***NAME:Hassaan Oumair***

***ROLL NO:I191777***

**MALWARE ANALYSIS REPORT**

****

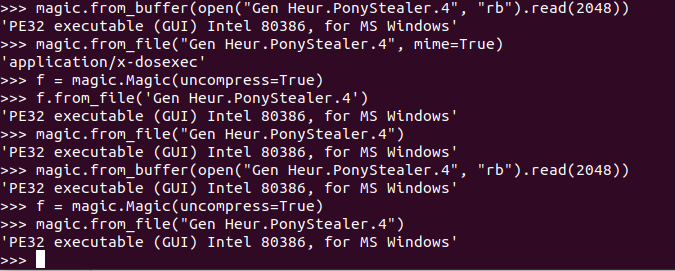
Through the inspection of the file with notepad++ it is known that the magic byte or the file signature is 4d 5a or MZ, this type of file signature is of an portable executable.

**EXE Type:**



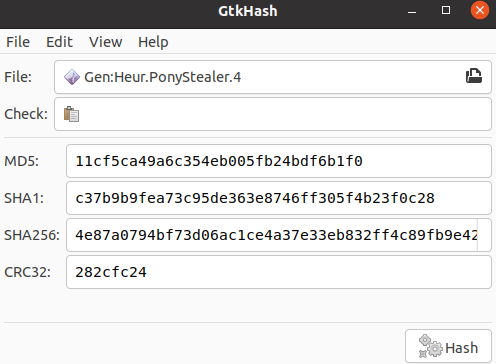
Python magic was used to know the exe type and It appears to be a 32bit executable

**File Type:**

****

The information extracted from the file was PE32 which means it is an executable.

**CalcHash:**

****

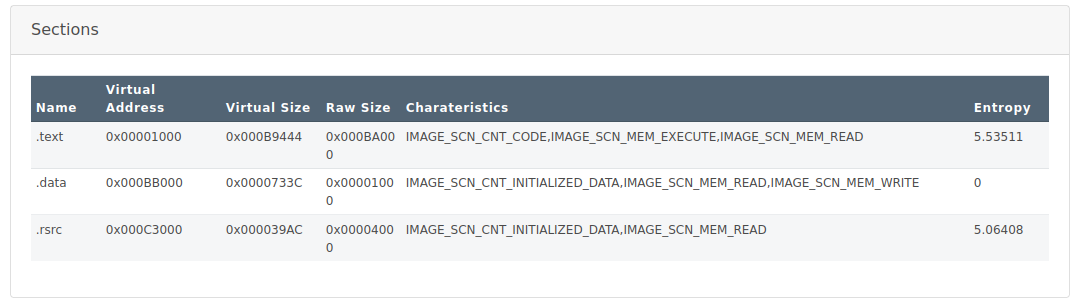
For this purpose I have used gtk hash as calchash was not available on ubuntu, from the screenshot provided above it is clear, SHA256 hash is used to identify the file, as it was the name of the compressed file it was in.

**The DLL:**

The dlls used by this file were found by **ANYRUN** which runs the file in a safe environment

* MSVBVM60.DLL

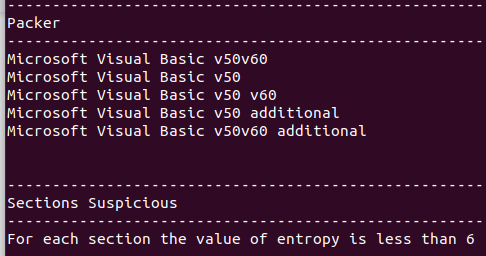
**Sections and their offsets:**

****

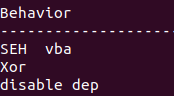
This information was gathered by **ANYRUN.**

**Packing Info:**

For this purpose I have used a program called Peframe which is used to collect information of an executable.



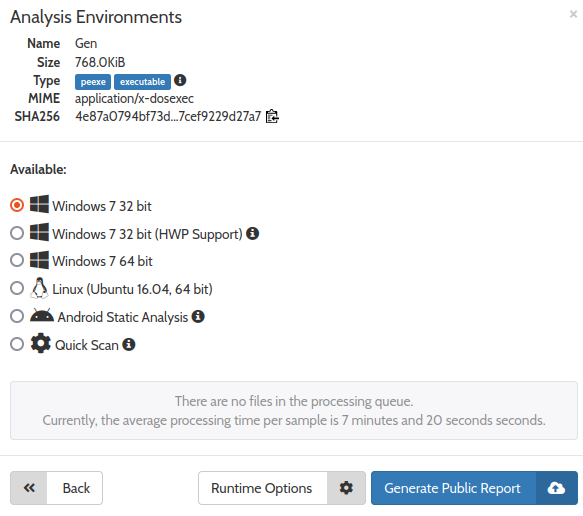
**Strings**

****

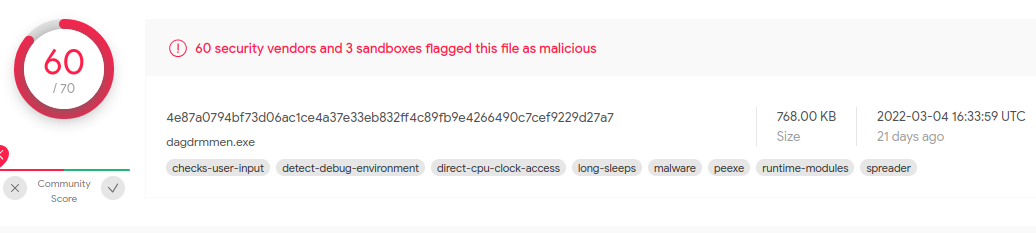
**These strings were extracted with the help of peframe.**

These are the malicious strings or breakpoints extracted from the Malware, I’ve written a yara script to search for these strings if any of these strings are found the .exec is a confirmed malware.

**Hybrid Analysis:**



**Virus total:**

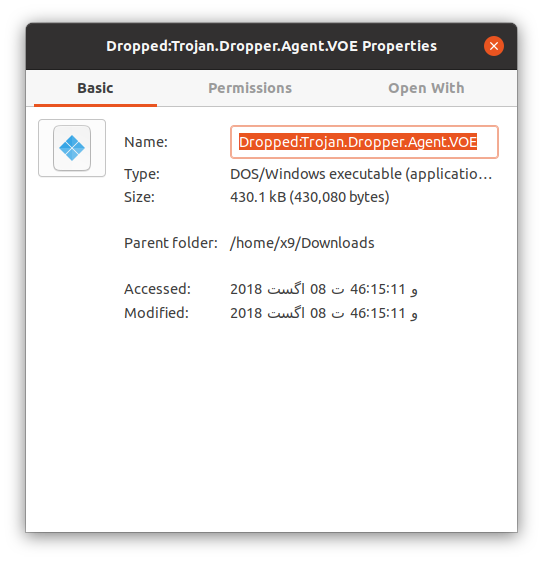


As Virus total inspected the file it came out to be malicious by 60 security vendors.

***2,Dropped:Trojan.Dropper.Agent.VOE:***

Trojan-Dropper:W32/Agent is a very large family of programs, most of which drop, install and execute other programs (usually malware) to the victim's machine.[[1]](#footnote-0)

**Machine Information**:



The file is shown to be a windows executable(.exe) in ubuntu.

