FLARE
SYSTEMS

Botnets and Black Market Proxies in Canada

March 2021

Authors

David Hétu, PhD, Chief Research Officer
Luana Pascu, Cybersecurity Researcher

Executive Summary

Malicious actors often rent out malware-infected computers (bots) to abuse the credentials they store. Flare Systems researchers investigated the criminal underground for bots to determine what types of threats they pose to organizations. We focused the scope of our research in Canada. Through threat intelligence analysis, our security researchers sought to find out how easy it is to impersonate a Canadian identity online and how profitable the business can be.

This research report offers a glimpse into misleading advertisements, the pricing of bots, and the stock and flow of Canadian bots for rent on the private Genesis Market. Flare Systems researchers found that only a few fresh bots are added to the inventory per day. As this scarcity of uploads comes amid constant sales, demand seems to exceed the current supply. Based on our investigation and predictive modelling, we estimate that Genesis Market's impact on the Canadian economy is close to $19 million. Canadian bots, although priced at less than $100, are not key sources of Genesis Market's overall revenue.

Since proxies are an essential part of credential abuse and account takeover, this report also surveyed the landscape for black market proxies in Canada. As of the time of writing, our team has found no Canadian mobile proxies for sale, but discovered many suppliers of residential proxies. This leads us to believe that using a mobile IP address may prove challenging for inexperienced malicious actors. Purchasing numerous proxies is expensive, and that needs to be taken into consideration when evaluating the profits of malicious actors.

Moving forward, organizations can protect themselves by implementing two-factor authentication and IP profiling for incoming connections, as well as reducing cookie lifespan and building a detailed map of their digital footprint. The access to information and tools we detail in this report reveal the importance of building defenses that are in line with the threat landscape, and designed for in-depth defense.

Table of Contents

1 | The Botnet Business

A botnet is a network of computers infected by malware that allows a malicious actor - the botmaster - to control them remotely. The infected computers - the bots - communicate with a command and control server (C&C) to receive their orders. **The use cases for bots** are too numerous to list here, but commonly include:

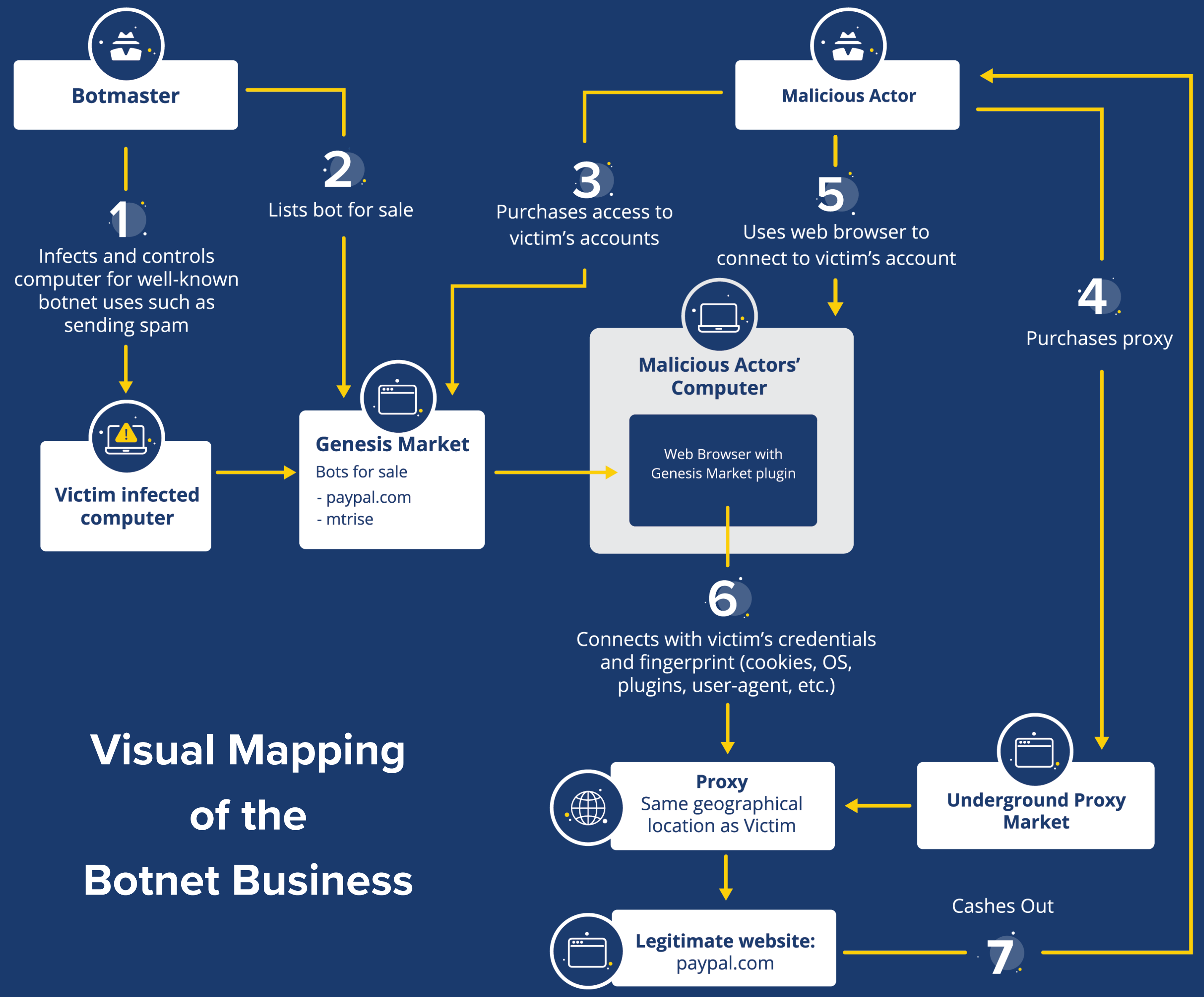
1. **Confidential and financial data theft**
2. **Credential theft**
3. **Sending of spam**
4. **The botnet's spread to other machines, either on the local network, or the internet**

A less-discussed aspect of **botnets is their use as proxies.** Botnets are ideal traffic relays as their bots are spread all over the world, in home and corporate settings, and generate traffic that covers the illicit communications sent through them. Proxies play an essential role to pretty much any online crime. They are used to hide the malicious actors' identity and prevent arrest. They also hide the origin of communications, and make it harder to flag and block them. When malicious actors use botnets as their personal proxy service, identification and prevention become that much more difficult.

Few botmasters have the time, expertise and resources to monetize the information and services coming out of their botnets. To grow a botnet to tens, if not hundreds, of thousands of bots requires serious dedication. It therefore makes much more sense for botmasters to concentrate on growing their botnets, and to rent out their bots to malicious actors in need of their information and resources.

This has led to the creation of surprisingly **large markets where bots can be rented**, and their information and credentials stolen and abused. While many markets are in the business of renting out bots, the first name that comes to mind to people in the criminal underground is Genesis Market.

Visual Mapping of the Botnet Business


Botmaster
1
Infects and controls computer for well-known botnet uses such as sending spam
Victim infected computer
2
Lists bot for sale
Genesis Market
Bots for sale
- paypal.com
- mtrise
Malicious Actor
3
Purchases access to victim's accounts
5
Uses web browser to connect to victim's account
Malicious Actors' Computer
Web Browser with Genesis Market plugin
4
Purchases proxy
6
Connects with victim's credentials and fingerprint (cookies, OS, plugins, user-agent, etc.)
Proxy
Same geographical location as Victim
Underground Proxy Market
Legitimate website:
paypal.com
Cashes Out
7

Genesis Market facilitates the rental of bots. Buyers rent the bots to access the credentials of its legitimate owner. The buyer can then impersonate the infected computer using a browser plugin and a proxy, then connect to commercial websites using the victim's credentials. From there, the buyer can steal funds, make purchases, or anything else the legitimate owner could.

