flare

Research Report

The Stealer Malware Ecosystem: A Detailed Analysis of How Infected Devices Are Sold and Exploited on the Dark & Clear Web

Samuel Couture, Security Researcher
Philippe Lebrun, Data Collection Specialist

About a year ago, we published a **report** on The Demand for Canadian Bots on Genesis Market, analyzing the demand and the impact of botnets sold on Genesis Market on the Canadian Market. Ever since then, our team has been wondering about the international scale of the botnet industry; Are some countries more targeted than others? What influences the price of a botnet on the international market? What kind of malware is used to collect the victim's information? Do attack patterns vary among distributors?

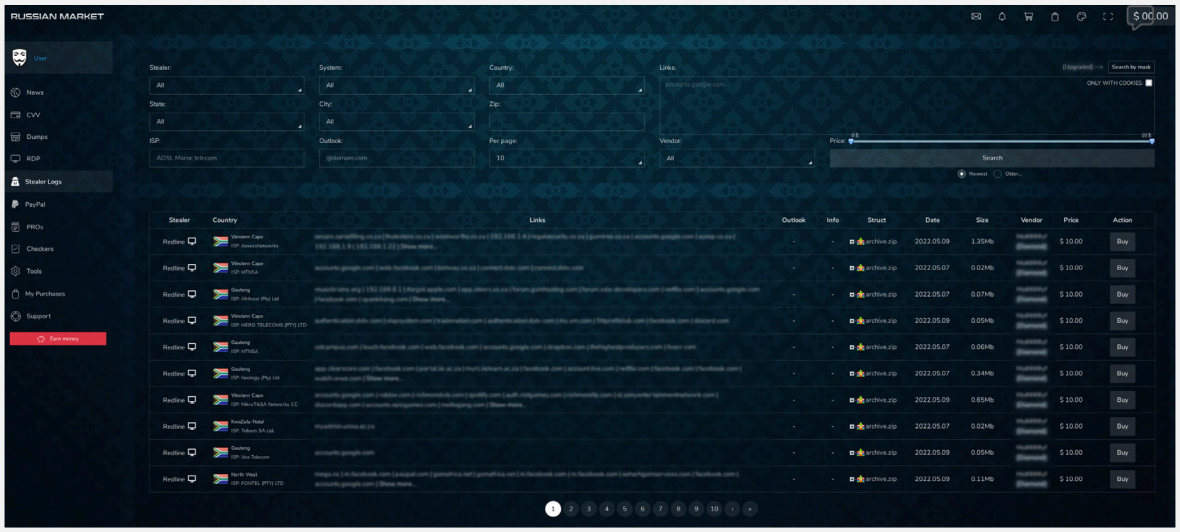
To answer those questions, our research team analyzed data from two major players in the industry, Genesis Market (GM) and Russian Market (RM). Whilst the two autoshops don't sell the exact same product, the intent is very similar and the objective of cyber-criminals purchasing the listings on both marketplaces is in the same line.

Without entering into details, Genesis Market specializes in the sale of "botnets"; computers that were infected with malware to steal the information stored in the web browsers, as well as the browser's **fingerprint**. Once in possession of the victim's browser fingerprint, the malicious actor can then "install" it on their own device. This allows cybercriminals to essentially impersonate the victim to: make fraudulent purchases while bypassing some security measures, drain the victim's bank accounts (or various financial services), or even achieve **account takeovers**. Whilst fingerprint isn't widely used in fraud prevention, the very high level of impersonation provided by botnets makes it incredibly difficult to identify malicious logins.

On the other hand, *Russian Market* sells what is known as Stealer Logs; a type of malware that once again steals the information stored on the victim's browser (e.g: forms, logins, cookies) as well as some basic device information. Although these do not provide as much information as GM's botnets, they are still incredibly powerful and in the hands of an experienced cyber-criminal, are just as dangerous to organizations.
With all of this in mind, we'll explore the key differences between the two marketplaces, as well as some specific data analysis of the offerings from both autoshops.

Russian Market

As previously mentioned, Russian Market is a dark web autoshop, specialized in the sale of various fraud-related items; from stolen credit cards, Paypal accounts, to our subject at hand, Stealer Logs.