**Magic Byte or File signature:**

****

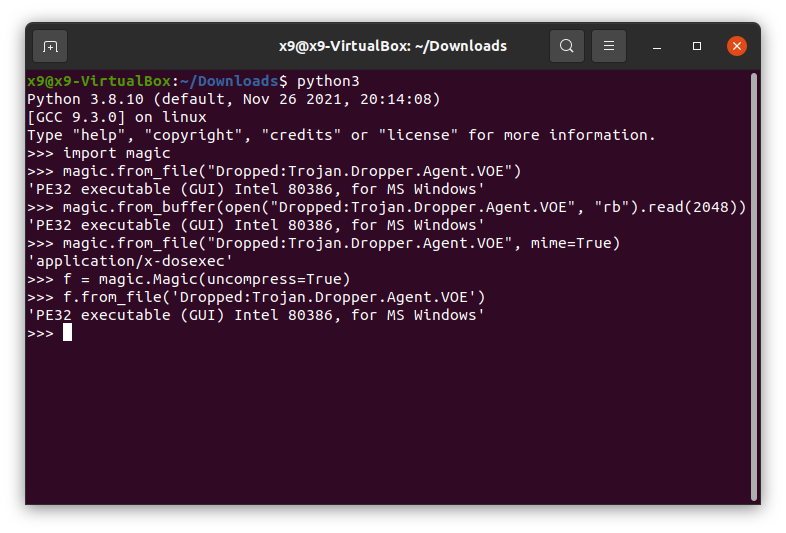
The magic byte or the file signature is 4d 5a or MZ, this type of file signature is of an windows executable.

**EXE Type:**

****

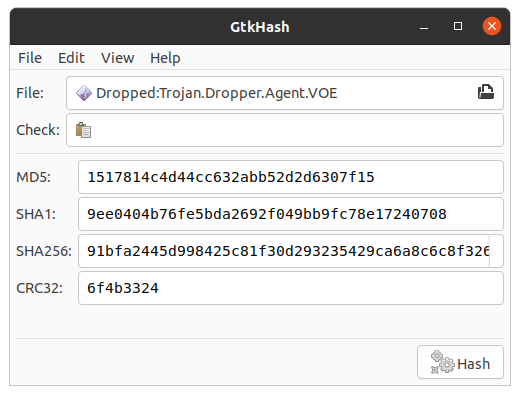
It is a 32 bit windows executable file.

**File type:**

****

This information was gathered from running python magic commands.

**CalcHash:**

****

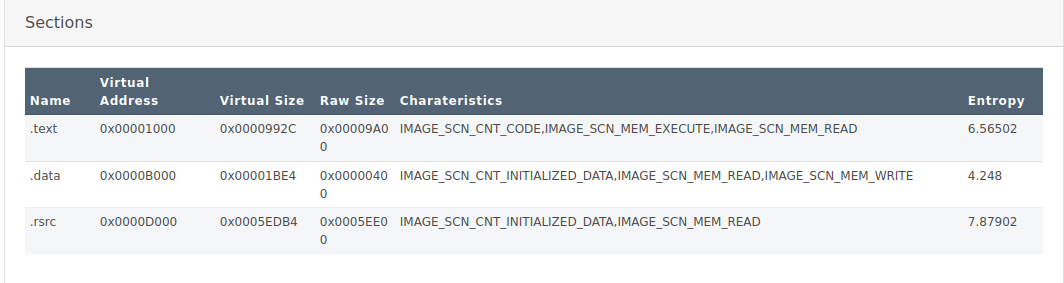
The hashing scheme used to identify the file is SHA256, it showed the same hash on the website from it was downloaded.

**DLLs:**

The following Dlls were used by the executable, the information was extracted from ANYRUN.

* ADVAPI32.dll
* KERNEL32.dll
* GDI32.dll
* USER32.dll
* COMCTL32.dll
* VERSION.dll

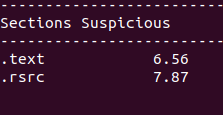
**SECTIONS and Offsets:**

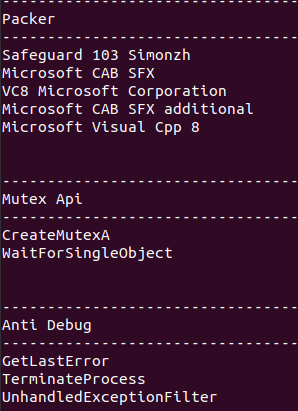
****

This information was gathered from the rapport of ANYRUN.

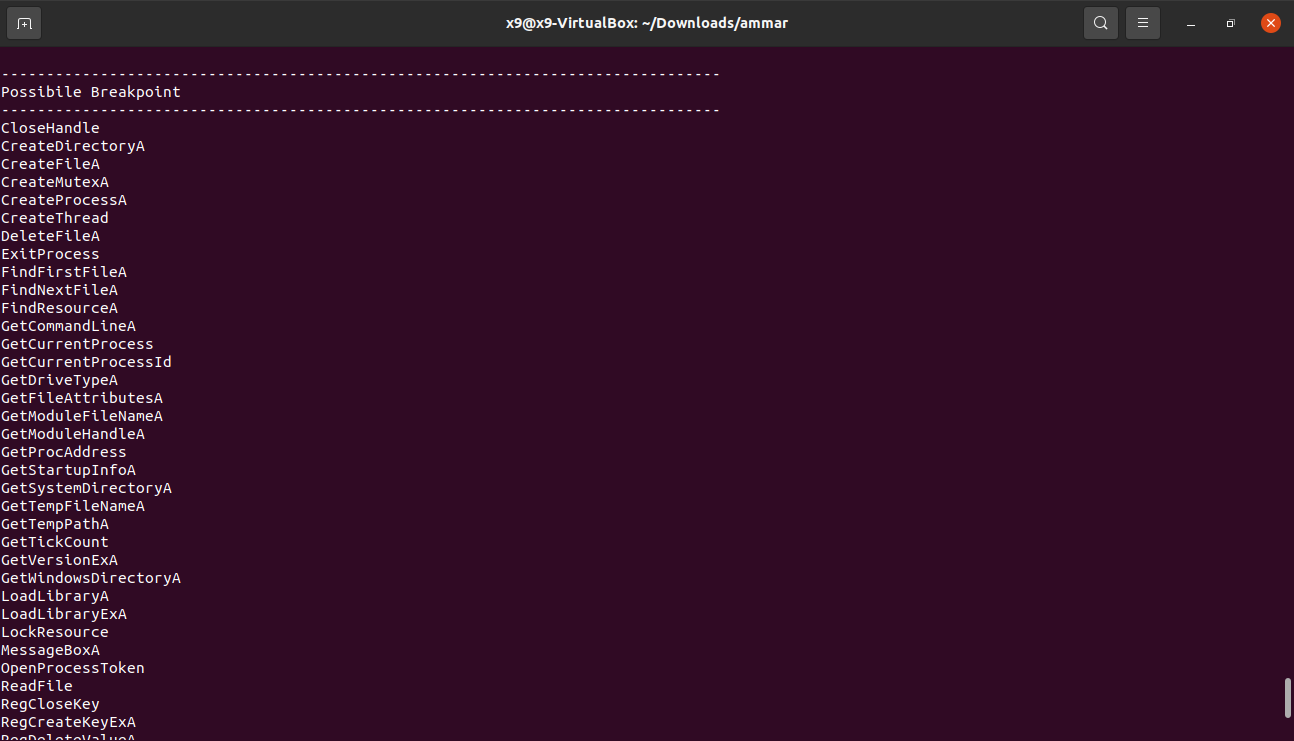
**PACKING INFORMATION:**

Peframe was used for this purpose it also extracted the information about in which sections the suspicious activity was taking place.





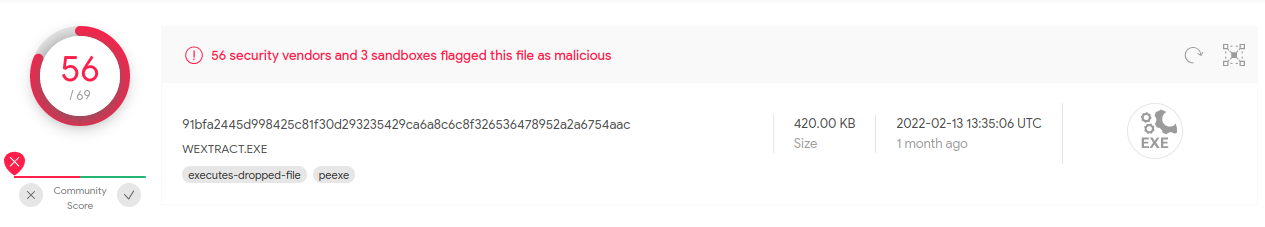
**Strings**

****

**These strings were extracted with the help of peframe.**

These are the malicious strings or breakpoints extracted from the Malware, I’ve written a yara script to search for these strings if any of these strings are found the .exec is a confirmed malware.

