Systematically Understanding the Cyber Attack Business: A Survey

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

Cyber attacks are increasingly menacing businesses. Based on the literature review and publicly available reports, this paper conducts an extensive and consistent survey of the services used by the cybercrime business, organized using the value chain perspective, to understand cyber attack in systematic way. Understanding the specialization, commercialization, and cooperation for cyber attacks help us to identify twenty four (24) key value-added activities and their relations. These can be offered "as a service" for use in a cyber attack. This framework helps to understand the cybercriminal service ecosystem and hacking innovations. Finally, a few examples are provided showing how this framework can help to build a more cyber immune system, like targeting cybercrime control-points and assigning defense responsibilities to encourage collaboration.

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

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

ACM Reference format:
Keman Huang, Michael Siegel, and Stuart Madnick. 2018. Systematically Understanding the Cyber Attack Business: A Survey. 1, 1, Article 1 (March 2018), 35 pages.
https://doi.org/0000001.0000001

1 INTRODUCTION

"Where there is commerce, there is also the risk for cybercrime"[131].

Cybercrime is a tremendous threat to today's digital society. It is estimated that the cost of cybercrime will grow from an annual sum of $3 trillion in 2015 to $6 trillion by the year 2021 [109]. 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 [124]. It has become generally accepted that, "there are only two types of companies: those that have been hacked and those that will be"[110]. Fighting an impending cyber attack has become an important issue for companies in all industries and governments, especially those relying heavily on information technologies.

This work is partially supported by the National Natural Science Foundation of China under grant 61502333, and Cybersecurity at MIT Sloan (the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, 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 .

XXXX-XXXX/2018/3-ART1 $15.00
https://doi.org/0000001.0000001

Ever since the first reported cybercrime in 1973, when Union Dime Savings Bank account data was manipulated, cybercrime has been continually evolving[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 [81]. 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 [97, 134, 145]. 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."[165] To combat cybercrimes in an effective way, we not only need to develop technical solutions to protect against attacks, but also need to understand the structure of the business of underground cybercrime, and its development:

- **The Challenge in Understanding Cyber Attack Operations**

It has been said that "the good guys are getting better, but the bad guys are getting badder faster"[93]. Much of published research on cyber attacks has been focused on how attackers clandestinely intrude on private systems [3, 60, 66, 129, 157]. 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 not winning [in the cyberdefense battle]"[102]. 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 [16, 18, 59, 67, 70, 86, 87, 90, 117, 126, 129, 147, 154, 160, 174]. Based on these individual elements, Thomas et al. [162] 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"[41], with the defense trying to catch up with the offense with, up until this point, little success to show for its efforts.

- **The Challenge in Understanding the Cyber Attack Economy**

The underground cybercriminal has proven difficult to study. Researchers have used "honeypots" [112] to identify cybercriminals, and have collected information on the activities of cybercriminals [147]. These efforts to monitor the development of cyber attacks offer relevant counter intelligence. In considering the adoption of the "as-a-service" model [50, 131, 145, 162], researchers have compiled the services offered to buyers by the cybercrime industry. However, these services are widely scattered and inconsistently described. Without a clear framework through which to study the cybercrime service economy, it remains difficult to understand the modern cyber attack effectively.

- **The Need to Gather Information about these Diverse Services and Provide a Framework to Systematically Understand the Cyber Attack Business**

[1]There is still much debate about the definition of cybercrime and what constitutes a cyber attack. Since no single, agreed-upon definition exists, in this paper we will consider all cyber activities that are related to a "cyber attack", or that which undermines the function of the digital system belonging to the cybercriminal ecosystem. Note that not all activities included in our model are illegal. In fact, there are many discussions, which are outside the scope of this paper, about cyber ethics and the legality of such activity [58, 149].

[2]During 2015, the CryptoWall ransomware virus raised more than $325 million for the hacking group. Please check http://thehackernews.com/2015/10/cryptowall-ransomware.html for details.

The goal of this paper is to develop an extensive and consistent survey based on a literature review and publicly available reports, organized using a value chain framework, to help understand cyber attacks in a systematic way. This can also help to develop more effective defense strategies.Cybercriminals run a business of selling cyber attacks, thus we concentrate on what could be considered as the "value-added" processes for cyber attacks. 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 cyber attack life-cycle operations, human resources, marketing and delivery, and technical support. It is important to note that both the defensive side (cybersecurity) and offensive side (cybercrime)[3] of cyberspace use similar innovations [37], and that not all activities included in the value chain model describing cybercrime are definitively 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, they can also represent techniques to identify opportunities for deliberate exploitation by criminals [4, 9, 70].

In addition, 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 expertise, and *cooperation*–cyber attackers can loosely or closely collaborate with each other to do complex attacks, in the cybercriminal ecosystem. Using the presented value chain model, we survey how diverse cybercrime activities can be executed in a service style, resulting in a cybercrime ecosystem framework to systematically understand the cyber attack business.

This framework enables us to systematically understand hacking innovations, which can help to redefine the cat-and-mouse game [41]. By following the "value-added" paths in the framework, we can understand the development, including availability and pricing models, of the cybercriminal services. 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.

Finally, based on the presented framework, identifying control points can help to improve the effectiveness with which cyber attack evolution is monitored and the business of cybercrime can be disrupted. Delegating responsibilities and actions among involved parties based on this framework is also helpful for realigning incentives of collaboration in the fight against cybercrime.

Therefore, the main contribution of this paper is the systematic survey of cybercrime services, which helps to understand the cybercrime ecosystem as a business and its evolution for further designing more effective 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 services. Section 4 reports the developed ecosystem framework to study the cyber attack business reconstruction and its evolution, including the emergence of the "cybercriminal service composition as a service". Section 5 summarizes this paper and briefly highlights possible ways to combat cyber attacks using the cybercriminal service ecosystem framework.

2 CYBER ATTACK ACTIVITIES: THE VALUE CHAIN MODEL

To effectively combat cyber attacks and enhance the cybersecurity on which our digital society relies, it is important to understand the operations behind a cyber attack, raising the following

[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 synonymously.

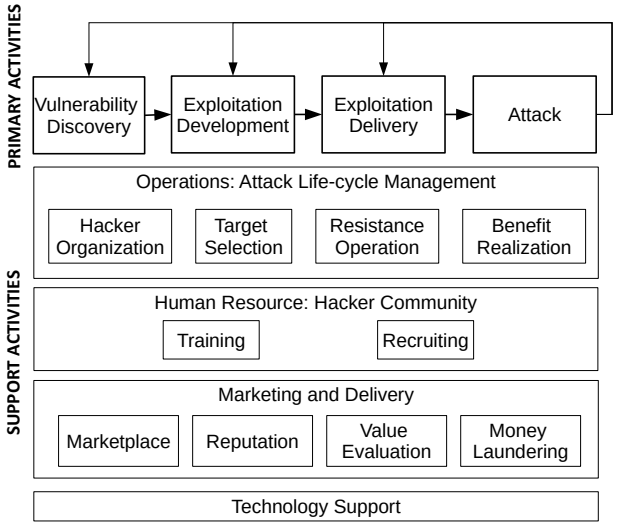


Fig. 1. Cybercriminal Value Chain Model

questions: *what activities are associated with a cyber attack?* The value chain model, developed by Michael Porter [122], is a powerful approach to understand the value-added procedures embedded within an organization. The value chain model views an organization as a system, made up of subsystems each with inputs, transformation processes and outputs, along with support activities. As cybercrime has become a business, from a value chain perspective, we can identify activities which add value for cyber attack operations, 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.* Straightforwardly, the primary activities which directly involve the attack are valuable for the attackers. The support activities, which are often overlooked, are also critical in facilitating the operation of the cybercrime business, as they can help the attacker to perform an attack with less cost and for higher benefit. Furthermore, we have validated the list of cybercrime services and 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 survey, which integrates the different components of the cyber attacks and uses value-chain model, to systematically understand cyber attacks from the business perspective.

