iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 Issue: V Month of publication: May 2019

DOI: https://doi.org/10.22214/ijraset.2019.5234

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Self Propogating Malware with Varying Signature

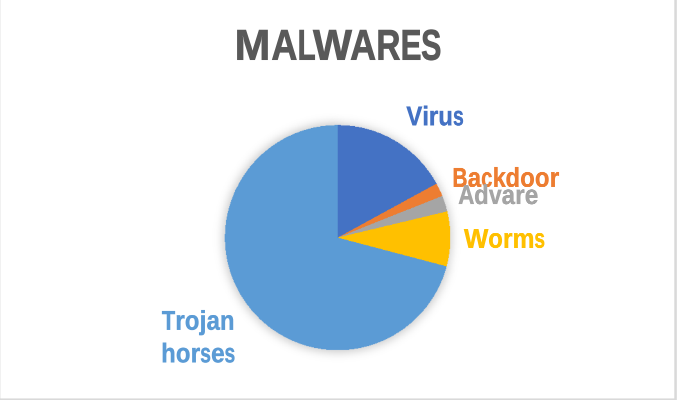
Mr. Subarna Panda[1], Mohammed Aseel. P. K[2]
[1]Asst. Professor, Dept. of MCA, School of CS & IT, Jain University, Bangalore, India
[2]MCA (ISMS, School of CS & IT, Jain University, Bangalore, India

Abstract: Malware is different from normal programs in a way that they most of them have the ability to spread itself in the network, remain undetectable, cause changes/damage to the infected system or network, persistence. They have the ability to bring down the machine's performance to knees and can cause a destruction of the network. Consider the case when the computer becomes infected and is no longer usable, the data inside becomes unavailable these are some of the malware damage scenarios. Malware attacks can be traced back to the time, even before the internet became widespread. As malware attacks become more frequent, attention has begun to shift from viruses and spyware protection, to malware protection, and programs that have been specifically developed to combat malware. Most of the malwares are detected by anti-malware programs since expected outcome won't be delivered. Python is an interpreted language, making it cross-platform, similar to other architecture-neutral bytecode-based languages. Therefore, it is one of the most popular programming languages used in wide ranging domains. In general, a malware tries to infect as many devices as possible while avoiding detection for as long as possible. Most antimalware programs scan for malware by looking for known signatures of malware. When a new malware is discovered, it is fingerprinted and added to the malware definitions database. Programs have a fixed signature after they are created. But there are various methods a program can alter its own signature. Such methods can be used by a malware to evade signature-based anti-malware programs. This project intends to program a malware that periodically alters its own signature

Keywords
Python: A computer programming language
Redbaron: A library file in python
Malware: Any malicious piece of code which harms a computer
Hacker: A hacker is someone do harm or steal data using technology

I. INTRODUCTION

Malware is any piece of software which is intended to cause harm to your system or network So, the malware tries to infect as many devices as possible while avoiding detection for as long as possible. When the victim interacts with the infected file the malware will get infected to the secondary memory of the victim's PC then passes the antivirus scan with the help of mutator by changing its own signature. Then the malware checks for the target files and propagate in victim's PC. Then the malware helps the attacker to transfer the file through internet to the attacker's machine. This project will help ethical hackers to reside their malware to a victim's system undetected. Since the malware is undetectable hackers can do reconnaissance or perform hacking using the same malware. Main motive is to create a malware which vary in their signature periodically. So that malware doesn't get detected by anti-malware programs. The below figure represents the infection of various malwares. Among them trojan horses infects almost 70% of the systems. Meanwhile virus infects 16% of the systems and the rest by other forms of malwares.



II. PROBLEM DEFENITION

Most of the malwares gets detected by either their behavior or their signature. Ethical hackers can get traced or they can't retrieve expected outcome because of anti-malware programs. Anti-malware program scan and detects then erase all files of malware. So that attacker cannot succeed the operation at the victim's system. In order to overcome this problem, the above-mentioned malware will be very useful to ethical hackers.

III. SCOPE OF THE PRODUCT

Development of this project will help ethical hackers to reside their malware to a victim's system undetected. Since the malware is undetectable hackers can do reconnaissance or perform hacking using the same malware. Most of the malwares are detected by their appearance or their behavior, here by changing the signature of the malware will make it very hard to detect and erase the malware from infected system. Varying its signature periodically will help the attacker to finish their task undetected. This malware gets infected to the files and transfer data to the attacker via internet.

