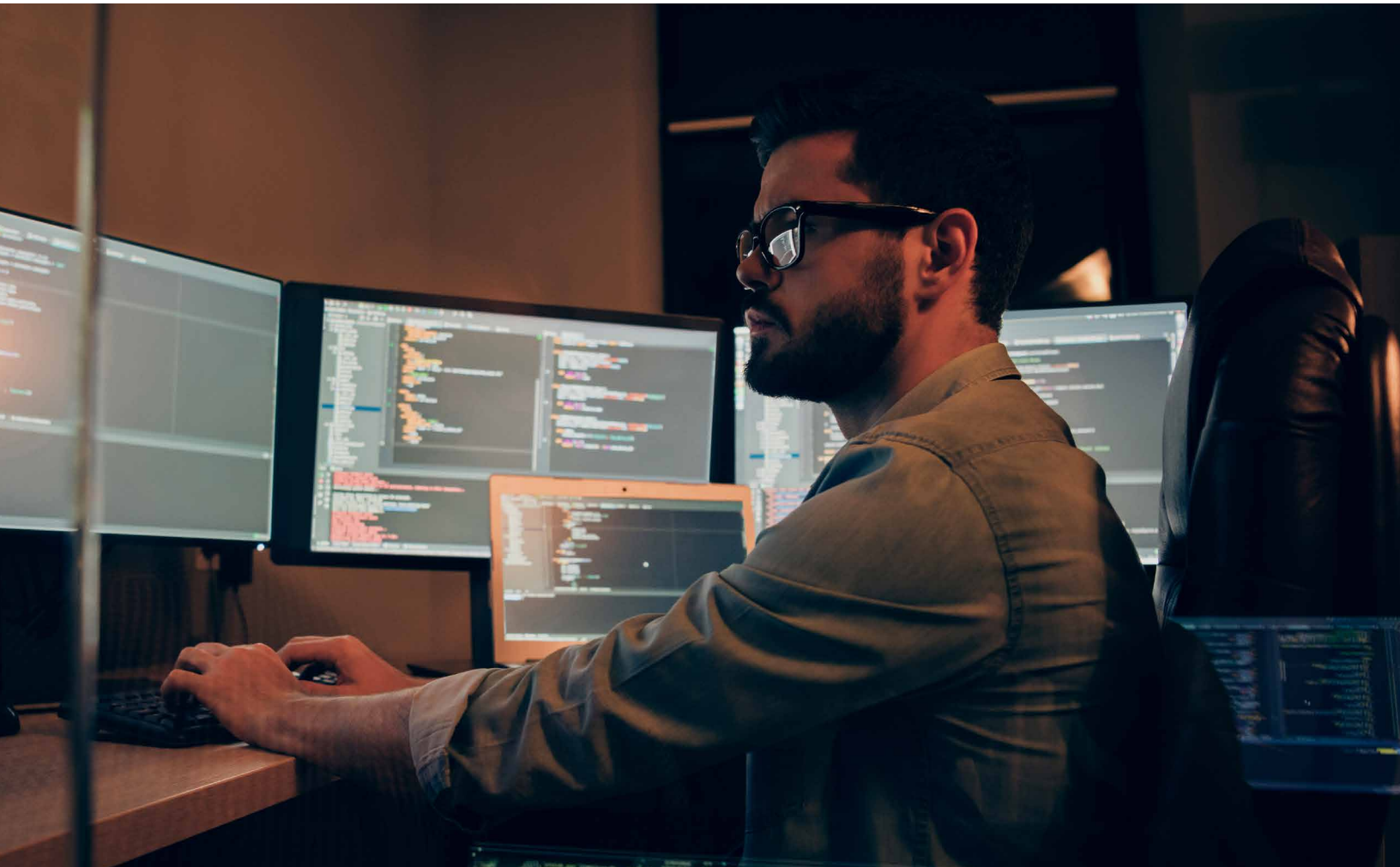


2020

ARMOR



DARK MARKET REPORT:

THE NEW ECONOMY

CONTENT

INTRODUCTION	3
PRICES FOR HACKER GOODS AND SERVICES	5
CYBERCRIME SERVICES	8
▪ Ecommerce Services	8
▪ Dark Web Advertising	9
▪ Money Laundering, DDOS, SMS Bombing	10
▪ Bulletproof Hosting	14
▪ Commercial Software	15
▪ Customer Service	15
UNDERGROUND MARKETPLACE PRODUCTS	17
▪ Business Fullz	17
▪ Financial Loans	18
▪ Crypters, Remote Access Trojans (RATs), and Exploit Kits	18
▪ Botnets	20
▪ Remote Desktop Protocol Credentials	21
▪ Credit Card Credentials and Cloned ATM/Debit Cards	22
▪ Social Media Accounts	25
▪ Hacker University	27
▪ Ransomware	29
▪ TV and Movie Streaming Accounts and Pizza Points	30
▪ COVID-19 Treatments, Tests, and Personal Protective Equipment	32
▪ Drugs	34
▪ Cryptocurrency	35
CONCLUSION	36
▪ Cyber Protections for IT and Security Teams	36
▪ Cyber Protections for Individuals	36

ARMOR 2020 DARK MARKET REPORT: THE NEW ECONOMY

In times of war, natural disaster, or political turmoil, underground economies thrive. In 2020, COVID-19 took the world by storm causing a pandemic, the likes of which have not been seen since the Spanish Flu of 1918 and the Hong Kong Flu of 1968. Although the coronavirus has wreaked havoc on economies around the world, it seems to have created new opportunities for underground cyber markets. This comes at a time when the tools and communication vehicles for cybercriminals are becoming more innovative, inexpensive, and readily available.

Today, the underground economy, comprised of stolen credentials, malicious software, bullet-proof hosting, tools for financial fraud, and more, continues to grow across hundreds of dark web markets, some claiming to have as many as 1 million monthly visitors. These markets are key drivers in the adoption of cryptocurrency and encrypted messaging—technologies with enormous potential that also challenge our notions of money and privacy.

THIS YEAR'S DARK MARKET REPORT

For the third year in a row, Armor's security research team, the Threat Resistance Unit (TRU), took a deep dive into underground hacker markets and forums, studying the illicit goods and services that cybercriminals are buying and selling. The TRU team investigated 15 markets and a variety of underground hacker forums, news sites, and open repositories between October 2019 and June 2020, to understand the state of what continues to be a growing and innovative ecosystem.

Also, for the first time, the TRU team researched pharmaceuticals and other healthcare products being advertised on the underground markets, primarily those related to COVID-19. This health crisis has not only affected legitimate marketplaces, but it has unfortunately created opportunities for cybercriminals to prey on thousands of individuals with an array of scams.

WHY DARK WEB THREAT INTELLIGENCE?

Why is threat intelligence important, and how does it benefit organizations to know what is currently happening on the dark web? In general, threat intelligence provides more information so you can make better security decisions. By knowing more about the tools and techniques of an adversary, organizations can better protect themselves. Finally, threat intelligence provides context for your complete security posture.

Threat intelligence about dark web marketplaces and forums is also important because of what one might discover at any time. On dark markets, threat researchers may see the sale or trade of malicious software, zero-day exploits, large data dumps, or the sale of intellectual property. Researchers may also identify cryptocurrency market signals, discover new forms of digital cash, or learn of a breach of a crypto exchange with millions of dollars at stake. It is here in the dark web, in marketplaces, and private forums where threat researchers find some of the latest malware and cybercrime services.

WHAT'S NEW ON THE DARK WEB?

- A Cybercrime Service Where Online Criminals Offer to “Destroy a Competitor’s Business”
- Turn-Key, Ecommerce Service for Setting up Illicit, Digital Storefronts on Underground Markets
- Full Identity Packets on Businesses for Sale (a.k.a. Business Fullz)
- A Hacker University Opens Its Doors
- Stolen Financial Loan Applications for Sale—Chock Full of Personal Identifiable Information (PII)
- Dark Web Advertising, News, and Hacker Reviews

Throughout the digital storefronts of these dark markets, Armor’s security researchers found that many of the illicit products and services outlined in Armor’s 2018 and 2019 reports continue to be staples in these criminal markets. They include stolen bank account and credit card data, Remote Desktop Protocol (RDP) credentials, full identity packets, cloned credit and ATM/debit cards, and an array of malware. Popular cybercrime services continue to be advertised, such as offers to take down a competitor’s website using a distributed denial of service (DDoS) attack, stealing an individual’s corporate email credentials, providing ransomware-as-a-service (RaaS), or transferring thousands of dollars of cash into a bank account or PayPal account of one’s choice.

There are several products and services that the TRU team spotted this year that are quite notable. The first was an offer to have a hacker “destroy a competitor’s business.” And, as if there are not already enough cybercriminals participating in illegal activities, there is a turn-key ecommerce service that provides fraudsters with everything they need to set up their own shop in an underground market.

Also, for the newbies just breaking into the cybercrime business, the TRU team discovered a growing ecosystem of advertisers, news sources, and shady services catering to underground buyers. One of the most worrisome items the TRU team saw this year was an array of business fullz for sale, as well as fullz culled from financial loan applications. Business fullz contain everything a criminal needs to appear as if they are a corporate officer of an actual business, whereas personal fullz from loan applications contain all kinds of personal identifiable information (PII) on an individual, enough to commit identity theft. There are also SMS bombing services and commercial software for rent. And if newbies are looking for a “formal” cybercrime education, they can now attend Hacker University. For \$125, to be paid in Bitcoin or Monero, the criminal group behind this online university claims that they will teach attendees everything from operational security and Wi-Fi hacking to network attacks and carding.

PRICE LIST FOR HACKER GOODS AND SERVICES

CREDIT CARD WITH CVV NUMBERS									
VISA/MASTERCARD					AMEX/DISCOVER				
US	UK	CANADA	AUSTRALIA	EU	US	UK	CANADA	AUSTRALIA	EU
\$5-12	\$15-20	\$10-20	\$5-25	\$18-35	\$5-12	\$10-25	\$15-25	\$8-30	\$18-35

PAYPAL ACCOUNTS							
AVG. PRICE	\$50	\$60	\$80	\$100	\$200	\$250-300	\$500-550
BALANCE	\$500	\$600	\$800	\$1,000-2,000	\$1,500-4,500	\$2,500-8,500	\$5,000-13,000

CLONED ATM CARDS FOR BANK ACCOUNTS										
AVG. PRICE	\$300-450	\$600-800	\$850-1,000	€150	€300	€450	€550	£154	£270	£385
BALANCE	\$5,000	\$10,000	\$15,000	€2,000	€5,000	€8,000	€10,000	£2,000	£3,000	£5,000

FULLZ DATA			
ORIGIN	AVG. PRICE	ORIGIN	AVG. PRICE
US	\$30-40	SWEDEN	\$20-25
UK	\$35-50	FRANCE	\$20-25
CANADA	\$30-45	GERMANY	\$20-25
AUSTRALIA	\$17-50	IRELAND	\$20-25
ITALY	\$20-25	MEXICO	\$15-20
SPAIN	\$20-25	ASIA	\$15-20
DENMARK	\$25-30	Other EU	\$17-60
Includes: Full Name, Date of Birth, Address, City, Zip Code, State, Country, Phone Number, Mother's Maiden Name, Social Security Number, Driver's License Number			

BUSINESS FULLZ DATA	
Includes: Bank Acct Numbers, Employee Identification Number (EIN), Certificate of Business, Corporate Officers' Names, Birth Dates, SSN.)	\$35-60

\$ = U.S. dollars; € = Euro; £ = British pound

RANSOMWARE	
Various Generic Ransomware	\$1.99-6.50

UNHACKED REMOTE DESKTOP PROTOCOL SERVERS	
Unhacked RDP Servers Worldwide	\$9.99-25 per server

DEGREE FROM HACKER UNIVERSITY	
Hacker University Degree	\$125

VARIOUS MALWARE	
TYPE	AVG. PRICE
Various Virus Packs	\$2.68-4.99
Remote Access Trojan (RAT)	\$.99-12
Cryptex Crypter	\$.99
TinyNuke Bank Botnet Source Code	\$75
Mirai Botnet Source Code	\$6
Drupal Exploit (SMS stealer)	\$80
	\$4.99-9.99

ATM SKIMMERS	
TYPE	AVG. PRICE
Wincor with keypad	\$700
Wincor Nixdorf	\$1,200
Wincor	\$1,200
Slimm	\$1,200
NCR	\$1,200
Diebold Opteva	\$1,000
Diebold	\$800
Universal	\$1,500
Small	\$1,200
Chip POS	\$700

CARD READERS/WRITERS	
Various Models	\$149-990

PHONES	
iPhone 11 Max Pro	\$179
iPhone 11 Xs Max	\$159

SETUP OF VENDOR SHOP ON AN UNDERGROUND MARKET	
Turn-key ecommerce service	€5,000 (\$5,828)- €10,000 (\$12,791)

DESTROY A TARGET'S BUSINESS	
DESTROY A TARGET'S BUSINESS (using spam emails and phone calls, shipping unwanted items to the victim's business, and including the victim's business phone number in advertisements.)	\$185

DDOS ATTACK			
DDoS a small website	\$100	DDoS a medium website	\$250

RENT ACCESS TO POPULAR SOFTWARE					
1 Week Access	\$250	1 Month Access	\$500	3 Months Access	\$1,000

SMS SPAMMING SERVICES	
1,000 SMS	\$18.99-19.99

BULLETPROOF WEB HOSTING	
Web hosting for illicit content (fraud, porn, money laundering schemes, etc.)	\$4-19 a month

TELEPHONE DENIAL OF SERVICE (TDOS) ATTACKS		
NUMBER OF CALLS	TIME PERIOD	PRICE
3,000	48-hour period	\$56.70
5,000	60-hour period	\$94.50
7,000	72-hour period	\$132.30
10,000	96-hour period	Contact seller for price