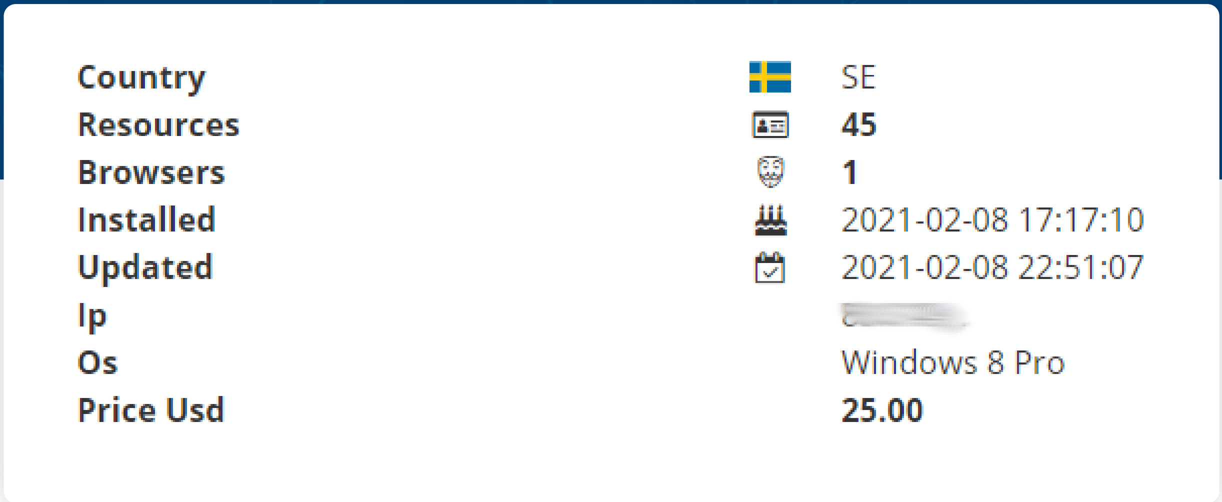
2 | Genesis Market: A $19M Business in Canada

Operating from various command and control centres, botnets have been used in bank fraud, DDoS attacks and spam campaigns. In January 2021, the Canadian Radio-Telecommunications and Telecommunications Commission (CRTC), the country's telecom regulator, warned that ISPs would have to get tougher on botnets, deploying security at the network level to block them.

Malicious actors vary greatly in their degree of sophistication. Companies with mature cybersecurity teams usually have less to fear from so-called script kiddies, or inexperienced and unskilled attackers, who use freely available hacking tools. Instead, they focus on malicious actors with the skills, and connections, to maximize their success rate through **customized and targeted attacks.**

Some services sold in the criminal underground, however, **enable even unskilled individuals to operate at an expert level.** They require little to no technical skill, but seriously elevate the user's chance of success. This is how **Genesis Market (GM)** operates. Launched in 2018, GM is a paid, private illicit market, though registration codes can now sometimes be obtained for free. The site repackages and resells infected computers that form part of botnets.

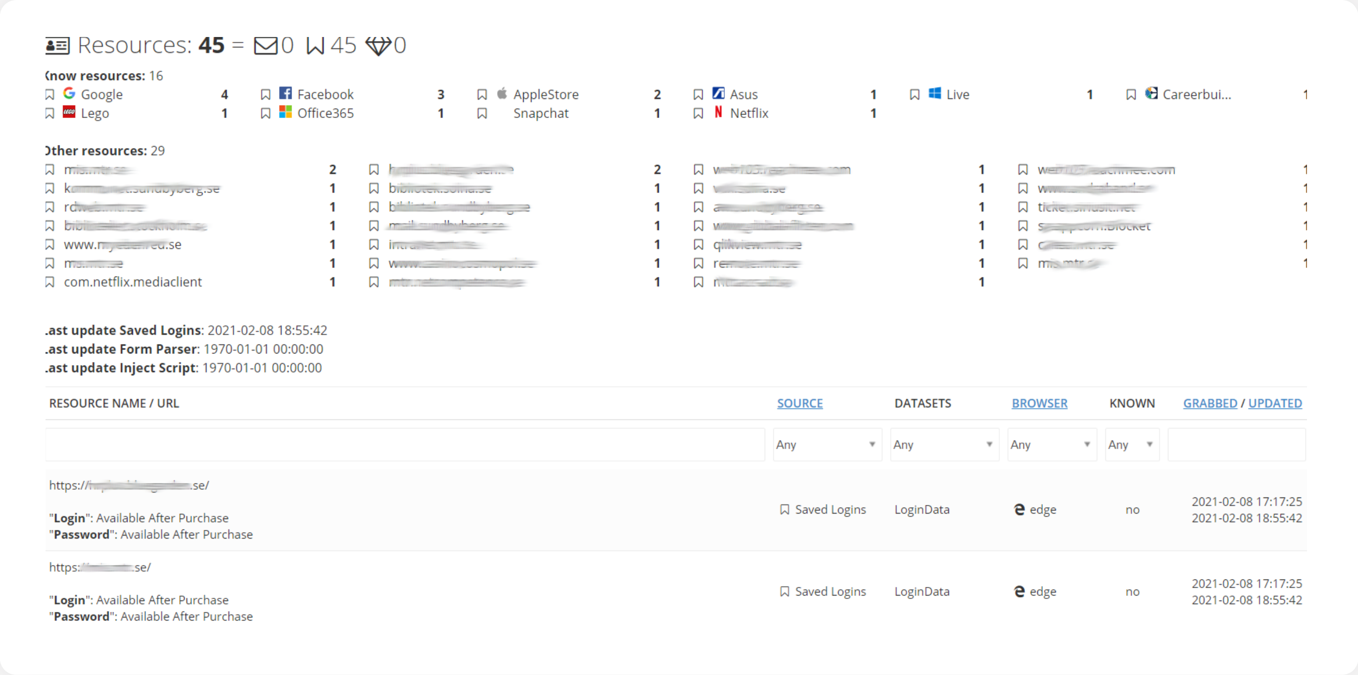
Genesis Market offers buyers **detailed information about the victim's computer**, including geolocation, IP address, OS, date of infection, and last connection to the command and control center. Customers can choose the bot that best fits their needs. The picture below shows the level of detail customers can expect, including how many credentials (resources) are included for the price of the bot.



Country	SE
Resources	**45**
Browsers	**1**
Installed	2021-02-08 17:17:10
Updated	2021-02-08 22:51:07
Ip	[redacted]
Os	Windows 8 Pro
Price Usd	**25.00**

Figure 1. Screenshot showing the levels of details customers can expect

With each bot it sells, Genesis Market provides a comprehensive **list of cookies and credentials stolen from a victim's computer**. This information is indexed and searchable, and includes minute details, as shown in the screenshot below. As a result, malicious actors can **buy bots with credentials for specific websites**, or combinations of websites that enable chained attacks.



