MIT MANAGEMENT SLOAN SCHOOL
INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY
(IC)³

Cybercrime-as-a-Service: Identifying Control Points to Disrupt

Keman Huang
Michael Siegel
Stuart Madnick

Working Paper CISL# 2017-17

November 2017

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Cybercrime-as-a-Service: Identifying Control Points to Disrupt

KEMAN HUANG, MICHAEL SIEGEL, and STUART MADNICK, Massachusetts Institute of Technology

Cyber attacks are increasingly menacing businesses. Based on literature review and publicly available reports, this paper analyses the growing cybercrime business and some of the reasons for its rapid growth. A value chain model is constructed and used to describe 25 key value-added activities, which can be offered on the Dark Web as a service, i.e., "cybercrime-as-a-service," for use in a cyber attack. Understanding the specialization, commercialization, and cooperation of these services for cyber attacks helps to anticipate emerging cyber attack services. Finally, this paper identifies cybercrime control-points that could be disrupted and strategies for assigning defense responsibilities to encourage collaboration.

CCS Concepts: • **General and reference** → **Surveys and overviews**; • **Social and professional topics** → **Computing and business**; **Socio-technical systems**; **Computer crime**; • **Security and privacy** → **Social aspects of security and privacy**;

Additional Key Words and Phrases: Cyber Attack Business; Value Chain Model; Cyber-crime-as-a-Service; Hacking Innovation; Control Point; Sharing Responsibility

1 INTRODUCTION

"Where there is commerce, there is also the risk for cybercrime"[139].

Cybercrime is a tremendous threat to today's digital society. It is extimated that the cost of cybercrime will grow from an annual sum of $3 trillion in 2015 to $6 trillion by the year 2021 [115]. Nearly one third of companies are affected by cybercrime (32%). Indeed, 61% of CEOs are concerned with the state of the cyber security of their company [131].It has become generally accepted that, "there are only two types of companies: those that have been hacked and those that will be"[116]. Fighting an impending cyber attack has become an important issue for companies in all industries and governments, especially to those relying heavily on information technologies.

This work is partially supported by partly supported by the National Natural Science Foundation of China under grant 61502333, and the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, also known as MIT-(IC)^3.

Authors' addresses: Keman Huang, Sloan School of Management, MIT, Cambridge, MA 02142, USA; email: keman@mit.edu; Michael Siegel, Sloan School of Management, MIT, Cambridge, MA 02142, USA; email: msiegel@mit.edu; Stuart Madnick, Sloan School of Management, School of Engineering, MIT, Cambridge, MA 02142, USA; email: smadnick@mit.edu .

Ever since the first reported cybercrime in 1973, when Union Dime Savings Bank account data was manipulated, cybercrime has continually evolved[1]. Beyond a nefarious hobby, cybercrime has become a way for cybercriminals to earn a living[2]. While it remains underground, it is a business nonetheless; attackers cooperate, and work to maximize profits and minimize risk of arrest [85]. Cybercrime as a profession is increasingly attractive for able hackers, and in turn, cyber attacks themselves are increasingly well organized [2]. With the wide-spread adoption of the"as-a-service" model for cyber attack, the attacker can purchase the desired "service" through the dark web without so much as a cursory understanding of what is involved in its execution [104, 142, 155]. This eliminates the barriers that previously existed to performing a crippling cyber attack, and pushes the attackers deeper underground and further from the grasp of authorities.

In the words of Sun Tzu, "Know yourself, know the enemy."[174] To combat cybercrimes in an efficient and effective way, we need not only develop technical solutions to protect against attacks, but also understand the structure of the business of underground cybercrime, and the drivers of its development:

- *How does the cybercriminal organize a cyber attack?*

It has been said that "the good guys are getting better, but the bad guys are getting badder faster"[100].Much of published research on cyberattacks has been focused on how attackers clandestinely intrude on private systems [3, 66, 72, 136, 166]. However, reacting passively to a cyber attack and attempting to keep up with the almost daily emergence of innovations on behalf of cybercriminals means that "[Corporations] are are not winning [in the cyberdefense battle]"[108]. Cybercrime has taken on the guise of a business in recent years. Without understanding the relevant operations of cybercrime, it is difficult to combat cybercrime effectively. Researchers have begun to study different components of this underground business, including the marketplaces connecting attackers and buyers, and the community of hackers ready to deliver services for a fee [22, 24, 65, 73, 76, 92, 94, 97, 123, 133, 136, 157, 163, 169, 186]. Based on these individual elements, Thomas et al. [171] proposes a framework for understanding the structure of the underground cybercrime service through the monetization process, offering what can be characterized as a Bird's-Eye view of the black market for cybercrime. What remains unclear, however, is how the cybercriminal coordinates a cyber attack, and making sense of innovations in hacking. "Cybersecurity is still a game of cat-and-mouse"[47], with the defense trying to catch up with the offense with, up until this point, little success to show for its efforts.

- *How does the cyber attack develop in the wild?*

The underground cybercriminal has proven difficult to study. Researchers have used "honeypots" [118] to identify cybercriminals, and have collected information on the activities of cybercriminals [157]. These efforts to monitor the development of cyberattacks offer relevant counter intelligence. In considering the adoption of the "as-a-service" model [56, 139, 155, 171], researchers have compiled the services offered to buyers by the cybercrime industry. Without a clear framework through which to study the cybercrime service economy, it remains difficult to understand the modern cyber attack effectively.

- *How to share responsibility to combat the evolving cyber attack?*

[1] There is still much debate about the definition of cybercrime and what constitutes a cyberattack. Since no single, agreed-upon definition exists, in this paper we will consider "cybercrime" all cyber activities that are related to a "cyberattack", or that which undermines the function of the digital system belonging to the cybercriminal ecosystem. In this paper, we will use "cyberattack" and "cybercrime" interchangeably. Note that not all activities included in our model are illegal. In fact, there are many discussions, outside the scope of this paper, about cyber ethics and the legality of such activity [64, 159].

[2] During 2015, the CrytoWall ransomware virus raised more than $325 million for the hacking group, http://thehackernews.com/2015/10/cryptowall-ransomware.html, last visited 2017-6-1

Though cybercrime and its threats have been thoroughly discussed [43], how exactly to combat cybercrime is still an open issue. Software/hardware developers, cybersecurity providers, infrastructure operators, financial sectors, governments, third-party organizations, companies and individuals need to work together toward to improve cybersecurity. The cybercrime reporting infrastructure, led by cybersecurity providers, infrastructure operators and vigilante groups emerged to combat infections [78]. Due to misaligned incentives, information asymmetries, and externalities [113], it has been difficult to develop a systematic understanding of the underground cybercrime ecosystem which is crucial to understand what responsibilities or actions should be assigned for each party in the ultimate achievement of a "cyber-immune" world.

- **Need for Framework to Understand Cyber Attack Business**.

The goal of this paper is to develop a framework based on literature review and publicly available reports related to cyber threat intelligence to facilitate the further study of cybercrime and the underground economy which surrounds it. Cybercriminals run a business of selling cyber attacks, and thus we concentrate on what could be considered as the "value-added" processes for the cyber-attack. To understand these processes, we develop the *cybercriminal value chain model* consisting of the primary activities of vulnerability discovery, exploitation development, exploitation delivery, and attack, as well as the supporting roles of cyberattack life-cycle operations, human resources, marketing and delivery, and technical support. It is important to note that both the defensive side (cybersecurity) and the offensive side (cybercrime)[3] of cyberspace use similar innovations [42], and that not all activities included in the value chain model describing cybercrime are illegal. For example, vulnerability discovery and disclosure are what are called "double-sword" activities. While they can be used to develop patches for a flawed system, can also represent techniques to identify opportunities for deliberate exploitation by criminals [5, 15, 76].

Inspired by the STAMP model [119, 141], we develop the service model-consisting of input, output, and support to systematically discuss the cybercrime ecosystem, considering its restructuring into an "as-a-service" model. This enables the *specialization*–cyber attackers can focus on specific components and promote the expertise level, *commercialization*–cyber attackers can monetize their attack expertises, and *cooperation*–cyber attackers can loosely or organizedly collaborate with each other to do complex attacks,for cyber attack in the ecosystem. Following the presented value chain model, we survey how cybercrime activities can be executed in a service style to develop a cybercrime ecosystem framework for thinking about the cyberattacks business.

Based on the framework developed herein, we discuss the methods that can effectively combat cyberattacks. The framework enables the systematic understanding of the hacking innovation, the evolution of the cybercriminal services, which can help to redefine the cat-and-mouse game [47]. Using the cyber threats identified by the McAfee 2017 Threats Prediction Report [107], we confirm the efficacy of our framework. Notably, we observe that by following the "value-added" paths in the framework, cybercriminals build the reinforcement loops that translate to the cyber threats more grave than previously expected. The Return-On-Investment (ROI) analysis reveals that cybercrime is a serious business, indicating the great value that "cybercriminal service composition as a service" represents to the cybercrime ecosystem. Additionally, identifying the control points can help to improve the effectiveness with which cyberattack evolution is monitored and ultimately disrupt the business of cybercrime. Delegating responsibilities and actions among involved parties based on the presented framework is helpful to realign incentives point to collaboration in the fight against cybercrime.

[3] There are two sides to cyberspace: the defensive side focus to improve the cyber security and protect the targets from attack while the offensive side is for cybercrime and try to attack the targets. In this paper, for the offensive side, we will use hackers and attackers exchangeable.

Therefore, the main contribution of this paper is the systematic study based on literature review to understand the cybercrime ecosystem as a business, its evolution and the effective intervention strategies against it. These consist of:

- The value chain model for understanding "value-added" cyberattack activities;
- The cybercriminal service ecosystem framework for understanding cyberattack evolution;
- The implications of the framework in designing intervention strategies.

In Section 2, we present the value chain model for understanding cybercrime activities. Section 3 introduces the service model and details the cybercriminal ecosystem framework to study the cyberattack business reconstruction and its evolution. Section 4 highlights the applications relevant to combat the cyber-attacks. Our conclusions are summarized in Section 5.

2 CYBERATTACK ACTIVITIES: THE VALUE CHAIN MODEL

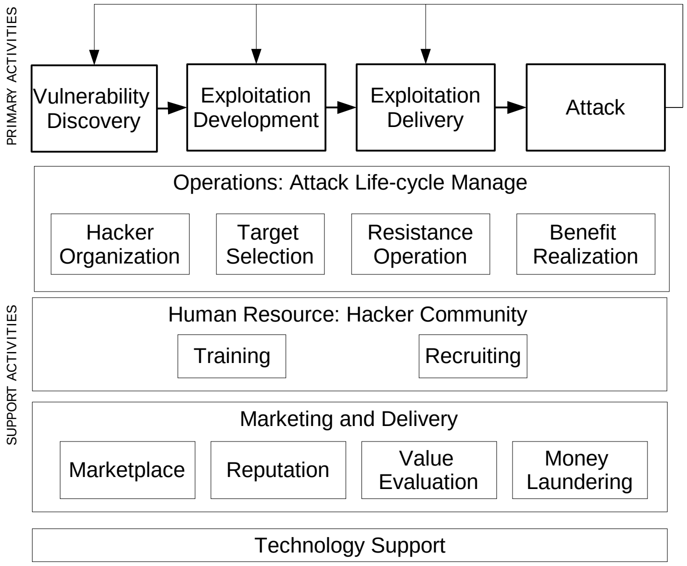


Fig. 1. Cybercriminal Value Chain Model

To effectively combat cyber-attacks and enhance the cybersecurity on which our digital society relies, it is imperative to understand the operation behind a cyberattack, raising the following questions: *what activities are associated with a cyberattack?* In considering cybercrime as the business that its has become, from a value chain perspective [129], we can identify the activities which add value for the cyber attack operation, as presented in Figure 1. These value-added processes include *any activity in the cybercrime business ecosystem which helps the attacker reduce the cost of, and increase the benefit incurred in cyber-attacks*. It is straightforward that the primary activities which directly involve the attack are valuable for the attackers. Additionally, the support activities, which are often overlooked are critical in facilitating the operation of the cybercrime business, as they can help the attacker to do an attack with less cost for higher benefit. Hence, following the value-added processes for a cyber attack, based on the literature review and the public available reports related to cyber threat intelligence, we can identify the value-added activities and build the value chain model for cyber attack. Furthermore, we have validated this value chain framework, as well as the cybercriminal service ecosystem framework in Section 3, with more than 30 senior executives, managers and researchers focusing on cybersecurity from Fortune 500 companies and key cybersecurity solution providers to improve the framework[4]. To the best of our knowledge, this is the first comprehensive value-chain model, which integrates the different components of the cyberattacks, to systematically understand cyberattacks from the business perspective. We will detail each component in the following sections.

2.1 Primary Activities: The Attack

2.1.1 Vulnerability Discovery. Logically speaking, cyber-attacks start with vulnerability discovery which finds the weakness that can be used to intrude into the victim's systems. This weakness may be a zero-day/one-day vulnerability in software/hardware, or a relatively simple password not modified for a long time which is easy to uncover by brute force [111]. Cybersecurity usually involves technology, people, and process [96]. Overlooking strategic, managerial, and operational issues related to cybersecurity significantly weakens an organization's defenses against cybercrime [101]. Hence, in this paper, vulnerability refers not only to weaknesses in software or hardware in IT/OT systems, but also to weaknesses found in processes, policy, and the human component of an organization.

Definition 1: Cyber Vulnerability refers to the cyber-related weaknesses which can be used by a cyber attacker to intrude into the organizations, including the weakness in software or hardware, named technical vulnerability V_t, and the weakness in the process, policy, and human, named operational vulnerability V_p.

Based on this definition, the vulnerabilities detailed in vulnerability databases like National Vulnerbaility Database (NVD) and Securiy Focus BID [76] are considered as the technical vulnerabilities in IT/OT systems. Most current vulnerability discovery research focuses heavily on the technical vulnerabilities [30, 61, 153]. However, with the development of the defensive technologies, it becomes more difficult for an attacker to intrude into a target's systems through only software or hardware vulnerabilities. This means that an organization's vulnerabilities related to process, policy and human aspects are often the "weakest link" in their security schemas and present themselves as opportunities for cybercriminals [144]. The typical cyber attack targeting these weakest links is the semantic social engineering attack which deceives the users in an organization [143, 170]. Furthermore, the cyber threat from the supply chain are increasing [149]. Some recent efforts have attempted to detect and understand operational vulnerabilities in the process and policy [102, 119]. For example, the causal analysis based on STAMP (CAST) [93, 119] identified the presence of damning operational vulnerabilities which were exploited by hackers and cost TJX over $170 million in losses in the 2007 TJX data breach incident.

2.1.2 Exploitation Development. The "Exploitation Development" activities try to exploit the discovered vulnerabilities, including both the technical and operational vulnerability. Once a technical vulnerability is discovered, a program can be developed to exploit the vulnerability and force a system to behave in unintended ways so that a cybercriminal can carry out actions that would otherwise not be permitted. In order to increase the chances of success of an attack, multiple vulnerabilities may be targeted as a part of an "exploit kit". For example, the well-known exploit kits, such as Angler, Magnitude, Neutrino, Nuclear, RIG, etc., are continually updated to reliably exploit technical vulnerabilities and guarantee continued success in disrupting normal function of the targeted system [38]. Furthermore, a payload [24, 148] could be a malicious program performing

[4] These senior managers and executives are from members of MIT (IC)^3. Please refers to http://ic3.mit.edu/about-us/members to see the member list.

a singular function, or a combination of many independent programs to offer a more complex, comprehensive functionality, which can be used to perform malicious actions.

On the other hand, to perform advanced attacks exploiting an operational vulnerability, some social engineer toolkits have been developed[5]. The Social Engineer Toolkit (SET) [127] was specifically designed for targeted attacks against a person or organization in a penetration test. Many semantic attack exploits are developed to manipulate the user-computer interface to breach a computer system's security [66]. Developing fake mobile apps that appear to be the same as their legitimate counterparts is one typical semantic attack to exploit the operational vulnerability that arises from what we consider the human factor of an organization [48]. The business email compromise scams [105], also known as "CEO fraud", is another example in which the attacker counterfeits a message from the boss to trick someone at the organization into wiring funds to them. These attacks exploit the operational vulnerability in the organization's financial process and human component, to develop the persuasive, but fake, message.

2.1.3 Exploitation Delivery. Once vulnerabilities are ripe for exploitation, the cybercriminal must deliver the developed exploitative programs to the victim's cyberspace niche. Based on the delivery medium (physical medium or digital channel) and infected approach (whether needs intermediate host or not; if yes, whether the host is individual server or distribution channel), there exist four typical delivery mechanisms:

- *Physical Infection.* This straightforward mechanism involves infecting the victim's system via a physical medium, such as hardware or USB; the delivery depends entirely upon physical transportation. The typical observed scenario that this mechanism describes is virus propagation: once one person with an infected system makes copies of files that are then used on another system, the virus will spread to the second system, from which even more systems can be infected. Though this physical infection mechanism is old-fashioned and ultimately not very effective, due to operational vulnerabilities, it remains relevant. An example would be purposefully dropping a USB drive loaded with an exploitative program inside an organization's offices, or even in the parking lot, with the hope that an employee may pick it up and plug it into a computer, at which point the company's systems can be infected. In the supply chain security scenario, the counterfeit hardware or hardware with embedded malware can be distributed to infect the victims [149].
- *Sent Directly.* This mechanism describes sending the exploitative program directly to the victim. In this scenario, the programs will be forwarded to the victim's cyberspace niche through digital channels, like SMS messages or email. Once the victim is tricked into accepting the exploitative program, such as by opening the fake emails or messages, the exploitation has been successfully delivered and the victim's system will be infected. One attack utilizing this mechanism in recent memory is the Ukraine power grid cyberattack. Spear phishing emails containing BlackEnergy malware were sent to the victims, and the corporate network was compromised by opening disguised documents attached to the emails [45].
- *Drive-by-download.* The third mechanism involves redirecting the victim online to reach a website loaded with the exploitative programs, at which it is delivered to the victim's system in a "drive-by-download". In this scenario, the victim is driven to the compromised website by following a maliciously disguised advertisement, and is redirected to a landing page where a downloader for the exploitative program will be installed on the victim's machine to contact the command-and-control (C&C) server and establish at least one download channel to deliver the exploitative programs to the target's cyberspace niche [22, 138, 169].

[5] Note that some social engineer toolkits may not be developed for cyber-attacks but penetration tests. However, due to the neutrality of the toolkits, they can also be used by the black hackers to do cyberattack.

- *Software-Distribution*. This fourth mechanism has been emerging with the rapid development of the mobile ecosystem. In this scenario, an original piece of software is infected during transmission to the user. One typical approach is to add malicious code to the software that requests permissions beyond those required by the original software through repacking [74]. Once the adulterated software runs, the malicious code will be executed and the exploitative programs will be downloaded to the victim's machine [62]. With the development of auto-update feature, the cybercriminal can also dynamically add malicious code to an application during runtime, or update an application to include malicious components so that a benign application becomes malicious after a software update [3, 132].

2.1.4 Attack Victim. Once a victim's system is successfully infected, the avenue is open for attack. For a single-step attack, once an initial action by the victim has been carried out, such as open a file, click on a link, run a program, accept a permissions request, the attack is already completed. For a multi-step attack, on the other hand, the initial action by the victim not only activates an immediate attack, but also opens the doors for subsequent attacks, including identifying further exploitable vulnerabilities. In this scenario, the attacker first gains privileged access to a victim's system so that they can move freely within the otherwise private environment. Once an attacker successfully intrudes upon a system, he or she can access and extract sensitive information, rewrite or erase files, and alter the functionality of the system, affecting the system's confidentiality, integrity and availability of data. To once again use the Ukraine power grid attack [45] as an example, the hackers used KillDish to erase important executable files and cause physical damages to the system. Some attackers may even want to establish a sustained presence in their victims' systems so that they may come and go, and do as they please. To study the cyberattack from the value-added perspective, instead of the detail cyber attack tricks, we must understand what a cybercriminal can gain from a successful cyberattack, and what these gains afford in terms of further attacks:

- *Digital Gains*. Once inside, an attacker can get all information contained in a victim's system, including sensitive information such as personal profiles, accounts, and intellectual property. The compromised system is another "trophy" for an attack while sometimes the human who is tricked by the attacker can prove a "trophy" themselves. One example is when someone can be tricked to work as a money mule for money laundering [72]. Furthermore, the attacker can gain valuable knowledge related to the victim's system, such as operational processes, network configuration, and organizational structure. With an understanding of these aspects of a system, an attacker can better hide further attacks from detection. What made the cyberattack on Bangladesh Bank's (BB) SWIFT payments system in February, 2016 [152] so hidden and damaging was the attacker's understanding of the bank's transaction confirmation process: the attacker was able to intercept confirmation messages and cover up fraudulent transactions. Attacks to the CIA [179], NSA [60], Hacking Team [68] etc. can offer attackers 0-day vulnerabilities, exploitations, and many tools developed and customized by these professional organizations that expand and strengthen their arsenal.
- *Psychological Gains*. The attacker who carries out attacks seeking the inherent satisfaction of success or for the fun or challenge of the process gains psychological benefits from an attack [85]. In this particularly twisted case, the attack is perceived as merely a test of hacking skills, and the successful attack carries with it not only a sense of accomplishment for the attacker, but also reputation in the hacker community. Some attackers may seek vengeance against a symbolic enemy, or see cybercrime as a way to further political agendas. The Anonymous is one such group, which attacked Freedom Hosting II, a service that hosts 20% of dark web websites, 50% of which contained child pornography in some forms [18].

