

North American Underground

The Glass Tank

Kyle Wilhoit and Stephen Hilt

Forward-Looking Threat Research (FTR) Team

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

4

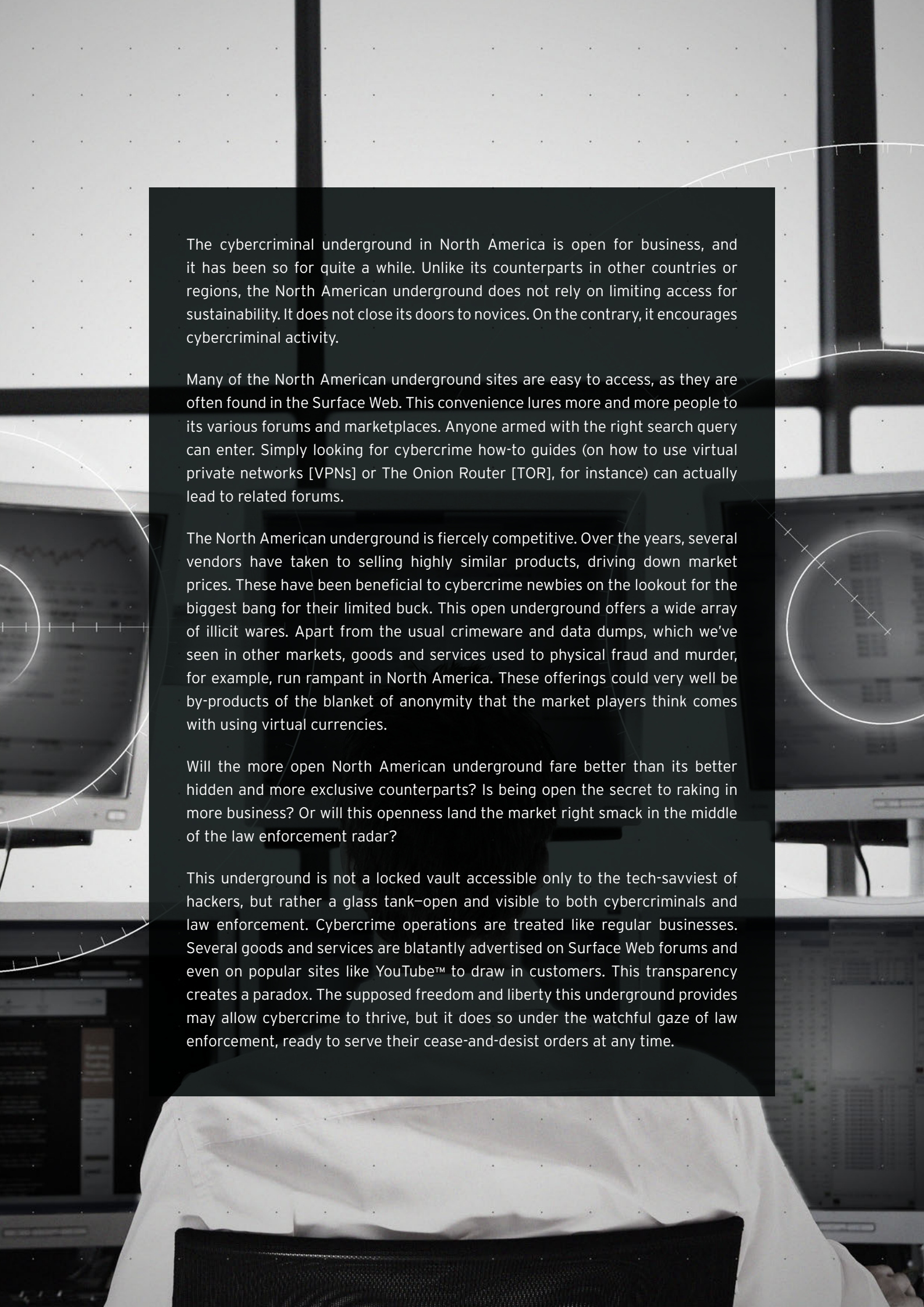
North American
underground wares

27

The future of the
North American
underground

29

Appendix



The cybercriminal underground in North America is open for business, and it has been so for quite a while. Unlike its counterparts in other countries or regions, the North American underground does not rely on limiting access for sustainability. It does not close its doors to novices. On the contrary, it encourages cybercriminal activity.

Many of the North American underground sites are easy to access, as they are often found in the Surface Web. This convenience lures more and more people to its various forums and marketplaces. Anyone armed with the right search query can enter. Simply looking for cybercrime how-to guides (on how to use virtual private networks [VPNs] or The Onion Router [TOR], for instance) can actually lead to related forums.

The North American underground is fiercely competitive. Over the years, several vendors have taken to selling highly similar products, driving down market prices. These have been beneficial to cybercrime newbies on the lookout for the biggest bang for their limited buck. This open underground offers a wide array of illicit wares. Apart from the usual crimeware and data dumps, which we've seen in other markets, goods and services used to physical fraud and murder, for example, run rampant in North America. These offerings could very well be by-products of the blanket of anonymity that the market players think comes with using virtual currencies.

Will the more open North American underground fare better than its better hidden and more exclusive counterparts? Is being open the secret to raking in more business? Or will this openness land the market right smack in the middle of the law enforcement radar?

This underground is not a locked vault accessible only to the tech-savviest of hackers, but rather a glass tank—open and visible to both cybercriminals and law enforcement. Cybercrime operations are treated like regular businesses. Several goods and services are blatantly advertised on Surface Web forums and even on popular sites like YouTube™ to draw in customers. This transparency creates a paradox. The supposed freedom and liberty this underground provides may allow cybercrime to thrive, but it does so under the watchful gaze of law enforcement, ready to serve their cease-and-desist orders at any time.



SECTION 1

North American
underground wares

North American underground wares

The North American Underground primarily caters to customers within the region—users based in the United States (US) and Canada. Unsurprisingly, most of the offerings (stolen accounts, products and services, and fake documents) are US based. This is consistent with what we see in the Japanese¹ and Brazilian² undergrounds and suggests that US-based information is most sought after in it.

We classified the goods and services found in the North American underground into three major groups—crimeware, stolen data dumps and fake documents, and drugs and weapons.

Crimeware

Hacking tools

We found several North American forums that solely sell hacking tools. These wares are considered basic essentials in any underground market—keyloggers, spamming tools, remote access tools (RATs), and botnets.

