

**Forensics [INFO-Y119]**

report

---

## **Project :Cyber forensics case study**

---

*Authors:*

Siéwé Kouéta ANICET : 00364245

*Professor: R.M.A*

Georgi NIKOLOV



UNIVERSITÉ LIBRE DE BRUXELLES

**ULB**

December 20, 2020

## Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Overview</b>	<b>3</b>
2.1	Investigation Tools . . . . .	3
2.2	Analysis of the PC Information . . . . .	3
2.3	The Target Subject PC Information . . . . .	3
<b>3</b>	<b>The Beginning of the Investigation</b>	<b>4</b>
3.1	Identification of unreliable processes . . . . .	4
3.2	Network connection analysis . . . . .	8
3.3	Look for evidence of code injection . . . . .	11
3.4	Hard disk analysis. . . . .	13
3.4.1	Extraction of objects and data. . . . .	13
<b>4</b>	<b>QUESTIONS FROM THE INVESTIGATOR</b>	<b>14</b>
4.1	summary of the attack . . . . .	14
4.2	Event calendar . . . . .	14
4.3	user involvement . . . . .	21

## List of Figures

1	imageinfo Result . . . . .	4
2	malfind Result (explorer.exe Pid:5052) . . . . .	5
3	Caption . . . . .	6
4	executable.3124.exe (IIwRWgTR) Scan result by virustotal . . . . .	6
5	executable.5052.exe (explorer) Scan result by virustotal . . . . .	6
6	handles Result for PID=3124 . . . . .	7
7	handles Result for PID=5052 . . . . .	7
8	netscan Result . . . . .	8
9	IP address of C2 . . . . .	9
10	IP address of second C2 . . . . .	9
11	yarascan Result for 239.255.255.250 . . . . .	11
12	pid:296 filter on pslist Result . . . . .	12
13	\$strings Data/3124.dmp   egrep 'document' Result . . . . .	12
14	search 239.255.255.250 in 3124.dmp.tx Result . . . . .	13
15	shema of attaker scenario . . . . .	14
16	att.ker.1n@gmail.com <b>to</b> vlc.t1m.m3r@gmai.com . . . . .	15
17	att.ker.1n@gmail.com <b>to</b> vlc.t1m.m3r@gmai.com . . . . .	15
18	vlc.t1m.m3r@gmai.com <b>to</b> att.ker.1n@gmail.com . . . . .	15
19	vlc.t1m.m3r@gmai.com <b>to</b> att.ker.1n@gmail.com . . . . .	16
20	vlc.t1m.m3r@gmai.com <b>to</b> att.ker.1n@gmail.com . . . . .	16
21	vlc.t1m.m3r@gmai.com <b>to</b> att.ker.1n@gmail.com . . . . .	17
22	att.ker.1n@gmail.com <b>to</b> vlc.t1m.m3r@gmai.com . . . . .	17
23	vlc.t1m.m3r@gmai.com <b>to</b> att.ker.1n@gmail.com . . . . .	18
24	att.ker.1n@gmail.com <b>to</b> vlc.t1m.m3r@gmai.com . . . . .	18
25	att.ker.1n@gmail.com(WeTranfert) <b>to</b> vlc.t1m.m3r@gmai.com . .	19
26	content of the file <b>slack.zip</b> download with WeTransfer . . . . .	19
27	modification ASEP HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run par <b>slack.exe</b> . . . . .	19
28	localisation IIwRWgTR.exe in the system . . . . .	20
29	attempt to connect to the central server with FileZilla . . .	20
30	central server connection . . . . .	20
31	FileZilla connection to the central server . . . . .	21
32	FileZilla connection to the central server . . . . .	21
33	content of DO_NO_FORGET.txt file . . . . .	21

## 1 Introduction

This report explains the way and the steps that allowed us to solve and identify the challenge of the investigation on GAST. This analysis is performed on a sample memory and a hard disk backup. That required a detailed volatility investigation and also some Windows malware analysis skills.

### Challenge Questions

1. Give an executive summary of what happened based on your findings.
2. What is the exact timeline of the events that lead to the incident as far as the Windows workstation is concerned?
3. was the workstation's user implicated in the incident, and if so:
  - a. was he willfully committing sabotage,
  - b. was he of good faith but negligent, or
  - c. was he acting responsibly and could not have prevented the incident?
4. what are the elements of evidence you have collected that support your answers to the previous questions?

## 2 Overview

### 2.1 Investigation Tools

Throughout this investigation, the main tools used are as follows:

tool name	version	sources
volatility Framework	2.5	<a href="https://www.volatilityfoundation.org/">https://www.volatilityfoundation.org/</a>
Autopsy	v4.17.0	<a href="https://www.autopsy.com/">https://www.autopsy.com/</a>
Atom	1.51.0	<a href="https://atom.io/">https://atom.io/</a>
IDA64	1.51.0	<a href="https://www.hex-rays.com/products/ida/support/download_freeware/">https://www.hex-rays.com/products/ida/support/download_freeware/</a>
virustotal	- -	<a href="https://www.virustotal.com/gui/">https://www.virustotal.com/gui/</a>

### 2.2 Analysis of the PC Information

The memory analysis was performed on an Ubuntu virtual machine, viewed with VMware on a MacOS laptop.

	Physical PC	Virtual pc (vmware Fusion 11.02)
<b>OS</b>	MacOS 10.15.6	Ubuntu 14.04.5 LTS
<b>RAM</b>	16 Go	4 Go
<b>CPU</b>	Intel Core i7 6 cœurs	- -
<b>HDD</b>	1 To	100 Go

### 2.3 The Target Subject PC Information

The environment and the data about the victim PC are as follows:

OS	Windows 7		
	File Name	File Type	File size
Memory	memcapture.ad1 memdump.mem pagefile.sys	Access Data 1 FoxPro Variable File Windows System File	701.3 Mo 1.07 Go 1.46 Go
hard disk	Image_Win_7.E01 Image_Win_7.E02 ... ... Image_Win_7.E15	Encase Image File Format Encase Image File Format Encase Image File Format Encase Image File Format Encase Image File Format	16 Go 16 Go 1.57 Go 1.57 Go 1.33 Go

### 3 The Beginning of the Investigation

It is a question of presenting how the questions were approached and resolved. The questions were not answered in order; they were understood as the survey progressed. This analysis part is written linearly over time to show our approach rather than sorting it by question number.

With the plugin `imageinfo` we determined which operating system was installed on the victim machine. The result in figure 1 reported Windows 7 SP1 x86.

```
forensics@slifftworkstation:~/Desktop/forensics/Nextcloud-Win7_memory_dump\$ volatility -f memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.5
INFO : volatility.debug : Determining profile based on KDBG search...
INFO : volatility.debug : Suggested Profile(s) : Win7SP1x86_0x1000KDBG
          AS Layer1 : 0x33PagedMemoryPage (Kernel AS)
          AS Layer2 : fileAddressSpace ('/home/forensics/Desktop/forensics/Nextcloud-Win7_memory_dump/mendump.nen')
          PAE type : PAE
          DTB : 0x1850000L
          KDBG : 0x8297bde8L
          Number of Processors : 1
          Image Type (Service Pack) : 1
          KPCR for CPU 0 : 0xb39be000L
          KUSER_SHARED_DATA : 0xf7fd0000L
          Image local date and time : 2020-03-20 13:01:27 UTC+0000
          Image local date and time : 2020-03-20 14:01:27 +0100
forensics@slifftworkstation:~/Desktop/forensics/Nextcloud-Win7_memory_dump\$
```

Figure 1: `imageinfo` Result

#### 3.1 Identification of unreliable processes

**NOTE:** : To better analyze the result of `certainty` command, the data flow of these have been directly saved in a `*.txt` file.

We first investigated whether there were any known malicious processes. `malfind` allows you to find codes/DLLs hidden or injected into memory.

```
#volatility -f memdump.mem --profile=Win7SP1x86 malfind >| Data/
malfind.txt
```

The results of figure 2 show us two processes that caught our attention: (**explorer.exe Pid: 5052** **IwRWgTR.exe Pid: 3124**) because although they differ, they have the same signature

### 3.1 Identification of unreliable processes

5

```

Process: explorer.exe Pid: 5052 Address: 0x3930000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 33, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x39300000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x39300010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x39300020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x39300030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x39300040 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x39300050 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x39300060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x39300070 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x39300080 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x39300090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x393000a0 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x393000b0 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x393000c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x393000d0 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x393000e0 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x393000f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x39300100 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x39300110 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x39300120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x39300130 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x39300140 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x39300150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x39300160 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x39300170 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x39300180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x39300190 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x393001a0 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x393001b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x393001c0 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x393001d0 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x393001e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x393001f0 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x39300200 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x39300210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x39300220 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x39300230 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x39300240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x39300250 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x39300260 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x39300270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x39300280 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x39300290 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x393002a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x393002b0 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0x393002c0 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
0x393002d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x393002e0 db 0x80
0x393002f0 dd 0x0

```

Figure 2: malfind Result (explorer.exe Pid:5052)

```

1 Process: llwRWgTR.exe Pid: 3124 Address: 0x18c0000
2 Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
3 Flags: CommitCharge: 33, MemCommit: 1, PrivateMemory: 1, Protection: 6
4
5 0x018c0000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
6 0x018c0010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@....
7 0x018c0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
8 0x018c0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

In addition to two other processes identified above, **Process: Dropbox.exe Pid: 3832** also caught our attention.

To verify this, we have, with the plugin `pstree` browsed the list of processes.

