Malware Injection in Operational Technology Networks

Mayuri Khadpe
Department of Electrical Engineering
Veermata Jijabai Technological Institute
Mumbai, Maharashtra, India
mskhadpe_m18@et.vjti.ac.in

Pranita Binnar
Department of Computer Engineering
Veermata Jijabai Technological Institute
Mumbai, Maharashtra, India
pbbinnar_p19@ce.vjti.ac.in

Dr. Faruk Kazi
Department of Electrical Engineering
Veermata Jijabai Technological Institute
Mumbai, Maharashtra, India
fskazi@el.vjti.ac.in

***Abstract*—Security Issues of Industrial Control System (ICS) increasing day by day because of this, it gets more and more attention. Hackers finding different methods or approaches to finding vulnerability of Operational Technology (OT) Networks. Some of the methods used by Attacker are injection of malware and backdoor. Programmable logic controller (PLC) and Supervisory Control and Data Acquisition (SCADA) both are important part of industry. Usually, Industrial Control System network is completely isolated from external network, but the administrative computer which is connected to the network are vulnerable, one of the reasons will be use of internet are increasing day by day. Stuxnet Attack is example of this type of vulnerability. The proposed work consist of are performing a Denial of service (DoS) attack on Allen Bradley PLC which is used to control Waste-Water Treatment Plant (WTP). To performing this attack we first, inject a malware into an administrative computer, which is connected to Waste-Water Treatment Plant network. The malware we inject into the network is capable of collecting all information of network which includes all IP address, its vendor information, MAC address etc. The data is stored into a text file which will downloaded from Victim Computer into Hacker computer by using Backdoor. And after finding target IP address, we will perform DoS attack. Also, this paper discussed about process of creating malware and backdoor as well as it includes analysis of network traffic before and after performing an attack.**

***Keywords*—ICS, PLC, SCADA, OT Network, IP address, MAC address, Malware, Backdoor, DoS Attack**

I. Introduction

The Industrial Control System (ICS) are majorly focuses on increase production and development, with the help of different types of automation systems. ICS having several types, most common are SCADA systems and DCS systems. SCADA system are used to monitor and have authority to control different process which are present in industry. Where this system is connected to many sub-components, such as PLC, RTU, Human Machine Interface (HMI) etc. SCADA systems have a momentous role in different domain specific industry. For remotely control and monitoring different types of automated process such as, To control flow and pressure in oil and gas industry, in water related process, used for water treatment and its distribution, SCADA systems are used. This Systems allow operator to operate all process from a control panel room which situated far from the actual plant. Because of this complexity and interconnectivity, SCADA system bare a wide range of vulnerable points in perspective of Cyber-security.

A common intimidation in Operational Technology Networks is that after doing a social engineering, attacker can inject a malware into a system with the help of infected portable USB or by using an Email attachment. In real scenario, hacker or atrocious employees can enter into OT Network to gain unauthorized access for finding vulnerabilities of system so that after performing attack it will lead to calamitous damages.[11] In 2010, Stuxnet Attack happen on Iranian Nuclear Plant. In this attack, attacker targets PLCs, which allow the automation of electrotechnical process used for nuclear plant. Stuxnet having 3 major parts: first is worm that used mainly for executing payload, Second part or module is basically a link file that used to spread that worm to others systems i.e. its creates the copies of worm, and Third part is rootkit component used for hiding all required malicious files and process to prevent Stuxnet detection. It is found that vulnerabilities of any system are not only from outside such as Hackers, industry rival, but also from inside service such as disgruntled employees, site engineers etc.

In this paper, we have an experimental setup of Waste-water Treatment Plant (WTP) which control by Micrologix-1400 PLC. Usually, PLC used a different types of communication protocols such as DNP3, Modbus Protocol, Ethernet-IP protocol etc. In our case, communication protocol used by Micrologix-1400 PLC is Modbus Protocol. This Paper mainly focused on following things:

- Creating a Malware which scan the whole network and find out vulnerable IP address. Malware is nothing but hiding a malicious code behind an image, PDF or Video. Also, it will discuss the process of creating a malware.
- This paper present how to stored data of Vulnerable IP address and its useful information such as vendor of PLC, protocols used by PLC, open port details etc. and with execution of Backdoor we download that data from victim PC to Attacker PC.
- Perform a different type of attacks on vulnerable IP address such as DoS attack, such that communication between PLC and SCADA monitoring system breaks, which will affect an waste water treatment plant.