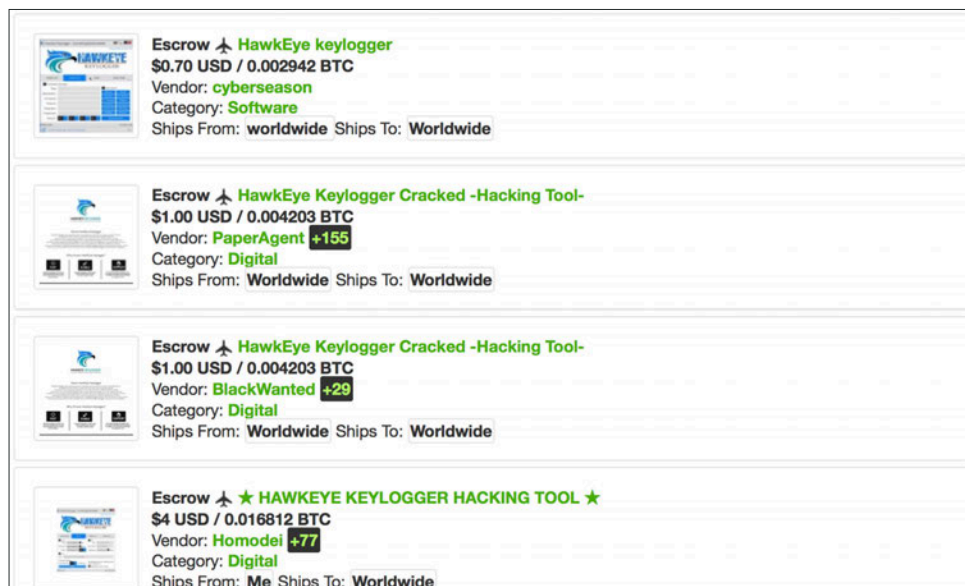


Figure 1: HawkEye, a keylogger, is sold for US\$1–4

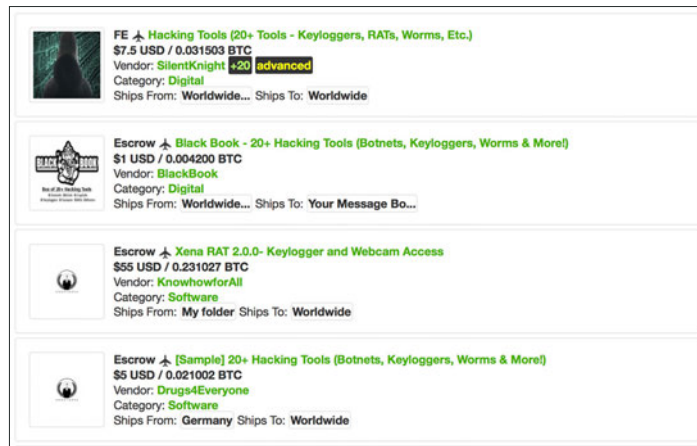
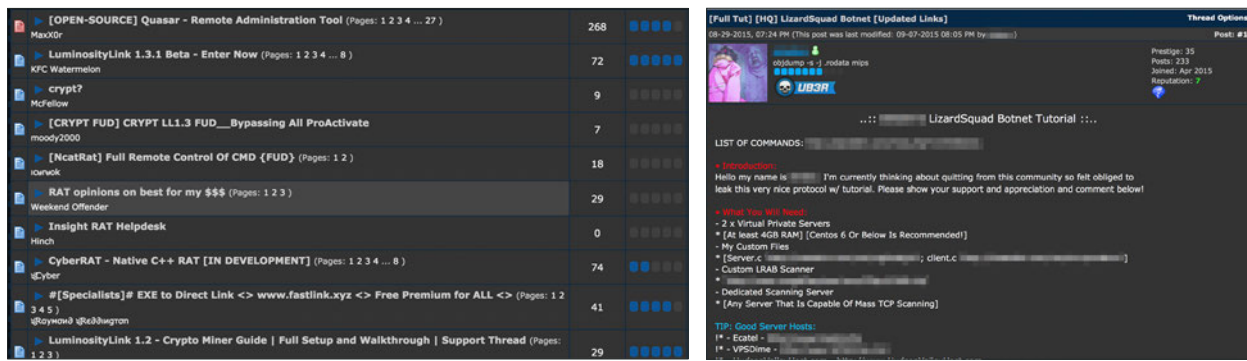


Figure 2: RATs, crypting services, and even botnet and Silk Road 3.0 access tutorials abound in the North American underground

In most cases, malware bought include technical support from their developers. The Xena RAT Builder, for instance, can be purchased with any of two service packages—Silver or Gold. The Gold package comes with crypting services to ensure that the malware the kit creates would be fully undetectable (FUD).



Figure 3: Xena RAT Silver and Gold package offerings

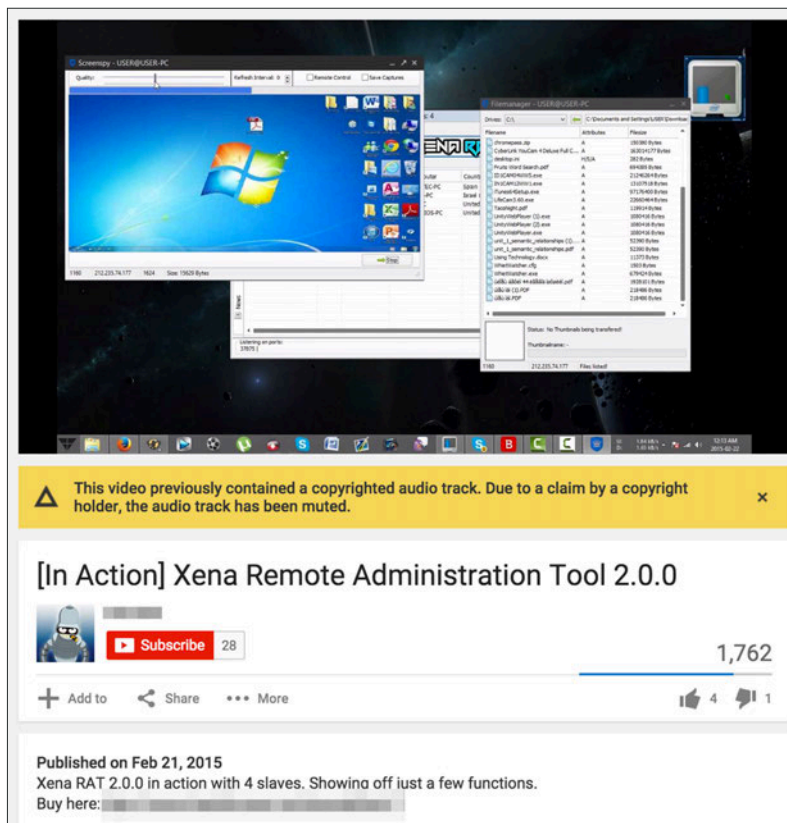


Figure 4: YouTube video showing off Xena's various features

Offering	Price
Keylogger	US\$1–4
Xena RAT builder	US\$1–50
Exploit	US\$1+ (depending on complexity)
Botnet and/or botnet builder	US\$5–200
Worm	US\$7–15
Ransomware	US\$10
Betabot DDoS tool	US\$74

Table 1: *Crimeware often found in the North American underground*

BPHSs

Any cybercriminal endeavor is built upon the use of bulletproof hosting services (BPHSs)³ to ensure smooth and undetected operation. BPHS providers allow users to store anything, including malicious content like phishing sites, pornographic materials, and command-and-control (C&C) infrastructure. As such, many major cybercriminal groups would not be able to operate without the aid of BPHSs with legitimate business fronts that shield them from the prying eyes of law enforcement.

Various BPHS offerings can be found in the North American underground. Custom BPHS tailored to specific needs can be obtained for US\$75 per month. This comes with a single Internet Protocol (IP) address and 100GB of hard disk drive (HDD) space on a machine with a 2GB random-access memory (RAM). Note though that basic access to a bulletproof server can also be obtained for as low as US\$3 a month.



Figure 5: *Ad for customized BPHS priced at US\$75 per month*



Figure 6: Ad for a Russian-based BPHS provider, touting the seller’s success in hosting botnets, RATs, exploits, spamming tools, fraud forums, and pornographic content

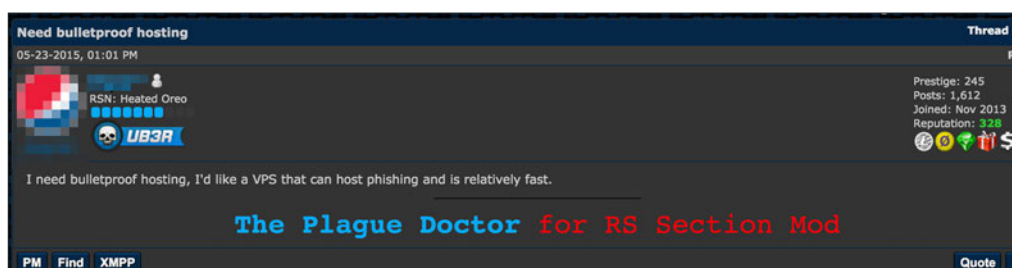


Figure 7: Post made by a user looking for a BPHS provider

Crypting services

Crypting services, arguably the most sought-after crimeware in the North American underground to date, obfuscate malware binaries’ creation dates and other malicious components. All customers need to do is send their malware to service providers who then check them against all standard anti-malware tools available in the market. Crypting service providers check how many products flag the code “malicious.” They then encrypt the malware as many times as it takes until these are no longer detected.

Crypting service offerings vary though most providers encrypt files designed to run on Windows® XP, 7, and 8 and Windows Server 2003 and 2008, among others. These are generally affordable and criminals buying in bulk even get discounts. Typical customers include those on the lookout for cost-effective ways to evade detection via anti-malware, firewalls, and intrusion detection and prevention systems (IDSs/IPSs).

<i>SINGLE</i>	<i>DAILY</i>	<i>WEEKLY</i>	<i>MONTHLY</i>
\$ 20	\$ 65	\$ 300	\$ 1000
* free customer service	* free customer service	* free customer service	* free customer service
API Support	API Support	API Support	API Support
Single crypt	Unlimited crypts	Unlimited crypts	Unlimited crypts
Single file	Unlimited files*	Unlimited files*	Unlimited files*
both checkers free	AV results from both checkers	AV results from both checkers	AV results from both checkers

Figure 8: Ad for one-time, daily, weekly, and monthly crypting services that usually come with application programming interface (API) support with prices ranging from US\$8 per file to US\$1,000 per month for use on an unlimited number of files

VPNs and proxies

VPNs and proxies are crucial cybercrime tools, as they are the best means to conceal criminal communications and anonymize identities.

VPNs encrypt all the data sent and received within them while proxy servers reroute traffic from one IP address to another so it looks like it's coming from a computer other than the real source. VPNs and proxies thus help facilitate anonymous connectivity and communication.

Most criminals seeking complete anonymity fear that reputable VPN service providers keep track of and log account activity. As such, many of their peers offer anonymous VPN or proxy server access for an average price of US\$102 per year.

