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

Keman Huang
Michael Siegel
Stuart Madnick

Working Paper CISL# 2017-17

November 2017

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

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

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

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

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

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

1 INTRODUCTION

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

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

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

Authors' addresses: Keman Huang, Sloan School of Management, MIT, Cambridge, MA 02142, USA; email: keman@mit.edu; Michael Siegel, SloanSchoolofManagement,MIT, Cambridge,MA02142,USA; email:msiegel@mit.edu; StuartMadnick, SloanSchoolofManagement,SchoolofEngineering,MIT,Cambridge,MA02142,USA; email: smadnick@mit.edu.

Ever since the firstreported cybercrime in 1973, when Union Dime Savings Bank account data was manipulated, cybercrime has continually evolved[1]. Beyond a nefarious hobby, cybercrime has become a way for cybercriminals to earn a living[2]. While it remains underground, it is a business nonetheless; attackers cooperate, and work to maximize

profits and minimize risk of arrest [85]. Cybercrime as a profession is increasingly attractive for able hackers, and in turn, cyber attacks themselves are increasingly well organized [2]. With the wide-spread adoption of the"as-a-service" modelfor cyber attack,the attacker can purchase the desired"service" through the dark web withoutsomuchasacursoryunderstandingofwhatisinvolvedinitsexecution[104,142,155]. This eliminates the barriers that previously existed to performing a crippling cyber attack, and pushes theattackersdeeperundergroundandfurtherfromthegraspofauthorities.

In the words of Sun Tzu, "Know yourself, know the enemy."[174] Tocombat cybercrimes in an efficient andeffectiveway,weneednotonlydeveloptechnical solutions toprotect against attacks, butalsounderstandthe structureofthebusinessofundergroundcybercrime,andthedriversofits development:

· *How doesthe cybercriminal organize a cyber attack?*

It has been said that "the good guys are getting better, but the bad guys are getting badder faster"[100].Much of published research on cyberattacks has been focused on how attackers clan destinelyintrudeonprivatesystems[3,66,72,136,166].However,reactingpassivelytoacyber attack andattemptingto keepupwiththe almostdailyemergenceofinnovationsonbehalf of cybercriminalsmeans that "[Corporations] are are not winning [in the cyberdefense battle]"[108]. Cybercrime has taken on the guise of a business in recent years. Without understanding the rele vant operations of cybercrime, it is difficult to combat cybercrime effectively. Researchers have begun to study different components of this underground business, including the marketplaces connecting attackers and buyers, and the community of hackers ready to deliver services for a fee [22,24,65,73,76,92,94,97,123,133,136,157,163,169,186].Basedontheseindividualelements, Thomas et al. [171] proposes a framework for understanding the structure of the underground cybercrime service throughthemonetizationprocess,offeringwhat canbe characterizedas 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. "Cybersecu
rityis still agameof cat-and-mouse"[47], withthedefense tryingtocatchupwiththeoffensewith, up until this point, little success to show forits efforts.

· *How doesthe cyber attack develop in the wild?*

The underground cybercriminal has proven difficult to study. Researchers have used "honeypots" [118]toidentifycybercriminals, andhave collectedinformationontheactivitiesof cybercriminals [157].These efforts tomonitorthedevelopmentof cyberattacksofferrelevant counterintelligence. In considering the adoption of the "as-a-service" model [56, 139, 155, 171], researchers have compiled theservicesofferedtobuyersbythecybercrimeindustry.Withoutaclearframeworkthrough which to study the cybercrime service economy, it remains difficult to understand the modern cyberattackeffectively.

· *How to shareresponsibility to combat theevolving cyber attack?*

[1]There is still much debate about thedefinition of cybercrime and what constitutes a cyberattack. Since no single, agreed upondefinitionexists,inthispaper wewill consider "cybercrime" all cyber activities that are relatedto a "cyberattack", or that which undermines the function of the digital system belonging to the cybercriminal ecosystem. In this paper, we will use "cyberattack" and "cybercrime" interchangeably. Note that not all activities included in our model are illegal. In fact,
there are many discussions, outside the scope of this paper, about cyber ethics and the legality of such activity [64, 159]. [2]During 2015, the CrytoWall ransomware virus raised more than $325 million for the hacking group, http://thehackernews.com/2015/10/cryptowall-ransomware.html, last visited 2017-6-1

Thoughcybercrime andits threatshave beenthoroughlydiscussed[43],howexactly tocombat cybercrime is still an open issue. Software/hardware developers, cybersecurity providers, infrastruc ture operators, financial sectors, governments, third-party organizations, companies and individuals needtowork togethertowardtoimprove cybersecurity.The cybercrime reportinginfrastructure, led by cybersecurity providers, infrastructure operators and vigilante groups emerged to combat infections [78]. Due to misaligned incentives, information asymmetries, and externalities [113], it has been difficult to develop a systematic understanding of the underground cybercrime ecosystem whichis crucialtounderstandwhatresponsibilitiesor actions shouldbe assignedfor eachpartyin the ultimate achievement of a "cyber-immune" world.

- **NeedforFrameworktoUnderstandCyberAttackBusiness**.

Thegoalofthispaperistodevelopaframeworkbasedonliteraturereviewandpubliclyavailable reports relatedto cyberthreatintelligence to facilitate the further studyof cybercrime andthe undergroundeconomywhichsurroundsit.Cybercriminalsrunabusinessof sellingcyberattacks, andthusweconcentrateonwhatcouldbeconsideredasthe"value-added"processesforthecyber attack. To understand these processes, we develop the *cybercriminal value chain model* consisting of the primary activities of vulnerability discovery, exploitation development, exploitationdelivery, and attack, as well as the supporting roles of cyberattack life-cycle operations, human resources, marketing and delivery, and technical support.It is important to note that both the defensive side (cybersecurity) and the offensive side (cybercrime)[3] of cyberspace use similar innovations [42], and that not all activities included in the value chain model describing cybercrime are illegal. For example, vulnerability discovery and disclosure are what are called "double-sword" activities. While they can be used to develop patches for a flawed system, can also represent techniques to identify opportunities for deliberate exploitation by criminals [5, 15, 76].

Inspired by the STAMP model [119, 141], we develop the service model-consisting of input, output, andsupporttosystematicallydiscussthecybercrimeecosystem, consideringitsrestructuringinto an "as-a-service" model. This enables the *specialization*–cyber attackers can focus on specific componentsandpromotetheexpertiselevel, *commercialization*–cyberattackerscanmonetizetheir attackexpertises, and*cooperation*–cyber attackers canlooselyororganizedlycollaboratewith each othertodo complex attacks,for cyber attack in the ecosystem. Following thepresentedvalue chain model, we survey how cybercrime activities can be executed in a service style to develop a cybercrime ecosystemframeworkforthinkingaboutthe cyberattacksbusiness.

Basedon the framework developedherein, wediscuss the methods that can effectively combat
cyberattacks.Theframeworkenablesthesystematicunderstandingofthehackinginnovation,the evolution of the cybercriminal services, which can help to redefine the cat-and-mouse game [47]. Usingthe cyberthreats identifiedbytheMcAfee 2017ThreatsPredictionReport[107],we confirm the efficacy of our framework. Notably, we observe that by following the "value-added" paths in the framework, cybercriminals build the reinforcement loops that translate to the cyberthreats more grave than previously expected. The Return-On-Investment (ROI) analysis reveals that cybercrime is a serious business, indicating the great value that "cybercriminal service composition as a service" represents to the cybercrime ecosystem. Additionally, identifying the control points can help to improve the effectiveness with which cyberattack evolution is monitored and ultimately disrupt the business of cybercrime. Delegating responsibilities and actions among involved parties based on thepresented framework is helpfulto realign incentives pointto collaboration in the fight against cybercrime.

[3]Therearetwosidestocyberspace:thedefensivesidefocustoimprovethecybersecurityandprotectthetargetsfrom

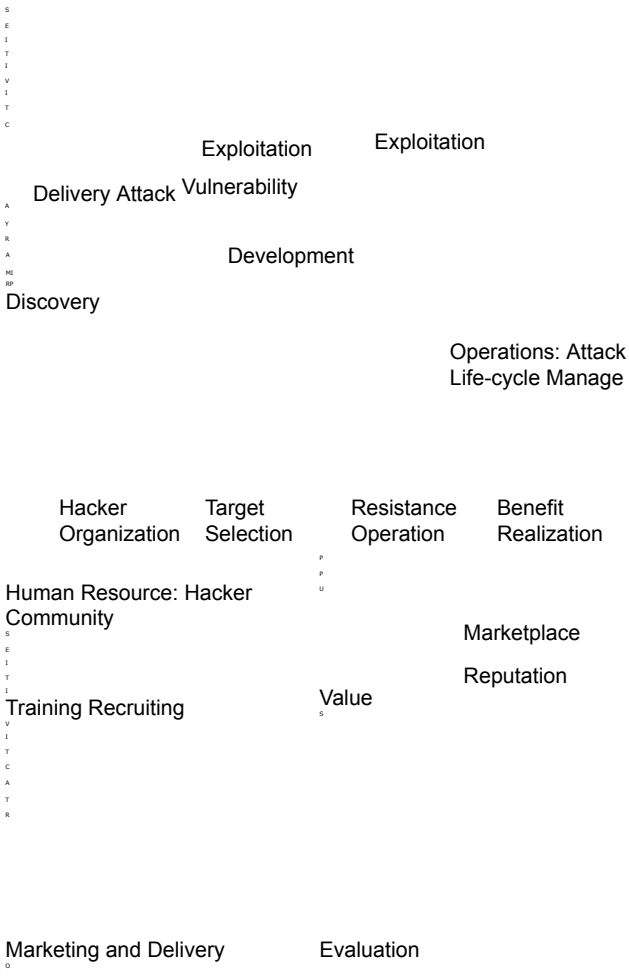
attack while the offensive side is for cybercrime and try to attack the targets. In this paper, for the offensive side, we will usehackersandattackersexchangeable.

Therefore,themaincontributionofthispaperis the systematic studybasedonliterature review tounderstandthe cybercrime ecosystemas abusiness,its evolutionandthe effective intervention strategies against it. These consist of:

- The value chain model for understanding "value-added" cyberattack activities;
- Thecybercriminalserviceecosystemframeworkforunderstandingcyberattackevolution;
- The implicationsofthe frameworkindesigninginterventionstrategies.

In Section 2,wepresentthe value chainmodelforunderstandingcybercrime activities. Section 3 introduces the service model and details the cybercriminal ecosystem framework to study the cyberattack business reconstruction and its evolution. Section 4 highlights the applications relevant to combatthe cyber-attacks. Our conclusions are summarizedin Section 5.

2 CYBERATTACK ACTIVITIES:THEVALUECHAINMODEL



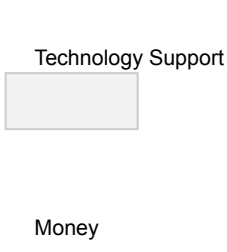


Fig. 1. Cybercriminal Value Chain Model

Toeffectively combat cyber-attacks and enhance the cybersecurity on which our digital society relies,itis imperative tounderstandthe operationbehinda cyberattack,raisingthe following questions: *what activities are associated with a cyberattack?* In considering cybercrime as the business thatits has become,from a value chain perspective [129], we can identify the activities which add value for the cyber attack operation, as presented in Figure 1. These value-added processes include *any activity in the cybercrime businessecosystem which helpsthe attackerreducethe cost of, and increasethe benefitincurred in cyber-attacks*.Itis straightforward thatthe primary activities whichdirectlyinvolvetheattackarevaluablefortheattackers.Additionally,thesupportactivities, which are often overlooked are critical in facilitating the operation of the cybercrime business, as theycanhelptheattackertodoanattackwithless costforhigherbenefit.Hence,followingthe value-added processes for a cyber attack, based on the literature review and the public available reportsrelatedtocyberthreatintelligence,wecanidentifythevalue-addedactivitiesandbuildthe value chain model for cyber attack. Furthermore, we have validated this value chain framework, as well as the cybercriminal service ecosystem framework in Section 3, with more than 30 senior

executives,managersandresearchers focusingoncybersecurityfromFortune500companiesand key cybersecurity solution providers to improve the framework[4]. To the best of our knowledge,
thisisthefirstcomprehensivevalue-chainmodel,whichintegratesthedifferentcomponentsofthe cyberattacks, to systematically understand cyberattacks from the business perspective. We will detail each componentin the following sections.

2.1 PrimaryActivities:TheAttack

2.1.1 VulnerabilityDiscovery. Logically speaking, cyber-attacks start with vulnerability discov ery which finds the weakness that can be used to intrude into the victim's systems. This weakness may be a zero-day/one-day vulnerability in software/hardware, or a relatively simple password not modified for a long time which is easy to uncover by brute force [111]. Cybersecurity usually involvestechnology,people,andprocess[96].Overlookingstrategic,managerial,andoperational issues related to cybersecurity significantly weakens an organization's defenses against cybercrime [101]. Hence, in this paper, vulnerability refers not only to weaknesses in software or hardware in IT/OTsystems,but alsotoweaknesses foundinprocesses,policy, andthehumancomponentofan organization.

Definition 1: Cyber Vulnerability refers to the cyber-related weaknesses which can be

used by acyberattackertointrudeintotheorganizations,includingtheweaknessinsoftwareorhardware, namedtechnicalvulnerability V_t,andtheweakness intheprocess,policy,andhuman,named operational vulnerability V_p.

Based on this definition, the vulnerabilities detailed in vulnerability databases like National Vulnerbaility Database (NVD) and Securiy Focus BID [76] are considered as the technical vulner abilities in IT/OT systems. Most current vulnerability discovery research focuses heavily on the technical vulnerabilities [30, 61, 153]. However, with the development of the defensive technologies, itbecomesmoredifficultfor anattackertointrude intoatarget's systems throughonlysoftware or hardware vulnerabilities. This means that an organization's vulnerabilities related to process, policy and human aspects are often the "weakest link" in their security schemas and present themselves as opportunities for cybercriminals [144]. The typical cyber attack targeting these weakest links isthesemanticsocialengineeringattackwhichdeceivestheusersinanorganization[143,170]. Furthermore,the cyberthreatfromthe supplychainare increasing [149]. Some recent effortshave attemptedtodetectandunderstandoperationalvulnerabilitiesintheprocessandpolicy[102,119]. For example,the causal analysis based on STAMP (CAST)[93, 119]identified the presence of damning operational vulnerabilities which were exploitedbyhackers andcostTJXover $170 million in losses in the 2007 TJX data breach incident.

*2.1.2 ExploitationDevelopment.*The"ExploitationDevelopment"activitiestrytoexploitthe discovered vulnerabilities, including both the technical and operational vulnerability. Once a technicalvulnerabilityisdiscovered, aprogramcan bedevelopedtoexploitthevulnerabilityand forceasystemto behave inunintendedways sothatacybercriminal cancarryout actions that wouldotherwisenotbepermitted.Inordertoincrease thechancesof successofanattack,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 exploittechnicalvulnerabilitiesandguaranteecontinuedsuccessindisruptingnormalfunctionof the targeted system [38]. Furthermore, a payload [24, 148] could be a malicious program performing

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

asingularfunction,oracombinationofmanyindependentprogramstoofferamorecomplex, comprehensive functionality,whichcanbeusedtoperformmaliciousactions. On the other hand, to perform advanced attacks exploiting an operational vulnerability, some so cial engineer toolkits have been developed[5]. The Social Engineer Toolkit (SET) [127] was specifically designedfortargetedattacksagainst apersonororganizationinapenetrationtest.Manysemantic attack exploits are developed to manipulate the user-computer interface to breach a computer system's security [66]. Developing fake mobile apps that appearto be the same as theirlegitimate counterparts isone typical semantic attacktoexploittheoperational vulnerabilitythat arises from whatwe considerthehumanfactorof anorganization[48].Thebusiness email compromise scams [105], alsoknownas "CEOfraud",is anotherexample inwhichtheattacker counterfeitsamessage fromthe boss to trick someone attheorganizationintowiringfunds tothem.These attacks exploit the operational vulnerability in the organization's financial process and human component, to

develop the persuasive, but fake, message.

*2.1.3 ExploitationDelivery.*Once vulnerabilities are ripe for exploitation,the cybercriminal must deliverthe developed exploitative programs to the victim's cyberspace niche. Based on the delivery medium (physical medium or digital channel) and infected approach (whether needs intermediatehostornot;ifyes,whetherthehostisindividualserverordistributionchannel),there existfourtypicaldeliverymechanisms:

- *PhysicalInfection*.Thisstraightforwardmechanisminvolvesinfectingthevictim'ssystemvia a physical medium, such as hardware or USB; the delivery depends entirely upon physical transportation. The typical observed scenario thatthis mechanismdescribes is virus propa gation: 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 notveryeffective,due tooperationalvulnerabilities,itremains relevant.Anexamplewould be purposefully dropping a USB drive loaded with an exploitative programinside an orga nization's offices, or evenin theparking lot, withthe hope that anemployee maypick it upandplugitintoacomputer,atwhichpointthe company's systems canbe infected.In the supply chain security scenario, the counterfeit hardware or hardware with embedded malware can be distributed to infect the victims [149].
- *Sent Directly*. This mechanism describes sending the exploitative program directly to the victim.Inthis scenario,theprogramswillbeforwardedtothevictim'scyberspaceniche through digital channels, like SMS messages or email. Once the victim is tricked into accepting the exploitative program, such as by opening the fake emails or messages, the exploitation hasbeensuccessfullydeliveredandthevictim's systemwillbeinfected.Oneattackutilizing this mechanism in recent memory is the Ukraine power grid cyberattack. Spear phishing emailscontainingBlackEnergymalwareweresenttothevictims,andthecorporatenetwork was compromisedbyopeningdisguiseddocumentsattachedtotheemails [45].
- *Drive-by-download*. The third mechanism involves redirecting the victim online to reach a websiteloadedwiththeexploitativeprograms,atwhichitisdeliveredtothevictim'ssystem 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 downloaderforthe exploitativeprogramwillbe installedonthevictim'smachine tocontact the command-and-control(C&C) serverandestablishatleastonedownloadchannelto deliverthe exploitative programs to the target's cyberspace niche [22, 138, 169].

[5]Notethat somesocial engineertoolkitsmaynotbedevelopedfor cyber-attacksbutpenetrationtests.However,duetothe neutrality of the toolkits, they can also be used by the black hackers to do cyberattack.

- *Software-Distribution*. This fourth mechanism has been emerging with the rapid development ofthemobile ecosystem.Inthis scenario, anoriginalpieceof software is infectedduring transmission to the user. One typical approach is to add malicious code to the software that requests permissions beyond those required by the original software through repacking [74]. Once theadulteratedsoftware runs,themalicious codewillbe executedandthe exploitative programs will be downloaded to the victim's machine

[62]. With the development of auto updatefeature,thecybercriminalcanalsodynamicallyaddmaliciouscodetoanapplication during runtime, or update an application to include malicious components so that a benign application becomes malicious after a softwareupdate [3, 132].