- Proposed system is also focusing on the analysis of network traffic before and after attack take place.

Above all is tested and validated on a real experimental setup of Waste-water Treatment Plant. Section II consist of related work in the area of SCADA Attack and Malware. Test Bed Architecture is described in section III, Detailed explanation of attack approach is present in section IV. Section V consist of Results and discussion and paper is concluded in section VI.

II. Related Work

Nowadays, In Industrial Control System (ICS) ratios of cyber-attacks are increasing day by day, which includes cyber attack on SCADA system, PLC, RTU etc. Malware injection plays very important part in cyber attacks. To do attack on any system is very important to find its vulnerable points of that system and anatomy of distribution of attack on different types of networks. The proposed work is mainly focused on various techniques used for malware injection within an isolated network with the help of e-mail, infected pen-drives etc. Along with this how malware is spread over a network to harm network that also discussed in this work [3]. Risk analysis of critical infrastructure in SCADA vulnerabilities and exploits based on statistical methods are given by various techniques[8]. Nowadays demand of connecting SCADA system with IIOT system leads to allow hacker give access potentially vulnerable SCADA system with the help of Backdoors. Vulnerability density is find out collecting total no of exploits related to CVE over total no of SCADA exploits. However, analyses are not done on updated data. For training large data set, GPU of normal windows machine is sometimes insufficient so user will do outsource training. New security risk introduced is outsourced training. In [6], They create BadNet i.e. backdoor neural network which harm the purpose of original model. However, prevention of this kind of attack is not mentioned in proposed work.

Malware attacks are increasing very vigorously. To do a Malware injection or Backdoor Injection, very important factor will be to know how to design it and its implementation. Injection of Malware is most probably done on windows operating system. But this proposed work brings forth a novel comprehensive study of Malware based on Linux OS. [10]. Design and its implementation and its related results are also discussed. However, Linux malware investigation should be more comprehensive. Backdoor attack is basically gaining all access of victim machine without prior permission of legitimate user. In [4], Implementation of backdoor attack which is based on classification of text is discussed. The effect of cyber-attack on neural network model such as LSTM is evaluated. However, the prevention of it not included in proposed work. To avoid malware injection in OT network it is important to detect it to avoid further problems. To do analysis of malware there are various techniques are present. In [7]-[9], how signature and its feature extraction play a vital role for detecting a malware is discussed. However, if malware is encrypted than the method fails.

Main Challenge in OT Network is to prevent it from different forms of attacks. Cyber attacks adversely affect SCADA systems. In [1], The elementary mode to safeguard the power industry depends on cyber physical system. Cyber net model which includes Firewall model and Password model and behaviour‘ of power system is discussed. However, an attack from within the substations should be analysis. Increasing attack on SCADA system, the proposed methodology focuses on to solve issue present between end points of SCADA systems[5]. How to secure system from different types of attack is also discussed in this work. In order to secure SCADA communication a scheme by the name trusted ID reference is used. However, Dynamically ID modification should be done. Similarly, to prevent ICS system from malware is also very important. There are different techniques for malware detection which uses three approaches [2]. The approach use for malware detection is machine algorithms which based on signature and behaviour-based data base, Deep learning-based model etc. However, it is failed to detect and prevent unknown malware.

The motivation of this proposed work, any malicious software has an aim to damage the network to steal sensitive data or to obtain root entitlement. Survey says that impact of malware is getting worse day by day specially in OT network. Because of this reason, this proposed work helps to understand how malware injection takes place and their impact on OT network. It, also discussed about malware detection techniques.

