An Experimental Design to Investigate Attacker Actions on an Access-as-a-Service 'Criminal' Platform

Roy Ricaldi*, Yasen Yalamov*, Michele Campobasso※, Luca Allodi*,
Hannah Kool†, Asier Moneva†, E. Rutger Leukfeldt†‡

*Eindhoven University of Technology, Department of Mathematics and Computer Science
{r.j.ricaldi.saavedra, y.yalamov, l.allodi}@tue.nl

†Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)
The Hague University of Applied Sciences, Center of Expertise Cyber Security
{hkool, amoneva, rleukfeldt}@nscr.nl

‡Leiden University, Department of Criminal Law and Criminology and
Institute of Security and Global Affairs

※Vedere Labs, Forescout Technologies
michele.campobasso@forescout.com

***Abstract*—Access-as-a-Service (AaaS) has reduced barriers to cybercriminal activity, enabling less skilled offenders to execute sophisticated attacks relying on remote access to compromised systems. Despite the growing accessibility of these services, little is understood about the factors influencing criminal decisions in the selection of their targets and the ensuing attack process. This short paper outlines the design and implementation of a 'criminal' AaaS platform aimed at attracting cybercriminal users to study their behavior. The platform, modeled after illicit marketplaces in the dark web, includes various market signals to assess their influence on cybercriminal decision-making and a 'honeypot' setup to evaluate attacker actions. In this paper, we describe the methodology and infrastructure for this purpose.**

***Index Terms*—Cybercrime, Target Selection, Underground Forums, Marketplace, Remote Access, Attackers, Honeypots, Field Experiment, Trust Signals**

1. Introduction

Access-as-a-Service (AaaS) has significantly reduced barriers to entry for cybercriminal activities. In contrast to the past, where cybercrime required specialized knowledge, complex technical infrastructure, and advanced skill sets, modern cybercriminals have access to tools and services that facilitate sophisticated attacks. These services are available through illicit online marketplaces that offer a diverse array of products at varying price points. Despite the growing accessibility of these services, there is still a limited understanding of the factors that influence the decision-making processes of offenders in selecting specific services, and ways to attack them. This is also due to a general lack of 'active' measurement experimental setups focusing on criminal actions and decision-making. The process of selecting a target is often overlooked in the literature, traditionally focusing on deploying 'honeypots' to measure attacker actions. Notably, honeypot setups preclude any mechanism on attacker selection (being generally open to any attacker – 'automated scripts' included), and data collected therein is often hard to interpret in terms of attack purpose. In this short paper, we present a novel experimental design aimed at addressing this gap. By focusing on users of cybercriminal communities, we investigate how market signals present on a real(-istic) AaaS platform designed to simulate a real-world illicit marketplace impact the selection of AaaS targets for cyberattacks. The experiment seeks to explore how potential cybercriminals interact with and exploit compromised systems made available through these platforms.

To ensure the operational functionality of our experimental setup prior to deployment in real-world cybercriminal forums, we conducted an internal pilot with members of our research group. This pilot was carried out in two phases. The first phase focused on pentesting the system from the perspective of a potential attacker, with participants actively searching for signs that could reveal the honeypot nature of the marketplace or the compromised machines. The second phase simulated the full user experience under realistic constraints, including time-limited access to targets and the requirement to interact with a Telegram bot for registration. These internal tests allowed us to identify and address issues related to usability, platform realism, and data collection integrity. Although this pilot did not involve external participants, it validated the core infrastructure and offered early insights into the types of data we expect to gather in the live experiment, such as attacker selection patterns, interaction behaviors on both the marketplace and machines, and responses to varying levels of target information. This paper outlines our goals and experimental design to collect community feedback and discuss implementation, ethical, and technical challenges of the proposed active measurement setup.

2. Literature Review and Research Gap

Cybercrime-as-a-Service (CaaS) marketplaces are online platforms where cybercriminals offer malicious services to buyers. These services can include everything from the sale of simple hacking tools to more sophisticated services such as Ransomware-as-a-Service, designer malware, and Hacking-as-a-Service [1] [2]. Studies have found that CaaS markets offer such a wide variety of services that getting involved in cybercrime through these markets has become much easier [3] [4] [5] [6]. In this way, cybercrime tools become more available and accessible to a wider audience.

