Profile of Persons Who Act in the Field of Computer Criminality

Vasile-Cătălin GOLOP, Natalia SĂVULESCU
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
catalin.golop@academiadepolitie.ro, natalia.savulescu@academiadepolitie.ro

Abstract

This article examines the profile of individuals involved in cybercrime activities, focusing on their psychological traits, motivations and technical skills. The study identifies common typologies of cybercriminals, ranging from individual hackers to organized groups, and examines the factors that contribute to choosing this type of illegal activity, such as social influences and opportunities in the online environment. The research hypothesis argues that individuals who commit cybercrime exhibit distinct characteristics that vary according to their goals and resources. The research method used combines case analysis with interviews and comparative studies, highlighting the diversity of profiles and the adaptability of offenders to emerging technologies. The results provide useful insights for implementing preventive measures and streamlining cybercrime investigations.

Index terms: cybercrime, phishing, website, cyberattack, financial crime

Introduction

The profile of people involved in computer crime (cybercrime) varies considerably, but there are some common characteristics that can be identified. This category of people can have diverse motivations and different levels of technical skills, which leads to different types of cyber attacks [1].

Most cybercriminals have good knowledge of IT and computer security. They can be programmers, network engineers, or even cyber security experts. In many cases, these skills are acquired formally (by studying computer science), but they are also often self-taught. They vary in age, but most of them are young, often between 18 and 35 years old. This is largely due to early access to technology and their ability to quickly adapt to new technologies.

Many hackers commit cybercrimes for financial gain, either through data theft or online fraud (e.g. phishing, ransomware, identity theft) [2]. Some cybercriminals are motivated by a political or social cause and engage in "hacktivism" attacks to promote ideas or beliefs. Some of these hackers are motivated by revenge, usually against former employers, business partners or people in their personal lives, as well as a desire to demonstrate their skills or gain respect in a particular cyber community.

1. Types of people who carry out attacks:

- **script kiddies**: people who do not have advanced knowledge, but use tools already created by others to carry out attacks [3].
- **professional hackers**: people with very advanced knowledge, able to write code and exploit complex vulnerabilities. They can work in teams or in organized groups.
- **hacktivists**: those who commit computer attacks to promote a political or ideological cause, such as groups like Anonymous [4].

2. Level of organization:

- **Individual criminals**: Hackers acting on their own are common, especially in small-scale financial fraud or phishing attacks.
- **Organized groups**: In cases of complex attacks, such as those orchestrated by organized crime groups or state-sponsored groups (APT - Advanced Persistent Threat), cybercriminals work in structured teams with a clear distribution of roles [5].

Cybercriminals are very aware of the need to protect their identity, so they use advanced anonymization tools such as TOR networks, VPNs, and data encryption. Some hackers are affiliated with organized crime networks or work for governments in espionage or cyber sabotage operations.

In short, the profile of cybercriminals is complex and diverse, ranging from isolated individuals with limited knowledge to well-organized and well-financed groups carrying out sophisticated attacks.

I. Typology of cybercriminals: classification based on level of expertise and motivation

Hackers who engage in online criminal activity vary significantly in their technical skills and motivations. Their classification provides a clear picture of the diversity of threats in cyberspace and the complexity of cybercriminal behavior.

1. Script kiddies. These hackers have little technical knowledge and do not create their own tools. Instead of developing attacks, they use software, scripts and tools available online, created by more experienced hackers. They often don't fully understand how the attacks they launch work.

Script kiddies generally do not have a major financial or ideological purpose. They attack systems to prove their skills to others, to gain some recognition in online communities, or simply out of boredom (motivation for attacks - *fun, social validation and curiosity*). They are responsible for simple attacks such as defacing websites or DoS (Denial of Service) attacks.

Example of attack: *a teenager launching a DDoS attack on an online gaming site using a tool found on public hacking forums*.

2. Black hat hackers. These hackers have extensive knowledge of operating systems, networks and software vulnerabilities, and are able to develop and implement their own cyber attacks. Black hats are malicious hackers, often involved in illegal activities for personal gain (technical skills - *advanced)* [6].

They are primarily motivated by money and are involved in activities such as stealing personal data, credit cards, financial fraud, ransomware and selling information on the dark web. This group represents a large part of organized cybercrime.

Example of attack: *a hacker who develops and distributes malware to steal banking data from unsuspecting users and then sell it on dark web markets.*

3. White hat hackers. These hackers have similar or even superior technical skills to black hats but use their knowledge for legitimate and legal purposes. They work in the cyber security industry to detect and correct security vulnerabilities (technical skills - *very advanced)* [7].

White hats are motivated by the desire to protect computer systems and users from cyber attacks. They may work as security analysts, pen-testers (penetration testers), or in other roles that involve assessing and improving the security of computer systems.

