TECHNIUM
SOCIAL SCIENCES JOURNAL

Vol. 30, 2022

A new decade for social changes

ISSN 2668-7798

www.techniumscience.com

Technium Social Sciences Journal
Vol. 30, 775-785, April, 2022
ISSN: 2668-7798
www.techniumscience.com

Trojan malware analysis using reverse engineering method in Windows 7

Ade Riyana, Banu Santoso, Rudi Hartono

Computer Engineering, Universitas Amikom Yogyakarta, Indonesia, Educational Technology, Universitas Ibn Khaldun Bogor, Indonesia

ade.riyana@students.amikom.ac.id

Abstract. Incidence response of malware attack or malware attack. Security attacks have now undergone many developments, which were originally individuals (hackers) now becoming more widespread (cyberwars). It is possible for someone to be attacked by malware on the computer system used. Malware can attack through offline or online media such as sms, chat or spam (whatsapp, instagram, email, telegram). Many think that malware can be easily handled with just an antivirus. Malware has its own defense system and can hide itself from an antivirus or even infect it. Malware can be handled by knowing how to work when attacking a computer system. Malware analysis is carried out by implementing trojan and bot malware on laptops and computers using reverse engineering methods. The downloaded application turns out to be a trojan in disguise, to find out whether the application is indeed infected with malware, it is necessary to analyze it firstr. This research will analyze the Danabot application that is infected with trojan malware by reverse engineering method. To check the authenticity of malware, it is necessary to check for md5 and sha256 malware, which means that the downloaded Danabot application has been infected with trojan malware, not a corrupt or damaged application.

Keywords. Malware, DanaBot Trojan, Reverse Engineering, Static Analysis, Windows 7

I. Introduction

The development of computer and laptop technology is accelerating, the number of computer and laptop users continues to grow. In recent years, the development of indicators of the use of computers and laptops reached 78.18% followed by the development of internet users and population growth of 18.83%. A fairly rapid increase occurred in 2016 to 2020 by 53.73% (AGENCY, 2021).

In the use of computers and laptops needed software - software, applications, websites that help daily life. However, the increasing number of applications and websites that can be profitable and useful for users, it opens up computer security gaps and causes malware attacks.

Technium Social Sciences Journal
Vol. 30, 775-785, April, 2022
ISSN: 2668-7798
www.techniumscience.com

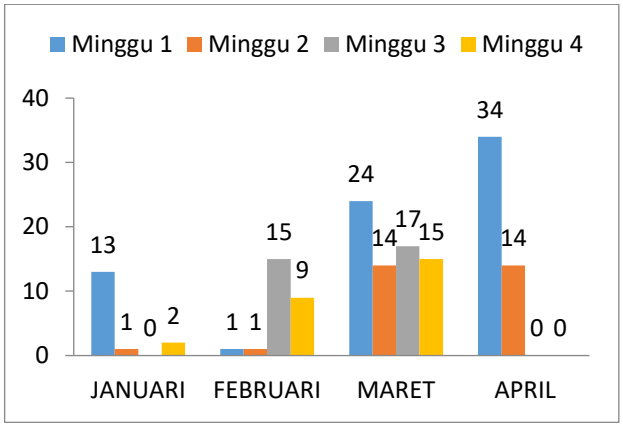


Table 1..1 CyberAttack January – April 2020 (BSSN, 2020).

Windows 7 focuses more on improving the basics of Windows, to better fit the applications in Windows 7 (Suharyanto, 2016) In 2008 Windows 7 focused on multi-touch screens, network systems, improved performance of Windows 7 and taskbar design. Basic applications that existed in windows before were not put back into windows 7, such as windows calendar, windows photo, and windows movie (Suharyanto, 2016). Microsoft offers users a separate free suit program so that windows users can connect with each other (microsoft.com, 2011).

