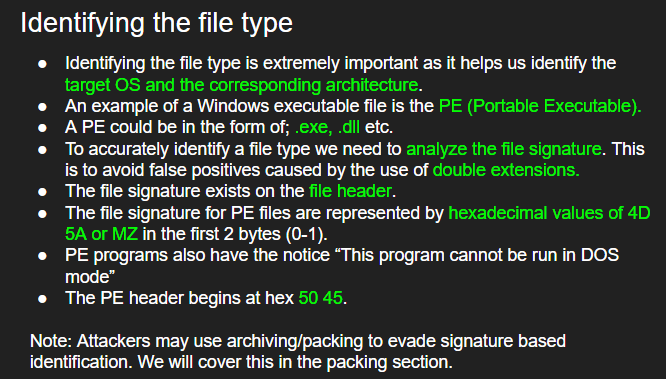
MALWARE ANALYSIS

FILE TYPE IDENTIFICATION:

<https://www.youtube.com/watch?v=idcvzyibrag&list=PLBf0hzazHTGMSlOI2HZGc08ePwut6A2Io&index=8>



Hackers try to change the extension. Ex: change .exe to doc file or file.exe.doc

Therefore, file signature is important.

Downloads required: (other than YARA)

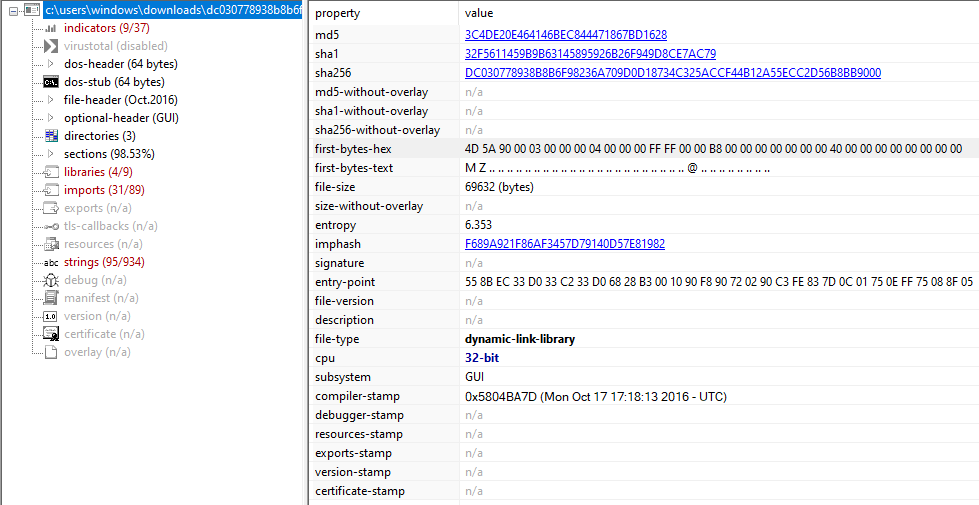
Malware Sample download: [https://s3.eu-central-1.amazonaws.com...](https://www.youtube.com/redirect?event=video_description&v=idcvzyibrag&redir_token=QUFFLUhqbVBQc2JwdFViVExTMTJnazZEUldUNFJReG9pQXxBQ3Jtc0tsMDItRzNYblhJNHpvRWl4c0tyZk5xaDROcUlIeWZSeWR4R0NmZXpsaFdIdVFzdnMyTllSVlp6djR4SVE1amVCU2J1dGs3RV9icWtjYWZHWHVwUFEtekhQN3U4SkMzbXVLWDdHVUpmYnZNYjBxd0FJZw%3D%3D&q=https%3A%2F%2Fs3.eu-central-1.amazonaws.com%2Fdasmalwerk%2Fdownloads%2Fdc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000%2Fdc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000.zip)

It is a generic password stealer/credential harvester.

PEStudio: <https://www.winitor.com/features>

Steps to setup the file:

* Extract the file
* It will ask for password: “infected”.
* Notice that it doesn’t have an extension but it doesn’t mean it can’t be an executable.
* Drag and drop in pestudio.