2.1.4 AttackVictim. Onceavictim'ssystemissuccessfullyinfected,theavenueisopenforattack. For a single-stepattack, once aninitial action bythevictimhas beencarriedout, such asopena file, click on a link,run a program, accept a permissions request, the attack is already completed. For a multi-stepattack,ontheotherhand,theinitialactionbythevictimnotonlyactivatesanimmediate attack, but also opens the doors for subsequent attacks, including identifying further exploitable vulnerabilities.Inthisscenario,theattackerfirstgainsprivilegedaccesstoavictim'ssystemso thattheycanmove freelywithintheotherwiseprivate environment.Onceanattacker successfully intrudesuponasystem,heor shecanaccessandextract sensitiveinformation,rewriteorerase files, and alterthe functionality ofthe system, affecting the system's confidentiality, integrity and availabilityofdata.TooonceagainusetheUkrainepowergridattack[45]asanexample,thehackers usedKillDishtoerase important executable files andcausephysicaldamages to the system. Some attackersmayevenwanttoestablishasustainedpresenceintheirvictims'systemssothatthey may come and go, and do as they please. To study the cyberattack from the value-added perspective, insteadofthedetail cyber attack tricks, we must understand what a cybercriminal can gain froma successful cyberattack, and whatthese gains affordin terms offurther attacks:

- *Digital Gains*.Once inside, anattacker can get all information containedin avictim's system, including sensitive information such as personal profiles, accounts, and intellectual property. Thecompromisedsystemisanother"trophy"foranattackwhilesometimesthehumanwho is tricked by the attacker can prove a "trophy" themselves. One example is when someone canbetrickedtoworkasamoneymuleformoneylaundering[72].Furthermore,theattacker can gain valuable knowledge related to the victim's system, such as operational processes, network configuration, and organizational structure. With an understanding of these aspects of a system, an attacker can better hide further attacks from detection. What made the cyberattack on Bangladesh Bank's (BB) SWIFT payments system in February, 2016 [152] so hidden and damaging was the attacker's understanding of the bank's transaction confirmation process: the attacker was able to intercept confirmation messages and cover up fraudulent transactions. Attacks to the CIA [179], NSA [60], Hacking Team [68] etc. can offer attackers 0-day vulnerabilities, exploitations, and many tools developed and customized by these professionalorganizationsthatexpandandstrengthentheirarsenal.
- *Psychological Gains*. The attacker who carries out attacks seeking the inherent satisfaction of success orforthe fun or challenge oftheprocess gains psychological benefits froman attack [85].Inthisparticularlytwistedcase,theattackisperceivedasmerelya test ofhackingskills, and the successful attack carries with it not only a sense of accomplishmentforthe attacker, but also reputation in the hacker community. Some attackers may seek vengeance against a symbolic enemy, or see cybercrime as a way tofurtherpolitical agendas.TheAnonymous is onesuchgroup,whichattackedFreedomHostingII,aservicethathosts20%ofdarkweb websites, 50%ofwhichcontainedchildpornographyinsome forms [18].

- *Loss-based Monetary Gains*. A successful attack can interrupt the business continuity of an organization by adversely affecting the confidentiality, integrity and availability of certain systems. This results in a direct monetary cost to an organization in the form of losses ordamages,but alsoinindirect costs suchas lossoftrustbycustomers,missedbusiness opportunities and increased defense costs for prevention, protection, detection, and recovery in response to the cyberattack [10]. The attacker can benefit by monetizing the victim's loss forthemselves.The typical scenariois thatthe attackerdraws fundsdirectlyfroma victim's accounts. A more eye-catching scenario with a recent surge in popularity involves the attacker proving his or her capability to interrupt the victim's business continuity and requesting money in return for not capitalizing on their abilities, effectively holding a business hostage for a ransom. The ransomware attacks of 2016 [120] are such examples and 88% of these attacks targeted hospitals and health systems, since cybercriminals correctly perceived theseorganizationsasmorevulnerableandreceptivetothreatsandeagertosatisfyaransom to avoid damage.

2.2 Support Activities: Facilitate the Attack

To supplement the primary activities discussed above, we see an emergence of what can be consideredas support activities inthe cybercrime ecosystemtomake cyber-attacksmore efficient: *greater benefit with less cost*.

2.2.1 Operations: Attack Life-cycle Management. A cybercrime operation, like a legitimatebusi ness [161][6], must actively manage and support the cyberattack life-cycle to reduce costs, increase profits, and mitigate risk. In addition, cybercrime operations must also make conscious efforts to avoid being identified, and its operatives punished underthe law. Tomeet these criteria, a cyber criminalwithinagreateroperationmust selectthevaluable attacktargets,decidehowtoorganize hackers (if more than one) to carry out primary cybercrime activities, manage the distribution of proceeds (payroll if you will) hide the operation from authorities, and if disrupted, recover the sidelined operation.

Definition 2:Cyberattack Operations referto the activities that manage and support primary activities to gain higher benefit with less costfromthe cyberattack. These include target selection, hackerorganization,benefitrealization,andresistanceoperation.

- *Target Selection: what arethe characteristicsthat make a valuabletarget?*

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

- **Ease of the attack** P_e. If hackers don't have a specific objective, they may take on an exploratory mindset to probe various targets, and identify those with sufficient weaknesses to be consideredforafull-scale cyberattack.Inthis scenario,themore easilyvulnerabilities can bediscoveredandexploitedin a certain organization's systems,the more attractive a target the organizationbecomes.Evenif a specific targethasbeenselected,the cybercriminals may take on an exploitation mindset to dig into the target's systems and attempt an attack;

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

however,ifbreakingintothecurrenttarget'ssystemsprovestoodifficult,andafterafew days or weeks no progress is made, the target can be abandoned in favour of anothertarget identifiedintheexploratoryphase.

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, orthe attacker can attempttoseekmoneydirectlyfromthevictimoftheattack.Theattackermayalsoexperience psychological gains. These encompass the two main categories with which we can understand the benefit to cybercriminals in the wake of a successful cyberattack: the monetary benefit B_{pm} andthepsychologicalbenefitB_{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: $B_e = P_e B_{pm} + B_{pp} E_r$.

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

PsychologicalCostsC_{ps}.Costsofthisnature refertothepsychological andmental energy expendedincommitting a cyberattack.These couldinclude the fear of being caught, or punishment.

Expected Penalty Costs C_p. This cost captures to the monetary opportunity costs of con viction if the attackers, which become real if the cybercriminals happen to be arrested and convicted following the attack. Straightforwardly, it is proportional to the arrestrate P_a for the particular kind of cyberattack, the ease ofthe judicial process involved in the conviction P_c and the monetary opportunity costifthe attackeris convictedC_c.$C_p = P_a P_c C_c$.

Operational Costs C_o refers to the cost to carry out the cyberattack. The investment cost C_{im} captures the up-front costs forthe cybercriminal to perform the attack, which could be rentingaserver,buyingorlearninganynecessarytoolsor services, andtheopportunitycost ofthetime takeninsearchingforvaluabletargets.Themonetaryopportunitycostofthe investment C_{om} in cyberattack should be also considered. Hence $C_o = C_{im} + C_{om}$.

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

Definition3:CyberattackTargetSelectionRule Forarationalcyber-attacker,thevictimorganization could be considered as a targetif andonly ifthe 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 in high level. They can help us to understand the values of different activities forthe cyberattack. Any activity that can reduce the expected cost or increase the expectedbenefitwillbehighlyvaluable inthe cybercrime ecosystem.Understanding this operation can shed lights into the decision-making forthe attackers.

· *Hacker Organization: how do cybercriminals collaborate with each otherfor an attack?* For an attack to be successful, especially for the organized cyberattack which involves multiple hackers, the cybercriminal in the executive role must organize his or herteam forthe attack. Typically, there exist the following six basic types of organization structures [110]:

- A*Swarm*refers to a group of hackers who work togetherin viralforms that have a minimal, if not nonexistent, chain of command;

- A*Hub* refers to the structuring scheme in whichthere is a core groupof hackers around whichperipheralassociatesgather;
- A*ClusteredHybrid* structure combinesonline andoffline activity, andtypicallyoperates ina similar way as *Hub*,focusing on specific activities or methods;
- An *Extended Hybrid* structure is like the *Clustered Hybrid* structure, but incorporates many associatesandsubgroupswhileretainingalevelof coordinationsufficienttoensurethe successofoperations;
- *Hierarchies*refertostructure reminiscentoftraditionalorganizationsaswellas criminal groups, buttake advantage of online technology to facilitate activities;
- An*Aggregate* structurereferstoalooselyorganizedgroupofhackerscommittedonlyto temporary collaboration, andoftenwithout a cleargoal.

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 importantroles in the collaboration between cybercrimals [121], online forums are servingasoffender convergence settings for cybercriminals andshapingamore fluid and flat structure so that all participants are able to get into contact with each other[91]. Furthermore, in online hackerforums, most hackers are novices with only a few more highly skilled hackers participating in forum activity [70, 94, 97] and this community forms the core and peripheral *Hubs*.

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

It is within the executive's responsibilities to maximize the benefit to be gained from a successful attack. Considering monetary benefit as an example, the executive may hire a

money laundering network so that the source of "dirty" money cannot be identified.Recently,researchers have presented the concept of "DDoSCoin", which allows a cybercriminal to prove their own participation inaDDoSattackbyhavingminers create a largenumberof connections toagiventarget andusing the target server's signed responses as a proof to receive the digital monetary rewards that they deserve [181]. Digital currency, especially Bitcoin, has become the main approach for cybercriminals to transfer monetary gains to one anotherin the wake of a successful attack [84]. Though the motivationfortheWannaCryHurricane attackonMay2017is still amystery,there isatheory that it is for currency manipulation to raise the Bitcoin value by increasing number of users [172]. Additionally, many markets or forums are constructed for cybercriminals to trade their digital gains fromsuccessfulattacks [33,130,157,186].Accordingtothetrackingofransomwarepayments [130],95%ofthetracedransomscashedoutviaBTC-E,adigitalcurrencytradingplatformand exchange. Forpsychological benefit, a "Hall ofFame" ofhackerswith thegreatestreputations can motivate cybercriminals to continue participating in attacks within the cybercrime ecosystem, consideringthevalueplacedonreputationandtrustforcybercriminalcommunity[44,69,91,183].

· *ResistanceOperation: how to skirt detection and recoverfrom a take-down?*

Straightforwardly, hackers do not want to be identified or have their attack detected. Common methods that aimto accomplishthis include employing aproxyserverto bounceonline activities, using anonymous tools such as a Tor network[8, 41, 109], clearing event logs, command history, andshreddinghistoryfiles.Toincreasethechanceofsuccessofacyberattacktheexecutivecan 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 acrossnetworkboundaries [122, 138].

Parts of the cybercrime ecosystem can be taken down by law enforcement, therefore, a plan for recoveryisextremelyvaluableforcybercriminals.Forexample,theRamnitbotnetthatinfected3.2 million computers was taken down in February 2015 only to quickly re-emerge and attack banks ande-commerceoperationsinCanada,Australia,theUnitedStates,andFinlandinDecember2015 [81]; someofRamnit's infrastructure survivedfromthe take-downanditsoperatorswerenot arrested.Additionally,itisbelievedthatthecybercriminalsacquiredthewebinjectionmechanism fromaseparategroupthatprovideswebinjectionsasaservice,makingRamnitevenmoreresilient.

*2.2.2 HumanResource:HackerCommunity.*Asdiscussedabove,thehackerforumis themost common form of communication forthe cybercriminal community. A hierarchical structure has lower coordination costs than a pure market structure, so most hackerforums have adopted hierarchicalmanagement systems consistingof administrators,moderators,reviewers,reviewed vendors, and general members to stratify, and organize the community [183]. There is a limited number of highly skilled hackers [94] and the cybercriminal tends to build a collegial culture that encourages sharing of information and values innovation [70]. Since most hackers are novices, part of the value-added activity forthe hacker community is training the novices. Note that both the offensive anddefensive sidesof cybercrime are leveragingthe same innovations [42], and hackers canlearnskills throughonline cybersecurityforumsor evenviaYouTubevideos.The near-termadvances inmachine learning, automationandartificialintelligence canalsobeusedby the criminals and nation-state adversaries [42] while the attacker may

even have the advantage inskill,asthe“worstisgettingworsefaster”[99].Somehackercommunitieswilloffertraining programs to train fledgling cybercriminals. For example, the Anonymous launched an online school calledOnionIRC allowingmembers to share technical skills andmaintain anonymity[52].

Togrowthehackercommunity,recruitingisanimportantactivityforthecybercrimeecosystem. To achieve this goal, many tutorials are available to reduce the barriers forthe novices to join the hacker community and benefit from the cyberattack. According to the research from Digital Shadows,theprocesshackersusetorecruitnewhiresisthemirrortoitslegitimatecounterpart [135]: post advertisements on forums, hacker-specific job boards, social networks to reach fresh talents, qualify candidates by application forms or even through the interviews, and maintain a time sensitivemembership.Thestudyofthe18investigationsintocriminalnetworks[90]demonstrates thattherelationshipsbasedonreal-worldsocialnetworksplaysanimportantroleintheoriginand growthofthemajorityofnetworkswhile theaccess toonline forums canincrease the criminal capabilities quickly. Forthe nation-supportedcyber-attacks,the recruiters may even hire hackers withspecific experiences fromthe criminalunderworld[154].

2.2.3 Marketing and Delivery. As discussed above, a marketplace for attackers to trade the digital gains from a cyberattack is the principal way for attackers to realize the benefit from successful cyber-attacks. Today, we can observe many different dark web marketplaces available for differentkindsofgoodsandservices:vulnerabilityandexploitation[5,76,125],dumps,skimmers, identities, attack tools andmules [186], credit card[65],fake tools [162] andBitcoin [130] etc. Some marketplacesevenallowcybercriminals tooperate“single-vendor stores”,inthe samewayasone could do on Amazon, eBay, or Taobao, where sellers willrun their own online website to selltheir products to their clients [65].

Sincethereexistmanydifferentdigitalgoodsandservicesinthemarketplace,determining thepriceofagoodisatypicalvalue-addedtaskforthehackers.Itisnosurprisethatazero-day vulnerabilitywillbemuchmorevaluable thanaone-dayvulnerability.Theone-dayvulnerability is still valuable because ofthe observed patch delay in practice [79]. Additionally,the going price changes based on supply and demand in the market. For example, in May 2016, due to the shutdown of Angler, the demand for Neutrino increased so much that the developer doubled the price per month from $3500 to $7000 [28].

Concerns about anonymitytranslate touncertaintyrelatedtoproductqualityinthehacker community [67, 183]. To mitigate this problem, trust and reputation plays a fundamental role in thecybercrimeecosystem[91].Anyactivitythatacybercriminalcanundertaketoshowthathe orsheistrustworthy,ortobolsterhisorherreputationisextremelyvaluable.Itisimportantfor the cybercriminal to make sure a potential trading partneris not in fact law enforcement; the take-down of Shadowcrew is a “painful” example of such a situation in hacker community [55].

Someforumsareopenexclusivelytowell-vetteduser sandoftenrequireafeetojoin,andother forums are invite-only [183] while some forumsmay evenrequestthe members “musthack a website within 3 months” to maintain the membership [135]. Some guarantors will offer vetting services to check a prospective user’s background, contributions, and trustworthiness [56]. Like the legitimate e-commence sites such as eBay and Amazon, some forums offer a rating system so that members canrate each other andevaluate

apotentialtraders'reputation.Due totheprevalenceof "rippers"whotradedishonestlybydouble selling, somemarketplaces, suchas credit cardforums, have introduced a review mechanism to review prospective vendors' goods and/or services and assigna"reviewedvendor" tagasanapprovalofqualityif avendorpasses the review[67];ifa reviewedvendoris foundtohave tradeddishonestly,thatvendorwillfacepunishment[183].

Cybercriminalsareleveraginginnovationstomaketheirproductsandservicesmoreattractive, trustworthy, and more easily delivered. For example, shifting to the "as-a-service" model has been a significanttrend in recent years [104]. These services are becoming easier and more user-friendly, whichsignificantlyincrease the resilienceof cyber-attacks.The innovations inservice alsomake it easierforacybercriminaltorealizethebenefitfromacyberattackandsignificantlyreduceexpected costs as the cybercriminal can operate evenfurtherunderground.

*2.2.4 TechnicalSupport.*Cybercrimereliesheavilyonthetechnical support.Asdiscussedabove, the offensive and defensive sides use similarinnovations [42]. Many technologies developed for "good"purposeshavebeencooptedbycybercriminals forlessthanpositiveends.The firstbotIRC wasinventedin1988,andthefirstmaliciousbotappeared10yearslater[173].Theanonymous communication network technology Onion Routing (Tor) and the Invisible Internet Project (I2P) weredevelopedtoprotectprivacyonline[8,37],andtheBitcoin,apeer-to-peerelectroniccash system,wasdevelopedtoallowanytwowillingpartiestotransactdirectlywitheachotherwithout the need for a third party [117]. Now these technologies have become the "cornerstones" for the cybercriminal ecosystem.

Additionally, the well-known tools such as *Application Specific Scanners, Debuggers, Encryption Tools, Firewalls, Forensics, Fuzzers, Intrusion Detection Systems, Multi-Purpose Tools, Packet Crafting Tools, Packet Sniffers, PasswordCrackers, Port Scanners, Linux Hacking Distros,Rootkit Detectors, Traffic Monitoring Tools, Vulnerability Exploitation Tools, Vulnerability Scanners, WebBrowserRelated Tools,WebProxies,WebVulnerabilityScanners andWirelessHackingTools*areusedbybothcyber criminals 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 moni toring host or service uptime, which is also widely used by attackers to intrude into the victim's network. Furthermore, many toolsdevelopedor customizedby theprofessional organizations or experts, even by the state-supported agencies like CIA [179] or NSA [60], may be taken and used tostrengthencybercriminal'sarsenal.

2.3 Cyberattack Ecosystem: Combination of Primary Activities and Support Activities

Hence,the cyberattackecosystemconsistsnotonlyoftheprimaryactivitiesdirectlyrelatedto a cyberattack, but also of the support activities that facilitate a cyberattack by reducing costs and increasing benefits. In addition to technical vulnerabilities, attackers also target operational vulnerabilities, the weaknesses related to the processes, policies, and humans in an organization. However, most current vulnerability discovery research focuses on the technical vulnerabilities. Operational vulnerability is often overlooked. Cyberattack operation activities, including target se lection, hacker organization, benefit realization, and resistance measures, can significantly improve

attackers'performanceinthedigital,psychological,andmonetarygains.Thehackercommunityis growing in both skill and scale to offer human resources for cyber-attacks, and the marketing and delivery activities further facilitate the benefit realization for cyberattack operation. The cyberattack ecosystem is already embedded in a comprehensive value chain. In orderto combat the modern cyberattackeffectively, beside theprimary attack activities,thedefensive community shouldalso payspecialattentiontotheseemergingvalue-addedactivities.

3 CYBERCRIMINAL SERVICE ECOSYSTEM: BUSINESS RECONSTRUCTION With the development of service science [89], cybercrime as a service (CaaS) has become an importanttrendforthecybercriminalecosystem[104,142,155].This innovationnotonlyputs cybercriminaltools and services in the hands of a widerrange ofthreat actors, but it also turns the cyberattack into a business that can provide a living for a career cybercriminal [2]. Furthermore, it restructures cybercrime activities and drives attackers even deeper underground, as activities related to cybercrime can now be offered as independent, modular components in a cybercrime supply chain with attackers benefiting fromeach component.In this section,following the value added processes discussed in Section 2, we will identify the relevant cyberattack services[7],to construct a systematic framework forthe cybercrime ecosystem,developing anunderstanding of the business and the evolution of cyberattack itself.

3.1 Service Model: Business Components for Cyberattack

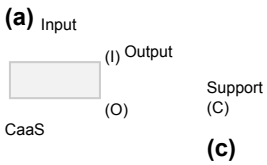
A cyberattack service provider can advertise a CaaS offering specific modules related to a cyber attack on the marketplace to reach as many potential users as possible. A buyer can purchase anyneededservices onamarketplace to builda cyberattack fromscratch, or canintegrate the purchasedservicesintohisorherownoperation,becomingaserviceprovider.As showninFigure 2,tobuildthe systematic frameworkforthe cybercriminal ecosystem, basedonthe STAMPmodel [119, 141],wedefine eachservice as thevalue-addedactivitythattakes some inputs, andproduces anoutputusingthe supporttools andtechniques:

Definition 4: Cybercrime Service refers to a value-added activity related to a cyberattack that takes input andproducesoutputusingthe supporttoolsandtechniques:

$$O = CS(I, C) \quad (2)$$

where Irefers to the input setforthe service,Orefers to the output setforthe service, while C refers tothe techniquesortools that supportor enable this service.Note thatthe input,output or support are not necessarily a single-element set, and could be a multi-element, meaning that itinvolvesdifferenttypes ofvariables, or evenanempty set if no variable isnecessary forthe given parameters.

