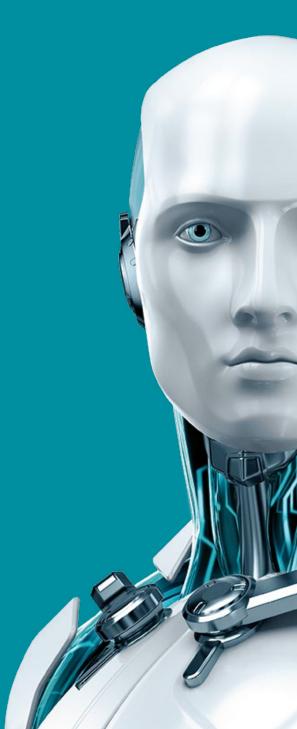


Operation Groundbait: Analysis of a surveillance toolkit





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	
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 2	25
Conclusion	27
Credits	28
APPENDIX A. Details of Prikormka Campaigns	29
APPENDIX B. Indicators of Compromise (IoC)	31
ESET detections3	
Host-based3	32
Mutexes 3	
C&C servers	
Servers used for sending spearphishing emails	
SHA-1 hashes3	33



Executive Summary

Operation Groundbait (Russian: Прикормка, Prikormka) is an ongoing cyber-surveil-lance 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.

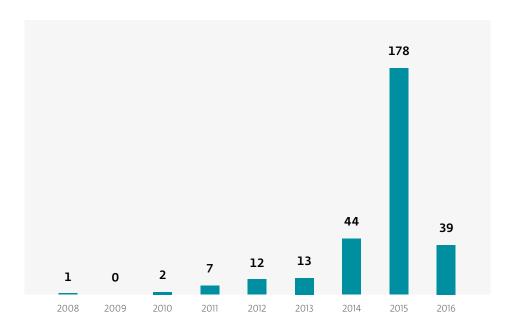


Figure 1. The number of unique samples retrieved by ESET, by years, based on timestamps.

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:

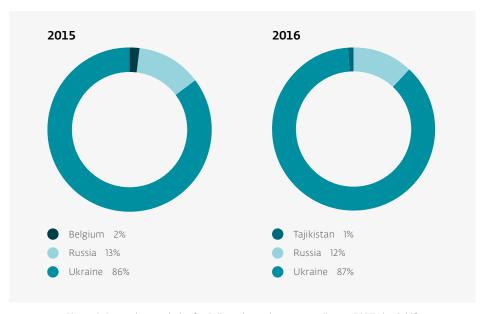


Figure 2. Detection statistics for Prikormka malware according to ESET LiveGrid®.

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 <u>Anti-Terrorist Operation (ATO) zone</u>. In May 11th 2014, the authorities of these self-proclaimed republics held a <u>referendum</u> 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:

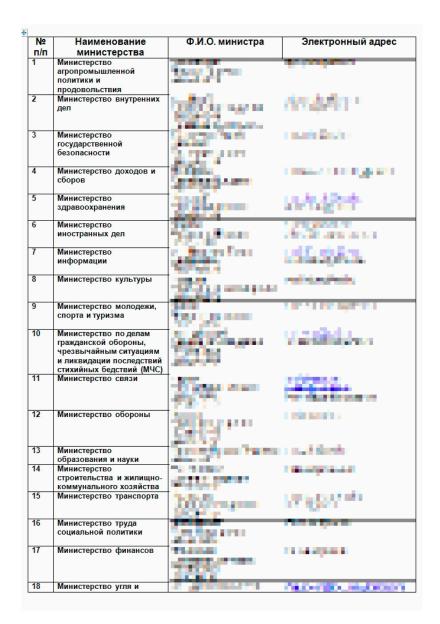
- Нацгвардейцы со шприцами сделали из донецкого мальчика мишень для ракет.exe (From the Russian: National Guard of Ukraine aimed rockets at boy from Donetsk). Compilation timestamp: November 5th 2014
- Последнее обращение командира бригады 'Призрак'
 Мозгового Алексея Борисовича к солдатам и офицерам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

- People's Republic and Luhansk People's Republic). Compilation timestamp: May 24th 2015
- Места дислокации ВСУ в зоне проведения ATO.scr (From the Russian: Dislocation of the armed forces of Ukraine in ATO zone). Compilation timestamp: December 15th 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 <u>Minsk agreement</u> 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 <u>Shyrokyne</u> (Shyrokyne written with a typo in Russian)). The Campaign ID was Lminfin. (Figure 5)





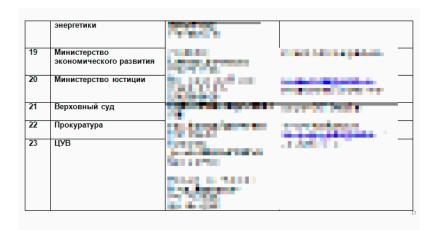


Figure 3. Decoy document, with a list of Ministries of DPR. (Here and in further images, potentially sensitive data have been redacted by ESET.)





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 І. Общие положения

Статья 1. Оперативно-розыскияя деятельность

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

Статья 2. Задачи оперативно-розыскиой деятельности

Задачами оперативно-розыскной деятельности являются:

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

ДОНЕЦКАЯ НАРОДНАЯ РЕСПУБЛИКА

Рабочая группа по реализации

Минских соглашений

Комплекса мер по выполнению

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

DONETSK PEOPLE'S REPUBLIC

Исх. № 1 от 04 июля 2015 г

то на при во предостава на применения в подражения на при во применения в применен

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

Полномочный представитель Донецкой Народной Республики на переговорах Контактной группы в Минске



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 COCT Ha 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 Эдуарда 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 1gm. Since we have identified detections in Russia, the RF prefix could mean Russian Federation.