- *Loss-based Monetary Gains*. A successful attack can interrupt the business continuity of an organization by adversely affecting the confidentiality, integrity and availability of certain systems. This results in a direct monetary cost to an organization in the form of losses or damages, but also in indirect costs such as loss of trust by customers, missed business opportunities and increased defense costs for prevention, protection, detection, and recovery in response to the cyberattack [10]. The attacker can benefit by monetizing the victim's loss for themselves. The typical scenario is that the attacker draws funds directly from a victim's accounts. A more eye-catching scenario with a recent surge in popularity involves the attacker proving his or her capability to interrupt the victim's business continuity and requesting money in return for not capitalizing on their abilities, effectively holding a business hostage for a ransom. The ransomware attacks of 2016 [120] are such examples and 88% of these attacks targeted hospitals and health systems, since cybercriminals correctly perceived these organizations as more vulnerable and receptive to threats and eager to satisfy a ransom to avoid damage.

2.2 Support Activities: Facilitate the Attack

To supplement the primary activities discussed above, we see an emergence of what can be considered as support activities in the cybercrime ecosystem to make cyber-attacks more efficient: *greater benefit with less cost*.

2.2.1 Operations: Attack Life-cycle Management. A cybercrime operation, like a legitimate business [161][6], must actively manage and support the cyberattack life-cycle to reduce costs, increase profits, and mitigate risk. In addition, cybercrime operations must also make conscious efforts to avoid being identified, and its operatives punished under the law. To meet these criteria, a cybercriminal within a greater operation must select the valuable attack targets, decide how to organize hackers (if more than one) to carry out primary cybercrime activities, manage the distribution of proceeds (payroll if you will) hide the operation from authorities, and if disrupted, recover the sidelined operation.

Definition 2: Cyberattack Operations refer to the activities that manage and support primary activities to gain higher benefit with less cost from the cyberattack. These include target selection, hacker organization, benefit realization, and resistance operation.

- *Target Selection: what are the characteristics that make a valuable target?*

Following the thought process suggested by basic economics, the cybercriminal in the executive role selects the target which would deliver the highest profit, the greatest positive difference between benefit and cost [85]. There are three factors to consider in evaluating the benefit brought about by the successful execution of an attack:

- **Ease of the attack** P_e. If hackers don't have a specific objective, they may take on an exploratory mindset to probe various targets, and identify those with sufficient weaknesses to be considered for a full-scale cyberattack. In this scenario, the more easily vulnerabilities can be discovered and exploited in a certain organization's systems, the more attractive a target the organization becomes. Even if a specific target has been selected, the cybercriminals may take on an exploitation mindset to dig into the target's systems and attempt an attack;

[6] Based on the definition presented by William J. Stevenson [161], operations management is *"the management of systems or processes that create goods and/or services"*. Operations management specialists are involved in *"product and service design, process selection, selection and management of technology, design of work systems, location planning, facilities planning and quality improvement of the organization's products and/or services"*.

however, if breaking into the current target's systems proves too difficult, and after a few days or weeks no progress is made, the target can be abandoned in favour of another target identified in the exploratory phase.

- **Potential Benefit** B_p. As mentioned above, a successful attack can bring the attacker the digital gains which themselves have value in the underground market, or the attacker can attempt to seek money directly from the victim of the attack. The attacker may also experience psychological gains. These encompass the two main categories with which we can understand the benefit to cybercriminals in the wake of a successful cyberattack: the monetary benefit B_{pm} and the psychological benefit B_{pp}. Hence $B_p = B_{pm} + B_{pp}$.
- **Ease of benefit realization** E_r. Converting unrealized benefit into tangible, realized benefit is of concern to the cybercriminal engaged in the business of cybercrime. The easier it is for cybercriminals to experience the benefit earned in an attack, the more true benefit is accrued.

Hence, we define the **expected benefit** B_e for an attack on a given target as follows: $B_e = P_e \times (B_{pm} + B_{pp}) \times E_r$.

In terms of costs, we can identify the following costs inherent to the execution of an attack:

- **Psychological Costs** C_{ps}. Costs of this nature refer to the psychological and mental energy expended in committing a cyberattack. These could include the fear of being caught, or punishment.
- **Expected Penalty Costs** C_p. This cost captures to the monetary opportunity costs of conviction if the attackers, which become real if the cybercriminals happen to be arrested and convicted following the attack. Straightforwardly, it is proportional to the arrest rate P_a for the particular kind of cyberattack, the ease of the judicial process involved in the conviction P_c and the monetary opportunity cost if the attacker is convicted C_c. $C_p = P_a \times P_c \times C_c$.
- **Operational Costs** C_o refers to the cost to carry out the cyberattack. The investment cost C_{im} captures the up-front costs for the cybercriminal to perform the attack, which could be renting a server, buying or learning any necessary tools or services, and the opportunity cost of the time taken in searching for valuable targets. The monetary opportunity cost of the investment C_{om} in cyberattack should be also considered. Hence $C_o = C_{im} + C_{om}$.

Based on these definitions, the expected cost C_e for an attack can be defined as: $C_e = C_{ps} + (P_a \times P_c \times C_c) + (C_{im} + C_{om})$

Definition 3: Cyberattack Target Selection Rule For a rational cyber-attacker, the victim organization could be considered as a target if and only if the expected benefit outweighs the expected cost.

$$P_e \times (B_{pm} + B_{pp}) \times E_r > C_{ps} + (P_a \times P_c \times C_c) + (C_{im} + C_{om}) \tag{1}$$

Note that the equations discussed above are in high level. They can help us to understand the values of different activities for the cyberattack. Any activity that can reduce the expected cost or increase the expected benefit will be highly valuable in the cybercrime ecosystem. Understanding this operation can shed lights into the decision-making for the attackers.

- *Hacker Organization: how do cybercriminals collaborate with each other for an attack?*

For an attack to be successful, especially for the organized cyberattack which involves multiple hackers, the cybercriminal in the executive role must organize his or her team for the attack. Typically, there exist the following six basic types of organization structures [110]:

- A *Swarm* refers to a group of hackers who work together in viral forms that have a minimal, if not nonexistent, chain of command;

- A *Hub* refers to the structuring scheme in which there is a core group of hackers around which peripheral associates gather;
- A *Clustered Hybrid* structure combines online and offline activity, and typically operates in a similar way as *Hub*, focusing on specific activities or methods;
- An *Extended Hybrid* structure is like the *Clustered Hybrid* structure, but incorporates many associates and subgroups while retaining a level of coordination sufficient to ensure the success of operations;
- *Hierarchies* refer to structure reminiscent of traditional organizations as well as criminal groups, but take advantage of online technology to facilitate activities;
- An *Aggregate* structure refers to a loosely organized group of hackers committed only to temporary collaboration, and often without a clear goal.

Different organizational structures have different pros and cons; the leaders need to consider which organizational structure is best suited to a given attack objective. For example, most state-supported cybercriminal hackers organize under a *Hierarchy* structure, while the well-known group, Anonymous, appears to adhere to an *Aggregate* structure. Though family ties, friendships and online relationships all play important roles in the collaboration between cybercrimals [121], online forums are serving as offender convergence settings for cybercriminals and shaping a more fluid and flat structure so that all participants are able to get into contact with each other [91]. Furthermore, in online hacker forums, most hackers are novices with only a few more highly skilled hackers participating in forum activity [70, 94, 97] and this community forms the core and peripheral *Hubs*.

- *Benefit Realization: how to gain benefit from an attack?*

It is within the executive's responsibilities to maximize the benefit to be gained from a successful attack. Considering monetary benefit as an example, the executive may hire a money laundering network so that the source of "dirty" money cannot be identified. Recently, researchers have presented the concept of "DDoSCoin", which allows a cybercriminal to prove their own participation in a DDoS attack by having miners create a large number of connections to a given target and using the target server's signed responses as a proof to receive the digital monetary rewards that they deserve [181]. Digital currency, especially Bitcoin, has become the main approach for cybercriminals to transfer monetary gains to one another in the wake of a successful attack [84]. Though the motivation for the WannaCry Hurricane attack on May 2017 is still a mystery, there is a theory that it is for currency manipulation to raise the Bitcoin value by increasing number of users [172]. Additionally, many markets or forums are constructed for cybercriminals to trade their digital gains from successful attacks [33, 130, 157, 186]. According to the tracking of ransomware payments [130], 95% of the traced ransoms cashed out via BTC-E, a digital currency trading platform and exchange. For psychological benefit, a "Hall of Fame" of hackers with the greatest reputations can motivate cybercriminals to continue participating in attacks within the cybercrime ecosystem, considering the value placed on reputation and trust for cybercriminal community [44, 69, 91, 183].

- *Resistance Operation: how to skirt detection and recover from a take-down?*

Straightforwardly, hackers do not want to be identified or have their attack detected. Common methods that aim to accomplish this include employing a proxy server to bounce online activities, using anonymous tools such as a Tor network[8, 41, 109], clearing event logs, command history, and shredding history files. To increase the chance of success of a cyberattack the executive can introduce obfuscations to avoid being detected by the target's defense tools, regularly update an attack's configurations and executable file builds, or use multiple channels and distribute servers across network boundaries [122, 138].

Parts of the cybercrime ecosystem can be taken down by law enforcement, therefore, a plan for recovery is extremely valuable for cybercriminals. For example, the Ramnit botnet that infected 3.2 million computers was taken down in February 2015 only to quickly re-emerge and attack banks and e-commerce operations in Canada, Australia, the United States, and Finland in December 2015 [81]; some of Ramnit's infrastructure survived from the take-down and its operators were not arrested. Additionally, it is believed that the cybercriminals acquired the web injection mechanism from a separate group that provides web injections as a service, making Ramnit even more resilient.

2.2.2 Human Resource: Hacker Community. As discussed above, the hacker forum is the most common form of communication for the cybercriminal community. A hierarchical structure has lower coordination costs than a pure market structure, so most hacker forums have adopted hierarchical management systems consisting of administrators, moderators, reviewers, reviewed vendors, and general members to stratify, and organize the community [183]. There is a limited number of highly skilled hackers [94] and the cybercriminal tends to build a collegial culture that encourages sharing of information and values innovation [70]. Since most hackers are novices, part of the value-added activity for the hacker community is training the novices. Note that both the offensive and defensive sides of cybercrime are leveraging the same innovations [42], and hackers can learn skills through online cybersecurity forums or even via YouTube videos. The near-term advances in machine learning, automation and artificial intelligence can also be used by the criminals and nation-state adversaries [42] while the attacker may even have the advantage in skill, as the "worst is getting worse faster" [99]. Some hacker communities will offer training programs to train fledgling cybercriminals. For example, the Anonymous launched an online school called OnionIRC allowing members to share technical skills and maintain anonymity [52].

To grow the hacker community, recruiting is an important activity for the cybercrime ecosystem. To achieve this goal, many tutorials are available to reduce the barriers for the novices to join the hacker community and benefit from the cyberattack. According to the research from Digital Shadows, the process hackers use to recruit new hires is the mirror to its legitimate counterpart [135]: post advertisements on forums, hacker-specific job boards, social networks to reach fresh talents, qualify candidates by application forms or even through the interviews, and maintain a time-sensitive membership. The study of the 18 investigations into criminal networks [90] demonstrates that the relationships based on real-world social networks plays an important role in the origin and growth of the majority of networks while the access to online forums can increase the criminal capabilities quickly. For the nation-supported cyber-attacks, the recruiters may even hire hackers with specific experiences from the criminal underworld [154].

2.2.3 Marketing and Delivery. As discussed above, a marketplace for attackers to trade the digital gains from a cyberattack is the principal way for attackers to realize the benefit from successful cyber-attacks. Today, we can observe many different dark web marketplaces available for different kinds of goods and services: vulnerability and exploitation [5, 76, 125], dumps, skimmers, identities, attack tools and mules [186], credit card [65], fake tools [162] and Bitcoin [130] etc. Some marketplaces even allow cybercriminals to operate "single-vendor stores", in the same way as one could do on Amazon, eBay, or Taobao, where sellers will run their own online website to sell their products to their clients [65].

Since there exist many different digital goods and services in the marketplace, determining the price of a good is a typical value-added task for the hackers. It is no surprise that a zero-day vulnerability will be much more valuable than a one-day vulnerability. The one-day vulnerability is still valuable because of the observed patch delay in practice [79]. Additionally, the going price changes based on supply and demand in the market. For example, in May 2016, due to the shutdown of Angler, the demand for Neutrino increased so much that the developer doubled the price per month from $3500 to $7000 [28].

Concerns about anonymity translate to uncertainty related to product quality in the hacker community [67, 183]. To mitigate this problem, trust and reputation plays a fundamental role in the cybercrime ecosystem [91]. Any activity that a cybercriminal can undertake to show that he or she is trustworthy, or to bolster his or her reputation is extremely valuable. It is important for the cybercriminal to make sure a potential trading partner is not in fact law enforcement; the take-down of Shadowcrew is a "painful" example of such a situation in hacker community [55]. Some forums are open exclusively to well-vetted users and often require a fee to join, and other forums are invite-only [183] while some forums may even request the members "must hack a website within 3 months" to maintain the membership [135]. Some guarantors will offer vetting services to check a prospective user's background, contributions, and trustworthiness [56]. Like the legitimate e-commence sites such as eBay and Amazon, some forums offer a rating system so that members can rate each other and evaluate a potential traders' reputation. Due to the prevalence of "rippers" who trade dishonestly by double selling, some marketplaces, such as credit card forums, have introduced a review mechanism to review prospective vendors' goods and/or services and assign a "reviewed vendor" tag as an approval of quality if a vendor passes the review [67]; if a reviewed vendor is found to have traded dishonestly, that vendor will face punishment [183].

Cybercriminals are leveraging innovations to make their products and services more attractive, trustworthy, and more easily delivered. For example, shifting to the "as-a-service" model has been a significant trend in recent years [104]. These services are becoming easier and more user-friendly, which significantly increase the resilience of cyber-attacks. The innovations in service also make it easier for a cybercriminal to realize the benefit from a cyberattack and significantly reduce expected costs as the cybercriminal can operate even further underground.

2.2.4 Technical Support. Cybercrime relies heavily on the technical support. As discussed above, the offensive and defensive sides use similar innovations [42]. Many technologies developed for "good" purposes have been coopted by cybercriminals for less than positive ends. The first bot IRC was invented in 1988, and the first malicious bot appeared 10 years later [173]. The anonymous communication network technology Onion Routing (Tor) and the Invisible Internet Project (I2P) were developed to protect privacy online [8, 37], and the Bitcoin, a peer-to-peer electronic cash system, was developed to allow any two willing parties to transact directly with each other without the need for a third party [117]. Now these technologies have become the "cornerstones" for the cybercriminal ecosystem.

Additionally, the well-known tools such as *Application Specific Scanners, Debuggers, Encryption Tools, Firewalls, Forensics, Fuzzers, Intrusion Detection Systems, Multi-Purpose Tools, Packet Crafting Tools, Packet Sniffers, Password Crackers, Port Scanners, Linux Hacking Distros, Rootkit Detectors, Traffic Monitoring Tools, Vulnerability Exploitation Tools, Vulnerability Scanners, Web Browser Related Tools, Web Proxies, Web Vulnerability Scanners and Wireless Hacking Tools* are used by both cybercriminals and security engineers. For example, Nmap is a very well-known open source hacking tool for network inventory, open port checking, managing service upgrade schedules and monitoring host or service uptime, which is also widely used by attackers to intrude into the victim's network. Furthermore, many tools developed or customized by the professional organizations or experts, even by the state-supported agencies like CIA [179] or NSA [60], may be taken and used to strengthen cybercriminal's arsenal.

2.3 Cyberattack Ecosystem: Combination of Primary Activities and Support Activities

Hence, the cyberattack ecosystem consists not only of the primary activities directly related to a cyberattack, but also of the support activities that facilitate a cyberattack by reducing costs and increasing benefits. In addition to technical vulnerabilities, attackers also target operational vulnerabilities, the weaknesses related to the processes, policies, and humans in an organization. However, most current vulnerability discovery research focuses on the technical vulnerabilities. Operational vulnerability is often overlooked. Cyberattack operation activities, including target selection, hacker organization, benefit realization, and resistance measures, can significantly improve attackers' performance in the digital, psychological, and monetary gains. The hacker community is growing in both skill and scale to offer human resources for cyber-attacks, and the marketing and delivery activities further facilitate the benefit realization for cyberattack operation. The cyberattack ecosystem is already embedded in a comprehensive value chain. In order to combat the modern cyberattack effectively, beside the primary attack activities, the defensive community should also pay special attention to these emerging value-added activities.

3 CYBERCRIMINAL SERVICE ECOSYSTEM: BUSINESS RECONSTRUCTION

With the development of service science [89], cybercrime as a service (CaaS) has become an important trend for the cybercriminal ecosystem [104, 142, 155]. This innovation not only puts cybercriminal tools and services in the hands of a wider range of threat actors, but it also turns the cyberattack into a business that can provide a living for a career cybercriminal [2]. Furthermore, it restructures cybercrime activities and drives attackers even deeper underground, as activities related to cybercrime can now be offered as independent, modular components in a cybercrime supply chain with attackers benefiting from each component. In this section, following the value-added processes discussed in Section 2, we will identify the relevant cyberattack services[7], to construct a systematic framework for the cybercrime ecosystem, developing an understanding of the business and the evolution of cyberattack itself.

3.1 Service Model: Business Components for Cyberattack

A cyberattack service provider can advertise a CaaS offering specific modules related to a cyberattack on the marketplace to reach as many potential users as possible. A buyer can purchase any needed services on a marketplace to build a cyberattack from scratch, or can integrate the purchased services into his or her own operation, becoming a service provider. As shown in Figure 2, to build the systematic framework for the cybercriminal ecosystem, based on the STAMP model [119, 141], we define each service as the value-added activity that takes some inputs, and produces an output using the support tools and techniques:

Definition 4: Cybercrime Service refers to a value-added activity related to a cyberattack that takes input and produces output using the support tools and techniques:

$$\mathrm{O} = CS\,(\mathrm{I}, \mathrm{C}) \tag{2}$$

where I refers to the input set for the service, O refers to the output set for the service, while C refers to the techniques or tools that support or enable this service. Note that the input, output or support are not necessarily a single-element set, and could be a multi-element, meaning that it involves different types of variables, or even an empty set $\emptyset$ if no variable is necessary for the given parameters.

[7] In this paper, we will use component and service exchangeable.

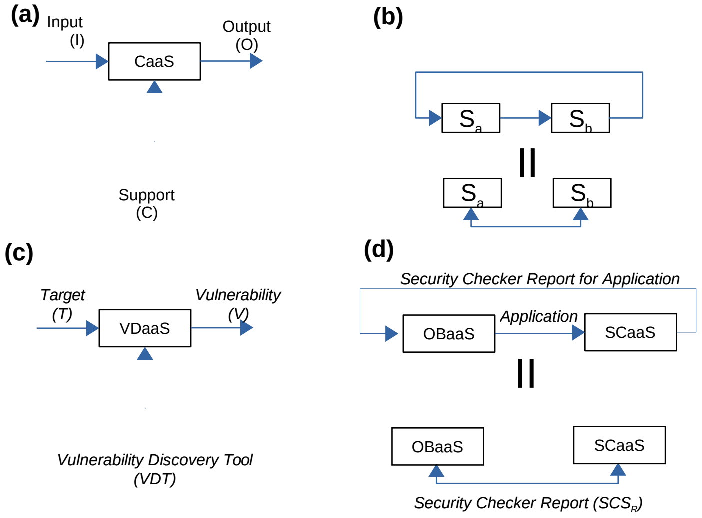


Fig. 2. Cybercriminal Service Model. (a) Each cybercrime value-added activity can be modelled as the service which takes input and produces output using supportive tools or techniques. (b) Two services form the composition based on their dependencies, further constructing a loop, simplified as a double arrow for convenience. (c) Taking the vulnerability discovery as an example, given the a target, using the vulnerability discovery tools, this component identifies the related vulnerabilities as the output. (d) Taking the obfuscation and the security checker components as examples, the obfuscation component (OBaaS) uses the service checker component (SCaaS) to check the obfuscation's effectiveness. It can continuously involve the security checker until the security check report (SCS$_R$) shows that the application can bypass the security software.

In the "as-a-Service" model, a cyber-attacker can concentrate on a particular value-added activity in the cybercriminal ecosystem, becoming an expert and driving the *"specialization"* for the cyber-attack activities. Cybercriminal specialists can then *"commercialize"* their skills as services/products that can support use by many users simultaneously and are intuitive enough so that buyers don't need to understand the details of their execution to use them. To overcome defensive efforts and execute a successful cyberattack, a cyberattack executive may combine related services so that they *"cooperate"* in performing more complex tasks to improve the performance of a cyberattack. Based on the definition above, if the output set of a service CS_a intersects with the input or support of another service CS_b, then there will exist a value-adding path from CS_a to CS_b and these two services can collaborate with each other to form a composition and lend an advantage in performing complex attack activities.

Definition 5: Cybercrime Service Composition. Given two cybercime services, they can collaborate with each others as a composition for value-adding and form a complex attack activity if and only if there exist intersection between the output set of the previous service and the input or support of the next service.

Note that the output set of the previous service don't need to be equal to the input or support of the next service. Once there exist some intersections, then they can collaborate with each other to generate added value.