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



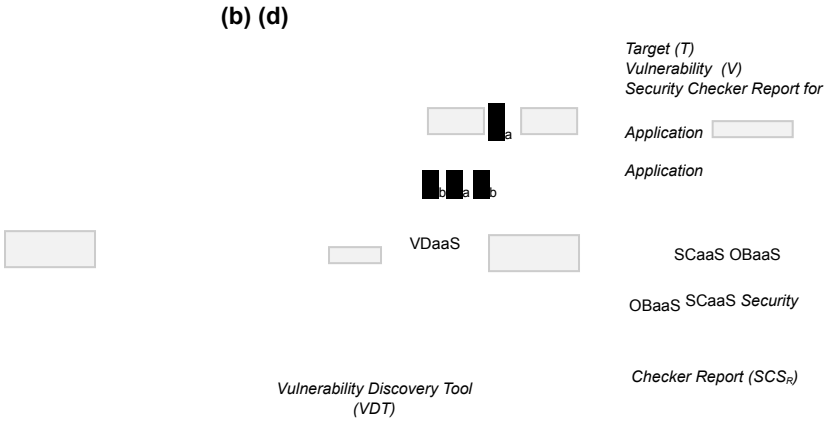


Fig. 2. Cybercriminal ServiceModel.(a) Each cybercrime value-added activity can bemodelled asthe service which takes input and produces output using supportive tools or techniques. (b) Two services form the composition based on their dependencies, further constructing a loop, simplified as a double arrow for convenience. (c) Taking the vulnerability discovery as an example, given the a target, using the vulnerability discoverytools,thiscomponentidentifiestherelatedvulnerabilitiesastheoutput.(d)Taking theobfuscation and the security checker components as examples, the obfuscation component (OBaaS) uses the service checkercomponent(SCaaS)tochecktheobfuscation'seffectiveness.Itcancontinuouslyinvolvethesecurity checker untilthe security check report(SCS_R)showsthatthe application can bypassthe security software.

In the "as-a-Service" model, a cyber-attacker can concentrate on a particular value-added activity in the cybercriminal ecosystem, becoming an expert and driving the *"specialization"* forthe 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 executeasuccessful cyberattack,acyberattackexecutivemaycombinerelatedservicessothat they *"cooperate"* in performing more complex tasks to improve the performance of a cyberattack. Basedon thedefinition above, ifthe output set of a serviceCS_a intersects with the input or support of another serviceCS_b,thenthere will exist avalue-addingpathfromCS_a toCS_b andthese two servicescancollaboratewitheachothertoformacompositionandlendanadvantageinperforming complexattackactivities.

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

Note thatthe output set oftheprevious service don't needto be equalto the input or support of the next service. Once there exist some intersections, then they can collaborate with each otherto generate added value.

Hence, with the adoption ofthe "as-a-Service" modelfor cybercrime,*specialization, commercial ization, and cooperation* in the cybercriminal ecosystem form the crux of the cybercrime business.

Inthefollowingsections,basedonthevaluechainmodelpresentedinSection2andtheservice model discussed above, we will formally identify the unique cybercriminal services, including thoseSystematic Thinking of Cyber Attack Business 1:15

directly related to the primary activities and those indirectly supporting a cyberattack, and how they collaborate with each otherforthe cyberattack.

In this paper, we are focusing on the added value and the business in the cybercriminal ecosystem, sothetechnicaldetails,orcyberattacktricks,asdiscussedinmanystudieslike[15,25,26,29,132,160, 165], are out of scope.Weconsiderthe attack service as a "black box" because in the cybercriminal service ecosystem,the buyers don't needto understandthe details ofthe services theypurchase.

3.2 CybercrimeServicesDirectlyRelatedtoPrimaryActivities

Thecybercrimeservicesdirectlyrelatedtoprimaryactivitiesconsistoftheservicesfortheprimary activities, and the related supportive activities to overcome the defensive efforts and to improve thecyberattackperformance.

3.2.1 Vulnerability Discovery as a Service (VDaaS). For the vulnerability discovery service, giventhetargetas theinput,withthesupportfromthevulnerabilitydiscoverytools,potential vulnerabilities ofthe target are identifiedandreturnedasoutputs.WedefineVDaaS as follows:

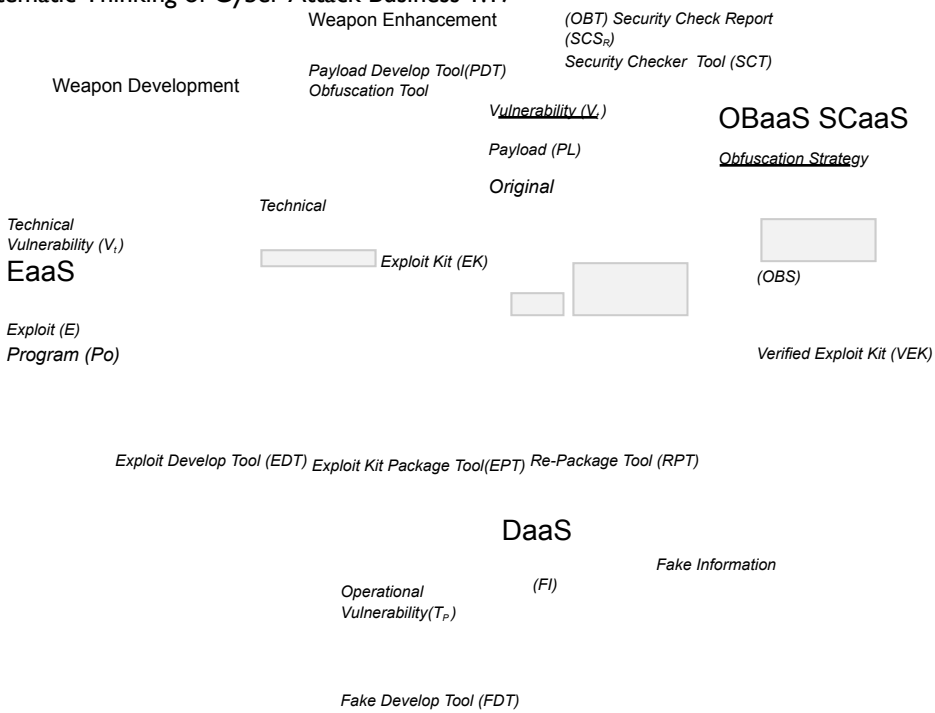
$$V = VDaaS(T, VDT) \quad (3)$$

whereTisthetarget,whichcanbetheinformationsystemoranemployeeinaspecificorganization, oraspecificinformationproductserieslikeWindow10operationsystem.Vreferstothediscovered vulnerabilities related to the given target T, including technical vulnerability V_t and operational vulnerabilityV_p. VDTrefers to the vulnerabilitydiscovery tools such asMetasploit,Wireshark, or W3af. Note that the more specific the given target is, the more targeted the cyberattack based on thediscoveredvulnerabilitycanbe.

Itisnot a surprise thatintheundergroundcybercrime ecosystem,hackers trade theirdiscovery directly in the dark web [5]. However, vulnerability discovery is a non-trivial, time consuming, uncertain,buthighlyvaluable task,Googleevenlaunchedavulnerabilityresearchgranttoreward *"security researchersthatlook into thesecurity ofGoogleproducts and serviceseveninthe casewhenno vulnerabilities are found"* [57]. Hence it is rare to observe the independent vulnerability discovery servicesinthecybercriminalecosystem.Onlysomehighlyskilfulhackers,especiallytheorganized cybercrime hackers, can offer services to help the clients, who could be nation-support agencies like FBI,to identify the vulnerability inthe target system.Giventhe success ofthe bug bounty programs [75,103, 185],whereorganizationsrewardexternalexpertswhodiscovervulnerabilities intheir systemsandpatchthembefore theyarepubliclydisclosed,itisverypossible thatdeep in the dark web there will exist offensive-versions of "bug bounty programs" where a platform isofferedtotakeadvantageofthehackercommunitytodigthevulnerabilityforagiventarget. Considering the menacing targetedcyber attacks, aka advancedpersistentthreat(APT)[156],this VDaaS as the offensive bug bounty programs is very likely to be reality, if not exist yet, in the cybercriminal ecosystem.

*3.2.2 ExploitationDevelopmentService(EKaaS).*Anexploitisaprogramthattakesadvantage 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 theirtrue functionality. Additionally, exploit kits can integrate additional payloads to bolster an attack on potential targets. For the *operational vulnerability*, the attacker can deploy the fakeWiFi, website, software, message or email to exploit the discovered operational weaknesses. Hence,the exploitdevelopment service is the service that convertsdiscoveredvulnerabilities into

effectivecyberattackweaponswiththesupportofdevelopmenttools.Thisprocessisdescribedby



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

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

the relationship below.

$$\text{VEK} = EKaaS(\text{V},\text{EKDT}) \quad (4)$$

whereVreferstothediscoveredvulnerabilities,includingtechnical$V_t$andoperation$V_p$vulnerability; VEK refers to the verified exploit kits, the cyberattack weapons which can be delivered to the target; EKDTrefers to the toolsusedto supportthe exploitationdevelopment process.

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

.

ExploitasaService(EaaS).GiventhediscoveredtechnicalvulnerabilityV_t,theexploitEis dev

eloped with the support ofthe exploit development tool set EDT.We can model EaaS as:

$$E = EaaS(V_t, EDT) \quad (5)$$

Normally, when the vulnerability is discovered, the proof-of-concept trial is also developed to demonstrate its practicality.Wecan explore many verified exploitations in ExploitDB [40].While responsiblevulnerabilitydisclosurepolicyensures the releaseof apatchbeforeanydetailsof the vulnerabilityarepubliclyrevealed,itispossible forthehackers to automaticallydevelop the exploitation[13]orreverse-engine thepatchwithoutthe relevantdetails [20].Thoughthe automatic exploitation generation is fairly basic now [153], it is not surprise to observe new tools

tosupportthishighlyvaluableactivity.

Exploit Package as a Service (EPaaS). Given a collection of exploits E, EPaaS combines them the exploitkitEKthatispotentiallymore effective thananyindividual exploit onitsown.An unintelligent exploitkit, one thatdelivers allits exploits at once regardlessofthe conditions inthe

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 whendelivering an exploit[56].In most exploit kits,the exploitativeprograms and strategies are hard-coded, but this may not be the case forlong; exploit kits can be developed insuchawaytoenabledynamicupdatesas conditions change.Considerthe followingdefinition:

$$EK = EPaaS(E, EPT) \quad (6)$$

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

DeceptionasaService(DaaS).GiventheoperationalvulnerabilityV_p,withthesupportof the developmenttoolsFDT,this componentgenerates the fake informationFI,like a fakewebsite [95, 178],fake emails [66, 124], orfake software [162] which can be delivered to the target. ADaaS is defined as follows:

$$FI = DaaS(V_p, FDT) \quad (7)$$

NotethatiftheV$_p$ containsdetailinformationaboutthespecifictarget,likeorganizationstructure, business process, network environment is available, the attack is referred as targeted attack [155], and normally it will have a higher probability of success. For example, for the whaling phishing attack in early 2016, employee payroll information was successfully stolen when an employee voluntarily gave it away in an email to whom he thought to be the company's CEO [112].

Payload as a Service (PLaaS). This component offers thepayloads PL involved in a cyber attack.Apayload[24,46,148] canrefertoanatomicmaliciousprogramperformingasingular function, or a combination of many independent ones to offer a more complex, comprehensive functionality.PLaaSisdefinedintermsofthe followingrelationship:

$$PL = PLaaS(V_t, PDT) \quad (8)$$

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

ObfuscateasaService(OBaaS).Givenanapplication,suchasexploit*E*, exploitkit*EK*,fake information *FI*, payload*PL*, this componentuses various obfuscation strategies andtechnologies such as packers, polymorphism and metamorphism to reduce the chance that an application is detected by antivirus software [59, 122, 145]. For example, the Qimplementation [146, 153] can be usedtohardenthe exploitsgeneratedbytheEaaS. Somemayinclude securitysoftware toconfirm the effectiveness of the obfuscation [56]. Wedefine OBaaD in terms of the following relationship:

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

where$A_I$refers tothe input application, suchas apayload, exploitkit, exploit,orfake information whileA_O referstotheoutputapplicationwithobfuscationmethodsapplied;OBTreferstothe obfuscation tools and strategies; 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 bypassthedefensivebarrierfromacertainsecuritysoftwareorplatform[59].Ifanapplication isdetectedbya securitysoftware,theOBaaScomponent canupdate theobfuscationstrategyuntil the application goesundetected,resulting in a loopbetween theOBaaS andSCaaS.

$$SCS_R = SCaaS(A_I, SCT) \quad (10)$$

where$A_I$refers tothe input applicationfromOBaaSandSCS_R refers tothe reportfromthe

security checker tool set SCT. For example, cybercriminals once used Google's VirusTotal platform to verify the effectiveness of malware [184].Itis believed thatforthe Ukrainian power grid attack,the attacker built a simulated power grid system similarto the Ukrainian power grid plant that they were able to evaluate and testthe developed firmware priorto the attack [45]. As shown in Figure 2 (d),OBaaS andSCaaS canforma loopto guarantee the effectivenessofthedevelopedcyber

weapons.Giventhehighvalueforthisloop,itisnotsurprisetoobservetheseplatforms,which may even be operated similarly to the mobile app testing cloud [53] forthe mobile ecosystem.

.

Repackage as aService (RPaaS). Given a list ofinputs,this component packages the elements of

theinputinaverifiedexploitkittoincreasetheeffectivenessofanattack,withsupportfrom obfuscation component, OBaaS, and repackaging tools. We define RPaaS as: VEK = *RPaaS*

$$(A_I,\{RPT,OBS\}) \quad (11)$$

where A_I refers to the input which can be the payload PL from PLaaS, exploit kit EK from EPaaS,

fakeinformationFIfromDaaS,theoriginalbenignapplication$P_o$ortheircombinations;VEKrefer s totheapplicationthatwillbedeliveredtothetargetforcyberattack;RPTreferstotherepackaging toolsandstrategiestoenhancetheinput.Thiscomponentplaysimportantroleforthecyberattack. Taking the playload development as an example. Since a payload may be identified by security software, hackers willrevisedetectedpayloads using the repackage component so thatthey may bypass detection on subsequent attacks [24]. This iterative process creates a so-called "family" of payloads [24, 166].Tocircumventdetectionmore effectively, an advancedpayloadprotects itself through redundant actions and encryption [122]. The malware "DenDroid" is even capable of detecting emulatedenvironments such asGoogleBouncer[164] andtheWannaCry malware can detect whetherthe running environments are sandboxes [137]. This dynamic awareness is what sets apartintelligent cyber weapons fromtheirless sophisticatedcounterparts. Forthe exploit kit fromEPaaS,theautomatedshellcodeplacementmethodsaredevelopedtogeneratethemodified exploitbychanging orreplacingtheoriginal shellcode ofthe existingexploitfornewattacks [15].

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

BasedonFigure3,variouswayscanbeobservedthatexploitationservicescanbecombined.For a given cyberattack, at least one of the "weapon development" activities will be employed while the "weapon enhancement" componentisnot a must. However,themore services an attacker can effectivelyemploy,thehigherthe chanceof success inanattackwhenapplyingthegenerated 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

differentphasesofamulti-stepattack.Forexample,intheUkrainepowergridcyberattack[45],the spear-fishing emails from DaaS (fake information), the exploit kit targeting vulnerabilities including CVE-2014-4114, CVE-2010-3333 from EPaaS (exploit kit), the KillDisk, a destructive data-wiping utility and the SSH backdoor to maintain persistent access from PLaaS (payload), were used in tandemtosuccessfullybreakintotheUkrainianpowergridsystem.Inthe secondstepofthe 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 uploadedto the systemandto attack the ICS components.

3.2.3 Exploitation Delivery Service (EDaaS). As shown in Figure 4, the purpose of these activities istodelivertheexploitativeprograms*VEK*fromEKaaStothe targetedsystems.Effectively,EDaaS serves as a pipeline forthe cybercrime ecosystem, consisting ofthe following components:

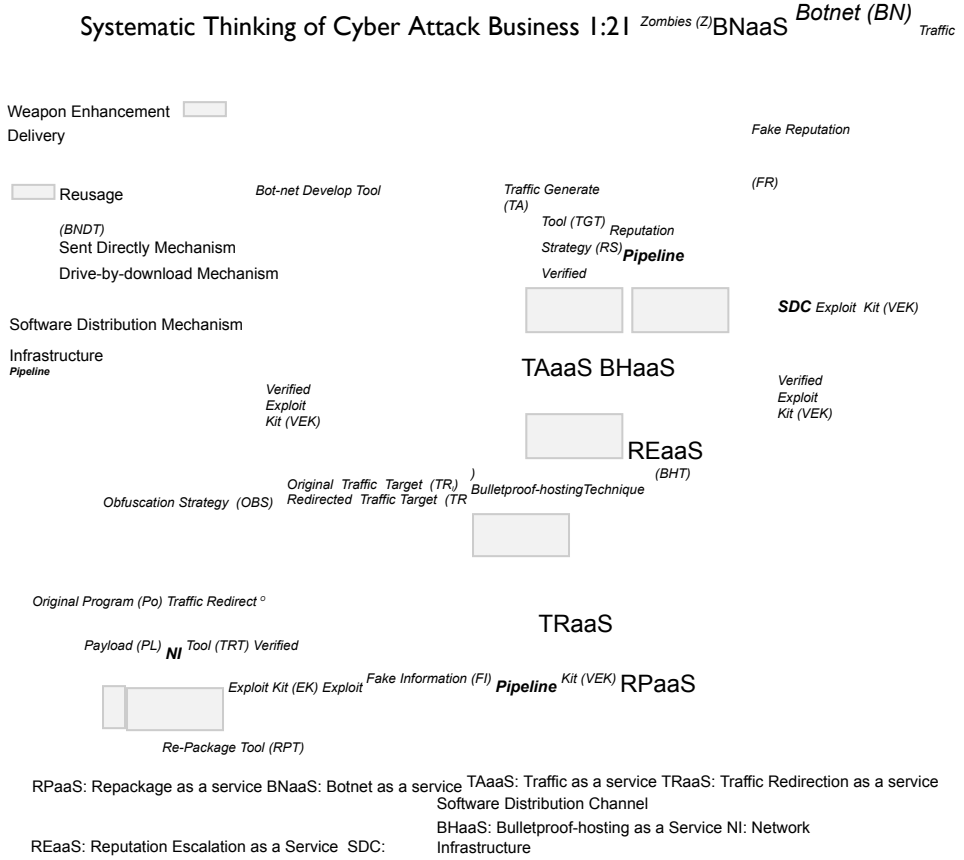


Fig. 4. Exploitation Delivery Services. "Delivery" refers to the services serving to support the exploitation delivery. "Reusage" refers to the services repurposing gains from previous successful attack."Infrastructure" refers to the network infrastructures which are operated by network infrastructure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

Botnet as aService (BNaaS).Aspresentedin [136], given a list of compromisedmachines, ·

calledzombies, adeveloper canuse tools, suchasZeus andAldi,toimplement aBotnetthatis 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,andfast-fluxnetworktomaintainandupdateabotnet.Wecanformallydefinethebotnet servicecomponentas follows:

$$BN = BNaaS(Z, BNDT) \quad (12)$$

whereZrefers toasetof zombiemachines,BNrefers tothebotnets,BNDTis the tool settodevelop and maintain the botnet [136].

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

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

whereTR$_I$refers to the originaltraffic target, and TR$_O$ refers to the redirected traffic target,TRTis the traffic redirection technique [54, 168] and BN can be used to construct a fast-flux network to supporttraffic redirection[71].

Bulletproof Hosting as a Service (BHaaS). Bulletproof hosting services, such asRussian BusinessNetwork,McColo,Troyak,andVline[83],arealotmorelenientaboutthecontentshosted on their servers so that the attackers can host any kind of materials on them without worry about being taken down: the service provider must make the servers harder to seize and be inconspicuous enough to avoid calling the attention of authorities [106]. Furthermore, the providers intend to

hosttheseversincountrieswithmorerelaxedlawstomakeiteasiertoevadelawenforcement [17]. Supporting by the botnet, some providers will hire the compromised servers out until they are discovered [106]. This kind of service is used by cybercriminals as the "gang's hideout" and is widelyavailable intheundergroundmarketdue toitsemphasisonanonymity.

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

whereBHT refers to the tools and strategies that protectthe servers, such as locatedoffshore, moving among different service providers, registering and dropping network blocks frequently [7], making them "bulletproof".

