International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 11 | Nov 2020 www.irjet.net p-ISSN: 2395-0072

ADVANCED SYSTEM CHECKER

Vishnu Rai[1], Dr. Amita Goel[2], Ms. Nidhi Sengar[3], Ms. Vasudha Behl[4]

[1]Vishnu Rai, Student, Dept. of Information Technology Maharaja Agrasen Institute of Technology New Delhi, India
[2]Dr. Amita Goel, Professor, Dept. of Information Technology, Maharaja Agrasen Institute of Technology, New Delhi, India
[3]Ms. Nidhi Sengar, Assistant Professor, Dept. of Information Technology, Maharaja Agrasen Institute of Technology, New Delhi, India
[4]Ms. Vasudha Behl, Assistant Professor, Dept. of Information Technology, Maharaja Agrasen Institute of Technology, New Delhi, India

---

Abstract - *"As we have come to realize, the idea that security starts and ends with the purchase of a prepackaged firewall is simply misguided." – Art Wittmann(Vice President, Business Technology Network)*

The extensive use of machines and softwares is increasing day by day, minute by minute which is making cybersecurity more and more important. We are moving forward to a time where many of the people will be doing most of the official work from there personal computer as world is shifting towards work from home and BYOD(bring your own device). There is a serious need to keep a check of your systems and the systems that you are accesing and using. Having said that there aren't many ways to do it and there is an emerging need of a file or application which keeps you and your systems in check.

1. INTRODUCTION

There is a constant increase in the use of electronic devices and internet in today's world. Everyone nowadays uses technology and internet in one way or other, for one reason and other. The internet use is having a huge escalation and it is not turning back any time soon. We all know that if we are using internet, we are not just accessing the data available on internet we are being vulnerable to our data being erupted or attacked. Another thing with internet is that it changes continuously and sometimes dangerously stop these vulnerabilities and we need to keep our systems at a check. Also, as we all know that we are all heading towards a time where major organizations will be shifting a lot of their work to work from home and therefore most of the attacks will be on personal computers and thus the need to secure the personal computers will be more than ever. Kali Linux is one Debian-based Linux distribution for advanced Penetration Testing as well as Security Auditing. Kali Linux contains around hundreds of tools which are geared for various information security tasks, For example: Penetration Testing, Computer Forensics, Security research and Reverse Engineering. It is developed, funded and maintained by Offensive Security, an information security training company. Bettercap is a linux tool used by security researchers and reverse engineers. It is a very powerful tool which offers an easy to use, all-in-one solution with all the features they might possibly need for performing hacks and attacking Wireless networks or Ethernet networks. The major feature which shall be brought to notice is a caplet file which can be downloaded from the internet. A caplet file is a file which contains a set of codes and instructions written and developed by a cybersecurity professional for doing certain tasks. Different Information Technology professionals upload different caplet files. The caplet file that is the main focus of this project is created by me that shows and describes each and every connection and threat your computer or device may have.