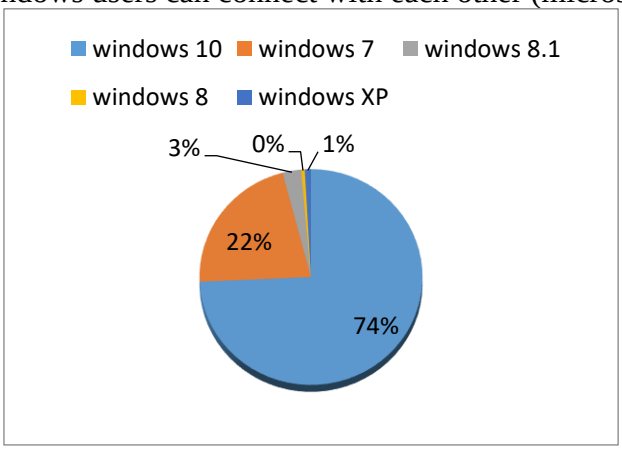


Figure 1.1 Windows Users In The Year 2021 (tekno.kompas.com, 2021)**.**

Malicious software analysis using reverse engineering methods to remodel files and research to trace unknown or hidden data. Data can be a buffer over the protection system or something else. Reverse engineering in malware analysis (malicious software) serves to extract data that includes existing information contained in malware (malicious software).

Table 1.2 Research Conducted

Researcher/year	Lokai	Method	Result
Raditya Faisal Waialua, Teguh Hidayat Iskandar	Windows XP	Reverse Engineering	WEBC2-DIV malware is a good malicious software when phishing email, credentials (phishing login), insert backdoors, remotely.

Nature. (2018) (Raditya Faisal Waliulua*, 2018).			
Aldy Putra Aldya, Nur Widya Sono, Tesa Pajar Setia. (2019) (Aldy Putra Aldya*, 2019).	Windows	Reverse Engineering	In running reverse engineering, you should analyze the string first, to find out the process of the malware and do the disassembly to find out the part in the malware.
Aaron Zimba, Luckson Simukonda & Mumbai Chishimba (2017) (Aaron Zimba*, 2017).	Linux (As a Server) & Windows (Malware Sample Testing)	Reverse Engineering	Ransomware uses the same encryption and attack methodology. However, unlike other ransomware, it produces sub-RSA key pairs that are used to encrypt the resulting symmetric keys. What made WannaCry spread rapidly and captured the world's attention was the inclusion of a worm component that allowed it to spread on its own on networks with vulnerable services.
Bram C.M. Cappers, Paulus N. Meessen, Sandro Etalle & Jarke J. van Wijk (2018) (Bram C.M. Cappers*, 2018).	Windows Virtual Machine	Reverse Engineering	In this paper demonstrate visualization tools to support rapid and cost-effective analysis of network traffic and malware, as well as the effectiveness of real-world ransomware systems. The tools created demonstrate how visualization can be used to quickly gain insights into malware and network activity by combining data reduction and automated techniques in a single interface using rules, aggregations, and options.
Michał Kędziora, Paulina Gawin, Michał Szczepanik & Ireneusz Jóźwiak (2019) (Michal Kedziora*, 2019).	Linux	Reverse Engineering	Android malware analysis is presented, in a unique set of features selected then used in the study of malware classification. Five classification algorithms (Random Forest, SVM, K-NN, Naive Bayes, Regression Logistics) and three attribute selection algorithms were checked to select which would provide the most effective malware detection. This analysis is done for features extracted from Java code. Specified which feature sources provide higher quality classification.

Technium Social Sciences Journal
Vol. 30, 775-785, April, 2022
ISSN: 2668-7798
www.techniumscience.com

This Research(2022)	Windows 7	Reverse Engineering	Detecting danabot malware samples can use total virus tools. Malware discovered during the 58/69 analysis. Not only malware is detected but also a lot of detailed information in total viruses such as md5, SHA 256, file types up to malware size.