```
#volatility -f memdump.mem --profile=Win7SP1x86 pstree >| Data/pstree.txt
```

	Name	Pid	PPid	Thds	Hnds	Time
1						
2						
3	. 0x84b2dd20 :llwRWgTR.exe	3124	3256	4	1161	2020-03-20 09:57:36
4	.. 0x84aea7d8 :PING.EXE	2932	3124	0	-----	2020-03-20 10:23:52
5	.. 0x84be7900 :PING.EXE	5564	3124	0	-----	2020-03-20 10:22:48
6	.. 0x84ae84b8 :PING.EXE	3260	3124	0	-----	2020-03-20 10:23:17
7	/	*				
8	[snip 93 PING.EXE processes]	*				
9	/	*				
10	.. 0x84b01a10 :PING.EXE	1968	3124	0	-----	2020-03-20 10:24:54
11	.. 0x8431e030 :PING.EXE	1628	3124	0	-----	2020-03-20 10:22:48
12	.. 0x859cfb00 :PING.EXE	3628	3124	0	-----	2020-03-20 10:22:48
13	... 0x851b86a8 :Dropbox.exe	3832	3628	93	1643	2020-03-20 08:06:55
14	.... 0x84beda98 :QtWebEnginePro	3212	3832	14	209	2020-03-20 08:08:47
15	.... 0x8433d878 :Dropbox.exe	5640	3832	5	227	2020-03-20 08:06:55
16	.... 0x8515fd20 :Dropbox.exe	5836	3832	7	79	2020-03-20 08:06:55

Note that the suspicious process **llwRWgTR.exe** (line 3) could be identified between the normal processes and has as child process of **Dropbox.exe** (line 13,15-16).

With "procdump" we have dumped the executable of the process **llwRWgTR.exe Pid: 3124** and **explorer.exe Pid: 5052**.

Figure 3: Caption

```

1  \$ volatility -f memdump.mem --profile=Win7SP1x86 procdump -p 3124,5052 --dump-
2    dir=Data/
3
4 Volatility Foundation Volatility Framework 2.5
5 Process (V) ImageBase Name Result
6
7 0x85994030 0x003d0000 explorer.exe OK: executable.5052.exe
8 0x84b2dd20 0x00400000 llwRWgTR.exe OK: executable.3124.exe

```

Then scan these executables with virustotal 2.1 to get more details about these processes.

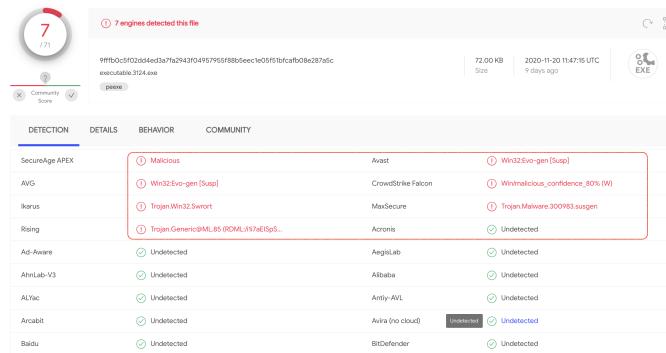


Figure 4: executable.3124.exe (llwRWgTR) Scan result by virustotal



Figure 5: executable.5052.exe (explorer) Scan result by virustotal

The result of figure 4 shows that **llwRWgTR.exe Pid: 3124** is a malicious program and contains the following malware:

- **Malicious**
- **Win32:Evo-gen [Susp]:[1](0, ), [2](0, )** Can Download and install other malware, log keystrokes and sites user visits, send PC information including usernames and browsing history to remote malicious hacker, ...
- **Trojan.Win32.Swroot [3](0, ), [4](0, )** may allow a malicious hacker to gain access to the PC
- **Trojan.Generic@ML.85 (RDML:/i1i7aEISpS5vybR [5](0, )** is ransomware used by internet crooks to demand ransom payment from target.
- **malware \_ confidence \_ 80% (W) [6](0, )** can modify system files, add new folders, create Windows tasks and display advertisements on computers and web browsers.

- **Trojan.Malware.300983.susgen** [7](0, ), [8](0, ) is a Trojan horse commonly used for spying and distributing ransomware

And those in figure 5 shows that **explorer.exe Pid: 5052** has been infected by two malicious programs:

- **malware\_confidence\_80% (W)**
- **DFI - Suspicious PE** [9](0, ) can also modify system files, create new virus folders and install new Windows services in order to infect and compromise the PC

How hackers got to steal documents, with the plugin "handles" we tried to check files handled by malicious processes.

