Private Clubs For Hackers: How Private Forums Shape The Malware Market

Sandra Langel[1], David Décary-Hétu[2], Olivier Beaudet-Labrecque[1], Luca Brunoni[1], Renaud Zbinden[1]

[1]Insitut de lutte contre la criminalité économique, HEG Arc // HES-SO, [2]Université de Montréal

Abstract

Offenders seek online private discussion forums where participants are screened before gaining access to connect with sophisticated peers and evade detection. Past research finds that most public discussion forum participants have a low level of technical skill and rely on more established participants for the tools and techniques they need to commit their offences. To date, research has mostly focused on public discussion forums of online offenders as gaining access to private forums comes with many challenges. The aim of this research is to describe and understand the impacts of the private nature of discussion forums on their participants' activities. Our driving hypothesis is that private discussion forums are host to more sophisticated participants that will, in turn, offer and have access to more sophisticated tools. To understand the impacts of the private nature of discussion forums, we selected two discussion forums available on the internet whose focus is the sale of malware; one of them is private, while the other is public. Our analysis suggests that while there are differences between private and public discussion forums, there are few significant differences between both inters of the products they advertise.

Keywords: malware, discussion forum, hacking.

1 Introduction

Discussion forums are the descendants of bulletin board systems (BBS) which were used in the pre-internet days. BBS were used to post public messages, exchange private messages as well as files [26]. Their main limit came from their access method which limited the speed at which participants could communicate, as well as their geographical reach. Using phone lines to connect to BBS meant that participants had to pay international fees when connecting to a distant BBS, unless they could somehow bypass the phone companies' billing systems. BBS were often associated with illicit activities as they facilitated the pirating of software and enabled the sharing of hacking tactics and methods [3].

Discussion forums did not inherit the bad reputation of BBS but provide many of the services that BBS did in the 1970s, 1980s and early 1990s. Discussion forums quickly replaced BBS as they could be reached by any internet users at no additional costs to their basic internet connection. At their core, discussion forums are asynchronous communication channels hosted on internet websites [20]. Discussion forums are divided into subforums, which contain multiple discussion threads. Each threat usually discusses a very specific topic (ex. how to hack a Windows password) within a more general subforum (ex. hacking techniques).

Discussion forum participants are divided into multiple groups [21, 28]. The first, the administrators, manage the forum and enforce the social rules [21]. They publish the rules under which everyone else must abide by, and hand out the punishments to those that abuse the rules. Administrators can be elected in some cases but are most often those that create a discussion forum or receive or purchase the title of administrator. The second group, the moderators, serve as the assistants to the administrators. Moderators usually regulate a subforum and are delegated with varying levels of authority [21]. They are nominated by the administrators. Finally, the third group features all of the other participants on the forum. Each forum has its own naming scheme and can subdivide the third group into smaller ones.

The hierarchy of discussion forum participants indicates that all are not equal in terms of rights, but also in terms of access to information. Administrators commonly create sections that are off-limits to certain participants [1]. These sections are considered as VIP, elite or private sections that supposedly feature more valuable content. Participants must either purchase the access to these sections, or be invited in because of their skills, their social contacts or past accomplishments. In addition to sections, whole discussion forums can also be labelled as private. These private forums enforce screenings of new participants who must, once again, use their skills, past accomplishments, money or social contacts to obtain an invitation [12]. In the case of social contacts, participants who vouch for new members can be held accountable should their reference act opportunistically and may be called upon to compensate the victims [22]. [12] evaluated the rejection decisions of candidates that applied to a private discussion forum. They found that candidates who had too large of an online footprint on multiple discussion forums demonstrated a lack of focus to one community, and one activity, and were therefore more likely to be rejected when applying. Interestingly, administrators and moderators of other discussion forums were not provided with special treatment when it comes down to gaining access to private forums. This status in the community is not recognized, especially when compared to the skill set and past accomplishments of candidates. Moreover, applicants who only mentioned an interest in the marketplace of the private discussion forum were often rejected. Marketplaces are indeed only one section of discussion forums and participants to private forums are expected to share their knowledge in addition to conducting business. This selection process's aim appears to be risk reduction through the elimination of candidates who might draw too much attention, or act opportunistically. [12] unfortunately are unable to evaluate whether this selection process does in fact reduce risks for participants. This behaviour is motivated by the awareness of offenders about the presence of law enforcement on public forums. Offenders therefore seek private forums to lower the odds of monitoring by law enforcement [22]. Because of their access controls, most research to date has focused on open forums [12, 22], and then again, only on their open sections.

Another reason to seek private discussion forums is to join communities with more skilled members. Past research [16, 14, 6] finds that most public discussion forum participants have a low level of technical skill and rely on more established participants for the tools and techniques they need to commit their offences. Participants on forums would be loosely affiliated in general, but high-performing participants are located at the core of the networks on public discussion forums [14].

While private forums are often mentioned but rarely discussed, recent research by [7] finds that private forums may not be as private as their members are led to believe. Indeed, [7] analysis of the Dark0de private discussion forum indicates that 95% of all applicants were accepted into the forum. The authors believe that this approval rate was engineered to increase profits for the administrators. By letting in more participants, they increased the number of sales and customers for their own services. The authors show surprise at their findings when analyzing a private forum that provides many of the same findings as past research on public forums (see for example [10, 16]). This means that the technical level of participants of the Dark0de private discussion forum was likely similar to that of any other public forum.