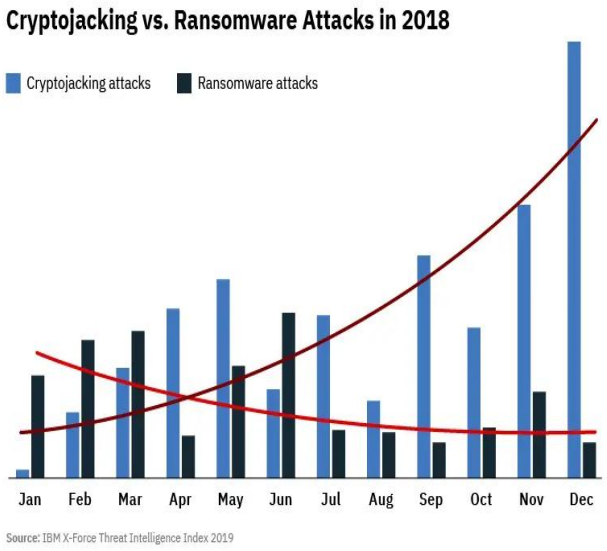
2. LITERATURE REVIEW

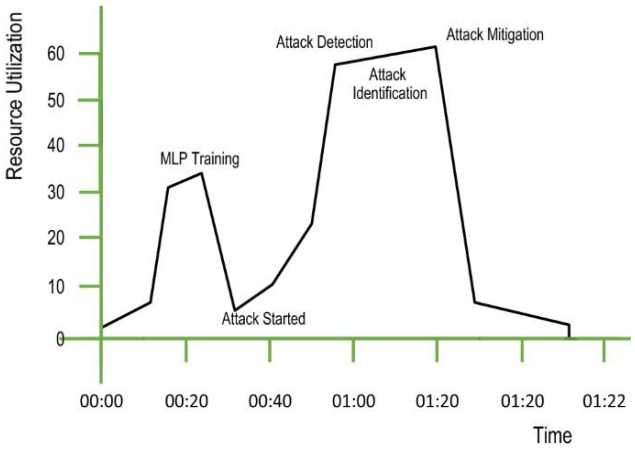
In my research I found different types of cyberattacks – big and small, infamous and unfamous orthodox and unorthodox, organizational and personal, carried out by whitehats, blackhats and greyhats, some of them were even carried out for fun. Following are some attacks which I think shall be brought into notice for the better understanding of this report. Also, I would like to bring into the notice that I am not the first to write about these incidents and they have been published at a lot of places. If you want to be a successful cybercriminal, you have to be very creative. It is not uncommon for cybercriminals to use social engineering or impersonate others. In one attack, a cybercriminal impersonated a bank CEO. The criminal was able to convince an employee at the bank to change all the information of the CEO with that of the hacker. After several months of the CEO not receiving any salary, the bank realized that they had been hacked. You have to admit, it's quite funny while still scary at the same time. In another story, a hacker caused a lot of chaos in a hotel. The attacker used hacking tools to bypass electronic doors in the hotel. Some customers were convinced that they were being haunted and the hotel went into a frenzy. The hacker used these tools and techniques to get into hotel rooms. Although the burglar was caught, it proved the vulnerability of electronic doors. So you have to be careful every time you go to a hotel—you never know who might walk in. The year was 1999. Jonathan James was 15 at the time but what he did that year secured him a place in the hacker's hall of fame. James had managed to penetrate the computers of a US Department of Defense division and installed a 'backdoor' on its servers. This allowed him to intercept thousands of internal emails from different

government organizations including ones containing usernames and passwords for various military computers. Using the stolen information, James was able to steal a piece of NASA software which cost the space exploration agency $41,000 as systems were shut down for three weeks. According to NASA, "the software [purported to be worth $1.7 million] supported the International Space Station's physical environment, including control of the temperature and humidity within the living space. "James was later caught but received a light sentence due to his young age. He committed suicide in 2008 after he was accused of conspiring with other hackers to steal credit card information. James denied the allegation in his suicide letter. Kevin Poulsen is famous for his work in hacking into the Los Angeles phone system in a bid to win a Ferrari on a radio competiton.LA KIIS FM was offering a Porsche 944 S2 to the 102th caller. Poulsen guaranteed his success as he took control of the phone network and effectively blocked incoming calls to the radio station's number. He won the Porsche but the law caught up to him and he was sentenced to five years in prison. Poulsen later became the senior editor for IT security publication, Wired News. These were examples of attacks on corporations and companies but now let's have a look at few personal attacks about which this report is majorly concerned about as we all know this ongoing pandemic (COIVD-19) has shown us that the world can consider shifting to work from home which will ensure the bringing of personal computers into the firing lines of hackers and other cybercriminals. The most common personal attack is the denial of service attack (DoS attack). In this attack the attacker once accesses a personal computer or device can perform operations like sniffing. Also, must be mentioned is that cyberattacks can very easily turn on webcams and mic of any device. Man, in the middle is also an attack worth mentioning as it is one the favorite attack of the cyberattacks as it gives them full access to any device on the network. Also, a point to be noticed is that this report won't be covering anything about common knowledge attacks such as worms and viruses as there are already so many antiviruses for them and neither bettercap or its caplet has to do anything about them

