Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 7, Issue 07, July -2020

Threat Intelligence Sharing Platform

Ravi Nandasana[1]
I.T. Department,
BVM,
Vallabh Vidyanagar, India

Sagar Akbari[2]
I.T. Department,
BVM,
Vallabh Vidyanagar, India

Priyank Bhojak[3]
I.T. Department,
BVM
Vallabh Vidyanagar, India

Abstract: *The rate of security application threats is growing more and more now in days. All the information technology industry and company as well as marking companies they all need the security of their data and information. The company wants to avoid Cyberattack, data leaks. In this digital world there are many threats that have been built and hackers will continually try to hack the systems. so there is "need to share" the information of threats between security providers, IT companies as well as industries which use digital technology. There is such a type of platform which has the latest information of all threats and this platform shares this information to all their partners or customers. And also threat information is updated by the user so the platform will be up-to-date. By collaboration of this platform with your business you will know the latest threat and security scenario. This protects your business from cyber-attacks.*

Keywords *— Threat information sharing, Threat Intelligence, Cyberattack, Threat analysis, Industry analysis*

I. INTRODUCTION

As we know security is most important in this digital world. Any transaction of data, sharing information, and digital communication all need privacy. There are four terms that define security Authentication, Integrity, Confidentiality, Non-repudiation. Authentication means a party with whom you communicate is authorized or known by the sender. Confidentiality means the information is not made available for unauthorized access. Integrity deals with completeness and accuracy of data. It takes care that the receiver receives the same data that the sender had sent. Non-repudiation deals with digital signatures and digital certificates. Security attacks have been made due to threats, malware, virus, etc. There are some security terms that can be taken care of in this digital world.

1.1. Malware

Malware is a piece of code that will be used to break into a system or to damage the system. Malware attacks can affect various systems like computers, laptops, servers, websites, etc.

1.2. Firewall

A firewall is to control incoming and outgoing network traffic based on some security rules. It acts as a wall between your personal computer and remote servers, desktop, etc.

1.3. Data Breach

A data breach is the exploit or release of confidential information or code of a system or product intentionally or unintentionally.

1.4. Exploit

Exploit is that the hacker can run some malicious script and application on your computer. so your data has been leaked.

1.5. Virtual Private Network (VPN)

VPN is used as an intermediate network between the user and public networks. While accessing public networks users will be shown as it is accessing from a private network.

1.6. Virus

A virus is a type of malware that harms your data by modifying data, erasing data, corrupting data, adding redundant data, and sharing data. Also the virus will affect your OS and other application programs.

1.7. Ransomware

Ransomware is a type of malware that will encrypt the files in the targeted system. The attacker will have a decrypter that can restore original data.

1.8. Trojan horse

Trojan horse piece of malware that gives remote access of your computer to hacker. so hackers can monitor your activity and steal your personal information like your credentials, credit card & debit card information, etc.

1.9. Worm
A worm is a type of malware that will replicate codes from the system in order to transmit itself into another system or into a network.

1.10. DoS Attack
Denial of Service(DoS) attack is a cyber-attack that floods the multiple requests to the target machine and uses multiple resources of the target machine to slow down the systems.

1.11. Phishing
Phishing is to retrieve useful and sensitive information showing us it's trustworthy. It can be done by sending emails, sending texts, or directly retrieving data.

We can build such a platform that can be connected to all industries as well as business so they come to know immediately about that new security attack. The basic idea to share the threats between multiple market vendors. If possible we can share the solution of that attack.

II. PLATFORM COMPARISON AND UNDERSTANDING

2.1. Without a threat sharing platform problems in data shared?
Without any central platform or system for data sharing, It's hard to maintain the standard, and also every vendor has to maintain connections individually for all other vendors for data sharing and collecting.
For sharing data with each other, vendors are using API to access other vendor's data and can retrieve data in the form of how the sender vendor has defined it. To retrieve data from different vendors, vendors have to configure connections according to the sender requirement.
Different vendors use different data formats to store the data and also have a different protocol for connections. To retrieve or share data with multiple vendors need to process data accordingly. Because of different format standards it requires the processing of data to set according to the current system. It's unavoidable and to do that it consumes additional resources and time for the organization.
The same goes for connection protocols for different vendors, they have their protocol for connections and for accessing data resources, so vendors can't have a common template for connections and data requests. so it will require individual configuration for every vendor. As it has different methods to access data resources it sends or takes data in different standards. So for all vendors, data processing will be different, and it gonna cost additional resources and time.

2.2. How can a platform solve this problem?
The platform will be centralized and accessible by the vendors. It will be much time and resource-saving for connection between vendors because they don't have to do individual connection procedures for all vendors Once connection configuration is defined it is not required to set every time unless it changes in protocol or credential.
All data will be stored in the platform from different vendors. So it will be easily available to other vendors. The platform will update data at a particular interval for the latest data. Even if end vendor services are temporarily not available, still historical data can be retrieved from the platform.
The platform is going to have one standard format for storing data into the platform. So when vendors retrieve data from the platform it will get in the same format, even if data is of multiple vendors. When the platform will get data from senders it will process it and store it into the platform. By doing this data has to process one time only unlike the conventional system every vendor requires the processing of data. So it will save resources and time for vendors. and The main benefit will be that data will be in the same format so one conversion will work to retrieve data from all vendors unlike individual conversion requires for individual vendors.