II. Research methodology

Reverse engineering is a method of disassembling and knowing how applications or files are then changed and researched. Plans about reverse engineering have been around since the latest technology or computers were created. Reverse engineering is often used to identify information, designs and ideas that have been made before but have little information available (Heru Ari Nugroho*, 2015).

DanaBot is a banking trojan that first targeted users in Australia via emails containing malicious URLs. The criminals then developed a second variant and targeted the US company - part of a series of large-scale campaigns. The third variant appeared in February 2019 which was significantly improved. In general, DanaBot multi-stage infections begin with tiered hacks. Including stealing networks, attacking applications, stealing sensitive information data and many others (threatpost, 2021).

2.1 Malware (malicious software)

Malware (malicious software) software that is created to disguise into the computer system without prior consent. Malware (malicious software) is designed for malicious purposes or specific purposes of programmers. Malware (malicious software) itself consists of various types.

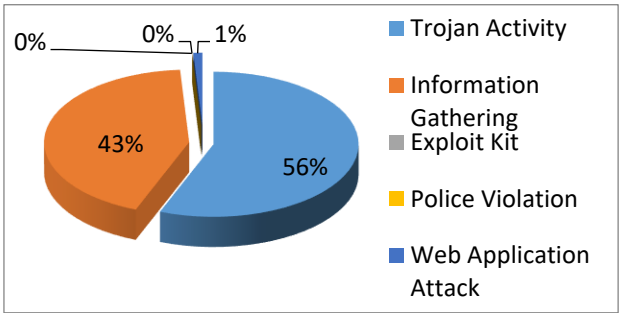


Figure 2.1 Classification of Attacks January to April (BSSN, 2020)**.**

Based on data throughout 2020, BSSN detected a technical cyber attack doubled compared to 2019. Traffic anomalies during 2020 reached 495,337,202. In order to improve the qualifications and readiness of cyber event control in the Information Infrastructure sector in a sustainable manner, the National Cyber and Password Agency of the Republic of Indonesia held the agenda of The 2021 Critical Information Infrastructure Cyber Exercise for the energy and mineral resources sector (BSSN, 2020).

Technium Social Sciences Journal
Vol. 30, 775-785, April, 2022
ISSN: 2668-7798
www.techniumscience.com

2.2 Malware analysis

Malware analysis is to disassemble malware to find out how it works, identification and how to keep malware from attacking again (Mylonas, 2012). Malware analysis can also be defined methods of determining the functionality of malware to provide a solution of a malware attack (ASLAN, 2017).

When analyzing malware, the malware sample used is an executable file format, which is difficult for humans to read. Therefore, several methods are used to extract files in order to get information from malware. Static analysis methods and dynamic analysis, both methods are categorized as basic (Alghamdi, et al., 2015).

A. Static Analysis

Programs suspected of being malware will be tested by scanning using antivirus, then hashing and detection packaged in the program. To detect the program used so that we can disassemble the malware file (S Megira*, 2018).

B. Dynamic Analysis

The basic method in dynamic analysis, which is observing the work of a system or the behavior of malware, virtual machines are used. So, if the executed malware damages the system then the main system is not damaged by the running malware.

C. Hybrid Analysis

Combines two pieces of information about static analysis malware and dynamic analysis. Other malicious forms of code become new types to achieve stronger attack functionality. Some other categories of commonly encountered malware can also be a nuisance for computer users, such as Spyware and the like. (YE, et al., 2017).

