Mules, Seals, and Attacking Tools:

Analyzing 12 Online Marketplaces

Ziming Zhao, Mukund Sankaran, and Gail-Joon Ahn | Arizona State University
Thomas J. Holt | Michigan State University
Yiming Jing | Arizona State University
Hongxin Hu | Clemson University

A six-year analysis of 12 multilingual online marketplaces focuses on underground commerce, including stolen user data, fake identities, and attacking tools and services. Migration trends, items for sale, and seller and buyer characteristics reveal commonalities among these fraudulent markets.

Researchers have dissected and analyzed many technologies designed to facilitate cybercrime, such as malware and botnets, and have proposed and deployed countermeasures against such technologies. However, studying the economy behind these technologies and campaigns is imperative for obtaining a holistic view of cybercrime. The majority of research examining online underground markets considers small samples of mostly English-language markets; few studies have systematically examined or compared multiple markets over long periods of time (see the "Related Work in Online Market Analysis" sidebar).

To remedy this, we collected multilingual online underground marketplace data from 12 market forums between December 2005 and July 2011 and systematically examined and compared them to gain a deeper understanding of cybercrime.

Forums and Data Overview

We first discovered three English-language forums through Google using common terms in stolen data markets, including "carding," "dump," "purchase," "sale," and "CVV" (card verification value).[1] By exploring the contents of the Russian Speaking Carder subforum of these three English-language forums, we discovered three Russian-language forums via user-shared links. We found the other six forums in the same way—by analyzing the posts in the previously discovered forums. These 12 forums were geared toward commerce, whereas most previously studied forums were designed for computer hackers to communicate and share.

Most of the 12 marketplace forums were publicly accessible without registration. A few were available only for registered users. To access these, we created a separate username for each forum but didn't interact with other registered users.

We don't claim the data we have is complete; in fact, we analyzed only certain subforums highly related to cybercrime. For each forum, we gathered data that a registered user would see, such as posts, replies, number of posts from a specific user, and so on. We didn't collect private data that was available only to specific users or administrators, such as private messages and banned user logs. The data was in HTML format and more than

 Copublished by the IEEE Computer and Reliability Societies

Related Work in Online Market Analysis

To peek into the understudied cybercrime economy, some groups have studied specific underground economy cases, such as keyloggers and spam campaigns; others have examined online marketplaces that rent, sell, and distribute malware, botnet, stolen user data, illegal services, and so forth. However, few published studies on cybercrime markets actually assess the pricing structures for data and services. Even though "Exploring Stolen Data Markets Online: Products and Market Forces" and "Examining the Risk Reduction Strategies of Actors in Online Criminal Markets" touch on the subject, few papers have systematically examined or compared multiple marketplaces communicating in different languages over long periods of time.[1,2] As a result, it's difficult to assess the scope of harm that cybercrime markets cause, whether they operate on the open Web or Internet relay chat (IRC). The 12 forums in our study were all geared toward commerce, whereas most forums analyzed in previous literature on underground society were designed for computer hackers to communicate and share.[1,3–7]. For instance, "Examining the Social Networks of Malware Writers and Hackers" explored the social networks of a group of Russian hackers to understand the nature of relationships and the ways that they affect information sharing and action. "SocialImpact: Systematic Analysis of Underground Social Dynamics" modeled online underground social dynamics by considering both social relationships and user-generated contents and systematically quantified social impacts of individuals and groups.

Our study also differs from studies on Silk Road, a fraudulent market that focused on illegal and controlled substances.[8] The forums in our dataset were fraught with threads that were highly related to financial crimes, identity fraud, and other suspicious activities.

References

1. T.J. Holt and E. Lampke, "Exploring Stolen Data Markets Online: Products and Market Forces," *Criminal Justice Studies*, vol. 23, no. 1, 2010, pp. 33–50.
2. T.J. Holt et al., "Examining the Risk Reduction Strategies of Actors in Online Criminal Markets," *Global Crime*, vol. 16, no. 2, 2015, pp. 81–103.
3. A. Abbasi et al., "Descriptive Analytics: Examining Expert Hackers in Web Forums," *Proc. IEEE Joint Intelligence and Security Informatics Conf.* (JISIC 14), 2014, pp. 56–63.
4. S. Afroz et al., "Doppelgänger Finder: Taking Stylometry to the Underground," *Proc. IEEE Symp. Security and Privacy* (SP 14), 2014, pp. 212–226.
5. T.J. Holt et al., "Examining the Social Networks of Malware Writers and Hackers," *Int'l J. Cyber Criminology*, vol. 6, no. 1, 2012, pp. 891–903.
6. M. Motoyama et al., "An Analysis of Underground Forums," *Proc. ACM SIGCOMM Conf. Internet Measurement Conference* (IMC 11), 2011, pp. 71–80.
7. Z. Zhao et al., "SocialImpact: Systematic Analysis of Underground Social Dynamics," *Proc. European Symp. Research in Computer Security* (ESORICS 12), 2012, pp. 877–894.
8. N. Christin, "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," *Proc. Int'l Conf. World Wide Web* (WWW 13), 2013, pp. 213–224.

6 Gbytes in size. Some of the forum webpages contained direct evidence of financial and computer-aided crime, whereas others contained conversations related to such suspicious activities.

Data Preprocessing Methodology

Manual analysis of this large volume of data is tedious and difficult; therefore, we chose a semiautomated approach by developing programs and scripts that were guided by our initial manual analysis. Then, we manually investigated and verified the extracted results.

