Malware Analysis

Lokibot Infostealer – Botnet

Dynamically Updating Information Stealer With Multiple Implementations And No Fixed Command and Control Server

M.Sc. Cybersecurity
School of Computing
National College of Ireland
Dublin, Ireland

Saptarshi Laha
x18170081

Table of Contents

Executive Summary

The Lokibot information stealer is one of the most persistent and dynamically updated malware since its creation in 2015. Till today (as recent as 6th April, 2020), there exist multiple "patched" variations of this malicious software each adding or trying to add a layer of protection and features that further allow it to bypass the currently implemented security mechanisms. Although some recently published "patched" versions come with a complete functionality revamp, most of the core functionalities have remained the same since the very early days (2015). The Lokibot malware specialises in malware packing, avoiding repeated execution and achieving persistence (although failing in some versions due to potential misconfiguration) apart from utilising advanced strategies such as process hollowing to hide its execution. In this report, a particular variant of Lokibot gets discussed, and the results of the dynamic and static analysis performed get highlighted.

Introduction

Lokibot falls under a category of malware known as an information stealer apart from emerging from the botnet origins. The botnet interactions of the malware help in the collection of critical user information and prevention of the same from reinfecting the system. The details regarding the same get discussed below in the main report. A botnet refers to several interconnected and internet-connected devices, each of which run one or more bots [1]. Contrary to popular belief, a botnet can be used for multiple malicious practices apart from performing distributed denial of service attacks, which are its most common use. A botnet network can find its use in the harvesting of user credentials (as in this case), sending spam based emails and other forms of communication, and also act as a RAT (Remote Access Trojan) thereby allowing the botmaster or the attacker access to the victim's system which can then get abused as per the needs of the attacker.

A general way to distinguish botnet based malware from the non-botnet based counterparts is to analyse the internet connection for potentially new and unordinary requests and responses, and further analyse the same to conclude the presence of malware and the type of malware present. In general, any malware that connects to a C2 (Command and Control) server is essentially a part of a botnet network. In the case of the Lokibot, the "patched" versions allow additional functionality in this regard which supersedes its previous versions, by allowing swappable C2 servers. This addition allows the attacker to change the server meant for interaction once it gets discovered and the information regarding the same has been made public. This modular design adds to the sophistication of this variety of malware in outliving other botnet based counterparts that utilise hardcoded C2 server credentials to perform interactions with victim machines, thereby living a short life and persisting only until the information regarding the server of contact has been discovered and made public.

Additionally, it is highly relevant to mention that botnets can undergo segregation based on the network architecture model they follow. There are in general two primary segregations of a botnet based on the same, out of which one depends on client-server network architecture, while the other follows a peer to peer network architecture. Despite these being the primary divisions, there are multiple examples where the partial or complete

implementation of both take place to add persistence to the malware further. In this case, however, the client-server based network architecture is followed by the malware, although because of the malware C2 implementation being modular in design and the several variants of the malware existing in the wild, it is very much possible and probable for a "patched" version to exist with a peer to peer C2 implementation or a hybrid implementation as well.

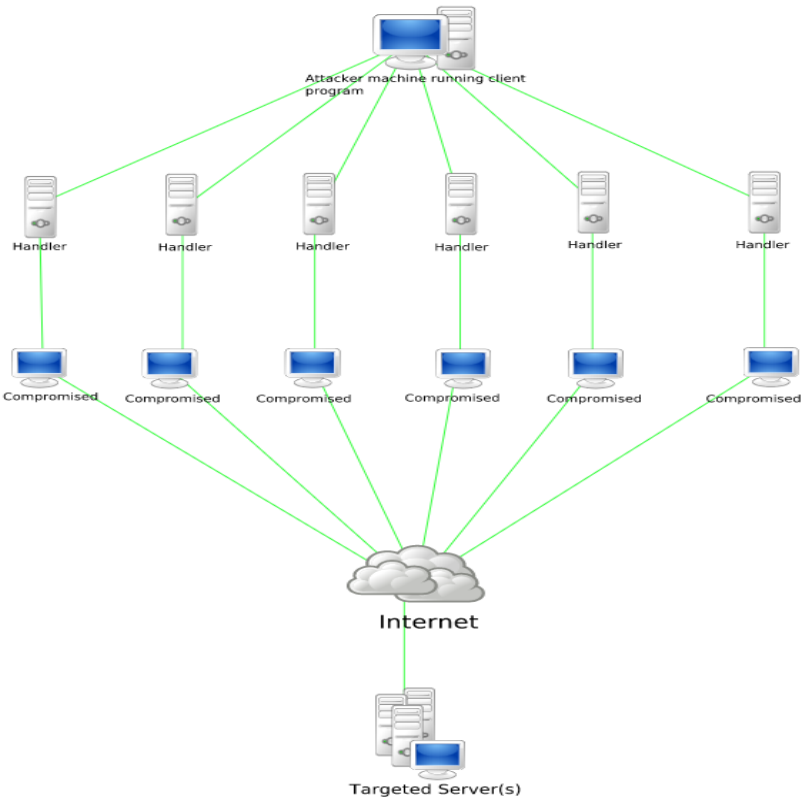

Fig 1. A botnet diagram, showing its use for a DDoS attack.

Methodology

Acquisition of the Malware

As multiple variants of the malware are available, one can acquire it from a variety of sources. However, the variant that undergoes discussion and detailing in this text is from VirusTotal [2]. Additionally, one can also download the sample from the Any.Run website [3], where the majority of its functionality undergoes documentation in a replayable virtualised sandbox desktop environment. The decision to choose this malware over the other ones present lies in the complexity of its working that it demonstrates along with the modular design approach and fancy persistence mechanisms that allow it to thrive to this date even after being released back in 2015.

Test Environment & Tools Used

The test environment used to firstly perform and confirm the findings based on analysis of the same variant was a Windows 10 x64 system for static analysis, Windows 10 x86 system for dynamic analysis and a Kali Linux x64 system for capture traffic. The installation of all the operating systems mentioned is on a type-2 hypervisor (Virtual Machine Software) called VMWare Workstation Pro. The host system, Windows 10 x64, is hardened with McAfee Total

Protection with custom-configured extremely potent firewall and real-time protection settings to detect and eliminate any suspicious content during the analysis. Additionally, the internet connection has undergone cut-off from the internal systems present in VMWare and have instead undergone connection to a custom VLAN (Virtual Lan) connecting the three operating systems. This setup gets used as the executable is a 32-bit .NET binary and is expected to run on any platform on or above Windows 7 x86, without the requirement of any service pack or updates being installed as it does not exploit any specific vulnerability. The x64 counterparts can also execute the same file without any issues as they are backwards compatible with the execution of code designed for x86 systems.

The tools used in this process are dnSpy for static analysis and dynamic analysis due to the executable file being a .NET binary. While INetSim gets used for dynamic analysis of network-related traffic. Additionally, IDA Pro finds its use for static analysis only, while Process Explorer and Procmon get used for dynamic analysis. As VirusTotal provides initial analysis details, hence mentioning of other tools used to gather additional useful information regarding the malware undergoes omission.

Academic Articles Referred

Since there exist a plethora of academic articles related to the topic of Lokibot due to its widespread nature, locking down on a single article was challenging. However, when the same search gets performed using the hashes, one does not take long to figure out potentially useful academic articles. The primary source of information to confirm the findings is the information present in the malicious activity report published by Infoblox [4] and the detail concerning the spread of the malware gets acquired from the Spamhaus Botnet Threat Report 2019 [5].

The Strategy of Analysis & Confirmation

The strategy of analysing this malware follows the same steps as in the case of any other malware of first finding the necessary information related to the malware and confirming it against the information provided by the VirusTotal webpage. Next, the malware gets analysed without any assistance or reference to any sources using multiple static and dynamic analysis methods that are felt necessary in this context. After this process, the findings are analysed and verified against a trusted report from an organisation. This approach gets followed as opposed to understanding and paraphrasing a company report to sharpen the malware analysis skills, which is an essential skill for any cybersecurity student apart from getting hands-on experience in performing malware triage.

The steps of exact analysis can find its division into two subsections as per standard analysis practices:

1. **Static Analysis** – This part of the analysis consisted of gaining initial information about the malware, apart from using a variety of decompilers to gain additional information regarding the working of the same.
2. **Dynamic Analysis** – The dynamic analysis consisted of execution of the malware to find details regarding the C2 server, the type of request used and the data sent in the request to gain additional information.

The critical details extracted from following this methodology gets highlighted in the next section.

Botnet Investigations & Findings

This section highlights all the findings related to the botnet in excruciating detail for the reader.

Botnet Identification

The filenames, types, creation times, file version information and hashes related to this file are present below.

Table 1. Malware Identification Information

File Name – 7d52796bb5cbc165029c623d85d2ca3b.virus	
File Type – PE32 executable for MS Windows (GUI) Intel 80386 32-bit Mono/.Net assembly	
Creation Time (Compilation Timestamp) – 2018-11-01 05:18:39	
Copyright Information – Copyright Â© VIRTUAL 2017	
Product Information – VirtualController	
Description – Virtual Controller	
File Size – 559.00 KB (572416 bytes)	
.NET Module Version ID – ceca68dc-0692-44ad-8e77-bf47ca46792d	
Number of AV Engines That Can Detect (VirusTotal) – 47/70	
MD5	**7d52796bb5cbc165029c623d85d2ca3b**
SHA – 1	**118e4386cf2bc8803d2b50ff2a3f1c1bd2a45cc1**
SHA – 256	**703a9cf507ddf1b8b42b63a16927b8b72fa79be3ee7f9d 898d52a243a010af46**
Vhash	**2550361555171z31z21**
Authentihash	**838d5e37a17bd9db26723fd9be7c81a56e1748fb0f863ffe 81a9242cad5cb338**
Imphash	**f34d5f2d4577ed6d9ceec516c1f5a744**
SSDEEP	**12288:NBMGQobSwsnYFlkq/RABC3183jix2riHBfWsdo8187S 8B6tlw5j3UWoZN4ShE3U0:QGQoewsnYkq/+BC31GjoZ5dd187SgGlC**

The unique characteristics of this malware include the collection of credentials and security tokens from the victim machine, allowing the attacker to change the C2 server URL, applying process hollowing to disguise as a legal Windows process, etc.

The exact execution stages are as follows:

1. The malware unpacks and utilises process hollowing to execute as vbc.exe.
2. The malware utilises the GUID (Global unique identifier) to generate an MD5 hash which then gets used to prevent re-infection of the system, thereby preventing refilling of the C2 server's database with the duplicate data.
3. It connects to the server and tries sendings collected information including but not limited to credentials from applications such as web browsers, FTP and mail clients, etc.

It is also important to note that the victim machine needs an active internet connection for the successful execution of the Lokibot information-stealing malware.

Attack Chain

Although the malware acquired in this case is directly from a malware share website for research purpose, the original intended attack chain used a malicious email to deliver the payload. This detail was, however, not discovered as a part of this analysis process and instead, the analysis document finds its use in providing the attack chain information apart from other crucial information regarding this malware. The attack chain could not be analysed as the malware got flagged in a honeypot set up by a researcher, and none other than the actual researcher would possibly know the method of delivery of the malware apart from other potential victims of the malware. The identification of information from the victims, however, in this case, is minimal due to the single time execution and use of the malware which makes it unique and prevents itself from executing again on an infected machine making it extremely stealthy.

