Operation Groundbait: Analysis of a surveillance toolkit

ANTON CHEREPANOV, ESET
Version 2016-05-17
Contents

Executive Summary .................................................................................................................................. 02
The discovery ........................................................................................................................................ 03
The campaigns ..................................................................................................................................... 04
  Campaigns against separatists ........................................................................................................ 05
  Campaign against Ukrainian nationalist political party ............................................................ 09
  Other campaigns ............................................................................................................................ 10
Technical details .................................................................................................................................. 12
  The dropper ...................................................................................................................................... 13
  Prikormka modules ......................................................................................................................... 15
  PERSISTENCE module .................................................................................................................... 16
  DOWNLOADER module .................................................................................................................. 17
  CORE module ................................................................................................................................. 17
  DOCS_STEALER module ................................................................................................................... 18
  KEYLOGGER module ....................................................................................................................... 19
  SCREENSHOTS module .................................................................................................................. 19
  MICROPHONE module .................................................................................................................... 19
  SKYPE module ............................................................................................................................... 19
  LOGS_ENCRYPTER module ............................................................................................................ 20
  GEOLOCATION module ................................................................................................................... 21
  OS_INFO module ............................................................................................................................. 21
  PASSWORDS module ....................................................................................................................... 22
  FILE_TREE module ......................................................................................................................... 22

C&C servers ......................................................................................................................................... 23
Attribution ............................................................................................................................................ 25
Conclusion ........................................................................................................................................... 27
Credits ................................................................................................................................................ 28
APPENDIX A. Details of Prikormka Campaigns .................................................................................. 29
APPENDIX B. Indicators of Compromise (IoC) .................................................................................... 31
  ESET detections ................................................................................................................................. 32
  Host-based ....................................................................................................................................... 32
  Mutexes .......................................................................................................................................... 32
  C&C servers .................................................................................................................................... 32
  Servers used for sending spearphishing emails .............................................................................. 32
  SHA-1 hashes ................................................................................................................................... 33
**Executive Summary**

Operation Groundbait (Russian: Прикормка, Prikormka) is an ongoing cyber-surveillance operation targeting individuals in Ukraine. The group behind this operation has been launching targeted and possibly politically-motivated attacks to spy on individuals.

This paper presents ESET’s findings about Operation Groundbait based on our research into the Prikormka malware family. This includes detailed technical analysis of the Prikormka malware family and its spreading mechanisms, and a description of the most noteworthy attack campaigns.

**Key findings:**

- The country where the malware has been seen most is Ukraine. It has been active since at least 2008.
- The primary targets of Operation Groundbait are anti-government separatists in the self-declared Donetsk and Luhansk People’s Republics in Eastern Ukraine.
- There have also been a large number of other targets, including Ukrainian government officials, Ukrainian politicians, Ukrainian journalists and others.
- The attackers most likely operate from within Ukraine.
The discovery

In the third quarter of 2015 ESET identified a previously unknown modular malware family, Prikormka. Further research revealed that this malware has been active since at least 2008 and the country where the malware has been seen most is Ukraine. The reason why it had gone unnoticed for so long is the relatively low infection ratio before 2015. The number of infections surged significantly in 2015.

Figure 1 shows the number of unique Prikormka samples compiled in each year since 2008, according to the PE header timestamps. While timestamps by themselves usually are not a reliable indicator, in this case, their accuracy was confirmed by ESET’s LiveGrid® telemetry.

One of the first examples of this malware that we analyzed in our laboratory had the name prikormka.exe. The Russian and Ukrainian word prikormka (Прикормка) means groundbait, a type of fish bait that is cast into the water to attract fish. We used this codename during our research and afterward we decided to keep it, so the malware has the names Win32/Prikormka and Win64/Prikormka respectively.

The low detection ratio and ability to stay undetected for years is a common characteristic of targeted attacks (APTs). The investigation of campaigns and Prikormka activity has increased our confidence that this malware is used in targeted attacks.

Targeted attacks are generally carried out for various purposes, including reconnaissance, intellectual property theft, sabotage, and espionage. After analyzing tactics, techniques and procedures employed by this particular malware group, we came to the conclusion that individuals are targeted rather than companies.

Even when the Prikormka malware was detected in a corporate environment, we never saw any lateral movement — a technique used by advanced adversaries in cyber-attacks.

We suspect that this group operates in Ukraine, where most of the victims are located. For that reason and due to the nature of these attacks, we classified them as cyber-surveillance operations.
The campaigns

In this section, we will show the most noteworthy and prominent campaigns and the decoy documents with which they are associated.

Let’s examine detection statistics by country based on our ESET LiveGrid® statistics:

According to our telemetry, Ukraine is the country with the majority of detections of this malware. In addition, our research revealed that the attackers behind this malware demonstrate native fluency of the Ukrainian and Russian languages and comprehensive understanding of the current political situation in Ukraine.

To answer the question of what kind of victims were attacked in the above-listed countries, we have analyzed the decoy documents used to target them.

The main infection vector that we identified during our research consists of spear-phishing emails with attached malicious executables or with a download link to a malicious file hosted on a remote server. When the user clicks on a malicious attachment that is masquerading as a document, the Prikormka dropper displays a decoy document in order to trick victims and distract their attention, since victims normally expect to see a document open when they click on an attachment. This technique works against less tech-savvy computer users; infection success, however, depends on the quality of spearphishing emails. The attacker has a greater chance to infect the computer when spearphishing letters and decoy documents are relevant to the victim — in other words, when the victim would not be surprised to receive such a message from someone. Thus, analyzing such decoy documents can reveal information about the intended targets of these cyber-attacks.

Secondly, there is another artefact embedded in each sample of Prikormka malware, that we call the Campaign ID. These Campaign IDs are unique text strings used to identify specific infections or attempts at infection by the Prikormka malware operators. The combinations of letters and numbers used can sometimes reveal information about the intended targets.

So far we have identified more than 80 different Campaign IDs and even more decoy documents linked to these IDs. It was observed that usually one Campaign ID is used against one target, which can be an individual, some entity, or group of people. This means that one particular ID might be discovered on multiple computers.

A more comprehensive listing of representative campaigns, along with their compilation timestamps and unique Campaign IDs is in Appendix A.

It is worth mentioning that in some cases it is hard to identify intended victims, especially when the Prikormka malware infections were discovered at the stage when the malware was already installed and active. However, we have become aware of some active Prikormka infections on computer networks belonging to high-value targets, including the Ukrainian government. Other noteworthy targets are mentioned in the following descriptions of Groundbait campaigns.
Campaigns against separatists

Among Prikormka’s primary targets are separatists in Eastern Ukraine. Since 2014 this region has been involved in an armed military conflict.

