Research on Network Attack Information Acquisition and Monitoring Method based on Artificial Intelligence

Lei Yan, Xinrui Liu, Chunhui Du, Junjie Pei
State Grid Gansu Electric Power Company, Lanzhou, China
yanleirty@163.com, 982157601@qq.com, 15002637533@163.com, peijunjie18@163.com

2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC) | 978-1-6654-2207-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ITAIC54216.2022.9836895

***Abstract*—Cyberspace is the fifth largest activity space after land, sea, air and space. Safeguarding Cyberspace Security is a major issue related to national security, national sovereignty and the legitimate rights and interests of the people. With the rapid development of artificial intelligence technology and its application in various fields, cyberspace security is facing new challenges. How to help the network security personnel grasp the security trend at any time, help the network security monitoring personnel respond to the alarm information quickly, and facilitate the tracking and processing of the monitoring personnel. This paper introduces a method of using situational awareness micro application actual combat attack and defense robot to quickly feed back the network attack information to the monitoring personnel, timely report the attack information to the information reporting platform and automatically block the malicious IP.**

Keywords—network attack;information acquisition; Monitoring method;artificial intelligence

I. INTRODUCTION

Nowadays, mobile Internet, cloud computing, big data, Internet of things and artificial intelligence are booming. They are constantly integrated across borders with various vertical industries. Various new technologies and applications emerge in endlessly, and the problems of information security and network security are becoming increasingly prominent. With the popularization and application of new artificial intelligence technology, hackers have begun to use artificial intelligence to carry out network attacks, which not only expands the attack surface of hackers, but also allows hackers to have more attack means. In the face of hacker attacks using artificial intelligence, the best defense strategy is to use artificial intelligence and new security architecture. There are two reasons: first, with the increase of network attacks, the degree of harm has increased, and there is a serious shortage of network security professionals. Second, new forms of attacks such as "0day attacks" have increased, making it more difficult to prevent. In the daily operation and maintenance of network security, especially during the guarantee period, it is very important to judge the IP address, attack time, attack mode, attack times, attacked equipment and other information of the external network attacker more quickly and accurately, and respond quickly. This paper will introduce a method of using situational awareness micro application actual attack and defense robot to quickly feed back the network attack information to the monitoring personnel, timely report the attack information to the information reporting platform and automatically block the malicious IP.

II. IMPLEMENTATION BACKGROUND

During the network security attack and defense drill and guarantee period, the monitoring personnel usually need to pay attention to different monitoring and traceability platforms for 24 hours at the same time, further analyze emerging threats, and write express reports and reports in time. The work task is heavy.

At the same time, after a long time of work, the monitoring personnel have always maintained a state of high concentration, which will inevitably lead to relaxation and inattention. Especially during the attack and defense drill, the attacker's information and the information of the attacked equipment need to be reported in time through the information reporting platform. Before the attack, the attacker usually scans the ports and vulnerabilities of the attacked equipment, resulting in a large number of attack information reported by the traceability monitoring system, which greatly increases the working pressure of the monitoring personnel.

In addition, the working mode of conventional network security analysis, monitoring and disposal is "finding abnormalities (security equipment alarm) → analysis and judgment (manual analysis) → event disposal (blocking attack source IP / disposal of assets)". The whole working process takes a long time and requires high personal ability of security personnel. It is more difficult to complete the disposal work when dispatchers are on duty at night.

To sum up, it is necessary to make full use of collaborative defense and linkage disposal technology to build an automatic operation and maintenance platform based on the security arrangement ability, provide the

security operation ability to gather and build different scenarios with automation arrangement as the core, provide customized security services for front-end business operations, and realize "integrating security resource components and precipitating security business scenarios", Provide services for the rapid delivery and operation of security services to reduce the cost of manual risk investigation, find a way to help network security monitors respond to alarm information quickly, improve security defense in depth, and build an intelligent and proactive three-dimensional security protection system.

The first version of the company's situation awareness and noise reduction has been reported to the first version of the company's internal situation awareness and noise reduction after the application of micro eye has been completed, and the current situation has been effectively filtered through the first version of the Internet. Realize technology to technology and technology to control technology, so as to ensure the safe and stable operation of the company's network under the severe situation.

A. Basic data management

Through syslog, WebService independent collection and other data access methods, realize the data collection of various existing monitoring subsystems, integrate the corresponding security capabilities, collect, de duplicate and normalize the data, realize the governance of the existing basic data, verify the data validity and integrity, and realize "one source of data".

B. Aggregation and analysis of effective equipment and effective data

By distinguishing the existing data sources according to the functional categories, it carries out time series analysis, statistical analysis, cluster analysis, scenario analysis and other dimensions, and provides a user-defined correlation analysis window for the security personnel to adjust the analysis model in time, merge the massive and unrelated alarm data into attack events, and reduce the energy spent by the security personnel in the process of event analysis, alarm data and data forensics.