Resources: **45** = 0 45 0

(now resources: 16

Google	4	Facebook	3	AppleStore	2	Asus	1	Live	1	Careerbui...	1
Lego	1	Office365	1	Snapchat	1	Netflix	1				

)ther resources: 29

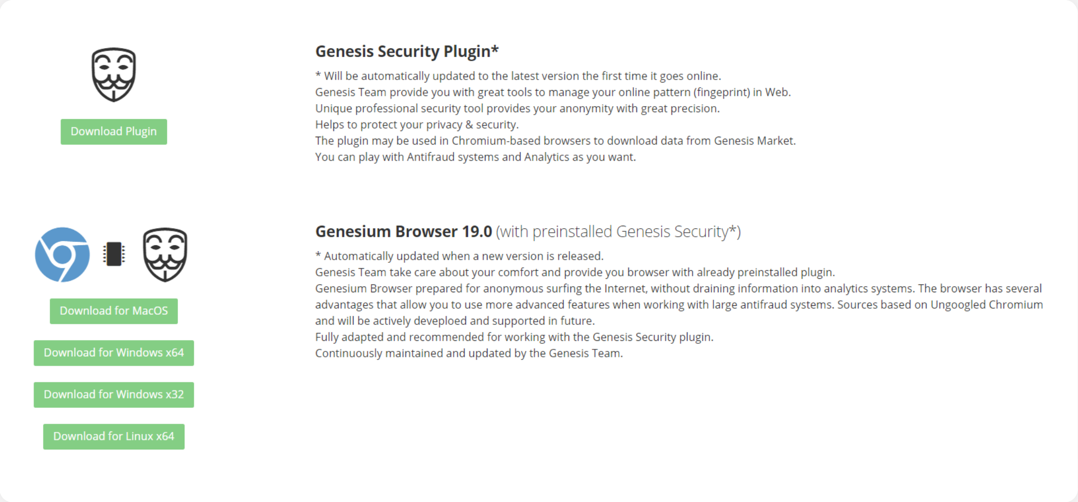
[redacted]	2	[redacted]	2	[redacted]	1	[redacted]	1
[redacted]	1	[redacted]	1	[redacted]	1	[redacted]	1
[redacted]	1	[redacted]	1	[redacted]	1	[redacted]	1
[redacted]	1	[redacted]	1	[redacted]	1	[redacted]	1
[redacted]	1	[redacted]	1	[redacted]	1	[redacted]	1
[redacted]	1	[redacted]	1	[redacted]	1	[redacted]	1
com.netflix.mediaclient	1	[redacted]	1	[redacted]	1		

.ast update Saved Logins: 2021-02-08 18:55:42
.ast update Form Parser: 1970-01-01 00:00:00
.ast update Inject Script: 1970-01-01 00:00:00

RESOURCE NAME / URL	SOURCE	DATASETS	BROWSER	KNOWN	GRABBED / UPDATED
	Any	Any	Any	Any	
https://[redacted].se/ **"Login"**: Available After Purchase **"Password"**: Available After Purchase	Saved Logins	LoginData	edge	no	2021-02-08 17:17:25 2021-02-08 18:55:42
https:[redacted].se/ **"Login"**: Available After Purchase **"Password"**: Available After Purchase	Saved Logins	LoginData	edge	no	2021-02-08 17:17:25 2021-02-08 18:55:42

Figure 2. Screenshot of cookies and credentials included with bot purchase

Genesis Market also offers a **plugin and an anonymous browser** that download victim profiles onto the attackers' computers. Thanks to these features, even unskilled actors can replicate their victim's fingerprint. If the right proxy is used, a company will likely not realize that a malicious actor, instead of a legitimate user, is connecting to their service. When the plugin is connected to the website, it provides the victim's information to bypass the web fingerprinting solution meant to detect malicious logins.



Genesis Security Plugin*

* Will be automatically updated to the latest version the first time it goes online.
Genesis Team provide you with great tools to manage your online pattern (fingeprint) in Web.
Unique professional security tool provides your anonymity with great precision.
Helps to protect your privacy & security.
The plugin may be used in Chromium-based browsers to download data from Genesis Market.
You can play with Antifraud systems and Analytics as you want.

Genesium Browser 19.0 (with preinstalled Genesis Security*)

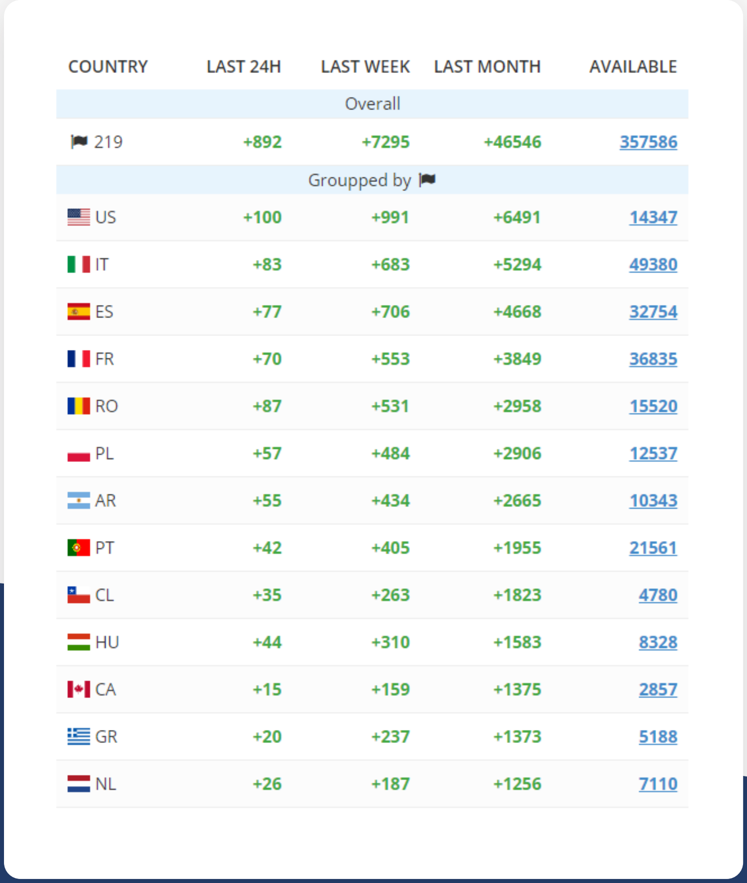
* Automatically updated when a new version is released.
Genesis Team take care about your comfort and provide you browser with already preinstalled plugin.
Genesium Browser prepared for anonymous surfing the Internet, without draining information into analytics systems. The browser has several advantages that allow you to use more advanced features when working with large antifraud systems. Sources based on Ungoogled Chromium and will be actively deveploed and supported in future.
Fully adapted and recommended for working with the Genesis Security plugin.
Continuously maintained and updated by the Genesis Team.

Figure 3. Screenshot of Genesis Market plugin and browser available for download

The fingerprint includes the victim's cookies and browser history, its advertised OS, plugins installed, and more. Each bot comes with a fingerprint of the infected machine.

2.1 | Deep Dive into Genesis Market Operations

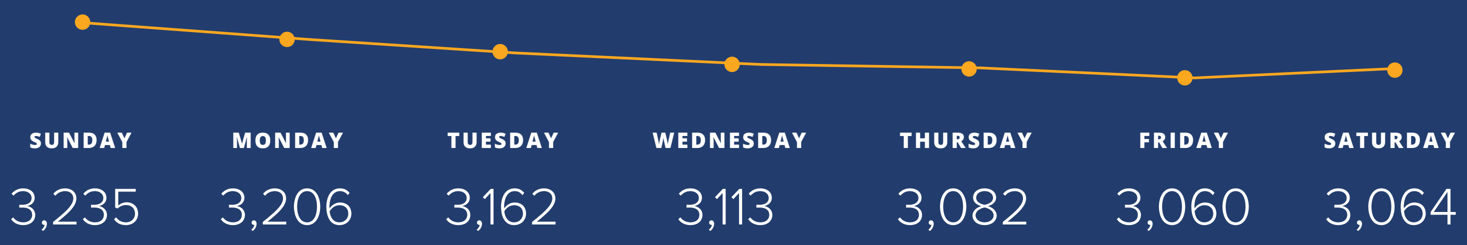
Genesis Market currently has over 350,000 bots for sale, and Canada accounts for less than 1% of the market, or 3,000 bots. Over the past year, the number of bots available has increased significantly, although the number has been stable for the past four months.



COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
⚑ 219	+892	+7295	+46546	357586
Groupped by ⚑				
US	+100	+991	+6491	14347
IT	+83	+683	+5294	49380
ES	+77	+706	+4668	32754
FR	+70	+553	+3849	36835
RO	+87	+531	+2958	15520
PL	+57	+484	+2906	12537
AR	+55	+434	+2665	10343
PT	+42	+405	+1955	21561
CL	+35	+263	+1823	4780
HU	+44	+310	+1583	8328
CA	+15	+159	+1375	2857
GR	+20	+237	+1373	5188
NL	+26	+187	+1256	7110

Figure 4. Screenshot of bot availability on Genesis Market per country

In December 2020, Genesis Market closed down for about four weeks to update its backend code and infrastructure. Flare Systems' threat intelligence team collected the data after the market reopened, so this may have influenced some of the analysis. For example, many buyers were likely waiting for the market to reopen to purchase bots, and this could have increased the number of sales at the beginning of our sample. On average, we found that **3,122 Canadian bots** were available for sale on any given day.



The **daily supply of new Canadian bots appears low,** ranging in the double, if not single, digits per day. This suggests vendors don't infect many bots daily, or they keep the infected bots for themselves. Vendors display older bots along with the new ones to make it look like thousands are available for purchase. The graph to the right shows the number of new Canadian bots added to Genesis Market on each day of our data collection.

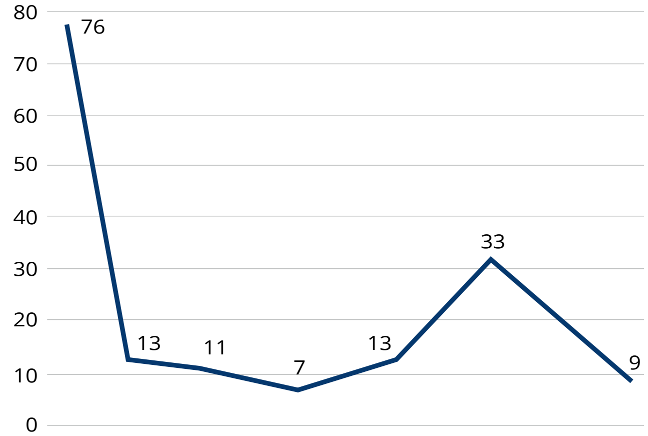


Figure 6. Number of new Canadian bots posted for sale per day

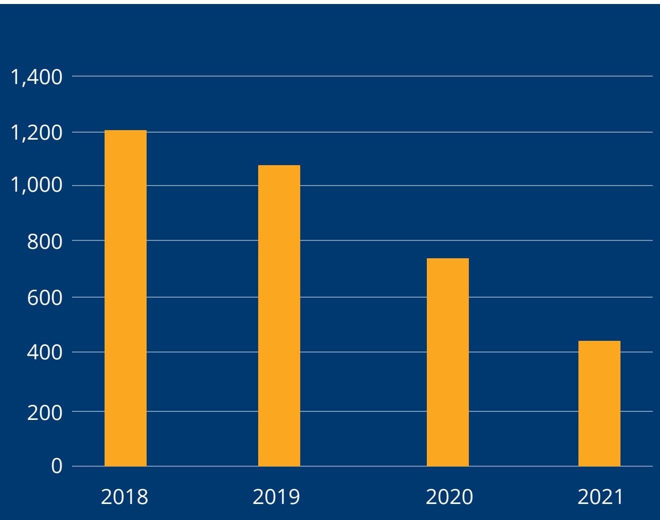


Figure 7. Bot distribution based on infection year

The graph on the left presents bot distribution based on the date of infection. Since our data collection covered the second half of January, only 400 bots have been added in 2021. Most of the bots were infected in 2018 and 2019. These older bots may not appeal to customers, and are likely there only to inflate the inventory. A customer can extract little to no value from an aged bot.

Genesis Market also discloses the date when the last credential was updated for a bot. A bot with no update in months is likely dead, and no longer of real value to malicious actors. The graph to the right presents the distribution of bots based on their last update. Only 25% of bots received fresh information in 2021, and less than 400 were updated in 2020. Many bots were apparently not updated in over two years, raising the question as to why they are being offered for sale at all.

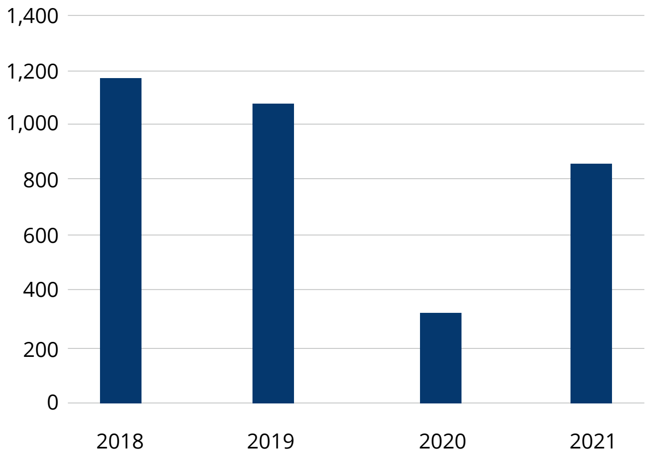


Figure 8. Bot distribution based on last update

2.2 | How Bots Are Priced

Vendors appear to base the price of Canadian bots on the date of their last update. If all data is considered, the overall median price of a bot is $9. However, bots that were recently updated fetch a median price of $35, while those updated in 2019 obtain a low median price of $5. The maximum price for a bot updated in 2021 is $350. These numbers suggest **Canadian bots can be purchased for well under $100.**

WEBSITE	MIN	MAX	MEAN	MEDIAN
OVERALL	$1	$350	$21	$9
2021	$1	$350	$58	$35
2020	$1	$19	$13	$15
2019	$1	$19	$6	$5
2018	$1	$30	$10	$8

Figure 9. Price distribution of Canadian bots based on last update

Price distribution suggests malicious actors can take a chance and pay a low price for a bot that has not been updated in years, with a likely lower payout.

2.3 | A Closer Look at Bot Inventory

A full **30% of Canadian bots for sale have a version of Windows enterprise installed,** suggesting they are operating within corporate networks. Most bots, then, are installed on personal computers. As many as 62% have Windows 10 installed, suggesting the market doesn't take advantage of older computers with vintage and unsupported Windows versions.

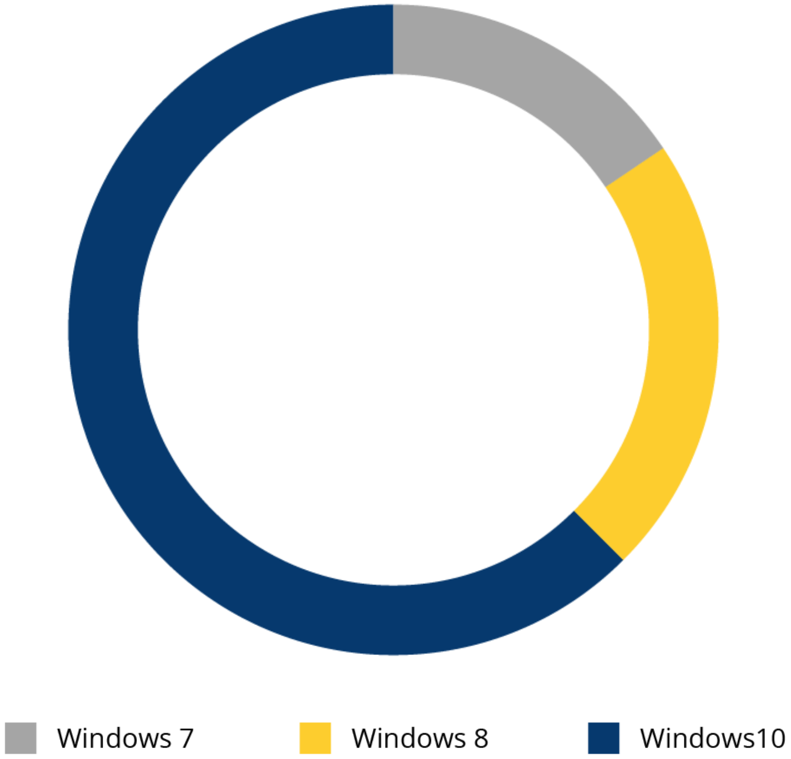


Figure 10. Distribution of Windows versions installed on Canadian bots

On average, Genesis Market facilitates **48 sales of Canadian bots per day.** The sales in our sample are concentrated at the beginning of our time series, as the market had just returned to business after weeks offline. The numbers on the right are likely more in line with the general flow of orders on Genesis Market (between 17 and 35).