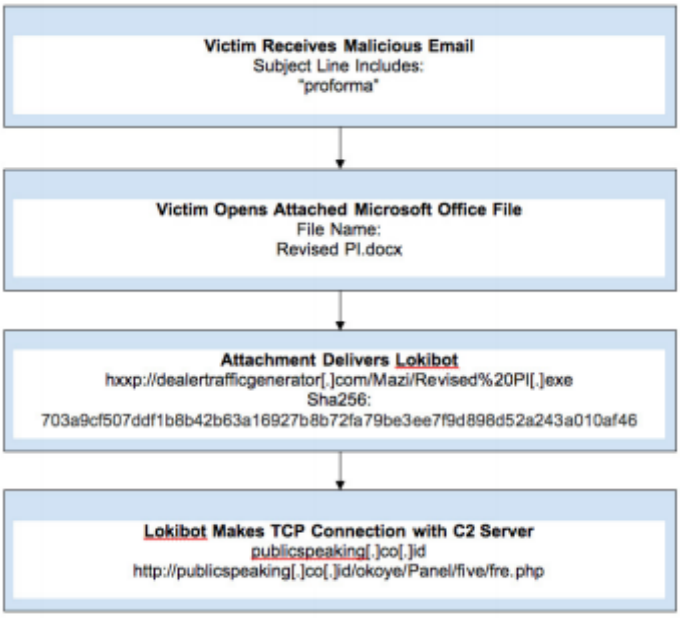

Fig 2. Attack Chain Information

Botnet Size & Damage

Although the inference from various internet sources pointed to Lokibot information stealer having a vast infection pool, no exact figures could be acquired. The closest approximation provided was by the Spamhaus Threat Report 2019 mentioning that Lokibot consisted of 2347 C2 servers in 2018 (based on the compile-time of this malware) which indicated a change per cent of +151% based on the previously present number of C2 servers related to Lokibot, thereby topping the chart in the total number of C2 servers being present. One can estimate the total spread of the malware based on the number of C2 servers deployed, which in this

case is enormous, suggesting that either the number of potential victims in the victim pool was significant as well, or the malware intended to target a vast audience.

Rank	C&Cs	Malware	Note	% change
1	2,347	Lokibot	Credential Stealer	+151 ▲
2	1,300	JBifrost	Java based Remote Access Tool (RAT)	+300 ▲
3	955	Pony	Dropper/Credential Stealer	−6 ▼
4	915	AZORult	Credential Stealer	+593 ▲
5	686	Heodo/Emotet	Dropper/Backdoor	+166 ▲
6	413	Gozi ISFB	e-banking Trojan	+47 ▲
7	322	NanoCore	Remote Access Tool (RAT)	–
8	269	Smoke Loader	Dropper/Backdoor	−31 ▼
9	241	TrickBot	e-banking Trojan	+19 ▲
10	203	RemcosRAT	Remote Access Tool (RAT)	–
11	157	RedAlert	Android Trojan	–
12	122	NetWire	Remote Access Tool (RAT)	–
13	117	AgentTesla	KeyLogger/Remote Access Tool (RAT)	–
14	107	Chthonic	e-banking Trojan	−75 ▼
15	106	PandaZeuS	e-banking Trojan	−19 ▼
16	98	ImminentRat	Remote Access Tool (RAT)	–
17	96	Neurevt	e-banking Trojan	–
18	82	ISRStealer	Credential Stealer	−49 ▼
19	70	ArkeiStealer	Credential Stealer	–
20	51	NjRAT	Remote Access Tool (RAT)	–
–	89	CoinMiners malware	Various crypto currency miners	–
–	46	IoT malware	Various IoT malware	−95 ▼
–	456	Generic	*	–
–	1,015	Others	Other malware families	–

* C&Cs where the associated malware could not be identified

Fig 3. Malware families associated with 2018 botnet C&C listings

Target Devices, Botnet Architecture & Botnet Resilience

The Lokitbot malware targets the devices running a Windows 7 or higher version of the operating system. The devices, in this case, include but is not limited to, anything from personal computers and laptops to virtual machines having Windows 7 or higher installed, mobile devices running Windows operating system and having the capability to execute .NET executable files, tablets, creativity devices such as Microsoft Surface, etc.

The architecture of the botnet discovered in this current sample is a client-server based C2 server model. However, as mentioned earlier, because of the sophisticated module-based programming of the C2 module and allowance to change its URL, it can be changed to a P2P based or a hybrid model if the need arises. The architecture of the botnet based on the information provided by the C2 server report of 2019, suggest that 2347 servers are present all of the world relating to the Lokibot botnet family, however not all may be connected to this malware sample and could relate to other modified versions of the same family of malware. In this case, only two such URLs get discovered from the binary. However, these could only relate to mediator links and not the actual C2 server that handles the interaction with the clients.

This variant of the Lokibot malware uses process hollowing to disguise itself as a genuine Windows process, prevents multiple infections by calculation of MD5 of an infected system based on GUID, therefore being stealthy and uses obfuscated functions and packing to prevent analysis of the same. Since it is intended for one-time use only, it does not find any

need for maintaining persistence and deals most of its damage on the first execution of the same.

Botnet Behavior

This subsection details the static analysis and dynamic analysis performed along with bits and pieces of additional information from the technical report to provide a comprehensive overview of the behaviour of the botnet.

Dynamic Analysis

After performing the initial static analysis (results mentioned in the botnet identification section), due to the obfuscated nature of the code on the first look, the dynamic analysis was performed first before performing advanced static analysis to get additional information regarding the execution process. The dynamic analysis showed the execution of a genuine windows binary in process explorer called vbc.exe, however, on comparing the strings of the file on disk and the file loaded in memory using Process Explorer, massive disparities get discovered suggesting process hollowing injection.

On running Wireshark along with INetSim on the Linux machine, the discovery of the executable performing a post request occurs. This discovery further provides information regarding the C2 server or the mediator link (publicspeaking.co.id) to which the malware tries to connect.

Procmon highlights other crucial information regarding the malware creating a registry key entry and a folder inside the AppData\Roaming directory. The registry entry is supposed to execute the executable from the AppData\Roaming directory; however, since it gets placed under the wrong subkey, the functionality does not come of use.

Advanced Static Analysis

Since dynamic analysis confirmed the presence of process hollowing, there needs to be a trigger point in the source code that injects an executable in the memory. Acquiring this executable, in this case, was performed using both the dynamic approach and the static approach as detailed below. In this case, the uncertainty of both the executable files acquired being the same, led to performing of both methods of unpacking. The stage diagram of the same gets very well presented in the report referred to as shown.

On analysing strings that get decoded, it is easy to find the unpacking executable. However, the first executable dropped drops one further executable that performs the actual functionality. In the dynamic approach, the dump from memory option can get used by any memory dumping toolkit and reconstructing the PE file.

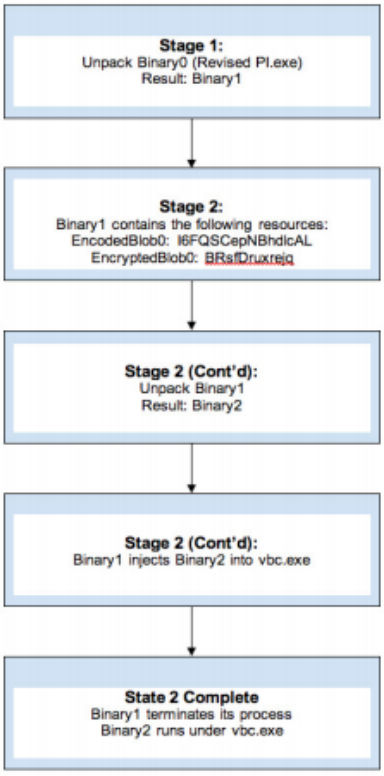

Fig 4. Unpacking Process of the Binaries

The mutex creation relies on the machine GUID parameter and is acquired using the registry key named MachineGuid from HKLM\Software\Microsoft\Cryptography. This parameter gets used to create a mutex which decides upon the launching of the application.

The second binary then tries to gain the credentials of the users based on multiple applications which the report details to be a total of 110. The same is found in this case using the memory image, while the report can find the disassembly of the same, which has not gone identification in this case due to time constraints.

Botnet Evolution

As mentioned earlier, Lokibot is an extremely advanced malware that can swap its C2 server URL, and thus it persists to this date. A table highlighting the various C2 servers related to the Lokitbot family of malware is presented below for reference from the cyber threat map. This threat map, however, covers multiple variants of Lokitbot and not just one of them. The most recent released variant is posted on VirusBay as recently as 6th April, 2020. Due to the low number of changes needed for modification with the potentially high gain, this model of malware finds extreme use in the darknet and underground internet communities as it targets easy to attack systems and naïve users gaining credential data which can then be misused, sold on the black market or used to perform credential stuffing attacks which are increasingly common in today's world.

Table 2. Cyber threat-map of Lokibot C2 servers [6]

Date	URL	IP Address	Type
29-04-2020	nicecars.com.ar/mine/Panel/five/PvqDq929BSx_A_D_M1n_a.php	190.61.250.140	Lokibot
29-04-2020	obimmaa.ir/todsay/Panel/five/PvqDq929BSx_A_D_M1n_a.php	104.237.252.50	Lokibot
28-04-2020	alforcargo.com/canna/five/PvqDq929BSx_A_D_M1n_a.php	185.102.136.183	Lokibot
28-04-2020	alforcargo.com/candy/five/PvqDq929BSx_A_D_M1n_a.php	185.102.136.183	Lokibot
28-04-2020	allenservice.ga/~zadmin/lmark/herm/uMc.php	8.208.82.254	Lokibot
28-04-2020	allenservice.ga/~zadmin/lmark/bill/uMc.php	8.208.82.254	Lokibot
28-04-2020	bubuyayatoolslog.ir/contnient-eight.com/los/panel/PvqDq929BSx_A_D_M1n_a.php	88.218.16.18	Lokibot
28-04-2020	bubuyayatoolslog.ir/emka/panel/PvqDq929BSx_A_D_M1n_a.php	88.218.16.18	Lokibot
28-04-2020	reacherp.sg/css/loki/Panel/five/PvqDq929BSx_A_D_M1n_a.php	148.66.135.80	Lokibot
27-04-2020	oneflextiank.com/cream/five/PvqDq929BSx_A_D_M1n_a.php	45.143.138.104	Lokibot
27-04-2020	oneflextiank.com/crazy/five/PvqDq929BSx_A_D_M1n_a.php	45.143.138.104	Lokibot
27-04-2020	oneflextiank.com/clock/five/PvqDq929BSx_A_D_M1n_a.php	45.143.138.104	Lokibot
27-04-2020	oneflextiank.com/cola/five/PvqDq929BSx_A_D_M1n_a.php	45.143.138.104	Lokibot
27-04-2020	oneflextiank.com/coco/five/PvqDq929BSx_A_D_M1n_a.php	45.143.138.104	Lokibot
27-04-2020	alforcargo.com/cutter/five/PvqDq929BSx_A_D_M1n_a.php	185.102.136.183	Lokibot
27-04-2020	alforcargo.com/cup/five/PvqDq929BSx_A_D_M1n_a.php	185.102.136.183	Lokibot
27-04-2020	alforcargo.com/craks/five/PvqDq929BSx_A_D_M1n_a.php	185.102.136.183	Lokibot
27-04-2020	alforcargo.com/copy/five/PvqDq929BSx_A_D_M1n_a.php	185.102.136.183	Lokibot
27-04-2020	alforcargo.com/clean/five/PvqDq929BSx_A_D_M1n_a.php	185.102.136.183	Lokibot
27-04-2020	alforcargo.com/clap/five/PvqDq929BSx_A_D_M1n_a.php	185.102.136.183	Lokibot