III. Test Bed Architecture

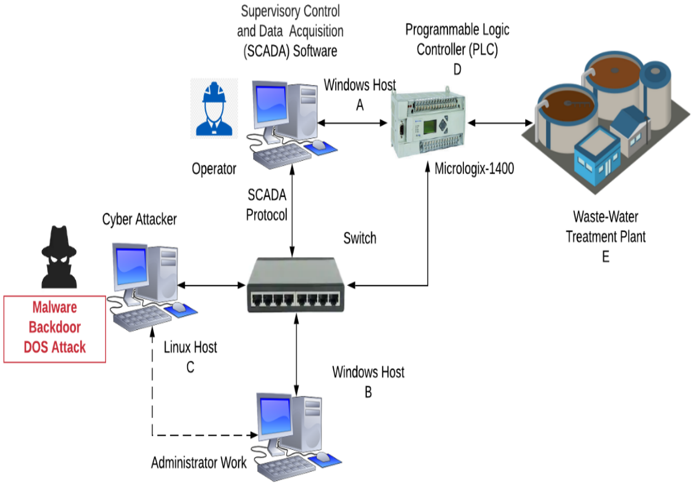

Supervisory Control and Data Acquisition (SCADA) Software
Programmable Logic Controller (PLC) D
Windows Host A
Operator
Micrologix-1400
SCADA Protocol
Switch
Waste-Water Treatment Plant E
Cyber Attacker
Malware Backdoor DOS Attack
Linux Host C
Windows Host B
Administrator Work

Fig. 1. Experimental setup Architecture of SCADA System

Fig. 1, illustrate a Experimental setup architecture which contains 3 computer from A to C, Switch, PLC and waste water treatment plant (WTP). Computer A is a windows host which simulate real-time SCADA communication with Allen-Bradley PLC. Where this programmable logic controller (PLC), control the whole waste-water Treatment Plant. In Windows Host A, is a Administrative PC where two SCADA software's are equipped, one is open source mySCADA control software and another one is proprietary iVisionmax control software. Which each software is used to monitor and give commands to Allen Bradley PLC which further send commands to control panel of waste water treatment plant (WTP). Windows Host B is used for administrative work within network. Host A and Host B connected by a switch. The Linux host C which is an attacker try to enter into the OT Network by injecting a malware into an administrative work PC. The way can be an email attachment or a Malicious USB. We enter into a network with the help of Malicious USB which can be plant by ex-employee or a site engineer. From Rockwell Automation, PLC used is Allen Bradley Micrologix-1400 which control WTP. This Plc support different types of protocols. In our experimental setup, we configure Allen Bradley PLC with Modbus protocol for communication of PLC and SCADA. Allen Bradley PLC has expansion slots for increasing the capacity of input and output channels.

- Waste-Water Treatment Plant Working:

Fig 2. Shows Process Flow Diagram of Waste Water Treatment Plant. The main motive of Waste Water Treatment Plant is to purify Sewerage Water into an accessible form which can use by an human for different industry purpose. In the waste water treatment control system there are total five tanks: Water Storage Tank (WST), Waste or Sewerage Water Tank (WWT), Treated Water Tank (TWT) are filled with water, cooling Tank (CT) which is filled with cold water. Chemical Tank (CT) is filled with 50% of liquid solution.