```
$ volatility -f memdump.mem --profile=Win7SP1x86 handles -p 3124 -t
file >| Data/handles_3124.txt
```

Offset(V)	Pid	Handle	Access Type	Details
0x85e3f3cd	3124	0x188	0x120195 File	\Device\NamedPipe
0x8514fd0d8	3124	0x2c	0x120189 File	\Device\NamedPipe
0x84fad850	3124	0x30	0x120196 File	\Device\NamedPipe
0x84a09bbd0	3124	0x3c	0x120189 File	\Device\NamedPipe
0x85c574fd	3124	0x40	0x120191 File	\Device\NamedPipe
0x85bad1b1	3124	0x68	0x160191 File	\Device\Afd\Endpoint
0x85cef630	3124	0x74	0x100001 File	\Device\KsecD0
0x8414d040	3124	0x7c	0x100001 File	\Device\KsecD0\p1\
0x85hc1980	3124	0x188	0x100000 File	\Device\Nsi
0x8426eb0b	3124	0x190	0x120191 File	\Device\NamedPipe
0x851c27fe	3124	0x198	0x120189 File	\Device\NamedPipe
0x85bf8996	3124	0x19c	0x120189 File	\Device\NamedPipe
0x8414da0c8	3124	0x1a0	0x120196 File	\Device\NamedPipe
0x849493d0	3124	0x1a4	0x120196 File	\Device\NamedPipe
0x851fa388	3124	0x1ac	0x120196 File	\Device\NamedPipe
0x84e25d8b	3124	0x1b0	0x120189 File	\Device\NamedPipe
0x8434d3f0	3124	0x1b8	0x120191 File	\Device\NamedPipe
0x850d1280	3124	0x1bc	0x120191 File	\Device\NamedPipe
0x850d1d00	3124	0x1c0	0x120189 File	\Device\NamedPipe
0x849493e0	3124	0x1c4	0x120196 File	\Device\NamedPipe
0x84e12036	3124	0x1d0	0x120189 File	\Device\NamedPipe
0x8586e970	3124	0x1db	0x120196 File	\Device\NamedPipe
0x85125440	3124	0x1dc	0x120196 File	\Device\NamedPipe
0x859493d0	3124	0x1e0	0x120191 File	\Device\NamedPipe
0x85a5d5ebe	3124	0x1e8	0x120189 File	\Device\NamedPipe
0x842a3a3b	3124	0x1fc	0x120191 File	\Device\NamedPipe
0x859493d4	3124	0x1fd	0x120196 File	\Device\NamedPipe
0x84e41838	3124	0x204	0x120189 File	\Device\NamedPipe
0x851d6600	3124	0x208	0x120191 File	\Device\NamedPipe
0x850ff480	3124	0x20c	0x120189 File	\Device\NamedPipe
0x852d2b0d	3124	0x210	0x120189 File	\Device\NamedPipe
0x8597b100	3124	0x214	0x100020 File	\Device\HarddiskVolume1\Users\TimmersVic\Documents\personal
0x8531d054	3124	0x218	0x100000 File	\Device\KsecD0
0x85180f80	3124	0x22c	0x100020 File	\Device\HarddiskVolume1\Windows\winxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0_7601.24388_none_2b2853e245779417	3124	0x238	0x120191 File	\Device\NamedPipe

Figure 6: handles Result for PID=3124

Offset(V)	Pid	Handle	Access Type	Details
0x85990310	3052	0xc	0x100020 File	\Device\HarddiskVolume1\Users\TimmersVic\Downloads
0x84e444ccf1df_6.0_7601.24388_none_2b2853e245779417	3052	0x100020 File	\Device\HarddiskVolume1\Windows\winxs\x86_microsoft.windows.common-	
0x849493d0	3052	0x144	0x100020 File	\Device\HarddiskVolume1\Windows\winxs\x86_microsoft.windows.common-
0x84e444ccf1df_6.0_7601.24388_none_2b2853e245779417	3052	0x1ec	0x100020 File	\Device\HarddiskVolume1\Windows\winxs\x86_microsoft.windows.common-
0x849493d0	3052	0x1fd	0x100020 File	\Device\HarddiskVolume1\Windows\winxs\x86_microsoft.windows.common-
0x84e444ccf1df_6.0_7601.24388_none_2b2853e245779417	3052	0x204	0x100020 File	\Device\HarddiskVolume1\Windows\winxs\x86_microsoft.windows.common-
0x849493d0	3052	0x208	0x100020 File	\Device\HarddiskVolume1\Windows\winxs\x86_microsoft.windows.common-
0x84e444ccf1df_6.0_7601.24388_none_2b2853e245779417	3052	0x210	0x100020 File	\Device\HarddiskVolume1\Windows\winxs\x86_microsoft.windows.common-
0x84e444ccf1df_6.0_7601.24388_none_2b2853e245779417	3052	0x214	0x100020 File	\Device\HarddiskVolume1\Users\TimmersVic\Documents\personal
0x84e444ccf1df_6.0_7601.24388_none_2b2853e245779417	3052	0x218	0x100000 File	\Device\KsecD0
0x8595b64144ccf1df_6.0_7601.24388_none_2b2853e245779417	3052	0x22c	0x100020 File	\Device\HarddiskVolume1\Windows\winxs\x86_microsoft.windows.common-
0x84e444ccf1df_6.0_7601.24388_0x100020	3052	0x238	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x23c	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x240	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x244	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x248	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x252	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x256	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x260	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x264	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x268	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x272	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x276	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x280	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x284	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x288	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x292	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x296	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2a0	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2a4	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2a8	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2b2	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2b6	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2b8	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2bc	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2d0	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2d4	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2d8	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2dc	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2e0	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2e4	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2e8	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2f2	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2f6	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2f8	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x2fc	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x300	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x304	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x308	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x312	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x316	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x320	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x324	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x328	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x332	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x336	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x340	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x344	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x348	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x352	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x356	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x360	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x364	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x368	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x372	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x376	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x380	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x384	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x388	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x392	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x396	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3a0	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3a4	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3a8	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3b2	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3b6	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3b8	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3bc	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3d0	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3d4	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3d8	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3dc	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3e0	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3e4	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3e8	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3f2	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3f6	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3f8	0x120191 File	\Device\NamedPipe
0x8595b64144ccf1df_6.0_7601.24388_0x100020	3052	0x3fc		

### 3.2 Network connection analysis

Likewise, the figure 7 shows that the process **explorer.exe Pid: 5052** has had access to the personal document of the user *TimmersVic*, particularly the "Project AMAR" folder.

### 3.2 Network connection analysis

The "netscan" plugin helped us to list open network connections on the system.

Offset(P)	Proto	Local Address	Foreign Address	State	PId	Owner	Created
0x1f4241f0	TCPv4	192.168.0.109:53757	0.0.0.0:0	LISTENING	436	services.exe	
0x1f5f52d48	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	436	services.exe	
0x1f63dcdb8	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	436	services.exe	
0x1f4241f0	TCPv4	192.168.0.109:53757	172.21.0.6:80	ESTABLISHED	-1		
0x2e47d3c0	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	452	lsass.exe	
0x2e47d3c0	TCPv4	:::49156	:::0	LISTENING	452	lsass.exe	
0x2d0190948	UDPv6	fe80::88dc:87f4%bed6:89b0::7329	1*	2396	svchost.exe	2020-03-07 11:41:32 UTC+0000	
0x2d4ec1cb8	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	436	services.exe	
0x2d4ec1cb8	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	436	services.exe	
0x2d5d68998	UDPv6	fe80::88dc:87f4%bed6:89b0::7329	1*	2396	svchost.exe	2020-03-07 11:41:32 UTC+0000	
0x3e4d65c8	UDPv4	192.168.0.109:137	*,*	4	System	2020-03-07 11:39:30 UTC+0000	
0x3e5051508	UDPv6	0.0.0.0:137	0.0.0.0:0	LISTENING	2396	svchost.exe	2020-03-07 11:39:30 UTC+0000
0x3e5051508	UDPv6	192.168.0.109:138	*,*	4	System	2020-03-07 11:39:30 UTC+0000	
0x3e51d4d88	UDPv4	0.0.0.0:0	*,*	1112	svchost.exe	2020-03-07 11:39:30 UTC+0000	
0x3e51d4d88	UDPv6	0.0.0.0:0	*,*	1112	svchost.exe	2020-03-07 11:39:30 UTC+0000	
0x3e6918608	UDPv4	0.0.0.0:5355	*,*	1112	svchost.exe	2020-03-07 11:39:30 UTC+0000	
0x3e6918608	UDPv4	0.0.0.0:0	*,*	2628	svchost.exe	2020-03-07 11:39:42 UTC+0000	
0x3e6918608	UDPv6	0.0.0.0:0	*,*	2628	svchost.exe	2020-03-07 11:39:42 UTC+0000	
0x3e6918608	UDPv6	192.168.0.109:137	*,*	2628	svchost.exe	2020-03-07 11:39:42 UTC+0000	
0x3e2a7cd0	TCPv4	0.0.0.0:22	0.0.0.0:0	LISTENING	1832	sshd.exe	
0x3e2a7cd0	TCPv4	0.0.0.0:22	0.0.0.0:0	LISTENING	1832	sshd.exe	
0x3e2a7cd0	TCPv6	:::22	:::0	LISTENING	1832	sshd.exe	
0x3e2a9f58	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System	
0x3e2a9f58	TCPv6	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System	
0x3e411a70	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	340	wlinit.exe	
0x3e411a70	TCPv6	0.0.0.0:49152	0.0.0.0:0	LISTENING	340	wlinit.exe	
0x3e411a70	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	676	svchost.exe	
0x3e41b348	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	676	svchost.exe	
0x3e41b348	TCPv6	:::135	:::0	LISTENING	724	svchost.exe	
0x3e457d98	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	724	svchost.exe	
0x3e457d98	TCPv6	0.0.0.0:49153	0.0.0.0:0	LISTENING	724	svchost.exe	
0x3e45a328	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	724	svchost.exe	
0x3e45a328	TCPv6	0.0.0.0:49153	0.0.0.0:0	LISTENING	724	svchost.exe	
0x3e4fc360	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	916	svchost.exe	
0x3e4fc360	TCPv6	0.0.0.0:49154	0.0.0.0:0	LISTENING	916	svchost.exe	
0x3e5139008	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	916	svchost.exe	
0x3e5139008	TCPv6	0.0.0.0:49154	0.0.0.0:0	LISTENING	916	svchost.exe	
0x3e2b8d30	TCPv4	192.168.0.109:56836	192.168.1.10:22	ESTABLISHED	-1		

Figure 8: netscan Result

Figure 8 shows some connections with invalid PIDs and their missing process names. Based on the branch network architecture and the fact that most malware will necessarily have network activity, we have refined our research to only have network connections that are either open, closed, or pending. 'to be closed:

1	\\$volatility -f memdump.mem --profile=Win7SP1x86 netscan   egrep '(ESTABLISHED CLOSED CLOSE_WAIT)'
Volatility Foundation Volatility Framework 2.5	
3	0x1f4241f0 TCPv4 192.168.0.109:53757 172.21.0.6:80 ESTABLISHED -1
4	0x3e2b8d30 TCPv4 192.168.0.109:56836 192.168.1.10:22 ESTABLISHED -1
5	0x3e45cc00 TCPv4 127.0.0.1:52310 127.0.0.1:52309 ESTABLISHED -1
6	0x3e4e3b40 TCPv4 127.0.0.1:52311 127.0.0.1:52312 ESTABLISHED -1
7	0x3e4ee538 TCPv4 127.0.0.1:52329 127.0.0.1:52328 ESTABLISHED -1
8	0x3e569520 TCPv4 127.0.0.1:53782 127.0.0.1:53781 ESTABLISHED -1
9	0x3e670aa8 TCPv4 127.0.0.1:51185 127.0.0.1:51184 ESTABLISHED -1
10	0x3e74f0f8 TCPv4 192.168.0.109:53719 172.21.0.6:80 ESTABLISHED -1
11	0x3e78b348 TCPv4 127.0.0.1:57900 127.0.0.1:57901 ESTABLISHED -1
12	0x3e7c5780 TCPv4 127.0.0.1:52312 127.0.0.1:52311 ESTABLISHED -1
13	0x3ecf4b78 TCPv4 127.0.0.1:53745 127.0.0.1:53746 ESTABLISHED -1
14	0x3ed5d480 TCPv4 127.0.0.1:53607 127.0.0.1:53606 ESTABLISHED -1
15	0x3ee664e0 TCPv4 127.0.0.1:57904 127.0.0.1:57905 ESTABLISHED -1
16	0x3ef08de8 TCPv4 127.0.0.1:52315 127.0.0.1:52316 ESTABLISHED -1
17	0x3ef589b0 TCPv4 127.0.0.1:53746 127.0.0.1:53745 ESTABLISHED -1
18	0x3ef706c0 TCPv4 127.0.0.1:57901 127.0.0.1:57900 ESTABLISHED -1
19	0x3efa9438 TCPv4 192.168.0.109:57903 192.228.79.201:80 CLOSED -1
20	0x3f0370c0 TCPv4 127.0.0.1:57905 127.0.0.1:57904 ESTABLISHED -1
21	0x3f037c10 TCPv4 192.168.0.109:57372 162.125.36.1:443 CLOSE_WAIT -1
22	0x3f1a8de8 TCPv4 192.168.0.109:53674 108.177.126.109:993 ESTABLISHED -1
23	0x3f428390 TCPv4 192.168.0.109:52877 52.41.39.5:443 ESTABLISHED -1
24	0x3f4c1de8 TCPv4 127.0.0.1:52328 127.0.0.1:52329 ESTABLISHED -1
25	0x3f4f9868 TCPv4 192.168.0.109:53511 162.125.65.3:443 CLOSE_WAIT -1
26	0x3f5249b8 TCPv4 127.0.0.1:52316 127.0.0.1:52315 ESTABLISHED -1
27	0x3f52ebb0 TCPv4 192.168.0.109:53592 162.125.65.3:443 CLOSE_WAIT -1
28	0x3fcc0af0 TCPv4 127.0.0.1:53081 127.0.0.1:53080 ESTABLISHED -1
29	0x3fd529f8 TCPv4 127.0.0.1:51184 127.0.0.1:51185 ESTABLISHED -1
30	0x3fd55330 TCPv4 127.0.0.1:57906 239.255.255.250:443 CLOSED -1

### 3.2 Network connection analysis

9

31	0x3fd86de8	TCPv4	127.0.0.1:57910	239.255.255.250:443	CLOSED	-1
32	0x3fd91008	TCPv4	127.0.0.1:52309	127.0.0.1:52310	ESTABLISHED	-1
33	0x3fa6370	TCPv4	127.0.0.1:53606	127.0.0.1:53607	ESTABLISHED	-1
34	0x3fdc4ad8	TCPv4	192.168.0.109:57267	34.225.12.148:443	CLOSE_WAIT	-1
35	0x3fdca4f0	TCPv4	127.0.0.1:53080	127.0.0.1:53081	ESTABLISHED	-1
36	0x3fdd21f8	TCPv4	127.0.0.1:53781	127.0.0.1:53782	ESTABLISHED	-1

From this result, we deduce that the Windows 7 victim machine had the address **192.168.0.109**, because this address is in the range of the intranet subnet of the subsidiary.

We can also see (line N 4) that the central server where the documents and codes are downloaded is **192.168.1.10**, because we have an SSH connection (port 22) on it.

After excluding his two addresses, we had to identify the following addresses:

- 172.21.0.6:80 (line 3)
- 192.228.79.201:80 (line 19)
- 162.125.36.1:443 (line 21)
- 108.177.126.109:993 (line 22)
- 52.41.39.5:443 (line 23)
- 162.125.65.3:443 (line 25)
- 239.255.255.250:443 (line 30)
- 34.225.12.148:443 (line 34)

By analyzing the logs of network equipment, we noticed that the address 172.21.0.6 established several connections with the machine in the branch's subnet (192.168.0.110) (See figure 9)

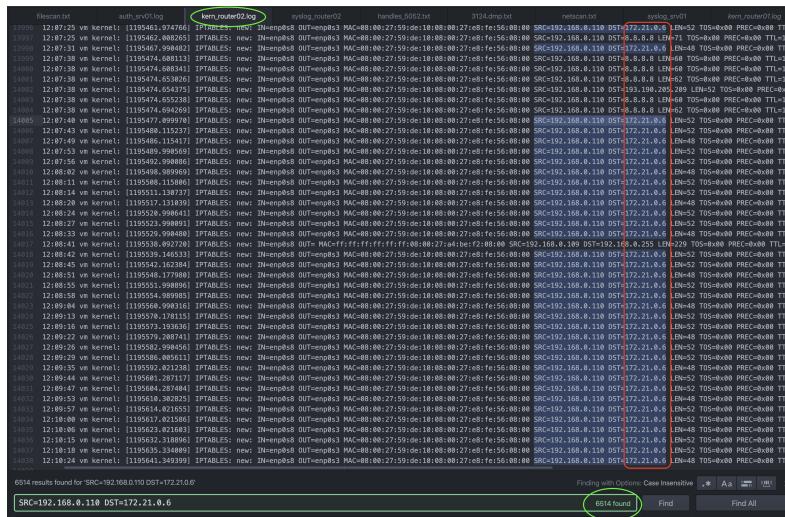


Figure 9: IP address of C2

Likewise the address 52.41.39.5 establishes a single connection with the victim machine Windows 7 (192.168.0.109) (See figure 10)

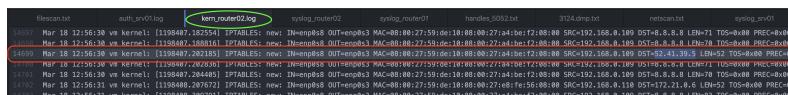


Figure 10: IP address of second C2

192.228.79.201 (line 19) is a DNS server of B.Root-Server-OPS [10](0, ), [11](0, ).