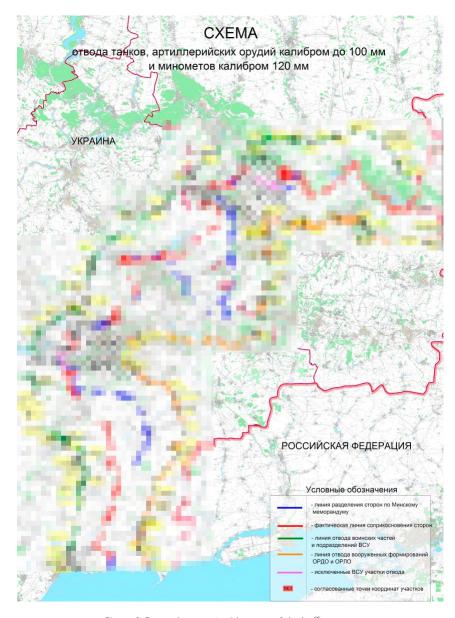


Figure 6. Decoy document with a map of the buffer zone.



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.

ДОНЕЦКАЯ НАРОДНАЯ РЕСПУБЛИКА



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

DONETSK PEOPLE'S REPUBLIC

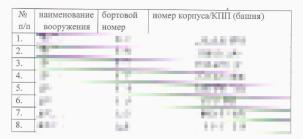
Рабочая группа по реализации Комплекса мер по выполнению Минских соглашений

Исх. от 20 июля 2015 г

Представителям СММ ОБСЕ в Донецкой Народной Республике

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

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





Полномочный представитель Донецкой Народной Республики на переговорах Контактной группы в Минске



Figure 7. Decoy document possibly used against members of a Ukrainian nationalist party.



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 HOBOE 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.



Figure 8. Decoy document possibly used against religious organizations.

Another campaign was discovered in March 2016. This time, the name of the malicious file was in Hungarian: Önéletrajz 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 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.

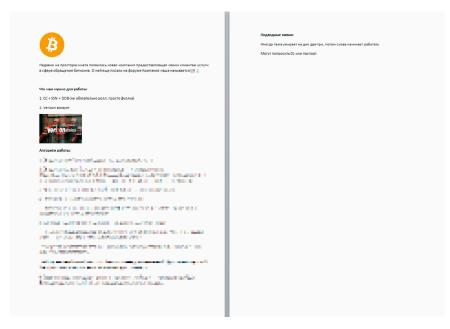


Figure 10. Decoy document that explains how to commit credit card fraud.

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.



Figure 11. The mysterious decoy document dropped by the file named prikormka.exe.

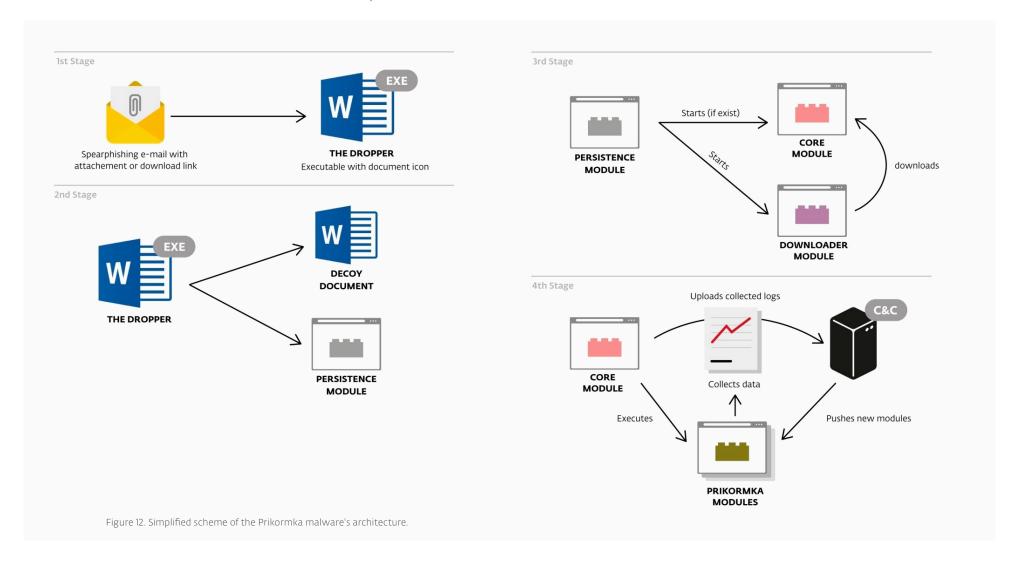
This decoy document contains the pricelist of a Ukrainian shop that sells various types of groundbait.



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.



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.



Figure 13. Icons used by Prikormka malware.

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.

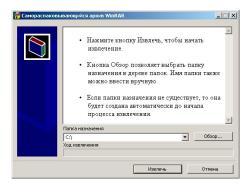


Figure 14. The Russian interface of SFX archive.

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.

Figure 15. The embedded application manifest embedded in Prikormka dropper.

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.

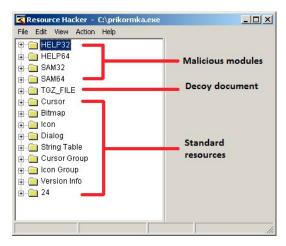


Figure 16. Resources located inside the Prikormka dropper binary.

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:

.1001903C:	2F 01 00 00	4D 01 00	00-6C 01	00 00-77	00 77	00 /	0 M0 10 ww
.1001904C:	77 00 2E 00	67 00 69	00-6C 00	73 00-2E	00 68	00 w	.gils.h
.1001905C:	6F 00 2E 00	75 00 61	00-00 00	00 00-6C	00 70	00 o	.ualp
.1001906C:	-6C 00 00 00	-6B 00 70	00-6C 00	00 00-69	00 70	00 1	kpl ip
.1001907C:	-6C 00 00 00	-6D 00 6D	00-74 00	6D 00-70	00 00	00 🔒	n n t n p
.1001908C:	-68 00 6D 00	79 00 72	00-33 00	-32 00-00	00 00	00 h	m y r 3 2
.1001909C:	-70 00 6C 00	-2E 00 70	00-68 00	70 00-00	00 00	00 📅	1.php
.100190AC:	-5C 00 00 00	2F 00 00	00-68 00	74 00-74	00 70	00 \	/ http://
.100190BC:	3A 00 2F 00	2F 00 00	00-73 00	65 00-00	00 00	00 :	// se
.100190CC:	69 00 65 00	72 00 64	00-69 00	-72 00-2E	00 64	00 i	erdir.d
.100190DC:	61 00 74 00	00 00 00	00-5B 45	6E 64-50	6F 69	6E a	t [EndPoin
.100190EC:	74 5D 00 00	D4 5C 01	10-6C 5E	01 10-64	5E 01	10 t] ^L \@►1^@►d^@►

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.