An example of a specialized service is Access-as-a-Service (AaaS), which consists of the sale of access to compromised systems, generally pertaining to organizations [7]. There are specialized marketplaces that focus on selling these types of access. These marketplaces often share similar characteristics: accesses are presented in tabular format such that the buyer can sort and filter based on different characteristics such as county of origin, price, type of access, and system specification [8].

In AaaS marketplaces, sellers typically offer access in the form of compromised credentials from an organization's network. These accesses often include Secure Shell (SSH) and Remote Desktop Protocol (RDP) credentials [8]. Using these accesses, buyers can then move within a company's network ('lateral movement' [9]), representing a possible initial foothold to additional attack steps (e.g. to implant ransomware on key systems). These marketplaces are known to sell access to environments with different characteristics. How and if a description of these characteristics is presented to the buyer varies from market to market [10]. This raises the question of whether, when having a choice, attackers have a preference for targets with certain characteristics.

2.1. Attacker Preferences and Choices

In online illicit markets, buyers cannot be sure of the intentions of a seller or product quality. This information asymmetry creates opportunities for scammers because it allows untrustworthy sellers to offer their low-quality products at competitive prices [11]. Akerlof [12] described this phenomenon as a "market for lemons" in which conditions of information asymmetry between buyers and sellers encourage sellers to offer low-quality goods, because buyers have no way to evaluate the qualities of the offered products (or trustworthiness of the seller). As a solution, sellers on dark web marketplaces and other CaaS platforms use trust signals to reassure buyers that they are reliable and trustworthy [13], [14]. These are distinguished between structural trust signals, such as review systems and escrow services, and user-driven trust signals, such as maintaining a credible profile, providing clear payment details, offering competitive prices, and providing professional customer service. However, trust signals do more than just shape buyer behavior, they also influence how attackers select their targets. For example, recent research suggests that attackers show clear preferences for certain regions over others [15]. In addition, by providing more detailed product or contact information on a platform, sellers show that they are more reliable and willing to help [3]. In this context, all available product attributes function as signals when analyzing the preferences of attackers for different products [16].

2.2. Attacker Interaction Measurement

Maimon et al. [17] conducted one of the first criminological studies using honeypots to examine how warning banners influence unauthorized access. Their findings illustrate how honeypots can be a valuable tool for (criminological) research. Honeypots are computer tools designed to attract Internet users to interact with them, allowing researchers to collect the data that these interactions generate [18]. Unlike traditional research methods employed in criminology that rely on self-reported data, honeypots allow researchers to observe actual user behavior. Moreover, they allow researchers to conduct controlled experiments in which they can manipulate specific conditions [19]. Because honeypots are often released in real-world environments, they can capture large volumes of interactions, resulting in large sample sizes [20]. Given these benefits, honeypots are valuable for studying attacker behavior and gaining insight into the measurement and decision-making processes of attacker interaction. However, traditional honeypots open to the Internet may attract actors with different purposes, including researchers, automated scanning tools, script-kiddies, as well as outright criminals. It remains therefore a challenge to study criminal behavior on traditional honeypot designs.

2.3. Research Gap and Contribution

Although the criminological literature on target selection in traditional crime is rich (e.g. [21]–[23]), there is a lack of empirical research on how attackers evaluate and choose a target in an online context. Existing studies focus on broader themes of cybercriminal behavior, such as motivations driving attacks or the technological tools available to them. There are some exceptions (e.g. [24] and [25]). However, this research does not provide insight into the tactical decisions that attackers make during their interactions with AaaS platforms. Furthermore, previous studies on attacker preferences and choices examine these factors in isolation, focusing either on the attacker's technical profile or the dynamics of the marketplace. To the best of our knowledge, no attempts have been made to integrate both aspects: how an attacker's technical skills and their positioning within illicit communities influence their interactions with AaaS platforms. This is a critical gap, as understanding how these different factors intersect can provide insights into attacker behavior and decision-making processes.

This paper addresses these gaps by proposing a novel experimental design for studying AaaS platforms in a way that allows for detailed measurement of attacker actions and decisions. The main research question that guides this study is the following:

How can we design and implement an Access-as-a-Service platform intended to attract cybercriminal users and measure their actions in terms of target selection and attack procedure and sophistication?

