Osploit - A Privacy Invader RAT for Cyber Threat Intelligence

[1]Md. Amdadul Bari; [2]Sharaban Tahura Nisa; [3]AKM Bahalul Haque

[1] Student of Department of ECE, North South University
Bashundhara, Dhaka-1229, Bangladesh

[2] Student of Department of ECE, North South University
Bashundhara, Dhaka-1229, Bangladesh

[3] Lecturer of Department of ECE, North South University
Bashundhara, Dhaka-1229, Bangladesh

Abstract - Computer technology in today's world is advancing briskly. Everyone surrounding us is leaning on the internet. In the globe of the Internet where it is a form of knowledge, entertainment, the medium of communication, a place of work; and also, on the other hand, it has become harmful and pitfall place. People around the world are getting trapped by the hackers, framed by predators in our day to day life. Cyber-crime is increasing on enormously these days. To prevent cyber-crime throughout the country we developed a spying software called Osploit which is a trojan horse. Trojan is a type of malicious code or software that looks legitimate but can take control of one's computer. Trojan is designed to spy on the victim's computer, access files or to extract sensitive data. The trojan can be used for both good and bad purpose. Osploit Trojan is beneficial for law enforcement intelligence, child monitoring, employee monitoring so on. Trojan is used for unethical activities such as hacking, bank robbery, and stealing personal data.

***Keywords*-Trojan, Spying Software, Monitoring tool, Cyber Crime, Attack**

1. Introduction

Technology is developed by people to improve the quality of human lives. In this modern age, we all are using technology in many various ways. People around the world, nowadays, are getting more dependent on the internet as the world scale usage is rapidly fattening in the in the globe of the internet. Starting from education to business purpose, working on the organization to bank, from adult to child entertainment, transferring money or gift; people are relying and working on the internet. Each and every one surrounding us is leaning on the internet.

Everything around the globe has both bright and dark sides. Internet has many bright sides in our lives. However, we can't ignore the fact that there are dark sides too. Somewhere internet is being used to give knowledge or a source of someone's income; whereas somewhere it has also become a source for someone as a place for robbery, hacking or a place of cyber bullying.

Every day a large number of people are getting trapped in the world of internet. Our goal is to create a safe environment in the cyber world. There are people in the world of the internet who are misusing it in the cyber world in their daily life to make others' lives miserable. In order to catch the criminals, we developed a spying software called Osploit Trojan. Osploit is a Trojan horse which spies on the cybercriminals on the internet. Our software will spy and record each and every movement of the criminals. Osploit Trojan is made basically for law enforcement intelligence so that via our software they can monitor every activity of the criminals in the cyber world. In a nutshell way, we can say a Trojan horse or Trojan is a type of malicious code or software that looks legitimate but can take control of your computer.

A Trojan is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network [1]. Cyber-criminals use Trojans to spy on the victim user, gain illegal access to the system to extract sensitive data. [2] Osploit is a Trojan designed to spy on the victim's computer, access files or to extract sensitive data.

2. Recent Attack of Trojan:

Trojan attacks are increasing day by day. Almost all the Trojan attacks are done by cybercriminals. The following

Copyright (c) 2018 International Journal of Computer Science and Network. All Rights Reserved.

figure shows that the number of trojan attack increases dramatically in 2018.

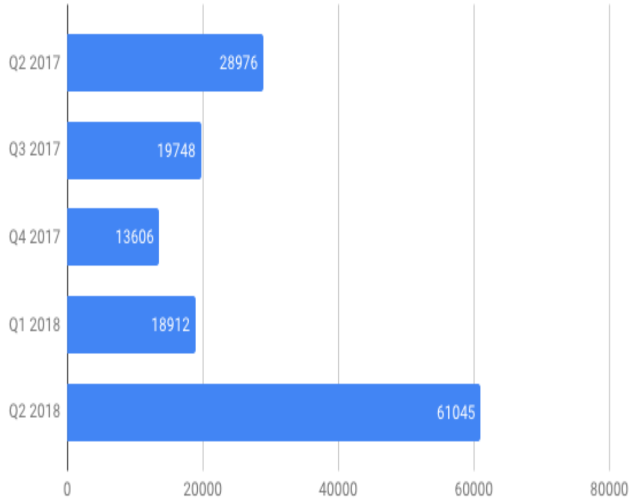


Fig 1: Mobile trojan detected by Kaspersky 2017-2018 [3]

The nature of malware attacks are much more sophisticated than other type of cyber-attack. One of the big portions of malware attack is belong to trojans. Trojans attacks are increasing and this trojans are also detected by anti-viruses.