Hence, with the adoption of the "as-a-Service" model for cybercrime, *specialization, commercialization, and cooperation* in the cybercriminal ecosystem form the crux of the cybercrime business.

In the following sections, based on the value chain model presented in Section 2 and the service model discussed above, we will formally identify the unique cybercriminal services, including those directly related to the primary activities and those indirectly supporting a cyberattack, and how they collaborate with each other for the cyberattack.

In this paper, we are focusing on the added value and the business in the cybercriminal ecosystem, so the technical details, or cyberattack tricks, as discussed in many studies like [15, 25, 26, 29, 132, 160, 165], are out of scope. We consider the attack service as a "black box" because in the cybercriminal service ecosystem, the buyers don't need to understand the details of the services they purchase.

3.2 Cybercrime Services Directly Related to Primary Activities

The cybercrime services directly related to primary activities consist of the services for the primary activities, and the related supportive activities to overcome the defensive efforts and to improve the cyberattack performance.

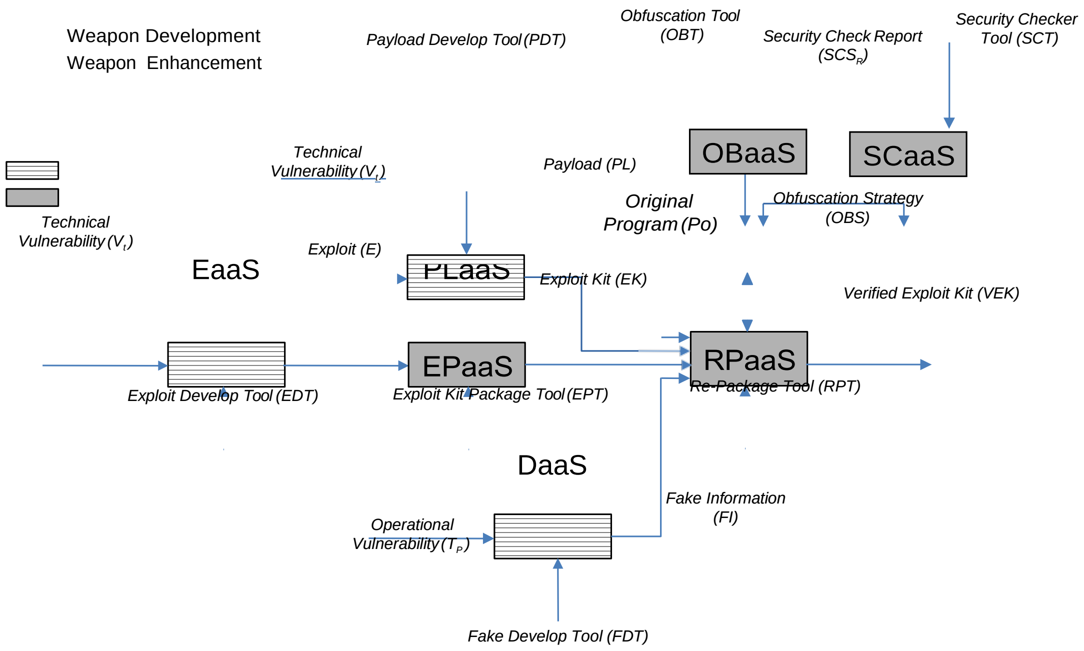
3.2.1 Vulnerability Discovery as a Service (VDaaS). For the vulnerability discovery service, given the target as the input, with the support from the vulnerability discovery tools, potential vulnerabilities of the target are identified and returned as outputs. We define VDaaS as follows:

$$\mathrm{V} = V\,DaaS\,(\mathrm{T}, \mathrm{VDT}) \tag{3}$$

where T is the target, which can be the information system or an employee in a specific organization, or a specific information product series like Window 10 operation system. V refers to the discovered vulnerabilities related to the given target T, including technical vulnerability V_t and operational vulnerability V_p. VDT refers to the vulnerability discovery tools such as Metasploit, Wireshark, or W3af. Note that the more specific the given target is, the more targeted the cyberattack based on the discovered vulnerability can be.

It is not a surprise that in the underground cybercrime ecosystem, hackers trade their discovery directly in the dark web [5]. However, vulnerability discovery is a non-trivial, time consuming, uncertain, but highly valuable task, Google even launched a vulnerability research grant to reward *"security researchers that look into the security of Google products and services even in the case when no vulnerabilities are found"* [57]. Hence it is rare to observe the independent vulnerability discovery services in the cybercriminal ecosystem. Only some highly skilful hackers, especially the organized cybercrime hackers, can offer services to help the clients, who could be nation-support agencies like FBI, to identify the vulnerability in the target system. Given the success of the bug bounty programs [75, 103, 185], where organizations reward external experts who discover vulnerabilities in their systems and patch them before they are publicly disclosed, it is very possible that deep in the dark web there will exist offensive-versions of "bug bounty programs" where a platform is offered to take advantage of the hacker community to dig the vulnerability for a given target. Considering the menacing targeted cyber attacks, aka advanced persistent threat (APT) [156], this VDaaS as the offensive bug bounty programs is very likely to be reality, if not exist yet, in the cybercriminal ecosystem.

3.2.2 Exploitation Development Service (EKaaS). An exploit is a program that takes advantage of discovered *technical vulnerabilities* to make a target's systems perform in an abnormal way. Hackers can package exploits in an exploit kit to simplify and increase the success rate of attacks. To avoid being detected by defensive security software, exploit kits can include components to obfuscate their true functionality. Additionally, exploit kits can integrate additional payloads to bolster an attack on potential targets. For the *operational vulnerability*, the attacker can deploy the fake WiFi, website, software, message or email to exploit the discovered operational weaknesses. Hence, the exploit development service is the service that converts discovered vulnerabilities into effective cyberattack weapons with the support of development tools. This process is described by


Weapon Development
Weapon Enhancement
Technical Vulnerability (V_t)
Payload Develop Tool (PDT)
Obfuscation Tool (OBT)
Security Check Report (SCS_R)
Security Checker Tool (SCT)
OBaaS
SCaaS
Technical Vulnerability (V_t)
Payload (PL)
Original Program (Po)
Obfuscation Strategy (OBS)
Exploit (E)
EaaS
PLaaS
Exploit Kit (EK)
Verified Exploit Kit (VEK)
EPaaS
RPaaS
Exploit Develop Tool (EDT)
Exploit Kit Package Tool (EPT)
Re-Package Tool (RPT)
DaaS
Fake Information (FI)
Operational Vulnerability (T_P)
Fake Develop Tool (FDT)

EaaS: Exploit as a service EPaaS: Exploit Package as a service DaaS: Deception as a service PLaaS: Payload as a service RPaaS: Repackage as a service SCaaS: Security Checker as a service OBaaS: Obfuscation as a service

Fig. 3. Exploitation Development Service (EKaaS). "Weapon development" means the service is related to transfer the vulnerability into the weapon which can be used for attack. "Weapon enhancement" means the service is used to improve the effectiveness of the weapons.

the relationship below.

$$\mathrm{VEK} = EKaaS(\mathrm{V}, \mathrm{EKDT}) \tag{4}$$

where V refers to the discovered vulnerabilities, including technical V_t and operation V_p vulnerability; VEK refers to the verified exploit kits, the cyberattack weapons which can be delivered to the target; EKDT refers to the tools used to support the exploitation development process.

As shown in Figure 3, based on the independence between different components, the innovations to increase the cyberattack performance and overcome the defensive efforts, we can dig deeper into this exploitation development process to identify the related cybercrime services, consisting of the "weapon development" services to transfer vulnerability into attack weapon and the "weapon enhancement" services to improve the effectiveness for cyberattack.

- **Exploit as a Service (EaaS)**. Given the discovered technical vulnerability V_t, the exploit E is developed with the support of the exploit development tool set EDT. We can model EaaS as:

$$\mathrm{E} = EaaS\,(\mathrm{V}_t, \mathrm{EDT}) \tag{5}$$

Normally, when the vulnerability is discovered, the proof-of-concept trial is also developed to demonstrate its practicality. We can explore many verified exploitations in ExploitDB [40]. While responsible vulnerability disclosure policy ensures the release of a patch before any details of the vulnerability are publicly revealed, it is possible for the hackers to automatically develop the exploitation [13] or reverse-engine the patch without the relevant details [20]. Though the automatic exploitation generation is fairly basic now [153], it is not surprise to observe new tools to support this highly valuable activity.

- **Exploit Package as a Service (EPaaS)**. Given a collection of exploits E, EPaaS combines them into the exploit kit EK that is potentially more effective than any individual exploit on its own. An unintelligent exploit kit, one that delivers all its exploits at once regardless of the conditions in the victim's systems, may adversely affect the performance of other active exploits and increase the possibility of detection. Meanwhile, intelligent exploit kits are developed to take into account the target's conditions when delivering an exploit[56]. In most exploit kits, the exploitative programs and strategies are hard-coded, but this may not be the case for long; exploit kits can be developed in such a way to enable dynamic updates as conditions change. Consider the following definition:

$$\mathrm{EK} = EPaaS\,(\mathrm{E}, \mathrm{EPT}) \tag{6}$$

where EPT refers to the strategies and tools used to package the exploits into exploit kit.

- **Deception as a Service (DaaS)**. Given the operational vulnerability $\mathrm{V_p}$, with the support of the development tools FDT, this component generates the fake information FI, like a fake website [95, 178], fake emails [66, 124], or fake software [162] which can be delivered to the target. A DaaS is defined as follows:

$$\mathrm{FI} = DaaS\,(\mathrm{V_p}, \mathrm{FDT}) \tag{7}$$

Note that if the $\mathrm{V_p}$ contains detail information about the specific target, like organization structure, business process, network environment is available, the attack is referred as targeted attack [155], and normally it will have a higher probability of success. For example, for the whaling phishing attack in early 2016, employee payroll information was successfully stolen when an employee voluntarily gave it away in an email to whom he thought to be the company's CEO [112].

- **Payload as a Service (PLaaS)**. This component offers the payloads PL involved in a cyber-attack. A payload [24, 46, 148] can refer to an atomic malicious program performing a singular function, or a combination of many independent ones to offer a more complex, comprehensive functionality. PLaaS is defined in terms of the following relationship:

$$\mathrm{PL} = PLaaS\,(\mathrm{V_t}, \mathrm{PDT}) \tag{8}$$

where PDT refers to the tools used to develop the payload.

- **Obfuscate as a Service (OBaaS)**. Given an application, such as exploit E, exploit kit EK, fake information FI, payload PL, this component uses various obfuscation strategies and technologies such as packers, polymorphism and metamorphism to reduce the chance that an application is detected by antivirus software [59, 122, 145]. For example, the Q implementation [146, 153] can be used to harden the exploits generated by the EaaS. Some may include security software to confirm the effectiveness of the obfuscation [56]. We define OBaaD in terms of the following relationship:

$$\mathrm{A_O} = OBaaS\,(\mathrm{A_I}, \{\mathrm{OBT}, \mathrm{SCS_R}\}) \tag{9}$$

where $\mathrm{A_I}$ refers to the input application, such as a payload, exploit kit, exploit, or fake information while $\mathrm{A_O}$ refers to the output application with obfuscation methods applied; OBT refers to the obfuscation tools and strategies; $\mathrm{SCS_R}$ refers to the interactions with the security checkers, if any.

- **Security Checker as a Service (SCaaS)**. This component verifies whether a given application can bypass the defensive barrier from a certain security software or platform [59]. If an application is detected by a security software, the OBaaS component can update the obfuscation strategy until the application goes undetected, resulting in a loop between the OBaaS and SCaaS.

$$\mathrm{SCS_R} = SCaaS\,(\mathrm{A_I}, \mathrm{SCT}) \tag{10}$$

where $\mathrm{A_I}$ refers to the input application from OBaaS and $\mathrm{SCS_R}$ refers to the report from the security checker tool set SCT. For example, cybercriminals once used Google's VirusTotal platform to verify the effectiveness of malware [184]. It is believed that for the Ukrainian power grid attack, the attacker built a simulated power grid system similar to the Ukrainian power grid plant that they were able to evaluate and test the developed firmware prior to the attack [45]. As shown in Figure 2 (d), OBaaS and SCaaS can form a loop to guarantee the effectiveness of the developed cyber weapons. Given the high value for this loop, it is not surprise to observe these platforms, which may even be operated similarly to the mobile app testing cloud [53] for the mobile ecosystem.

- **Repackage as a Service (RPaaS)**. Given a list of inputs, this component packages the elements of the input in a verified exploit kit to increase the effectiveness of an attack, with support from obfuscation component, OBaaS, and repackaging tools. We define RPaaS as:

$$\mathrm{VEK} = RPaaS\,(\mathrm{A_I}, \{\mathrm{RPT}, \mathrm{OBS}\}) \tag{11}$$

where $\mathrm{A_I}$ refers to the input which can be the payload PL from PLaaS, exploit kit EK from EPaaS, fake information FI from DaaS, the original benign application $\mathrm{P_0}$ or their combinations; VEK refers to the application that will be delivered to the target for cyber attack; RPT refers to the repackaging tools and strategies to enhance the input. This component plays important role for the cyber attack. Taking the playload development as an example. Since a payload may be identified by security software, hackers will revise detected payloads using the repackage component so that they may bypass detection on subsequent attacks [24]. This iterative process creates a so-called "family" of payloads [24, 166]. To circumvent detection more effectively, an advanced payload protects itself through redundant actions and encryption [122]. The malware "DenDroid" is even capable of detecting emulated environments such as Google Bouncer [164] and the WannaCry malware can detect whether the running environments are sandboxes [137]. This dynamic awareness is what sets apart intelligent cyber weapons from their less sophisticated counterparts. For the exploit kit from EPaaS, the automated shellcode placement methods are developed to generate the modified exploit by changing or replacing the original shellcode of the existing exploit for new attacks [15].

We have discussed the main value-added components related to exploitation development in the "as-a-service" model. The EaaS (exploit), PLaaS (payload) and DaaS (fake information) are related to develop the weapons to attack the victims based on the discovered vulnerability, which belongs to the *"exploitation development"* activities, aka *"weapon development"*. Meanwhile, the EPaaS (exploit kit package), the RPaaS (repackage), OBaaS (obfuscation) and SCaaS (security checker) are used to improve the effectiveness of the developed weapons, which belongs to the support activities *"resistance operation"*, aka *"weapon enhancement"*.

Based on Figure 3, various ways can be observed that exploitation services can be combined. For a given cyberattack, at least one of the "weapon development" activities will be employed while the "weapon enhancement" component is not a must. However, the more services an attacker can effectively employ, the higher the chance of success in an attack when applying the generated verified exploit kits: the VEK will be more difficult to detect for security programs and more effective in the attack. Additionally, the employed services can be used simultaneously, or can be used in different phases of a multi-step attack. For example, in the Ukraine power grid cyberattack [45], the spear-fishing emails from DaaS (fake information), the exploit kit targeting vulnerabilities including CVE-2014-4114, CVE-2010-3333 from EPaaS (exploit kit), the KillDisk, a destructive data-wiping utility and the SSH backdoor to maintain persistent access from PLaaS (payload), were used in tandem to successfully break into the Ukrainian power grid system. In the second step of the same attack, malicious firmware (from PLaaS) developed based on domain knowledge collected from the distribution manage system (DMS), which was tested by the simulated power grid system (from SCaaS), was uploaded to the system and to attack the ICS components.

3.2.3 *Exploitation Delivery Service (EDaaS).*

As shown in Figure 4, the purpose of these activities is to deliver the exploitative programs *VEK* from EKaaS to the targeted systems. Effectively, EDaaS serves as a pipeline for the cybercrime ecosystem, consisting of the following components:

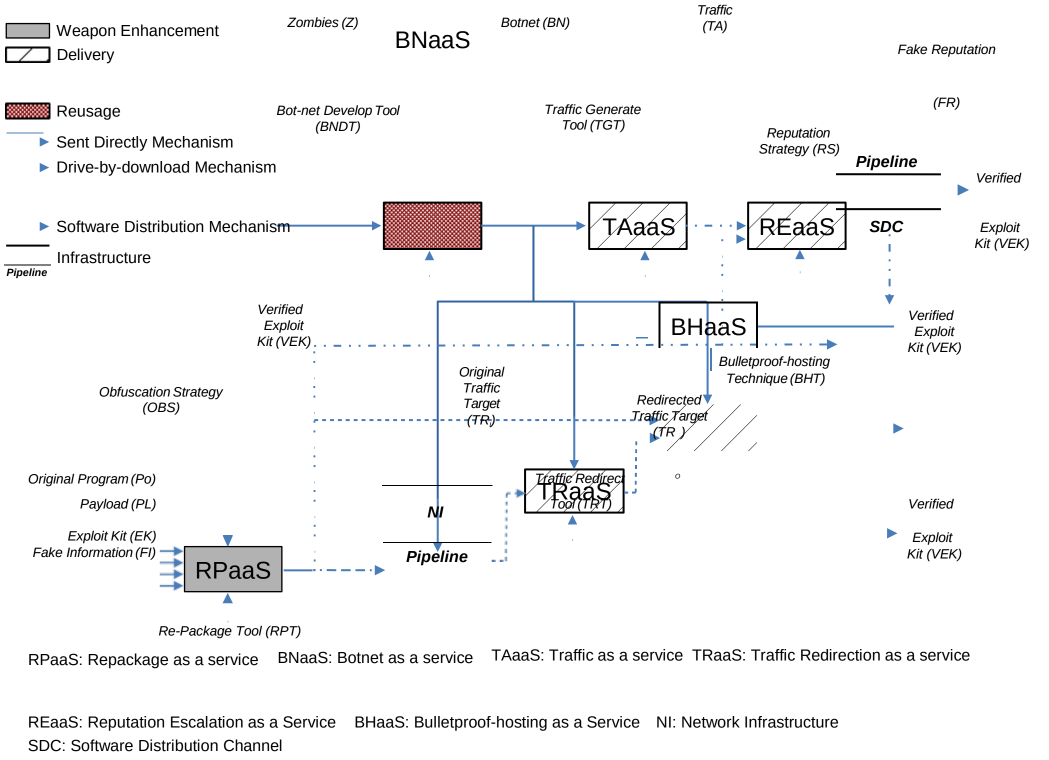

Weapon Enhancement
Delivery
Reusage
Sent Directly Mechanism
Drive-by-download Mechanism
Software Distribution Mechanism
Infrastructure
Pipeline
Zombies (Z)
BNaaS
Botnet (BN)
Traffic (TA)
Fake Reputation
(FR)
Bot-net Develop Tool (BNDT)
Traffic Generate Tool (TGT)
Reputation Strategy (RS)
Pipeline
Verified
Exploit Kit (VEK)
TAaaS
REaaS
SDC
BHaaS
Verified Exploit Kit (VEK)
Verified Exploit Kit (VEK)
Bulletproof-hosting Technique (BHT)
Obfuscation Strategy (OBS)
Original Traffic Target (TR)
Redirected Traffic Target (TR)
Original Program (Po)
Payload (PL)
Exploit Kit (EK)
Fake Information (FI)
RPaaS
NI
Pipeline
Traffic Redirect Tool (TRT)
TRaaS
Verified
Exploit Kit (VEK)
Re-Package Tool (RPT)
RPaaS: Repackage as a service
BNaaS: Botnet as a service
TAaaS: Traffic as a service
TRaaS: Traffic Redirection as a service
REaaS: Reputation Escalation as a Service
BHaaS: Bulletproof-hosting as a Service
NI: Network Infrastructure
SDC: Software Distribution Channel

Fig. 4. Exploitation Delivery Services. "Delivery" refers to the services serving to support the exploitation delivery. "Reusage" refers to the services repurposing gains from previous successful attack. "Infrastructure" refers to the network infrastructures which are operated by network infrastructure operators and serve as the pipeline.

- **Botnet as a Service (BNaaS)**. As presented in [136], given a list of compromised machines, called zombies, a developer can use tools, such as Zeus and Aldi, to implement a Botnet that is controlled by a human operator, the bot-master, in some cases through Command and Control (C&C) channels. To improve resilience with respect to being taken down, a bot-master may use tools such as multi-hopping, ciphering, binary obfuscation, polymorphism, IP spoofing, Email spoofing, and fast-flux network to maintain and update a botnet. We can formally define the botnet service component as follows:

$$BN = BNaaS(\mathrm{Z}, \mathrm{BNDT}) \tag{12}$$

where Z refers to a set of zombie machines, BN refers to the botnets, BNDT is the tool set to develop and maintain the botnet [136].

- **Traffic Redirection as a Service (TRaaS)**. Using this component, incoming web traffic to a specific address will be redirected to a server hosting the verified exploit kits, which is a fundamental component for the "drive-by-download" mechanism. A typical example is search-engine poisoning, in which cyber-criminals compromise links to popular websites and redirect search traffic to the other websites [73, 178]. We formally define TRaaS as:

$$\mathrm{TR_O} = TRaaS\,(\mathrm{TR_I}, \{\mathrm{TRT}, \mathrm{BN}\}) \tag{13}$$

where TR_I refers to the original traffic target, and TR_O refers to the redirected traffic target, TRT is the traffic redirection technique [54, 168] and BN can be used to construct a fast-flux network to support traffic redirection [71].

