System Detection and Prevention of Malware Wannacry Distribution Using Short Message Service

Agus Tedyyana

Informatics Engineering Department, Polytechnic of Bengkalis
Jl. Bathin Alam, Sungai Alam - Bengkalis

*Corresponding Email : agustedyyana@polbeng.ac.id

Abstract. Internet network is not something new today. In almost every place like corporate, education, offices and even public places, have also found the Internet to facilitate the flow of information.In the daily life of the Internet network becomes one of the important needs. With the Internet network, it will be easier for us in terms of sharing of data and information. Computer network security system has become a major part of an important and need to be considered in an agency, as reported in some media either inside or outside the country, there has been a phenomenon WannaCry malware attacks in several countries, including Indonesia. This WannaCry malware attacks spread and massive character and attacking computer connected to the internet, to provide protection or protection on an Internet network to avoid the various external threats in order to avoid WannaCry malware attacks by using application Spreading Malware Detection and Prevention Based WannaCry Short Message Service. From the test results have shown that the system is capable of detecting interference or intrusion into the network connected to the network and the Internet through a router to the rejection of the action and then send alerts in the form of a short message via Short Message Service to the network administrator phone.

1. Introduction

Almost no aspects of human life can separated from technology. Especially computer technology as it can see from the widespread use of computers. Advances in communications technology have an influence on the development of data processing, data from one place sent to another place by means of telecommunications, computer networking is not something new today, almost every company and there is a government agency computer networks to facilitate the flow of information. Internet are gaining popularity today is a giant computer network which is a computer network and can interact, so that within a few years the number of network users who are members of the Internet doubled.

Polytechnic of Bengkalis is one of the agencies whose activities supported by a network of internet in daily activities ranging from data processing, information systems, Mail Server, Web Server and several other functions. UPT-Computer as network administrators who manage the Internet network on the campus of Polytechnic of Bengkalis build network security systems by implementing Firewall and Proxy Server. Security with Firewall and Proxy Server system is sometimes still a gap for hackers, viruses, and so on to gain entrance into the existing network system using a variety of tools to bypass the firewall and proxy servers are used.

As reported in several media either inside or outside the country, there has been a phenomenon WannaCry malware attacks in several countries, including Indonesia. Malware attacks from WannaCry it is spread and massive and infect a computer connected to the internet. Therefore, to improve network security systems on campus Polteknik State Bengkalis one solution that used to help administrator in monitoring the condition of the network, analyzing packets and prevent anything that can harm the tissue is to use an application Spreading Malware Detection and Prevention Based Wannacry.

This system will detect interference or intrusion into the network connected to the Internet network, a warning mechanism is by way of sending messages to mobile phones in the form of SMS administrator.

The technology used to send Short Message Service is to utilize the Short Message Service Gateway. With the alert via Short Message Service, a security system would be better.

2. Method

The study had stage-by-stage settlement is structured in a research procedure. Research procedure starts with identifying the problem, at this stage, will be presented the stages that done in the system design. The stages on design of this system are the preparation, planning, design, implementation, operation, and optimization as shown in Figure 1.

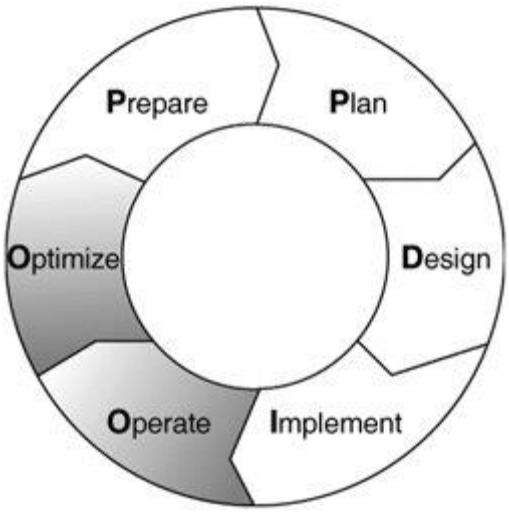

Figure 1 Stages in system design.

2.1. Preparation phase

At this stage, preparations will be made to establish the needs or data that will be used to design the proposed system. As for the preparations to be done is to collect research data such as ports that are frequently accessed by malware and Determining the software that will be used to design the system.

2.2. Planning phase

Phase Plan (planning) to identify the network requirements based on destination, amenities, and user needs. This phase describes the characteristics of a network, which aims to assess the network, perform gap analysis on the best design of an architecture, by looking at the behavior of the operational environment. A project plan was developed to manage tasks (tasks), the parties responsible, stepping stones (milestones), and all the resources to undertake the design and implementation. Project planning should be in line with the scope (limitations), cost and resource parameters that are tailored to business needs. The project plan is followed (and renewed) during the phases in the cycle.