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 the relatively simple use of passwords which are not modified for a long time and easy to uncover by brute force [106]. Cybersecurity usually involves technology, people, and process [89]. Overlooking strategic, managerial,

[4]These senior managers and executives are from members of Cybersecurity at MIT Sloan. Please check https://ic3.mit.edu/ for the member list. In addition, we use WannaCry attack as an example to show the efficiency of this framework in understanding a specific cyber attack. Due to the space limitation, please check Section F in Support Materials for more details.

and operational issues related to cybersecurity significantly weakens an organization's defenses against cybercrime [94]. Hence, vulnerability refers to both weaknesses in software or hardware in IT/OT systems, and 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 Vulnerability Database (NVD) and Security Focus BID [70] are considered as technical vulnerabilities in IT/OT systems. Most current vulnerability discovery research focuses heavily on the technical vulnerabilities [24, 55, 143]. However, with the development of 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 [135]. The typical cyber attack targeting these weakest links is the social engineering attack which deceives the users in an organization [161]. Furthermore, cyber threats from the supply chain are increasing [140]. Some recent efforts have attempted to detect and understand operational vulnerabilities in process and policy [113]. For example, a causal analysis based on STAMP [133] 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 technical and operational vulnerabilities. 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 the normal function of the targeted system [31]. Furthermore, a payload [18, 139] could be a malicious program performing 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.

Additionally, to perform advanced attacks by exploiting an operational vulnerability, some social engineering toolkits have been developed[5]. The Social Engineer Toolkit (SET) [121] was specifically designed for targeted attacks against a person or organization in a penetration test. Many social engineering exploits begin with the manipulation of the user-computer interface to breach a computer system's security [60]. For example, developing fake mobile apps that appear to be the same as their legitimate counterparts is one typical cyber attack to exploit the operational vulnerability that arises from what we consider the human factor of an organization [42]. The business email compromise scams [98], also known as "CEO fraud" or "whaling phishing", is another example in which the attacker counterfeits a message from a senior executive to trick someone at the organization into wiring funds to them. The operational vulnerability in the organization's financial process and human component is exploited to develop a persuasive, but fake, message.

[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 black hat hackers to perform cyber attacks.

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 is that this mechanism uses 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, counterfeit hardware or hardware with embedded malware can be distributed to infect many victims [140].

• ***Sent Directly***. This mechanism involves 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 exploit 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 cyber attack. Spear phishing emails containing BlackEnergy malware were sent to the victims, and the corporate IT network was compromised by opening disguised documents attached to the emails, which then propagated to the OT network [39].

• ***Drive-by-download***. The third mechanism involves redirecting the victim online to a website loaded with the exploitative programs, at which are 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 [16, 130, 160].

• ***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 [68]. Once the adulterated software runs, the malicious code will be executed and the exploitative programs will be downloaded to the victim's machine [56]. 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, 125].

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, 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 [39] as an example, after disrupting the power grid, the hackers used KillDish to erase important executable files and cause physical damages to the control system. Some attackers may 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 cyber attack from the value-added perspective, instead of the detailed cyber attack mechanisms, we must understand what a cybercriminal can gain from a successful cyber attack, and what these gains afford in terms of further attacks:

• ***Digital Gains***. Once inside, an attacker can get information contained in a victim's system, including sensitive information such as personal profiles, accounts, and intellectual property. The compromised system can be a "trophy" for the attack, while sometimes the human who is tricked by the attacker can be a "trophy". One example is when someone is tricked to work as a money mule for money laundering [66]. 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 cyber attack on Bangladesh Bank's (BB) SWIFT payments system in Feb, 2016 [142] 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 [168], NSA [54], Hacking Team [62] etc. can offer attackers 0-day vulnerabilities, exploitations, and many tools developed and customized by these professional organizations that expand and strengthen their arsenal.

• ***Direct 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 not only a direct monetary cost to an organization in the form of losses or damages, but also in indirect costs such as loss of trust, missed business opportunities and increasing defense costs for prevention, protection, detection, response and recovery to the cyber attack [7]. 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. The 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 [114] 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 pay a ransom to avoid damage.

• ***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 [81]. In this particular 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. Anonymous is one such group. A particular interesting case was when Anonymous attacked Freedom Hosting II which hosts 20% of dark web websites, 50% of which contained child pornography in some forms [13]. In this case, the Anonymous was trying to "do something good".

2.2 Support Activities: Facilitate the Attack

To supplement the primary activities discussed above, support activities are emerging in the cybercrime ecosystem to make cyber attacks more efficient: *gaining greater benefit with less cost.*

2.2.1 Operations: Attack Life-cycle Management. A cybercrime operation, like a legitimate business [152], must actively manage and support the cyber attack life-cycle to reduce costs, increase profits, and mitigate risk. In addition, cybercrime operations must also make conscious efforts to avoid being identified, and their 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.[6]

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

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

The cybercriminal in the executive role selects the target which would deliver the highest profit, the greatest positive difference between benefit and cost [81]. There are three factors to consider in evaluating the benefit from a successful cyber 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 cyber attack. In this scenario, the more easily vulnerabilities can be discovered and exploited in a certain organization's systems, the more attractive of a target the organization becomes. Once a specific target was selected, the cybercriminals may take on an exploitation mindset to dig into the target's systems and attempt an attack; 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 favor 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 cyber attack: 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 cyber attack. 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 cyber attack, the ease of the judicial process involved in the conviction P_c and the monetary opportunity cost if the attacker is convicted C_c. $C_p = P_a \times P_c \times C_c$.

[6]Based on the definition presented by William J. Stevenson [152], 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"*.

• **Operational Costs** C_o refers to the cost to carry out the cyber attack. 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 cyber attack 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: Cyber attack Target Selection Rule. For a rational cyber attacker, the target can be considered as valuable if and only if the expected benefit outweighs the expected cost.

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

Note that the equations discussed above are at a high level. They can help us to understand the values of different activities for the cyber attack. 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 process 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 cyber attack which involves multiple hackers, the cybercriminal in the executive role must organize his or her team for the attack. There exist the following six basic types of organization structures [104]:

- 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 [115], 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 contact with each other [85]. Furthermore, in online hacker forums, most hackers are novices with only a few more highly skilled hackers participating in forum activity [64, 87, 90] 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 [169]. 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 [80]. Though the motivation for the WannaCry ransomware 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 the number of users [163]. Additionally, many markets or forums are constructed for cybercriminals to trade their digital gains from successful attacks [26, 123, 147, 174]. According to the tracking of ransomware payments [123], 95% of the traced ransoms are cashed out via BTC-E, a digital currency trading and exchange platform. For psychological benefit, "Hall of Fame" for 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 within the cybercriminal community [38, 63, 85, 171].

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

Generally, 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[6, 36, 103], clearing event logs, command history, and shredding history files. To increase the chance of success of a cyber attack, 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 [116, 130].

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 but quickly re-emerged and attacked banks and e-commerce operations in Canada, Australia, the United States, and Finland in December 2015 [76]. This is because that 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 [171].

• **Hacker Training**. There is a limited number of highly skilled hackers [87] and the cybercriminal tends to build a collegial culture that encourages sharing of information and values innovation [64]. 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 [37], 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 [37] while the attacker may even have the advantage in skill, as the "worst is getting worse faster" [92]. 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 [46].

• **Hacker Recruiting**. 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 cyber attack. According to the research from Digital Shadows, the process hackers use to recruit new hires is the mirror to its legitimate counterpart [128]: post advertisements on forums, hacker-specific job boards, social networks to reach fresh talents, qualify candidates by application forms or even through interviews, and maintain a time-sensitive membership. The study of 18 investigations into criminal networks [84] demonstrates that the relationships based on real-world social networks play 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 [144].

2.2.3 Marketing and Delivery. The "booming" underground marketing and delivery activities play critical roles for attackers to realize potential benefits from successful cyber attacks.

• **Marketplace**. A marketplace for attackers to trade the digital gains is the principal way for attackers to realize the benefit from successful cyber attacks. We can observe many different dark web marketplaces available for different kinds of goods and services: vulnerability and exploitation [4, 70, 119], dumps, skimmers, identities, attack tools and mules [174], credit card [59], fake tools [153] and Bitcoin [123] etc. Some marketplaces even allow cybercriminals to operate "single-vendor stores", in the same way as one could do on eBay, where sellers will run their own online website to sell their products to their clients [59]. In June 2017, a black market framework was offered as "platform-as-a-service" for buyers to build their own darknet marketplace [35].

• **Reputation**. Anonymity can translate to uncertainty related to product quality in the hacker community [61, 171]. To mitigate this problem, trust and reputation play fundamental roles in the cybercrime ecosystem [85]. 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 the hacker community [49]. Some forums are open exclusively to well-vetted users and often require a fee to join, and other forums are invite-only [171] while some forums may even request that the members "must hack a website within 3 months" to maintain the membership [128]. Some guarantors will offer vetting services to check a prospective user's background, contributions, and trustworthiness [50]. 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 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 [61]; if a reviewed vendor is found to have traded dishonestly, that vendor will face a punishment [171].