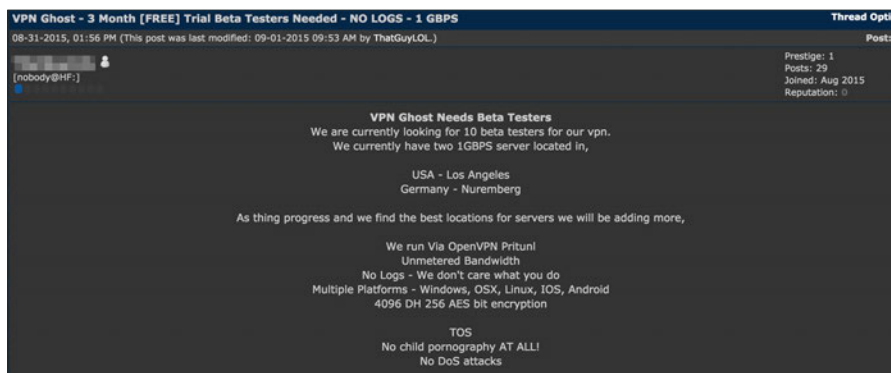


Figure 9: VPN access with unmetered bandwidth, guaranteed no activity logging, and works across platforms

DDoS attack or Web-stressing services

Distributed denial-of-service (DDoS) or Web-stressing attacks are a common component of cybercrime arsenals. DDoS offerings are, in fact, an underground staple available at fairly affordable prices.

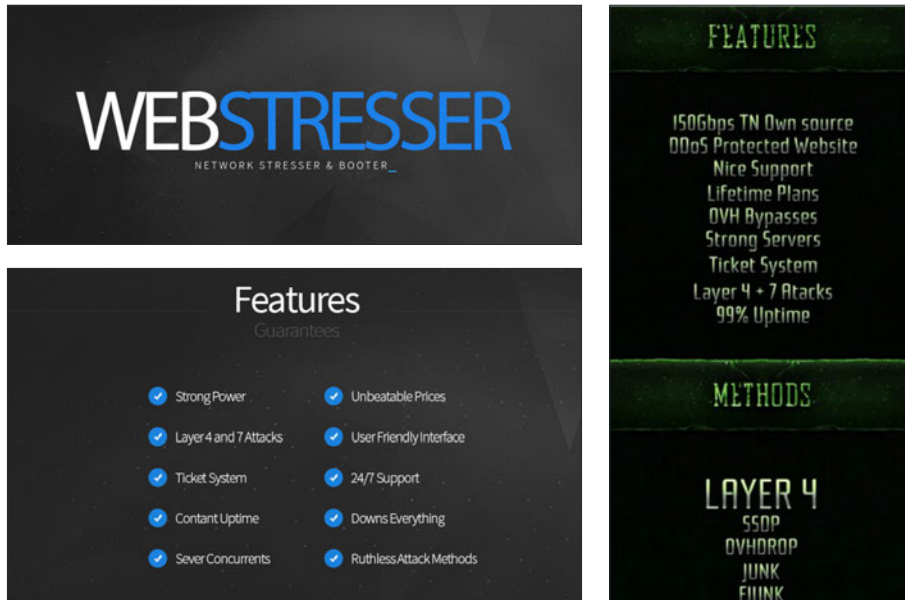


Figure 10: Various DDoS attack and Web-stressing services available in the North American underground

Premium Web-stressing services boast of as much as 300GBps DDoS traffic attack capabilities that users can use on their intended victims.

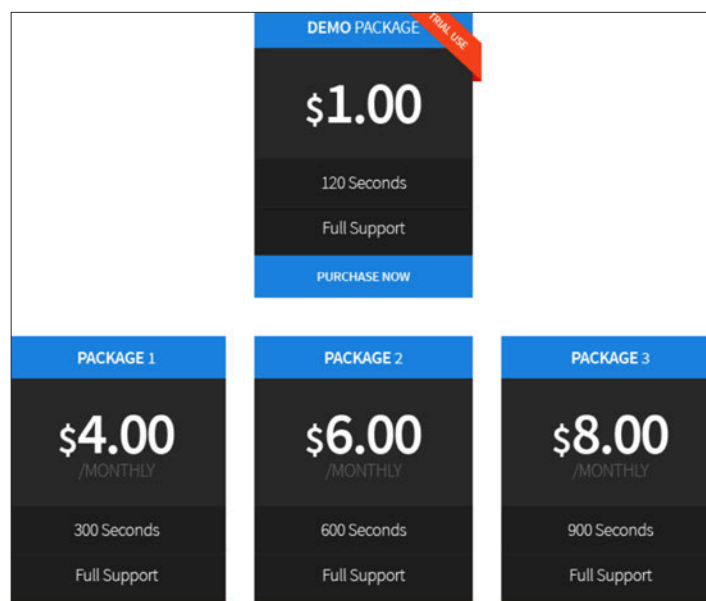


Figure 11: DDoS attack service packages available in the North American underground

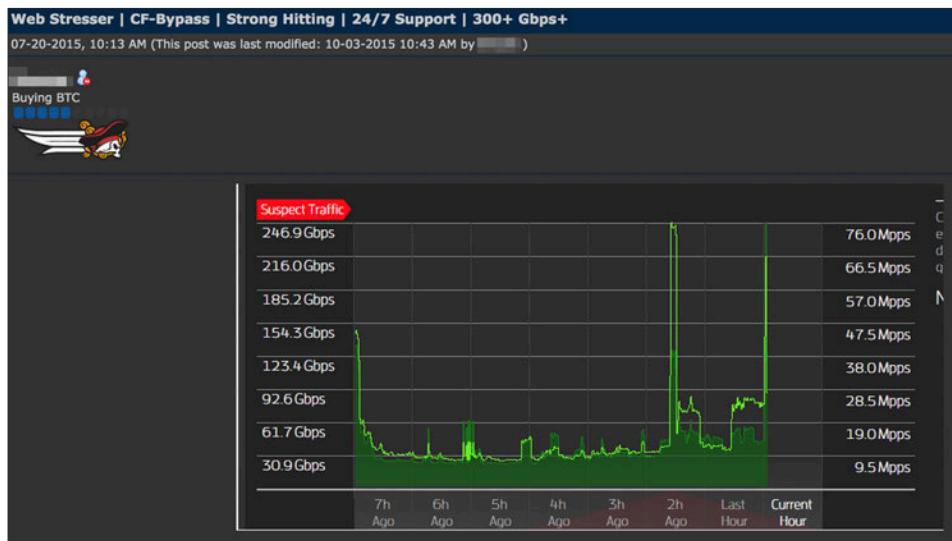


Figure 12: Post touting proof of a provider’s DDoS attack service capabilities

Offering	Price
40GBps for 300 seconds	US\$5
70GBps for 300 seconds	US\$9
40GBps for 2,700 seconds	US\$25
125GBps for 300 seconds	US\$25
70GBps for 7,200 seconds	US\$30
125GBps for 2,000 seconds	US\$60

Table 2: DDoS attack and Web-stressing services available in the North American underground

Access to compromised sites

Access to compromised sites, including via Remote Desktop Protocol (RDP), is also a notable North American underground offering. The prices of such services vary, depending on type. Sellers offer access to a single compromised site, multiple sites, and even full root access to servers.

Cybercriminals often use compromised sites or servers to distribute malware. These sites or servers act as jump-off proxies to launch attacks on chosen sites or servers.

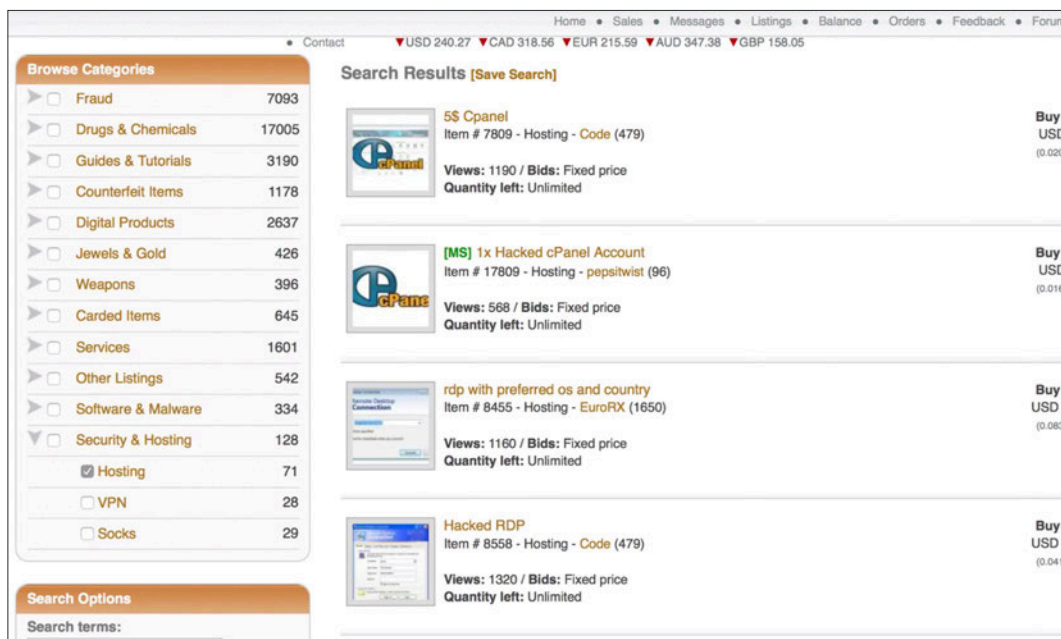


Figure 13: Cpanel sold for US\$4–10 that can be used for RDP access; available for US\$20 if customized with buyer’s operating system (OS) and target country preferences

RDP access tools generally sell for US\$10–25, depending on the intended target region, victim type, and access rights. Access to hacked site management portals (Cpanel) ranges from US\$3–5.