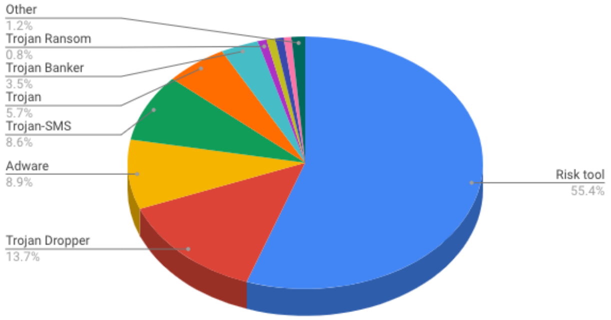


Fig 2: Newly detected mobile apps, Q2 2018 [3]

3. Technology used for Osploit Trojan:

For making Osploit Trojan we have used four technologies. The protocol which we have used for making Osploit Trojan is MQTT (Message Queuing Telemetry Transport) we have used MQTT because it is designed for devices which run on low bandwidth [9]. Fundamentally is a published/subscribed protocol. It allows clients to connect as a publisher, subscriber, or both. To make the trojan undetectable by antiviruses we need a protocol that consumes low bandwidth and works in a pub/sub model. MQTT fulfills both of this requirement, that's why we have chosen it.

We have used the framework "Spring Boot" to implement the backend.

The language which we have used for making Osploit is "java language".

For Database, we used MySQL. It is a relational database management based on SQL structured Query language. MySQL is used for storing information. We used MySQL for our software because it has a lot of advantages such as for data security MySQL is globally renowned for being most secured and reliable, it gives a high and flawless performance and many more. [10]

The main four Technologies used for Osploit are:
Protocol: MQTT
Framework: Spring Boot
Language: JAVA
Database: MySQL

4. System Architecture:

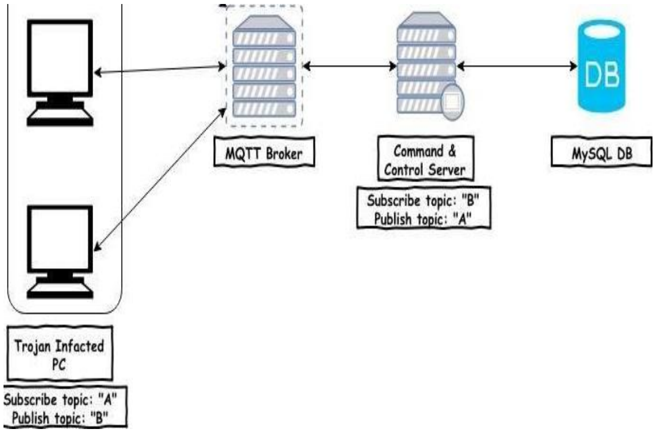


Fig 3: Architecture of Osploit Trojan

When a pc gets infected by the Osploit trojan, it opens a connection and subscribes to an MQTT broker in a particular topic. The command and control center server publish command on the topic which the OSploit trojan has subscribed to. OSploit gets the commands from subscribed topic and execute the command on targeted pc and publishes back the result in a topic where the command and control center server are subscribed. By this

Copyright (c) 2018 International Journal of Computer Science and Network. All Rights Reserved.

way, Command and Control Center server sends the command and receives the results. After receiving the result, the server stores the result in the MySQL database and the command and control center dashboard fetches data from the database and visualize those data.

5. Features:

5.1 Key stroke:

Osploit is able to capture the keystroke of any windows machine. Keystroke logging is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. The keystroke can then be retrieved from the command and control center.