C. Event warning and intelligent linkage

In the event, through the intelligent linkage and joint defense with the firewall, automatically identify the attack entrance of the attack source, automatically identify the blocking path and the working state of the blocking node equipment in use, and carry out the IP blocking of the point-to-point attack source, so as to realize the automatic discovery and linkage blocking of the IP address of the attack source and malicious attacks (multiple attacks within seconds, complex attack rules, etc.). Afterwards, through the vulnerability and early warning platform, carry out vulnerability disposal and control, and give real-time feedback on the repair status.

III. IMPLEMENTATION METHOD

At present, the user-defined robot function carried in the nailing program supports independent programming in Java and python. On this basis, combined with the analysis results of the situation awareness platform and defense and disposal measures, the situation awareness platform, nailing program and fire wall are associated through API to build an automatic actual combat attack and defense robot, so as to realize the timely submission of alarm information and the automatic disposal of malicious IP. The specific contents include:

A. Monitoring attack information with robot program

After we get the webhook address of a nail group, the user can send an HTTP post request to this address, which realizes the function of sending messages to the group. Therefore, you only need to download and set up the robot client on the office extranet computer, write the actual attack and defense robot program, send the situation awareness micro application information to the robot, and then send it to the nail group by the robot. In the robot program, set the alarm level to be sent, the threshold of the number of attacks, and the content to be displayed in the group sent by the nailing robot. After de duplication, it can be tested and put into use.

B. Using robot program to deal with attack information

Report attack information to the information reporting platform.

If you need to report attack information to the information reporting platform, you need to set the actual attack and defense robot to send an HTTP post request to the website of the information reporting platform, and set the format and content to complete the information reporting function. After the submission is completed, you can consider setting up to send the submission completion information to the nail group to remind the monitoring personnel, which is also convenient for the monitoring personnel to identify whether there is missing or wrong information.

Realize linkage with firewall equipment for IP interception.

Conduct linkage and joint defense through firewall scheduling engine, and issue sealing and prohibition disposal tasks in combination with API or linkage tools; Automatically identify the attack entrance where the attack source is located, automatically identify the blocking path and the working state of the blocking node equipment in use, and block the IP of the attack source; Set the blocking time, which is not limited to handling according to the cycle of hour / day / week; It can be linked with the work order flow module of on duty work to carry out the security monitoring closure and prohibition IP form in daily / weekly / monthly units; The interface of firewall is developed through NETCONF interface protocol to realize the automatic issuance and deletion of security policies of business application and

internal business application system. This function uses the actual attack and defense robot program to record and store the submitted attack IP in a specific format, and then send these IP addresses to the FTP server. Netshield system will automatically identify these IP addresses in the FTP server regularly, join the intelligence base and block them.

C. Develop and apply automatic disposal tools for attack monitoring.

Data collection, weight configuration, attack source and attack type, filtering, noise reduction and comprehensive analysis are carried out in combination with the alarm of existing security equipment, and the accurate classification of attack source IP is realized in combination with the correlation analysis of internal and external threat intelligence and alarm conditions. The joint defense is carried out with the deep threat security protection gateway, and the blocking disposal task is issued in combination with API or linkage tools, Automatically identify the blocking path and the working state of the blocking node equipment in use, conduct the point-to-point attack source IP blocking, and realize the automatic discovery and linkage blocking of the attack source IP address and malicious attacks (multiple attacks within seconds, complex attack rules, etc.). Develop the actual attack and defense robot program, record and store the submitted attack IP in a specific format, and send it to the intelligence base of the network shield system for blocking and interception. Afterwards, through the vulnerability and early warning platform, the vulnerability disposal and control work are carried out, and the repair status is fed back in real time, so as to realize the centralized network security monitoring information, analysis and disposal, and form a grid network security early warning disposal mechanism and real-time command mechanism.

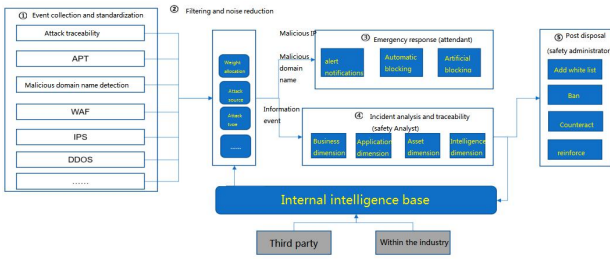

Fig. 1. architecture of attack monitoring automatic disposal tool.