IV. PROPOSED ARCHITECTURE

Malware loads from secondary memory (hard disk) and reads its own source code from hard disk and modifies its signature so that it has a different signature (mutator) and then writes it back to the hard disk which can replace the already running process to make it look like a different process , info collector collects information about the host that will be used by the attacker , hostfinder tries to find out which host to affect next , infector get the details about the next host to affect and infects it, the data transmitter sends the collected data back to the attacker

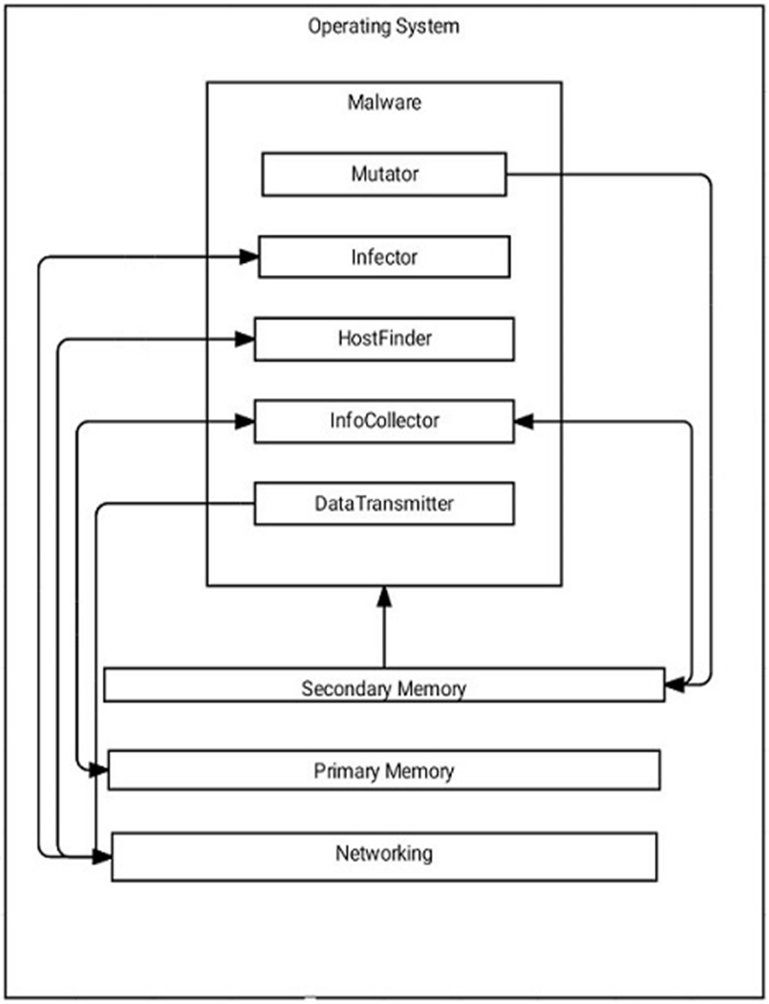


Figure 1: System architecture

V. UNITS

1) *Mutator:* Mutator helps the malware to mutate itself into a malcious program or the actual form of it , what it is meant to be as a malware. Once the malware gets into the system it passes the anti-virus check as a normal program because initially it acts as a normal program then the mutator mutate the program into malware and infect the system. After infecting the malware collect desired information from the victim’s machine and send it to the attacker.
2) *Infector:* Infector has the payload to infect a targeted system. It shows its malicious behaviour once the program mutate itself after the anti-virus check. Meanwhile it acts a normal program inorder to hide its behaviour. Then the infector unwrap itself and helps the attacker to find information in victim’s system and also helps it to send the file remotely. Infector plays a vital role in this malware and hiding it is really a challenging job.
3) *Hostfinder:* Hostfinder helps he malware to find the path where it has to go and move according to the path which has shown by the attacker. So here hostfinder has to search the target system then move to the specific system. Hostfinder will be connected to the internet inorder to find its target, then only hostfinder can complete its job succesfully.
4) *Infocollector:* Infocollecor helps the attacker to collect information from victim’s system. It acts a carrier of information which needs to be collected. Infocollector needs network to complete its job succesfully. So infocollector will be connected to the secondary memory as well as the internet inorder to communicate.
5) *Data Transmitter:* Data transmitter helps the malware to transmit data from victim’s system to attcker’s machine. Data transmitter is connected to the primary memory as well as the network inorder to transmit the data. It has the job to be sneaky and stealthy while transmitting the data. Once the data transmitter finishes its job the overall purpose of the malware is done.