Some of the binaries of the dropper contain a PDB-path, which can reveal the directory structure used by attackers.

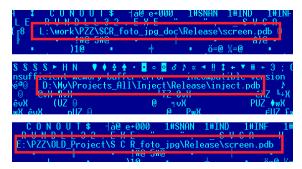


Figure 19. Some of the PDB-paths discovered inside Prikormka droppers.

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.

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

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 <code>%USERPROFILE%\AppData\Local\</code> MMC and copies the following files there from the <code>%WINDIR%</code> 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 Pa6. программы, which translates as "computer programs for work".





Figure 20. Some of the PDB-paths discovered inside Prikormka's PERSISTENCE module

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.

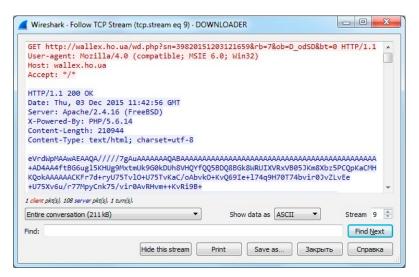


Figure 21. Traffic captured from the Prikormka malware's DOWNLOADER module.

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 PDBpaths, revealing that internally this module is called Loader or helpldr:



Figure 22. PDB-paths discovered inside Prikormka's DOWNLOADER module.

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\



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.

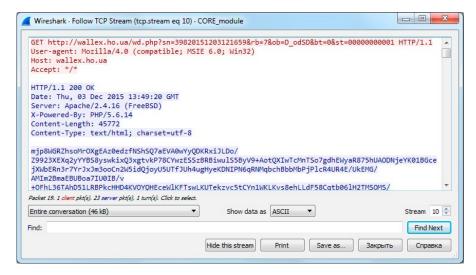


Figure 23. Traffic captured from the Prikormka malware's CORE module.

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:

• hxxp:/server.ua/wd.php?sn=%DATE TIME OF INFECTION%

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.

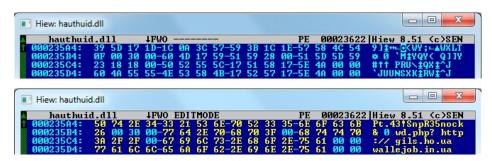


Figure 24. Example of simple encryption used by Prikormka to hide C&C servers.

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, .PPSX, .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:

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
- fplid
- 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 <code>%DATE%_%TIME%.snm</code>.

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 <u>Skype Desktop API</u>. 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.

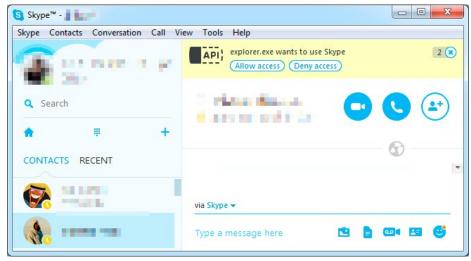


Figure 25. The warning displayed by Skype.

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*.

```
.data:1001D0EC ; char str MINISHELL[]
.data:1001D0EC str_MINISHELL db 'CREATE APPLICATION minishell',0
                                                        ; DATA XREF: ProcessMessage+671o
.data:1001D0EC
.data:1001D0EC
                                                        ; SkypeAPI Windows WindowProc+3F1o
.data:1001D109
                               align 4
.data:1001D10C ; char str_CALL[]
                               db 'CALL %d',0
                                                        ; DATA XREF: qet CALL ID+CTo
.data:1001D10C str_CALL
.data:1001D114 ; char str ALTER CALL[]
.data:1001D114 str_ALTER_CALL db 'ALTER CALL %d',0
                                                       ; DATA XREF: get CALL ID+26<sup>†</sup>o
.data:1001D122
                               align 4
.data:1001D124 ; char str_GET_CALL[]
.data:1001D124 str GET CALL db 'GET CALL %d PARTNER DISPNAME',0
.data:1001D124
                                                        ; DATA XREF: ProcessMessage+1611o
```

Figure 26. The string CREATE APPLICATION minishell suggests copied-and-pasted code.

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:

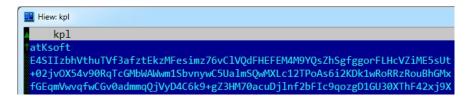


Figure 27. The "atKsoft" signature at the beginning of encrypted log files.

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.

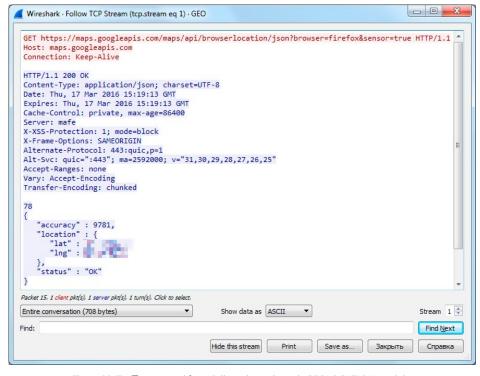


Figure 28. Traffic captured from Prikormka malware's GEOLOCATION module.

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:



Figure 29. The PDB-path discovered inside the GEOLOCATION module.

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.



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.

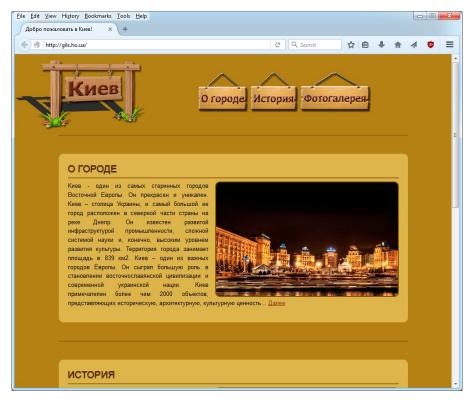


Figure 31. Bogus website created by attackers.