MONEY TRANSFER SERVICES							
WESTERN UNION		BANK TRASFER		PAYPAL		SKRILL (Moneybookers)	
AVG. PRICE	BALANCE	AVG. PRICE	BALANCE	AVG. PRICE	BALANCE	AVG. PRICE	BALANCE
\$150-240	\$1,800-2,400	\$150-250	\$1,800-2,500	\$120-200	\$1,200-1,500	\$150	\$1,800
\$300-400	\$3,500-4,500	\$250-350	\$3,000-3,500	\$180-250	\$1,800-2,500	\$250	\$3,000
\$500-550	\$6,000-7,000	\$350-450	\$4,500	\$300-350	\$4,000-4,500	\$350	\$4,500
		\$500	\$5,000-7,000	\$500-550	\$5,000-7,000	\$500	\$7,000
		\$700-800	\$9,000-10,000	\$700	\$9,000-10,000	\$700	\$8,000-9,000
		\$1,000-1,300	\$15,000	\$800-900	\$10,000-12,000	\$800	\$10,000
				\$1,000	\$15,000	\$900	\$12,000
						\$1,000	\$15,000

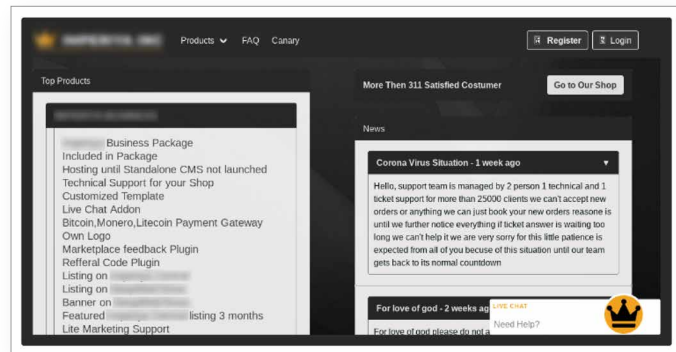
SOCIAL MEDIA							
TWITTER		FACEBOOK		ITUNES		TIKTOK	
SERVICES	PRICE	SERVICES	PRICE	SERVICES	PRICE	SERVICES	PRICE
Likes (5,000)	\$16	Followers (1,000)	€9	Podcasts (1,000)	\$10	Views (2,000)	€2
						Views (100,000)	€13

CHANGES TO CREDIT HISTORY	
Permanently delete negative items from one's credit report	\$135-150

CYBERCRIME SERVICES

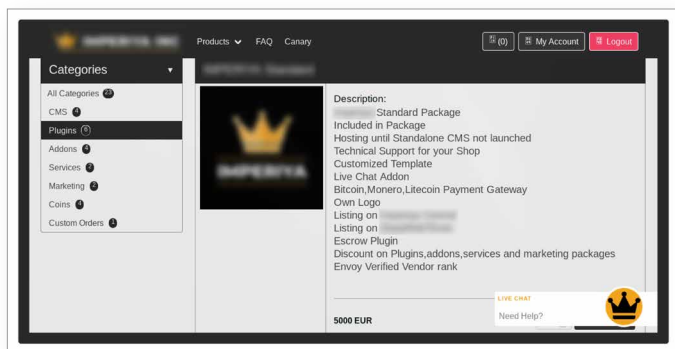
A TURN-KEY, ECOMMERCE SERVICE FOR DARK WEB VENDORS

One of the most interesting services the TRU team spotted on the cyber underground is a complete turn-key, ecommerce service that provides dark web sellers with almost everything they need to establish their own digital shop on an underground marketplace from which to sell their illegal wares and services. The vendor offers four levels of their digital marketplace services. They have the “standard,” “business,” “plus,” and an “ultimate” package. The standard package includes website hosting services, technical support, an escrow plug-in, and payment gateways for Bitcoin, Litecoin, and Monero. This turn-key service will cost a cybercriminal €5,000 (euro).

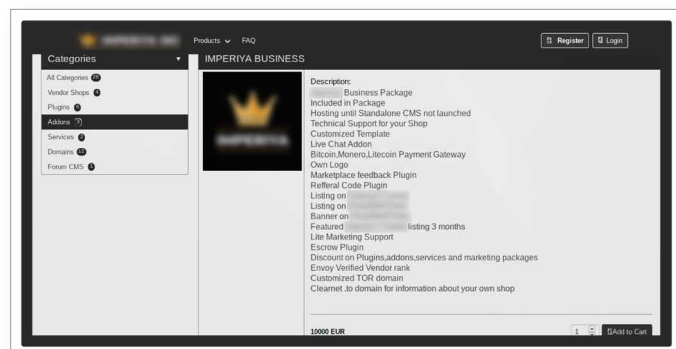


A dark web, turn-key, ecommerce services vendor provides cybercriminals with the key elements needed to set up a dark market shop online.

The service provider also offers a “business” package for €10,000. It includes all the bells and whistles of the €5,000 package, plus “light” marketing support, including a banner ad and a featured listing on three top dark web news sites for three months, and they also get a “verified vendor” rank from a popular forum that gives dark market vendors a stamp of approval. In addition, vendors can purchase plug-ins for features such as a lottery or a prize wheel. The “plus” package provides everything included in the “business” package, plus “medium” marketing support. And the “ultimate” package provides services “at the highest priority.” The all-in-one service is similar to those offered by legitimate ecommerce agencies. This ecommerce service boasts over 240 customers.



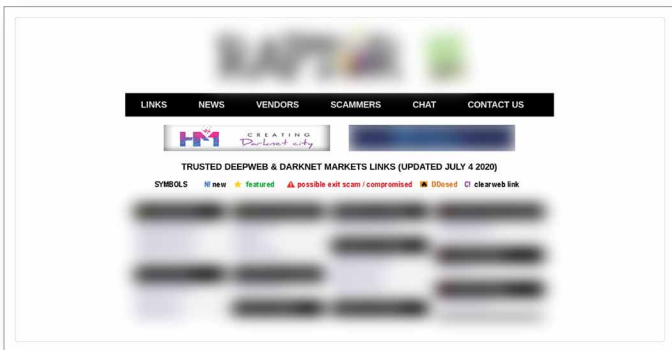
The vendor package for €5,000 includes web hosting, payment gateways, technical support, and an escrow plug-in.



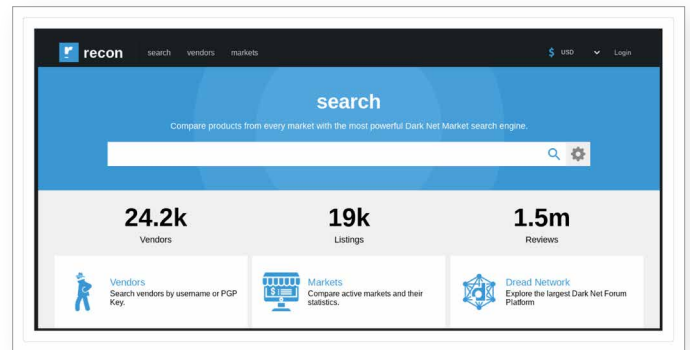
The business package for €10,000 includes standard features plus marketing support and promotions.

DARK WEB ADVERTISING, NEWS, AND HACKER REVIEWS

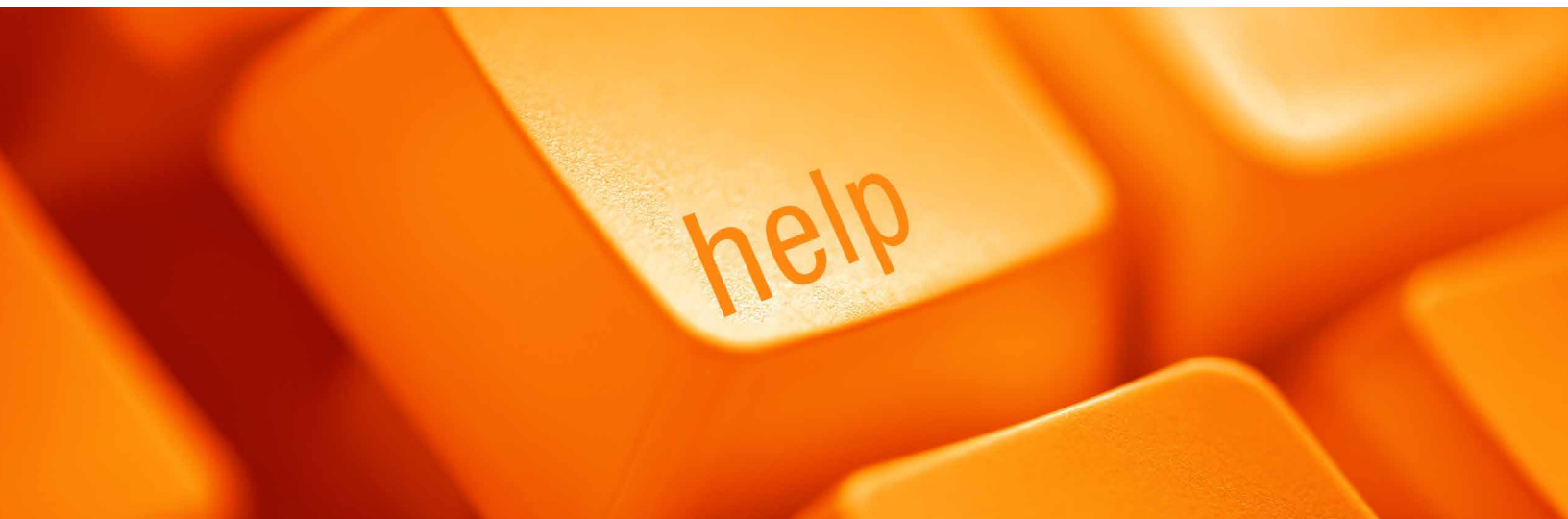
As dark web markets grow and evolve, so do ancillary services and support businesses. The TRU team discovered an array of advertising sites, news sources, and shady services catering to underground buyers on onion sites. These are anonymous websites on the dark web that can only be accessed via the Onion router (Tor) browsers. The TRU team found these sites offering sellers banner ads on the most popular forums, live links to rotating dark web pages, and curated reviews of “highly-rated and trustworthy” dark market vendors, as well as lists of scammers to avoid. The onion sites also provide the latest news on emerging marketplaces, law enforcement efforts, and which dark market vendors and buyers have been arrested or prosecuted.



Underground sites offer the latest rotating mirror links, advertising opportunities, vendor reviews, and news.



The dark web search engine offers listings and details of dark markets, vendors, and forums.



CYBERCRIME-AS-A-SERVICE: DESTROY A BUSINESS, MONEY LAUNDERING, DDOS, SMS BOMBING

As the TRU team saw last year, there continues to be lots of advertisements from hackers offering a list of eyebrow-raising, illegal services such as offers to destroy a business, launder money, and conduct DDoS attacks and SMS bombing attacks. There are also other consumer services being offered: hack a spouse's email account, delete criminal records, improve one's credit score, delete unwanted pictures or videos online, and more.

Cybercrime-as-a-service allows those with limited technical skills to participate in very lucrative hacking schemes. With professionally designed websites, easy-to-use tools, and customer service functions such as live chats and video tutorials, cybercriminals have developed models to expand their business. There are underground markets that even allow potential employers to leave money in escrow to recruit other hackers.

DESTROY A BUSINESS

One of the most alarming services the TRU team discovered on the dark web is a vendor offering to "destroy an individual's business" by hitting them with a barrage of spam emails and phone calls, shipping unwanted items to the victim's business, and including their business phone number in advertisements.

Fix Your Credit and boost your credit score to 750 (SALE SALE SALE!!!)
 Get Negative Items Permanently Deleted from your credit report quickly. You don't have to wait for 7 to 10 years for your adverse i...
 Sold by [redacted] - 215 sold since April 27, 2019 Vendor Level 5 Trust level 4 D 640 (4.76)
 Unlimited items available for auto-dispatch

Product Class	Features	Origin Country	Features
Digital	Unlimited	Ships to Payment	World Wide
Quantity Left	Never		World Wide
Ends In			Escrow

default - 1 day - USD + 0.00
 Purchase price: **USD 25.00**
 Qty: 1 [Buy Now] [Buy Now] [Buy Now] [Queue]
 0.002700 BTC / 0.555926 LTC / 0.361533 XMR

A dark net vendor offers to permanently delete negative items from a person's credit report for only \$25.

DESTROY SOMEONES BUSINESS(SPAMMING EMAIL,PHONE,REVIEWS)
 Do you wanna destroy someone's business? I could help you by: ordering pizza to him and his neighbours ordering cond...
 Sold by [redacted] - 0 sold since March 26, 2020 Vendor Level 1 Trust level 1
 NO IMAGE AVAILABLE

Product Class	Features	Origin Country	Features
Digital	Unlimited	Ships to Payment	World Wide
Quantity Left	Never		World Wide
Ends In			Escrow

DM - 1 days - USD + 1.00 / item
 Purchase price: **USD 185.00**
 Qty: 1 [Buy Now] [Buy Now] [Queue]
 0.020064 BTC / 2.887918 XMR

The hacker sells this service for only \$185 and brags that "after 2 days of doing these type of things, his business will be ruined!"



TELEPHONY DENIAL OF SERVICE (TDoS) ATTACKS AND SMS BOMBING SERVICES

The TRU team continues to see dark web vendors offering telephony denial of service (TDoS) attacks. The FBI first warned businesses and consumers about this threat in 2010. TDoS attacks occur when a criminal launches a high volume of automated calls against the phone network of a business or individual, tying up the system from receiving legitimate calls. The target will get inundated with calls, as many as thousands of calls a day, over and over again. In the past, malicious actors have used this type of attack against state or local governments entities, high-ranking officials (e.g., mayors), law enforcement agencies, and Public Safety Answering Points (PSAPs), and then demanded a ransom payment to stop the TDoS attack.