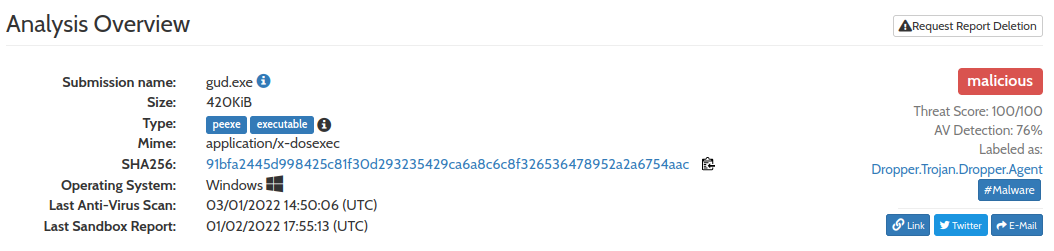
**VirusTotal:**

****

The file is said to be malicious by 56 security vendors according to VirusTotal.

**Hybrid Analysis:**

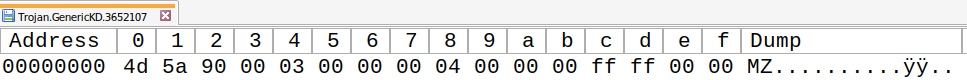
The web application described the executable as malicious.



***3.Trojan.GenericKD.3652107:***

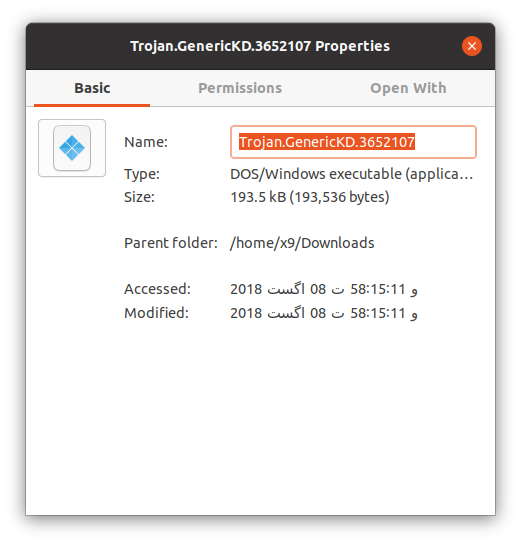
This malware is distributed via a spam email message that pretends to be a notification from either the POSTNORD or AUPOST postal services (POSTNORD caters to Denmark and Sweden, while AUPOST deals with delivery in Australia). The text content of the message is typically about lost or undelivered packages and the email includes a contain ZIP file attachment that is the actual ransomware file. Malicious links in the email text content reportedly could also lead the user into downloading the ransomware file.[[2]](#footnote-1)

**Magic byte or File signature:**

****

**Machine information:**

The file is shown to be an portable executable at first glance.

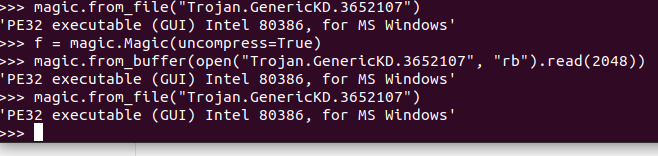
****

**Exe type (32/64 bit):**

****

This appears to be a 32 bit portable executable windows (.exe) file.

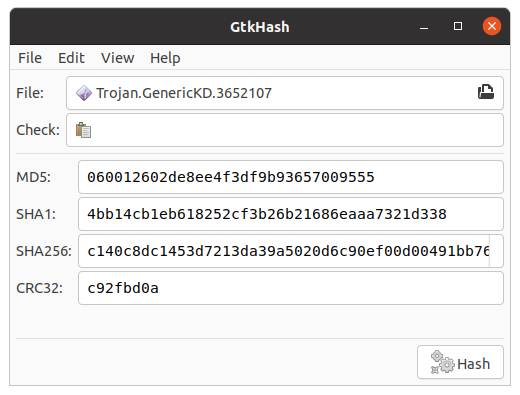
**File Type:**

****

This is an executable file by python magic.

**CalcHash:**

The hash type used for the identification of the file is SHA256, by the website from where it was download.

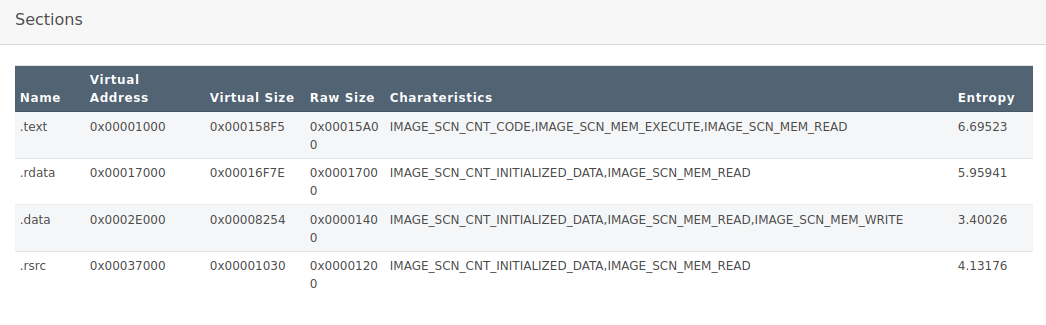
****

**DLLs:**

The Dlls used by the executable are Known by **Anyrun:**

* **USER32.dll**
* **SHELL32.dll**
* **ole32.dll**
* **ADVAPI32.dll**
* **GDI32.dll**
* **COMCTL32.dll**
* **VERSION.dll**
* **SHLWAPI.dll**
* **KERNEL32.dll**

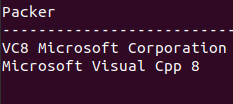
**SECTIONS and OFFSET:**

****

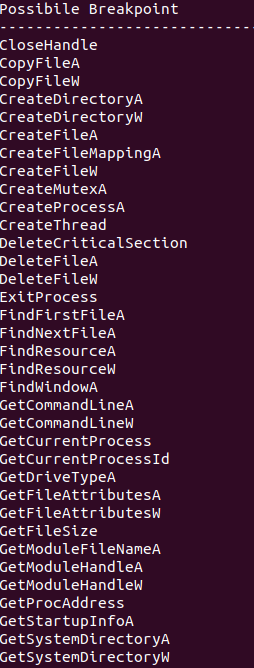
The sections and their offsets of the file are known by **ANYRUN**.

**PACKING INFO:**

The packing information of the file is gathered by a tool known as peframe.



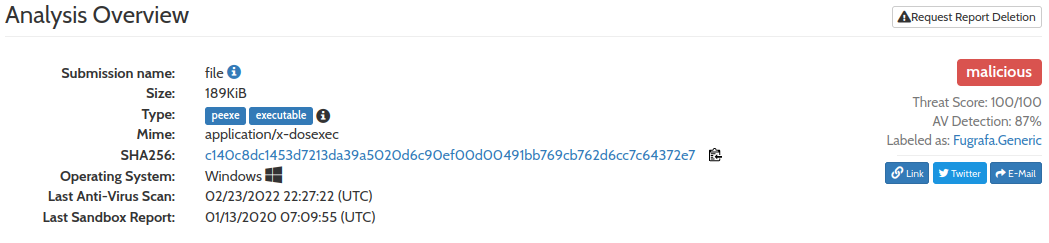
**Strings**

****

**These strings were extracted with the help of peframe.**

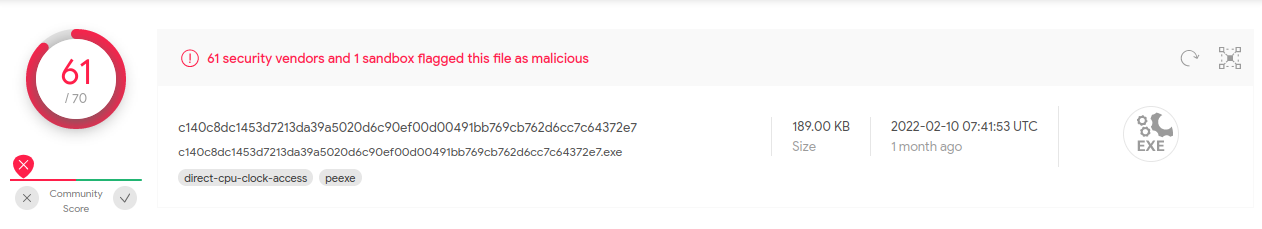
These are the malicious strings or breakpoints extracted from the Malware, I’ve written a yara script to search for these strings if any of these strings are found the .exec is a confirmed malware.