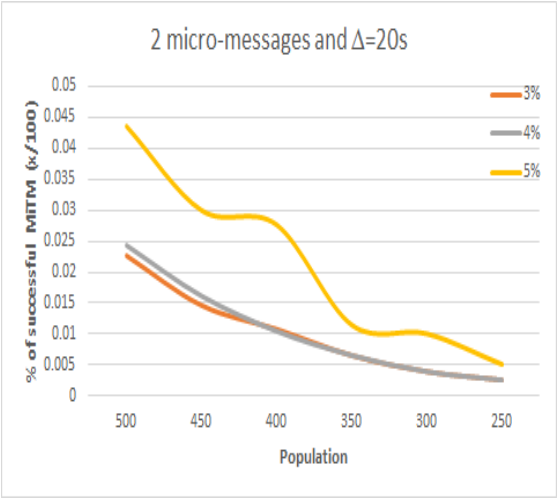
3. CONCLUSIONS

95 of security breaches are because of a human error or failing to notice the attacks and issues that are present in front of them. Some of the common issues overlooked by the users are DoS(Denial of service attack), Cryptojacking and Man in the middle (MITM). For the people who are new in Information Technology cryptojacking is hiding on someone's personal computer and mining cryptocurrencies.





Also here are some statistics for MITM and DoS Attacks



Percentage of successful MITM attacks. (a) Getting key information in 3 micro-messages; (b) Getting key information in 4 micro-messages; (c) Getting key information in 5 micro-messages

From above statistics it's clear that we need to be very careful about our computer systems. There are a lot of people aware about the antiviruses and firewalls available to stop the viruses and worms that try to enter our system. However, there are not many people aware about the codes and commands to check for the security of their system and their network. "Advanced System Checker" supported on Kali Linux Operating system is a caplet file which has all the codes and commands inbuilt with all people needing to do is run it and see everything and everyone connected to their system and whether or not someone is using their system for any malicious activity or trying of spoofing and sniffing there important data such as IDs and Passwords or some important and confidential emails. People should not take cybersecurity lightly and should make a habit of keeping their devices safe and secure as it is nobodies but their own responsibility to do so. However, the "Advanced System Checker" can surely help them sharing this responsibility as there not many easy ways to check your systems.

As mentioned previously this pandemic has shown us a lot of organisations are planning to shift all their work from home and work from home is going to become the brand-new trend of the coming time therefore the attackers will set personal computers as their primary targets and hence there will be a lot of need to be careful about people's personal computers.

METHODOLOGY

The methodology of writing the caplet file "Advanced System Checker" was done after four different stages.

First there was a detailed research on the problem faced by personal computer users and a lack of solutions for them as not everybody is an expert in computers. After the research all the problems were listed together and the try to find their solution began.

Second, all the different solutions were brought together and pros and cons for all of them were put onto the table.

Third, the best solution was selected for which user has to put in the least effort and has an easy and good implementation with no feature disregarded or dropped.

The solution was a caplet file which had all the codes already written and stored and could be downloaded from any website that it has been uploaded on.

Now, of course we know that cybersecurity is an ever-evolving field and new technologies will come bringing in new challenges as the technology won't only evolve for us defenders but also the attackers. Hence, there will be a constant need of improvements and updates to the caplets which will be taken care of.

Implementation

The implementation of the caplet file is super easy. It just requires two things Kali OS and a software known as bettercap. Other than that, not even extra space is required. All the user has to do is open terminal, and locate the caplet which will have a .cap extension. Once the caplet starts it will show the user all the connections and networks which then can be monitored by the user. The user can then see if there are any unwanted connections or processes going on with their system.

REFERENCES

1. https://academic.oup.com/cybersecurity/article/6/1/tyaa015/5905457?searchresult=1
2. https://web.archive.org/web/20200924083049/https://www.getsecurestaysecure.net/security-in-a-package
3. https://www.kali.org/
4. https://www.bettercap.org/intro/
5. https://securityboulevard.com/2019/06/top-unusual-cybersecurity-hacking-strategies/
6. https://www.arnnet.com.au/
7. https://www.cybintsolutions.com/cyber-security-facts-stats/
8. https://securityintelligence.com/cryptojacking-rises-450-percent-as-cybercriminals-pivot-from-ransomware-to-stealthier-attacks/
9. https://www.researchgate.net/