Stolen Data Markets on Telegram: A Crime Script Analysis and Situational Crime Prevention Measures

Taisiia Garkava [1] (https://orcid.org/0000-0002-4330-4739)

Asier Moneva [1, 2] (corresponding author) (https://orcid.org/0000-0002-2156-0213)

E. Rutger Leukfeldt [1, 2] (https://orcid.org/0000-0002-3051-0859)

Author affiliations

[1] Center of Expertise Cyber Security, The Hague University of Applied Sciences

Johanna Westerdijkplein 75, 2501 EH The Hague (Netherlands)

[2] Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)

De Boelelaan 1077, 1081 HV Amsterdam (Netherlands)

E-mail address of the corresponding author

amoneva@nscr.nl

Stolen Data Markets on Telegram: A Crime Script Analysis and Situational Crime Prevention Measures

Abstract

Illicit data markets have emerged on Telegram, a popular online instant messaging application, bringing together thousands of users worldwide in an unregulated exchange of sensitive data. These markets operate through vendors who offer enormous quantities of such data, from personal identification information to financial data, while potential customers bid for these valuable assets. This study describes how Telegram data markets operate and argues what interventions could be used to disrupt them. Using crime script analysis, we observed 16 Telegram meeting places encompassing public and private channels and groups. We obtained information about how the different meeting places function, what are their inside rules, and what tactics are employed by users to advertise and trade data. Based on the crime script, we suggest four feasible situational crime prevention measures to help disrupt these markets. These include takedowns of data marketplaces, reporting, application of spamming and flooding techniques and the use of warning banners.

Keywords: cybercrime; cyber offenders; data markets; Telegram; crime script; situational crime prevention

Introduction

Since the advent of the Internet, the world has entered an era of globalization that has changed the way businesses operate (Demant et al., 2019). Companies have quickly embraced the technological advances of this era, including the storage of personal and customer data in large digital databases (Holt & Smirnova, 2014). At the same time, cyber offenders have found ways to exploit vulnerabilities in such storage systems to gain illicit access to valuable goods and data and sell them in illicit markets (Holt & Lampke, 2010). Both individuals and criminal organizations participate in these markets—which act as offender convergence settings—either as administrators, moderators, vendors, or customers. Illicit marketplaces democratize cybercrime by making a range of cybercrime products and services available to the public at reasonable prices. It is crucial to understand how these markets operate in order to disrupt them.

There are many illicit online marketplaces—both on the clear and the dark web—that offer products such as cybercrime tools and malware (Leukfeldt et al.,2017a;2017c; van Hardeveld et al., 2017), drugs (Aldridge & Askew, 2017; Cunliffe et al., 2017; Décary-Hétu & Giommoni, 2017; Demant et al., 2019; Jardine, 2021; Ladegaard, 2019; Morselli et al., 2017), forged identity documents (Holt & Lee, 2022a), firearms (Broadhurst et al., 2021; Copeland et al., 2020; Holt & Lee, 2022b; Lee et al., 2022) and stolen data (Dupont et al., 2017; Hutchings & Holt, 2017; Ouellet et al., 2022).

These markets can be defined as "collection[s] of the skilled and unskilled suppliers, vendors, potential buyers, and intermediaries for goods or services surrounding digitally based crimes" (Ablon et al., 2014, p. 3). Since the trend of compromising databases is increasing among cyber offenders, online markets for trading data of illicit origin or the so-called *stolen data* have emerged (Dupont et al., 2017; Holt et al., 2016; Holt & Lampke, 2010; Holt & Smirnova, 2014; Hutchings & Holt, 2017; Motoyama et al., 2011; Ouellet et al., 2022). Stolen data refers to the electronic information collected as a result of "exploitation of the vulnerability in a computer system or an unauthorized leak by someone with access to the data" (Thomas et al., 2017, p. 1). Several of such stolen data markets have been discovered in an application called 'Telegram' (Kamps & Kleinberg, 2018).

Telegram is an encrypted messaging service that has gained popularity among cyber offenders due to its convenience and acclaimed anonymity (Telegram, 2022b). In Telegram, users can create groups and channels to 'meet' and communicate. Groups and channels therefore act as online 'meeting places'. These meeting places can be separated into private and public places, depending on access restrictions. While public places can be accessed by anyone who does a search inside the application, private places can only be accessed by invitation (Telegram, 2022b).

There are many different meeting places on Telegram that cover a variety of topics, varying from legal to illegal. Some of them are used to trade sensitive data containing millions of records. These meeting places constitute 'gold mines' for cyber offenders aiming to use the data for various purposes, including phishing and creating fake credit cards (Hutchings, 2014). Some meeting places can therefore act as online offender convergence settings (Leukfeldt et al., 2017a; 2017c; Miró Llinares & Johnson, 2018; Moneva, 2020). The ability to disseminate files to large audiences within Telegram enables cyber offenders to continually exploit sensitive data circulating through the platform. However, the specifics of how these stolen data markets operate in Telegram are largely unknown, which complicates their disruption (Holt & Lampke, 2010; Hutchings, 2014; Hutchings & Holt, 2015, 2017). This paper investigates the stolen data markets on Telegram, to unravel how they operate and propose measures to disrupt them.

Telegram as an online offender convergence setting

"The offender convergence setting is a stable and predictable source of co-offenders [… and] provides structure and continuity in the face of individual, group, or network instabilities" (Felson, 2003, p. 158). Such settings may refer to physical spaces where offenders meet to relax, exchange information and buy or sell stolen goods. Bars, parks, and safe houses are examples of offender convergence settings. For these settings to be suitable for offender convergence, they must remain undisturbed (Felson, 2003). Just like offenders may prefer certain settings over others for specific operations due to their configuration and available features, so do cyber offenders (Leukfeldt et al., 2017a; Moneva & Caneppele, 2020).

The rise in popularity of online forums and instant messaging applications has inspired offenders to also converge in online settings to form alliances, exchange electronic information, and trade different products and services such as account credentials (Soudijn & Zegers, 2012), information on allegedly fixed matches (Moneva & Caneppele, 2020) and malware (Leukfeldt & Holt, 2020; Leukfeldt et al., 2017a, 2017b, 2017c). Prior research has identified three main functions of online convergence settings: the market function, the social function, and the learning function (Leukfeldt et al., 2017a). The market function refers to the trade of illegal goods and data with products that vary per market type; the social function refers to the use of the setting as a platform to interact with potential or actual offenders; the learning function refers to the exchange of information and knowledge between individuals in the setting. Telegram channels are mainly used for the first function, serving as a marketplace for various types of data, while groups also provide the social and learning functions that allow users to interact with and learn from each other. Besides, the alleged protection of user anonymity, the ability of meeting places to host a large or even an unlimited number of users, and the versatility to exchange different types of files—among other features (Telegram, 2022b)—may make

Telegram an attractive setting for cyber offenders interested in trading stolen data. The trade can be carried out both on channels and in groups, although in different ways.

There are several differences between channels and groups. Both of them can be public and private. If a channel is public, anyone can subscribe to it; when a channel is private, a subscription is possible only if the administrator adds the user to the channel or if the user gets an invite link to join (Telegram, 2022b). On channels, the communication is usually unidirectional; this means that it is broadcasted by an administrator, who may act as the primary data provider. Users of such channels are called subscribers and they cannot see each other. While subscribers cannot send messages on channels, they are sometimes able to comment on the posts published by the administrators. But this is only possible if the administrators themselves enable this function. Enabling this commenting function creates a separate discussion group for each publication on the channel, in which the comments of subscribers are collected. After publishing a comment, the name of the subscriber automatically becomes visible to other subscribers who have also left a comment, which means that they sacrifice their anonymity to be heard. Telegram users can also create and administer groups, where communication is bidirectional. Some channel administrators may also create associated groups to facilitate interaction among users. When users join groups, they become members and are able to see the other group members without having to post a message. Telegram users can also start private bilateral conversations with other users through direct messages or secret chats. The difference is that messages sent in secret chats can be deleted for both ends of the communication—instantly or at the end of a countdown—, that they cannot be forwarded and that they are not stored in the cloud. This means that they can only be accessed locally from the sending or receiving device (Telegram, 2022b). Table 1 provides a classification of the Telegram meeting places.