**HYBRID ANALYSIS:**

******

The file is malicious.

**VIRUSTOTAL:**

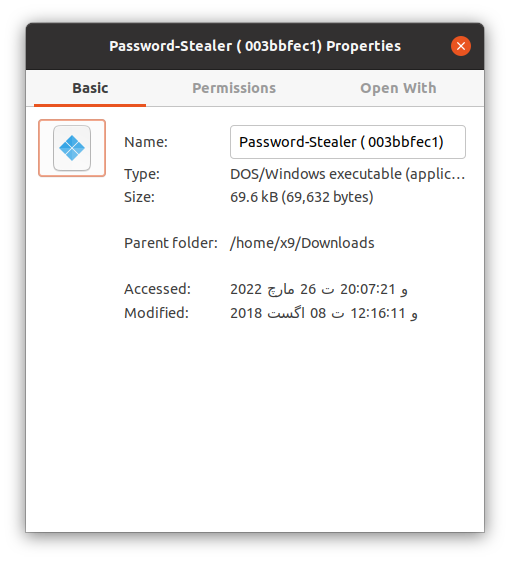
****

61 security vendors and 1 sandbox flagged the file as malicious.

***4.Password-Stealer ( 003bbfec1)***

Password stealers are a type of malware that steals account information. In essence, it is similar to a banking Trojan, but instead of intercepting or substituting entered data, it usually steals information already stored on the computer: usernames and passwords [saved in the browser](https://www.kaspersky.com/blog/browser-data-theft/27871/), cookies, and other files that happen to be on the hard drive of the infected device. Moreover, sometimes game accounts are just one of the targets of stealers — some are no less interested in your online banking credentials.[[3]](#footnote-2)

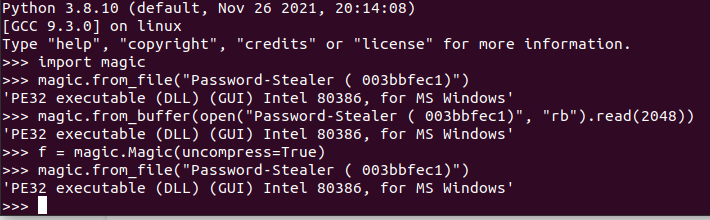
**Machine Information:**

****

**Magic byte or File signature:**

****

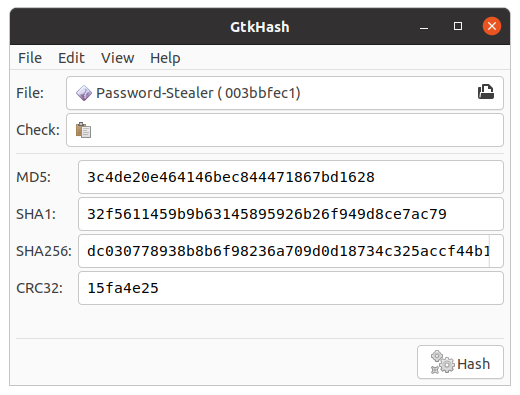
**File type:**

****

**Exe Type:**

****

**CalcHash:**

****

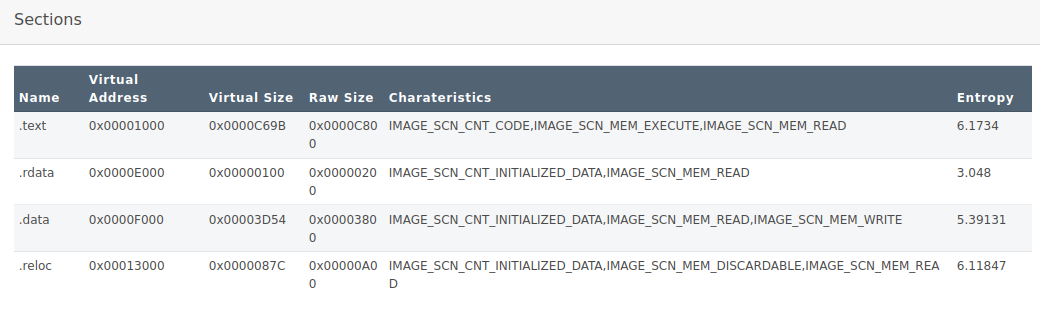
The hash type used for the identification of the file is SHA256, from the website from where it was download.

**DLLs:**

The Dlls used by the executable are Known by **Anyrun:**

* **wsock32.dll**
* **kernel32.dll**
* **urlmon.dll**
* **userenv.dll**
* **ole32.dll**
* **user32.dll**
* **advapi32.dll**
* **wininet.dll**
* **shlwapi.dll**

**SECTIONS and OFFSET:**

****

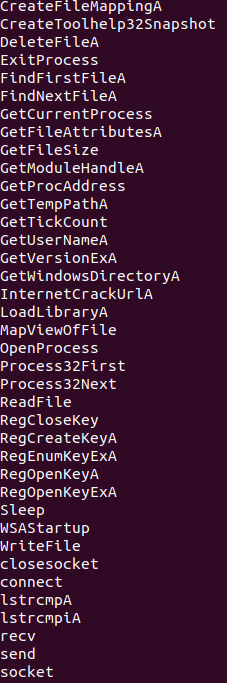
The sections and their offsets of the file are known by **ANYRUN**.

**PACKING INFO:**

**By peframe.**

****

**Strings**

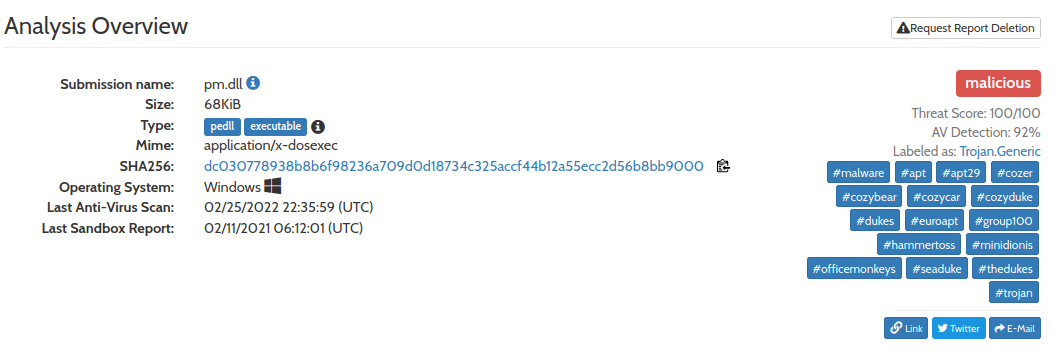
****

**These strings were extracted with the help of peframe.**

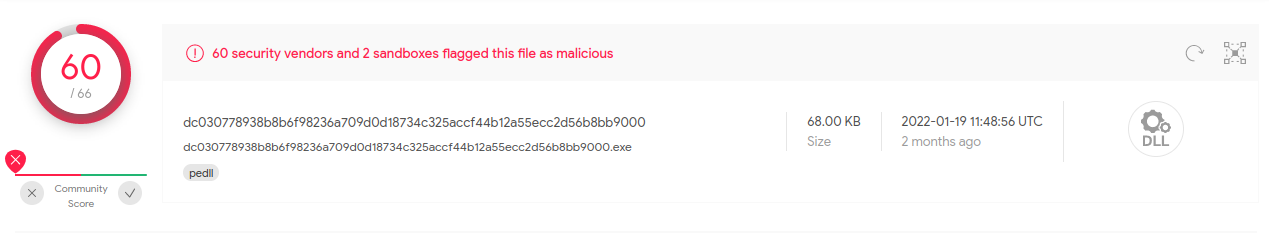
These are the malicious strings or breakpoints extracted from the Malware, I’ve written a yara script to search for these strings if any of these strings are found the .exec is a confirmed malware.