2.3. stage Design

Network design developed based on technical requirements, and business acquired from previous conditions. Network design specifications is a design that is comprehensive and detailed, which meet the technical and business requirements today. The network should provide availability, reliability, security, scalability and performance. Results designs include network diagrams and a list of equipment. The project plan must be constantly updated, with more detailed information to be implemented. Once the design phase is completed, the implementation phase begins

2.4.Implementation of phase

In this phase, new appliances do installation and configuration, appropriate design specifications. These new devices will replace or add to the existing infrastructure. Project planning must also be followed during this phase, if there is a change should be addressed at the meeting (meeting), with the necessary

approvals to proceed. Each step in the implementation, should include a description, detailed guidelines for the implementation, the estimated time for implementation, evaluation (rollback) measures if there is a failure, and other information as additional references. As the changes have been implemented, the stage is also a testing step, before moving to the operational phase (phase Operate)

2.5. Operational phase

Operational phase is to maintain daily activities resilience network. Operations include management and monitoring of network components together components, maintenance routing, manage the activities of the upgrade, manage performance, identify and correct network errors. This stage is the ultimate test for the design stage. During operation, network management should monitor the stability and performance of the network, error detection, correction configuration and performance monitoring activities, which provides preliminary data for the next phase, namely the phase of optimization (optimize phase).

2.6. Phase Optimization

The optimization phase, involving a proactive awareness by identifying network management and resolve problems before they affect network issues. Optimization phase, allowing to modify the design of the network, if too many network problems that arise, and also to fix the performance problems, or to solve the problems in the application (software). Requirements-requirement for the modified network design directs the development of the network, back to the beginning of the life cycle in phase models PPDIOO

3. Research Result

Figure 1 shows that there is a system designed to monitor the network traffic flow that occurs in the router. The flow of traffic in the flow monitoring is at the port. The system will detect ports passing through the router. Therefore, there are multiple ports indicated as the commonly used ports on the spread of malware such as Wannacry. The ports indicated as ports used, as a stream of malware is port 137, 138, 139, 445 and 3389. Therefore, when there is a flow from the ports, then the system will take action. The action taken is to close the port and simultaneously sends flow information contains no malware. The information sent via Short Message Service Gateway. Users will receive information in the form of Short Message Service.

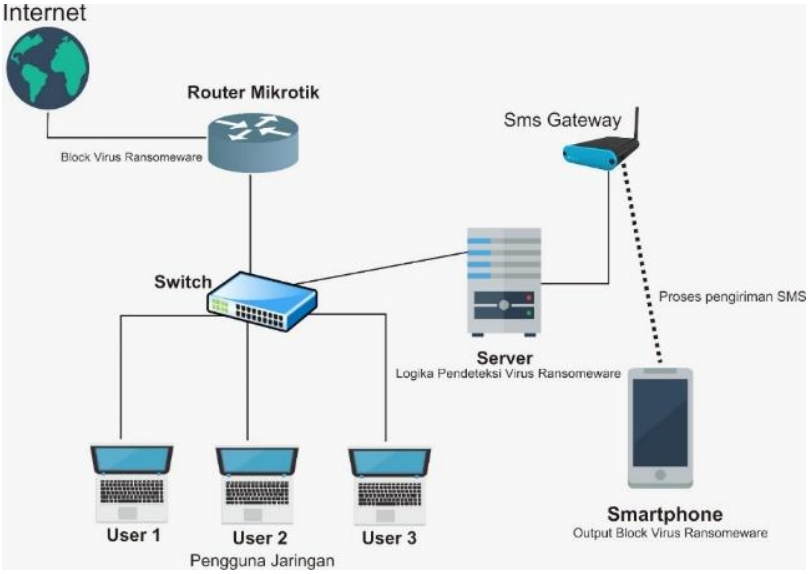

Figure 1 Results Design System.

The process flow looks like the following picture

Vol 3-Sep2018
ISSN: 2541-3023

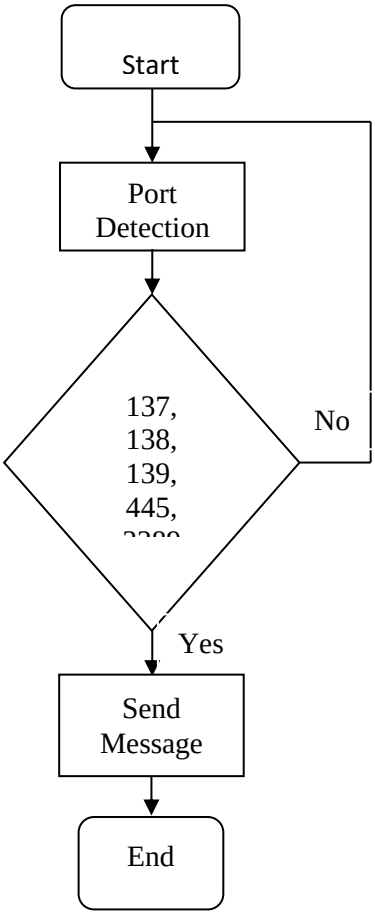

Figure 2 Flowchart of system design.

igure 2 shows the flow of the proposed process. In the diagram shows some of the processes used starting from the detection port. Port detection used to detect whether there is a network that passes through the ports in the selection. If there is a network that passes through the ports selected then the system will send information in the form of a Short Message Service via Short Message Service Gateway.