Table 1 Characteristics of the Telegram meeting places

Characteristics	Meeting places			
	Channels	Groups	Direct messages	Secret chats
Access	Public or private	Public or private	Private	Private
Communication	Unidirectional	Bidirectional	Bidirectional	Bidirectional
Participants	Administrators and subscribers	Administrators and members	Any user	Any user
Storage	Local and cloud	Local and cloud	Local and cloud	Local

Crime scripts and situational crime prevention measures to tackle cybercrime

The Rational Choice Perspective regarding the study of criminal behavior assumes that offenders are rational beings who interpret information from the environment to decide whether or not they will engage in crime (Clarke, 2016; Clarke & Cornish, 1985). For each crime, rational offenders develop a specific decision-making process that can be fragmented into a series of decisions (Cornish & Clarke, 2003). To understand this sequence of decisions, researchers developed the concept of a 'crime script' (Cornish, 1994; Dehghanniri & Borrion, 2021): "a framework to provide an account of the choices and decisions made by offenders before, during, and after committing a specific type of crime" (Leclerc, 2016, p. 119). Beyond the crime-commission process, crime scripts also help to understand the environment where crime occurs since they present a detailed description of the operations within that environment (Cornish, 1994; Hutchings & Holt, 2017; Leclerc, 2016). Crime scripts also recognize the fact that crime may be a lengthy process—it may take days or weeks until offenders accomplish their goals (Cornish, 1994; Leclerc, 2016).

Users who join Telegram settings where stolen data is traded, must act deliberately. If—once inside the setting—users want to trade, either by offering data or bidding for it, they must make a series of decisions taking them from the moment of entry, to the moment of completion of the transaction, and a possible exit from the setting. Just as in a marketplace, buyers must decide which vendor to trust, what qualities they want in the product, and what price they are willing to accept (Dupont et al., 2017; Holt, 2013). This means that there is not just a single point in which a rational decision is made, but that it is a sequence of decision points that offers possibilities for potential interventions (Cornish, 1994; Leclerc, 2016; Wortley & Townsley, 2017). By identifying every step of the offender's decision-making process, opportunities to prevent or disrupt crime do significantly increase (Leclerc, 2016). Therefore, crime scripts would not only improve the understanding of this decision-making process, but also allow the analysis of its weaknesses to inform possible intervention strategies aimed at preventing offenders from accessing their targets or contacting each other (Felson, 2003).

Situational crime prevention (SCP) suggests that crime can be prevented by manipulating the environmental settings that impact the offender's decision to commit the crime (Clarke, 2016; Cornish & Clarke, 2003). To successfully prevent the crime from happening, interventions should aim at reducing criminal opportunities by creating the circumstances that make the offender's decision to commit the crime less appealing to them (Brewer et al., 2019; Chiu et al., 2011; Wortley & Townsley, 2017). By identifying the main decisions offenders make when committing crime, crime scripts "maximize the potential effectiveness of situational crime prevention" (Leclerc, 2016, p. 119). According to Clarke (1997), opportunity reducing techniques must be crime specific, involve the permanent manipulation of the environment, and make crime riskier, more complex, less rewarding or excusable (Chavez & Bichler, 2019; Clarke, 2016). This translates into five categories of SCP measures that are aimed at increasing the effort offenders have to make, increasing the risks they have to face, reducing the rewards they may gain, reducing any provocations they may encounter, and removing any excuses they may have for non-compliance with the norm—or any combination of the above (Cornish & Clarke, 2003). These measures are likely to make the trade of stolen data on Telegram more difficult.

The present study

Several studies have used crime scripts to understand cybercrime and suggest interventions based on SCP measures (Dehghanniri & Borrion, 2021). Objects of study include phishing (Leukfeldt, 2014; Loggen & Leukfeldt, 2022), carding (Soudijn & Zegers, 2012; van Hardeveld et al., 2017), money mules (Leukfeldt & Jansen, 2016), dark web firearm purchasing (Holt & Lee, 2022b), and stolen data markets (Hutchings & Holt, 2015). This study aims to disentangle the operations of Telegram meeting places that operate as stolen data marketplaces, to propose feasible SCP measures for law enforcement agencies and service providers. We therefore pose two research questions:

RQ$_1$: How do stolen data markets operate on Telegram?

RQ$_2$: What feasible situational crime prevention measures can be used to disrupt such markets?

Methods

To investigate stolen data markets on Telegram, we used an exploratory approach. In an initial phase of reconnaissance, we combined internet searches and covert non-participant observation to locate the first marketplace for stolen data. In a second phase of data collection, we used snowball sampling to identify additional stolen data markets and exported their contents from the Telegram application. In a third phase of analysis, we used content analysis and crime scripts to extract, process, and structure the textual information shared in the marketplaces.

Sampling

The first Telegram marketplace for stolen data was accidentally found while we were browsing through cybercrime forums on the dark web. We came across a thread where participants were discussing a data breach, and one of them shared a link to the Telegram channel of a ransomware group responsible for the breach. By following the link, we discovered that the Telegram channel was actually a marketplace for stolen data, where adverts were being displayed and free data samples were provided. Scrolling further through the channel, we observed that some publications were forwarded from other marketplaces and included data files as attachments. This suggested that there were other similar marketplaces, which inspired us to investigate them in more detail.

To minimize the risk of disrupting the data collection process and avoid being exposed to cyber offenders, we conducted covert non-participant observation and initiated a snowball sample procedure (Holt & Lampke, 2010; Hutchings & Holt, 2015; Melde & Weerman, 2020; Thomas et al., 2017). That is how we identified 30 meeting places. Of these 30 meeting places, 16 were active marketplaces that we selected for analysis. This resulted in a sample of seven public channels (PUC), four public groups (PUG), two private groups (PRG) and three backup public channels (BPUC) (see Table 2).

Since we do not know what the universe of stolen data marketplaces is, we cannot make strong statements about the representativeness of our sample. Based on our (ongoing) observations, these marketplaces could be considered small (up to 2000 subscribers) to medium (between 2000 and 5000 subscribers) in size. Note that these are rough estimates. Private groups and backup public channels tend to be smaller than public groups and channels due to their lower visibility and discoverability, and greater access restrictions.

Table 2 Overview of the selected Telegram meeting places

Telegram meeting places			
ID	Language	Type	Subscribers
PUC1.1	EN	Public channel	2709
PUG1.2		Public group	870
BPUC1.3		Backup public channel	230
PUC2.1	EN	Public channel	2188
PRG2.2		Private group	1056
BPUC2.3		Backup public channel	477
PUG3	EN	Public group	678
PUC4	EN	Public channel	1549
PUC5.1	RU	Public channel	3315
PUG5.2		Public group	1027
PUC6.1	EN	Public channel	4816
PRG6.2		Private group	516
PUC7	EN	Public channel	1113
PUC8.1	EN	Public channel	5113
PUG8.2		Public group	1614
BPUC8.3		Backup public channel	804

Ethical considerations

Prior to collecting data, we sought advice from the ethical committee of [anonymized for peer-review] regarding conducting research on stolen data: data obtained through "exploitation of the vulnerability in a computer system or an unauthorized leak by someone with access to the data" (Thomas et al., 2017, p. 1). To comply with the ethical committee's advice, our research does not disclose the names of the stolen data marketplaces or their members.

Data

We collected data from the Telegram application by exporting the textual content of the meeting places into HTML files. In total, we exported 10,348 messages. The main language used in the meeting places was English, except on one channel and in one public group where the language used was Russian. All messages in Russian were translated into English by the first author, who is fluent in Russian.