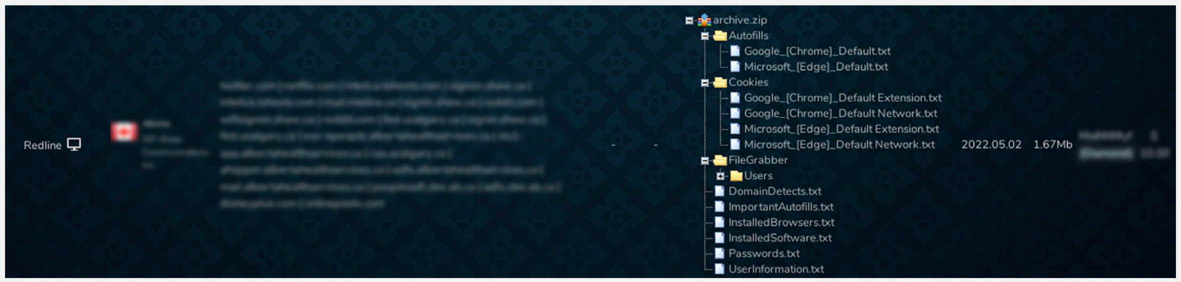
Stealer: All
System: All
Country: All
Links: accounts.google.com
ONLY WITH COOKIES: □
State: All
City: All
Zip:
ISP: ADSL Maroc telecom
Outlook: @domain.com
Per page: 10
Vendor: All
Price: 0 $ – 10 $
● Newest ○ Older...

Stealer	Country	Links	Outlook	Info	Struct	Date	Size	Vendor	Price	Action
Redline	Western Cape ISP: AxxessNetworks	[redacted]	-	-	archive.zip	2022.05.09	1.35Mb	[redacted]	$ 10.00	Buy
Redline	Western Cape ISP: MTNSA	[redacted]	-	-	archive.zip	2022.05.07	0.02Mb	[redacted]	$ 10.00	Buy
Redline	Gauteng ISP: Afrihost (Pty) Ltd	[redacted]	-	-	archive.zip	2022.05.07	0.07Mb	[redacted]	$ 10.00	Buy
Redline	Western Cape ISP: HERO TELECOMS (PTY) LTD	[redacted]	-	-	archive.zip	2022.05.09	0.05Mb	[redacted]	$ 10.00	Buy
Redline	Gauteng ISP: MTNSA	[redacted]	-	-	archive.zip	2022.05.07	0.06Mb	[redacted]	$ 10.00	Buy
Redline	Gauteng ISP: Neology (Pty) Ltd	[redacted]	-	-	archive.zip	2022.05.07	0.34Mb	[redacted]	$ 10.00	Buy
Redline	Western Cape ISP: MikroTikSA Networks CC	[redacted]	-	-	archive.zip	2022.05.09	0.65Mb	[redacted]	$ 10.00	Buy
Redline	KwaZulu-Natal ISP: Telkom SA Ltd.	[redacted]	-	-	archive.zip	2022.05.07	0.02Mb	[redacted]	$ 10.00	Buy
Redline	Gauteng ISP: Vox Telecom	[redacted]	-	-	archive.zip	2022.05.09	0.05Mb	[redacted]	$ 10.00	Buy
Redline	North West ISP: FONTEL (PTY) LTD	[redacted]	-	-	archive.zip	2022.05.09	0.11Mb	[redacted]	$ 10.00	Buy

Figure 1. The Stealer Logs page on Russian Market

When browsing for Stealer Logs, each listing contains information about the victim's device; you can usually expect to find:

- The stealer malware family
- The computer's operating System
- The country in which the computer is located
- The victim's internet service provider
- A list of the services (websites) for which a login is available
- The directory content of the archive made by the stealer software
- The date on which the device was infected



Redline [redacted] [redacted] - -

```
archive.zip
  Autofills
    Google_[Chrome]_Default.txt
    Microsoft_[Edge]_Default.txt
  Cookies
    Google_[Chrome]_Default Extension.txt
    Google_[Chrome]_Default Network.txt
    Microsoft_[Edge]_Default Extension.txt
    Microsoft_[Edge]_Default Network.txt
  FileGrabber
    Users
  DomainDetects.txt
  ImportantAutofills.txt
  InstalledBrowsers.txt
  InstalledSoftware.txt
  Passwords.txt
  UserInformation.txt
```

2022.05.02 1.67Mb [redacted]

Figure 2. A Stealer Log listing example

This information is invaluable for cyber-criminals to evaluate the potential gains to be made from a Stealer Log; Logs with more services available represent more fraud opportunities. We'll come back to how that is reflected in the price of the available Logs on Russian Market further below.

While we are on the topic of Russian Market, since they publicize which stealer malware was used to infect the victim's computer, we thought it would be valuable to see how the different families are represented on the market.