.

Traffic as a Service (TAaaS). This component may use many servers or sources, typically the

botnet BN, to generate the traffic forthe given target. One typical scenario is the well-known DDoS attack [80] which flood the bandwidth orresources of the targeted system, usually one or more web servers, with traffic from multiple compromised systems. For example, on October 21, 2016,abotnetconsistingoftensofmillionsofInternet-connecteddevicesinfectedbyMiraiflooded Dyn's servers,resultingin11hoursofblockedaccess topopularwebsites suchasTwitter,Spotify, Netflix,Amazon,Tumblr,Reddit, andPaypal, among others [16].Anothertypical application for this componentis in an advertising fraud scheme, in which fake traffic generates vast amounts of undeserved revenue [50]. We formally define TAaaS in terms of the following relationship:

$$TA = TAaaS(BN, TGT) \quad (15)$$

.

inc

Reputation Escalation as a Service (REaaS). For the "software distribution" mechanism, to r ease the exposure of the malicious applications, this component will exploit the vulnerabilityof the currentrecommendationsystem[151]tocraft a fake reputation[182]forthegivenapplication, forexample,downloadingthesoftwareandpostingfictitiouspositiveratingsandreviews.

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

where$A_I$refers tothegivenmalicious applications andTArefers tothe trafficusedtogenerate the fake reputation FR;RS refers to mechanisms to establish reputation on a given platform.

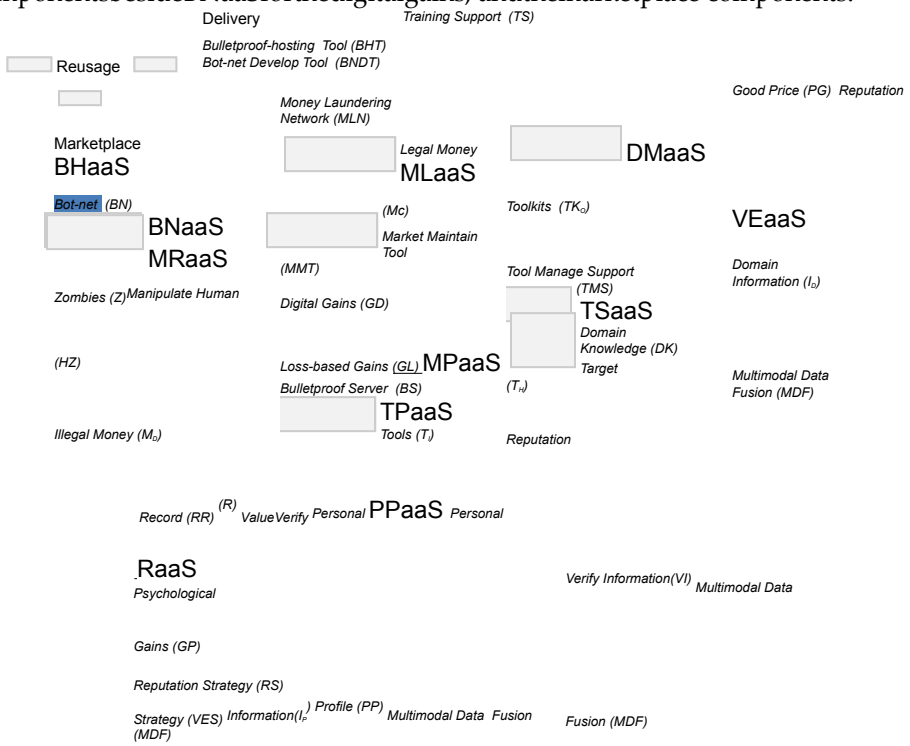
3.2.4 Multi-stepAttackService(AaaS). Once a target's systems are compromised,the avenue for attack is open and cybercriminals make their entrance seeking benefits ofthe following forms: digital gains (GD) including intellectual property, sensitive information, domain knowledge, com promised machines,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

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

Untilnow,wehaveexploredthevalue-addedprocessesoftheprimaryactivitiesandthedirectly related supportive services, behind a cyberattack. In the following sections, we will discuss the supporting components that are not directly related to a cyberattack, but nonetheless critical to operations inthe cybercrime ecosystem.

3.3 Cybercriminal Services Indirectly Support Primary Activities

Beyondtheservicesthat supporttheprimaryactivitiesdiscussedabove,therearesupport services related to benefitrealization, focusing on monetization of cyberattack gains on different market places. Personal profile information can be listed for sale or exposed publicly on underground markets todamage theorganizationorindividualtowhomthe informationbelongs [123];domain information are extremely valuable for the targeted cyber attack [156]; compromised computers can be sold to assemble a botnet [136]; the stolen tools can be used to construct the toolkits which offer"one-stop-shop"tool support[82];whileanmanipulatedpersoncanserveasthemoneymule [72].Psychologicalgains can helpattackers builda reputationforthemselves intheunderground. Furthermore, to mitigate the identity and quality uncertainty [183], the reputation and pricing systems are importantforthe cybercriminal ecosystem. Forloss-basedgains, attackers can collect benefitsdirectlyfromtheirvictims;however,ifitprovestoodifficultorriskyforattackerstointeract with victims to realize benefits, attackers can opt to trade the potential benefit on the market, supportedby the value evaluation services. For example, a groupofundergroundcybercriminals created Ran$umBin, a dark web service to monetize ransomware attacks that allows cybercriminals to uploadstolendata, motivating victims to pay to get back their stolendata [126]. Finally but straightforwardly, offering themarketplace to enable the tradingis a fundamental componentfor the cybercriminal ecosystem. Hence, as shownin Figure 5, we canidentifythe additionalre-usage componentsbesideBNaaSforthedigitalgains, andthemarketplace components.



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

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

3.3.1 DigitalGainRepurposingService. Throughthemarketplace,thesecomponents turnthe Systematic Thinking of Cyber Attack Business 1:25 digital gains from the successful cyber attacks into services which can be reused to facilitate the further cyberattack.

Personal Profile as a Service (PPaaS). This component offers personal profile PP about ·

targets such as passport numbers, driver's licenses, email accounts, social media accounts, or credit

card numbers. Any personal information I_p that can be used to build a complete personal profile, for an individual or an organization, can be included in this component, whether it comes from data breaches [176] or public sources on the internet, such as social media pages.

$$PP = PPaaS(I_p, MDF) \quad (18)$$

where MDF refers to the multimodal data fusion [86] that can be used to manage and analyse the collecteddata.Itisextremelyvaluablebecausedifferentdatasetscaninteractandinformeach other [23] to offer value-adding information about the targets. One typical application could be offeringthedetailinformationforthegivenindividualororganizationforthebuyerswhichcanbe used forfurther attack, especially forthe whaling phishing attack [66, 72].

Domain Knowledge as a Service (DMaaS). This component refers to domain information I_d . gainedfrompastattackstoofferspecificknowledgeDKrelevanttofutureattackswiththesupport ofthedevelopingdatamanageandanalysis technologyMDF.

$$DK = DMaaS(I_d, MDF) \quad (19)$$

Thebasicformofthedomainknowledgeisthestep-by-stepguidancesforcyberattack.Inspiredby the emergences of the WikiHow, eHow, Howcast etc. which offers extensive information about how-to tasks, as well as the development of the knowledge graph techniques [34], the DMaaS in the cybercriminal ecosystem could evolve into the similar how-to knowledge systems which can beusedacrossdifferent scenarios.

ToolPoolasaService(TPaaS).Cyber-attacks,liketherecentCIAbreach[179]orNSAcyber incident[60], andtheHackerTeamhack[68], canresultincybercriminalsgainingaccess tohacking toolsusedbythetargetedorganizationsthat canberepurposedandappliedinfuturecybercrimes. Hackercommunities,oftencybercrimegroupsornation-supportgroups,will collectthesetoolsT_I anddevelopnewvariantstoaddresstheirspecificgoals.Sincethesetoolscanbenefitthentire cybercrime ecosystem by facilitating new attacks, it is no surprise that toolkits or platforms TK_O onthedarkwebexisttofacilitate the access to these tools.For example,the "ShadowBrokers" announcedtoofferasubscription-basedservice[82]withaccesstoup-to-dateexploitsgainedfrom the NSAcyberincident.We can formally define TPaaS as:

$$TK_O = TPaaS(T_I, TMS) \quad (20)$$

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

Target Selection as a Service(TSaaS). As discussed above, informed target selection is very valuable in the cybercrime ecosystem, because it significantly reduces the cost and increase the benefitfromthecyberattack.Giventhepotentialapplicationsofpersonalinformationanddomain knowledge, as well as the development of advanced data analysis and artificial intelligence, the emergence of target selection as a service is a reasonable and valuable forthe cybercriminal ecosystem[107].We formally define TSaaS as follows:

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

whereT_H refers tothe identifiedvaluable targets,whichmayevenbe rankedaccordingtothe differentvaluefordifferentattackers.

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 importantto bridge the gapbetween thedark webandlegitimate busi nesses by money laundering, mitigate the identity through

reputation system and reduce quality uncertaintybyvalueevaluationandpricing.

.

Money Laundering as a Service (MLaaS). Given the illegal, "dirty" moneyM_D from a cyb erattack,this componentmakesuseofamoneylaunderingnetworkMLNtomake it appearas though it was earned by legal means M_C. We define MLaaS as follows.

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

Note thattheM$_C$ couldalso be inthe formofdigital currency, such asBitcoin[84] sinceBitcoincan be easily cashedout viadigital currency tradingplatforms such asBTC-Eor exchanged with each other[130]. MLN refers to the money laundering network consisting of many money mules, who make available their own bank or digital accounts to be used as conduits fortransferring money outofthecybercrimeecosystemforafee[31,49,72].

money laundering network, the mule herders, those who establish connections with would-be

up

.

MoneyMuleRecruitingasaService(MRaaS).Torecruitthemoneymuleswhowillmake a money mules, send out believable fake emails advertising normal jobs such as Financial Department Managerandcontactagaintheoriginalrecipientswhorespondtotheemail.Theseindividualswill be trained and brought into the money laundering network [158].

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

where HZrefers to thepeople acting as the money mules in the money laundering network MLN, whocouldbe trickedtojointhenetworkbecause itisanacceptable"job" forthemespeciallyif they are unemployed [1]. TS refers to training support, including tools and relatedknowledge. Normally,theDaaS componentis aprerequisite forthe MRaaS component, sinceMRaaS relies on creatinganddistributingfakeemails.

.

Reputationas aService (RaaS).Aspreviouslydiscussed,reputationisveryimportantin the cybercrime ecosystem as it serves as a metric to mitigate the uncertainty associated with dealing users who hide their true identities [183]. As a result, most marketplaces, especially forums, incorporatereputationmechanismintotheircoreservicethatgeneratesareputationratingbased onauser'spreviousinteractionsinthemarketplace.Towarntheundergroundvisitorstostayaway from fraudsters[8], some third-party services such as Ripper.cc and Kidala.info [167] were developed to maintained a database of rippers.

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

whereGPreferstothepreviousconductedattacksofthegivenuserwhileRRreferstotheinteraction records,Rrefers to the user's reputation determined by the reputation evaluation mechanism RS which can be similarto the mechanisms [151] employed by a legitimate business.

.

ValueEvaluationas aService(VEaaS).Similartoalegitimatebusiness, judgingthevalue of goods traded in a marketplace plays a fundamental role, mitigating the riskassociated with qualityuncertainty[183].Inthe caseof credit cards,thequalityofa stolencardmaydependonthe

credit limit of the account, and this will drive the price. Recently, Fatboy, a new ransomware-for hire scheme, automatically adjusts its ransomdemands according to the Big Mac Index, a way to measure the extent to which currencies are overvalued or undervalued [58]. Additionally, some cybercriminals use scanned documents, such as passports or driver's licenses, to confirm other users'identities.Forexample,ahackermayverifyaPaypalaccountwithascannedcopyofthe purported owner's passport [56].

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

[8]Inthecybercriminalecosystem,itisnot clearwhoarethe"goodguys"and"badguys".A"fraudster"canbeactuallyalaw enforcement associate trying to track down hackers [183]. The attackers can even condust attacks against each other[27].

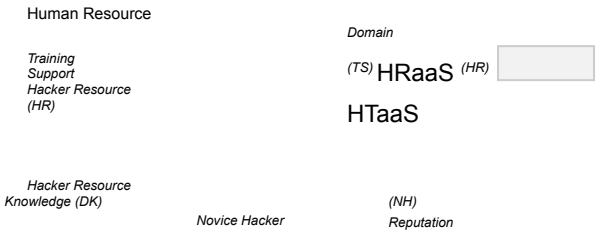
where PG_I refers to the goods offered by the providers on the marketplace; R refers to the seller's reputation;VIreferstotheverifyinformationwhichcanbepartofthepersonalprofilefromPPaaS; VES is the methodology to evaluate the value to determine the good's price PG_O.

MarketplaceasaService(MPaaS).Asdiscussedabove,themarketplace isafundamental component, serving as the trading place to realize the benefitfromthe cyber attacks.It serves as a pipeline to transferthe gains from a successful cyberattack into input for many different types of serviceswhichcanfacilitate the further cyber attack, andthemonetary benefitwhichcanbemade aslegalthroughmoneylaundering.

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

where$G_I$referstotheproductsor servicestradedinthemarketplace,whichcanbethedigitalgains GD orthe 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 webtobuilda specificmarketplace for some attackers.G_O refers tothedifferenttypesofmaterials likepersonalinformationI_p,domaininformationI_d,stolentool setT_l,compromisedmachines Z, manipulate humanHZ.M_D refers to the illegal monetary benefitthe seller achieve fromthe trading; MMT refers to the tool and technique to build the marketplace in the dark web, BS refers to the bulletproof serverto host the marketplace; RR refers to the seller's activities records while PGrefers tothe evaluatevalue forthegoods,representingthe supportfromtheRaaSandVEaaSto mitigatetheidentityandqualityuncertainty.

3.3.3 HumanResourceService. Themainfunctionalityofhumanresources is to trainnovice hackers so that they attain the necessary skills to participate in cyber-attacks, and to recruit new hackers to join the community orto participate in a specific cyberattack. As shown in Figure 6, it consists ofthe following two main services:



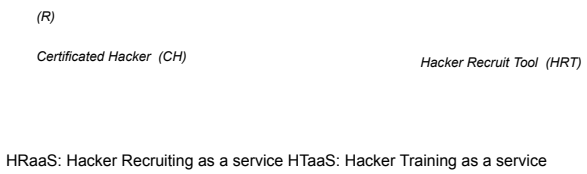


Fig. 6. Human resource service. These services prepare the necessary human resource forthe cyber attack business through training and recruiting.

.

Hacker Training as a Service (HTaaS). Given specific domain knowledge related to a cyb

erattack,this componenthelps ahacker, especiallyanovicehacker,gainskills relevantto cybercrime and become a qualified member in the hacker community. In its most basic form, HTaaS offers step-by-step guides or online school like OnionIRC [52]. Nowadays, it has grown into an industryofitsown,andisnotnecessarilyanundergroundactivityoranillegalbusinessatthis point. For example, the offensive security provides the "true performance-based penetration testing training" [147]offeringcertificationsonce trainingis completed, andevenruns abugbounty program to reward those who find qualifying vulnerabilities in their sites. We formally define

HTaaS as follows:

$$CH = HTaaS(NH, \{DK, TS, HR\}) \quad (27)$$

where NH refers to the hackers without the specific hacking skill, who are normally the novice in the community; CHrefers to the hackers gaining the necessary skills, namely certificatedhackers; DK refers to the necessary domain knowledge; TS refers to the tools or platforms supporting training;HRreferstothehackerswhocanofferthetrainingmaterials,suchaspersonalexperience, domain knowledge, or mentorship.

Hacker Recruiting as a Service (HRaaS). Cybercriminals may need to recruit additional hackerstocollaborateonaparticularattack.Asanexample,anation-statesponsoringacybercrime operation may hire non-affiliated hackers to carry out an attack, reducing the political risk that accompanies the sponsorshipof cybercrime [154].Wedefine HRaaS as follows:

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

where HRare the hacking resources that can beusedfor 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 orto participate into a cyber attack.

3.4 Cybercriminal Service Ecosystem Framework: Systematic Understandingof Cyberattacks

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

It canbe seenthatthe cybercrime ecosystemcanbeviewedasacomplete cyber-threat capability supply chain. "Weapon Development" activities transform discovered vulnerabilities from "Vulnera bility Discovery" into effective weapons by "Exploitation Development" for cyber-attacks. "Weapon Enhancement" activities make a cyberattack more powerful and better suited to avoid detection, which are components of the "Resistance Operation". The "Delivery" activities represent the act of delivering cyberattack weapons to their targets. "Marketplace Support" activities create the platforms for cybercriminals totrade thegains fromsuccessful attacks, while "Reusage" activities re-purpose thesegains toenable furtherattacks, servingas the"BenefitRealization"componentin the value chain. "Human resource" activities represent human resources that support the cybercrime ecosystem.Finally,the toolsandplatforms tosupportthese identifiedservices arepartsofthe "TechnologySupport"inthevaluechainmodel.

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

4 IMPLEMENTATION

4.1 Change the Cat-and-Mouse Game: Understand the Hacking Innovations Using this framework, we can systematically understand the hacking innovations in thecybercrimi nal ecosystem, including the development of these cyberciminal services, the evolving cyber-threat, andthe emergingservices,like"cyberciminal service compositionasaservice".

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

BN
RS
Cyber Attack
BNaaS

TS
Z

Weapon Development Weapon Enhancement Delivery

Reusage

Marketplace Human Resource

Infrastructure

BHaaS TR^{O} BHT

REaaS FR

SDC

VEK

TAaaS TGT TA

BS
BNDT

MMT

MRaaS

HZ

MLaaS

M^{T_I}
MLN

Mc

Pipeline EDT

EPaaS

TRaaS

RPaaS

TK_o

o
v
e
m
b
e
r
V
t

DaaS
EPT EK P^O_TR,TRT^D
MPaaS
GL

20
1
7.
VDaaS EaaS E VDT FDT
V_P

V,
Fl

PLaaS
PL

OBT
NI

RPT

OBS

OBS
VEK GD G

P

HR
RR

RaaS RS
PG

R
VEaaS VES

TMS

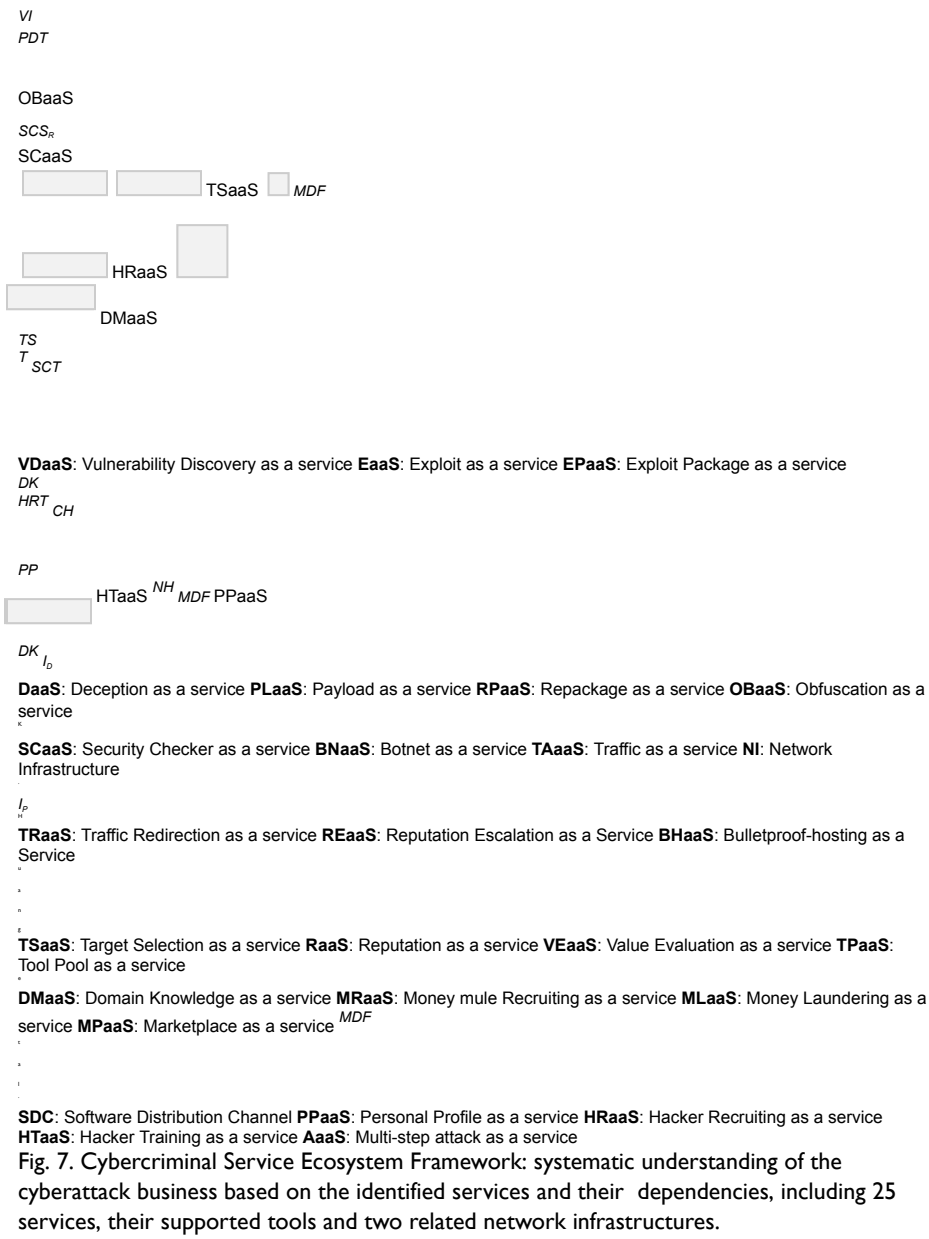


Fig. 7. Cybercriminal Service Ecosystem Framework: systematic understanding of the cyberattack business based on the identified services and their dependencies, including 25 services, their supported tools and two related network infrastructures.