5.2 Webcam capture:

Osploit can capture pictures using the webcam of victim's computer while the user is using computer without his or her permission. Osploit is able to take picture of the user and send it to the monitoring person. This feature works in every java installed machine.

5.3 Screenshot capture:

It can also capture screenshots. While the victim is browsing any website or working on the computer, Osploit is able to take screenshot. Interestingly Osploit does not allow the user to know that a screenshot has been taken. Osploit is able to send the screenshot to the controlling person after taking the screenshot.

5.4 Microphone Record:

It can record the auditory surroundings using a microphone and can send that to the command and control center.

5.5 Command Executor:

Osploit has a module which can execute system command directly. It is the most powerful feature that Osploit has. Basically, this feature can give full access of target PC to command and control center.

5.6 Undetectable:

This trojan horse is fully undetectable by antiviruses. We have tested it in virustotal.com and found that no antivirus detects it.

6. Benefits of using Osploit Trojan:

6.1 Child Monitoring:

In this generation we can't think of a day without using internet. Somehow Internet has become our daily necessity of life. Children starting at the age of one are given mobile tablet by their parents to watch rhymes so that they don't cry. Internet can entertain and educate children but it can be a place of danger for them too. By using different applications, they make unknown friends and share personal information, they trust a fraud without even knowing them which can put the child and her family into danger. While browsing the internet, children may enter pornography site without the knowledge that it can put them into uncomfortable situations. [9] Nowadays children are getting framed by online predators, they are being bullied online, they are being sexually assaulted in the world of internet. [10] Using Osploit Trojan, we can now monitor what our children are doing in the virtual world. We can control them and protect them from the harmful websites and evil person in the internet world through Osploit Trojan.

6. 2 Employee Monitor

When in an office or a company you have more than 100 employees, it is quite impossible to monitor each employee weather or not they are accomplishing their tasks. Sometimes it happens that someone in the office is sharing the confidential information to another one which sometimes causes huge loss to the office. By using our Osploit Trojan, the admin of the office or Organization can monitor each employee. Admin can spy and control each and every movement of the employee without having the employee getting any idea that he is being monitored by his admin.

6.3 Intel collection

Internet has become an enormous medium of communication throughout the world which include, thieves, hijackers, auction fraud, sweepstakes, various Criminal sources of communication too. [5] In our daily life, the criminals are trapping many innocent people in many ways in the virtual and real world. Through Osploit Trojan we can monitor the movements of the criminal very easily. It is possible to monitor their conversation and know about their next plan to trap another innocent life by catching the criminal's red handed without having their knowledge. Osploit trojan can save many people's life from harm on cyber world starting from hacking to robbery, this not only saves people in virtual life but also

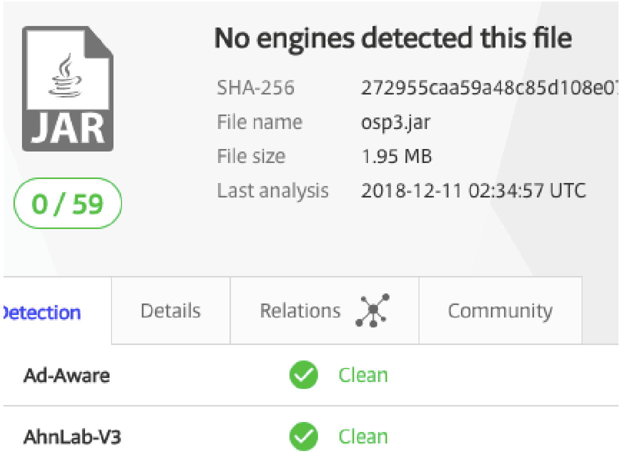
Copyright (c) 2018 International Journal of Computer Science and Network. All Rights Reserved.

in real world too. Our Osploit could be very useful for the law enforcement intelligence to catch the criminals in the cyber world and real world very easily.