- **Bulletproof Hosting as a Service (BHaaS)**. Bulletproof hosting services, such as Russian Business Network, McColo, Troyak, and Vline [83], are a lot more lenient about the contents hosted on their servers so that the attackers can host any kind of materials on them without worry about being taken down: the service provider must make the servers harder to seize and be inconspicuous enough to avoid calling the attention of authorities [106]. Furthermore, the providers intend to host the severs in countries with more relaxed laws to make it easier to evade law enforcement [17]. Supporting by the botnet, some providers will hire the compromised servers out until they are discovered [106]. This kind of service is used by cybercriminals as the "gang's hideout" and is widely available in the underground market due to its emphasis on anonymity.

$$\mathrm{VEK_O} = BHaaS\ (\{\mathrm{VEK_I}, \mathrm{TR}\}, \{\mathrm{BHT}, \mathrm{BN}\}) \tag{14}$$

where BHT refers to the tools and strategies that protect the servers, such as located offshore, moving among different service providers, registering and dropping network blocks frequently [7], making them "bulletproof".

- **Traffic as a Service (TAaaS)**. This component may use many servers or sources, typically the botnet BN, to generate the traffic for the given target. One typical scenario is the well-known DDoS attack [80] which flood the bandwidth or resources of the targeted system, usually one or more web servers, with traffic from multiple compromised systems. For example, on October 21, 2016, a botnet consisting of tens of millions of Internet-connected devices infected by Mirai flooded Dyn's servers, resulting in 11 hours of blocked access to popular websites such as Twitter, Spotify, Netflix, Amazon, Tumblr, Reddit, and Paypal, among others [16]. Another typical application for this component is in an advertising fraud scheme, in which fake traffic generates vast amounts of undeserved revenue [50]. We formally define TAaaS in terms of the following relationship:

$$\mathrm{TA} = TAaaS(\mathrm{BN}, \mathrm{TGT}) \tag{15}$$

- **Reputation Escalation as a Service (REaaS)**. For the "software distribution" mechanism, to increase the exposure of the malicious applications, this component will exploit the vulnerability of the current recommendation system [151] to craft a fake reputation [182] for the given application, for example, downloading the software and posting fictitious positive ratings and reviews.

$$\mathrm{FR} = REaaS\ (\{\mathrm{A_I}, \mathrm{TA}\}, \mathrm{RS}) \tag{16}$$

where $\mathrm{A_I}$ refers to the given malicious applications and TA refers to the traffic used to generate the fake reputation FR; RS refers to mechanisms to establish reputation on a given platform.

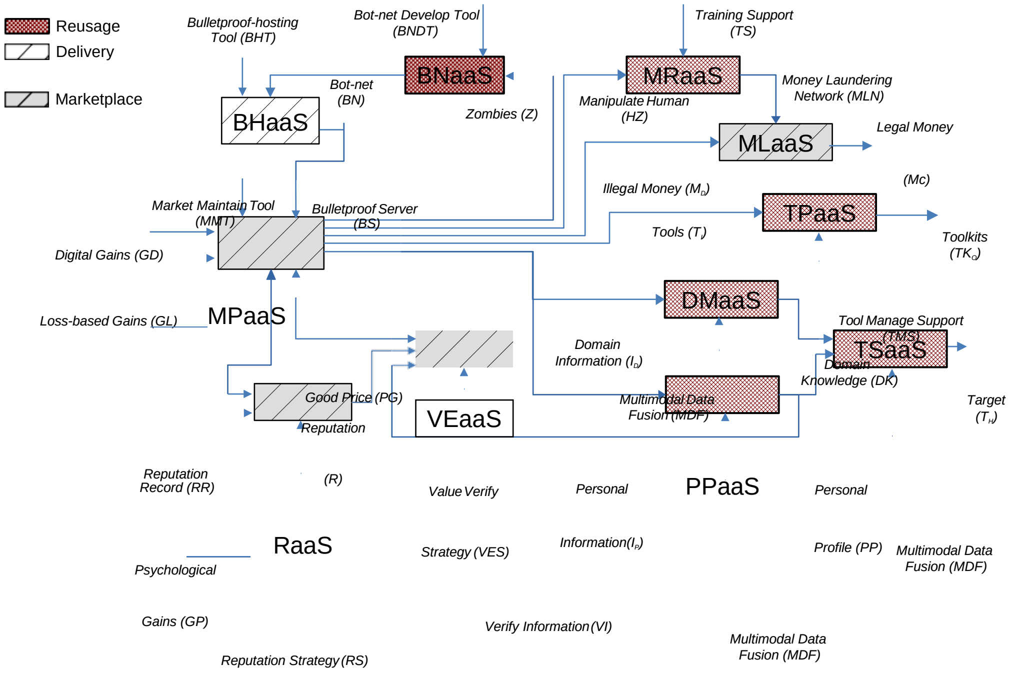
3.2.4 Multi-step Attack Service (AaaS). Once a target's systems are compromised, the avenue for attack is open and cybercriminals make their entrance seeking benefits of the following forms: digital gains (GD) including intellectual property, sensitive information, domain knowledge, compromised machines, or even a targeted user who can be manipulated; psychological gains (GP) affecting reputation, and monetized forms of benefit (GL) from damages incurred by targets. When performing a cyberattack, a cybercriminal must hide the attack from detection using an obfuscation strategy (OBS) informed by relevant domain knowledge (DK). Examples that have already been discussed include the attack on the Bangladesh Bank's (BB) SWIFT payment system [152], where attackers clearly exhibited knowledge of SWIFT operations which may be from willing-or coerced -domain experts, and the Ukraine power grid attack [45], in which power grid network structure information is believed to have been collected in previous attacks. Considering the necessary human resources (HR) services supporting a cybercrime operation in addition, we can define the component representing the attack itself as follows:

$$\{\mathrm{GD}, \mathrm{GP}, \mathrm{GL}\} = AaaS\ (\{\mathrm{VEK}, \mathrm{TA}\}, \{\mathrm{OBS}, \mathrm{HR}, \mathrm{DK}\}) \tag{17}$$

Until now, we have explored the value-added processes of the primary activities and the directly related supportive services, behind a cyberattack. In the following sections, we will discuss the supporting components that are not directly related to a cyberattack, but nonetheless critical to operations in the cybercrime ecosystem.

3.3 Cybercriminal Services Indirectly Support Primary Activities

Beyond the services that support the primary activities discussed above, there are support services related to benefit realization, focusing on monetization of cyberattack gains on different marketplaces. Personal profile information can be listed for sale or exposed publicly on underground markets to damage the organization or individual to whom the information belongs [123]; domain information are extremely valuable for the targeted cyber attack [156]; compromised computers can be sold to assemble a botnet [136]; the stolen tools can be used to construct the toolkits which offer "one-stop-shop" tool support [82]; while an manipulated person can serve as the money mule [72]. Psychological gains can help attackers build a reputation for themselves in the underground. Furthermore, to mitigate the identity and quality uncertainty [183], the reputation and pricing systems are important for the cybercriminal ecosystem. For loss-based gains, attackers can collect benefits directly from their victims; however, if it proves too difficult or risky for attackers to interact with victims to realize benefits, attackers can opt to trade the potential benefit on the market, supported by the value evaluation services. For example, a group of underground cybercriminals created Ran$umBin, a dark web service to monetize ransomware attacks that allows cybercriminals to upload stolen data, motivating victims to pay to get back their stolen data [126]. Finally but straightforwardly, offering the marketplace to enable the trading is a fundamental component for the cybercriminal ecosystem. Hence, as shown in Figure 5, we can identify the additional re-usage components beside BNaaS for the digital gains, and the marketplace components.



TSaaS: Target Selection as a service RaaS: Reputation as a service VEaaS: Value Evaluation as a service TPaaS: Tool Pool as a service
BHaaS: Bulletproof Hosting as a service MRaaS: Money mule Recruiting as a service MLaaS: Money Laundering as a service
DMaaS: Domain Knowledge as a service PPaaS: Personal Profile as a service MPaaS: Marketplace as a service BNaaS: Botnet as a service

Fig. 5. Marketplace and Gain Repurposing. "Marketplace" refers to the services to enable the trade for benefit realization while "Reusage" refers to the services which repurpose the digital gains from previous successful cyber attack to facilitate the further attacks.

3.3.1 Digital Gain Repurposing Service. Through the marketplace, these components turn the digital gains from the successful cyber attacks into services which can be reused to facilitate the further cyberattack.

- **Personal Profile as a Service (PPaaS)**. This component offers personal profile PP about targets such as passport numbers, driver's licenses, email accounts, social media accounts, or credit card numbers. Any personal information I_p that can be used to build a complete personal profile, for an individual or an organization, can be included in this component, whether it comes from data breaches [176] or public sources on the internet, such as social media pages.

$$\mathrm{PP} = PPaaS(\mathrm{I_p}, \mathrm{MDF}) \tag{18}$$

where MDF refers to the multimodal data fusion [86] that can be used to manage and analyse the collected data. It is extremely valuable because different data sets can interact and inform each other [23] to offer value-adding information about the targets. One typical application could be offering the detail information for the given individual or organization for the buyers which can be used for further attack, especially for the whaling phishing attack [66, 72].

- **Domain Knowledge as a Service (DMaaS)**. This component refers to domain information I_d gained from past attacks to offer specific knowledge DK relevant to future attacks with the support of the developing data manage and analysis technology MDF.

$$\mathrm{DK} = DMaaS(\mathrm{I_d}, \mathrm{MDF}) \tag{19}$$

The basic form of the domain knowledge is the step-by-step guidances for cyberattack. Inspired by the emergences of the WikiHow, eHow, Howcast etc. which offers extensive information about how-to tasks, as well as the development of the knowledge graph techniques [34], the DMaaS in the cybercriminal ecosystem could evolve into the similar how-to knowledge systems which can be used across different scenarios.

- **Tool Pool as a Service (TPaaS)**. Cyber-attacks, like the recent CIA breach [179] or NSA cyber incident [60], and the HackerTeam hack [68], can result in cybercriminals gaining access to hacking tools used by the targeted organizations that can be repurposed and applied in future cybercrimes. Hacker communities, often cybercrime groups or nation-support groups, will collect these tools T_I and develop new variants to address their specific goals. Since these tools can benefit the entire cybercrime ecosystem by facilitating new attacks, it is no surprise that toolkits or platforms TK_O on the dark web exist to facilitate the access to these tools. For example, the "Shadow Brokers" announced to offer a subscription-based service [82] with access to up-to-date exploits gained from the NSA cyber incident. We can formally define TPaaS as:

$$\mathrm{TK_O} = TPaaS\ (\mathrm{T_I}, \mathrm{TMS}) \tag{20}$$

where TMS refers to the technology enabling tool customization and management.

- **Target Selection as a Service(TSaaS)**. As discussed above, informed target selection is very valuable in the cybercrime ecosystem, because it significantly reduces the cost and increase the benefit from the cyberattack. Given the potential applications of personal information and domain knowledge, as well as the development of advanced data analysis and artificial intelligence, the emergence of target selection as a service is a reasonable and valuable for the cybercriminal ecosystem [107]. We formally define TSaaS as follows:

$$\mathrm{T_H} = TSaaS\ (\{\mathrm{PP}, \mathrm{DK}\}, \mathrm{MDF}) \tag{21}$$

where T_H refers to the identified valuable targets, which may even be ranked according to the different value for different attackers.

3.3.2 Marketplace Service. To support monetization efforts on dark web marketplaces, bulletproof servers are necessary to guarantee the availability and reliability of these services. The following components are important to bridge the gap between the dark web and legitimate businesses by money laundering, mitigate the identity through reputation system and reduce quality uncertainty by value evaluation and pricing.

- **Money Laundering as a Service (MLaaS)**. Given the illegal, "dirty" money M_D from a cyberattack, this component makes use of a money laundering network MLN to make it appear as though it was earned by legal means M_C. We define MLaaS as follows.

$$M_C = MLaaS(M_D, MLN) \quad (22)$$

Note that the M_C could also be in the form of digital currency, such as Bitcoin [84] since Bitcoin can be easily cashed out via digital currency trading platforms such as BTC-E or exchanged with each other [130]. MLN refers to the money laundering network consisting of many money mules, who make available their own bank or digital accounts to be used as conduits for transferring money out of the cybercrime ecosystem for a fee [31,49,72].

- **Money Mule Recruiting as a Service (MRaaS)**. To recruit the money mules who will make up a money laundering network, the mule herders, those who establish connections with would-be money mules, send out believable fake emails advertising normal jobs such as Financial Department Manager and contact again the original recipients who respond to the email. These individuals will be trained and brought into the money laundering network [158].

$$MLN = MRaaS(HZ, TS) \quad (23)$$

where HZ refers to the people acting as the money mules in the money laundering network MLN, who could be tricked to join the network because it is an acceptable "job" for them especially if they are unemployed [1]. TS refers to training support, including tools and related knowledge. Normally, the DaaS component is a prerequisite for the MRaaS component, since MRaaS relies on creating and distributing fake emails.

- **Reputation as a Service (RaaS)**. As previously discussed, reputation is very important in the cybercrime ecosystem as it serves as a metric to mitigate the uncertainty associated with dealing users who hide their true identities [183]. As a result, most marketplaces, especially forums, incorporate a reputation mechanism into their core service that generates a reputation rating based on a user's previous interactions in the marketplace. To warn the underground visitors to stay away from fraudsters[8], some third-party services such as Ripper.cc and Kidala.info [167] were developed to maintained a database of rippers.

$$R = RaaS(\{GP, RR\}, RS) \quad (24)$$

where GP refers to the previous conducted attacks of the given user while RR refers to the interaction records, R refers to the user's reputation determined by the reputation evaluation mechanism RS which can be similar to the mechanisms [151] employed by a legitimate business.

- **Value Evaluation as a Service (VEaaS)**. Similar to a legitimate business, judging the value of goods traded in a marketplace plays a fundamental role, mitigating the risk associated with quality uncertainty [183]. In the case of credit cards, the quality of a stolen card may depend on the credit limit of the account, and this will drive the price. Recently, Fatboy, a new ransomware-for-hire scheme, automatically adjusts its ransom demands according to the Big Mac Index, a way to measure the extent to which currencies are overvalued or undervalued [58]. Additionally, some cybercriminals use scanned documents, such as passports or driver's licenses, to confirm other users' identities. For example, a hacker may verify a Paypal account with a scanned copy of the purported owner's passport [56].

$$PG_O = VEaaS(\{PG_I, R, VI\}, VES) \quad (25)$$

[8] In the cybercriminal ecosystem, it is not clear who are the "good guys" and "bad guys". A "fraudster" can be actually a law enforcement associate trying to track down hackers [183]. The attackers can even condust attacks against each other [27].

where PG_I refers to the goods offered by the providers on the marketplace; R refers to the seller's reputation; VI refers to the verify information which can be part of the personal profile from PPaaS; VES is the methodology to evaluate the value to determine the good's price PG_O.

- **Marketplace as a Service (MPaaS)**. As discussed above, the marketplace is a fundamental component, serving as the trading place to realize the benefit from the cyber attacks. It serves as a pipeline to transfer the gains from a successful cyberattack into input for many different types of services which can facilitate the further cyber attack, and the monetary benefit which can be made as legal through money laundering.

$$\{G_O, M_D\} = MPaaS\ (G_I, \{MMT, BS, RR, PG\}) \tag{26}$$

where G_I refers to the products or services traded in the marketplace, which can be the digital gains GD or the loss-based gains GL from a cyber attack. Note that each service mentioned in this paper can also be traded in the marketplace, including the MPaaS itself can also be available in the dark web to build a specific marketplace for some attackers. G_O refers to the different types of materials like personal information I_p, domain information I_d, stolen tool set T_l, compromised machines Z, manipulate human HZ. M_D refers to the illegal monetary benefit the seller achieve from the trading; MMT refers to the tool and technique to build the marketplace in the dark web, BS refers to the bulletproof server to host the marketplace; RR refers to the seller's activities records while PG refers to the evaluate value for the goods, representing the support from the RaaS and VEaaS to mitigate the identity and quality uncertainty.

3.3.3 Human Resource Service. The main functionality of human resources is to train novice hackers so that they attain the necessary skills to participate in cyber-attacks, and to recruit new hackers to join the community or to participate in a specific cyberattack. As shown in Figure 6, it consists of the following two main services:

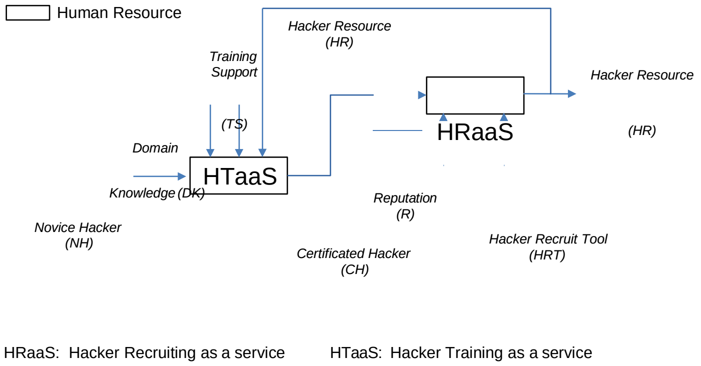


Fig. 6. Human resource service. These services prepare the necessary human resource for the cyber attack business through training and recruiting.

- **Hacker Training as a Service (HTaaS)**. Given specific domain knowledge related to a cyberattack, this component helps a hacker, especially a novice hacker, gain skills relevant to cybercrime and become a qualified member in the hacker community. In its most basic form, HTaaS offers step-by-step guides or online school like OnionIRC [52]. Nowadays, it has grown into an industry of its own, and is not necessarily an underground activity or an illegal business at this point. For example, the offensive security provides the "true performance-based penetration testing training" [147] offering certifications once training is completed, and even runs a bug bounty program to reward those who find qualifying vulnerabilities in their sites. We formally define

HTaaS as follows:

$$\mathrm{CH} = \mathit{HTaaS}\,(\mathrm{NH}, \{\mathrm{DK}, \mathrm{TS}, \mathrm{HR}\}) \tag{27}$$

where NH refers to the hackers without the specific hacking skill, who are normally the novice in the community; CH refers to the hackers gaining the necessary skills, namely certificated hackers; DK refers to the necessary domain knowledge; TS refers to the tools or platforms supporting training; HR refers to the hackers who can offer the training materials, such as personal experience, domain knowledge, or mentorship.

. **Hacker Recruiting as a Service (HRaaS)**. Cybercriminals may need to recruit additional hackers to collaborate on a particular attack. As an example, a nation-state sponsoring a cybercrime operation may hire non-affiliated hackers to carry out an attack, reducing the political risk that accompanies the sponsorship of cybercrime [154]. We define HRaaS as follows:

$$\mathrm{HR} = HRaaS\ (\mathrm{CH}, \{\mathrm{R}, \mathrm{HRT}\}) \tag{28}$$

where HR are the hacking resources that can be used for an attack while CH are the available, certificated hackers; R refers to support from the reputation system RaaS; HRT refers to the tools or platforms to recruit the reliable hackers to join the group or to participate into a cyber attack.

3.4 Cybercriminal Service Ecosystem Framework: Systematic Understanding of Cyberattacks

Following the value chain model presented in Section 2, we have identified 25 different services [9] related to cybercrime activities in primary and supporting roles. Using the definitions about service composition discussed above, we can combine these services, preserving their dependences, to form the systematic framework shown in Figure 7.

It can be seen that the cybercrime ecosystem can be viewed as a complete cyber-threat capability supply chain. "Weapon Development" activities transform discovered vulnerabilities from "Vulnerability Discovery" into effective weapons by "Exploitation Development" for cyber-attacks. "Weapon Enhancement" activities make a cyberattack more powerful and better suited to avoid detection, which are components of the "Resistance Operation". The "Delivery" activities represent the act of delivering cyberattack weapons to their targets. "Marketplace Support" activities create the platforms for cybercriminals to trade the gains from successful attacks, while "Reusage" activities re-purpose these gains to enable further attacks, serving as the "Benefit Realization" component in the value chain. "Human resource" activities represent human resources that support the cybercrime ecosystem. Finally, the tools and platforms to support these identified services are parts of the "Technology Support" in the value chain model.