In April 2014 a group of people unilaterally proclaimed independence in two regions of Eastern Ukraine: Donetsk and Luhansk. In response, the Ukrainian government classified these two entities as terrorist organizations and, therefore, the territory of these regions was declared an Anti-Terrorist Operation (ATO) zone. In May 11th 2014, the authorities of these self-proclaimed republics held a referendum seeking to legitimize the establishment of the republics.

A significant number of decoy documents that were used in Prikormka attacks exploited various topics related to the self-proclaimed states of the Donetsk People’s Republic (DPR) and the Luhansk People’s Republic (LPR). Moreover, a number of decoy documents contain private data including internal statistics and documents apparently used in the internal workflow of these self-proclaimed states. This fact leads us to believe that operators are intentionally targeting people located in these two regions. These assumptions are confirmed by our ESET LiveGrid® telemetry: the Donetsk and Luhansk regions are at the two most infected regions in Ukraine by the Prikormka malware.

The attackers use social engineering tricks to convince a victim to open a malicious attachment. These tricks include giving provocative or attractive names to the email attachments. Here are few examples of such filenames:

- Нацгвардейцы со шприцами сделали из донецкого мальчика мишень для ракет.exe (From the Russian: National Guard of Ukraine aimed rockets at boy from Donetsk). Compilation timestamp: November 5th 2014
- Последнее обращение командира бригады 'Призрак' Мозгового Алексея Борисовича к солдатам и офицерам ДНР и ЛНР.scr (From the Russian: Leader of the Prizrak Brigade Aleksey Borisovich Mozgovoy’s last appeal to soldiers and officer of Donetsk People’s Republic and Luhansk People’s Republic). Compilation timestamp: May 24th 2015

Here are examples of decoy documents that were used in attacks against separatists in Luhansk and Donetsk regions.

- The first example is an executable with the filename СПРАВОЧНИК по МИНИСТЕРСТВАМ обновленный.exe (From the Russian: Ministries directory – updated) that drops a decoy document with a list of Ministries of the self-proclaimed republic. The Campaign ID for this executable is D _ xxx. (Figure 3)
- Here is another example of a decoy document, which was dropped by an executable named материалы к зачету по законодательству.exe (From the Russian: Materials for the law exam). This executable drops several documents including the LPR temporary constitution and other legal and political documents. The Campaign ID is L _ ment; the word “ment” is Russian slang for a policeman. Thus, the attackers demonstrate intimate knowledge of the Russian language. (Figure 4)
- Some of the decoy documents use the Minsk agreement topic. Here is an example of one such document, which comes from a dropper with the filename Схема демилитаризованной зоны в районе Шиокино.exe (From the Russian: Scheme of the demilitarized zone in the Shyrokyne (Shyrokyne written with a typo in Russian)). The Campaign ID was Lminfin. (Figure 5)
Figure 3. Decoy document, with a list of Ministries of DPR. (Here and in further images, potentially sensitive data have been redacted by ESET.)
ЛУГАНСКАЯ НАРОДНАЯ РЕСПУБЛИКА

ЗАКОН

Об оперативно-розыскной деятельности

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

Глава 1. Общие положения

Статья 1. Оперативно-розыскная деятельность

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

Статья 2. Задачи оперативно-розыскной деятельности

Задачами оперативно-розыскной деятельности являются:

Figure 4. Decoy document containing the law, which describes the rules for special crime investigation activities.

Figure 5. Decoy document, which exploits the Minsk Agreement topic.
Another decoy document even contains a map of the buffer zone established by the Minsk Protocol. Here is an example, which came from a dropper with the filename Отвод с 4 участками по сост на 14.08.exe (From the Russian: Pullout [of heavy weapons] on 14.08). The Campaign ID was BUR. (Figure 6)

Important note: Most of the Prikormka binaries that seem to have been intended for use against separatists have Campaign IDs starting with D or L characters. It's possible that this means Donetsk People's Republic and Luhansk People's Republic, respectively. Also, we observed an executable named Заявление Эдуард Басаргина 13 октября 2015 года в 15 часов.exe (From the Russian: Eduard Basargin's statement on 13th October 2015 at 3pm), which uses the Campaign ID RF _ lgm. Since we have identified detections in Russia, the RF prefix could mean Russian Federation.
Campaign against Ukrainian nationalist political party

All previously mentioned decoy documents were extracted from executables that had Russian filenames. Ukrainian is the official state language; however, people in Eastern Ukraine tend to use Russian, as opposed to Western regions, which use Ukrainian.

Some of the Prikormka binaries had names in Ukrainian. For example, we have seen the filename План ДНР на 21 липня, щодо відводу військ.exe (From the Ukrainian: The DPR plan for withdrawal of troops on 21st July). Names of attachments in the Ukrainian language might suggest that the receiver of such malicious letters prefer to speak Ukrainian over Russian. The fact that Prikormka malware was detected in Western regions of Ukraine strengthens this assumption. The Campaign ID for this particular executable was Psek, which inclines us to believe with a high degree of confidence that members of Ukrainian nationalist party Right Sector (Ukrainian: Pravyi Sektor) were targeted with Prikormka malware.
Other campaigns

Separatists in Donetsk and Luhansk and the other targeted high profile victims weren't the only targets of Operation Groundbait. We have observed some other campaigns with interesting decoy documents, but we can't identify the intended victims solely on the basis of those documents.

Here is an example of a decoy document which was possibly used against a religious institute. The decoy document comes from dropper with filename Новое слово жизни.exe (From the Russian: New word of life). The Campaign ID was medium. This choice of Campaign ID may refer to mediumship and spiritualism.

Another campaign was discovered in March 2016. This time, the name of the malicious file was in Hungarian: Önélétrauj fizikai munka 2.pdf.scr, which translates to English as "CV physical work". The decoy document dropped by this file was a person's CV (curriculum vitae or resume), written in Hungarian. This malicious .SCR file was sent compressed in single archive with two other documents: the CV of the same person in Ukrainian, and a certificate in Hungarian that confirms that this person is able to perform the physical job. Based on this information it is hard to say who might be the intended target, but the fact its recipient possibly knows Hungarian and Ukrainian makes this campaign interesting. The Campaign ID was F _ ego.

Figure 8. Decoy document possibly used against religious organizations.