The objective of this paper is to present the design of an Access-as-a-Service (AaaS) platform that can attract

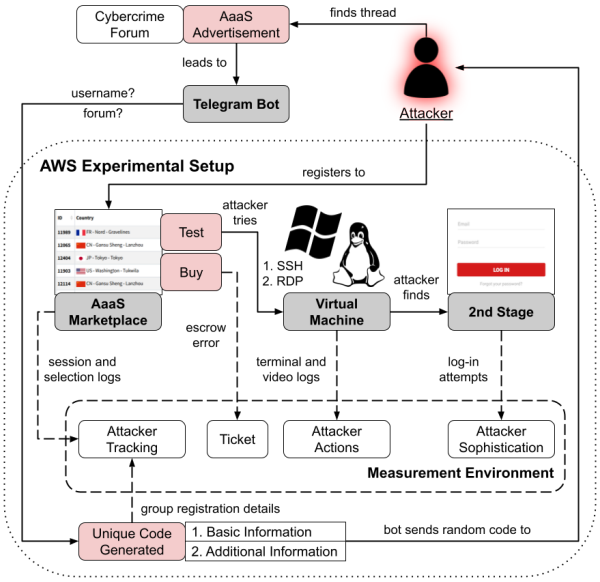

Figure 1. Overview of the methodological approach

cybercriminal users and allow for detailed measurement of their interactions with the system. Understanding attacker preferences within AaaS platforms enables more precise deployment of defensive mechanisms and more targeted law enforcement interventions, particularly in distinguishing opportunistic versus highly strategic attackers.We present the design of a research infrastructure aimed at attracting and observing cybercriminal users in a (simulated, but realistic) illicit environment. Further we provide a methodology for the measurement of attacker interactions, capturing and analyzing attacker behavior within AaaS platforms, setting a foundation for future research aimed at understanding attacker modus operandi.

3. Methodology

The following explains the approach we propose and the implementation requirements that our experimental process entails. More technical elements such as network architecture, logging mechanisms, and VM reset protocols are abstracted. We stress that, because the experiment has still to be run, we refrain from giving very specific details on the implementation (e.g. market advertisement, UI/UX of the marketplace, etc.) to avoid jeopardizing the experiment run. Rather, we focus on the high-level method we propose and adopt.

The overall idea is to build and advertise in the cybercriminal ecosystem a 'criminal' AaaS service that allows users to, for a limited time, 'test' the service by accessing one of several bot machines (i.e. honeypot systems) available on the platform. Users are randomized to either a treatment or a control group, differing only by the amount of technical information provided on the available bots. To evaluate attacker decisions, we track attacker actions on the marketplace related to target selection, and have full visibility of attacker actions on the 'hacked' system. Figure 1 provides an overview of the proposed methodology. The first phase involves advertising our 'AaaS' infrastructure on selected forum marketplaces. Participants of these forums can choose to register for access on our platform,

TABLE 1. SUMMARY OF DATA COLLECTED PER STAGE.

Stage	Data Collected	Purpose
Telegram Bot	- Attacker recruitment registration details: Forum and Username	To track the origin of attackers and enforce the authenticity of registrations.
AaaS Marketplace	- Session logs (attacker interactions: clicks, mouse hovers, etc.) - Target selection (virtual environments, RDP/SSH options)	To monitor the attacker's interaction with the marketplace and identify usage, preferences, and selection patterns.
'Compromised' Machine	- Terminal logs (SSH commands) - Video logs (RDP interactions)	To track attacker behavior within the VMs and understand their attack tactics.
Landing Page	- Password attempts (username and password combinations)	To measure the sophistication of the attacker based on their ability to crack passwords.

and are assigned to either the treatment and control group upon registration. Registered users have access to a list of available bots and are informed that they can try any bot of their choice, for free, for a maximum of 10 minutes. We track user choices on which bots to evaluate before making a decision.[1] Attackers can choose to access a Linux machine via SSH (i.e. command line), or a Windows machine via RDP (i.e. remote desktop). They can only try one machine for a maximum of ten minutes. We record attacker actions on both machines. If the attacker finds relevant information on the machine, they can access a 'second stage' website where we track whether they were able to solve a technical challenge related to cracking encrypted passwords found on the selected machine. A summary of the recorded data is provided in Table 1. Our platform closely mirrors real-world AaaS marketplaces by incorporating common elements such as Telegram-based registration, access listings with metadata (e.g., OS, location, price), and marketplace-style trust signals. While it abstracts away social dynamics like direct messaging or long-term reputation, it isolates core decision-making processes in a controlled yet realistic setting. This design enables us to draw meaningful insights about attacker behavior that can generalize to AaaS criminal markets. We detail the whole procedure below.