After acquiring the forum webpages, we used freshly designed parsers and our in-house social analysis tool to perform preprocessing.[2] Our parsers automatically went through all the collected HTML pages and identified and extracted basic information such as each thread's title, date information, usernames, and post contents. Even though the input HTML format differed among forums, our parsers output well-formatted information and stored it in a database. Our in-house tool then took over and went through all the webpages stored in the database, using a language detection tool to determine the posts' languages. Posts that weren't in English were translated using a language translation tool. Our in-house tool computed the most active and influential users in the dataset and visualized their social dynamics.

To understand our marketplaces, we first automatically identified selling and buying posts. For selling posts, we used four criteria, classifying a post as a selling post when the first and at least one other criterion were satisfied:

- At least one word related to selling appeared in the post. Such words include "sell," "offer," "sale," "give," "trade," "vendor," "dealer," "merchant," and their derivatives.
- The post's length was sufficiently long (more than 150 characters). We used this feature because sellers usually provide product information, which invariably made their posts quite long.
- The words "ICQ" or "PM" appeared in this post.

Table 1. Basic information about the 12 forums' domain names.*

Name	Registrant country	IP locations	Registration and expiration dates
Forum1	Russia	Germany (2), Lithuania (1), Ukraine (1), Portugal (1), Netherlands (1), Moldova (1), Netherlands (1), and Germany (2)	Nov. 2010 to Nov. 2011
Forum2	N/A	Canada (1), Netherlands (1), and Germany (1)	N/A
Forum3	Russia	England	Feb. 2006 to Feb. 2015
Forum4	US, Netherlands	US (1), Canada (3), Netherlands (1), Germany (1), and Ukraine (1)	Sept. 2009 to Mar. 2011
Forum5	Russia	England	Apr. 2004 to Apr. 2015
Forum6	Russia	Sweden	Dec. 2004 to Dec. 2015
Forum7	N/A	N/A	N/A
Forum8	Russia	N/A	Apr. 2011 to ??
Forum9	Ukraine	Germany	Apr 2009 to Apr. 2015
Forum10	Brazil	N/A	N/A
Forum11	Russia	N/A	N/A
Forum12	N/A	N/A	N/A

** Numbers in parentheses indicate the number of consecutive IP locations in each country.*

Sellers usually provided their ICQ (an IM program) numbers or asked to use private message (PM) for further communications.
- At least one word related to money was present. Examples include a dollar sign, "webmoney," "wm," "roubles," "cash," and "wallet."

Buying posts had to meet the following two criteria:

- At least one word related to buying appeared in the post. Such words include "buy," "seek," "look," "search," "purchase," and their derivatives.
- The post was short (less than 150 characters).

Our tool's search engine component indexed all original and translated text in webpages. Given one or more keywords, our tool returned the webpages, posts, and users related to such words. By building programs and scripts on top of our in-house tool, we were able to perform more sophisticated analysis on the original and translated data.

During an initial manual analysis of our dataset, we noticed that a substantial volume of valuable information resided in nontextual resources, so we also analyzed images and flashes in this dataset. To make this analysis scalable, our tool first went through all folders in our dataset and extracted unique images (based on their hash values) larger than 20 Kbytes. This resulted in fewer than 1,000 unique GIF and JPEG files. We manually went through these images to choose the ones that pertained to commerce. After this process, we ended up with fewer than 100 images. A Russian translator helped us understand the content on those images.

Domain Names, Whois Records, and IP Addresses

In addition to the previous data, we acquired the Whois records and IP address histories of the 12 domain names while the forums were active. Our funding agencies requested that we not publish the domain names publicly. Such information would provide unique insights into where these underground forums were registered and hosted and how they migrated from country to country during their lifetime. Table 1 summarizes each forum's basic information, including registrant country, IP locations, and registration and expiration dates, and Table 2 shows the data we collected from each forum, including its subforums; dates analyzed; and number of threads, posts, and users.

Forum1 was an English-language forum dedicated to trading credit cards and other financial information. It was registered in November 2011 by a person who lived in Russia for a year. During that year, the forum had 10 different IP addresses that indicate that the server migrated across six countries. Forum1 data contains 56 threads from the Market subforum, generated by 86 users.

Forum2 was an English-language forum that had a Russian-language carders subforum. Its domain name was registered through privacyprotect.org, which acts as a registrant proxy and obfuscates the real registrants' identities. Therefore, we don't know how

Table 2. Summary of data from the 12 forums.

Name	Subforums	Dates covered	No. of threads	No. of posts	No. of users
Forum1	Market	Dec. 2010 to Jan. 2011	56	112	81
Forum2	Russian speaking carders	Dec. 2010 to Jan. 2011	118	378	114
Forum3	Hacking & Security > Money	Dec. 2005 to Feb. 2011	398	8,751	1,652
Forum4	Buy/Sell/Exchange/Jobs	Sept. 2009 to Feb. 2011	508	1,637	478
Forum5	Flea market	May 2008 to Jan. 2011	891	1,892	792
Forum6	Banks, Auction	July 2008 to Mar. 2011	775	7,983	1,585
Forum7	Russian speaking carders	Dec. 2010 to July 2011	300	1,710	344
Forum8	Verified services only > accounts, enroll > bank drops > botnets, viruses, exploits > call services, translation text > cashing atm payment system > cc with ccv > design, scans documents, id > drops for stuff > dumps, sell, cashout > hacking services > money exchanges, wu > other services > plastic, holograms > security, vpn, socks, proxy > servers, hosting, rdp > spam, flooding, job posting > ssn, mmn, dob > traffic, load	Apr. 2011 to July 2011	385	1,734	727
Forum9	Shop > Buy/Sell > Job	Aug. 2009 to Mar. 2011	600	1,960	614
Forum10	Hacking & Security > Payment systems	Apr. 2007 to Mar. 2011	86	824	320
Forum11	Ack Software > Trojans and keyloggers > Scanners and rest > SEO/Financial Objectives	July 2007 to Feb. 2011	824	2,534	808
Forum12	> Carding Forum >> Fraud Sell/Buy/Exchange	June 2007 to Feb. 2011	749	1,842	871