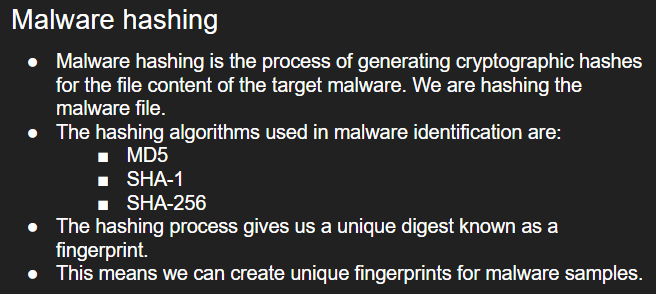
You can see first bytes as 4D 5A i.e M Z which tells us it is a PE file.

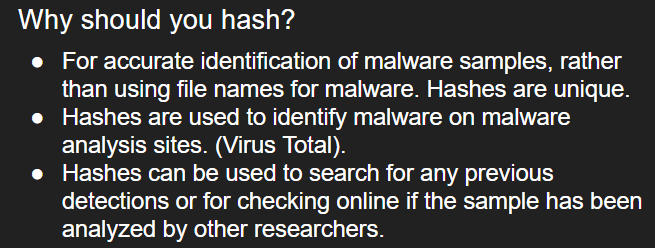


File type is DLL

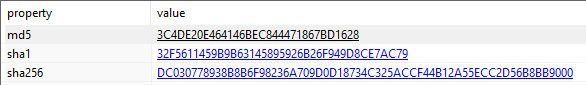
MALWARE HASHES AND VIRUS TOTAL:

<https://www.youtube.com/watch?v=-Z0d6q73Lsg&list=PLBf0hzazHTGMSlOI2HZGc08ePwut6A2Io&index=9>

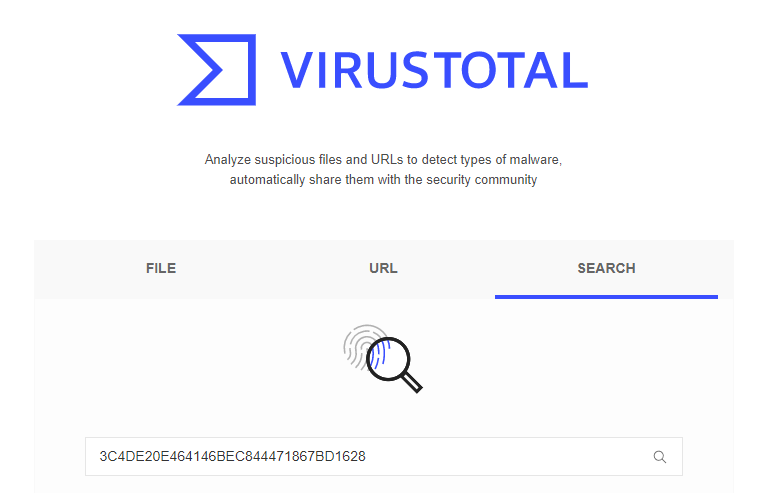




You can see the different hash values in PEstudio.