Content analysis

To systematically extract and analyze the text data collected, we conducted a content analysis in four steps. First, we carried out observations daily for three months to understand how the stolen data markets worked and how their users communicated (e.g., language, jargon used). We documented any relevant observations. Second, we randomly selected twenty days of activities for each marketplace and read all messages posted during that period of time. Next, we applied in vivo codes on those days, based on our previous observation of Telegram marketplaces and findings from previous studies on the online illicit markets (Demant et al., 2019; Holt & Smirnova, 2014; Hutchings & Holt, 2015; Leukfeldt et al., 2017b; Motoyama et al., 2011). Third, we compiled all the codes and arranged them following a hierarchical structure (see Appendix A) :

i. [Phase of the universal crime script]
    a. [Indicators]
        i. [In vivo codes]

Lastly, we applied the codes to all the text data from each marketplace to identify all the relevant information to build a crime script. For analysis, we used ATLAS.ti version 9.1.6—a qualitative data analysis software.

Crime script analysis

In the last phase of our analysis, we used crime scripts. Crime scripts are useful to analyze the underlying patterns and situational factors that influence criminal behavior, which can be used to propose situational crime prevention measures. Here we use crime scripts to analyze the information extracted from the Telegram meeting places and, in this way, reconstruct the sequential steps required to participate in the stolen data markets.

So far, only a few researchers have used crime scripts to analyze stolen data markets (Hutchings & Holt, 2015). This study applies the universal script as proposed by Cornish (1994), which was previously used to examine different illicit online markets, such as stolen data markets and firearm markets (Holt & Lee, 2022b; Hutchings & Holt, 2015). The universal script consists of nine stages (Cornish, 1994), which can be described as follows:

- Preparation: Planning the logistics of crime.
- Entry: Gaining access to the crime location.
- Pre-condition: Establishing the conditions for the crime.
- Instrumental pre-condition: Acquiring the tools, skills, or knowledge for the crime.
- Instrumental initialization: Finalizing preparations just before the crime.
- Instrumental actualization: Executing the crime.
- Doing: Committing the crime.
- Post-condition: Taking responsive action after the crime.
- Exit: Leaving the crime location. .

However, there are no specific guidelines on how crime scripts should be designed (Borrion, 2013) or what sources should be used to create them (Hutchings & Holt, 2015). We use a universal crime script with sub-sections inspired by Hutchings and Holt (2015).

Interviews with law enforcement

Between October and November of 2021, we held two online semi-structured interviews with the team leader and an operational specialist of the Cyber Offender Prevention Squad (COPS), Team High Tech Crime, of the Netherlands Police. We interviewed the two people with full knowledge of the capabilities of the unit and the cybercrime operations being carried out. Our conversations focused on the current and future operations carried out by the COPS and the feasibility of our own suggestions.

Results: A crime script of stolen data trade in Telegram

Figure 1 shows an overview of the crime script for trading stolen data in Telegram from the perspective of both vendors and customers. When referring to a specific meeting place, we cite its ID. We elaborate on each stage below.

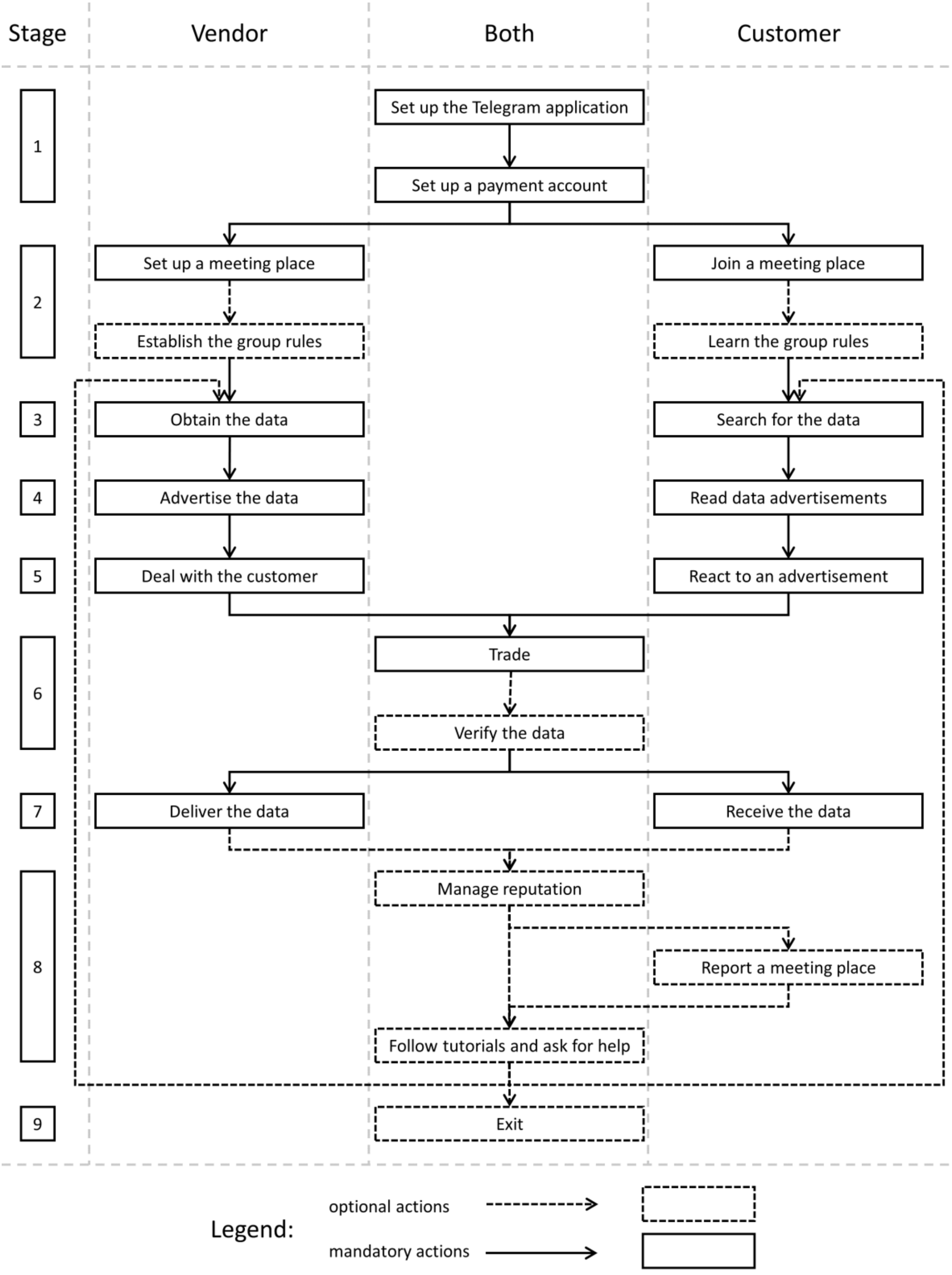

Fig. 1 Crime script of stolen data trade in Telegram. Stages: (1) preparation, (2) entry, (3) pre-condition, (4) instrumental pre-condition, (5) instrumental initiation, (6) instrumental actualization, (7) doing, (8) post-condition, (9) exit.

Preparation

Setting up the Telegram application

To join a Telegram meeting place, users need to download and install the Telegram application on a suitable internet-connected device such as computer, tablet, or phone. To install the application, users must provide a valid mobile phone number. After the application is installed, users need to create a profile by introducing a name, a profile picture, and—optionally—a nickname. Such information can be real or fictitious. Upon completing their profile, users receive a message at the phone number they provided to verify it. Then the Telegram application is ready for use.

Setting up a payment account

To make a purchase from data vendors on Telegram, ‘customer’ users need to have or set up an account in an online payment system that allows them to pay with cryptocurrencies such as Bitcoin (BTC), Litecoin (LTC), and Ethereum (ETH). Two of the Telegram channels advertised the ‘blockchain.com' and 'ethereum.org' platforms as the platforms preferred by vendors and customers (PUC5.1; PUC8.1).