long the domain name was actually registered to the original registrants. From December 2010 to January 2011, Forum2 changed its IP address three times, migrating from Canada to the Netherlands and then to Germany.

Forum3 was a Russian-language website and forum that was active at the time of this writing. It features technology news and blogs, most of which focus on hacking skills, such as vulnerability discovery and exploit writing. Forum3 had a domain name registration record for 10 years, and was hosted in England. We have an archive of 398 threads, most of which belong to the subforum Money.

Forum4 was a Russian-language forum whose subforum Buy/Sell/Exchange/Jobs was fraught with the sale of rogue programs and VPN (virtual private network) services. The domain name was registered by registrants living in the US and the Netherlands from September 2009 to March 2011, during which the domain migrated across five countries.

Forum5 was a Russian-language website and forum that was active at the time of this writing. Its Whois

records indicate it had an 11-year registration from April 2004 to April 2015, and was hosted in England. Forum5 data belongs mainly to the subforum Flea market.

Forum6 was an active Russian-language website and forum that reported crime-related news. It also had a registration record of 11 years, from December 2004 to December 2015, and was hosted in Sweden. Its data mainly belongs to the subforum Banks, Auction.

Forum7 was an active English-language forum with a Russian-language carders subforum. Its domain name was registered through several privacy-reserving proxies, including privacyprotect.org. Forum7 data covers December 2010 to July 2011 in the Russian-language carders subforum.

Forum8 was an English forum with a subforum called Verified services only, which was further divided into many subforums, each of which focused on one area, such as bank drops and botnet, viruses, or exploits. Forum8 acted like a "one-stop shop" where users could find a variety of services. Our Forum8 data includes user-generated content from 727 users.

Forum9 was an active Russian-language hacker forum. The records indicate that it was registered by someone living in Ukraine, and its server was located in Germany. The domain name was registered from April 2009 to April 2015. We have data from its Buy/Sell and Job subforums.

Forum10 was a Russian-language hacker forum with a Payment systems subforum under Hacking & Security. We have data posted by 320 users from April 2007 to March 2011.

Forum11 was an active Russian-language hacker forum. Its registration record is obfuscated. We have the posts from subforums Trojans and keyloggers, Scanners and rest, and SEO/Financial Objectives—all subforums of Ack Software.

Forum12 is a live Russian-language hacker forum that has a popular carding subforum and Fraud Sell/Buy/Exchange subforum with more than 700 posts and 800 users. The domain name was registered through privacyprotect.org.

In summary, five out of the 12 forums were out of service at the time of writing. According to our Whois and IP address information, these five forums changed their IP addresses many times during their life cycles. All five forums provided few features apart from discussion boards on selling and buying. Their Whois registration records also show relatively short registration periods that could indicate that the administrators planned to run these forums and domain names for a short period of time. These forums might have been reincarnated through new domain names.

On the other hand, most of the active forums were part of a larger website. Even though evidence of financial and computer-aided crime can be found in these forums, their parent websites host legitimate news articles and blogs. Their Whois records also show that their domain names were registered for up to 11 years. We assume such websites weren't designed merely for underground commerce; however, the communities built around them participate in suspicious activities.

Marketplace Analysis

Here, we present analysis results on the marketplaces, describing representative goods, seller and buyer characteristics, popular payment methods, and some persistent advertisements.

Goods

Common goods sold in underground markets include dumps, skimmers, identities, attack tools, and mules.

Dumps. Dumps comprise stolen credit card or bank account numbers and associated customer data;[1,3] they were the most popular goods for sale in our 12 marketplaces. Using our semiautomatic approach, we found 1,781 dumps sellers in this dataset. The prices for dumps ranged from US$6 for a standard American credit card to $200 for a corporate Canadian corporate card.

We found dumps all over the world including Europe, Asia, the Middle East, Canada, and the US. Some had service code 101 or 201, which means the cards could be used internationally with a normal authorization process and no restrictions on merchant type. Some dumps had both International Air Transport Association track 1 data, which contains the cardholder's name as well as account number and other discretionary data, and American Banking Association (ABA) track 2 data, which contains the cardholder's account, encrypted PIN, plus other discretionary data. Some had only track 2 data, for which sellers often offered free tools to extract track 1 data.

There were some dumps with track 2 data and customer names. Dumps were sold either with or without PINs and CVVs. Buyers sometimes left feedback on sellers and helped other buyers to decide where to buy. Examples include, "Bought 43 dumps with bonuses … 90% HIT OVER 2K AMAZING!" It's hard to estimate the amount of dumps in these markets of the sellers' revenue, but most sellers claimed to update dumps every day. Even though most sellers didn't broadcast how they acquired these dumps, one post, as shown in Figure 1a, says the dumps were stolen with skimmers.

Skimmers. Users could buy skimmers for many types of ATMs (such as Wincor, NCR, and Diebold Opteva); prices ranged from $425 to $6,000 for a skimmer and its accessories. Our tool identified 17 posts selling skimmers.

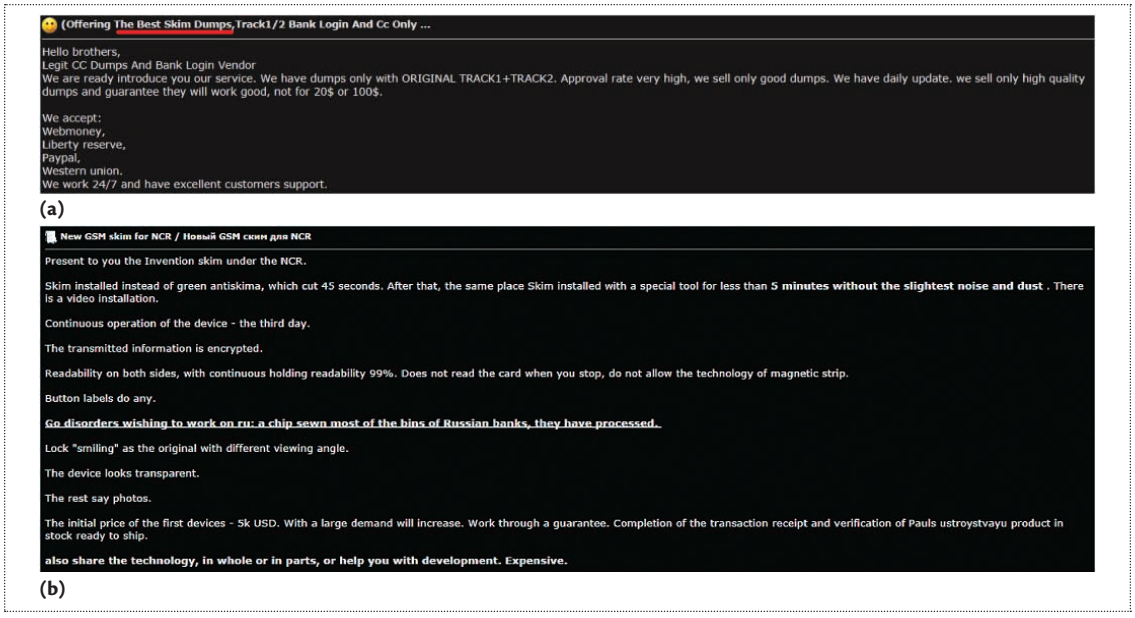


Figure 1. Dumps and skimmers. (a) A post selling dumps. The title implies the dumps were obtained by skimming. (b) A post selling skimmers. The presented skimmer cost US$5,000 and claimed to work on NCR ATMs. The original post was in English and Russian.

Figure 1b shows such a selling post in which the seller promoted Global System for Mobile Communications (GSM) skimmer for NCR ATMs. The seller advertised that this skimmer could be installed in less than six minutes, including the time for removing NCR ATMs' green antiskimming solution.

Identities. Identity-related goods were popular in our marketplaces. Figure 2a shows the identity-related items a user can buy from these markets. The left column shows a fake Russian passport, Israeli passport, and Russian driver's license. The middle column shows a fake Russian ID with a hologram that the seller claimed could "pass tests." A Russian-speaking seller created these fake IDs and charged 5,000 rubles apiece. This seller claimed to provide customized fake IDs within days. The right column shows several fake holograms, which resembled the Russian Federation's coat of arms.

English-speaking sellers also provided fake IDs. For example, we found an English-speaking seller who claimed to provide fully swipeable and scannable IDs with correct hologram and ultraviolet display. This person claimed to have holograms of Florida, Rhode Island, New Jersey, Illinois, and Pennsylvania (with UV) in stock and asked for $1 per hologram for orders of less than 200 IDs. The price dropped to $0.50 per hologram for orders over 500.

Attacking tools and services. The marketplaces were fraught with attacking tools and services. For example, 89 posts were selling distributed denial-of-service (DDoS) tools and services. Figure 2b shows such a post wherein the seller sold DDoS attacks for $50 per night. The seller claimed the DDoS service had been verified by three markets, including Forum4, and sold the Optima botnets as well.

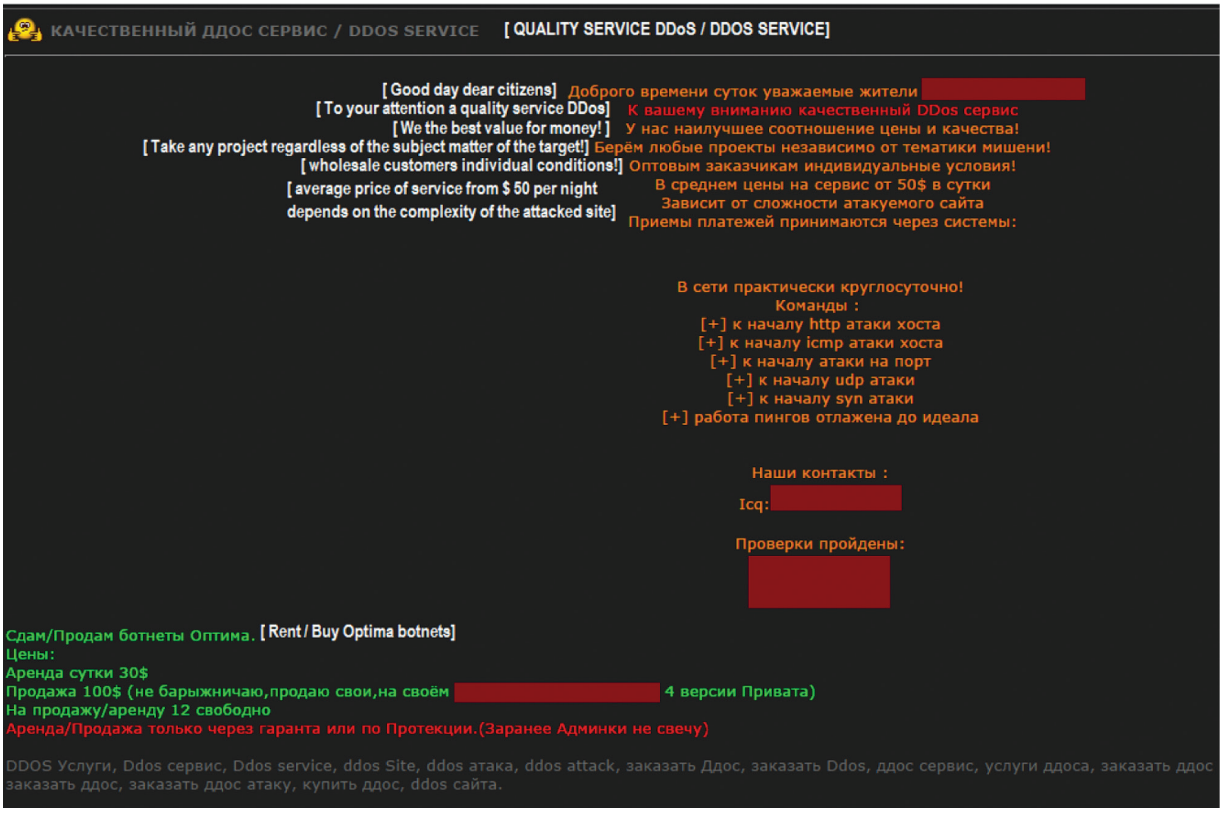
An April 2011 post was selling the famous bankbot Carberp, including links to a video of the tool. The seller asked 2,500 WMZ (WebMoney transfer title unit that's equivalent to US dollars) for a version with loader and grabber, 5,000 WMZ for a version with backconnect and the ability to inject Internet Explorer and Firefox, and 8,000 WMZ for a version with Virtual Network Computing (VNC)-like remote control. Other attack tools in the market were the PickPockeT botnet, Katrin exploits pack for rent, webinjects for Zeus/Spyeye, and a black hole exploits kit.

Mules. Four posts were either selling or buying mules. The buyers posted the destinations for which they needed muling services; however, it's unclear which goods they were trying to move.

Sellers and Buyers

We were interested in whether sellers were as well connected as buyers and other users. Because no explicit social networks were defined in these forums, it was impossible to retrieve users' buddy lists or contacts, as we can in Facebook or LinkedIn. Instead, we generated the connections between users based on the visible

(a)



(b)

Figure 2. Identity-related goods and attacking tools. (a) Identity-related goods found in the studied markets. The left column shows fake Russian and Israeli passports and a fake Russian driver's license. The middle column shows a fake ID with a hologram selling for 5,000 rubles. The right column features fake holograms for US$1 each. (b) A post selling distributed denial-of-service attacks. The post was in Russian; the white text in square bracket is the translation from an automated tool.

interactions among them in forum threads. If two users posted in the same thread, our algorithm added them to each other's contact list.

We use contacts per user (CPU) as a metric to

Table 3. Number of sellers, buyers, and unclassified users in each forum.*

Name	Buyers	Sellers	Other
Forum1	31 (55)	21 (34)	39 (76)
Forum2	26 (180)	42 (201)	65 (318)
Forum3	203 (9,338)	279 (11,992)	1,329 (30,659)
Forum4	214 (607)	335 (807)	129 (624)
Forum5	363 (287)	623 (491)	134 (655)
Forum6	123 (2,964)	189 (4,469)	1,348 (18,406)
Forum7	95 (1,899)	108 (2,144)	216 (1,940)
Forum8	264 (1,143)	343 (1,183)	365 (3,222)
Forum9	242 (584)	408 (825)	181 (849)
Forum10	25 (633)	53 (1,036)	261 (3,237)
Forum11	217 (1,297)	348 (1,460)	434 (2,327)
Forum12	318 (1,078)	416 (1,495)	400 (3,570)
Total	**2,121 (20,065)**	**3,165 (26,137)**	**4,901 (65,833)**
Contacts per user	**9.4**	**8.2**	**13.4**

** The numbers in parentheses indicate the total number of contacts.*

represent users' social connectivity in each category. As Table 3 shows, we identified the number of sellers, buyers, other users, and their CPUs in each forum using the aforementioned criteria. There were a total of 2,121 buyers and 3,165 sellers. On average, sellers had 8.2 contacts and buyers had 9.4, whereas users who weren't classified as a seller or a buyer had 13.4 contacts on average. We conducted two-sample *t*-tests (with the significance level set at 5 percent) to determine whether the two user groups differed in terms of number and type of contacts. We found that the buyers and sellers didn't significantly differ in number of contacts ($p = 0.127$, H_0 accepted at a 5 percent significance level). However, buyers and sellers did significantly differ from unclassified users in terms of number of contacts ($p < 0.001$, H_0 rejected at a 5 percent significance level).

Manual verification reveals two reasons behind this phenomenon. First, the selling and buying posts possibly triggered fewer replies than other types of threads. We suspect that selling and buying transactions were moved to private channels, such as PM or ICQ, soon after an initial advertisement or solicitation, as research has shown that private communications are frequently used rather than overt purchases on the forums.[1,4,5] However, other types of posts, such as discussion of recent news, would receive more comments. Second, sellers and buyers preferred to keep a low profile and weren't seen participating in other threads as much as other users.

We classified the 3,165 sellers into dumps sellers and other types of sellers. There were 1,781 dump sellers in the 12 forums, as Table 4 shows, which is more than other sellers in total.

We were interested in whether dumps sellers' posts generated more discussions in public than other sellers' posts. Although dumps sellers did dominate all products sold, other resources were needed to facilitate actual thefts. Thus, feedback is invaluable to assess their quality. We used replies per user to represent the average number of comments that users in a category receive. We conducted a two-sample *t*-tests to determine whether dump sellers' posts received equal replies to other sellers' posts. No significant difference was found between the groups in number of replies per user ($p = 0.085$, H_0 accepted at a 5 percent significance level).

We analyzed the number of overlapping usernames across all pairs of marketplaces. The results show these forums didn't share many users, with most pairs of forums having less than 5 percent overlapping usernames. However, 57 percent of Forum2 users were also members of Forum7, and 18.9 percent of Forum7 users were members of Forum2. Besides user overlap, we were also interested in seller overlap across all pairs of marketplaces. By comparing the seller usernames, we found that most of the overlapping usernames belonged to sellers. In the 66 market pairs, the shared usernames from five pairs all belonged to sellers. In addition, 21 market pairs had more than 50 percent of shared users acting as sellers.

Table 4. Number of dump sellers and other sellers.*

Name	Dump sellers	Other sellers
Forum1	14 (20)	7 (4)
Forum2	24 (129)	18 (88)
Forum3	165 (1,950)	114 (1,814)
Forum4	194 (526)	141 (309)
Forum5	318 (456)	305 (379)
Forum6	84 (896)	105 (1,866)
Forum7	60 (309)	48 (274)
Forum8	291 (847)	52 (63)
Forum9	210 (596)	198 (429)
Forum10	19 (169)	34 (240)
Forum11	178 (538)	170 (396)
Forum12	224 (449)	192 (313)
Total	**1,781 (6,885)**	**1,384 (6,175)**
Replies per user	**3.8**	**4.5**

**Numbers in parentheses indicate replies received by sellers.*

Payment Methods

We identified several payment methods mentioned in these forums and counted their occurrence in each forum. Manual analysis revealed that most buyers and sellers mentioned acceptable payment methods, whereas in some cases, sellers were trying to sell credentials of those payment methods.

We differentiated the number of times a payment method appeared in original posts and the number of times it appeared in replies. This is because our manual analysis revealed that a payment method's appearance in an original post was an indicator for buyers or sellers to regard it as an acceptable financial channel to make transactions. And, its appearances in the replies might have been due to discussions and queries. However, we don't have transaction data to show the actual use of any payment method. We use original post–to–all posts ratio (OAR)—that is, the number of times a payment method appeared in an original post divided by the number of times it showed in all posts—as a metric to denote how often a method appeared in an original post. The higher the OAR, the more likely the payment method was acceptable for buyers and sellers.

Table 5 shows our database's most popular payment methods. WebMoney was mentioned the most and had a 66.3 percent OAR. Yandex was the second most popular with 1,247 occurrences and a 55.3 percent OAR. Liberty Reserve, a Costa Rica–based digital currency, was mentioned the third most times. Liberty Reserve, which was shut down by law enforcement agencies in May 2013 for money laundering, was mentioned 702 times and had a 26.3 percent OAR. Western Union and PayPal were mentioned 669 times and 530 times, respectively. E-gold—a digital gold currency operated by Gold & Silver Reserve located in Florida—appeared 179 times and had a 64.2 percent OAR. E-gold was shut down by the US government around 2008.

Most studies capture only a few months of data at a time, which limits the assessment of preferred payment types to what's popular during that period. Even though E-gold is no longer used, it's still found in our sample due to the fact that some posts were made when it was in circulation. Nowadays, Bitcoin is the dominant anonymous online payment system.[6] However, there were only 6.5 million bitcoins in circulation among an estimated 10,000 users as of June 2011, compared to 12.5 million bitcoins and more than 6.5 million users today.[7,8] In our dataset, Bitcoin was mentioned only 43 times in total, and its OAR was significantly lower than average.

Persistent Advertisements

The marketplaces featured some persistent advertisements, which were placed as banner images using GIF files or flashes. These ads weren't posted by forum users but by website administrators. The most common were dump ads, shown in Figure 3a. These ads, both in English and Russian, usually had contact information—either ICQ numbers or email addresses.

Black markets also advertised on other black markets to attract more visitors. We found two ads for Forum2 and Forum1 in Forum4 and Forum11, respectively. Recall that Forum11 was still running at the time of

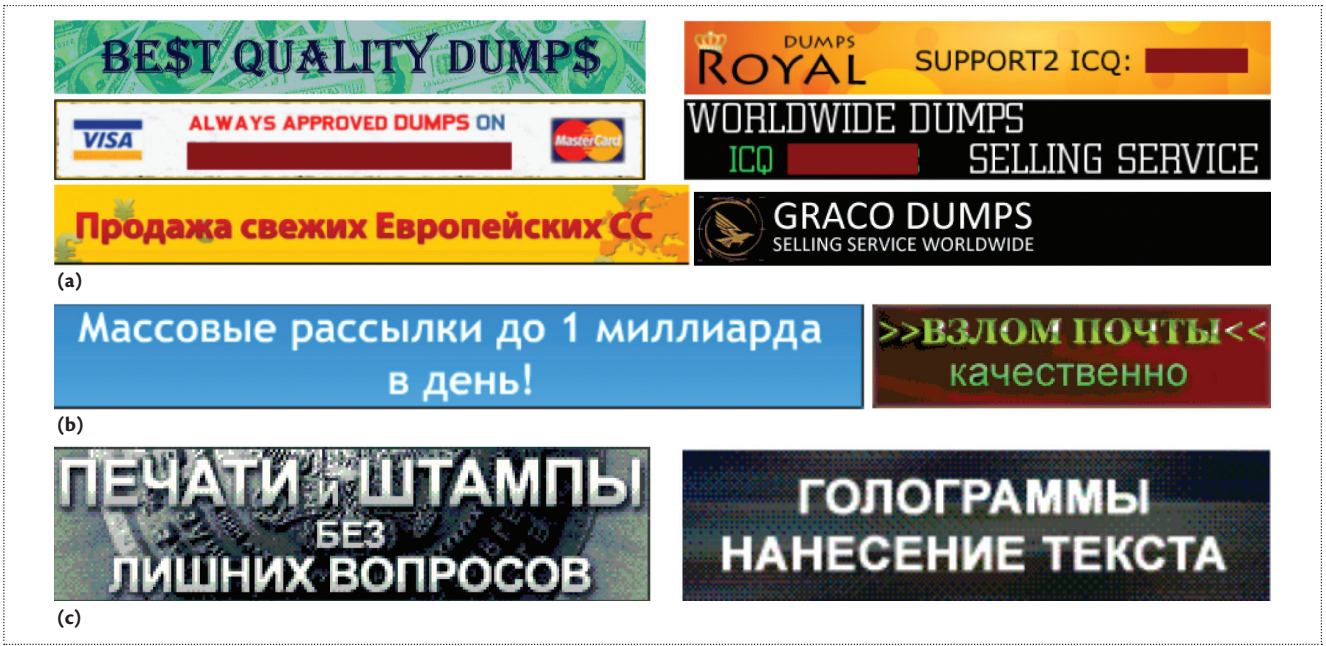


Figure 3. Persistent advertisements. (a) Dumps ads. The image on the bottom left says "The sale of fresh European CC [Credit Card]." (b) Spamming and email account hacking ads. The Russian text on the left translates to "Spam mailings up to 1 billion a day!," and the one on the right means "Hacking mail without advance payments." (c) Seal and hologram ads. The Russian text on the left translates to "Seal and stamp alterations with no questions asked." The text on the right means "Holograms and drawing text."

writing, and our Forum11 data dates back to July 2007. Based on the length of its lifetime, we suspect Forum11 has a reputation in this community and attracts new markets to promote on it.

Discussion

Although this analysis provides an important overview of the practices of cybercrime markets, it's necessary to recognize our data's limitations. First, the forums in this study were accessible during December 2005 to July 2011 without using an anonymity network. Some were even indexed by commercial search engines, such as Google. Evidence suggests that more popular underground forums aren't open to the public and require vetting by known members to gain access.[9] Second, the forum data we collected comprises only posts made in the forum threads, rather than PM exchanges between users. Third, we don't have users' payment transaction data, which is important for understanding actual money movement. This kind of data might be available only from collaborations with financial sectors.

Despite these limitations, publicly accessible forums provide an entry point in the underground cybercrime marketplace, which many low-skilled hackers might use to engage in illegal activity.[1,4] The services available and price points might differ from those of more hidden communities, although there is some evidence that a proportion of the vendors operating in this sample had solid reputations and engaged in transactions across multiple forums to increase their prominence underground. As such, this analysis demonstrates that sellers in these markets have some degree of complexity and sophistication, even though the communities aren't closed or vetted.

Analysis of our marketplace dataset led to several key findings. First, the domain names and websites dedicated to black markets had shorter lifespans, and their website servers migrated among multiple countries in their lifetimes. Second, most goods sold in these marketplaces included dumps, identity-related documents and services, and attacking tools and services. Third, sellers and buyers had fewer contacts in public threads than other users. Their posts triggered fewer replies, and they were less likely to participate in others' threads. Fourth, there were more dump sellers than other kinds of sellers. Fifth, dump sellers did not receive more feedback than other forms of sellers in public threads. And finally, even though many pairs of marketplaces didn't share many users, most of the shared users were sellers. ■

Acknowledgments

This research was supported in part by grants from Army Research Office and Center for Cybersecurity and Digital Forensics at Arizona State University. The information