This type attack also has been used by financial cyber-criminals. They plunder a victim's bank account or stock trading account, and the target is prevented from receiving a notification from their financial institution of the unauthorized financial transaction. The TRU team saw one particular scammer offering to make 3,000 automated phone calls to a specific phone number in a 48-hour period; 5,000 calls in a 60-hour period; and 10,000 calls within 96 hours. The vendor states: "I've been on Dark Markets since Agora, Evolution and Blackbank days. Use your imagination for the many possibilities with flooding."

In addition to DDoS and TDoS services, there is also SMS bombing or spamming services. This is when a criminal floods a target's smartphone with text messages. One scammer advertises that for just under \$20, they will send 1,000 text messages to a target's phone over a 7- or 24-hour period.

Order 2 = 3,000 calls (48hrs)
 Order 3 = 5,000 calls (60hrs)
 Order 4 = 7,000 calls (72hrs)
 Order 5 = 10,000 calls (96hrs)

Special pricing for over 10k
 Provide phone # and will start immediately (you can specify start time / duration)

Duration can be set to "Auto" for max full throttle calls, if requested in advance. 1k sms calls in "Auto" setting the duration can burn in 7hrs instead of 22hrs and 10k can burn up in @38hrs on auto. Can update you with current time remaining on job.

- Absolutely NO changes once job is running
- Currently NO custom sms messages
- See other listings for more professional flooding options
- Log file available upon request once job is finished running
- SMS currently available USA & Canada only

I've been on DM since Agora, Evolution and Blackbank days. Use your imagination for the many possibilities with flooding.

*** Telephony Denial of Service (TDoS) is flood of incoming calls from Unknown Caller / see listing image). The objective is to make a significant number of calls and to keep those calls active for as long as possible, to overwhelm or at least "clog" all or a portion of the targets system. TDoS attacks (a.k.a Call Flooding) overwhelm phone lines and systems, attempting to prevent legitimate calls from getting through.

A scammer advertises their TDoS (call-flooding) service.

== MASS SMS SPAMMING SERVICE ==
 This new service is available for our clients, allowing perform flood by way of SMS. Now you can spam via SMS. Now you ...

Sold by [Vendor] - 3 sold since May 22, 2020 [Vendor Level 5] [Trust level 4]

Product Class	Quantity Left	Ends In	Features	Origin Country	Ships to	Payment
Digital	Unlimited	Never		World Wide	World Wide	Escrow

1000 SMS - 1 days - USD + 0.00 / item

Purchase price: **USD 19.99**

Qty: 1 [Buy Now] [Buy Now] [Buy Now] [Queue]

0.002168 BTC / 0.464020 LTC / 0.312051 XMR

SMS BOMBER SMS SPAMMING BLASTER SERVICE SMARTPHONE SABOTAGE NEGATIVE ATTACK
 1,000 SMS FLOODING SERVICE (default @22hrs or @7hrs auto) NEGATIVE STRIKE!!! *** What is sms flood and what is ...

Sold by [Vendor] - 3 sold since February 26, 2020 [Vendor Level 2] [Trust level 1]

Product Class	Quantity Left	Ends In	Features	Origin Country	Ships to	Payment
Digital	Unlimited	Never		World Wide	World Wide	Escrow

default - 1 day - USD + 0.00

Purchase price: **USD 18.90**

Qty: 1 [Buy Now] [Queue]

0.002050 BTC

Dark market vendors advertise SMS bombing services for cheap.

MONEY LAUNDERING IS MORE POPULAR THAN EVER! – COLD, HARD CASH FOR 10 CENTS TO 12 CENTS ON THE DOLLAR!

It was while preparing the 2019 Dark Market Report that the TRU team first noticed a large increase in cybercriminals offering to sell cold, hard cash for a mere 10 cents to 12 cents on the dollar. Now, a year later, money laundering advertised on the underground markets as “Transfers” seems to be more popular than ever. The prices continue to remain approximately the same, 10 cents to 12 cents on the dollar. All a buyer has to do is provide the seller with a bank account or a PayPal account in which to transfer the money. If the buyer prefers, they can also pick up the cash at a Western Union location.

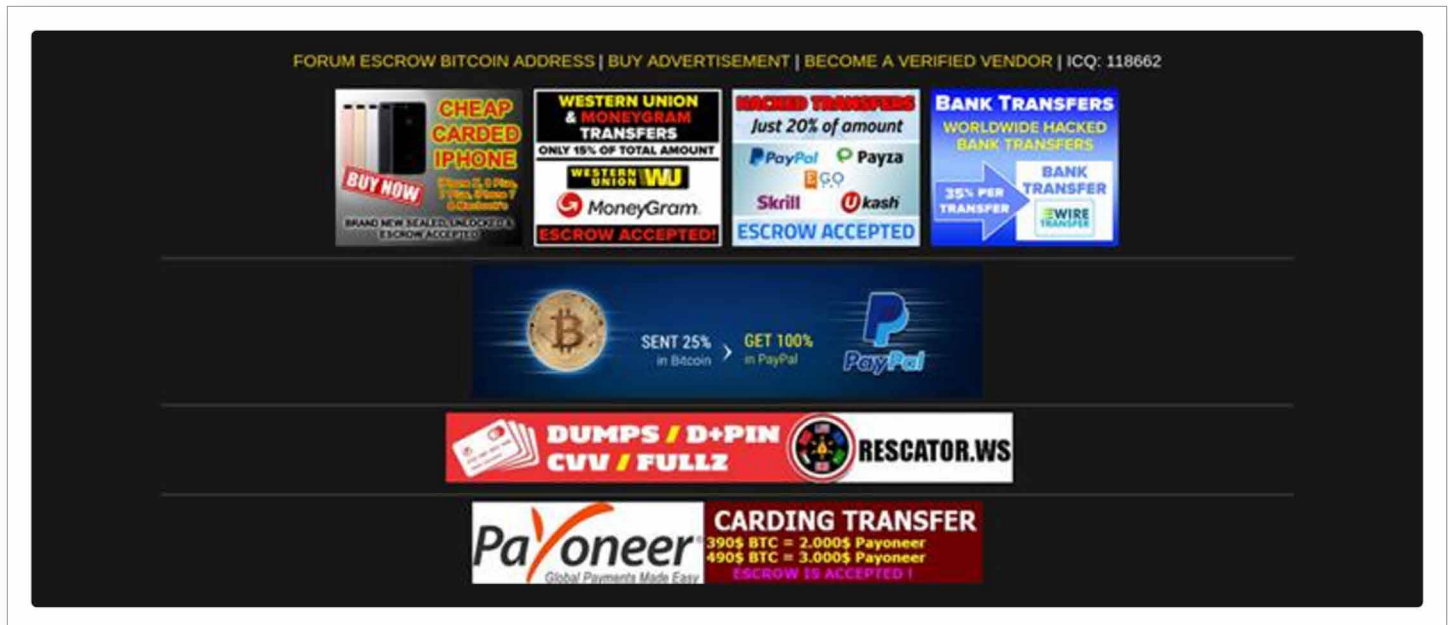
This scheme is convenient for the buyer and the seller. The buyer does not have to have advanced computer skills, and they don’t have to know how to transfer funds from one bank account to another, how to get around the bank’s fraud alerts, or how to disguise the location of the computer they are using.

For the seller, because they do not ultimately receive the stolen funds, the risk to them is greatly reduced. Plus, they do not have to manage a network of money mules. Money mules are persons who have a bank account or multiple bank accounts and who knowingly, or unknowingly, permit cybercriminals to transfer stolen funds into their bank account so it can later be withdrawn. The cybercriminal pays the mule a portion of the siphoned-off funds. A well-established money mule, with a solid reputation and one who has multiple accounts in various top financial institutions, will command approximately 10% of the take. However, the payout can run up to 20% depending on the risk and the amount being stolen. Also, the hacker has to trust that the mule is going to remit the remainder of the stolen monies to them after the mule has taken their cut. It is for this reason that the threat actor will seek out a mule or a mule network operator with a solid reputation. They may pay a higher percentage, but it is critical to work with a mule that has established bank accounts and can be trusted to remit the funds. Experienced hackers will always use mules when stealing money from a bank account. This way, if law enforcement discovers the theft in its early stages, it is the money mule who will get caught holding the bag.

Threat actors also offer similar “transfer” services for high-balance PayPal, Skrill, Moneybookers, and Western Union accounts. The cost for having the money in one of these accounts stolen and transferred to a buyer is similar to that of transferring money out of a bank account, 10 cents to 12 cents per dollar transferred.

The TRU team did spot a cybercriminal on one of the forums questioning whether using stolen credit cards was more profitable and easier than purchasing “PayPal Transfers.”

“Hey guys, I’m new here and I’ve been researching a few different ways to make cash. Can anyone tell me if you have had more success with using stolen card details to buy items or with PayPal transfers? PayPal method only in my opinion is kinda long process and a little or so, expensive to obtain. Cause if you buy dirty transfers then it has to be laundered first pass through different at least 1 to 2 middleman PayPal accounts. Now, owner will file a claim. Disputes and claims will send a notice to those money mule accounts that are involved. It will be very careful so as not to get scammed.”



An underground vendor advertises bank, PayPal, and Western Union transfers, and more.

DDOS SERVICES

DDoS services continue to be popular. One vendor advertises that he will DDoS a small website for \$100 and medium websites for \$250. He even brags that his DDoS tools can bypass the DDoS protection offered by web security companies Cloudflare and BlazingFast.

DDoS services, email spamming, and ransomware-as-a-service continue to be offered by organized cybercriminal organizations on dark net markets.

DDOS ATTACK - SMALL SITES

I will perform a DDOS attack to your target. I will use a botnet to send several GB per second packages to saturate the site....

Sold by • 0 sold since April 24, 2020 Vendor Level 4 Trust level 3

Product Class	Features	Origin Country	Features
Digital	Unlimited	World Wide	World Wide
Quantity Left	Never	Ships to	World Wide
Ends In	Never	Payment	Escrow

1 days - 2 days - USD + 0.00 / item

Purchase price: **USD 100.00**

Qty: Buy Now Buy Now Buy Now Queue

0.010826 BTC / 2.238138 LTC / 1.455816 XMR

DDOS ATTACK - MEDIUM SITES

NEW PRICES!!! I will perform a DDOS attack to your target. I will use a botnet to send several GB per second packages to...

Sold by • 0 sold since March 03, 2020 Vendor Level 4 Trust level 3

Product Class	Features	Origin Country	Features
Digital	Unlimited	World Wide	World Wide
Quantity Left	Never	Ships to	World Wide
Ends In	Never	Payment	Escrow

1 days - 3 days - USD + 0.00 / item

Purchase price: **USD 250.00**

Qty: Buy Now Buy Now Buy Now Queue

0.027066 BTC / 5.595345 LTC / 3.639540 XMR

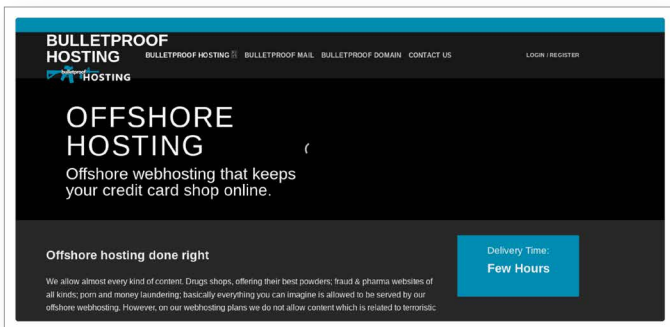
DDoS attacks are offered by size and duration of attack.

DDoS services offer to send "several GB per second packages to saturate the target site."

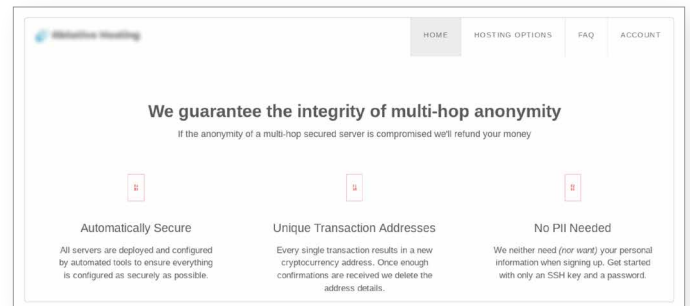
BULLETPROOF WEB HOSTING SERVICES

Just as threat actors need software to conduct business, they also need reliable IT infrastructure in which to host their malware, botnets, and spam and phishing sites, among other things. Where do they go to rent this infrastructure? They typically look for [web hosting companies](#) that don't mind working with criminals—those involved in everything from cybercrime to illegal pornography to online gambling. Naturally, the criminals don't want to be asked questions about what they are hosting on the servers, and they want to feel confident that their IT infrastructure will stay online and will not be taken down by the hosting provider, should the company receive an abuse report.

This morally liberal service is called “[bulletproof hosting](#)” for the way it can largely withstand scrutiny, and it can run between \$4 and \$19 a month. Bulletproof hosting companies can be found in any country. However, many of them are located in China, Russia, and many of the countries that formerly made up the Soviet Union and now make up the Commonwealth of Independent States (CIS), such as Ukraine and Belarus.



A bulletproof hosting company advertises that they will host all kinds of content: drug shops, fraud, porn, and money laundering. Interestingly, although it says it will host fraud and money laundering content, it will not host hacking, spamming, and botnet content.



A bulletproof hosting company promotes the security and anonymity of its service.