Stolen data dumps and fake documents

Stolen credit card credentials and clones

Cybercriminals go underground if they wish to monetize stolen data. They most commonly sell information like credit card credentials. But credentials are not the only credit-card-related goods found in cybercriminal markets. Clones or copies of stolen credit cards also abound.

Selling credit card clones is quite common in the North American underground though we weren’t able to find posts that detailed how these were used. Buyers, however, showed a preference for credit card credentials than clones since the latter brought risks of actually getting caught red-handed.

Credit-card-related offerings varied in price, depending on reliability, anonymity (pre-, during, and post-sales), issuing country, and credit limit. Most goods available for purchase were issued in the US, Canada, or European countries.

CCSale Home Price & Order F.A.Q. Contact

Price and order

HOW DO I PLACE AN ORDER?
 To place an order We will need few things from you:
 1)The balance range you want. (Check price list below)
 2)The number of cards you want.(Discount on bulk orders)
 3)We will calculate your order value and get back to you as soon as possible.
 4)Then, we will tell you a secure way of sending us your shipping address.
 5)And then we feed you with payment details.

WHAT ARE THE PRICES OF CARDS?

US
 Balance between \$2000-\$2999 for \$250
 Balance between \$3000-\$3999 for \$350
 Balance between \$4000-\$4999 for \$450
 Balance between \$5000-\$5999 for \$550
 Balance between \$6000-\$6999 for \$650
 Balance between \$7000-\$7999 for \$750
 Balance between \$8000-\$8999 for \$850

EU
 Balance between 2000EUR-2999EUR for 270EUR
 Balance between 3000EUR-3999EUR for 370EUR
 Balance between 4000EUR-4999EUR for 470EUR
 Balance between 5000EUR-5999EUR for 570EUR
 Balance between 6000EUR-6999EUR for 670EUR
 Balance between 7000EUR-7999EUR for 770EUR
 Balance between 8000EUR-8999EUR for 870EUR

DO YOU HAVE CARDS WITH HUGE BALANCES, OTHER THAN THE ONE LISTED ABOVE?
 Yes we do, but most at times we keep those cards to ourselves.Feel free to ask

FOR FURTHER QUESTIONS AND ENQUIRY, CONTACT US

CONTACT INFO

Figure 14: Ad for credit-card-related offerings in a popular marketplace

Offering	Price
Classic US-issued credit card credentials	US\$19–22 (100 sets)
Gold, Platinum, or Business US-issued credit card credentials	US\$36–42 (50 sets)
Classic Canada-issued credit card credentials	US\$47–50 (40 sets)
Gold, Platinum, or Business Canada-issued credit card credentials	US\$50–65 (35 sets)
Fake US-issued credit card (physical)	US\$210–874

Table 3: Credit-card-related offerings in the North American underground

Europay, MasterCard, and Visa (EMV) standard-adhering and chip-and-personal identification number (PIN) (technology recently declared a European, US, and Canadian standard) cards and related goods are commonly sold in the North American underground. These generally cost US\$30–40 more than normal (non-EMV and -chip-and-PIN) cards.

The cards have balances between 800 and 1300 USD or EUR depending on weather you get a chipped card or plain magnetic stripe card.

If you're ordering within the US, regular magnetic cards will work fine, if you're ordering out of any european country we advise you buy our chipped cards as chipped cards are required for authorization in all european countries and many others.

The price brackets(discounts) for the cards are below, if you wish to order more than 20 cards, just ask and we'll give you a price.

MAGNETIC CARDS		CHIPPED CARDS	
• (1) One Card	• \$110 USD	• (1) One Card	• \$145 USD
• (3) Three Cards	• \$290 USD	• (3) Three Cards	• \$380 USD

Figure 15: Users who buy cards with US\$800–1,300 remaining balances that work in the US and European countries in bulk (more than 20 cards in a single purchase) get discounts




	<p>FE ✈️ FRESH CC/CVV FROM USA VISA/MASTER/DISCO... \$14.00 USD / 0.058483 BTC Vendor: 609austin14 +585 advanced Category: Money Ships From: Unknown Anime Land Ships To: Worldwide</p>
	<p>Escrow ✈️ Carding CC to BTC in 5 steps (NEW) \$6 USD / 0.025064 BTC Vendor: etimbuk +1195 Category: Money Ships From: Me Ships To: Worldwide</p>
	<p>Escrow ✈️ 2X USA FULLZ- SSN-DOB-BANK INFO ETC I g... \$2.50 USD / 0.010443 BTC Vendor: CarderPro95 +80 Category: Money Ships From: Virtual message Ships To: Worldwide</p>

Figure 16: Posts by sellers of stolen credit card information

Credit-card-related offerings often come with a disclaimer. Not all of the credentials in a dump bought will work. Users who buy 100 sets of credentials, for instance, are guaranteed the use of at least 15 cards or they can get their money back.

Online account credentials

Stolen online account credentials also abound in the North American underground. Cybercriminals hack Spotify and Netflix accounts then sell access to these. Buying such wares allows users access to the services of their choice for a fraction of the legitimate price as long as the compromised account owners don't change their passwords.

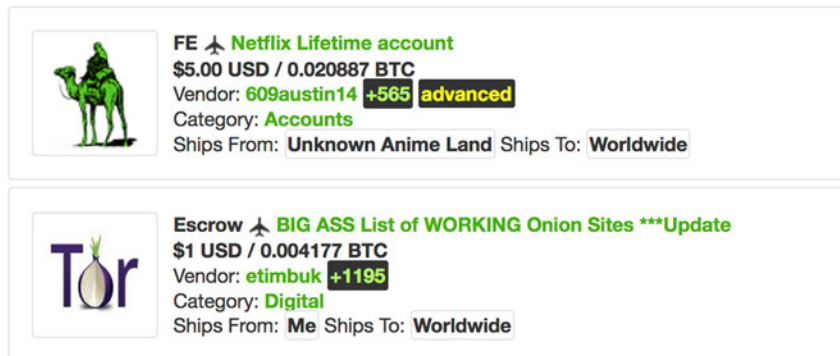


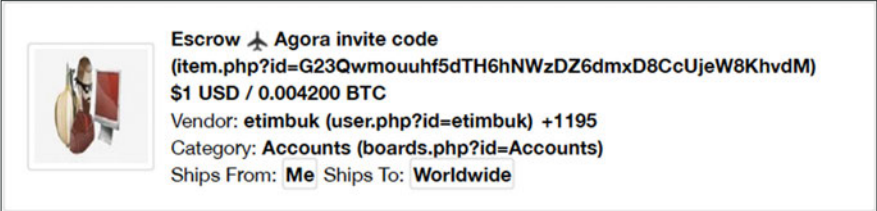
Figure 17: Netflix lifetime-access account sold for US\$5 (cheaper by ~US\$3–4 compared with legitimate service offerings)

Origin, Spotify, and Hulu account access sells for very cheap prices. Access to Beats Music accounts is also sold at very low prices. We expect these offerings to disappear soon, as the service is no longer available.