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





Figure 32. Operation Groundbait C&C server directory listing.

Figure 33. The internal directory structure of a subfolder.

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).

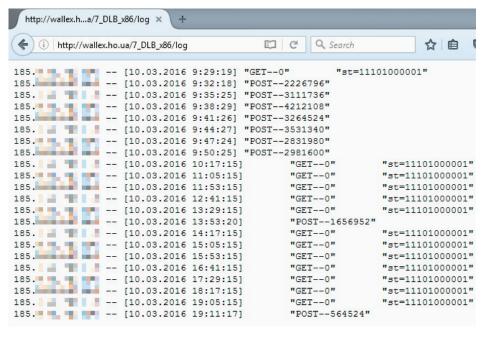


Figure 34. The content of one log file located on the Operation Groundbait C&C server.

The journal file contains the communication log between the server and the malware operator. The communication log contains the IP address of the operator, the date, time, and type of request. It should be noted that once downloaded by the malware operator, the file with exfiltrated data gets removed from the server.

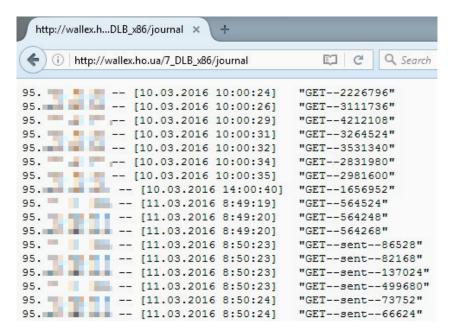


Figure 35. The content of the journal file located on an Operation Groundbait C&C server.

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.

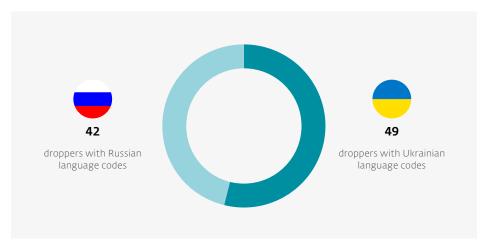


Figure 36. The language codes distribution between droppers.

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.

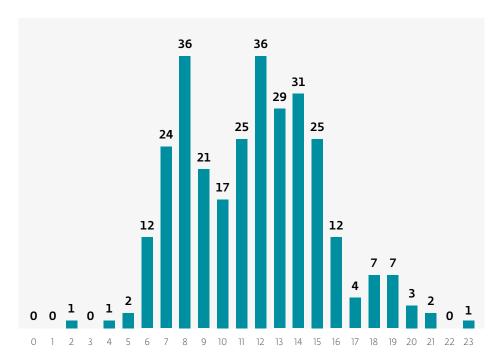


Figure 37. Samples sorted by hour (UTC).

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 Potao 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 *aithub*.

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



Credits

Special thanks to <a>@TheEnergyStory



APPENDIX A. Details Of Prikormka Campaigns

Apr 19 09:11:27 2012 N/A (corrupted) N/A Jul 25 08:31:32 2012 SKt N/A Sep 13 08:21:54 2013 MNa N/A Mar 12 15:17:23 2014 Pgks N/A Jul 15 12:18:51 2014 Abk N/A	
Sep 13 08:21:54 2013 MNa N/A Mar 12 15:17:23 2014 Pgks N/A	
Mar 12 15:17:23 2014 Pgks N/A	1
	1
Jul 15 12:18:51 2014 Abk N/A	1
	1
Oct 03 08:57:13 2014 W_zp7a N/A	1
Nov 05 07:56:00 2014 zma N/A	1
Nov 05 19:30:35 2014 Psep N/A	1
Nov 13 10:20:10 2014 hmod N/A	١
Nov 25 15:12:31 2014 1ff N/A	1
Dec 01 08:07:07 2014 hmyr3 N/A	1
Dec 05 13:11:35 2014 1ii N/A	1
Jan 31 13:19:22 2015 Ivo N/A	1
Feb 10 18:31:49 2015 Pgad5 N/A	١
Feb 19 15:51:33 2015 Pkof N/A	1
Mar 02 16:23:42 2015 Ptrop N/A	١
Mar 11 08:43:12 2015 I01u001 N/A	1
Mar 23 12:46:24 2015 Asap N/A	١
Mar 23 16:03:19 2015 P647 N/A	١
Apr 10 12:26:20 2015 Plg8_ N/A	١
May 06 06:08:52 2015 W_cu6a N/A	1
May 24 08:46:38 2015 Pod13_ N/A	1
Jun 11 14:59:45 2015 Aste N/A	1
Jun 21 15:36:24 2015 MVD_LNR_kontakt 7	
Jun 26 13:25:22 2015 r03u0002 N/A	1
Jun 29 06:19:36 2015 Dmindoh_zb 7	
Jul 0112:42:04 2015 r03u0002 N/A	1

PT Time stamp (UTC)	Campaign ID	Malware Operator ID
Jul 05 06:21:49 2015	Lminfin	7
Jul 09 14:48:56 2015	gm	1
Jul 16 14:29:29 2015	Lmgb	7
Jul 16 14:55:50 2015	Lrod	7
Jul 16 15:03:59 2015	Dmo	7
Jul 18 04:35:41 2015	Lsck3	7
Jul 18 05:07:50 2015	Dmo	7
Jul 19 07:41:54 2015	PMil_6	N/A
Jul 19 08:11:26 2015	PLmgb2	N/A
Jul 20 17:51:04 2015	Psek	7
Jul 21 06:08:53 2015	medium	3
Jul 26 19:17:52 2015	MDLV2	7
Jul 26 19:22:27 2015	OSCE	7
Aug 07 09:23:57 2015	BOY_D	12
Aug 14 06:11:43 2015	BUR	7
Aug 17 17:58:58 2015	RBx	7
Aug 17 18:32:51 2015	MRV1	N/A
Aug 22 11:35:37 2015	D_00732	7
Aug 28 13:42:34 2015	D_xxx	7
Sep 03 12:02:35 2015	zkonv	N/A
Sep 24 16:39:43 2015	L_mgb	7
Oct 13 10:52:47 2015	R_pol_x	7
Oct 13 11:54:58 2015	RF_lgm	7
Oct 14 06:55:23 2015	LKos_xx	7
Oct 21 12:56:05 2015	K83_mo	10
Oct 21 19:33:21 2015	DLB3	7
Oct 22 08:48:26 2015	DLB_sgrish	7