```

1 \$ whois 192.228.79.201
2
3 refer: whois.arin.net
4 inetnum: 192.0.0.0 - 192.255.255.255
5 organisation: Administered by ARIN
6 status: LEGACY
7
8 [snip]
9
10 OrgName: B. Root-Server-OPS
11 OrgId: BROOT
12
13 [snip]
```

162.125.36.1 (ligne 21) and 162.125.65.3 (line 25)  
belong to *Dropbox*

```

1 \$ whois 162.125.36.1
2 [snip]
3
4 NetRange: 162.125.0.0 - 162.125.255.255
5 CIDR: 162.125.0.0/16
6 NetName: DROPB
7 NetHandle: NET-162-125-0-0-1
8 Parent: NET162 (NET-162-0-0-0-0)
9 NetType: Direct Assignment
10 OriginAS:
11 Organization: Dropbox, Inc. (DROPB)
12 RegDate: 2015-11-20
13 Updated: 2015-11-20
14 Ref: https://rdap.arin.net/registry/ip/162.125.0.0
15
16 [snip]
```

108.177.126.109 (line 22) Belong to Google, as it connects to port 993 with IMAP protocol [12](0, ), we can suggest that it is the Gmail mail server or all other Google service linked to messaging.

```

1 \$ whois 108.177.126.109
2 [snip]
3
4 NetRange: 108.177.0.0 - 108.177.127.255
5 CIDR: 108.177.0.0/17
6 NetName: GOOGLE
7 NetHandle: NET-108-177-0-0-1
8 Parent: NET108 (NET-108-0-0-0-0)
9 NetType: Direct Allocation
10 OriginAS: AS15169
11 Organization: Google LLC (GOGL)
12 RegDate: 2012-03-07
13 Updated: 2012-03-07
14 Ref: https://rdap.arin.net/registry/ip/108.177.0.0
15 OrgName: Google LLC
16
17 [snip]
```

52.41.39.5:443 (line 23) and 34.225.12.148 (line 34) were servers hosted on the Ama-

zon cloud

```

1  \$ whois 34.225.12.148
2  [snip]
3
4  Organization: Amazon Technologies Inc. (AT-88-Z)
5  RegDate: 2016-09-12
6  Updated: 2016-09-12
7  Ref: https://rdap.arin.net/registry/ip/34.192.0.0
8
9  [snip]
```

### 3.3 Look for evidence of code injection

As 239.255.255.250:443 is a multicast address, its port number textbf 443, we are somewhat confused.

We used the plugin "yarascan" to search the address space for the IP address 239.255.255.250.