Discussion forums are usually organized around a certain geographical area [17], as well as a topic. Russians are therefore likely to participate in discussion forums where messages are in Russian; a French fraudster is equally likely to post on discussion forums in French. Many forums try to bridge the gap across cultures and languages, but our past experience suggests that this is rarely the case. Most often, discussion forums openly cater to a specific group of actors who are engaged, moreover, in a specific type of activity. Financial fraud discussion forums may, of course, venture into hacking discussions because of the need for hacker tools to attack banks, but most of their discussion will be the financial angle rather than the hacking angle. This suggests that most forums, even large ones, are still relatively narrow in terms of scope and cater to a specific group. This significantly impacts research projects as one must understand where their subjects are discussing in order to collect the most relevant data for research purposes. It also suggests that many participants are not active in more than one forum, as suggested by [9]. This finding is controversial, however, based on other findings [25].

For many (e.g. [13]), discussion forums are on their way out. Forums lag in many ways behind social networks that provide constant alerts, playful interactions and very visual interactions. Forums have improved over time but are still not as attractive and effective at luring in participants at every hour of the day or night. The advertised downfall of forums can also be explained by the rise of similar websites such as Reddit and Stack Overflow where participants can vote up and down each other's messages and have a voice in what is displayed prominently on the websites themselves. These new evolution of discussion forums share many of their benefits, such as the ability to search for past posts and users and build profiles of users. They are, however, also geared towards increasing engagement and putting the participants, rather than the hierarchy, at the core of discussions. There are unfortunately no statistics on the total number of forums on the internet, nor how many active daily users discussion forums have.

A number of discussion forums are part of the criminal underground [4]. This term englobes all of the infrastructure that online offenders use as part of their crimes. This infrastructure can be used to launch attacks, but also to support those attacks before and after they happen. The criminal underground is therefore present throughout all the criminal scripts of offenders who happen to use online tools and technologies. Within the criminal underground, discussion forums play four main roles [29], though more recent research by [19] points towards a fight role. They first provide formal control and coordination. It is well known that offenders operate outside of the control of the law, and that offenders are therefore in search of some higher authority to help them manage conflicts. Traditionally, the Italian mafia has played this role of a neutral arbiter, but this role is now being transferred to discussion forum administrators when the conflicts are linked to their participants, and activities facilitated by their platform. The second role of forums is to provide social networking to their participants [28]. While anyone can contact anyone on the internet, it is still difficult for offenders to find potential partners and like-minded individuals online. Discussion forums are convergence settings where offenders meet, talk and exchange [19]. The third and fourth role of discussion forums are to mitigate both identity and product uncertainty. Online, anyone can claim to be who they want, and to be able to offer any good or service. Discussion forums serve as ledgers of the past accomplishments – and failures – of their participants. These can be used to build up an online persona, attract new partners, and establish trust and credibility, even though creating a trustful environment remains a challenge across all types of discussion forums, even private ones [7]. They also serve as warnings to those who wished to act opportunistically as their actions can lead to their banishment, and traces of their past offences. A fifth role of forums identified by [19] revolves around the acquisition of competence and knowledge. Forums appear to be valuable sources of information for offenders to learn about new tools and techniques [28]. This is echoed in [24] work that identifies the structure of communication networks on forums. She finds clear mentorship relationships where a small group of participants share their knowledge and answer other participants' questions.

If discussion forums play such roles, it is because conflicts are part of the daily life of online offenders [22]. [21] found for example 160 complaints against participants in a single discussion forum. Those complaints were mostly made against junior members of the discussion forum, and against participants who failed to deliver on their end of a deal. Many complaints were also about defective products and the opportunistic nature of interactions with a participant. Because of the dark nature of interactions on the forum, however, in most cases, [21] could not identify what and if a resolution was reached regarding those complaints. Since the forum studied in their paper was private, the authors were surprised to find just how common complaining was on the forum, and how difficult it appeared to be to obtain justice, even in an environment that touted itself as private, elitist and only accepting quality participants with a good background. Fraud appears to be present in public forums as well [17]. In one case, administrators even appear to be the ones abusing their participants and banning the participants to prevent them from alerting others. There appears to be no single type of abuse in discussion forums. [24] examines the structure of these conflicts and finds that a small group of participants, who also act as mentors, appear to be bullies that control who is able to say what on the forum. These individuals create conflicts with others and seek to intimidate them into silence. Interestingly, conflicts appear to represent only a small fraction of all communications on forums.

These conflicts are perhaps indicative of why discussion forums appear not to be at the core of the activities of many cybercrime groups that were investigated in the Netherlands, the United States and the UK [19]. Indeed, it appears that cybercrime groups form around offline social ties first and foremost. Contacts made online also play a role and help in the formation of criminal groups, but only between individuals who have known each other for extended periods of time online. Forums would therefore be most useful to find enablers, individuals who can supply specific and technical tools and services to cybercrime groups [14, 21, 11]. The networks that are built through discussion forums could hardly be labelled as organized crime, or tight-knit criminal groups [21].

An important component of discussion forums is the marketplace section most forums host [11, 17]. This section enables official and unofficial vendors to post messages about goods and services for sale, and for customers to request certain products as well [21]. Most transactions appear to be negotiated outside of the forums through direct messaging applications like Jabber, Skype or Telegram. [17] shows that most participants in forums are not interested or able to make purchases in these marketplaces. Rather, they are looking for free samples or to benefit from the charity of others who are willing to leak valuable personal and financial information, as well as technical guides about hacking and other offences, for free. A small subset of participants do end up making purchases on forums and this would be enough to sustain an underground economy.

The same abnormal distribution is witnessed for sellers and buyers [6, 9]. Indeed, most sellers make perhaps one, if no sales at all, while a few high-profile actors make numerous sales [6]. There is therefore a great divide between actors, that reminds of a tournament setting as seen in other parts of the criminal underground [2]. There are also much less rewards to becoming a seller than is reported in industry and grey analyses of the criminal underground [7]. Sellers appear to be diversified in that they commonly offer a wide array of products and services. [9] could not explain how or why offenders managed to offer so many different products and services at the same time, and question whether the sellers could indeed deliver on all of their promises. Their analyses could not link the criminal performance of sellers with their degree of diversification. [15] did find, regarding the criminal performance of sellers, that those that were awarded trusted status by forum administrators made more sales [11]. Buyers therefore appeared to have faith in the evaluation of sellers by administrators. Other factors that contribute to criminal performance include posting advertisements in the language of the forum (in their case, Russian), providing detailed contact information, and publishing clear warranty and refund policies.