4.1.1 Cybercriminal Service Development. Based on the above discussions, we follow the value added processes to construct the cybercriminal service ecosystem framework[10] and we can observe cases for mostidentified services in the dark web. Those that were not yet observed in the cy bercriminal ecosystem are related to the supportive activities, like the services related to hacker organization, target selection and benefit realization. A possible reason forthis is that these sup portive activities are not offeredas independent components and are muchdeeperunderground, because they are notrelated directly to the cyber-attacks. Forthe vulnerability discovery services, due tothehighuncertaintyforvulnerabilitydiscovery,wehavenotobservedinstances inthedark

webduringourresearch.

The offensive side and the defensive side are using similar innovations, and the innovations in legitimate businesses can drive the evolution of the components in the cybercriminal service ecosystemsothattheattackerscantapintothebenefitofthesedevelopments.Hence,itisreasonable toexpectthat,iftheydonot alreadyexist,theoffensiveversionsoflegitimatedefensive techniques will emerge forthe cyber-attacks, eithertrading on the dark web or used by the organized and nation supportedcybercrimes.Wecanfindsimilar applications andscenarios inlegitimate businesses to predictdevelopmentsofthecybercriminal servicesasfollow:

- Forthe *"hacker organization"*, hacker assignmenttools resemblingprojectmanagement applications can be usedto organize hackers involvedin an attack;
- For *"vulnerability discovery"*, inspired by the rapid growth of the bug bounty program platforms,itispossiblethatwewillobservesimilarapplicationsinthedarkwebtotakeadvantage of wisdomfromthe whole hacker community for a targeted cyber attack. Additionally, ser viceswhichcandigintotheoperational vulnerabilities [119,140,141] couldemerge and prove attractive to attackers;
- For*"targetselection"*,giventherapidgrowthofthetargetedcyberattack[98,107,156],targets rankingbasedonvalue canspreadto, andprovepopular,inthedarkweb; *"Repackaging"* to produce a verified exploit kit, including the EPaaS and RPaaS, requires specific skills andsome attackers aredoing by themselves. However, withthedevelopment ofthetechnology,itisreasonabletoexpectthatplatformswillemergetomaketherepackage mucheasier, or offerrelatedtools tohelpthe attackers todo this task inamore effectiveway [13,20,153];
- Providing the *"security checking"* platform for testing, similar to the emerging mobile app testing cloud in mobile ecosystem [53], can increase the succeed rate of cyber-attacks;
- For *"domain knowledge"* services, the most likely services we may expect to observe would resemble the "how-to" knowledge systems similar to the emerging online platforms like WikiHow,eHowandHowcast[34];
- Many comparison shopping websites [63] help the customers filter and compare products basedonprice,reviews andother criteria.It canbe expectedthat similar*"valuation"* services will emerge on the dark web to help cybercriminals choose the most reliable components, andtohelpsellers competitivelyprice theirgoods;
- Forthe *"personal profile"* services,the availabledata fromdata breaches andsocial media, as well as the development of the multimodal data fusion techniques, will further enable new services thatwilloffervalue-addedinformationonthegiventargetswhenrequested. Hackersmayevenoffercloud-style*"bulletproofservers"* [106]onthedarkwebtotapinto the benefit of cloud computing [12];

[10]Please refertoFigure 9inAppendixforthedetails aboutthemappingbetweenthevalue chainmodel andthe ecosystem framework.

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

Additionally,basedonthepresentedframework,we canexpectthe rapidgrowthforthese services.Wehave alreadyobservedanincreasingnumberofdata breachincidents inrecentyears [176] and this trend is unlikely to change in the near future. The development of the multimodal data fusion technologies [34, 86]including machine learnings, data analysis, knowledge management technology etc., will further enables the growth of the PPaaS (personal profile) and DMaaS (domain knowledge) in our framework. The website "Have I been pwned?" reports that about 3,806,000,000 accounts from220websiteshave beencompromisedasofJune 14th,2017 while thenumberis stillincreasing.It canbe expectedthatthese two components will become increasingly active andcommonintheundergroundcybercrime community.ThedevelopmentofPPaaSandDMaaS will further drive the development of TSaaS (target selection), which itself is an input to the "weapondevelopment"process fortargetedcyber-attacks.Usingthe semantic social engineering attack as anexample [66, 72, 124], we see anevolutionfromlarge-scalephishing emailsusing templates, to spear-phishing emails that are formatted for a specific user by taking into account that person's personal profile. Spear-phishing attacks are trending toward targeting high value victims, driving the evolution of whaling phishing. In the future, with the development of the TSaaS (target selection), the cost for whaling phishing will significantly reduce so that it is expected to observelarge-scalewhalingphishingattacks.Ingeneral,wecanforeseeanemergenceofmoreand morepersonalized,large scale cyber-attacks as target selectionservicesbecome more advance.

Another growing component in the framework is "Repackage-as-a-Service (RPaaS)", which finds itself at the crossroads of many value-added paths. If this kind of services is already available on thedark web, itis verypossible that we will experience a significantnumber of newmalware attacks relying on repackaged payloads and new obfuscation methods. It has been observed that traditional security technologies such as firewalls and intrusion detection systems are limited in their capabilities to defend against the threat posed by evolving malware [29, 46, 165]. The defensive sideis constantlyhavingtocatchupwiththeemergenceofnewmalware,butifmalwaredetection approacheswereretotakeintoaccounttherepackagingtrend,identificationofnewmalwareandthe level ofreadiness in the face of malware cyber-attacks need to be improved. For example, the use ofthe artificialintelligence inprogramming,likeneuralprogrammerinterpreters (NPI)[134] and Decoder[14], could support the automatic malware generation so that the detection approaches can bedeveloped before the malware is available in the wild.

*4.1.2 CybercriminalThreatDevelopment.*Toevaluatewhetherthepresentedframeworkcan thoroughly describe the cybercriminal ecosystem and serve as a tool to study the evolving cyber threat, we considerthe cyberthreatsdiscussedintheMcAfeeLabs 2017ThreatsPredictionreport [107] as an example. ThisMcAfee report proposes 14 predictions for cybersecuritydevelopments in2017.Not allpredictions are relatedto cyber-attacks, and weonlyconsiderthose relatedto cybercrime, mapping them into the presented framework to understand the cyber-threats they pose[11]. Those specially related to the potential defense efforts, such as "*Leveraging increased cooperation between law enforcement and industry, law enforcement takedown operations will put a dent in cybercrime*" or "*Threat intelligence sharing will make great developmental strides in 2017*", are notincludedinthefollowingdiscussions.

[11]Please refertoFigure 10 inAppendixtoseethedetailmappingofthe cybercriminalthreats totheecosystemframework.

Ransomware Attacks, especially to compromise business processes.

Ransomware at ·

tacks continue to pose a significant threat. Often, the victim of a ransomware attack will be redirected to a server where an exploit kit, such as RIG or Neutrino, is hosted. The exploit kit capitalizesonvulnerabilities inthevictim's systems toinstalladownloader,openingthedoor forthe attackerto activate a ransomware payload like Wana Decrypt0r, Locky, or CryptoWall to lock the victim's computer and compromise the business continuity of the victim's operations. It canbeseenthatthisthreatfollowsapathinourframeworkinvolvingEPaaS(exploitpackage), DaaS (fake information), PLaaS (payload), RPaaS (repackage), TRaaS (traffic redirection), BHaaS (bulletproof server), BNaaS (bot net), AaaS (multi-step attack), MPaaS (marketplace) and MLaaS (money laundering).

·

Social engineering attacks accelerates by machine learning. With greater accessibility to

machine learning technology, the FBI-labeled Business Email Compromise (BEC) scam [105], inwhichthe scammers target employeeswithaccess to companyfinances andtricktheminto making wire transfers to bank accounts thought to belong to trusted partners, has become much more prevalent due to the available information to manipulate the target's perception. Based on datagatheredfromdatabreaches, socialmedia,publicdisclosures, aswell asdomainknowledge, cybercriminals can train a model to identify valuable targets, and then generate convincing fake messages for a semantic social engineering attack. This threat begins at PPaaS (personal profile), andDMaaS(domain knowledge),makesuseofTSaaS (target selection) andVDaaS (vulnerability discovery)to identify the operational vulnerability in the specific targets; and finally relies on the DaaS (fake information)to generatepersuasive butfake message forthe attack.

·

Fake reputationgenerationbybotnet.Reputation systems are animportant component of

any digital community. Due to the vulnerabilities inherent in a reputation system, services to falsify a user's reputation are available and growing in scope. To support this activity, a botnet, no matterif constructed by infected machines, or physical servers located in data centers, can be usedtogeneratethefakeclicksorcommentsthatincreaseauser'sonlinenotoriety.Thisattack represents the application of the online traffic, involving BNaaS (botnet), TAaaS (traffic) and REaaS (reputation escalation).

ho

·

Adwars bilities.Advertisersdisplayadsin p es that a user will click on them. Once the ad is clicked, a user profile is generated that allows **technologytoboostmalwaredeliverycapa** for targeted advertisements, and greater revenue for advertisers. This technology will likely be used by cybercriminals to redirect traffic to a compromised website, representing the recent growth ofTRaaS(trafficredirection).

Privacy explosion by hacktivists. The data breaches are expected to increase,

targeting at ·

some ofthe corporate clouds that contain customer data. Stolen data is sure to bring profitto cybercriminals,meaningthatPPaaS(personalprofile)willbecomemoreaccessible.

Cyber threats to hardware,firmware, drone, mobile ecosystem, and IoT increase while ·

attacktoWindowssubside.Thisthreatpredictiondiscussesabout cyberthreatstothedifferent targets with different technical environment, which is related to the TSaaS (target selection). These threats can be mapped into ourframework. Hence, the presented ecosystem model can serve as a tool, allowingus to think systematically aboutthe evolutionof cyber-threats.More importantly, these threats are not independent, in fact, they form the reinforcement loops, including the reuse of the compromised machines, stolen tools, stolen information and the hacking experience, by which each threat reinforces and empowers the others. Note that the McAfee report does not consider many components related to cybercrime support activities, although we understand them to beveryimportantinthe systematicunderstandingof cyber-threat evolution.For example, understanding of the OBaaS (obfuscation) [145] will be very important for the security software providers to prepare before the attacks. The development of the money laundering network driven

bytheuseofdigitalcurrencyinthecybercrimeecosystem[21]willalsobringchangetoapproaches usedinbenefitrealization.

4.1.3 Profitability of Cybercriminal Business: the Emergence of Composition Services. As discussed above, components involved into the cyberattack are offered as services that a would be attacker can purchase on the dark web to equip themselves for an attack. To analysis the profiabilityofthe cybercriminal business, as shown in Figure 8, we use the ransomware attack as an example. The price of each involving service are based on the observed instances in the dark web.Forthebenefit, weuse the indicators fromtheAnglerrevenue reportedby Cisco [35] as a baselinebutmake a muchmoreconservativeestimateacknowledgingthedefensiveefforts.

cybercriminal can y
BNaaS (botnet)for $999permonth, a traffic redirectionprotocolfor $600, six servers as apart

bu
·

Costs of sample services. To run a ransomware attack as a business, a ofBHaaS(bulletproof server)for$1,800permonth,accesstotheNeutrinoexploitkitinEPaaS (exploitpackage)for$4,000,aransomwarepayloadwithcustomer supportinPLaaS(payload)for $3,000 and the traffic redirection service TRaaS to redirect victims to servers for $600 per month. Tofurtherincrease the effectiveness of an attack, a cybercriminal can hire a qualified hackerfrom HRaaS for $2,000permonth, andemployanobfuscationservice fromOBaaS to repackage the exploit kit and payload for $600 per month. Finally, to reduce risk of arrest, services to monetize benefits in the wake of a cyberattack as a part of MLaaS (money laundering) can be accessed for a feeof $400 and40%commissiononprocessedfunds.

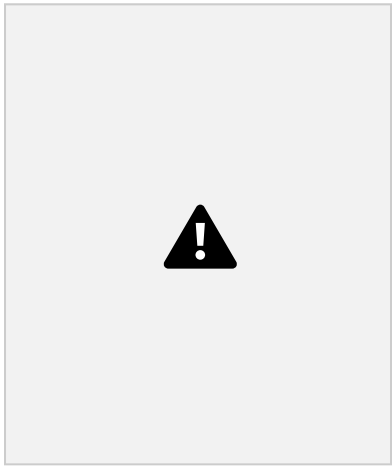


Fig. 8. ROI for the Ransomware Attack Business: Value of the cybercriminal service composition. Blue color means that the monetization service request 40% commission from the benefit the attacker gains. Red color refers to the case that the number of victims who pay the ransom from Angler Revenue Report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

.

Example of Return on Investment (ROI). For calculating benefit, we assume that 30,000 pe

opleare redirectedperday,ofwhich10%arevictimsof aransomwareattackwhere0.5%of victims pay a $300 ransom. Though only 450 victims (0.05% of total users redirected) will end up paying the ransomover a period of one month (30 days), this brings the cybercriminal's monthly earnings to $135,000. We can see that the Return-On-Investment (ROI), even when only a small proportion of people end up paying a ransom, is as high as 504.52%, an impressive ROI for a business.

Using the reports from CSIMarket [39] for comparison, the highest industrial ROI, which is from the Tobacco industry, is only 50.63% in August 2017; in fact, this theoretical cybercrime operation wouldbe rankedasoneofthe topsevenbestperformingcompanies intheworldintermsofROI.If weuse the numbers fromthe Anglerrevenue report which shows that 9,515 userspay the ransom per month, a number more than 20 times larger than the 450 users dictated by our assumptions, then theROI ofthis operation would be 12,682.30%, which is significantly higherthan the highest ROIfromCheniereEnergyPartnersLpHoldings,Llc(7020.69%)inAugust2017.

Cybercriminal servicecompositionasaservice. Hence,wecanconclude that

combining ·

separate services to perform a cyberattack has great value for cybercriminals. This motivates the emergence of *"cybercriminalservice composition as a service"*. In this scenarios, the attacker can collaborate and apply services available on multiple dark web marketplaces and combine them together to offer a "one-stop shop" style service, which will continuously reduce the barriers to entry of cybercrime and performing complex cyber-attacks. More importantly, thisdevelopment alsoallows cybercriminals involvinginthe cybercrime ecosystemtofocusonthepartsofthevalue chainmodelatwhichtheyarebest, andprovide theirexpertiseasaservice toothercybercriminals. Following this "specialization,

commercialization and cooperation" trend, cybercriminals have been able to hide themselves even deeperin the dark web, and in certain cases, some of their activities may no longer be characterizedas illegal.

More importantly, this framework can not only help us to systematically understand the cyberattacks, but also inspire several strategies to more effectively combat them. Due to the space limitation,wewilltakethecontrolpointidentificationandresponsibilitysharingastwoexamples.

4.2 StrikingtheDarkSide:IdentifyingControlPointstoImproveEffectiveness

Tounderstandthedarkwebitselfis a stepinthe rightdirectioninthe efforttostymie thegrowthof theunderground cybercrime ecosystem; however,this is more easily saidthandone, as collecting data on dark web activity proves difficult [66]. The "honeypot" is a technology to detect, deflect, or counteract attempts to use information systems in an unauthorized way, and many honeypot systemshave beenusedto revealinformationfromhowandwhycybercriminals intrude into certain systems, to what threats exist or are developing in the wild [4, 29, 118]. The Telekom Fruhwarnsystem project [118] was launched in 2013 to establish a worldwide multi-honeypot platformtocollectunbiasedquantitativedatathatwouldpresentarealisticpictureofinternet threats. The data the system collects is related to attack profile, and describes the attack's sources, vulnerabilities it exploits, tools it employs, and level of sophistication. The HoneyCirculatior monitor system behaves like a compromised systems to collect the malware, bait credentials, fraudulent access andcompromisedwebcontent[4].It canbe seenthatthesehoneypotsarepurposefully plantedincertaincornersofcyberspace totarget certaincybercriminals,asdescribedbyAaaS (multi-stepattack). Some researchershave also triedtounderstandexactly what goods are traded on the dark web [6, 33, 76, 186],focusing on MPaaS (marketplace).

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

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

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

- OBaaS (obfuscation), work with SCaaS (security checker) to circumvent detection, which can bypass the effort from defensive side to improve the success rate for a cyber attack.
- BHaaS (bulletproof server), offers bullet-proof server access toimprove the resilience ofthe underground economy.

- HRaas(hackerrecruiting)recruitshackerstojointhecybercriminalecosystemorparticipate into a cyberattack.
- BNaas (botnet)providesbotnets tosupportnumerous components inthe ecosystem,which isa fundamentalinfrastructure forthe cybercriminal ecosystem.
- MRaaS (money mule recruiting) constructs the money laundering network to transfer the illegal money into legal one, acting as the connection between the underground economy andthelegitimatebusinesses.
- DMaaS(domainknowledge)yieldsnecessarydomainknowledge,PPaaS(personalprofile) revealspersonalinformation,andTPaaS(toolpool)offerstoolsthat supportotheractivities.

Ifthedefensesidecanbuildthe"honeypot"styleservicesforthesecontrolpoints,itcanhelp the cybersecurity community, the defensive side, more effectively understand and monitor the evolution of the cybercrime ecosystem. For example, the infrastructure developed by Onaolapo et al.[123], whichplantthe honeypotinthePPaaS, can be usedto monitor how compromised Gmail accounts are used on the dark web. This research reveals that cybercriminals tend to evade security mechanisms employed by online services meant to flag suspicious logins, and proposes a behavioral model based on the contents of search queries that could signal malicious activity. Taking down these control point components, especially the reuse related components including BNaaS,DMaaS,PPaaS,TPaaSandMRaas,canalsohelptobreakthereinforcementloopsinthe cybercriminal ecosystem.

Furthermore, such a scheme could also help law enforcement associates collecting critical evi dence to convict cybercriminals and strike at the heart of cybercrime business. More interesting aspecthere is thatgiventheuncertainties relatedtoidentityandquality,the cybercriminalmarket isatypical"marketforlemons"[113,177,178].Ifthedefensivesidecanfloodthecybercriminal ecosystem with honeypot-style orfake goods, it will make the dark web less attractive for cyber criminals lookingtopurchase services.Thepracticewhichdemonstrates the feasibilityis that whenthedarkwebmarketplaceAlphaBaywasclosedandtheserversforHansa,anotherdarkweb marketplacewasseizedbythegovernment,theycontinuedtorunHansaforamonthtocollect information about the vendors and customer [51]. This strategy, running Hansa under control, furtherraise the concerns forthe hacker community that the other dark web markets, like Dream market,was alsocompromisedina similarmanner andunderpolice control.

