# Cyber Threats and Exploring the Sources of Cyber Threat Intelligence

**Adelaida STĂNCIULESCU, Constantin-Alin COPACI, Ioan C. BACIVAROV**
Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
adelaida.deatcu@stud.etti.upb.ro, constantin.copaci@stud.etti.upb.ro, ioan.bacivarov@upb.ro

**Abstract**

*Cyber threat intelligence technology becomes a necessity in the context of the exponential evolution of information systems. The methods used by malicious actors are constantly evolving, becoming more and more sophisticated over time, thus making the task of security teams more difficult. This article aims to investigate cyber threats, providing information necessary to understand and detect the mode of operation of the attack, to then decline and disseminate it within the information systems to be protected. Advanced threat intelligence thus supports proactive monitoring of emerging threats by determining trends in the cyber landscape.*

**Index terms:** cyber security, cyber threats, intrusion, Threat Intelligence, security incidents, vulnerability management

## 1. Introduction

The concept of threat intelligence took shape in the early 2000s, when more and more companies began to recognize the role of gathering and analyzing threat data to proactively protect against attacks. This change in approach to cyber security has been driven primarily by the increasing prevalence of activities such as phishing schemes, ransomware incidents and distributed denial of service (DDoS) attacks.

Cyber threat intelligence (**CTI**) is a subfield of cybersecurity that focuses on the structured collection, analysis, and dissemination of data on potential or existing cyber threats.

Today, the main objective of **cyber threat intelligence** is to equip organizations with as much knowledge as possible. necessary for proactive defense against cyber threats. **Cyber threat intelligence** includes techniques such as network monitoring, log analysis, and gathering information from human sources to identify potential security vulnerabilities and detect signs of malicious behavior. Investigating cyber threats provides organizations with the information they need to continually refine their defenses.

## 2. Source of information and methods of collection

*Threat Intelligence*: May include broader intelligence sources and may involve data collection techniques that are not necessarily related to IT or cyber security, e.g. OSINT open-source data, government intelligence, market analysis.

*Cyber Threat Intelligence:* Uses specific IT&C sources and methods to gather information related to cyber threats. This may include:

- OSINT (Open Source Intelligence) to collect data from the Internet about attackers and attack techniques;
- Dark Web Intelligence to track online criminal activity;
- Indicators of Compromise (IoCs) to detect malware and attacks;
- TTPs (Tactics, Techniques and Procedures) used by attackers.

## 3. Threat Intelligence application areas

Threat Intelligence is an essential element that supports and complements many areas of security in an organization. **Threat Intelligence** can be considered a **support function** for the other areas of security within an organization.

More specifically, threat intelligence provides critical information that helps **improve** and **optimize** other security functions, such as network protection, security incident management, application security, database security policy development, and more.

**Protecting a network**

Threat Intelligence provides information about the techniques and tactics used by attackers, such as malicious IPs, infected domains or indicators of compromise (IoCs), which can be integrated into network protection systems (e.g. firewalls, IDS/ IPS).

This information helps proactively block attacks before they reach the organization's internal network, thereby preventing DDoS attacks or exploiting network vulnerabilities.

**Security incident management**

In the incident management process, threat intelligence plays a key role in quickly identifying an attack, as it provides indicators (e.g. malware file hashes, malicious IP addresses) that can be used to detect and isolate attackers.

In addition, information from threat intelligence helps response teams better understand attacker tactics and techniques, speeding response time and minimizing the impact of incidents.

**Application security**

Threat Intelligence helps identify security vulnerabilities and their associated exploits. For example, if zero-day vulnerabilities or SQL Injection or Cross-Site Scripting (XSS) attacks are identified, this information can be used to protect applications in development or production.

Also help protect applications by analyzing the techniques used by attackers to exploit applications so that security teams can apply proactive protection measures.

**Vulnerability management**

Threat intelligence provides information about emerging vulnerabilities and specific exploits, providing context about threats targeting specific vulnerabilities. This allows security teams to prioritize security patches and updates based on the risk and impact of an attack.

For example, if threat intelligence signals an increase in attacks targeting a specific vulnerability (for example, a vulnerability in the software being used), the vulnerability management team will be able to act quickly to apply patches or implement countermeasures. migration.

**Perimeter security**

Threat Intelligence supports perimeter security solutions (such as firewalls, IDS/IPS, and intrusion prevention systems) by providing information about malicious activities or new attack techniques. Thus, security teams can configure security rules and filters to block malicious traffic or detect unusual activity.