Discussion forums are not the only marketplaces of the criminal underground. [23] compared advertisements for stolen accounts on paste sites, darkweb marketplaces and discussion forums. They found that forums enabled more discussions between vendors and customers, and allowed for bidding on specific products that were highly sought. Paste sites were mostly used to disseminate free samples and information whereas darkweb marketplaces offered a lot of flexibility on the number of stolen accounts one could buy. Discussion forums tended to offer mostly stolen accounts in bulk. All three platforms presented for each vendor warranty, refund and replacement policies to induce trust between the vendors and buyers. These policies are meant to reassure potential customers should a problem arise, though, once again, no higher authority other than the platform administrators can be called upon should the vendor default on their obligations.

2 Problem

The review of the literature suggests that researchers have managed to study and analyze public discussion forums of online offenders on numerous occasions over the past decade. The general conclusion from these studies is that the leadership of forums plays a significant role in organizing and controlling the social order of their forums [11, 5] though this control is in no way, shape or form perfect [21]. Public discussion forums are convergence settings where mostly unskilled online offenders meet, converse and transact [29]. These public discussion forums appear to facilitate the sale of a wide array of illicit goods and services [14, 11] in a low trust ecosystem [6]. Most actors on public discussion forums appear to be lurkers, and a minority of vendors make up the bulk of all sales [9]. Public discussion forums are not tightly knit communities, and do not lead to the creation of organized crime groups [19]. Most strong ties appear to be coming from offline social ties that also use online communications to network.

These valuable findings have helped us propose and develop new public policies to control and regulate online offences. They are, however, limited by the nature of their research subjects, the public discussion forums. [8] and [7] did download a leaked file that contained much of the activities of a private discussion forum, but their studies provide little in terms of validation with only one source of data. [12] and [7] both stress the need for researchers to study private discussion forums, and develop an understanding of how the private nature of the discussion forums impacts who their participants are, and what activities they undertake. [12] question whether our understanding of online offenders can be generalized, and suggest that leaks of private discussion forums, although rare, be used to study this dark population. [7] also stress the generalization problem, and question whether researchers are missing out on the most sophisticated and impactful offenders by only studying public discussion forums.

The aim of this research is to describe and understand the impacts of the private nature of discussion forums on their participants' activities. Our driving hypothesis is that private discussion forums are host to more sophisticated participants that will, in turn, offer and have access to more sophisticated tools. More specifically, this paper will compare public and private discussion forums to describe and understand the primary and secondary types of malware their participants advertise, the infrastructure the malware targets, the freshness of the malware being advertised, the quality based on price of the malware being advertised and, finally, the level of trust in the sellers of malware.

The main contribution of this paper is to generate new insights into the nature of private discussion forums. While this paper only studies one private discussion forum, the analyses we provide will build on past research and help steer future research into this dark population of offenders. Past research has shown that investigating private discussion forums is difficult because of the ethical challenges associated with gaining access to the private forums [12]. The slow but continuous flow of new papers in this area will ensure that, in time, all participants in online offences will be equally studied and understood.

2.1 Data

To understand the impacts of the private nature of discussion forums, we selected two discussion forums available on the internet whose main focus is the sale of malware. In the context of this paper, malware is to be understood as any software, code, or piece of code, that executes harmful operations on a third party's computer system – such as, for example, ransomware, worms, and spywares. This definition excludes by definition phishing software, spamming software and encryption services which support malware infections and spreading, but is not malware itself.

Our discussion forum sample is one of convenience. A private cybersecurity company based in Montreal, Canada, called Flare Systems provided us with access to a private discussion forum. The private discussion forum is first and foremost a Russian language speaking forum, with over 62,000 members and 1,100,000 public posts (average 18 posts per member). The forum is often mentioned in news and industry reports that look for information about the most prominent malware producers, distributors and users. All Russian posts were translated using the Google Translate free service. Our analysis focuses on the Buying/Selling subforum, and more specifically the section advertising malware for sale. The public forum was chosen from a pool of candidates based on its similarities with the private discussion forum, and its public profile. The forum is also often mentioned in industry and news reports on malware. The public discussion forum also has a mix of Russian and English posts, and we used the Google Translate service to translate the posts to English. We focused on four subsections of the forums that facilitate the sale of malware. The public discussion forum appears to have much more lurkers with over 185,000 members but only 345,000 posts (average 2 posts per member).

Because of constraints in time and resources, we limited our data collection to threads whose last post was between June 1st 2020 and February 10th 2021. All data was collected manually by browsing through the forum between March and May 2021, but copies of messages were saved for future references. Our team read each thread title and identified the threads that explicitly mentioned the sale of malware. Whenever the title did not provide the necessary information, the whole thread was read to evaluate whether the thread was to be included or excluded from the analyses.

362 threads were analyzed on the public discussion forum, and 86 were confirmed to offer the sale of malware as understood by our definition. On the private discussion forum, we examined 806 threads and found 136 that advertised the sale of malware. The threads that were not selected for analysis were either for sales of non-malware products, or for product or partnership research.

2.2 Methodology

For each thread, we collected data on the threads, the sellers and the malware. For the threads, we collected the thread name, its description, its URL and its unique identifier. For the sellers, we collected their unique identifiers, their reputation score and their number of public posts. Finally, for the malware, we collected the malware name, the malware type, the method of payment for the malware as well as the price in US dollars. Once the data had been compiled, we cross-referenced the results in order to compare the two forums based on 5 criteria: a) the types of malwares; b) the targeted infrastructure; c) the malware freshness; d) the malware quality and; e) the trust in vendors.

The types of malwares were identified either based on what the vendors stated in the discussions or based on internet searches for the name of the malware (when the vendor mentioned it). If no information was available, the malware was classified as "undefined". A preliminary analysis of the malware showed a wide variety of products for sale. In order to facilitate the comparison between the two types of forums, the malware has been classified in two primary categories: those that allow accessing a machine and those that exfiltrate data and information. Products that could not be placed within these categories were listed as "unidentified". A secondary typology of malware was also elaborated based on our review of the malware description and is presented in the Results section.

The targeted infrastructure was extracted from the description of the malware. We searched for mentions of the targets of malware which could either be computers, mobile phones or other devices such as critical infrastructure or the internet of things appliances.

Based on the assumption that malware that is recent and features a unique source code is potentially more threatening (as it is less easily detected by antivirus software), it was deemed useful to determine whether one of the types of forums offered malware launched more recently than the other. In order to do this, we looked at the description of the malware, and searched for its name on Google to identify the first mention of the malware. This enabled us to find the launch date of malware. This search proved difficult, and yielded results for only 37 private forum malware (27%) and 36 public forum malware (42%) The private discussion forum malware about which the most information was found are stealers (17, of which 10 are ransomware), and RATs (9). With regard to the public forum, they are stealers (16) and RATs (14).

Pricing is a major indicator of quality in the criminal underground, as in many things in life. Malware offered for higher prices is expected to operate at a higher level, and to deliver more resources. We collected the price for each malware to determine its quality. When prices were not indicated in the main topic, all questions and answers within the thread were analyzed to see if the information could be found there. As a last resort, a request was made to the seller via a private message. The private discussion forum provided us with a more complete dataset for the pricing of malware. As such, we used its distribution to create a scale of the distribution of malware prices based on the detected fluctuations.

Finally, the trust put in vendors is evaluated by the forum participants themselves. A participant can be rated positively, negatively or not rated at all (rating a seller is also not mandatory). The sum of all received ratings gives the popularity of the seller on the forum. As vendors can be evaluated on discussion forums, a categorization based on these ratings has been established. Same as for the prices, the private forum features a wider and more detailed range of evaluations; it has therefore been used to create a trend line and define several categories: negative / 0 / 1-10 / 11-20 / 21-30 / 31-40 / 41-50 / 50+. The ratings obtained by a vendor are added and subtracted (if negative) to the vendor's total. A rating of 0 can therefore signify either that the vendor has never been evaluated, or that his total amount to 0 - the first being the most likely possibility.

3 Results

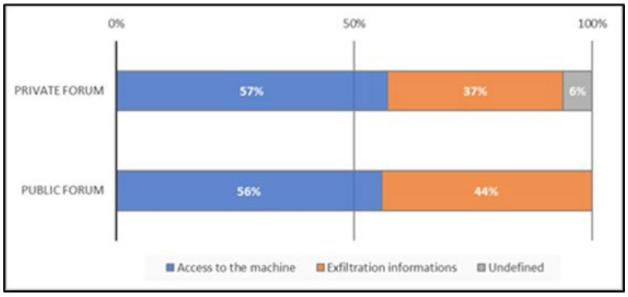
The results of this research are presented below and cover the four areas of concern which are the types of malwares, the freshness of malware, the quality of malware and the reputation of vendors. Before we move on however, we share below three general insights about private forums.

First, private discussion forum participants observe a code of conduct regarding the use of malware and its targets. Many vendors state in their advertisements that buyers are not allowed to use their malware against individuals, structures or companies in the Commonwealth of Independent States area. In one thread, a vendor prohibited using his malware against State structures like hospitals or schools. This was not observed in the public forum. On the private discussion forum some sellers stated that they would not sell their malware to people from the United States of America. Indeed, on this forum, which is totally Russian-speaking, an American-Russian rivalry was clearly felt. This was less visible on the public forum, which is not entirely Russian speaking. Second, no transaction or mention of a transaction is visible on either forum. On the private discussion forum, almost all vendors use their treads as bait, and demand that further conversation with potential buyers take place on messaging platforms such as Jabber and Telegram. Answers to their posts include general questions regarding prices, technical information, system compatibility, and mentions of interest from buyers. On the public forum, demands to move the conversation to other platforms are observed less frequently, and vendors appear to prefer discussing over the private messaging system of the forum. Third, on both forums, several threads link to websites featuring further information about the malware for sale. Some threads even link to YouTube videos showing the user interface of the malware and explaining how the malware works.

3.1 Primary Types of Malwares

As shown in Figure 1, the malware for sale on public and private discussion forums can be divided into two classes. Malware that provides access to computers represents just over half of all malwares for sale on both public (56%) and private (57%) forums. Malware that exfiltrates information like financial records and passwords is more prevalent on public (44%) than private (37%) discussion forums. This could be, however, an artefact of the fact that private discussion forums are lacking information on 6% of malware, either because the name and type of malware were not specified in the advertisement, or because the type was not specified and searching for the name of the malware returned no hits. Another explanation is that the malware is so new that it is still not widely known. In any case, our analysis suggests a relatively even split between the two types of malwares for sale, and a marginal difference between the two types of discussion forums.

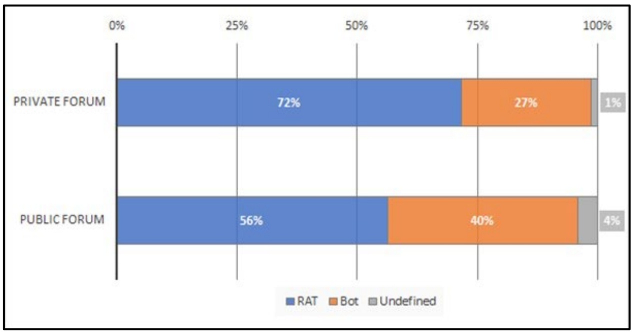
Figure 1: Distribution of malware



3.2 Secondary Types of Malwares

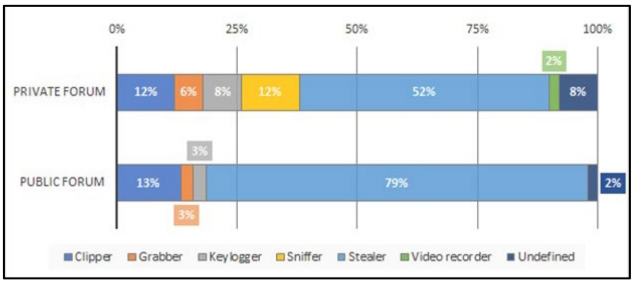
Malware can be further organized into secondary types. Table 1 summarizes all secondary types of malwares. For malware that provides access to a machine, we found two types: RATs (Remote Access Trojan) and botnets. RATs are malware that covertly create access points for malicious actors that allows them to remotely log in and operate the victim's devices. Botnets also take control of a computer, but with the aim of putting it under the control of a command and control centre (C&C). The most common use case of botnets is the exploitation of the device resources (storage, bandwidth, computational power). RATs are more prevalent in private discussion forums with 72% of all malwares for sale. Botnets are found in greater proportion in public discussion forum with 56% of malware for sale. While the difference is not significant enough to find either type of forum are specialized, it does suggest that the supply of each type is geared towards a type of forum. The unidentified category groups other types of malwares that could not clearly be labelled as one or the other.

Figure 2: Distribution of malware that provides access to a machine



The malware that exfiltrates information can be grouped into six sub-categories. Clippers are malware that monitor, extract or replace confidential and sensitive information from a device's clipboard. It is commonly used to replace a cryptocurrency wallet being copied to send or receive funds to steal the victim's funds. Grabbers are malware that steal information from web forms in browsers. They monitor the victim's web surfing, and opportunistically steal usernames and passwords when they are entered in online forms. Keyloggers are malware that are very similar, but that monitor all keystrokes, not only those entered on web forms. Sniffers are malware that monitors network traffic in real time and collect sensitive information. Stealers are malware that steal sensitive information such as passwords and usernames, or that encrypts data (ransomware and ATM stealers). Video recorders are malware that records screen activity or webcam images. They are commonly used to extort victims after private pictures of them are taken. Finally, undefined malware are those that did not fit in any of the above categories.

Figure 3: Distribution of malware that exfiltrates information



Private discussion forums offer a wider range of malware than public discussion forums. Stealers are the most prevalent secondary type of malware on private (52%) and public (79%) discussion forums. Sniffers and video recorders are found exclusively on private discussion forums, totalling 12% and 2% respectively. Keyloggers and grabbers are present on both private and public discussion forums and are prevalent on private (14%) rather than public (6%) discussion forums. Clippers are found in similar percentages on both types of discussion forums (12% for private, 13% for public forums).

Table 1: Secondary types of malwares

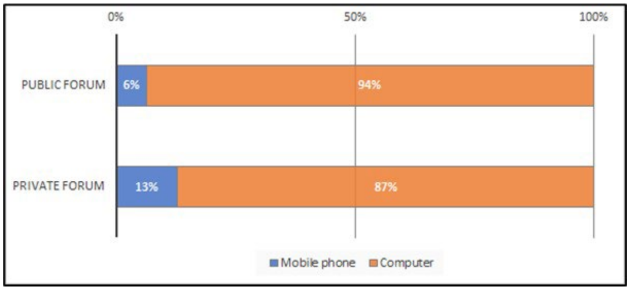
Primary type	**Secondary type**	**Definition**
Access to machine	Botnet	Malware that takes control of a device in order to exploit its resources.
	RAT	Malware that enables remote control of the device.
Information exfiltration	Clipper	Malware that monitors, extracts or replaces confidential and sensitive information from the clipboard.
	Grabber	Malware that steals information from web forms.
	Keylogger	Malware that records keystrokes.
	Sniffer	Malware that monitors network traffic in real time.
	Stealer	Malware that steals sensible information such as passwords and usernames, or that encrypts data (ransomware).
	Video recorder	Malware that records screen activity or webcam images.
	Undefined	All malware that could not be placed within the above categories.

Five specific malwares were found several times on the private discussion forum: Avalon clipper (2x), Cobalt Strike (9x) and Osiris (3x) RATs, Cerberus mobile malware (3x), and Zeppelin ransomware (2x). On the public discussion forum, two malwares were found several times: the Anubis mobile malware (7x) and Echelon stealer (2x). Only three of these specific malwares were found on both types of forums: "Anubis" and "Cerberus", two Android mobile malware that empty their victims' bank accounts, and a ransomware named "Makop". No other connections could be observed, as the other malware present on the forums are identified with different names or had no name. Nameless malware is more prominent in the private discussion forum (27%) than in the public discussion forum (18%). Only one vendor, Makop, who offers the stealer (ransomware) of the same name appears on both forums. His registration date is the same on both forums; he has been inactive on the public forum for almost one year, and his last activity on the private forum dates back to only 1-2 months.

3.3 Targeted Infrastructure

Malware targets multiple electronic devices, from computers to internet of things devices, as well as critical infrastructure like gas pipelines. Through our analyses, we found that the malware for sale on the public and private discussion forums only targeted two types of devices, computers and mobile phones. Figure 4 presents the distribution of targets of malware.

Figure 4: Distribution of targeted infrastructures

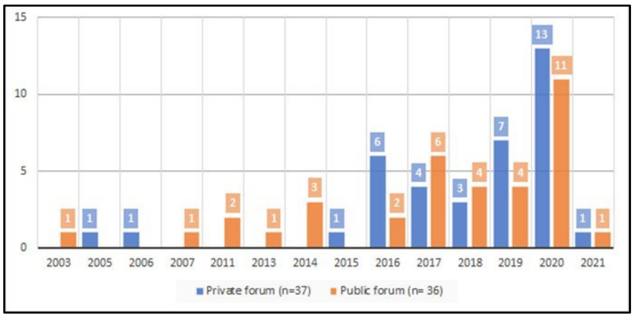


Mobile phone malware represents only a small portion of all malwares for sale (6% of public discussion forums and 13% of private discussion forums). In all cases, Android phones are targeted. The vast majority of malware therefore targets exclusively computers. While computers represent the most common target on both types of forums, private discussion forums show a noticeable higher presence of mobile phone-targeting malware.

3.4 Malware Freshness

In order to determine whether the types of discussion forums offer malware of the same freshness, we evaluated the pricing of malware offered in both settings. All the malware for sale was launched between 2000 and 2021. In both public and private forums, about one third of the malware was launched in 2020, and both types of discussion forums featured 1 malware categorized as a stealer that launched in 2021. In general, the malware sold on the private discussion forum appears to be more recent with 56% of the private discussion forum malware launching in 2019 or later, compared to 44% on the public discussion forum.

Figure 5: Distribution of malware freshness



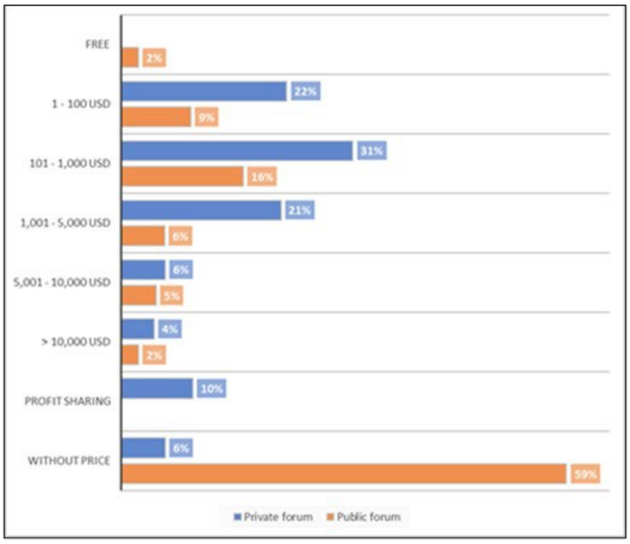
3.5 Malware Quality

Many malware advertisements display no price. This is much more common on the public discussion forum (60%) than on the private discussion forum (6%). Our team sought to obtain prices by contacting the vendors on the discussion forums directly but was asked to engage with the vendors on instant messaging services. For ethical reasons, we decided not to contact the vendors there and only analyze the data we collected from open sources. Transparency regarding prices is much higher on the private than on the public discussion forum.

On the public discussion forum, two malwares were offered for free: a botnet and a stealer. In the latter case, however, the vendor was flagged as a ripper (scammer) in the comments. The private discussion forum offered no such offers. On the private discussion forum, more than 50% of the malware offered for sale does not exceed USD$1,000, compared to a little more than 25% for the public discussion forum. On both forums, the USD$101 to USD$1,001 price range is the most common. On the public discussion forum, the cheapest malware - a malware that redirects victims to fake Bitcoin Exchange sites - is sold for USD$26. The comments state that the malware is fake and probably doesn't work. On the private discussion forum, the cheapest product is a RAT priced at USD$25.

Malware sells for more than USD$10,000 on both types of forums but is uncommon at that price point. On the private discussion forum, 5 malwares out of 136 range from USD$12,000 to USD$30,000. A sixth, undefined malware is available at $USD12,000. On the public discussion forum, only 2 malwares are priced above USD$10,000: a malware costing USD$18,000 USD and a stealer costing 1 bitcoin or approximately USD$30,000. For the latter, however, the comments accuse the vendor of being a ripper.

Figure 6: Distribution of malware prices

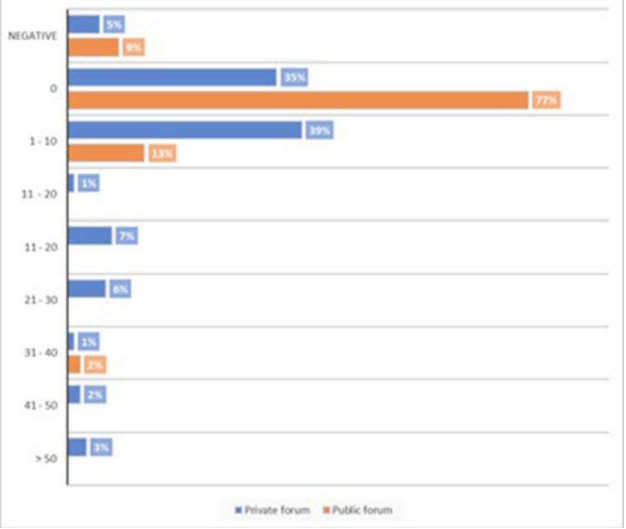


Profit sharing is a way of selling malware in exchange for a percentage of the profit that the buyer will gain through its use. This practice is present on the private discussion forum exclusively. As an example, the Exorcist ransomware can be obtained in exchange for 30% of the profits. Of the 13 malwares offered through profit sharing, 3 are RATs, 1 is a sniffer and the others are stealers (ransomware). As this method implies a trust-based agreement, profit sharing might be an indicator of the presence of a more professional, tightly knit community on the private discussion forum. For example, the Makop ransomware (available on both types of forums) is sold for USD$250 USD on the public forum, while on the private discussion forum, the seller also offers a profit-sharing agreement.

3.6 Vendor reputation

In the public discussion forum, 77% of vendors received a rating of 0, compared to only 35% in the private discussion forum. Moreover, 89% of the ratings given to the vendors in the public discussion forum does not exceed the 1 to 10 range. The proportion of vendors with a negative rating is nearly 9% in the public discussion forum, versus 5% in the private discussion forum. These results show that private discussion forum users are more likely to evaluate vendors, and that a higher importance is given to such evaluations than in the public discussion forum. It must also be noted that 13 public forum vendors have been accused of being rippers by other users. No such accusations are found on the private discussion forum. However, two vendors warned users to be vigilant against scammers usurping their username.

Figure 7: Distribution of vendor ratings



Almost all the advertisements on the private discussion forum mention that a guarantor must be used in order to finalize the sale. The guarantor is a neutral third party who verifies that the transaction happens as agreed. On the public discussion forum, only a small percentage of the advertisements (N = 10) mention the need for a guarantor. Some vendors question potential buyers, e.g. about their experience and the countries they intend to target. This is observable mostly in connection to profit-sharing agreements on the private discussion forum, but also on the public discussion forum, for example in connection with the Makop ransomware.

4 Discussion and conclusion

The main aim of this paper was to describe and understand the impacts of the private nature of discussion forums on their participants' activities. Our driving hypothesis was that private discussion forums are host to more sophisticated participants that will, in turn, offer and have access to more sophisticated tools. To achieve this goal, we analyzed the primary and secondary types of malwares their participants advertise, the infrastructure the malware targets, the freshness of the malware being advertised, the quality based on price of the malware being advertised and, finally, the level of trust in the sellers of malware.

Our analysis suggests that while there are differences between private and public discussion forums, these differences were not what we had guessed. Indeed, the pricing of malware – our proxy for its quality – suggests that there are no wide differences between the pricing of private and public discussion forum malware for sale. The same can be said of the year that malware was launched. Here again, we find some differences, but nothing that would set the two forums completely apart. This suggests at least that both public and private discussion forum offer some basic and sophisticated malware for sale, and that the differences could be found elsewhere.

The first difference lies in the trust between participants. Private discussion forums often require the use of a guarantor to ensure the positive outcome of a transaction. They also foster enough trust for participants to work collaboratively as profit-sharing partners, something we could not see in the public discussion forum. We saw a vendor that demonstrated this best as he offered the same malware on both types of forums, but under very different conditions. The vendor reputation score echoes this with many reputation scores of 0 on the public discussion forum. This suggests that the community on this type of forum is not as thick and involved as that of the private discussion forum. Already, comparing the average number of posts (18 vs 2) had shown that private discussion forums are more engaging for their participants. Private discussion forums may in essence foster more trust and take advantage of more tools to build trust. As such, it could be more organized than public discussion forums and lead to more positive outcome for malicious actors.

The often-mentioned Russian ties are very explicit in the private discussion forum. It is explicitly mentioned that the malware is not to be used against Russian companies and individuals, and that sales to Western countries is even prohibited. This reinforces the belief that malicious actors gather to the same discussion forum based on their activities, and geographical origin. This raises some interesting question regarding the offline ties of malicious actors, and whether these individuals also connect offline, in addition to online. The impacts of this on the regulation of their activities would be significant, as the investigation tools are not the same for online and offline organized crime groups.

Our paper also shows that malicious actors do not appear to be worried with hiding themselves. They link to videos of their malware on public services such as YouTube and use discussion forums hosted directly on the internet. This sense of impunity is present in both public and private discussion forum participants and serves as a reminder of the vast number of malicious actors online, and the dearth of resources to regulate their activities.

This paper is limited first by the limited number of discussion forums that we analyzed. Further research should seek to replicate this study and increase the number of forums that they collect information from. It is difficult at this stage to generalize our findings, and replication will be important moving forward. Another limit is the lack of Russian native speaker in our research team. We used popular Google Translate to translate the text to English, but some information was likely lost in translation. Future research teams should thrive to include a native speaker of the language they are studying in order to get the best possible meaning of all posts. Still, our research has helped us better understand how and why private discussion forums matter. It may not be the place where unknown and more sophisticated malware are offered for sale, but it just may be the place where the most significant and organized threats come from.

Author details

Sandra Langel

Institut de lutte contre la criminalité économique
Haute école de gestion Arc // HES-SO
Espace de l'Europe 21, 2000 Neuchâtel, Suisse
ilce@he-arc.ch

David Décary-Hétu

Université de Montréal
3150 Jean-Brillant, Montréal, Canada, H3T1N8
david.decary-hetu@umontreal.ca

Olivier Beaudet-Labrecque

Institut de lutte contre la criminalité économique
Haute école de gestion Arc // HES-SO
Espace de l'Europe 21, 2000 Neuchâtel, Suisse
olivier.beaudet-labrecque@he-arc.ch

Luca Brunoni

Institut de lutte contre la criminalité économique
Haute école de gestion Arc // HES-SO
Espace de l'Europe 21, 2000 Neuchâtel, Suisse
luca.brunoni@he-arc.ch

Renaud Zbinden

Institut de lutte contre la criminalité économique
Haute école de gestion Arc // HES-SO
Espace de l'Europe 21, 2000 Neuchâtel, Suisse
renaud.zbinden@he-arc.ch

References

[1] Décary-Hétu, D. (2017). Online crime monitoring. In The Routledge International Handbook of Forensic Intelligence and Criminology (pp. 238-248). Routledge.