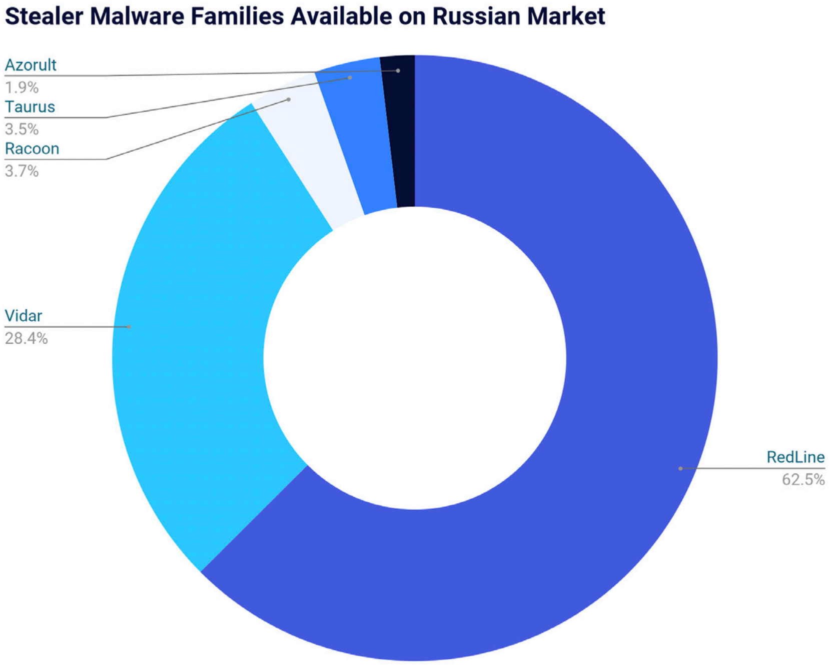
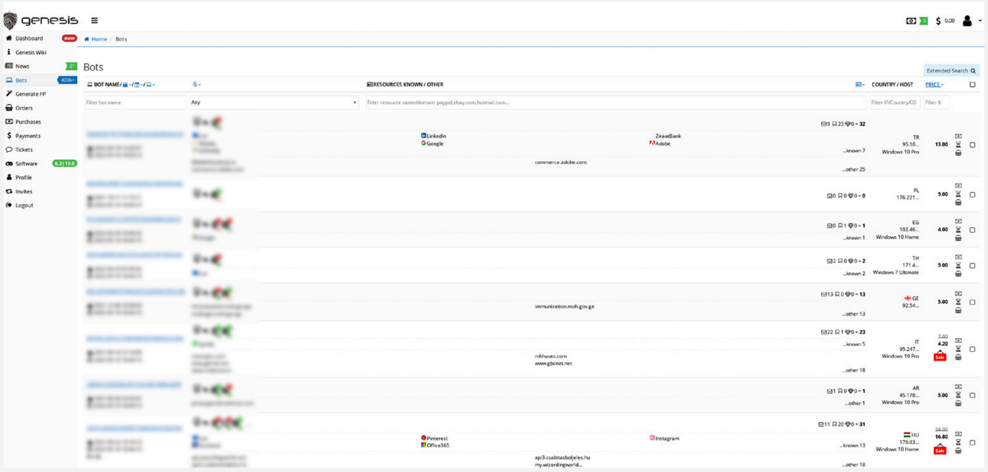


Figure 3. The distribution of available stealer malware

Apparently, RedLine and Vidar make up for the majority of the logs sold on RM, with RedLine coming out on top. This comes as no surprise, as the RedLine malware is inexpensive and widely distributed among hacking communities. Furthermore, methods of infection and distribution are well known and extensively shared in aforementioned communities.

Genesis Market

As opposed to its "Russian" counterpart, Genesis Market operates strictly on the clearweb, and is specialized solely in the sale of its bots, offering over 400 thousand bots at the time of writing.