Figure 9. The Hungarian document that was sent to the victim in a single archive with the Prikormka malware.
Here is an example of a decoy document, dropped from a file with the name bitcoin.exe. The Campaign ID in this case was hmod.

The Russian text in the decoy document explains, step by step, how to buy bitcoins using stolen credit cards. The text abounds in slang words often used by Russian-speaking carders.¹

Another example is a mysterious decoy document extracted from a malware dropper with the name prikormka.exe. The Campaign ID is 30K _ alfa.

This decoy document contains the pricelist of a Ukrainian shop that sells various types of groundbait.

---

¹ Cybercriminals involved in stolen credit card crime.
Technical details

In this section, we will describe technical aspects of Prikormka malware, including malware architecture, C&C communication and detailed analysis of modules used.

Figure 12. Simplified scheme of the Prikormka malware’s architecture.
The dropper

The dropper is the initial component of this malware, which is usually sent through email as an attachment. Usually the dropper has a `.SCR` or `.EXE` file extension and is compressed into an archive. In order to trick the victim, the Prikormka dropper can masquerade as various types of document or self-extracting archive.

When executed, the dropper infects the computer, but also displays one or more decoy documents. To this end, the malware displays a WinRAR self-extraction (SFX) archive window. In some cases, the dropper creates a legitimate, non-malicious SFX executable on disk and then launches it. Interestingly, that SFX archive always has a Russian localized graphic user interface, even in cases where the filename of the dropper is in Ukrainian. The dropper which has a Hungarian filename does not display this window at all.

The SFX executable can contain one or more decoy documents. For example one SFX that was dropped by Prikormka contained 24 documents. Of course, the number and size of the decoy documents affects the size of the droppers. The biggest dropper we identified had a file size of 25MB.

Most of the dropper executables have an embedded application manifest, which specifies that the executable requires administrator privileges in order to run on the system. If the user does not have administrator privileges, the system will prompt for credentials.

The dropper needs administrator privileges because of the technique used by the malware to become persistent on the infected system. Specifically, the malware uses so-called DLL load-order hijacking in order to start automatically on every system boot. The dropper saves one of the Prikormka DLL modules to the Windows directory under the name `ntshrui.dll`. Because this DLL file is stored in the Windows directory, it will be loaded on system boot by the `explorer.exe` process instead of the legitimate `ntshrui.dll` file, which is stored in the `C:\Windows\System32` subdirectory. Thus, the Prikormka module hijacks the order of loading DLL files. This persistency method is not something new; it has been publicly examined multiple times by anti-malware research community.

Another interesting technique is used by the Prikormka malware, specifically by droppers with `.SCR` file extensions. The `.SCR` file extension stands for screensaver and represents a standard Windows executable file. The main difference between `.EXE` and `.SCR` is that a screensaver is executed with `special command line arguments`. Usually, cybercriminals just rename an executable with the `.SCR` extension in order to bypass various security measures based on file extension. Prikormka's authors implemented a check for such command line arguments, so when the
binary is executed as a standard executable (without the required arguments), it won’t infect the system. Thus, this simple check allowed the malware to bypass some sandboxes used for automatic sample processing.

In the case where the infection starts from a .SCR file, the Trojan uses standard methods for loading its DLL via rundll32.exe and for maintaining persistence, by setting an entry with the name guidVGA or guidVSA in the registry Run key:

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

In order to be loaded by the 32-bit and the 64-bit version of Windows Explorer the malware has binaries for both platforms. Most modules are written in the C programming language and compiled with Microsoft Visual Studio.

The dropper stores modules in its resources; some of these resources are encrypted with a simple XOR operation.

![Figure 16. Resources located inside the Prikormka dropper binary.]

The dropper is responsible for creation of the rbcon.ini file, which used by the malware to store Campaign ID and other values.

Earlier versions of Prikormka used a different technique – Campaign IDs were embedded in the binary file of one of modules:

![Figure 17. The Campaign ID with value hmyr32 is embedded in the binary.]

The Campaign ID value was hardcoded in the Prikormka binary at compilation time; moreover, the ID in the 32-bit version of binaries ended with 2, while the Campaign ID in 64-bit version of binaries ended with 4.

This technique was probably efficient for a small number of victims, but it presumably created problems for the attackers once the number of victims grew. Perhaps recompiling and repacking the core parts of a toolset for every new victim became too time consuming, so somewhere around mid-2015, the attackers changed this scheme. Since June 2015 the Campaign ID is stored in a separate file named rbcon.ini, which the attackers call objectset. The malware authors have also included a new value called roboconid, which represents the Operator’s ID. Our investigation allowed us to confirm that this ID is a unique number for the malware operator, who performs cyber operations and is assigned to infect, spy on, and track a particular target.

![Figure 18. The rbcon.ini file which contains both Campaign ID and Operator ID.]

The malware authors have also included a new value called roboconid, which represents the Operator’s ID. Our investigation allowed us to confirm that this ID is a unique number for the malware operator, who performs cyber operations and is assigned to infect, spy on, and track a particular target.
Some of the binaries of the dropper contain a PDB-path, which can reveal the directory structure used by attackers.

Figure 19. Some of the PDB-paths discovered inside Prikormka droppers.

The malware writers internally call this Trojan PZZ; we have other evidence that supports this theory. The Prikormka family is a typical cyber-espionage Trojan with a modular architecture. The functionality of the Trojan allows attackers to steal sensitive data from the infected computer and upload them to command and control (C&C) servers.

**Prikormka modules**

The Prikormka modules are stored on disk in the infected system in the form of DLL files. There are modules for various purposes, such as communication with C&C servers, auxiliary purposes (e.g. persistence), and exfiltration of different types of sensitive information from the infected computer. As mentioned before, Prikormka modules are compiled for both 32- and 64-bit Windows platforms.

There is a standard set of downloadable modules with pre-defined names, which will be described in detail in the next sections. So as to be executed, the module (DLL file) should be stored under a specific filename on the disk and should have one of the following export functions: Starting, KickInPoint, Cycle. However, attackers are able to push any custom module to a particular victim. Specifically, we observed that custom modules are usually named mp.dll.

It should be noted that malware operators are responsible for deciding which modules should be pushed to the infected computer.

Prikormka might store modules with different functionality under similar names or, conversely, it can store modules with similar functionality under various names. Some versions of the malware store modules with a filename that contains only the current date and time. For these reasons we refer to the plugins by code names in the following text.

