при помощи библиотеки графических изображений и передаются на командный сервер.

## 4.6. Деинсталляция

C&C сервер может приостановить работу вредоносного ПО и очистить компьютер. Команда позволяет очистить файлы и записи реестра, созданные во время работы RTM. Затем при помощи DLL-библиотеки осуществляется удаление вредоносного ПО и файла winlogon, после чего команда выключает компьютер. Как показано на рисунке ниже, DLL-библиотека удаляется разработчиками при помощи erase.dll.


Сервер может отправить трояну деструктивную команду uninstall-lock. В этом случае при наличии прав администратора RTM удалит загрузочный сектор MBR на жестком диске. Если это не получится, троян попытается сместить загрузочный сектор MBR на случайный сектор – тогда компьютер после выключения не сможет загрузить ОС. Это может привести к полной переустановке ОС, то есть уничтожению улик.

В отсутствие полномочий администратора вредоносное ПО записывает .EXE, закодированный в основной библиотеке DLL RTM. Исполняемый файл выполняет код, необходимый для выключения компьютера, и регистрирует модуль в разделе реестра HKCU\CurrentVersion\Run. Каждый раз, когда пользователь начинает сессию, компьютер немедленно выключается.

## 4.7. Файл конфигурации

По умолчанию, RTM почти не имеет файла конфигурации, но командный сервер может отправить значения конфигурации, которые будут храниться в реестре и использоваться программой. Список ключей конфигурации представлен в таблице ниже:

| | | |
|---|---|---|
| keylogger.last-data | botnet-id | cc.url.1 |
| keylogger.last-wnd-caption | cc.connect-interval | cc.url.2 |
| keylogger.last-exe-path | scan-files | scards.monitoring-interval |
| botnet-prefix | post-install-report | dbo.detected |
| scan-files | multiinstance-off | post-install-report-url |
| modules-data.%modulename% | keylogger-off | dbo-detector-off |
| scard-off | modules-off | modules.%modulename% |

Конфигурация хранится в ключе реестра Software[Pseudo-random string]. Каждое значение соответствует одной из строк, представленных в предыдущей таблице. Значения и данные кодируются при помощи алгоритма RC4 в RTM.

Данные имеют ту же структуру, что сеть или строки. Четырехбайтный ключ XOR добавляется в начале кодированных данных. Для значений конфигурации ключ XOR отличается и зависит от размера значения. Он может вычисляться следующим образом:

xor_key = (len(config_value) << 24) | (len(config_value) << 16)
| len(config_value)| (len(config_value) << 8)

## 4.8. Другие функции

Далее рассмотрим другие функции, которые поддерживает RTM.

### 4.8.1. Дополнительные модули

Троян включает дополнительные модули, являющиеся файлами DLL. Модули, отправляемые с командного C&C сервера, могут выполняться как внешние программы, отражаться в оперативной памяти и запускаться в новых потоках. Для хранения модули сохраняются в файлах .dtt и кодируются при помощи алгоритма RC4 с тем же ключом, который используется для коммуникаций сети.

Пока мы наблюдали установку модуля VNC (8966319882494077C21F66A8354E2CBCA0370464), модуля извлечения данных браузера (03DE8622BE6B2F75A364A275995C3411626C4D9F) и модуля 1c_2_kl (B1EE562E1F69EFC6FBA58B88753BE7D0B3E4CFAB).