• **Value Evaluation**. 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 [74]. 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 [22].

• **Money Laundering**. Money laundering is a traditional activity for underground crime, to make illegally-gained proceeds appear legal [15]. Likewise, money laundering plays a critical value-added role to support the benefit realization activities for cybercriminals, especially for those attackers motivated by financial gains. In addition, the advantage of digital currency–the protocol's

anonymity and resilience through flexibility–enables money launderers to do their business faster, cheaper and more discretely than before.

2.2.4 Technical Support. Cybercrime relies heavily on the technical support. Notably, the offensive and defensive sides use similar innovations [37]. Many technologies developed for "good" purposes have been coopted by cybercriminals for less than positive ends. The first IRC (Internet Relay Chat) bot was invented in 1988, then the first malicious bot appeared 10 years later [164]. The anonymous communication network technology Onion Routing (Tor) and the Invisible Internet Project (I2P) were developed to protect privacy online [6, 30]. Bitcoin, a peer-to-peer electronic cash system, was developed to allow any two willing parties to transact directly without the need for a third party [111]. Now these technologies have become the "cornerstones" for cybercriminals.

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*[7] 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 professional organizations or experts, even by the state-supported agencies like CIA [168] or NSA [54], may be taken and used to strengthen cybercriminal's arsenal.

2.3 Cyber attack Ecosystem: The Combination of Primary and Support Activities

The cyber attack ecosystem consists of not only primary activities directly related to a cyber attack, but also support activities that facilitate a cyber attack 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, which are often overlooked. Cyber attack operation activities, including target selection, hacker organization, benefit realization, and resistance measures, can significantly improve attackers' performance in the digital, direct monetary, and psychological gains. The hacker community is growing in both skill and scale to offer human resources, and marketing and delivery activities are available to further facilitate the benefit realization for cyber attack operation.

In addition, these value-added cyber attack activities are not isolated but related to each other. The cyber attack ecosystem is already well embedded within a comprehensive value chain. Some attackers, especially the highly skilled hackers, can be involved in multiple activities. A more eye-catching scenario is that, these activities can be orchestrated to collaborate within a more complex cyber attack, even when they are provided by different actors.

Hence, in order to combat the modern cyber attack effectively, beside the primary attack activities, the defensive community should also pay special attention to those emerging support activities. More importantly, it is critical to understand the cyber attack ecosystem from a systematic perspective, not only focusing on the individual activities, but also their relations with each others.

3 CYBERCRIMINAL SERVICE ECOSYSTEM: BUSINESS RECONSTRUCTION

With the development of service science [83], cybercrime as a service (CaaS) has become an important trend for the cybercriminal ecosystem [97, 134, 145]. Cybercriminals are leveraging this innovation to make their products and services more attractive, trustworthy, and more easily

[7]For these tools, we follow the kali linux tool taxonomy. Please check https://tools.kali.org/tools-listing for details.

delivered. This innovation not only puts cybercriminal tools and services in the hands of a wider range of threat actors, but it also turns the cyber attack 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 cyber attack services, to construct a systematic framework for the cybercrime ecosystem, developing an understanding of the business and the evolution of cyber attack itself[8].

3.1 Service Model: Business Components for Cyber attack

A cyber attack service provider can advertise a cybercrime service offering specific modules related to a cyber attack on the marketplace to reach as many potential users as possible. A buyer can purchase any needed services on a marketplace to build a cyber attack 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, 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 cyber attack that takes input and produces output using the support tools and techniques:

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

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. 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.

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 cyber attack, a cyber attack executive may combine related services so that they *"cooperate"* in performing more complex tasks to improve the performance of a cyber attack. 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 intersections 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 doesn't need to be equal to the input or support of the next service. Once there exists some intersection, then they can collaborate with each other to generate added value. Hence, with the adoption of the "as-a-Service" model for cybercrime,

[8]In this paper, we will use component and service synonymously. In addition, we further map these services into the value chain model. Please check Section C in the Support Materials for details.

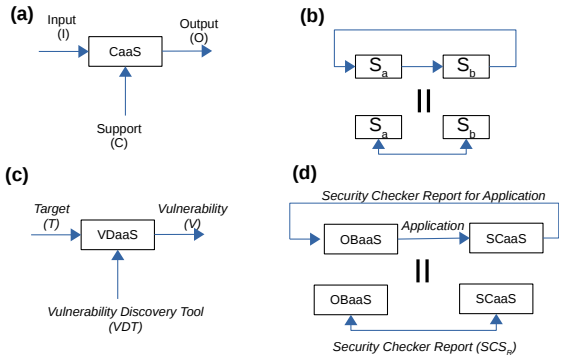


Fig. 2. Cybercriminal Service Model. (a) Each cybercrime value-added activity can be modeled as the service which takes input and produces output using supportive tools or techniques. (b) Two services form the composition based on their dependencies, further constructing a loop, simplified as a double 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.

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[9], including those directly related to the primary activities and those indirectly supporting a cyber attack, and how they collaborate with each other for the cyber attack.

In the following sections, using the value chain model presented above, we will define and describe the key cybercrime services, listed in Table 1, along the current status, examples (with references), and sample pricing.

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 cyber attack 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:

$$\mathbf{V} = VDaaS\ (\mathbf{T}, \mathbf{VDT}) \tag{3}$$

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 cyber attack based on the discovered vulnerability can be.

[9]In this paper, we are focusing on the added value and the business in the cybercriminal ecosystem, so the technical details, or cyber attack mechanims, as discussed in many studies like [9, 19, 20, 23, 125, 150, 156], are out of scope. We consider the attack service as a "black box" as the buyers don't need to understand the details of the services they purchase.

Service	Status	Pricing Model	Example Case	Estimated Price
EaaS	Existing	License	Exploit Trading [71]	up to more than $250, 000
		Subscription	Up-to-date Zero-day Exploits [151]	$150, 000 per month
PLaaS	Existing	Pay-per-install	Payload Renting [10, 16]	$0.02 – 0.10 per install
		Commission		40%
DaaS	Existing	Subscription	Phishing Service [145]	$85 – $115 per month
		Commission	Fake Anti-virus [97]	40%
OBaaS	Existing	Subscription	Obfuscation Platform [50]	$50 – 150 per month
SCaaS	Existing	Subscription	Scan4you [72]	$25 per month
TRaaS	Existing	Pay-per-click	Traffic Redirection [50]	$7 – $15 per 1, 000 visitors
BNaaS	Existing	Subscription	Botnet Shops [145]	$40 per month
BHaaS	Existing	Subscription	Cloud Bulletproof Servers [100]	$300 per month
TAaaS	Existing	Subscription	DDoS Attack Service [134]	$999 per month
REaaS	Existing	Pay-per-record	Reputation Escalation Markets [170]	$0.4 – 0.7 per record
MPaaS	Existing	License	Market Framework [35]	$4, 500 per licence
		Commission	Marketplace [34]	2% – 10%
MRaaS	Existing	License	Money Laundering Recruitment Package [99]	$1, 700 per licence
MLaaS	Existing	Commission	Money Laundering Service [127]	2% – 30%
HTaaS	Existing	License	Hacker Training Courses [138]	$250 – $800 per person
PPaaS	Evolving	License	Personal Profile Investigator [59]	$4 – $20 per record
TPaaS	Evolving	Subscription	"One-stop-shop" Platform [2, 73]	$4, 000 per month
RaaS	Evolving	Subscription	Smart Contract [79]	/
HRaaS	Evolving	Subscription	Online Hacker Recruiting Market [105]	/
VDaaS	Emerging	Subscription	Bug Bounty Program [132]	$542.04 – $1810.31 per vulnerability
TSaaS	Emerging	Subscription	Targets Ranking based on Value [101]	/
EPaaS,RPaaS	Emerging	Subscription	Repackaging Platform [143, 151]	$4, 000 per month
DMaaS	Emerging	Subscription	"How-to" Knowledge Systems [27]	/
VEaaS	Emerging	Subscription	Comparison "Shopping" Service [57]	/

Table 1. Status and Typical Pricing of Cybercrime Services. Services are defined and explained in the following sections. Examples for existing services are actual, emerging and evolving services are based on offensive versions of actual legitimate services. Prices listed here are intended to be representative of current prices and are constantly evolving.