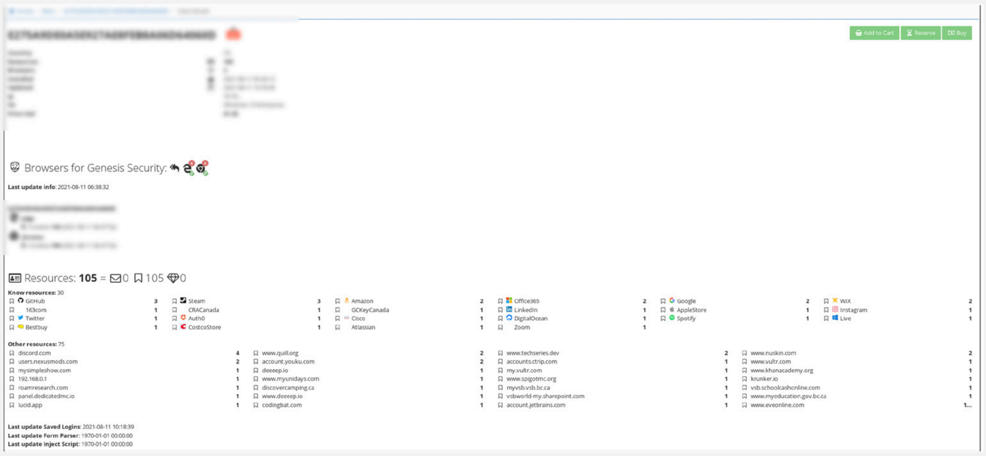
Bots

BOT NAME		RESOURCES KNOWN / OTHER				COUNTRY / HOST	PRICE
Filter bot name	Any	Filter resource name/domain: paypal,ebay.com,hotmail.com...				Filter IP/Country/OS	Filter $
[redacted]	[redacted]	LinkedIn Google	ZiraatBank Adobe	commerce.adobe.com	✉9 🔖23 💎0 = 32 ...known 7 ...other 25	TR 95.10... Windows 10 Pro	13.00
[redacted]	[redacted]				✉0 🔖0 💎0 = 0	PL 176.221...	5.00
[redacted]	[redacted]				✉0 🔖1 💎0 = 1 ...known 1	EG 102.46... Windows 10 Home	4.00
[redacted]	[redacted]				✉2 🔖0 💎0 = 2 ...known 2	TH 171.4... Windows 7 Ultimate	5.00
[redacted]	[redacted]			immunization.moh.gov.ge	✉13 🔖0 💎0 = 13 ...other 13	GE 92.54...	5.00
[redacted]	[redacted]			mhhauto.com www.gbcnet.net	✉22 🔖1 💎0 = 23 ...known 5 ...other 18	IT 95.247... Windows 10 Pro	~~7.00~~ 4.20 Sale
[redacted]	[redacted]				✉1 🔖0 💎0 = 1 ...other 1	AR 45.178... Windows 10 Pro	5.00
[redacted]	[redacted]	Pinterest Office365	Instagram	api3.csabitasboljeles.hu my.wizardingworld...	✉11 🔖20 💎0 = 31 ...known 13 ...other 18	HU 176.63... Windows 10 Home	~~28.00~~ 16.80 Sale

Figure 4. Genesis Market Bots overview

The listings on Genesis provide the following information before purchase:

- The country where the bot is located
- The number of resources attached to the bot
- The number of browsers from which information was stolen (Fingerprints)
- The date on which the bot was installed, and last updated
- A partial IP address
- The operating system of the bote
- A list of all resources available



[redacted]

Browsers for Genesis Security:

Last update info: 2021-08-11 06:38:32

[redacted]

Resources: **105** = ✉0 🔖105 💎0

Know resources: 30

GitHub	3	Steam	3	Amazon	2	Office365	2	Google	2	WIX	2
163com	1	CRACanada	1	GCKeyCanada	1	LinkedIn	1	AppleStore	1	Instagram	1
Twitter	1	Auth0	1	Cisco	1	DigitalOcean	1	Spotify	1	Live	1
Bestbuy	1	CostcoStore	1	Atlassian	1	Zoom	1				

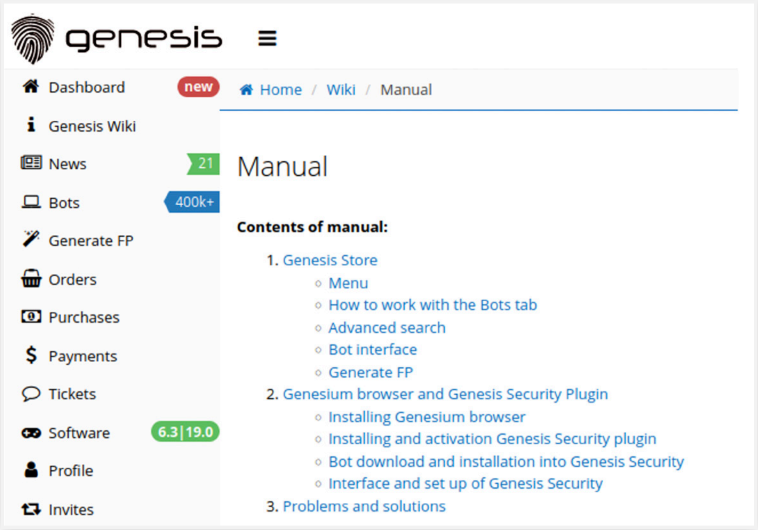
Other resources: 75

discord.com	4	www.quill.org	2	www.techseries.dev	2	www.nuskin.com	2
users.nexusmods.com	2	account.youku.com	2	accounts.ctrip.com	1	www.vultr.com	1
mysimpleshow.com	1	deeeep.io	1	my.vultr.com	1	www.khanacademy.org	1
192.168.0.1	1	www.myunidays.com	1	www.spigotmc.org	1	krunker.io	1
roamresearch.com	1	discovercamping.ca	1	myvsb.vsb.bc.ca	1	vsb.schoolcashonline.com	1
panel.dedicatedmc.io	1	www.deeeep.io	1	vsbworld-my.sharepoint.com	1	www.myeducation.gov.bc.ca	1
lucid.app	1	codingbat.com	1	account.jetbrains.com	1	www.eveonline.com	1...

Last update Saved Logins: 2021-08-11 10:18:39
Last update Form Parser: 1970-01-01 00:00:00
Last update Inject Script: 1970-01-01 00:00:00

Figure 5. A Genesis Bot listing example

As previously mentioned, when buying a bot on Genesis, the malicious actor not only gains access to the victim's credentials of all listed "Resources", but the marketplace in itself offers a very detailed guide explaining how to use the bot fingerprint.