```
$ volatility -f memdump.mem --profile=Win7SP1x86 yarascan -Y "
239.255.255.250" >| Data/yarascan_for_239.255.255.250.txt
```

The screenshot shows the volatility interface with the command \$ volatility -f memdump.mem --profile=Win7SP1x86 yarascan -Y "239.255.255.250" >| Data/yarascan\_for\_239.255.255.250.txt. The results window displays memory dump data for process svchost.exe (pid 2396). The data is organized into two columns: memory address and hex dump. Several entries in the hex dump column are highlighted in red, indicating matches for the search term 239.255.255.250. These red-highlighted entries are primarily located at the top of the dump, corresponding to the first few kilobytes of memory.

Figure 11: yarascan Result for 239.255.255.250

la figure 11 montre que l'adresse IP 239.255.255.250 est présent dans l'espace d'adressage du processus **svchost.exe pid: 2396**

By digging, the process track svchost.exe pid: 2396 we quickly realize that it leads nowhere. Because in figure 12 there is no parent process **296**. That is suspicious but does not allow us to learn more about the investigation.

	Settings	difflist.txt	pslist.txt	largefilelistname.txt	psxview.txt	yarascan_for_239_259_255..txt	ldmodules.txt			
	Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Startt	Exit
1	0x8013a0d8	System	4	0	74	574	—	0	2020-03-07 11:39:21 UTC+0000	
2	0x804fed028	smss.exe	236	4	3	29	—	0	2020-03-07 11:39:21 UTC+0000	
3	0x8580e3988	csrss.exe	384	296	9	555	0	0	2020-03-07 11:39:22 UTC+0000	
4	0x8580e3980	wininit.exe	340	296	3	76	0	0	2020-03-07 11:39:26 UTC+0000	
5	0x91547860	services.exe	436	348	9	242	0	0	2020-03-07 11:39:27 UTC+0000	
6	0x8580e3984	kernel32.exe	432	436	9	734	0	0	2020-03-07 11:39:28 UTC+0000	
7	0x8587e1208	user32.exe	468	348	10	161	0	0	2020-03-07 11:39:28 UTC+0000	
8	0x8580b4040	svchost.exe	564	436	10	371	0	0	2020-03-07 11:39:28 UTC+0000	
9	0x8580b4030	VboxService.exe	624	436	12	116	0	0	2020-03-07 11:39:29 UTC+0000	
10	0x84f5e20	svchost.exe	676	436	9	307	0	0	2020-03-07 11:39:29 UTC+0000	
11	0x85d2a1508	svchost.exe	724	436	18	468	0	0	2020-03-07 11:39:29 UTC+0000	
12	0x8587e0700	svchost.exe	844	436	18	499	0	0	2020-03-07 11:39:30 UTC+0000	
13	0x8580e3984	RPCSS.exe	884	436	15	446	0	0	2020-03-07 11:39:31 UTC+0000	
14	0x8580a3438	svchost.exe	916	436	32	1266	0	0	2020-03-07 11:39:29 UTC+0000	
15	0x85d252308	svchost.exe	1112	436	18	508	0	0	2020-03-07 11:39:30 UTC+0000	
16	0x8580f1750	psolvive.exe	1284	436	13	276	0	0	2020-03-07 11:39:30 UTC+0000	
17	0x85d4578	svchost.exe	1248	436	18	313	0	0	2020-03-07 11:39:30 UTC+0000	
18	0x8580e3980	vmicsvc.exe	1336	436	6	98	0	0	2020-03-07 11:39:31 UTC+0000	
19	0x8580e3980	vmicsvc.exe	1336	436	5	106	0	0	2020-03-07 11:39:31 UTC+0000	
20	0x8580b4040	vmicsvc.exe	1336	436	3	70	0	0	2020-03-07 11:39:31 UTC+0000	
21	0x8580b4030	vmicsvc.exe	1488	436	4	83	0	0	2020-03-07 11:39:31 UTC+0000	
22	0x8580b4030	vmicsvc.exe	1436	436	4	83	0	0	2020-03-07 11:39:31 UTC+0000	
23	0x85d252308	svchost.exe	1472	436	11	380	0	0	2020-03-07 11:39:31 UTC+0000	
24	0x85d3c1a08	crygmrnrv.exe	1612	436	6	162	0	0	2020-03-07 11:39:31 UTC+0000	
25	0x8580e3980	cryptui.dll	1704	436	10	162	0	0	2020-03-07 11:39:31 UTC+0000	
26	0x8580e3980	cryptui.dll	1776	436	4	33	0	0	2020-03-07 11:39:31 UTC+0000	
27	0x85c5e0440	cryptui.dll	1832	1756	4	101	0	0	2020-03-07 11:39:31 UTC+0000	
28	0x8580f7808	svchost.exe	2028	436	5	93	0	0	2020-03-07 11:39:33 UTC+0000	
29	0x85d205850	SearchIndexer.exe	1976	436	13	758	0	0	2020-03-07 11:39:35 UTC+0000	
30	0x85d38e340	svchost.exe	2396	436	12	187	0	0	2020-03-07 11:41:32 UTC+0000	
31	0x8580e3980	svchost.exe	2474	436	15	445	0	0	2020-03-07 11:41:32 UTC+0000	
32	0x8580e3980	svchost.exe	2476	436	14	672	0	0	2020-03-07 11:41:32 UTC+0000	
33	0x8580e3980	svchost.exe	2494	5444	3	123	4	0	2020-03-12 07:49:42 UTC+0000	
34	0x85d2e2830	taskhost.exe	5668	436	9	213	4	0	2020-03-12 07:49:44 UTC+0000	
35	0x8580e3980	dmu.exe	3168	844	3	73	4	0	2020-03-12 07:49:44 UTC+0000	
36	0x8580e3980	VBoxTray.exe	2328	4688	12	160	4	0	2020-03-12 07:49:45 UTC+0000	
37	0x8580e3980	taskhost.exe	2016	436	6	258	4	0	2020-03-12 07:49:48 UTC+0000	
38	0x8580e3980	WindowsLiner.exe	5000	4680	47	801	4	0	2020-03-12 07:50:00 UTC+0000	
39	0x8580e3980	WindowsLiner.exe	3588	4684	8	0	4	0	2020-03-12 07:50:00 UTC+0000	
40	0x858373f30	firefox.exe	3196	4684	63	1353	4	0	2020-03-16 11:04:28 UTC+0000	2020-03-12 07:50:00 UTC+0000
41	0x85fc40900	firefox.exe	3332	3196	10	266	4	0	2020-03-16 11:04:28 UTC+0000	

Figure 12: pid:296 filter on pslist Result

We therefore continue to explore the process track **IIwRWGTR.exe Pid: 3124** and **explorer.exe Pid: 5052**, by extracting their virtual address space to analyze them.

```
\$ volatility -f memdump.mem --profile=Win7SP1x86 memdump -p 3124 --dump-dir=Data/  
Volatility Foundation Volatility Framework 2.5  
*****  
Writing llwRWGTR.exe [ 3124] to 3124.dmp
```

From process core dump we have filtered out the keyword "*document*"

```
$strings Data/3124.dmp | egrep 'document'
```

Figure 13: \$strings Data/3124.dmp | egrep 'document' Result

In the figure 13 the line in green has attracted our attention. We therefore further analyzed this core dump by extracting the strings from the "3124.dmp" dump into a file \*.txt [13](0, )

