СУБЕКТИ И УПРАВЛЕНИЕ НА КИБЕР ЗАПЛАХИТЕ

CYBER THREAT ACTORS AND CYBER THREAT MANAGEMENT

Александра Станковска
Aleksandra Stankovska

Abstract: *Cyberspace is an exciting, dynamic and ever-evolving arena of challenge and opportunity. This paper provides an overview of cyber threats actors, cyber threat intelligence and cyber threat management. Cyber threat actors have a global reach and cyber threat mitigation strategies need to be considered through a global lens. Cyber threat intelligence and management, defined as the protection of systems, networks and data in cyberspace, is a critical issue for all businesses.*

Key words: *cyberspace, cyber threats actors, cyber threat intelligence, cyber threat management*

INTRODUCTION

Digital technology continues to transform and disrupt the world of business, exposing organizations to both opportunities and threats. So it's hardly surprising that cybercrime continues to escalate – ranking as this year's second most reported economic crime.

Cyber-attacks can be simple or sophisticated, take unexpected forms and come from unknown sources. They can be aimed at unsuspecting victims or high profile targets. They can start, and stop, without a trace. Cyber threat relates to the source of a particular attack. By analyzing and understanding threats, security policies and procedures can be created to protect against certain types of cyber-attacks. Vulnerabilities refer to a security flaw that could lead to a successful attack. Testing for vulnerabilities allows for constant monitoring of weaknesses and gaps in a system and also helps identify what types of network vulnerabilities to test for in the future.

As cyber threats grew in scale and complexity, the industry realized the gap between perceived threat and real threat. This led to the emergence of threat landscape monitoring and threat intelligence capabilities. Cyber threat intelligence strengthens response capabilities by supplying the required information, which can be made actionable and help enterprises prepare for emerging threats.

Cyber threats actors could be financially or socially motivated hackers, disgruntled employees, organized criminal gangs, competitors or state actors. Some of these actors are well trained and will persist a campaign to achieve their goal of data theft or damage over weeks to months. A well organized cyber threat management is needed to detect and stop these threats.

CYBER THREAT ACTORS

To better understand the cyber threats, we need to understand who is behind them. A threat actor, also called a malicious actor, is an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an organization's security. In threat intelligence, actors are generally categorized as external, internal or partner. With external threat actors, no trust or privilege previously exists, while with internal or partner actors, some level of trust or privilege has previously existed. External actors are the primary concern of threat intelligence services not only because they are the most common, but also because they tend to be the most severe in terms of negative impact.[1]

In cybercrime, three distinct classes of threat actor has been identified: the Cyber Criminal, the Cyber Terrorist, and the Hostile State.[2] Verisign iDefense Security Intelligence Services classifies cyber-attacks into three categories: Hacktivism, Cyber Crime and Cyber-Espionage.[3]

Hacktivism actors can be quite loud in comparison to other threat actors, often using social media to discuss operations and to recruit members to attack a target. Hacktivist groups such as Anonymous use many of the same tools employed by financially-motivated cybercriminals to detect website vulnerabilities and gain unauthorized access or carry out distributed denial-of-service (DDoS) attacks. The motivation of most hacktivists is to gain access to sensitive information that will negatively impact the reputation of an individual, a brand, a company or a government.[4]
Common hacktivist attack vectors include:[5]

---

[1] http://whatis.techtarget.com/definition/threat-actor
[2] https://www.globalservices.bt.com/.../financial.../Finance_sector_Cyber_Final
[3]http://www.circleid.com/posts/understanding_the_threat_landscape_cyber_attack_actors_and_motivations
[4] http://whatis.techtarget.com/definition/threat-actor
[5]http://www.circleid.com/posts/understanding_the_threat_landscape_cyber_attack_actors_and_motivations

- ✓ Distributed Denial of Service (DDoS) attack: A malicious attempt to debilitate networks, Web-based applications, or services by using a large number of networked computers to overwhelm these assets with resource requests, or impair them in some other way.
- ✓ Website defacement: Changing the appearance of a website via unauthorized access such as through a cross-site scripting vulnerability.
- ✓ Information disclosure: Publicizing information about the targeted institution that was not previously publicly known or releasable.
- ✓ Doxing: The publication of personally identifiable information (PII) about a specific person for malicious purposes.