Offering	Price
Origin account access	Less than US\$1
Spotify account access	US\$2
Beats Music account access	US\$2
Hulu Plus account access	US\$4
Netflix account access	US\$5
Dish Network Anywhere account access	US\$7
Luminosity account access	US\$7
Verified PayPal account access	US\$9
Sirius Satellite Radio account access	US\$15

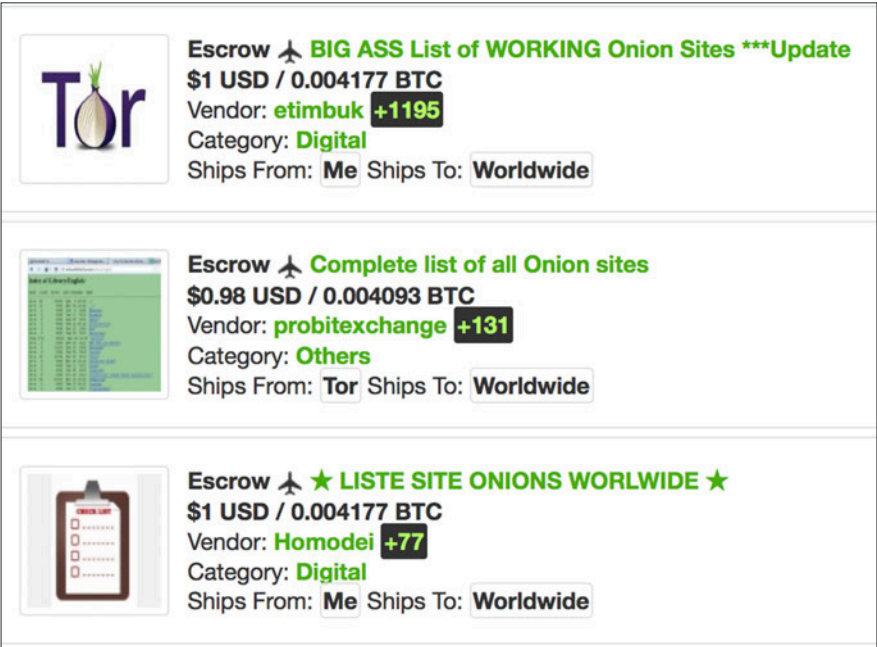
Table 4: Stolen online account access offerings in the North American underground

Interestingly, access to North American underground forum accounts is also sold. Most of the forums these are associated with are closed environments and require invitations or access fees. These forums filter users to ensure the safety of already-existing members.



Escrow ✈️ **Agora invite code**
(item.php?id=G23Qwmouuhf5dTH6hNWzDZ6dmxD8CcUjeW8KhvdM)
\$1 USD / 0.004200 BTC
Vendor: **etimbuk** (user.php?id=etimbuk) +1195
Category: **Accounts** (boards.php?id=Accounts)
Ships From: **Me** Ships To: **Worldwide**

Figure 18: Ad selling an invitation code to Agora, a popular underground forum, for US\$1



Escrow ✈️ **BIG ASS List of WORKING Onion Sites ***Update**
\$1 USD / 0.004177 BTC
Vendor: **etimbuk** +1195
Category: **Digital**
Ships From: **Me** Ships To: **Worldwide**

Escrow ✈️ **Complete list of all Onion sites**
\$0.98 USD / 0.004093 BTC
Vendor: **probitexchange** +131
Category: **Others**
Ships From: **Tor** Ships To: **Worldwide**

Escrow ✈️ **★ LISTE SITE ONIONS WORLDWIDE ★**
\$1 USD / 0.004177 BTC
Vendor: **Homodei** +77
Category: **Digital**
Ships From: **Me** Ships To: **Worldwide**

Figure 19: Posts touting access to a wide array of .onion sites for US\$1 each

Fake documents

Identity theft accounts for a huge chunk of the North American underground economy. This isn't limited to stealing access to victims' credit cards and online accounts. A market for fake identification (ID) cards and documents also exists. Buyers (mostly illegal aliens and criminals) flock underground in search of documents to support citizenship claims or applications, obtain lines of credit to put up a business, open untraceable bank accounts, prove their residence status, commit insurance fraud, and purchase illicit items that require valid IDs, among others.

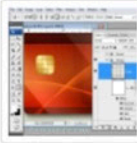



	<p>Escrow ✈️ 13GB of PSDs - Fake bills, Scans, Passports, DL & \$1 USD / 0.004177 BTC Vendor: Homodei +77 Category: Digital Ships From: Me Ships To: Worldwide</p>
	<p>Escrow ✈️ ★ FRENCH Passport Scan ★ \$5 USD / 0.020887 BTC Vendor: Homodei +77 Category: Digital Ships From: Me Ships To: Worldwide</p>
	<p>Escrow ✈️ Custom United States Passport Scan, Any Details \$30 USD / 0.125322 BTC Vendor: kingscan +9 Category: Counterfeit Ships From: PM Ships To: Worldwide</p>
	<p>FE ✈️ ☆-- USA Passport & Passport Card Template --☆ \$10 USD / 0.041774 BTC Vendor: z0mbie666 +20 advanced Category: Counterfeit Ships From: Online Ships To: Worldwide</p>

Figure 20: Forum posts selling fake passports



<p>Main News Services Samples faq Order Contacts</p>  <p>Welcome to BuyPassportsFake.cc - the unique producer of quality fake documents. We offer only original high-quality fake passports, driver's licenses, ID cards, VISA, stamps and other products for following countries: Australia, Belgium, Brazil, Canada, Finland, France, Germany, Ireland, Italy, Netherlands, Norway, Spain, Sweden, Switzerland, UK, USA and some others.</p> <p>If you want to learn more about what kinds of documents can be found in our website please visit the sections "Services" and "Samples". You can find more details about ordering procedure and additional details visiting the sections "FAQ" and "Order".</p> <p>© 2008-2014 Copyright BuyPassportsFake.cc For entertainment only. Not a government document. Terms and Conditions</p>	<p>Main News Services Samples faq Order Contacts</p>  <p>Passports:</p> <ul style="list-style-type: none"> PASSPORT ROYAUME DE BELGIQUE / KONINKRIJK BELGIË REPÚBLICA FEDERATIVA DO BRASIL CANADA / PASSEPORT BURROOPAN UNIONEN / EUROPEISKA UNIONEN SUOMI / FINLAND / PASSEPORT Union européenne / République française
--	---

Figure 21: Underground marketplace for fake passports from various countries

Counterfeit documents are also widely available. These are also known as “manufactured documents” and are completely falsified. They typically use the personal information of deceased individuals. They can also be crafted using information provided by the buyers.

Offering	Price
Canadian passport scan	US\$17–24
UK passport scan	US\$28
US passport scan	US\$30
Counterfeit US auto insurance card	US\$38
US driver’s license scan	US\$145
Counterfeit Canadian driver’s license	US\$630
Counterfeit Canadian passport	US\$670
Counterfeit UK driver’s license	US\$700
Counterfeit UK passport	US\$730
Counterfeit US driver’s license	US\$727
Counterfeit US passport	US\$780

Table 5: Fake documents sold in the North American underground
(Note that prices vary, depending on the document quality but also on the buyer’s nationality.)

Drugs and weapons

Drugs

Among the original purposes for establishing North American underground forums was to enable the sale of illegal drugs and paraphernalia. While they have moved far past selling drugs, these are still a core product in many underground forums.

Individuals involved drug-related transactions often hope to retain their anonymity. As such, many underground forums use code to conceal what they are looking for or selling. Some sell drugs in the guise of food. Cannabis-infused peanut butter cups, for instance, are openly advertised in many forums.





	<p>FE ✈️ 1g 90% purity Coke \$85 USD / 0.355079 BTC Vendor: Bird +128 advanced Category: Cocaine Ships From: Spain Ships To: Worldwide</p>
	<p>FE ✈️ 1g --- Blue Cheese --- Organic \$19 USD / 0.079370 BTC Vendor: boomers +5 advanced Category: Weed Ships From: United Kingdom Ships To: Worldwide</p>
	<p>Escrow ✈️ x10 Methylphenidate XL 18mg (Concerta/Ritalin) \$70 USD / 0.292418 BTC Vendor: mrshah +139 verified Category: Weed Ships From: United Kingdom Ships To: Worldwide</p>
	<p>Escrow ✈️ 1g HIGH QUALITY indica. Free p+p. UK only \$19.08 USD / 0.079704 BTC Vendor: Shadow +605 verified advanced Category: Weed Ships From: United Kingdom Ships To: United Kingdom</p>

Figure 22: Forum posts selling all kinds of drugs

Since drug sales involve sending and receiving physical items (as opposed to virtual wares or digital information), transactions that occur in the North American underground involves several steps to keep both buyers' and sellers' anonymity.