[2] Décary-Hétu, D., Morselli, C., & Leman-Langlois, S. (2012). Welcome to the scene: A study of social organization and recognition among warez hackers. Journal of Research in Crime and Delinquency, 49(3), 359-382.

[3] Denning, D. E. (1996). Concerning hackers who break into computer systems. High noon on the electronic frontier: Conceptual issues in cyberspace, 137164.

[4] Dunham, K., & Melnick, J. (2008). “Malicious Bots : An Inside Look into the Cyber-Criminal Underground of the Internet” (1er éd.). Auerbach Publications. Online: https://doi.org/10.1201/9781420069068

[5] 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. Online: https://doi.org/10.1177/0002764217734263

[6] Dupont, B., Côté, A.-M., Savine, C., Décary-Hétu, D. (2016). “The ecology of trust among hackers”. Global Crime, 17(2), 129–151. Online: https://doi.org/10.1080/17440572.2016.1157480

[7] Dupont, B., Côté, A. M., Boutin, J. I., & Fernandez, J. (2018). Darkode: Recruitment patterns and transactional features of “the most dangerous cybercrime forum in the world”. American Behavioral Scientist, 61(11), 1219-1243.

[8] Dupont, B. & J. Lusthaus. (2021). “Countering Distrust in Illicit Online Networks : The Dispute Resolution Strategies of Cybercriminals”. Social Science Computer Review, Online: https://doi.org/10.1177/0894439321994623

[9] Haslebacher, A., Onaolapo, J., Stringhini, G. (2017). “All your cards are belong to us: Understanding online carding forums”. In 2017 APWG symposium on electronic crime research (eCrime), 41–51. Online: https://www.uvm.edu/~jonaolap/papers/ecrime17carding.pdf

[10] Herley, C. & D. Florencio. (2010). “Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy” In Moore, T., Pym, D., Ioannidis, C. (Eds.) Economics of Information Security and Privacy, 33-53. Online: 10.1007/978-1-4419-6967-5_3

[11] Holt, T. J. (2013). “Examining the forces shaping cybercrime markets online”. Social Science Computer Review, 31(2), 165–177. Online: https://doi.org/10.1177/0894439312452998

[12] Holt, T. J. & B. Dupont. (2018). “Exploring the Factors Associated With Rejection From a Closed Cybercrime Community”. International Journal of Offender Therapy and Comparative Criminology, 63(8), 1127-1147. Online: https://doi.org/10.1177/0306624X18811101

[13] Holt, K. (2020). “As internet forums die off, finding community can be harder than ever.” Online: https://www.engadget.com/2020-02-27-internet-forums-dying-off.html.

[14] Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. International Journal of Cyber Criminology, 6(1).

[15] Holt, T., 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. Online: https://doi.org/10.1080/01639625.2015.1026766

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

[17] Kigerl, A. (2020). “Behind the Scenes of the Underworld: Hierarchical Clustering of Two Leaked Carding Forum Databases”. Social Science Computer Review. Online: https://doi.org/10.1177/0894439320924735

[18] Lavigne, M. (2021). “C.E.I. (Communauté des États indépendants)”, Encyclopaedia Universalis. Online: http://www.universalis-edu.com/encyclopedie/communaute-des-etats-independants/

[19] Leukfeldt, R., Kleemans, E., Stol, W. (2017). “Cybercriminal networks, social ties and

online forums: Social ties versus digital ties within phishing and malware networks". British Journal of Criminology, 57(3), 704–722. Online: https://doi.org/10.1093/bjc/azw009

[20] Luhrs, C. & L. McAnally-Salas. (2016). "Collaboration Levels in Asynchronous Discussion Forums: A Social Network Analysis Approach". Journal of Interactive Online Learning, 14(1): 29-44.

[21] Lusthaus, J. (2013). "How organised is organised cybercrime?" Global Crime, 14(1), 52–60. Online: https://doi.org/10.1080/17440572.2012.759508

[22] Lusthaus, J. (2019). "Beneath the dark web: Excavating the layers of cybercrime's underground economy". In 2019 IEEE European symposium on security and privacy workshops, 474–480. Online: 10.1109/EuroSPW.2019.00059

[23] Madarie, R., Ruiter, S., Steenbeek, W., & Kleemans, E. (2019). "Stolen account credentials : An empirical comparison of online dissemination on different platforms". Journal of Crime and Justice, 42(5), 551-568. Online: https://doi.org/10.1080/0735648X.2019.1692418

[24] Montegiani, C. (2017). L'apprentissage social chez les pirates informatiques: Analyse de l'influence des relations d'entraide et de conflit sur le processus d'apprentissage. Université de Montréal. Online: https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/19590/Montegiani_Caroline_2017_Travail_dirige.pdf?sequence=1

[25] Motoyama, M., McCoy, D., Levchenko, K., Savage, S., Voelker, G. (2011). "An analysis of underground forums". In Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement, 71-80. Online: https://doi.org/10.1145/2068816.2068824

[26] Rafaeli, S. (1984). "The Electronic Bulletin Board: A Computer-Driven Mass Medium". Social Science Micro Review, 2(3): 123-136. Online: https://doi.org/10.1177/089443938600200302

[27] Reuter, P. (1983). "Disorganized crime: The economics of the visible hand". MIT Press.

[28] Shakarian, J., Gunn, A. T., & Shakarian, P. (2016). Exploring malicious hacker forums. In Cyber deception (pp. 259-282). Springer, Cham.

[29] Yip, M., Shadbolt, N., Webber, C. (2013). "Why forums? An empirical analysis into the facilitating factors of carding forums". In Proceedings of the 5th annual ACM web science conference, 453-462. Online: https://dl.acm.org/doi/abs/10.1145/2464464.2464524.