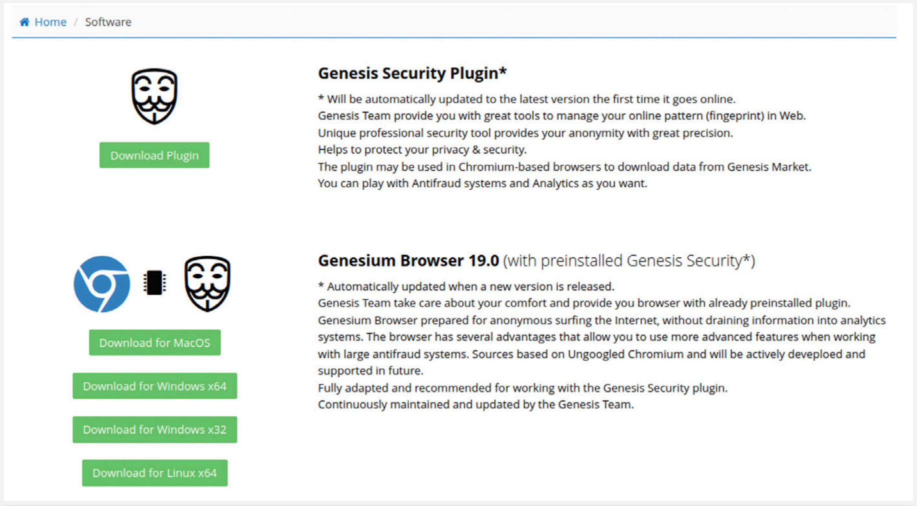
Manual

Contents of manual:

1. Genesis Store
   - Menu
   - How to work with the Bots tab
   - Advanced search
   - Bot interface
   - Generate FP
2. Genesium browser and Genesis Security Plugin
   - Installing Genesium browser
   - Installing and activation Genesis Security plugin
   - Bot download and installation into Genesis Security
   - Interface and set up of Genesis Security
3. Problems and solutions

Figure 6. Genesis Market's manual's table of content

To make full use of the *Browser Fingerprints* sold on Genesis, the online store distributes its own software; a browser plugin that can be used on various browsers to easily "install" the fingerprint a malicious actor has bought, as well as a complete browser based on the open source project Chromium that comes with the preinstalled plugin. We won't go into too much detail as the point of this article is mostly to analytically compare the two markets, but if you're interested in learning more about the inner workings of Genesis, this **report** from NETACEA should answer most of your questions.



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 7. Software available on Genesis Market

Genesis Market vs Russian Market - At a Glance

Before starting our more in-depth analysis, two elements immediately drew the attention of our researchers; the amount of bots / logs for sale and their pricing. Indeed, at the time of writing, Russian Market had over 2.7 million logs available for sale, whereas Genesis had about 425 thousand bots listed on the market. Furthermore, the volume at which new infected devices were published on both markets varied greatly, with Russian Market averaging 40,000 new devices per week, and Genesis averaging a little over 1,600 new bots.

As for the price, the cost of a bot on Genesis Market varies greatly, ranging from less than a dollar to a little over 170$. On the other hand, Russian Market recent logs seem to be priced at exactly 10$ with no variance in between logs, going down to about 5$ for older ones. Interestingly, 170$ for a Genesis bot is far from what used to be their higher end pricing; in fact, our research report from last year analyzing Canadian bots mentions bots going for upwards of 350$. Perhaps this new lower pricing on Genesis is a reflection of the evolving ecosystem and increasing competition.

Whilst we are fully aware that Russian Market and Genesis Market don't provide the exact same product, for the intent of this article we'll treat both their offerings as infected devices, and compare them as such.

The major differences in volume of both markets leads our team to think the methods employed for distributing their malware must vary. Considering both markets publish the Operating System (OS) of the infected device, let's look at which OS is the most represented on each platform.