3.1. Attacker Recruitment

Our approach starts with the recruitment of the attackers on cybercriminal forums. The AaaS marketplace is advertised by posting threads in different dark web forums. We choose a starting list of five forums of different type (in the sense of [11]) with related sections, and draft a single thread to advertise the platform in all of them. The thread has a link to the AaaS Marketplace, and a link to a Telegram Bot needed to receive a registration code to be able to register on the Marketplace. The attacker must give the Telegram bot information on which forum they come from and what their username is in it. The association between forum identity and telegram ID is

1. The option to buy a bot will not work, showing a technical error preventing the purchase (to minimize backfire, the market is advertised as in 'beta testing').

used to mitigate the risk that the same user will register to the market multiple times with different accounts. Users are then provided with a unique registration code from a list of random codes that the Telegram bot keeps. This code is used by the attacker to register an account on the advertised AaaS marketplace.

The researcher uses this code to uniquely identify and track the attacker and the forum from which they come from. The attacker is randomly assigned to one of two distinct experimental groups. Attackers in Group 1 have access to an AaaS Marketplace that provides only basic information on their targets; attackers in Group 2 have access to an AaaS Marketplace that gives them the option to get additional information through a drop-down button on the targets. This between-markets design allows to examine the effect of providing additional information to potential attackers on their target selection. After the attacker authenticates the unique code granted by the Telegram Bot, they register on the AaaS Marketplace and can view its offerings.

3.2. Access to the AaaS Marketplace

The AaaS marketplace simulates services found on cybercriminal platforms, catering to attackers seeking remote access to systems. The site displays many access targets. Session logs are saved at this stage for attacker tracking. The platform records all attacker interactions with the marketplace, such as clicks, mouse hover events, page visits, and selections of virtual environments, using (obfuscated) JavaScript-based telemetry tools.

Attackers can select and test a single target for free within a trial period of ten minutes. The interface allows attackers to connect to and interact with these environments directly from their browser. Each target has different characteristics that the attacker can consider, such as country, access type, operating system, price, and date added (capped at one year prior). Additionally, attackers in Group 2 have access to 'additional information' about the advertised bot, such as obfuscated IP address and software pre-installed on the machine. The specific characteristics of each VM target vary, and some countries are more represented than others, as is often found in the wild [26]. We provide two types of access: RDP for Windows machines or SSH for Linux machines. The advertised prices range from 3 to 30 dollars and are assigned following findings in [26]. The action column is binary, and attackers can only select whether to 'test' or 'buy' a machine.

When a customer selects the 'test' option, they are informed they only have 10 minutes to test the machine and that their choice of which machine to test is final. The 10-minute window balances the risk of honeypot detection with the time needed for an attacker to meaningfully interact with the system—exploring files, accessing the database, and attempting password cracking. While it appears effective, we remain open to adjusting it based on attacker behavior once deployed on cybercrime forums. Upon confirmation, a new browser tab opens with access to their machine of choice via the dedicated method (SSH, RDP). All attempts to buy a machine return a fictitious escrow error. To mitigate potential frustration, users are subtly informed during recruitment and in the marketplace interface that the service is currently in beta and that some functions may be temporarily unavailable. In addition, users can submit private feedback through a ticketing system, visible only to themselves and the platform operators. Although we acknowledge that this cannot prevent forum users from voicing their discontent publicly, this design aims to redirect and contain negative feedback by managing expectations early and offering a private channel for complaints. We discuss this threat in section 4.

