Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 50-55 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Virus Detection In Windows 10 Using Nist Method And Smadav Application 13.4

Ahmad Fajar Sidiq[1], Anton Yudhana[2], Rusydi umar[3]

[1,2,3]Magister Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta

Email: fajarmaneh082@gmail.com

ARTICLE INFO

Article history:
Received: 12/02/2020
Revised: 09/03/2020
Accepted: 01/05/2020

Keywords:
Viruses, Nist, Smadav, Data.

ABSTRACT

This research has a background in virus detection on a computer, because a virus is something that can damage and damage data on a computer, because the impact is very bad for the computer so that many anti-virus viruses develop and continue to be developed each year, the development of the virus first against anti-virus causes the impact of damage that is getting worse, the most severe is data loss, data is very important for a computer, in this study the authors use a method created by the National Institute of Standards and Technology (NIST), with this method will facilitate research carried out, the results of the study will be in the form of detection carried out by the Smadav software version 13.4.

1. Introduction

A virus is a computer program that can copy itself and spread by inserting a copy of itself into a program or document, a computer virus can damage the computer user to make it feel disturbed or have no effect at all[6]. Ransomware is a dangerous type of virus that attacks by blocking access to data and displaying messages that make payments. Ransomware can only actually lock the system, so people who are knowledgeable in the IT field can easily reverse the situation by passing the block. because this Trojan Ransomware uses malicious code to interfere with the system before the user realizes it, can encrypt a person's important files and ask him to pay to the attacker so that the file is used again by the user to damage the user's entire Hard drive[5].

The problem raised in this study is by checking the data that comes in and out of a device, with the initial detection carried out it will reduce the attack that will be carried out by the ransom virus. With the development of many viruses in this study raised the method using Nest, using this Nest method will conduct research in accordance with a clear sequence and stages of research. In this study the authors raise the problem of ransom virus attacks and how to protect data from ransom virus attacks[1-4].

2. Research Methods

The more developed a technology, the greater the chance of cybercrime through malware attacks. Malicious software (malware) is a malicious software deliberately designed to run foreign content that harms or damages the victim's system without his knowledge. With many malware categories scattered, making all systems vulnerable to malware attacks. One of the most dangerous malware categories is the Remote Access Trojan (RAT) which can completely control the system to steal personal information, delete files, modify files, disrupt user performance, and install malware or backdoor in the system. 1. Dynamic Malwer analysis of RAT malware is done by executing a back door from the RAT server application in an isolated environment so that RAT malware does not infect other systems. 2. Malware RAT behavior when initiated using the API and accessing the Windows Registry are associated with RPC and making connections between infected systems and RAT server applications. Malware is software that

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 50-55 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

is made for a specific purpose by looking for system security gaps. The purpose of malware is created by an attacker to damage or break into an operating system through a secret script or can be said to be hidden by the attacker hidden. However, with the results of these studies we can find out how the ransomware activity patterns and detect and anticipate Ransomware attacks. Support vector machine is a technique for making predictions, both in particular classification and regression in dynamic and static analysis[7]. Classification is the process by which classifiers (users who classify) learn from sample data that has been labeled as data used for testing sample data. Support vector machine This research uses LIBSVM implementation with polynomial kernel functions to train SVM even though it still uses the technique used for binary classification.

In this study the authors use the NIST method in conducting research, NIST created by the National Institute of Standards and Technology (NIST) with the NIST method will facilitate research and will conduct research systematically, the NIST method can be seen in the picture below:

Fig 1. Steps NIST

From the picture of the NIST step in Figure 1, it will be explained in the explanation below:

a. Collection
   At this stage is the stage where all the evidence is collected to record and find out whether there is enough evidence.
b. Examination
   At this stage is the stage where the data is backed up to store data securely, so that the data back is safe and cannot be hacked.
c. Analysis
   At this stage is the stage of executing based on applicable law so that the data can be protected properly and not misused.
d. Reporting
   At this last stage is the stage of the report from the results of research from the data obtained until analyzed, until the data can be protected properly, as a tool for digital forensic. Of the four stages carried out, the writer conducts research on a website www.armansp.com, whose data will be hacked or hacked by irresponsible parties, the results of research and discussion are in the next chapter.

3. Result

In this study the authors took a study about the detection of ransom virus on a computer and how to handle it, can be seen in the picture below:

a. Collection

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 50-55 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