It is not a surprise that in the underground cybercrime ecosystem, hackers trade their discovery directly in the dark web [4]. 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"* [51]. Hence it is rare to observe the independent vulnerability discovery services in the cybercriminal ecosystem. Only some highly skillful hackers, especially the organized cybercrime hackers, can offer services to help the clients to identify vulnerabilities in a target system. Given the success of the bug bounty programs [69, 95, 173], 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 within a given target. Considering the menacing targeted cyber attacks, aka advanced persistent threat (APT) [146], this VDaaS as the offensive bug bounty programs is very likely to be reality, if it does 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 a 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

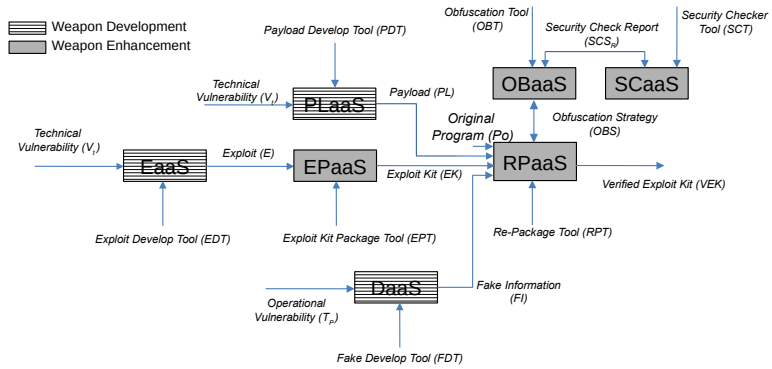


Fig. 3. Exploitation Development Service (EKaaS). "Weapon development" means the service is related to transfer the vulnerability into the weapon which can be used for attack. "Weapon enhancement" means the service is used to improve the effectiveness of the weapons.

effective cyber attack weapons with the support of development tools. As shown in Figure 3, the independence between different components can be used to increase the cyber attack performance and overcome the defensive efforts. For example, in the exploitation development process, the "weapon development" services can be used to transfer a vulnerability into an attack weapon and the "weapon enhancement" services can be used to improve its effectiveness for cyber attack.

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

$$\mathbf{E} = EaaS\ (\mathbf{V_t}, \mathbf{EDT}) \tag{4}$$

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 [33]. 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 [8] or reverse-engine the patch without the relevant details [14]. Though the automatic exploitation generation is fairly basic now [143], it is not surprising to observe new tools to support this highly valuable activity.

• **Exploit Package as a Service (EPaaS)**. Given a collection of exploits $\mathbf{E}$, EPaaS combines them into the exploit kit $\mathbf{EK}$ that is potentially more effective than any individual exploit. 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[50]. 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:

$$\mathbf{EK} = EPaaS\ (\mathbf{E}, \mathbf{EPT}) \tag{5}$$

where $\mathbf{EPT}$ refers to the strategies and tools used to package the exploits into exploit kit.

• **Deception as a Service (DaaS)**. Given the operational vulnerability $\mathbf{V_p}$, with the support of the development tools $\mathbf{FDT}$, this component generates the fake information $\mathbf{FI}$, like a fake website [88, 167], fake emails [60, 118], or fake software [153] which can be delivered to the target. A DaaS

is defined as follows:

$$\mathbf{FI} = DaaS\ (\mathbf{V_p}, \mathbf{FDT}) \tag{6}$$

Note that if the $\mathbf{V_p}$ contains detail information about the specific target, like organization structure, business process, network environment is available, the attack is referred as targeted attack [145], and normally it will have a higher probability of success. For example, in a 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 [107].

• **Payload as a Service (PLaaS)**. This component offers the payloads **PL** involved in a cyber attack. A payload [18, 40, 139] 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:

$$\mathbf{PL} = PLaaS\ (\mathbf{V_t}, \mathbf{PDT}) \tag{7}$$

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 [53, 116, 136]. For example, the Q implementation [137, 143] can be used to harden the exploits generated by the EaaS. Some may include security software to confirm the effectiveness of the obfuscation [50]. We define OBaaD in terms of the following relationship:

$$\mathbf{A_O} = OBaaS\ (\mathbf{A_I}, \{\mathbf{OBT}, \mathbf{SCS_R}\}) \tag{8}$$

where $\mathbf{A_I}$ refers to the input application, such as a payload, exploit kit, exploit, or fake information while $\mathbf{A_O}$ refers to the output application with obfuscation methods applied; **OBT** refers to the obfuscation tools and strategies; $\mathbf{SCS_R}$ 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 [53]. 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.

$$\mathbf{SCS_R} = SCaaS\ (\mathbf{A_I}, \mathbf{SCT}) \tag{9}$$

where $\mathbf{A_I}$ refers to the input application from OBaaS and $\mathbf{SCS_R}$ 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 [172]. 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 [39]. As shown in Figure 3 (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 surprising to observe these platforms, which may even be operated similarly to the mobile app testing cloud [47] 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:

$$\mathbf{VEK} = RPaaS\ (\mathbf{A_I}, \{\mathbf{RPT}, \mathbf{OBS}\}) \tag{10}$$

where $\mathbf{A_I}$ 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 $\mathbf{P_o}$ 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 an important role for the cyber attack. Take 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 [18]. This iterative process creates a so-called "family" of payloads [18, 157]. To circumvent detection more effectively, an advanced payload protects itself through redundant actions and encryption [116]. The malware "DenDroid" is even capable of detecting emulated environments such as Google Bouncer [155] and the WannaCry malware can detect whether the running environments are sandboxes [96]. 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 [9].

Until now, 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. 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"*. Based on Figure 3, various ways can be observed that exploitation services can be combined. For a given cyber attack, at least one of the "exploitation development" activities will be employed while the "resistance operation" component is not a must. However, the more services an attacker can effectively employ, the higher the chance of success in an attack will be. For example, 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 cyber attack [39], 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:

• **Botnet as a Service (BNaaS)**. As presented in [129], 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.

$$\mathbf{BN} = BNaaS\ (\mathbf{Z}, \mathbf{BNDT}) \tag{11}$$

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 [129].

• **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

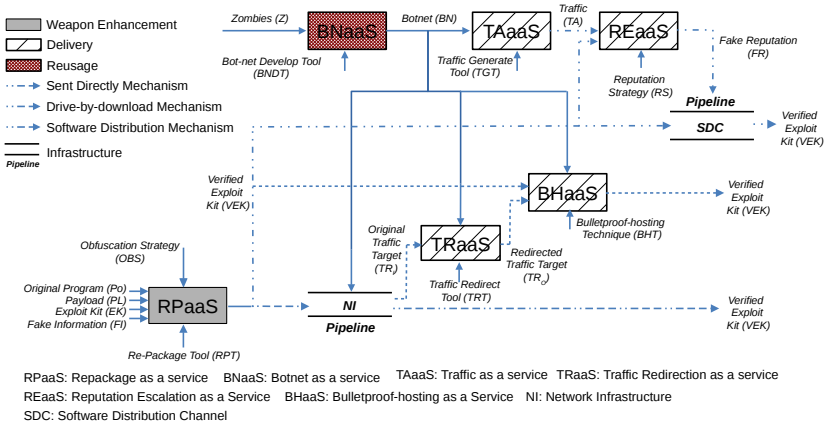


Fig. 4. Exploitation Delivery Services. "Delivery" refers to services serving to support the exploitation delivery. "Reusage" refers to services repurposing gains from previous successful attack. "Infrastructure" refers to network infrastructures which are operated by network infrastructure operators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

other websites [67, 167]. We formally define TRaaS as:

$$\mathbf{TR_O} = TRaaS\ (\mathbf{TR_I}, \{\mathbf{TRT}, \mathbf{BN}\}) \tag{12}$$

where $\mathbf{TR_I}$ refers to the original traffic target, and $\mathbf{TR_O}$ refers to the redirected traffic target, **TRT** is the traffic redirection technique [48, 159] and **BN** can be used to construct a fast-flux network to support traffic redirection [65].