PT Time stamp (UTC)	Campaign ID	Malware Operator ID
Oct 29 14:00:05 2015	FSfarm	11
Oct 30 07:40:28 2015	piter	8
Nov 11 08:57:44 2015	45K_perev	10
Nov 20 16:43:20 2015	30K_alfa	10
Nov 26 12:54:58 2015	REP_L	12
Nov 28 07:39:26 2015	L_K_geniy	7
Dec 03 07:21:31 2015	D_odSD	7
Dec 03 09:40:43 2015	L_min1	7
Dec 03 10:33:27 2015	D_newsG	7
Dec 15 11:48:39 2015	M_raz_	N/A
Dec 18 09:12:40 2015	7_L_xxx	7
Dec 18 12:12:10 2015	33K_pushkin	10
Dec 28 13:57:12 2015	38K_135_vnos	10
Dec 29 14:58:11 2015	Kvk_ham	7
Jan 12 11:44:22 2016	38K_83_parf	10
Jan 14 09:14:22 2016	L_ssa	7
Jan 19 15:30:41 2016	shubin	35
Jan 19 15:31:31 2016	shubin	35
Jan 19 15:33:35 2016	shubin	35
Jan 22 10:04:27 2016	34_Ffot	11
Jan 30 06:38:17 2016	MM_mmh	7
Jan 30 07:56:11 2016	L_m3	7
Feb 01 09:46:49 2016	38_Faro	11
Feb 05 08:00:05 2016	MM_leco	7
Feb 05 08:20:01 2016	MM_1kur	7
Feb 05 08:51:46 2016	L_lm1	7
Feb 08 14:49:52 2016	L_ment	7
Feb 17 15:06:39 2016	sdd1	12
Feb 22 14:25:18 2016	L_rozysk	7
Feb 22 14:29:36 2016	L_rozyskR	7
Feb 25 10:26:58 2016	33K_037	10
Feb 25 14:18:30 2016	F_ego	11

PT Time stamp (UTC)	Campaign ID	Malware Operator ID
Mar 22 15:25:59 2016	sgukiev	11
Apr 08 12:13:20 2016	avl	6
Apr 18 11:10:21 2016	L_ukrB	7
Apr 27 12:40:46 2016	puh	6
May 05 11:42:54 2016	L_gp	7



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.XRA 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\ocp8.1\ %USERPROFILE%\AppData\Local\MMC\ %USERPROFILE%\AppData\Local\PMG\ %USERPROFILE%\AppData\Local\SKC\ %USERPROFILE%\AppData\Local\CMS\ %USERPROFILE%\AppData\Local\VRT\ %USERPROFILE%\AppData\Local\ioctl\ %WINDIR%\nt.shrui.dll %WINDIR%\haut.huid.dll %WINDIR%\hlpuctf.dll %WINDIR%\atiml.dll %WINDIR%\iomus.dll %WINDIR%\swma.dll %WINDIR%\helpldr.dll %WINDIR%\rbcon.ini %USERPROFILE%\AppData\Local\CMS\krman.ini %USERPROFILE%\AppData\Local\VRT\ wputproc.dll

Mutexes

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

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)



SHA-1 hashes

Prikormka droppers:

42041871308B5711041B7AF69B78F45DF642546C 37F75844C0D0F7F80A699153AF131984D2CE2B6D 029F054A52FE93B0CD6C4D1D815A795EAE9CAAB4 66C143D7C33666903B174F4B94D609BE8791914D 60351035ECDEED071E3FB80AFFE08872A0B582C9 0296191B323900B2BC014E2ACB5E0614C679B682 1BF0E90027EF798727A4496B1928F1FA79146051 76CAE58E4DF4D029155BF2E44BA0F8075DC99020 C0FBE31F1E6E56E93932076BA55A5229E22B5C4A CF09B0CD03C9D0553F0B82827C989D04F1A1FAF1 7C28B907E1053F825478A74FDC1090FBF71DD878 D7F35B66C554EE1076279DF54C4E931651A7A211 2B0FB236DDC0098ADDF051531912FC2601FFCCDC EAB122E5857DF838469B5B00DA0A3BD06DF8DA05 00BCCEBB7614BA270CA2908EE5711F25D3740E7E F908824DB35EFD589449D04E41F8BCEA057F6E52 A8CED2FF8F3D4B77160CB81843652D971469A30B 6002357FB96A786401BAA40A89A85DBA3A7D7AD4 E3E9CA2AC83CFADD80FECD002B377B6B41AC5250 EAFC458AAC3F1564E940BAC7D45C1E659636CC86 FCBC8C75246511F9E4D49FE501F956A857FACE84 803C48A93785581AA89422B6B1E73677BF8DC749 87C34623EBEC481FD430F6CE26849220C641742C A1EE4E4BA27B4035F29FA6AB943AE072D42E65B8 19AAB5FAE0809F87EF27A18208A3C0C52DEA182A C88218C2C23555D5E39596B2110BDA54A7AD50DB EC16141D6C0399B74A26B7B572580B3AC4CBC811 76B77E40182DA242307272B9F77132ABB0B46515 7AB44936E5545C5778C697ABCC20FD8955E35F36 86DD049877B564158020AB9B1A6CA3C30371979D 8665C7A753BA5F619FE79D52DC49724F17D81DAC