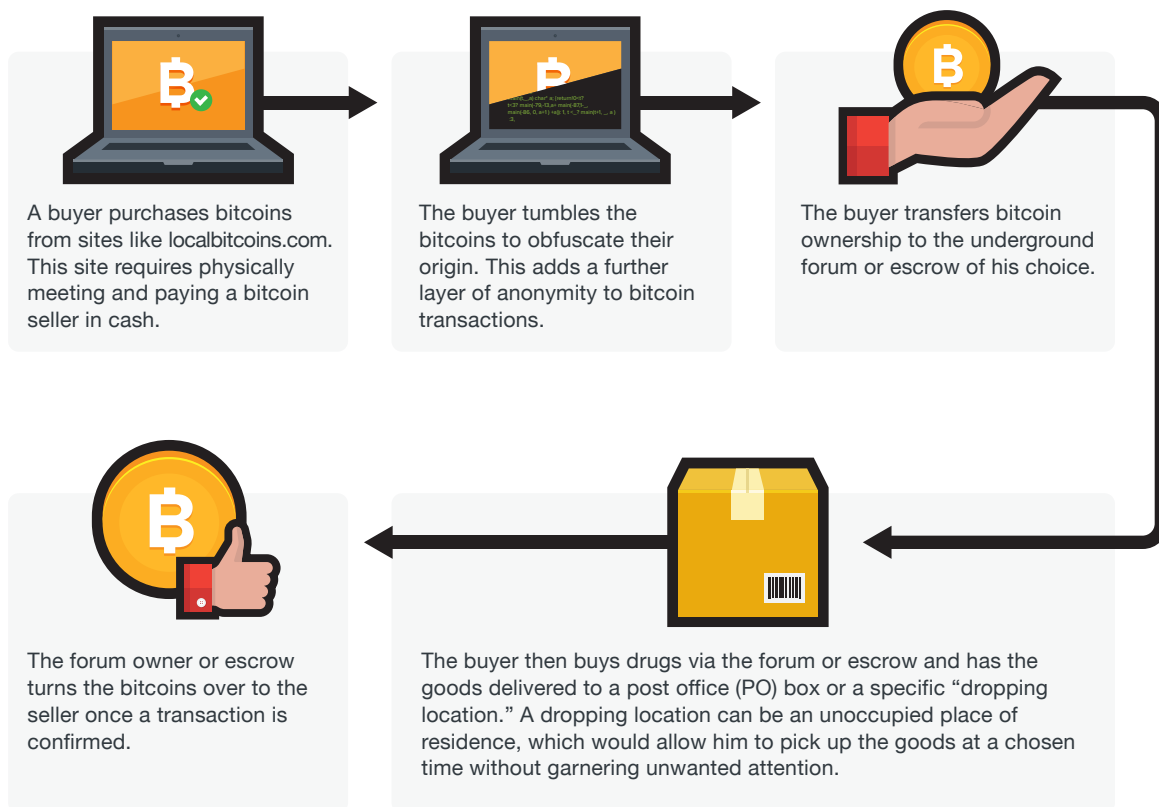


Figure 23: Sample drug transaction flow

(Bitcoin tumbling, also known as "bitcoin mixing" or "bitcoin laundering," is the process of using a third-party service to break a connection between a sender's and receiver's addresses⁴. Since the bitcoin blockchain is a public ledger that records every transaction, mixing coins is critical for anyone who doesn't want the entire world to know exactly where he sends/receives bitcoins to/from.)

Apart from actual drugs, forged prescription labels for use in the US are also gaining traction. We saw posts selling fake prescription labels for establishments like Walgreens, CVS, and Walmart. These labels can help addicts evade arrest if they are caught in possession of prescription drugs.

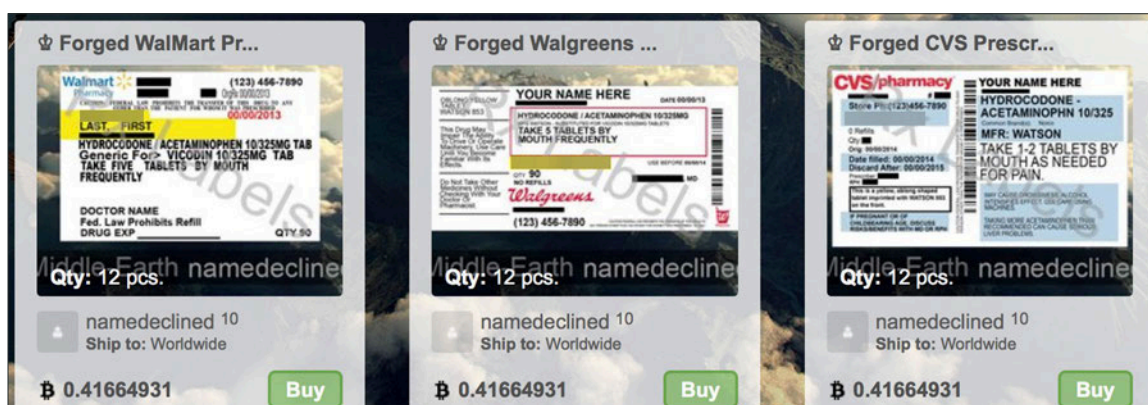



Figure 24: Forged prescription labels for use in the US

Offering	Price
Blue cheese marijuana	US\$19 per gram
THC vape oil	US\$24 per cartridge
Sharif hash	US\$53 per 5 grams
Valium	US\$66 per 75 pills
High-quality Bolivian cocaine	US\$69 per gram
Methylphenidate (18mg)	US\$70 per 10 pills
Clonazepam	US\$71 per 100 tablets
MMDA	US\$86 per pill
Counterfeit CVS, Walgreens, or Roland prescription labels	US\$100 per 3 labels
Methamphetamine	US\$136 per gram
Afghan heroin	US\$209 per gram

Table 6: *Drugs and related goods sold in the North American underground*

Apart from actual drugs, guides on producing them or the tools needed to do so are also available. We found a guide for making crack, for instance, sold for a mere US\$5.



How To Make Crack and Freebase Cocaine

How To Make Crack and Freebase Cocaine tutorial crack freebase cocaine coke coca crack freebase cocaine coke coca crack freebase cocaine coke coca crack freebase cocaine coke coca crack freebase cocaine coke coca crack freebase cocaine coke coca

Vendor [fake \(2508\)](#) **Price** ~~฿~~0.02090126 **Location** PM(site messages)

Figure 25: *How-to guide for making crack*

Weapons

Weapons ranging from batons to high-powered guns are offered in the North American underground. We found a Midwest-based seller peddling handguns, shotguns, rifles, and all kinds of ammunition. We also came across forums dedicated to selling batons and all sorts of knives.

The screenshot shows a marketplace interface with a sidebar on the left and search results on the right. The sidebar, titled "Browse Categories", lists various categories with their respective item counts. The "Weapons" category is selected and expanded, showing sub-categories like Ammunition, Pistols, Long-Range Guns, Explosives, Hand Weapons, and Other. Below the sidebar is a "Search Options" section with a "Search terms:" input field. The main area, titled "Search Results [Save Search]", displays five search results for items sold by a user named "markedone". Each result includes a small image of the item, the item name, item number, views, bids, and price information.

Item Name	Item #	Views	Bids	Price
[MS] [Bulk] iPhone Stun Gun (Taser)	Item # 744 - Other - markedone (206)	5185	Fixed price	USD 27.76 (0.1154 BTC)
[MS] [Bulk] Telescopic Baton	Item # 755 - Other - markedone (206)	2055	Fixed price	USD 22.19 (0.0922 BTC)
[MS] [Bulk] CS-Gas (Pepperspray)	Item # 754 - Other - markedone (206)	1694	Fixed price	USD 8.86 (0.0366 BTC)
[MS] [Bulk] Butterfly Knife (Balisong)	Item # 751 - Other - markedone (206)	2461	Fixed price	USD 22.19 (0.0922 BTC)
[MS] [Bulk] Knuckle Duster (Black)	Item # 749 - Other - markedone (206)	2082	Fixed price	USD 16.63 (0.0691 BTC)

Figure 26: Stun guns and batons advertised in the North American underground

Weapons marketplaces often had foreign contacts and so could deliver goods outside North America. We found one such seller capable of shipping (through partners) to Canada, Australia, the United Kingdom (UK), Germany, and Russia.

Home Order & Delivery Payment About Us Contacts

CATEGORIES

- Handguns
 - .22LR
 - 25ACP
 - 32ACP
 - .38 Special
 - 380ACP
 - 40S&W
 - 45ACP
 - .357 Magnum
 - 9mm
- Rifles
 - 22 LR
 - .50 Cal
 - 5.56x45mm
 - 7.62x39mm
 - 7.62x51mm NATO
- Shotguns
 - 12 Gauge
- Ammo

MANUFACTURERS





- Beretta
- Browning
- Bushmaster
- Glock
- Kel-Tec

All manufacturers

Our shop and warehouses are located in the Midwest US, and International Reshippers are located in the following countries:

Canada Australia United Kingdom Germany Russian Federation

FEATURED PRODUCTS

			
Ruger MINI-14/20	Bushmaster M4-A3 Type...	Browning 1911-22 A1	Ruger SR22PB
View > \$1,250.00	View > \$1,769.00	View > \$878.00	View > \$618.00

100% SUCCESS RATE. MONEY BACK GUARANTEE. ONLY 40% PREPAYMENT. FREE SHIPPING. 100% SECURE PAYMENT PROCESSING.