• **Bulletproof Hosting as a Service (BHaaS)**. Bulletproof hosting services, such as Russian Business Network, McColo, Troyak, and Vline [78], are a lot more lenient about the contents hosted on their servers so that the attackers can host most types 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 [100]. Furthermore, the providers intend to host the severs in countries with more relaxed laws to make it easier to evade law enforcement [12]. Supported by the botnet, some providers will hire the compromised servers out until they are discovered [100]. 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.

$$\mathbf{VEK_O} = BHaaS\ (\{\mathbf{VEK_I}, \mathbf{TR}\}, \{\mathbf{BHT}, \mathbf{BN}\}) \tag{13}$$

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 [5], 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 [75] 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 [11]. Another typical application for this component is in an advertising fraud scheme, in which fake traffic generates vast amounts of undeserved revenue [44]. We formally define TAaaS in terms of the following relationship:

$$\mathbf{TA} = TAaaS\ (\mathbf{BN}, \mathbf{TGT}) \tag{14}$$

• **Reputation Escalation as a Service (REaaS)**. For the "software distribution" mechanism, this component will exploit the vulnerability of the current recommendation system [141] to craft a fake reputation [170] for the given malicious applications. Due to the fake ratings, search engines or rating services will list them as a popular service. This will significantly increase the exposure of the malicious applications. We formally define REaaS as:

$$\mathbf{FR} = \mathit{REaaS}\ (\{\mathbf{A_I}, \mathbf{TA}\}, \mathbf{RS}) \tag{15}$$

where $\mathbf{A_I}$ 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 cyber attack, 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 [142], where attackers clearly exhibited knowledge of SWIFT operations which may be from willing - or coerced -domain experts, and the Ukraine power grid attack [39], 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:

$$\{\mathbf{GD}, \mathbf{GP}, \mathbf{GL}\} = \mathit{AaaS}\ (\{\mathbf{VEK}, \mathbf{TA}\}, \{\mathbf{OBS}, \mathbf{HR}, \mathbf{DK}\}) \tag{16}$$

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

3.3 Cybercriminal Services Indirectly Supporting Primary Activities

There exist support services related to benefit realization, which are focusing on monetization of cyber attack gains through 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 [117]; domain information is extremely valuable for the targeted cyber attack [146]; compromised computers can be sold to assemble a botnet [129]; the stolen tools can be used to construct the toolkits which offer "one-stop-shop" tool support [77]; while a manipulated person can serve as the money mule [66]. For direct monetary 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 and motivate victims to pay to get back their stolen data [120]. Psychological gains can help attackers build reputation in the hacker community. Furthermore, to mitigate identity and quality uncertainty [171], the reputation and pricing systems are important for the cybercriminal ecosystem. 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.

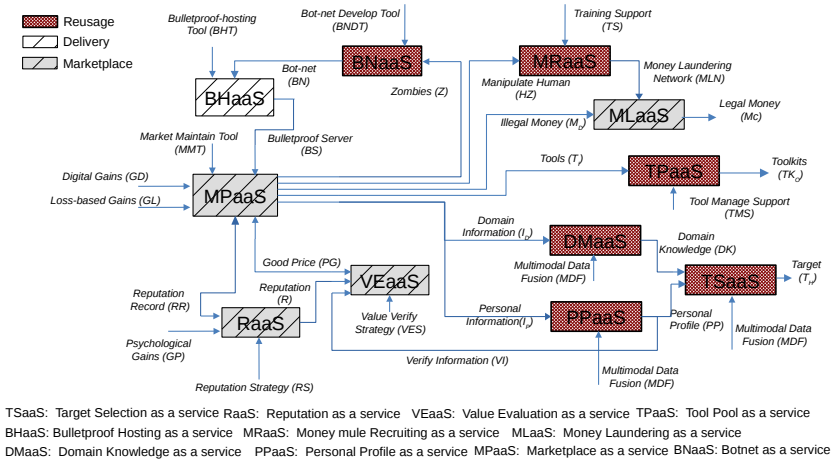


Fig. 5. Marketplace and Gain Reuse. "Marketplace" refers to the services to enable the trade for benefit realization while "Reusage" refers to the services which reuse the digital gains from previous successful cyber attack to facilitate the further attacks.

3.3.1 Digital Gain Reuse 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 cyber attack.

• **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 $\mathbf{I_p}$ 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 [166] or public sources on the internet, such as social media pages.

$$\mathbf{PP} = PPaaS\ (\mathbf{I_p}, \mathbf{MDF}) \tag{17}$$

where **MDF** refers to the multimodal data fusion [82] that can be used to manage and analyze the collected data. It is extremely valuable because different data sets can interact and inform each other [17] 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 a whaling phishing attack [60, 66].

• **Domain Knowledge as a Service (DMaaS)**. This component refers to domain information $\mathbf{I_d}$ 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**.

$$\mathbf{DK} = DMaaS\ (\mathbf{I_d}, \mathbf{MDF}) \tag{18}$$

The basic form of the domain knowledge is the step-by-step guidance for cyber attack. 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 [27], 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 CIA breach [168] or NSA cyber incident [54], and the HackerTeam hack [62], 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 $\mathbf{T_I}$

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 $\mathbf{TK_O}$ on the dark web exist to facilitate the access to these tools. For example, the "Shadow Brokers" offered a subscription-based service [77] with access to up-to-date exploits gained from the NSA cyber incident. We can formally define TPaaS as:

$$\mathbf{TK_O} = TPaaS\ (\mathbf{T_I}, \mathbf{TMS}) \tag{19}$$

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 can significantly reduce the cost and increase the benefit from the cyber attack. Given the availability of personal information and domain knowledge, as well as the development of advanced data analysis and artificial intelligence, it is possible for attackers to identify the valuable targets based on the expected benefit and cost, before they actually perform the cyber attack. Hence we can expect the emergence of target selection as a service for the cybercriminal ecosystem [101]. We formally define TSaaS as follows:

$$\mathbf{T_H} = TSaaS\ (\{\mathbf{PP}, \mathbf{DK}\}, \mathbf{MDF}) \tag{20}$$

where $\mathbf{T_H}$ 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, bullet-proof 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 $\mathbf{M_D}$ from a cyber attack, this component makes use of a money laundering network **MLN** to make it appear as though it was earned by legal means $\mathbf{M_C}$. We define MLaaS as follows.

$$\mathbf{M_C} = MLaaS\ (\mathbf{M_D}, \mathbf{MLN}) \tag{21}$$

Note that the $\mathbf{M_C}$ could also be in the form of digital currency, such as Bitcoin [80] since Bitcoin can be easily cashed out via digital currency trading platforms such as BTC-E or exchanged with each other [123]. **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 [25, 43, 66].

• **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 the recipients who respond to the email. These individuals will be trained and brought into the money laundering network [148].

$$\mathbf{MLN} = MRaaS\ (\mathbf{HZ}, \mathbf{TS}) \tag{22}$$

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)**. 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 [171]. 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[10], some third-party services such as Ripper.cc and Kidala.info [158] were developed to maintain a database of rippers.

$$\mathbf{R} = RaaS\ (\{\mathbf{GP}, \mathbf{RR}\}, \mathbf{RS}) \tag{23}$$

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 [141] 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 to mitigate the risk associated with quality uncertainty [171]. 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 measurement for to what extent the currencies are overvalued or undervalued [52]. Some cybercriminals can use scanned documents, like passports, to confirm other users' identities. For example, a hacker may verify a Paypal account with a scanned copy of the purported owner's passport [50].

$$\mathbf{PG_O} = VEaaS\ (\{\mathbf{PG_I}, \mathbf{R}, \mathbf{VI}\}, \mathbf{VES}) \tag{24}$$

where $\mathbf{PG_I}$ 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 $\mathbf{PG_O}$.

• **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 cyber attack 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.

$$\{\mathbf{G_O}, \mathbf{M_D}\} = MPaaS\ (\mathbf{G_I}, \{\mathbf{MMT}, \mathbf{BS}, \mathbf{RR}, \mathbf{PG}\}) \tag{25}$$

where $\mathbf{G_I}$ 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. $\mathbf{G_O}$ refers to the different types of materials like personal information I_p, domain information I_d, stolen tool set T_I, compromised machines Z, manipulate human HZ. $\mathbf{M_D}$ 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 cyber attack. As shown in Figure 6, it consists of the following two main services:

• **Hacker Training as a Service (HTaaS)**. Given specific domain knowledge related to a cyber attack, this component helps a hacker, especially a novice hacker, gain skills relevant to cybercrime

[10]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 [171]. The attackers can even conduct attacks against each other [21].

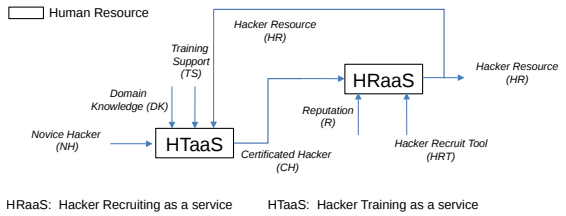


Fig. 6. Human resource service. These services prepare the necessary human resource for the cyber attack business through training and recruiting.