**Development of security policies**

Threat intelligence can influence the development of security policies by providing information about recent threats and trends in cyber-attacks. This enables the organization to adopt more appropriate policies and proactively protect against the latest threats.

For example, if threat intelligence identifies a trend in increasing phishing or ransomware attacks, the organization can implement stricter policies regarding email management and user authentication.

**Endpoint security**

Threat intelligence can help protect endpoints (computers, mobile devices, servers) by providing indicators of compromise (IoCs) that can be integrated into endpoint security solutions to detect and remove malware before it can spread.

Thus, we observe that threat intelligence provides key information in the essential areas of ensuring cyber security:

- **Active and proactive security monitoring** - improves cyber-attack prevention capabilities;
- **Vulnerability management** - by prioritizing vulnerabilities based on perspectives and contexts provided by threat intelligence data;
- **Security incident response** - by accelerating incident investigations, analysis and countermeasures.

## 4. The benefits of Threat Intelligence as a support function

- *Risk anticipation:*

Threat intelligence helps organizations anticipate security risks, understand new attack techniques, and take preventative measures before attacks occur.

- *Improving collaboration between security teams:*

Threat intelligence information is useful to different teams in an organization (for example, incident management teams, network protection teams, application security teams), who can use the same data to create an integrated defense.

- *Faster and more effective response to attacks:*

With access to up-to-date threat intelligence, security teams can react faster and more accurately, limiting damage and recovery time in the event of an attack.

- *Reducing exposure and overload with false alerts:*

Threat intelligence helps organizations reduce false alerts and focus on real threats, saving resources and improving the efficiency of security processes.

## 5. The main types of malicious actors

Malicious actors in cybersecurity are individuals, groups, or organizations that conduct malicious activities to compromise systems, steal data, defame, espionage, or other illegal activities. Depending on their motivations and available resources, they can vary significantly. Below are the main types of malicious actors based on their intentions and goals:

### a. Cybercriminals

Persons or groups that commit illegal activities for financial purposes. Cybercriminals can include isolated individuals or organized groups that specialize in fraud, identity theft, data theft, and other illegal activities.

### b. Nation-states (State-Sponsored Actors / APTs)

Government or state-sponsored actors conducting cyber attacks for political, economic or military purposes. This type of actor is usually very well funded and has significant resources.

### c. hacktivist

Groups or individuals who use cyber attacks to promote their political, social or economic ideologies. These attacks are usually ideologically motivated and not primarily aimed at financial gain.

**d. Insider Threats**

These threats come from people inside the organization, such as employees, contractors, or business partners. Insiders can be both intentionally malicious and people who inadvertently cause harm.

**e. "Script Kiddies"**

The term refers to people, usually young or inexperienced, who use pre-built hacking tools (usually downloadable scripts and software) to launch cyber-attacks without deep knowledge of the domain.

Regardless of motivation, these actors pose a significant risk to organizations' cybersecurity, and to effectively protect themselves, organizations must understand the types of actors that threaten their infrastructure and implement appropriate safeguards.

### 5.1. Examples of Malicious Actors

**a. Anonymous**

- Type: Hacktivist
- Origin: decentralized
- Period of Activity: 2003 - present
- Targets: Brazil, Kazakhstan, Russia, Thailand, Turkey
- Techniques: Guy Fawkes mask, website defacement, DDoS, social media compromises
- Significant Attacks: Defacement of SOHH and AllHipHop websites (2008), Iranian election protests (2009), Operation Facebook (2011), Occupy Wall Street (2011), Syrian Government E-mail Hack (2012), Vatican website DDoS Attacks (2012) ), Federal Reserve ECS Hack (2013), Operation Hong Kong (2014), Operation KKK (2015).

**b. The Lazarus Group**

- Type: Advanced Persistent Threats (APT)
- Origin: Pyongyang, North Korea
- Period of Activity: 2010 - present
- Targets: Bitcoin, Cryptocurrency, Ecuador, Mexico, Sony Corp, South Korea, United States
- Techniques: DDoS, EternalBlue, Mimikatz, Wannacry, Zero-days
- Significant Attacks: 2014 Sony Pictures Hack, Operation Troy

## 6. Collecting relevant data from public reports

Gathering Threat Intelligence from public reports involves pulling data from various sources and formats. Here are some essential items that can be obtained:

**a. Indicators of Compromise (IoCs):**

IP addresses, domains, file hashes, URIs and URLs that are associated with malware or attack activities. The tactics, techniques, and procedures (TTPs) used by attackers. These are described in detail in reports that are based on attack models, such as the MITER ATT&CK Framework.