```
$strings -a -n 8 Data/3124.dmp >| Data/3124.dmp.txt  
$strings -a -n 8 -el Data/3124.dmp >> Data/3124.dmp.txt
```

In the 3124.dmp.txt file, we have looked for the IP address 239.255.255.250. This IP address exists, but with a different port : **port 1900** . (figure 14)

Figure 14: search 239.255.255.250 in 3124.dmp.tx Result

Now on Windows systems, the **1900** [14](0, ) port is associated with the SSDP (Simple Service Discovery Protocol) protocol which allows the discovery of services and information. presence on a network. The address 239.255.255.250 is a multicast address and has been hardcoded in the malicious binary.

Source [14](0, ) «... Many devices, including some residential routers, have a vulnerability in the UPnP software that allows an attacker to get replies from port number 1900 to a destination address of their choice ... » We can therefore assume that attackers use this vulnerability. [15](0, ),[16](0, )

### 3.4 Hard disk analysis.

### 3.4.1 Extraction of objects and data.

as in the paragraph 3.2 (page 10) we had to identify an address as being a Gmail server. We started by extracting emails with Autopsy.

Two email exchanges between **att.ker.1n@gmail.com** (**Attilus**) and **v1c.t1m.m3r@gmai.com** (**Virtoria**) we seem suspicious . Indeed the conversation (figure 22, 23, 24, 25) between the two characters shows that *Virtoria* has downloaded a file ziper slack .zip

## 4 QUESTIONS FROM THE INVESTIGATOR

### 4.1 summary of the attack

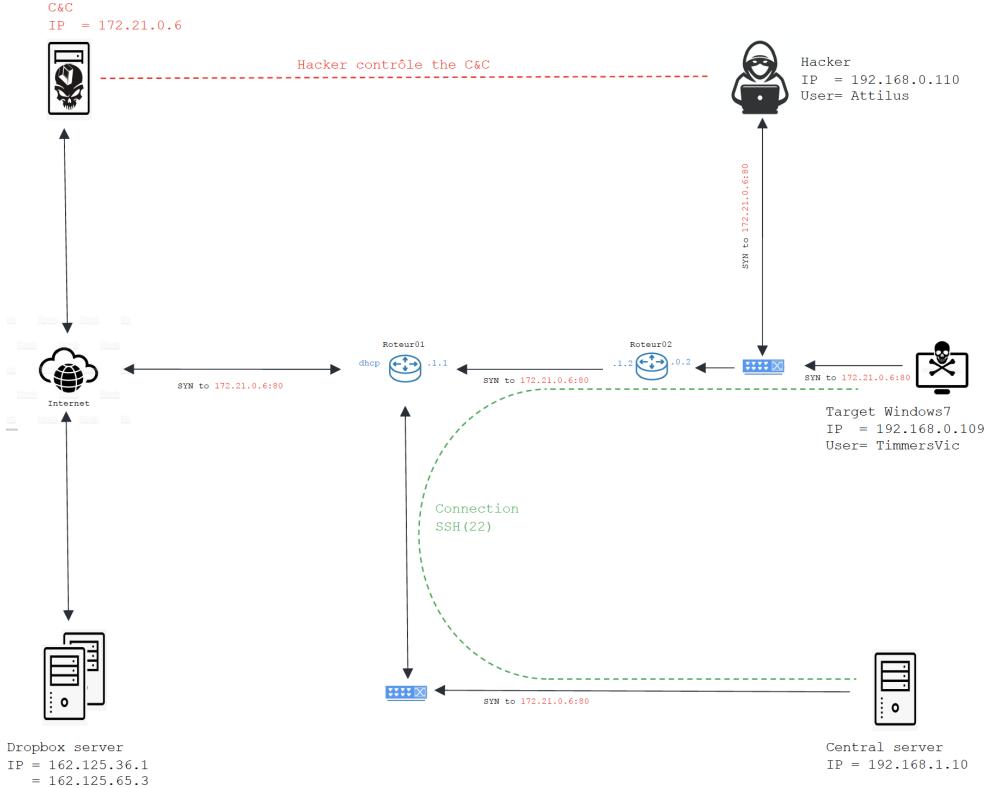


Figure 15: shema of attaker scenario

The Hackers infect the victim's machine via E-mail. They sent malicious software to the victim via WeTransfer. (**slack .zip**). Once the victim has had to unzip the file and open it, the **lIwRWgTR.exe** virus automatically installs itself on the victim's machine. They managed to steal the documents from the central server by connecting via FikeZilla with the victim's identifier (User = "TimmerVic", password = "password1") see figure 29. Once connected, the hackers had to steal the documents of the VIVALDI project by downloading them in the user's directory (See figure 32)

### 4.2 Event calendar

In this section, we have reconstructed a timeline of the events that occurred on the infecting machine window. Dates in red represent events or items that were intentionally deleted.

● | 2020-03-10 at 11:55:04 TimmerVic user creation

● | 2020-03-10 at 13:58:04 Mail: New Working station

## 4.2 Event calendar

15

Source File S C O E-Mail From E-Mail To Subject ▲ Date Received

INBOX att.ker.ln@gmail.com; vlc.t1m.m3r@gmail.com; New Working Station 2020-03-10 13:58:04 CET [H]

INBOX att.ker.ln@gmail.com; vlc.t1m.m3r@gmail.com; Forgot to mention 2020-03-10 13:59:19 CET [H]

INBOX no-reply@accounts.google.com; vlc.t1m.m3r@gmail.com; Security alert 2020-03-10 14:41:09 CET [In]

INBOX no-reply@accounts.google.com; vlc.t1m.m3r@gmail.com; Security alert 2020-03-11 00:25:17 CET [In]

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 3 of 114 Result: ⏪ ⏩

From: att.ker.ln@gmail.com  
To: vlc.t1m.m3r@gmail.com  
Cc:  
Subject: New Working Station

Headers: Text HTML RTF Attachments (0) Accounts  
Download Images

Hello Victoria,  
your new work station has been set up and you have the tools needed to continue working as before. Let me know if you need anything.  
Our plans for Sunday are still on?  
Atticus

Figure 16: att.ker.ln@gmail.com to vlc.t1m.m3r@gmail.com

- | 2020-03-10 at 13:59:19 Mail: forgot to mention

Source File S C O E-Mail From E-Mail To Subject ▲ Date Received

INBOX att.ker.ln@gmail.com; vlc.t1m.m3r@gmail.com; New Working Station 2020-03-10 13:58:04 CET [H]

INBOX att.ker.ln@gmail.com; vlc.t1m.m3r@gmail.com; Forgot to mention 2020-03-10 13:59:19 CET [H]

INBOX no-reply@accounts.google.com; vlc.t1m.m3r@gmail.com; Security alert 2020-03-10 14:41:09 CET [In]

INBOX no-reply@accounts.google.com; vlc.t1m.m3r@gmail.com; Security alert 2020-03-11 00:25:17 CET [In]

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 4 of 114 Result: ⏪ ⏩

From: att.ker.ln@gmail.com  
To: vlc.t1m.m3r@gmail.com  
Cc:  
Subject: Forgot to mention

Headers: Text HTML RTF Attachments (0) Accounts  
Download Images

Hi Victoria,  
forgot to mention in the previous email that a new account was created for you on the repository server.  
account: timermsvc  
password: password1  
Please contact the IT department once you can connect to the server to change the password to something more secure.  
Atticus

Figure 17: att.ker.ln@gmail.com to vlc.t1m.m3r@gmail.com

- | 2020-03-11 at 08:31:15 Mail: Re:New Working station

Source File S C O E-Mail From E-Mail To Subject ▲ Date Received Message (PlainText)

Sent Mail vlc.t1m.m3r@gmail.com; att.ker.ln@gmail.com; Re: New Working Station 2020-03-11 08:31:15 CET [H] Attilus, the worksta

Sent Mail vlc.t1m.m3r@gmail.com; att.ker.ln@gmail.com; Re: New Working Station 2020-03-11 08:31:15 CET [H] Attilus, the worksta

Sent Mail vlc.t1m.m3r@gmail.com; att.ker.ln@gmail.com; Re: Forgot to mention 2020-03-11 08:31:57 CET [H] Okido I am still getti

Sent Mail vlc.t1m.m3r@gmail.com; att.ker.ln@gmail.com; Re: Forgot to mention 2020-03-12 08:46:02 CET [H] Attilus, everything is wo

Sent Mail vlc.t1m.m3r@gmail.com; att.ker.ln@gmail.com; Re: Project VIVALDI update 2020-03-20 09:00:56 CET [H] Attilus, i will look into it.

Hex Text Application File Metadata Context Results Annotations Other Occurrences

Result: 3 of 29 Result: ⏪ ⏩

From: vlc.t1m.m3r@gmail.com  
To: att.ker.ln@gmail.com  
Cc:  
Subject: Re: New Working Station

Headers: Text HTML RTF Attachments (0) Accounts

Hi Attilus,  
the workstation is in order. Thank you!  
Sunday is still on :)

On 3/10/2020 5:58 AM, Attilus Kerrin wrote:  
= Hello Victoria,  
=  
= your new work station has been set up and you have the tools needed to  
= continue working as before. Let me know if you need anything.  
=  
= Our plans for Sunday are still on?  
=  
= Attilus

Figure 18: vlc.t1m.m3r@gmail.com to att.ker.ln@gmail.com

- | 2020-03-11 at 08:31:57 Mail: Re:forgot to mention

The screenshot shows the NetworkMiner interface with the 'Gmail' tab selected. A specific email entry is highlighted in red. The message body contains a quoted reply from 'Attilus' (att.ker.in@gmail.com) on March 10, 2020, at 08:59 AM, regarding account creation and password security.

Source File	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message [MarkText]
Sent Mail	vlc.t1m.m3r@gmail.com	att.ker.in@gmail.com				Re: New Working Station	2020-03-11 08:31:15 CET	Hi Attilus, the workstation
Sent Mail	vlc.t1m.m3r@gmail.com	att.ker.in@gmail.com				Re: New Working Station	2020-03-11 08:31:15 CET	Hi Attilus, the workstation
Sent Mail	vlc.t1m.m3r@gmail.com	att.ker.in@gmail.com				Re: Forgot to mention	2020-03-11 08:31:57 CET	Okido! I am still getting
Sent Mail	vlc.t1m.m3r@gmail.com	att.ker.in@gmail.com				Re: Forgot to mention	2020-03-12 08:40:02 CET	Hi Attilus,everything is wo
Sent Mail	vlc.t1m.m3r@gmail.com	att.ker.in@gmail.com				Re: Project ViVALDI Update	2020-03-20 09:09:56 CET	Ok Attili, will look into it

Figure 19: vlc.t1m.m3r@gmail.com to att.ker.in@gmail.com

- | 2020-03-12 at 08:46:02 Mail: Re:forgot to mention

Victoria lets Attilus know that she can't run some programs on his machine

The screenshot shows the NetworkMiner interface with the 'Gmail' tab selected. A specific email entry is highlighted in red. The message body contains a quoted reply from 'Victoria' (att.ker.in@gmail.com) on March 12, 2020, at 08:46:02 CET, regarding account creation and password security.

Source File	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	M
All Mail	no-reply@accounts.google.com	vlc.t1m.m3r@gmail.com				Security alert	2020-03-11 08:46:02 CET	P
All Mail	no-reply@accounts.google.com	vlc.t1m.m3r@gmail.com				Security alert	2020-03-11 08:25:17 CET	P
All Mail	att.ker.in@gmail.com					Re: New Working Station	2020-03-11 08:29:32 CET	H
All Mail	att.ker.in@gmail.com						2020-03-12 08:46:02 CET	H
All Mail	no-reply@accounts.google.com	att.ker.in@gmail.com				Re:Forgot to mention	2020-03-12 08:46:02 CET	H
All Mail	no-reply@accounts.google.com	att.ker.in@gmail.com				Take Dropbox on the go!	2020-03-20 09:09:57 CET	H
All Mail	welcomeswh.com	att.ker.in@gmail.com				Welcome to Wahl!	2020-03-20 09:21:40 CET	H
All Mail	Maureen7ydrDugot32@charlessears.com	att.ker.in@gmail.com				Ready for vacation?	2020-03-20 09:36:25 CET	D

Figure 20: vlc.t1m.m3r@gmail.com to att.ker.in@gmail.com

- | 2020-03-12 at 08:46:00 Mail: Re:forgot to mention

Attilus elevated the privileges of the timmervic account to the administrator.

The screenshot shows a digital forensics interface with a sidebar containing various data sources and search filters. The main area displays a table of search results for emails. One specific email is highlighted in red, showing its details:

**Email Details:**

- From: att.ker.1n@gmail.com
- To: vlc.tlm.m3r@gmail.com
- Subject: Re: Forget to mention
- Date Received: 2020-03-12 15:59:10 CET
- Message Plan: 14 Victoria (org)

**Email Content Preview:**

Lucky you caught me during coffee break. I changed your account type, now it should not make trouble any more  
A

**Message Body:**

On Thu, Mar 12, 2020 at 8:46 AM Victoria Timmers <vlc.tlm.m3r@gmail.com> wrote:  
Hi Attilus  
everythings is working fine, but I have some trouble running some  
programs on the machine. Would it be possible to change that?  
Victoria

On 3/10/2020 5:59 AM, Attilus Kerim wrote:  
> Hi Victoria,  
>  
> forgot to mention in the previous email that a new account was created  
> for you on the repository server.  
>  
> account: timmersvict  
> password: password1  
>  
> Please contact the IT department once you can connect to the server to  
> change the password to something more secure.  
>  
> Attilus

Figure 21: vlc.tlm.m3r@gmail.com to att.ker.1n@gmail.com

- | 2020-03-17 at 11:48:25 creation of the password file by Victoria

voir figure 33

- | 2020-03-20 at 08:59:44 Mail: project VIVALDI Update

The attacker wants to exist victoria to download the VIVALDI project with his own username.

The screenshot shows a digital forensics interface with a timeline editor on the left and an email message viewer on the right. The timeline editor highlights a specific event (④) on March 18, 2020, which corresponds to the email message shown in the viewer (⑤). The email message content is as follows:

C:\Users\timmersVic\Downloads\att.ker.1n@gmail.com; ... : Project VIVALDI update  
we received news that the ... to draft a new 2020-03-18

**Email Details:**

- From: att.ker.1n@gmail.com
- To: vlc.tlm.m3r@gmail.com
- Subject: ... : Project VIVALDI update
- Date: 2020-03-20 08:59:44 CET

**Email Content Preview:**

Victoria,  
I am not happy with the work that we did with VIVALDI is going through. We will need to draft a new design document though as it seems like we are not content with the previous one.  
I am at the moment still outside the country, so I can't be in person at the office to discuss it. I would imagine that the changes to be brought to the document will be minimal as the design itself is very close to what they wanted from the start. They just want more attention on security by design and easier data flow.

Figure 22: att.ker.1n@gmail.com to vlc.tlm.m3r@gmail.com

- | 2020-03-20 at 09:00:56 RE:project VIVALDI Update

Victoria responded to Attilus.

The screenshot shows a digital forensic interface with a sidebar containing various data sources like 'Data Sources', 'File Types', 'Deleted Files', 'File Size', 'Emails', 'Extracted Content', 'ENF Metadata', 'Encryption Detected', 'Email Suspected', 'Extension Suspected', 'Installed Programs', 'Metadata', 'Operating System Information', 'Operating System User Account', 'Process Commands', 'Recycle Bin', 'Run Programs', 'Shell Bags', 'USB Device Attached', 'User Content Detected', 'Web Cache', 'Web Cookies', 'Web Downloads', 'Web Form Autofill', 'Web History', and 'Web Search'. The main pane displays an email inbox with the following entries:

- Sent Mail (4)

The selected email is from 'vlc.t1m.m3r@gmail.com' to 'att.ker.1n@gmail.com' with the subject 'Re: Project VIVALDI update'. The message body is as follows:

```

From: vlc.t1m.m3r@gmail.com
To: att.ker.1n@gmail.com;
CC:
Subject: Re: Project VIVALDI update

Headers Text HTML RTF Attachments Accounts

Ok Attilus,
i will look into it and see what changes need to be done
U:

On 3/20/2020 8:59 AM, Attilus Kerrin wrote:
> Victoria,
>
> we received news that the deal with VIVALDI is going through. We will
> need to draft a new design document though as it seems they are not
> content with the previous one.
> I am at the moment still outside my country, so I can't be in person
> at the office to discuss it. I would imagine that the changes to be
> made in the document will be minimal as the design itself is very
> close to what they wanted from the start. They just want more
> attention on security by design and easier data flow.
>
> Attilus

```

Figure 23: vlc.t1m.m3r@gmail.com to att.ker.1n@gmail.com

- | 2020-03-20 at 09:20:03 Mail: Smarl requette

Attilus fake a request, which will force Victoria to leave her machine unattended for a short time..

- | 2020-03-20 at 10:49:51 Mail: useful tool for your

The attacker makes Victoria believe that he has good tools to help her in her work and offers to send it to her through another channel (WeTransfer).

The screenshot shows a digital forensic interface with a timeline editor. The timeline spans from March 18, 2020, to March 20, 2020. A single event is highlighted on March 19, 2020, at 10:49:51 CET, showing an email from 'at.k3r.1n@gmail.com' to 'vlc.t1m.m3r@gmail.com' with the subject 'Hello, useful tool for you!'. The message body is as follows:

```

From: at.k3r.1n@gmail.com
To: vlc.t1m.m3r@gmail.com;
Subject: Hello, useful tool for you!

Headers Text HTML RTF Attachments Accounts
Download Images

Hello Victoria,
i found a useful tool that can help us at work!
I can't send it with email because it is a exe [But I sent you link of WeTransfer with it. Had to put in zip with password, but its easy]
password is "password"
Attilus

```

Figure 24: att.ker.1n@gmail.com to vlc.t1m.m3r@gmail.com

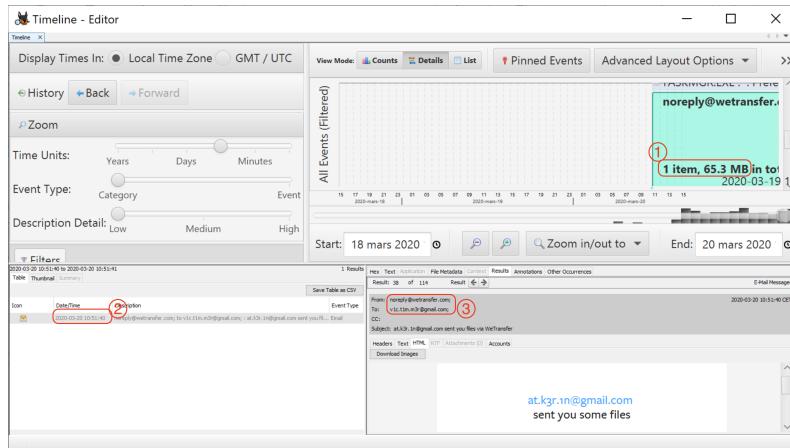


Figure 25: `att.ker.ln@gmail.com` (WeTransfer) **to** `vlc.t1m.m3r@gmail.com`

- | 2020-03-20 at 10:52:02 downloaded **slack.zip** file

with FTK Image, by exploring the hard disk images provided, we can see that the zip file **slack.zip** contains a malicious executable because the latter has the same **MZ** signature as our **IIwRWGTR.exe** **Pid: 3124** process. see figure 26

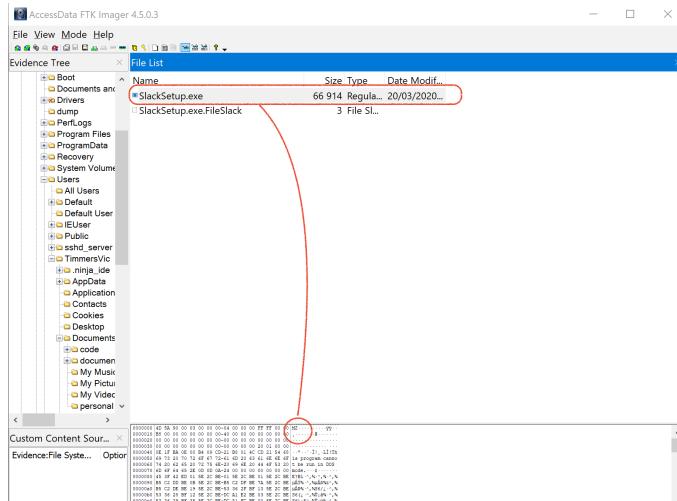


Figure 26: content of the file **slack.zip** download with WeTransfer

- | 2020-03-20 at 10:57:35 malware persistence on their target machine

As most malware tries to hide and achieve persistence on their target machine, in order to run even after restarting the system, we have to check known registry keys to see if the malware does not modify one of the registry keys of one of the Windows AutoStart Extension Points (ASEP).

```
forensics@slifworkstation:~/Desktop/forensics/Nextcloud-Win7_memory_dump$ volatility -f memdump.mem --profile=Win7SP1x8
$ printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"
Volatility Foundation Volatility Framework 2.5
Legend: (S) = Stable (V) = Volatile

-----
Registry: \??\C:\Users\TimmersVic\ntuser.dat
Key name: Run (S)
Last updated: 2020-03-20 09:54:00 UTC+0000

Subkeys:

Values:
REG_SZ      com.squirrel.slack.slack : (S) "C:\Users\TimmersVic\AppData\Local\slack\slack.exe" --process-start-args -
-startup
forensics@slifworkstation:~/Desktop/forensics/Nextcloud-Win7_memory_dump$
```

Figure 27: modification ASEP HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run par slack.exe

in the figure 27 slack.exe is actually in the *RUN*.

and in the C:\Users\TimmersVic\AppData\Local\Temp\ directory we found the malicious process IIwRWgTR.exe Pid: 3124. (see figure 28)

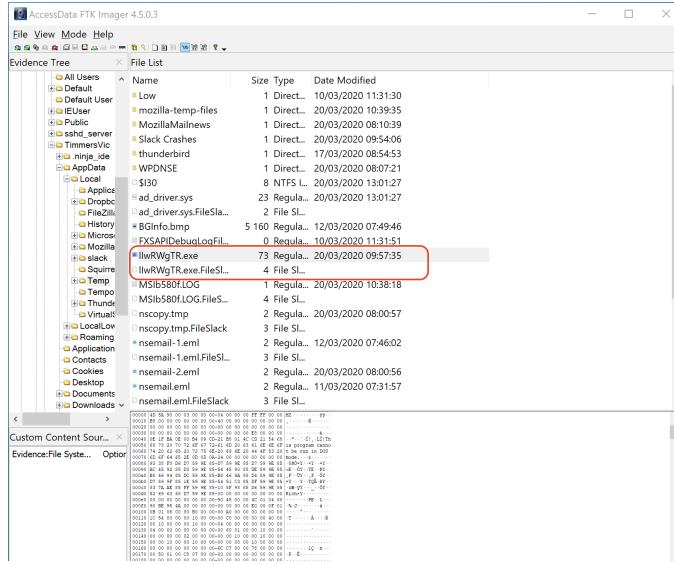


Figure 28: localisation IIwRWgTR.exe in the system

- | 2020-03-20 at 11:13:26 central server connection

at 11:13:26 we notice the user TimmersVic made a connection to the central server, with the identifiers same identifier which had been entrusted to him

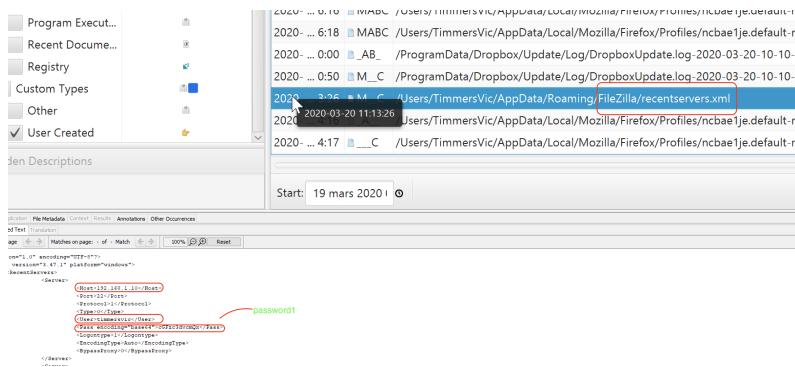


Figure 29: attempt to connect to the central server with FileZilla  
this connection goes through the router02 at 12:34:39

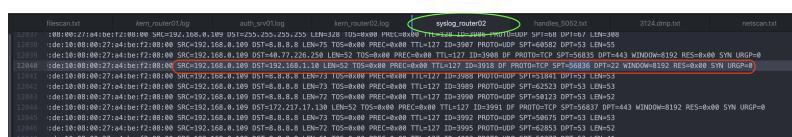


Figure 30: central server connection

and is finally accepted at 12:34:40 by the central server