27-04-2020	alforcargo.com/cake/five/PvqDq929BSx_A_D_M1n_a.php	185.102.136.183	Lokibot
27-04-2020	alforcargo.com/cage/five/PvqDq929BSx_A_D_M1n_a.php	185.102.136.183	Lokibot
24-04-2020	jastex.info/ig7/PvqDq929BSx_A_D_M1n_a.php	89.208.210.215	Lokibot
24-04-2020	jastex.info/ig6/PvqDq929BSx_A_D_M1n_a.php	89.208.210.215	Lokibot
24-04-2020	avertonbullk.com/ig5/PvqDq929BSx_A_D_M1n_a.php	89.208.210.215	Lokibot
24-04-2020	avertonbullk.com/ig4/PvqDq929BSx_A_D_M1n_a.php	89.208.210.215	Lokibot
24-04-2020	avertonbullk.com/ig3/PvqDq929BSx_A_D_M1n_a.php	89.208.210.215	Lokibot
23-04-2020	mecharnise.ir/da5/PvqDq929BSx_A_D_M1n_a.php	104.237.252.50	Lokibot
23-04-2020	mecharnise.ir/da4/PvqDq929BSx_A_D_M1n_a.php	104.237.252.50	Lokibot
23-04-2020	mecharnise.ir/da3/PvqDq929BSx_A_D_M1n_a.php	5.56.133.174	Lokibot
23-04-2020	mecharnise.ir/da2/PvqDq929BSx_A_D_M1n_a.php	88.218.16.218	Lokibot
22-04-2020	jackmoynehan.com/zjack/Panel/five/PvqDq929BSx_A_D_M1n_a.php	192.254.186.177	Lokibot
21-04-2020	toyo-at-jp.info/ig2/PvqDq929BSx_A_D_M1n_a.php	89.208.85.227	Lokibot
21-04-2020	toyo-at-jp.info/ig1/PvqDq929BSx_A_D_M1n_a.php	89.208.85.227	Lokibot
20-04-2020	modcloudserver.eu/dave/five/PvqDq929BSx_A_D_M1n_a.php	213.108.241.164	Lokibot
20-04-2020	bubuyayatoolslog.ir/farma/panel/PvqDq929BSx_A_D_M1n_a.php	89.33.246.124	Lokibot
16-04-2020	taruntextlies.com/cutter/five/PvqDq929BSx_A_D_M1n_a.php	2.57.184.212	Lokibot
16-04-2020	taruntextlies.com/cup/five/PvqDq929BSx_A_D_M1n_a.php	95.142.44.172	Lokibot
16-04-2020	taruntextlies.com/craks/five/PvqDq929BSx_A_D_M1n_a.php	95.142.44.172	Lokibot
16-04-2020	taruntextlies.com/copy/five/PvqDq929BSx_A_D_M1n_a.php	95.142.44.172	Lokibot

Recommendation

The recommendations, in this case, can only be in terms of recommending users to download a legitimate piece of antivirus or complete protection suite (recommended) and turn up the settings to the highest level. Although Windows Defender was able to detect the old versions of the Lokitbot, it is still not up to date yet to identify the latest version that has released. Additionally, subverting the Windows defender is far more comfortable than subverting a commercial-grade antivirus software and hence is recommended to have the same installed to ensure protection against such threats.

The use of identification vectors from the previous subsection can also find use in avoiding this specific variant of malware. However, due to the ever-evolving nature of the malware, it is ideal for enforcing protection against the entire family rather than a single variant of a piece of malware.

Conclusion

The details mentioned above conclude the malware analysis report of the Lokibot botnet. There is a possibility of further discovery even after the details laid out by the current report based on deobfuscation of functions to uncover other potential functionalities provided by the Lokibot builder, but the same has not been ventured due to time constraints. However, the main functionalities have been discovered and documented in the report.

References

[1]"Botnet", *En.wikipedia.org*, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Botnet. [Accessed: 03- May- 2020].

[2]"VirusTotal", *Virustotal.com*, 2020. [Online]. Available: https://www.virustotal.com/gui/file/703a9cf507ddf1b8b42b63a16927b8b72fa79be3ee7f9d898d52a243a010af46/summary. [Accessed: 01- May- 2020].

[3]"703a9cf507ddf1b8b42b63a16927b8b72fa79be3ee7f9d898d52a243a010af46 (MD5: 7D52796BB5CBC165029C623D85D2CA3B) - Interactive analysis - ANY.RUN", *App.any.run*, 2020. [Online]. Available: https://app.any.run/tasks/b510a71b-1340-4c3b-8ac0-7da3eb749ba8/. [Accessed: 01- May- 2020].

[4]*Infoblox.com*, 2020. [Online]. Available: https://www.infoblox.com/wp-content/uploads/threat-intelligence-report-elements-of-lokibot-infostealer.pdf. [Accessed: 01- May- 2020].

[5]*Deteque.com*, 2020. [Online]. Available: https://www.deteque.com/app/uploads/2019/02/Spamhaus-Botnet-Threat-Report-2019.pdf. [Accessed: 01- May- 2020].

[6]"CyberCrime", *Cybercrime-tracker.net*, 2020. [Online]. Available: http://cybercrime-tracker.net/index.php?search=lokibot. [Accessed: 01- May- 2020].

Appendix

This section contains the screenshots related to the analysis of the malware.

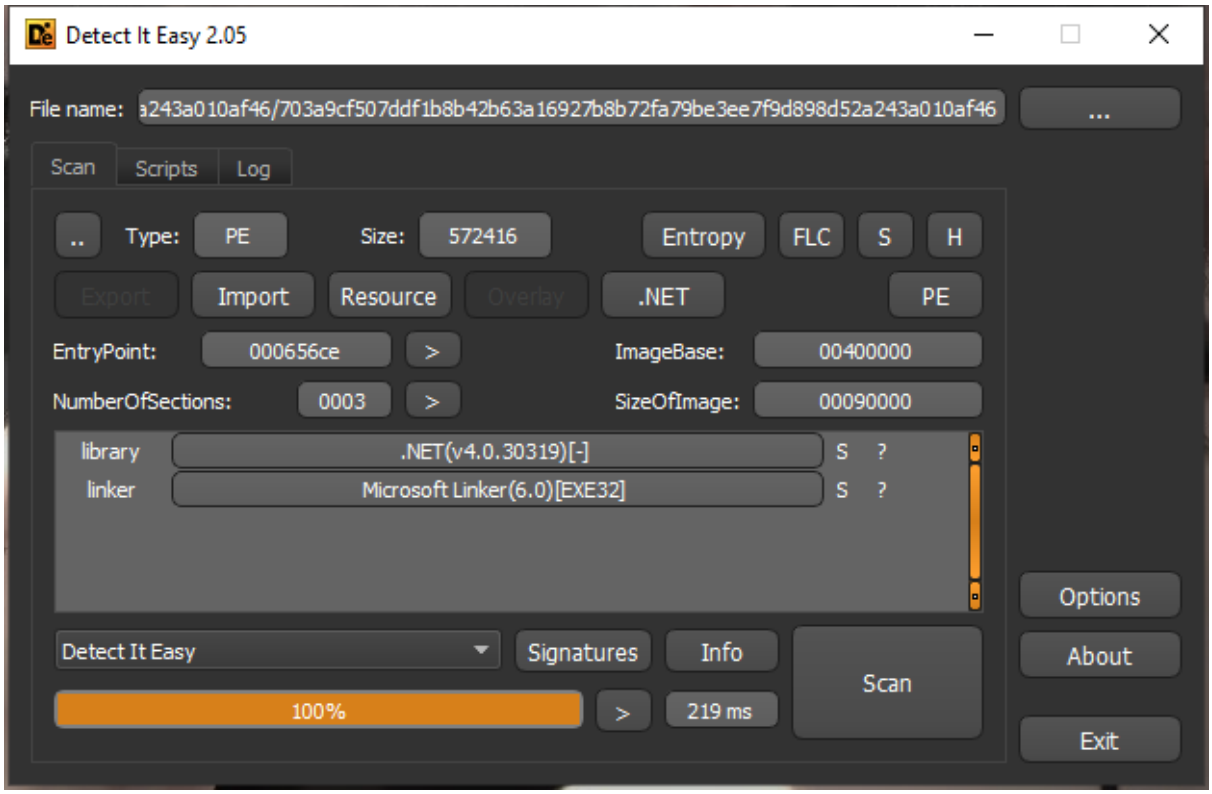

Fig 5. Detect It Easy Analysis of Lokibot malware

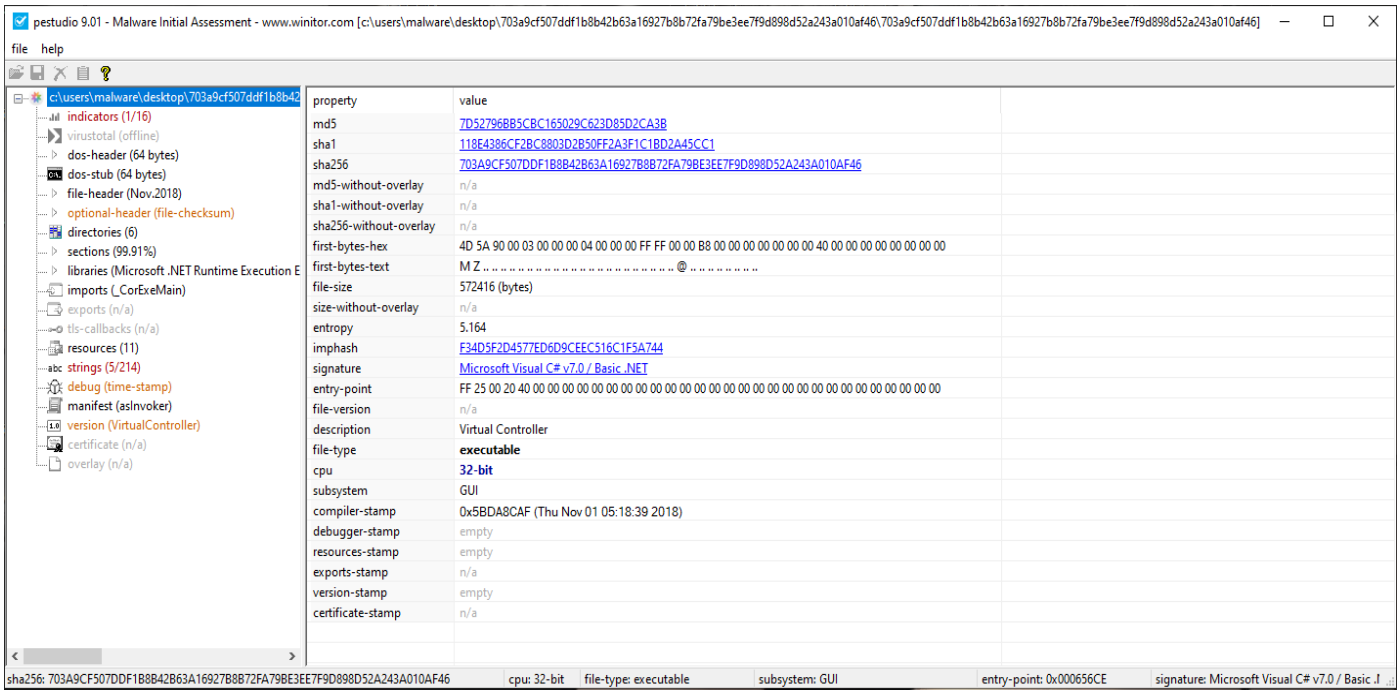

Fig 6. PE Studio Static Analysis of malware (Part 1)