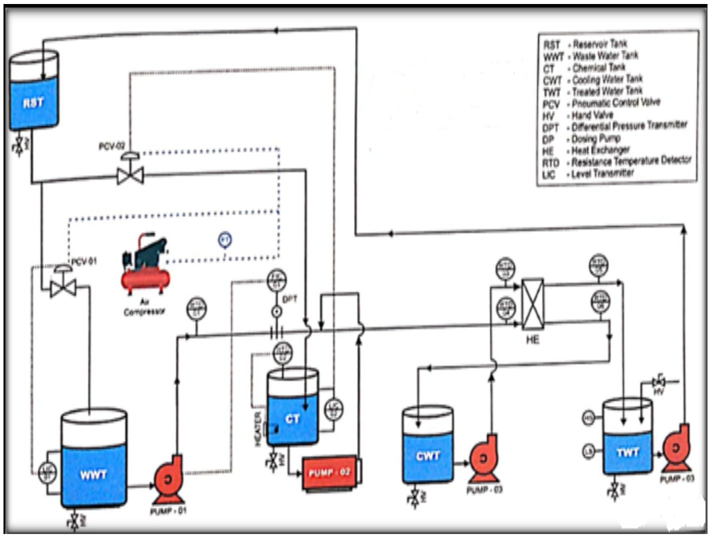


Fig. 2. Waste Water Treatment Plant

In system there are three centrifugal pumps, one of them are operated using Variable Frequency Drive (VFD), waste water tank outlet pump is operated using ABB VFD whereas cooling water tank flow is handled through cooling water pump by ON/OFF operation. Dosing pump is used to add chemical in process stream from chemical tank. Heated process stream is cooled in plate type heat exchanger and sent to treated water tank. Treated Water tank has Low-level switch (LS) and High-level switch (HS), depending upon the status of switches Treated water pump is operated. The liquid from treated water tank is sent to reservoir tank. The Process proceeds in the following manner:

- Water is added to Waste Water Tank (WWT). Three phase centrifugal pump is used for pumping water from WWT, dosing of chemical is done in the stream using Dosing pump.
- After addition of chemical the temperature of process fluid increases, hence it is passed through Plate type heat exchanger.
- In heat exchanger the hot process stream is cooled using circulation of chilled water. The cooled process stream is then passed to treated water tank. Cooling water is circulated after passing through heat exchanger in cold water tank.
- When treated water tank is filled till High level switch, pump which control treated water tank will ON and purify water again passed in the reservoir tank.

IV. Attack Approach

In our experimental setup, Allen Bradley MicroLogix PLC controls the waste water treatment plant whereas by using SCADA software, we remotely monitor all the activities e.g. Water level, Chemical level, Flow control, Heater Temperature etc. of Waste Water Treatment Plant. Main motive is to gather all OT network information by accessing an administrative Computer which is connected within a same network and Harm that Waste Water Treatment Plant without user's permission. We are targeting administrative computer because in industry such plant is completely isolated so it's difficult to access main network directly, whereas administrative computer is always connected to internet and comparatively easily accessible for attackers.

It is found that vulnerabilities of any OT Network are not only from outside such as Hackers, industry rival, but also from inside service such as disgruntled employees, site engineers etc. So, we create a scenario such that disgruntled employees or site engineer inject a Malware into an administrative computer. Once's the Malware is activated it will Start scanning whole network and gather all network information such as IP address, protocol used by each IP address, its vendor, communication port etc. After collecting all the information, it will be stored into a text file. Start Searching an IP address which uses port no 502 for its communication and use Modbus protocol for transmission of data.

After finding this data backdoor will activate such that attacker can access the victim Computer. It can alter any configuration file by uploading malicious file or download any file from victim Computer. After gathering all information from victim, we will do a DoS attack on Allen Bradley PLC for that first we terminate the backdoor such that no one can find out information about attacker, and then perform DoS attack on selected IP address such that communication

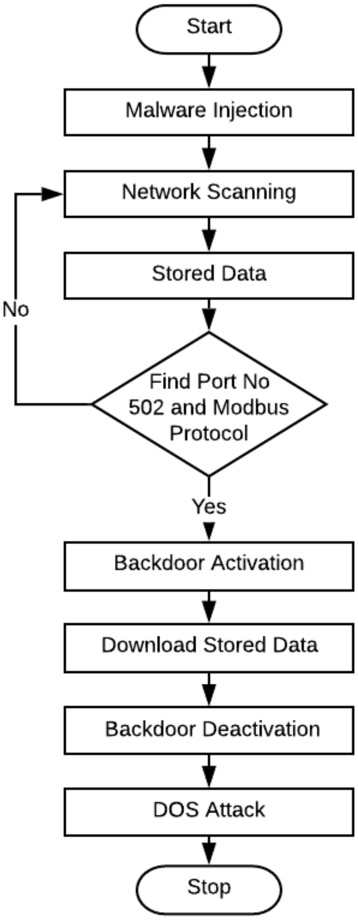


Fig. 3. The Attack process

between PLC and SCADA will break. So, Operator will unable to give command to PLC to monitor WTP plant. Fig.3 illustrate Attack process in detail.