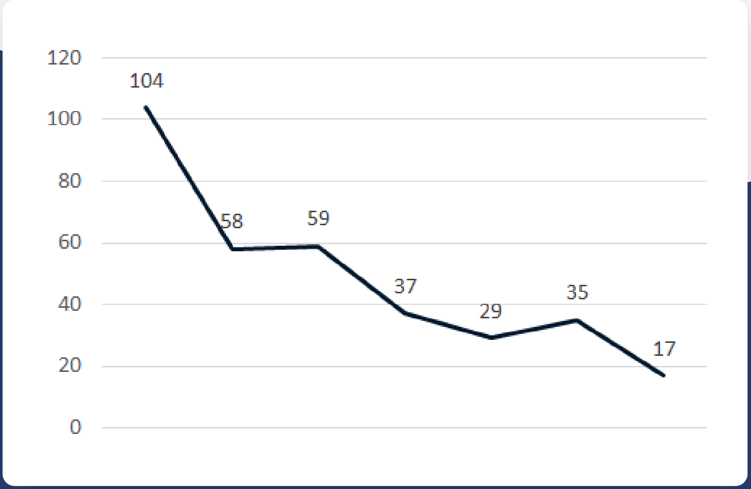


Figure 11. Number of Canadian bots sold on a daily basis

2.4 | Types of Credentials for Sale

Genesis Market provides stolen credentials with complete details to access various online services. Typically, victims have entered their information into these websites, only to later be collected by a keylogger. Since this is not the case for stolen cookies, we can only analyze identity theft in terms of credentials. Canadian bots provide **credentials for close to 18,000 websites.**

The credentials most frequently seen for sale on Canadian bots are shown in the table below. The list includes familiar names such as Google and Facebook. Some credentials are missing a username and/or a password. Most bots come with the username and password for each of their credentials. Facebook passwords are often missing, with only 76% of bots providing this information.

WEBSITE	SHARE OF BOTS	HAS USERNAME	HAS PASSWORD
google.com	52%	99%	93%
facebook.com	36%	96%	76%
live.com	35%	96%	79%
netflix.com	15%	98%	94%
amazon.ca	13%	95%	94%
twitter.com	12%	92%	95%
epicgames.com	11%	98%	92%
roblox.com	11%	100%	85%
amazon.com	10%	96%	96%
discordapp.com	10%	97%	92%

Figure 12. Most frequently stolen credentials for sale on Canadian bots

As far as Canadian and Quebec-based websites are concerned, the credentials of a small number of public institutions have been compromised. Leaked credentials still pose a significant risk, as they can be used to pivot to other resources within the organization. In most cases, at least for Canadian websites, the usernames and passwords have been recently updated. The chart below shows the distribution of updated credentials across time. In 2021, over 1,900 websites had at least one updated set of credentials. In comparison, only 45 websites had their last updated set of stolen credentials uploaded on Genesis Market in 2020.

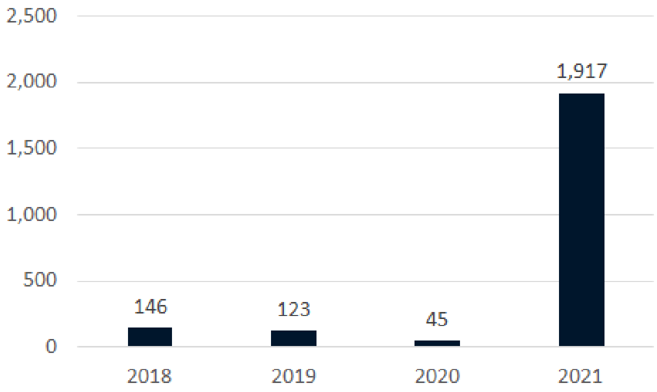


Figure 13. Yearly distribution of credentials since 2018

3 Genesis Market Dynamics

The bots on Genesis Market can be used to obtain credentials for thousands of websites, including many linked to financial and government institutions. Although thousands of bots are available for purchase, competition is stiff. We explain below why some bots are sold more than others.

Sale Predictions for Canadian Bots

Flare Systems' threat intelligence team has built a predictive model based on the following variables:

Time since last update

A variable that counts the number of days between today and the date when updated credentials were last uploaded to a bot.

Infection length

A variable that counts the number of days between the date the bot was infected, and the date the last set of credentials from that bot was uploaded to Genesis Market.

Number of cookies

A variable that counts the number of cookies available through the bot to take over accounts, without the need for credentials.

Price

A variable that measures the price of the bot.

Number of credentials

A variable that counts the number of stolen credentials available through the bot to take over accounts.

Windows enterprise version

A variable that checks if the bot is installed on a corporate network.

Windows version

A variable that checks the age of the Windows version.

3.1 | Sale Predictions for Canadian Bots

Flare Systems' threat intelligence team has built a predictive model based on the following variables:

- Variables with **no bars** have no statistically significant relationship to sales. No matter how high or low they are, sales are not impacted.
- Variables with a **yellow bar** have a positive relationship with sales: as they increase, so do sales.
- Variables with a **blue bar** have an inverse relationship with sales: as they increase, sales decline.
- The bar's length shows the variable's importance.

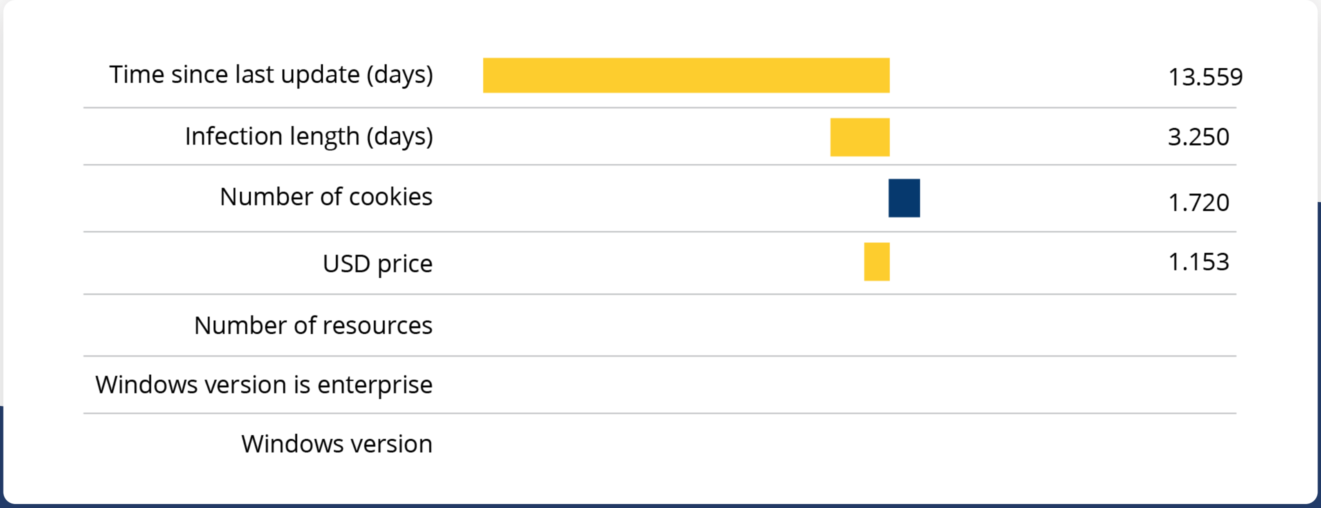


Figure 14. Variables that influence bot sales (longer bar means a stronger influence)

Our model suggests that malicious actors mostly want fresh bots on Genesis Market. The **date of the last update** is over four times as important as any other variable.