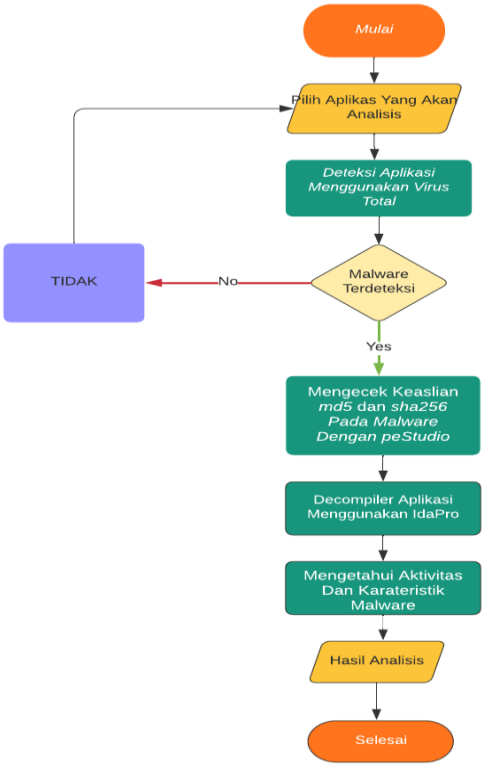


Figure 2.2 Research Flowchart

Technium Social Sciences Journal
Vol. 30, 775-785, April, 2022
ISSN: 2668-7798
www.techniumscience.com

2.5 Tools and Materials

The tools and materials used in the study were divided into 2 hardware, devices that can be seen and touched physically directly and device software that can only be seen but cannot be touched physically directly as follows:

Table 2.1 Hardware Specifications

Operation System	Windows 7 Ultimate 64-bit
system manufacturer	Dell Inc
System Model	Inspiron 1464
Processor	Intel(R) Core (TM) i3 CPU M330 @ 2.136GHz(4CPUs), ~2.1GHz
RAM	2048MB RAM

Table 2.2 Classification of Software Analysis

Tools Reverse Engineering	Virus Total
	PEstudio
	IdaPro

III DISCUSSION

In order for the analysis to run smoothly the process must be done sequentially and in a well-ordered manner. Installation of tools and equipment used make sure it is checked properly and can be used properly.

3.1 Application Detection Using VirusTotal

VirusTotal is a subsidiary of Google. The tool is publicly available online, allowing users to upload, scan files, scan URLs and ip addresses. VTZilla is a Firefox extension that allows scanning of files and URLs. Uploading virusTotal windows allows scanning files in windows (Prerna Agrawal*, 2019). To detect applications suspected of being trojan malware. Researchers use VirusTotal tools, such as the following:

Technium Social Sciences Journal
Vol. 30, 775-785, April, 2022
ISSN: 2668-7798
www.techniumscience.com

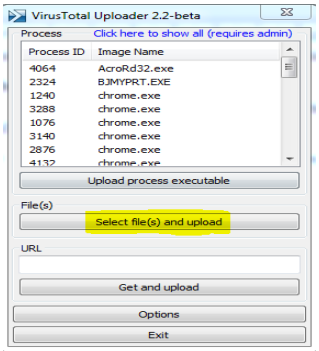


Figure 3.1 Upload App.

It can be seen in figure 3.1 is the process of selecting applications suspected of being malware by means of, click the select file(s) and upload the application suspected of trojan malware and wait until the malware detection process is completed and the results of analysis from the application appear.

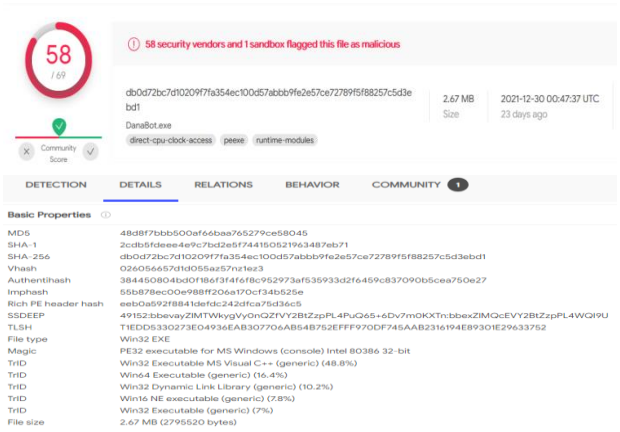


Figure 3.2 Detection Results And Details of Application Analysis Using VirusTotal

It can be seen in Figure 3.2 that the DanaBot application has been correctly detected as a trojan malware with a ratio of 58/69 which means VirusTotal as of December 30, 2021 by getting 58 malicious malware from 69 detected malware. With MD5 *48d8f7bb b500af6baa765279ce58045* and SHA 256 db0d72bc7d10209f7fa354ec100d57abbb9fe2e57 ce72789 f5f88257c5d3ebd1.