COMMERCIAL SOFTWARE FOR RENT

Looking to rent expensive software for a specific project? Look no further. The TRU team saw cybercriminals mimicking the offerings of many legitimate software-as-a-service providers but at a much lower rate. One vendor is selling a license for one user to the 2019 version of Adobe Premiere Pro (a program for video editing) for \$5.67, and another vendor is selling a license for one user to Adobe Creative Suite Master Collection CS6 with 18 different popular Adobe products.

Several other threat actors are advertising that they will sell access to popular software for \$250 per day and up to \$1,000 for three months' access. However, one does not list the specific applications, but rather requests that interested buyers private message him to find out the types of software he has access to.

■ \$250 for 1 week of activation

■ \$500 for 1 month of activation

■ \$1,000 for 3 months of activation

CUSTOMER SERVICE – HACKER STYLE

One of the things that the TRU team saw this year was an increase in the number of dark market vendors putting a lot of effort into showcasing the high quality of their illicit goods. For example, one criminal boasts that all of his credit cards come with big limits and all the CVV numbers have been verified. Many sellers also offer to go through a guarantor or that they have a 24-hour return policy, should anything be wrong with the goods they are selling.

The TRU team spotted a seller on a Russian underground market offering bank transfer services, credit cards, and Venmo accounts, and he even swears on the life of his first child that he can be trusted.

"I took on this business as an opportunity to render a steppingstone to the masses to ease up the challenges the masses are encountering today so they can live up to the expectations of life. I work with trust and sincerity which is why I am willing to put in all it takes and as well vow with the life of my first child. Building a long term business partnership. I only work with reliable buyers...And I Need Good Buyer For Business Long Time..."

The quality of service we offer is up to the highest standards. You will feel like the KING of carding when buying dumps & cards from us."



Cracked versions of commercial software are inexpensive on dark markets.

Another dark market vendor is extremely adamant that they will always respond if a buyer has a complaint and that the buyer needs to reach out to this vendor to get any questions or problems resolved, but DO NOT open a dispute on the marketplace. In essence they were asking buyers not to file a complaint with the dark market administrator.

"We are a very experienced company specializing in all aspects of the Dark Web and trading on many of the Dark Web Market places. Because of this we can offer the personal and friendly service. Please be advised all orders are sent to the customer within 24 hours and usually less. All orders are sent direct to your personal messages in-box. We do not send to e-mail addresses or Jabber e.c.t.(sic)

We reciprocate all feedback. All passwords and links are working when we send them to you. However should you have a problem with any purchase please contact us before opening a dispute. Anyone opening a dispute or leaving anything other than 100% feedback will not be serviced again and will have any warranty or after sales help nullified.

We pride ourselves on customer satisfaction so should you have any questions or queries or issues please contact us first. We are here to help. We guarantee to resolve any problems and issues with you including replacements, extra free items and of course refunds. We reply to all queries and questions within 24 hours but PLEASE allow us to reply to you first."



UNDERGROUND MARKETPLACE PRODUCTS

When it comes to the variety and the amount of illicit goods on the underground markets, Armor's findings illustrate that the cybercriminals participating in these businesses are resilient, innovative, and agile. They are constantly coming up with creative ways to sell their goods and to monetize any type of data.

HACKERS ADD BUSINESS FULLZ TO THEIR REPERTOIRE

Although financial data is sold as a commodity, personal fullz continue to be one of the most popular items on the dark net. And now, hackers have added "business fullz" to their repertoire. Personal fullz are packets of information about individuals. They contain all kinds of Personal Identifiable Information (PII) on an individual. Personal fullz typically contain the victim's full name, social security number, date of birth, phone number, address, driver's license, and mother's maiden name—everything a criminal needs to commit identity theft. Similarly, business fullz contain everything a criminal needs to appear as if they are a corporate officer of an actual business. One vendor states that his business fullz contains a corporate officer's credit score (promises a 700 to 850 credit score), certificate of business, bank account numbers, and Employee Identification Number (EIN), also known as a Tax Identification Number. An EIN is a unique, nine-digit number assigned by the IRS to business entities operating in the U.S. for the purposes of opening a bank account or filing tax returns.

The business fullz also come with a background report, the Social Security Number (SSN), and full names and birthdays of the corporate officers. The seller also promises that the business does not have a credit lock. Business fullz cost between \$35 and \$60 depending on the seller.

What can one do with this packet of valuable business documents? As billions of dollars in small business loans flow to organizations as a result of the COVID-19 crisis, the TRU team believes this type of information could potentially help criminals apply for these small business loans, as well as standard business loans, lines of credit, and high-limit credit cards. Cybercriminals can also use this information to help stage business email compromise schemes and open business bank accounts, enabling them to move larger amounts of money in and out of the account without drawing unwanted attention to their activities.



***UPDATE* High Quality Business Fullz w/ bank account #s and documents**
 NEW UPDATE! Information included: Company name address owner owner phone phone email tax exempt # Federal ID number...
 Sold by [redacted] - 408 sold since November 27, 2018 Vendor Level 5 Trust Level 5
 12 items available for auto-dispatch

Product Class	Features	Origin Country	Features
Digital	16	United States	World Wide
Quantity Left	Never	Ships to	Escrow
Ends In		Payment	

Bulk Discount	Price
From qty 5 to 9	USD 25.00
From qty 10 to 79	USD 20.00

default - 1 day - USD + 0.00
 Purchase price: **USD 35.00**

Underground criminals advertise business fullz, a packet of key, identifying information about a business and its owner(s) or corporate officers, so that scammers can commit fraud against the business, such as applying for bank loans, setting up money mule accounts, etc.

FRESH BUSINESS FULLZ WITH CREDIT SCORE 700-850(SSN, CERTIFICATE OF BUSINESS, BUSINESS NAME, CERTIFICAT)
 GET ACTIVE BUSINESS FULLZ IN THIS LISTING NO FREEZE, NO CREDIT ALERT, NO RESELL!!!!!!! no custom here, just ran...

Sold by [redacted] - 50 sold since September 05, 2019 Vendor Level 4 Trust level 3

Product Class	Features	Origin Country	Features
Digital	Unlimited	United States	World Wide
Quantity Left	Never	Ships to	World Wide
Ends In		Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: **USD 55.00**

Qty: 1 [Buy Now](#) [Buy Now](#) [Queue](#)

0.006023 BTC / 1.313276 LTC / 0.058168 XMR

USA BUSINESS FULLZ - EIN - BUSINESS DOCUMENTS - CREDIT REPORT - BACKGROUND REPORT - SSN - DOB
 NO FRAUD ALERT OR CREDIT LOCK OR FREEZE ON CREDIT REPORT. NEVER USED BY ANYONE A PACKAGE THAT YOU...

Sold by [redacted] - 79 sold since September 05, 2019 Vendor Level 5 Trust level 5

Product Class	Features	Origin Country	Features
Digital	Unlimited	World Wide	World Wide
Quantity Left	Never	Ships to	World Wide
Ends In		Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: **USD 60.00**

Qty: 1 [Buy Now](#) [Queue](#)

0.006571 BTC

Business fullz are offered on the dark web for between \$35 and \$60.

FINANCIAL LOAN APPLICATIONS REAP PERSONAL FULLZ

One of the most worrisome items the TRU team saw being advertised on the dark net were personal, U.S.-based fullz that the seller claims to have received from stolen financial loan applications. Loan applications contain particularly valuable details, typically chock full of personal and financial data such as employment and income information, bank account information, bank statements, credit report, SSN, driver's license or passport (some form of government issued photo ID), utility bills, lease agreement, and proof of insurance (to prove one's address). Lenders might also require information about the loan applicant's current expenses—such as mortgages, vehicles, student loans, credit cards, and rent—to make sure the applicant has enough cash flow to take on an additional loan payment. Full identity packets, which contain much of this data, can be used to steal someone's identity, withdraw money from the victim's bank account, use the victim's credit card, apply for many new credit cards using the victim's name and credit history, apply for personal loans in the victim's name, or buy an expensive car (if the victim's credit is good). These fullz are being offered for \$50 and \$75 apiece.

Standard fullz currently run between \$20 to \$50 depending on the country of origin. These usually contain the victim's full name, social security number, date of birth, phone number, address, driver's license, and even their mother's maiden name. Healthcare information is sold at a premium for the detailed information it contains.

TOOLS OF THE CYBERCRIME TRADE: CRYPTERS, REMOTE ACCESS TROJANS (RATS), AND EXPLOIT KITS

On marketplaces and in forums, malicious software is one of the key items being sold along with access to hijacked servers, botnets, and individual computers. Among the most popular tools of the cybercrime trade are remote access trojans (RATs), exploit kits, and crypters. A crypter is software that can encrypt and obfuscate malware, making it undetectable to some anti-virus programs. Threat actors can find these handy tools for as little as \$1. RATs continue to be popular because they can give cybercriminals complete access to a victim's computer, just as if they had physical access to the device. With this access, the cybercriminal can access the victim's files, their camera, and even turn on or off their device. The TRU team saw a variety of RATs advertised on the underground markets ranging from \$1 to \$12.

Exploit kits used to be very popular on the underground. An exploit kit is a type of toolkit packaged with exploits that cybercriminals use to attack vulnerabilities in commonly installed software, such as Internet Explorer and Adobe Flash Player. Their goal is to successfully compromise the computer system so they can distribute malware onto the device. Exploit kits are typically designed to be modular and are updated to add newer exploits to replace the older exploits. Some threat actors sell complete kits outright, while others rent their kits per week or per month. The rental fees can range from \$800 a month to \$2,000. The TRU team is also seeing threat actors sell individual exploits. One cybercriminal is offering to sell an exploit for the popular Drupal content management system for \$80. He claims it can successfully exploit Drupal version 7 and 8.



Cryptex Crypter

Cryptex Crypter Why Buy from us: - We deliver full support on all of our products, So if you have any questions please let u...

Sold by [Vendor Level 5] - 49 sold since February 14, 2018

Unlimited items available for auto-dispatch

Product Class	Features	Origin Country	Features
Digital	Digital	World Wide	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow


default - 1 day - USD + 0.00

Purchase price: **USD 0.99**

Qty: [Buy Now](#) [Buy Now](#) [Buy Now](#) [Queue](#)

0.000107 BTC / 0.022262 LTC / 0.014251 XMR

A vendor advertises crypters, software that can encrypt and obfuscate malware, making it undetectable to some anti-virus programs.




[MS] Set up Remote Administration Tool Zeus BotNet (RAT) INSTANT DELIVERY

Item # 19974 - Software & Malware / Botnets & Malware - (19156)

Views: 2354 / Sales: 55

Quantity left: Unlimited (Unlimited automatic items)

Buy Price
USD 2.57
(0.000250 BTC)




2020 AndroRAT -Android Remote Admin Tool (RAT)

Item # 23587 - Digital Products / Fraud Software - (37607)

Views: 902 / Sales: 41

Quantity left: Unlimited (Unlimited automatic items)

Buy Price
USD 0.99
(0.000096 BTC)




[MS] njRAT v0.7d By njq8 RAT PACKAGE

Item # 6941 - Software & Malware / Botnets & Malware - (2034)

Views: 3402 / Sales: 38

Quantity left: Unlimited

Buy Price
USD 11.73
(0.001136 BTC)



[MS] Droid Jack Android Rat INSTANT DELIVERY


Item # 19984 - Software & Malware / Botnets & Malware - (19156)

Views: 1706 / Sales: 34

Quantity left: Unlimited (Unlimited automatic items)

Buy Price
USD 1.29
(0.000125 BTC)

A cybercriminal promotes a variety of remote access trojans (RATs) for cheap.



★ DANGEROUS VIRUSES PACK


(RATs ✓ keyloggers ✓ stealers ✓ DDOS) ★ +NordVPN Premium account ✓

Item # 58434 - Digital Products / Fraud Software - (23480)

Views: 18068 / Sales: 1387

Quantity left: Unlimited (Unlimited automatic items)

Buy Price
USD 2.68
(0.000379 BTC)



★ 2020 DANGEROUS VIRUSES PACK


(RATs ✓ keyloggers ✓ stealers ✓ DDOS) ★ +NordVPN Premium account ✓

Item # 81001 - Services / Other - (23480)

Views: 3527 / Sales: 307

Quantity left: Unlimited (Unlimited automatic items)

Buy Price
USD 4.99
(0.000706 BTC)




DDos Programs free [watch picture for more info]

Item # 12696 - Digital Products / Fraud Software - (1454)

Views: 1961 / Sales: 232

Quantity left: Unlimited (Unlimited automatic items)

Buy Price
USD 0.01
(0.000001 BTC)



★ 2020 DANGEROUS VIRUSES PACK

(RATs ✓ keyloggers ✓ stealers ✓ DDOS) ★ +NordVPN Premium account ✓

Item # 58429 - Software & Malware / Exploits - (23480)

Views: 2711 / Sales: 114

Quantity left: Unlimited (Unlimited automatic items)

Buy Price
USD 2.92
(0.000413 BTC)

Threat actors sell virus packs really cheap. Their packs most likely contain old malware, which can be found for free on the dark web.



[POWERFUL] Drupal RCE Exploit [Fully Weaponized] [88% OF BUILDS VULN]

This offer is for a vastly unpatched and undiscovered exploit in Drupal 7 and 8 which allows for writing to the web root and remot...

Sold by [Vendor Level 1] - 4 sold since May 11, 2019

671 items available for auto-dispatch

Product Class	Features	Origin Country	Features
Digital	Digital	Russian Federation	Russian Federation
Quantity Left	21	Ships to	World Wide
Ends In	Never	Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: **USD 80.00**

Qty: [Buy Now](#) [Buy Now](#) [Buy Now](#) [Queue](#)

0.007737 BTC / 1.621731 LTC / 1.029336 XMR

A dark market vendor advertises an attack tool that claims to successfully exploit a vulnerability in the Drupal Content Management System version 7 and 8.