**HYBRID ANALYSIS:**

The website marked the file as malicious.

******

**VIRUSTOTAL:**

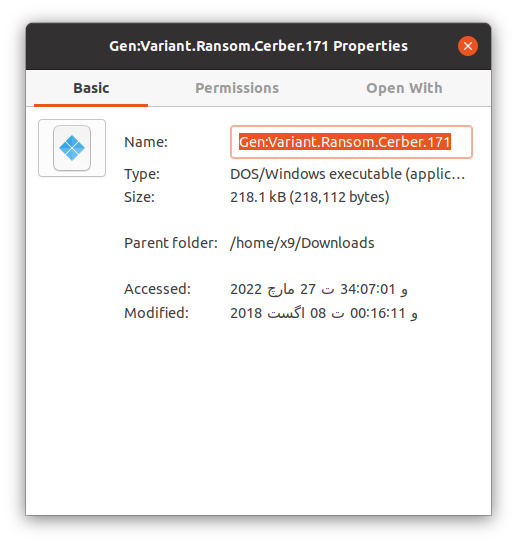
****

The file known to be malicious by 60 security vendors by VIRUSTOTAL.

***5.Gen:Variant.Ransom.Cerber.171***

Ransom.Cerber is a [ransomware](https://www.malwarebytes.com/ransomware) application that uses a ransomware-as-a-service (RaaS) model where affiliates purchase and then subsequently spread the malware. Commissions are paid to the developers for the use of the malware. Ransom.Cerber uses strong encryption, and there are currently no free decryptors available..[[4]](#footnote-3)

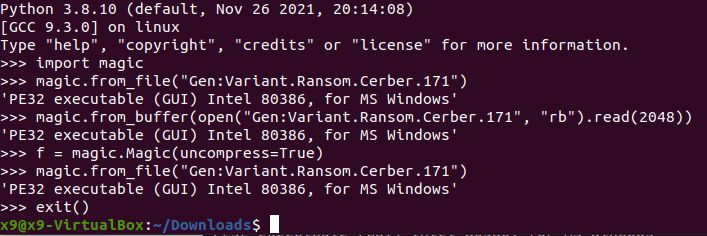
**Machine Information:**

****

**Magic byte or File signature:**

****

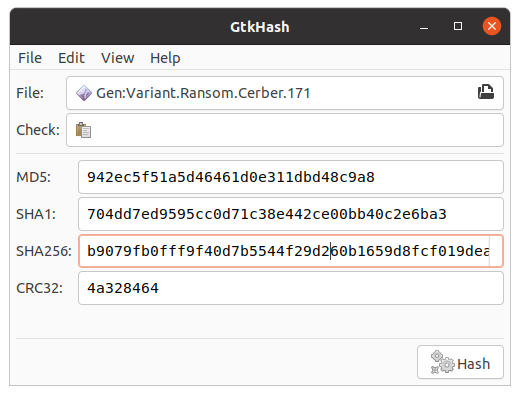
**File type:**

****

**Exe Type:**

****

**CalcHash:**

****

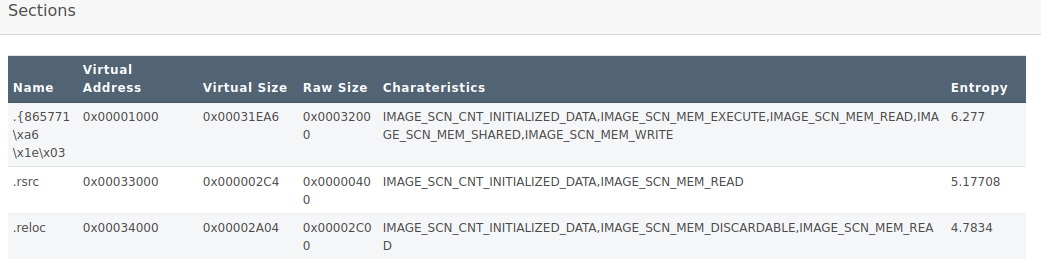
The hash type used for the identification of the file is SHA256, from the website from where it was download.

**DLLs:**

* **WINHTTP.dll**
* **KERNEL32.dll**
* **USER32.dll**
* **ADVAPI32.dll**
* **ole32.dll**
* **OLEAUT32.dll**
* **SHLWAPI.dll**
* **RPCRT4.dll**
* **urlmon.dll**
* **Secur32.dll**
* **PSAPI.DLL**

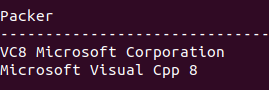
The Dlls used by the executable are Known by Anyrun:

**SECTIONS and OFFSET:**

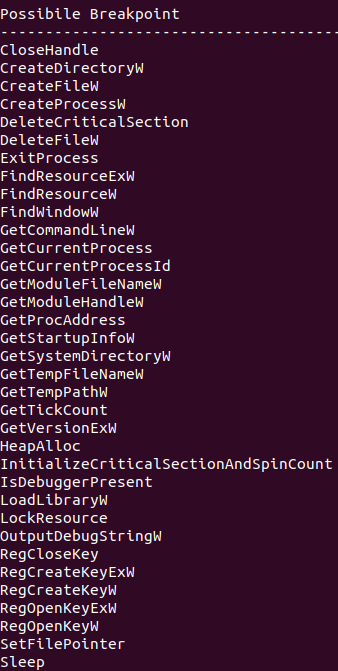


The sections and their offsets of the file are known by ANYRUN.

**PACKING INFO**:



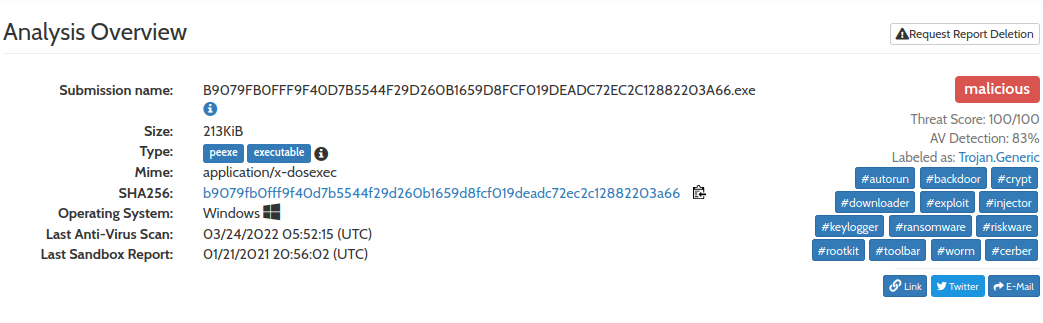
**Strings**

****

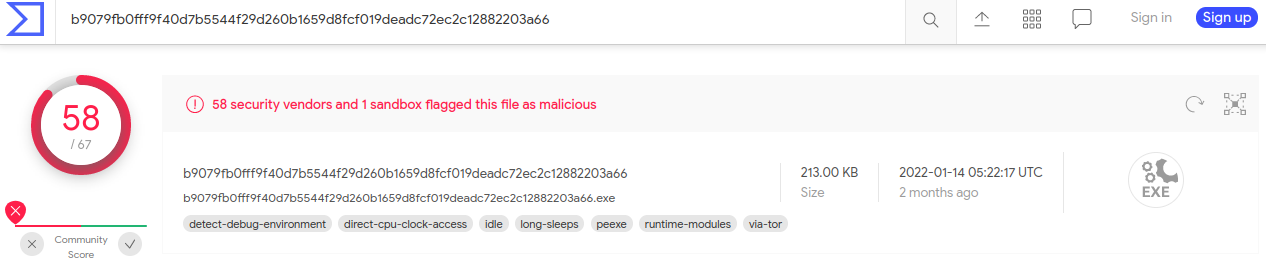
**These strings were extracted with the help of peframe.**

These are the malicious strings or breakpoints extracted from the Malware, I’ve written a yara script to search for these strings if any of these strings are found the .exec is a confirmed malware.