8839ED42EC1440CBF30CC345F11B88450EA8FE46 4D2C8CD6C514202CBC133347E2C35F63F03A77BF CDF0734730EA786AD2D3B0E9D0D82F85D3C4AD07 99345C5E6FC6901B630C044DD5C6A5015A94B046 93FE501BCDF62060798E35643B7E5F4E3FFF05A6 1287205FE5B83583CB28D39D965D182EA1DFCFDB C0C4DB689F393A26611B7F8FE08F38B456A173DA 3F867CF4AE4B1232B08E40ADABE7BC21EF856FE2 E9A2B1611EDC105FBA65AFFCDAB062D6FA5C67B0 ADDF8193442D145C6BCB4C54B95A5CFE759C6436 CD5AA66AD7C8D418F19B486211591E31B5B74AB6 8A01C06DF6E59F1513146DFE07936E4ACA59B152 E35081B99C5445952AD4E204A4C42F06D7C3707D A6D8431EFBA501864C4646A63071D28B30EEBF99 613F631D0E384954D2FEA5BE39124AD821C8E5D6 D45CECD9DDD79259C6518300ED77257A9ABBDF92 642033A50EF2C51E1F391D85ED870B09A308469A FD95C6B33AF4B29EFBD26D388C50164C3167CB68 9A578C7C305BE62167EF87AB52E59A12F336186A FE9F5018198567F3D3FB3AA09279C65DBE981171 62487DD8EC172462F9B4CBB790EF6F7878D20352 E397F1D784B4A9EEE7EEAC427C549A301DEC0C7C E8A2734C3FFECB76DD4D1C28D646EE59188BE7BF 8DF79B2734BCD83B3D55FF99521D10E550DFCFF3 64D31BBCF8E224E06BB5F1B350D2F18BFDD78A8E D5B785F8F92C7588CFAD7A1A21DAFFA6EB9CFA5C 8327A743756FA1B051725BF8EC3FDD9B9E844E9A 98440EC18A7E78925CB760F5016111115C89F1F8 6E56BC6023085D6E88668D1C66B91AB5AA92F294 160CF2ABB25495188A0ACB523BD201B0369CFFD2 6E5A098A3EDDEEC2E4986DE84FB00D7EA7EE26B8 8358EA16A0DE64994FBECE1AAC69E847F91BB1B3 3A6C8CB6688E2A56057BA9B3680E5911D96B2C8C AB011CD03B3F211F43930AABD909B5611A829D9D 279711B6828B6CF642C0DAB4D16411C87956F566

2BF9CA8B16BCD679AFB6E9E53C3BB0B04E65044A 9551C390B2DF178DED895D531F440FDDBAE122AA BB8D93A4049968C6D5A243DCFB65A6F4B4DE22A2 80CB14652E8251C79187DF8A01D29ABD46A3118C 6E24C24O3DAFAE05C351C5A0A16E2B64O3E0F398 09EA7B2F67797915BBFED16F0B21E4E31F4980A3 0AA48DEE8F528B037D8D72AAD039BB2759F362E3 40D7D09053BF60925CBB820417A42DBC6293E017 A6600BD9752E041ED7EE026123A60B19C96259AB 506CCEBDAC5754D1E20D9C3FB280CEC7782EEA6E 40F33CD2AD98FE1E6BF4AB199021498F9E3125A1 9F03A4E0ACD38635104292B8054485E6BF898C48 B373BF4B3AA28FF6D373DA5EAA848AF9772F6454 FD83C2484E2986F22B09623E5971AA54FBD8BCD3 065B075293968732F2BE433B7B492869E4260EE5 B358687593FEBDFD0E1858726098DCFD61D9F8B5 FD2FBB8E4676673A35276B46F2C74562703BCF39 CCD19FD4A1408FCD855B7909578340846904E707 9D84665C00F81C2835E2A41711A139547351D850 69536CAF0522C1A915D6AC4C65177A26EFA7944B 243421FE7C1FC007EFA0C9CCAB6F6E2A0C94FCC2 5B7D6D7C3C4AD74A7F1E32B780776DB41FF18DDD 4418A32BBD215F5DE7B0063B91731B71804E7225 EE1E5D95FCAD429126944804D80D7C2412AF492E E494328255EF2B9ED9B332EE845513A93339217F 6B53A3A3CB9D87D5925C82839015DAD16042C2FF

Prikormka early versions:

1B8BC6924F4CFC641032578622BA8C7B4A92F65E B5F1B3BD6AD281C8EB9D633A37E0BE63B97A8BEB BCEDAB81CC5F4D2EA1DA8A71F91DF6E16362723B DC52EE62B94DC38790C3EF855CE5773E48D6CD55 44B6B8375CF788076C0DD64A93E27F69A01F5DFD 539033DE14539D485481549EF84C9E49D743FC4C



Prikormka PERSISTENCE modules:

AD9A6F7BA895769844663B4936E776239D3A3D17 E1B5CD1978F6C6D72AA6B07ADD1EE83E9BB8480D 6E312A999EE7DCD9EC8EB4F0A216F50F50EB09F6 8F8BD3C4CE2F932ABFB31B9F586C40D1E22EE210 3F8D8B20B8FCC200939BBB92FB3B93BB3B4ECD24 756730D1C542B57792F68F0C3BC9BCDE149CF7C6 4F1441F16E80272F488BB114DB6508F0BB9B9E1B 2E1C7FFAB7B1047E3438E6BA920D0914F8CC4E35 3C9990B5D66F3AE9AD9A39A10AC6D291DD86A8F9 CC7091228C1B5A0DAF39ECDA570F75F122BE8A16 26FAEAAE2C042C0A416287A7C54D63D5B4C781B3 854F7CB3A436721F445E0D13FB3BEFF11BF4153D 0596EFE47D6C143BE21294EB4E631A4892A0651A 7DAE2A15E364EE06C9301236AE8FC140884CEA95 C2F720DEF2264F08E5211671D46E73311DC6C473 36215D9A691D826E6CEBC65925BFA6B579675158 0354A768508F6B9D88588641397B76A0CBB10BF2 1790B3D73A5DD676D17B39C01A079DEBD6D9F5C5 2F1E4AF1A5A95B3483E901ABDD96454C57419BA4 53174F09C4EDB68ED7D9028B86154B9C7F321A30 FCD81737FF261A84B9899CB713933AA795279364