<table>
<thead>
<tr>
<th>Module code name</th>
<th>Internal name of module</th>
<th>Filename Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERSISTENCE</td>
<td>samlib.dll</td>
<td>samlib.dll, ntshrui.dll Used for persistence</td>
</tr>
<tr>
<td></td>
<td>helpldr.dll</td>
<td>helpldr.dll, _wshdmi.dll Downloads CORE module</td>
</tr>
<tr>
<td>CORE</td>
<td>hauthuid.dll</td>
<td>hauthuid.dll, _svga.dll, _wshdmi.dll Loads all other modules, communicates with C&amp;C-servers, uploads logs</td>
</tr>
<tr>
<td>DOCS_STEALER</td>
<td>iomus.dll</td>
<td>iomus.dll Collects documents</td>
</tr>
<tr>
<td>KEYLOGGER</td>
<td>kl.dll, hlpuctf.dll</td>
<td>hlpuctf.dll Logs keystrokes</td>
</tr>
<tr>
<td>SCREENSHOTS</td>
<td>scrsh.dll</td>
<td>scrsh.dll Grabs screenshots of desktop</td>
</tr>
<tr>
<td>MICROPHONE</td>
<td>snm.dll</td>
<td>snm.dll Captures audio from microphone</td>
</tr>
<tr>
<td>SKYPE</td>
<td>swma.dll</td>
<td>swma.dll Records Skype audio calls</td>
</tr>
<tr>
<td>LOGS_ENCODER</td>
<td>atiml.dll</td>
<td>atiml.dll Compresses and encrypts collected logs</td>
</tr>
<tr>
<td>GEOLOCATION</td>
<td>geo.exe</td>
<td>Inv.exe Geo-locates the infected computer</td>
</tr>
<tr>
<td>OS_INFO</td>
<td>InfoOS</td>
<td>mp.dll Collects information about infected computer</td>
</tr>
<tr>
<td>PASSWORDS</td>
<td>Brother</td>
<td>mp.dll Collects saved passwords for various installed applications</td>
</tr>
<tr>
<td>FILE_TREE</td>
<td>mpTREE</td>
<td>mp.dll Collects file tree of fixed disk of infected computer</td>
</tr>
</tbody>
</table>

Table 1. List of Prikormka modules identified during our research.
The following list contains filenames of modules that were referenced within malware code, but we haven't seen them during our research and thus were unable to assess their functionality:

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

It is important to note that Prikormka components made in the "old" period (between 2008 and 2010) used a completely different naming scheme. Here are some examples of such filenames:

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

**PERSISTENCE module**

As described above, this module uses the DLL load-order hijacking technique to maintain persistence in the system.

When launched, this module creates the folder `%USERPROFILE%\AppData\Local\MMC` and copies the following files there from the `%WINDIR%` directory:

- hauthuid.dll (CORE)
- hlpuctf.dll (KEYLOGGER)
- atiml.dll (LOGS _ ENCRYPTER)
- iomus.dll (DOCS _ STEALER)
- swma.dll (SKYPE)
- helpldr.dll (DOWNLOADER)
- rbcon.ini

This component then loads and passes execution to the CORE module, or to the DOWNLOADER module if the CORE module is not found.

If the `%USERPROFILE%\AppData\Local\MMC\nullstate.cfg` file exists, then the component deletes all the filenames listed above from the MMC directory and quits, thus deactivating itself.

Some of the binaries of the PERSISTENCE module contain a PDB-path, which reveals the directory structure used by the malware authors at compile time. Three of these paths contain a time stamp, possibly from when the project was created or modified. One such path contains the Russian string Раб. программы, which translates as "computer programs for work".
**DOWNLOADER module**

The main purpose of this component is to download the CORE module and execute it. The DOWNLOADER module makes an HTTP request to one of its C&C servers, receives data, decrypts the data, saves it under the name `hauthuid.dll` and then loads the DLL. The communication is encrypted with the Blowfish cipher and then base64 encoded.

Along with the Campaign ID and Operator ID, the module includes in the request a date and time when infection occurred and whether the platform is 32-bit or 64-bit Windows. Some of the binaries of the DOWNLOADER module contain PDB-paths, revealing that internally this module is called `Loader` or `helpldr`:

**CORE module**

The CORE module is responsible for communications with C&C servers and other tasks, including downloading additional modules, loading them, and uploading stolen data to the remote server.

Since this malware (and specifically the CORE module) has existed for several years, the details of implementation might vary, but the main concept of the CORE module has remained unchanged over the years. The concept of the Prikormka malware is simple: the CORE module downloads additional components, which are used to harvest various types of data. When such a component is loaded, it gathers sensitive information and saves this information to some specific log file. The log file might store collected data in plain-text or it may be encrypted. The CORE module checks periodically for such log files and when a log is available, it uploads it to the remote server. The CORE module won’t upload a log file if it is bigger than 500MB.

In order to store downloadable modules and collected log files, the CORE module creates two directories:

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

![Traffic captured from the Prikormka malware's DOWNLOADER module.](image)
The MMC folder is primarily used for additional downloadable malware components; the SKC folder is used for storing collected log files. In the subsequent text we will use the term “log folder” to refer the SKC directory.

The downloadable modules are not able to upload collected data. In fact, only the CORE and DOWNLOADER modules communicate with C&C servers. The communication protocol of the CORE module is very similar to that of the DOWNLOADER module.

The only difference between DOWNLOADER and CORE HTTP requests is the st parameter in the URL. This parameter indicates which of the downloadable modules are active and loaded by Prikormka. With the current implementation, there is room for 11 additional modules. The server responds with the content of the module that should be executed, or with a dummy answer.

The logs are uploaded during a POST request to a similar URL:

```
• http://server.ua/wd.php?sn=%DATE_TIME_OF_INFECT% 
```

It is worth mentioning that early versions of Prikormka stored C&C servers in plain-text; later, attackers used the base64 algorithm in order to hide the servers’ addresses. Finally, the latest versions of the CORE modules use simple encryption: to decrypt it, the researcher should add the hexadecimal value 0x17 to each encrypted byte.

```
{encrypted_data} + 0x17
```

Figure 24. Example of simple encryption used by Prikormka to hide C&C servers.

**DOCS_STEALER module**

This module is responsible for collecting documents from removable media or fixed drives, connected via a USB interface.

The module focuses on collecting files with document-type extensions: .DOC, .XLS, .DOCX, .XLSX, .PPT, .PPTX, .PPS, .PPSAX, .PDF, .RTF, .TXT, .ODT. However, it does not collect all files, but only those which were modified in the last 7 days (or 14, or 30, depending on which version of the module).