Infection length is the second main driver, meaning that buyers look for bots that have not been infected long. As time passes, we see an increase in both credential value, and in risk that a bot will be detected. Bot price does play a role, but its contribution to our model is marginal. This means that **buyers do not seem sensitive to pricing.**

Finally, the number of cookies available does drive sales, and it does so more than logins. Malicious actors may be concerned that many accounts are protected by two-factor authentication, or that credentials could have been changed or are missing. Cookies offer a surer way to take over accounts, so they're more prized.

3.2 | How to Predict the Price of Canadian Bots

We built a similar model to explain the price of bots. Given the wide range of prices (from $1 to $350), we were curious as to what makes a bot more expensive. Based on our model, bot prices are driven by the number of credentials (resources) it contains. This factor is three times as important as the date of the last update. A lack of updates for a lengthy period and a long infection time lower the price.

Counter-intuitively, though, newer Windows versions and corporate Windows versions also drive the price down. Our hypothesis is that newer versions and corporate environments may represent a harsher environment for malware, and make them more prone to detection. Since malicious actors are not guaranteed full control of the bot, the price could drop.

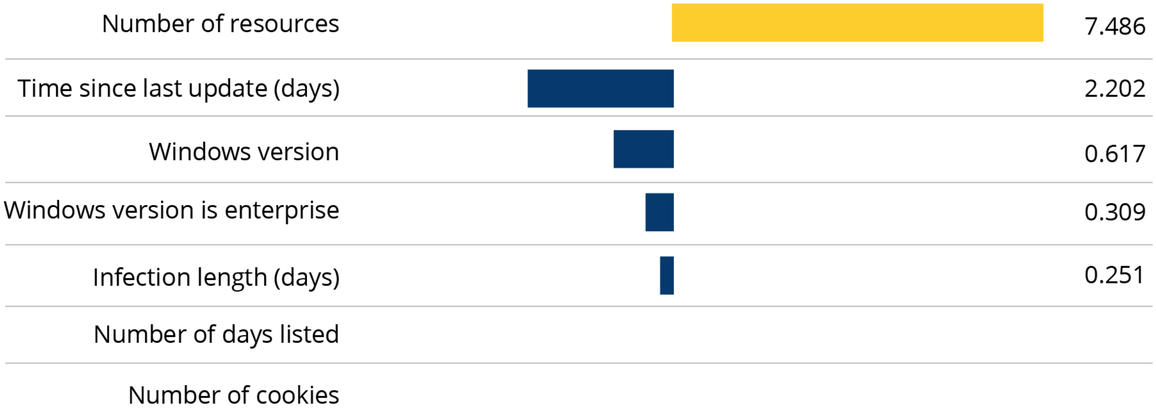


Figure 15. Graph showing the variables that drive bot prices

4 | Genesis Market's Impact on the Canadian Economy

How can we assess the impact of Genesis Market on the Canadian economy and, more specifically, on organizations? Since we can't know the intent of all malicious actors who purchase a bot on Genesis Market, we must resort to estimates, guided by our past experience, and the data we generated in this intelligence report.

We built three models to help assess the impact of Genesis Market. Of course, this impact varies depending on the values we assign to certain indicators. These are our indicators:

Number of bots sold per day
Our data suggests that between 15 and 60 Canadian bots are sold every day, with a conservative estimate falling at around 30.

Cost of bots
Prices vary widely but, based on the bots sold in our database, 25% of bots are offered very cheap. Barely 8% of these were sold, and half were priced for less than $32. As many as 75% were sold for under $71. We used these as pricing cutoffs for botnet sales.

Bot success rate
Not all bots generate fraud. Bot success rate is unknown for now, but given the solid reputation of Genesis Market, we can assume that at least 60% of bots sold will generate some sort of fraud. Not all bot purchases lead to fraud, so the highest fraud rate is pegged at 90%.

Fraud impact per bot
Reports on the economics of botnets vary (see here for a review). We err on the side of caution by using relatively low numbers, ranging between $300 and $1,000 in revenue generated per bot.

We used these indicators to build three models that can be labeled as optimistic, conservative and pessimistic. With the optimistic model, we test what happens when few Canadian bots are sold, they are expensive to buy, they enable fraud only 60% of the time, and generate a small amount of fraud. The conservative and pessimistic models use the same indicators, but increase to different degrees the number of Canadian bots sold per day, the success rate of bots in enabling fraud, and the costs of fraud. Both models also factor in a much lower purchase price for the bots. We outline the models in the table below.

	NUMBER OF BOTS SOLD PER DAY	COSTS OF BOTS	SUCCESS RATE OF BOTS	IMPACT OF FRAUD PER BOT
Optimistic	15	$71	60%	$300
Conservative	30	$32	80%	$600
Pessimistic	60	$8	90%	$1,000

The optimistic, conservative and pessimistic models generate very different impact curves, as presented in the graph below. After a year, our estimate of the impact of the Canadian bots sold could be as low as $590,000, or as high as $19 million. A more reasonable, and conservative, estimate evaluates the impact of Genesis Market at $4.8 million.

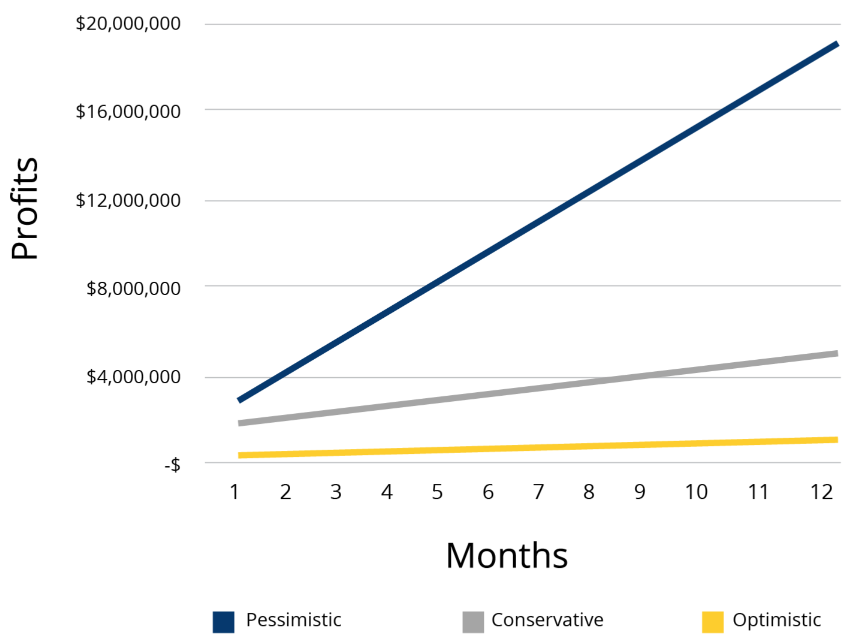


Figure 17. Economic impact of optimistic, conservative and pessimistic models

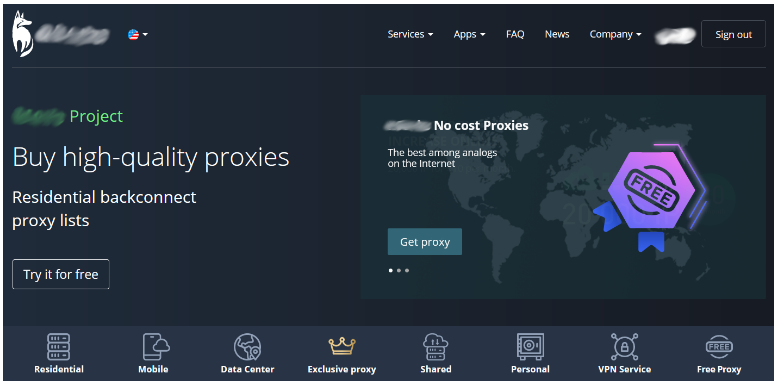
Given the lack of information on bots in other countries, it would be reckless at this point to extrapolate our results to the entire market. If the data were the same, though, the impact of Genesis Market would range in the hundreds of millions of dollars. This impact would greatly depend on the four variables we presented in the table at the beginning of this section. Based on resource distribution from Canada and Quebec, we should expect that financial institutions and merchant websites would bear the brunt of this impact.

