Microsoft Engage 2022

Research Paper Topic: Preventive Measures for Cyber Attacks on ITD

By- Hem Shah

Introduction:

This research paper is mainly focussed on providing an exclusive report to prevent a Stuxnet like attack on any agency in India that has an impact on most of the citizens. This report lists down all the possibilities and their possible countermeasures that one can take in case of any cyber war.

Methodology:

My Client is the Income Tax Department of India, which is a government agency undertaking direct tax collection of the Government of India. It functions under the Department of Revenue of the Ministry of Finance handling the tax returns of all the account holders in India (40% of the whole population).

ITD deals in managing and logging tax returns of all the taxpayers keeping insync with their activities in banking and other financial-related services like Loans, Investments, Securities, Accounts, Markets, etc. Any damage to its data or data theft in an cyber attack can be catastrophic to almost half the population causing a loss of more than 45 Billion Rupees. Also, any virus or trojan spread inside the network can also affect its financial connections like banks, as it resides at the centre of all the critical Infrastructure provided to the banks, resulting in damaging the whole economy.

Hence Active Cyber Defence practices have to be equipped well in advance to be able to tackle such cases if problems may arise.

Assumptions:

ITD consists of a software infrastructure which has an offline and an online presence: Offline being the central office where all the logs and tax activities are maintained in a remote database. We have to assume that all the Operating Systems used under these devices function on servers which cannot be accessed by outsiders as they are blocked by necessary firewalls.

Online is the portal and the website where the customers can access their data and make changes respectively. According to sources, we know that the portal hasn't been developed by the IT team at ITD, it has been outsourced from Infosys (Infosys-ITD). Hence it is also obvious that other softwares used by ITD are also outsourced according to their need.

Cyber Deterrence Challenges:

Insider Risk:

Insider Risk is one the most important challenges faced in an ITD which could cripple our cyber defences. We could have clients trying to bribe insiders, to find out a way to avoid tax paying. We also have to consider the possibility of attackers trying to get into the system to gain confidential data through the aid of any insider, corrupting the network where the virus can spread easily leading to a spyware installation compromising the ITD.

Zero Day Exploit:

There can also be a possibility of Zero Day Exploit when the attacker learns about the vulnerability earlier than the developer, exploiting this advantage to perform a Web Sniff using XSS or an SQL injection. It is advised to perform penetration testing to the fullest

extent before launching on the production server to minimise Zero Day Attack as much as possible.

Attribution:

Using various procedures like IP Hopping, IP Spoofing, IP Duplicacy it becomes extremely difficult to track the source of the malware. Also hackers don't typically carry out attacks from their own homes or places of business, but launch cyberattacks using computers or devices owned by other victims that the attacker has previously compromised leading to blame being sent on someone else, intending to waste time in Forensics Investigations.Hence attribution of the correct entity is a major challenge in Cyber Deterrence.

Ransomware:

There is a high chance of ransomware attack for a data leak during any counter retaliation activity where the hacker can lock the admin out of the system and ITD would be left without any choice to pay the ransom to protect the privacy of all the taxpayers

Silent Injections:

There can also be certain intrusions by hackers which are aimed only to get information about the plans to be put forward by ITD regarding any new ACT or about the data on those people which are under observation by the ITD.

Legal and Treaty Assumptions:

India currently is in a good position in the cyber space with respect to other countries. India has signed a cyber treaty with Russia which allows supporting one another in case of adversity and allows governmental agencies to start working together on counter-cyber terrorism.

India has positioned itself such that it is unlikely to be blindsided by a bilateral conversation between Russia and the United States on cyber arms control. Its agreement with Russia leaves New Delhi as the only major power to have concluded formal negotiations with both Moscow and Washington D.C

India and Israel have also signed an agreement to further expand collaboration in dealing with cyber threats amid rapid digitisation due to the coronavirus pandemic that exposed the vulnerabilities of the virtual world.

In case of any cyber attack, India will be provided with assistance from countries of major power, ready to extradite on call.