All the above features collectively the malware is built. Its string mangling ability and self propogating ability makes it more interesting for ethical hackers. Using various libraries of python the malware is build. Redbarron library is used for its signature variation once the anti-virus detects it. Another feature of the malware is its varying signature when it gets caught. The malware changes its signature own its own with the help of the redbarron library.so the anti-virus detect it as a different program than before. So even the victim find the behaviour of the virus through the logs , according to the system the program has been eliminated from the system. Meanwhile the malware only changes its signature and continue doing its job.

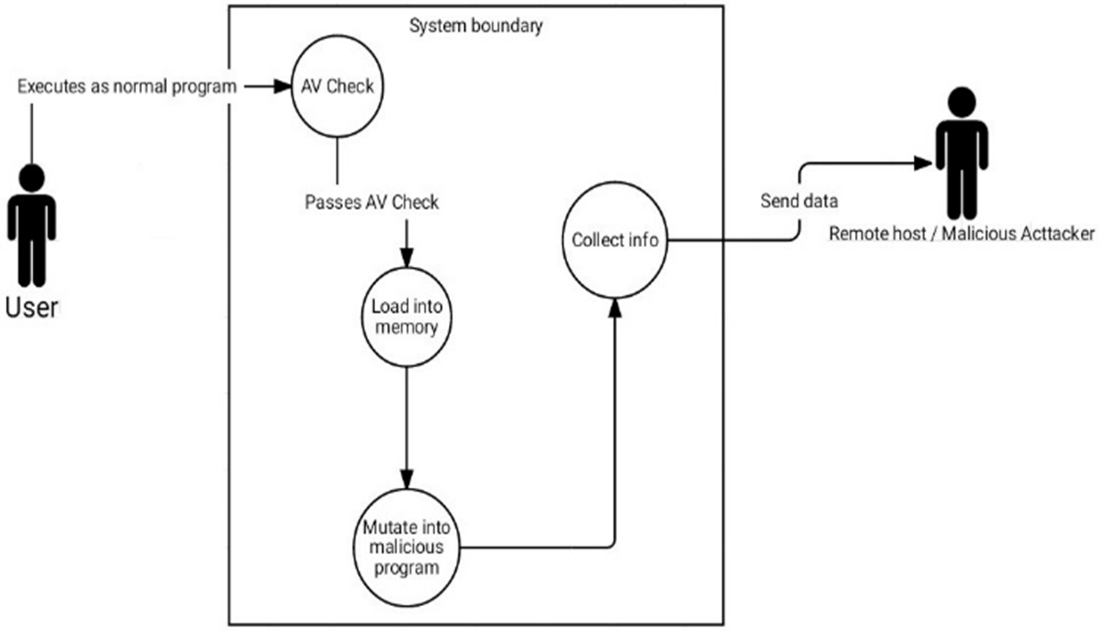

System boundary
Executes as normal program
AV Check
Passes AV Check
Load into memory
Mutate into malicious program
Collect info
Send data
Remote host / Malicious Acttacker
User

Figure 2: Use case diagram

The above diagram illustrates how the malware behaves when loaded into a system. The malware executes as a normal program, then proceed for anti-virus check. Here the malicious behavior of the malware is hidden because of its mutating nature. After passing through the anti-virus check the malware mutate itself into malicious program. Being a malicious program, it collects and send data to the attacker who is remotely connected to the victim’s machine.