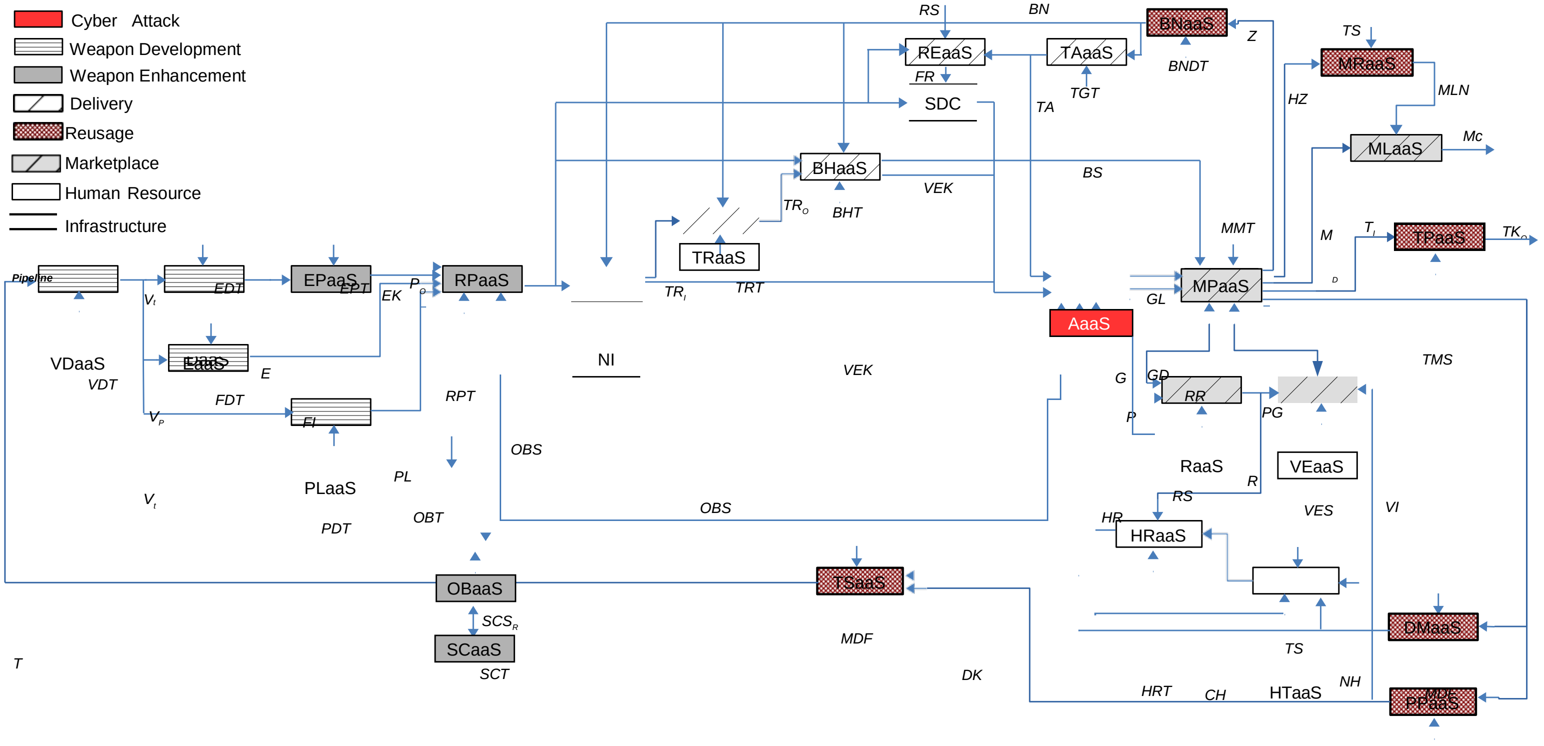
In the following section, we will present how this cybercriminal service ecosystem framework can help us to systematically understand the hacking innovations of the cyberattacks which can change the "Cat-and-Mouse" game for cybersecurity defense. Additionally, we can identify two example strategies, if implemented, can help to more effectively combat cyberattacks and build a more "cyber-immune" world.

4 IMPLEMENTATION

4.1 Change the Cat-and-Mouse Game: Understand the Hacking Innovations

Using this framework, we can systematically understand the hacking innovations in the cybercriminal ecosystem, including the development of these cyberciminal services, the evolving cyber-threat, and the emerging services, like "cyberciminal service composition as a service".

[9] Please check the Appendix to see the glossary.



VDaaS: Vulnerability Discovery as a service **EaaS**: Exploit as a service **EPaaS**: Exploit Package as a service
DaaS: Deception as a service **PLaaS**: Payload as a service **RPaaS**: Repackage as a service **OBaaS**: Obfuscation as a service
SCaaS: Security Checker as a service **BNaaS**: Botnet as a service **TAaaS**: Traffic as a service **NI**: Network Infrastructure
TRaaS: Traffic Redirection as a service **REaaS**: Reputation Escalation as a Service **BHaaS**: Bulletproof-hosting as a Service

TSaaS: Target Selection as a service **RaaS**: Reputation as a service **VEaaS**: Value Evaluation as a service **TPaaS**: Tool Pool as a service
DMaaS: Domain Knowledge as a service **MRaaS**: Money mule Recruiting as a service **MLaaS**: Money Laundering as a service **MPaaS**: Marketplace as a service

SDC: Software Distribution Channel **PPaaS**: Personal Profile as a service **HRaaS**: Hacker Recruiting as a service **HTaaS**: Hacker Training as a service **AaaS**: Multi-step attack as a service

Fig. 7. Cybercriminal Service Ecosystem Framework: systematic understanding of the cyberattack business based on the identified services and their dependencies, including 25 services, their supported tools and two related network infrastructures.

4.1.1 Cybercriminal Service Development. Based on the above discussions, we follow the value-added processes to construct the cybercriminal service ecosystem framework[10] and we can observe cases for most identified services in the dark web. Those that were not yet observed in the cybercriminal ecosystem are related to the supportive activities, like the services related to hacker organization, target selection and benefit realization. A possible reason for this is that these supportive activities are not offered as independent components and are much deeper underground, because they are not related directly to the cyber-attacks. For the vulnerability discovery services, due to the high uncertainty for vulnerability discovery, we have not observed instances in the dark web during our research.

The offensive side and the defensive side are using similar innovations, and the innovations in legitimate businesses can drive the evolution of the components in the cybercriminal service ecosystem so that the attackers can tap into the benefit of these developments. Hence, it is reasonable to expect that, if they do not already exist, the offensive versions of legitimate defensive techniques will emerge for the cyber-attacks, either trading on the dark web or used by the organized and nation-supported cybercrimes. We can find similar applications and scenarios in legitimate businesses to predict developments of the cybercriminal services as follow:

- For the *"hacker organization"*, hacker assignment tools resembling project management applications can be used to organize hackers involved in an attack;
- For *"vulnerability discovery"*, inspired by the rapid growth of the bug bounty program platforms, it is possible that we will observe similar applications in the dark web to take advantage of wisdom from the whole hacker community for a targeted cyber attack. Additionally, services which can dig into the operational vulnerabilities [119, 140, 141] could emerge and prove attractive to attackers;
- For *"target selection"*, given the rapid growth of the targeted cyber attack [98, 107, 156], targets ranking based on value can spread to, and prove popular, in the dark web;
- *"Repackaging"* to produce a verified exploit kit, including the EPaaS and RPaaS, requires specific skills and some attackers are doing by themselves. However, with the development of the technology, it is reasonable to expect that platforms will emerge to make the repackage much easier, or offer related tools to help the attackers to do this task in a more effective way [13, 20, 153];
- Providing the *"security checking"* platform for testing, similar to the emerging mobile app testing cloud in mobile ecosystem [53], can increase the succeed rate of cyber-attacks;
- For *"domain knowledge"* services, the most likely services we may expect to observe would resemble the "how-to" knowledge systems similar to the emerging online platforms like WikiHow, eHow and Howcast [34];
- Many comparison shopping websites [63] help the customers filter and compare products based on price, reviews and other criteria. It can be expected that similar *"valuation"* services will emerge on the dark web to help cybercriminals choose the most reliable components, and to help sellers competitively price their goods;
- For the *"personal profile"* services, the available data from data breaches and social media, as well as the development of the multimodal data fusion techniques, will further enable new services that will offer value-added information on the given targets when requested.
- Hackers may even offer cloud-style *"bulletproof servers"* [106] on the dark web to tap into the benefit of cloud computing [12];

[10] Please refer to Figure 9 in Appendix for the details about the mapping between the value chain model and the ecosystem framework.

- *"Tool-kit platforms"* will emerge to collect the hacking tools, especially those developed or customized by the highly skilled hackers or nation-supported hacker organizations, and make them available even in a "one-stop-shop" style [2, 19, 171, 186] to enable the attackers to do some more destructive attacks.

Additionally, based on the presented framework, we can expect the rapid growth for these services. We have already observed an increasing number of data breach incidents in recent years [176] and this trend is unlikely to change in the near future. The development of the multimodal data fusion technologies [34, 86] including machine learnings, data analysis, knowledge management technology etc., will further enables the growth of the PPaaS (personal profile) and DMaaS (domain knowledge) in our framework. The website "Have I been pwned?" reports that about 3,806,000,000 accounts from 220 websites have been compromised as of June 14th, 2017 while the number is still increasing. It can be expected that these two components will become increasingly active and common in the underground cybercrime community. The development of PPaaS and DMaaS will further drive the development of TSaaS (target selection), which itself is an input to the "weapon development" process for targeted cyber-attacks. Using the semantic social engineering attack as an example [66, 72, 124], we see an evolution from large-scale phishing emails using templates, to spear-phishing emails that are formatted for a specific user by taking into account that person's personal profile. Spear-phishing attacks are trending toward targeting high value victims, driving the evolution of whaling phishing. In the future, with the development of the TSaaS (target selection), the cost for whaling phishing will significantly reduce so that it is expected to observe large-scale whaling phishing attacks. In general, we can foresee an emergence of more and more personalized, large scale cyber-attacks as target selection services become more advance.

Another growing component in the framework is "Repackage-as-a-Service (RPaaS)", which finds itself at the crossroads of many value-added paths. If this kind of services is already available on the dark web, it is very possible that we will experience a significant number of new malware attacks relying on repackaged payloads and new obfuscation methods. It has been observed that traditional security technologies such as firewalls and intrusion detection systems are limited in their capabilities to defend against the threat posed by evolving malware [29, 46, 165]. The defensive side is constantly having to catch up with the emergence of new malware, but if malware detection approaches were to take into account the repackaging trend, identification of new malware and the level of readiness in the face of malware cyber-attacks need to be improved. For example, the use of the artificial intelligence in programming, like neural programmer interpreters (NPI) [134] and Decoder [14], could support the automatic malware generation so that the detection approaches can be developed before the malware is available in the wild.

4.1.2 Cybercriminal Threat Development. To evaluate whether the presented framework can thoroughly describe the cybercriminal ecosystem and serve as a tool to study the evolving cyber threat, we consider the cyber threats discussed in the McAfee Labs 2017 Threats Prediction report [107] as an example. This McAfee report proposes 14 predictions for cybersecurity developments in 2017. Not all predictions are related to cyber-attacks, and we only consider those related to cybercrime, mapping them into the presented framework to understand the cyber-threats they pose[11]. Those specially related to the potential defense efforts, such as *"Leveraging increased cooperation between law enforcement and industry, law enforcement takedown operations will put a dent in cybercrime"* or *"Threat intelligence sharing will make great developmental strides in 2017"*, are not included in the following discussions.

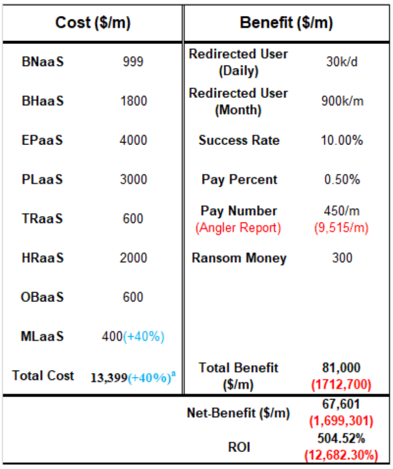
[11] Please refer to Figure 10 in Appendix to see the detail mapping of the cybercriminal threats to the ecosystem framework.

- **Ransomware Attacks, especially to compromise business processes**. Ransomware attacks continue to pose a significant threat. Often, the victim of a ransomware attack will be redirected to a server where an exploit kit, such as RIG or Neutrino, is hosted. The exploit kit capitalizes on vulnerabilities in the victim's systems to install a downloader, opening the door for the attacker to activate a ransomware payload like Wana Decrypt0r, Locky, or CryptoWall to lock the victim's computer and compromise the business continuity of the victim's operations. It can be seen that this threat follows a path in our framework involving EPaaS (exploit package), DaaS (fake information), PLaaS (payload), RPaaS (repackage), TRaaS (traffic redirection), BHaaS (bulletproof server), BNaaS (bot net), AaaS (multi-step attack), MPaaS (marketplace) and MLaaS (money laundering).
- **Social engineering attacks accelerates by machine learning**. With greater accessibility to machine learning technology, the FBI-labeled Business Email Compromise (BEC) scam [105], in which the scammers target employees with access to company finances and trick them into making wire transfers to bank accounts thought to belong to trusted partners, has become much more prevalent due to the available information to manipulate the target's perception. Based on data gathered from data breaches, social media, public disclosures, as well as domain knowledge, cybercriminals can train a model to identify valuable targets, and then generate convincing fake messages for a semantic social engineering attack. This threat begins at PPaaS (personal profile), and DMaaS (domain knowledge), makes use of TSaaS (target selection) and VDaaS (vulnerability discovery) to identify the operational vulnerability in the specific targets; and finally relies on the DaaS (fake information) to generate persuasive but fake message for the attack.
- **Fake reputation generation by botnet**. Reputation systems are an important component of any digital community. Due to the vulnerabilities inherent in a reputation system, services to falsify a user's reputation are available and growing in scope. To support this activity, a botnet, no matter if constructed by infected machines, or physical servers located in data centers, can be used to generate the fake clicks or comments that increase a user's online notoriety. This attack represents the application of the online traffic, involving BNaaS (botnet), TAaaS (traffic) and REaaS (reputation escalation).
- **Ad wars technology to boost malware delivery capabilities**. Advertisers display ads in hopes that a user will click on them. Once the ad is clicked, a user profile is generated that allows for targeted advertisements, and greater revenue for advertisers. This technology will likely be used by cybercriminals to redirect traffic to a compromised website, representing the recent growth of TRaaS (traffic redirection).
- **Privacy explosion by hacktivists**. The data breaches are expected to increase, targeting at some of the corporate clouds that contain customer data. Stolen data is sure to bring profit to cybercriminals, meaning that PPaaS (personal profile) will become more accessible.
- **Cyber threats to hardware, firmware, drone, mobile ecosystem, and IoT increase while attack to Windows subside**. This threat prediction discusses about cyber threats to the different targets with different technical environment, which is related to the TSaaS (target selection).

These threats can be mapped into our framework. Hence, the presented ecosystem model can serve as a tool, allowing us to think systematically about the evolution of cyber-threats. More importantly, these threats are not independent, in fact, they form the reinforcement loops, including the reuse of the compromised machines, stolen tools, stolen information and the hacking experience, by which each threat reinforces and empowers the others. Note that the McAfee report does not consider many components related to cybercrime support activities, although we understand them to be very important in the systematic understanding of cyber-threat evolution. For example, understanding of the OBaaS (obfuscation) [145] will be very important for the security software providers to prepare before the attacks. The development of the money laundering network driven by the use of digital currency in the cybercrime ecosystem [21] will also bring change to approaches used in benefit realization.

4.1.3 Profitability of Cybercriminal Business: the Emergence of Composition Services. As discussed above, components involved into the cyberattack are offered as services that a would-be attacker can purchase on the dark web to equip themselves for an attack. To analysis the profiability of the cybercriminal business, as shown in Figure 8, we use the ransomware attack as an example. The price of each involving service are based on the observed instances in the dark web. For the benefit, we use the indicators from the Angler revenue reported by Cisco [35] as a baseline but make a much more conservative estimate acknowledging the defensive efforts.

- **Costs of sample services**. To run a ransomware attack as a business, a cybercriminal can buy BNaaS (botnet) for $999 per month, a traffic redirection protocol for $600, six servers as a part of BHaaS (bulletproof server) for $1,800 per month, access to the Neutrino exploit kit in EPaaS (exploit package) for $4,000, a ransomware payload with customer support in PLaaS (payload) for $3,000 and the traffic redirection service TRaaS to redirect victims to servers for $600 per month. To further increase the effectiveness of an attack, a cybercriminal can hire a qualified hacker from HRaaS for $2,000 per month, and employ an obfuscation service from OBaaS to repackage the exploit kit and payload for $600 per month. Finally, to reduce risk of arrest, services to monetize benefits in the wake of a cyberattack as a part of MLaaS (money laundering) can be accessed for a fee of $400 and 40% commission on processed funds.



Cost ($/m)		Benefit ($/m)	
BNaaS	999	Redirected User (Daily)	30k/d
BHaaS	1800	Redirected User (Month)	900k/m
EPaaS	4000	Success Rate	10.00%
PLaaS	3000	Pay Percent	0.50%
TRaaS	600	Pay Number (Angler Report)	450/m (9,515/m)
HRaaS	2000	Ransom Money	300
OBaaS	600		
MLaaS	400(+40%)		
Total Cost	13,399(+40%)[a]	Total Benefit ($/m)	81,000 (1712,700)
		Net-Benefit ($/m)	67,601 (1,699,301)
		ROI	504.52% (12,682.30%)

Fig. 8. ROI for the Ransomware Attack Business: Value of the cybercriminal service composition. Blue color means that the monetization service request 40% commission from the benefit the attacker gains. Red color refers to the case that the number of victims who pay the ransom from Angler Revenue Report [35] is used. In this case, the ROI (12,682.30%) is much higher than the best performing company, Cheniere Energy Partners Lp Holdings, Llc (7020.69%) in August 2017 reported by CSIMarket [39].

- **Example of Return on Investment (ROI)**. For calculating benefit, we assume that 30,000 people are redirected per day, of which 10% are victims of a ransomware attack where 0.5% of victims pay a $300 ransom. Though only 450 victims (0.05% of total users redirected) will end up paying the ransom over a period of one month (30 days), this brings the cybercriminal's monthly earnings to $135,000. We can see that the Return-On-Investment (ROI), even when only a small proportion of people end up paying a ransom, is as high as 504.52%, an impressive ROI for a business.

Using the reports from CSIMarket [39] for comparison, the highest industrial ROI, which is from the Tobacco industry, is only 50.63% in August 2017; in fact, this theoretical cybercrime operation would be ranked as one of the top seven best performing companies in the world in terms of ROI. If we use the numbers from the Angler revenue report which shows that 9,515 users pay the ransom per month, a number more than 20 times larger than the 450 users dictated by our assumptions, then the ROI of this operation would be 12,682.30%, which is significantly higher than the highest ROI from Cheniere Energy Partners Lp Holdings, Llc (7020.69%) in August 2017.

. **Cybercriminal service composition as a service.** Hence, we can conclude that combining separate services to perform a cyberattack has great value for cybercriminals. This motivates the emergence of *"cybercriminal service composition as a service"*. In this scenarios, the attacker can collaborate and apply services available on multiple dark web marketplaces and combine them together to offer a "one-stop shop" style service, which will continuously reduce the barriers to entry of cybercrime and performing complex cyber-attacks. More importantly, this development also allows cybercriminals involving in the cybercrime ecosystem to focus on the parts of the value chain model at which they are best, and provide their expertise as a service to other cybercriminals. Following this "specialization, commercialization and cooperation" trend, cybercriminals have been able to hide themselves even deeper in the dark web, and in certain cases, some of their activities may no longer be characterized as illegal.

More importantly, this framework can not only help us to systematically understand the cyberattacks, but also inspire several strategies to more effectively combat them. Due to the space limitation, we will take the control point identification and responsibility sharing as two examples.

4.2 Striking the Dark Side: Identifying Control Points to Improve Effectiveness

To understand the dark web itself is a step in the right direction in the effort to stymie the growth of the underground cybercrime ecosystem; however, this is more easily said than done, as collecting data on dark web activity proves difficult [66]. The "honeypot" is a technology to detect, deflect, or counteract attempts to use information systems in an unauthorized way, and many honeypot systems have been used to reveal information from how and why cybercriminals intrude into certain systems, to what threats exist or are developing in the wild [4, 29, 118]. The Telekom-Fruhwarnsystem project [118] was launched in 2013 to establish a worldwide multi-honeypot platform to collect unbiased quantitative data that would present a realistic picture of internet threats. The data the system collects is related to attack profile, and describes the attack's sources, vulnerabilities it exploits, tools it employs, and level of sophistication. The HoneyCirculatior monitor system behaves like a compromised systems to collect the malware, bait credentials, fraudulent access and compromised web content [4]. It can be seen that these honeypots are purposefully planted in certain corners of cyberspace to target certain cybercriminals, as described by AaaS (multi-step attack). Some researchers have also tried to understand exactly what goods are traded on the dark web [6, 33, 76, 186], focusing on MPaaS (marketplace).

Based on the presented cybercrime ecosystem framework, if we can rig with "honeypots" the important control points in the cybercrime ecosystem, representing the value-added paths of the cyber-threat supply chain, we can achieve a better understanding of the underlying economy of cybercrime and profile what has until now been the "dark side" of a cyberattack. Inspired by [36], we can define the control point as the critical components which can support the other components in the cybercrminal service ecosystem.

Definition 6: Control Point Services. A cybercrime service is considered as a control-point service, if and only if its output can be the support for another service.

Hence, it can be seen from the framework that followings are control-point services in the cybercriminal service ecosystem[12]

- OBaaS (obfuscation), work with SCaaS (security checker) to circumvent detection, which can bypass the effort from defensive side to improve the success rate for a cyber attack.
- BHaaS (bulletproof server), offers bullet-proof server access to improve the resilience of the underground economy.
- HRaas (hacker recruiting) recruits hackers to join the cybercriminal ecosystem or participate into a cyber attack.
- BNaas (botnet) provides botnets to support numerous components in the ecosystem, which is a fundamental infrastructure for the cybercriminal ecosystem.
- MRaaS (money mule recruiting) constructs the money laundering network to transfer the illegal money into legal one, acting as the connection between the underground economy and the legitimate businesses.
- DMaaS (domain knowledge) yields necessary domain knowledge, PPaaS (personal profile) reveals personal information, and TPaaS (tool pool) offers tools that support other activities.