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

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

4.3 Sharing Responsibility: Action Suggestions for BetterCollaboration There exist several challenges plaguing cybersecurity and cybersecurity policy when it comes to working together to build a safer connected world [113]: the externalities [87], misaligned

incentives [11]andthe informationasymmetries [9].Thesemarketfailures calls forimplementationofpolicy toallocateresponsibilitiestodifferentpartiessocybersecuritycanbeimprovedintheplaceswhere economic forces disincentive it. Given the presented cybercrime ecosystem framework, we can identifywhichresponsibilitiesor actions falltowhichactorsbasedonwhetherthe actorshave the capability to take the actions[13]:

- *Individuals and Corporations* have a responsibility to protect themselves by investing in security software or hardware, altering processes, or educating people on common cyber attacks. There is also a responsibility forthe defenders to share cyberrisk information. However, how to design effective mechanisms to motivate the information sharing while bypass its negative effort is still an open but challenging issue [32, 88, 99, 180].
- *Software/Hardware Providers* have a responsibility to monitor vulnerabilities and exploitations in their products. Nonetheless, issues persist related to the delays in the application of patches for discovered vulnerabilities [150] so that software/hardware providers must acknowledge these delays and work with users to accelerate the rate at which patches take effect. Furthermore, in practice, once the lifecycle of a piece of software/hardware has run its course, providers no longer offer automatic fixes, updates, or online technical assistance forthe product. This leaves those older, yet widely used products vulnerable to attack. The WannaCry Hurricane attack in May 2017 is one recent example of such cyberincidents [137].Thus,there is aneedto discusspolicyrelatedtoproduct supportlifecycle, andthe responsibilityforproviders anduserswhenolder versions ofproducts are stillwidelyused. *SecurityCompanies*,put simply,mustfight cyber-attacks, especiallythepayloads.Many technologies such as pattern matching, static analysis, dynamic analysis, hybrid analysis, and even human analysis have been presented overthe years as solutions to defend against cyber-attacks [3, 46, 165, 166].Beside these catch-upefforts, it will be beneficialto adopt the frame of mind of a hacker and work accordingly to identify ways in which security defenses could be bypassed. Inspired by bug bounty programs for the vulnerability discovery, securitycompanies couldoffer similarprograms tohire external experts, suchas cybersecurity researchers,todevelopeffective obfuscation techniques andrenderthemineffective by updatingsecuritymeasuresbeforethesametechniquesaredevelopedorexploitedbycyber criminals. Additionally, if security companies can set up honeypot-style security checkers through SCaaS (security checker), it could be possible for the security companies to collect informationtocombatfuture cyber-attacks.
- *Infrastructure operators* such as the Internet Service Providers (ISP), according to ourframework, should work to disrupt the delivery of cyber-attacks because they are in the position tomonitortheInternettraffic.Thoughsomeinfrastructureoperatorsactivelyparticipatedin botnetdetection and abuse reporting [56, 77, 78, 128, 175], how to incentivize ISPs to involve themselvesinthefightagainstcybercrimeisanimportantoneforthedefenseside.Italso requires the international collaboration [17] to fight against the delivery of the cyberattack, as the Internet, and the cybercriminals with which itis infested, knows no borders.
- *Financial Systems*, such as payment networks, must take responsibility for curbing themoneti

zationactivitiesofcybercriminals.However,inthecaseofthemoneymulerecruitingservice (MRaaS) to build a money laundering network, no banks ortake-down companies actively pursue the elimination of money mule recruitment websites [114].Wedeem it necessary to

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

rethink financial systems'responsibilities when it comes to combatting cybercrime-related financialtransactions.Inaddition,theanti-moneylaunderingoperations are illpreparedto dealwithdigital currencies, such asBitCoin, whichinhabit a legalgray area [21]. Hence,the financialsector shouldemphasizecollaboration,andacknowledgeitsshortcomingswhenit comestodigitalcurrency-relatedcybercrimemonetizationactivities.

Government has an important role in combatting cybercrime, given its position to address market failures related to cybersecurity. Just as we mentioned above, it may be in the gov ernment's interest to develop strategies to take down or controlthe dark web market places directly, orflood them with fake goods to destroy its reputation system foridentify uncer tainty mitigation. Furthermore, because the defensive and offensive sides are using largely the similarinnovations, it is paramount to ensure trainees work forthe right side. The government should consider strategies to recruit skilled individuals to the defensive side and combat incentives that drive themto join the cybercrime business.

Third-party threatintelligenceservice providers should monitordark webactivity to study how cybercriminals reuse the achievements from the successful attacks. More third-party services focused on TPaaS (tool pool), DMaaS (domain knowledge), PPaaS (personal profile), and TSaaS (target selection) would be welcomed in the cybersecurity community, since more informationtranslates togreaterpreparedness inthe faceof cyber-threats. However,howto motivate them to work for defensive side instead of the cybercriminal ecosystem is still an unclear but paramount issue.

5 CONCLUSION

Cybersecurity has become relevant on the scale of nations. The "double-edged sword" nature of cybersecurity technology means that the defensive and offensive sides use similar innovations, and until now, the offense has been able to nurse its advantage: "the bad guys are getting badder faster". Cybercrime is no longer just a hobby. Cybercrime has become a business, and even less than-prodigious hackers may choose it as a profession. The cybercrime ecosystemhas 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 growthofthe cybercrimebusiness,reconstructingintoa specialization, commercialize, andcoop eration system. Without a systematic understanding of this trend in the cybercrimeecosystem, effectivelycombattingcyber-attackshasbeenproveddifficult.

Thispaper constructs thevalue chainmodelbasedonasurveyofthevalue-addedprocesses for cyber-attacks. We see that aside from the primary activities of vulnerability discovery, exploitation development, exploitationdelivery, andattack,manysupport activitiesare emergingtofacilitate cyber-attacks, including attack lifecycle operations, human resource management, marketing and delivery, and technology support. Combining the value chain

model with the developments of the"as-a-service"innovations,wemodelcybercrimeactivitiesasservicecomponentswithinputs, outputs, and supports. In this way, we can identify the relationships betweencomponents and construct a global view of this underground business: the cybercrime serviceecosystem framework.

Finally, we discuss the implementation of our framework to understand the hacking innovation, identify the control-point activities and assign responsibility to encourage collaboration among interested parties. The framework enables us to systematically understand the hacking innovations in the cybercriminal ecosystem, including the cybercriminal service development, cyber-threat evolution and the emergence of composition service: "cybercriminal service composition as a service", which can offer "one-stop-shop" style cyberattack services forthe cybercriminal ecosystem. More importantly, it inspires several strategies to more effective combat cyberattacks. For example, strikingthedarksidebyidentifyingthecontrolpointswhichrepresentthekeycomponentsof

the cybercriminal ecosystem can help the defensive side to effectively deploy the "honeypots" to monitor and combat the cybercriminal activities; assigning responsibility to different actors with vestedinterests in cybersecurity following the value-added processes can encourage meaningful collaborationtowardsasaferworld.

By conceptualizing the moderncyber attack business systematically, we can better design cyberattack combat strategies. More research about how to disrupt the business of cybercrime by stymieing the development of the threat capability supply chain in the cybercrime ecosystem isneededforthe securitycommunity.Additionally,there is roomfordiscussionsonissuesof ethicssurroundingcyberattack,whichcanhelpinthedesignofnewregulationsthatimprove cybersecurityacross theboard.

ACKNOWLEDGMENTS

The authorswouldlike tothankthemembers fromtheMIT-$(IC)^3$ fortheirvaluable comments and inputstoimprovethevalue-chainmodelsandthecybercriminal service ecosystemframework,as wellastheimplementationinspirations.

REFERENCES

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

[2] LillianAblon,MartinC.Libicki,andAndreaA.Golay.2014. *MarketsforCybercrimeToolsandStolenData:Hackers' Bazaar*. TechnicalReport.RANDCorporation. 1–85pages.

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

[4] Mitsuaki Akiyama, Takeshi Yagi, Takeo Hariu, and Youki Kadobayashi. 2017. HoneyCirculator: distributing credential honeytokenforintrospectionofweb-basedattackcycle. *InternationalJournal ofInformationSecurity* (2017),1–17. https://doi.org/10.1007/s10207-017-0361-5

[5] Abdullah M. Algarni and Yashwant K. Malaiya. 2014. Software Vulnerability Markets : Discoverers and Buyers. *InternationalJournalofComputer,Electrical,Automation,ControlandInformationEngineering*8,3(2014),480–490.

[6] LucaAllodi,Marco Corradin, andFabioMassacci. 2016. Then and Now: On theMaturity ofthe CybercrimeMarkets theLessonThatBlack-HatMarketeersLearned. *IEEETransactions onEmergingTopicsinComputing* 4, 1 (2016), 35–46. [7] Sumayah Alrwais, Xiaojing Liao, Xianghang Mi, Peng Wang, XiaoFeng Wang, Feng Qian, Raheem Beyah, and Damon McCoy. 2017. Under the Shadow of Sunshine : Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks. In *2017 IEEE Symposium on Security and Privacy,*. 805–823.

[8] Mashael Alsabah and Ian Goldberg. 2014. Performance and Security Improvements for Tor: A Survey. *Comput.*

Surveys 49, 2 (2014), 1–38.
[9] RossAnderson.2001.Whyinformationsecurityishard-aneconomicperspective.In*Proceedings17thAnnualComputer Security Applications Conference*. IEEE, 358–365.
[10] RossAnderson,ChrisBarton,RainerBöhme,RichardClayton,MichelJ.G. vanEeten,MichaelLevi,TylerMoore, and StefanSavage.2013. MeasuringtheCostofCybercrimeRoss.In*TheEconomicsofInformationSecurityandPrivacy*. 265–300.
[11] Ross Anderson and Tyler Moore. 2006. The economics of information security. *Science* 314, 5799 (2006), 610–613. [12] Claudio A. Ardagna, Rasool Asal, Ernesto Damiani, and Quang Hieu Vu. 2015. From Security to Assurance in the Cloud: A Survey. *Comput. Surveys* 48, 1 (2015), 2:1–2:50.
[13] Thanassis Avgerinos, Sang Kil Cha, Brent Lim, Tze Hao, and David Brumley. 2011. AEG: Automatic Exploit Generation. In*18thAnnualNetworkandDistributedSystemSecuritySymposium*,Vol.14.1–18.
[14] Matej Balog, Alexander L. Gaunt, Marc Brockschmidt, Sebastian Nowozin, and Daniel Tarlow. 2016. DeepCoder: Learning to Write Programs. *arXiv preprint arXiv:1611.01989* (2016), 19. http://arxiv.org/abs/1611.01989
[15] TiffanyBao,RuoyuWang,YanShoshitaishvili, andDavidBrumley. 2017. YourExploitisMine:AutomaticShellcode Transplant for Remote Exploits. In *2017 IEEE Symposium on Security and Privacy*. 824–839.
[16] EliBlumenthalandElizabethWeise.2016. HackedhomedevicescausedmassiveInternetoutage. (2016). https: //www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/
[17] DannyBradbury. 2014. Testingthedefencesofbulletproofhostingcompanies. *NetworkSecurity* 2014, 6(2014), 8–12.

[18] RussellBrandom. 2017. An Anonymous group justtookdown a fifth ofthedark web. (2017). https://www.theverge. com/2017/2/3/14497992/freedom-hosting-ii-hacked-anonymous-dark-web-tor
[19] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, and Steve Chon. 2014. Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology* 8, 1 (2014), 1–20. [20] David Brumley, Pongsin Poosankam, Dawn Song, and Jiang Zheng. 2008. Automatic patch-based exploit generation is possible: Techniques and implications. In *IEEE Symposium on Security and Privacy*. 143–157.
[21] DantonBryans.2014.*Bitcoinandmoneylaundering:Miningforaneffectivesolution*.Vol.89. 441–472pages. [22] JuanCaballero,ChrisGrier,ChristianKreibich,VernPaxson,andUCBerkeley.2011. MeasuringPay-per-Install:The CommoditizationofMalwareDistribution.In*USENIXSecuritySymposium*.13:1–13:16.
[23] Vince D. Calhoun and Tülay Adali. 2009. Feature-based fusion of medical imaging data. *IEEE Transactions on Information TechnologyinBiomedicine*13,5(2009),711–720.
[24] Alejandro Calleja, Juan Tapiador, and Juan Caballero. 2016. A look into 30 years of malware development from a softwaremetricsperspective.In*InternationalSymposiumonResearchinAttacks,Intrusions,andDefenses*,Vol.9854 LNCS. 325–345.
[25] DavideCanali andDavideBalzarotti. 2013. Behindthe scenes of online attacks: ananalysis of exploitationbehaviors on the web. In *20th Annual Network & Distributed System Security Symposium*. n–a.
[26] OnurCatakoglu,MarcoBalduzzi,andDavideBalzarotti.2016.AutomaticExtractionofIndicatorsofCompromisefor WebApplications.In*InProceedingsoftheWorldWideWebConferernce*.333–343.
[27] OnurCatakoglu,MarcoBalduzzi,andDavideBalzarotti.2017.AttacksLandscapeintheDarkSideoftheWeb.In*ACM Symposium on Applied Computing*. 1739–1746.
[28] New Jersey Cybersecurity & Communications Integration Cell. 2016. Exploit Kit Variants: Neutrino. (2016). https: //www.cyber.nj.gov/threat-profiles/exploit-kit-variants/neutrino
[29] Jian Chang, Krishna K. Venkatasubramanian, Andrew G. West, and Insup Lee. 2013. Analyzing and defending against web-based malware. *Comput. Surveys* 45, 4 (2013), 1–35.
[30] ChiaYuanCho,DomagojBabic,PongsinPoosankam,KevinZhijieChen,EdwardXueJunWu, andDawnSong. 2011. MACE: model-inference-assistedconcolic exploration for protocol and vulnerability discovery. In *USENIX Security Symposium*. 139–154.
[31] KimKwangRaymondChoo. 2011. Thecyberthreatlandscape:Challenges andfutureresearchdirections. *Computers and Security* 30, 8 (2011), 719–731. http://dx.doi.org/10.1016/j.cose.2011.08.004
[32] Nazli Choucri, Stuart Madnick, and PriscillaKoepke. 2016. Institutions for Cyber Security:InternationalResponses andDataSharingInitiatives.(2016), 34pages.
[33] NicolasChristin.2013.TravelingtheSilkRoad:AMeasurementAnalysisofaLargeAnonymousOnlineMarketplace. In*Proceedings ofthe22nd international conference onWorldWideWeb*.213–224.
[34] Cuong Xuan Chu, Niket Tandon, and Gerhard Weikum. 2017. Distilling Task Knowledge from How-To Communities.. In *World Wide Web Conference*. 805–814. http://dblp.uni-trier.de/db/conf/www/www2017.html [35] Cisco. 2016. *Cisco 2016 Annual Security Report*. Technical Report. 1–87 pages. http://www.cisco.com/c/dam/assets/ offers/pdfs/cisco-asr-2016.pdf
[36] David D Clark. 2012. Control point analysis. In *TRPC Conference*. 25. http://papers.ssrn.com/sol3/papers.cfm?abstract [37] Bernd Conrad and Fatemeh Shirazi. 2014. A Survey on Tor

and I2P. In *Proceedings of the 9th International Conference on Internet Monitoring and Protection*. 22–28.
[38] Contagio. 2015. An Overview of Exploit Packs (Update 25) May 2015. (2015). http://contagiodump.blogspot.com/2010/ 06/overview-of-exploit-packs-update.html
[39] CSIMarket. 2017. CSIMarket Return on Investment Screening. (2017). https://csimarket.com/screening/index.php?s=roi [40] ExploitDatabase.2017.TheExploitDatabase.(2017).https://www.exploit-db.com/
[41] RogerDingledine,NickMathewson,andPaulSyverson.2004. Tor:Thesecond-generationonionrouter.(2004), 17 pages.
[42] Thomas Donilon, Chair Samuel Palmisano, Keith Alexander, Ana Antón, Ajay Banga, Steven Chabinsky, Patrick Gallagher, Peter Lee, Herbert Lin, Heather Murren, Joseph Sullivan, Maggie Wilderotter, and Kiersten Todt. 2016. *Commission on Enhancing NationalCybersecurity*. TechnicalReport. 1–100 pages. https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf
[43] Charles Doyle. 2012. Cybercrime: An Overview of the Ferderal Computer Fraud and Abuse Statue and Related Federal CriminalLaws. *JournalofCurrentIssuesinCrime,Law&LawEnforcement*5,1/2(2012),69–162. [44] BenoitDupont,Anne-MarieCote, Claire Savine, andDavidDecary-Hetu. 2016. The ecology oftrust amonghackers. *Global Crime* 17, 2 (2016), 129–151.
[45] E-ISAC and SANS. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Technical Report. 23pages. https://ics.sans.org/media/E-ISAC

[46] Manuel Egele, Theodoor Scholte, Engin Kirda, and Christopher Kruegel. 2012. A survey on automated dynamic malware analysis techniques and tools. *Comput. Surveys* 44, 2 (2012), 1–42. http://dl.acm.org/citation.cfm?doid=2089125.2089126 [47] JoseEsteves,ElisabeteRamalho, andGuillermodeHaro. 2017. ToImprove Cybersecurity,ThinkLike aHacker. *MIT SloanManagementReview*58,3(2017),71–77.
[48] AdriennePorterFeltandDavidWagner.2011. Phishingonmobiledevices.In*Web2.0Security andPrivacy*,Vol.2. 1–10.
[49] KristinMFinkleaandCatherineATheohary. 2015. *Cybercrime:ConceptualIssuesforCongress andU.S.LawEnforcement*. TechnicalReport. 1–27pages.
[50] Thomas Fox-Brewster. 2016. Android Gooligan Hackers Just Scored The Biggest Ever Theft Of Google Accounts. (2016). https://www.forbes.com/sites/thomasbrewster/2016/11/30/gooligan-android-malware-1m-google-account-breaches-check-point-finds
[51] Thomas Fox-Brewster. 2017. Forget Silk Road, Cops Just Scored Their Biggest Victory Against The Dark Web Drug Trade. (2017). https://www.forbes.com/sites/thomasbrewster/2017/07/20/alphabay-hansa-dark-web-markets-taken-down-in-massive-drug-bust-operation
[52] Anonymous France. 2016. Anonymity and Privacy first lesson taught on OnionIRC. (2016). https://www.anonymous-france.eu/anonymity-and-privacy-first-lesson-taught-on-onionirc.html
[53] JerryGao,XiaoyingBai,Wei-TekTsai, andTadahiroUehara. 2014. MobileApplicationTesting:ATutorial. *Computer* 47, 2 (2014), 46–55. http://ieeexplore.ieee.org/document/6693676/
[54] Glen Gibb, Hongyi Zeng, and Nick McKeown. 2012. Outsourcing network functionality. In *ACM HotSDN 2012*. 73. http://dl.acm.org/citation.cfm?doid=2342441.2342457
[55] MishaGlenny.2011. *DarkMarket:Cyberthieves,Cybercops andYou*. 283pages. http://books.google.nl/books?id=uxAcuzbyw9YC
[56] MaxGoncharov.2012.*RussianUnderground101*.TechnicalReport.TrendMicro.1–29pages. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf [57] Google. 2015. Vulnerability Research Grant Rules. (2015). https://www.google.com/about/appsecurity/research-grants/ [58] DianaGranger. 2017. FatboyRansomware-as-a-ServiceEmergesonRussian-LanguageForum. (2017). https://www.recordedfuture.com/fatboy-ransomware-analysis/
[59] Mariano Graziano, Davide Canali, Leyla Bilge, Andrea Lanzi, and Davide Balzarotti. 2015. Needles in a Haystack: Mining Information from Public Dynamic Analysis Sandboxes for Malware Intelligence. In *24th USENIX Security Symposium*. 1057–1072.
[60] ANDYGREENBERG.2016. HackersClaimtoAuctionDataTheyStoleFromNSA-LinkedSpies. (2016). https://www.wired.com/2016/08/hackers-claim-auction-data-stolen-nsa-linked-spies/
[61] Gustavo Grieco, Guillermo Luis Grinblat, Lucas Uzal, Sanjay Rawat, Josselin Feist, and Laurent Mounier. 2016. Toward large-scale vulnerability discovery using Machine Learning. In *Proceedings of the ACM Conference on Data and Application Security and Privacy*. 85–96.
[62] FelixGröbert,Ahmad-RezaSadeghi, andMarcelWinandy.2009. Softwaredistributionas amalwareinfectionvector. In*2009InternationalConferenceforInternetTechnologyandSecuredTransactions*.1–6.
[63] Chen Hajaj, Noam Hazon, and David Sarne. 2017. Enhancing comparison shopping agents through ordering

and gradual information disclosure. *Autonomous Agents and Multi-Agent Systems* 31, 3 (2017), 696–714. [64] Ashley Harris. 2016. *CyberEthics: An assessment of government and privateindustry*. Ph.D.Dissertation. Utica College. [65] Andreas Haslebacher, Jeremiah Onaolapo, and Gianluca Stringhini. 2016. All Your Cards Are Belong ToUs: Under standing Online Carding Forums. *CoRR abs/1607.00117* 1 (2016). http://arxiv.org/abs/1607.00117 [66] RyanHeartfieldandGeorgeLoukas.2015.ATaxonomyofAttacksandaSurveyofDefenceMechanismsforSemantic Social Engineering Attacks. *Comput. Surveys* 48, 3 (2015), 1–39.