**b. Campaign and attack analytics:**

Reports published by security firms often provide descriptions of attack campaigns (eg, APT attacks), including information about the actors involved, their goals, and the methods used. Attacker groups: Some reports will provide information about specific attackers or hacker groups, such as APT28, Lazarus Group, or Charming Kitten.

**c. Emerging vulnerabilities and exploits:**

Data on recent vulnerabilities and exploits that may affect organizational infrastructure is particularly important. These are usually documented in CVEs (Common Vulnerabilities and Exposures) and can be found in security reports.

**d. Critical infrastructure security:**

Some public reports focus on specific threats to critical sectors such as energy, health, transportation and finance. For example, government organizations and security solution providers publish detailed reports on cyber-attacks targeting these sectors.

### 6.1. Tools for analyzing and visualizing Cyber Threat Intelligence

There are a number of **software tools** that can help collect, analyze and visualize **Threat Intelligence data** from public reports, such as:

- ***SIEM (Security Information and Event Management)***: Tools such as **Splunk, Elastic Stack** or **IBM QRadar** allow the collection, correlation and visualization of data from multiple sources, including public reports, to create a clear view of security risks and events.
- ***Threat Intelligence Platforms (TIPs)***: Platforms such as **ThreatConnect**, **MISP**, **Anomali** or **AlienVault OTX** enable the collection, analysis and distribution of Threat Intelligence information from open and private sources.
- ***OSINT Tools*: Open Source Intelligence (OSINT)** tools, such as **Shodan**, **VirusTotal, Censys**, or **Spyse**, can help identify suspicious activity and vulnerabilities in public sources and correlate them with actual attacks.

### 6.2. Email-based Threat Intelligence collection using the AlienVault OTX platform

In this article, we set out to analyze **the email service,** given the essential role it plays within an organization, as well as considering the high degree of exposure it offers. Thus, we set out to identify the types of attacks that use **the service** of e-mail as a propagation vector.

**AlienVault OTX (Open Threat Exchange)** platform contains collections of Indicators of Compromise (IoCs), shared by the community. Platform members can share indicators of compromise (IoCs) such as malicious IP addresses, domains, URLs, file hashes and more.

**AlienVault OTX (Open Threat Exchange) is an** open-source and collaborative **Threat Intelligence** platform created by **AT&T Cybersecurity** that enables organizations and security professionals to collect, share and analyze information about cyber threats (Figure 1).

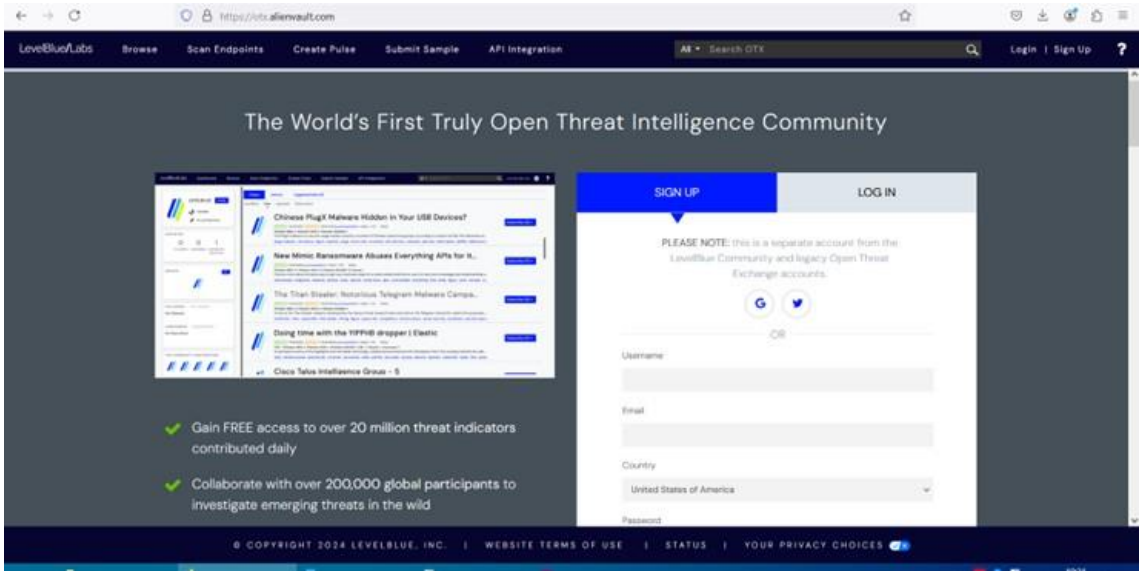


**Fig. 1.** AlienVault OTX (Source: https://otx.alienvault.com/)

As we can see in the following image (Figure 2), the platform brings together, at this time, 92 million Indicators of Compromise (IoCs), and the existing pulses are 320,000.