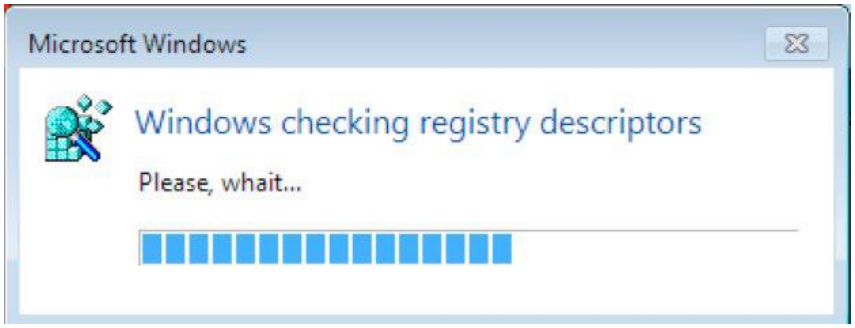
Для загрузки модуля VNC командный сервер направляет команду, запрашивая соединения с сервером VNC по определенному IP-адресу в порте 44443. Плагин извлечения данных браузера выполняет TBrowserDataCollector, который может считывать историю посещений IE. Затем отправляет полный список посещенных URL адресов на командный C&C сервер.

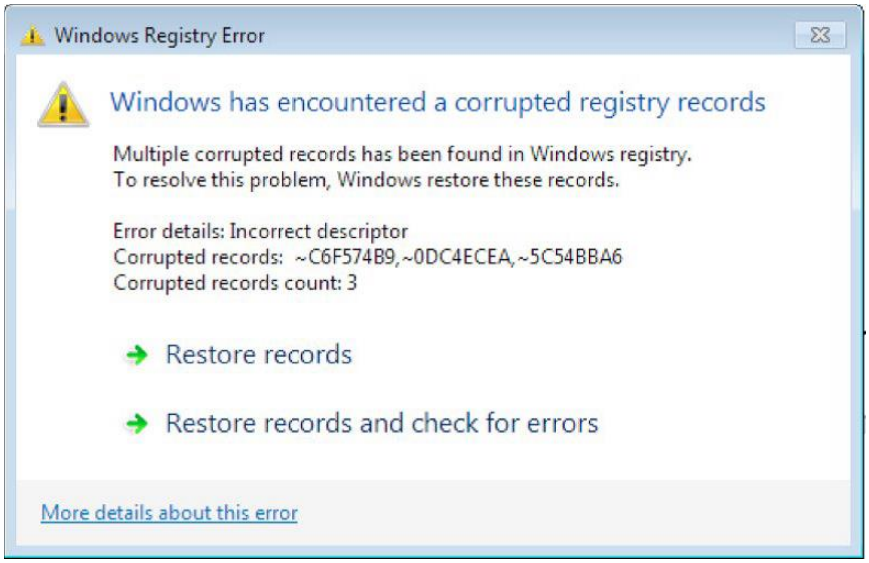
Последний обнаруженный модуль называется 1c_2_kl. Он может взаимодействовать с программным пакетом 1C Предприятие. Модуль включает две части: основную часть – DLL и два агента (32-х и 64-х битные), которые будут внедряться в каждый процесс, регистрируя привязку к WH_CBT. Внедрившись в процесс 1C, модуль привязывает функции CreateFile и WriteFile. Когда бы не вызывалась привязанная функция CreateFile, модуль хранит в памяти путь файла 1c_to_kl.txt. После перехвата вызова WriteFile, он вызывает функцию WriteFile и отправляет путь файла 1c_to_kl.txt на основной модуль DLL, передавая ему созданное сообщение Windows WM_COPYDATA.

Основной модуль DLL открывает и анализирует файл для определения платежных поручений. Он распознает сумму и номер транзакций, содержащиеся в файле. Эта информация направляется на командный сервер. Мы считаем, что этот модуль в данный момент находится в разработке, поскольку он содержит сообщение об отладке и не может автоматически модифицировать 1c_to_kl.txt.