[67] Cormac HerleyandDineiFlorêncio. 2010. NobodySellsGoldforthePrice of Silver:Dishonesty,Uncertaintyandthe Underground Economy. In *Economics of Information Security and Privacy*. 33–53.

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

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

[70] Thomas JHolt,DeborahStrumsky,OlgaSmirnova, andMaxKilger. 2012. Examiningthesocialnetworks ofmalware writersandhackers.*InternationalJournalofCyberCriminology*6,1(2012),891–903.

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

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

[73] Danny Yuxing Huang, Doug Grundman, Kurt Thomas, Abhishek Kumar, Elie Bursztein, Kirill Levchenko, and Alex C Snoeren. 2017. Pinning Down Abuse on Google Maps. In *26th International World Wide Web Conference*. 1471–1479. [74] Keman Huang,Jinjing Han, Shizhan Chen, andZhiyong Feng. 2016. A Skewness-BasedFramework for Mobile App Permission Recommendation and Risk Evaluation. In *14th International Conference on Service-Oriented Computing*. 252–266.

[75] Keman Huang, Michael Siegel, Stuart Madnick, Xiaohong Li, andZhiyong Feng. 2016. Diversity or Concentration ? Hackers 'StrategyforWorkingAcrossMultipleBugBountyPrograms.In*IEEESymposiumonSecurityandPrivacy*. 2. [76] Keman Huang, JiaZhang, WeiTan, andZhiyong Feng. 2017. Shifting to Mobile: Network-based Empirical Study of Mobile Vulnerability Market. *IEEE Transactions on ServicesComputing* pp, 99 (2017), 1–14.

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

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

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

[80] Mohammad Karami, Youngsam Park, and Damon McCoy. 2016. Stress testing the Booters: Understanding and underminingthebusinessofDDoS services.In*Proceedings ofthe25th InternationalConference onWorldWideWeb*. 1033–1043.

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

[82] SwatiKhandelwal. 2017. ShadowBrokers,WhoLeakedWannaCrySMBExploit,AreBackWithMore0-Days. (2017). http://thehackernews.com/2017/05/shodow-brokers-wannacry-hacking.html

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

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

[85] Nir Kshetri. 2006. The simple economics of cybercrimes. *IEEE Security and Privacy* 4, 1 (2006), 33–39. [86] DanaLahat,TulayAdali, andChristianJutten. 2015. MultimodalDataFusion:AnOverviewofMethods,Challenges, andProspects. *Proc.IEEE*103, 9 (2015), 1449–1477.

[87] AronLaszka,MarkFelegyhazi,andLeventeButtyan.2014. ASurveyofInterdependentInformationSecurityGames. *ACM Computing Surveys (CSUR)* 47, 2 (2014), 1–38.

[88] Stefan Laube andRainer Böhme. 2017. Strategic Aspects of CyberRisk Information Sharing. *Comput. Surveys* Forthcomin (2017).

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

[90] E.R.Leukfeldt.2014. Cybercrimeandsocialties:PhishinginAmsterdam. *TrendsinOrganizedCrime*17,4 (2014), 231–249.

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

[92] Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Mark FelegyhaziGrier, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, andStefanSavage. 2011. Clicktrajectories:End-to-endanalysis ofthe spamvalue chain.In*Proceedings-IEEE Symposium on Security and Privacy*. 431–446.
[93] Nancy G. Leveson. 2011. *Engineering a Safer World: Systems Thinking Applied to Safety*. 555 pages. http://medcontent. metapress.com/index/A65RM03P4874243N.pdf
[94] Weifeng Li, Hsinchun Chen, and Jay F Nunamaker Jr. 2017. Identifying and Profiling Key Sellers in Cyber Carding Community : AZSecure Text Mining System. *Journal of Management Information Systems* 33, 4 (2017),1059–1086. [95] Xiaojing Liao, Damon Mccoy, and Elaine Shi. 2016. Characterizing Long-tail SEO Spam on Cloud Web Hosting Services. In*Proceedings oftheWorldWideWebConference*. 321–332.
[96] VincentLoy,KyraMattar,TanShongYe,BahgyaPerera,JimmySng,andMaggieLeong.2015.*Reclaimingcybersecurity: The Global State of Information Security Survey 2016*. Technical Report. PwC. 1–8pages.
[97] Yong Lu, Xin Luo, Michael Polgar, and Yuanyuan Cao. 2010. Social Network Analysis of a Criminal Hacker Community. *The Journal of Computer Information Systems* 51, 2 (2010), 31.
[98] Robert Luh, StefanMarschalek, ManfredKaiser, Helge Janicke, andSebastian Schrittwieser. 2017. Semantics-aware detectionoftargetedattacks:asurvey.*JournalofComputerVirologyandHackingTechniques*13,1(2017),47–85. [99] Stuart Madnick. 2016. DarkWeb: hackers trump goodguys in sharing information.(2016), 2pages.

[100] StuartMadnick.2017.PreparingfortheCyberattackThatWillKnockOutU.S.PowerGrids.*HarvardBusinessReview* (2017), 5.
[101] Stuart Madnick. 2017. What Executives GetWrongAbout Cybersecurity. *Sloan ManagementReview* January (2017), 22–24.
[102] StuartMadnick,MohammadSJalali,MichaelSiegel,VickiDeng,andDinshaMistree.2017. MeasuringStakeholders 'PerceptionsofCybersecurityforRenewableEnergySystems.In*DataAnalyticsforRenewableEnergy Integration*. 67–77.
[103] Thomas Maillart, Mingyi Zhao, Jens Grossklags, and John Chuang. 2016. Given Enough Eyeballs , All Bugs Are Shallow? Revisiting Eric Raymond with Bug Bounty Programs. In *Workshop on the Economics of Information Security (WEIS)*. 1–19.
[104] Derek Manky. 2013. Cybercrime as a service: A very modern business. *Computer Fraud and Security* 6 (2013), 9–13. [105] Steve Mansfield-Devine. 2016. The imitation game: how business email compromise scams are robbing organisations. *Computer Fraud and Security* 11 (2016), 5–10.
[106] Max Goncharov. 2015. *Criminal Hideouts for Lease: Bulletproof Hosting Services*. Technical Report. Trend Micro. 28 pages.
[107] Inc. McAfee. 2016. *McAfee Labs 2017 Threats Predictions*. Technical Report November 2016. 1–51 pages. http: //www.mcafee.com/us/resources/reports/rp-threats-predictions-2014.pdf
[108] Michael McCaul. 2017. The War in Cyberspace: Why We Are Losing–and How to Fight Back. (2017). https: //www.rsaconference.com/videos/the-war-in-cyberspace-why-we-are-losing-and-how-to-fight-back [109] Damon Mccoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker. 2008. Shining Light in Dark Places : Understanding the Tor Network. In *International Symposium on Privacy Enhancing Technologies Symposium*. 63–76.
[110] Michael McGuire. 2012. *Organised Crime in the Digital Age*. Technical Report September. [111] William Melicher, Blase Ur, Sean M Segreti, Saranga Komanduri, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Fast,Lean,andAccurate:ModelingPasswordGuessabilityUsingNeuralNetworks.In*UsenixSecurity*.239. [112] Max Metzger. 2016. Snapchat got whaled, employee payroll released. (2016). https://www.scmagazineuk.com/ snapchat-got-whaled-employee-payroll-released/article/530493/
[113] TylerMoore.2010. IntroducingtheEconomicsofCybersecurity:PrinciplesandPolicyOptions.In*Workshopon Deterring Cyberattacks: Informing Strategis and DEveloping Options for US Policy*. 3–23.
[114] TylerMooreandRichardClayton.2009.TheImpactofIncentivesonNoticeandTake-down.In*ManagingInformation Risk and the Economics of Security*. 199–223. http://dx.doi.org/10.1007/978-0-387-09762-6
[115] SteveMorgan.2016. *Hackerpocalypse:ACybercrimeRevelation*. TechnicalReport.CybersecurityVentures.1–24 pages.
[116] Robert S. Mueller III. 2012. Combating Threats in the Cyber World: Outsmarting Ter rorists, Hackers, and Spies. (2012). https://archives.fbi.gov/archives/news/speeches/ combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies
[117] Satoshi Nakamoto. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Technical Report. 9 pages. https://bitcoin. org/bitcoin.pdf
[118] Marcin Nawrocki, Matthias Wählisch, Thomas C. Schmidt, Christian Keil, and Jochen Schönfelder. 2016. A Survey on HoneypotSoftware andDataAnalysis.*eprint arXiv:1608.06249* (2016), 1–38.

[119] Arash Nourian andStuart Madnick. 2015. ASystems TheoreticApproach to the SecurityThreats in Cyber Physical Systems Applied to Stuxnet. *IEEE Transactions on Dependable and Secure Computing* PP, 99 (2015), 20. [120] NTTSecurity. 2016. *SERTQuarterlyThreatReport Q2 2016*. TechnicalReport.
[121] G. Odinot, M.A. Verhoeven, R.L.D. Pool, and C.J. de Poot. 2017. *Organised Cybercrime in the Netherlands*. Technical Report. 1–87 pages. https://english.wodc.nl/binaries/Cahier2017-1
[122] Philip O'Kane, Sakir Sezer, and Kieran McLaughlin. 2011. Obfuscation: The Hidden Malware. *IEEE Security & Privacy* 9, 5 (2011), 41–47.
[123] Jeremiah Onaolapo, Enrico Mariconti, and Gianluca Stringhini. 2016. What Happens After YouAre Pwnd : Under standing The Use Of Leaked Account Credentials In The Wild. In *Proceedings of the ACM SIGCOMM Conference on Internet Measurement Conference*. 1–15.
[124] Hilarie Orman. 2013. The compleat story of phish. *IEEE Internet Computing* 17, 1 (2013), 87–91. [125] Andy Ozment. 2004. Bug auctions: Vulnerability markets reconsidered. In *Workshop on Economics of Information Security (WEIS)*. 1–23.
[126] PierluigiPaganini. 2016. Ran$umBinadarkweb servicededicatedtoransomware. (2016). http://securityaffairs.co/ wordpress/46770/breaking-news/46770.html
[127] N Pavkovic and L Perkov. 2011. Social Engineering Toolkit - A systematic approach to social engineering. In *Proceedings ofthe34th InternationalConventiononInformationandCommunicationTechnology,Electronics andMicroelectronics*.

1485–1489.
[128] JeroenPijpker andHarald Vranken. 2016. TheRole ofInternet ServiceProviders inBotnetMitigation.In*2016 European Intelligence and Security Informatics Conference*. 24–31. https://doi.org/10.1109/EISIC.2016.013 [129] Michael Porter. 1985. *Competitive advantage: creating and sustaining superior performance*. The Free Press. 580 pages. [130] Rebecca S Portnoff, Sadia Afroz, U C Berkeley, Greg Durrett, Jonathan K Kummerfeld, Taylor Berg-kirkpatrick, Damon Mccoy, and Vern Paxson. 2017. Tools for Automated Analysis of Cybercriminal Markets. In *World Wide Web Conference*. 657–666.
[131] PwC. 2016. *Global Economic Crime Survey 2016: Adjusting the Lens on Economic Crime*. Technical Report. PwC. 1–31 pages.
[132] Bradley Reaves, Jasmine Bowers, Sigmund Albert, Gorski Iii, North Carolina, Olabode Anise, Rahul Bobhate, Raymond Cho, Hiranava Das, Sharique Hussain, Hamza Karachiwala, Nolen Scaife, Byron Wright, Kevin Butler, and Patrick Traynor. 2016. * droid : Assessment and Evaluation of Android Application Analysis Tools. *Comput. Surveys* 49, 3 (2016), 1–30.
[133] BradleyReaves, Nolen Scaife,DaveTian, Logan Blue,PatrickTraynor, andKevinR.B.Butler. 2016. SendingOut an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. In *2016 IEEE Symposium on Security and Privacy*. 339–356.
[134] Scott Reed and Nando de Freitas. 2016. Neural Programmer-Interpreters. In *ICLR*. 1–13. arXiv:1511.06279 http: //arxiv.org/abs/1511.06279
[135] Rick Holland. 2016. the hacker talent shortage: what organizations can learn from the re cruitment efforts of their attackers. (2016). https://www.digitalshadows.com/blog-and-research/the-hacker-talent-shortage-what-organizations-can-learn-from-the-recruitment-efforts-of-their-attackers/
[136] Rafael a. Rodríguez-Gómez, Gabriel Maciá-Fernández, and Pedro García-Teodoro. 2013. Survey and taxonomy of botnetresearch through life-cycle. *Comput. Surveys* 45, 4 (2013), 1–33.
[137] Charles H. Romine. 2017. Bolstering Government Cybersecurity Lessons Learned from WannaCry. (2017). https: //www.nist.gov/speech-testimony/bolstering-government-cybersecurity-lessons-learned-wannacry [138] ChristianRossow. 2013. *UsingMalware Analysisto EvaluateBotnetResilience*. Ph.D. Dissertation. VrijeUniversiteit.
[139] RSA Whitepaper. 2016. *2016: Current State of Cybercrime*. Technical Report. RSA. 1–7 pages. [140] Hamid Salim and Stuart Madnick. 2016. Cyber Safety : A Systems Theory Approach to Managing Cyber Security Risks-AppliedtoTJXCyberAttack.(2016), 17pages.
[141] HamidMSalim.2014. *Cybersafety : a systemsthinking and systemstheory approach tomanaging cybersecurity risks*. Ph.D. Dissertation. Massachusetts Institute of Technology.
[142] Raj Samani and Francois Paget. 2013. *Cybercrime Exposed: Cybercrime-as-a-Service*. Technical Report. McAfee. 1–18 pages. http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf
[143] Bruce Schneier. 2000. InsideRisks: Semantic NetworkAttacks. *Commun. ACM* 43, 12 (2000), 168. [144] Bruce Schneier. 2015. *Secrets and Lies: Digital Security in a Networked World*. Wiley. 418 pages. [145] Sebastian Schrittwieser,Johannes Kinder, GeorgMerzdovnik,EdgarWeippl, and Stefan Katzenbeisser. 2015. Protecting SoftwarethroughObfuscation:CanIt KeepPacewithProgress inCodeAnalysis? *Comput.Surveys* 49, 4(2015), 1–40.
[146] Ej Schwartz, Thanassis Avgerinos, and David Brumley. 2011. Q: Exploit hardening made easy. In *USENIX Security '11*, Vol. 8. 25.
[147] Offensive Security. 2017. Offensive Security Training, Certifications and Services. (2017). https://www.offensive-security.com/

[148] Securityfocus. 2012. Payload Definition. (2012). http://www.securityfocus.com/glossary/P [149] DaveShackleford. 2015. *CombattingCyberRisksintheSupplyChain*. TechnicalReport. 20pages. https://www.google.co.uk/url?sa=t
[150] Muhammad Shahzad, Muhammad Zubair Shafiq, and Alex X Liu. 2012. A large scale exploratory analysis of software vulnerability life cycles. In *Proceedings of the 34th International Conference on Software Engineering*. 771–781.
[151] Wanita Sherchan, Surya Nepal, and Cecile Paris. 2013. A Survey of Trust in Social Networks. *Comput. Surveys* 45, 4 (2013), 47–47:33.
[152] Sergei Shevchenko. 2016. TWO BYTES TO $951M. (2016). http://baesystemsai.blogspot.com/2016/04/ two bytes-to-951m.html
[153] Yan Shoshitaishvili, Ruoyu Wang, Christopher Salls, Nick Stephens, Mario Polino, Andrew Dutcher, John Grosen, Siji Feng, Christophe Hauser, Christopher Kruegel, and Giovanni Vigna. 2016. SOK: (State of) the Art of War:Offensive Techniques in Binary Analysis. In *IEEE Symposium on Security and Privacy*. 138–157.
[154] Johan Sigholm. 2013. Non-State Actors in Cyberspace Operations. *Journal of Military Studies* 4, 1 (2013), 1–37.
[155] Aditya K. Sood andRichard J. Enbody. 2013. Crimeware-as-a-service-A survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection* 6, 1 (2013),28–38.

[156] AdityaK.SoodandRichardJ.Enbody. 2013. Targetedcyberattacks:Asupersetofadvancedpersistentthreats. *IEEE SecurityandPrivacy* 11,1(2013),54–61.
[157] Kyle Soska, Nicolas Christin, Kyle Soska, and Nicolas Christin. 2015. Measuring the Longitudinal Evolution of the OnlineAnonymousMarketplaceEcosystem.In*the 24thUSENIXSecuritySymposium*. 33–48.
[158] Melvin R J Soudijn and Birgit C H T Zegers. 2012. Cybercrime and virtual offender convergence settings. *Trendsin Organized Crime* 15, 2-3 (2012), 111–129.
[159] RichardSpinello.2016.*Cyberethics:MoralityandLawinCyberspace*(sixthedited.).Jones&BartlettLearning.239 pages.
[160] OleksiiStarov,JohannesDahse,SyedShariqueAhmad,ThorstenHolz,andNickNikiforakis.2016. NoHonor Among Thieves: A Large-Scale Analysis of Malicious Web Shells. In *In Proceedings of the World Wide WebConferernce*. 1021–1032.
[161] William J. Stevenson. 2012. *Operations management* (11th editi ed.). Tim Vertovec. 908 pages. [162] Brett Stone-gross,Ryan Abman,RichardaKemmerer, ChristopherKruegel,Douglas GSteigerwald, andGiovanni Vigna. 2013. TheUnderground Economy of FakeAntivirus Software.In *Economics ofInformation Security andPrivacy III*. 55–78. http://www.springerlink.com/index/10.1007/978-1-4614-1981-5
[163] GianlucaStringhini,OliverHohlfeld,ChristopherKruegel,andGiovanniVigna.2014. Theharvester,thebotmaster, and the spammer: on the relations between the different actors in the spam landscape. In *Proceedings of the 9th ACM symposiumonInformation, computerandcommunicationssecurity*.353–364.
[164] Guillermo Suarez-Tangil, Juan E. Tapiador, Pedro Peris-Lopez, and Jorge Blasco. 2014. Dendroid: A textmining approachto analyzingandclassifyingcode structures inAndroidmalware families. *Expert Systems with Applications* 41, 4 PART 1 (2014), 1104–1117.
[165] Sufatrio, Darell J J Tan, Tong-wei Chua, and Vrizlynn L. L. Thing. 2015. Securing Android : A Survey , Taxonomy , and Challenges. *Comput. Surveys* 47, 4 (2015), 1–45.
[166] Kimberly Tam, A L I Feizollah, N O R Badrul Anuar, Rosli Salleh, and Lorenzo Cavallaro. 2017. The Evolution of AndroidMalwareandAndroidAnalysisTechniques. *Comput.Surveys* 49, 4(2017), 1–41.
[167] Digital Shadows Analyst Team. 2017. Innovation in the underworld: Reducing the Risk of Ripper Fraud. (2017). https:
//www.digitalshadows.com/blog-and-research/innovation-in-the-underworld-reducing-the-risk-of-ripper-fraud
[168] VrizlynnL.L.Thing, HenryC.J.Lee, andMorris Sloman. 2005. Traffic redirectionattackprotectionsystem(TRAPS). In *IFIP Advances in Information and Communication Technology*, Vol. 181. 309–325.
[169] Kurt Thomas, Juan Antonio Elices Crespo, Ryan Rasti, Jean-Michel Picod, Damon Mccoy, Lucas Ballard, Elie Bursztein, Moheeb Abu Rajab, and Niels Provos. 2016. Investigating Commercial Pay-Per-Install and the Distribution of Unwanted Software.In*25thUSENIXSecuritySymposium*. 721–738.
[170] KurtThomas, ChrisGrier,JustinMa, VernPaxson, andDawnSong. 2011. Designandevaluationof a real-timeURL spam filtering service. In *Proceedings - IEEE Symposium on Security and Privacy*. 447–462.
[171] KurtThomas,DannyHuang,DavidWang,ElieBursztein,ChrisGrier,Thomas JHolt, ChristopherKruegel,Damon McCoy,Stefan Savage, andGiovanni Vigna. 2015. FramingDependencies Introducedby UndergroundCommoditization. In*Workshop ontheEconomics ofInformationSecurity*.1–24.
[172] KevinTownsend. 2017. LatestWannaCryTheory: CurrencyManipulation. (2017). http://www.securityweek.com/ latest-wannacry-theory-currency-manipulation
[173] AmitKumarTyagiandGAghila. 2011. AWideScaleSurveyonBotnet. *InternationalJournal ofComputerApplications* 34, 9 (2011), 975–8887.