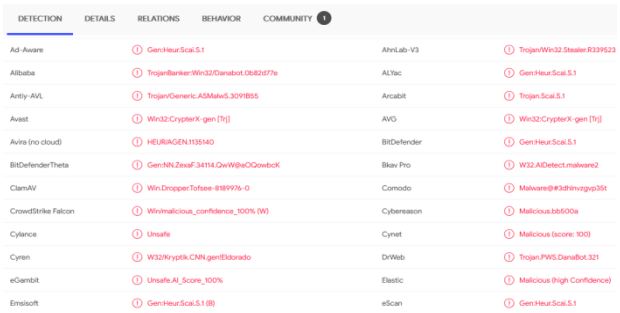


Figure 3.3 Detection DanaBot App

In figure 3.3 can be seen the results of scanning Trojan malware using virustotal. There is also antivirus software in the danabot application that is detected as a Trojan virus.

Technium Social Sciences Journal
Vol. 30, 775-785, April, 2022
ISSN: 2668-7798
www.techniumscience.com

3.2 Malware analysis using Pestudio

PEstudio is one of the static analysis tools that aims to see libraries imported by malware (Leidy Kurnia Hatika*, Agustus 2019). PEstudio can also check the authenticity of md5 and sha256 on malware, the purpose of checking authenticity to prove the integrity of the downloaded files in good and not lost partially (corrupt).

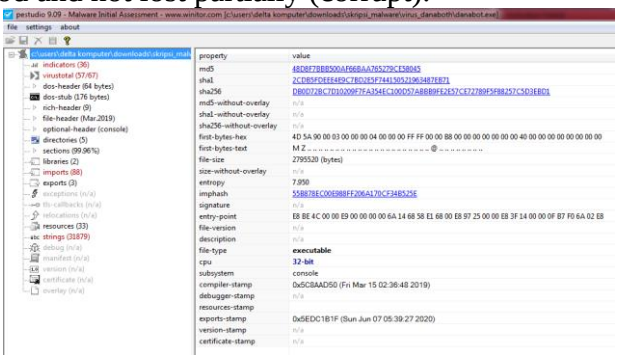


Figure 3.4 Authenticity of md5 And sha256

From figure 3.4 it can be concluded that the DanaBot application has the results of checksum md5 "48D8F7BBB500AF66 BAA765279CE58045", sha1 "2CDB5FDEEE4E9C7BD2E5F7 44150521963487EB7", sha256 "DB0D72BC7D 10209F7FA354EC100D57ABBB9F E2E57CE72789F5F88257C5D3EBD1" and file-size 2795520 bytes.

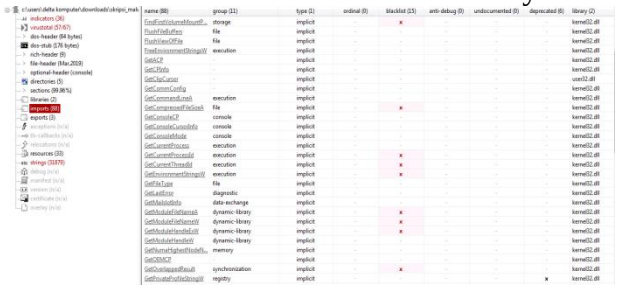


Figure 3.5 Import Malware

In figure 3.5 Import contains other important information such as groups that have been blacklisted by pestudio for having malware or malicious intent contained in the malware, although the category of kernel32 libraries is not dangerous, but keep in mind that malware has the ability to change and delete files without prior consent.

