CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2020-1223

FORUMS, MARKETPLACES, AND SHOPS REMAIN ESSENTIAL VENUES FOR THE CRIMINAL ECONOMY

Recorded Future®

This report will detail the key differences and similarities among the three primary dark web resources where criminal goods and services are bought, sold and traded: forums, shops, and marketplaces. This analysis is intended for those interested in understanding the social dynamic of the cybercriminal underground.

Executive Summary

Cybercrime often happens on a large scale. Out of circumstances like the mass scanning of the internet for vulnerable systems, breaches of millions of payment cards at a time, and the international drug trade, three primary types of dark web communities have emerged: the forum, the shop, and the marketplace. Each is similar in that they allow cybercriminals to vet the buyers and sellers in their communities, though there are key differences in structure due to the type of product or services that are offered and how the transactions take place.

Key Judgments

- Forums, shops, and marketplaces are all still essential to the underground economy and facilitate different types of criminal activities.
- Forums facilitate communication and collaboration among cybercriminals by providing a wide array of specialized abilities essential to build trusted partnerships for complex operations.
- Shops solve the logistical problem of large-scale fraud operations by automating the sale of payment cards, e-commerce and financial accounts, large collections of compromised PCs, and proxy networks.
- Marketplaces, also referred to as "darknet markets," were born out of a need for less-technical users primarily to buy and sell narcotics, and incorporate elements of both forums and shops.
- Popular encrypted chat services used by threat actors, such as Telegram, will not replace forums, shops, or marketplaces, as these chat services provide no method for participants to vet one another effectively, nor can they handle the sale of large amounts of stolen data.

Background

Criminal forums were born out of a need for collaboration, and, from those same communities, shops were created to handle large amounts of inventory that otherwise would be nearly impossible to do manually. Markets, generally referred to as "darknet markets", came about when non-technical sellers and buyers of narcotics required a platform that provided a built-in cryptocurrency escrow service and a way for buyers to leave positive or negative reviews about their purchases. There occasionally is overlap in both naming and functionality among the three; these general distinctions still usually apply.

Despite the large-scale adoption of Telegram by threat actors for encrypted group chat channels, it will not replace the need for forums, shops, or markets. Telegram channels do not provide ways in which members are vetted or rated for the rest of the community to see. It would be virtually impossible for a seller to manage the bulk in which payment cards are stolen and sold, especially to a large group of buyers. Lastly, for the sale of narcotics, managing the order specifics, shipping addresses, and payments for each client would be a highly manual process, as opposed to the automated nature of marketplaces. Telegram will be suitable for smaller groups of threat actors who have already established a rapport on a forum, or for a vendor to answer questions about their goods or service to a potential buyer.

Threat Analysis

Forums

Aside from buying, trading, and selling goods and services, the mainstays of a typical dark web forum are discussion, collaboration, and validation. Running a ransomware affiliate program, spreading a JavaScript sniffer on e-commerce websites, or cashing out credit or debit card dumps virtually always requires recruitment and cooperation of a team of individuals to be successful. Ransomware requires coders to build and maintain a payload, spammers and hackers to infect those larger corporate networks, hosting for C2 infrastructure and extortion websites, "customer support" to handle the ransom negotiation, and money laundering and cashout services for the cryptocurrency they receive from the victim. Those operating JavaScript sniffers need to scan for vulnerable e-commerce websites, and use drop and reshipping services to purchase high-demand items with the stolen payment data they collect. Monetizing credit and debit card dumps stolen from POS systems or ATM skimmers requires mules to encode the stolen track data onto fresh cards and make in-store purchases or withdraw at ATM machines.

Figure 1: Banner ads on a popular forum advertising a variety of popular carding shops such as Joker's Stash, BriansClub, and Trump's Dumps.