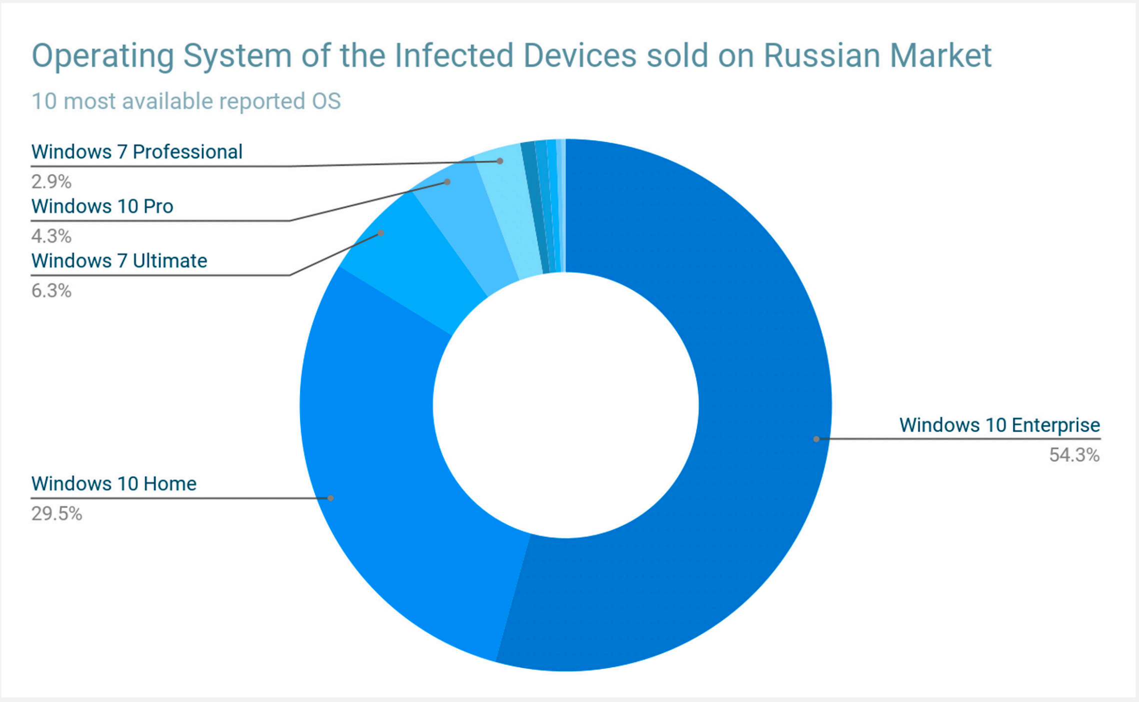


Figure 8

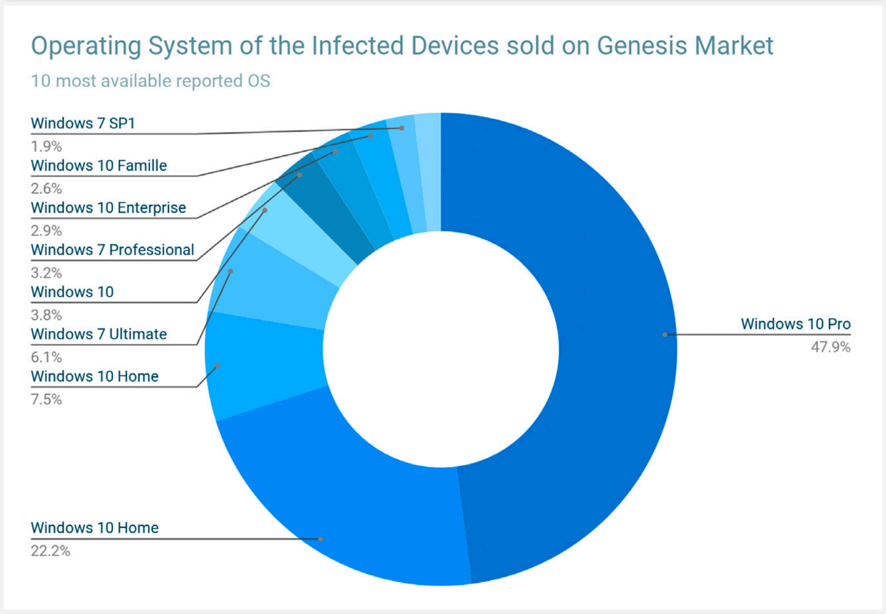


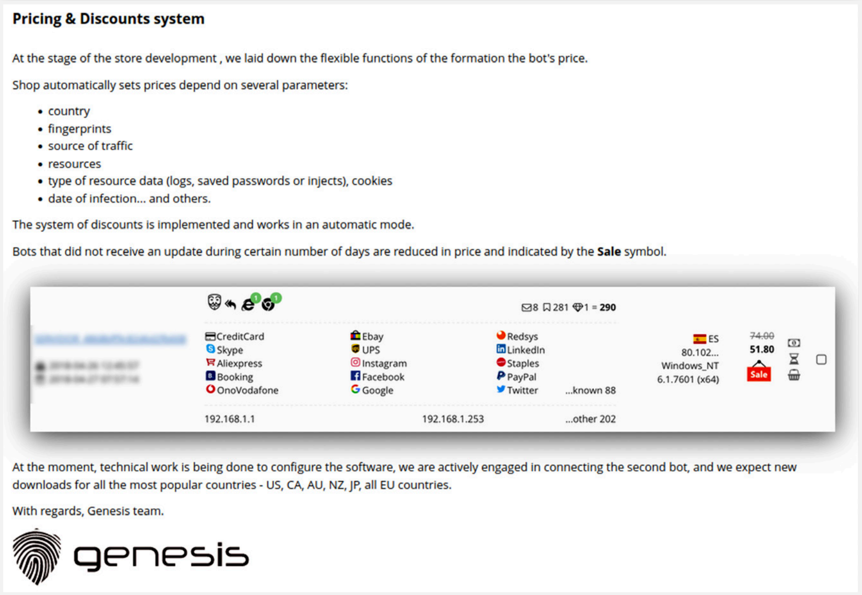
Figure 9

As showcased in Figure 8, more than half of available infected devices on the Russian Market are a Windows 10 Enterprise machine, whereas the same OS on Genesis represents a measly 2.9% of available devices.

The major differences in Operating System distribution further confirms our research team's hypothesis that the malware distribution methods must vary greatly between the markets; coupled with the vast discrepancy in pricing and volume, it seems the modus operandi of both markets must be very distinct, despite operating in the same sphere.

Going back to the pricing of the infected devices, the fact that Russian Market seems to have a uniform pricing model, independent of the infected device's location, number of available credentials, or type of service available leads our research team to believe the platform is a fully automated operation; where sellers can upload big batches of infected devices that they infected through various means, and Russian Market simply displays them for sale without analyzing their content.

On the other hand, Genesis Market, as previously mentioned, sees the prices of their bots vary greatly; they even published a short explanation of how they price their bots.



Pricing & Discounts system

At the stage of the store development , we laid down the flexible functions of the formation the bot's price.

Shop automatically sets prices depend on several parameters:

- country
- fingerprints
- source of traffic
- resources
- type of resource data (logs, saved passwords or injects), cookies
- date of infection... and others.

The system of discounts is implemented and works in an automatic mode.

Bots that did not receive an update during certain number of days are reduced in price and indicated by the **Sale** symbol.

[redacted]
[redacted]

✉8 🔖281 💎1 = **290**

CreditCard
Skype
Aliexpress
Booking
OnoVodafone
Ebay
UPS
Instagram
Facebook
Google
Redsys
LinkedIn
Staples
PayPal
Twitter
...known 88

192.168.1.1
192.168.1.253