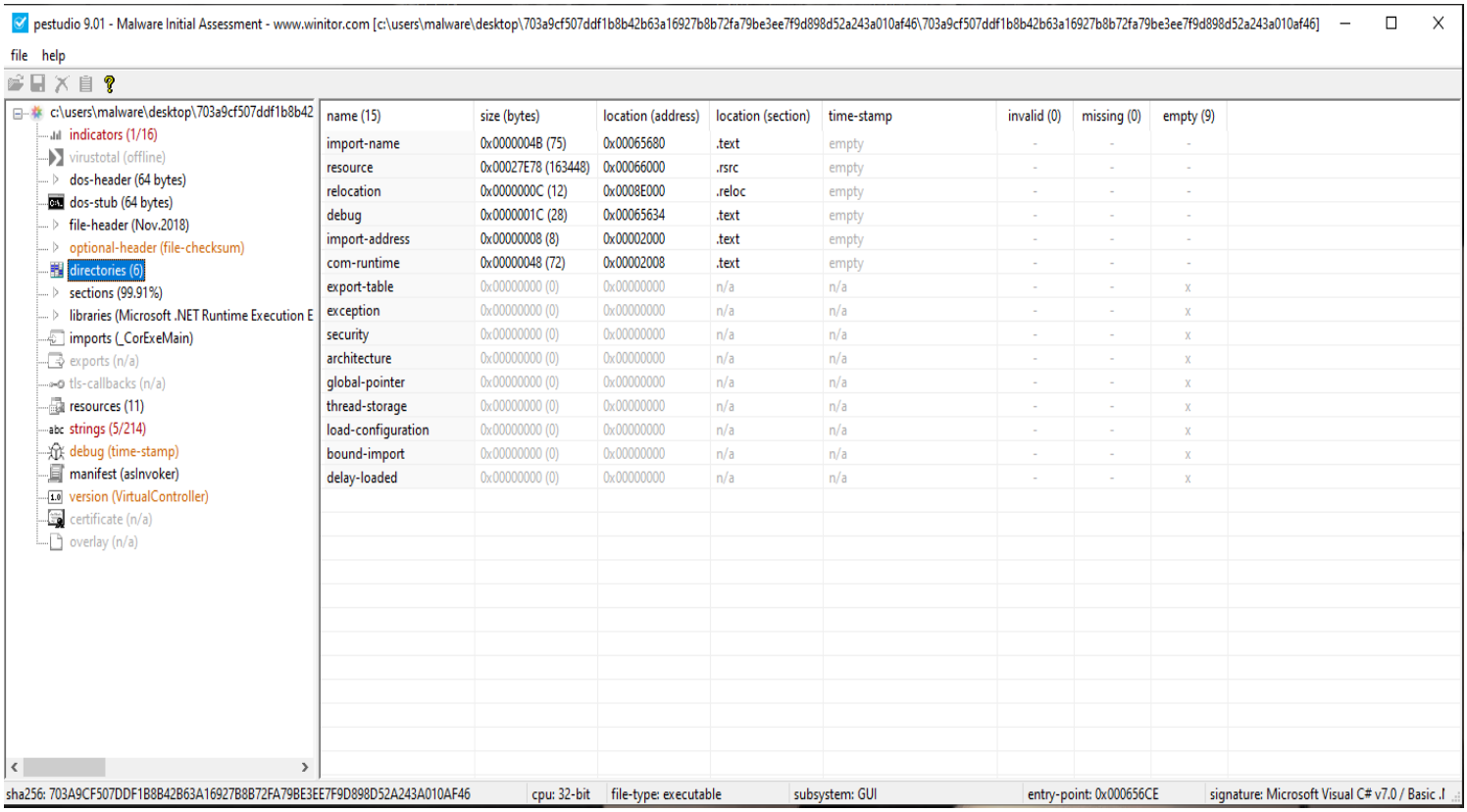

Fig 7. PE Studio Static Analysis of malware (Part 2)

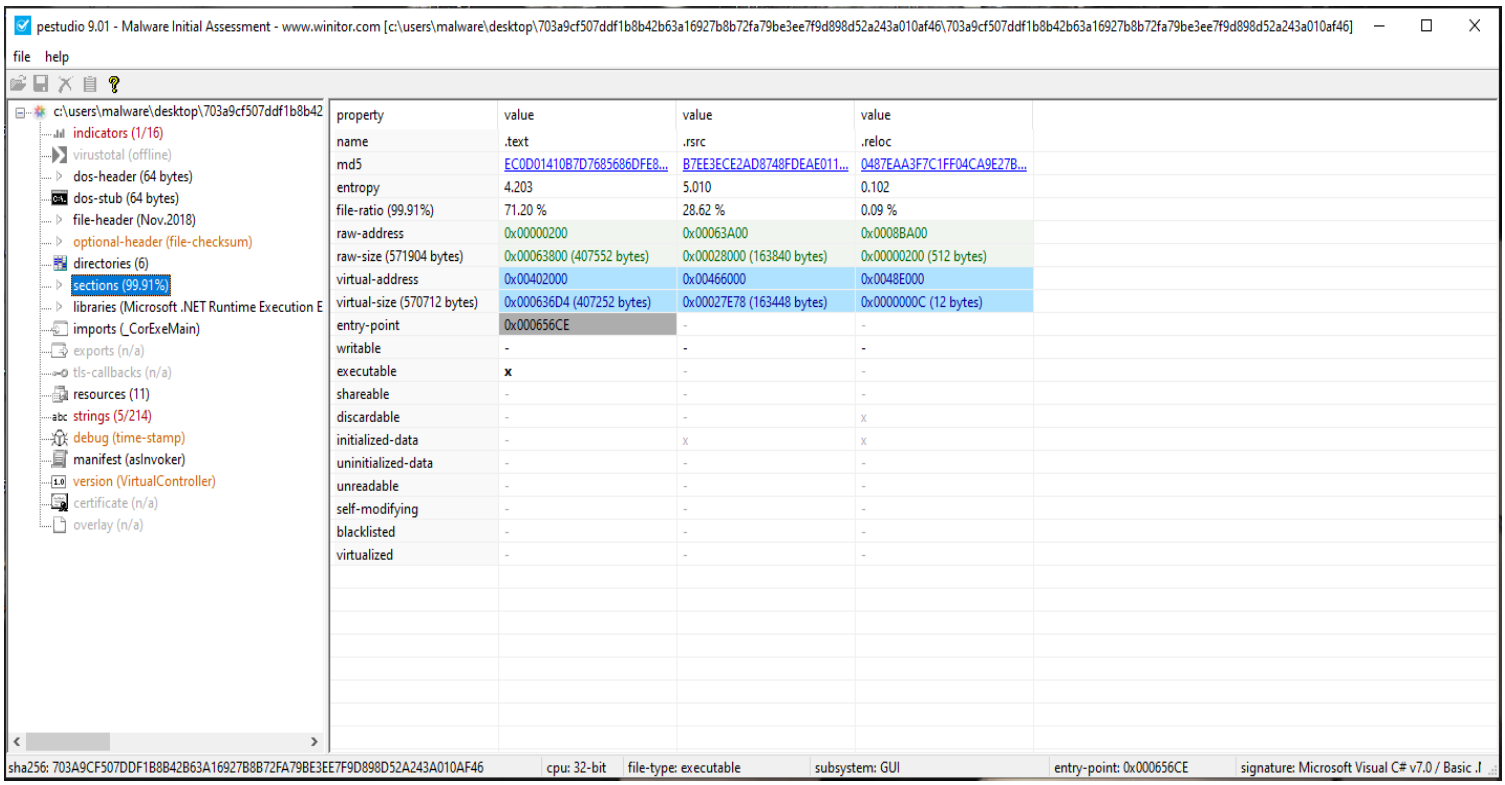

Fig 8. PE Studio Static Analysis of malware (Part 3)

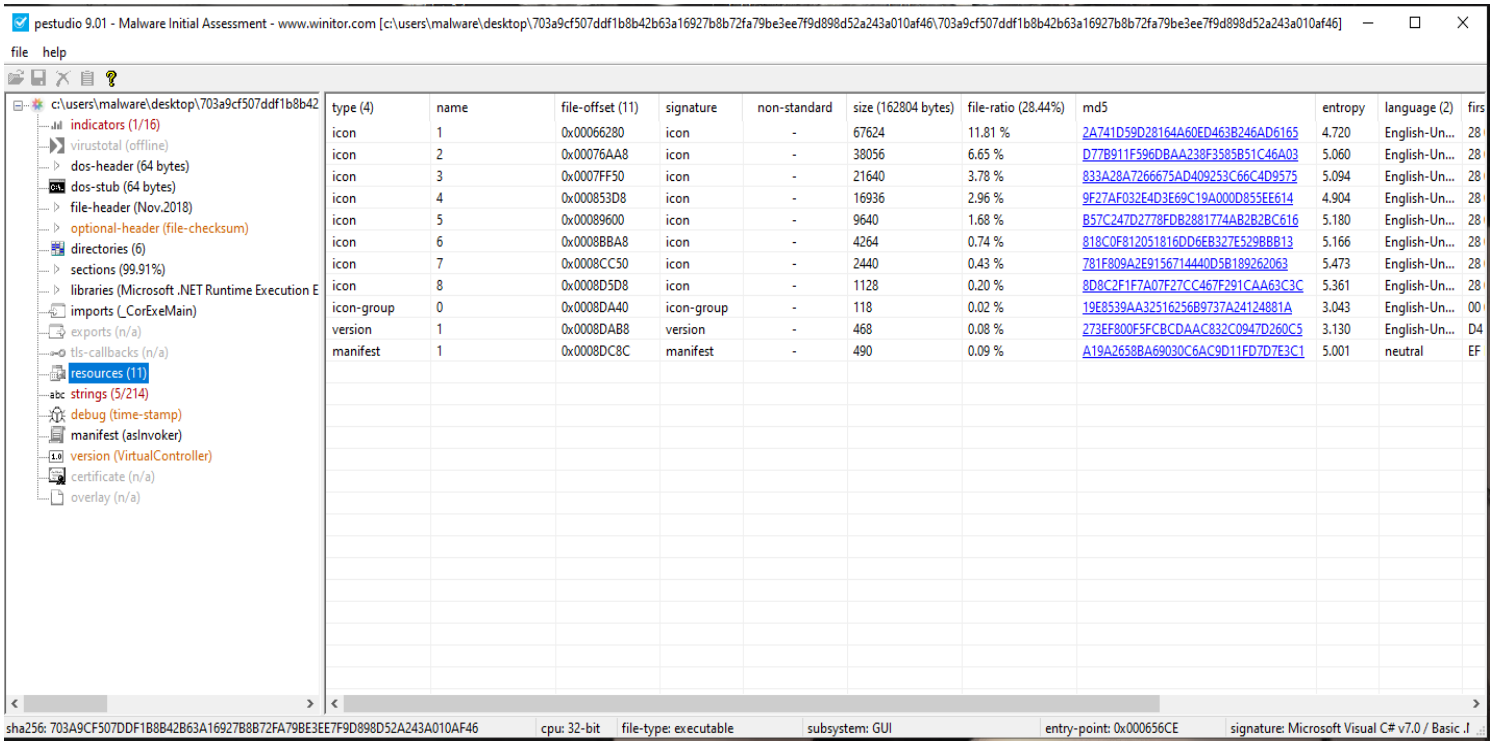

Fig 9. PE Studio Static Analysis of malware (Part 4)