Forums help their members find the support they need, but their structure also allows members to decide who they can trust and those who are less reliable. For this trust system to work, forum admins and moderators test and vet the goods and services offered by members, provide a rating system for buyers to post feedback, and have an arbitration section where complaints are heard and resolved by the forum's staff. A forum member's moniker is essentially their brand name. Bad reviews from unsatisfied buyers or complaints posted on the arbitration finding them at fault can ruin a moniker's reputation and their business. This often results in the user being banned and labeled a "ripper" (a forum member who has ripped someone off), which is often propagated across other dark web forums. If that same individual (banned or branded ripper) wishes to resume business, they must start over with a new moniker and a rebranded service, and hope no one discovers their past.

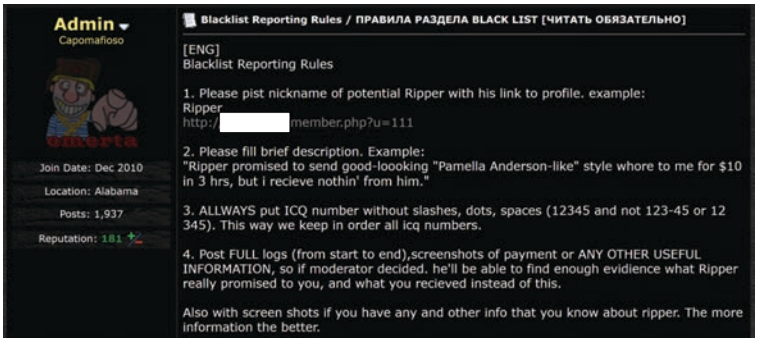


Figure 2: Instructions for how to use the blacklist feature to handle disputes between buyers and sellers.

Like their members, forums themselves live or die based on their reputation. The more reputable "closed" communities employ safeguards to unreliable individuals from joining and those who have no interest in participating in some form of cybercrime. At minimum, they have a paywall that can range from $50 to $1,000. These high-tier forums require potential members to both pay and to contact the admin for an explanation for what kind of services they offer, or to provide their activities on other forums for validation. Charging a registration fee is also one of the primary ways forum admins to make revenue for themselves.

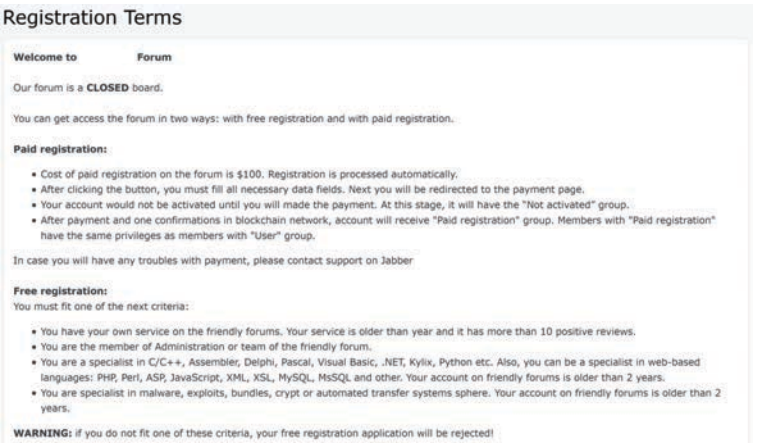


Figure 3: The Exploit application form.

Advertising is another way forum admins generate revenue for themselves. Referred to as "adverts," forum advertisements are often animated or static banners. For forums that have corresponding Jabber servers, adverts can also be pushed out in mass to all the users. Vendors who buy adverts are seen as more reliable and less likely to scam buyers, as they've invested in their forum presence. The more popular vendors (Joker's Stash and Genesis Store, for example) will have adverts across many of the major forums. This type of marketing is essential especially for vendors of dumps and CVVs, where the market is saturated.