A. Malware Injection

A Malicious Software is known as Malware, which designed to damage or harm a computer system without user's permission. In simple words, hiding any malicious code behind an Image, PDF or Video such that it used for harm that network without a prior permission of authentic person. Malware is having different categories depending upon its functions. Categories is known as Virus, Trojan, Worms, Spyware and Rootkit. We create a Rootkit Malware, which basically having a program which creates a backdoor into the system for attacker use. Rootkit is a malevolent code that gives an honored to access Victim machine for an illegal user. It contains different malicious tools e.g. Keylogger, Password Stealer and bots for DDoS Attacks. In our case, we wrote a python script which having a code for performing a DoS attack on target IP address. In simple words, Hacker will get the access of victim Computer and it will study the network behaviour of victim and alter log files or destroy the data files and perform DoS attack.

- Process of creating Malware:

Write a python code as per the requirement of Attack. A code which contain 3 Function or Module such as Network Scanning function which collect all IP address and its related information which present within an network and find out IP address whose using a Modbus protocol and port no 502 for its communication, Second Module is Backdoor Function which use for enter into the system without permission of authentic User and Third function is used for performing DoS attack on target IP address. After a writing a python script we have to convert that .py file into an .exe file using a Wine Software.

Wine stands for **W**ine **I**s **N**ot an **E**mulator is an open Source Software which provides its own windows runtime environment. So, by using Wine Software we create .exe file for that first we have to install Wine on Linux Computer. After Installation of Wine Software with help of few commands we convert .py file into .exe file. That exe file contains all the environment which required to execute a code i.e. exe file in the windows computer. Wine Software is also used for hiding that .exe file behind an Image, PDF or Video. By using Command which add data i.e. .exe file behind an PDF or Image. In, Fig 4 illustrate the construction of Malware in detail.

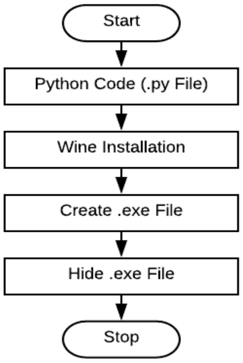


Fig. 4. Construction of Malware Flowchart

B. Network Scanning

For a Hacker/Attacker, once Malware is activated in a specific environment, first thing is do Scan the whole OT network and find out Target IP address. After Scanning whole OT network, it collects all the network information. The Scanner collects following Information:

- Get IP address within a network
- Save information regarding its services e.g. TCP service
- Save Vendor details and MAC address of IP's
- Save information of Hostnames and find all port which is used for communicating

After scanning complete network, we save that data into a text file. Network Scanner append one by one IP's information which mentioned above in a text file. Major Part is finding an

PLC IP address. In our experimental setup, we are using an Allen Bradley MicroLogix PLC, which configure on Modbus Protocol and uses Port No 502 for its communication. Usually, PLC uses an open port no 102 or 502, but in our case, we used a 502 port. So, to find an PLC IP address we wrote a condition which use 502 port and Modbus protocol for its communication. Data stored in form of string, so we wrote condition which use to find out target IP address of PLC, using port 502 and mbap for communication. mbap stands for Modbus Application.

C. Backdoor

A Backdoor is a nothing but gaining all access of victim machine without authenticate or legitimate prior permission. Attacker use to alter data and gain system access of Victim Computer. There are Two types of Backdoor are as follows:

- Bind/Direct Connection: Attacker/Hacker directly communicate with Victim Machine with help of open port. Normally TCP 80 port is open port. But in this method its high possibility that firewall can detect this type of Backdoor.
- Reverse Connection/ Reverse Shell: In this method, attacker is in listening mode means he will not get a connection till backdoor code get executed. Once's Backdoor codes get executed, we establish connection with victim and get a complete access of that system. Fig. 5 shows overview of Reverse Shell Backdoor.