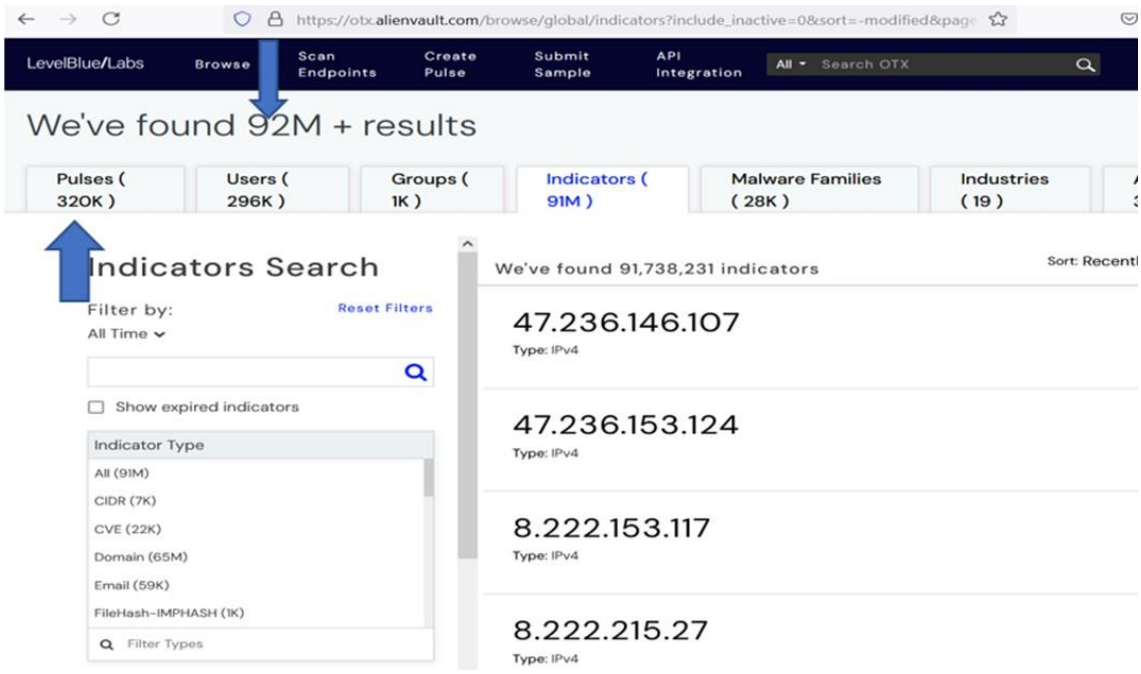


**Fig. 2.** Indicators of Compromise (IoCs)

Indicators of Compromise (IoCs) are basically attack indicators that help identify and prevent attacks. These indicators may include: IP addresses: addresses associated with malicious activities; Domains and URLs: Websites used by attackers to launch phishing or malware campaigns; File Hashes: Hashes that help identify malicious files; Email addresses: used in phishing or spam attacks.

Threat Pulses are sections of information that users can view or add to the platform. Each pulse is a description of an attack or threat campaign and contains detailed data about the tactics, techniques and procedures (TTPs) used by the attackers. Pulses can be added by users and are public, allowing stakeholders to access global threat information.

From the **AlienVault OTX platform** we will extract, with the help of filters, the relevant information from the perspective of the service under analysis: thus, in the Indicator Type section we select the email service, and in the Role section, we choose the Delivery Email parameter in conjunction with Ransomware, we notice that HAVE over 750 indicators, which represent email addresses used by malicious actors in various attacks (Figure 3).