ARMOR ARMOR.COM | 20030923 Copyright © 2020. Armor, Inc., All rights reserved.

19

BOTNETS AND BOTNET SOURCE CODE FOR SALE

The TRU team also spotted underground merchants purporting to sell the source code for several botnets. One vendor, which lists the Russian federation as their home, is actually trying to sell some unsuspecting newbie the source code for the TinyNuke Banking Botnet for \$75. The source code for TinyNuke was actually posted for free on GitHub back in March 2017. So unless this threat actor has added a lot of additional functionality to this banking botnet, buyers are definitely being defrauded.

In another example, a dark net vendor tries to peddle what they describe as the “source code” for the Mirai botnet for \$6. From the ad enclosed, it does not appear that the seller has interested buyers. This is not really surprising considering the source code for the original [Mirai botnet](#) was released to the public in Fall 2016 by its creator, according to news reports. Mirai is also known as an internet of things (IoT) botnet because Mirai spreads to vulnerable routers, IP cameras, digital video recorders, and other easily hackable IoT devices. The devices are then infected with malware, turning them into bots (digital devices controlled remotely). This network of hijacked computers can be used to mount distributed denial of service (DDoS) attacks against a target. Mirai was reported to have taken down large portions of the internet in 2016 with a massive DDoS attack, affecting such popular services and news sites as Twitter, CNN, The Guardian, Netflix, Reddit, and many others in both Europe and the U.S.

Adept hackers can use the original Mirai source code to create their own variant. In March, for example, a new variant of Mirai was observed targeting [network-attached storage devices](#). Perhaps this underground merchant is actually selling a new Mirai variant for \$6. However, for that low price, the TRU team thinks it is very unlikely.

NO IMAGE AVAILABLE

TinyNuke Banking Botnet

This repository contains the source code of TinyNuke which is a zeus-style trojan written by me. Main Features: =====

Sold by - 2 sold since May 11, 2019 Vendor Level 1 Trust level 2

120 items available for auto-dispatch

Product Class	Features	Origin Country	Features
Digital	13	Russian Federation	World Wide
Quantity Left	Never	Ships to	World Wide
Ends In		Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: **USD 75.00**

Qty: Buy Now Buy Now Buy Now Queue

0.008041 BTC / 1.702997 LTC / 1.165864 XMR

The TinyNuke Banking Botnet source code was released on GitHub in 2017. This dark web vendor is trying to sell it for \$75.

NO IMAGE AVAILABLE

Mirai botnet Source Code strongest botnet

Mirai botnet Source Code strongest botnet

Sold by - 0 sold since March 22, 2020 Vendor Level 1 Trust level 1

Unlimited items available for auto-dispatch

Product Class	Features	Origin Country	Features
Digital	Unlimited	Russian Federation	World Wide
Quantity Left	Never	Ships to	World Wide
Ends In		Payment	Escrow

default - 1 day - USD + 0.00

Purchase price: **USD 6.00**

Qty: Buy Now Buy Now Buy Now Queue

0.000842 BTC / 0.136705 LTC / 0.092951 XMR

An underground merchant advertises the source code for Mirai, an infamous internet of things (IoT) botnet used for DDoS attacks.




REMOTE DESKTOP PROTOCOL CREDENTIALS – GET ‘EM WHILE THEY’RE HOT!

One of the ways cybercriminals are infecting organizations with ransomware and other malware is by targeting open Remote Desktop Protocol (RDP) servers. The hackers will scan the internet for “open” internet-facing servers running the RDP service. An RDP service is commonly used by organizations so that their employees can log in to office computers remotely. The service also allows IT administrators to perform IT tasks such as software installation, PC maintenance, computer troubleshooting, printer setup, and email setup, among other activities.

When the cybercriminals detect open RDP servers, they will often try and use a brute force, password-spray attack to attempt to log in to the server using common or default usernames such as “administrator” along with multiple, commonly used passwords to gain access. Once the threat actors have obtained working credentials, they simply utilize it as a pivot point for lateral movement into other areas of the network and proceed to steal data and install ransomware or other malware onto target machines.

As in 2019, the TRU team found cybercriminals offering to sell credentials to publicly available RDP servers. These credentials have grown widely popular, and there are countless dark market vendors selling them, bringing the average price down from \$20 to \$24 each to between \$16 and \$25 apiece.



+++ Super RDP | USA | EU +++ Not hacked !
 HM Super RDP Service Hello everybody! We are selling new RDP | Proxy | socks5 for 1 month (you can renew it later if y...
 Sold by [Vendor Level 4] - 25 sold since February 01, 2019 [Trust level 3] 9400 4.82

Product Class	Features	Origin Country	Features
Digital	Unlimited	World Wide	World Wide
Quantity Left	Never	Ships to	World Wide
Ends In	Never	Payment	Escrow

Silver RDP Regular RDP with admin access - 1 days - USD + 1.00 / item

Purchase price: **USD 16.00**

Qty: 1 [Buy Now](#) [Buy Now](#) [Buy Now](#) [Queue](#)

0.001733 BTC / 0.370456 LTC / 0.249454 XMR



--= RDP with Admin Access - WORLDWIDE ==--
 =====WELCOME===== Have worldwide RDPs which are very useful for different carding method...
 Sold by [Vendor Level 5] - 379 sold since March 28, 2018 [Trust level 4]


Product Class	Features	Origin Country	Features
Digital	Unlimited	World Wide	World Wide
Quantity Left	Never	Ships to	World Wide
Ends In	Never	Payment	Escrow

Rdp with admin access RANDOM COUNTRY LEAVE NOTE EMPTY NO USA - 1 days - USD + 0.00 / it

Purchase price: **USD 9.99**

Qty: 1 [Buy Now](#) [Buy Now](#) [Buy Now](#) [Queue](#)

0.001083 BTC / 0.231304 LTC / 0.155948 XMR



Atlanta, GA - Non hacked RDP Service or VPS. RDP server
 BIGGEST RDP VENDOR SINCE ALPHABAY! PLEASE SPECIFY IN THE ORDER NOTES IF YOU WANT WINDOWS 7, W...
 Sold by [Vendor Level 2] - 5 sold since April 23, 2019 [Trust level 1]

Product Class	Features	Origin Country	Features
Digital	Unlimited	World Wide	World Wide
Quantity Left	Never	Ships to	World Wide
Ends In	Never	Payment	Escrow

Linux GUI - 1 days - USD + 10.00 / item

Purchase price: **USD 25.00**

Qty: 1 [Buy Now](#) [Buy Now](#) [Buy Now](#) [Queue](#)

0.002710 BTC / 0.578838 LTC / 0.390259 XMR

Atlanta, GA - Non hacked RDP Service or VPS. RDP server
 BIGGEST RDP VENDOR SINCE ALPHABAY!
 PLEASE SPECIFY IN THE ORDER NOTES IF YOU WANT WINDOWS 7, WINDOWS 10, LINUX VPS OR WINDOWS GUI (windows GUI costs 43 USD)

 SPECIAL REQUESTS VIA PM

I am selling RDP access (windows 7 or windows 2008 server), or linux VPS, or Linux RDP (Ubuntu + GUI) as customer's wish.
 DON'T ASK FOR RDPs FROM ZIPCODES I JUST HAVE WHAT YOU SEE IN THIS LISTING

Leads at least 30 days (if you need more time, I can help you with that)
 Strong, test,
 Reliable
 just what you need to card / Paypal / Amazon /
 No Ip Logs
 Uptime of 99.99%
 IP available in

 Windows 7 / 10 / Linux VPS / Linux GUI

Non-hacked RDP credentials, guaranteed not to have been used previously, are advertised for the U.S., Europe, and other parts of the world.

CREDIT CARD CREDENTIALS AND CLONED ATM AND DEBIT CARDS FROM ALL COUNTRIES, INCLUDING RUSSIA AND CHINA

Although criminals on the underground have been hawking credit card credentials for years, these items have not lost their allure. There are countless ads offering to sell credit card dumps. These are credit card credentials that include the Track 1 and Track 2 data and pin code. The track data is contained on the magnetic stripe on the back of the credit card and includes such information as the Primary Account Number (the credit card number printed on the front or back of the card). It also contains the name of the card owner, card expiration date, service code, Pin Verification Key Indicator, PIN Verification Value, and Card Verification Value (CVV), or Card Verification Code (CVC). Using this data, criminals can clone the actual credit card. Like in 2019, these card credentials today are running between \$110 and \$150 per card, depending on the country in which the card was issued and the type of card.

One of the most interesting items Armor saw in the last few months was a criminal on a Russian forum offering to sell credit card and ATM cards from any bank in the Russian Federation. It is not common to see cybercriminals on the forums, especially Russian-speaking forums, offering to commit crimes against Russian organizations or their citizens—it has also been an unspoken rule. Typically, criminals located in Russia, Ukraine, and many of the surrounding republics state very clearly that they will not target businesses or citizens in the Commonwealth of Independent States (CIS), which is made up of Russia, Ukraine, and nine other republics. However, the COVID-19 pandemic has triggered a deep global recession and, according to a recent report from the [World Bank](#), Russia's 2020 growth is projected to contract by 6 percent, an 11-year low. So, it is certainly plausible that some of the cybercriminals in Russia are struggling to the extent that they are willing to break the unspoken rule.

The other finding that caught the TRU team's attention is that there are dark net vendors offering to sell stolen credit card credentials originating from banks in China. Currently, cards from banks in mainland China and Hong Kong, complete with Track 1 and Track 2 data and the accompanying pin, are running \$100 apiece. The TRU team anticipates that researchers will continue to see more credit card credentials from China being offered in the dark web markets, especially as more residents of China begin traveling for leisure. According to a report by the China Tourism Academy, Chinese tourists made 149 million overseas trips in 2018, with total spending amounting to \$130 billion.

CREDIT CARD DATA WITH TRACK 1 AND TRACK 2 DATA

The prices for U.S.-based credit cards with Track 1 and Track 2 data currently range between \$70 and \$110, whereas last year they were going for between \$85 and \$110; U.K.- and Canada-based cards dropped from an average of \$110 to \$120 to an average price between \$85 and \$120. We also saw a similar drop in prices for credit cards originating from Europe. In 2019, they ranged from \$120 to \$150, but this year, the prices range from \$90 to \$150. The TRU team considers the possibility that the COVID-19 pandemic forced some sellers to reduce their prices as economies across the world began to decline due to the coronavirus. Regardless, criminals can still spend between \$70 and \$150 for one set of card credentials, and these can be written to a blank card and used to purchase high-end luxury items, which can then be sold to underground market buyers or on shady websites. The cloned cards can also be used to withdraw money from ATM machines.

One dark market seller advertises his specially made, counterfeit ATM cards as being able to take money directly from any ATM machine vault and says they have very “special features,” including two extremely amusing ones providing instructions for how to avoid being recorded on the ATM and CCTV cameras. If a buyer wants to know the price, then they have to text the underground merchant.

“BEST WAY TO HAVE GOOD AMOUNT TO START A GOOD BUSINESS OR TO START LIVING A GOOD LIFE....Hack and take money directly from any ATM Machine Vault with the use of MY ATM Programmed Card which runs in automatic mode. Text 111111111111 for how to get it and its cost.

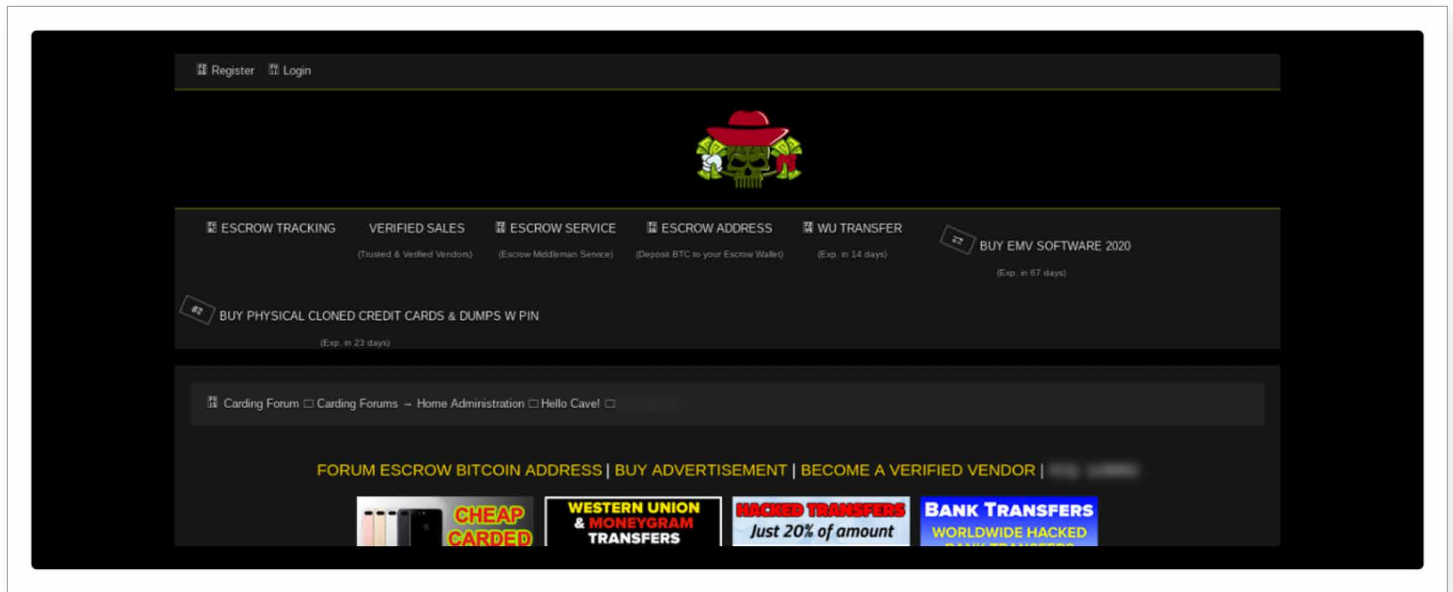
..... EXPLANATION OF HOW THESE CARD WORKS.....