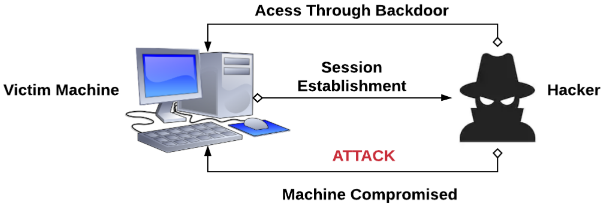


Fig. 5. Overview of Reverse Shell Backdoor

In our setup, we use a Reverse Shell Method for Activating a Backdoor. Because of use of reverse shell method, it will undetectable by antivirus software's or firewall. Backdoor Commands shown in Table I

TABLE I
BACKDOOR COMMANDS

Command	Output
whoami	Display Username and its Operating System
ipconfig	Displays all network configuration details
dir	Displays Data present in current working directory
cd	Used to change the current working directory
more file_name	Used to read data from file
Upload file_name	Used to upload file into Victim Machine
Download file_name	Used to download file from Victim Machine

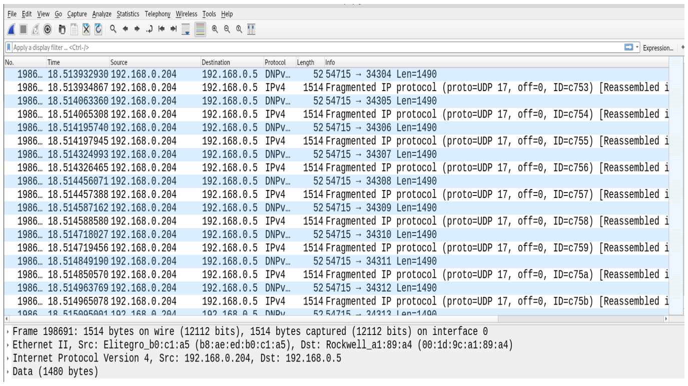
Above all commands, hacker can execute without a legitimate permission into an Victim Machine. Hacker can download or upload any file namely PDF, Video, Text file, configuration File respectively. In this paper, we went to directory where that text file is stored which contains all the OT network IP related information. After finding that text file we download that file to hacker computer. After collecting all the information, we have to terminate this backdoor for further attack. So, no one can identify the attacker.

D. DoS Attack

DoS Attack stands for Denial of Service Attack. This attack is one of the oldest forms of cyber coercion Attack. As name indicates, it denies service of any legitimate or authenticate user.

A DoS Attack execute in two ways:

- Specially Crafted Data: In this type, Attacker send a Specially Crafted data to victim Machine such that, if victim is unable to handle this specially crafted data then there are chances that victim machine will get crash. This type doesn't contain huge data but includes special designed crafted data packets. This involve server exploitation, manipulating fields in the network protocol packets and so on. E.g. Teardrop Attack and Ping of Death.
- Flooding: To slow down victim machine, attacker sends too much data. So, victim will spend its resources on consuming the attacker's data and fail to serve the legitimate data. E.g. DDoS attack.Attackers can use a combination of both the types. E.g. UDP Flooding and SYN Flooding.



```
No.      Time        Source         Destination  Protocol Length Info
 1986… 18.513932930 192.168.0.204  192.168.0.5  DNPv…      52 54715 → 34304 Len=1490
 1986… 18.513934867 192.168.0.204  192.168.0.5  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=c753) [Reassembled i
 1986… 18.514063360 192.168.0.204  192.168.0.5  DNPv…      52 54715 → 34305 Len=1490
 1986… 18.514065308 192.168.0.204  192.168.0.5  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=c754) [Reassembled i
 1986… 18.514195740 192.168.0.204  192.168.0.5  DNPv…      52 54715 → 34306 Len=1490
 1986… 18.514197945 192.168.0.204  192.168.0.5  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=c755) [Reassembled i
 1986… 18.514324993 192.168.0.204  192.168.0.5  DNPv…      52 54715 → 34307 Len=1490
 1986… 18.514326465 192.168.0.204  192.168.0.5  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=c756) [Reassembled i
 1986… 18.514456071 192.168.0.204  192.168.0.5  DNPv…      52 54715 → 34308 Len=1490
 1986… 18.514457388 192.168.0.204  192.168.0.5  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=c757) [Reassembled i
 1986… 18.514587162 192.168.0.204  192.168.0.5  DNPv…      52 54715 → 34309 Len=1490
 1986… 18.514588580 192.168.0.204  192.168.0.5  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=c758) [Reassembled i
 1986… 18.514718027 192.168.0.204  192.168.0.5  DNPv…      52 54715 → 34310 Len=1490
 1986… 18.514719456 192.168.0.204  192.168.0.5  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=c759) [Reassembled i
 1986… 18.514849190 192.168.0.204  192.168.0.5  DNPv…      52 54715 → 34311 Len=1490
 1986… 18.514850570 192.168.0.204  192.168.0.5  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=c75a) [Reassembled i
 1986… 18.514963769 192.168.0.204  192.168.0.5  DNPv…      52 54715 → 34312 Len=1490
 1986… 18.514965078 192.168.0.204  192.168.0.5  IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=c75b) [Reassembled i
 1986… 18.515095001 192.168.0.204  192.168.0.5  DNPv…      52 54715 → 34313 Len=1490

› Frame 198691: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
› Ethernet II, Src: Elitegro_b0:c1:a5 (b8:ae:ed:b0:c1:a5), Dst: Rockwell_a1:89:a4 (00:1d:9c:a1:89:a4)
› Internet Protocol Version 4, Src: 192.168.0.204, Dst: 192.168.0.5
› Data (1480 bytes)
```