2.3. What new challenges it creates for vendors.
In case of platform maintenance or accidentally for some reason, platform service is not available then all vendor's data transfer will be stopped. Whenever a sender vendor will change in protocol for connection or data transfer platform plugin needs to update accordingly. If the platform plugin will have bugs then all of the other consumer vendors are going to have bad data because of it so one has to very carefully need to test it because one problem can affect many vendors. The platform is updating data at a particular interval for the latest data. But if there is no data from the vendor side platform will do a request to retrieve data in case new data is there. If the platform changes in data format at that time vendors also need to change in data conversion to fit data into their system accordingly.

III. THREAT SHARING PLATFORM

Threat intelligence sharing platform is a core part of our research. Here we give access to all different users so they can share new threat information here. Also, users can decide from which vendors they want to get new threat information. Users will get new threat information from this platform. Users will get notification of the new threats as a log in their system.

In system first you need to log in with a valid credential. The proper validation of login information and security of login information is taken care of while login. Also we give users three tries to login with wrong credentials, after three unsuccessful attempts the platform will block this IP for some time and notify users about this activity by Email. With the right credentials, the user will be able to log in and redirect to the homepage of the system.

The home page of the system will show a summary of threats based on different users. In summary users can see total threats, threat sources, and threats come in the user's system last week or month. Also users can see graphs to this data as a responsive UI with dynamic value. Users can see threat sources (different vendors) status whether it is active or inactive or in a maintenance state. Users can see the top 10 Indicator of Compromise (IoC). This IoC can be a virus, malware, etc. This IoC can be filtered by its hash key, name, type, severity, etc. Users can see the number of hits done for each threat so they can know if someone is continuously trying to push a virus or threat in their system (In case of more hits) or someone tries periodically to hack the system. The home page will show the user's personal information which users are given at a time of purchase. Also users can update this information except for contact number and email because it is registered in the systems database and threat notification will be sent there.

Another module can contain the ability to add plugins by individual users for them. When the user wants to join our platform at that time we make some code based on their APIs. While we need to make sure that proper comments are code is required. Also we need to add logging logic in code for each step we can track it. After building the code we will upload is in the system. The system first checks the code and verifies it. Then it runs all the test cases. if there is some error in code then this code is not accepted. Based on the logging mechanism users will come to know about the error in code. If everything is ok then the plugin is shown in the UI. Users can upload different versions of a plugin then can be automatically updated. Once the final version of the plugin is built then there is no need to code again. This plugin refers to a particular vendor. Each vendor must configure the plugin. To configure the plugin users need to provide basic information such as API base URL, tenant name, etc. Here users can see all plugins uploaded by different vendors. Each user must provide username or password or some private information in plugin configuration so no one can miss using this plugin. Use can set API hit limit per day this is the best way to achieve protection against cyber attacks. There is some common parameter that appears in all plugins like retry count of threat fetch cycle (It has type time. periodically run this plugin and fetch new threats and virus), retry interval, the number of hits, enable SSL verification, proxy site setting, etc. The platform will suggest new requirements as well based on the vendor's requirements. A configured plugin is able to fetch data of threats. Without configure, the user can't fetch threats. When the user configures the plugin then this plugin is shown in the configured plugin tab with these details, plugin name, status, pool interval edit plugin, delete the plugin, change state, and the last run. Here status can be two types active and inactive. Poll interval is a time for each particular time plugin will run to fetch new threats. Users can change plugin configuration and delete the plugin by selecting edit plugin and delete the plugin option respectively. by delete, the plugin disappears in the configured plugin tab but still visible as an unconfigured plugin. So you can re-configure it.

Another module is that threat IoC. It is the main part of this system. the user gets new threat details here. Users can see threats name, threat type, threat value (It is in hash code), threat source (from which vendor this threat is arrived at), internal hits, external hits, reputation, and last seen (when this threat is shown last). Users can filter threats based on some conditions like name, type, source, last seen, value, comments, severity, tags, active, last seen, first seen, expire at, shared with, and tested. Also users can apply multiple of these at a time to get more specific data.

The system contains the main part known as the sharing of threats. In the threat IoC module we can analyze the threats and viruses, but in real life we don't have time to go there and filter new threats. We can use this module for some specific reason like to analyse threats frequency or particular affected vendors etc. In this module there are two field sources and targets. both source and target is dynamically populated having data of configured plugins. If the plugin is not configured then it is not shown in this field list. We need to select the source (from which vendor we want to get new things like threats, viruses, etc.) and target (new threats and viruses can be delivered in which vendor). Generally users use targets as their own systems. Because they want a threat's information in their system. The information received from different vendors is in an understandable form for technical as well as non-technical people. so to convert threats into understandable form id done by the system. When a vendor applies some threat sharing mechanism by defining source and target it will be shown in the sharing configured tab. From this tab users can remove sharing or stop receiving new information for some time. One thing is that we can set configure based on our requirements. all general threats will be shown in the Threat Ioc module. vendors will get notification on their platform only selected vendors. We can feed new threat information into the vendor system using API which resides in code on the plugin. This code helps here to show threats at specific positions of the vendor's system.