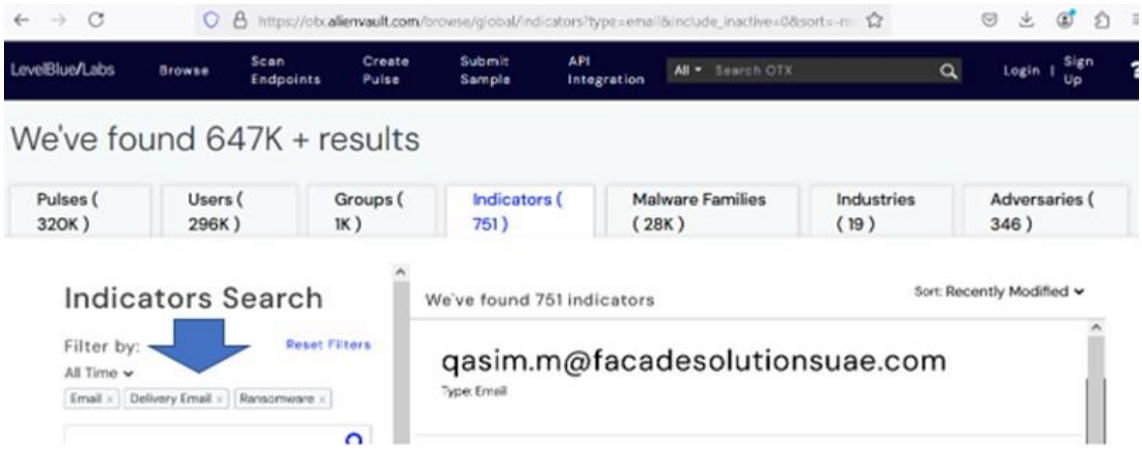


**Fig. 3.** The Indicator Type section

In these circumstances, reactive data analysis involves a comparison between the data collected at the level of equipment that ensures the perimeter protection of e-mail servers and this list of results, in order to update the security policies that ensure the protection of e-mail servers. By doing this, we ensure that all known threats do not reach the email client (in the recipient's inbox).

After collecting the data from the public reports, a careful analysis is required to interpret them correctly and apply them in the context of the organization. Properly understanding the context in which the threats were detected is essential. For example, information about a ransomware attack targeting the financial sector may be relevant to a bank, but not to a transport company.

After analyzing and interpreting the data, organizations can adjust security strategies to protect against identified threats. This may include applying security patches, updating firewall rules, strengthening authentication measures.

## 7. Conclusions

At the core of threat intelligence is understanding the cybersecurity landscape and monitoring emerging forms of malware, zero-day exploits, phishing attacks, and other cybersecurity issues.

Gathering and analyzing Threat Intelligence is an essential element in protecting organizations against cyber-attacks. By obtaining up-to-date information from open sources, organizations can better understand the threat landscape and implement proactive measures to protect their infrastructure and sensitive data. The process includes identifying relevant information sources, collecting data, analyzing it in the organization's specific context, and using appropriate tools to visualize and integrate it into security strategies.

## References

[1]. https://www.microsoft.com/ro-ro/security/business/security-101/what-is-cyber-threat-intelligence

[2]. https://www.bitdefender.com/en-us/blog/businessinsights/targeted-threat-intelligence-for-security-operations/

[3]. https://www.bitdefender.com/ro-ro/business/products/advanced-threat-intelligence

[4]. R. Trifonov, O. Nakov, V. Mladenov, "Artificial Intelligence in Cyber Threats Intelligence". 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC). IEEE. pp. 1-4. doi: 10.1109/ICONIC.2018.8601235. ISBN 978-1-5386-6477-3. S2CID 57755206.

[5]. CyberProof Inc. (n.d.). Managed Threat Intelligence. CyberProof. Retrieved on April 03, 2023 from https://www.cyberproof.com/cyber-101/managed-threat-intelligence/

[6]. Dalziel, Henry (2014). How to Define and Build an Effective Cyber Threat Intelligence Capability. Syngress. ISBN 9780128027301.

[7]. Kant, Neelima (2024). "Cyber Threat Intelligence (CTI): An Analysis on the Use of Artificial Intelligence and Machine Learning to Identify Cyber Hazards". Cyber Security and Digital Forensics. Lecture Notes in Networks and Systems. Vol. 36. pp. 449-462. doi: 10.1007/978-981-99-9811-1_36. ISBN 978-981-99-9810-4.

[8]. Conti, M. (2021). "Measuring and Visualizing Cyber Threat Intelligence Quality". International Journal of Information Security. 20:21-38. doi: 10.1007/s10207-020-00490-y.

[9]. Shackleford, D. (2015). Who's Using Cyberthreat Intelligence and How?. SANS Institute. https://cdn-cybersecurity.att.com/docs/SANS-Cyber-Threat-Intelligence-Survey-2015.pdf