Entry

Setting up or joining a meeting place

Users can use the built-in search function in Telegram to search for and join any of the public meeting places. Many meeting places in which stolen data are traded have the keywords ‘data’ or ‘leak’ in their names, making them easy to find. It is also not mandatory to join public meeting places to view their contents. The number of views a post has is usually higher than the number of subscribers or members in the meeting place. This means that some users do not join them, but only observe or *lurk*. As opposed to subscribers, lurkers do not receive notifications when new ads or data dumps are released. However, not subscribing or joining the meeting place does not prevent users from downloading the files leaked there.

Establishing or learning the group rules

Some of the groups have rules that participants must follow. In most of them, administrators indicate what is forbidden (PUG5.2), while in others they specify what is expected from users (PUG8.2). Forbidden behavior includes offending other participants of the group, spamming the chat, publishing violent or pornographic content, and falsely accusing participants of being scammers or *rippers*.

Discussions about the presence of rippers among vendors were common in the meeting places. In one of them, from time of time, the administrator published a list of rippers titled “Scam Alert” (PUG8.2). Such list was updated whenever a customer could prove that a vendor was in fact a ripper by sending a direct message to the administrator with a screenshot as proof. Vendors could be labelled as rippers if, for example, they attempted to sell data that could be found for free elsewhere (e.g., on the Dark Web), the data they traded did not correspond to what was promised, or they did not send any data after receiving payment. Customers could also be accused of ripping if they resold products under different names in other groups. A user accused the administrator of a private group (PRG2.2) in another private group (PRG6.2) of not sending the data after the user had paid for it. This means that some users are active in several meeting places at the same time. Administrators accused of ripping see their reputation damaged and often lose customers as a result. For this reason, some meeting places emphasize the importance of using escrows when trading (PUC1.1; PUG3; PUC4; PUG8.2). Escrows are trusted third parties that are assigned by administrators and to whom customers send the payment until the data is verified (Mirea et al., 2019).

Some groups have additional rules about trading. For example, in one of the public groups (PUG3), the administrator had monopolized the sale of data and did not allow others to advertise data or forward links and files from other meeting places. In other groups, users had to get permission from the administrator to offer data or services (PUG1.2; PRG6.2), or they were required to use a payment bot or an escrow (Telegram, 2022a). A payment bot is a small application that runs from within Telegram allowing admins to accept the payment. One of the groups even used bots to remind new members of the rules. Not following the rules could result in users being banned from groups.

Pre-condition: obtaining or searching for the data

While there are several possible sources of stolen data (e.g., phishing, insider incidents), a large portion of the data traded on Telegram appears to originate from data breaches. We found supporting evidence in several meeting places, such as: "I have Nitro 2020 breached data" (PUG1.2), "106 million traveler's Thailand database for sale" (PUC4), or "Santander Bank Database for Sale! It's just 250 $" (PUC6.1). On one of the channels, the administrator stated that all data being sold was obtained by "his group of hackers" (PUC4). On another channel, the administrator was reselling data released on a dark web forum (PUC7). The nickname of the individual who initially sold the data on the relevant forum was also referenced in the Telegram announcement. It is likely that the administrator purchased this data to profit from reselling it to the many users of the channel. In several groups (PRG2.2; PUG3; PUG8.2), users often tried to sell data that—according to other users—was available for free elsewhere. Often, vendors who attempted to sell publicly available data were called rippers and risked being expelled from the group as a result of that.

Instrumental pre-condition: advertising the data or reading a data advertisement

If users have data to sell, they tend to advertise it first. Ads differ depending on the chat. On one of the channels, the administrator published the following ad to promote the data: "3 million Lines USA Gold Database. Good for shopping, gaming and crypto. Full private. Checked with Priv8 and MYRZ Antipublic. Data is clear of duplicates and garbage. Price per part: 100K = $30, all parts = $550" (PUC1.1). An hour after posting the ad, the administrator announced that the data had been sold. On another channel, the administrator advertised particularly attractive data to certain customers under the label "critical data time". The ad stated that the data contained "client cases, passports, driving licenses, addresses, bank statements, and other documents" (PUC4). The asking price for the data was $1000. Ten minutes after posting the ad, the administrator stated that the data had been sold.

Three channels offered subscription services to access unique and recent data. (PUC1.1; PUC2.1; PUC8.1). An administrator advertised a subscription to a cloud for $75 per month (PUC8.1). According to the ad, this subscription would provide users with access to unique data of the best quality that would be regularly updated. In addition, users would receive unlimited online support and would have access to a variety of tools. Other subscriptions were for specific time periods, such as one week for $35, one month for $70, three months for $165, and a lifetime for $500 (PUC1.1). Linked to the main channel in which the ads were posted, the admin set up an additional channel containing screenshots of conversations with customers, proving that the vendor was not a *ripper* and that customers were happy with the service (PUC1.1). During holidays, vendors also offered discounts to customers (e.g., 20% Christmas discount).

To attract more customers, administrators regularly dump data that can be downloaded by any user for free. In some of the meeting places (PUC1.1; PUG3; PUC5.1; PUC6.1), administrators often provided free data samples, such as login credentials for Netflix or VPN accounts, proxy servers, and all sorts of documents such as driving licenses, social security numbers, proofs of address, and ID pictures of the holders. Most of the time, administrators published several samples, such as passport scans with ID pictures, to demonstrate the reliability of the contents of some data. Some users commented positively on using these data for their own purposes: "I managed to set up a bank account with the sample pictures, thank you" or "thank you, it worked perfectly for me" (PUG5.2).

Data were in fact shared regularly on all the channels observed. Together with the free data samples, vendors often advertised additional data for sale, emphasizing that the quality of the paid data was much better than that of free samples, and that there was a lot of money to be made from them. An administrator posted the following message on his channel:

> *"Of course we know that the best things always cost money, therefore we provide you with an option to purchase the best data. This data is extracted from the databases of various sites. As you know, if you try data on something several times, it will lose its quality. So the best things are always the most hidden things. This we call a 'Private Data' that you can buy from us. We upload a lot of data every day, but it may lose its quality because another + 2000 are viewing it. Therefore, contact me DM for the best things and I will give you the data you want"* (PUC8.1).

Another administrator posted the following intriguing message: "In the next 3-5 hours, I will release a huge amount of free data for specific countries. This data is completely private! Stay with me" (PUC4). Often, customers also posted announcements expressing their interest in data related to a particular country or company. Should any vendor have such data, they could contact the customer to discuss the terms of the exchange. In one of the groups, presumably on behalf of a company, a user posted an ad for specific data.

> *"We are a data company with extensive OSINT experience. We are looking for specific data and are ready to pay a lot for it. We are interested in medical data, health alignment data, insurance data, debt settlement/personal loan for the past 6 – 8 months, consumer marketing and social media data. We are not interested in anything whose main purpose is to break into the websites/wallets or steal identities. Reach out to us with what you have"* (PUG5.2).

This suggests that companies might also be interested in purchasing stolen data through Telegram.

Instrumental initiation: dealing with the customer or reacting to an ad

Customers interested in data advertised may contact the seller through a direct message. In these messages, customers can specify the data they want or simply forward the ad of interest to the vendor. There are two ways to send a direct message: using the 'secret chat' option, in which contents expire and are deleted after a certain time, or sending a regular direct message. Both options establish a private communication channel between vendor and customer.

Instrumental actualization

Trading

On two channels, the administrators created separate channels with screenshots of their trades (PUC1.1; PUC8.1). The screenshots show that after responding to an ad, vendors respond by listing different payment methods. Payment methods included cryptocurrencies such as BTC, ETH, and LTC. After a customer has selected a payment method, they have to pay and attach a screenshot confirming the transaction. The vendor then sends a message to the customer indicating the time at which they can expect the data. In some cases, the data was sent immediately; in other cases it took a few hours. In one case we observed the customer making an installment payment of 2/3 upfront and 1/3 upon receipt of the data.

