EJCBLT
ISSN : 3031-7355
https://doi.org/ 10.61796/ejcblt.v1i6.653

CYBER INTELLIGENCE PRACTICE IN PREVENTING CYBER THREATS AND ITS PRIORITIES

Ganiyev Abdukhalil
Docent, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

Tojimatov Dostonbek
PhD student, Tashkent University of Information Technologies named after Muhammad al- Khwarizmi, Fergana, Uzbekistan

Received: Feb 22, 2024; Accepted: March 29, 2024; Published: Jun 22, 2024;

Abstract: The practice of cyber intelligence is a comprehensive data collection process aimed at identifying, identifying, classifying, and strategizing any threats or risks to information assets. This article aims to describe and explain the current relevance of cyber-intelligence practice in preventing cyber-threats, the methods and techniques of conducting cyber-intelligence, and the basics of technologies. The article contains suggestions for increasing the effectiveness of cyber defense and developing the systemic immune response against various cyber threats

Keywords: cyber intelligence, identification, cyber attack, malware, network monitoring, cyber vandalism, social engineering, cyber crime, digital forensics, cyber espionage.

This is an open-acces article under the CC-BY 4.0 license

Introduction

Currently, digitization processes are developing rapidly all over the world. Digitization processes are making it easier for services and information of many industries to move from reality to cyberspace, thereby providing services to users remotely at any time. Cyberspace continues to expand and form a large database. Depending on the asset value of cyberspace information, the risk of those who include it is also increasing [9]. This creates threats to the interests of individuals, society and the state. As cybercrime is on the rise, there are more and more cases where their actions lead to interruptions in the operation of information systems and (or) violations of the openness, integrity and free use of information in them. If threats and risks are not prevented, it can lead to very harmful negative consequences [8]. Cyber security is the main direction of protecting the interests of individuals, society and the state from such cyber situations.

As measures to ensure cyber security are developed, it is important to have some information about threats and dangers[6]. Cyber intelligence is invaluable in detecting and stopping incidents before they happen.

Cyber intelligence information about current or emerging threats or risks to information assets (for example, unauthorized access, unauthorized use of assets, disclosure of classified information, unauthorized changes to an asset) and their methods, technologies, indicators, effects and is the

practice of collecting evidenced data on harmful effects. Collected cyber intelligence provides knowledge about the behavior and intentions of cybercriminals, as well as awareness of their past attacks and prediction of future attacks[7].

Conducting cyber intelligence is a proven method of collecting and analyzing information that helps security officials at all levels protect their critical assets by providing knowledge about cybercrime and its motives, intentions, and methods. As is clear from the definitions, cyber intelligence is the process of gathering information about cyber criminals, their tools, infrastructure and methods[3].

We can determine the specific goals of conducting cyber intelligence practice by an expert as follows:

- identification of attack types;
- determining the goals, methods, instructions of the attack;
- understanding the threat's capabilities, tactics, techniques and procedures;
- installation of reflection attack detection systems;
- development of defense strategies[2].

For an expert, having knowledge about common cyber threats helps to understand the motivation behind their implementation. There are many types of cyberthreats, and annual reports are issued by international cyber security organizations on the most frequently implemented ones. In particular, the European Union Agency for Cybersecurity ENISA (The European Union Agency for Cybersecurity) classifies the main cyber threats in the 2023 report as follows:

- the threat of malicious programs;
- Threat of SQL injection attacks;
- threat of web application attacks;
- threat of ddos attacks;
- threat of botnets;
- phishing threat;
- spam threat;
- threat of ransomware (ransomware);
- threat of insider;
- threat of physical manipulation;
- the threat of exploit kits;
- threat of data breach;
- threat of personal data theft;
- the threat of information leakage[1].

In order to prevent or minimize the risks against such threats, it is important to understand and analyze the five methods of threat detection and response. They are:

1) Implementation of continuous and comprehensive network monitoring[4];
2) Know how to filter network traffic data to detect and alert on suspicious behavior in real time;

3) Know how to detect and isolate malware;
4) have knowledge of how to react to attack incidents;
5) Ability to use Open Source Intelligence (OSINT) practices

Methods

In writing the article, the scientific conclusions of a number of scientists were studied, in particular the "Threat Landscape Report" of the European Union Cyber Security Agency [1], Ensar Seker's "Cyber Threat Intelligence Understanding Fundamentals" [2], D. Planque's "Cyber Threat Intelligence - From Confusion to Clarity; An Investigation into Cyber Threat Intelligence" [3] "Network security auditing and compliance" [4] by D. Tojimatov, M. Turdimatov, N. Ibrokhimov, "Cyber security: threats, problems, solutions" [5] by D. Kh. Tojimatov, "Implementation of cyber intelligence the role of artificial intelligence technologies in development"[6], "The role of social engineering in the implementation of cyber intelligence"[7], "Network security monitoring in cloud environments" by J. Mirzayev, U. Khudoinazarov, D. Tojimatov[8] , D.Tojimatov, J.Mirzayev's scientific articles such as "Prediction of cyber threats and use of artificial intelligence capabilities in protection against risks" [9] are studied and quotes from them are given.

Results and Discussion

To properly understand the methodology of cyberthreats, we need to know the sequence of the threat implementation algorithm. For this, we can understand the actions of the cyber threat chain through the following scheme

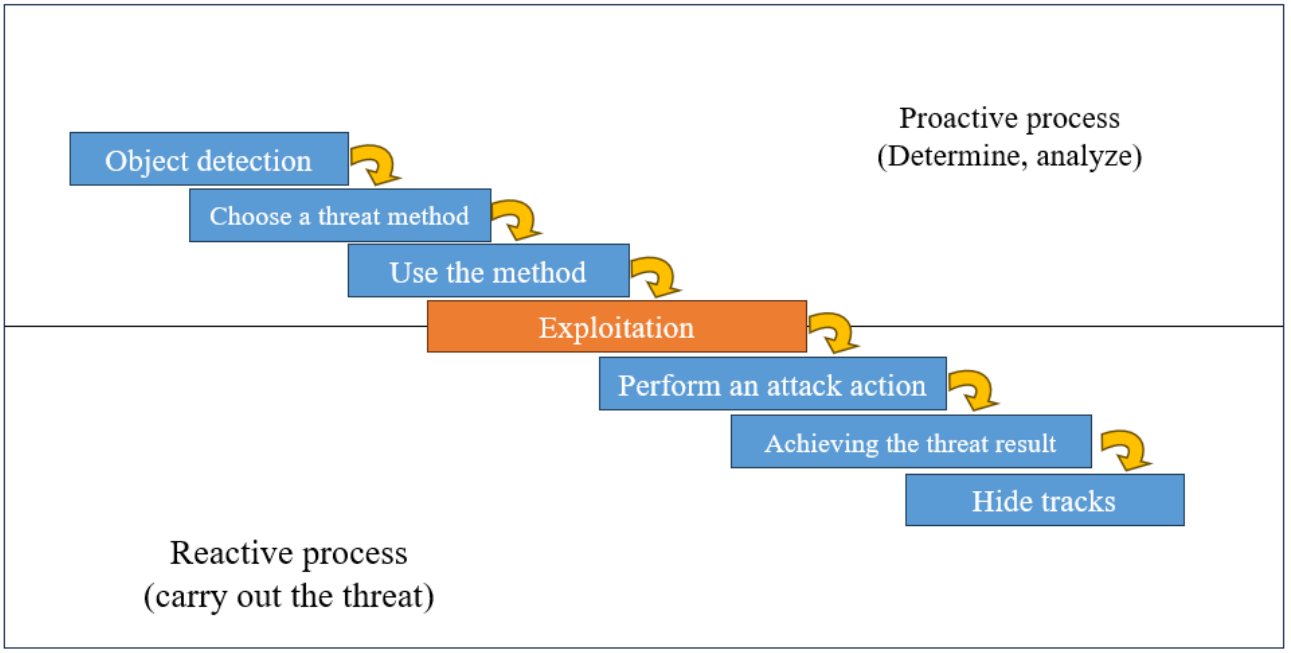

Figure 1. The life cycle of the "Threat chain" algorithm.

Based on the sequence of the "Threat Chain" algorithm, cybercriminals carry out their cyberthreat actions. The practice of cyber intelligence serves to develop a defense strategy against cyber threats by studying the life cycle of their actions in proactive processes.

In the effective implementation of cyber intelligence, the following features should be taken into account.

- Timeliness: Time is of the essence for effective threat intelligence. Therefore, the timely implementation of cyber-intelligence practice serves to collect more and accurate evidence.
- Relevance: Threat analysis should be applied to the relevant environment, i.e. appropriate actions are taken for the defined environments.
- Accuracy: More accurate analytics are needed to take smarter and more effective countermeasures against attacks. Therefore, the information provided by cyber intelligence should be correct, complete and accurate.
- Completeness: More detailed and accurate threat intelligence enables defenders to choose appropriate countermeasures.
- Agility: It is necessary to implement the necessary countermeasures to respond to threats.

Taking into account the above features, we can develop the "Threat Hunting" cyber intelligence model for cyberattacks carried out according to the sequence of the "Threat Chain" algorithm in the following form.

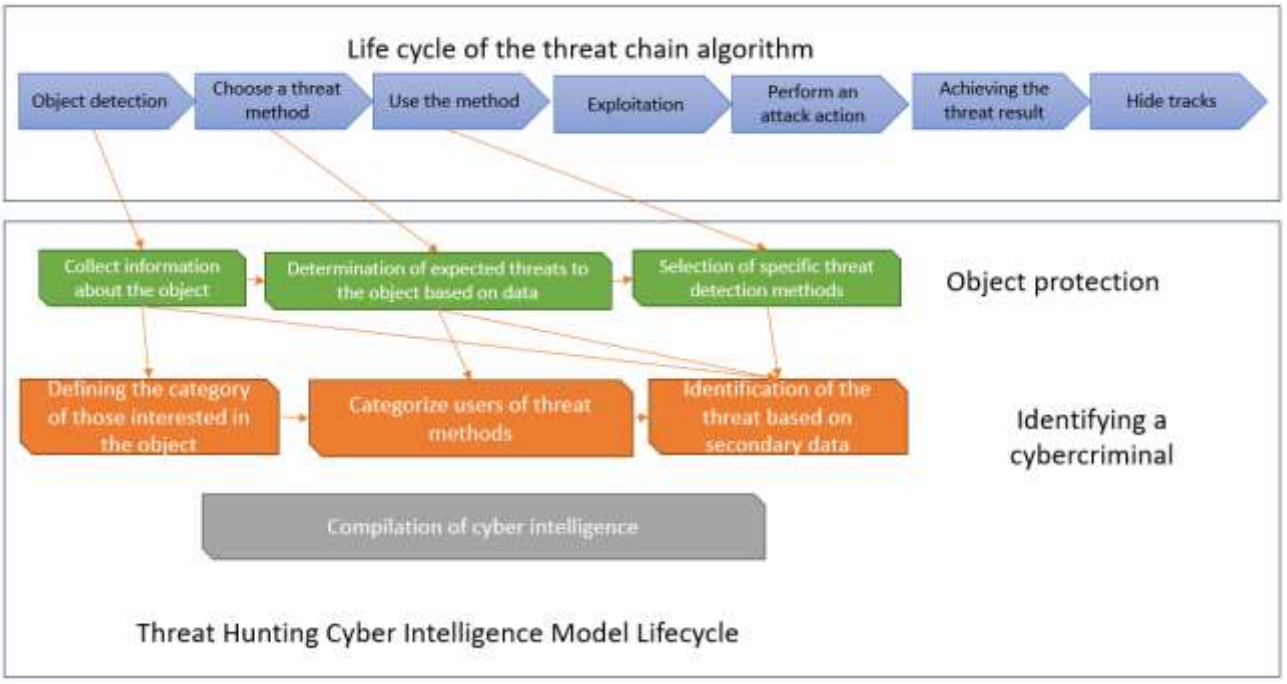

Figure 2. Lifecycle of the Threat Hunting Model for Cyber Intelligence Practice on the Threat Chain Algorithm

The "Threat Hunting" model represents the processes that should be implemented from the first stage of cyber intelligence. In the proposed model, the implementation of cyber intelligence involves the implementation of the "Threat Chain" algorithm, studying the characteristics of potential actions at the proactive process stage. The proactive process stage has uncertainty characteristics, and in cyber intelligence at this stage, experts or expert systems must have a certain level of knowledge.

The model consists of two sections, the first is "Protection of the object" and the second is "Identification of the cybercriminal". The object protection department first collects information about the object and serves to determine the object's asset value, its characteristics, and type. After studying the data of the object, its weaknesses and potential threats to the object are determined. Based on the identified threats, countermeasures are implemented. In the cybercriminal identification department, cases are organized based on the information collected by the object protection department. The category of those interested in the first object is studied and a list of suspects is formed. Second-threat attack methods are analyzed and categorized into which types of attackers use these methods. The identity of the cybercriminal is determined on the basis of forensic investigation, based on information such as preliminary data of the attacker, list of suspects, categories of attack methods, address from which attack requests were made, verification of threat file signatures. All the collected intelligence is compiled and handed over to specialists for use in the work.

"Threat Hunt" uses the "Threat Chain" algorithm as part of proactive processes. If sufficient intelligence is not obtained in this process, it is necessary to use a separate cyber intelligence method for the reactive process section of the "Threat Chain" algorithm

Conclusion

This article analyzes and explores the priority tasks that cyber intelligence can add to cyber security through threat detection. The article provides information about common types of modern threats. It also explains the specific objectives, methods and methods of conducting cyber intelligence operations.

The steps of the "Threat Chain" algorithm are developed in the article, taking into account the sequence of actions performed by cybercriminals. Based on the developed algorithm, the "Threat hunting" model was proposed for conducting initial cyber intelligence practice. The article also explains the purpose of the "Threat Hunting" model and the sequence of the principle of operation.

The information presented in the article is a part of the ongoing scientific research in this regard and is based on the preliminary conclusions of the cyberintelligence practice based on the obtained results.

References

[1] Threat Landscape Report of the European Union Cyber Security Agency., 2023/19/10.
[2] Ensar Sekerning “Cyber Threat Intelligence Understanding Fundamentals”., NATO CCD COE - 2017.
[3] D.Planque “Cyber Threat Intelligence - From Confusion to Clarity; An Investigation into Cyber Threat Intelligence”., 2017.
[4] Тожматов, Д., Турдиматов, М., & Иброхимов, Н. (2023, October). NETWORK SECURITY AUDITING AND COMPLIANCE. In Conference on Digital Innovation:" Modern Problems and Solutions".
[5] Tojimatov, D. X. (2022). Kiberxavfsizlik: tahdilar, muammolar, yechimlar,“. Axborot-kommunikatsiya texnologiyalari va telekommunikatsiyalari sohasida zamonaviy muammolar va yechimlar” Respublika Ilmiy-texnik anjumani TATU Farg ‘ona filiali.
[6] Tojimatov, D. (2023, October). KIBERRAZVEDKANI AMALGA OSHIRISHDA SUN’IY

INTELEKT TEXNOLOGIYALARINI O ‘RNI. In Conference on Digital Innovation:" Modern Problems and Solutions".

[7] Tojimatov, D. (2023, October). KIBERRAZVEDKANI AMALGA OSHIRISHDA IJTIMOIY INJINERIYANI RO ‘LI. In Conference on Digital Innovation:" Modern Problems and Solutions".

[8] Мирзаев, Ж., Худайназаров, У., & Тожматов, Д. (2023, October). NETWORK SECURITY MONITORING IN CLOUD ENVIRONMENTS. In Conference on Digital Innovation:" Modern Problems and Solutions".

[9] Tojimatov, D. (2023). u KIBER TAHDIDLARNI BASHORAT QILISH VA XAVF-XATARLARDAN HIMOYALANISHDA SUN’IY INTELEKT IMKONIYATLARIDAN FOYDALANISH: DX Tojimatov. Katta o ‘qituvchi, TATU Farg’ona filiali. Потомки Аль-Фаргани, 1(2), 41-44.