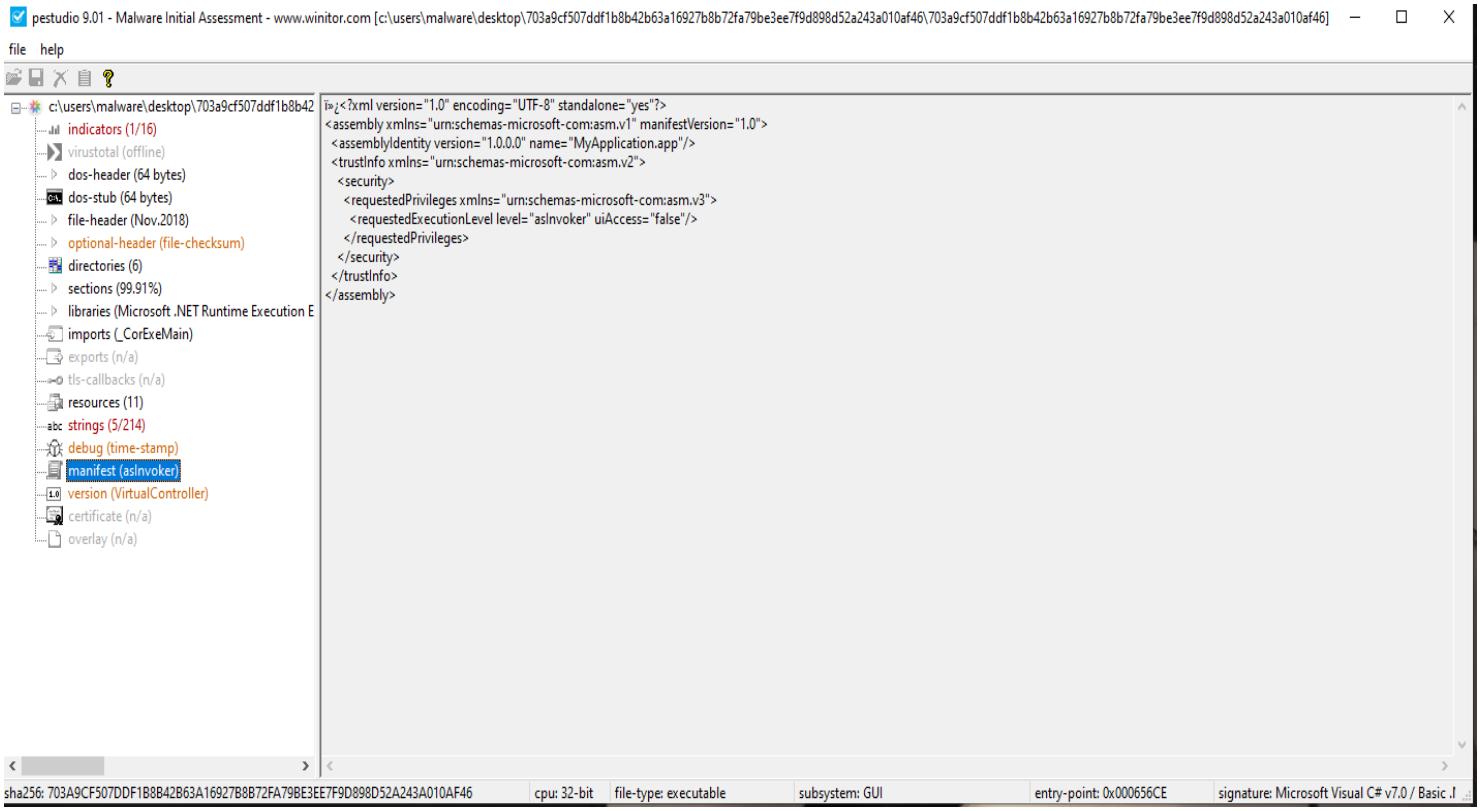

Fig 10. PE Studio Static Analysis of malware (Part 5)

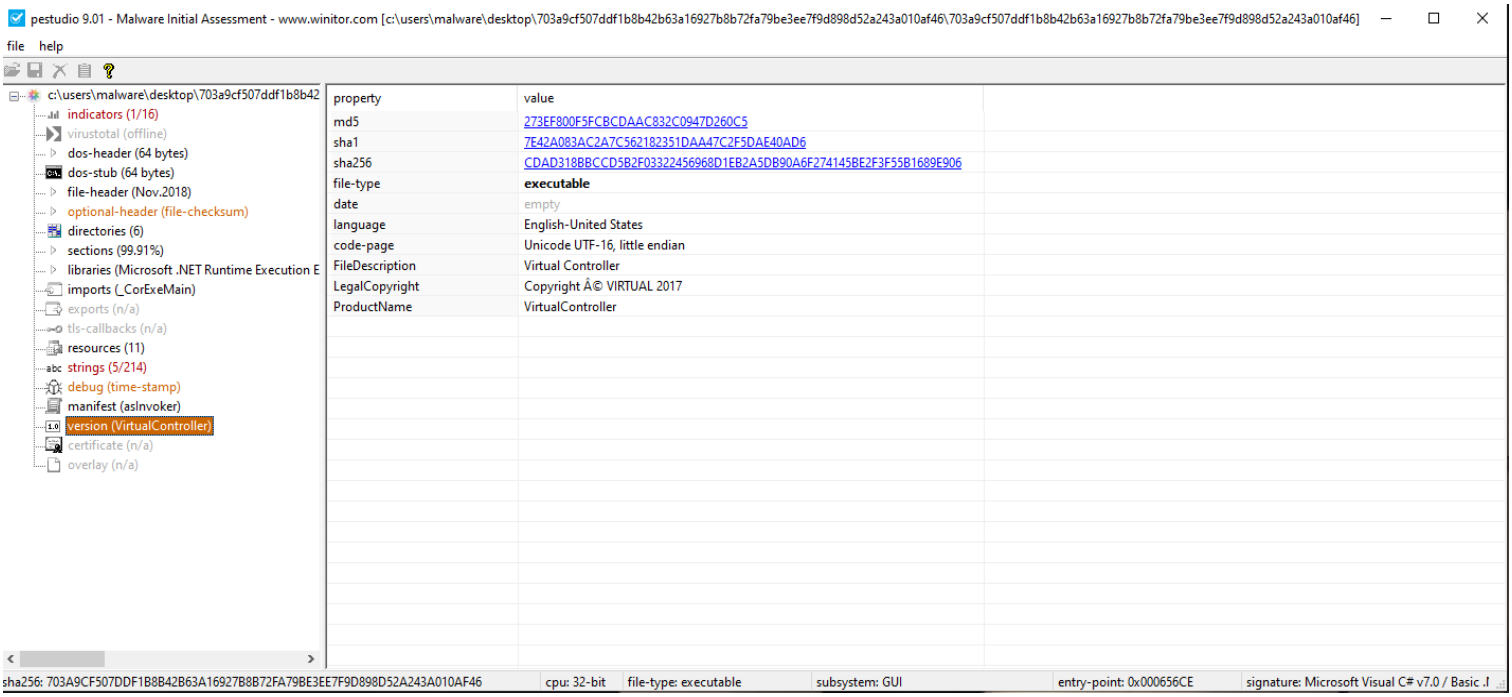

Fig 11. PE Studio Static Analysis of malware (Part 6)

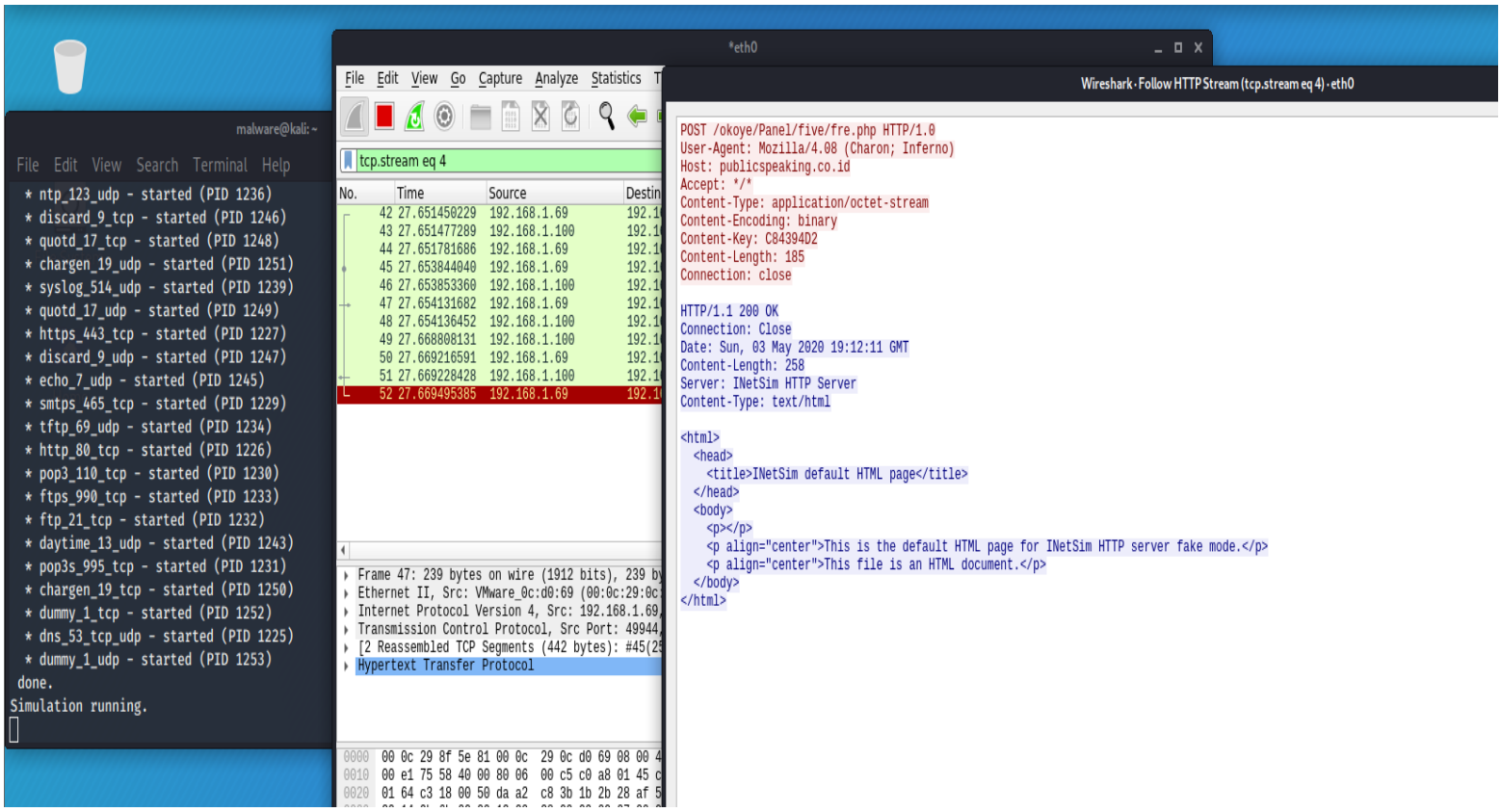

Fig 12. Wireshark and INetSim used together to gain C2 server related information

8:42:2...	vbc.exe	2216	WriteFile	C:\Users\malware\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-676032896-3894265858-437539164-1001\167817...	SUCCESS	Offset: 0, Length: 4...
8:42:2...	vbc.exe	2216	CloseFile	C:\Users\malware\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-676032896-3894265858-437539164-1001\167817...	SUCCESS	
8:42:2...	vbc.exe	2216	RegOpenKey	HKLM\Software\Policies\Microsoft\Cryptography	SUCCESS	Desired Access: R...
8:42:2...	vbc.exe	2216	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Cryptography\ForceKeyProtection	NAME NOT FOUND	Length: 16
8:42:2...	vbc.exe	2216	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Cryptography	SUCCESS	
8:42:2...	vbc.exe	2216	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider	SUCCESS	
8:42:2...	vbc.exe	2216	RegCreateKey	HKCU\https://publicspeaking.co.id/okoye/Panel/five/fre.php	SUCCESS	Desired Access: S...
8:42:2...	vbc.exe	2216	RegSetValue	HKCU\https://publicspeaking.co.id/okoye/Panel/five/fre.php\A0F460	SUCCESS	Type: REG_EXPA...
8:42:2...	vbc.exe	2216	RegCloseKey	HKCU\https://publicspeaking.co.id/okoye/Panel/five/fre.php	SUCCESS	
8:42:2...	vbc.exe	2216	CreateFile	C:\Users\malware\AppData\Roaming\A0F460\0A6BCE.exe	SUCCESS	Desired Access: W...
8:42:2...	vbc.exe	2216	SetBasicInform...	C:\Users\malware\AppData\Roaming\A0F460\0A6BCE.exe	SUCCESS	CreationTime: 1/1/...
8:42:2...	vbc.exe	2216	CloseFile	C:\Users\malware\AppData\Roaming\A0F460\0A6BCE.exe	SUCCESS	
8:42:2...	vbc.exe	2216	CreateFile	C:\Users\malware\AppData\Roaming\A0F460	SUCCESS	Desired Access: W...
8:42:2...	vbc.exe	2216	SetBasicInform...	C:\Users\malware\AppData\Roaming\A0F460	SUCCESS	CreationTime: 1/1/...
8:42:2...	vbc.exe	2216	CloseFile	C:\Users\malware\AppData\Roaming\A0F460	SUCCESS	
8:42:2...	vbc.exe	2216	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider Types\Type 001	SUCCESS	Desired Access: R...