Verifying the data

Before being traded, the data often needs to be verified and scanned for malware. To do this, some administrators make use of bots in their groups. These bots are small applications that automatically react to specific inputs and can be manually triggered with specific commands. One of the most frequently used bots was 'Dr. Web', which scans files for malware. But users can also develop their own bots. Such customized bots are usually named "guarantee bots" or "payment bots", and their name is sometimes preceded by the name of the meeting place. While some meeting places use bots for data verification, others use escrows to protect vendors and customers.

One of the administrators of a private group advised users to "[…] be careful before the trade. Check the blocklist first and then use escrow when you make a trade" (PRG6.2). Upon data verification, the escrow sends the money to the vendor. In two groups (PRG2.2; PUG5.2), users were advised to use an online escrow service and not trust third-parties, because apparently some vendors use a second account or a friend's account as escrow. One user wrote: "Which escrow... They bring a friend as an escrow and disappear after receiving the payment" (PRG2.2).

While some Telegram groups require data to be verified before trading, not all of them have such requirements. Meeting places in which these requirements are not imposed often feature discussions in which customers claim that one or another vendor is a ripper.

Doing: delivering or receiving the data

After purchasing the data, customers receive the corresponding files through a direct message. Telegram allows transferring files of up to 2 GB (Telegram, 2022b). If the data file is larger than that, it is sent as a compressed file. On one of the channels (PUC8.1), the vendor would provide customers with access to a cloud from which the file could be downloaded. On another channel (PUC4), the administrator stated that upon purchasing the data, customers would receive a link to the platforms "Mega" or "Anonfiles" together with a decryption key to download and read the data.

Post-condition

Managing reputation

Reputation management was also an essential aspect of maintaining trust in these markets. Typically, it was the vendors who had to defend themselves against accusations of being rippers, when customers claimed not to have received the purchased data. Often, when such accusations were made, other users and administrators would ask customers to provide evidence of the 'rip-off'. If customers could not provide evidence, they risked being banned from the group for making false accusations.

Reporting a meeting place

Users were able to report meeting places to Telegram by clicking on the 'Report' button in their description. There are a number of reasons why a user would report a meeting place: for being spammed, identifying fake accounts, and for receiving messages about, among other things, violence, child abuse or pornography. When multiple users report a meeting place, Telegram flags it with the 'scam' tag next to its name and changes its description to the following: "Warning: Many users reported this account as a scam or a fake account. Please be careful, especially if it asks you for money" (PUC4). The administrator of a flagged meeting place responded by creating a backup channel and posting a number of screenshots of successfully concluded trade deals.

Following tutorials and asking for help

In some of the meeting places, users often get the advice from administrators or other users to install additional software or to use specific tools, even in the form of tutorials, to get the most benefit from the stolen data traded. For example, on one of the channels (PUC5.1) the administrator provided instructions on how to install a tool that would allow users to send spam through WhatsApp, SMS, and email. Other tutorials addressed topics such as "finding IP addresses through Telegram" (PUC2.1), and "how to create a phishing page on Facebook, Instagram and PayPal" (PUC5.1). The most practical tutorials were provided for free, while others could only be accessed for an additional cost, varying between $50 and $150 (PUC2.1; PRG2.2). Most of the tutorials provided such detailed instructions that even users with minimal computer skills would be able to follow them.

On another channel (PUC8.1), the administrator posted an ad for the subscribers to learn how to breach PayPal accounts for an additional cost. This announcement included some screenshots with messages from former users sharing their positive reviews of the course.

On another channel, the administrator mentioned that any file distributed through the channel should only be opened in a virtual machine, or else users would risk infecting their operating systems with a virus. Additional advice throughout different channels include: "Using a different number from the regular to set up the Telegram account, using fake credentials to register a new SIM card, and using a VM [virtual machine] and virtual private network (VPN) services" (PUC1.1). In one of the private groups (PRG2.2), a user shared some advice regarding physical security that involved using a separate VLAN and non-shared Wi-Fi. Another user from the same group mentioned the use of a self-made router. There were also recommendations about tools that would allow to forever delete all the files from a computer (PUC5.1), programs to encrypt files (PUC5.1), and tools to change a MAC address weekly (PUG2.1). Besides trading and leaking stolen data, some channels and groups also shared login credentials for VPN services, hosting services, sock proxies, and passport and ID card scans.

Users ask for help frequently in groups too. Their questions may be about programming or related to the use of a specific tool. And usually the rest of the users do answer the questions. Sometimes responses given were very detailed, even specifying the code that users had to enter into the terminal or describing the sequence of steps needed to run the tool.

Exit

The data we collected does not show whether users prefer to stay or leave the meeting places—or Telegram altogether—after a successful purchase. There may be external factors that influence this decision, such as the withdrawal of the administrator, the inactivity of the channel, or its take down by law enforcement.

Discussion

The crime script revealed that running a stolen data market on Telegram is a process that involves a significant amount of time and effort from the administrator's side. It has been described as "tedious supportive and maintenance work" (Collier et al., 2021, p. 1414).

This work requires the daily execution of various tasks, such as obtaining the data to trade, creating ads, replying to messages, sending data, managing reputation, screening the channel, and sometimes managing the discussion group on the side. For a channel to stay attractive to participants and to draw new subscribers, administrators must regularly post new content and provide data that is unique compared to the competition, while they do all the administrative work involved in running these channels at the same time (Collier et al., 2021).

The crime script shows that Telegram's stolen data markets adequately fulfill the functions of an online convergence setting (Leukfeldt et al., 2017a). The platform satisfies the market function by enabling appropriate functionalities for marketing products, such as the virtually unlimited capacity of meeting places, and enabling the secure exchange of services, such as private channels. The social function is satisfied by enabling different forms of communication between users—public or private, unilateral or bilateral—which allows users, for example, to initiate and terminate relationships, close deals, and establish trust systems. The educational function is also fulfilled by allowing new users to join public meeting places, where they can learn from more experienced users how the market works. They can either remain lurkers or advance their criminal careers by becoming customers or vendors. Eventually, they may be invited to join private channels where the content is more exclusive and explicit. They may even end up administering their own channel.

Similarities and differences with other online illicit marketplaces

If we compare Telegram's online convergence meeting settings to other types of online criminal marketplaces, we notice several similarities and differences. Similarities include the preferred use of cryptocurrencies as the payment method (Holt, 2013; Holt & Lampke, 2010; Hutchings & Holt, 2015), the clarification of what is allowed and forbidden in the marketplace (Holt, 2013, p. 20; Holt & Smirnova, 2014; Morselli et al., 2017), the availability of learning tutorials (Dupont et al., 2017; Holt & Smirnova, 2014), conditions under which a vendor could be called 'ripper' (Dupont et al., 2017; Holt et al., 2015; Holt & Smirnova, 2014; Hutchings & Holt, 2015) and the preference to utilize escrows in transactions (Aldridge & Décary-Hétu, 2014; Décary-Hétu & Dupont, 2013; Holt & Lampke, 2010). When advertising data, vendors on Telegram and dark web marketplaces also provide a detailed description of their product, including pricing information, preferred payment method and contact information, and they try to emphasize the uniqueness of the data or the availability of the discounts (Aldridge & Décary-Hétu, 2014; Holt & Lampke, 2010). If customers are interested, they must contact vendors by sending a direct message or via secret chat (Décary-Hétu & Dupont, 2013; Holt, 2013). Another similarity is the importance of reputation management. Independently of the platform, vendors must ensure that they are not falsely accused of being rippers (Décary-Hétu & Dupont, 2013; Motoyama et al., 2011). Similarly, vendors sometimes referenced one another on their channels, but there was no evidence of them working together (Décary-Hétu & Dupont, 2013). The availability of private groups, channels or clubs on Telegram and dark web markets has also been observed (Holt, 2013).

Two differences between Telegram and other online marketplaces are their accessibility and organizational structure. Telegram is an application that can be accessed via application or web on the clear net, while for access to marketplaces on the dark web the use of the TOR browser is often required. When registering on a dark web forum, users are required to provide personal information to create an account, such as their email account (Jardine, 2021). Next, Telegram's organizational structure varies from those of other marketplaces. On dark web forums, roles are usually divided into customers, vendors, administrators, and moderators, performing each a different function (Holt et al., 2015; Holt & Lampke, 2010). On Telegram, administrators are often both vendors and channel moderators, which gives them an even more prominent role. Additionally, on Telegram, we observed only two channels that included information about the feedback from the users purchasing the data (PUC1.1; PUC8.1). These channels had more subscribers compared to the other channels and groups on Telegram (see Table 2). Future research could examine which factors are associated to meeting place popularity. In contrast to Telegram, customers on the dark web often provide feedback on the performance of vendors by either leaving feedback or by rating them (Décary-Hétu & Dupont, 2013; Holt, 2013; Morselli et al., 2017). Vendors with better reputations are deemed more trustworthy and therefore have a higher chance of being contacted by potential customers (Dupont et al., 2017; Holt, 2013; Holt et al., 2015; Holt & Lampke, 2010; Jardine, 2021). Considering the organizational structure of the Telegram marketplace and the absence of a rating system, we can assume that it is more difficult for users to determine which channel or group they can trust and which not.

Feasible situational crime prevention measures

Based on the crime script, and after discussions with law enforcement officers dedicated to implementing cybercrime prevention operations, below we suggest four interventions inspired by situational crime prevention measures to disrupt stolen data markets on Telegram (Cornish & Clarke, 2003; Hutchings & Holt, 2015).

Taking down the meeting place

The first intervention that might significantly impact the administrators is the takedown of the channel. If channels are taken down, administrators might realize that the benefits do not outweigh the effort required to run the meeting places (e.g. time, risk), especially when they can be taken down again at any time (Collier et al., 2019). According to official information, Telegram can process legitimate requests to take down meeting places that offer illegal content (Telegram, 2022b). Law enforcement agencies could therefore pull this lever to take down stolen data (and other illicit) markets. The simultaneous takedown of several meeting places is likely to be more effective in disrupting illicit markets than the takedown of a single marketplace (Collier et al., 2019). Taking down meeting places would not only help disrupt the business but also undermine the sense of impunity administrators may have (Collier et al., 2022).

Because some administrators know that there is a risk for meeting places to be taken down, they set up backup channels and ask subscribers to join them—thus enabling a form of spatial displacement (Barr & Pease, 1990). However, the number of subscribers to those channels was between 4 and 12 times smaller than to the original channel in our sample (see Table 2). This means that it can take a long time for administrators to get back to the same number of subscribers. Note that take downs can also give a false sense of security to law enforcement which could simply be due to a temporary absence of activity while the administrators set up a new meeting place.

Reporting spam and scam

A crowdsourced alternative to disrupt stolen data markets would be through the report function. When users click on 'Report spam', they forward the selected message(s) to a team of Telegram moderators for review (Telegram, 2022b). If moderators decide that the message(s) do(es) indeed constitute spam, they will block the spammer and attach the 'scam' logo next to their username (Ricle, 2019). If it was the administrator who was reported, the logo is attached to the name of the meeting place. This will likely generate distrust among potential customers—some of which may unsubscribe—and will prevent others from subscribing. The only solution for the reported administrator to get rid of the scam tag would be to build a new meeting place from scratch, which requires considerable effort. Eventually, administrators may lose motivation and run out of business.

However, this measure can also be abused to falsely report competitors or other users with whom scammers have conflicts. Overreporting can cause a delay in the review process that affects legitimate users of the platform. In addition, any delay in identifying and blocking scammers may prolong their activity on the platform. Furthermore, if the scam logo is over-reported and becomes ubiquitous, users may question the credibility of the tagging system, which could lead to a decrease in legitimate reports over time.

Flooding meeting places with forbidden terms

Telegram can automatically block meeting places through their abuse detection system, which is currently being used to detect messages related to terrorism and extremism. Therefore, if users post words linked to terrorism and extremism in the chat, there is a chance the meeting place gets blocked (Collier et al., 2022; Europol, 2019). This is why many administrators incorporate explicit rules related to certain prohibited behaviors that violate Telegram's policies (Europol, 2019). This leads to another intervention strategy: the use of bots programmed to flood meeting places with contents that will trigger Telegram's abuse detection system.

A potential negative outcome of this measure are false positives. Even if the abuse system is effective, a broad implementation could lead to blocking meeting places that do not actually engage in illegal activities, but merely discuss how to avoid them. This could cause disruption of legitimate activities and reputational damage to well-intentioned administrators.

Using discouraging banners

Another option to disrupt the trade is to target stolen data vendors with discouraging banners. Instead of threatening sellers with punishment as is customary with warning banners, discouraging banners would emphasize that the job is indeed tedious, low-skilled, low-paid and low-status (Collier et al., 2021). Discouraging banners might change the minds of those who aspire to become cybercriminals, who believe in the alleged excitement, glamour and prestige this job brings (Collier et al., 2021). Law enforcement agencies could also use discouraging banners to highlight how exciting the job of a pentester or ethical hacker can be, and also mention that there is a shortage of cybersecurity professionals which offers a great opportunity for talented users to get a well-paying legal job (Collier et al., 2021; Legg, 2021; Moneva et al., 2022). These banners would remind cybercriminals that the benefits of managing Telegram channels are not really that great compared to the high costs and effort required. Another advantage of the placement of these banners is that they create the feeling of being watched and increase the perceived likelihood of being detected. This could therefore deter participants, especially potential young offenders, from starting or continuing to offend (Collier et al., 2022; Maimon et al., 2014; Moneva et al., 2022). It might also help to stress out that novice offenders may not be as anonymous online as they might think (Brewer et al., 2019).

The use of such banners can also have unintended consequences. Criminals may respond to the banners in a defiant manner, viewing them as a challenge rather than a deterrent, which could intensify or escalate activities. Moreover, criminals may respond to banners with mockery, which could make the banners a source of amusement within stolen data communities, potentially diminishing their impact and fostering a counter-narrative that portrays law enforcement as ineffective.

Conclusion

This study offers one of the first insights into how Telegram data markets operate. Using a universal crime script, we have analyzed the operations involved in each of the nine stages of the trade of stolen data and we have suggested four feasible situational crime prevention measures to disrupt them. Overall, the process of running a Telegram meeting place could be compared to owning an e-commerce store that involves many administrative, monotonous tasks that take considerable time and effort. Most maintenance work includes marketing to keep customers engaged, ensuring safe trading in order to maintain the cash flow, and vendor reputation management to improve market reliability.

Law enforcement could take advantage of this situation by informing administrators, vendors and customers of the effort it takes to maintain a stolen data marketplace, emphasizing how tedious it is, and the perceived risk of being arrested. In addition, they could adopt more proactive strategies that leverage Telegram's infrastructure to collaboratively disrupt markets. Future research should focus on implementing and evaluating the suggested interventions and examining the functioning of other illicit marketplaces on Telegram and other online platforms to assess the generalizability of the results reported here.

Acknowledgements

We thank Floor Jansen and Wouter Klijnsoon, Cyber Offender Prevention Squad (COPS), Team High Tech Crime (THTC), Netherlands Police, for finding time to discuss the potential interventions with us.

References

Ablon, L., Libicki, M., & Abler, A. (2014). *Markets for Cybercrime Tools and Stolen Data: Hackers’ Bazaar*. RAND Corporation. https://doi.org/10.7249/RR610

Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy*, *41*, 101–109. https://doi.org/10.1016/j.drugpo.2016.10.010

Aldridge, J., & Décary-Hétu, D. (2014). Not an “Ebay for Drugs”: The Cryptomarket “Silk Road” as a Paradigm Shifting Criminal Innovation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2436643

Barr, R., & Pease, K. (1990). Crime placement, displacement, and deflection. *Crime and Justice*, *12*, 277-318.

Borrion, H. (2013). Quality assurance in crime scripting. *Crime Science*, *2*(1), 6. https://doi.org/10.1186/2193-7680-2-6

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime Prevention: Theory and Applications*. Springer International Publishing. https://doi.org/10.1007/978-3-030-31069-1

Broadhurst, R., Foye, J., Jiang, C., & Ball, M. (2021). Illicit firearms and other weapons on darknet markets. *Trends and Issues in Crime and Criminal Justice*, *662*, 1–20. https://doi.org/10.3316/agispt.20210504046046

Chavez, N., & Bichler, G. (2019). *Guarding against Cyber-Trespass and Theft: Routine Precautions from the Hacking Community*. https://doi.org/10.5281/ZENODO.3551489

Chiu, Y.-N., Leclerc, B., & Townsley, M. (2011). Crime Script Analysis of Drug Manufacturing In Clandestine Laboratories: Implications for Prevention. *British Journal of Criminology*, *51*(2), 355–374. https://doi.org/10.1093/bjc/azr005

Clarke, R. V. (Ed.). (1997). *Situational crime prevention: Successful case studies* (2. ed). Criminal Justice Press.

Clarke, R. V. (2016). Situational crime prevention. In R. K. Wortley & M. Townsley (Eds.), *Environmental Criminology and Crime Analysis*. Routledge.

Clarke, R. V., & Cornish, D. B. (1985). Modeling Offenders' Decisions: A Framework for Research and Policy. *Crime and Justice*, *6*, 147–185. https://doi.org/10.1086/449106

Collier, B., Clayton, R., Hutchings, A., & Thomas, D. (2021). Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture. *The British Journal of Criminology*, *61*(5), 1407–1423. https://doi.org/10.1093/bjc/azab026

Collier, B., Thomas, D. R., Clayton, R., & Hutchings, A. (2019). Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks. *Proceedings of the Internet Measurement Conference*, 50–64. https://doi.org/10.1145/3355369.3355592

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2022). Influence, infrastructure, and recentering cybercrime policing: Evaluating emerging approaches to online law enforcement through a market for cybercrime services. *Policing and Society*, *32*(1), 103–124. https://doi.org/10.1080/10439463.2021.1883608

Copeland, C., Wallin, M., & Holt, T. J. (2020). Assessing the Practices and Products of Darkweb Firearm Vendors. *Deviant Behavior*, *41*(8), 949–968. https://doi.org/10.1080/01639625.2019.1596465

Cornish, D. B. (1994). Crimes as scripts. In D. Zahm & P. Cromwell (Eds.), *Proceedings of the International Seminar on Environmental Criminology and Crime Analysis, University of Miami, Coral Gables, Florida, 1993*.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies*, *16*, 41–96.

Cunliffe, J., Martin, J., Décary-Hétu, D., & Aldridge, J. (2017). An island apart? Risks and prices in the Australian cryptomarket drug trade. *International Journal of Drug Policy, 50*, 64–73. https://doi.org/10.1016/j.drugpo.2017.09.005

Décary-Hétu, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. *Global Crime*, *14*(2–3), 175–196. https://doi.org/10.1080/17440572.2013.801015

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change, 67*(1), 55–75. https://doi.org/10.1007/s10611-016-9644-4

Dehghanniri, H., & Borrion, H. (2021). Crime scripting: A systematic review. *European Journal of Criminology, 18*(4), 504–525. https://doi.org/10.1177/1477370819850943

Demant, J., Bakken, S. A., Oksanen, A., & Gunnlaugsson, H. (2019). Drug dealing on Facebook, Snapchat and Instagram: A qualitative analysis of novel drug markets in the Nordic countries. *Drug and Alcohol Review, 38*(4), 377–385. https://doi.org/10.1111/dar.12932

Dupont, B., Côté, A.-M., Boutin, J.-I., & Fernandez, J. (2017). Darkode: Recruitment Patterns and Transactional Features of "the Most Dangerous Cybercrime Forum in the World." *American Behavioral Scientist, 61*(11), 1219–1243. https://doi.org/10.1177/0002764217734263

Europol. (2019, November 25). *Europol and Telegram take on terrorist propaganda online*. Europol. https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online

Felson, M. (2003). The Process of Co-offending. In M. J. Smith & D. B. Cornish, *Theory for Practice in Situational Crime Prevention. Crime Prevention Studies, 16,* 149–167. Criminal Justice Press.

Holt, T. J. (2013). Exploring the social organisation and structure of stolen data markets. *Global Crime, 14*(2–3), 155–174. https://doi.org/10.1080/17440572.2013.787925

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies, 23*(1), 33–50. https://doi.org/10.1080/14786011003634415

Holt, T. J., & Lee, J. R. (2022a). A Crime Script Analysis of Counterfeit Identity Document Procurement Online. *Deviant Behavior, 43*(3), 285–302. https://doi.org/10.1080/01639625.2020.1825915

Holt, T. J., & Lee, J. R. (2022b). A crime script model of Dark web Firearms Purchasing. *American Journal of Criminal Justice, 48*(2), 509-529. https://doi.org/10.1007/s12103-022-09675-8

Holt, T. J., & Smirnova, O. (2014). *Examining the Structure, Organization, and Processes of the International Market for Stolen Data.* [Data set]. ICPSR - Interuniversity Consortium for Political and Social Research. https://doi.org/10.3886/ICPSR35002.V1

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and Estimating the Revenues and Profits of Participants in Stolen Data Markets. *Deviant Behavior*, *37*(4), 353-367. https://doi.org/10.1080/01639625.2015.1026766

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81–103. https://doi.org/10.1080/17440572.2015.1013211

Holt, T.J., T. J., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies*, *23*(1), 33-50. https://doi.org/10.1080/14786011003634415

Hutchings, A. (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, *62*(1), 1-20. https://doi.org/10.1007/s10611-014-9520-z

Hutchings, A., & Holt, T. J. (2015). A Crime Script Analysis of the Online Stolen Data Market. *British Journal of Criminology, 55*(3), 596-614. https://doi.org/10.1093/bjc/azu106

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime*, *18*(1), 11-30. https://doi.org/10.1080/17440572.2016.1197123

Jardine, E. (2021). Policing the Cybercrime Script of Darknet Drug Markets: Methods of Effective Law Enforcement Intervention. *American Journal of Criminal Justice*, *46*(6), 980–1005. https://doi.org/10.1007/s12103-021-09656-3

Kamps, J., & Kleinberg, B. (2018). To the moon: Defining and detecting cryptocurrency pump-and-dumps. *Crime Science*, *7*(1), 1-18. https://doi.org/10.1186/s40163-018-0093-5

Ladegaard, I. (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy*, *63,* 113–121. https://doi.org/10.1016/j.drugpo.2018.09.013

Leclerc, B. (2016). Crime scripts. In R. K. Wortley & M. Townsley (Eds.), *Environmental Criminology and Crime Analysis*. Routledge.

Lee, J. R., Holt, T. J., & Smirnova, O. (2022). An assessment of the state of firearm sales on the Dark Web. *Journal of Crime and Justice*, 1–15. https://doi.org/10.1080/0735648X.2022.2058062

Legg, J. (2021, October 21). *Confronting The Shortage Of Cybersecurity Professionals*. Forbes. https://www.forbes.com/sites/forbesbusinesscouncil/2021/10/21/confronting-the-shortage-of-cybersecurity-professionals/

Leukfeldt, E. R., & Holt, T. J. (2020). Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline. *International Journal of Offender Therapy and Comparative Criminology*, *64*(5), 522–538. https://doi.org/10.1177/0306624X19895886

Leukfeldt, R. (2014). Cybercrime and social ties: Phishing in Amsterdam. *Trends in Organized Crime,17(*4*), 231-249*. https://doi.org/10.1007/s12117-014-9229-5

Leukfeldt, R., & Jansen, J. (2015). Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands. *International Journal of Cyber Criminology*, *9*(2), 173. https://doi.org/10.5281/zenodo.56210

Leukfeldt, R., Kleemans, E. R., & Stol, W. P. (2017a). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change*, *67*(1), 21–37. https://doi.org/10.1007/s10611-016-9662-2

