Multi-Knowledge Electronic Comprehensive Journal for Education and Science Publications (MECSJ) ISSUE (34), July (2020)
ISSN: 2616-9185

Analysis of IoT devices' Vulnerability Attack Using a Honeypot

Reham Al-thakafi

Dept. Computer Science, Jeddah University

ralthakafi@tvtc.gov.sa

prof. S.Yahya

Dept. Computer Science, Jeddah University

Sbyahya@uj.edu.sa

Dr. Amani T. Jamal

Dept. Computer Science, King Abdulaziz University

Atjamal@kau.edu.sa

Abstract

IoT (Internet-of-Things) attacks have been accompanied by attempts to exploit inherent threats leading to large scale destruction and corroborated fears about the safety of devices connected to the IoT. The emergence of any new technology will always accompanies with a variety of vulnerabilities that are ready to be exploited. In this paper,

we have proposed a method of analyzing vulnerability attacks by deploying honeypot log data to identify vulnerability attack patterns. Honeypot on an AWS cloud was used to collect cyber incident log data. The log data is analyzed by using Amazon Elasticsearch Service, Amazon Kinesis, Kibana, and POT (EKK-POT). We also aim to find new trends of threats to IoT devices by extracting logs from the EKK stack and enhance current mechanisms to face these alarming trends.

Keywords: IoT, Honeypot, Malware attacks, Cloud, Security, Botnet.

1. INTRODUCTION

Internet of Things (IoT) exploits networking, sensing, big data, and computer science technology to deliver complete systems for a product or service. However, several challenges face the widespread usage of IoT, like security, privacy, standards, interoperability, and emerging economies and development. During this paper, we perform a vulnerability scanning of IoT devices using the IoT Shodan and a honeypot for threat and vulnerability analysis.

This permits the analysis of IoT devices' vulnerability attacks using Honeypot by analyzing the vulnerability scanning results and showing how IoT devices could be easily attacked and be exposed by hackers.

A honeypot system could be a program made to operate as an actual attraction system to trick and capture the intruders who try to gain entry into the system. During this process, the invader is keenly tracked and observed, in his or her oblivion. This paper proposes using this technique to know the IoT trends and threat landscape and the way to counter them employing a honeypot.

Honeypots produce an enormous amount of data. It is not easy for general-purpose data analysis tools to analyze such amount of data. During this paper, we invoke Amazon Elasticsearch Service, Amazon Kinesis, Kibana, and POT (EKK-POT) technology to analyze honeypots data as it gives the pliability of searching on any size of data set. With the good advancements of technology, society has become greatly connected through the various devices that currently have a direct connection to the Internet. These devices have become vulnerable to attacks as indicated Matheu-García et al (2019).

There are many forms of attack that can be performed on the IoT system to make it more vulnerable, including Man-In-The-Middle (MITM), Sniffing, Denial of Service (DoS), Crypto graphical invasion, Botnet invasion, Dos attack (Denial of Service) and Distributed DoS (DDoS). The main problem with the growing technology is the fact that a huge number of devices are being joined to the global network. Likewise, many of these devices are used by individuals with very small knowledge of the technology they are using, making them extremely vulnerable to attacks and threats (Fahrnberger, Gopinathan, & Parida, 2019). Besides, it has been noticed that the security measures of systems are not expanding proportionally with the growth of the systems itself. Currently, the Internet is considered as a laboratory for hackers and exploiters to use their knowledge to their benefit, which most of the time result in harm to others (Kamesh & Sakthi, 2016). This calls for a definition of a cyber-security certification framework Matheu-García et al (2019).

The main function of the Intrusion Detection System (IDS) system mechanism is to detect and correct malicious or irregular activities in a network.

This tool runs constantly in the background and does not cause great interference in the normal functioning of the network. More recently, a new alternative began to be used involving the use of honeypots and honeynets (Spitzner, 2003).

In 1999, Spitzner linked a computer to the Internet to execute applications with clearly known exposures. The idea was to make this system act as a honey pot (from the name) to attract the attackers.

It was surprising to see that in less than 15 minutes the host had already been compromised (Spitzner, 2003).

Then the honeypot idea emerged: a network of resources to be attacked and compromised (invaded).

It meant a honeypot could be tried and invaded. By permitting such attacks, it is possible to register the events taking place in fact and then provide the necessary information on the plans used by the attackers (Spitzner, 2003).

We examined the EKK-POT over a few weeks, and data were recorded. Afterward, the logs were collected in an elastic search index, and Kibana was used to visualize the analysis-results of these data.

This Paper gives a significant amount of contribution to the IoT security landscape to invite more work in this field. Furthermore, it used EKK stack tools and makes the deployment steps clear and concise to study the data in an integrating environment with a suite of great tools for cybersecurity.

2. RELATED WORK

Cyberspace search engines such as Shodan, FOFA, and other public platforms are introduced to collect honeypots servers.

Only a section of the attacking devices of the honeypots was used to estimate the number of devices used globally and of a given type. Devoted search services such as Shodan, Censys, and ZoomEye help scan IP spectra for related services, polling them and indexing the outcomes. The search carried out for the most frequent headers, routers, and DVRs using Shodan, Censys, and ZoomEye.

Shodan was once the main search tool of the IoT before 2013 when Censys came up as the free competing tool. It also served as an IoT search engine, being dependent on the same fundamental principles. However, as the creator states, it was more accurate in searching for potential IoT vulnerabilities.

Censys provides a collection of devices that share a common vulnerability, such as the ones vulnerable to Heartbleed.

This review is available on all existing honeypot methods that scientists have improvised with time.

2.1 Honeypot Attacks

One vital condition for honeypots is their capacity to maintain undetected attacks: hiding the details of the honeypot. Shodan is a special search tool, which crawls on the Internet and tries to find linked devices such as IP web-cameras and routers (Roland Bodenheim, et al, 2014). In the progressive procedure of crawl and index, the Shodan system updates the database of all systems as well as services connected to or exposed to the Internet. Recently execution and deployment of Shodan detection mechanisms were done for the identification of honeypots. It did several probes and monitoring, and then created scores for every checked device. From the value of this score, Shodan decides if the system is a honeypot system or not.

2.2 Security of IoT application protocols

This sub-section discusses the existing circumstances and problems associated with the current communication protocols used in IoT applications and devices.

2.1.1. Present circumstances

Although the attention for the security of IoT technology is increasing, it is agreed that it still has not matured enough. The security problems for the application protocols are normally considered from three distinct aspects (Al-Shaer, Wei, & Hamlen, 2019) . Flaws in the protocol itself, troubles during the protocol implementation and vulnerabilities during the implementation itself. **Table 1** shows the security mechanisms applied in each protocol.

Table (1): Security Mechanism of IoT communication protocols

MQTT	Simple Username/password Authentication, Transport Layer Security/ Secure Sockets Layer (TLS/SSL) for data encryption
XMPP	Simple Authentication and Security Layer (SASL) authentication, TLS/SSL for data encryption
AMQP	SASL authentication, TLS/SSL for data encryption
CoAP	Datagram Transport Layer Security (DTLS) / Internet Protocol Security (IPsec)
JMS	Vendor specific but typically based on TLS/SSL. Commonly used with Java Authentication and Authorization Service (JAAS) API
Simple Object Access Protocol (SOAP)	Address by WS-Security

It can be observed that Transport Layer Security cryptographic protocol is used in MQTT, XMPP, AMQP, and JMS. Datagram Transport Layer Security is used in CoAP while WS-Security is used in SOAP protocol. Simple Authentication and Security Layer (SASL) is the most used authentication framework by these protocols.

2.2.2 Present Problems with Security of IoT

As previously stated, IoT security problems are taken from three-point of views. The Exposures of the connection protocols:

There are some security issues common with all protocols and others which are specific to a specific protocol.

First, common issues are introduced, and then the specific issues are discussed.

2.2.3 Common Problems with protocols:

The common problems include security of booting, firewall system, and security in the update and patch problems in all the protocols. For example, only authorized software applications ought to be allowed to download in the linked device. That is why precautions must be taken, such as digital signatures or keys for encryption are needed (Fahrnberger, Gopinathan, & Parida, 2019). Therefore, it is considered a security challenge with large deployment and limited resources (Maarof, Senhadji, Labbi, & Belkasmi, 2018).

CoAP:

According to Nastase (2017a) and Nastase (2017b), DTLS has a problem because its design does not match CoAP. First, DTLS cannot enable multicast. Among the weaknesses of using DTLS in CoAP or other proposals for solving the problems(Görmüş et al., 2018). Nevertheless, the plans may not be proper for CoAP and can cause security issues. More research is required.

• CoAP**:** Issues with CoAP's "NoSec Mode"

Four safety modes are brought in (Görmüş et al., 2018), with the initial one being "NoSec Mode". During this mode, there is the transmission of a CoAP message with no security methods implemented.

• MQTT**:** Issues with encryption as well as authentication of MQTT, (Salman & Jain, 2017) discusses a new protocol referred to as Secure MQTT (Singh, Rajan, Shivraj, & Balamuralidhar, 2015), which applies encryption based on "lightweight attribute-based encryption". SMQTT is different from MQTT due to the weakness of MQTT.

• XMPP**:** Issues with SASL authentication There may be possible problems with SASL authentication as explained by Melo (2013) , concerning the security factor that several SASL methods cannot provide enough safety.

Additional protective services may be required to safeguard against the attacks. In addition, XMPP uses SASL for authentication (Lehto & Neittaanmäki, 2018) .Therefore, any form of weakness in SASL is also a weakness in XMPP.

- UPnP: Known UPnP weakness

The problem with the UPnP is not a new subject. It has had lots of discussions concerning it on various publications online (Michael Mimoso, 2015)(Brewster, 2013) and in the academic area (Michael Mimoso, 2015) (Al Hasib & Mottalib, 2010). Michael Mimoso (2015) points to security weaknesses in UPnP that put millions of domestic networking tools at the danger of being compromised. (Brewster, 2013) also gives explanations on the use of vulnerabilities of the UPnP to run the attacks.

- Protocol Execution Problems:

Security issues related to development could occur during the implementation of the protocol, which includes building and installing the server. These issues could vary from bugs, weaknesses, and lack of validation in addition to other issues. Unfortunately, these issues can compromise the full execution. The weaknesses can be mapped to Common Vulnerabilities and Exposures (CVE), a database with a list of known exposures to software applications, including Operating Systems, archives, and frameworks.

The implementations can be from open or closed sources. Various databases share a common collection of CVEs identifiers describe all the present information concerning the vulnerability, including vendor, product, time, vulnerable forms, the kind of vulnerability and description (Russell & Duren, 2018) . This makes it easy to identify exploitation directions for applications on the IoT or IoT platforms with the protocols.

- Vulnerabilities When integrating with IoT:

Since IoT platforms integrate various IoT techniques and protocols to operate as a single unit, therefore, the IoT is viewed as an immature platform and is prone to several security attacks. Some specific approaches can be taken to put together, analyze, and finally identify the pattern of threats on the IoT platforms.

2.3 Types of Attacks

The different forms of invasion can be conducted by malicious users such as Port scan, MITM attack (Man-In-The-Middle) and Denial of Service (DoS). A brief overview of these attacks is given on these attacks.

2.3.1 Port scan attack

This is among the passive attacks, which means it does not harm the system or the server. However, it can store all the details related to the machine or the server of the victim. A port scan aims to find any active port among a spectrum of port addresses for the server by sending a request to the client (Cruz-Cunha, 2014) . The different port scans include Connect Synchronization (SYN) scanning; UDP scan, XMAS scan, Acknowledgement (ACK) scanning, and FINISH (FIN) scan are commonly used by the popularity of the scans applied by the attacker.

2.3.2 Man-In-The-Middle (MITM)

In this kind of attack, the invader tries to intercept communication between two partners. The attacker emulates a reliable connection and transfers messages from one party to the other to establish the belief that this is a private conversation. **Figure 1** shows how this attack is made; instead of the network transferring the information between the two users, the attacker does this part without the victims knowing; in exchange, all the transferred data is accessible by the attacker.

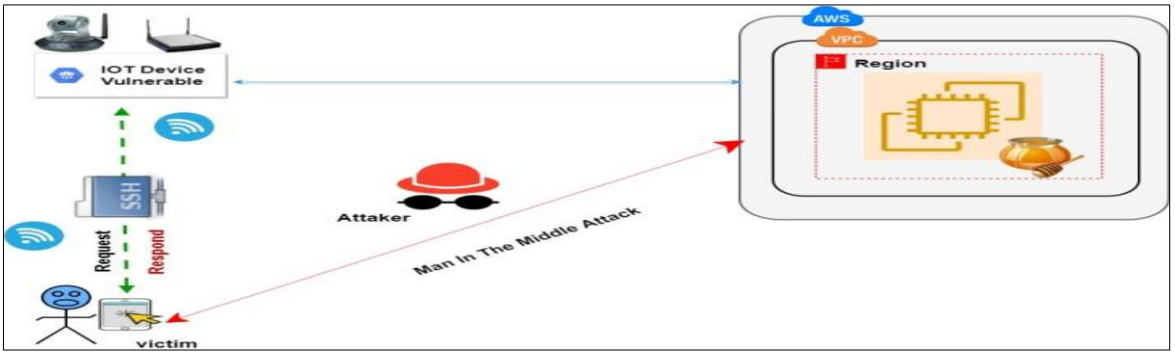


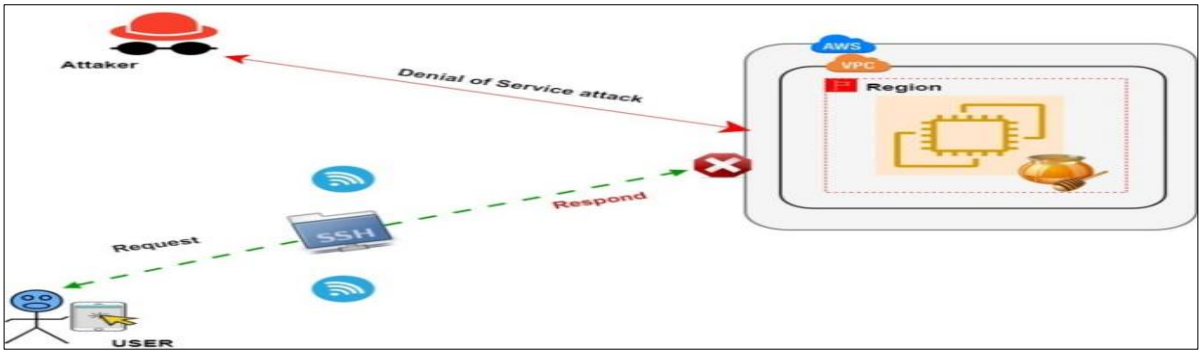
Figure (1): Man in the middle atta

2.3.3 Denial of Service attack

This attack aims to close the machine, network, or software for some time to deny the use of the service. In this attack, the system/network is pinged with heavy spam requests that the system/network cannot handle, so it crashes. Governments and banks are usually the main targets for this attack, as it causes them to lose time and money to re-run the system/network.

This type of attack is shown in **Figure 2**

Figure (2): Denial of service attack



2.3.4 Distributed Denial of Service attack

This is the same as denial of service attack, but it differs in the use of many systems by the attacker to take down the system/network. A typical DDoS attack has a master and a zombie.

The master refers to the invaders who begin the attack by exploring all the vulnerabilities in the system and finds the weak systems and attains control over them by applying infection on the systems via malware or by bypassing.

2.3.5 Sniffing attack

One of the most common types of attacks is the sniffing attach, carried out over connections and wireless links. It enables the attacker to gain access to and collect, and change data from the user's system by gaining access over it(Salman & Jain, 2017). The attacker uses two most important methods in the sniffing, including ARP poisoning and methods of theft of TCP sessions. ARP poisoning as a sniffing method is used for attacking the network using packet-spoofing invasion and router-based weaknesses.

On the other hand, the TCP session theft approach is applied in catching the IP address of the packets at the source and destination in promiscuous mode. The attack is illustrated.

2.4 Honeypot technology

After showing that the previously explained protocols determine a standard for normal behavior, the processes of collecting, analyzing, and identifying infrequent activities are done in a dynamic protocol analysis, which includes payload (content) handling, context, and overall pattern examination. In the case of IoT, protocols do not define only the way IoT tools can exchange data but also their inclusion into the IoT platform.

Honeypot technology is considered an approach from many that processes data and recognizes the pattern(Salman & Jain, 2017) Mainly, Honeypot technology is a mechanism that is used to detect malicious activity through simulation of an actual system in a safe environment. Therefore, the invader is lured into the system, thinking it is an actual one; however, it does not affect the system since it is protected, and all activities the invader is being recorded.

The major idea about the Honeypot is to deploy the communication protocols previously mentioned on software that the hacker attacks while recording their activities.

2.4.1 Advantages of Honeypot

One advantage of a honeypot is that several security solutions exist in the market and anybody can explore the choices on the internet to find the most appropriate solution to fit their needs. According to Mokube and Adams (2007), honeypots capture invasions and provide information concerning the kind of attacks and where necessary due to the logs, one can see the added information on the attack. New threats can be noticed, and newer security options can be formed by having a look at them. Further analysis can be done by having a look at the kind of misbehaviors. It aids in understanding more attacks, which may take place. Honeypots are not heavy when it comes it comes to capturing data. They are mainly handling the inflow of malicious traffic. Consequently, the data that caught is not the whole traffic. Concentrating only on the malicious traffic simplifies the investigation. For that reason, honeypots become very beneficial. For the few malicious attacks, there is no need for large data storage and new technology to utilize.

Any type of computer can be configured for use as a honeypot system. Therefore, a honeypot system does not increase the cost of the security system. They are easy to understand, configure and deploy. They have no complicated algorithms and need no need for updates and modifications. Since honeypots can detect any malicious attackers, it provides more ideas and does deepen the security solutions.

2.4.2 Disadvantages of Honeypot

Since there are several vital advantages of the application of honeypots, they also have disadvantages. As Mokube & Adams (2007) state, they can only pick data while the malicious intruder attacks the system live, otherwise, catching the information becomes difficult. Any attack taking place on another system cannot be detected by the honeypot on a different IoT system.

Consequently, attacks on the external honeypot system can damage other IoT systems and lead to huge problems. The second disadvantage of a honeypot is the fingerprinting of honeypots by an experienced attacker. It is very easy for the attacker to study whether he attacks the honeypot system, or an actual system and this identification can determine his or her activities.

Fingerprinting enables the distinguishing between the two but is not a desirable outcome of the experiment. The honeypot can be utilized as a zombie to reach external systems and weaken their security systems, and this is hazardous.

Related work, as much we have done the research, no study has been done where the complete methodology of honeypot deployment had been explained. Moreover, simulating devices and collecting data of attacks with the help of the EKK stack has not been used to find the unknown attacks by IoT honeypots.

The study focused on the installation of IoT honeypots. They proposed a procedure to install necessary honeypots on IoT systems, given the rank of popular chosen tools and the request to avoid detecting the trap nodes as honeypots among some of the most used IoT scanners. They found that these IoT tools are not designed with adequate security standards, and they are doing vital and sensible roles in our life's specific to our privacy and security (Acien, Nieto, Fernandez, & Lopez, 2018).

To attain the objective of this research, the steps below are followed

• Carry out a study on shared IoT based protocols including MQTT, XMPP, AMQP, and UPnP to access and comprehend their design. In this survey, we provide a platform for focusing on precise protocols and possible research sub-topics.

In answering the question of whether the honeypot techniques are appropriate for identifying security problems on the IoT platforms,

A Proof of Concept (POC) of the ThingPot applied. By mainly executing the ThingPot POC runs for 46 days on the four nodes (thee of the nodes are for REST API while one is for XMPP), it catches a massive amount of valued information. By conducting detailed data analysis, they found and summarized hackers' actions besides the IoT system. Thus, ThingPot has presented the ability for identifying security problems on the IoT Platforms and demonstrates that honeypot equipment is suitable for identifying safety problems on the IoT system (Wang, 2017).

Intelligent interaction was presented as a method to build IoT honeypot automatically and intelligently. This leverages multiple heuristics as well as an interactive machine learning mechanism for customizing the scan of process and enhances the replying logic to extend to capture the exploit code.

They proposed a general framework to build an intelligent-interaction honeypot for the IoT tools. They explained why and how we require intelligent-interactive honeypot (Wang, 2017).

The aim of interactive intelligence is for learning the right behaviors for interaction with the clients from the zero-knowledge on the IoT tools. The appropriate reactions to the clients ought to be fit for the expansion of the session with potential hackers, tricking them to pass the inspection, while sending the exploit needs as described by Maarof et al (2018). For this goal to be accomplished it needs the system to collect the valid responses as the candidates automatically, via interaction with the hackers; the learning procedure aids the honeypot to enhance the right behaviors for each request (Ramirez et al., 2017) .

Any release of the source code has to lead to 2 important outcomes:

- The principal and most observable that it has provided cybercriminals and hackers not only a functional process for the creation of an active botnet but also the creation of a customized one.

• The second outcome is the formation of demand for IoT safety following its demonstrated the weakness of IoT tools and related operating systems for simple malware infection and enslavement trials. The devices are not only weak, but some are also infected.

From the publication of the source code, there is an increased need for IoT safety and a race to enslave, increasingly Internet of Things devices by attackers and bot-herders. However, about 6 billion IoT devices are connected to the internet and the number is expected to reach 20 billion during the year 2020. Hackers compete aggressively, prompting the initiation of malware to erase other malware from manipulating the device, which simplifies espionage, data stealing, or launching of lots of DDoS attacks and looking around for other weak devices and adding them to the botnet (Antonakakis et al., 2017).

IoTPOT proposed a unique honeypot to imitate Telnet services of many IoT tools to monitor and record continuous active attacks on the IoT devices in detail. IoTPOT has distinguished low-interaction responses to cooperation with the backend high-interaction computer-generated environments called IoTBOX. IoTBOX controls many virtual environments usually applied through fixed systems for various Central Processing Unit (CPU) designs (Minn et al., 2015). In the 39 days of operation, there was an observation of 76,605 attempted downloads of malware, an increase from 16,934 visits to the Internet Protocol (IP). (Ramirez et al., 2017) confirm that present honeypots could not capture any of these binaries. Telnet protocol that as telnet password honeypot and honey because they are unable to manage different inflowing commands sent via the hackers(Shodan, 2019) .

To analyze the captured malware binaries; they proposed IoTBOX as the first environment for malware analysis for the IoT devices. IoTBOX runs 8 CPU architectures, that spa ARM, PPC, and MIPS.

The sandbox exploration of 17 samples through IoTBOX shows that the samples were used for performing ten distinct types of DDoS attacks as well as scans on port 23. Ultimately, merging the outcomes of the observations of IoTPOT and the analysis of sandbox IoTBOX, we confirm that:

1) At least 4 distinctive malware families are spreading by Telnet

2) Their typical activity is performing additional broadcast over Telnet and DDoS

3) Some families develop frequently, update quickly, and ship binaries for the varieties of CPU designs, even within the restricted observation period of 39 days (Minn et al., 2015).

An automatic framework for detection and identification of compromised devices of botnets and analysis of malware was developed. They proposed some essential research questions like "What are the characteristics of compromised machines belonging to botnets?"

Dionaea a low interaction, server-side honeypot which emulates a vulnerable system or device was installed on the Amazon Elastic Compute Cloud (Amazon EC2) to record attack data and malicious software binaries. Virus Total was utilized in malware grouping while and Shodan was used in device identification as described by Thangavel et al (2014). The top malware variations, types of devices, products, countries, organizations and open ports were examined to find compromised devices, with the continued existence of critical router weakness(Chinn, 2015) .

Thus, we proposed a deception tool based on IoT Honeypot. The deception idea is an emergent class of cyber-security protection. Deception equipment can analyze and detect weaknesses and protect the system and devices from zero-day and radical attacks frequently. They are automated, provide, and accurate awareness of malicious motion in the internal networks, which could be hiding among other forms of cyber guards. The deception concept enables a security system with a more proactive position to seek to trick the invaders, detect them, and conquer them,

Permitting the innovativeness to yield to normal processes.

3. EXPERIMENT SETUP

This section describes the experimental setup using the central logs and observing server based on): the EKK stack (Amazon Elasticsearch Service, Amazon Kinesis, and Kibana) which helps to present data, create visualization and a dashboard for any size of data. The research is based on the EKK stack (Amazon Kinesis, Amazon Elasticsearch Service and Kibana). Elasticsearch refers to a search engine with analytics. Logstash refers to a server-side pipeline for processing of data that takes in data from numerous sources concurrently, transforms the data before sending it to a "stash" like Elasticsearch. Kibana allows users to visualize data with analysis charts and graphs in the Elasticsearch.

We used the alternative to the known log combination solution, the ELK stack (Elasticsearch, Logstash, and Kibana): the EKK stack (Amazon Elasticsearch Service, Amazon Kinesis, and Kibana). The EKK solution removes the simple heavy lifting of deployment, management, and scaling of the log aggregating resolution. Through the EKK stack, we emphasize an analysis of logs and debugging of the application, instead of management and up-scaling the system that groups the logs.

3.1 Data Analysis using Kibana

In Kibana, we performed several keyword searches using Elasticsearch. The main goal was to find attack events in our honeypots. We have identified several events from the log data analysis. Kibana was used as an open-source tool for visualizing and exploring data. Also, it was applicable in log and time-series analytics, application checking, and operating intelligence use cases. Kibana was considered a very useful tool helpful feature such as bar graphs, trend lines, histograms, line graphs, and other visual figures. Kibana allowed tight integration with Amazon Elastic search, making it our default choice for visualization.

The EKK implementation eradicated the homogeneous heavy lifts of deploying, management, and scaling of the log aggregate resolution. With the focus on the EKK stack, the emphasis was on analyzing logs and correcting the application, instead of management and up-scaling the system to aggregate these logs.

3.2 The most common attack

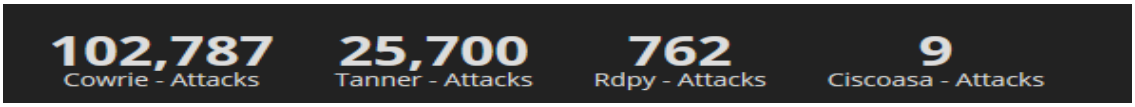


Figure (3): Most common attacks

The Cowrie honeypot experienced more than 100,000 attacks. It was not surprising that the majority of the Telnet & SSH honeypot had the most attacks. Cowrie is a standard high-interaction honeypot planned to entice and log physical force occurrences and any shell dealings by the attacker. Its main purpose is to interact with an attacker whilst monitoring how they behave when they think they've breached a system.

It was no surprise that of the *102,787* attacks, *32,607* came from China, with the United States of America coming second with a modest *14,115* attacks.

3.3 What they did once they logged in

Understanding what attackers are doing once they gain access is key to building a defense. Not every attack is going to come from an unknown user from an unknown IP. With most SIEMs, it is possible to trigger alarms if a user uses any of the listed commands. This way, should a user on the network ever lose their credentials, if any of those commands are used, we can tag it as suspicious behavior and set up rules to block the account till there's confirmation it's not a breach.

We noted that Cyber-attacks are more than just the Big Four (Russia, China, USA & Iran). For security teams, understanding this is essential for building your strategy. Regularly reviewing where the service attacks occur can help determine if there is any internal sabotage going on.

We did notice however that a few of the honeypot Dockers went on knocking over after a small brute force and we set up an Elastic cluster separately to monitor the server to see if it was being attacked. We propose using the latest version of Elastic to use their SIEM function to monitor some of the test environments. We also recommend for future research, to declutter the honeypots and deploy them individually for better analysis in addition to making use of machine learning from Elastic.

3.4 Statistics

Statistical analysis of the results provided a better insight to the readers about what we observed in the EKK experiment. The first section of this analysis includes the whole structure of attacks on honeypots. It carries the wider idea of attack vector as well as that of common IPs that link different honeypot systems. It also carries the IPs that have had the greatest number of attacks in the connection of all the procedures.

Analysis of this information from REST logs shows that the invaders noticed the IoT environment and all devices. In general terms, all the attackers look for devices such as Philips Hue, Belkin Wemo and TPlink. Particularly, they are interested in getting information regarding smart devices and more importantly the taking over of control. The methodology that the attackers seemed to prefer is first a general scanning to look for vulnerabilities, followed by a more targeted and specific attack via brute force or fuzzing. We set up the T-honeypot (traps) that imitated various devices and connected to the Internet to see what happened to them ‘in the wild’. Through

the entire 24-hour time span, the attempts of connection attacks were in the tens of thousands from various unique IP addresses.

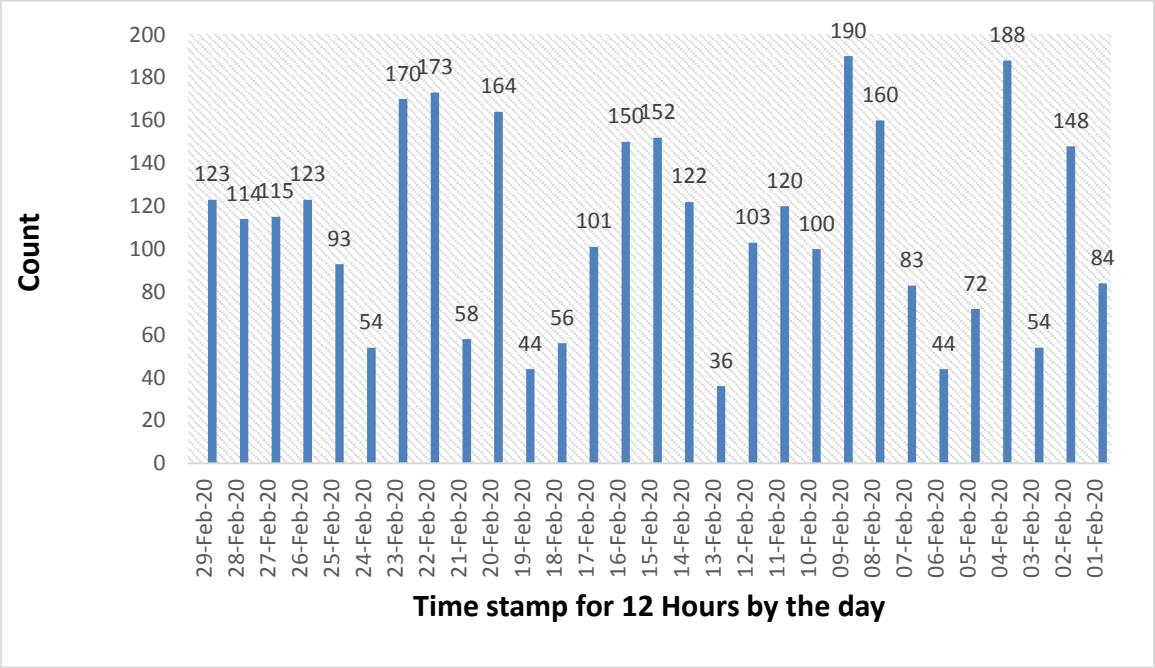


Figure (4): The number of unique hits on honeypots from unique IP addresses. Feb 01-Feb 2020.

In many instances, the attempts to do connections applied to the telnet protocol; the others applied SSH.

TABLE (3): DISTRIBUTION OF ATTEMPTED ATTACKS BY TYPE OF CONNECTION

Type of connection	Number
Telnet	6700
SSH	1182
Total	7882

We analyzed the types of devices from which the attacks originated. More than 60% of the attack could be seen in the form of DVR services and IP-based cameras, but approximately 17% were various forms of network tools as well as routers from several main manufacturers. About 1% were Wi-Fi repeaters while other network hardware, TV tuners, VOIP devices, exiting nodes at Tor, printers and all the devices that make up the 'smart-home'. Other devices could not be identifying and were simply registered as unidentifiable devices, forming 20%.

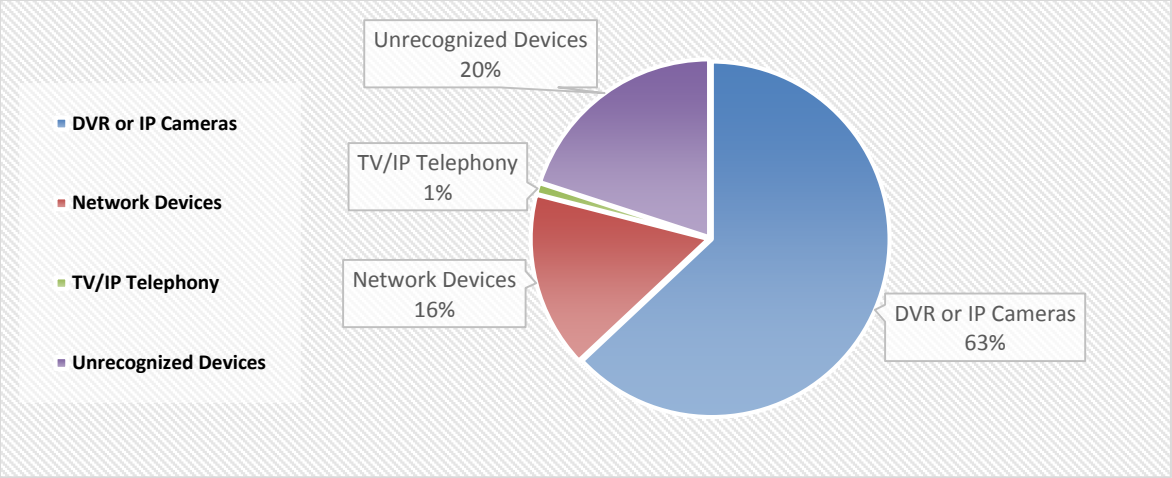


Figure (5): Distribution of attack sources by device type Feb 10-Feb29 2020

Several connections attempted to get into some IP addresses at the honeypots system we constructed, and they responded to the HTTP requests. Naturally, so many devices used each IP address through the NAT technology application. It was common to find that the device, which responded to the HTTP server request was not the ones that caused attacks on the honeypot, as is usually expected.

There were web pages and device controlling panel in response to and in the maintenance of the request and carrying out monitoring through the camera. With the returned page, the devices can be identified. The table below shows the most often used headers for web pages detected by the invading devices:

TABLE (4): NUMBER OF ATTACKS ON DEVICES, CLASSIFIED BY TITLE

Devices	Number of IP addresses
DVR or IP Cameras	4966
Network Devices	1261
TV/IP Telephony	79
Unrecognized Devices	1576
Total	7882

TABLE (5): NUMBER OF ATTACKS ON DEVICES, CLASSIFIED BY HTTP TITLE

HTTP Title	Devices
WEB SERVICE	2569
NETSurveillance WEB	1432
Dvrdvs	621
DVR Components Download	777
NetDvrV3	960
IVSWeb	1523
Total	7882

Several IP addresses are a potential vulnerability. The vulnerable devices are shown below.

TABLE (6): NUMBERS OF IP ADDRESSES OF VULNERABLE DEVICES: IP CAMERAS AND DVRS

HTTP Title	Devices
Eltex NTP	653
RouterOS router	823
GPON Home Gateway	1878
TL-WR841N	1969
ZXHN H208N	1038
TD-W8968	642
iGate GW040 GPON ONT	879
Total	7882

He honeytraps we setup not only recorded attacks coming from network hardware classed as home devices but also enterprise-class hardware.

Amid all IP addresses that released the attacks, a number of them checked and managed the devices with initiative and safety links, such as:

- Point-of-sale devices at stores, restaurants and filling stations
- Digital TV broadcasting systems
- Physical security and access control systems
- Environmental monitoring devices
- Monitoring at a seismic station in Bangkok
- Industry-grade programmable microcontrollers
- Power management systems

It is not easy to confirm that these devices have an infection. However, some attacks on the honeypots arrived from the IP addresses used by these devices, which means at least one or more devices were infected on the network where they reside.

3.5 Geography of infected devices

As already stated, the majority of the infected tools are IP-based cameras and also DVRs. A large number of them are prevalent in China and Vietnam. Others are found in Russia and Brazil among many other countries. The geographic distribution of the devices with the IP addresses that attacked the honeypots is represented in the pie chart below:

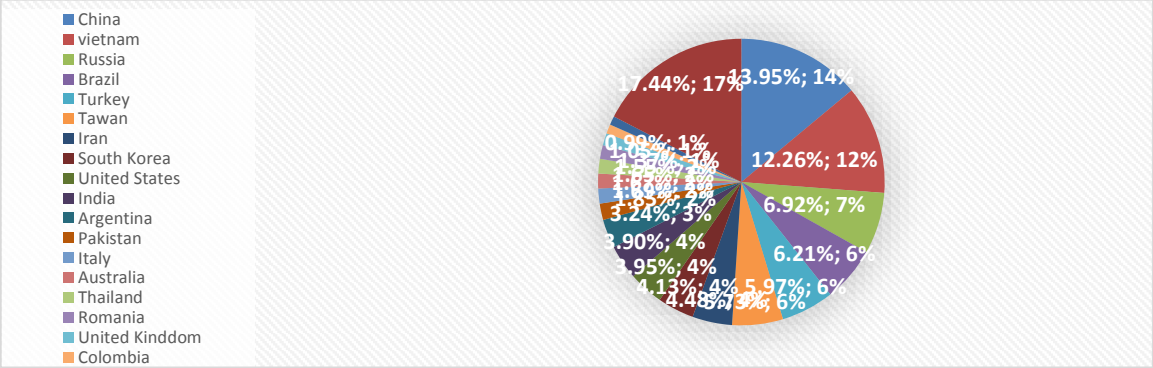


Figure (6): Breakdown of attacking device IP addresses by country Feb 02- Feb 29 2020

3.6 Geographical distribution of server IP addresses

We recorded over 100000 hacking attempts and more than 8000 unique IP addresses from which malware for IoT devices was downloaded. The breakdown of the IP addresses is shown below by countries.

Table 7 Geographical distribution of server IP addresses from which malware was downloaded to devices

Country	Unique IPs
Vietnam	2136
Taiwan, Province of China	1356
Brazil	1124
Turkey	696
Korea, Republic of	620
India	504
United States	429
Russian Federation	373
China	361
Romania	283
Total	7882

It can be deduced that the difference is due to the presence in some of these countries of bulletproof servers, meaning it's much faster and easier to spread malware than it is to infect IoT devices.

4. CONCLUSION

Honeypot technology is helpful and utmost important part of security strategies in a network. Although honeypot technology is constantly improving, attackers are constantly searching for vulnerabilities in IoT devices and in honeypots to identify them.

We have analyzed IoT devices' vulnerability using honeypot data collected from AWS. The data was analyzed using an EKK stack for log data analysis and visualization. It is worth noting that EKK uses elasticsearch, which helped to identify various types of vulnerabilities. It has become apparent that honeypots are constantly being targeted by attackers.

Throughout the paper, we have outlined how to set up a honeypot using the EKK technology and to emphasize the threat to the community of IoT devices' vulnerabilities and their users. The average Internet daily user is not aware of the dangers as these devices have not been designed with enough security measures. Also, they are increasingly performing important and sensible roles and impacting privacy and security.

The experimental result provides a reference for the improvement of honeypots and promotes the development of honeypot technology using EKK technology.

Unlike the old-style security discovery approaches, the honeypot structure, particularly on the IoT research area, is meant for attacks and habitually monitor possible attacks by exploring network packages or log files. Using the EKK technology we were able to extract the exact IoT devices' vulnerabilities and threats, effective actor tactics, techniques, and procedures from these data. This provides a powerful tool that can be used to generate more defense strategies.

4.1 Recommendations

In future work, we aim to extend the analysis of IoT devices' vulnerability attack using Machine Learning in AWS EKK POT. Recommendations for further research include but are not limited to the following:

1. Improvement of the honeypot mechanism to prevent recognition by attackers, and silently capture their behaviors. This calls for intelligent techniques to automatically check whether a remote server is running a honeypot service or not.
2. Furthermore, research should extend the Honeypot with capabilities to stimulate even more architectures and environments that are common on IoT devices.
3. We, therefore, recommend further research on Honeypots with Machine Learning based Detection Framework for defending IoT based attacks.
4. As future work, we can deploy the Honeypot in a larger public network and evaluate its average session time and data capture performance.

References

Acien, A., Nieto, A., Fernandez, G., & Lopez, J. (2018). A comprehensive methodology for deploying IoT honeypots. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11033 LNCS*, 229–243. https://doi.org/10.1007/978-3-319-98385-1_16

Al Hasib, A., & Mottalib, M. A. (2010). Vulnerability analysis and protection schemes of Universal Plug and Play protocol. *Proceedings - 2010 13th IEEE International Conference on Computational Science and Engineering, CSE 2010*, 222–228. https://doi.org/10.1109/CSE.2010.37

Anagnostakis, K. G., et al. "Detecting targeted attacks using shadow honeypots." Proceedings of the 14th conference on USENIX Security Symposium. ACM, 2005. 129-144.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Arbor, A., Bursztein, E., … Zhou, Y. (2017). Understanding the Mirai Botnet. *USENIX Security*, 1093–1110. https://doi.org/10.1016/j.religion.2008.12.001

Al-Shaer, E., Wei, J., & Hamlen, K. W. (2019). *Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings.* NY: Springer.

Brewster, T. (2013). How Attackers Can And Will Exploit UPnP Weaknesses[20]. Retrieved from https://www.silicon.co.uk/workspace/how-attackers-will-exploit-upnp-105868

Chinn, R. (2015). Botnet Detection: Honeypots and the Internet of Things, *I*. Retrieved from https://msmis.eller.arizona.edu/sites/msmis/files/documents/sfs_papers/ryan_chinn_sfs_masters_paper_0.pdf

Christian Seifert, Ian Welch, and Peter Komisarczuk. Taxonomy of honeypots, 2006.

Cruz-Cunha, M. M. (2014). *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance.* NY: IGI Global.

CVE Details. (2019). CVE security vulnerability database. Retrieved from https://www.cvedetails.com/

ElasticSearch-Contributors. (2013). ElasticSearch Documentation. Retrieved from http://www.elasticsearch.org/guide/

Fahrnberger, G., Gopinathan, S., & Parida, L. (2019). *Distributed Computing and Internet Technology: 15th International Conference, ICDCIT 2019, Bhubaneswar, India, January 10–13, 2019, Proceedings.* Los Angeles: Springer.