CATEGORIES **MY ACCOUNT**

- Handguns My orders
- Rifles My credit slips

Figure 27: Weapons available for shipping outside the US

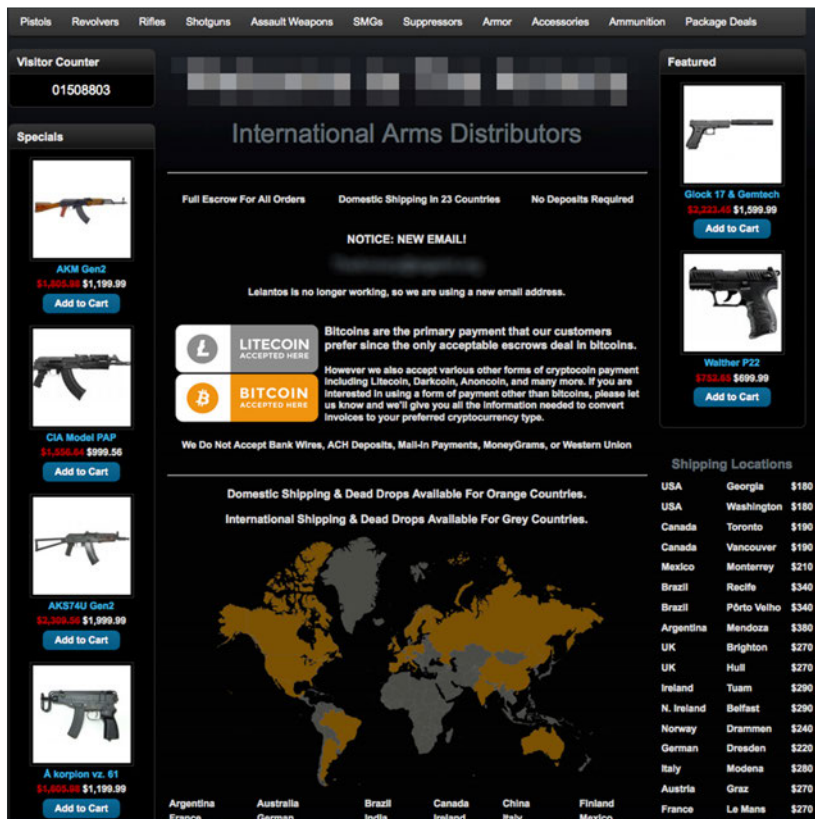


Figure 28: A weapons site that offers firearms to almost anyone anywhere in the world

The weapons forums and marketplaces we studied had similar offerings at standard prices.

Offering	Price
Aerosol pepper spray	US\$8 per can
A pair of brass knuckles	US\$18
Knife	US\$20
Stun gun	US\$30
.45ACP ammunition can	US\$450 per 1,000 rounds
.30-06 ammunition can	US\$490 per 1,000 rounds
Beretta handgun	US\$550
AK-47 machine gun	US\$800
Handgun with silencer	US\$1,500
.50-caliber rifle	US\$6,500

Table 6: Weapons offered in the North American underground

Murder for hire

Perhaps more disturbing than drugs and weapons is the ubiquity that murder-for-hire services are enjoying in the North American underground.

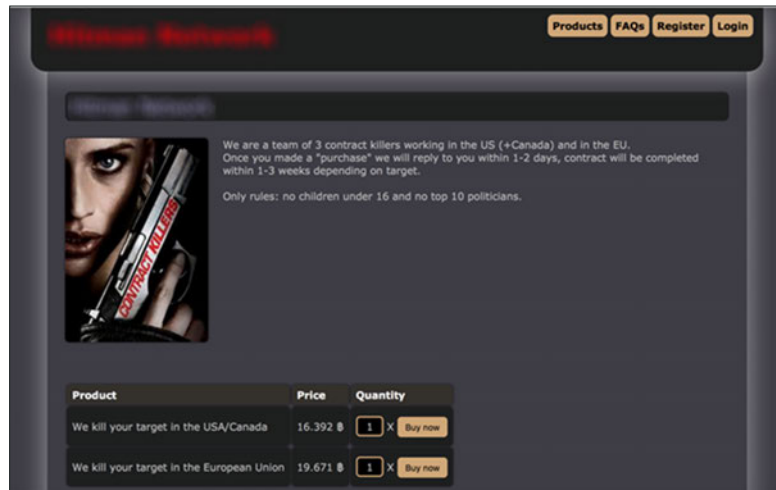


Figure 29: Murder-for-hire ad seen underground

Some murder-for-hire sites even itemized their service offerings. The more popular or important the victim and the greater the damage inflicted it seemed, the more expensive the service was.

Murder Types	Regular Person	Public Persons	1-2 Guards	3-5 Guards
Regular	\$45,000	\$180,000	\$360,000	\$540,000
Missing in action	\$60,000	\$240,000	\$480,000	\$720,000
Death in accident	\$75,000	\$300,000	\$600,000	\$900,000
Cripple Types	Regular Person	Public Persons	1-2 Guards	3-5 Guards
Regular	\$12,000	\$48,000	\$120,000	\$180,000
Uglify	\$18,000	\$72,000	\$160,000	\$240,000
Two Hands	\$24,000	\$96,000	\$200,000	\$300,000
Paralyse	\$30,000	\$120,000	\$240,000	\$360,000
Rape	Regular Person	Public Persons	Family	Members
Regular	\$8,000	\$16,000	\$32,000	\$32,000
Under age	\$21,000	\$32,000	\$36,000	\$36,000
Bombing	Regular Person	Public Persons	Family	Members
Simple	\$7,000	\$28,000	\$32,000	\$32,000
Complex	\$21,000	\$32,000	\$48,000	\$48,000
Beating	Regular Person	Public Persons	Family	Members
Simple	\$3,000	\$12,000	\$30,000	\$30,000

We need: Name.
Country and City.
Clear and recent picture of target.
And any other information you can provide is very helpfull and will speed things up.

Figure 30: Heinous crime service offerings with their prices

Many murder-for-hire sites guarantee a certain level of “professionalism.” Hit men provide certain guarantees of keeping their clients anonymous. They offer varied menus with services ranging from beating regular individuals for US\$3,000 to killing public figures for US\$180,000.



SECTION 2

The future of the
North American
underground

The future of the North American underground

Law enforcement efforts in North America are generally much stronger compared with any other region's worldwide. The US and Canadian governments have always been committed to protecting their citizens from cybercrime by continuously beefing up their legislative and enforcement efforts. The fruits of which, we've seen over time. Just this year, we at Trend Micro aided US law enforcement agencies in taking down DRIDEX⁵, SIMDA⁶, and BEEBONE⁷ —major botnet operations that previously served as backbone to many cybercriminal operations. But despite these major hits against cybercrime, we are still seeing a brazen and thriving underground economy in the region.

The open nature of North American underground can mean greater profit for sellers and overall market growth. Accessibility may help underground sellers gain more and more customers at the expense of visibility. This may encourage rapid albeit fluctuating transactions between cybercriminals, but this also presents a challenge to law enforcement. As previously stated, this underground is a glass tank, as much as it is transparent, it is also fragile. Although several criminal transactions are done out in the open, they are very fickle. The life span of most underground sites is short. They could be up one day and gone the next. Investigations will have to keep up with this fast pace.

To make the Internet safer for our customers and the rest of the world, we will continue to closely work with law enforcement agencies in both the US and Canada and support their efforts to topple cybercrime. With these ongoing partnerships, we expect to see more takedowns and arrests in the near future.

Appendix

Anonymizing underground transactions

Underground buyers know that using credit cards and other traceable payment methods to purchase goods and services is likely to lead to arrests. To mitigate related risks, many underground sellers accept alternative means of payment. Virtual currencies like bitcoins and WebMoney, along with payment transfers through service providers like Western Union and MoneyGram are thus often used. These modes of payment allow for maximum shielding by keeping transfers anonymous. Unlike traditional online payment service providers like PayPal, which requires ties to legitimate bank accounts, these alternative payments don't.

Western Union and MoneyGram

Western Union and MoneyGram are two of the most popular international money-transfer service providers. They are, however, legitimate businesses that are, unfortunately, often abused by cybercriminals. These services allow anyone to send money almost instantly to anyone anywhere in the world. They have thousands of establishments worldwide that intended recipients can collect payments from. Senders and receivers don't even need bank accounts to avail of their services. They can even use fake identities (as long as they have IDs [usually counterfeit] as proof of identification) to send and receive payments, leaving virtually no trace of ties to illegal transactions.

Every underground forum and marketplace we visited accepts Western Union or MoneyGram payments.

Bitcoins

As expected, bitcoins are also accepted in any North American underground forum or marketplace. Forum and marketplace owners even provide step-by-step instructions on how to use the virtual currency.