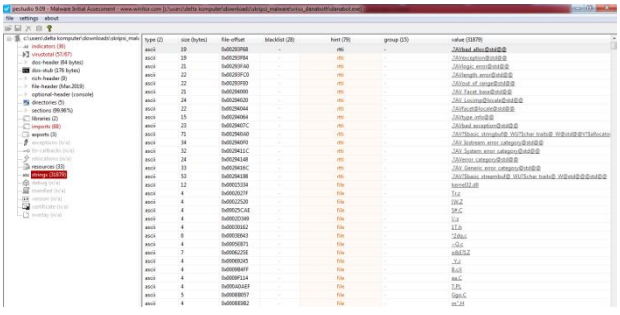


Figure 3.6 Malware String

In Figure 3.6 of the string, the type code used in malware is ascii, size (bytes) to see the size of the ascii code and hints or malware instructions in the form of files.

Technium Social Sciences Journal
Vol. 30, 775-785, April, 2022
ISSN: 2668-7798
www.techniumscience.com

3.3 Application Decompiler Using IDA PRO

IDA Pro is a disassembler that produces assembly languages from binary executables. It supports a variety of different operating systems (Microsoft Windows OS, Mac OS, and Linux OS) and executable file formats such as PE, common object file formats, and links (ASLAN, 2017). It can also be interpreted as decompiler or decompile is the process of dismantling applications that aim to get source code that can be read and understood, while decompiler is a tool used in the decompile process.

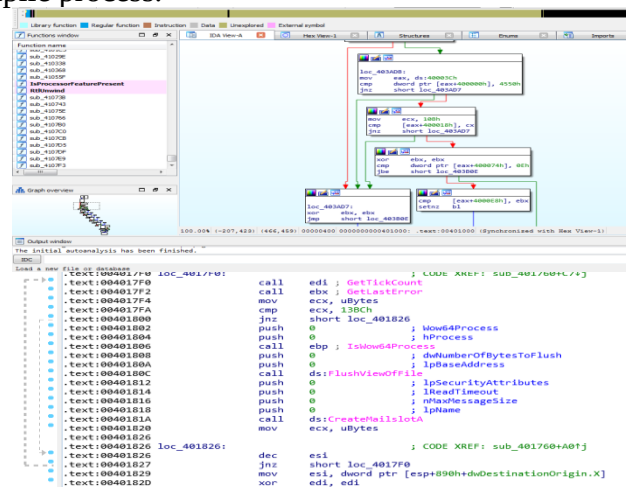


Figure 3.7 IDA View

In the research in figure 3.7 can be seen how malware works and can find out what commands are in the malware and the way of the command will be redirected to any part.

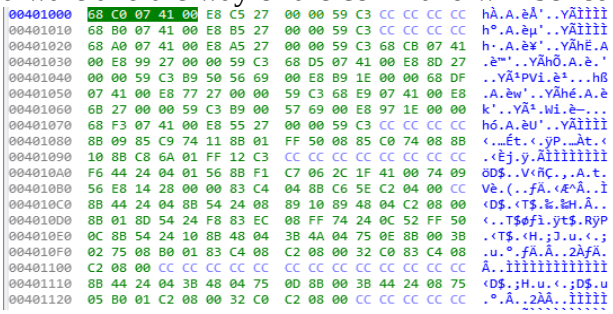
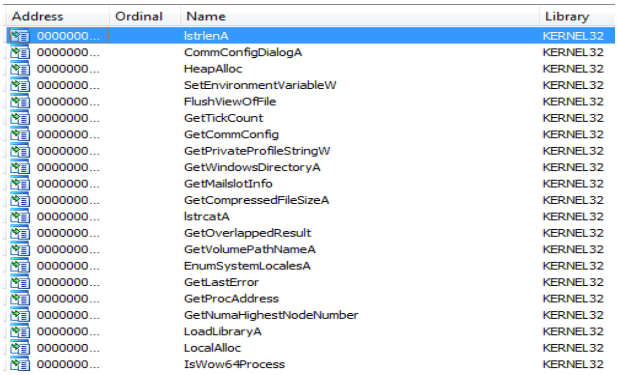