Prikormka DOWNLOADER modules:

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

Prikormka CORE modules:

2A64606DB1DB872E7176F0C6C3FF932E2146BFC9 328DE44A4B6140EF49CE1465482EFE0E4C195399 520AA689066D0C69F6FD9C623E263211022CCF21 790367A2032951488FC6F56DCF12062AE56CAA61 551CD9D950A9C610E12451550BD6A3FBF5B00B77 EF3244AB1DF7D74F1FC1D8C3AF26A3D3EA4364A5 1636112D8441A6616B68CBE9DC32DDB5D836BBA1 8A57E5EED18A6DB6F221B1B9E8831FE4A9CAD08C DCB813E5D2A1C63027AADC7197FD91505FD13380 A360EAC305946FF468E1A33E84ED38176D95CAC9 8F67C4BD2EE7C68249DCD49AD7A3924D3EC6810C C020EFFD3C7AD06907ECFEA424BE1DCB60C7447D D2A98115DF0C17648CCB653AF649D24B528B471D D7EEB8DB22AAD913B38E695A470E8B2F1440D4D3 154AA820D552ABD65C028DED7E970C8DEFA8C237 83B492A2905CE6ACFADE43AB52BF52E6F02FDCD5

963963004E4CA0D966D84324EC8ED3694F6A7F5B 9DE8860AD499E64F8BDCFC800DDAFF49D4F948E5 C9C2510654081D621A5B1768520D7D7C04219FCB 9D025A015FDB720C0FDEBCFE54661F3ACED94E3E D09B6194453BFC59EB438E455D14621B280DF4A6 1A865E934EFF339A826979C70A2FC055E3C9D12F 4C5F412C915FB3F178A81BC4FBDA336F69A22086 7372639A9E5C274DFFAA35ABF4C8E7A0BEBD4305 311672ECB756E52AD396227DD884D1C47234961A 7A22E549BE02F7F4753BB9CBA34079CEB15CA381 6AB00FCABC6BC06586F749F54C4955592285608C 66248AE0A3D6B5091C629343CC535F98E08A2947 ODD8E1922CEB96061C9F6678728DD45CBDC6F675 A093993B9488A9427300B2AC41460BE8164A0F9A 6D861826206D834A224583898BE6AF1A3D46E7CF 64679BDB8A65D278CDA0975F279D8881E1ABD40A 92476C6AE5F976C58D11BDD956878451F361776D 202637EF3C9B236D62BE627C6E1A8C779EB2976B C41BB97C203D6221FB494D732CB905FF37376622 986E739948E3B5C303F7766F9F9AF3D2E1A5BCA7 3AB61FEC417686AFC1AC430AAF5A17254D05A14A 0D7785E53AB1A7F43902AFF50E7A722C0E0B428F B5EEAE045F1082438E4C7B7F12F7F4630043A48E 57E345893F508F390F2947E83092A47D845EA445 C9756E95679EAD052D53ADCFA39BB4B1402C9126 D864067BFA52383BC012BA1AAF8FFB893D419C07 CDD58347F873EB7E0BC602DA9930A519683C67C7 DFABE31E58334C873AEDD361D69D5C80016F9F42 625D822EE0D95C6E581B929C6C4E4B44D749D2BB A224A76DABE62BD7CA055CA1119108AD5812AF06 E4C56D11E84497EEC3E275043E36845EB2F3F57E B43713CBD307BC12AD7BA61C87975F74221A3439 AED9C3BCA2B42889A9110B92D3D31B5FD3324BDF 6AE2C768D932EDA538983DD7A50CF7DE14BF54D2

4F945A3B3EB058668C3DFC0A8469B42E16C277A7



BE73A2C17AAE689BC1A20761850374636B67BF0F 80FFA899CB3A6595FAFA66421BCCD6E5AAAD8552 7C5F7296DDDA9B188B572DF348843F822BD6ED21 F9EB705D8A1EDC7FF9B93D9CF9211840C4482865 7979BEC789770860A6F12B7A7D41470DE4AFC873 6DF75137E8966537BB921EAB30DF4F7BC2C6FEB4 2115C50CAF8D1B365D78818DF84A8CE29F7FD9E8 AFDAD724A2C351C750DB43688D107B1300B1D1D4 64002D2C4C6678776C64BB018736C9B0745F47F4 7843CB7DE03C8B564FD72D923B4BD6D28A466A3C EB4647CA60FEA9049A34EC59D9658946A2C26D9D ED3D4EEF28174F60F1653F35000B871F6E023D21 860D0CDFC065E91083979DD50A72251C26A638A4 FC2C689C507FED54432AD1726E524B38F52B187A D219640BA205A7013A23BA19CD6C2B32439F105E DE60C2A81AE2F3E5DBD2B2D0DBEBDB56FED62F7C D38FDAE48EABF2642F3327FAC865B079233CC7C6 B23995462751EDFAD19B72BEA4A047CC89533A59 88ED6686CF59F12AA984216EC60097C4BD319007 DEF9B207BFD7C6D4B216DF2B37C33CD851DC7FE1 8D49305FD140B179D2293FBAFF6E7CE46A03AF16 F35B1D2165EC00A56EE6DE89D09963DD3FD02744 B42234F5A5EFB6423E9D4904BA282127F1282C8E 326ADEA3AC1F8FAC3B522E6B47941263DA110A42 3E023A83EAA85A77B935B2D3A00AEB5B1ADCD9CC 129B852E62CB7BF487D5F37E17F6E3CC9A838DB8 F030559F81B8DC3CC0DED6C46C6D1BBB67A2CA65 3C904AFB938EFCF210F388E5AA46379AEADBCD50 D8921385ADAFF131C9D452A4D9BBA2C7D755880E 915F7F5471A94A6E095EE8D90FCFE84E7A5FE1D5 ODB71AA8B51FAACEA7D4C5819EC6AF9C342D02FD A4847B06E603E90640051FCDD5D1515F007F7BD5 7C9E4CC3F5B260439D69E93376AA668BF32123D0 3246B5F43756DC8DC4438933005DF66A3C8CE25F E97B383E3CF55D0792F22D57273C18848B849C6E