As of January 31, 2021, the Canadian Anti-Fraud Centre had received 4,833 reports of fraud and states that $10.1 million has been lost to fraud. Compared to overall fraud costs in Canada, the numbers may not seem impressive. However, it is important to note the data come from a single illicit market. Its private and exclusive nature limits the number of malicious actors who access it. This small number of individuals could still commit a significant amount of fraud, however, generating direct and indirect costs for Canadian companies.

5 | Combining Underground Proxy Services with Bot Rentals

When malicious actors buy a bot on Genesis Market, they only get access to the victim's accounts (cookies, user-agent. etc). The market does not sell access to the bot to use as a proxy. Malicious actors must secure access to a Canadian proxy separately, and route their traffic through it when they use the stolen accounts.

The internet abounds in offers of proxy services, many on **professional-looking websites** with careful marketing to make them look legitimate. There are, however, indications that a significant number of underground proxy providers operate in a grey - if not black - market.



[redacted]

[redacted] Project

Buy high-quality proxies

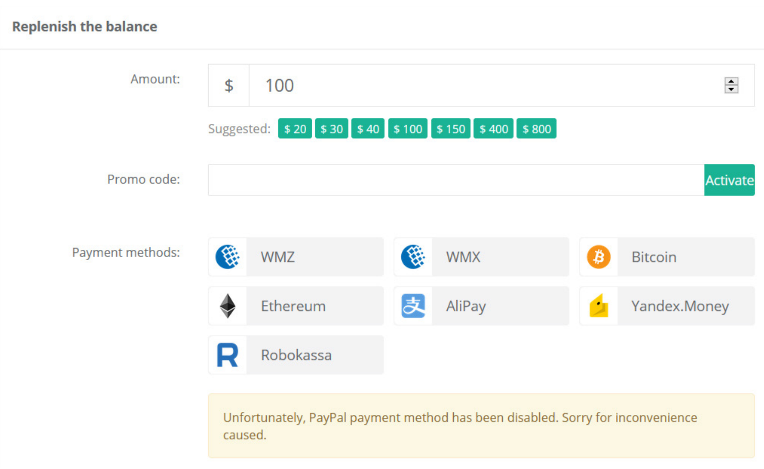
Residential backconnect proxy lists

[redacted] No cost Proxies

The best among analogs on the Internet

Figure 18. Screenshot of a proxy vendor's website

First, **proxy providers often do not accept credit cards directly**. As seen below, in some cases, cryptocurrencies and alternative payment methods such as AliPay are the only ones accepted. In other cases, credit cards are accepted, but only through payment gateways that charge exorbitant fees and operate from small, unregulated countries. A legitimate service should have no problem accepting credit cards through major payment processors such as Swipe.



Replenish the balance

Amount: $ 100

Suggested: $ 20 $ 30 $ 40 $ 100 $ 150 $ 400 $ 800

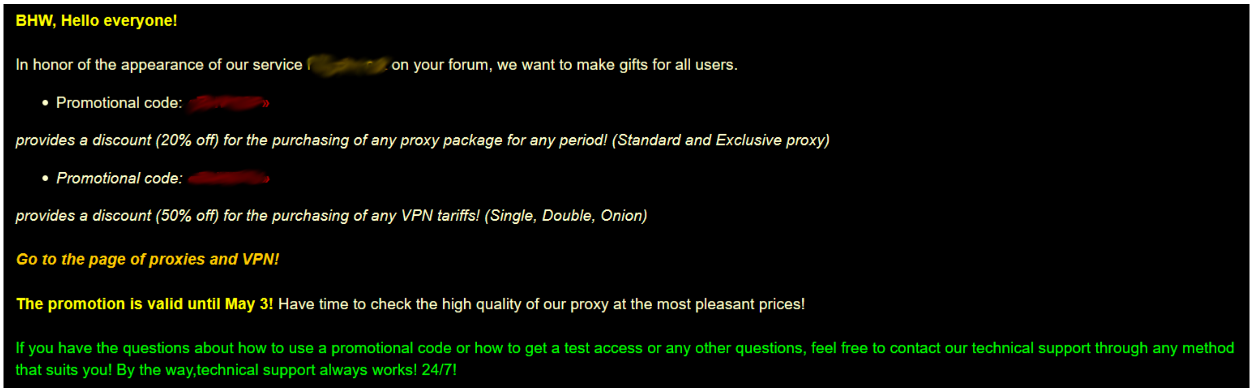
Promo code: Activate

Payment methods: WMZ WMX Bitcoin Ethereum AliPay Yandex.Money Robokassa

Unfortunately, PayPal payment method has been disabled. Sorry for inconvenience caused.

Figure 19. Screenshot of payment methods accepted by proxy provider

Second, most **proxy providers advertise their services on the criminal underground.** The provider mentioned above goes so far as to offer promotional codes for customers it recruits on the criminal underground. A legitimate company would not seek out the type of individuals who spend their time in this underground.



BHW, Hello everyone!

In honor of the appearance of our service [redacted] on your forum, we want to make gifts for all users.

- Promotional code: [redacted]

provides a discount (20% off) for the purchasing of any proxy package for any period! (Standard and Exclusive proxy)

- *Promotional code:* [redacted]

provides a discount (50% off) for the purchasing of any VPN tariffs! (Single, Double, Onion)

Go to the page of proxies and VPN!

The promotion is valid until May 3! Have time to check the high quality of our proxy at the most pleasant prices!

If you have the questions about how to use a promotional code or how to get a test access or any other questions, feel free to contact our technical support through any method that suits you! By the way,technical support always works! 24/7!

Figure 20. Screenshot of an advertisement for a proxy service on a criminal forum

Third, **proxy providers remain elusive as to where their proxies are sourced from**. Rumours on the criminal underground and anecdotal evidence suggest that some proxies are misconfigured servers left open for anyone to abuse. Other proxies are run through bulk data plans, purchased from legitimate telecom companies who turn a blind eye to the real use of their bandwidth.

Finally, proxies also come from **hacked systems whose bandwidth is abused** without their owners' consent. Failure to provide details on the source of the proxies is a clear sign that they are not all obtained legitimately.

5.1 | How Private Rotating Mobile Proxies Hide Fraudsters' Tracks

Malicious actors take advantage of the anonymity that proxies provide to avoid being blocked from connecting to servers, and to protect against identification as a high-risk source of attack (ex. Russian malicious actor). **Proxies are advertised under many labels, each with its own benefits and limits**. Multiple labels can be combined to increase anonymity. As a result, malicious actors can mix and match services, depending on their needs.