Figure 3.8 Hex View And Ascii code

In figure 3.8 Hex view or hex code is used to manipulate binary on a file on a computer, It is very important to understand the workflow of the program. In contrast to hex code ascii code helps us read what is hidden by hex code.

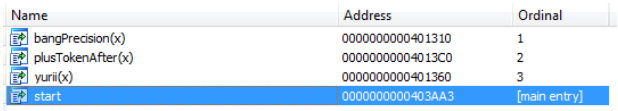
Technium Social Sciences Journal
Vol. 30, 775-785, April, 2022
ISSN: 2668-7798
www.techniumscience.com



Address	Ordinal	Name	Library
0000000...		lstrlenA	KERNEL32
0000000...		CommConfigDialogA	KERNEL32
0000000...		HeapAlloc	KERNEL32
0000000...		SetEnvironmentVariableW	KERNEL32
0000000...		FlushViewOfFile	KERNEL32
0000000...		GetTickCount	KERNEL32
0000000...		GetCommConfig	KERNEL32
0000000...		GetPrivateProfileStringW	KERNEL32
0000000...		GetWindowsDirectoryA	KERNEL32
0000000...		GetMailslotInfo	KERNEL32
0000000...		GetCompressedFileSizeA	KERNEL32
0000000...		lstrcatA	KERNEL32
0000000...		GetOverlappedResult	KERNEL32
0000000...		GetVolumePathNameA	KERNEL32
0000000...		EnumSystemLocalesA	KERNEL32
0000000...		GetLastError	KERNEL32
0000000...		GetProcAddress	KERNEL32
0000000...		GetNumaHighestNodeNumber	KERNEL32
0000000...		LoadLibraryA	KERNEL32
0000000...		LocalAlloc	KERNEL32
0000000...		IsWow64Process	KERNEL32

Figure 3.9 Import

Just like import in figure 3.5 malware analysis using pestudio. The import file on idapro also describes its address, name and library, the difference in figure 3.5 does not describe the blacklisted group.



Name	Address	Ordinal
bangPrecision(x)	0000000000401310	1
plusTokenAfter(x)	00000000004013C0	2
yurii(x)	0000000000401360	3
start	0000000000403AA3	[main entry]

Figure 3.10 Export

In the export menu in figure 3.10 there is a start command that serves to return to the initial menu, but does not affect the running malware decompiler.

IV Conclusion

Based on the results of research on the analysis of the danaBot Trojan malware, it can be concluded that. Detecting danabot malware samples can use the total malware virus tool found at the time of 58/69 analysis. Not only malware is detected but also a lot of detailed information in total viruses such as md5, SHA 256, file types up to malware size. Check the authenticity of md5 and SHA 256 on malware, to ensure that the malware analyzed in the form of apk is not in a damaged or corrupt state. Decompiler danabot application using ida pro. Obtained results of hex code, ascii code on malware. Researchers use static methods of analysis with pro ida tools.

References

[1] CENTRAL STATISTICS AGENCY, "Indonesian Telecommunication Statistics 2020," bps.go.id, vol. Catalog Number: 8305002, Publication Number: 06300.2113, October 2021.

[2] STATE CYBER AGENCY AND PASSWORD, "Cyber Attack Recap (January – April 2020)," https://bssn.go.id/rekap-serangan-siber-januari-april-2020/, April 2020.

[3] Cosmas Eko Suharyanto, "Putera Batam University, Batam 29434, Indonesia," Comparative Analysis of Windows 7 and Windows 8 Security Systems, vol. Vol.4, no. 2337-8379, pp. Number 1, March 2016.