3.3. Access to a 'Compromised' Machine

Once attackers access the 'compromised' (virtual) machine via RDP or SSH, all their actions on the machine are monitored. We record the terminal history when connected via SSH and do a video capture of actions when connected via RDP. Terminal logs are kept to capture commands executed via SSH. Video logs record interactions via RDP sessions to visually document the attacker's behavior. The technical implementation of both options is such that it is invisible to the attacker (i.e. does not run as a process in the accessed machine). The use case for the machinies is that of a fictional e-commerce backend system containing customer information related to purchases on a e-commerce website. This is implemented as a database on the machine containing a 'user' table and a 'tickets' table. Each table is filled with the fabricated data related to the use case. The attacker can authenticate to the database and view (and edit) its contents. The user table contains hashed passwords and username combinations. To avoid suspicion, the database contains a mix of well-known passwords that are trivial to crack, and more difficult ones. The ticket table contains plausible but fictitious tickets all linking to the second-stage website (see below).

The use case is implemented on Windows (RDP connection) and Linux (SSH), but the two machines are identical otherwise. The machines are hosted by a popular service provider who was informed of the experiment in advance and agreed to host the infrastructure. Each attacker accesses a fresh instance of the machine they choose, i.e. their environment is not affected by previous attackers.

3.4. Second Stage Landing Page

Lastly, the attacker can find the landing page referenced in the database on the VM. This leads to a log-in page where the attacker can username and password combinations based on the information they found in the database. The sophistication of the attacker is measured by whether they were able to find all relevant information and crack the passwords. We note that authentication always fails, even if the attacker finds the right password, so no further attack steps are possible at this stage. All activity is recorded on the backend and retrieved when the trial time runs out. The attacker is then redirected to the website panel where they can select to buy the machine they tested, or other machines available.

4. Discussion on Experimental Challenges

Due to the complexity and novelty of the experimental setup, ethical and technical challenges arise. We discuss these in the following section.

4.1. Ethical Challenges

Active measurement of criminal actions entails new risks and ethical questions that are not generally relevant when 'simply' passively observing attackers (e.g. by crawling forum data). The experiment raises questions on user deception, the capturing of behavioral data, the advertising of (pretended) illegal services, and the provision of a platform were to seemingly engage in illegal activities. To uphold ethical standards, we sought advice from our institutions as well as the Ethics Committee for Legal and Criminological Research (CERCO) of the Vrije Universiteit Amsterdam. We received ethical clearance from the ethics committee; following the considerations above, our environment does not collect private data on the attackers, but only on their interactions. We ensure that the study does not inadvertently encourage or promote illegal activities by educating participants about the illegality of the service: at the end of the experiment, users of the forums in which the market is advertised are informed that the service has been stopped by the hosting provider due to illegal activity.

Further, the simulated environment is carefully designed not to provide real-world utility for engaging in cybercriminal actions. Attackers cannot utilize the infrastructure we created to continue their illicit activities. Importantly, we had to strike a balance between realism of the platform and minimizing negative impact on the (deceived) users. The users freely choose to engage in an activity they may well engage in otherwise and in which they are interested. In this sense, we do not believe our setup 'wastes' subject time by deceiving them in engaging in a behaviour they wouldn't engage with otherwise, given the opportunity to. On the other hand, we draw a line the moment a financial interaction is initiated on the side of the user, to avoid any negative economic repercussion on them, at the cost of creating the perception that our experimental setup is a market that cannot, effectively, sell anything. This may negatively affect experimental outcomes by, for example, compromising our stance on the market in which we advertise the platform. On the other hand, we consider this a necessary ethical trade-off.

4.2. Technical Challenges

4.2.1. Experimental Setup and Infrastructure. The goal is to design an experiment that accurately simulates a 'criminal' AaaS marketplace while controlling for exogenous variables. This balance between experimental control and realistic conditions (e.g., attacker motivations, credible recruitment tactics, environmental factors, etc.) presents a technical challenge in terms of how the marketplace is designed, how interactions are structured, and how 'realism' is preserved through the experiment without crossing ethical boundaries. Beyond the methodology design, building the technical infrastructure requires hosting VMs with different operating systems and configurations for attackers to test. Ensuring that each VM instance is fresh and properly isolated for each attacker is important to maintain the integrity of the experiment. Automation of this process is technically complex, especially when the system must scale or handle a larger number of simultaneous users.