```

files.txt          kern_router01.log           auth_srv01.log          kern_router02.log           syslog_router01.log
736 Mar 20 11:28:53 VM SSM01[2404]: Did not receive identification string from 192.168.1.2
737 Mar 20 11:39:01 VM CRON[24766]: pam_unix(cron:session): session opened for user root by (uid=0)
738 Mar 20 11:39:01 VM CRON[24766]: pam_unix(cron:session): session closed for user root
739 Mar 20 11:50:57 VM sshd[24748]: Did not receive identification string from 192.168.1.2
740 Mar 20 12:09:01 VM CRON[24749]: pam_unix(cron:session): session opened for user root by (uid=0)
741 Mar 20 12:09:02 VM CRON[24749]: pam_unix(cron:session): session closed for user root
742 Mar 20 12:17:01 VM CRON[24791]: pam_unix(cron:session): session opened for user root by (uid=0)
743 Mar 20 12:17:01 VM CRON[24791]: pam_unix(cron:session): session closed for user root
744 Mar 20 12:30:37 VM sshd[24794]: Connection closed by 192.168.1.2 port 56830 [preauth]
745 Mar 20 12:31:10 VM sshd[24796]: Did not receive identification string from 192.168.1.2
746 Mar 20 12:32:19 VM sshd[24797]: Accepted password for timmersvc from 192.168.1.2 port 56832 ssh2
747 Mar 20 12:32:19 VM sshd[24797]: pam_unix(sshd:session): session opened for user timmersvc by (uid=0)
748 Mar 20 12:32:19 VM systemd: pam_unix(systemd-user:session): session opened for user timmersvc by (uid=0)
749 Mar 20 12:32:23 VM systemd-logind[834]: New session 627 of user timmersvc.
750 Mar 20 12:32:23 VM systemd-logind[834]: pam_unix(sshd:session): session closed for user timmersvc
751 Mar 20 12:32:23 VM systemd-logind[834]: Removed session 627.
752 Mar 20 12:32:55 VM sshd[24878]: Connection closed by 192.168.1.2 port 56833 [preauth]
753 Mar 20 12:33:29 VM sshd[24881]: Connection closed by 192.168.1.2 port 56834 [preauth]
754 Mar 20 12:34:49 VM sshd[24882]: Accepted password for timmersvc from 192.168.1.2 port 56836 ssh2
755 Mar 20 12:34:49 VM sshd[24882]: pam_unix(sshd:session): session opened for user timmersvc by (uid=0)

```

Figure 31: FileZilla connection to the central server

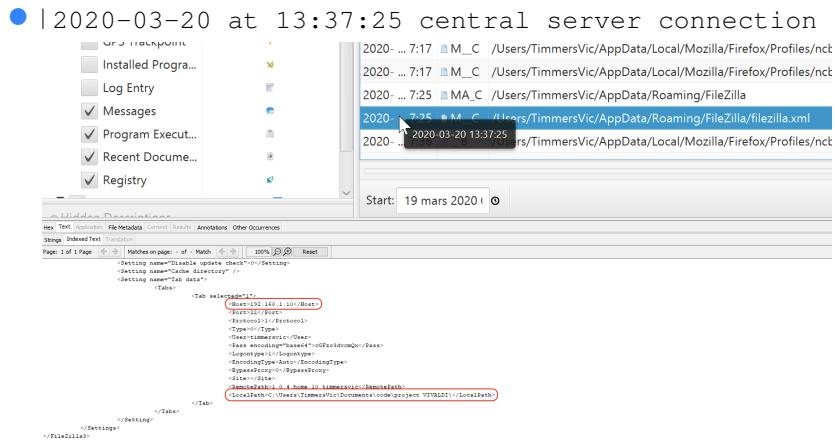


Figure 32: FileZilla connection to the central server

### 4.3 user involvement

The Windows workstation user was not directly involved. From the conversation in figure 24, it can be deduced that she was negligent and reckless because it is not advisable to install software preventing unknown sources. This recklessness can be found in the fact that she recorded her passwords in `.txt` files (see figure 33)

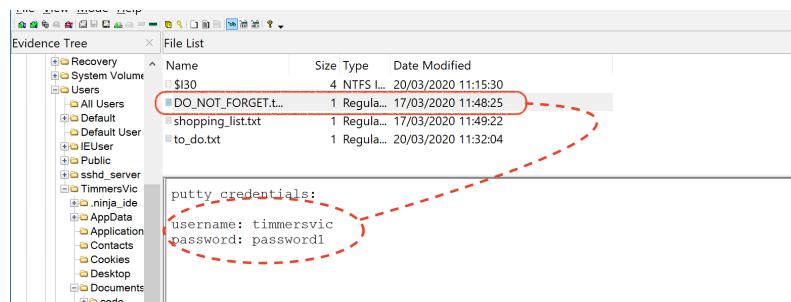


Figure 33: content of DO\_NO\_FORGET.txt file

In addition, the conversation of figure 18 and 19 shows a more than professional complicity. Because the two plan to meet on a Sunday.

## References

- [1] Olivia Morelli. (solved) win32:evo-gen explained. thorough removal guide for 2020. <https://www.2-spyware.com/remove-win32evo-gen.html>, 2020. Accessed on 2020-11-10.
- [2] Olivia Morelli. Haal win32:evo-gen weg (verwijdering handleiding) - nov 2020 update. <https://zondervirus.nl/win32evo-gen/>, 2020. Accessed on 2020-11-10.
- [3] Microsoft Defender. Trojan: Win32 / swrort.a. <https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan%3AWin32/Swrort.A>, 2020. Accessed on 2020-11-10.
- [4] Robert Bailey. Trojan: Win32 / swrort.a how to fix guide. <https://howtofix.guide/trojanwin32-swrort-a/>, 2020. Accessed on 2020-11-10.
- [5] Robert Bailey. Trojan.crypt.msil.generic. <https://howtofix.guide/trojan-crypt-msil-generic/>, 2020. Accessed on 2020-11-10.
- [6] Max. How to remove malicious confidence 80% (d) virus. [https://www.fixyourbrowser.com/removal-instructions/remove-malicious\\_confidence\\_80-d-virus/](https://www.fixyourbrowser.com/removal-instructions/remove-malicious_confidence_80-d-virus/), 2020. Accessed on 2020-11-10.
- [7] Brandon Skies. Trojan.malware.300983.susgen removal. <https://howtoremove.guide/trojan-malware-300983-susgen/>, 2020. Accessed on 2020-11-10.
- [8] joesandbox]. Analysis report securiteinfo.com.trojan.malware.300983.susgen.2470. <https://www.joesandbox.com/analysis/277707/0/html>, 2020. Accessed on 2020-11-10.
- [9]. , 2020. Accessed on 2020-11-10.
- [10] University of Southern California. B-root. <https://b.root-servers.org/>, 2020. Accessed on 2020-11-12.
- [11] dnslytics. Ip information 192.228.79.201. <https://dnslytics.com/ip/192.228.79.201>, 2020. Accessed on 2020-11-12.
- [12] siteground. Email protocols - pop3, smtp and imap tutorial. <https://www.siteground.com/tutorials/email/protocols-pop3-smtp-imap/>, 2020. Accessed on 2020-11-12.
- [13] Wiley. The art of memory forensics: Detecting malware and threats in windows, linux, and mac memory. <https://www.amazon.com/Art-Memory-Forensics-Detecting-Malware/dp/1118825098>. Part II: Windows Memory Forensics, Page 246.
- [14] wikipedia. Simple service discovery protocol. [https://en.wikipedia.org/wiki/Simple\\_Service\\_Discovery\\_Protocol](https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol), 2020. Accessed on 2020-11-12.
- [15] Christian Beedgen. Malware faq: Microsoft windows upnp vulnerabilities. <https://www.sans.org/security-resources/malwarefaq/win-upnp>, 2020. Accessed on 2020-11-12.
- [16] speedguide. Port 1900 details. <https://www.speedguide.net/port.php?port=1900>, 2020. Accessed on 2020-11-12.