[174] Sun Tzu. 2005. *The art of war*. Shambhala Publications.
[175] Michel vanEeten,JohannesM.Bauer,HadiAsghari,andShirinTabatabaie. 2010. TheRoleofInternet Service Providers inBotnetMitigation:AnEmpiricalAnalysis BasedonSpamData.(2010), 67pages. [176] Verizon. 2017. *2017 Data Breach Investigations Report*. Technical Report. 76 pages.
[177] Timothy Vidas and Nicolas Christin. 2013. Sweetening Android Lemon Markets: Measuring and CombatingMalware in Application Marketplaces. In *3rd ACM conference on Data and Application Security and Privac*, Vol. 2011. 197–207. [178] JohnWadleigh,JakeDrew,andTylerMoore. 2015. TheE-CommerceMarketforâĂIJLemons âĂİ:Identificationand Analysis of Websites Selling Counterfeit Goods. In *Proceedings of the 24th International Conference on World Wide Web*. 1188–1197.
[179] Wikileaks.2017. Vault7:CIAHackingToolsRevealed.(2017). https://wikileaks.org/ciav7p1/ [180] TrentonAWilliams,DanielAGruber,KathleenMSutcliffe,DeanAShepherd,andEricYanfeiZhao.2017. Organiza tionalResponse ToAdversity: Fusing Crisis Management andResilience Research Streams. *Academy of Management Annals* March (2017), 1–70.
[181] Eric Wustrow and Benjamin VanderSloot. 2016. DDoSCoin: Cryptocurrency with a Malicious Proof-of-Work. In *USENIX Workshop on Offensive Technologies*.

[182] Haitao Xu, Daiping Liu, Haining Wang, and Angelos Stavrou. 2015. E-commerce Reputation Manipulation: The Emergence of Reputation-Escalation-as-a-Service. In *Proceedings of the 24th International Conference on World Wide Web*.InternationalWorldWideWebConferences Steering Committee, 1296–1306.
[183] MichaelYip,NigelShadbolt,andCraigWebber.2013.Whyforums?:anempiricalanalysis intothefacilitatingfactors of carding forums. In *Proceedings of the 5th Annual ACM Web Science*. 453–462.
[184] Kim Zetter. 2014. A Google Site Meant to Protect You Is Helping Hackers Attack You. (2014). https://www.wired. com/2014/09/how-hackers-use-virustotal/
[185] MingyiZhao,JensGrossklags, andPengLiu. 2015. AnEmpiricalStudyofWebVulnerabilityDiscoveryEcosystems. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 1105–1117. [186] ZimingZhao, MukundSankaran,GailJoonAhn,Thomas J. Holt,YimingJing, and Hongxin Hu. 2016. Mules, Seals, and Attacking Tools: Analyzing 12 Online Marketplaces. *IEEE Security and Privacy* 14, 3 (2016), 32–43.

A NOTATION FOR THE CYBERATTACK TARGET SELECTION RULE For a rational cyber-attacker,the victimorganization couldbe consideredas a targetif andonly if the expected benefit B_e outweighs the expected cost C_e.

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

Wesummarize thenotations as following:

- P_e : Ease of the attack, represents how easy to do the cyber attack;
- B_{pm}:Monetarybenefitfromthesuccessful cyberattackagainstthetarget;

B_{pp}: Psychological benefit from the successful cyber attack against the target;

B_p:Potentialbenefitfromthesuccessful cyberattack;$B_p = B_{pm} + B_{pp}$

E_r:Easeofbenefitrealization,representshoweasyforthe attackerto realize thebenefit, includingbothmonetaryandpsychologicalbenefit,fromthe successfulattack;

C_{ps} : Psychological Costs for the attacker to do the cyber attack;

P_a:Arrestrate,represents the attacker being identifiedandarrestedfordoing the cyber attack;

· P_c: Ease of the judicial process involved in the conviction; · C_c: The opportunity cost if the attackeris convicted; · C_p:The expectedpenaltycosts$C_p = P_a \times P_c \times C_c$; · C_{im}:Theinvestmentcostfortheattackertodothecyberattack; · C_{om}:Theopportunitycostfortheattackertodothecyberattack; · C_o: The operational cost$C_o = C_{im} + C_{om}$;

B GLOSSARY FOR CYBERCRIMINAL SERVICE ECOSYSTEM

Table 1. Cybercriminal Services

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

Table 2. Informations for the Cybercriminal Service Ecosystem

V Operational Vulnerability

Vulnerability	V_p

Technical Vulnerability	T
Verified Exploit Kit	E
Exploit Kit	FI
Payload	SCS_R
Botnet	Z
Bulletproof Server	TA
Digital Gain	GP
Monetized Forms of Benefit Directed from Attack	HR
Domain Knowledge	PP
Personal Information	Id
Legal Money	M_D
Money Laundering Network	HZ
User Interaction Records	R
Verified Information	PG
Certificated Hacker with necessary skills	NH

V_t Target VEK Exploit EK Fake Information PL Security Checker Report BN Zombie Machine BH Traffic GD Psychological Gain

GL Human Resource

DK Personal Profile I_p Domain Specific Information M_C Illegal Money MLN Manipulated/Tricked Human RR User Reputation VI Good's Price

CH Novice in the hacker community

Table 3. Tools for the Cybercriminal Service Ecosystem

VDT Obfuscation Tool

Vulnerability Discovery Tool	OBT

Exploit Development and Improvement Tool	*EDT*
Exploit Package Tool	*FDT*
Payload Development Tool	*SCT*
Repackaging tool	*BNDT*
Traffic Redirection Technique	*BHT*
Traffic Generate Tool	*RS*
Multi-modal Data Fusion Technology	*TMS*
Training Support	*V ES*
Online Marketplace Development Tool	*HRT*

EKDT Exploit Development Tool

EPT Deception Development Tool *PDT* Security Check Tool *RPT* Botnet Development and Maintain Tool

TRT Bulletproof Server Tool *TGT* Reputation Mechanism *MDF* Customization and Management Tool

TS Value Verification Tool *MMT* Hacker Recruiting Tool

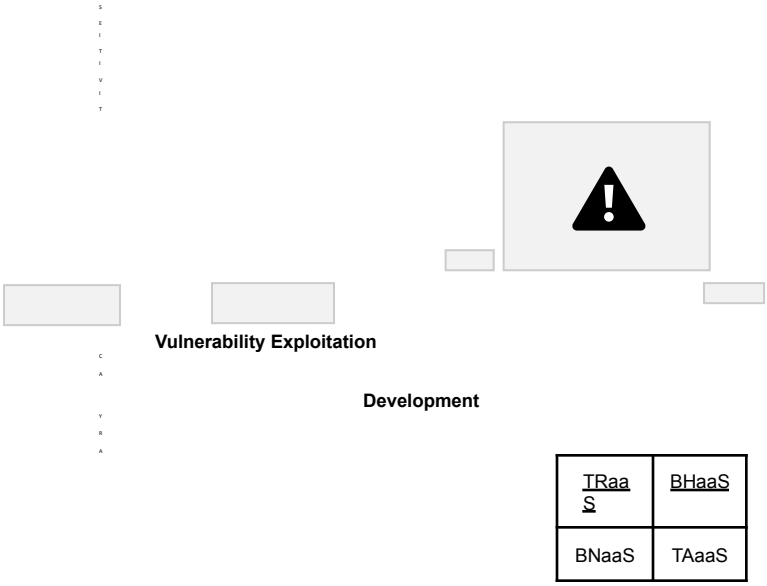
C APPENDIX FIGURES

As showninFigure9,wemapthe services inthe cybercriminal service ecosystemframework constructed in Section 3 into the value chain model presented in Section 2 and group the services intothreedifferent categories:

"No independentservices observed yet":refers to the services which were not observed during .

our study but expected to emerge due to its specialization and existence of the similar innovations in legitimate businesses.

- *"Newserviceforms"*:refers to the services which are available in thedark webbut can evolve into anew business model because ofthedevelopment ofthe technologies.
- *"Others"*:referstotheserviceswhosebusinessmodelisnotexpectedtochangesignificantly.



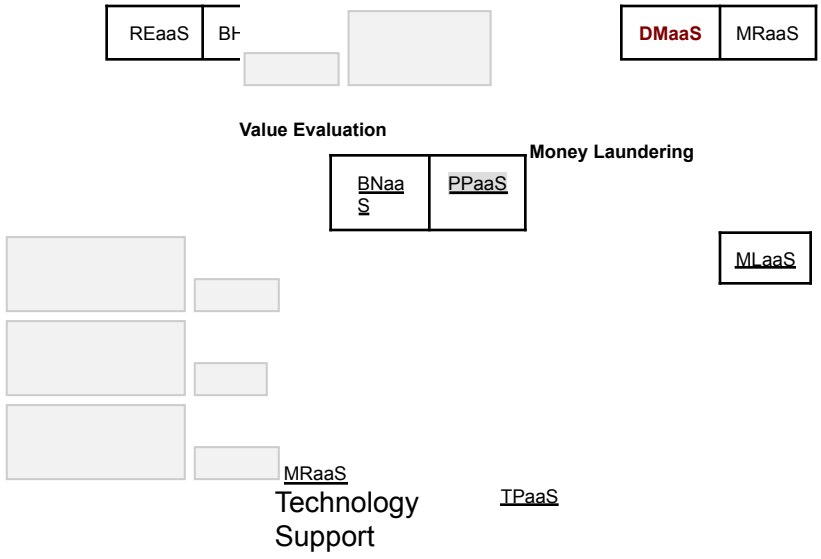
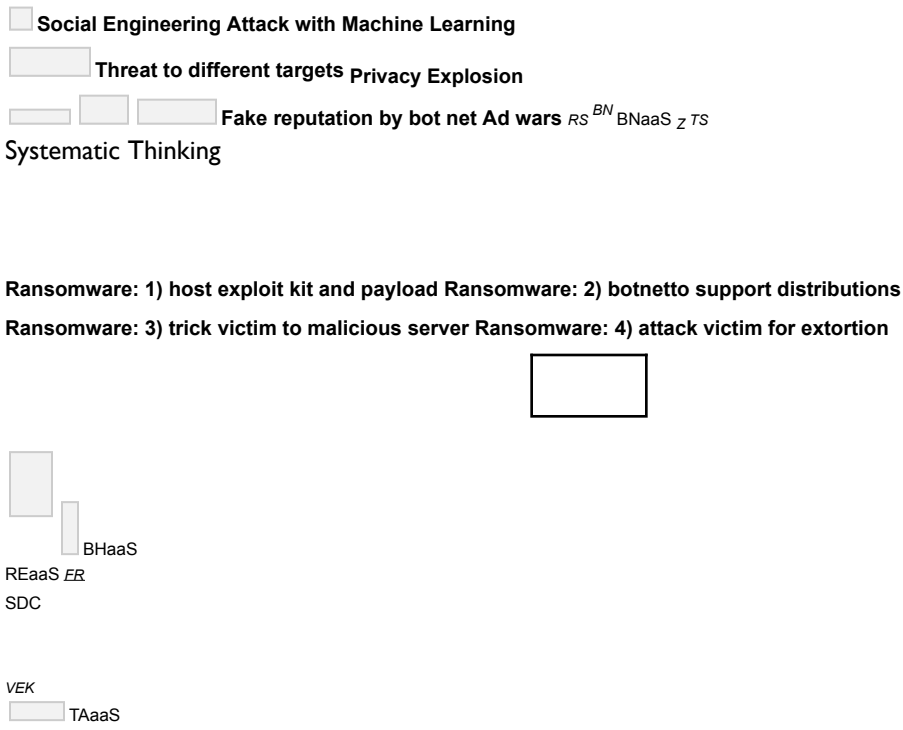


Fig. 9. Mapping between the ecosystem framework and the value chain model to understand the development of the cybercrime services.



TA TGT BS

BNDT

1
MRaaS
HZ

MLaaS
MLN

Mc

of
Cyb
er
Attack

Ransomware: 5) achieveBitcoinTRaaS *TR*
BHT

M T
MMT

Business

EDT

EPT P EK TR TRT GL
V

VDaaS EaaS *E VDT FDT V*

DaaS
EPaaS RPaaS *RPT*

FI

PLaaS *PL*
NI
VEK VEK VEK GD GP

OBS

MPaaS

RR PG RaaS *R*

TMS 4

VEaaS

V_t

PDT^{OB}_{T}

OBaaS

$SCS_{\underline{R}}$
OBS

~~MDF~~

HR 3

$RS_{VES\ VI}$

2

T

SCaaSSCT
DK
HRaaS
TS

1 Loop 1: Compromised Machine reused for attack 2 Loop 2: Breach Information reused for attack

TSaaS
PP
HRT_{CH} HTaaS ^{NH} $_{DK}$

MDF

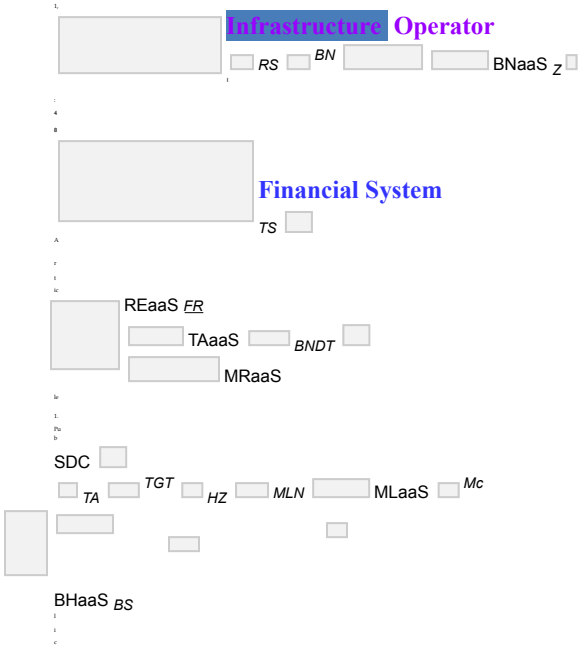
DMaaS $^{I}_{D}$

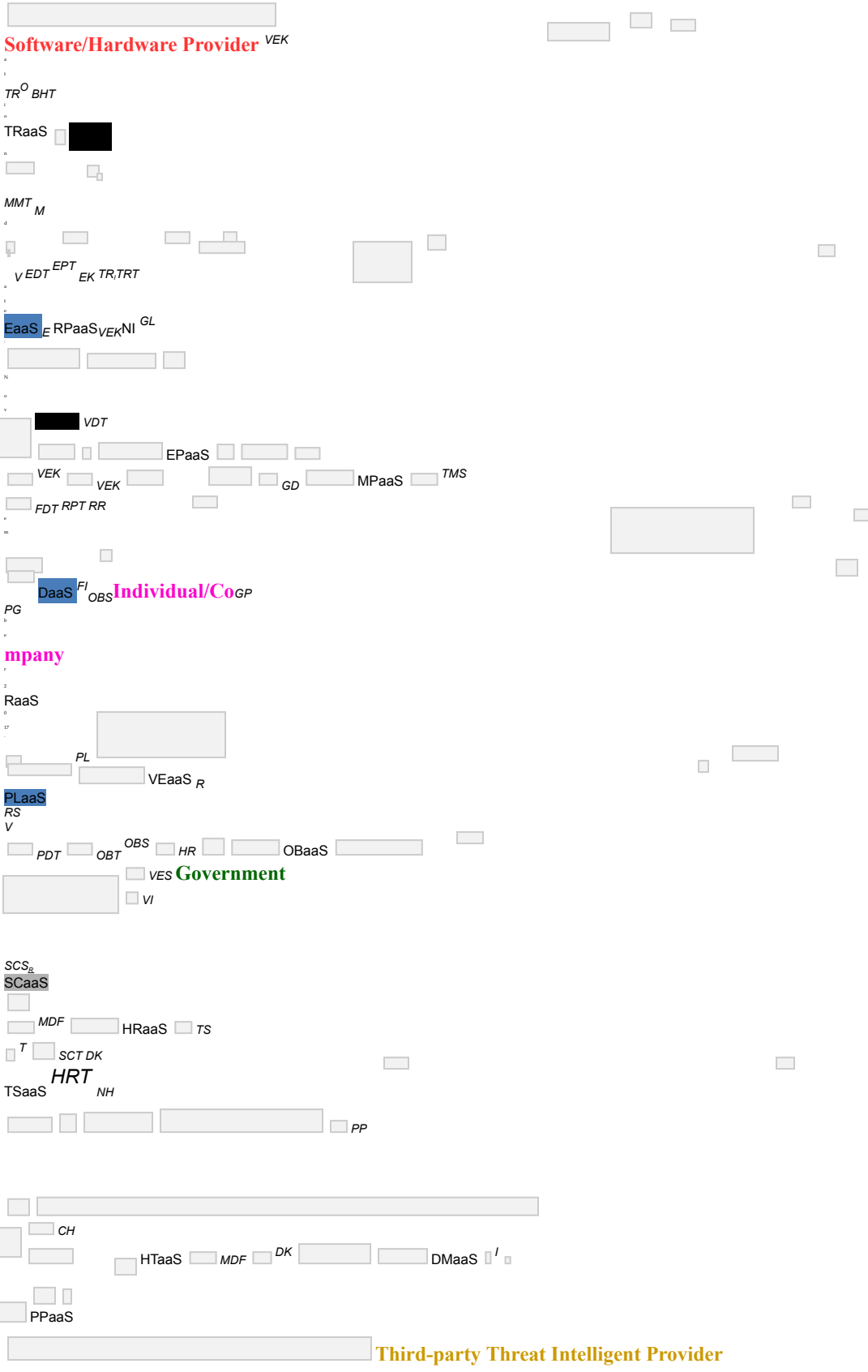
3 Loop 3: Hacking Experience reused for attack 4 Loop 4: Stolen Tools reused for attack

PPaaS

MDF
I_P

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




Software/Hardware Provider
TRaaS
EaaS
RPaaS
NI
EPaaS
MPaaS
DaaS
Individual/Co
mpany
RaaS
PLaaS
VEaaS
OBaaS
Government
SCaaS
HRaaS
TSaaS
HTaaS
DMaaS
PPaaS
Third-party Threat Intelligent Provider

MDF

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