Cyber crime is groups of criminals that intend to engage in illegal activity, most commonly for monetary profit. Attacks are designed to either extort money from the target, or the actors are funded to carry out an attack.[6]

Table 1. Actor: Who Conducted The Attack/Will Conduct The Attack?

Category	Description	Examples
State-sponsored	The Actor or group is employed by the government of a nation-state.	Chinese government hackers, National Security Agency (NSA), United Kingdom Government Communications Headquarters
Individual	A specific person or group acting on their own, and not a member of any other Actor threat category.	Kid at school brings down school network 'for fun'. Group of people that deface sites in hopes of impressing someone (no political reason)
Hacktivist	An actor that performs attacks in order to draw attention to a cause (such as free speech or human rights), or hinder the support of a cause. If the cause is political, and/or designed to inflict terror, they are instead considered a Cyber terrorist.	Anonymous, Lulzsec_root, Syrian Electronic Army

[6] https://www.surfwatchlabs.com/threat-categories#Actor

Cyber terrorist	Actor carries out an attack designed to cause alarm or panic with ideological or political goals.	Alternatively, if the actor is party to a known terrorist organization.
Organized Crime	Groups of criminals that intend to engage in illegal activity, most commonly for monetary profit. Attacks are designed to either extort money from the target, or the actors are funded to carry out an attack.	Producers of ransomware, Black-market data thieves
Identity Unknown	Actor is not identified within the document, either by handle or affiliation.	A report indicates that abc.com has been taken down by an attacker, with no additional information.
Organization	Organizations not specifically associated with information security but having some affect over the information security space.	Microsoft patch release notes, organization deploying new firewall/security measures
Information Security	Includes organizations or persons from, or whose actions affect, the Information Security sector. These are security researchers, computer scientists, antivirus vendors, CERTs, threat intelligence (non-state-sponsored).	Brian Krebs, IntelCrawler, Kaspersky Lab
Law Enforcement /Authority	Will include anyone involved in law enforcement (police, police cybercrime units, courts, judges) as well as attorneys and lawyers.	INTERPOL, United States Attorney, NYPD, Baltasar Garzon

Source: https://www.surfwatchlabs.com/threat-categories

Cybercriminal enterprises vary in size and typically involve persons working together, though they may not know each other in real life. They rely on Web-based forums, ICQ , Jabber and Internet Relay Chat (IRC) for communication and for the recruitment of prospective partners. Data stolen in cybercrime attacks is often circulated on the black market where it is made available for purchase via forums and automated Web shops.

Data cyber-criminals frequently seek includes:[7]

- ✓ ATM and point-of-sale (PoS) skimming: Stealing bank and PIN information when cards are used at ATMs, credit/debit card terminals and other card readers.
- ✓ Random Access Memory (RAM) scraping: Stealing credit/debit card information when the card information is stored in the server's memory system.
- ✓ Code injection: Introducing malicious code into a computer program to redirect the system's actions.
- ✓ Keylogging: Using a program to record computer keystrokes in order to gain confidential information.
- ✓ Phishing: Creating fraudulent, socially engineered electronic content (websites, emails, etc.) that is from a seemingly legitimate source, enticing victims to provide confidential information.

State-sponsored espionage (the actor or group is employed by the government of a nation-state), also referred to as Advanced Persistent Threat (APT), is typically very quiet and practices operational security. The main objective is to support a nation state's economic, political or military objectives.[8]

The advent of the digital world, and the inherent interconnectivity of people, devices and organizations, opens up a whole new playing field of vulnerabilities. The attacking power of criminals is increasing at an astonishing speed. Attackers have access to significant funding; they are more patient and sophisticated than ever before; and they are looking for vulnerabilities in the whole operating environment — including people and processes. Threat actors are constantly inventing new tools and techniques to enable them to get to the information they want and are getting better at identifying gaps and unknown vulnerabilities in an organization's security.[9]

CYBER THREAT INTELLIGENCE

The discipline of cyber threat intelligence focuses on providing actionable information on adversaries. This information is becoming

---

[7]http://www.circleid.com/posts/understanding_the_threat_landscape_cyber_attack_actors_and_motivations/

[8] http://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.