	Pros	Cons
Type of Proxy		
Data Center	Plentiful and cheap	Little to no protection against detection and often blocked
Residential	Rarely blocked as they are on IP addresses that are used by multiple users at the same time, and blocking them may create much ill will from legitimate customers	Expensive
Mobile		Expensive Low bandwidth
Change Rate of Proxy		
Static	Cheap	Easily Blocked
Routing	Very Difficult to Block	Not commonly available for all types of proxies Expensive
Public Nature of Proxy		
Yes	Plentiful and cheap	Little to no protection against detection and often blocked
No	Lower risk of detection and of being contaminated by other users	Expensive

Figure 21. Table explaining benefits and limits of proxy services

Malicious actors can manually configure proxies to influence how victims perceive their traffic. Criminals who use **residential and mobile proxies, especially when coupled with private and rotating proxies, become moving targets that are very hard to shut down.** These proxies are expensive (see business model analysis below) but give malicious actors the cover needed to launch large-scale operations, such as credential stuffing attacks.

Mobile proxies represent a unique case with a significant benefit. **All mobile phone internet traffic from telecom companies can only be traced back to a limited number of IP addresses with static geolocation.** Therefore, security practices that verify a user's location based on IP address **cannot be trusted when a mobile IP address is used.**

5.2 | Proxy Providers And Their Business Model

Genesis Market is limited in terms of opportunities for the Canadian market. Indeed, malicious actors who rent out its bots are likely to make fewer profits due to the high cost of proxies as detailed below.

We investigated the supply of Canadian proxies on the internet and the darkweb and found a total of 26 providers with either residential or mobile services, the two most useful types. Residential proxies are the most common service provided, with 23 providers, whereas mobile proxies are the least common, with three.

Providers offer various packages based on the number of proxies, bandwidth volume and number of concurrent users. Our team **built two malicious actor profiles to estimate the costs** of proxy services.

- **Low activity:** 500 proxies, 50GB in a month
- **High activity:** 5,000 proxies, 500GB in a month

Our investigation shows that data centers are, on the median, the cheapest option for malicious actors. The **premium for residential versus data center proxies varies between 47% and 67%**, depending on the activity level. **Mobile proxies cost three to eight times more than data centers,** making them exceptionally expensive.

		Price (USD)		
	Activity	**Min**	**Max**	**Median**
Data Center	High	$260	$10,000	$1,700
	Low	$50	$1,000	$285
Mobile	High	$12,500	$14,900	$13,000
	Low	$1,320	$1,490	$1,400
Residential	High	$129	$60,000	$2,500
	Low	$10	$6,000	$475

Figure 22. Table describing price options for proxies

Proxies are **not only used by malicious actors for illegal activities.** They are legal, and often recommended to secure online activity, because they can be easily installed on most devices and browsers. A number of companies use proxy servers as intermediaries to control internet traffic and reduce breaches, or to manage social media and collect data, while private users might use them to access streaming services or websites that block users from their country or region.

6 | Conclusion

Genesis Market allows unskilled actors to operate on a level close to that of skilled attackers. It is a very noisy platform with many 'aged' bots for sale in Canada. We found thousands of bots had not been updated in two years. These aged bots likely no longer offer any value, and are included to inflate the portfolio. We have seen this marketing strategy on other dark web marketplaces, where administrators **inflate the number of listings and post fake feedback** from fictitious customers to make their market appear more active. Any monitoring of Genesis Market will need to filter out the noise from these aged bots.

Canadian bots do not appear to be driving Genesis Market when we take into account the number of U.S. and international bots available. Only a handful are added every day, and more are sold than added on a daily basis. This suggests a constrained market for Canadian bots, where demand exceeds supply. Should this dynamic persist, Genesis Market will likely attract less and less interest from Canadian malicious actors.

If organizations have **access to lists of stolen credential and partial IP addresses**, they can detect and block corporate account takeover. The leak of a single credential online could cause millions of dollars in damage to a business. Just because one credential is leaked instead of hundreds, does not mean it cannot have a devastating impact.

With a price well under $100, bots on Genesis Market are affordable, and appear to be very profitable for malicious actors who understand how to take advantage of stolen credentials. Companies are protected by its somewhat private nature, as its status as a normally paid market reduces the number of potential buyers. These buyers appear to have limited interest in Canadian bots, offering Canadian organizations some natural protection from attacks.

Our investigation into the nature of Canadian residential proxies has helped us define **what proxy providers can offer customers** who seek to take over a Canadian identity. To the best of our knowledge, it is not possible to buy Canadian mobile proxies. We could not find a single proxy provider that exclusively offered mobile proxies from Canada. This suggests that using a mobile IP address may be more difficult for malicious actors who have few connections in the criminal underground.

Additionally, it is not realistic to expect to detect most proxies simply by profiling IP addresses and subscribing to IP fraud score services. Based on our results, proxies can come from dozens of ISPs, and from any city in the country. In over half of the cases, the fraud score was under 10, meaning that security systems relying on the IP Quality Score service would not automatically flag them.

7 | Recommendations

Proxies still play an essential role in most malicious attacks your organization is likely to face. Canada does not appear to be a major source of proxies. We found few Canadian providers, and, even then, there is no guarantee that they can in fact offer Canadian residential and mobile proxies. If your organization is involved with law enforcement agencies, highlight the fact that this threat can still currently be mitigated at the government or ISP level.

Even though proxies are now easily available, it is important for your organization to continue to implement security solutions that monitor and filter connections based on IP addresses. These solutions will not necessarily protect your organization from sophisticated attacks, but will raise the bar for attackers. This ensures your organization is not a soft target for malicious actors. **In today's world, the role of these solutions is more about lowering the number of attacks, rather than decreasing their odds of success.**

Another solution is to **invest in behavior analysis tools** that can track user and employee activity on your network. A credential stuffing attack, for example, will lead to thousands of users logging in and performing a limited number of actions before they stop making requests. These patterns can be detected, and prompt an increase in security for the accounts that were targeted.

Above all, **collecting reliable intelligence on malicious actors** through active monitoring of the criminal underground is an essential part of good cybersecurity hygiene. This ensures that you remain informed about the tactics and methods of malicious actors, and can better understand what your security tools can and cannot do to protect your digital assets.

Still, more mature cybersecurity teams may be able to identify the botnet victim using the **partial IP addresses, Windows version and credentials for sale**. Genesis Market is now being indexed in our database of the criminal underground, and you can set up alerts for domain names related to your companies to learn whenever a new bot with your credentials is put up for sale.

More generally, to protect themselves against markets like Genesis, organizations can implement the following guidelines:

- Activate **two-factor authentication** on all accounts. This is an effective solution against stolen credentials such as those exposed by Genesis Market. Indeed, GM does not offer authentication tokens.

- Activate **IP profiling of all incoming connections**. Genesis Market does not provide proxies for its customers, who must find a proxy near their victim. By checking where a connection comes from, organizations can detect suspicious activities.

- Limit the **lifespan of cookies** your employees and customers receive when they log in. Cookies appear to be of great interest to malicious actors. A short lifespan (measured in hours) can make them worthless to attackers, and make it harder to take over an account, especially if two-factor authentication is activated on employee and customer accounts.

- Build a detailed **map of your digital footprint.** Our analysis found that Genesis Market was populated with many old bots that are probably now worthless. This map should reduce the noise and help you prioritize which bots could be coming from inside your organization, and help you remediate the infection as soon as possible.

Unfortunately, Genesis Market provides little actionable intelligence about your customers or employees that have been victimized.

About Flare Systems

Since 2017, Flare Systems has been developing AI-driven technologies that automate fraud detection and prevention. Firework offers an easy-to-use platform that gets you the right information before risks become unmanageable. Reduce digital risk and fraud with Firework, the digital risk protection (DRP) platform that automates your dark and clear web monitoring to deliver real-time actionable intelligence.

Book a Demo

www.flare.systems
hello@flare.systems

1751 Rue Richardson, Unit 3.107
Montreal, Quebec, H3K 1G6