If the defense side can build the "honeypot" style services for these control points, it can help the cybersecurity community, the defensive side, more effectively understand and monitor the evolution of the cybercrime ecosystem. For example, the infrastructure developed by Onaolapo et al. [123], which plant the honeypot in the PPaaS, can be used to monitor how compromised Gmail accounts are used on the dark web. This research reveals that cybercriminals tend to evade security mechanisms employed by online services meant to flag suspicious logins, and proposes a behavioral model based on the contents of search queries that could signal malicious activity. Taking down these control point components, especially the reuse related components including BNaaS, DMaaS, PPaaS, TPaaS and MRaas, can also help to break the reinforcement loops in the cybercriminal ecosystem.

Furthermore, such a scheme could also help law enforcement associates collecting critical evidence to convict cybercriminals and strike at the heart of cybercrime business. More interesting aspect here is that given the uncertainties related to identity and quality, the cybercriminal market is a typical "market for lemons" [113, 177, 178]. If the defensive side can flood the cybercriminal ecosystem with honeypot-style or fake goods, it will make the dark web less attractive for cybercriminals looking to purchase services. The practice which demonstrates the feasibility is that when the dark web marketplace AlphaBay was closed and the servers for Hansa, another dark web marketplace was seized by the government, they continued to run Hansa for a month to collect information about the vendors and customer [51]. This strategy, running Hansa under control, further raise the concerns for the hacker community that the other dark web markets, like Dream market, was also compromised in a similar manner and under police control.

Finally, from the control point analysis, we can observe that HRaaS (hacker recruit) also serves a control-point role for the cybercriminal ecosystem, which can be considered as the pipeline to recruit the cybersecurity workforce into the offensive side. Without considering the impact from HRaas, the effectiveness of many efforts to improve the cybersecurity workforce supply by offering related training [42] will be significantly reduced.

[12] Please refer to Figure 11 in Appendix C for the list of the control-point services.

4.3 Sharing Responsibility: Action Suggestions for Better Collaboration

There exist several challenges plaguing cybersecurity and cybersecurity policy when it comes to working together to build a safer connected world [113]: the externalities [87], misaligned incentives [11] and the information asymmetries [9]. These market failures calls for implementation of policy to allocate responsibilities to different parties so cybersecurity can be improved in the places where economic forces disincentive it. Given the presented cybercrime ecosystem framework, we can identify which responsibilities or actions fall to which actors based on whether the actors have the capability to take the actions[13]:

- *Individuals and Corporations* have a responsibility to protect themselves by investing in security software or hardware, altering processes, or educating people on common cyber-attacks. There is also a responsibility for the defenders to share cyber risk information. However, how to design effective mechanisms to motivate the information sharing while bypass its negative effort is still an open but challenging issue [32, 88, 99, 180].
- *Software/Hardware Providers* have a responsibility to monitor vulnerabilities and exploitations in their products. Nonetheless, issues persist related to the delays in the application of patches for discovered vulnerabilities [150] so that software/hardware providers must acknowledge these delays and work with users to accelerate the rate at which patches take effect. Furthermore, in practice, once the lifecycle of a piece of software/hardware has run its course, providers no longer offer automatic fixes, updates, or online technical assistance for the product. This leaves those older, yet widely used products vulnerable to attack. The WannaCry Hurricane attack in May 2017 is one recent example of such cyber incidents [137]. Thus, there is a need to discuss policy related to product support lifecycle, and the responsibility for providers and users when older versions of products are still widely used.
- *Security Companies*, put simply, must fight cyber-attacks, especially the payloads. Many technologies such as pattern matching, static analysis, dynamic analysis, hybrid analysis, and even human analysis have been presented over the years as solutions to defend against cyber-attacks [3, 46, 165, 166]. Beside these catch-up efforts, it will be beneficial to adopt the frame of mind of a hacker and work accordingly to identify ways in which security defenses could be bypassed. Inspired by bug bounty programs for the vulnerability discovery, security companies could offer similar programs to hire external experts, such as cybersecurity researchers, to develop effective obfuscation techniques and render them ineffective by updating security measures before the same techniques are developed or exploited by cyber-criminals. Additionally, if security companies can set up honeypot-style security checkers through SCaaS (security checker), it could be possible for the security companies to collect information to combat future cyber-attacks.
- *Infrastructure operators* such as the Internet Service Providers (ISP), according to our framework, should work to disrupt the delivery of cyber-attacks because they are in the position to monitor the Internet traffic. Though some infrastructure operators actively participated in botnet detection and abuse reporting [56, 77, 78, 128, 175], how to incentivize ISPs to involve themselves in the fight against cybercrime is an important one for the defense side. It also requires the international collaboration [17] to fight against the delivery of the cyberattack, as the Internet, and the cybercriminals with which it is infested, knows no borders.
- *Financial Systems*, such as payment networks, must take responsibility for curbing the monetization activities of cybercriminals. However, in the case of the money mule recruiting service (MRaaS) to build a money laundering network, no banks or take-down companies actively pursue the elimination of money mule recruitment websites [114]. We deem it necessary to

[13] Please refer to Figure 11 in Appendix for the responsibility allocation.

rethink financial systems' responsibilities when it comes to combatting cybercrime-related financial transactions. In addition, the anti-money laundering operations are ill prepared to deal with digital currencies, such as BitCoin, which inhabit a legal gray area [21]. Hence, the financial sector should emphasize collaboration, and acknowledge its shortcomings when it comes to digital currency-related cybercrime monetization activities.

- *Government* has an important role in combatting cybercrime, given its position to address market failures related to cybersecurity. Just as we mentioned above, it may be in the government's interest to develop strategies to take down or control the dark web market places directly, or flood them with fake goods to destroy its reputation system for identify uncertainty mitigation. Furthermore, because the defensive and offensive sides are using largely the similar innovations, it is paramount to ensure trainees work for the right side. The government should consider strategies to recruit skilled individuals to the defensive side and combat incentives that drive them to join the cybercrime business.
- *Third-party threat intelligence service providers* should monitor dark web activity to study how cybercriminals reuse the achievements from the successful attacks. More third-party services focused on TPaaS (tool pool), DMaaS (domain knowledge), PPaaS (personal profile), and TSaaS (target selection) would be welcomed in the cybersecurity community, since more information translates to greater preparedness in the face of cyber-threats. However, how to motivate them to work for defensive side instead of the cybercriminal ecosystem is still an unclear but paramount issue.

5 CONCLUSION

Cybersecurity has become relevant on the scale of nations. The "double-edged sword" nature of cybersecurity technology means that the defensive and offensive sides use similar innovations, and until now, the offense has been able to nurse its advantage: "the bad guys are getting badder faster". Cybercrime is no longer just a hobby. Cybercrime has become a business, and even less-than-prodigious hackers may choose it as a profession. The cybercrime ecosystem has evolved to encompass a comprehensive supply chain built around certain value-added processes. Furthermore, recent "as-a-service" innovations accelerate the evolution of the cybercrime ecosystem and the growth of the cybercrime business, reconstructing into a specialization, commercialize, and cooperation system. Without a systematic understanding of this trend in the cybercrime ecosystem, effectively combatting cyber-attacks has been proved difficult.

This paper constructs the value chain model based on a survey of the value-added processes for cyber-attacks. We see that aside from the primary activities of vulnerability discovery, exploitation development, exploitation delivery, and attack, many support activities are emerging to facilitate cyber-attacks, including attack lifecycle operations, human resource management, marketing and delivery, and technology support. Combining the value chain model with the developments of the "as-a-service" innovations, we model cybercrime activities as service components with inputs, outputs, and supports. In this way, we can identify the relationships between components and construct a global view of this underground business: the cybercrime service ecosystem framework.

Finally, we discuss the implementation of our framework to understand the hacking innovation, identify the control-point activities and assign responsibility to encourage collaboration among interested parties. The framework enables us to systematically understand the hacking innovations in the cybercriminal ecosystem, including the cybercriminal service development, cyber-threat evolution and the emergence of composition service: "cybercriminal service composition as a service", which can offer "one-stop-shop" style cyberattack services for the cybercriminal ecosystem. More importantly, it inspires several strategies to more effective combat cyberattacks. For example, striking the dark side by identifying the control points which represent the key components of the cybercriminal ecosystem can help the defensive side to effectively deploy the "honeypots" to monitor and combat the cybercriminal activities; assigning responsibility to different actors with vested interests in cybersecurity following the value-added processes can encourage meaningful collaboration towards a safer world.

By conceptualizing the modern cyber attack business systematically, we can better design cyberattack combat strategies. More research about how to disrupt the business of cybercrime by stymieing the development of the threat capability supply chain in the cybercrime ecosystem is needed for the security community. Additionally, there is room for discussions on issues of ethics surrounding cyberattack, which can help in the design of new regulations that improve cybersecurity across the board.

ACKNOWLEDGMENTS

The authors would like to thank the members from the MIT-(IC)^3 for their valuable comments and inputs to improve the value-chain models and the cybercriminal service ecosystem framework, as well as the implementation inspirations.

REFERENCES

[1] ABC NEWS. 2008. Bad economy helping Web scammers recruit mules. (2008). http://abcnews.go.com/Technology/story?id=6428943

[2] Lillian Ablon, Martin C. Libicki, and Andrea A. Golay. 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Technical Report. RAND Corporation. 1–85 pages.

[3] Yasemin Acar, Michael Backes, Sven Bugiel, Sascha Fahl, Patrick Mcdaniel, and Matthew Smith. 2016. SoK : Lessons Learned From Android Security Research For Appified Software Platforms. In *2016 IEEE Symposium on Security and Privacy*. 433–451.

[4] Mitsuaki Akiyama, Takeshi Yagi, Takeo Hariu, and Youki Kadobayashi. 2017. HoneyCirculator: distributing credential honeytoken for introspection of web-based attack cycle. *International Journal of Information Security* (2017), 1–17. https://doi.org/10.1007/s10207-017-0361-5

[5] Abdullah M. Algarni and Yashwant K. Malaiya. 2014. Software Vulnerability Markets : Discoverers and Buyers. *International Journal of Computer, Electrical, Automation, Control and Information Engineering* 8, 3 (2014), 480–490.

[6] Luca Allodi, Marco Corradin, and Fabio Massacci. 2016. Then and Now: On the Maturity of the Cybercrime Markets the Lesson That Black-Hat Marketeers Learned. *IEEE Transactions on Emerging Topics in Computing* 4, 1 (2016), 35–46.

[7] Sumayah Alrwais, Xiaojing Liao, Xianghang Mi, Peng Wang, XiaoFeng Wang, Feng Qian, Raheem Beyah, and Damon McCoy. 2017. Under the Shadow of Sunshine : Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks. In *2017 IEEE Symposium on Security and Privacy,*. 805–823.

[8] Mashael Alsabah and Ian Goldberg. 2014. Performance and Security Improvements for Tor : A Survey. *Comput. Surveys* 49, 2 (2014), 1–38.

[9] Ross Anderson. 2001. Why information security is hard-an economic perspective. In *Proceedings 17th Annual Computer Security Applications Conference*. IEEE, 358–365.

[10] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2013. Measuring the Cost of Cybercrime Ross. In *The Economics of Information Security and Privacy*. 265–300.

[11] Ross Anderson and Tyler Moore. 2006. The economics of information security. *Science* 314, 5799 (2006), 610–613.

[12] Claudio A. Ardagna, Rasool Asal, Ernesto Damiani, and Quang Hieu Vu. 2015. From Security to Assurance in the Cloud: A Survey. *Comput. Surveys* 48, 1 (2015), 2:1–2:50.

[13] Thanassis Avgerinos, Sang Kil Cha, Brent Lim, Tze Hao, and David Brumley. 2011. AEG: Automatic Exploit Generation. In *18th Annual Network and Distributed System Security Symposium*, Vol. 14. 1–18.

[14] Matej Balog, Alexander L. Gaunt, Marc Brockschmidt, Sebastian Nowozin, and Daniel Tarlow. 2016. DeepCoder: Learning to Write Programs. *arXiv preprint arXiv:1611.01989* (2016), 19. http://arxiv.org/abs/1611.01989

[15] Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, and David Brumley. 2017. Your Exploit is Mine : Automatic Shellcode Transplant for Remote Exploits. In *2017 IEEE Symposium on Security and Privacy*. 824–839.

[16] Eli Blumenthal and Elizabeth Weise. 2016. Hacked home devices caused massive Internet outage. (2016). https://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/

[17] Danny Bradbury. 2014. Testing the defences of bulletproof hosting companies. *Network Security* 2014, 6 (2014), 8–12.

[18] Russell Brandom. 2017. An Anonymous group just took down a fifth of the dark web. (2017). https://www.theverge.com/2017/2/3/14497992/freedom-hosting-ii-hacked-anonymous-dark-web-tor

[19] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, and Steve Chon. 2014. Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology* 8, 1 (2014), 1–20.

[20] David Brumley, Pongsin Poosankam, Dawn Song, and Jiang Zheng. 2008. Automatic patch-based exploit generation is possible: Techniques and implications. In *IEEE Symposium on Security and Privacy*. 143–157.

[21] Danton Bryans. 2014. *Bitcoin and money laundering: Mining for an effective solution*. Vol. 89. 441–472 pages.

[22] Juan Caballero, Chris Grier, Christian Kreibich, Vern Paxson, and U C Berkeley. 2011. Measuring Pay-per-Install : The Commoditization of Malware Distribution. In *USENIX Security Symposium*. 13:1–13:16.

[23] Vince D. Calhoun and Tülay Adali. 2009. Feature-based fusion of medical imaging data. *IEEE Transactions on Information Technology in Biomedicine* 13, 5 (2009), 711–720.

[24] Alejandro Calleja, Juan Tapiador, and Juan Caballero. 2016. A look into 30 years of malware development from a software metrics perspective. In *International Symposium on Research in Attacks, Intrusions, and Defenses*, Vol. 9854 LNCS. 325–345.

[25] Davide Canali and Davide Balzarotti. 2013. Behind the scenes of online attacks: an analysis of exploitation behaviors on the web. In *20th Annual Network & Distributed System Security Symposium*. n–a.

[26] Onur Catakoglu, Marco Balduzzi, and Davide Balzarotti. 2016. Automatic Extraction of Indicators of Compromise for Web Applications. In *In Proceedings of the World Wide Web Conferernce*. 333–343.

[27] Onur Catakoglu, Marco Balduzzi, and Davide Balzarotti. 2017. Attacks Landscape in the Dark Side of the Web. In *ACM Symposium on Applied Computing*. 1739–1746.

[28] New Jersey Cybersecurity & Communications Integration Cell. 2016. Exploit Kit Variants: Neutrino. (2016). https://www.cyber.nj.gov/threat-profiles/exploit-kit-variants/neutrino

[29] Jian Chang, Krishna K. Venkatasubramanian, Andrew G. West, and Insup Lee. 2013. Analyzing and defending against web-based malware. *Comput. Surveys* 45, 4 (2013), 1–35.

[30] Chia Yuan Cho, Domagoj Babic, Pongsin Poosankam, Kevin Zhijie Chen, Edward XueJun Wu, and Dawn Song. 2011. MACE: model-inference-assisted concolic exploration for protocol and vulnerability discovery. In *USENIX Security Symposium*. 139–154.

[31] Kim Kwang Raymond Choo. 2011. The cyber threat landscape: Challenges and future research directions. *Computers and Security* 30, 8 (2011), 719–731. http://dx.doi.org/10.1016/j.cose.2011.08.004

[32] Nazli Choucri, Stuart Madnick, and Priscilla Koepke. 2016. Institutions for Cyber Security: International Responses and Data Sharing Initiatives. (2016), 34 pages.

[33] Nicolas Christin. 2013. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In *Proceedings of the 22nd international conference on World Wide Web*. 213–224.

[34] Cuong Xuan Chu, Niket Tandon, and Gerhard Weikum. 2017. Distilling Task Knowledge from How-To Communities.. In *World Wide Web Conference*. 805–814. http://dblp.uni-trier.de/db/conf/www/www2017.html

[35] Cisco. 2016. *Cisco 2016 Annual Security Report*. Technical Report. 1–87 pages. http://www.cisco.com/c/dam/assets/offers/pdfs/cisco-asr-2016.pdf

[36] David D Clark. 2012. Control point analysis. In *TRPC Conference*. 25. http://papers.ssrn.com/sol3/papers.cfm?abstract

[37] Bernd Conrad and Fatemeh Shirazi. 2014. A Survey on Tor and I2P. In *Proceedings of the 9th International Conference on Internet Monitoring and Protection*. 22–28.

[38] Contagio. 2015. An Overview of Exploit Packs (Update 25) May 2015. (2015). http://contagiodump.blogspot.com/2010/06/overview-of-exploit-packs-update.html

[39] CSIMarket. 2017. CSIMarket Return on Investment Screening. (2017). https://csimarket.com/screening/index.php?s=roi

[40] Exploit Database. 2017. The Exploit Database. (2017). https://www.exploit-db.com/

[41] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. Tor: The second-generation onion router. (2004), 17 pages.

[42] Thomas Donilon, Chair Samuel Palmisano, Keith Alexander, Ana Antón, Ajay Banga, Steven Chabinsky, Patrick Gallagher, Peter Lee, Herbert Lin, Heather Murren, Joseph Sullivan, Maggie Wilderotter, and Kiersten Todt. 2016. *Commission on Enhancing National Cybersecurity*. Technical Report. 1–100 pages. https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

[43] Charles Doyle. 2012. Cybercrime: An Overview of the Ferderal Computer Fraud and Abuse Statue and Related Federal Criminal Laws. *Journal of Current Issues in Crime, Law & Law Enforcement* 5, 1/2 (2012), 69–162.

[44] Benoit Dupont, Anne-Marie Cote, Claire Savine, and David Decary-Hetu. 2016. The ecology of trust among hackers. *Global Crime* 17, 2 (2016), 129–151.

[45] E-ISAC and SANS. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Technical Report. 23 pages. https://ics.sans.org/media/E-ISAC

[46] Manuel Egele, Theodoor Scholte, Engin Kirda, and Christopher Kruegel. 2012. A survey on automated dynamic malware-analysis techniques and tools. *Comput. Surveys* 44, 2 (2012), 1–42. http://dl.acm.org/citation.cfm?doid=2089125.2089126

[47] Jose Esteves, Elisabete Ramalho, and Guillermo de Haro. 2017. To Improve Cybersecurity, Think Like a Hacker. *MIT Sloan Management Review* 58, 3 (2017), 71–77.

[48] Adrienne Porter Felt and David Wagner. 2011. Phishing on mobile devices. In *Web 2.0 Security and Privacy*, Vol. 2. 1–10.

[49] Kristin M Finklea and Catherine A Theohary. 2015. *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. Technical Report. 1–27 pages.

[50] Thomas Fox-Brewster. 2016. Android Gooligan Hackers Just Scored The Biggest Ever Theft Of Google Accounts. (2016). https://www.forbes.com/sites/thomasbrewster/2016/11/30/gooligan-android-malware-1m-google-account-breaches-check-point-finds

[51] Thomas Fox-Brewster. 2017. Forget Silk Road, Cops Just Scored Their Biggest Victory Against The Dark Web Drug Trade. (2017). https://www.forbes.com/sites/thomasbrewster/2017/07/20/alphabay-hansa-dark-web-markets-taken-down-in-massive-drug-bust-operation

[52] Anonymous France. 2016. Anonymity and Privacy first lesson taught on OnionIRC. (2016). https://www.anonymous-france.eu/anonymity-and-privacy-first-lesson-taught-on-onionirc.html

[53] Jerry Gao, Xiaoying Bai, Wei-Tek Tsai, and Tadahiro Uehara. 2014. Mobile Application Testing: A Tutorial. *Computer* 47, 2 (2014), 46–55. http://ieeexplore.ieee.org/document/6693676/

[54] Glen Gibb, Hongyi Zeng, and Nick McKeown. 2012. Outsourcing network functionality. In *ACM HotSDN 2012*. 73. http://dl.acm.org/citation.cfm?doid=2342441.2342457

[55] Misha Glenny. 2011. *DarkMarket: Cyberthieves, Cybercops and You*. 283 pages. http://books.google.nl/books?id=uxAcuzbyw9YC

[56] Max Goncharov. 2012. *Russian Underground 101*. Technical Report. Trend Micro. 1–29 pages. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

[57] Google. 2015. Vulnerability Research Grant Rules. (2015). https://www.google.com/about/appsecurity/research-grants/

[58] Diana Granger. 2017. Fatboy Ransomware-as-a-Service Emerges on Russian-Language Forum. (2017). https://www.recordedfuture.com/fatboy-ransomware-analysis/

[59] Mariano Graziano, Davide Canali, Leyla Bilge, Andrea Lanzi, and Davide Balzarotti. 2015. Needles in a Haystack: Mining Information from Public Dynamic Analysis Sandboxes for Malware Intelligence. In *24th USENIX Security Symposium*. 1057–1072.

[60] ANDY GREENBERG. 2016. Hackers Claim to Auction Data They Stole From NSA-Linked Spies. (2016). https://www.wired.com/2016/08/hackers-claim-auction-data-stolen-nsa-linked-spies/

[61] Gustavo Grieco, Guillermo Luis Grinblat, Lucas Uzal, Sanjay Rawat, Josselin Feist, and Laurent Mounier. 2016. Toward large-scale vulnerability discovery using Machine Learning. In *Proceedings of the ACM Conference on Data and Application Security and Privacy*. 85–96.

[62] Felix Gröbert, Ahmad-Reza Sadeghi, and Marcel Winandy. 2009. Software distribution as a malware infection vector. In *2009 International Conference for Internet Technology and Secured Transactions*. 1–6.