On the other hand, India is also targeted by Slovenia, Ukraine, Czech Republic, China, etc with which we don’t have any treaties signed yet. In a study it is learnt that India has been a victim of the most number of phishing mails from China.(India Attacked)

Solution Architecture and Prototypes:

Offline Data Network Compromised:

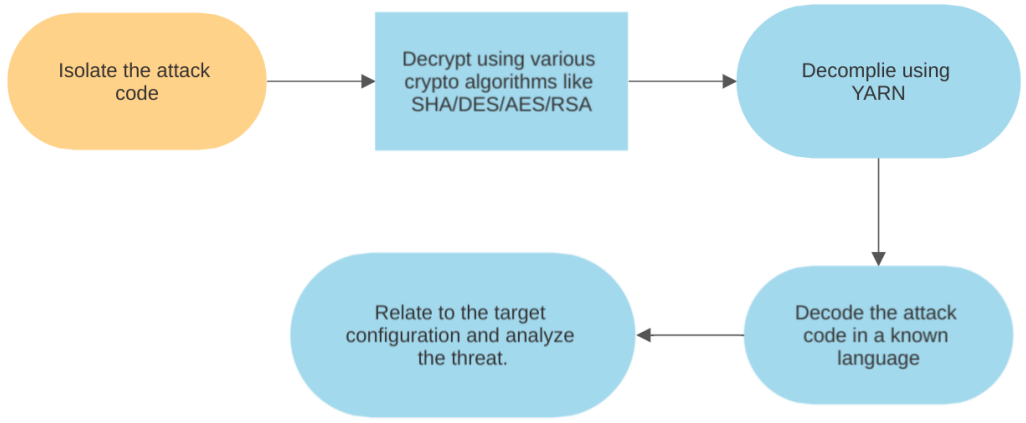
There are high chances that ITD monitoring systems present on remote servers are being attacked by Malware. Just like the Stuxnet attack we can have a worm injected along with rootkits trying to hide it, assisting in its spread across the internal network.

Solution:

To counter this we should prohibit the use of USB for data transfer as viruses can be introduced into the system using hidden files that are always present. Always prefer cloud transfer over USB in the same system along with keeping logs which can alarm incase of any foriegn activities bringing malware.

Also build stronger firewalls with a specific source, destination, port and action. All rules should be well defined earlier ensuring lesser time in debugging and handling edge cases.

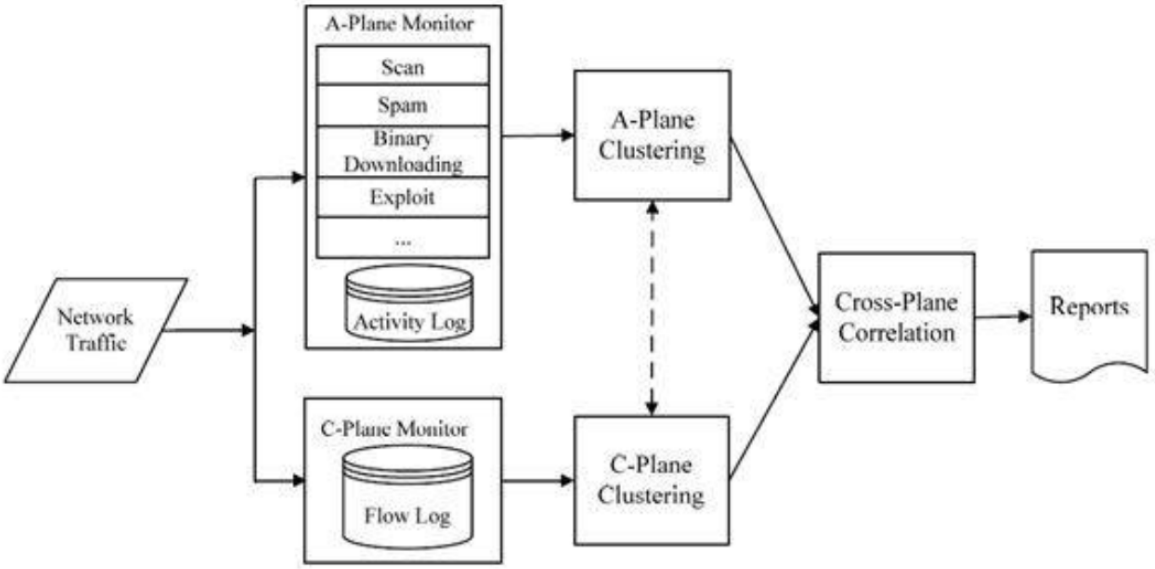
This will avoid the virus from being mutated across the network even after entering the network by breaking into one system.
Make use of a dedicated source code management system for control system code allowing for version control and rollback to a known good version when undesirable behaviour occurs after modification is made.
Incase of a malware detection using an active cyberdefense technique, start forensics and reverse engineer the attack code to understand the intentions of the hacker, giving a hint to its attribution and determining other prospective attack sites.
Passive Countermeasure Prototype:



Online Data Network Compromised:
There can also be cases when hackers could compromise the portal by gathering data by performing a successful SQL injection in which case they can get access to admin creds.
Countermeasures
Firstly Non Disclosure Agreements should be ensured between the software service agencies regarding data privacy as the portal is outsourced, we need to eliminate the risk of the attack coming from a software bug or data leak caused by the site maintainer. Regular pentesting should be performed on sites to eliminate the possibility of sniffing through cookies, XSS, SQL injections as shown here. (Security Certificates)
Secondly, predicting the site traffic using firewalls and differentiating it with Bots as the software could also be under an APT using botnets. Here Slowloris bots could cause the site to exceed ping limit and undergo a successful Distributed Denial of Service Attack.
Here we can use an ML based botnet detector like Botminer to filter out their IP's and stop their connections. Botminer is a botnet detection tool that uses a clustering algorithm, which doesn't require any training data. It's independent of protocol and structure, and requires no signature specification. Botminer monitors two planes for botnet detection: namely C-plane (C&C communication place) and A-plane (malicious activity plane).

Clustering occurs in the C-plane by finding the statistical distribution per unit time or per unit packet. Generally, a communication between a local host and a remote server consists of protocol, source IP, destination IP and destination port.

Botminer Prototype



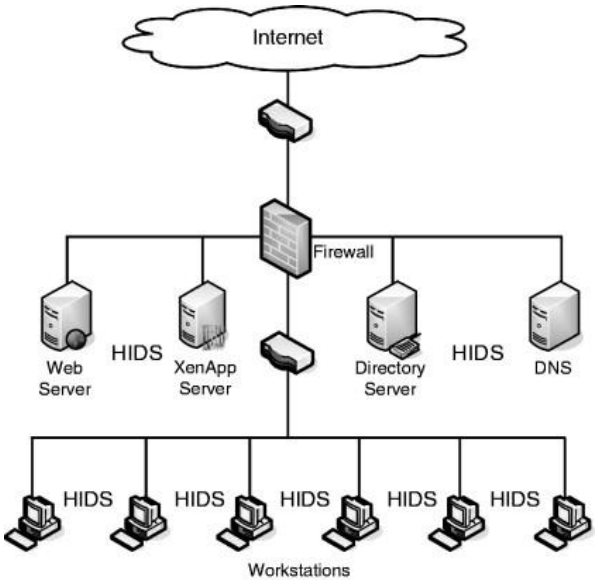
User Accounts Breached:

There have also been cases of user accounts being breached due to the presence of many vulnerabilities present in the online ITD services. This is signalled by signs of irregularities in user data caused by many queries run by the hackers to breach in for more information. This could occur in 2 cases:

1. Where we find irregularities in a single user data which could be if the hacker has an APT for that person specifically
2. There are modifications in a series of user data implying that the hacker has had control of some part of the database and we need to be equipped with counter measures to defend against such an intrusion.

Solution: Using well maintained Host based IDS services like Cisco IDS which provide ML algorithms to alarm in case of trends irregular to the anomalies. Price: $8000

Prototype:



Snort IDS can also be used incase of a network IDS as it is easy to understand and define rules. Price: Open Source

Prototype:

To run IDS based on sample rules

```
$my_path/bin/snort -c $my_path/etc/snort/snort.lua -R $my_path/etc/snort/sample.rules \
    -r a.pcap -A alert_test -n 100000
```

Adding an new rule(defined to block all pings from suspected hacker IP)

```
$my_path/bin/snort -c $my_path/etc/snort/snort.lua -R $my_path/etc/snort/sample.rules \
    -r a.pcap -A alert_test -n 100000 --lua "suppress = { { gid = 1, sid = 2123 } }"
```

Accounts hacked by phishing:

ITD has had a series of cases where accounts have been hacked using phishing mails from hackers claiming to be from ITD and retrieving confidential information from the users, compromising their own security.(ITD Phishing)

Solution: To educate all the taxpayers by sending Automated Phishing Exercise Mails: These mails help people understand the general trends in phishing and keep them cautious from being a prey to such activities. Hackers generally gain access to the system using user data when a user sends out their login credentials or discloses other private details. A sample exercise could be like this:

Prototype:

Benchmarks for Success:

Success is when our cyberdefense can catch out a malware at the correct time before it spreads and infects our entire system data.

It can be a case of intrusion detected by an IDS by observing a model deviating from its anomaly, also identifying DDOS attacks and blocking the botnet IPs.

Hackers unable to penetrate the system through any loopholes available due to an efficient firewall can also be regarded as success.

In case of any deterrence challenge, virus infiltrating the system can cause some damage but presence of a strong antivirus system alarming at the right time can help us in attribution and backtracking the malware, which would be a successful cyberdefense.