The collected files then are compressed, encrypted with Blowfish, and stored under the following scheme:

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

Figure 23. Traffic captured from the Prikormka malware’s CORE module.
KEYLOGGER module

This module is responsible for collecting keystrokes and the titles of foreground windows. The collected information is saved to the log folder under the following names:

- %DATE%_%TIME%_fix.lg
- lgfix
- lpl
- fpli
- fmmlg

If the log file is bigger than 10Mb, the module removes the log and starts anew. Some versions of the module encrypt the log file using Blowfish.

SCREENSHOTS module

This module is responsible for capturing screenshots of the victim’s desktop. By default, the module captures a screenshot every 15 minutes. However, if the victim opens a VoIP application Skype or Viber, then the period between screenshots is lowered dramatically to 5 seconds. The captured screenshot is saved in the JPEG format. The collected information is saved to the log folder under filenames %DATE%_%TIME%.tgz.scrsh or %DATE%_%TIME%.stgz.

MICROPHONE module

This module is responsible for recording sound from a microphone. The module records audio with 10 minutes duration. It stops recording on command, or when there is no more free disk space available. The recorded audio is encoded with the LAME MP3 encoder. The collected information is saved to the log folder under the filename %DATE%_%TIME%.snm.

SKYPE module

This module is responsible for recording Skype audio chats. In order to record Skype calls, the module uses a legitimate interface, called the Skype Desktop API. When a third party application is about to use this API, the Skype messenger displays a warning, which asks the user to allow the access. To bypass this Skype security feature, the Prikormka module creates a thread that attempts to find the window and click the “Allow access” button programmatically, without human interaction.

The strings and some code fragments in this Prikormka module suggest that the implementation of this module was partly borrowed from the code published on the website openrce.org in 2006.
The collected information is saved to the log folder using \%DATE\%  \_ \%TIME\%.skw and _skype.log filenames.

**LOGS ENCRYPTER module**

This module is responsible for log encryption. The module compresses data via the LZSS algorithm and encrypts the following log files with Blowfish:

- \%USERPROFILE\%\AppData\Local\MMC\inf
- \%USERPROFILE\%\AppData\Local\MMC\fsh
- \%USERPROFILE\%\AppData\Local\SKC\*.scrsh
- \%USERPROFILE\%\AppData\Local\SKC\*.snm
- \%USERPROFILE\%\AppData\Local\SKC\*.skw
- Files listed in \%USERPROFILE\%\AppData\Local\MMC\ierdir.dat

The file ierdir.dat is created by the CORE module; it contains an encrypted list of files requested by attackers to upload from victim’s computer.

After encryption, the original (but not the encrypted) files are deleted. Results of the encryption are stored in the following files:

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

The encrypted content is additionally encoded with the base64 algorithm. Interestingly, before the content starts, the module puts an additional signature there:

![Signature Example](image-url)

We have not found any legitimate application which can read such files or any other meaning of this mysterious “atKsoft” signature.
GEOLOCATION module

This module is responsible for geo locating the infected computer. Unlike other modules, this module is written in the C# programming language. This module collects information about currently available WiFi networks, including Service Set Identifier (SSID) and MAC-address. Afterward, the module makes a request to the Google service, providing collected information as parameters; the Google service response contains the possible location based on the information supplied.

The collected information is saved to the log folder under the filename geo%DATE%.inf.

The binary of the GEOLOCATION module has a PDB-path; the structure of this path is similar to the PDB-path of the DOWNLOADER module:

![Image of the GEOLOCATION module binary](https://example.com/image)

OS_INFO module

This module is responsible for collecting information about the infected computer.

The following information is collected by this module:

- Battery info for Notebooks
- Windows OS version
- Computer name and User name
- IP Addresses and MAC Addresses
- Physical memory
- Available disk drives
- Available printers
- Desktop resolution
- Installed antivirus software

The module uses Windows API functions in order to collect this information. The collected information is saved to the log folder under the filename %DATE%_%TIME%.inf.
**PASSWORDS module**

This module is responsible for collecting passwords stored in applications installed on the infected computer.

The module gathers the application version, logins and passwords stored in the following applications:

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

For some reason, this module does not collect passwords for Microsoft Internet Explorer and Microsoft Edge browsers. Because the Yandex Browser and the Rambler Browser are popular mostly in Russian speaking countries, we think that it indicates that this module was designed for use against users located in such countries.

The collected information is saved to the log folder under the filename `%DATE% _ %TIME%.inf`.

**FILE_TREE module**

This module is responsible for collecting information about the file system of the computer’s fixed drives, including paths of files with specific file extensions, their size and creation time. The actual content of the file is not collected by this module.

The attackers are interested in the following file extensions:

- Documents: TXT, DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF
- Archives: ZIP, RAR
- Databases: DB, SQLITE
- The Bat! email client: TBB, CFG, CFN, TBN, TBB
- Microsoft Outlook: OST, PST
- Other: DAT, WAV, EXE

Since The Bat! email client is popular in Russian-speaking countries, the fact that malware is focused on file extensions associated with this email client is another indicator that the malware is created with the intention of using it against Russian-speaking users.

It should be noted that the list of all file extensions does not represent the list found in any particular sample. This list contains all the possible file extensions that we observed in different versions of the FILE_TREE module. The attackers might build a custom version of this module for a specific victim. The collected information is saved to the log folder under the filename `%DATE% _ %TIME%_tree.inf`. Some binaries of FILE_TREE modules have PDB-paths; one such path reveals the username of the malware writer.

![Figure 30. A PDB-path discovered inside a FILE_TREE module.](image-url)
C&C servers

During our research into Operation Groundbait we have observed a number of C&C server domain names and IP addresses. Most of them are located in Ukraine and are hosted by Ukrainian hosting providers. Appendix B contains a more comprehensive listing.

One of the C&C servers, gils.ho[.]ua has been in operation since 2008, according to information from the hosting company. In order to hide their illegal activity, the attackers created a bogus website. The website is dedicated to the capital of Ukraine—Kiev.

During our investigation we obtained access to an Operation Groundbait C&C server that was misconfigured and allowed a public directory listing.

At one point, the root directory contained 33 subdirectories, with an individual folder for each victim. This means that the server was used to control 33 Prikormka-infected computers. The name of each sub-folder contains an Operator ID, a Campaign ID and the architecture of the infected device.

Each folder contains two sub-folders with the following names: data and util. The first folder contains encrypted exfiltrated data and the second folder has encrypted Prikormka modules.
In addition to the data and util folders, each victim-specific subfolder contained two plain-text log files: journal and log, revealing interesting findings about the malware operators and their victims.