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 [46]. 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" [138] offering certifications once training is completed, and even runs a bug bounty program to reward those who find qualifying vulnerabilities in their sites.

$$\mathbf{CH} = HTaaS\ (\mathbf{NH}, \{\mathbf{DK}, \mathbf{TS}, \mathbf{HR}\}) \tag{26}$$

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 [144].

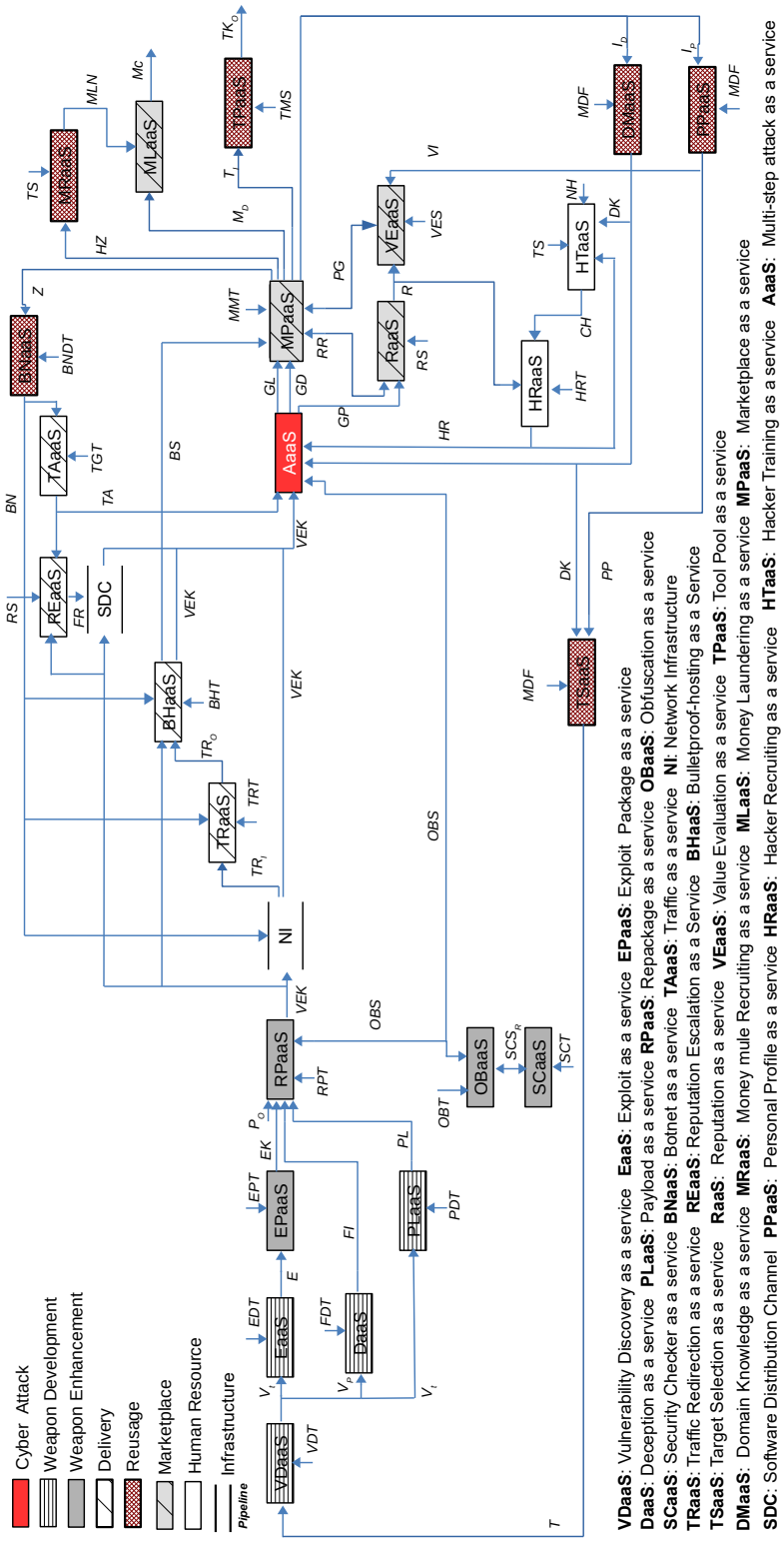
$$\mathbf{HR} = HRaaS\ (\mathbf{CH}, \{\mathbf{R}, \mathbf{HRT}\}) \tag{27}$$

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.

4 CYBERCRIMINAL SERVICE ECOSYSTEM FRAMEWORK

Following the value chain model presented in Section 2, we have identified twenty four (24) key value-added services[11] 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. The discovered vulnerabilities from "Vulnerability Discovery" can be transformed into effective weapons by "Exploitation Development" for cyber attacks. "Resistance Operation" activities make a cyber attack more powerful and better suited to avoid detection. The "Delivery" activities represent the act of delivering cyber attack 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

[11]Please check Section B in Support Materials 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 cyber attack business based on the identified services and their dependencies, including 25 services, their supported tools and two related network infrastructures.

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

4.1 Cybercriminal Service Development

4.1.1 Service Status. Based on the above discussions, we follow the value-added processes to construct the cybercriminal service ecosystem framework[12], to integrate widely-scattered services into a consistent framework and to understand these services' development. As shown in Table 1, for most identified services, we can observe many actual cases on the dark web. More importantly, as the offensive side and defensive side use similar innovations, the innovations in the context of legitimate businesses can drive the evolution of components in the cybercriminal service ecosystem. Hence, it is reasonable to expect that, even for those services that have not yet been observed as independent services, if they do not already exist, the offensive versions of legitimate defensive techniques are likely to emerge. Therefore, these identified services can be grouped into three different categories based on the their availability:

- **Existing Services** refers to the existing services whose business model is not expected to change significantly in a short term.
- **Evolving Services** refers to the services which are currently available in the dark web, in some form, but are expected to evolve into a new service model due to technological development. For example, in the cybercriminal service ecosystem, new reputation mechanisms like smart contract based on blockchain technology [79] or cyber grand challenge [9, 169] could be further developed to mitigate the uncertainty, beside existing services like Ripper.cc and Kidala.info to maintain a database of rippers [158], or relationships based on real-world social networks [84].
- **Emerging Services** refers to the services, though not observed as independent services on the dark web yet but expected to emerge, due to their specialization, the desirability of such services, and the existence of the similar innovations in legitimate businesses. Taking TSaaS as an example, given the rapid growth of the targeted cyber attack [91, 101, 146], targets ranking based on value can spread to and prove popular in the dark web;

4.1.2 Service Pricing Mechanism. For the pricing mechanism, some services, especially those providing digital goods, are generally offered with one-time fees and unlimited use. For example, the price of EaaS, which provides exploit using this license model, range from free to up to more than $\$250,000$, depending on its exploited vulnerability. It is important to realize that the cybercrime ecosystem is constantly evolving and the pricing models and prices even more so. The prices listed in our table are intended to be representative of current prices.

Increasingly, service providers charge buyers based on outputs or require commission sharing from successful cyber attacks. One example is the Pay-per-install model [16] for PLaaS, where buyers purchase the service and pay only $\$0.02 - \$0.10$ for each successful installment. Another example is REaaS in the reputation escalation markets where buyers buy "fault positive" feedback records with a very low price at $\$0.4 - \$0.7$ per record. One eye-catching example of requiring commission sharing price mechanism recently is that the "GandCrab", a ransomware payload service discovered in Jan 2018, offers a partner program, in which members share 40% profits

[12]Please check Section C in Support Materials for discussions about the mapping to value chain model and developments for each service.

with the developers[10]. Another pricing mechanism uses a subscription model that the buyer pays a membership to access provided service. One example is that the Shadow Brokers released zero-day vulnerabilities and exploits as a subscription-based service-"TheShadowBrokers Dump Service"[151]. Notably, providers may adopt various pricing models for different customers at different service prices for a given service.

4.1.3 Rapid Growth of Services. Based on the presented framework, it can be expected that services with more available inputs tend to grow faster. For instance, the increasing occurrence of data breach incidents [166] will enable the growth of the PPaaS (personal profile) and DMaaS (domain knowledge) in our framework, which will further drive the development of TSaaS (target selection). With TSaaS is an input to the "weapon development" process for targeted cyber attacks, the cost for a whaling phishing will substantially drop and therefore whaling phishing attacks can scale up. Due to the advancement of target selection services, we can foresee more personalized, large-scale cyber attacks.