One module platform can have which contains the log of all activity occurring in the platform with consideration of that user. Reason for this module will help the user to track their side of activity occurring in the platform. In this module there will be default platform logs that will generate for platform activity and another type of log that will be generated from the plugin that the user configures. Users should not be able to change the default platform log. plugin generated log will be fully controlled by the user. Users can configure it as per their requirements. There should be different types of

the log so that users can go through according. And also can generate according to the level so that it will be easy to track the log. Ideally there should be 4 priority levels for log ex, low medium high critical.

IV. STRUCTURE OF PLATFORM

4.1. Structure of Plug-in

The below image shows the work of the plugin. Here code is written in a specific language and format. then this code is uploaded in the system. system verify this code if it is correct the system accept plugin and give an option to configure the plugin. After successful configuration on the plugin user is able to get new threat information.

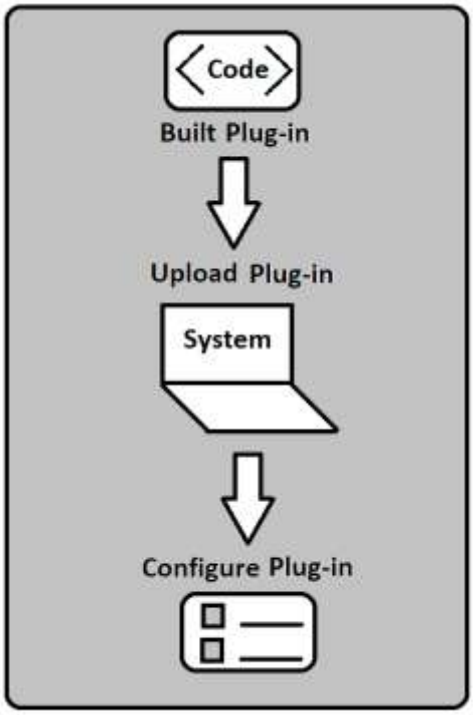

Fig 1. Plug-in working model

4.2. Structure of Sharing Threats

Below figure shows threat sharing mechanism. Here source system and Target system both have a configured plugin. vendors select appropriate source and target systems and make workflow by using a centralized platform known as our main system shown in figure.

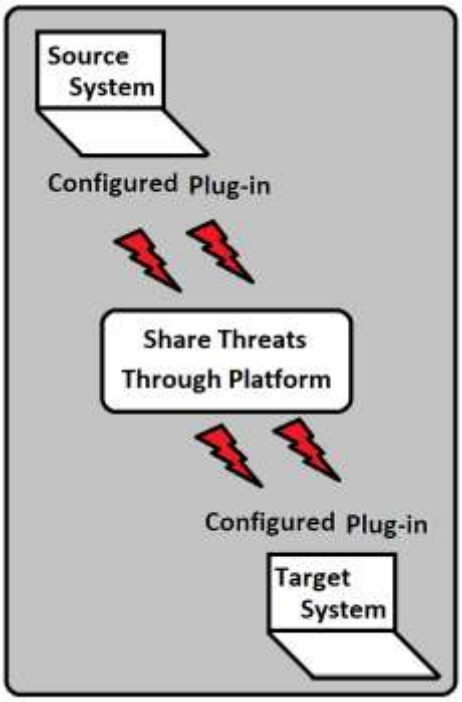

Fig 2. Threat sharing working model

CONCLUSION AND FUTURE WORK

Platform helps vendors to ease their information transfer and also convenient for configuration in case of protocol change in sharing for any vendor. It provides cleaner view and filtering in the platform. Also one format for all data is very helpful instead of different formats.

Currently the platform provides only data sharing between vendors. Future platforms might include solutions for threats. Platform can include information about suspicious threats. It can also include connections between threats so it can keep tabs on possible source of threats.

ACKNOWLEDGEMENTS

We are grateful to the IT Department, BVM, V.V.Nagar, Anand for their support and for giving essential direction concerning project development. We would like to express our deep and sincere gratitude to Mr. Priyank Bhojak sir for providing guidance.

REFERENCES

[1]. "Threat Intelligence Sharing: A Survey" research paper published at https://www.researchgate.net/ Dept of Computer Science and Engineering HKBK College of Engineering, Bangalore-India.
[2]. "MISP - The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform " research paper published at https://www.researchgate.net/
[3]. "Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives" research paper published by University of Innsbruck, Department of Computer Science, Innsbruck, Austria
[4]. "Journal of Cybersecurity" Volume 4, Issue 1, 2018 book https://doi.org/10.1093/cybsec/tyy008. Published: 13 December 2018
[5]. "Cyber Security Terms That Everyone Who Uses A Computer Should Know"https://www.cybintsolutions.com/20-cyber-security-terms-that-you-should-know/