Fig. 6. Screenshot of Wireshark of UDP Packets Flooding

In this paper, we did a User Datagram Protocol (UDP) flooding Attack. In this type of attack, we specially craft a User Datagram Protocol (UDP) data packet and send to target IP address of PLC. We continuously send this UDP packets such that whole network is flooded with UDP packets such that the connection between PLC and SCADA breaks. So, SCADA computer could not communicate or send command to PLC. Fig.6 shows Screenshot of Wireshark of UDP Packets Flooding

V. RESULTS AND DISCUSSION

In this section, we will do an Analysis of Network Traffic. In our experimental setup, any two machine uses a TCP protocol for its communication and Programmable Logic Controller (PLC) is used Modbus Protocol for its communication with Supervisory Control and Data Acquisition (SCADA). In normal condition, protocols used by a OT network is TCP protocol and Modbus Protocol, whereas after performing a DoS attack, since we Specially crafted a UDP data packets so that whole network is flooded with UDP packets and Internet Control Message Protocol (ICMP) packets for its acknowledgment.

We collect all network traffic in csv format in normal traffic condition as well as after performing a DoS attack on Target IP address. After collecting this data, we conclude that, in normal condition, network uses a maximum TCP protocol followed by Modbus protocol, there is no UDP as well as ICMP Protocol used by any machine within a network, whereas after a DoS attack, TCP packet is replaced by UDP packets. Whole network is flooded with the UDP packets. In Fig 7 and Fig. 8, we plot the network traffic before a DoS attack and After a DoS attack. After plotting this graph, we can conclude that before an attack take place, 97.3% TCP protocol and 2.7% Modbus protocol is used for communication. After performing an Attack, UDP protocol used is 96.4% and ICMP protocol as 3.6% respectively. Thus, from the result we can conclude that after an attack whole network is flooded with UDP packets.