[4] microsoft.com, "Windows Live Essentials 2011," Photos on Windows Live Windows Movie Maker, 2011.

[5] tekno.kompas.com, "A Year of "Retirement", Windows 7 Is Still Widely Used," Kompas.com Tekno Apps & OS, January 2021.

[6] Raditya Faisal Waliulua and Teguh Hidayat Iskandar Alamb, "Reverse Engineering Analysis Static Forensic Malware Webc2-Div," vol. Vol 4, No 1, 2018.

Technium Social Sciences Journal
Vol. 30, 775-785, April, 2022
ISSN: 2668-7798
www.techniumscience.com

[7] Nur Widiyasono,Tesa Pajar Setia Aldy Putra Aldya, "Reverse Engineering for remote access trojan malware analysis," 2019.
[8] Aaron Zimba, Luckson Simukonda, and Mumbi Chishimba, "Demystifying Ransomware Attacks Reverse Engineering and Dynamic Malware Analysis of WannaCry for Network and Information Security," vol. 1, no. 1, 2017.
[9] Bram C.M. Cappers, Paulus N. Meessen, Sandro Etalle, and Jarke J. van Wijk, "Eventpad: Rapid Malware Analysis and Reverse Engineering using visual Analytics.," 2018.
[10] Michal Kedziora, Paulina Gawin, Michal Szczepanik, and Ireneusz Jozwiak, "Malware Detection Using Machine Learning Algorithms And Reverse Engineering Of Android Java Code," vol. Vol. 11, No.1, 2019.
[11] Mujahidin, E., Hartono, R., Profesor, A., & Bogor, K. (2020). The Role of Leader Assessment in Developing Teacher Teams in the Industrial Revolution 4.0. International Journal of Innovation, Creativity and Change. Www. Ijicc. Net, 13(11), 2020.
[12] Nugroho and Prayudi, "The Use of Reverse Engineering Techniques in Malware Analysis For Malware Attack Identification.," KNSI STMIK Dipanegara Makasar, pp. 1-8., 2015.
[13] threatpost, "https://threatpost.com/danabot-malware-roars-back/163358/," 2021.
[14] BSSN. (2020, april) Classification of Attacks January through April. [Online]. https://bssn.go.id/rekap-serangan-siber-januari-april-2020/
[15] Alexis, Gritzalis, Dimitris Mylonas, "Computers & Security," Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, vol. 31, no. 6, September 2012.
[16] Omer ASLAN, "International Multidisciplinary Studies Congress (IMSC)," Performance Comparison of Static Malware Analysis Tools Versus Antivirus Scanners To Detect Malware, November 2017.
[17] Rubayyi Alghamdi, Khalid Alfalqi, and Mofareh Waqdan, "Android Platform Malware Analysis," vol. vol 6,no1, 2015.
[18] Hartono, R., & Mujahidin, E. (2021). Development of Virtual Reality-Based Learning Videos in Smk Negeri 2 Bengkulu Utara. Annals of the Romanian Society for Cell Biology, 25(6), 4765-4774.
[19] S Megira, A R Pangesti, and F W Wibowo, "Malware Analysis and Detection Using Reverse," 2018.
[20] YANFANG YE, TAO LI, DONALD ADJEROH, and S. SITHARAMA IYENGAR., "A Survey on Malware Detection Using Data Mining Techniques," vol. 50, no. 3, 2017.
[21] Prerna Agrawal and Bhushan Trivedi, "Analysis of Android Malware Scanning Tools," vol. Vol.-7, no. Issue-3, 2019.
[22] Leidy Kurnia Hatika, Avon Budiyono, and Ahmad Almaarif, "ACCURATE ANALYSIS OF MALWARE DETECTION IN ANTIVIRUS SOFTWARE," vol. 6, 2019.