We can also expect that services located at crossroads of many value-added paths will grow more rapidly. One example for this is "Repackage-as-a-Service (RPaaS)". As this type of services becomes more available, it is very possible that we will experience a significant number of new malware attacks relying on repackaged payloads and new obfuscation methods. A sign for this is that repacking attacks are becoming common for mobile devices, especially for Android ecosystem [143]. More importantly, services in the framework are not isolated. They actually have already formed four reinforcing loops, including the reuse of the compromised machines, stolen tools, stolen information and hacking experience. These loops and interactions among services enable each cyber incidence to reinforce and empower other incidences[13].

4.2 Profitability of Cybercriminal Business: the Emergence of Composition Services

As discussed above, components for a cyber attack are offered as services that a would-be attacker can purchase on the dark web to equip themselves for an attack. To analyze the profitability of the cybercriminal business, 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 [28] 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 cyber attack as a part of MLaaS (money laundering) can be accessed for a fee of $400 and 40% commission on processed funds.

• **Example of Return on Investment (ROI)**[14]. 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

[13]Please check Section D in Support Materials for discussions about the cyber threat reinforcements.
[14]Please refer to Section E in Support Materials for more details about the benefit and cost.

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 [32] 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 reach 12,682.30%.

• **Cybercriminal service composition as a service.** Hence, we can conclude that combining separate services to perform a cyber attack has great value for cybercriminals. This motivates the emergence of *"cybercriminal service composition as a service"*. In this scenario, hackers 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 would allow cybercriminals 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 may be able to hide themselves even deeper, and in certain cases, some of their activities may no longer be characterized as illegal.

5 CONCLUSION AND IMPLEMENTATION

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 will be difficult.

This paper provides a comprehensive survey of cybercrime services, based on an extensive literature review and publicly available reports, and organized them using a value chain framework. 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. These activities are not isolated but can collaborate with each other. Combining the value chain model with the developments of the "as-a-service" innovations, we can 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. The framework enables us to systematically understand the hacking innovations in the cybercriminal ecosystem, including the cybercriminal service's development (availability status, pricing model and growth), as well as the emergence of composition service: "cybercriminal service composition as a service", which can offer "one-stop-shop" style cyber attack services for the cybercriminal ecosystem.

Finally, based on the systematic understanding about the cyber attack business, the framework inspires several strategies to more effectively combat cyber attacks, including:[15]

• **Striking the dark side by identifying the Control Points to improve effectiveness.**

[15]Please check Section G in Support Materials for more detailed discussions about these two examples.

Inspired by [29], we can define the control point as *"the critical components which can support the other components in the cybercrminal service ecosystem"*. Based on the presented cybercrime ecosystem framework, if we can use "honeypots" to monitor 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 cyber attack. Furthermore, such a scheme could also help law enforcement associates collecting critical evidence to convict cybercriminals and to strike at the heart of cybercrime business. Another interesting aspect is that given the uncertainties related to identity and quality, the cybercriminal market is a typical "market for lemons" [108, 167]. If the defensive side can flood the cybercriminal ecosystem with honeypot-style or deceptive goods, it will make the dark web less attractive for cybercriminals looking to purchase services. For example, as Hansa (one of the largest dark web markets) was once compromised by police but kept running, now hackers are suspecting that the other dark web markets, like "Dream Market", was also compromised in a similar manner and under police control [45]. In addition, the framework can help to access the effectiveness and the side-effect for the cybersecurity policies. For example, HRaaS (hacker recruit) serves a control-point role to recruit skillful hackers into the cybercriminal ecosystem. Without considering its impact, the efforts to train cybersecurity workforce [37] for defensive side will also increase the cybercriminal workforce supply.

• **Assigning responsibility to different actors for meaningful collaboration.**

There exist several challenges plaguing cybersecurity and cybersecurity policy when it comes to working together to build a safer connected world [108]: the externalities, misaligned incentives and the information asymmetries. These market failures call 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, including the *individuals and corporations, software/hardware providers, security companies, infrastructure operators, financial systems, governments* and *third-party threat intelligence service providers*. For example, the government has an important role in combatting cybercrime, given its position to address market failures related to cybersecurity and strategies to recruit skilled individuals to the defensive side and combat incentives that drive them to join the cybercrime business should be considered. Intuitively, only emphasizing the *individuals and corporations* to protect themselves is not an effective policy. All these actors need to take specific responsibilities and collaborate with each other to strike the cyber threat capability supply chain. Policies to motivate them to take actions are urgently needed.

Overall, by conceptualizing the modern cyber attack business systematically, we will be able to design better strategies to combat cyber attacks. 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.

ACKNOWLEDGMENTS

The authors would like to thank members from the Cybersecurity at MIT Sloan for their valuable comments and inputs. In addition, we thank all the reviewers for their comments and improvements.

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] 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.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] Bradley Barth. 2018. RIG and GrandSoft exploit kits shell out new GandCrab ransomware. (2018). www.scmagazine.com/rig-and-grandsoft-exploit-kits-shell-out-new-gandcrab-ransomware/article/740900/

[11] 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/

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

[13] 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

[14] 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.

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

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

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

[23] 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.

[24] 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.

[25] Kim Kwang Raymond Choo. 2011. The cyber threat landscape: Challenges and future research directions. *Computers and Security* 30, 8 (2011), 719–731.

[26] 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.

[27] Cuong Xuan Chu, Niket Tandon, and Gerhard Weikum. 2017. Distilling Task Knowledge from How-To Communities.. In *World Wide Web Conference*. 805–814.

[28] Cisco. 2016. *Cisco 2016 Annual Security Report*. Technical Report. 1–87 pages.

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

[30] 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.

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

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

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

[34] DEEPDOTWEB. 2018. Updated: List of Dark Net Markets. (2018). https://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/

[35] DEEPWEBADMIN. 2017. Build a Black Market in Dark Web only for $4500; Cybercrime goes PAAS. (2017). https://www.deepweb-sites.com/build-black-market-dark-web-4500-cybercrime-goes-paas/

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

[37] 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.

[38] 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.

[39] E-ISAC and SANS. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Technical Report. 23 pages.

[40] 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.

[41] 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.

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

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

[44] 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

[45] 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

[46] 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

[47] Jerry Gao, Xiaoying Bai, Wei-Tek Tsai, and Tadahiro Uehara. 2014. Mobile Application Testing: A Tutorial. *Computer* 47, 2 (2014), 46–55.

[48] 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

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

[50] Max Goncharov. 2012. *Russian Underground 101.* Technical Report. Trend Micro. 1–29 pages.

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

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

[53] 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.

[54] 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/

[55] 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.

[56] 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.

[57] 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.

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

[59] 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

[60] 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.
[61] 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.
[62] 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
[63] Thomas J. Holt. 2017. Identifying gaps in the research literature on illicit markets on-line. *Global Crime* 18, 1 (2017), 1–10.
[64] 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.
[65] Thorsten Holz, Christian Gorecki, Konrad Rieck, and Felix C Freiling. 2008. Measuring and Detecting Fast-Flux Service Networks. In *Ndss*. 24 – 31.
[66] Jason Hong. 2012. The Current State of Phishing Attacks. *Commun. ACM* 55, 1 (2012), 74–81.
[67] 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.
[68] Keman Huang, Jinjing Han, Shizhan Chen, and Zhiyong Feng. 2016. A Skewness-Based Framework for Mobile App Permission Recommendation and Risk Evaluation. In *International Conference on Service-Oriented Computing*. 252–266.
[69] 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.
[70] 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.
[71] Inj3ct0r. 2018. Oday.today. (2018). https://0day.today
[72] Steven K. 2011. Tracking Cyber Crime: scan4you.net (Private AV Checker). (2011). http://www.xylibox.com/2011/10/scan4younet-private-av-checker.html
[73] Vitaly Kamluk and Alexander Gostev. 2016. *Adwind-a cross platform RAT*. Technical Report February. Kaspersky. 83 pages.
[74] Karthik Kannan, Mohammad S. Rahman, and Mohit Tawarmalani. 2016. Economic and Policy Implications of Restricted Patch Distribution. *Management Science* 62, 11 (2016), 3161–3182.
[75] Mohammad Karami, Youngsam Park, and Damon McCoy. 2016. Stress testing the Booters: Understanding and undermining the business of DDoS services. In *the 25th International Conference on World Wide Web*. 1033–1043.
[76] 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/
[77] 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
[78] Maria Konte and Nick Feamster. 2015. ASwatch : An AS Reputation System to Expose Bulletproof Hosting ASes. In *Sigcomm 2015*. 625–638.
[79] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. 2016. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In *2016 IEEE Symposium on Security and Privacy*. 839–858. https://doi.org/10.1109/SP.2016.55
[80] Brian Krebs. 2016. Money Mule Gangs Turn to Bitcoin ATMs. (2016). https://krebsonsecurity.com/2016/09/money-mule-gangs-turn-to-bitcoin-atms/
[81] Nir Kshetri. 2006. The simple economics of cybercrimes. *IEEE Security and Privacy* 4, 1 (2006), 33–39.
[82] 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.
[83] 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.
[84] E. R. Leukfeldt. 2014. Cybercrime and social ties: Phishing in Amsterdam. *Trends in Organized Crime* 17, 4 (2014), 231–249.
[85] 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.
[86] 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.
[87] 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.