[9]http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey 2014/$FILE/EY-global-information-security-survey-2014.pdf

increasingly important to enterprise cyber defense. This importance has resulted in investment and creation of many new/innovative sources of information on threat actors. Within the context of cyber-security, threat intelligence represents the synthesis of information detailing potential threats with a solid understanding of network structure, operations, and activities.[10]

Cyber threat intelligence (CTI), is organized, analyzed and refined information about potential or current attacks that threaten an organization. The primary purpose of threat intelligence is helping organizations understand the risks of the most common and severe external threats, such as zero-day threats, advanced persistent threats (APTs) and exploits. Although threat actors also include internal (or insider) and partner threats, the emphasis is on the types that are most likely to affect a particular organization's environment. Threat intelligence includes in-depth information about specific threats to help an organization protect itself from the types of attacks that could do them the most damage.

Since the earliest days of the cybersecurity industry, security professionals have focused on identifying network vulnerabilities and then implementing solutions to either eliminate or reduce the vulnerability. This is a widely used practice and is generally effective in mitigating cybersecurity risks, however it results in millions of dollars spent needlessly each year to address vulnerabilities that pose little, to no risks.[11]

Figure 1. Five key sources of cyber threat intelligence

Cloud Threat Feeds: - Cisco (Threat Grid) - Symantec (DeepSight) - McAfee - FireEye	Open Source: - Exploit –db - Metasploit - Open Threat Exchange (Alien Vault)	Security Products: - Endpoint Security (McAfee, Symantec, Trend Micro) - NIPS (Source File)
Vendor Neutral: - CVE,SWE - CPE	Vendor Specific: - Cisco - Checkpoint	

Source: sourcehtt://digitally.cognizant.com/cyber-threat-intelligence-matters/

[10] https://www.cert.gov.uk/wp-content/uploads/2015/03/An-introduction-to-threat-intelligence.pdf

[11] https://www.mdcyber.com/blog/understanding-cyber-threats-and-vulnerabilities

Cyber threat intelligence (CTI) is an advanced process that enables the organization to gather valuable insights based on the analysis of contextual and situational risks and can be tailored to the organization's specific threat landscape, its industry and markets. This intelligence can make a significant difference to the organization's ability to anticipate breaches before they occur, and its ability to respond quickly, decisively and effectively to confirmed breaches — proactively maneuvering defense mechanisms into place, prior to and during the attack.[12]

Security analytics in a network defence setting usually takes one of two forms: 1. 'Big data' platform crunching network data to ascertain trends 2. Security information and event management (SIEM) infrastructure with rules set up to automate the detection of anomalous activities; both of these are stand alone and do not require threat intelligence to function, however they are informed by it at a strategic and operational level.[13]

The idea behind cyber threat intelligence is to provide the ability to recognize and act upon indicators of attack and compromise scenarios in a timely manner. While bits of information about attacks abound, cyber threat intelligence (CTI) recognizes indicators of attacks as they progress, in essence putting these pieces together with shared knowledge about attack methods and processes.

The fundamental assumption of CTI is that the planning, resourcing and execution of an attack is not instantaneous, it does require human intervention and it can take up to years in case of the advanced persistent threats. Organizations can use this time to analyze information and gather intelligence that can be used to understand the tools and techniques used by the attackers and try to interfere with each of the attack phases, overall referred to as the kill chain.

CYBER THREAT MANAGEMENT

Leaders need to take a holistic approach to cybersecurity planning and management. Cyber Threat Management (CTM) is an advanced management program enabling early identification of threats, data driven

---

[12] ttp://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.pdf

[13]https://www.cert.gov.uk/wp-content/uploads/2015/03/An-introduction-to-threat-intelligence.pdf

situational awareness, accurate decision-making, and timely threat mitigating actions.[14] CTM includes:

✓ Manual and automated intelligence gathering and threat analytics.

✓ A comprehensive methodology for real-time monitoring including advanced techniques such as behavioral modeling.

✓ Use of advanced analytics to optimize intelligence, generate security intelligence, and provide Situational Awareness.

✓ Technology and skilled people leveraging situational awareness to enable rapid decisions and automated or manual actions.

Figure 2. CTM existing practice areas

Source: www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

Key Cyber Risk Management Concepts:[15]

➢ Incorporate cyber risks into existing risk management and governance processes. Managing cybersecurity risk as part of an

[14] https://ioctm.org/What-is-Cyber-Threat-Management
[15]https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf)

organization's governance, risk management, and business continuity frameworks provides the strategic framework for managing cybersecurity risk throughout the enterprise.