The log file contains the communication log between the server and the infected computer: specifically, the IP address of the infected computer, date and time, type of request (GET or POST), the size of request, and the status of Prikormka modules (in cases where it is a GET request).

According to our analysis of the communication logs from one server there were 33 victims, located mostly in Eastern Ukraine. In addition to those, there were a few victims located in Russia or in Kiev, Ukraine.

The analysis of logs revealed that several malware operators connected to the server using various internet service providers in Kiev and Mariupol. Some of them accessed the C&C via the Tor network.
Attribution

In this section we make an attempt to identify the origin of the threat based on clues that were intentionally or unintentionally left by the attackers:

- Most of Prikormka's C&C servers are located in Ukraine and hosted by Ukrainian hosting companies
- The group behind this threat has fluent knowledge of the Russian and Ukrainian languages, as evidenced by text in the decoy documents and malware binaries
- Some of the PDB-paths revealed that attackers used directories with names in Russian
- All analyzed Prikormka droppers contained language codes that correspond to Ukrainian (hexadecimal code 0x0422) or Russian (0x0419) languages in their PE resources (Figure 37)
- The compilation timestamps of Prikormka binaries suggest that the malware authors operate in the Eastern European time zone
- According to C&C server logs, a number of malware operators participating in Operation Groundbait have been making connections through various internet providers in two Ukrainian cities: Kiev and Mariupol.
Interestingly, the droppers from earlier period (2012-2015) do contain resources with Russian language codes. The malware authors gradually switched from Russian to Ukrainian in the mid of 2015.

Figure 38 depicts the distribution of the compilation hour of Prikormka samples.

We can deduce from this that the malware authors work from 6.00 to 16.00 (UTC), sometimes staying late in the evening. This corresponds to the period 8.00 to 18.00 Eastern European Time, which would include normal Ukraine working hours.

Based on our research and the abovementioned facts, we conclude that the attackers behind Operation Groundbait are people with an interest in surveillance or spying on separatists in the Donetsk and Luhansk regions and a few specific high-profile targets, including Ukrainian politicians. The malware operators and/or authors have a knowledge of the Ukrainian and Russian language, and likely operate from within Ukrainian borders.
Conclusion

Our research into these attack campaigns and the Prikormka malware itself suggests that this threat is the first publicly known Ukrainian malware that is being used in targeted attacks.

In terms of technical advancement, the attackers didn't demonstrate any sophisticated methods or novel techniques. But whether an attacker uses sophisticated methods or not does not matter as long as they reach their ultimate goal: stealing the sensitive information they need from their targets.

The most noteworthy achievement accomplished by the attackers behind Operation Groundbait is that they have stayed under the radar for over 7 years. The malware has been seen in the wild since at least 2008. This finding is confirmed by the timestamps of binaries, ESET telemetry, and by hosting providers used.

Operation Groundbait is, after BlackEnergy and Operation Potato Express, yet another demonstration that that using highly targeted malware for espionage amidst an armed conflict is an everyday reality.

Indicators of Compromise (IOC) that can be used to identify an infection can be found in Appendix B or on github.

For any inquiries or to make sample submissions related to the subject, contact us at: threatintel@eset.com
Credits

Special thanks to @TheEnergyStory
# APPENDIX A.
## Details Of Prikormka Campaigns