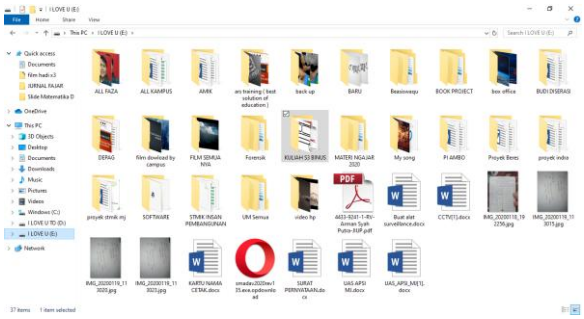

Fig 2 *Windows Explorer on the computer in question.*

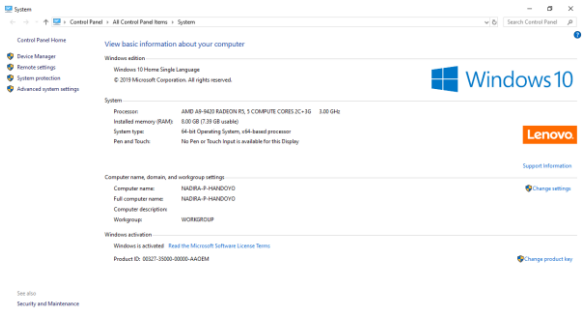

Fig 3 Basic information about Windows used

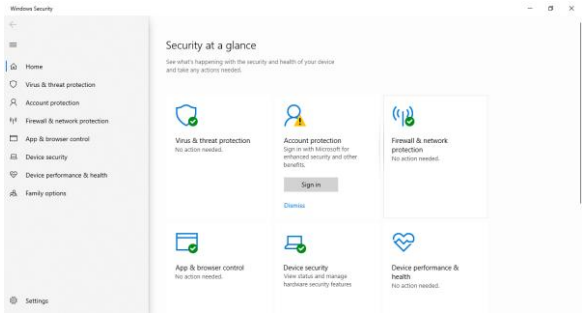

Fig 4 Information about protection on a computer

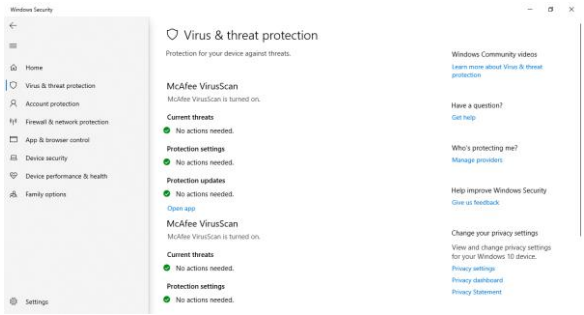

Fig 5. Information about a virus and its protection on a computer

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 50-55 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

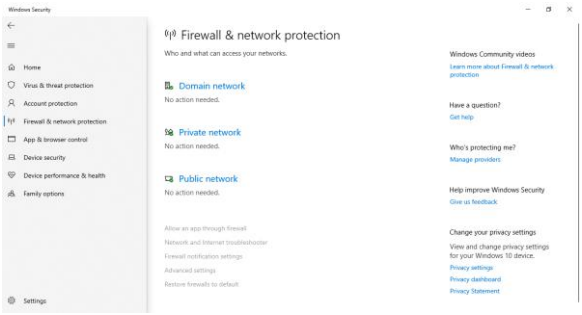

Fig 6. Information about protecting the computer part of the firewall that protects the computer from attacks from outside.

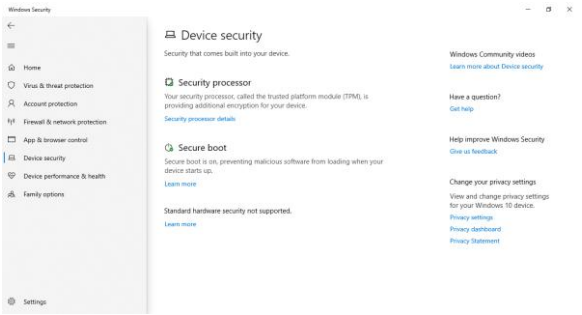

Fig 7. Information about security devices on a computer in the event of an attack will be useful

b. Examination

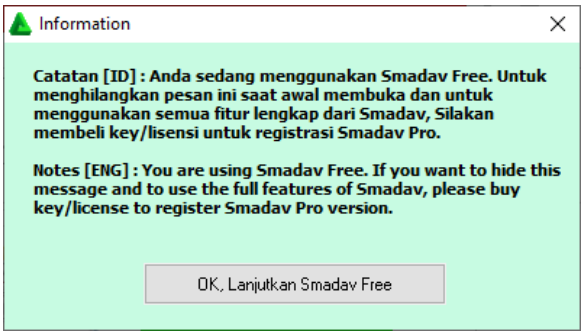

Fig 8. Information about using SMADAV anti-virus.