Leukfeldt, R., Kleemans, E., & Stol, W. (2017b). The Use of Online Crime Markets by Cybercriminal Networks: A View From Within. *American Behavioral Scientist*, *61*(11), 1387–1402. https://doi.org/10.1177/0002764217734267

Leukfeldt, R., Kleemans, E. R., & Stol, W. P. (2017c). Cybercriminal Networks, Social Ties and Online Forums. *British Journal of Criminology*, *57*(3), 704-722. https://doi.org/10.1093/bjc/azw009

Loggen, J., & Leukfeldt, R. (2022). Unraveling the crime scripts of phishing networks: An analysis of 45 court cases in the Netherlands. *Trends in Organized Crime, 25*(2), 205-225. https://doi.org/10.1007/s12117-022-09448-z

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive Deterrent Effects of a Warning Banner in an Attacked Computer System: Restrictive Deterrent Effects of a Warning. *Criminology*, *52*(1), 33–59. https://doi.org/10.1111/1745-9125.12028

Melde, C., & Weerman, F. (Eds.). (2020). *Gangs in the Era of Internet and Social Media*. Springer International Publishing. https://doi.org/10.1007/978-3-030-47214-6

Mirea, M., Wang, V., & Jung, J. (2019). The not so dark side of the darknet: A qualitative study. *Security Journal*, *32*(2), 102–118. https://doi.org/10.1057/s41284-018-0150-5

Miró Llinares, F., & Johnson, S. D. (2018). *Cybercrime and Place* (G. J. N. Bruinsma & S. D. Johnson, Eds.; Vol. 1). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190279707.013.39

Moneva, A. (2020). *Cyber Places, Crime Patterns, and Cybercrime Prevention: An Environmental Criminology and Crime Analysis approach through Data Science* [Doctoral dissertation]. https://core.ac.uk/download/pdf/392256988.pdf

Moneva, A., & Caneppele, S. (2020). 100% sure bets? Exploring the precipitation-control strategies of fixed-match informing websites and the environmental features of their networks. *Crime, Law and Social Change*, *74*(1), 115–133. https://doi.org/10.1007/s10611-019-09871-4

Moneva, A., Leukfeldt, R., & Klijnsoon, W. (2022). Alerting consciences to reduce cybercrime: A quasi-experimental design using warning banners. *Journal of Experimental Criminology*, 1-28. https://doi.org/10.1007/s11292-022-09504-2

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2017). Conflict Management in Illicit Drug Cryptomarkets. *International Criminal Justice Review*, *27*(4), 237–254. https://doi.org/10.1177/1057567717709498

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. *Proceedings of the 2011 ACM SIGCOMM*

Conference on Internet Measurement Conference - IMC ’11, 71. https://doi.org/10.1145/2068816.2068824

Ouellet, M., Maimon, D., Howell, J. C., & Wu, Y. (2022). The Network of Online Stolen Data Markets: How Vendor Flows Connect Digital Marketplaces. *The British Journal of Criminology*, *62*(6), 1518–1536. https://doi.org/10.1093/bjc/azab116

Ricle, J. (2019, October 2). *What Is “Scam” Label Next To Telegram Username? How To Report Telegram Scammers?* Telegram Adviser. https://www.telegramadviser.com/scammers-in-telegram-and-how-to-report

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, *15*(2–3), 111–129. https://doi.org/10.1007/s12117-012-9159-z

Telegram. (2022a). *Bot Payments API*. Telegram. https://core.telegram.org/bots/payments

Telegram. (2022b). *Telegram FAQ*. Telegram. https://telegram.org/faq#q-there-39s-illegal-content-on-telegram-how-do-i-take-it-down

Thomas, D. R., Pastrana, S., Hutchings, A., Clayton, R., & Beresford, A. R. (2017). Ethical issues in research using datasets of illicit origin. *Proceedings of the 2017 Internet Measurement Conference*, 445–462. https://doi.org/10.1145/3131365.3131389

van Hardeveld, G. J., Webber, C., & O’Hara, K. (2017). Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets. *American Behavioral Scientist*, *61*(11), 1244–1266. https://doi.org/10.1177/0002764217734271

Wortley, R., & Townsley, M. (Eds.). (2017). *Environmental criminology and crime analysis* (Second Edition). Routledge, Taylor & Francis Group.

Appendix A. Coding Scheme used for Analysis

i. [**Preparation**]

   a. [*Set up the Telegram application*]

      i. [anonymous, application, assurance, connect, defense, guarantee; install, link, messaging app, precaution, protection, safeguard, security, surely, Telegram, turn on, unknown; verification; warranty, wire]

   b. [*Set up a payment account*]

      i. [account, ADA (Cardano), amount, balance, bank card, BCH (Bitcoin Cash), blockchain, BTC(Bitcoin), cash, charge, commission, cost, credit, crypto, currency, debit, debt, DOGE(Dogecoin), DOT (Polkadot), ETH (Ethereum), expense, fee, income, LINK (Chainlink), LTC (Litecoin), payment, PayPal, price, repayment, salary, stocks, transaction, value, wallet, wage, withdrawal, worth, XLM (Stellar), XMR (Monero), XRP(Ripple)]

ii. [**Entry**]

   a. [*Join a meeting place*]

      i. [access, backup channel, backup group, chat, connect, join, link, plug in, private channel, private group, public channel, public group, register, sign up for, switch on, turn on]

   b. [*Learn the group rules*]

      i. [abide by, agree, allowed, approved, banned, become a member, code, comply, conform, correct, customs, disapproved, follow, forbidden, illegal, keep in mind, obey, permitted, prohibited, respect, restricted, right, ripper, rules, statutes, subscribe, take part in, to use, valid]

   c. [*Get started with tutorials and ask for help*]

      i. [answer, assist, comprehend, educational, help, issue, learn, learn how, process, problem, question, study, support, tutorial, understand]

iii. [**Pre-condition**]

   a. [*Obtain the data*]

        i. [acquired, bought, breached, browsed, collected, dumped, found, forwarded, free, forum, hacked, obtained, purchased, spotted, uploaded]

iv. [**Instrumental pre-condition**]

  a. [*Advertise the data*]

    i. [best data, bonus, critical data, discount, escrow, exceptional, good for, guarantee, guaranty, insurance, one in a lifetime offer, outstanding, perfect, rare, sale, suitable for, subscription, top product, top seller, trade, unique, voucher, warrant]

v. [**Instrumental initiation**]

  a. [*React to an ad*]

    i. [approach, contact, connection, direct message, DM, PM, private message, secret chat, touch]

vi. [**Instrumental actualization**]

  a. [*Trade*]

    i. [deal, evidence, paid, proof, reference, screenshots, selling, trade, transactions]

  b. [*Verify the data*]

    i. [antivirus, approved, confirm, confirmed, escrow, feedback, guarantee bot, payment bot, reliable, review, scanned, validate, verification, verify]

vii. [**Doing**]

  a. [*Receive the data*]

    i. [AnonFiles, archive, cloud, decryption key, download, drive, key, mega, password, sent, SharePoint, transferred, unzip, uploaded, zip file]

viii. [**Post-condition**]

  a. [*Manage reputation*]

    i. [banished, banned, confident, confidence, excluded, recommended, ripper, scammer, trust]

  b. [*Report a meeting place*]

        i. [fake, mark, report, scam, spammer]

ix. [**Exit**]

    a. [*Exit*]

        i. [delete, exit, leave]

Declarations

Funding

Not applicable.

Competing interests

The authors have no competing interests to declare that are relevant to the content of this article.

Ethics approval

This study received ethics approval from the Ethical Committee of The Hague University of Applied Sciences.

Authors contribution statements

Taisiia Garkava: Conceptualization, Methodology, Investigation, Data Curation, Writing – Original Draft. **Asier Moneva**: Conceptualization, Methodology, Validation, Writing - Review & Editing, Visualization, Supervision, Project Administration. **E. Rutger Leukfeldt**: Conceptualization, Writing - Review & Editing, Supervision, Funding Acquisition.