Fig 13. Procmon logs showing dropping of malicious binary and creation of registry key

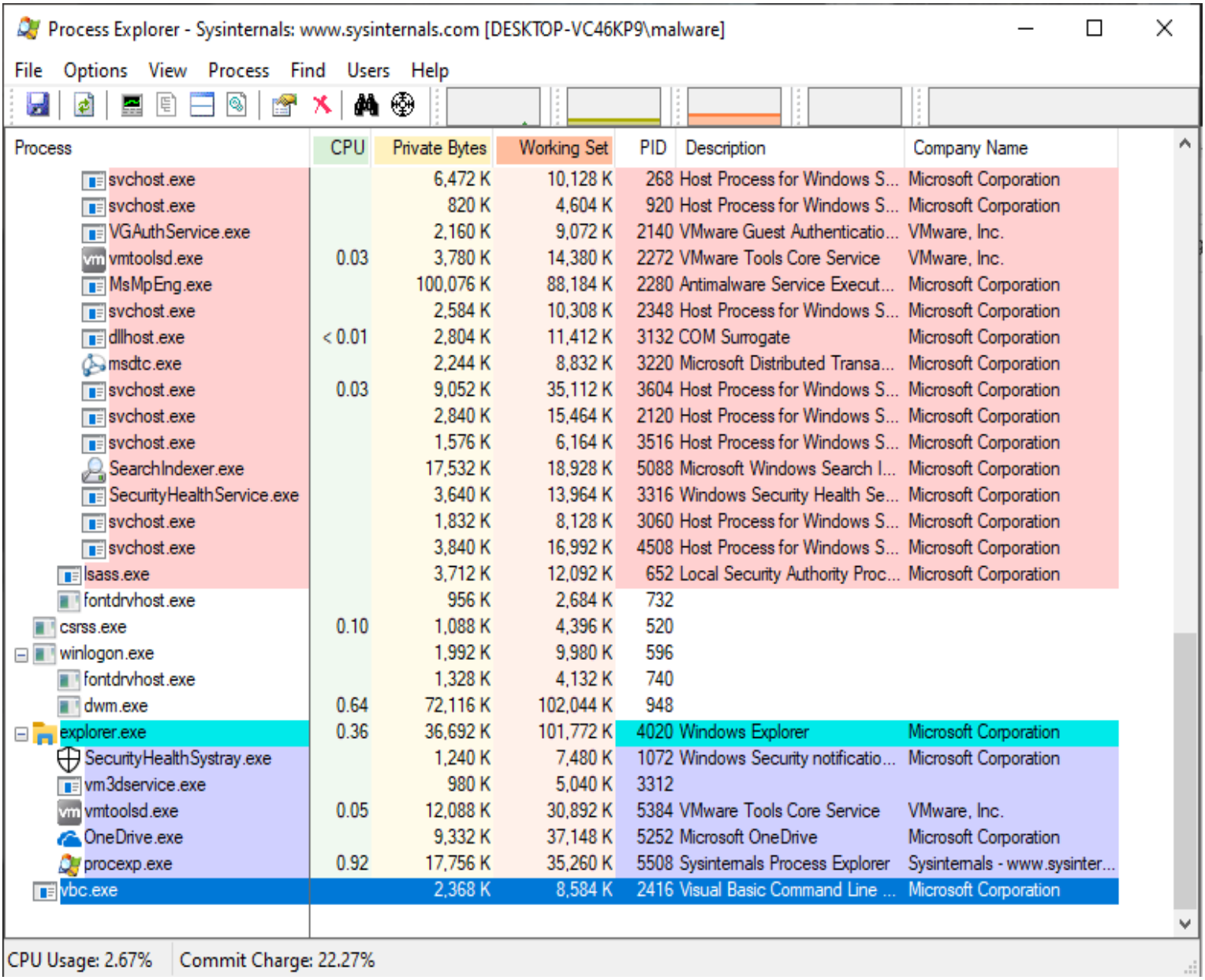

Fig 14. vbc.exe abruptly launched on execution of malware

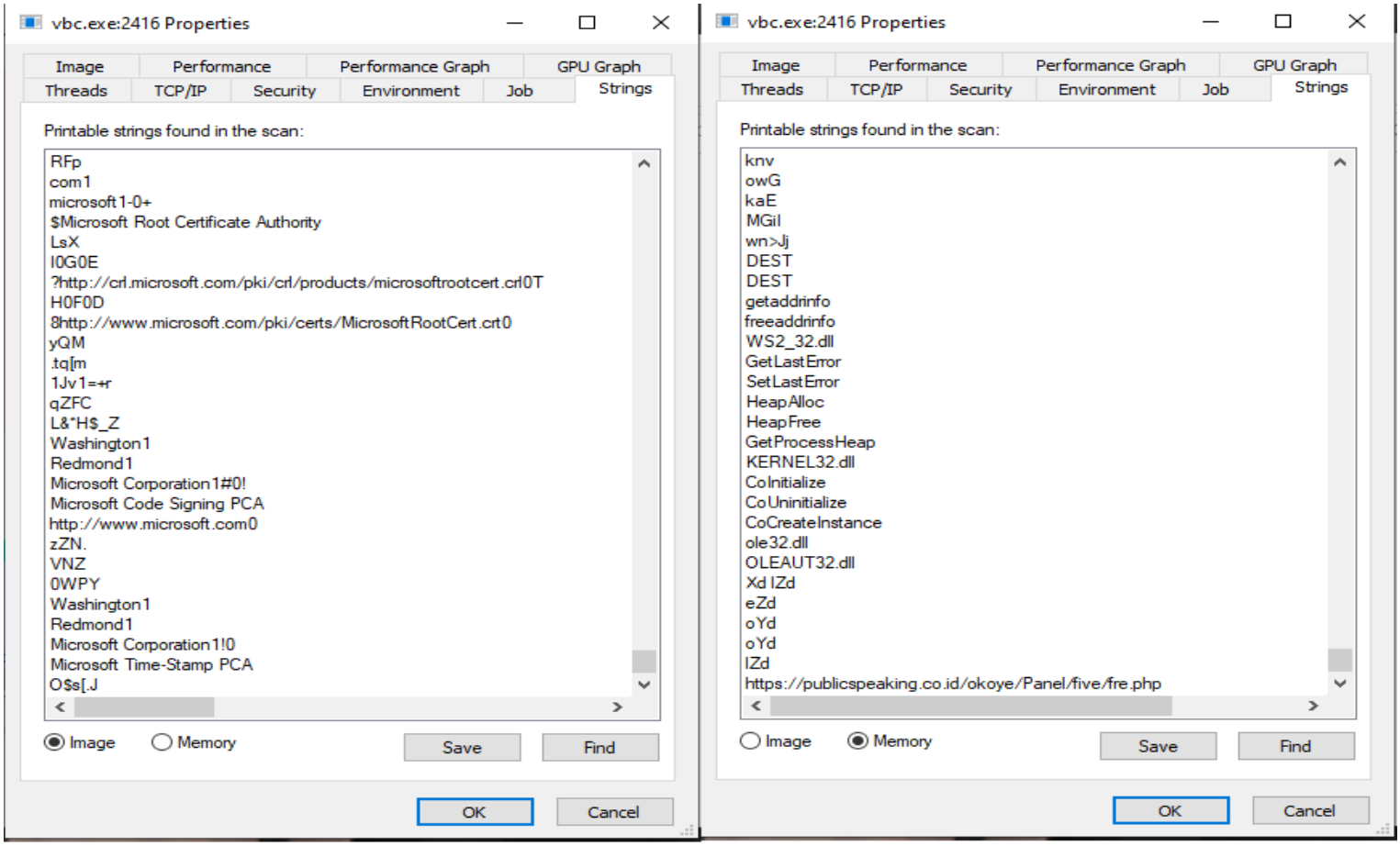

Fig 15. vbc.exe string differing drastically in memory and in image file on disk (Also memory string showing C2 server URL)