Table 5. Number of different payment methods in each forum.*

Name	WebMoney	Yandex	Liberty Reserve	Western Union	PayPal	E-gold	Bitcoin
Forum1	4 (4)	0 (0)	2 (2)	0	7 (7)	0	0
Forum2	45 (37)	5 (3)	26 (10)	30 (11)	4 (4)	0	0
Forum3	585 (174)	134 (36)	65 (11)	78 (15)	159 (39)	18 (3)	43 (6)
Forum4	456 (429)	92 (85)	47 (43)	27 (26)	24 (19)	2 (2)	0
Forum5	1,721 (965)	176 (148)	23 (20)	25 (21)	17 (16)	7 (6)	0
Forum6	218 (70)	177 (52)	6 (1)	71 (6)	3 (0)	2 (0)	0
Forum7	55 (34)	170 (3)	16 (13)	13 (9)	80 (59)	5 (3)	0
Forum8	645 (625)	42 (34)	440 (365)	353 (292)	124 (87)	5 (4)	0
Forum9	511 (436)	159 (142)	25 (22)	12 (10)	15 (13)	7 (0)	0
Forum10	312 (110)	50 (17)	11 (6)	16 (15)	40 (22)	132 (97)	0
Forum11	768 (605)	187 (132)	18 (14)	9 (7)	12 (11)	0	0
Forum12	385 (294)	55 (38)	23 (17)	35 (31)	45 (42)	1 (0)	0
Total	**5,705 (3783)**	**1,247 (690)**	**702 (524)**	**669 (443)**	**530 (319)**	**179 (115)**	**43 (6)**
Original post–to–all posts ratio (percentage)	**66.3**	**55.3**	**26.3**	**66.2**	**60.2**	**64.2**	**13.9**

**Numbers in parentheses represent the number of times the original poster mentioned the payment method.*

reported here does not reflect the position or the policy of the funding agencies.

References

1. T.J. Holt and E. Lampke, "Exploring Stolen Data Markets Online: Products and Market Forces," *Criminal Justice Studies*, vol. 23, no. 1, 2010, pp. 33–50.
2. Z. Zhao et al., "SocialImpact: Systematic Analysis of Underground Social Dynamics," *Proc. European Symp. Research in Computer Security* (ESORICS 12), 2012, pp. 877–894.
3. J. Franklin et al., "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants," *Proc. ACM Conf. Computer and Communications Security* (CCS 07), 2007, pp. 375–388.
4. T.J. Holt, "Examining the Forces Shaping Cybercrime Markets Online," *Social Science Computer Rev.*, vol. 31, no. 2, 2013, pp. 165–177.
5. M. Motoyama et al., "An Analysis of Underground Forums," *Proc. ACM SIGCOMM Conf. Internet Measurement Conference* (IMC 11), 2011, pp. 71–80.
6. V. Kostakis, and C. Giotitsas, "The (A)political Economy of Bitcoin," *tripleC: Communication, Capitalism & Critique*, vol. 12, no. 2, 2014, pp. 431–440.
7. S. Barber et al., "Bitter to Better—How to Make Bitcoin a Better Currency," *Proc. Financial Cryptography and Data Security*, 2012, pp. 399–414.
8. F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," arXiv:1107.4524, 2013.
9. B. Stone-Gross et al., "The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns," *Proc. USENIX Workshop on Large-Scale Exploits and Emergent Threats* (LEET 11), 2011, pp. 4–11.

Ziming Zhao is an assistant research professor in the School of Computing, Informatics, and Decision Systems Engineering, Ira A. Fulton Schools of Engineering, Arizona State University. His research interests include system and network security and cybercrime analysis. Zhao received a PhD in computer science from Arizona State University (ASU). Contact him at zmzhao@asu.edu.

Mukund Sankaran is a junior Java developer at ShareStream and was a student at ASU at the time of this writing. His research interests include social network analysis, text mining, and natural language processing. Sankaran received an MS in computer science from ASU. Contact him at msankar2@asu.edu.

Gail-Joon Ahn is a professor in the School of Computing, Informatics, and Decision Systems Engineering, Ira A. Fulton Schools of Engineering and the

Director of the Center for Cybersecurity and Digital Forensics at ASU. His research has been supported by the US National Science Foundation, US National Security Agency, US Department of Defense, US Department of Energy, Bank of America, Hewlett Packard, Microsoft, and the Robert Wood Johnson Foundation. Ahn received a PhD in information technology from George Mason University. He received the US Department of Energy CAREER Award and the Educator of the Year Award from the Federal Information Systems Security Educators Association. Contact him at gahn@asu.edu.

Thomas J. Holt is an associate professor in the School of Criminal Justice at Michigan State University. His research focuses on computer hacking, malware, and the role of the Internet in facilitating all manner of crime and deviance. His work has been published in various journals including Crime and Delinquency, Deviant Behavior, the Journal of Criminal Justice, and Youth and Society. Contact him at holtt@msu.edu.

Yiming Jing is a senior software engineer at Samsung Research America. His research interests include access control models and mechanisms, security and privacy in mobile computing, and secure software engineering. Jing received a PhD from ASU and a BS from Shanghai Jiao Tong University. Contact him at ymjing@asu.edu.

Hongxin Hu is an assistant professor in the Division of Computer Science, School of Computing, Clemson University. His research interests include access control models and mechanisms, security and privacy in social networks, security in cloud and mobile computing, network and system security, and secure software engineering. He received a PhD in computer science from ASU. Contact him at hongxinh@clemson.edu.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.