- Elevate cyber risk management discussions to the CEO. Regular communication between the CEO and those held accountable for managing cyber risks provides awareness of current risks affecting their organization and associated business impact.
- Implement industry standards and best practices, don't rely on compliance. A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems, along with processes to be informed of current threats and enable timely response and recovery. Using a risk based approach to apply cybersecurity standards and practices allows for more comprehensive and cost effective management of cyber risks than compliance activities alone.

Cyber Threat Management Framework (CTMF) is a comprehensive framework build upon the OODA (Observe, Orient, Decide, Act) decision cycle that enables cyber threat management with the speed and agility needed in today's real-time dynamic threat environment:[16]

- Observe:
  - Detect use case development
  - Content architecture
  - Use case optimization
  - Use case control testing
  - Honeypot development
  - Sensor data
  - Use case cost modeling
- Orient:
  - Intelligence gathering
  - Intelligence data mining
  - Risk assessment
  - Control assessment
  - Behavior modeling
  - Context enrichment
  - Threat data warehousing
  - Security Data Science
- Decide:
  - Situational awareness

[16] https://ioctm.org/Cyber-Threat-Management-Framework

- Automated triage
- Security analyst (human) triage

➢ Act:

- Malware Analysis
- Automating responses
- Incidents Response
- Response operations
- Security Operations Center

The key benefits of CTMF are: early detection of threats, instant recognition of potential impact, faster decision for expedient & damage limiting actions.

CONCLUSION

Cyber threats to a control system refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. To protect corporate data from cyber threats, companies need to have the right security technology, policies, and operations in place. But perhaps most important is having the right information.

Cyber threat intelligence is an advanced process that enables an organization to continually gather valuable insights based on the analysis of contextual and situational risks and can be tailored to the organization's specific threat landscape, its industry and markets. By constantly quantifying and qualifying threats in cyberspace, cyber threat intelligence can help decision makers and security teams get ahead of cybercrime by providing timely, accurate, actionable and relevant intelligence via a dynamic cycle of planning, collecting, processing, analyzing, vetting, and dissemination processes.

Cyber threat management is an advanced management program enabling early identification of threats, data driven situational awareness, accurate decision-making, and timely threat mitigating actions. The goal of a cyber threat management system is to protect the confidentiality, integrity and availability of information assets.

REFERENCE

http://www.trendmicro.co.uk/technology-innovation/cyber-security/

https://www.actiac.org/sites/default/files/cybersecurity-innovation.pdf

https://www.isightpartners.com/wpcontent/uploads/2014/07/iSIGHT_Partners_What_Is_20-20_Clarity_Brief1.pdf

http://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.pdf

https://www.ida.liu.se/~johsi32/docs/JMS_4-1_Sigholm_Non-State_Actors_in_CyberOps.pdf

http://www.circleid.com/posts/understanding_the_threat_landscape_cyber_attack_actors_and_motivations/

https://www.surfwatchlabs.com/threat-categories

https://www.globalservices.bt.com/.../financial.../Finance_sector_Cyber_Final

http://whatis.techtarget.com/definition/threat-actor

http://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.

http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

15.http://cyber.lockheedmartin.com/hubfs/docs/Reports/ponemon-risk-and-innovation-in-cybersecurity-investments-2015.pdf

1https://www.sans.org/reading-room/whitepapers/basics/cyber-security-management-system-conceptual-mapping-591

http://www.ey.com/Publication/vwLUAssets/EY-cyber-program-management/$FILE/EY-cyber-program-management.pdf

http://www.ey.com/Publication/vwLUAssets/EY-cyber-breach-response-management/$FILE/EY-cyber-breach-response-management.pdf

www.ey.com/Publication/vwLUAssets/EY-how-do-you-find-the-criminal-before-they-commit-the-cybercrime

https://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375

http://www.isaca.org/Journal/archives/2015/Volume-1/Documents/Effective-Cyberthreat-Management-Evolution-and-Beyond_joa_Eng_0115.pdf

https://www.cert.gov.uk/wp-content/uploads/2015/03/An-introduction-to-threat-intelligence.pdf
https://ioctm.org/Cyber-Threat-Management-Framework