You just slot in these card into any ATM Machine and it will automatically bring up a MENU of 1st VAULT \$1,000, 2nd VAULT \$5,000, RE-PROGRAMMED, EXIT, CANCEL. Just click on either of the VAULTS, and it will take you to another SUB-MENU of ALL, OTHERS, EXIT, CANCEL. Just click on others and type in the amount you wish to withdraw from the ATM and you have it cashed instantly... Done.

NOTE: DON'T EVER MAKE THE MISTAKE OF CLICKING THE “ALL” OPTION. BECAUSE IT WILL TAKE OUT ALL THE AMOUNT OF THE SELECTED VAULT.

Some “special features” included are:

1. Your illegal ATM activity is undetectable and untraceable.
2. Card can be used anywhere in the world, on any model ATM machine.
3. \$5,000 daily withdrawal possible. More, if you purchase a pricier card.
4. A secret mechanism or technique which prevents ATM and CCTV cameras from recording your face. Hmm. Maybe a can of spray paint or roll of duct tape to cover the camera lens is included? Or maybe a free Groucho Marx mask comes in the box???



A dark market website specializes in credit card fraud and other financial crimes.

CREDIT CARD DATA MISSING TRACK 1 AND TRACK 2 DATA

Dark market merchants also are peddling credit cards without Track 1 and 2 data. These credentials usually contain the card owner's name, billing address, card number, expiration data, and CVV or CVC number. These cards, depending on the country location from which they are issued, range in price. Today, credit cards, complete with CVV or CVC number and issued from U.S.-based financial institutions, cost between \$5 and \$12 depending on the type of credit card (Visa, MasterCard, Discover, or American Express). The price for similar credit cards, issued from the EU, are priced between \$18 to \$35, basically the same price as in 2019. However, the TRU team did find one cybercriminal selling U.S. and European-based credit cards for a flat rate of \$15 per card. When purchasing credit card numbers from underground markets, buyers can pay a small fee to check if the card is activated and receive the credit limit of the card.

These cards are also desirable because cybercriminals can simply sit behind a computer and use the stolen credit cards to purchase expensive, luxury items online. These are called "card not present" purchases. The scammer does have to resell the goods to cash out, but there are many gray markets in which to do so, as well as underground markets for selling stolen goods. There is less risk to the scammer because they can be anywhere in the world. They merely need a computer and a safe address in which to have the items shipped. Often the criminal heading the operation will engage money mules in the country in which the retailer has a big presence and task them to ship the goods to them once received. The TRU team firmly believes that stolen credit cards and gift cards will continue to be sought after. In 2019, an [estimated 33%](#) of the credit card industry's chargebacks were due to criminal fraud.

CARD SKIMMERS, CARD READERS/WRITERS

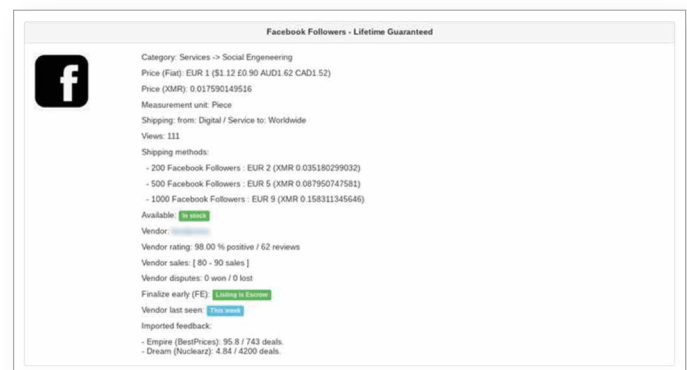
In order for threat actors to clone credit card and ATM cards, they need the Track 1 and Track 2 data from a card's chip or the magnetic strip on the back of the card. One of the ways that criminals get this information is by using skimming devices, which they surreptitiously attach to an ATM machine or point-of-sale device, such as those found at gas stations. New skimmers have emerged with the rise of "tap-and-pay" features and mobile payment platforms. Threat actors have been selling skimming devices in the underground markets for years, and prices for the skimmers are basically the same as last year, running between \$700 and \$1,200, depending on the model.

Once the threat actor has captured the Track 1 and Track 2 data and pin codes from the cards, they can then use a card reader/writer to clone the data onto card blanks. The TRU team spotted card readers/writers ranging in cost from \$449 to \$990, depending on the model. They could be paid for with Bitcoin, Perfect Money, Visa, American Express, or MasterCard gift cards. This year, the TRU team noted that there were numerous dark market sellers accepting payment via credit card gift cards, as well as Bitcoin, Monero, Litecoin, Dash, and Perfect Money.

BUY FOLLOWERS, LIKES, AND VIEWS FOR YOUR SOCIAL MEDIA ACCOUNTS

Another popular item on the underground hacker markets is the purchase of followers, likes, and views to boost influence and traffic on social media platforms such as TikTok, Instagram, and YouTube. For as little €9, a person can increase their Facebook followers by an extra 1,000. If a computer user wants to increase their views on TikTok then they can be purchased. One merchant is selling 2,000 views for €2 up to 100,000 views for €13, while 5,000 Twitter "likes" can be purchased for as little as \$16.

For \$19.99, a vendor advertises software that they claim can automatically increase the views of a YouTube channel or increase the ranking of a video. For only \$10, a buyer can download 1,000 podcasts from iTunes.



Purchase additional Facebook followers.

TikTok Views - Lifetime Guaranteed

Category: Services -> Social Engineering

Price (Fiat): EUR 1 (\$1.12 €0.90 AUD1.63 CAD1.52)

Price (XMR): 0.017590149516

Measurement unit: Piece

Shipping: from: Digital / Service to: Worldwide

Views: 105

Shipping methods:

- 2000 TikTok Views : EUR 2 (XMR 0.035180299032)
- 5000 TikTok Views : EUR 4 (XMR 0.070360598065)
- 10000 TikTok Views : EUR 6 (XMR 0.105540897097)
- 50000 TikTok Views : EUR 8 (XMR 0.140721196130)
- 100000 TikTok Views : EUR 13 (XMR 0.228671943711)

Available: [In stock](#)

Vendor: [Buyer's Choice](#)

Vendor rating: 98.00 % positive / 62 reviews

Vendor sales: [80 - 90 sales]

Vendor disputes: 0 won / 0 lost

Finalize early (FE): [Waiting to Escrow](#)

Vendor last seen: [This week](#)

Imported feedback:

Twitter Likes HIGH QUALITY - EXTRA Delivery - Warranty

Category: Services -> Other Services

Price (Fiat): USD 4 (£3.55 €3.20 AUD5.77 CAD6.41)

Price (XMR): 0.062392762439

Measurement unit: Piece

Shipping: from: Digital / Service to: Digital / Service

Views: 28

Shipping methods:

- 1000 Twitter Likes : USD 0 (XMR 0.000000000000)
- 2000 Twitter Likes : USD 4 (XMR 0.062392762439)
- 3000 Twitter Likes : USD 8 (XMR 0.124785524879)
- 4000 Twitter Likes : USD 12 (XMR 0.187178287318)
- 5000 Twitter Likes : USD 16 (XMR 0.249571049758)

Available: [In stock](#)

Vendor: [Buyer's Choice](#)

Vendor rating: 100.00 % positive / 18 reviews

Vendor sales: [20 - 30 sales]

Vendor disputes: 0 won / 2 lost

Finalize early (FE): [Waiting to Escrow](#)

Vendor last seen: [Yesterday](#)

Imported feedback:

Purchase additional Twitter likes and YouTube and TikTok views.

Youtube Views Bot

Youtube Views Bot With this software you can: - Increase Youtube views - Increase video rank FAQ: Do you delivery supp...

Sold by [Buyer's Choice](#) - 9 sold since February 23, 2020 Vendor Level 5 Trust level 4 D 32 5.00

Unlimited items available for auto-dispatch

Product Class	Features	Origin Country	Features
Quantity Left	Digital	World Wide	World Wide
Ends In	Unlimited	Ships to	World Wide
	Never	Payment	Escrow

Instant Delivery - 1 days - USD + 0.00 / item

Purchase price: **USD 19.99**

Qty: [Buy Now](#) [Buy Now](#) [Buy Now](#) [Queue](#)

Itunes Podcast Downloads | 1000 For 10\$ | Lifetime Warranty

Itunes Podcast Downloads | 1000 For 10\$ | Lifetime Warranty - Quality = High - Start Time = Up to 24 Hours - Speed = 2K ...

Sold by [Buyer's Choice](#) - 0 sold since December 01, 2019 Vendor Level 5 Trust level 4 D 32 5.00

Product Class	Features	Origin Country	Features
Quantity Left	Digital	World Wide	World Wide
Ends In	Unlimited	Ships to	World Wide
	Never	Payment	Escrow

1000 Podcast Downloads - 1 days - USD + 0.00 / order

Purchase price: **USD 10.00**

Qty: [Buy Now](#) [Buy Now](#) [Buy Now](#) [Queue](#)

0.001082 BTC / 0.231642 LTC / 0.155909 XMR

Software is advertised on the dark net as being able to increase a person's YouTube views and video ranking.

Buyers can purchase 1,000 podcasts from iTunes for \$10.

Underground criminals are not just buying and selling usernames and passwords for U.S.-based social media accounts such as LinkedIn, Twitter, Instagram, and Facebook. Scammers are also interested in purchasing account credentials for social media platforms located in other parts of the world. One such platform is VK, a popular Russian online social media and networking service based in St. Petersburg, Russia. VK is reported to have 600 million users. One interested buyer posted:

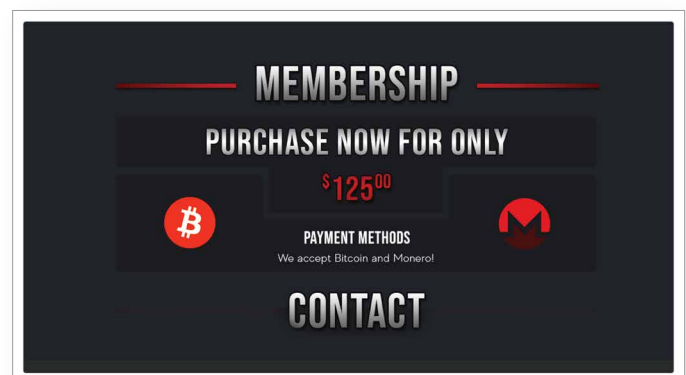
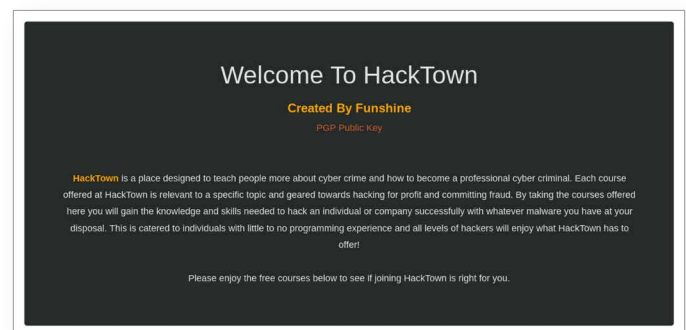
"I will buy VKI accounts, I am interested in ACTIVE 100+ friends, 18+ age (80% friends must be over 18 years old). Ready to redeem in large quantities! Write only to those who have reviews on such a forum or a high rating. Please do not disturb the rest. If you do not have a high rating or reviews - give 10 accounts for the test, I check them, if everything is in order - we work further, if not, then no. I want to buy accounts VERY MUCH!"

GET YOUR DEGREE AT HACKER UNIVERSITY

Video tutorials and instruction guides on how to commit an array of different kinds of cybercrime, from PayPal cash-outs to creating bank drops and identity fraud, continue to be peddled on the underground for only \$10 each. One seller boasts in their ad “Earn \$1,000s every day. We have guides on just about EVERYTHING!!!”

However, one criminal group is offering a much better option than do-it-yourself instruction guides. They have established what they call “Hacker University.” They are selling memberships for \$125, to be paid in Bitcoin or Monero. For this one low fee, Hacker University purportedly offers members courses on everything from operational security and Wi-Fi hacking to network attacks and carding.

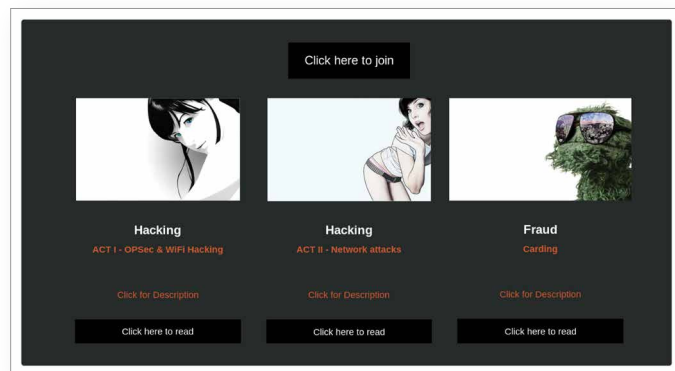
Creators of the site advertise that they want to “teach people about cybercrime and how to become a professional cybercriminal. By taking the course offered you will gain the knowledge and skills needed to hack an individual or company successfully with whatever malware you have at your disposal.” They offer training to those who want to become “hackers, fraudsters, dark market vendors and people who want to remain anonymous online.”