**HYBRID ANALYSIS:**

******

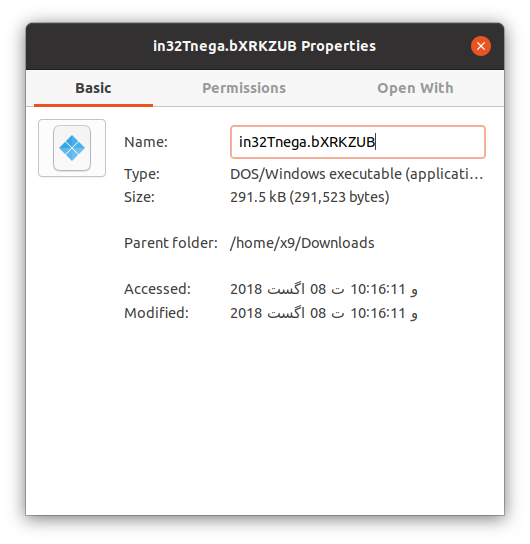
**VIRUSTOTAL:**

****

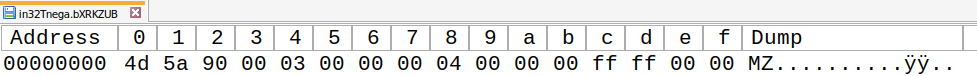
***6.in32Tnega.bXRKZUB***

**Trojan:Win32/Tnega.ml** is a computer virus that can infect executable PE files. It is being utilized by hackers to download a more hazardous virus on the computer. Once it infects the computer, Trojan:Win32/Tnega.ml also acts as a computer network worm by exploiting the unpatched DCOM RPC vulnerability. As a result, this virus can spread over the network and infect other PE executable that further compromised the computers.

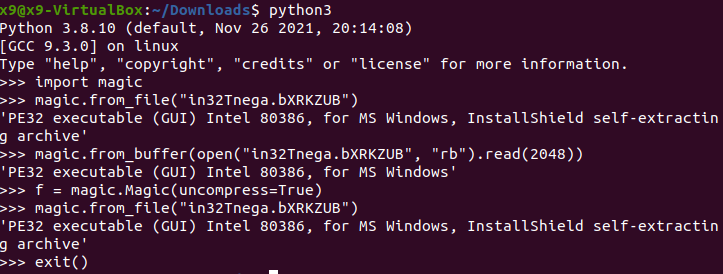
**Machine Information:**

****

**Magic byte or File signature:**

****

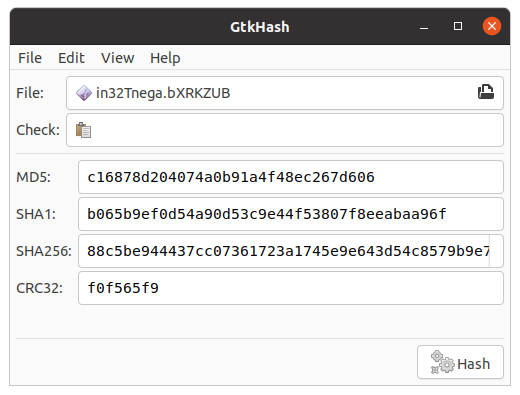
**File type:**

****

**Exe Type:**

****

**CalcHash:**

****

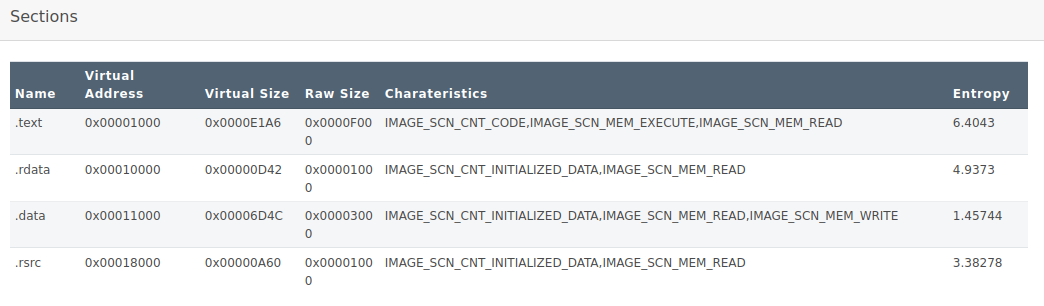
The hash type used for the identification of the file is SHA256, from the website from where it was download.

**DLLs:**

The Dlls used by the executable are Known by Anyrun:

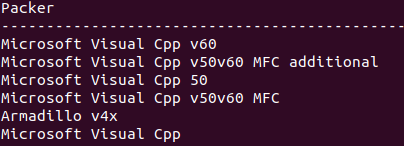
* KERNEL32.dll
* USER32.dll
* SHELL32.dll

**SECTIONS and OFFSET:**

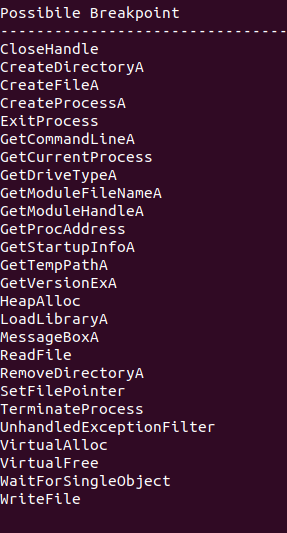
****

The sections and their offsets of the file are known by ANYRUN.

**PACKING INF**O:



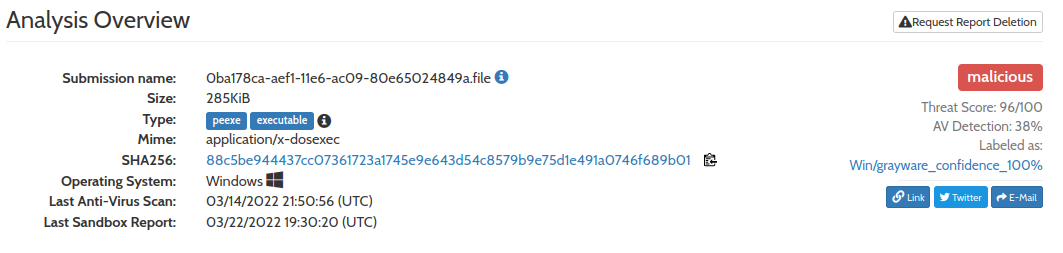
**Strings**

****

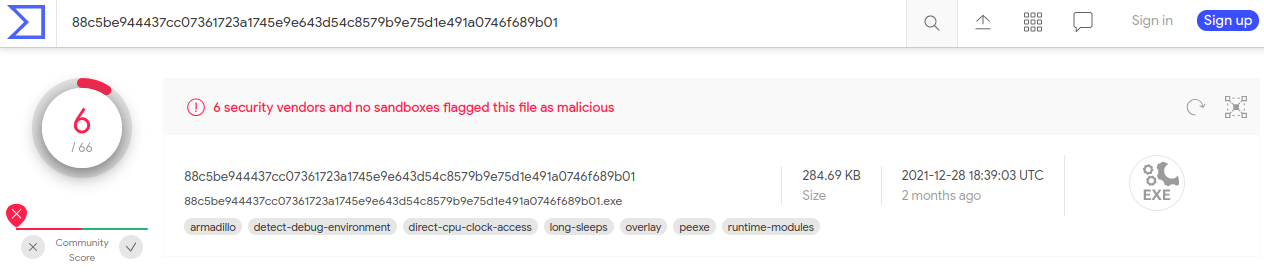
**These strings were extracted with the help of peframe.**

These are the malicious strings or breakpoints extracted from the Malware, I’ve written a yara script to search for these strings if any of these strings are found the .exec is a confirmed malware.