Görmüş, S., Aydın, H., & Ulutaş, G. (2018). Security for the internet of things: A survey of existing mechanisms, protocols, and open research issues. *Journal of the Faculty of Engineering and Architecture of Gazi University*, *33*(4), 1247–1272. https://doi.org/10.17341/gazimmfd.416406

Guide, U. (2012). Amazon Elastic Compute Cloud User Guide for Linux Instances. *Copyright © 2016 Amazon Web Services*. Retrieved from http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-ug.pdf

Mokube, I. and Adams, M. (2007). "Honeypots: concepts, approaches, and challenges," in Proceedings of the 45th Annual Southeast Regional Conference, pp. 321–326, ACM, Winston-Salem, NC, USA, March 2007. View at Publisher

Kamesh, & Sakthi Priya, N. (2016). A survey of cybercrimes Yanping. *Security and Communication Networks*, *5*(February), 422–437. https://doi.org/10.1002/sec

Kemmerer, R.A. and G. Vigna. "Intrusion detection: a brief history and overview." Computer 2002: 27-30.

Lehto, M., & Neittaanmäki, P. (2018). *Cyber Security: Power and Technology.* NY: Springer.

L. Spitzner, (2003). Honeypots: Tracking Hackers. Addison-Wesley, [Online]. Available:

http://www.tracking-hackers.com/book/

L. Spitzner, (2003) "The honeynet project: trapping the hackers," IEEE Security & Privacy, vol. 1, no. 2, pp. 15–23, 2003.

Maarof, A., Senhadji, M., Labbi, Z., & Belkasmi, M. (2018). Security on the internet of things. *Security and Privacy in Smart Sensor Networks*, 105–121. https://doi.org/10.4018/978-1-5225-5736-4.ch006

Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labeling of IoT devices. *Computer Standards & Interfaces*, *62*, 64–83.

Mokube, I. & Adams M.,2007.Honeypots:Concepts,Approaches,and Challenges. ACMSE 2007, March 23-24, 2007, Winston-Salem, North Carolina, USA ,pp.321-325.

Melo, A. C. M. (2013). Simple Authentication and Security Layer (SASL). *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Michael Mimoso. (2015). Filet-o-Firewall UPnP Security Vulnerability in Home Routers _ Threatpost[19]. Retrieved from https://threatpost.com/upnp-trouble-puts-devices-behind-firewall-at-risk/114493/

Minn, Y., Pa, P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., & Rossow, C. (2015). IoTPOT: analyzing the rise of IoT compromises. *Emu*, *9*, 1.

Mohammed, M., & Rehman, H.-u. (2015). *Honeypots and Routers: Collecting Internet Attack.* Washington: CRC Press.

Nastase, L. (2017a). Security in the Internet of Things: A Survey on Application Layer Protocols. *Proceedings - 2017 21st International Conference on Control Systems and Computer, CSCS 2017*, (July 2016), 659–666. https://doi.org/10.1109/CSCS.2017.101

Nastase, L. (2017b). Security in the Internet of Things: A Survey on Application Layer

Protocols. *Proceedings - 2017 21st International Conference on Control Systems and Computer, CSCS 2017*, (July 2016), 659–666. https://doi.org/10.1109/CSCS.2017.101

Nicholson, D. (2017). *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17−21, 2017, The Westin Bonaventure Hotel.* Los Angeles, California, USA: Springer.

Ramirez, D., Uribe, J. I., Francaviglia, L., Romero-Gomez, P., Fontcuberta I Morral, A., & Jaramillo, F. (2017). IoTCandyJar: Towards an Intelligent-Interaction Honeypot for IoT Devices. *Journal of Materials Chemistry C*, *6*(23), 6216–6221. https://doi.org/10.1039/C8TC01582A

Russell, B., & Duren, D. (2018). *Practical Internet of Things Security: Design a security framework for an Internet-connected ecosystem, 2nd Edition.* Chicago: Packt Publishing Ltd.

Salman, T., & Jain, R. (2017). Networking protocols and standards for the internet of things. *Internet of Things and Data Analytics Handbook*, 215–238. https://doi.org/10.1002/9781119173601.ch13

Shodan. (2019). Shodan Exploits. *Shodan*. Retrieved from https://exploits.shodan.io/welcome

Singh, M., Rajan, M. A., Shivraj, V. L., & Balamuralidhar, P. (2015). *Simple Authentication and Security Layer (SASL). Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*. https://doi.org/10.1109/CSNT.2015.16

Matheu-Garc´ıa, S. N., Hern´andez-Ramos, J. L., Skarmeta, A. F., and Baldini, G. (2019). "Risk-based automated assessment and testing for the cyber-security certification and labeling of IoT devices," Computer Standards& Interfaces, vol. 62, pp.

64–83.

Roland Bodenheim, Jonathan Butts, Stephen Dunlap, and Barry Mullins. (2007). Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. International Journal of Critical Infrastructure Protection, 7(2):114–123, 2014.

Talabis, Ryan. "Honeypots 101: A Honeypot By Any Other Name.".

Thangavel, D., Ma, X., Valera, A., Tan, H. X., & Tan, C. K. Y. (2014). Performance evaluation of MQTT and CoAP via a common middleware. *IEEE ISSNIP 2014 - 2014 IEEE 9th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Conference Proceedings*. https://doi.org/10.1109/ISSNIP.2014.6827678

Wang, M. (2017). *Understanding the security flaws of IoT protocols through honeypot technologiess Meng*. *Journal of the Optical Society of America*.

المستخلص:

مع ظهور أنترنت الأشياء بدات هجمات لمحاولة استغلال الثغرات على نطاق واسع وكان هنالك عدة مخاوف بشأن سلامة هذه الأجهزة، ودائما يصاحب ظهور أي تقنيات جديدة محاولات لإستغلال الثغرات الأمنية ونقاط الضعف في هذه الأجهزة.

في هذه الورقة العلمية اقترحنا طريقة لتحليل هجمات الثغرات الأمنية عن طريق نشر بيانات سجل المصائد لتحديد أنماط هجوم الثغرات الأمنية.

على سحابة أمازون لجمع بيانات السجلات ثم يتم (EKK-POT) تم استخدام وعاء مصيدة العسل و Amazon Kinesis و Amazon Elasticearch Serviceتحليلها عن طريقة استخدام خدمة Kibana.

نهدف في هذه الورقة العلمية إلى العثور على اتجاهات جديدة للتهديدات التي تتعرض لها أجهزة إنترنت وتعزيز الآليات الحالية لمواجهة هذه الاتجاهات EKKالأشياء عن طريق استخراج السجلات من حزمة المقلقة.