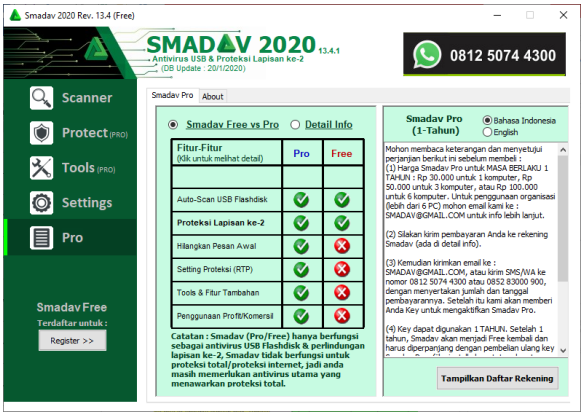

Fig 9 Information on using the SMADAV anti-virus when it is running

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 50-55 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

c. Analysis

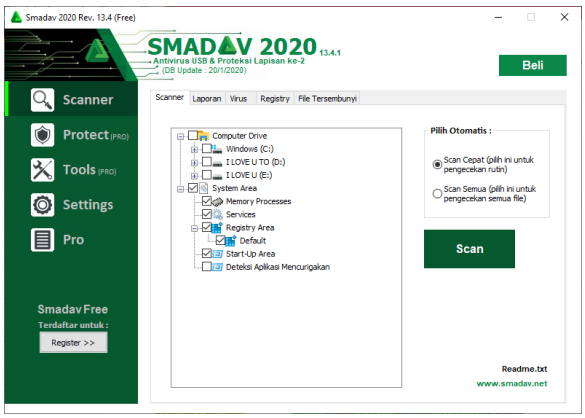

Fig 10. Information on using the SMADAV anti-virus if you are choosing

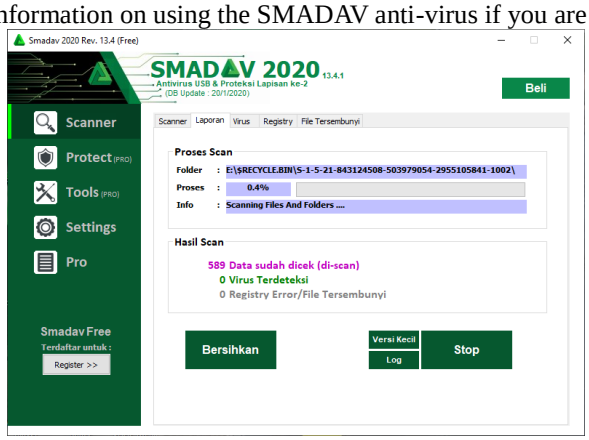

Fig 11. Information on using SMADAV anti-virus when running a virus scan, especially ransom virus.

d. Reporting

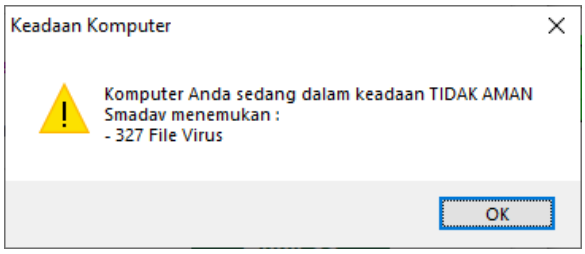

Fig 12. Information on using the SMADAV anti-virus when finding a virus file on a computer.

4. Conclusion

The results obtained from the above experiments are finding a virus and can be removed and can maintain computer security, and the Nist method can be used in various studies based on digital forensics, the use of anti-Smadav virus or others that can prevent computer viruses, if data secured, it will be computer safe, in this study using Smadav version 13.4, with diligent anti-virus updates it will protect your computer and data to be safe. Future research is making local or domestic anti-virus which can be worldwide, and can be used throughout the world, with free giving, making it easier to distribute worldwide, local products with international markets.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 4 Number 1 May 2020, pp. 50-55 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

5. References

[1]. Jinliang Shen,Shiming Gong,Wencong Bao, Analysis of Network Security in Daily Life, School of Computer Science and Technology, Shiyan University of Science and Technology, Hubei, China, Information and Computer Security (2018).
[2]. R.Sakthi Uma1, Prof. R. Angelin Preethi2, Cryptography Techniques, 12 Department of Computer Science, Kamban College Of Arts and Science for Women, Tiruvannamalai, Tamil Nadu, India, International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT | Volume 4 | Issue 3| ISSN : 2456-3307.
[3]. Yi Cao,Hao Tang,Jiangang Zhou, Research on Secure Communication Based on QQ Chat Platform, *Software Research and Development Center, College of Computer Science, Ningde University, Fujian, China, Journal of Secure Communication and System (2017).*
[4]. Zhang Jing, Research on Security Management and Preventive Measures of Library Computer Network System, Wuhan University of Technology Library, Wuhan 430070, China 694593@qq.com 2018 International Conference on Computer, Civil Engineering and Management Science (ICCEMS 2018).
[5] Ritzkal, Manajemen Jaringan Untuk Pemula,Bogor:UIKA PRESS,2018
[6] Ritzkal, Keamanan Jaringan Cyber,,Bogor:UIKA PRESS,2019.
[7] P. Peniarsih, "RANCANGAN SISTEM JARINGAN STP (SPANNING TREE PROTOCOL) BERBASIS VLAN," JSI J. Sist. Inf. Univ. Suryadarma, vol. 2, no. 1, Mar. 2018, doi: 10.35968/jsi.v2i1.39.
[8] D Setiadi, Pengamanan Data Dengan Algoritma Kriptografi Advanced Encryption Standard (AES),Jurnal Sibernetika.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.