[63] Chen Hajaj, Noam Hazon, and David Sarne. 2017. Enhancing comparison shopping agents through ordering and gradual information disclosure. *Autonomous Agents and Multi-Agent Systems* 31, 3 (2017), 696–714.

[64] Ashley Harris. 2016. *Cyber Ethics: An assessment of government and private industry*. Ph.D. Dissertation. Utica College.

[65] Andreas Haslebacher, Jeremiah Onaolapo, and Gianluca Stringhini. 2016. All Your Cards Are Belong To Us: Understanding Online Carding Forums. *CoRR abs/1607.00117* 1 (2016). http://arxiv.org/abs/1607.00117

[66] Ryan Heartfield and George Loukas. 2015. A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *Comput. Surveys* 48, 3 (2015), 1–39.

[67] Cormac Herley and Dinei Florêncio. 2010. Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy. In *Economics of Information Security and Privacy*. 33–53.

[68] Alex Hern. 2015. Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim. (2015). https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim

[69] Thomas J. Holt. 2017. Identifying gaps in the research literature on illicit markets on-line. *Global Crime* 18, 1 (2017), 1–10. https://www.tandfonline.com/doi/full/10.1080/17440572.2016.1235821

[70] Thomas J Holt, Deborah Strumsky, Olga Smirnova, and Max Kilger. 2012. Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology* 6, 1 (2012), 891–903.

[71] Thorsten Holz, Christian Gorecki, Konrad Rieck, and Felix C Freiling. 2008. Measuring and Detecting Fast-Flux Service Networks. In *Ndss*. 24 – 31.

[72] Jason Hong. 2012. The Current State of Phishing Attacks. *Commun. ACM* 55, 1 (2012), 74–81.

[73] Danny Yuxing Huang, Doug Grundman, Kurt Thomas, Abhishek Kumar, Elie Bursztein, Kirill Levchenko, and Alex C Snoeren. 2017. Pinning Down Abuse on Google Maps. In *26th International World Wide Web Conference*. 1471–1479.

[74] Keman Huang, Jinjing Han, Shizhan Chen, and Zhiyong Feng. 2016. A Skewness-Based Framework for Mobile App Permission Recommendation and Risk Evaluation. In *14th International Conference on Service-Oriented Computing*. 252–266.

[75] Keman Huang, Michael Siegel, Stuart Madnick, Xiaohong Li, and Zhiyong Feng. 2016. Diversity or Concentration ? Hackers' Strategy for Working Across Multiple Bug Bounty Programs. In *IEEE Symposium on Security and Privacy*. 2.

[76] Keman Huang, Jia Zhang, Wei Tan, and Zhiyong Feng. 2017. Shifting to Mobile: Network-based Empirical Study of Mobile Vulnerability Market. *IEEE Transactions on Services Computing* pp, 99 (2017), 1–14.

[77] M. O'Reirdan J. Livingood, N. Mody. 2011. Recommendations for the Remediation of Bots in ISP Networks draft-oreirdan-mody-bot-remediation-16. *Internet Engineering Task Force* c (2011), 1–33.

[78] Mohammad Hanif Jhaveri, Orcun Cetin, Carlos Gañán, Tyler Moore, and Michel Van Eeten. 2017. Abuse Reporting and the Fight Against Cybercrime. *Comput. Surveys* 49, 4 (2017), 1–27.

[79] Karthik Kannan, Mohammad S. Rahman, and Mohit Tawarmalani. 2016. Economic and Policy Implications of Restricted Patch Distribution. *Management Science* 62, 11 (2016), 3161–3182.

[80] Mohammad Karami, Youngsam Park, and Damon McCoy. 2016. Stress testing the Booters: Understanding and undermining the business of DDoS services. In *Proceedings of the 25th International Conference on World Wide Web*. 1033–1043.

[81] Limor Kessem. 2015. The Return of Ramnit: Life After a Law Enforcement Takedown. (2015). https://securityintelligence.com/the-return-of-ramnit-life-after-a-law-enforcement-takedown/

[82] Swati Khandelwal. 2017. Shadow Brokers, Who Leaked WannaCry SMB Exploit, Are Back With More 0-Days. (2017). http://thehackernews.com/2017/05/shodow-brokers-wannacry-hacking.html

[83] Maria Konte and Nick Feamster. 2015. ASwatch : An AS Reputation System to Expose Bulletproof Hosting ASes. In *Sigcomm 2015*. 625–638.

[84] Brian Krebs. 2016. Money Mule Gangs Turn to Bitcoin ATMs. (2016). https://krebsonsecurity.com/2016/09/money-mule-gangs-turn-to-bitcoin-atms/

[85] Nir Kshetri. 2006. The simple economics of cybercrimes. *IEEE Security and Privacy* 4, 1 (2006), 33–39.

[86] Dana Lahat, Tulay Adali, and Christian Jutten. 2015. Multimodal Data Fusion: An Overview of Methods, Challenges, and Prospects. *Proc. IEEE* 103, 9 (2015), 1449–1477.

[87] Aron Laszka, Mark Felegyhazi, and Levente Buttyan. 2014. A Survey of Interdependent Information Security Games. *ACM Computing Surveys (CSUR)* 47, 2 (2014), 1–38.

[88] Stefan Laube and Rainer Böhme. 2017. Strategic Aspects of Cyber Risk Information Sharing. *Comput. Surveys* Forthcomin (2017).

[89] Angel Lagares Lemos, Florian Daniel, and Boualem Benatallah. 2015. Web Service Composition: A Survey of Techniques and Tools. *Comput. Surveys* 48, 3 (2015), 1–41.

[90] E. R. Leukfeldt. 2014. Cybercrime and social ties: Phishing in Amsterdam. *Trends in Organized Crime* 17, 4 (2014), 231–249.

[91] Rutger Leukfeldt. 2015. Organised Cybercrime and Social Opportunity Structures: A Proposal for Future Research Directions. *The European Review of Organised Crime* 2, 2 (2015), 91–103.

[92] Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Mark FelegyhaziGrier, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage. 2011. Click trajectories: End-to-end analysis of the spam value chain. In *Proceedings - IEEE Symposium on Security and Privacy*. 431–446.

[93] Nancy G. Leveson. 2011. *Engineering a Safer World: Systems Thinking Applied to Safety*. 555 pages. http://medcontent.metapress.com/index/A65RM03P4874243N.pdf

[94] Weifeng Li, Hsinchun Chen, and Jay F Nunamaker Jr. 2017. Identifying and Profiling Key Sellers in Cyber Carding Community : AZSecure Text Mining System. *Journal of Management Information Systems* 33, 4 (2017), 1059–1086.

[95] Xiaojing Liao, Damon Mccoy, and Elaine Shi. 2016. Characterizing Long-tail SEO Spam on Cloud Web Hosting Services. In *Proceedings of the World Wide Web Conference*. 321–332.

[96] Vincent Loy, Kyra Mattar, Tan Shong Ye, Bahgya Perera, Jimmy Sng, and Maggie Leong. 2015. *Reclaiming cybersecurity: The Global State of Information Security Survey 2016*. Technical Report. PwC. 1–8 pages.

[97] Yong Lu, Xin Luo, Michael Polgar, and Yuanyuan Cao. 2010. Social Network Analysis of a Criminal Hacker Community. *The Journal of Computer Information Systems* 51, 2 (2010), 31.

[98] Robert Luh, Stefan Marschalek, Manfred Kaiser, Helge Janicke, and Sebastian Schrittwieser. 2017. Semantics-aware detection of targeted attacks: a survey. *Journal of Computer Virology and Hacking Techniques* 13, 1 (2017), 47–85.

[99] Stuart Madnick. 2016. Dark Web : hackers trump good guys in sharing information. (2016), 2 pages.

[100] Stuart Madnick. 2017. Preparing for the Cyberattack That Will Knock Out U.S. Power Grids. *Harvard Business Review* (2017), 5.

[101] Stuart Madnick. 2017. What Executives Get Wrong About Cybersecurity. *Sloan Management Review* January (2017), 22–24.

[102] Stuart Madnick, Mohammad S Jalali, Michael Siegel, Vicki Deng, and Dinsha Mistree. 2017. Measuring Stakeholders ' Perceptions of Cybersecurity for Renewable Energy Systems. In *Data Analytics for Renewable Energy Integration*. 67–77.

[103] Thomas Maillart, Mingyi Zhao, Jens Grossklags, and John Chuang. 2016. Given Enough Eyeballs , All Bugs Are Shallow? Revisiting Eric Raymond with Bug Bounty Programs. In *Workshop on the Economics of Information Security (WEIS)*. 1–19.

[104] Derek Manky. 2013. Cybercrime as a service: A very modern business. *Computer Fraud and Security* 6 (2013), 9–13.

[105] Steve Mansfield-Devine. 2016. The imitation game: how business email compromise scams are robbing organisations. *Computer Fraud and Security* 11 (2016), 5–10.

[106] Max Goncharov. 2015. *Criminal Hideouts for Lease: Bulletproof Hosting Services*. Technical Report. Trend Micro. 28 pages.

[107] Inc. McAfee. 2016. *McAfee Labs 2017 Threats Predictions*. Technical Report November 2016. 1–51 pages. http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2014.pdf

[108] Michael McCaul. 2017. The War in Cyberspace: Why We Are Losing–and How to Fight Back. (2017). https://www.rsaconference.com/videos/the-war-in-cyberspace-why-we-are-losing-and-how-to-fight-back

[109] Damon Mccoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. 2008. Shining Light in Dark Places : Understanding the Tor Network. In *International Symposium on Privacy Enhancing Technologies Symposium*. 63–76.

[110] Michael McGuire. 2012. *Organised Crime in the Digital Age*. Technical Report September.

[111] William Melicher, Blase Ur, Sean M Segreti, Saranga Komanduri, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks. In *Usenix Security*. 239.

[112] Max Metzger. 2016. Snapchat got whaled, employee payroll released. (2016). https://www.scmagazineuk.com/snapchat-got-whaled-employee-payroll-released/article/530493/

[113] Tyler Moore. 2010. Introducing the Economics of Cybersecurity: Principles and Policy Options. In *Workshop on Deterring Cyberattacks: Informing Strategis and DEveloping Options for US Policy*. 3–23.

[114] Tyler Moore and Richard Clayton. 2009. The Impact of Incentives on Notice and Take-down. In *Managing Information Risk and the Economics of Security*. 199–223. http://dx.doi.org/10.1007/978-0-387-09762-6

[115] Steve Morgan. 2016. *Hackerpocalypse : A Cybercrime Revelation*. Technical Report. Cybersecurity Ventures. 1–24 pages.

[116] Robert S. Mueller III. 2012. Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies. (2012). https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

[117] Satoshi Nakamoto. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Technical Report. 9 pages. https://bitcoin.org/bitcoin.pdf

[118] Marcin Nawrocki, Matthias Wählisch, Thomas C. Schmidt, Christian Keil, and Jochen Schönfelder. 2016. A Survey on Honeypot Software and Data Analysis. *eprint arXiv:1608.06249* (2016), 1–38.

[119] Arash Nourian and Stuart Madnick. 2015. A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet. *IEEE Transactions on Dependable and Secure Computing* PP, 99 (2015), 20.

[120] NTTSecurity. 2016. *SERT Quarterly Threat Report Q2 2016*. Technical Report.

[121] G. Odinot, M.A. Verhoeven, R.L.D. Pool, and C.J. de Poot. 2017. *Organised Cybercrime in the Netherlands*. Technical Report. 1–87 pages. https://english.wodc.nl/binaries/Cahier2017-1

[122] Philip O'Kane, Sakir Sezer, and Kieran McLaughlin. 2011. Obfuscation: The Hidden Malware. *IEEE Security & Privacy* 9, 5 (2011), 41–47.

[123] Jeremiah Onaolapo, Enrico Mariconti, and Gianluca Stringhini. 2016. What Happens After You Are Pwnd : Understanding The Use Of Leaked Account Credentials In The Wild. In *Proceedings of the ACM SIGCOMM Conference on Internet Measurement Conference*. 1–15.

[124] Hilarie Orman. 2013. The compleat story of phish. *IEEE Internet Computing* 17, 1 (2013), 87–91.

[125] Andy Ozment. 2004. Bug auctions: Vulnerability markets reconsidered. In *Workshop on Economics of Information Security (WEIS)*. 1–23.

[126] Pierluigi Paganini. 2016. Ran$umBin a dark web service dedicated to ransomware. (2016). http://securityaffairs.co/wordpress/46770/breaking-news/46770.html

[127] N Pavkovic and L Perkov. 2011. Social Engineering Toolkit - A systematic approach to social engineering. In *Proceedings of the 34th International Convention on Information and Communication Technology, Electronics and Microelectronics*.

1485–1489.

[128] Jeroen Pijpker and Harald Vranken. 2016. The Role of Internet Service Providers in Botnet Mitigation. In *2016 European Intelligence and Security Informatics Conference*. 24–31. https://doi.org/10.1109/EISIC.2016.013

[129] Michael Porter. 1985. *Competitive advantage: creating and sustaining superior performance*. The Free Press. 580 pages.

[130] Rebecca S Portnoff, Sadia Afroz, U C Berkeley, Greg Durrett, Jonathan K Kummerfeld, Taylor Berg-kirkpatrick, Damon Mccoy, and Vern Paxson. 2017. Tools for Automated Analysis of Cybercriminal Markets. In *World Wide Web Conference*. 657–666.

[131] PwC. 2016. *Global Economic Crime Survey 2016: Adjusting the Lens on Economic Crime*. Technical Report. PwC. 1–31 pages.

[132] Bradley Reaves, Jasmine Bowers, Sigmund Albert, Gorski Iii, North Carolina, Olabode Anise, Rahul Bobhate, Raymond Cho, Hiranava Das, Sharique Hussain, Hamza Karachiwala, Nolen Scaife, Byron Wright, Kevin Butler, and Patrick Traynor. 2016. * droid : Assessment and Evaluation of Android Application Analysis Tools. *Comput. Surveys* 49, 3 (2016), 1–30.

[133] Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin R.B. Butler. 2016. Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. In *2016 IEEE Symposium on Security and Privacy*. 339–356.

[134] Scott Reed and Nando de Freitas. 2016. Neural Programmer-Interpreters. In *ICLR*. 1–13. arXiv:1511.06279 http://arxiv.org/abs/1511.06279

[135] Rick Holland. 2016. the hacker talent shortage: what organizations can learn from the recruitment efforts of their attackers. (2016). https://www.digitalshadows.com/blog-and-research/the-hacker-talent-shortage-what-organizations-can-learn-from-the-recruitment-efforts-of-their-attackers/

[136] Rafael a. Rodríguez-Gómez, Gabriel Maciá-Fernández, and Pedro García-Teodoro. 2013. Survey and taxonomy of botnet research through life-cycle. *Comput. Surveys* 45, 4 (2013), 1–33.

[137] Charles H. Romine. 2017. Bolstering Government Cybersecurity Lessons Learned from WannaCry. (2017). https://www.nist.gov/speech-testimony/bolstering-government-cybersecurity-lessons-learned-wannacry

[138] Christian Rossow. 2013. *Using Malware Analysis to Evaluate Botnet Resilience*. Ph.D. Dissertation. Vrije Universiteit.

[139] RSA Whitepaper. 2016. *2016: Current State of Cybercrime*. Technical Report. RSA. 1–7 pages.

[140] Hamid Salim and Stuart Madnick. 2016. Cyber Safety : A Systems Theory Approach to Managing Cyber Security Risks-Applied to TJX Cyber Attack. (2016), 17 pages.

[141] Hamid M Salim. 2014. *Cyber safety : a systems thinking and systems theory approach to managing cyber security risks*. Ph.D. Dissertation. Massachusetts Institute of Technology.

[142] Raj Samani and Francois Paget. 2013. *Cybercrime Exposed: Cybercrime-as-a-Service*. Technical Report. McAfee. 1–18 pages. http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf

[143] Bruce Schneier. 2000. Inside Risks: Semantic Network Attacks. *Commun. ACM* 43, 12 (2000), 168.

[144] Bruce Schneier. 2015. *Secrets and Lies: Digital Security in a Networked World*. Wiley. 418 pages.

[145] Sebastian Schrittwieser, Johannes Kinder, Georg Merzdovnik, Edgar Weippl, and Stefan Katzenbeisser. 2015. Protecting Software through Obfuscation: Can It Keep Pace with Progress in Code Analysis? *Comput. Surveys* 49, 4 (2015), 1–40.

[146] Ej Schwartz, Thanassis Avgerinos, and David Brumley. 2011. Q: Exploit hardening made easy. In *USENIX Security '11*, Vol. 8. 25.

[147] Offensive Security. 2017. Offensive Security Training, Certifications and Services. (2017). https://www.offensive-security.com/

[148] Securityfocus. 2012. Payload Definition. (2012). http://www.securityfocus.com/glossary/P

[149] Dave Shackleford. 2015. *Combatting Cyber Risks in the Supply Chain*. Technical Report. 20 pages. https://www.google.co.uk/url?sa=t

[150] Muhammad Shahzad, Muhammad Zubair Shafiq, and Alex X Liu. 2012. A large scale exploratory analysis of software vulnerability life cycles. In *Proceedings of the 34th International Conference on Software Engineering*. 771–781.

[151] Wanita Sherchan, Surya Nepal, and Cecile Paris. 2013. A Survey of Trust in Social Networks. *Comput. Surveys* 45, 4 (2013), 47–47:33.

[152] Sergei Shevchenko. 2016. TWO BYTES TO $951M. (2016). http://baesystemsai.blogspot.com/2016/04/ two-bytes-to-951m.html

[153] Yan Shoshitaishvili, Ruoyu Wang, Christopher Salls, Nick Stephens, Mario Polino, Andrew Dutcher, John Grosen, Siji Feng, Christophe Hauser, Christopher Kruegel, and Giovanni Vigna. 2016. SOK: (State of) the Art of War: Offensive Techniques in Binary Analysis. In *IEEE Symposium on Security and Privacy*. 138–157.

[154] Johan Sigholm. 2013. Non-State Actors in Cyberspace Operations. *Journal of Military Studies* 4, 1 (2013), 1–37.

[155] Aditya K. Sood and Richard J. Enbody. 2013. Crimeware-as-a-service-A survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection* 6, 1 (2013), 28–38.

[156] Aditya K. Sood and Richard J. Enbody. 2013. Targeted cyberattacks: A superset of advanced persistent threats. *IEEE Security and Privacy* 11, 1 (2013), 54–61.

[157] Kyle Soska, Nicolas Christin, Kyle Soska, and Nicolas Christin. 2015. Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. In *the 24th USENIX Security Symposium*. 33–48.

[158] Melvin R J Soudijn and Birgit C H T Zegers. 2012. Cybercrime and virtual offender convergence settings. *Trends in Organized Crime* 15, 2-3 (2012), 111–129.

[159] Richard Spinello. 2016. *Cyberethics: Morality and Law in Cyberspace* (sixth edit ed.). Jones & Bartlett Learning. 239 pages.

[160] Oleksii Starov, Johannes Dahse, Syed Sharique Ahmad, Thorsten Holz, and Nick Nikiforakis. 2016. No Honor Among Thieves: A Large-Scale Analysis of Malicious Web Shells. In *In Proceedings of the World Wide Web Conferernce*. 1021–1032.

[161] William J. Stevenson. 2012. *Operations management* (11th editi ed.). Tim Vertovec. 908 pages.

[162] Brett Stone-gross, Ryan Abman, Richard a Kemmerer, Christopher Kruegel, Douglas G Steigerwald, and Giovanni Vigna. 2013. The Underground Economy of Fake Antivirus Software. In *Economics of Information Security and Privacy III*. 55–78. http://www.springerlink.com/index/10.1007/978-1-4614-1981-5

[163] Gianluca Stringhini, Oliver Hohlfeld, Christopher Kruegel, and Giovanni Vigna. 2014. The harvester, the botmaster, and the spammer: on the relations between the different actors in the spam landscape. In *Proceedings of the 9th ACM symposium on Information, computer and communications security*. 353–364.

[164] Guillermo Suarez-Tangil, Juan E. Tapiador, Pedro Peris-Lopez, and Jorge Blasco. 2014. Dendroid: A text mining approach to analyzing and classifying code structures in Android malware families. *Expert Systems with Applications* 41, 4 PART 1 (2014), 1104–1117.

[165] Sufatrio, Darell J J Tan, Tong-wei Chua, and Vrizlynn L. L. Thing. 2015. Securing Android : A Survey , Taxonomy , and Challenges. *Comput. Surveys* 47, 4 (2015), 1–45.

[166] Kimberly Tam, A L I Feizollah, N O R Badrul Anuar, Rosli Salleh, and Lorenzo Cavallaro. 2017. The Evolution of Android Malware and Android Analysis Techniques. *Comput. Surveys* 49, 4 (2017), 1–41.

[167] Digital Shadows Analyst Team. 2017. Innovation in the underworld: Reducing the Risk of Ripper Fraud. (2017). https://www.digitalshadows.com/blog-and-research/innovation-in-the-underworld-reducing-the-risk-of-ripper-fraud

[168] Vrizlynn L.L. Thing, Henry C.J. Lee, and Morris Sloman. 2005. Traffic redirection attack protection system (TRAPS). In *IFIP Advances in Information and Communication Technology*, Vol. 181. 309–325.