Hacker University advertises the topics you will learn about, including:

- How to access the router admin panel
- How to find proper targets once in the network
- Router exploitation
- Printer exploitation
- How to brute force a router admin panel
- Getting up to date on current MITM attacks
- How to perform MITM attacks
- All scripts and programs provided

There is also a planned section where members will be able to purchase malware including: ransomware, remote access trojans (RATs), crypters, password stealers, and keyloggers.



Hacker University courses include Wi-Fi hacking, network attacks, and carding.

RANSOMWARE EVOLVES TO BE MORE HEINOUS

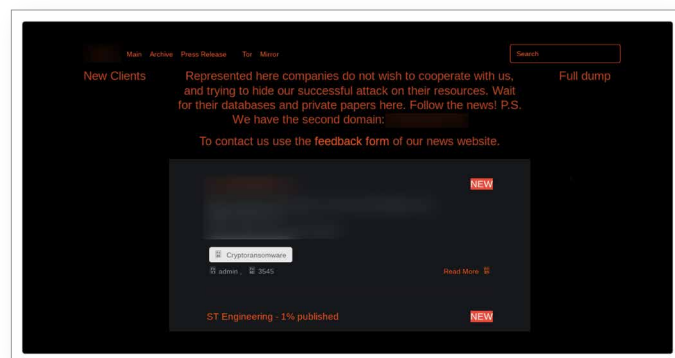
In 2019, Armor identified approximately 300 publicly reported organizations that have suffered a ransomware attack. Thus far, in 2020, from Jan. 1 to July 10, Armor has identified over 80 publicly reported U.S. organizations that have suffered a ransomware attack.

In [November 2019](#), cybercriminals added yet another lethal element to their ransomware schemes, causing ransomware attacks to become an even bigger problem for its victims. Threat actors began copying off the victim organization's data before encrypting it. They then threatened to publish portions of the data and sell it to other criminals or simply give it away if the ransom was not paid. Security staffing firm Allied Universal was the first organization to experience this additional form of extortion. The ransomware attackers demanded \$3.8 million after Allied missed two payment deadlines. The threat actors did release some of Allied's data on the internet and threatened to give all of it to WikiLeaks.

By May 2020, a ransomware attack using this approach had asked a record \$42 million ransom payment from celebrity law firm [Grubman Shire Meiselas & Sacks](#). There have been no public reports about whether or not the law firm paid a ransom. The threat actors behind the attack, called Sodin, rereported holding thousands of the law firm's documents hostage—allegedly including private information on Lady Gaga, Madonna, Nicki Minaj, Bruce Springsteen, Mary J. Blige, Christina Aguilera, and Mariah Carey. The digital kidnappers increased their demand for payment to \$42 million, double their initial \$21 million ask, when the firm failed to respond. The group threatened to publicly release more data if they were not paid within a week. On July 10, the ransomware gang kicked off an auction site with items being sold through July 18, purportedly containing data of their clients Bruce Springsteen, Usher, Nicki Minaj, Mariah Carey, Jessica Simpson, and LeBron James with a “buy now price” of \$1.5 million for each cache.

Grubman pack - Bruce Springsteen				Grubman pack - Usher			
All Bruce Springsteen legal documents from Grubman office.				All Usher legal documents from Grubman office.			
Minimum deposit:	\$60,000	Top bid:	--	Minimum deposit:	\$60,000	Top bid:	--
Start price:	\$600,000	Bid price:	\$1,500,000	Start price:	\$600,000	Bid price:	\$1,500,000
Opened Time left: 8 days, 03 hours, 22 minutes and 15 seconds				Opened Time left: 8 days, 03 hours, 24 minutes and 49 seconds			

Ransomware data was offered for sale on the Sodin website on July 10, 2020.



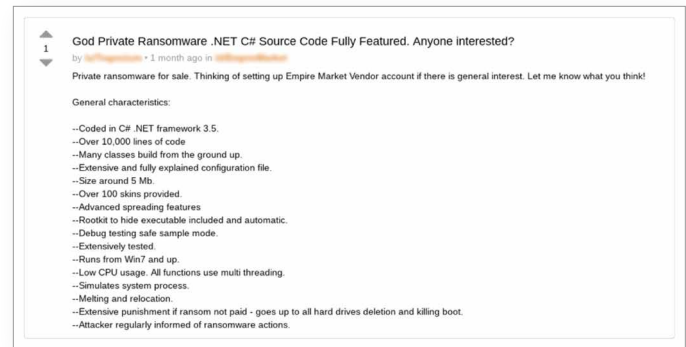
The Maze website lists its purported victims and samples of each victim's data.

	The Ultimate Blackmail Bitcoin Ransomware Item # 30461 - Botnets & Malware - (34618)	Buy Price USD 2.99 (0.000327 BTC)
	6 BITCOIN RANSOMWARE EASY INSTANT DELIVERY Item # 15060 - Exploit Kits - (18171)	Buy Price USD 3.75 (0.000418 BTC)
	The Ultimate Blackmail Bitcoin Ransomware Item # 7076 - Botnets & Malware - (5542)	Buy Price USD 6.50 (0.000712 BTC)
	6 BITCOIN RANSOMWARE EASY INSTANT DELIVERY Item # 30446 - Exploit Kits - (34618)	Buy Price USD 2.99 (0.000327 BTC)

For those who want to conduct their own ransomware campaigns, older source code can be purchased on dark markets.

Ransomware groups such as Sodin, Maze, Nemty, Lockbit, and Doppelpaymer have all openly taken part in this new extortion tactic. The group behind Maze hosts a website announcing its latest victims and includes samples of stolen files to show they mean business. Regular press releases by the group bully victims into paying. Few victims listed on the site have publicly reported a ransomware attack.

Ransomware continues to be offered as a stand-alone software product, as well as sold as a service (RaaS). There are also close-knit ransomware gangs that recruit affiliates to work with them to launch attacks.



A threat actor provides details on an underground forum about a specific type of ransomware he claims to have developed and wants to determine the interest level from prospective buyers.

HIJACKED LOGINS FOR POPULAR TV AND MOVIE STREAMING SERVICES AND PIZZA LOYALTY POINTS FOR SALE

Although it seems comical and almost impossible to believe, the TRU team even spotted dark market vendors selling access to Domino's Pizza accounts with points ranging from 60 to 120 points, and the price is a \$1.99. According to the Points Guy, one can get a medium, two-topping pizza with 60 Dominos points.



★INSTANT DELIVERY★ USA DOMINOS ACCOUNTS WITH 60+/120+ POINTS FOR A FREE PIZZA *ONLY 1.99\$!★

★INSTANT DELIVERY★ USA DOMINOS ACCOUNTS WITH 60+/120+ POINTS FOR A FREE PIZZA *ONLY 1.99\$!★ ✓F...

Sold by  - 576 sold since September 28, 2019 Vendor Level 6 Trust level 6

Product Class	Features	Origin Country	Features
Quantity Left	Digital	Ships to	United States
Ends In	Unlimited	Payment	World Wide
	Never		Escrow

60 to 120 points - 1 days - USD + 0.00 / item

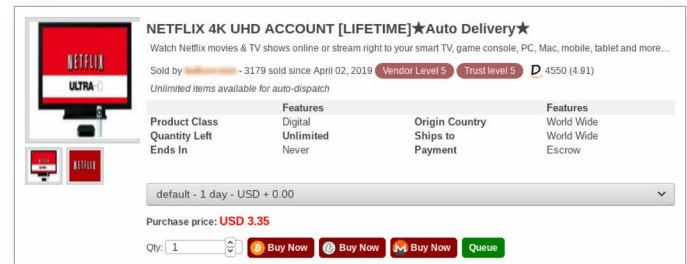
Purchase price: **USD 1.99**

Qty: Buy Now Buy Now Buy Now Queue

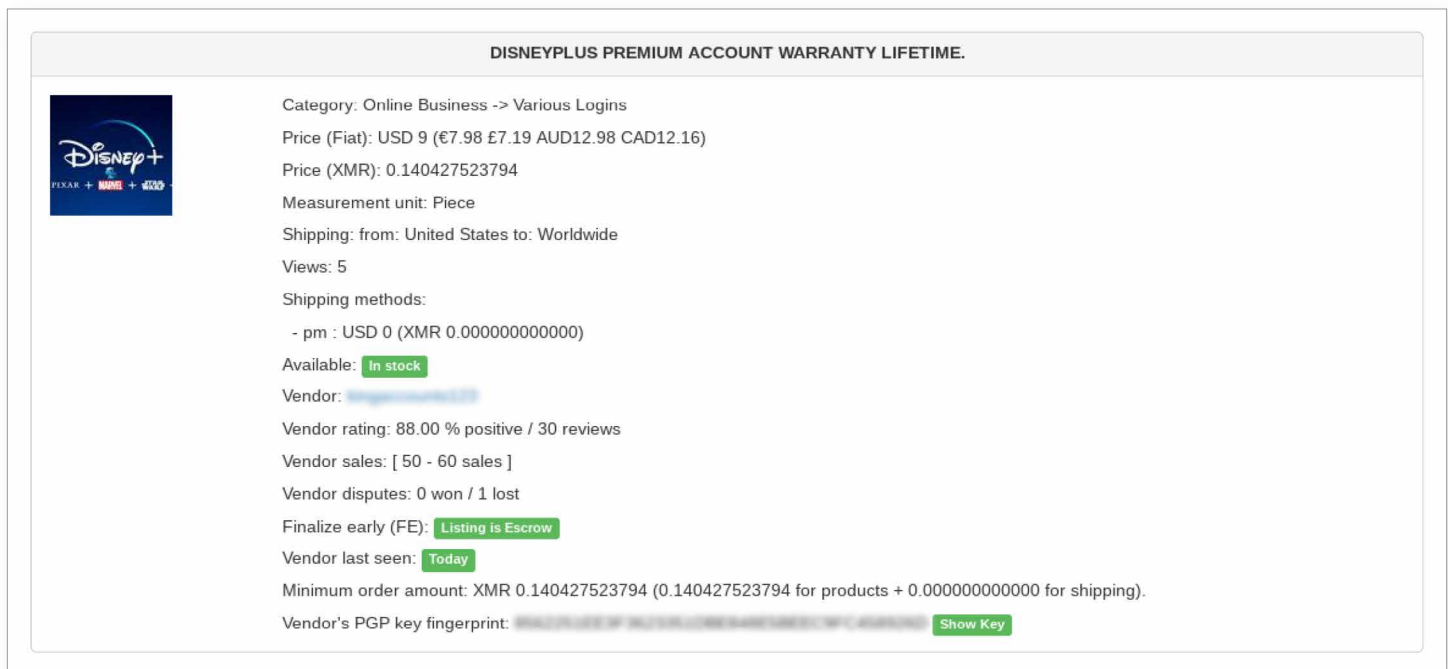
0.000216 BTC / 0.046193 LTC / 0.030925 XMR

Vendors selling credentials for Domino's Pizza accounts.

There are also vendors selling account logins for Netflix for \$3.35 and, according to the ad, the vendor has sold 3,179 Netflix account credentials in the past 14 months. Sales are recorded by the marketplace administrator so that the seller cannot fake their sales numbers. Disney+ and Spotify accounts begin at 99 cents each, with some vendors offering a lifetime replacement if the accounts stop working.



Vendors selling credentials for Netflix.



Vendors selling credentials for Disney+ accounts.

COVID-19 TREATMENTS, TESTS, AND PERSONAL PROTECTIVE EQUIPMENT PRICED AT SKY-HIGH PRICES

Just as thriving businesses capitalize on market opportunities when they present themselves, so do illicit businesses. Not surprisingly, when the COVID-19 pandemic began to wreak havoc across the world in February 2020, criminals on the dark net quickly jumped on the band wagon, hawking personal protection equipment (PPE), COVID-19 testing kits, and purported “treatments” for the virus at sky-high prices.

The TRU team saw scammers advertising N95 masks and surgical masks at a 400% to 500% markup. One dark net vendor advertises 1,000 N95 respirators for \$5,200, while 1,000 respirators normally costs \$1,000. Surgical masks, which typically cost 46 cents apiece sell for \$4 each. A box of 1,000 surgical masks costs the buyer \$4,000. Armor’s researchers also saw criminals selling coronavirus testing kits for \$39 to \$44.

In March, a much more serious situation began to materialize on the underground involving the selling of purported treatments for the deadly coronavirus. On Monday, March 23, just four days after U.S. President Donald Trump stated in a press briefing that hydroxychloroquine had shown “encouraging early results” in treating COVID-19, underground criminals began peddling what they claim to be “Chloroquine.” Hydroxychloroquine is an FDA-approved drug typically used to treat malaria, lupus, and rheumatoid arthritis. It is a derivative of Chloroquine.

COVID-19 Antibody Test Kit
 COVID-19 (SARS-CoV-2) Antibody Test Kit
 Sold by [Vendor] - 11 sold since March 26, 2020 Vendor Level 6 Trust level 6 D 4700 (5.00) [Buy] 656 (5.00)

Product Class	Features	Origin Country	Features
Quantity Left	Physical Package	Ships to	Europe
Ends In	Never	Payment	World Wide Escrow

Registered Shipping - 10 days - USD + 11.25 / order
 Purchase price: **USD 44.98**
 Qty: 1 [Buy Now] [Buy Now] [Buy Now] [Queue]
 0.004933 BTC / 1.071524 LTC / 0.702864 XMR

A vendor on a dark market advertises purportedly authentic COVID-19 testing kits.