<table>
<thead>
<tr>
<th>PT Time stamp (UTC)</th>
<th>Campaign ID</th>
<th>Malware Operator ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 19 09:11:27 2012</td>
<td>N/A (corrupted)</td>
<td>N/A</td>
</tr>
<tr>
<td>Jul 25 08:31:32 2012</td>
<td>Skt</td>
<td>N/A</td>
</tr>
<tr>
<td>Sep 13 08:21:54 2013</td>
<td>MNa</td>
<td>N/A</td>
</tr>
<tr>
<td>Mar 12 15:17:23 2014</td>
<td>Pgks</td>
<td>N/A</td>
</tr>
<tr>
<td>Jul 15 12:18:51 2014</td>
<td>Abk</td>
<td>N/A</td>
</tr>
<tr>
<td>Oct 03 08:57:13 2014</td>
<td>W_zkp7a</td>
<td>N/A</td>
</tr>
<tr>
<td>Nov 05 07:56:00 2014</td>
<td>zma</td>
<td>N/A</td>
</tr>
<tr>
<td>Nov 05 19:30:35 2014</td>
<td>Psep</td>
<td>N/A</td>
</tr>
<tr>
<td>Nov 13 10:20:10 2014</td>
<td>hmod</td>
<td>N/A</td>
</tr>
<tr>
<td>Nov 25 15:12:31 2014</td>
<td>Iff</td>
<td>N/A</td>
</tr>
<tr>
<td>Dec 01 08:07:07 2014</td>
<td>hmyr3</td>
<td>N/A</td>
</tr>
<tr>
<td>Dec 05 13:11:35 2014</td>
<td>lii</td>
<td>N/A</td>
</tr>
<tr>
<td>Jan 31 13:19:22 2015</td>
<td>Ivo</td>
<td>N/A</td>
</tr>
<tr>
<td>Feb 10 18:31:49 2015</td>
<td>Pgad5</td>
<td>N/A</td>
</tr>
<tr>
<td>Feb 19 15:51:33 2015</td>
<td>Pkof</td>
<td>N/A</td>
</tr>
<tr>
<td>Mar 02 16:23:42 2015</td>
<td>Ptrop</td>
<td>N/A</td>
</tr>
<tr>
<td>Mar 11 08:43:12 2015</td>
<td>I0u001</td>
<td>N/A</td>
</tr>
<tr>
<td>Mar 23 12:46:24 2015</td>
<td>Asap</td>
<td>N/A</td>
</tr>
<tr>
<td>Mar 23 16:03:19 2015</td>
<td>P647</td>
<td>N/A</td>
</tr>
<tr>
<td>Apr 10 12:26:20 2015</td>
<td>Pig8_</td>
<td>N/A</td>
</tr>
<tr>
<td>May 06 06:08:52 2015</td>
<td>W_cu6a</td>
<td>N/A</td>
</tr>
<tr>
<td>May 24 08:46:38 2015</td>
<td>Pod13_</td>
<td>N/A</td>
</tr>
<tr>
<td>Jun 11 14:59:45 2015</td>
<td>Aste</td>
<td>N/A</td>
</tr>
<tr>
<td>Jun 21 15:36:24 2015</td>
<td>MVD_LNR_kontakt</td>
<td>7</td>
</tr>
<tr>
<td>Jun 26 13:25:22 2015</td>
<td>r03u0002</td>
<td>N/A</td>
</tr>
<tr>
<td>Jun 29 06:19:36 2015</td>
<td>Dmindoh_zb</td>
<td>7</td>
</tr>
<tr>
<td>Jul 01 12:42:04 2015</td>
<td>r03u0002</td>
<td>N/A</td>
</tr>
<tr>
<td>PT Time stamp (UTC)</td>
<td>Campaign ID</td>
<td>Malware Operator ID</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Oct 29 14:00:05 2015</td>
<td>FSfarm</td>
<td>11</td>
</tr>
<tr>
<td>Oct 30 07:40:28 2015</td>
<td>piter</td>
<td>8</td>
</tr>
<tr>
<td>Nov 11 08:57:44 2015</td>
<td>45K_perev</td>
<td>10</td>
</tr>
<tr>
<td>Nov 20 16:43:20 2015</td>
<td>30K_alfa</td>
<td>10</td>
</tr>
<tr>
<td>Nov 26 12:54:58 2015</td>
<td>REP_L</td>
<td>12</td>
</tr>
<tr>
<td>Nov 28 07:39:26 2015</td>
<td>L_K_geniy</td>
<td>7</td>
</tr>
<tr>
<td>Dec 03 07:21:31 2015</td>
<td>D_odSD</td>
<td>7</td>
</tr>
<tr>
<td>Dec 03 09:40:43 2015</td>
<td>L_minl</td>
<td>7</td>
</tr>
<tr>
<td>Dec 03 10:33:27 2015</td>
<td>D_newsG</td>
<td>7</td>
</tr>
<tr>
<td>Dec 15 11:48:39 2015</td>
<td>M_raz_</td>
<td>N/A</td>
</tr>
<tr>
<td>Dec 18 09:12:40 2015</td>
<td>7_L_xxx</td>
<td>7</td>
</tr>
<tr>
<td>Dec 18 12:12:10 2015</td>
<td>33K_pushkin</td>
<td>10</td>
</tr>
<tr>
<td>Dec 28 13:57:12 2015</td>
<td>38K_135_vnos</td>
<td>10</td>
</tr>
<tr>
<td>Dec 29 14:58:11 2015</td>
<td>KvK_ham</td>
<td>7</td>
</tr>
<tr>
<td>Jan 12 11:44:22 2016</td>
<td>38K_83_parf</td>
<td>10</td>
</tr>
<tr>
<td>Jan 14 09:42 2016</td>
<td>L_ssa</td>
<td>7</td>
</tr>
<tr>
<td>Jan 19 15:30:41 2016</td>
<td>shubin</td>
<td>35</td>
</tr>
<tr>
<td>Jan 19 15:31:31 2016</td>
<td>shubin</td>
<td>35</td>
</tr>
<tr>
<td>Jan 19 15:33:35 2016</td>
<td>shubin</td>
<td>35</td>
</tr>
<tr>
<td>Jan 22 10:04:27 2016</td>
<td>34_Flot</td>
<td>11</td>
</tr>
<tr>
<td>Jan 30 06:38:17 2016</td>
<td>MM_mmh</td>
<td>7</td>
</tr>
<tr>
<td>Jan 30 07:56:11 2016</td>
<td>L_m3</td>
<td>7</td>
</tr>
<tr>
<td>Feb 01 09:46:49 2016</td>
<td>38_Faro</td>
<td>11</td>
</tr>
<tr>
<td>Feb 05 08:00:05 2016</td>
<td>MM_teco</td>
<td>7</td>
</tr>
<tr>
<td>Feb 05 08:20:01 2016</td>
<td>MM_Tkur</td>
<td>7</td>
</tr>
<tr>
<td>Feb 05 08:51:96 2016</td>
<td>L_lml</td>
<td>7</td>
</tr>
<tr>
<td>Feb 08 14:49:52 2016</td>
<td>L_ment</td>
<td>7</td>
</tr>
<tr>
<td>Feb 17 15:06:39 2016</td>
<td>sddl</td>
<td>12</td>
</tr>
<tr>
<td>Feb 22 14:25:18 2016</td>
<td>L_rozysk</td>
<td>7</td>
</tr>
<tr>
<td>Feb 22 14:29:36 2016</td>
<td>L_rozyskR</td>
<td>7</td>
</tr>
<tr>
<td>Feb 25 10:26:58 2016</td>
<td>33K_037</td>
<td>10</td>
</tr>
<tr>
<td>Feb 25 14:18:30 2016</td>
<td>F_ego</td>
<td>11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PT Time stamp (UTC)</th>
<th>Campaign ID</th>
<th>Malware Operator ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 22 15:25:59 2016</td>
<td>sgukiev</td>
<td>11</td>
</tr>
<tr>
<td>Apr 08 12:13:20 2016</td>
<td>avl</td>
<td>6</td>
</tr>
<tr>
<td>Apr 18 11:30:21 2016</td>
<td>L_ukrB</td>
<td>7</td>
</tr>
<tr>
<td>Apr 27 12:40:46 2016</td>
<td>puh</td>
<td>6</td>
</tr>
<tr>
<td>May 05 11:42:54 2016</td>
<td>L_gp</td>
<td>7</td>
</tr>
</tbody>
</table>
APPENDIX B.
Indicators of Compromise (IoC)

Users of ESET security software are fully protected from the Prikormka 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
**ESET detections**

- Win32/Agent.UIG trojan
- Win32/Agent.XOR trojan
- Win64/Agent.XOR trojan
- Win32/Agent.XQX trojan
- Win32/Agent.XRB trojan
- Win32/Agent.XRC trojan
- Win64/Agent.DX trojan
- Win32/TrojanDropper.Agent.RGH trojan
- Win32/TrojanDropper.Agent.RHN trojan
- Win32/Prikormka trojan
- Win64/Prikormka trojan
- MSIL/Prikormka trojan

**Host-based**

- \%PROGRAMFILES\IntelRestore\%
- \%USERPROFILE\Resent\roaming\oop8.1\%
- \%USERPROFILE\AppData\Local\MMC\%
- \%USERPROFILE\AppData\Local\FMG\%
- \%USERPROFILE\AppData\Local\SKC\%
- \%USERPROFILE\AppData\Local\CMS\%
- \%USERPROFILE\AppData\Local\VRT\%
- \%USERPROFILE\AppData\Local\ioctl\%
- \%WINDIR\ntshrui.dll
- \%WINDIR\hauthuid.dll
- \%WINDIR\hlpuctf.dll
- \%WINDIR\atiml.dll
- \%WINDIR\iomus.dll
- \%WINDIR\swma.dll
- \%WINDIR\helpldr.dll
- \%WINDIR\rbcon.ini
- \%USERPROFILE\AppData\Local\CMS\krman.ini
- \%USERPROFILE\AppData\Local\VRT\_wputproc.dll