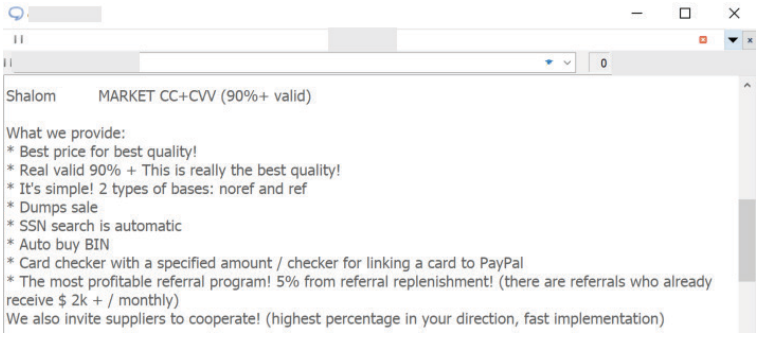


Figure 4: Jabber advert for a carding shop.

Escrow services are an essential part of any forum, adding an additional layer of security to transactions and allowing members to conduct business with unvetted buyers or sellers. Escrow services can be privately offered by trusted members for a percentage, or as an official service of the forum, many of which are free. They function like legitimate escrow services, where a third party (a trusted member or a forum moderator) receives payment from the buyer, and only releases it to the seller after the buyer confirms receipt of the product.

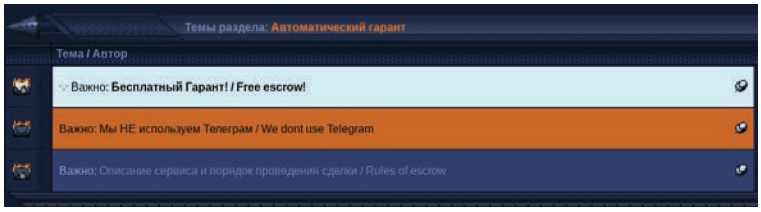
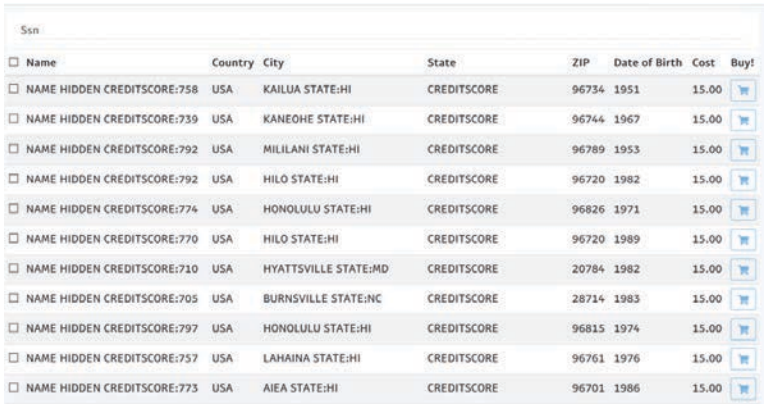


Figure 5: Free escrow service advertised on a prominent Russian carding forum.

Shops

Attackers often manage to steal millions of credit and debit card information at a time. Bot-herders who have infected victims with stealer malware will have thousands of logs (browser data such as account credentials and cookies) to sell. Those who scan the internet en masse for exposed and vulnerable Secure Shell (SSH) or remote desktop protocol (RDP) connections will have remote access to hundreds or thousands of computers at a time. In the dark web, the "shop" solves the logistical problem of handling and selling such large amounts of stolen data to a very large buyer base. They are entirely automated, offering a point-and-click environment like any legitimate e-commerce website. If it weren't for shops, these criminal merchants would have to interact with each buyer individually on the forums or over chat, which would be prohibitively time-consuming.

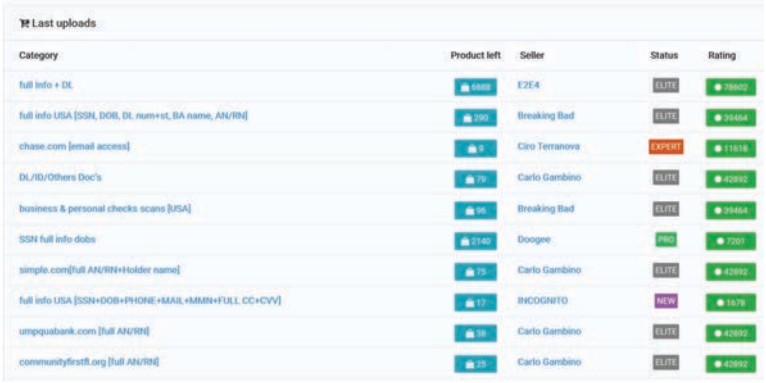


Ssn

Name	Country	City	State	ZIP	Date of Birth	Cost	Buy!
NAME HIDDEN CREDITSCORE:758	USA	KAILUA STATE:HI	CREDITSCORE	96734	1951	15.00	
NAME HIDDEN CREDITSCORE:739	USA	KANEOHE STATE:HI	CREDITSCORE	96744	1967	15.00	
NAME HIDDEN CREDITSCORE:792	USA	MILILANI STATE:HI	CREDITSCORE	96789	1953	15.00	
NAME HIDDEN CREDITSCORE:792	USA	HILO STATE:HI	CREDITSCORE	96720	1982	15.00	
NAME HIDDEN CREDITSCORE:774	USA	HONOLULU STATE:HI	CREDITSCORE	96826	1971	15.00	
NAME HIDDEN CREDITSCORE:770	USA	HILO STATE:HI	CREDITSCORE	96720	1989	15.00	
NAME HIDDEN CREDITSCORE:710	USA	HYATTSVILLE STATE:MD	CREDITSCORE	20784	1982	15.00	
NAME HIDDEN CREDITSCORE:705	USA	BURNSVILLE STATE:NC	CREDITSCORE	28714	1983	15.00	
NAME HIDDEN CREDITSCORE:797	USA	HONOLULU STATE:HI	CREDITSCORE	96815	1974	15.00	
NAME HIDDEN CREDITSCORE:757	USA	LAHAINA STATE:HI	CREDITSCORE	96761	1976	15.00	
NAME HIDDEN CREDITSCORE:773	USA	AIEA STATE:HI	CREDITSCORE	96701	1986	15.00	

Figure 6: Credit reports sold in a shop.

Much like any legitimate e-commerce website, the ability to quickly select items, submit payments, and handle customer complaints is a must for any successful operation. For many of these shops, the only seller is the owner/operator of the shop and their dedicated team. There are, however, exceptions where a shop will not only offer multiple items (such as dumps, PayPal accounts, and RDP connections), but also have multiple sellers selling different items. Any major dark web shop will have adverts and threads across multiple forums. Their success relies heavily on the popularity of a given forum and the reputation of the shop's "representative," and their ability to handle questions and complaints from the forum's user base.



Last uploads

Category	Product left	Seller	Status	Rating
full info + DL	6888	E2E4	ELITE	78602
full info USA [SSN, DOB, DL num+st, BA name, AN/RN]	299	Breaking Bad	ELITE	39464
chase.com [email access]	9	Ciro Terranova	EXPERT	11618
DL/ID/Others Doc's	79	Carlo Gambino	ELITE	42892
business & personal checks scans [USA]	96	Breaking Bad	ELITE	39464
SSN full info dobs	2140	Doogee	PRO	7201
simple.com[full AN/RN+Holder name]	75	Carlo Gambino	ELITE	42892
full info USA [SSN+DOB+PHONE+MAIL+MMN+FULL CC+CVV]	17	INCOGNITO	NEW	1679
umpquabank.com [full AN/RN]	38	Carlo Gambino	ELITE	42892
communityfirstfl.org [full AN/RN]	25	Carlo Gambino	ELITE	42892

Figure 7: A shop with multiple vendors selling items such as bank accounts, scans of IDs, and "full info" (PII).

Due to their large, global inventories, shops provide the ability for buyers to search for victims. This is a must, as threat actor groups are almost always focused on specific regions and would have no use for victims outside of them. Shops are usually specialized in certain items, and can be categorized as either a carding shop, account shop, logs shop, bot shop, or those that sell combinations of these items. For each, buyers can selectively choose items from victims in different states, cities, and countries through dropdown menus. Some carding shops allow buyers to automatically purchase fresh items the moment they're released. Below is a breakdown of the different types of shops, and what they typically sell:

- Carding shops sell dumps and CVVs, and frequently include a checker service to verify if a given card is working. Some carding shops also include searchable databases of Social Security numbers, dates of birth, physical addresses, and phone number histories.
- Account shops sell username and password combinations for a wide variety of e-commerce websites and financial services that are popular targets for carders, such as Amazon, PayPal, and Wells Fargo.
- Logs shops sell data stolen from a victim's browser such as account credentials, session cookies, and IP address, which are ideal for account takeover and circumventing anti-fraud mitigation.
- RDP, SSH, and proxy shops sell remote access to victim machines and proxy networks, providing attackers with legitimate-looking IP addresses to commit fraud and circumvent anti-fraud mitigation.

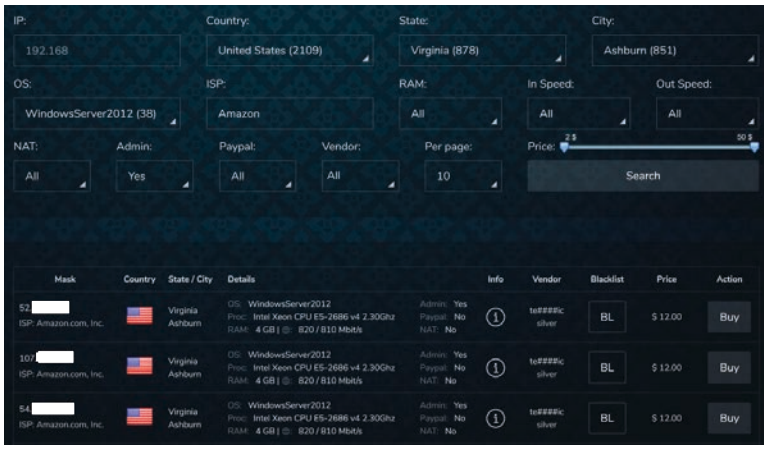


Figure 8: A screenshot of an RDP shop filtered by a specific operating system, city, state, and ISP.

Marketplaces

Marketplaces, often referred to specifically as the "darknet markets," developed out of a need to buy and sell narcotics — very different from the forums and shops that facilitate hacking and fraud. Hosted nearly entirely as Tor onion services (.onion websites), they offer anonymity and security for less-technical users involved in the illegal drug trade. Silk Road (2011), Dream Market (2013), and AlphaBay (2014) were some of the more prominent marketplaces worldwide, selling millions of dollars of narcotics. As these marketplace grew in popularity, other dark web vendors began to list other non-narcotic products and services, including compromised accounts and data, how-to guides, fraud tutorials, malware variants, and mule recruitments.

Marketplaces are neither very social communities like the forums, nor do they have the ability to handle a massive inventory like shops can. Despite this, marketplaces do incorporate limited features of both forums and shops, and can be seen as a hybrid of the two. Like forums, most prominent marketplaces require sellers to verify what they're selling before becoming active. Buyers can leave positive or negative feedback for sellers with a rating system and brief reviews,

and disputes are reported to and solved by official moderators. Buyers and sellers can communicate directly through private messaging that allows easy integration of PGP keys to encrypt these conversations.