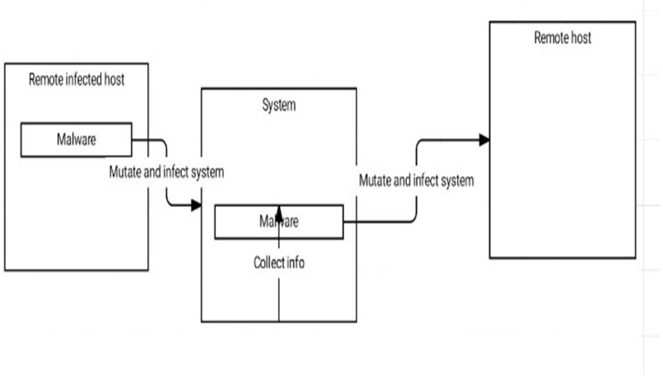


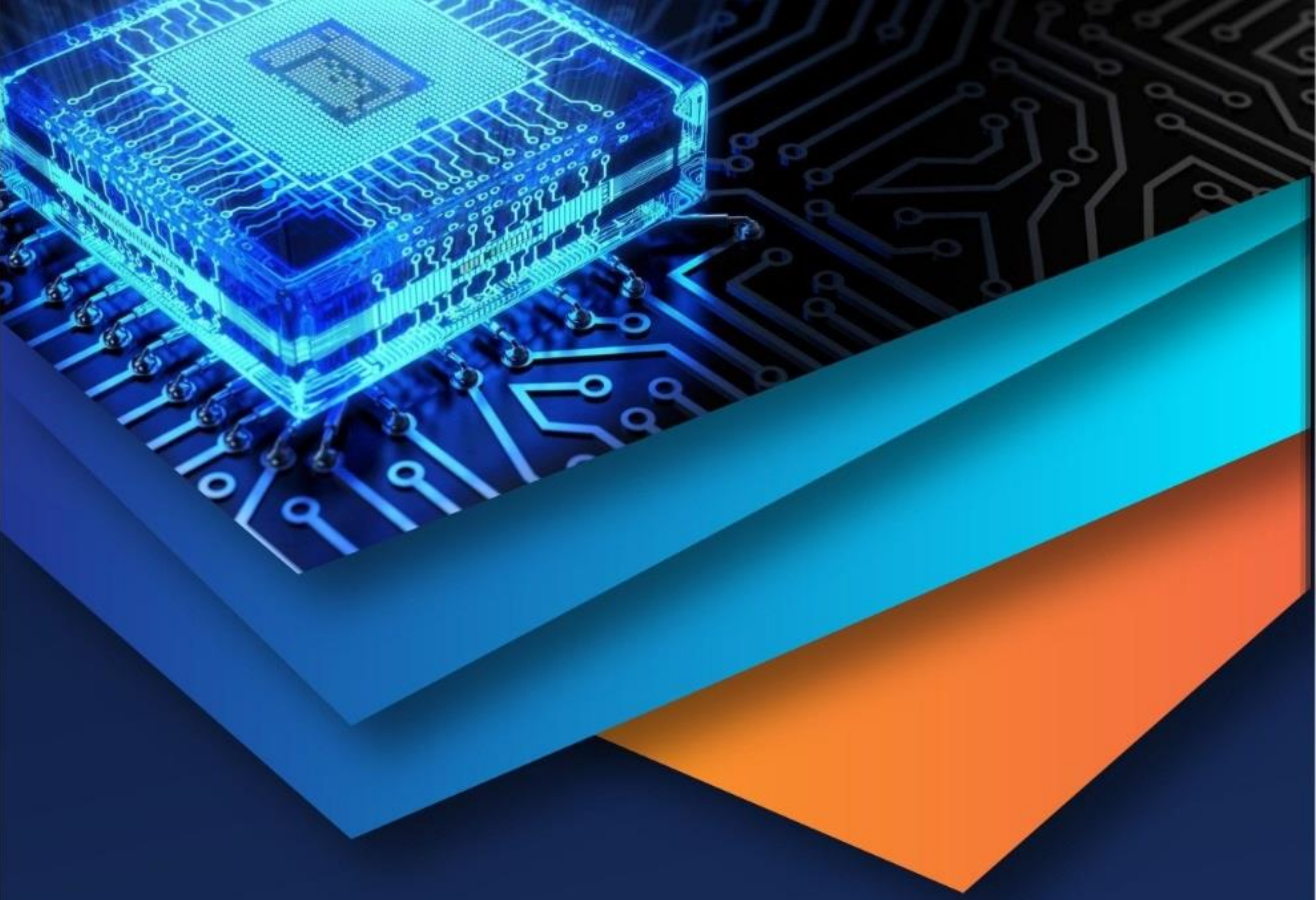
Figure 3: Context diagram

VI. COCNLUSION

In this paper it is clearly explained how a malware can affect a system and how to execute a malware without getting detected by the anti-virus software. The malware is coded in python with the help of various libraries embedded in it, like redbaron for mutation. Hence the malware affects the victim's system and gives access to the victim's system via internet. So that the hacker can collect required information from the victim's system.

REFERENCES

A. Research Papers
[1] A Case Study in Malware Research Ethics Education: When Teaching Bad is Good
[2] A Case Study in Malware Research Ethics Education
B. Web References
[1] https://ieeexplore.ieee.org/document/6957276
[2] http://www.ieeesecurity.org/TC/SPW2014/papers/5103a001.PDF-0-09
[3] http://www.github.com
[4] https://docs.python.org/2/library/
[5] https://pypi.python.org/pypi/
[6] https://code.tutsplus.com/tutorials/
[7] https://www.geeksforgeeks.org/socket-programming- python
[8] http://www.pythonforbeginners.com/os/pythons-os-module
[9] https://stackoverflow.com/
[10] https://www.us-cert.gov/publications/virus-basics
[11] http://ieeexplore.ieee.org/document/7979312/
[12] http://ieeexplore.ieee.org/abstract/document/1407486



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY