УДК 004.056.57
МРНТИ 81.93.29

KEY TASKS, TOOLS AND CHALLENGES IN THREAT INTELLIGENCE

KUSMANOVA A.M.

Abstract: *Spam, viruses, spyware are the risks that they expose themselves to users, using the services of the Internet. Modern threats of the Internet is much more complicated than those that were before. They are more resistant to remedies. Threats of the 21st century possess such properties as dynamism and transformability. Often they are carried out using zero-day vulnerabilities - unresolved vulnerabilities or vulnerabilities for which a defense mechanism has not yet been developed. Such attacks often pass unnoticed by many protection tools, IPS, antivirus Software and firewalls. The market critically lacks not only the resources that can handle all incidents, but also the overall system, thanks to which it would be possible to respond to them in the early stages of cyberattacks - ideally before operation, as well as to accumulate distributed knowledge about threats, exchange received data, investigate causes of threats and respond immediately to them. For faster accumulation of information about possible threats, one should strive to share useful data from a wide range of sources. At the same time, it is important that this information is standardized, that is, the standards and protocols for the transmission and provision of data defined in advance. The capability to detect, analyze, and defend against such threats in near real-time conditions is not possible without the employment of threat intelligence. This paper reviews the main definitions, instruments in Threat Intelligence technology. Moreover, how this technology may help to reduce cyber security risk. Threat Intelligence can help to prevent many problems recurring in information systems.*

Key words: *Threat Intelligence, Cybersecurity, security, threat*

КЛЮЧЕВЫЕ ЗАДАЧИ, ИНСТРУМЕНТЫ И ВЫЗОВЫ В РАЗВЕДКЕ КИБЕРУГРОЗ

Аннотация: *Спамы, вирусы и шпионские программы – это риски, которые они подвергают себя пользователям, пользуясь услугами Интернета. Угрозы в данное время намного сложнее, чем были раньше. Они более устойчивы к средствам, которые применяются для борьбы с ними. Угрозы XXI века обладают такими свойствами, как динамичность и способность к трансформации. Часто они выполняются с использованием уязвимостей нулевого дня - неразрешенных уязвимостей или уязвимостей, для которых еще не разработан механизм защиты. Такие атаки часто проходят незамеченными многими средствами защиты, IPS, антивирусами и брандмауэрами. На рынке критически не хватает не только ресурсов, которые могут справиться со всеми инцидентами, но и всей системы, благодаря которой можно было бы реагировать на них на ранних стадиях кибератаки – в идеале до самой атаки, а также для накопления распределенных знаний об угрозах, обмениваться полученными данными, расследовать причины угроз и незамедлительно реагировать на них. Для более быстрого сбора информации о возможных угрозах следует стремиться делиться данными из широкого круга источников. В то же время важно, чтобы эта информация была стандартизирована, то есть стандарты и протоколы для передачи и предоставления данных должны быть определены заранее. Возможность обнаружения, анализа и защиты от таких угроз в условиях, близких к реальному времени, невозможна без использования анализа угроз. В данной статье рассматриваются основные определения, инструменты в технологии анализа киберугроз. Кроме*

того, как эта технология может помочь снизить риск кибербезопасности. Аналитика угроз может помочь предотвратить много проблем, повторяющихся в информационных системах.

Ключевые слова: *анализ киберугроз, кибербезопасность, безопасность, угроза*

КИБЕР ҚАУІПТІЛІКТІ БАРЛАУДЫҢ НЕГІЗГІ МІНДЕТТЕРІ, ҚҰРАЛДАРЫ, МӘСЕЛЕЛЕРІ

Аңдатпа: *Спам, вирустар және шпиондық бағдарламалар – бұл Интернетті пайдаланушылар үшін қауіп-қатер. Қазіргі кездегі қауіп-қатер бұрынғыға қарағанда әлдеқайда күрделі. Олар кибер қауіптермен күресу үшін қолданылатын құралдарға анағұрлым төзімді. XXI ғасырдың қауіптері динамизм және өзгеру қабілеті сияқты қасиеттерге ие. Көбінесе олар нөлдік күндік осалдықтарды – қорғаныс механизмі әлі жетілдірілмеген осалдықтарды немесе осалдықтарды қолдана отырып жасалады. Мұндай шабуылдар көбінесе көптеген қорғаныс құралдары, IPS, антивирустар және брандмауэрлердің назарынан тыс қалады. Нарықта барлық оқиғаларды жеңе алатын ресурстар ғана емес, сонымен қатар кибершабуылдың алғашқы кезеңдерінде оларға жауап қайтаруға болатын барлық жүйе жоқ, шабуылдың өзінде-ақ, сонымен қатар қауіптер туралы таратылған білімді жинақтау, алмасу мүмкіндігі бар, алынған мәліметтерді қараңыз, қауіптің себептерін зерттеңіз және оларға дереу жауап беріңіз. Ықтимал қауіптер туралы ақпаратты тезірек жинау үшін сіз көптеген дерек көздерінен деректерді бөлісуге тырысуыңыз керек. Сонымен бірге, бұл ақпараттың стандарттылғандығы маңызды, яғни деректерді беру және беру стандарттары мен хаттамалары алдын ала анықталуы керек. Нақты уақытқа жақын жағдайларда осындай қауіптерді анықтау, талдау және қорғауға мүмкін қауіптерді талдауды қолдануға тура келеді. Мақалада кибертерроризмді талдау технологиясының негізгі анықтамалары, құралдары қарастырылады. Сондай-ақ технологияның киберқауіпсіздік қаупін азайтуға өз септігін тигізеді. Қауіп-қатерді талдау ақпараттық жүйелерде пайда болатын көптеген мәселелердің алдын алуға көмектеседі.*

Түйінді сөздер: *кибер қауіптер, киберқауіпсіздік, қауіпсіздік, қауіп*

I. Introduction

New methods and tools are emerging every few years in the field of information security, which allows protecting information systems of the organizations effectively. One of the latest trends is Threat Intelligence.

Threat intelligence is the analysis of internal and external threats to an organization in a systematic way. The treats that threat intelligence attempts to defend against include zero-day threats, exploits and advanced persistent threats (APTs). Threat intelligence involves in-depth analysis of both internal and external threats [1]. It consists of many techniques and technologies that can be applied in many industries. It consists of five main disciplines:

1. Human Intelligence (HUMINT) - this type of intelligence based on gathering information using human sources. A source may have information obtained from the senses.
2. Open Source Intelligence (OSINT) - research, development and improvement, information about which is generally available to the public.
3. Signals Intelligence (SIGINT) - the collection of information obtained from various transmitters of communication systems, radars and other means of communication.
4. Imagery Intelligence (IMINT) - geospatial intelligence that collects information from airborne and satellite sensor.

5. Measurement and Signature Intelligence (MASINT) - technical type of intelligence that uses information obtained from lasers, passive electron-optical, seismic and other sensors.
6. Cyber intelligence (CYINT) – This type of exploration is not a core discipline, but it is quite new and combines the qualities of all five-core disciplines. It can be used as a key component of information security by any government or industry [2].

This paper will begin the main definition and importance of cyber threat intelligence, describe fundamental tasks of cyber security intelligence, main users of this technology and observe cyber intelligence providers that used by the security specialists.

II. Cyber Threat Intelligence

Cyber intelligence services let you know about threats, leaks, hacks and hacker activity before they can harm companies. They combine a high-tech cyber monitoring infrastructure with the expertise of experienced analysts, virologists, forensic scientists, and specialists in investigation and response centers.

Threat Intelligence Tasks:

1. Data collection of vulnerability and threats:

Threat Intelligence should be integrated into the security system and should provide the ability to centrally collect information from public and private sources about vulnerabilities and threats.

2. Analytics:

Threat Intelligence should analyze and build up a knowledge base on the detection, disclosure, development and issuance of recommendations for responding to threats.

3. Data exchange:

Threat Intelligence should also provide the ability to exchange received data in real time. Analytical information should be instantly disseminated in a standardized format to both internal and external safeguards.

4. Quick alert:

Threat Intelligence must promptly notify about attacks and threats at any endpoint, using a single standardized database with classified data.

The importance of threat intelligence in information security.

There are four reasons why threat analysis becomes critical and important tool for information security:

1. Significant changes in the types of Internet threats and narrowing the field malware attacks;
2. The ability to access and use the resources and experience of organizations may not be available; 3. A huge amount of vulnerabilities in security systems and vectors attack by attackers - this is what they should pay attention to organization.
3. A constantly expanding range of technologies, which should be protected.

The amount of information that employees must analyze information security services can be truly huge. Organizations must respond to the daily influx of new vulnerabilities, zero-day threats, exploits, botnets, targeted attacks, and others “Trouble” [3].

Who uses threat intelligence?

Intelligence, as a discipline, is perhaps best understood in relation to the specific problem it is being used to solve. For example, in the case of a nation, intelligence can be used to counteract terrorism, to facilitate law enforcement, to gain information about other nations’ activities, to support warfare preparedness (or actual warfare itself) and to accomplish numerous other strategic goals.

The application of techniques, methods and tradecraft will be different depending on the specific goal being pursued. This is true also when it comes to the employment of cyber security threat intelligence for an enterprise. As such, it is useful and productive to examine the potential audiences of threat information and how they might apply it. Numerous teams within a typical organization can be consumers of threat information, including the following:

1. Information security management—these personnel manage information security strategy for the enterprise, author policies and procedures and contribute to resilience plan-

ning, compliance efforts and organizational risk management initiatives. They can use threat intelligence information to help prioritize investments in staffing and controls, help prioritize attention for security resources based on the likelihood of what might be attacked (and for what purpose) and provide visibility to other areas based on the changing threat landscape.

2. Information security operations team or security operation center (SOC). These personnel systematically analyze security-relevant event information by monitoring security tools, by analyzing and weeding out false positives originating from detective controls and by working to support the incident response process (for example, by initiating the incident process based on events they observe). These personnel can employ threat intelligence information to help identify known threat actors (for example, IP addresses that are known to correlate to attacker activity) and indicators of compromise (i.e., specific patterns or other signs known to be indicative of an attack scenario).
3. Digital forensics and incident response. These personnel investigate attacks and malicious activity such as malware by triaging, collecting evidence, analyzing information, coordinating with law enforcement and (depending on the role of the team) assisting in recovery planning. These personnel can leverage threat intelligence information to assist in the analysis of evidence—for example, by using information about adversary tradecraft to inform how their investigation will proceed and areas where additional information can be gleaned. These examples represent only a subset of the potential utility within an enterprise. The specific nuances of the enterprise (e.g., the region it is in, the type of business it conducts, etc.) and other organization-specific factors can influence which specific groups derive the most value.

There are commercial threat suppliers in Russia, for example: Group-IB, Cisco, and Kaspersky. In addition to tactical and strategic information, the company provides a web interface that tracks notifications about threats and risks. Kaspersky provides a service to receive tactical and strategic information by e-mail or in JSON format. For services provided by Group-IB and Kaspersky, you must directly contact with them. In turn, the Cisco Threat solution Intelligence Director, which also allows you to receive information from various data sources, pre-constitutes an extension of remedies, supplies- commercially available from Cisco. The following factors affect the effectiveness of threat intelligence: feeds, platform, API, and standards used. Feeds are threat data such as IP and DNS addresses, URLs, CVE records, registry keys, etc. Threat data can be shared (information about malware, DNS, spam, etc.) and highly specialized (the information is intended for a specific industry). There are many external sources of such information. Among Russian suppliers stand out: Group-IB, Kaspersky, Cisco, among foreign - Check Point, Arbor ATLAS and others. Namely choosing a source of threat data is one from the very first tasks that need to be solved at the planning stage of the implementation of threat intelligence into the existing information security system. At finding a data provider for the needs of the organization many questions arise, such as: how much are the data they provide complete? How quickly are they updated? How much do they take into account industry specifics? To solve this problem, when choosing a data source, it is recommended evaluate the following parameters: number of records, Reception to the source of users, the frequency of information, formalized presentation information, the possibility of automation.

Platforms of Threat intelligence.

Choosing a platform is also a serious task when planning the implementation of threat intelligence. Criteria for platforms may be based on various factors: popularity of use, ease of use, etc. But also there are solutions provided by threat intelligence providers. For example, Group-IB provides a web interface without pre-installation, visualizing everything necessary for the organization threat information.

Market of Threat intelligence platforms is diverse:

BAE Systems Detica CyberReveal – CyberReveal consists of three main components: platform, analytics and investigator. It is created to expand the analysts protection tools to make process of information protection faster, adding value by integrating with existing infrastructure and security systems, with plug-in analytic packages that provide cost-effective protection to deal with evolving threats.

Platform: A scalable technology platform that analyzes data from the entire IT space to identify high-priority security events.

Analytics: Behavioral-based threat detection using unique attack models and recent Detica threat research.

Investigator: A powerful set of research tools developed by analysts for analysts that provides visualization of alerts by priority [4]

IBM i2 – proven analytical platform for solving the most important tasks in the field of national security and defense, law enforcement, combating fraud, financial crime and cyber threats.

Solution features:

1. Obtaining structured and unstructured data from internal and external sources, including open sources and the deep Internet, to create an extensive array of data for queries.
2. Combining advanced analytics with powerful tools for geospatial, visual, temporal and social analysis to increase situational awareness.
3. Turning huge volumes of disparate data into valuable, effective information in almost real time for informed decisions and proper response [5]

Palantir – At the heart of the Palantir Cyber are three unique features that allow analysts to investigate the origins and characteristics of cyberattacks and develop very individual answers. With Palantir Cyber, businesses go beyond simple black box test, automated detection systems. Palantir allows organizations to diagnose attacks and take preventive measures against future cyber threats [6].

Maltego it is a software designed for conducting visual investigations related to IT, working with cyber intelligence and forensics.

One of the basic functions of Maltego is Transform or enrichment, that is, the selection of a multitude of related data based on an input value. For example, applying the transformation to a host, you can get a list of IP addresses that it has ever hosted. Then, applying the transformation to any of the received IP addresses, you can find out all the domains that were on it. Moreover, Maltego will display this information in the form of links [7].

Obviously the choice platforms will depend on usage goals threat intelligence and organization capabilities.

Threat Intelligence Challenges

Statistical and historical prediction methods can only go so far. As most risk and security practitioners already know, a generic threat analysis typically includes threats and risk scenarios that stem from nonhuman sources. For example, a generic threat analysis might include information about natural disasters, geopolitical risks, pandemic or other scenarios that don't involve a specific adversary. While information about those threat sources might be desirable, as a practical matter, much of the value derived from threat intelligence (whether an internal capability or an external feed) relates to information about human actors (whether individual attackers or state-sponsored or criminal hacking groups). Likewise, the information typically derived relates often to specific artifacts connected to the actions that these attackers perform. Although quite a bit of additional information might be gathered through a threat intelligence capability, other threats that concern security practitioners are not addressed directly by typical threat intelligence data sources. Beyond this, intelligence analysis is not a skill that is typically sourced as a normal part of building an information security team. As such, there can be hurdles both in demonstrating the return on investment for acquiring those skills, as well as potential staffing challenges in acquiring the appropriate resources to generate,

contextualize and integrate, and ultimately socialize and use threat intelligence information.