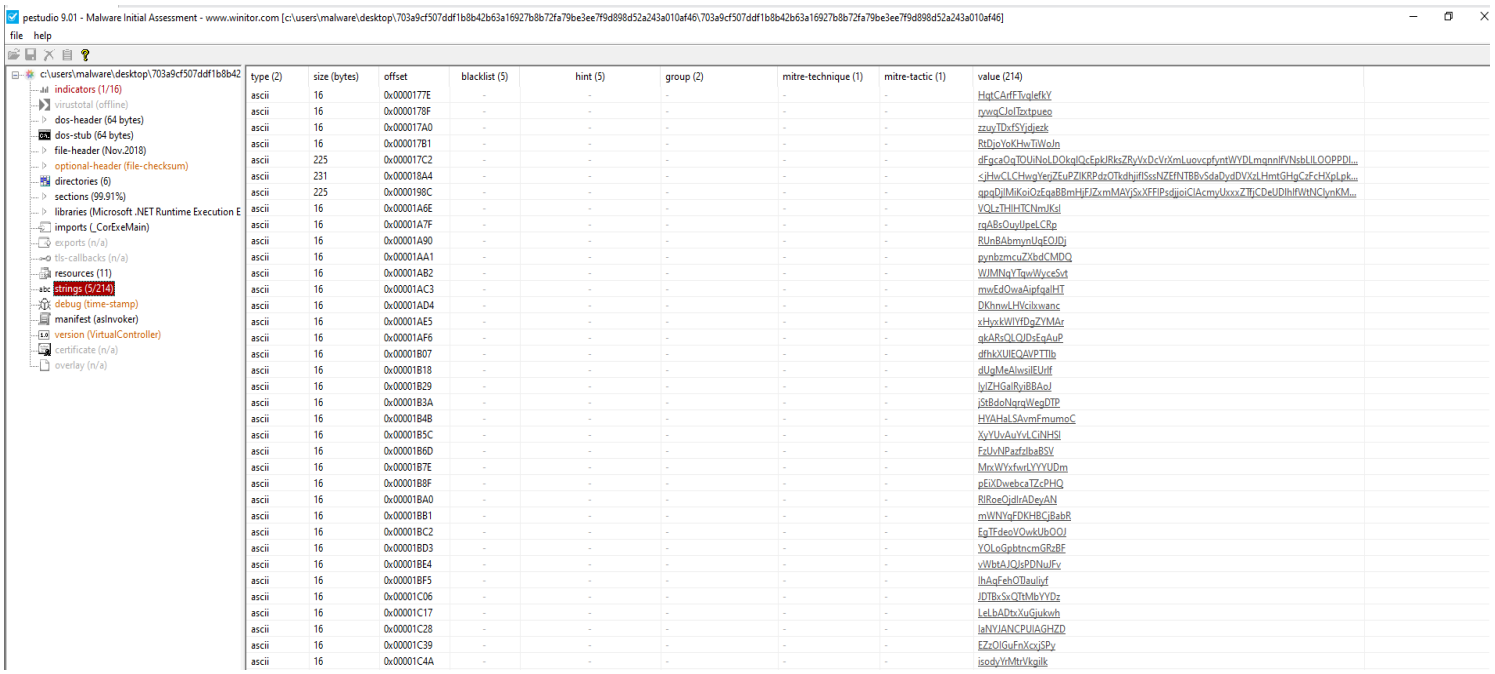

Fig 16. Obfuscated function names leading to difficult Advanced Static Analysis

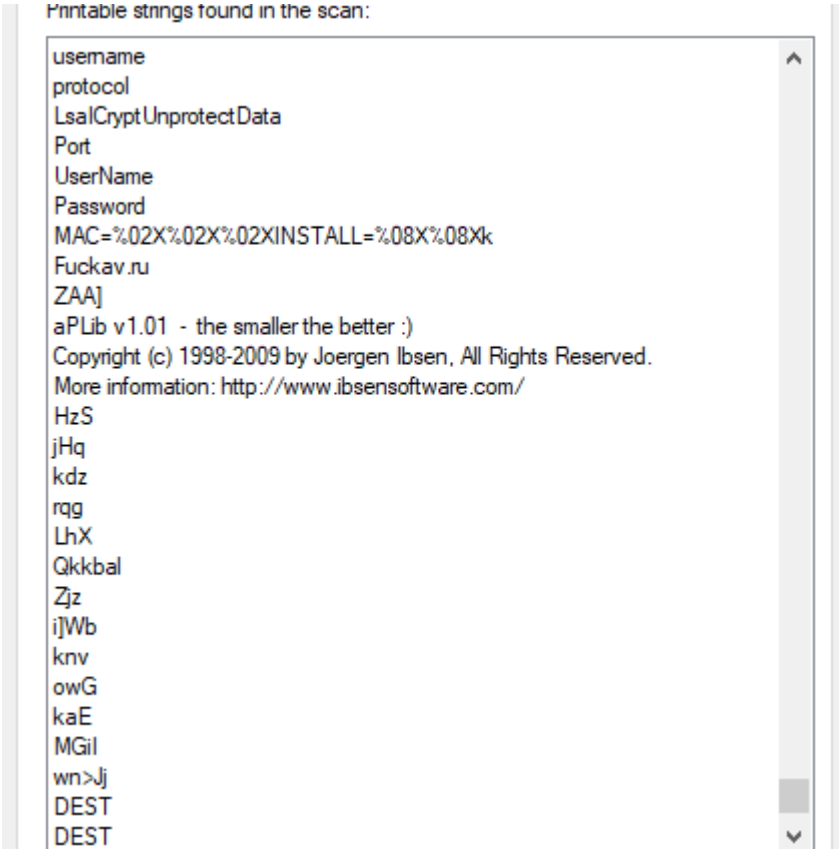

Fig 17. Another potential domain name (Fuckav.ru) linked to C2 server

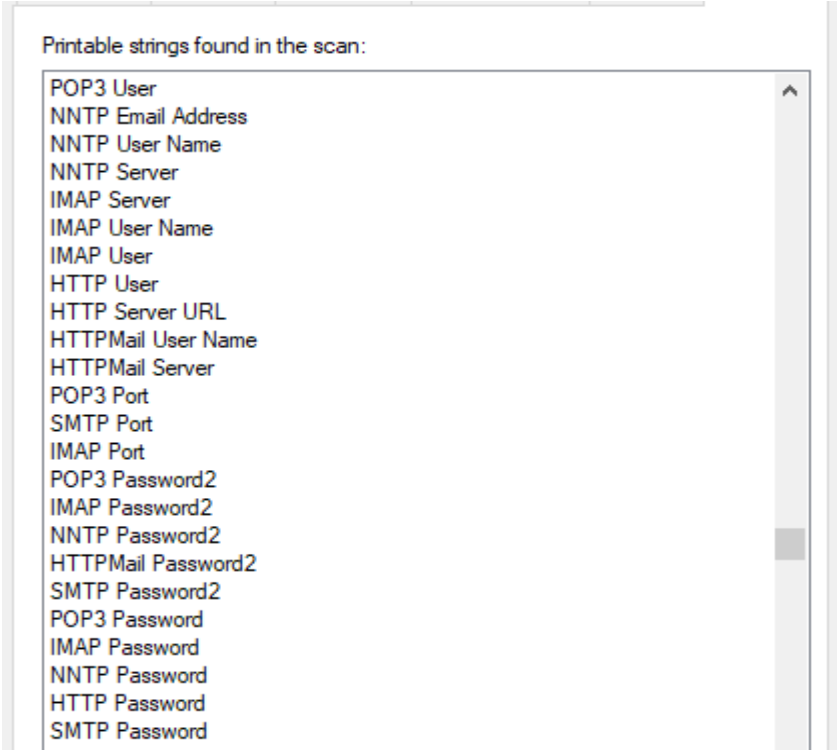

Fig 18. Credential Harvesting Variables

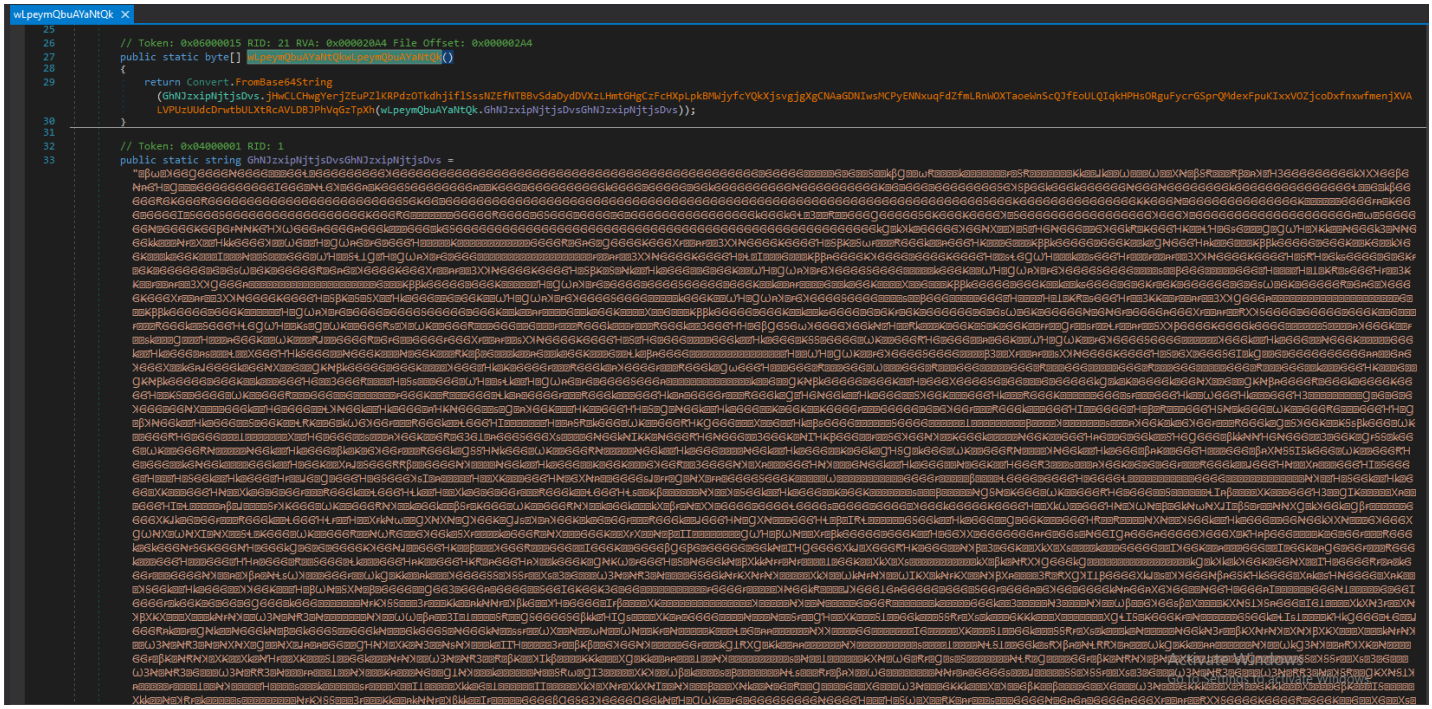

Fig 19. Manual Unpacking – Encrypted and Base64 Encoded

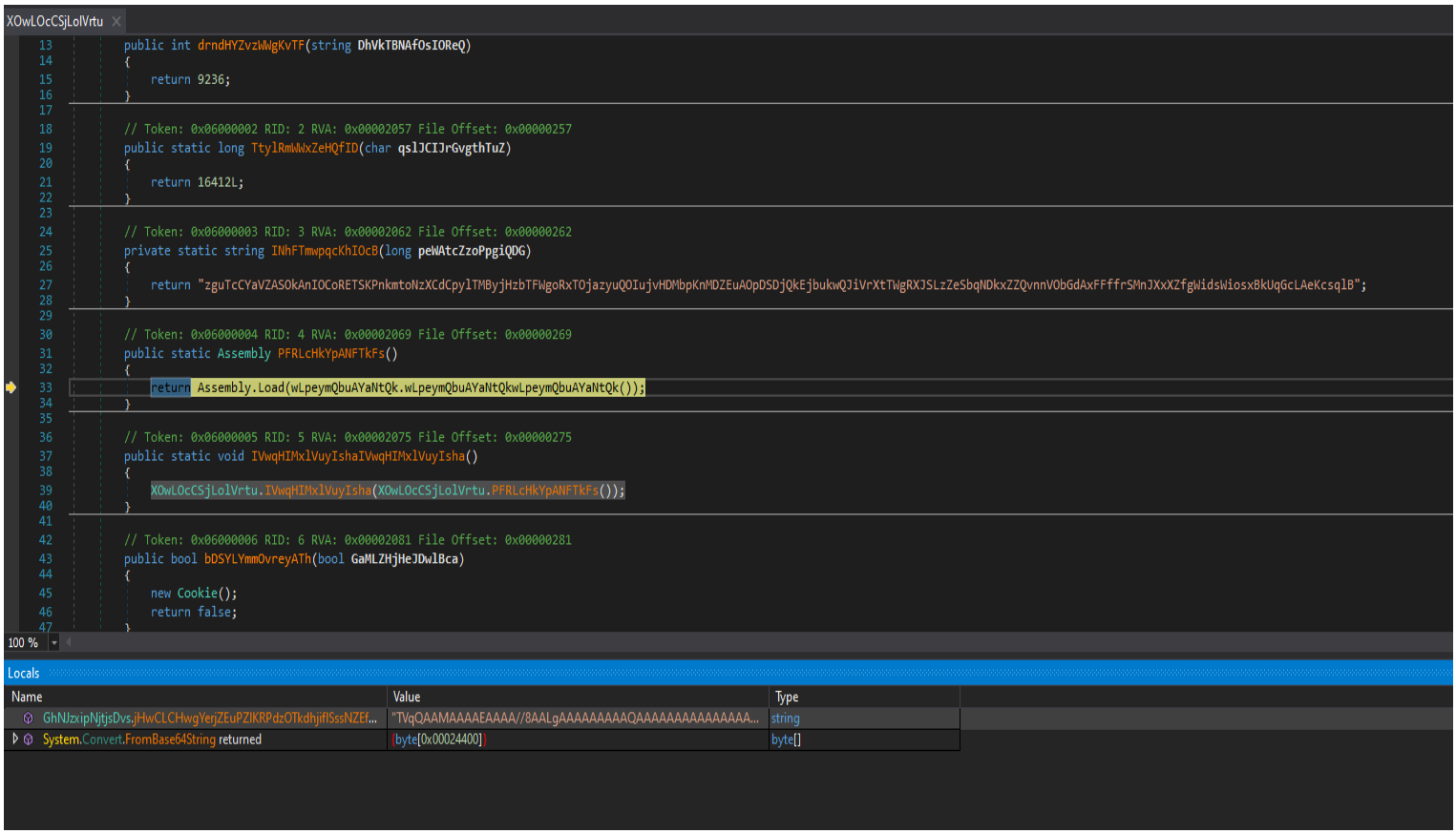