Fig. 2. Artificial intelligence robot platform

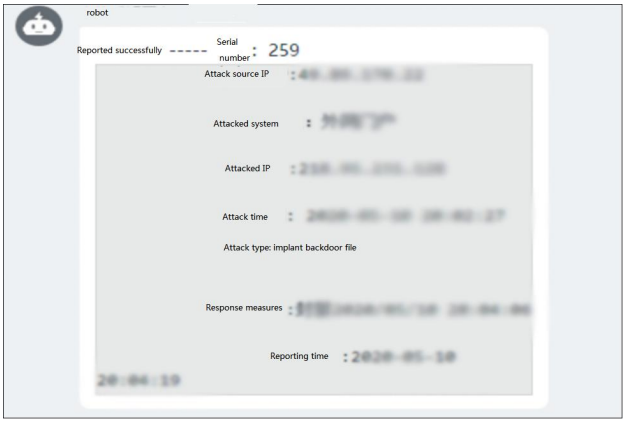

Fig. 3. Robot automatic report

IV. APPLICATION SCENARIO

In order to avoid the robot sending a lot of spam information, the nail robot can only send 20 messages per minute at most. Therefore, in order to improve the monitoring effect, de reset is carried out. When it is found in the actual application that if a large number of attack messages are submitted by the nailing robot every minute, the monitoring personnel need to verify whether there is missing information within this time period through situational awareness micro application, traceability monitoring, WAF, etc. At the same time, the applet can be debugged according to the type of information platform that needs to be reported at present, and a way to adapt to the current mainstream reporting platform can be constructed. In addition, different safety disposal processes are set in combination with daily duty scene, night duty scene and re insurance period scene to realize intelligent linkage disposal, including:

A. Daily duty scene

Daily duty mainly refers to the daily duty of safety personnel on working days in non re insurance period. Its characteristics are: there are safety personnel on duty, which can be handled through automatic / manual discrimination in combination with the types of safety events.

B. *Night duty scene*

Night duty mainly refers to the duty period of non re insurance period, which is usually assisted by the dispatcher to watch the safety system. Its characteristics are: there is no safety personnel on duty, so it is difficult to manually judge whether to deal with it at the first time, and it needs to be handled automatically according to different types of events.

C. *Reinsurance period scenario*

The re insurance period mainly refers to the duty period of the re insurance period, which is characterized by 24-hour safety personnel on duty. For different types of safety events, it is handled in combination with the blocking time and blocking equipment.

V. IMPLEMENTATION EFFECT

Through testing and practical application, the network security analysis room automatically intercepts 890124 large-scale scanning attacks, 1746867 forward attacks and 90156 reverse outreach IP addresses such as viruses and Trojans through the intelligent linkage defense system. It also collects the alarm information of security equipment, automatically sends it to the nail group, detects and blocks the network boundary, terminal, server and virtualization level, innovates the network security situation monitoring platform, intelligent linkage, whole scene situation awareness platform and automatic attack disposal tool, automatically and accurately locates the root cause of security events, and makes rapid judgment, disposal and recovery, Comprehensively support the safe and stable operation of the company's information system, improve the ability to deal with network security, and lay a solid foundation for the company's network security construction.

By applying the network attack information acquisition and monitoring method based on artificial intelligence, we can fill the non intelligent gap that the previous monitoring, analysis, disposal, tracking and tracing are all manual participation, and improve the efficiency of dealing with security events in the whole process. After establishing the linkage mechanism, we can effectively get rid of "individual combat", establish a security ecosystem, increase network flexibility and maximize business support, Conduct real-time linkage between defense equipment and analysis equipment to share intelligence in real time, so that there is no escape from the threat. When attacked by the network, the security equipment can respond quickly, intercept the spread of the virus in time, ensure the normal operation of the business system, meet the compliance requirements, effectively monitor and prevent, so that the information managers can know more about all the information in the system and the health of the system than ever before, and become passive to active, "Resist the enemy outside the gate". Achieve the intelligent and automatic disposal of the whole process of information security, such as prevention in advance, incident detection and analysis, rapid response in the event and traceability afterwards. Achieve effective early warning, timely disposal, orderly recovery and continuous improvement.

REFERENCE

[1] [6] Xiang Chengcheng Research and application of network security situation prediction method based on parallel deep forest [D] University of Electronic Science and technology, 2021.

[2] Yang Yiyue, Fu Zhibo, Xiao Xiao Analysis of power system network security architecture [J] Electronic technology and software engineering, 2020 (22): 247-248

[3] Deng Tao Research on information security protection technology scheme of power supply company [J] Communication power technology, 2020,37 (11): 154-156.

[4] Xiong Shenduo Research on information protection of power monitoring system based on regional energy Internet [D] North China Electric Power University (Beijing), 2019 .

[5] Li Yichen Research on abnormal flow detection technology of power industrial control network based on machine learning [D] Shanghai Jiaotong University, 2019.

[6] Kang Wenjie Research on Robustness Analysis and new security model of smart grid based on information physical fusion [D] National University of defense technology, 2018.