7. Why Osploit Trojan is Undetectable:

Osploit Trojan cannot be detected by any sort of antivirus on any computer. User will never be able to know that all the works he is doing on the computer is getting tracked and recorded through our osploit. OSploit uses very light weight protocol MQTT to communicate and runs only one service in background. Beside it encrypts the data and then send it to the server.This things makes this trojan undetectable.

We have tested it on virustotal.com to make sure whether or not our virus Osploit Trojan can be detected by any antivirus. [11] The result is shown below in the picture shows that none of the antivirus was able to detect Osploit Trojan



No engines detected this file

SHA-256 272955caa59a48c85d108e0

File name osp3.jar

File size 1.95 MB

Last analysis 2018-12-11 02:34:57 UTC

0 / 59

Ad-Aware ✓ Clean

AhnLab-V3 ✓ Clean

Fig 4: Virus Scan Result of Osploit Trojan

8. Conclusions

Every year several successful cyber-attacks and countless attempts are taking place. In the expanding world of Internet, we need to be alert and protected from cybercriminals. We cannot always protect ourselves from evil people of the cyber world. However, if we get trapped, Osploit Trojan can easily track the vile or the hacker instantly. Osploit Trojan is a fruitful software for law enforcement agencies for tracking down criminals.

Acknowledgments

We sincerely thank Mr. AKM Bahalul Haque for his guidance and encouragement for carrying out this project.

References

[1] What is a Trojan? Is it a virus or is it malware? https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html

[2] What is a Trojan Virus? | How to Prevent Trojan Horse Virus Attacks https://enterprise.comodo.com/what-is-a-trojan-virus.php

[3] IT threat evolution Q2 2018. Statistics https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/?fbclid=IwAR0aKeuBDlJf67Vsm8vCFmI-HF8Cl937SIoI1oq_fr5y6Hm8WdsOUKfR8_w.

[4] How Online Fraud Alerts Work https://computer.howstuffworks.com/how-online-fraud-alerts-work1.htm

[5] MQTT http://mqtt.org/

[6] A Comparison Between Spring and Spring Boot | Baeldung https://www.baeldung.com/spring-vs-spring-boot

[7] Major Advantages of Using MySQL https://www.datamation.com/storage/8-major-

[8] advantages-of-using-mysql.html

[9] Child Monitoring https://www.bbc.com/news/technology-30930512?fbclid=IwAR0DSOnbpRA15GEoJ8UvwUUEabv1ugIBCn47Bztjir6CLqtE6w1--OKyBw8.

[10] Child Monitoring https://www.bbc.com/news/technology-30930512?fbclid=IwAR0DSOnbpRA15GEoJ8UvwUUEabv1ugIBCn47Bztjir6CLqtE6w1--OKyBw.

[11] Virus total.com https://www.virustotal.com/?fbclid=IwAR1TqsY4aa99zYJKj01lrxQz68StnJKIx_pwyWoXK8HKJmKdtBWxllN-kas#/home/upload

First Author: Md. Amdadul Bari is currently pursuing his Bachelor of Science in Computer Science and Engineering in the Department of ECE, North South University, Bashundhara, Dhaka 1229. He has one published paper in International journal. His area of interest is Cyber Security & Vulnerability Analysis. He has 3 years' experience as a Cyber Security specialist.

Second Author Sharaban Tahura Nisa is currently pursuing her Bachelor of Science in Computer Science and Engineering in the Department of ECE, North South University, Bashundhara, Dhaka 1229

Third Author: AKM Bahalul Haque is currently working a Lecturer of Department of ECE, North South University, Bashundhara, Dhaka 1229. He has achieved is M.Sc. in Information Technology from Germany, 2018. He achieved his Bachelor of Science (Engineering) in Computer Science and telecommunication engineering in 2014. Has published two of his papers in International Journal. He specializes in Cyber Security, Cloud Computing, Data Privacy and protection. He has one-year experience as Security Engineer and one-year experience as Vulnerability Detection Consultant in Cyber Security Division. He worked for Security Manager for almost a year.

Copyright (c) 2018 International Journal of Computer Science and Network. All Rights Reserved.