[169] Kurt Thomas, Juan Antonio Elices Crespo, Ryan Rasti, Jean-Michel Picod, Damon Mccoy, Lucas Ballard, Elie Bursztein, Moheeb Abu Rajab, and Niels Provos. 2016. Investigating Commercial Pay-Per-Install and the Distribution of Unwanted Software. In *25th USENIX Security Symposium*. 721–738.

[170] Kurt Thomas, Chris Grier, Justin Ma, Vern Paxson, and Dawn Song. 2011. Design and evaluation of a real-time URL spam filtering service. In *Proceedings - IEEE Symposium on Security and Privacy*. 447–462.

[171] Kurt Thomas, Danny Huang, David Wang, Elie Bursztein, Chris Grier, Thomas J Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, and Giovanni Vigna. 2015. Framing Dependencies Introduced by Underground Commoditization. In *Workshop on the Economics of Information Security*. 1–24.

[172] Kevin Townsend. 2017. Latest WannaCry Theory: Currency Manipulation. (2017). http://www.securityweek.com/latest-wannacry-theory-currency-manipulation

[173] Amit Kumar Tyagi and G Aghila. 2011. A Wide Scale Survey on Botnet. *International Journal of Computer Applications* 34, 9 (2011), 975–8887.

[174] Sun Tzu. 2005. *The art of war*. Shambhala Publications.

[175] Michel van Eeten, Johannes M. Bauer, Hadi Asghari, and Shirin Tabatabaie. 2010. The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data. (2010), 67 pages.

[176] Verizon. 2017. *2017 Data Breach Investigations Report*. Technical Report. 76 pages.

[177] Timothy Vidas and Nicolas Christin. 2013. Sweetening Android Lemon Markets: Measuring and Combating Malware in Application Marketplaces. In *3rd ACM conference on Data and Application Security and Privac*, Vol. 2011. 197–207.

[178] John Wadleigh, Jake Drew, and Tyler Moore. 2015. The E-Commerce Market for âĂIJ Lemons âĂİ: Identification and Analysis of Websites Selling Counterfeit Goods. In *Proceedings of the 24th International Conference on World Wide Web*. 1188–1197.

[179] Wikileaks. 2017. Vault 7: CIA Hacking Tools Revealed. (2017). https://wikileaks.org/ciav7p1/

[180] Trenton A Williams, Daniel A Gruber, Kathleen M Sutcliffe, Dean A Shepherd, and Eric Yanfei Zhao. 2017. Organizational Response To Adversity: Fusing Crisis Management and Resilience Research Streams. *Academy of Management Annals* March (2017), 1–70.

[181] Eric Wustrow and Benjamin VanderSloot. 2016. DDoSCoin: Cryptocurrency with a Malicious Proof-of-Work. In *USENIX Workshop on Offensive Technologies*.

[182] Haitao Xu, Daiping Liu, Haining Wang, and Angelos Stavrou. 2015. E-commerce Reputation Manipulation: The Emergence of Reputation-Escalation-as-a-Service. In *Proceedings of the 24th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 1296–1306.

[183] Michael Yip, Nigel Shadbolt, and Craig Webber. 2013. Why forums?: an empirical analysis into the facilitating factors of carding forums. In *Proceedings of the 5th Annual ACM Web Science*. 453–462.

[184] Kim Zetter. 2014. A Google Site Meant to Protect You Is Helping Hackers Attack You. (2014). https://www.wired.com/2014/09/how-hackers-use-virustotal/

[185] Mingyi Zhao, Jens Grossklags, and Peng Liu. 2015. An Empirical Study of Web Vulnerability Discovery Ecosystems. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 1105–1117.

[186] Ziming Zhao, Mukund Sankaran, Gail Joon Ahn, Thomas J. Holt, Yiming Jing, and Hongxin Hu. 2016. Mules, Seals, and Attacking Tools: Analyzing 12 Online Marketplaces. *IEEE Security and Privacy* 14, 3 (2016), 32–43.

A NOTATION FOR THE CYBERATTACK TARGET SELECTION RULE

For a rational cyber-attacker, the victim organization could be considered as a target if and only if the expected benefit B_e outweighs the expected cost C_e.

$$B_e = (P_e \times (B_{pm} + B_{pp}) \times E_r) > C_e = (C_{ps} + (P_a \times P_c \times C_c) + (C_{im} + C_{om})) \tag{29}$$

We summarize the notations as following:

- P_e : Ease of the attack, represents how easy to do the cyber attack;
- B_{pm}: Monetary benefit from the successful cyber attack against the target;
- B_{pp}: Psychological benefit from the successful cyber attack against the target;
- B_p: Potential benefit from the successful cyber attack; $B_p = B_{pm} + B_{pp}$
- E_r: Ease of benefit realization, represents how easy for the attacker to realize the benefit, including both monetary and psychological benefit, from the successful attack;
- C_{ps} : Psychological Costs for the attacker to do the cyber attack;
- P_a: Arrest rate, represents the attacker being identified and arrested for doing the cyber attack;
- P_c: Ease of the judicial process involved in the conviction;
- C_c: The opportunity cost if the attacker is convicted;
- C_p: The expected penalty costs $C_p = P_a \times P_c \times C_c$;
- C_{im}: The investment cost for the attacker to do the cyber attack;
- C_{om}: The opportunity cost for the attacker to do the cyber attack;
- C_o: The operational cost $C_o = C_{im} + C_{om}$;

B GLOSSARY FOR CYBERCRIMINAL SERVICE ECOSYSTEM

Table 1. Cybercriminal Services

CaaS	*Cybercrime as a Service*
V DaaS	Vulnerability Discovery as a Service
VKaaS	*Exploitation Development Service*
EaaS	Exploit as a Service
EPaaS	Exploit Package as a Service
DaaS	Deception as a Service
PaaS	Payload as a Service
OBaaS	Obfuscate as a Service
SCaaS	Security Checker as a Service
RPaaS	Repackage as a Service
BNaaS	Botnet as a Service
TRaaS	Traffic Redirection as a Service
BHaaS	Bulletproof Hosting as a Service
TAaaS	Traffic as a Service
REaaS	Reputation Escalation as a Service
AaaS	Multi-step Attack Service
PPaaS	Personal Profile as a Service
DMaaS	Domain Knowledge as a Service
TPaaS	Tool Pool as a Service
TSaaS	Target Selection as a Service
MLaaS	Money Laundering as a Service
MRaaS	Money Mule Recruiting as a Service
RaaS	Reputation as a Service
V EaaS	Value Evaluation as a Service
MPaaS	Marketplace as a Service
HTaaS	Hacker Training as a Service
HRaaS	Hacker Recruiting as a Service

Table 2. Informations for the Cybercriminal Service Ecosystem

V	Vulnerability	V_p	Operational Vulnerability
V_t	Technical Vulnerability	T	Target
VEK	Verified Exploit Kit	E	Exploit
EK	Exploit Kit	FI	Fake Information
PL	Payload	SCS_R	Security Checker Report
BN	Botnet	Z	Zombie Machine
BH	Bulletproof Server	TA	Traffic
GD	Digital Gain	GP	Psychological Gain
GL	Monetized Forms of Benefit Directed from Attack	HR	Human Resource
DK	Domain Knowledge	PP	Personal Profile
I_p	Personal Information	I_d	Domain Specific Information
M_C	Legal Money	M_D	Illegal Money
MLN	Money Laundering Network	HZ	Manipulated/Tricked Human
RR	User Interaction Records	R	User Reputation
VI	Verified Information	PG	Good's Price
CH	Certificated Hacker with necessary skills	NH	Novice in the hacker community

Table 3. Tools for the Cybercriminal Service Ecosystem

VDT	Vulnerability Discovery Tool	OBT	Obfuscation Tool
$EKDT$	Exploit Development and Improvement Tool	EDT	Exploit Development Tool
EPT	Exploit Package Tool	FDT	Deception Development Tool
PDT	Payload Development Tool	SCT	Security Check Tool
RPT	Repackaging tool	$BNDT$	Botnet Development and Maintain Tool
TRT	Traffic Redirection Technique	BHT	Bulletproof Server Tool
TGT	Traffic Generate Tool	RS	Reputation Mechanism
MDF	Multi-modal Data Fusion Technology	TMS	Customization and Management Tool
TS	Training Support	VES	Value Verification Tool
MMT	Online Marketplace Development Tool	HRT	Hacker Recruiting Tool

C APPENDIX FIGURES

As shown in Figure 9, we map the services in the cybercriminal service ecosystem framework constructed in Section 3 into the value chain model presented in Section 2 and group the services into three different categories:

- *"No independent services observed yet"*: refers to the services which were not observed during our study but expected to emerge due to its specialization and existence of the similar innovations in legitimate businesses.
- *"New service forms"*: refers to the services which are available in the dark web but can evolve into a new business model because of the development of the technologies.
- *"Others"*: refers to the services whose business model is not expected to change significantly.

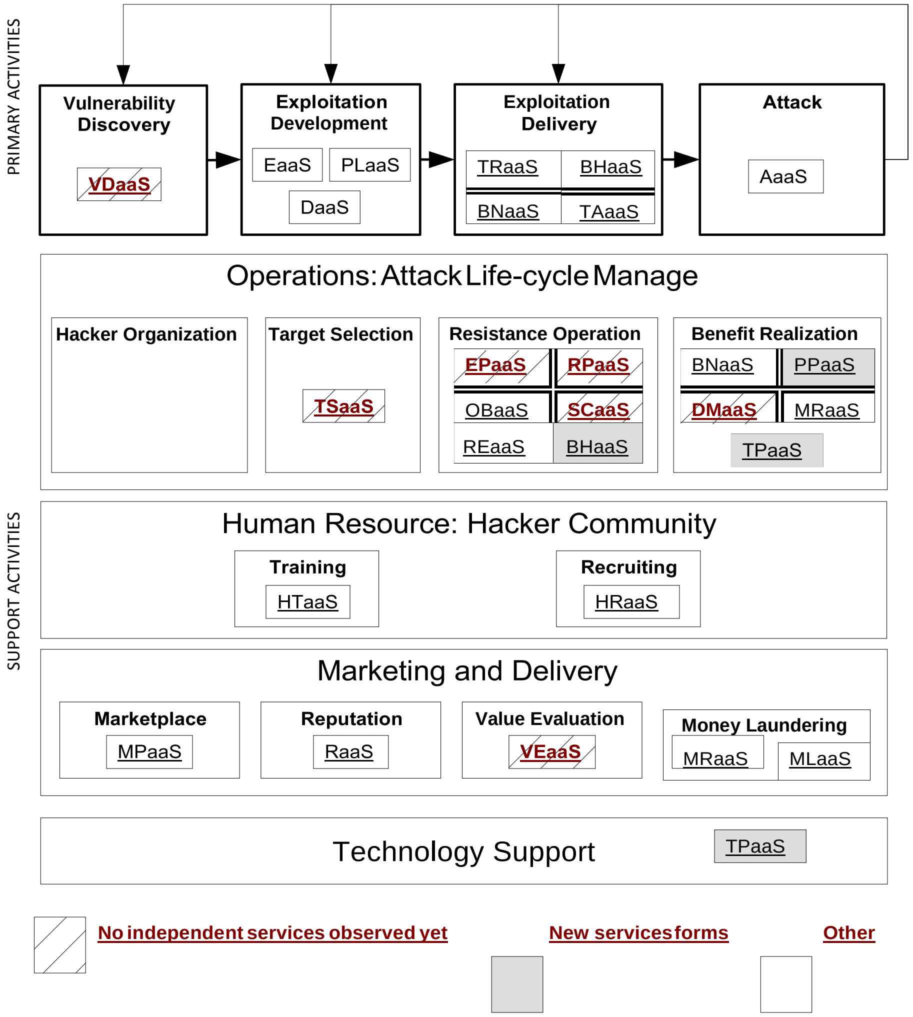
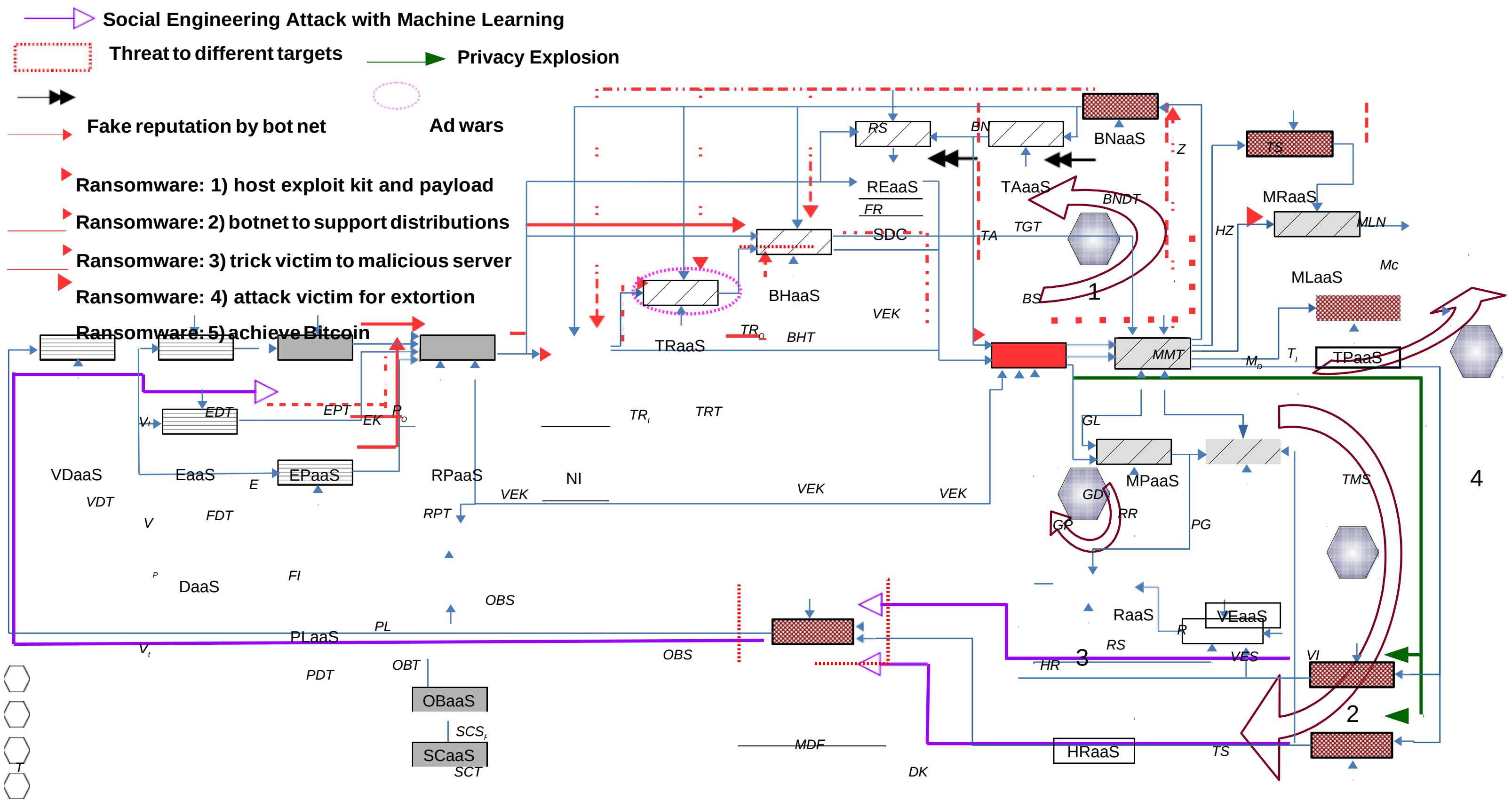


Fig. 9. Mapping between the ecosystem framework and the value chain model to understand the development of the cybercrime services.

Systematic


Social Engineering Attack with Machine Learning
Threat to different targets
Privacy Explosion
Fake reputation by bot net
Ad wars
Ransomware: 1) host exploit kit and payload
Ransomware: 2) botnet to support distributions
Ransomware: 3) trick victim to malicious server
Ransomware: 4) attack victim for extortion
Ransomware: 5) achieve Bitcoin
RS
BN
BNaaS
Z
TS
REaaS
FR
TAaaS
BNDT
MRaaS
SDC
TA
TGT
HZ
MLN
BHaaS
VEK
BS
1
MLaaS
Mc
TRaaS
TR_O
BHT
MMT
M_D
T_I
TPaaS
EDT
V_I
EPT
EK
P_O
TR_I
TRT
GL
VDaaS
EaaS
EPaaS
E
RPaaS
NI
VEK
VEK
VEK
GD
MPaaS
TMS
4
VDT
V
FDT
RPT
GP
RR
PG
P
DaaS
FI
OBS
RaaS
VEaaS
PLaaS
PL
R
RS
V_I
OBT
OBS
HR
3
VES
VI
PDT
OBaaS
2
SCS_I
SCaaS
MDF
SCT
HRaaS
TS
DK
T

TSaaS

PP

HRT CH HTaaS NH MDF

DK

DMaaS I_D

I_P

PPaaS

MDF

1 Loop 1: Compromised Machine reused for attack

2 Loop 2: Breach Information reused for attack

3 Loop 3: Hacking Experience reused for attack

4 Loop 4: Stolen Tools reused for attack

Fig. 10. Systematic Understanding of Cyber-threats. Using the predictions from the McAfee Labs 2017 Threats Prediction Report, we map the identified threats into the framework which forms two reinforcement loops including the reusage of the compromised machines and the breach information. Furthermore, based on the framework, we can also observe two other loops including the hacking experience and the stolen tools for further cyber attacks.

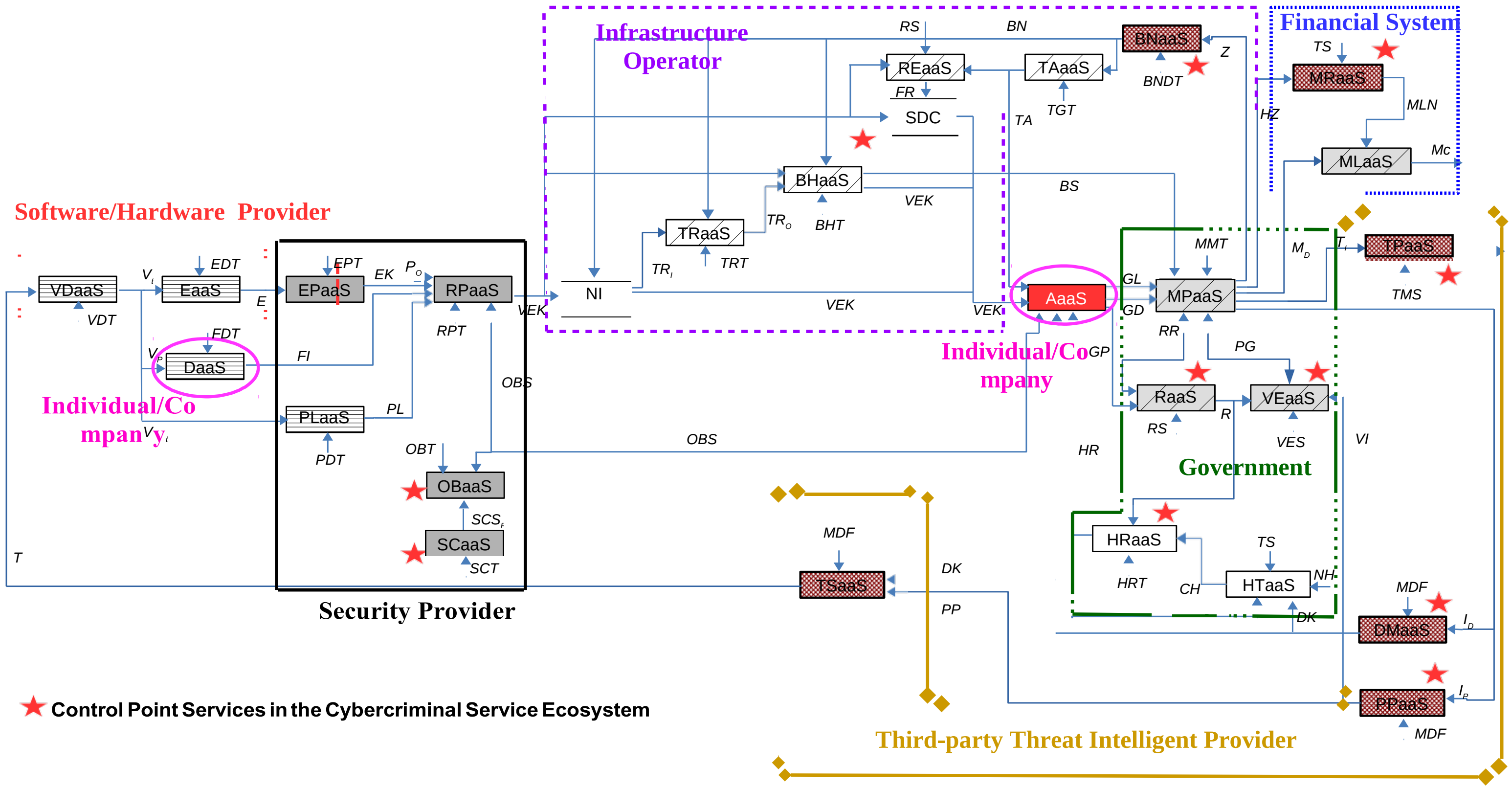


Fig. 11. Responsibility Allocations between the individual/Company, security provider, software/hardware provider, infrastructure operator, government, financial system and third party threat intelligent provider as well as the identified control-point services which can support the other services in the cybercriminal service ecosystem.