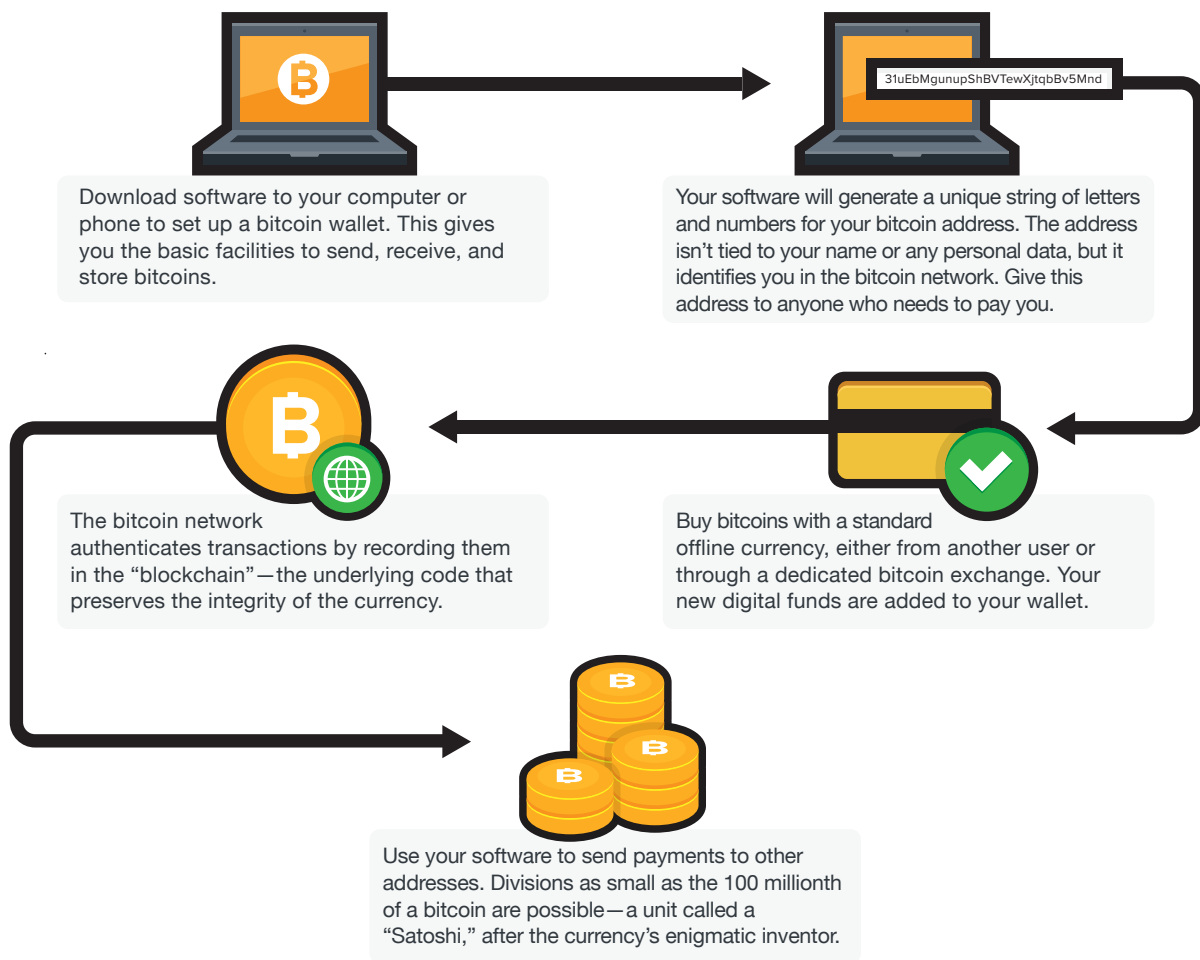


Figure 31: Step-by-step guide on using bitcoins for payment

Bitcoin users rely on the inherent level of ambiguity that the currency's infrastructure provides. All that changes hands in transactions are blockchain addresses, which isn't enough to attribute wallet ownership to any individual. Anyone can anonymously buy bitcoins online or in person.

WebMoney

WebMoney is also a widely used payment means in the North American underground. It is, in fact, a heavily advertised payment-settlement service in forums and marketplaces. WebMoney use involves "guarantors" or escrows who underwrite transaction amounts. Guarantors or escrows ensure that funds are smoothly transferred from buyers to sellers.

WebMoney offers "services that allow clients to keep track of their funds, attract funding, resolve disputes, and carry out safe transactions. The technology that WebMoney uses offers all users a set of standardized interfaces to allow them to manage their valuables. All of which are kept safe by specialized companies—guarantors."⁸ That said, it does not only offer anonymity but also insurance that transactions are properly settled.

What makes up the North American underground?

We used the following criteria to determine what sites are part of the North American underground:

- Marketplaces and forums that primarily catered to North American clientele (based on regional focus and target audience)
- Marketplaces and forums hosted within North America
- Marketplaces and forums that primarily used English (based on textual analysis)
- Marketplaces and forums that had ties to leaked domain information that helped attribute location

Note that the North American underground (which primarily uses English) is open to virtually anyone worldwide. Anyone who can understand English can find his way to its various forums and marketplaces. Several sellers ship even physical items to other countries outside the region.

Breakdown of the North American underground sites monitored

Staying true to its roots, drugs remain the primary North American underground commodity. More than half of the sites we found in it sold various kinds of drugs; crimeware like malware code and stolen account information only followed.

This trend likely sets the North American underground apart from its peers. While other underground markets focus more on crimeware trade, North American underground forums can be better categorized North American underground buyers could be taking advantage of the anonymity that it offers to support their drug addiction, as opposed to trading traditional cybercriminal wares.

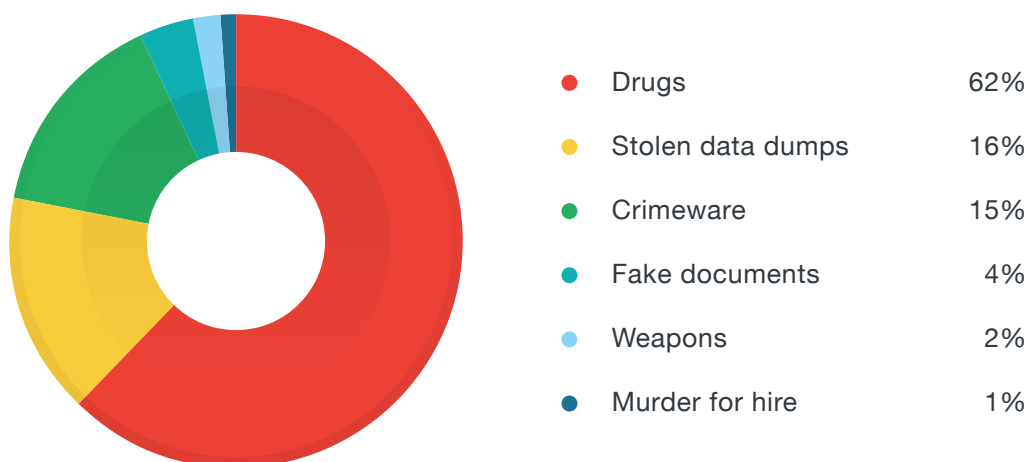


Figure 32: North American underground site type distribution*

* Note that the sites classified were limited to those that we visited and analyzed during the course of research.

References

1. Akira Urano. (2015). *Trend Micro Security Intelligence*. “The Japanese Underground.” Last accessed on 21 November 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-japanese-underground.pdf>.
2. Fernando Mercês. (2014). *Trend Micro Security Intelligence*. “The Brazilian Underground Market: The Market for Cybercriminal Wannabes?” Last accessed on 21 November 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf>.
3. Max Goncharov. (2015). *Trend Micro Security Intelligence*. “Criminal Hideouts for Lease: Bulletproof Hosting Services.” Last accessed on 21 November 2015, <http://www.trendmicro.fr/media/wp/wp-criminal-hideouts-for-lease-en.pdf>.
4. Darknetmarkets.org. (10 July 2015). *Darknet Markets*. “A Simple Guide to Safely and Effectively Tumbling (Mixing) Bitcoins.” Last accessed on 23 November 2015, <https://darknetmarkets.org/a-simple-guide-to-safely-and-effectively-mixing-bitcoins/>.
5. Trend Micro. (13 October 2015). *TrendLabs Security Intelligence Blog*. “FBI, Security Vendors Partner for DRIDEX Takedown.” Last accessed on 21 November 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/us-law-enforcement-takedown-dridex-botnet/>.
6. Trend Micro. (12 April 2015). *TrendLabs Security Intelligence Blog*. “SIMDA: A Botnet Takedown.” Last accessed on 21 November 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/simda-a-botnet-takedown/>.
7. Dianne Lagrimas. (9 April 2015). *Trend Micro Security News*. “Beebone Botnet Takedown: Trend Micro Solutions.” Last accessed on 27 November 2015, <http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/151/beebone-botnet-takedown-trend-micro-solutions>.
8. WebMoney. (1998). *WebMoney*. “Description: In Brief.” Last accessed on 21 November 2015, <http://www.wmtransfer.com/eng/information/short/index.shtml>.

Created by:

TrendLabs

The Global Technical Support and R&D Center of **TREND MICRO**

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.



Securing Your Journey
to the Cloud