In the solution marketplace, there are also additional challenges. Some solution vendors have marketed their products and services as threat intelligence without a clear understanding of what it is or how it might be used by customers. For example, individual vendors have marketed all of the following as threat intelligence:

1. Feeds of technical data designed to be integrated into existing controls. These might be delivered as lists of "bad IP's" (i.e., addresses with a reputation for being involved in attacks), hashes of file data (designed to flag specific malware, command and control software, etc.), DNS names, URLs or other artifacts.

2. Feeds containing daily or real-time updates of regular expression signatures

3. Portals and integration platforms (usually via APIs) that automate aspects of the security workflow (e.g., incident response)

4. Visualization capabilities such as world maps highlighting attacks happening in real time by geography of origin or destination

5. Existing product features renamed as "threat intelligence"

6. High-level attribution reports about actions by hacker individuals, groups, collectives or nation-states While all of these offerings are potentially valuable (depending on the context in which they are used), they are not equivalent. Therefore, grouping them all together in the same product category can blur the market and make it challenging for customers looking to assess the vendor landscape and make a purchasing decision for their particular needs.

III. Conclusion and Future of Threat Intelligence

Over time, products and methodologies in the threat intelligence space will mature. The following areas may reflect near- or intermediate-term advances in threat intelligence capabilities:

1. Machine learning and artificial intelligence can help extract insights from internal information as well as from global monitoring systems (for example, better identification of what observed behavior is normal vs. abnormal)

2. Fusion of threat intelligence information with other business processes and data (via either automation or correlation of data)

3. Cross-integration between products and vendors (for example, consolidation in the marketplace and tighter integration between players in the market)

New challenges may likewise emerge:

Public cloud-computing platforms are becoming more and more crucial. However, threat analysis in the cloud can be more challenging compared to other environments due to fluidity (i.e., the rate at which the environment changes) and to the difficulty of monitoring devices outside the enterprise's direct control.

Higher level of machine-to-machine integration and automation of business processes may make it more difficult to identify indicators of compromise.

As a result of this research we identified that the implementation and operation of a threat intelligence allows organizations to gain knowledge about threats and risks in real time, which will allow maintain the information security system up to date, and, accordingly, ensure a high level of information security in the organization. For example, according to a study by the SANS Institute threat intelligence consumer organizations noted the following positive changes received after the introduction of threat intelligence:

63% of respondents consider that understanding of methods and tactics has improved attackers;

51% of organizations claim that the detection and response to information security incidents has become faster and more accurate;

48% say to reduce the number of recorded incidents by reducing the number of false positives information security tools;

28% of respondents noted an increase in the accuracy and speed of monitoring and incident management. [8].

REFERENCES

1. Definition from Technopedia. Available at: https://www.techopedia.com/definition/32367/threat-intelligence.
2. Solutionary, Threat Intelligence Defined. Available at: https://dsimg.ubm-us.net/envelope/352683/369322/1421853880_solutionary_threat.pdf pp.5
3. Crest Threat Intelligence Professionals, "What is Cyber Threat Intelligence and how is it used?", 2019
4. BAE Systems Detica Unveils Detica CyberReveal. Available at: https://www.darkreading.com/risk/bae-systems-detica-unveils-detica-cyberreveal/d/d-id/1139672
5. IBM, IBM i2 Enterprise Insight Analysis for Cyber Threat Hunting. Available at: https://www.ibm.com/downloads/cas/WZKLWGPB
6. Palantir, An End-to-End Cyber Intelligence Platform for Analysis & Knowledge Management. Available at: https://www.palantir.com/wp-assets/wp-content/uploads/2013/11/Palantir-Solution-Overview-Cyber-long.pdf
7. Groupsense, How to Use Maltego to Conduct Threat Research. Available at: https://www.groupsense.io/how-to-use-maltego-to-conduct-threat-research/
8. SANS Institute InfoSec Reading Room "Who's Using Cyberthreat Intelligence and How?". Available at: https://www.sans.org/reading-room/whitepapers/analyst/ cyberthreat-intelligence-how-35767