Figure 3 shows the ports that often used by malware like Wannacry. So these ports used to detect malware.

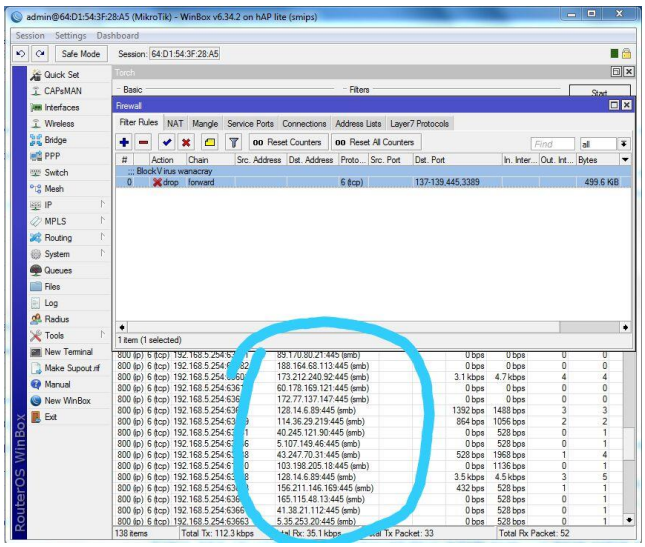

Figure 3 Block SMB.

Figure 4 shows the contents of Short Message malware detection results. When there is malware that infiltrate into the router, the router will block these sites then the router will send an SMS containing that no malware infiltrated the network through the Short Message Service gateway.

Figure 4 Short Message malware detection results

4. Conclusion

Of the system that produced show, which the system is able to detect malware infiltrating through the router, as for ports that are often passed malware that is 137, 138, 139, 445 and 3389. Ports used to detect malware that goes through the network. The system is designed to make web-based applications built using web programming languages like html, php, css, web applications are built are placed on a server or hosting. The application used to monitor a proxy router. So that when there are access ports (137, 138, 139, 445 and 3389) on the router, the system will take action that is sending information to the administrator or other parties via Short Message. Short Message will be sent by using Short Message Service Gateway.

There is a downside of the proposed system is that all the networks will access or pass through ports which have been determined (137, 138, 139, 445 and 3389) will be considered as malware activity. So this system cannot distinguish between that which passes through the ports malware is malware or not.

References

[1] M. Howard, A. Pfeffer, M. Dalal, and M. Reposa, "Predicting Future Signatures of Malware Variants," *12th Int. Conf. Unwanted malicious softw. (Malware 2017)*, Pp. 126-132, 2017.
[2] M. Kalash, M. Rochan, N. Mohammed, NDB Bruce, Y. Wang, and F. Iqbal, "Malware Classification with Deep Convolutional Neural Networks," *2018 9th IFIP Int. Conf. New Technol. Car. Secur.*, Pp. 1-5, 2018.
[3] S. Hsiao and D. Kao, "The Static Analysis of WannaCry G Ransomware," pp. 153-158, 2018.
[4] D.-Y. Kao and S.-C. Hsiao, "The dynamic analysis of WannaCry ransomware - IEEE Conference Publication,"*Int. Conf. Adv. Commun. Technolo gy (ICACT*, Pp. 159-166, 2018.
[5] N. Hampton and ZA Baig, "Ransomware: Emergence of the cyber-extortion menace," *Aust. Inf. Secur. Manag. Conf.*, Vol. 13, pp. 47-56, 2015.

[6] Q. Chen and RA Bridges, "Behavioral Analysis of Automated Malware A Case Study of WannaCry Ransomware," pp. 454-460, 2017.
[7] S. Mohurle and M. Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017" *Int. J. Adv. Res. Comput. Sci.*, Vol. 8, no. 5, pp. 2016-2018, 2017.
[8] X. Lu, W. Lei, and W. Zhang, "The design and implementation of XMPP-based SMS gateway," *Proc. - 2012 4th Int. Conf. Comput. Intell. Commun. Syst. Networks, CICSyN 2012*, Pp. 145-148, 2012.
[9] C. Taddia and G. Mazzini, "Architectures for an efficient SMS Gateway service," *2015 23rd Int. Conf. Software, Telecommun. Comput. Networks, SoftCOM 2015*, Pp. 254-258, 2015.
[10] M. Kashif, "Secure SMS gateway communication using encryption and digital signatures," *Proc. - 17th IEEE Int. Conf. Comput. Sci. Eng. CSE 2014, Jointly with the 13th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC 2014, 13th Int. Symp. Pervasive Syst. Algorithms, Networks, I-SPAN 2014 8th Int. Conf. Front. Comput. Sci. Technol. FCST 2014*, Pp. 1430-1434, 2015