7C6FA82657B291FAFE423B7B45D0ED732F4D5352 4595EAB593594860985F5FB501B85386F1F1A5B8 45F1F06C3A27CE8329E2BDCDEEA3C530711B5B72 476DCA86DE7AF1F15327084021A3BB7F42818248 70A362985D5237ACD6282E16A238B0FDB1002A1F 73596D1587549DC234588FCB5666BEEFD7C90D81 97958B3124EC5DCAB64DD88A1E97E6B585B04628 B47640C4952ACC2705F7EAD9E8EAA163059FD659 596F945AB52AE0E780905E150ACD2017AB2ECDFC 5CEFFF9C7D016364D40F841CB74D65BB478BA0C6 424DD485FA8572DB84CF6845C27C1F8679A61AEC 099C5611F3BDBB8D453DFBF7967F30891906FF2C 7C2587B85178AD89389D957F11AF1065C46F66DB 840AFB728FDA57195E53F225CB3F6E788B96A579 12ACC64605D4FE2F3CEEEFBD0A7C4FD655E6AEAA

Prikormka DOCS STEALER modules:

BA434FB6169E8A1785E353EEBF9B907505759A07 A34BD2A059F57FB1FE281A2BD7247A9A72A467B8 04DEB60B6A1D53448EFFB34EA7C55E6916FE32B1 C75D8850273431A41F0EFCF8F74E86BCFE1DFA5A 7C9CB1619FFCF36B32273E1A78A58D817D2B7C8C A580856FA6AC3159F0A7E91D5992810B953A36A1 5C82CA8B2E8320E6B6C071CCB0D4EF9B03001CAA 7275A6ED8EE314600A9B93038876F853B957B316 9286B96452C519D5E1E74D1CDDBDD76B51F4FBAA FAB3B3371AA5878B6508DA487735E3A674A9F61B 0D4839F99C30AD76E082851A214A32116CE932A7 652B012E0ACACB78221CAA7A3C3EE461F07264EA

Prikormka KEYLOGGER modules:

BFDCD0A3F7495C43D8D42B4272BDC90695DC44D7 CC42C6BEEB70D3A9BC7E1159C644E54DE2BE5CBC

6A4F24665569DD61FD29AF8FDCB3E2C90961DFF0 D1DA3076830813EC6FFF0B0DE3462BB5B713A090 E6D92C025CF726B08288B6798AEEFCF550D51C31 0B81BA761C6BA88C0AFC682693D99355E55F5A76 OCDC66ACBB5B7D6FAA85F7DF8D747A96CED7A9BD 194316ADC74AEDED98EE2696B4AB54900A6EDF15 45959818DBA4924E129E22CF1B0BDF02C2DD7B49 820EAC424FC27296FE725E1C5DAA8F6C53E104A7 25D6F1EFD758AACE399C6D62A89BE039281CFF69 722E1CDA3C516D43F17A6D4F5F1390D16113BC30 DE966273DD5AD4DAA01562109932EBD39A13A5A2

Prikormka SCREENSHOTS modules:

645DFA35E41F6442793CF7647A75956E05563DE8 AD74ABEA34A20D0196A152E66668E3C29135B22D4

Prikormka MICROPHONE modules:

FCE83DF7018A49072F9A28A8E135EB00C011D9EB 2C76974722287C7CDB0FCA2BC6CCEDEE62E77D24

Prikormka SKYPE modules:

C3AA3DBD33751F85002F2F65562098F516737435 2A0EA9E0F3F8E6507D212640594ACF52910275E9 1BB3BBCA79BA45E4215DFC2A6960E03BA60A2B71 OCB528C69706A6513A0E70D3A07A75822F79E6EC 423BCEFC82A14258BDC2CD9740454D28F894DC06 FEAB6E92B905114980B5633F8742E4A7DCD0B4FA BB6CE0957F7E8430007FA4DE1E47C190E1C97AC5 658DF9B4BB13459A9507466BB7D22B723C85D1C5 6C24E244A0DDA2CADED4D1B5CC8B820A46DC19F4



Prikormka LOGS_ENCRYPTER modules:

D5C2C7C3D670D63AD6998848747A0418665EA2CB 352C36ED1BF7EB74C9649615F9A40C13D80EE55D 6740A385AB33B9CC3EC22FB7971F93538BE44997 22F10F17AB9F18D9BF1FE9EEEA413A9787B29D4C E95458CA9663E4FAB94DD232121D5E994A76015D 2BD3FE012486BD89C87858CC4C3DC9D86742738C

Prikormka GEOLOCATION modules:

50CCCD576A815AC8EFFB160A628646C876DF8CB0

Prikormka OS_INFO modules:

4B8EE967F44ECA2EEB3B8420A858CECFE0231208 72C17994336FE4E1B3CF0D7A6CBC45AA43A8DDF0 824F0E198A8A6E08FB95920AEF06870A6305FE3F 6C902496AC1FEF60D343B03822F49DB5F66BE038

Prikormka PASSWORDS modules:

B986114C5173052FCB9583A55D5099D99B709352 17F5E1FC52D6C617CD81B0983B70FAC7A60F528C

Prikormka FILE_TREE modules:

3EDD14E6FA0297ED3162D7F119D8D126662ED28B 2A5AF8E43887051C1F1B488756AAC204B95561CE 4E40286676FCBAC48070BA86B72761A21AC2466C 3E4BE58421DBAEA7651DA13B16CB900DB82A7DEF D1396938E981DD807103B7B9F9442B99952C21AA 74CDA4D4C776CA2A661AC49B6D0E0F0560380A04 8EFDC716FDFD704EC0296860E61AFF9C952946D4 93E196B59771647828BBC3C3B61831150FE1FE02 8384ED4EA9E299306F15A1082231C427A8742271 6E70BE32954E41FAFFC496EAF890B279832B4530 8EA98A8D3D8F62C4543B3DD36E6D6F79F1ACB9E7