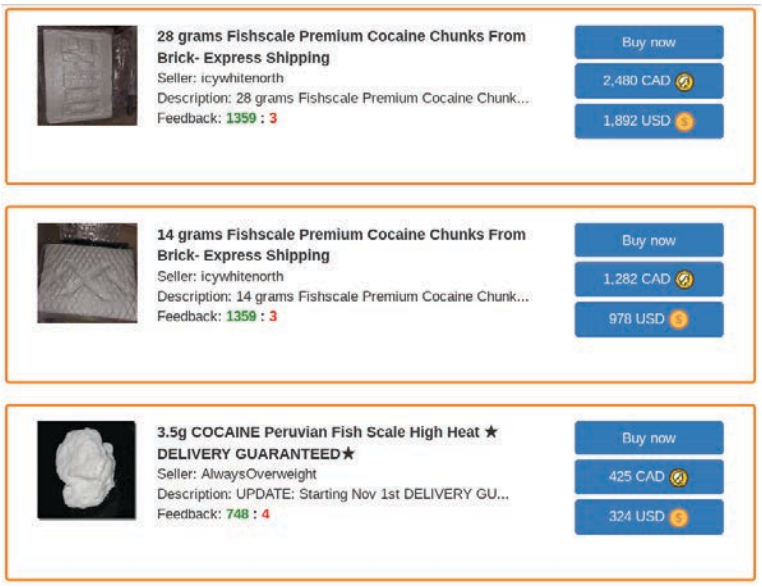


Figure 9: Cocaine vendors on a darknet marketplace. Note the positive (green) and negative (red) feedback ratings for each.

Similar to shops, marketplaces have a point-and-click interface where buying is entirely automated. Payment methods are also similar to shops, as some marketplaces allow users to deposit cryptocurrency directly into their account for making purchases. Virtually all marketplaces mandate that buyers and sellers use their automated escrow service, which are cryptocurrency addresses controlled by the marketplace staff. This system only releases payment to the seller after the buyer is satisfied. However, this centralized management of cryptocurrency is one of the main reasons exit scams are so prevalent on darknet marketplaces, in which the operators shut down their marketplace unannounced and abscond with all of the cryptocurrency stored in user accounts and escrow.

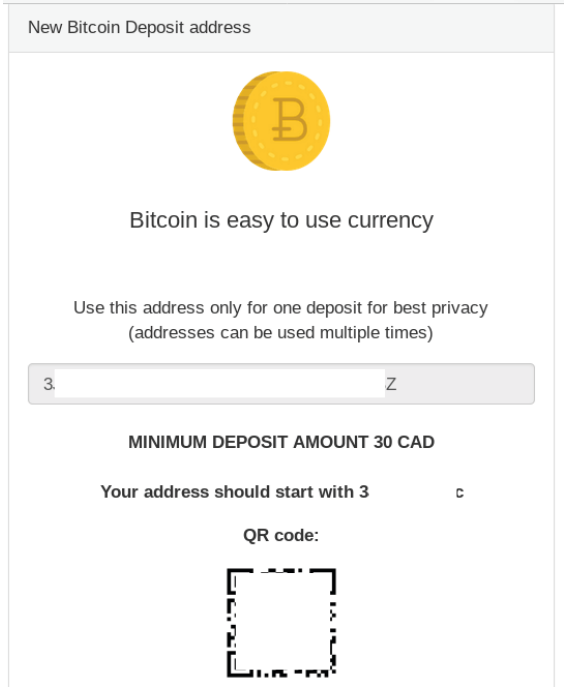


Figure 10: A Bitcoin deposit address for users on a darknet marketplace.

Outlook

Over the past 20 years, forums, shops, and marketplaces have been created and improved upon to solve problems around vetting individuals and handling different types of illicit inventory varying from narcotics to ransomware. These three types of communities will remain a mainstay of the underground economy, as the need for reaching buyers, sellers, and collaborators globally, and knowing whom to trust, will always be the most important elements for any successful threat actor.

Monitoring forums, shops, and marketplaces is essential for protecting an organization for identifying both direct and indirect attacks. A large increase in credit and debit inventory in a carding shop is a likely indicator of a major breach of an e-commerce website or the POS system of a popular brick-and-mortar establishment. Furthermore, on many occasions, forum members state publicly the name of the victim organization whose network they are selling access to. An organization's defenders cannot afford to overlook threat intelligence of that nature or caliber.

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.