Attack example*: A security specialist performing penetration tests on an e-commerce system to discover vulnerabilities and prevent potential attacks.*

4. Gray hat hackers. Gray hat hackers have skills similar to black hats and white hats, but they use these skills in an ethically ambiguous way. They can break laws or rules without explicit malicious intent, but often without the victims' consent (technical skills - *advanced)* [8].

Gray hats are motivated by technological curiosity and a desire to demonstrate their skills. While not acting out of malice, they can break into systems without permission, and then inform

owners of discovered vulnerabilities, sometimes asking for a reward (motivation of attacks **-** *curiosity, recognition and sometimes ethical*).

Example attack: *a hacker who breaks into a government system without permission, only to later report the breach and provide security solutions.*

5. Hacktivists. Some hacktivists have advanced technical knowledge, while others use tools available to the general public. They usually attack government, corporate or public interest websites (technical skills - *range from limited to advanced)*.

Hacktivists are motivated by a desire to advance a political, social or ideological cause. They use cyber attacks to draw attention to issues they support or to sabotage organizations and governments that run counter to their beliefs.

Example attack: *groups such as Anonymous, which launch DDoS attacks on government websites to protest certain policies or events*.

6. Offenders from organized groups (cybercrime gangs). These groups are made up of hackers with varying skills, from malware and exploit developers to networking and cryptography experts. They often operate at a sophisticated level, carrying out well-planned and coordinated attacks (technical skills - *very advanced*) [9].

Criminals in organized groups are motivated by financial gain and often have corporate structures. These groups develop fraud schemes, ransomware, phishing, cyberespionage and other forms of cybercrime on a large scale. Some groups are supported by states and are involved in espionage or attacks on critical infrastructure.

Example of attack: *groups like REvil or Conti that launch ransomware attacks on companies and demand enormous sums for data decryption.*

7. State-Sponsored hackers. These hackers are part of highly trained teams, often supported financially and logistically by states or governments. They have access to considerable resources and have the ability to carry out highly sophisticated cyber-attacks (technical skills **-** *extremely advanced*) [10].

States sponsoring such hackers use cyber attacks as weapons in international political and economic conflicts. They can target cyber espionage, destabilizing critical infrastructures or influencing political processes.

Example of attack: *government-backed hacker groups, such as APT28 (Fancy Bear) or APT29 (Cozy Bear), involved in cyber espionage and political influence campaigns.*

This classification highlights the diversity in the world of cybercriminals, each with their own skills and motivations. Understanding the identity of these hackers and their operating techniques is critical to developing effective cybersecurity defenses.

II. Child pornography

The impact of the level of expertise on the types of attacks launched and the economic and security consequences in the context of the dissemination of child pornography online is a complex and sensitive subject, involving not only technical aspects, but also legal, psychosocial and ethical dimensions. In this analysis, we explore how different levels of technical expertise of criminals influence the dissemination of illegal content and the economic and security implications arising from these activities.

1. The level of expertise and types of attacks used in the dissemination of child pornography

Differences in technical skills influence the methods used to disseminate and conceal criminal activity related to child pornography.

In the case of child pornography, **script kiddies** can distribute the material through peer-to-peer (P2P) networks or through social networks using fake accounts and simple VPNs to hide their

identity. Their activity is relatively easy to detect because they do not use advanced encryption or anonymization methods. However, given the large volume of content disseminated through common platforms, the ability of authorities to intercept all cases is limited, creating a major vulnerability for the protection of minors.

Black Hat hackers use advanced techniques to avoid detection, such as encrypting files, using anonymous networks such as *Tor* or *I2P*, and manipulating meta data to hide digital traces. They can create and use dark web forums that are encrypted and password protected to disseminate child pornography. Some of them may also be involved in *cyberlockers* - sites that host illegal password-protected files.

The activity of these hackers is much more difficult to detect and has serious consequences for cyber security. Encrypted and anonymous networks such as Tor greatly complicate efforts by authorities to identify and dismantle such networks. Also, the criminal economy surrounding these platforms is vast, including both direct sales and material exchanges, making it nearly impossible to trace the financial flow.

Organized crime groups use sophisticated and well-coordinated infrastructures to manage large child pornography dissemination platforms. These networks use hidden servers, *bulletproof hosting* infrastructure (which provides dedicated hosting services for illegal activities), and cryptocurrencies for payments. These groups can also create *pay-per-view platforms*, where users pay to access illegal content [11].

Networks run by organized groups have a devastating impact on global security as they systematically exploit vulnerabilities in networks and use cryptocurrencies to evade financial tracking. In addition to promoting the sexual abuse of minors, these networks generate substantial income from illegal activities, funds that can be used for other forms of cybercrime. The dissemination of child pornography in this setting can become part of a wider ecosystem of organized crime, including human trafficking.

2. The economic and security consequences of the dissemination of child pornography

This type of dissemination has major consequences, both economically and from a security point of view, and these vary according to the level of sophistication of the networks involved.