CHLOROQUINE PHOSPHATE TABLETS AND AZITHROMYCIN
 All packages are shipped in letterbox sized parcels. Larger orders are cleverly packed using several different d...
 Sold by [Vendor] - 0 sold since March 22, 2020 Vendor Level 1 Trust level 1

Product Class	Features	Origin Country	Features
Quantity Left	Physical Package	Ships to	Australia(c)
Ends In	Unlimited	Payment	World Wide Escrow

DELIVERY - 5 days - USD + 10.00 / order
 Purchase price: **USD 1,000.00**
 Qty: 1 [Buy Now] [Queue]
 0.147433 BTC

Underground vendors begin selling Chloroquine on one dark web market in March 2020.

	CHLOROQUINE PHOSPHATE TABLETS BP 250MG Views: 61 / Sales: 0 Quantity left: Unlimited	Buy Price USD 500.00 (0.075211 BTC)
	CHLOROQUINE PHOSPHATE TABLETS AND AZITHROMYCIN Views: 23 / Sales: 0 Quantity left: Unlimited	Buy Price USD 1,000.00 (0.150423 BTC)
	chloroquine it kill Coronavirus 150pils Views: 20 / Sales: 0 Quantity left: Unlimited	Buy Price USD 500.00 (0.075211 BTC)

Vendors on a dark web market in March 2020 advertise 250 mg Chloroquine pills.

Despite FDA warnings and news of several overdoses from Chloroquine, shortages of the two drugs at U.S. pharmacies were widely reported in March and April. The U.S. Food and Drug Administration issued an emergency use authorization of the drug on March 28. This emergency use authorization simply spurred more dark market vendors to advertise the drug. It was during this time that the TRU research team spotted many ads for Chloroquine pills in both popular English- and Russian-speaking underground markets. They found one vendor advertising 30 Chloroquine pills, each 250 mg, for \$500. Not surprisingly, the same dosage and amount of the drug can be purchased from U.S. pharmacies for between \$111 and \$165, according to [GoodRx](#) (a drug price-comparison platform).

The FDA ended up [revoking the authorization](#) on June 15 after medical trials indicated that the drugs were ineffective and harmful if taken without the oversight of a doctor. Interestingly in July, one dark web marketplace, despite openly selling fentanyl and cocaine, blocked the sale of chloroquine and hydroxychloroquine on their site.

Another drug combination, Lopinavir and Ritonavir, which was initially considered as a possible treatment for COVID-19, was also spotted on the dark web. However, on July 4, the [World Health Organization](#) (WHO) announced that they were no longer trialing the drugs, as their trials showed that the drugs were not effective in treating patients infected with the coronavirus.

The pandemic not only spurred the sale of COVID-19-related medical supplies and medications on the underground, but it also created a perfect opportunity for scammers to plague internet users with malicious phishing scams and websites, which pretend to be news sites providing updates about the virus. According to domain management services company Mark Monitor, over [100,000 website URLs](#) have been registered with COVID-19-themed names since January 2020. While many of them were created for legitimate reasons, thousands have proven to be fraudulent. In March, the FBI Internet Crime Complaint (IC3) reported a 400% increase in the number of complaints, primarily due to messages surrounding the pandemic.

Ritoheet-L (Lopinavir & Ritonavir 200/50 mg) 60 tabs, for cure Covid 19
 Ritoheet-L, manufactured by Mcneil & Argus Pharma. Each of tablet Ritoheet-L contains Lopinavir (200mg) and Ritonavir (50mg)...

Product Class	Features	Origin Country	Features
Quantity Left	Physical Package	Singapore	Singapore
Ends In	Unlimited	Ships to	World Wide
	Never	Payment	Escrow

Singapore Post with tracking 60 pills - 16 days - USD + 17.00 / order

Purchase price: **USD 80.00**

Qty: 1 Buy Now Buy Now Queue

0.008771 BTC / 1.250977 XMR

A dark web merchant advertises that the combination of Lopinavir and Ritonavir is a possible cure for COVID-19.

Coronavirus Covid-19 Scam Shop Script
 We sell full eCommerce shop script for scamming! You need just upload files to server, connect it with stripe account and start rec...

Product Class	Features	Origin Country	Features
Quantity Left	Digital	World Wide	World Wide
Ends In	Unlimited	Ships to	World Wide
	Never	Payment	Escrow

FREE Shipping - 2 days - USD + 0.00 / order

Purchase price: **USD 187.26**

Qty: 1 Buy Now Queue

0.020532 BTC

A cybercriminal promotes their \$187.26 turn-key, COVID-19 malicious script/ scheme to fraudsters so they can run their own phishing scam against unsuspecting internet users.

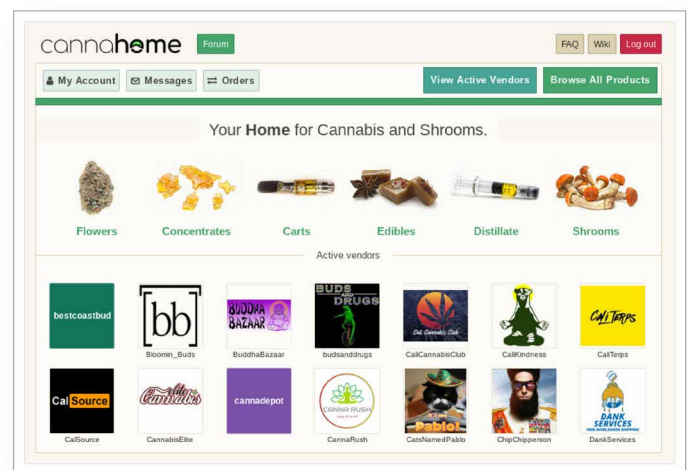
RECREATIONAL DRUGS AND PHARMACEUTICAL DRUGS

Illicit drugs were the first products sold on dark net markets, and today they continue to be the largest category of sales. The United Nations Office on Drugs and Crime's [World Drug Report 2019](#) estimates 35 million people around the world suffer from drug addiction. The size of the global, illicit drug market is estimated to be between \$426 million and \$652 billion.

These marketplaces are the modern frontier in street drug sales, relying on Bitcoin and the U.S. Postal Service. [Featured in popular media](#) such as Vice, these underground markets are depicted as a safer and more consistent model for drug-dealing.

Still, high-profile arrests include two brothers who created a [\\$2.8 million drug business](#) using the dark web. The dark web news source Darknetlive has tracked 443 dark web market vendors who have been arrested since 2011, but only 143 have occurred since 2015. Efforts by the Northern California Illicit Digital Economy Task Force (NCIDETF) and a host of government agencies including the FBI and the Department of Homeland Security have resulted in arrests of large-scale vendors, site administrators, and drug users.

As a result of the COVID-19 pandemic, these virtual drug markets have shown an increase in drug sales, with some vendors reporting increased sales due to shelter-in-place orders and panic buying. Other vendors report a decline in business due to challenges in postal delivery. Recreational drugs are now, more than ever, joined by a growing list of [pharmaceutical drugs](#), both real and potentially counterfeit.



In the U.S. where cannabis for recreational use is legal in only 11 states, the dark market has spawned sites that specialize in cannabis and psychedelics. California's cannabis industry is estimated to be [\\$12.8 billion in 2020](#), with \$8.7 billion flowing through illicit markets.

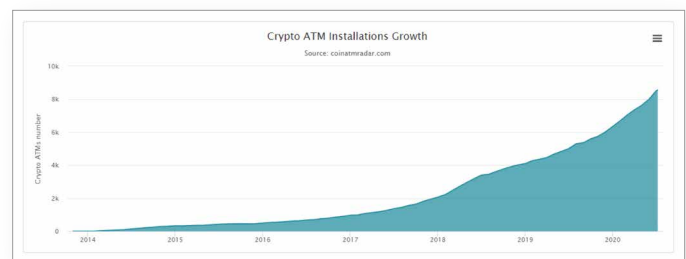
THE STATE OF CRYPTOCURRENCY

Bitcoin, the world's first truly digital currency, saw an initial proof of concept on dark web markets. It introduced a pseudoanonymous way of making purchases, with a form of money that was based on cryptography, was faster than wire transfers, and was not tied to any government monetary system or central bank—de facto digital cash. Starting with CryptoLocker in 2013, modern ransomware schemes began demanding Bitcoin as payment from victims, dramatically changing the cybercrime landscape.

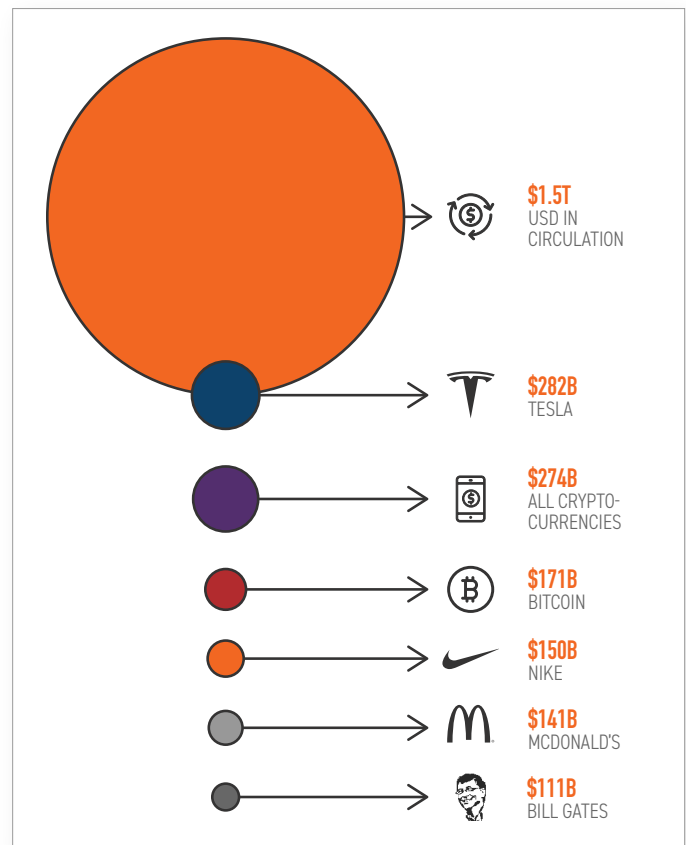
But Bitcoin is not the only cryptocurrency; today it is one of over 5,000. The sale and purchase of bitcoin and other cryptocurrencies continue to be largely obscured, as trading is often conducted on over 20,000 exchanges worldwide, many of which are decentralized, virtual, and require little or no user identification.

Bitcoin is also not the most anonymous, as its open ledger of transactions is available for all to see. Each movement of even the smallest unit of bitcoin (.00000001 or one Satoshi) is tracked, allowing for a variety of forensic techniques by companies such as Chainalysis to help determine ownership or find other transaction details. A number of Bitcoin Tumblr services and techniques exist to thwart those forensic efforts, and cryptocurrencies such as Monero and Dash offer anonymity features beyond those found in Bitcoin. In addition to Bitcoin, cryptocurrencies Monero, Dash, ZCash and Litecoin are all used to purchase goods on dark marketplaces.

One factor responsible for the increased activity on markets and the adoption of cryptocurrencies is the increased number of Crypto Teller Machines (CTMs, a.k.a. Cryptocurrency ATMs). Today there are over 8,000 CTMs worldwide, with over 6,000 located in the U.S.



The growth of Cryptocurrency ATM machines helps drive adoption. [Source: Coin ATM Radar.](#)



The size of the cryptocurrency market compared to the size of other markets.

CONCLUSION

Dark, underground, or shadow economy markets have been in existence for decades. They rise and fall with world events, filling demand for goods and services that might otherwise be unavailable, and unfortunately, they attract many people who are not interested in earning a legitimate living. Dark web markets are no different, but they present new challenges.

Following the U.S.'s Great Recession, which ran between December 2007 and June 2009, the U.S. shadow economy grew to an estimated 5.4% of Gross Domestic Product (GDP) or \$2.7 trillion. Following times of economic turmoil, including recessions, wars, or natural disasters, shadow economies thrive. Armor believes this will hold true for dark web markets as cybercriminals are motivated by economic uncertainty, emboldened by the success of recent cyberattacks, and obscured by the chaos of a global pandemic. Thus, it is more important than ever for organizations and individuals to implement proven and comprehensive security practices. The TRU team recommends the following cybersecurity protections for organizations and individuals.

CYBER PROTECTIONS FOR IT AND SECURITY TEAMS

- Train your employees on how to identify suspicious activity, phishing emails, etc.
- Find, classify, and protect your most sensitive data, particularly information impacted by compliance regulations such as PCI-DSS and HIPAA.
- Deploy patches as promptly as possible to shorten the vulnerability window.
- Employ data encryption to protect sensitive data in transit and at rest.
- Monitor cloud usage, manage access to cloud services, and secure any data or applications you migrate.
- Use security technologies such as firewalls, anti-malware software, and intrusion detection and prevention systems to build a shield around your environment.
- Implement multi-factor authentication when providing access to your most critical systems. This provides an extra layer of security to prevent unauthorized access.
- Use offline backup storage. We can't stress this enough. Users must have backups of their data, which is air-gapped from the internet. Ensure all critical data, applications, and application platforms are backed up and password-protected.

CYBER PROTECTIONS FOR INDIVIDUALS

- Do not click on suspicious links or open email attachments from unknown senders.
- Use anti-malware software.
- Update your software regularly for security patches.
- Be cautious accessing online banking sites, email, or other sensitive sites when using public Wi-Fi hotspots. Many of them lack strong security and can leave you susceptible to attacks.
- Do not use the same password for multiple websites or services and allow a single compromised account to turn into many.
- Consider using credit and financial account monitoring services to detect suspicious activity.

Click here to see how Armor protects your data: <https://www.armor.com/demo/>



[ARMOR.COM](https://armor.com) | (US) +1 844 682 2858 | (UK) +44 800 500 3167

20030923 Copyright © 2020 Armor, Inc., All rights reserved.