**Mutexes**

- ZxWinDefContexLNKINFO64
- Zw_accessldrContext43
- Paramore756Contex43
- ZxWinDefContexSMD64
- ZxWinDefContexWriteUSBIO64x
- ZxWinDefContexRNDRV45scr
- ZxWinDefContexRNDRV45and
- ZxWinDefContexSkSwmA
- ZxWinDefContexKINP64
- ZxWinDefContexRNDRV65
- ZxWinDefContexRNDRV65new
- ZxWinDefContexRNDRV65xyz
- ZxWinDefContexRNDRV65xy
- ZxWinDefContexRNDRV64
- Client67WorkProc98List3To

**C&C servers**

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

**Servers used for sending spearphishing emails**

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

SHA-1 hashes

E8A2734C3F3ECEBC76D4D1C28D6E6EE6E8BE7BF
8FD9BF72B34CD83BD5FF9521D05D5DFC7F
6D31AB1CBE8224E06E8BF13502D18BFD7D8A8E
DSB578F892C7588CFDA7A121DAFFAE6B9C5AC
32783A747F5A1B5725BF8E93FD99BE4A99EA9
98440EC18A78725CB76F501611115C899F1F8
E565B6C2D03506DE566B66D6F8C68B19A2F924F
160CF2ABBB25495180AAB5230D201B369CF2D
6E5A9089ACDEDECE29486DE48FBD107EAE2EE6B8
35858A16A06DE4499FEB1CA4AC6BE8491B91BB13
36AC8CB6686E2A56057B9A83E6059119D62BC8
AB011CD0B3B32F11F439300AB909B561A829D9D
279711B88B82BC6D204CBAD1611C8795FE566

2BF9CA8B16B6CD76A9F6E953C3BB0B04E6504A
9551C930B2DF7187DE0895D51S40FDFDAB112AA
BB8D93A0409968C6D5A243DF6B5A6F4B4DE22A
80C1B452E8251C79187DFA601929ABD04A3118C
6E242C403DFABA053C153CA1AE6B24630E3F093
09EA7B2F67797915BBF6D1F0B21E431F990A3
0AA48DE8F52B03708D72AA2D039BB795F36E3
40D7D9053BF690295CB820417A4D2BC6293E017
A660BD9752E041DE20E26213A60B9196259AB
6E96CBBADCA57541E20D9CF32B80C8E72EAA6E
40F33C2D2AD98FE1E6BF4AB199021498F93125A1
9F03A4EA0ACD36531042928B0548456EF8988C8
B373BFB3AA2885FD373DA5EA848AF9772FD453
D6831C452E82966F228096235971A54FD5B65C3
065B705938E6732F243E37B49286964206E5
B356875935FDBF021858726098CD61DF9FB5B
FD2FBB8E467663A3527646B62F2C74562703BCF3
CCD19FD4A1408FC8D58B9709573834064980407E7
984D665C00F8C8238E2A4171A1394735D1850
69536CA0F252CA195646C456717A26EFA7944B
243421FE7C1FCFO07EFAOC6B3FEAC620AC94FCC2
57BD67C34CA474F1E382B70876478418FD18DD
418A32BB21D5F7EB06B9713717B10847225
EE1E595DC4AD219264948040870C7421APF92E
4934282558EF2B9ED933EE485513A93392917
6B53A3AC3B9D8592C58290519DAD16042CF2F

Prikormka early versions:

1BB8C6924F4CFC6410325786228BAC7B4A92F65E
B5F1B3BD6A0281C8EB9633A37E08B63B978ABEB
BCEDAB1C50F4D2EA0A871F9DF6616312723B
DC52EE62B944CD378903CEF855C5E7373E48D6C55
44B8B8375CF788076CD06493E27F69A01F5FD
539033DE14539D4854815498F849E49D74FC4
Prikormka PERSISTENCE modules:

Prikormka CORE modules:

Prikormka DOWNLOADER modules:

Operation Groundbait: Analysis of a surveillance toolkit
Operation Groundbait: Analysis of a surveillance toolkit

Prikormka DOCS_STEALER modules:

Prikormka KEYLOGGER modules:

Prikormka SCREENSHOTS modules:

Prikormka MICROPHONE modules:

Prikormka SKYPE modules:

Prikormka KEYLOGGER modules:
Prikormka LOGS_ENCRYPTER modules:

D5C2C7C3D670D63AD699848747A0418665EA2CB
352C36ED1BF7EB749649615F9A40C13D80EE55D
6740A385A33B9CC3EC22FB7971F93538BE44997
2F10F17A89F18D9BF1FE98896A1413A9787B29D4C
E95458CA9663E4FAB94DD232121D5E994A76015D
2B03FE012486BD89C87858CC43DC9D86742738C

Prikormka GEOLOCATION modules:

50CCCD576A815AC8EFFB160A628646C876DF8CB0

Prikormka OS_INFO modules:

4B8EE967F44CECA2EEB3B8420A858CECFE0231208
72C17994336FE4183CF07A6BCB45AA43A80DF0
824F0E198A86E08FB95920A6F06870A6305FE3F
6C902496AC1F6F60D343B03822F49DB5666BE038

Prikormka PASSWORDS modules:

B986114C5173052FCB0583A55D5099D99B709352
17F5E1FC52D6C617CD81B0983B70FAC7A60F528C

Prikormka FILE_TREE modules:

3EDD14E6FA0297ED3162D7F119D8D126662ED28B
2A5AF8E43887051C1F1B488756AAC204B95561CE
4E40286676FCBAC48070BA86B72761A21AC2466C
3E4BE58421DBAEAA7651DA13B16CB900DBB82A7DEF
D1396938E901DD807103B7B9F9442B99952C21AA
74CDAA4DC776CA2A661AC49B6DDE0F0560380A04
8EFDC716FDFD704EC0296860E61AFF9C952946D4
93E196B59771647828BCC3CB61831150FE1FE02
8384ED4EA9E299306F15A1082231C427A8742271
6E70BE32954E41FAFFC496EAF890B279832B4530
8EA98A83D8F62C45435DD36E6D6F79F1ACB9E7