...other 202

ES
80.102...
Windows_NT
6.1.7601 (x64)

~~74.00~~
51.80
Sale

□

At the moment, technical work is being done to configure the software, we are actively engaged in connecting the second bot, and we expect new downloads for all the most popular countries - US, CA, AU, NZ, JP, all EU countries.

With regards, Genesis team.

genesis

Figure 10. Genesis Market Pricing Algorithm

In the hopes of further understanding their pricing algorithm, our research team sampled 30,000 recently installed or updated bots, and analyzed which factors make the price of bots vary. Following the order listed on the Genesis website, let's look at how the bot's country, and listed resources impact its price.

Firstly, the average price of bots from our sample was 15.77$, and the median price 10$, with an average of 337 saved resources available. Saved resources on Genesis can vary, as some will come with either a username, password, cookie, or a combination of the former, with recent cookies being the most valuable since they allow malicious actors to take over a potentially working session and not be met with a 2 factor authentication request. For the purposes of this research, we've elected to count resources indiscriminately.

Secondly, we have analyzed the average price of bots depending on the country in which they are located.

Country	Average bot Price
Canada	$50.08
New Zealand	$32.13
United States	$26.15
Kenya	$24.37
Venezuela	$23.32
Nigeria	$21.24
Dominican Republic	$20.78
United Kingdom	$20.65
Argentina	$19.61
Ivory Coast	$19.40

Figure 11. Top 10 Countries with the highest average price

Whilst our team expected the top 10 to be mostly comprised of developed countries, we were surprised to find a mix of developed and developing countries. However, upon further inspection, we found that some of the countries that made their way into the top had a very high Crypto Adoption Index (CAI), according to this report by Chainalysis, with Kenya figuring at the 5th position of the CAI ranking, Venezuela 7th, Nigeria 6th, Argentina 10th, and both Dominican Republic and Ivory Coast hovering around the 50th rank.