**HYBRID ANALYSIS:**

******

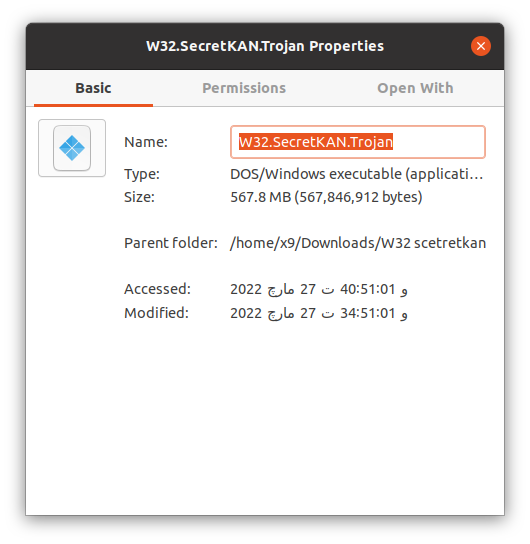
**VIRUSTOTAL:**

****

***7.W32.SecretKAN.Trojan***

Trojan:W32/DatCrypt drops a DLL file that encrypts files with specific extensions on the system. The DLL then informs the user that the affected files should be decrypted with a certain "utility program", which it also attempts to download and install on the system.A malware that engages in this type of behavior is known as [ransomware](https://www.f-secure.com/v-descs/ransomware.shtml). [[5]](#footnote-4)

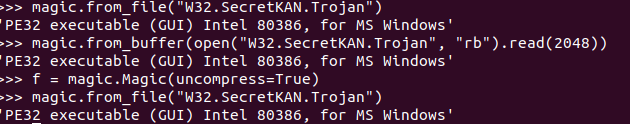
**Machine Information:**

****

**Magic byte or File signature:**

****

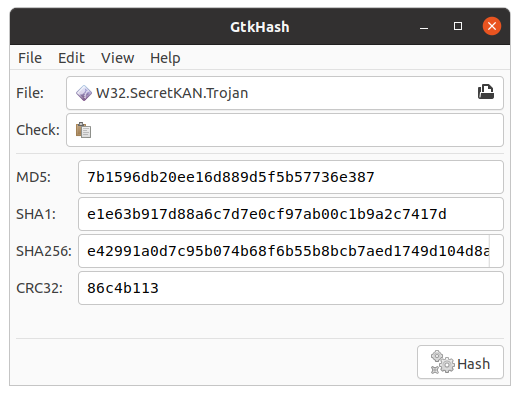
**File type:**

****

**Exe Type:**

****

**CalcHash:**

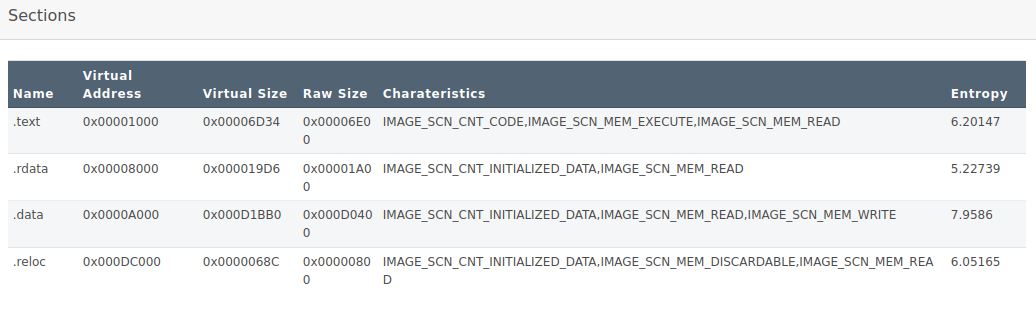
****

The hash type used for the identification of the file is SHA256, from the website from where it was download.

**DLLs:**

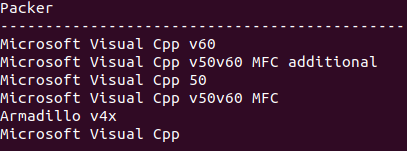
The Dlls used by the executable are Known by Anyrun:

* WININET.dll
* KERNEL32.dll
* USER32.dll
* ADVAPI32.dll
* SHELL32.dll
* ole32.dll

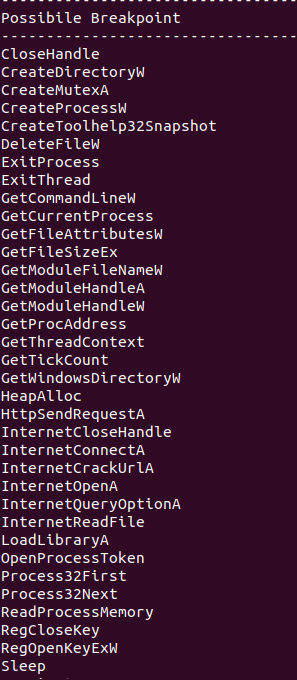
**SECTIONS and OFFSET:**

The sections and their offsets of the file are known by ANYRUN.

**PACKING INFO:**

****

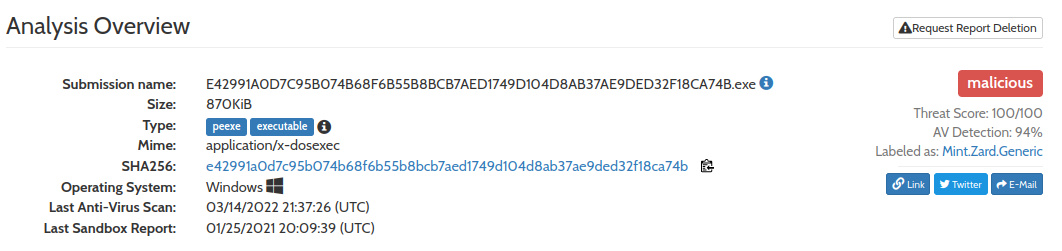
**Strings**

****

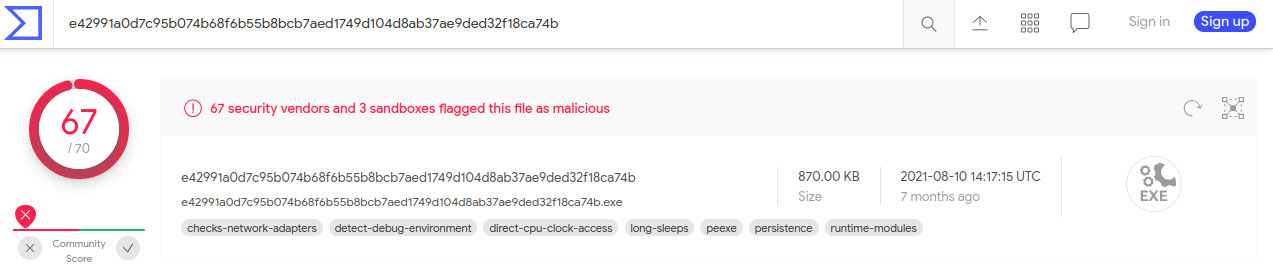
**These strings were extracted with the help of peframe.**

These are the malicious strings or breakpoints extracted from the Malware, I’ve written a yara script to search for these strings if any of these strings are found the .exec is a confirmed malware.