4.2.2. Recruitment and Participant Verification. A key challenge is ensuring that users registering on the platform are unique participants. While attackers could, in principle, create multiple Telegram accounts to obtain more registration codes, Telegram requires each account to be linked to a unique phone number,[2] adding a real-world barrier to mass registration. Given that our platform is advertised as a beta service with no real purchasing functionality, we believe the incentive for attackers to invest effort into creating multiple accounts is low.

Although we cannot verify the truthfulness of self-reported forum usernames, we collect this information to study community-level differences in behavior and as a deterrent against casual multi-registration. We acknowledge this limitation but argue it does not undermine our greater goal of measuring attacker decision-making in a controlled setting.

4.2.3. Data Collection and Tracking. The experiment involves collecting large amounts of interaction data, session logs, mouse clicks, page visits, terminal histories, and video captures of what the user does within the VM. Storing, organizing and analyzing these is a major technical hurdle. It is key that data capture ensures that it is done efficiently without overwhelming the storage or network infrastructure, and making sure it remains transparent to the user. For example, reliance on JavaScript-based telemetry to track mouse movements, clicks, and page views, as well as SSH/RDP monitoring, presents a potential challenge in ensuring the accuracy and reliability of the data: misleading data could occur due to browser compatibility, latency issues, or a failure to capture interactions properly.

We conduct an internal pilot to thoroughly study the flaws in data collection and tracking. Ensuring that all attacker actions are fully logged and captured for later analysis, while also reverting machines to their original state after the experiment concludes, poses both technical and logistical challenges that must be verified for a successful experience. This can be complicated even more by technical limitations, such as insufficient backup systems or challenges in automating the reset of VMs, which can affect the experiment's validity and reliability. We employ a mix of obfuscation to record attacker choices on the marketplace, and container services outside of the VM to record actions on the accessed machines. This ensures that it remains hard or impossible for users to notice the data capturing. To assess this risk, we included a pentesting phase in our internal pilot, where participants attempted to identify monitoring. Their feedback helped refine the setup, though we accept that sophisticated users may still look for signs of deception.

Acknowledgment

The authors would like to thank the Cyber Offender Prevention Squad of Team High Tech Crime, Netherlands Police, for their helpful comments and suggestions during the design of the experiment. This publication is part

2. Telegram enforces a one-account-per-phone-number policy, which adds cost and friction to creating multiple identities. Virtual numbers may be used, but they are not free or trivially scalable.

of the INTERSECT project (Grant: NWA.1160.18.301) which is partly financed by the Dutch National Research Council (NWO). This research was also supported by Politie en Wetenschap under Grant No. PW/OV/2023/27.10.

References

[1] T. Hyslip, *Cybercrime-as-a-Service Operations*. Springer International Publishing, 2020, pp. 815–846.

[2] H. Saleous, M. Ismail, S. H. AlDaajeh, N. Madathil, S. Alrabaee, K.-K. R. Choo, and N. Al-Qirim, "Covid-19 pandemic and the cyberthreat landscape: Research challenges and opportunities." *Digital Communications and Networks*, vol. 9, pp. 211–222, 2023.

[3] A. Hutchings, R. Clayton, and R. Anderson, "Taking down websites to prevent crime." in *2016 APWG Symposium on Electronic Crime Research (eCrime)*, 2016, pp. 1–10.

[4] L. Sebagh, J. Lusthous, E. Gallo, F. Varese, and S. S, "Cooperation and distrust in extra-legal networks: A research note on the experimental study of marketplace disruption," *Global Crime*, vol. 23, no. 3, pp. 259 – 283, 2022.

[5] U. Akyazi, M. van Eeten, and C. H. Gañán, "Measuring cybercrime as a service (caas) offerings in a cybercrime forum," in *Proceedings of the 2021 Workshop on the Economics of Information Security (WEIS)*. Online Conference, 2021. [Online]. Available: https://weis2020.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-akyazi.pdf

[6] D. Manky, "Cybercrime as a service: A very modern business," *Computer Fraud & Security*, vol. 2013, 2013.