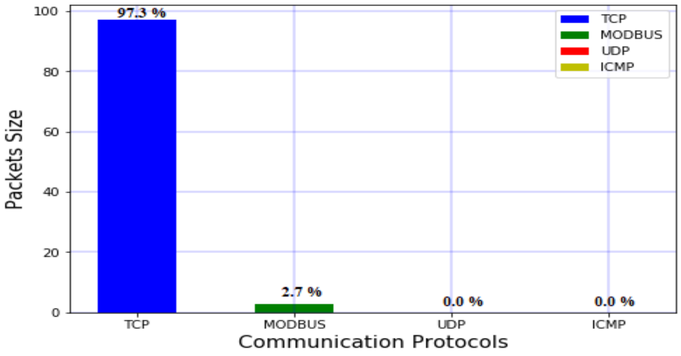


Fig. 7. Network Traffic Before Performing DoS Attack

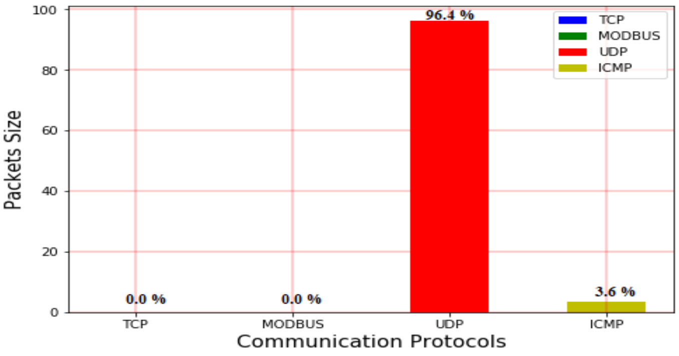


Fig. 8. Network Traffic After Performing DoS Attack

VI. Conclusion

Cyber attacks includes Identify Theft, Malware, Spoofing, Spyware and Unauthorized Access etc. PLC and SCADA is a major component for cyber attacks. In this paper, we proposed a malware which capable of collecting whole OT network information which includes IP address, Vendor details etc. Also, how to create Malware and Backdoor which used to get useful data from Victim Machine into Hacker Machine is developed. Proposed work, perform a DoS attack on Allen Bradley PLC such that complete network is jam because of excess of UDP Packets so that communication between PLC and SCADA breaks, eventually it affect Waste Water Treatment plant. The proposed work only perform an DoS attack, we can perform different types of attack on OT network with the help of malware injection.

The paper is only focusing on performing an attack but it is important to prevent it also. To monitor different types of threat in Industry, mostly used a Intrusion Detection System (IDS) and to prevent this threat from system, commonly used an Intrusion Prevention System (IPS) or Firewall. So, future aspect will be preventing the system from this type of attack and malware analysis using forensic procedure and evidence management of traces found in malware attack of SCADA/ICS network.

Acknowledgment

We are thankful to Mr. Akshay Rajapkar, Mr. Shahrukh Khan and members of COE-CNDS lab, VJTI, Mumbai for providing us platform to conduct reseacrch on topic ”Malware Injection in Operational Technology Networks” and for their continuous support during the entire research period.

References

[1] C. Ten, C. Liu and G. Manimaran, ”Vulnerability Assessment of Cybersecurity for SCADA Systems,” in IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.

[2] O. A. Aslan and R. Samet, ”A Comprehensive Review on Malware Detection Approaches,” in IEEE Access, vol. 8, pp. 6249-6271, 2020.

[3] S. Kim, ”Anatomy on Malware Distribution Networks,” in IEEE Access, vol. 8, pp. 73919-73930, 2020

[4] J. Dai, C. Chen and Y. Li, ”A Backdoor Attack Against LSTM-Based Text Classification Systems,” in IEEE Access, vol. 7, pp. 138872-138878, 2020.

[5] J. Qian, C. Hua, X. Guan, T. Xin and L. Zhang, ”A Trusted-ID Referenced Key Scheme for Securing SCADA Communication in Iron and Steel Plants,” in IEEE Access, vol. 7, pp. 46947-46958, 2019.

[6] T. Gu, K. Liu, B. Dolan-Gavitt and S. Garg, ”BadNets: Evaluating Backdooring Attacks on Deep Neural Networks,” in IEEE Access, vol. 7, pp. 47230-47244, 2019.

[7] Y. Liu, Y. Lai, Z. Wang and H. Yan, ”A New Learning Approach to Malware Classification Using Discriminative Feature Extraction,” in IEEE Access, vol. 7, pp. 13015-13023, 2019.

[8] G. Falco, C. Caldera and H. Shrobe, ”IIoT Cybersecurity Risk Modeling for SCADA Systems,” in IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4486-4495, Dec. 2018.

[9] O. P. Samantray, S. N. Tripathy and S. K. Das, ”A study to Understand Malware Behavior through Malware Analysis,” 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2019, pp. 1-5.

[10] E. Cozzi, M. Graziano, Y. Fratantonio and D. Balzarotti, ”Understanding Linux Malware,” 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2018, pp. 161-175.

[11] Y. Yang et al., ”Man-in-the-middle attack test-bed investigating cybersecurity vulnerabilities in Smart Grid SCADA systems,” International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012), Hangzhou, 2012, pp. 1-8.