[88] 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.
[89] 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.
[90] 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.
[91] 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.
[92] Stuart Madnick. 2016. Dark Web : hackers trump good guys in sharing information. (2016), 2 pages.
[93] Stuart Madnick. 2017. Preparing for the Cyberattack That Will Knock Out U.S. Power Grids. *Harvard Business Review* (2017), 5.
[94] Stuart Madnick. 2017. What Executives Get Wrong About Cybersecurity. *Sloan Management Review* January (2017), 22–24.
[95] 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 *WEIS*. 1–19.
[96] MalwareTech. 2017. How to Accidentally Stop a Global Cyber Attacks. (2017). https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html
[97] Derek Manky. 2013. Cybercrime as a service: A very modern business. *Computer Fraud and Security* 6 (2013), 9–13.
[98] Steve Mansfield-Devine. 2016. The imitation game: how business email compromise scams are robbing organisations. *Computer Fraud and Security* 11 (2016), 5–10.
[99] Etay Maor. 2013. No Money Mule, No Problem: Recruitment Website Kits for Sale. (2013). https://securityintelligence.com/money-mule-problem-recruitment-website-kits-sale/
[100] Max Goncharov. 2015. *Criminal Hideouts for Lease: Bulletproof Hosting Services.* Technical Report. Trend Micro. 28 pages.
[101] Inc. McAfee. 2016. *McAfee Labs 2017 Threats Predictions.* Technical Report November 2016. 1–51 pages.
[102] 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
[103] 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.
[104] Michael McGuire. 2012. *Organised Crime in the Digital Age.* Technical Report September.
[105] McKinsey & Company. 2015. *A Labor Market That Works : Connecting Talent With Opportunity in the Digital Age.* Technical Report June. 88 pages.
[106] 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.
[107] Max Metzger. 2016. Snapchat got whaled, employee payroll released. (2016). https://www.scmagazineuk.com/snapchat-got-whaled-employee-payroll-released/article/530493/
[108] 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.
[109] Steve Morgan. 2016. *Hackerpocalypse : A Cybercrime Revelation.* Technical Report. Cybersecurity Ventures. 1–24 pages.
[110] 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
[111] Satoshi Nakamoto. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Technical Report. 9 pages.
[112] 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.
[113] 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.
[114] NTTSecurity. 2016. *SERT Quarterly Threat Report Q2 2016.* Technical Report.
[115] 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.
[116] Philip O'Kane, Sakir Sezer, and Kieran McLaughlin. 2011. Obfuscation: The Hidden Malware. *IEEE Security & Privacy* 9, 5 (2011), 41–47.
[117] 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.

[118] Hilarie Orman. 2013. The compleat story of phish. *IEEE Internet Computing* 17, 1 (2013), 87–91.
[119] Andy Ozment. 2004. Bug auctions: Vulnerability markets reconsidered. In *Workshop on Economics of Information Security (WEIS)*. 1–23.
[120] Pierluigi Paganini. 2016. Ran$umBin a dark web service dedicated to ransomware. (2016). http://securityaffairs.co/wordpress/46770/breaking-news/46770.html
[121] 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.
[122] Michael Porter. 1985. *Competitive advantage: creating and sustaining superior performance*. The Free Press. 580 pages.
[123] 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.
[124] PwC. 2016. *Global Economic Crime Survey 2016: Adjusting the Lens on Economic Crime*. Technical Report. PwC. 1–31 pages.
[125] 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.
[126] 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.
[127] Peter Reuter and Edwin M Truman. 2003. Money Laundering: Methods and Markets. In *Chasing Dirty Money: The fight against money laundering*. 25–43. https://doi.org/10.1108/13685200310809699
[128] 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/
[129] 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.
[130] Christian Rossow. 2013. *Using Malware Analysis to Evaluate Botnet Resilience*. Ph.D. Dissertation. Vrije Universiteit.
[131] RSA Whitepaper. 2016. *2016: Current State of Cybercrime*. Technical Report. RSA. 1–7 pages.
[132] Ryan Ellis, Keman Huang, Michael Siegel, Katie Moussouris, and James Houghton. 2017. Fixing a Hole: The Labor Market for Bugs. In *New Solutions for Cybersecurity*, Alex Pentland Howard Shrobe, David Shrier (Ed.). 122–147.
[133] 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.
[134] Raj Samani and Francois Paget. 2013. *Cybercrime Exposed: Cybercrime-as-a-Service*. Technical Report. McAfee. 1–18 pages.
[135] Bruce Schneier. 2015. *Secrets and Lies: Digital Security in a Networked World*. Wiley. 418 pages.
[136] 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.
[137] Ej Schwartz, Thanassis Avgerinos, and David Brumley. 2011. Q: Exploit hardening made easy. In *USENIX Security '11*, Vol. 8. 25.
[138] Offensive Security. 2017. Offensive Security Training, Certifications and Services. (2017). https://www.offensive-security.com/
[139] Securityfocus. 2012. Payload Definition. (2012). http://www.securityfocus.com/glossary/P
[140] Dave Shackleford. 2015. *Combatting Cyber Risks in the Supply Chain*. Technical Report. 20 pages.
[141] Wanita Sherchan, Surya Nepal, and Cecile Paris. 2013. A Survey of Trust in Social Networks. *Comput. Surveys* 45, 4 (2013), 47–47:33.
[142] Sergei Shevchenko. 2016. TWO BYTES TO $951M. (2016). http://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html
[143] 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.
[144] Johan Sigholm. 2013. Non-State Actors in Cyberspace Operations. *Journal of Military Studies* 4, 1 (2013), 1–37.
[145] 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.
[146] 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.

[147] 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.
[148] 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.
[149] Richard Spinello. 2016. *Cyberethics: Morality and Law in Cyberspace*. Jones & Bartlett Learning. 239 pages.
[150] 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.
[151] Steemit. 2017. theshadowbrokers. (2017). https://steemit.com/@theshadowbrokers
[152] William J. Stevenson. 2012. *Operations management* (11th editi ed.). Tim Vertovec. 908 pages.
[153] 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.
[154] 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.
[155] 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.
[156] 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.
[157] 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.
[158] 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
[159] 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.
[160] 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.
[161] 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.
[162] 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.
[163] Kevin Townsend. 2017. Latest WannaCry Theory: Currency Manipulation. (2017). http://www.securityweek.com/latest-wannacry-theory-currency-manipulation
[164] Amit Kumar Tyagi and G Aghila. 2011. A Wide Scale Survey on Botnet. *International Journal of Computer Applications* 34, 9 (2011), 975–8887.
[165] Sun Tzu. 2005. *The art of war*. Shambhala Publications.
[166] Verizon. 2017. *2017 Data Breach Investigations Report*. Technical Report. 76 pages.
[167] John Wadleigh, Jake Drew, and Tyler Moore. 2015. The E-Commerce Market for "Lemons": Identification and Analysis of Websites Selling Counterfeit Goods. In *the 24th International Conference on World Wide Web*. 1188–1197.
[168] Wikileaks. 2017. Vault 7: CIA Hacking Tools Revealed. (2017). https://wikileaks.org/ciav7p1/
[169] Eric Wustrow and Benjamin VanderSloot. 2016. DDoSCoin: Cryptocurrency with a Malicious Proof-of-Work. In *USENIX Workshop on Offensive Technologies*.
[170] Haitao Xu, Daiping Liu, Haining Wang, and Angelos Stavrou. 2015. E-commerce Reputation Manipulation: The Emergence of Reputation-Escalation-as-a-Service. In *the 24th International Conference on World Wide Web*. 1296–1306.
[171] 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.
[172] 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/
[173] 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.
[174] 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.