[7] TrendMicro, "Investigating the emerging access-as-a-service market," 2021. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/investigating-the-emerging-access-as-a-service-market

[8] KelaCyber, "Access-as-a-service - remote access markets in the cybercrime underground," 2020. [Online]. Available: https://www.kelacyber.com/blog/access-as-a-service-remote-access-markets-in-the-cybercrime-underground/

[9] MITRE ATT&CK, "Mitre att&ck®," 2023, accessed: 2023-02-24. [Online]. Available: https://attack.mitre.org

[10] SentinelOne, "More evil markets — how it's never been easier to buy initial access to compromised networks," 2022. [Online]. Available: https://www.sentinelone.com/blog/more-evil-markets-how-its-never-been-easier-to-buy-initial-access-to-compromised-networks/

[11] M. Campobasso, R. Rădulescu, S. Brons, and L. Allodi, "You can tell a cybercriminal by the company they keep: A framework to infer the relevance of underground communities to the threat landscape," *22nd Workshop on the Economics of Information Security*, 2023.

[12] A. Akerlof, G, "The market for "lemons": Quality uncertainty and the market mechanism." *The Quarterly Journal of Economics*, vol. 84, 1970.

[13] J. R. Lee, "Understanding markers of trust within the online stolen data market: An examination of vendors' signaling behaviors relative to product price point," *Criminology & Public Policy*, vol. 22, no. 4, pp. 665–693, 2023. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/1745-9133.12651

[14] D. Laferrière and D. Décary-Hétu, "Examining the uncharted dark web: Trust signalling on single vendor shops. deviant behavior," *Deviant Behavior*, vol. 44, 2023.

[15] M. Campobasso and L. Allodi, "Know your cybercriminal: Evaluating attacker preferences by measuring profile sales on an active, leading criminal market for user impersonation at scale," pp. 553–570, Aug. 2023. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23

[16] B. Connelly, T. Certo, R. Ireland, and C. Reutzel, "Signaling theory: A review and assessment," *Journal of Management - J MANAGE*, vol. 37, pp. 39–67, 01 2011.

[17] D. Maimon, M. Alper, B. Sobesto, and M. Cukier, "Restrictive deterrent effects of a warning banner in an attacked computer system," *Criminology*, vol. 52, pp. 33–59, 2014.

[18] L. Spitzner, *Honeypots: tracking hackers*. Addison-Wesley, Boston, 2002.

[19] R. C. Perkins and C. J. Howell, *Honeypots for cybercrime research.* Palgrave Macmillan, 2021, pp. 233–261.

[20] A. Moneva, E. R. Leukfeldt, and M. Romagna, *Fieldwork experiences researching cybercriminals*. Springer International Publishing, 2023, pp. 511–533.

[21] M. Townsley, D. Birks, W. Bernasco, S. Ruiter, S. D. Johnson, G. White, and S. Baum, "Burglar target selection: A cross-national comparison," *Journal of Research in Crime and Delinquency*, vol. 52, no. 1, pp. 3–31, 2015, pMID: 25866418. [Online]. Available: https://doi.org/10.1177/0022427814541447

[22] E. Beauregard, M. F. Rebocho, and D. K. Rossmo, "Target selection patterns in rape," *Journal of Investigative Psychology and Offender Profiling*, vol. 7, no. 2, pp. 137–152, 2010. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/jip.117

[23] M. Townsley, D. Birks, S. Ruiter, W. Bernasco, and G. White, "Target selection models with preference variation between offenders," *Journal of Quantitative Criminology*, vol. 32, no. 2, pp. 283–304, Jun 2016. [Online]. Available: https://doi.org/10.1007/s10940-015-9264-7

[24] W. S. Danielle Stibbe, Stijn Ruiter and A. Moneva, "Rational choice on a hacker forum: The effect of risk and reward cues on target selection for account hijacking," *Deviant Behavior*, vol. 0, no. 0, pp. 1–22, 2025. [Online]. Available: https://doi.org/10.1080/01639625.2025.2459699

[25] M. Tajalizadehkhoob and S. Author, "Title of the paper," in *Proceedings of the 2014 Workshop on the Economics of Information Security (WEIS)*, 2014. [Online]. Available: https://econinfosec.org/archive/weis2014/papers/Tajalizadehkhoob-WEIS2014.pdf

[26] M. Campobasso and L. Allodi, "Impersonation-as-a-service: Characterizing the emerging criminal infrastructure for user impersonation at scale," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1665–1680. [Online]. Available: https://doi.org/10.1145/3372297.3417892