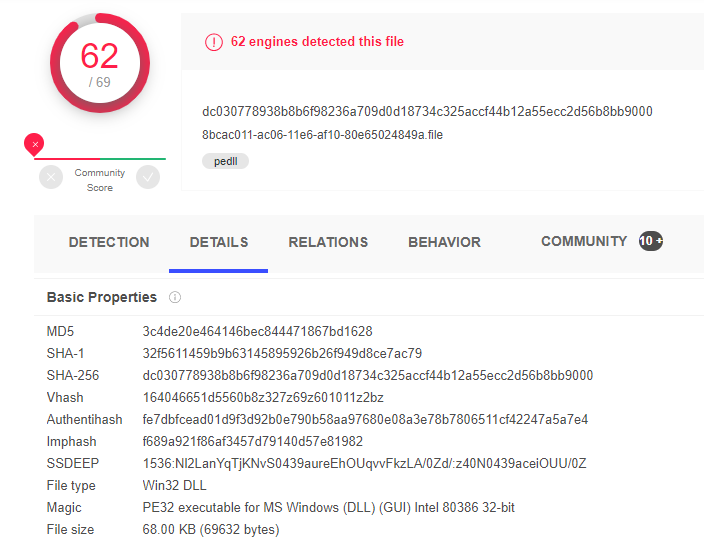


Copy md5 hash and search it on virus total website



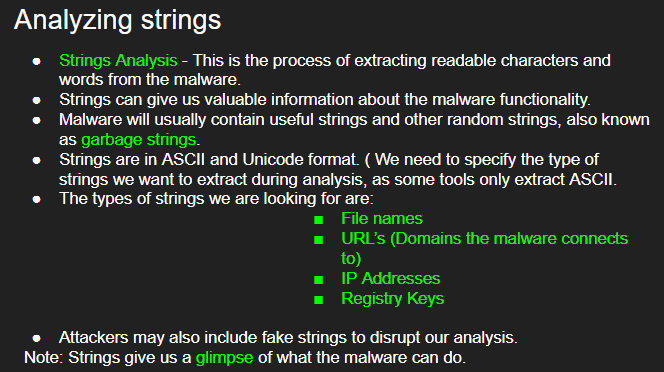
62/69 engines have detected this malware before.

Select details and you can see the file type, other hash values ,its history, various names it goes by etc.

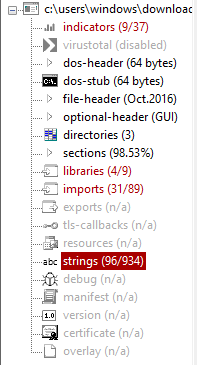


ANALYZING STRINGS

<https://www.youtube.com/watch?v=V3_vc7BO9lU&list=PLBf0hzazHTGMSlOI2HZGc08ePwut6A2Io&index=10>



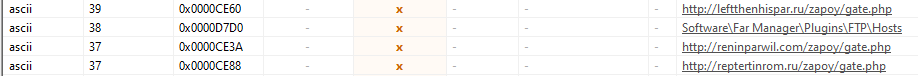
Select strings section in PEStudio to analyze them and find strings that might identify the malware family.



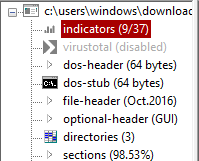
You can observe a number of things.

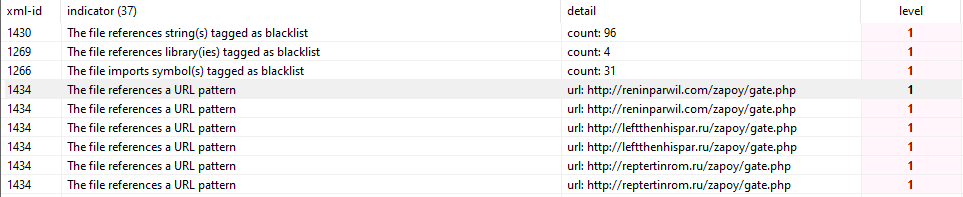
A POST method called meaning that the hacker might be sending information. We can see registry key strings too.

Notice the three url strings. They might be the Russian command and control centers from where the attack is controlled or where all the credentials are sent back to.



For more help checkout the indicators section.





url: http://reninparwil.com/zapoy/gate.php

url: http://leftthenhispar.ru/zapoy/gate.php

url: http://reptertinrom.ru/zapoy/gate.php

CREATING YARA RULE:

<https://www.youtube.com/watch?v=35Exd9GrR5I&list=PLBf0hzazHTGMSlOI2HZGc08ePwut6A2Io&index=16>

Why use yara rules?

Hashing is not accurate because any change the hacker makes, changes the hash value too (even though the functionality remains same). Yara rules are powerful because if the hacker uses the same functionality, yara can detect it.

So we will write a yara rule based on the C&C center urls which we identified just above. It will also identify a PE.

rule creds

{

meta:

description = "Simple YARA rule to detect Command and control centers"

date="12th June 2020"

strings:

$a = "http://reninparwil.com/zapoy/gate.php"

$b = "http://leftthenhispar.ru/zapoy/gate.php"

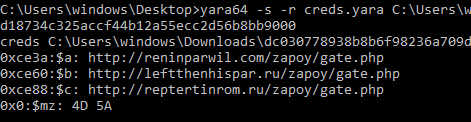
$c = “http://reptertinrom.ru/zapoy/gate.php”

$mz = {4D 5A}

condition:

($a or $b or $c)

}



Virus companies use yara rules to identify malware (not as simple as this one). Now, when you download a file, it can be scanned to check if it’s a PE and if it interacts with those malicious urls.