Authorities are devoting considerable resources to investigating and dismantling networks involved in the distribution of child pornography. In cases where criminals use advanced encryption and anonymization technologies, investigative efforts become very expensive and time-consuming. For example, operations involving infiltration in dark web networks or tracking cryptocurrencies can take years and require international collaboration.

Hosting services and digital infrastructure can be compromised by criminal groups that use these resources to host illegal content without the operators' knowledge. This affects the reputation of the companies involved and can lead to substantial economic losses. In addition, the use of cryptocurrencies in transactions related to illegal content undermines trust in these technologies, affecting emerging digital payment markets [12].

Networks that distribute child pornography are also often involved in other illegal activities, including cyberattacks, data theft, and espionage. For example, servers hosting illegal material can be compromised to launch *botnet attacks*, thereby using a criminal infrastructure for massive cyber attacks on organizations and governments [13]. In this way, criminals create a multifunctional digital crime infrastructure that affects global security. Also, this type of networks is often linked to human trafficking rings, which exacerbates the impact of these crimes on victims. In addition, these criminals create a demand for such materials, encouraging continued abuse of minors and generating an illegal market that is difficult to suppress.

III. Relevant case studies

Operation "Playpen" (2015)

The FBI conducted a large-scale operation targeting a global child pornography network, *Playpen*, hosted on the dark web. This network, accessed through *Tor*, had approximately 150,000 users. The FBI used a legal hacking technique to compromise Playpen users and identify them. In this operation, it was revealed that well-organized criminal groups use sophisticated infrastructures and advanced anonymization, which made it difficult for the authorities to intervene [14].

Consequences: Authorities were able to identify and arrest thousands of users globally, but the operation was costly and generated legal debate over the use of hacking by authorities.

Operation Blackwrist (2017)

Police in Thailand, working with Europol and other international agencies, dismantled a child pornography network operating on the dark web and coordinated by an organized crime group. The materials were accessible on a subscription basis paid with cryptocurrencies [15].

Consequences: This case highlighted the role of cryptocurrencies in financing cybercrime and showed how difficult it is for authorities to track anonymous payments. The operation led to arrests in several countries and the shutdown of several sites involved.

Conclusions

The level of expertise of criminals in this field who handle, in any way, child pornography has a direct impact on the types of attacks used and the difficulty with which the authorities can intervene. Those with very advanced knowledge create well-hidden networks, using encryption and anonymization, which makes combating these crimes extremely difficult. The economic and security consequences are major, affecting both infrastructures and trust in digital technologies, while suppressing this activity requires significant resources and very good international coordination.

References

[1]. Manualul Investigatorului în Criminalitatea Informatică, Ministerul Comunicațiilor și Tehnologiei Informației [Online] Available: https://www.scribd.com/doc/268511908/Manualul-Investigatorului-Criminalitatii-informatice. Accessed: October 6, 2024.

[2]. Phishing: A Cyber-Security Guide for Employers and Individuals, Zywave, 2020 [Online] Available: www.sutcliffeinsurance.co.uk/wp-content/uploads/2020/03/Phishing-Attacks-Guide.pdf. Accessed: October 10, 2024.

[3]. https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie

[4]. https://www.imperva.com/learn/application-security/hacktivism/

[5]. Phising, raportul privind situația amenințărilor, European Union Agency for Cybersecurity, January 2019-April 2020 [Online] Available: www.enisa.europa.eu/publications/report-files/ETL-translations/ro/etl2020-phishing-ebook-en-ro.pdf. Accessed: October 14, 2024.

[6]. https://www.kaspersky.com/resource-center/threats/black-hat-hacker

[7]. https://www.hackerone.com/knowledge-center/white-hat-hacker

[8]. Convenția privind Criminalitatea Informatică, Council of Europe, 2023 [Online] Available: https://eur-lex.europa.eu/RO/legal-content/summary/convention-on-cyber crime.html Accessed: October 10, 2024.

[9]. Convenția privind Criminalitatea Informatică, Council of Europe, 2023 [Online] Available: https://eur-lex.europa.eu/RO/legal-content/summary/convention-on-cyber crime.html Accessed: October 10, 2024.
[10]. https://www.cyberpolicy.com/cybersecurity-education/state-sponsored-hacking-explained
[11]. https://www.consilium.europa.eu/ro/infographics/cyber-threats-eu/
[12]. Legea nr. 161 din 19 aprilie 2003 cu modificările și completările ulterioare, Romanian Parliament, Romanian Official Monitor nr. 279 din 21 aprilie 2003. [Online] Available: https://legislatie.just.ro/Public/DetaliiDocument/43323
[13]. Legea nr. 161 din 19 aprilie 2003 cu modificările și completările ulterioare, Romanian Parliament, Romanian Official Monitor nr. 279 din 21 aprilie 2003. [Online] Available: https://legislatie.just.ro/Public/DetaliiDocument/43323
[14]. https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years
[15]. https://www.interpol.int/News-and-Events/News/2019/50-children-rescued-9-sex-offenders-arrested-in-international-operation