## 4.8.2. Повышение привилегий

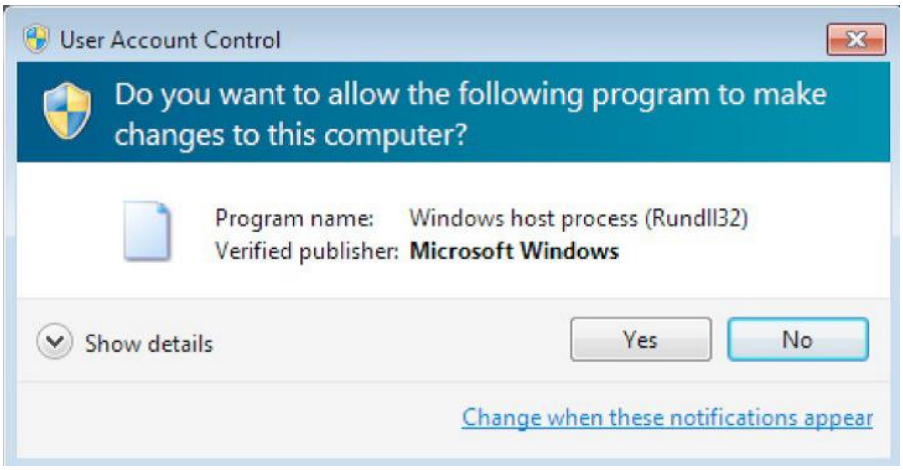
RTM может пытаться повысить привилегии, показывая ложные сообщения об ошибке. Малварь имитирует проверку реестра (см. рисунок ниже) или использует настоящую иконку редактора реестра. Обратите внимание на ошибку в написании wait – whait. Через несколько секунд сканирования программа выводит ложное сообщение об ошибке.




Ложное сообщение легко обманет обычного пользователя, несмотря на грамматические ошибки. Если пользователь нажмет на одну из двух ссылок, RTM попытается повысить свои привилегии в системе.

После выбора одного из двух вариантов восстановления, троян запускает DLL при помощи опции runas в функции ShellExecute с полномочиями администратора. Пользователь увидит настоящий запрос Windows (см. рисунок ниже) о повышении полномочий. Если пользователь даст необходимые разрешения, троян будет работать с привилегиями администратора.




В зависимости от языка по умолчанию, установленного в системе, троян показывает сообщения об ошибке на русском или английском.

### 4.8.3. Сертификат

RTM может добавлять сертификаты в Windows Store и подтверждать надежность добавления автоматическим нажатием на кнопку «да» в диалоговом окне csrss.exe. Такое поведение не является новым, например, банковский троян Retefe тоже самостоятельно подтверждает установку нового сертификата.

### 4.8.4. Обратное соединение

Авторы RTM также создали туннель Backconnect TCP. Пока мы не видели функцию в эксплуатации, но она предназначена для дистанционного контроля зараженных ПК.

### 4.8.5. Управление файлом узла

Командный C&C сервер может отправлять трояну команду модифицировать файл узла Windows. Файл узла используется для создания пользовательских разрешений DNS.

### 4.8.6. Найти и отправить файл

Сервер может запросить поиск и загрузку файла в зараженной системе. Например, в ходе исследования мы получили запрос файла 1c_to_kl.txt. Как ранее описывалось, этот файл генерирует система бухгалтерского учета 1С: Предприятие 8.

### 4.8.7. Обновление

Наконец, авторы RTM могут обновлять ПО, отправляя новый DLL на смену текущей версии.

## 5. Заключение

Исследование RTM показывает, что российская банковская система до сих пор привлекает киберзлоумышленников. Такие группировки как Buhtrap, Corkow и Carbanak успешно крадут деньги у финансовых учреждений и их клиентов в России. RTM – новый игрок в этой индустрии.

По данным телеметрии ESET, вредоносные инструменты RTM применяются как минимум с конца 2015 года. Программа обладает полным диапазоном шпионских возможностей, включая чтение смарт-карт, перехват нажатия клавиш и мониторинг банковских операций, а также поиск транспортных файлов 1С: Предприятие 8.

Использование децентрализованного нецензурируемого домена верхнего уровня .bit обеспечивает высокую устойчивость инфраструктуры.