**HYBRID ANALYSIS:**

******

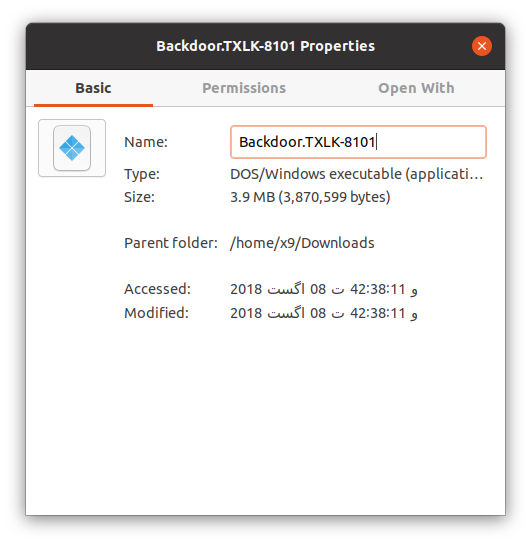
**VIRUSTOTAL:**

****

***8.Backdoor.TXLK-8101***

B[ackdoor](https://blog.malwarebytes.com/glossary/backdoor/) refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka [root access](https://en.wikipedia.org/wiki/Superuser)) on a computer system, network, or software application. Once they're in, cybercriminals can use a backdoor to steal personal and financial data, install additional malware, and hijack devices.

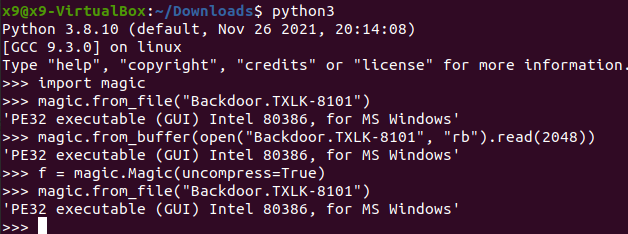
**Machine Information:**

****

**Magic byte or File signature:**

****

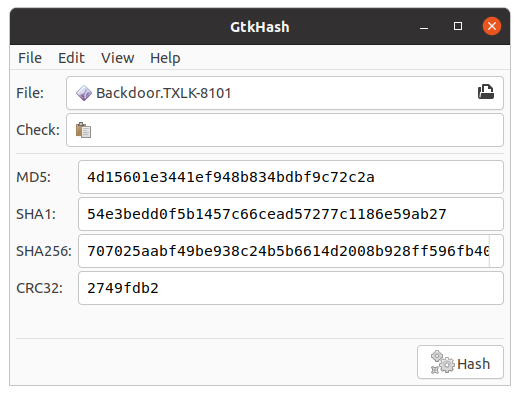
**File type:**

****

**Exe Type:**

****

**CalcHash:**

****

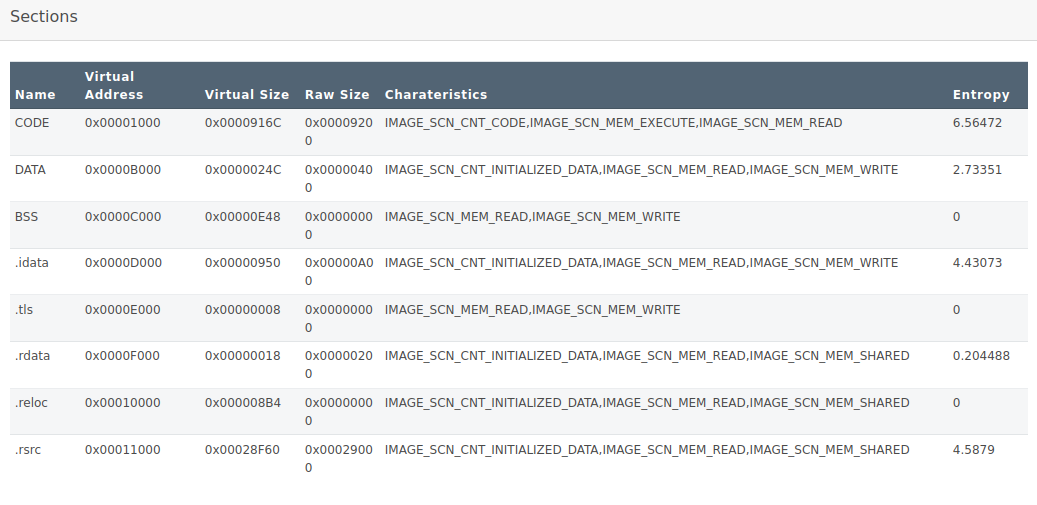
The hash type used for the identification of the file is SHA256, from the website from where it was download.

**DLLs:**

The Dlls used by the executable are Known by Anyrun:

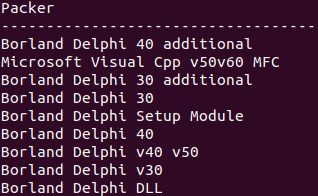
* kernel32.dll
* user32.dll
* oleaut32.dll
* advapi32.dll
* comctl32.dll

**SECTIONS and OFFSET:**

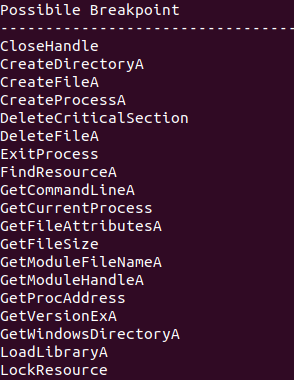


The sections and their offsets of the file are known by ANYRUN.

**PACKING INFO:**

****

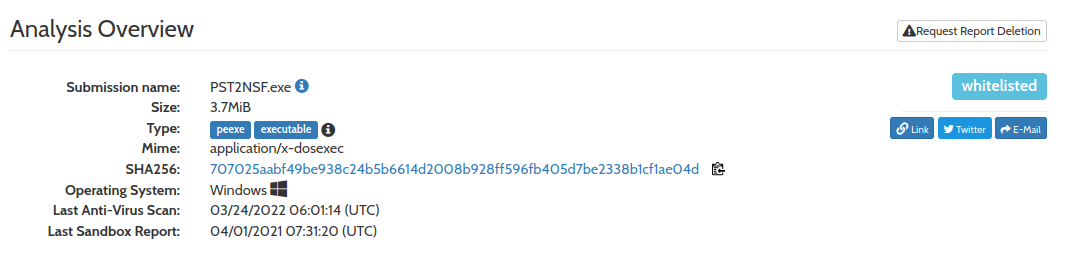
**Strings**

****

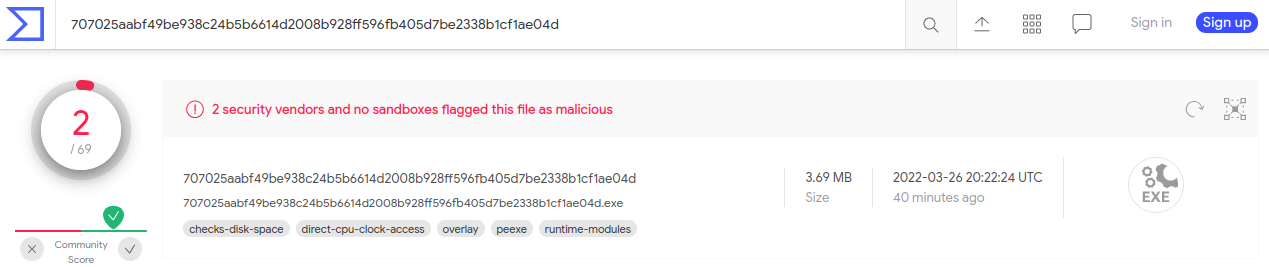
**These strings were extracted with the help of peframe.**

These are the malicious strings or breakpoints extracted from the Malware, I’ve written a yara script to search for these strings if any of these strings are found the .exec is a confirmed malware.

**HYBRID ANALYSIS:**

******

**VIRUSTOTAL:**

****

1. <https://www.f-secure.com/v-descs/trojan-dropper_w32_agent.shtml> [↑](#footnote-ref-0)
2. https://www.f-secure.com/v-descs/trojan\_w32\_generickd\_3016333.shtml [↑](#footnote-ref-1)
3. https://www.kaspersky.com/blog/gaming-password-stealers/35895/ [↑](#footnote-ref-2)
4. https://blog.malwarebytes.com/detections/ransom-cerber/ [↑](#footnote-ref-3)
5. https://www.f-secure.com/v-descs/trojan\_w32\_datcrypt.shtml [↑](#footnote-ref-4)