Fig 20. Loading of decoded and deciphered executable file data

Fig 21. PE File decoded from the string

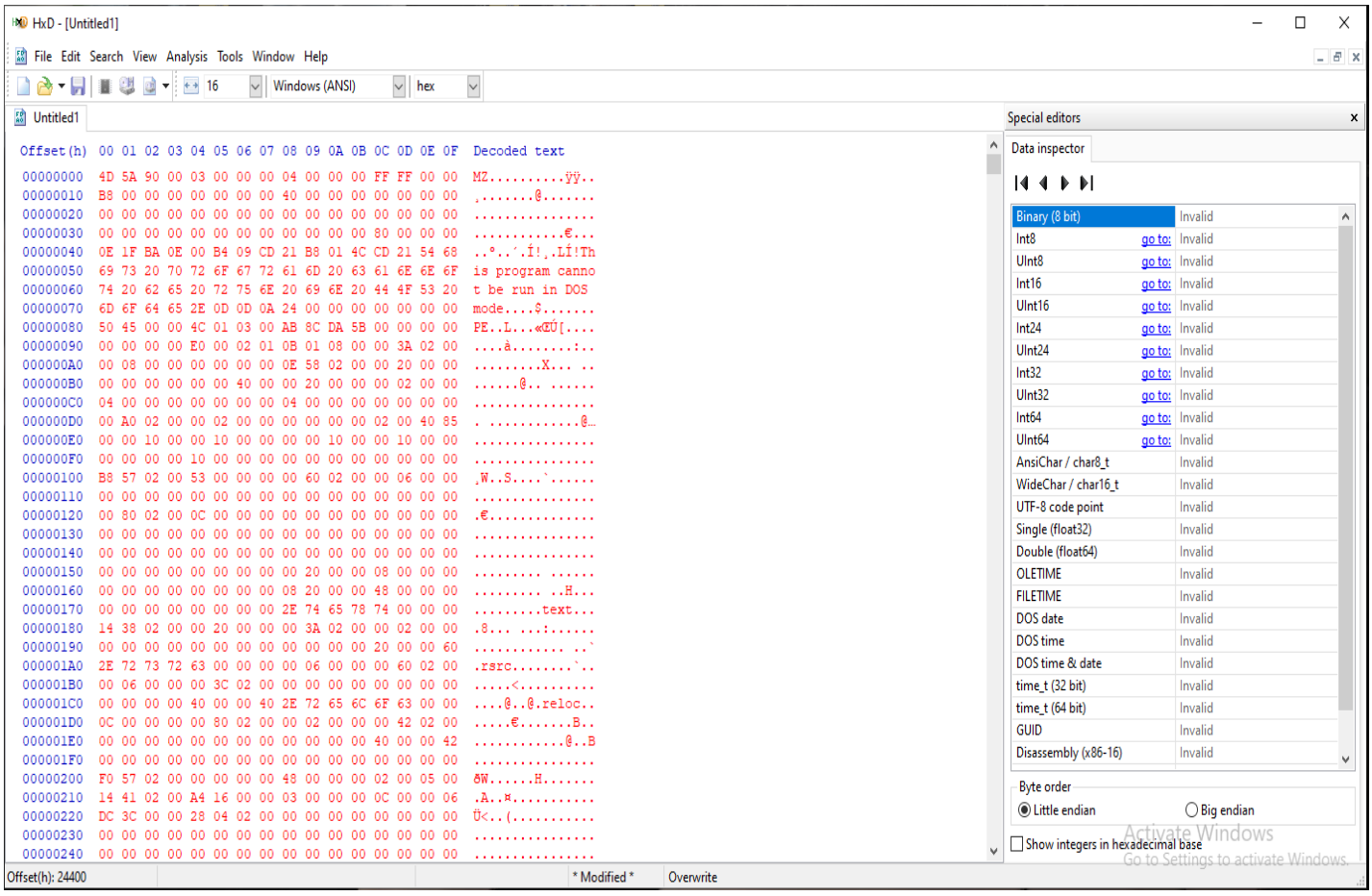

Fig 22. Manually reconstructing the PE file using HxD Hex Editor

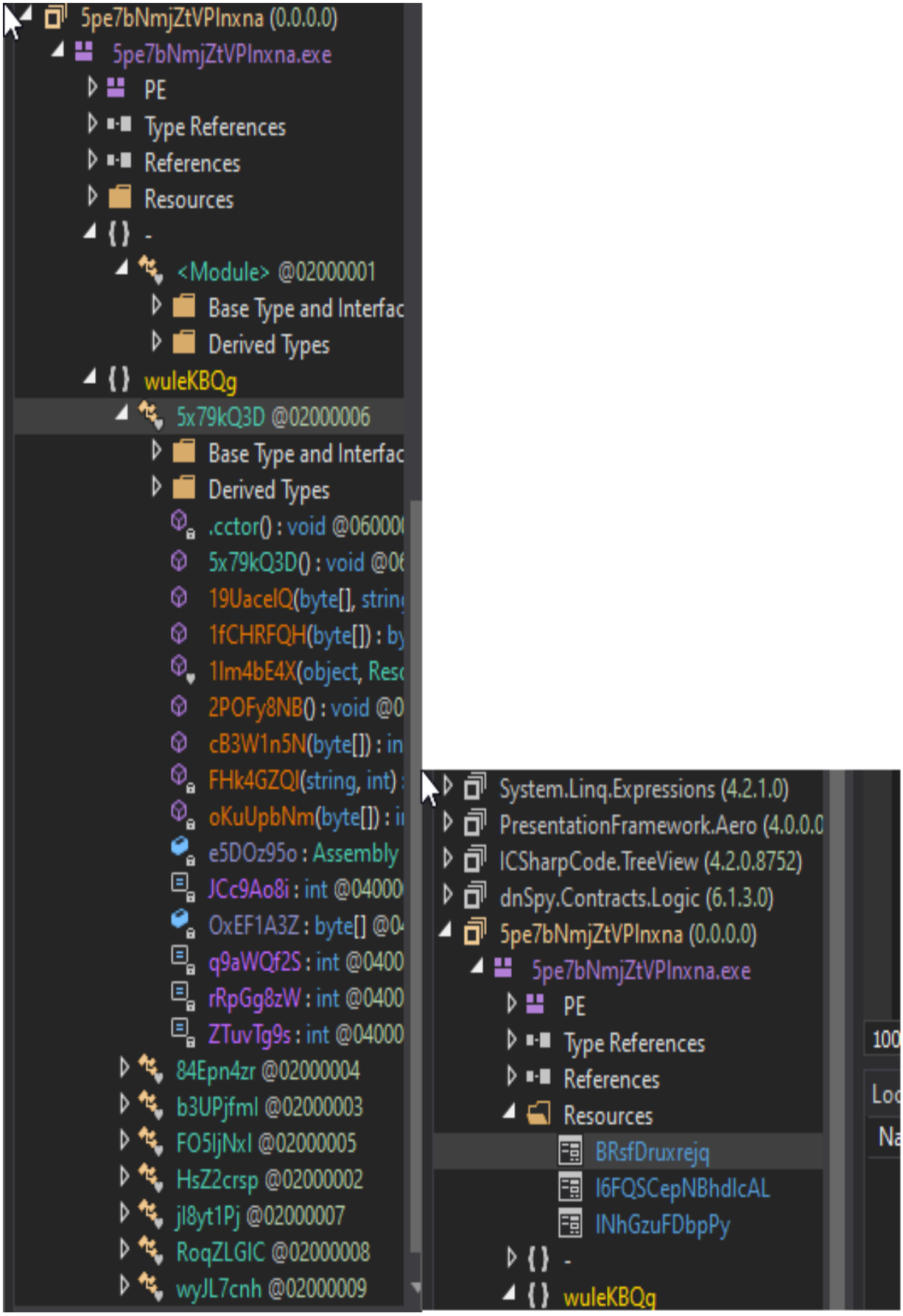

Fig 23. Further obfuscation being present in reconstructed PE file

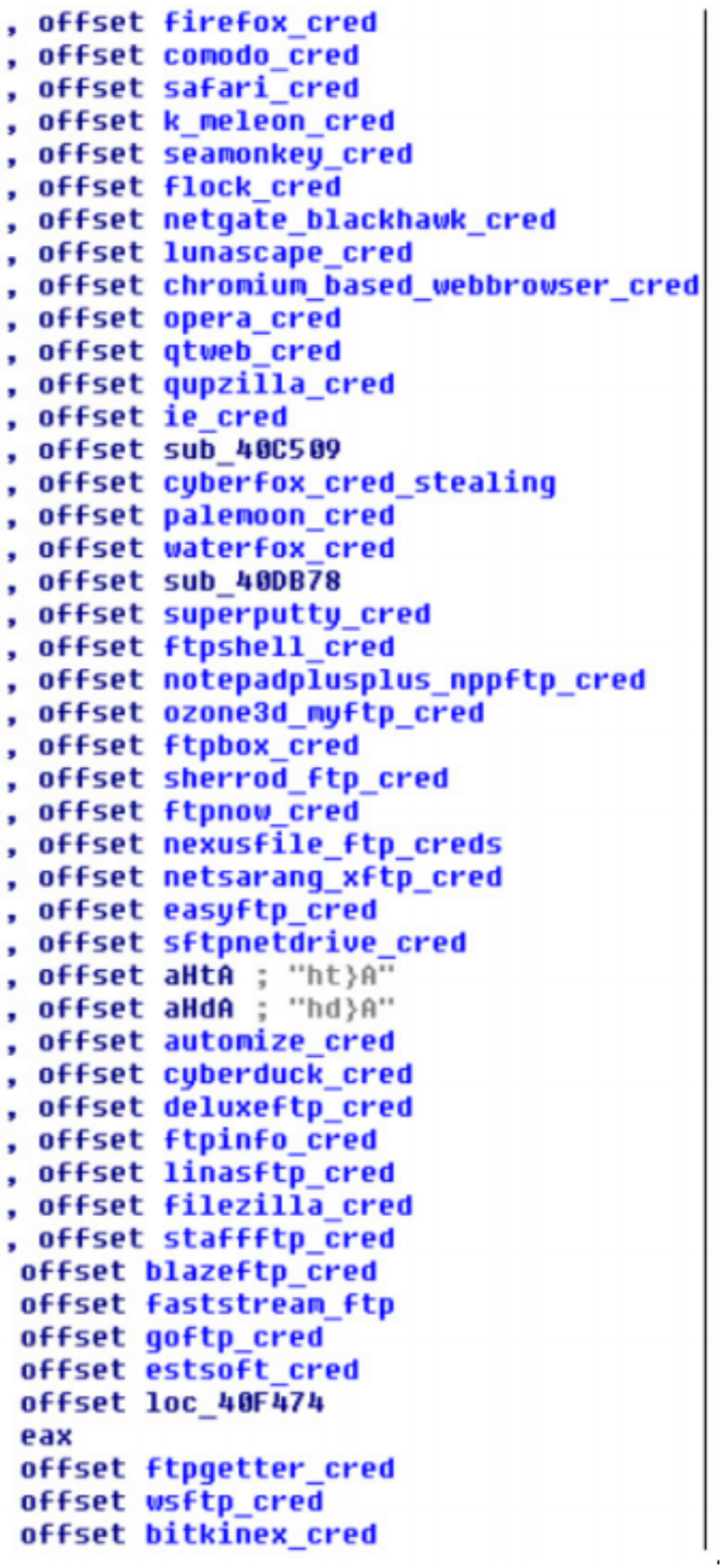

Fig 24. Report detailing credential harvesting variables.