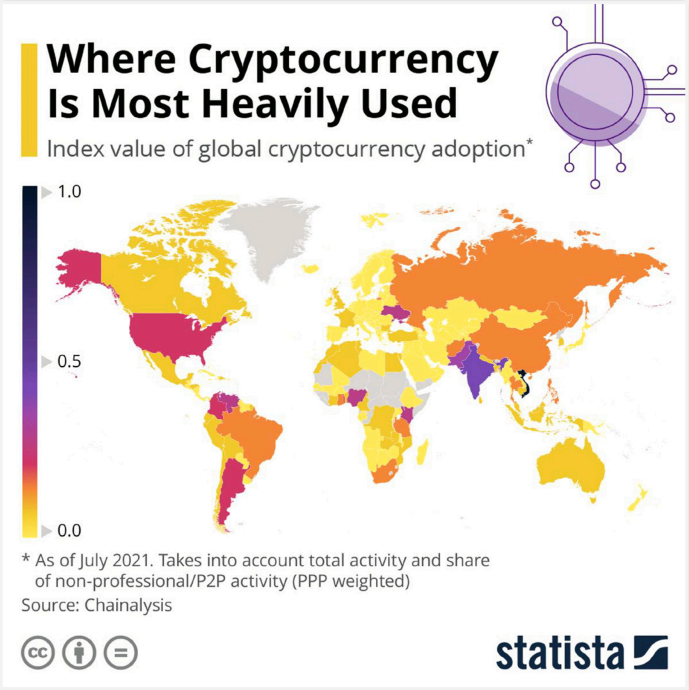

Where Cryptocurrency Is Most Heavily Used
Index value of global cryptocurrency adoption*
1.0
0.5
0.0
* As of July 2021. Takes into account total activity and share of non-professional/P2P activity (PPP weighted)
Source: Chainalysis
statista

Figure 12

Although it was definitely surprising to see Canada being featured as the most expensive country on average for which to purchase bots, since this contradicts some of our findings from our last report, this could be explained by other factors (that we'll highlight below) or simply an increase in demand. After all, Genesis Market themselves puts Canada as being in the "most popular" countries.

This conclusion ties in nicely to our next analysis element; the type of resource offered. Considering the purpose of those bots to be mostly tailored around committing fraud in its broader sense, our team was expecting that the presence of a financial service would affect the bot's price.

Since we couldn't possibly come up with a list of all banking websites from the whole world, we've established a list of keywords that we feel are widely and internationally adopted, in order to identify a potential correlation between the presence of a financial service in the resources category of the bots listing. The list we've opted to use is the following (in no specific order): Paypal, Bank, Paysafe, Binance, CoinBase, Kucoin, f2pool, NiceHas, Monero, and Bitcoin. We then averaged the price of the bots if any of the aforementioned terms were featured in the bot's Resource section.

	Average Price	Median Price
With Financial Service	$32.79	$24.00
Average Bot Price	$15.77	$10.00
Without Financial Service	$13.28	$9.00

Figure 13. The price of infected devices based on the presence of a linked financial service.

As you can see, there is a very strong correlation between the presence of a financial service, including cryptocurrency, and the price of a bot on Genesis Market, which further explains why countries with a higher Crypto Adoption Index were featured in the top 10 countries with the most expensive bots, as the chances of an infected device featuring a log-in to a crypto exchange is higher.

Finally, Genesis Market specifies "resources" as being a factor in a bot's pricing, which our team understood as "the number of resources available". Here is the result of the analysis of whether the number of resources affects the price of a bot.

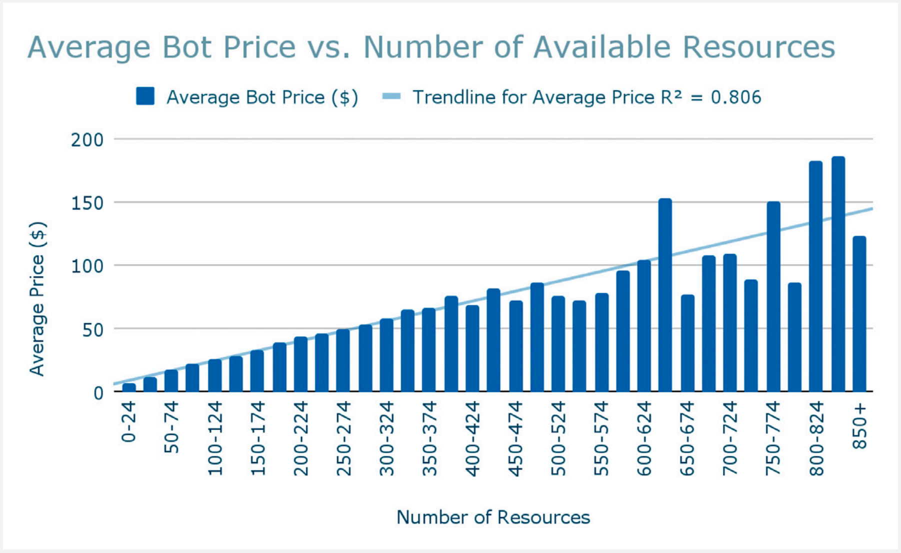


Figure 14

The results are clear, once again there is a strong correlation between the number of available resources and the price of a bot, with a greater variance above 450 available resources.

All things considered, we have found the single most influential factor of a bot's price to be the presence of a linked financial service, followed closely by the number of resources available. It is worth noting that a bot's value diminishes quickly over time, and that this might be the most influential factor; however, to circumvent this issue, our team worked with a sample of relatively fresh bots, in the hopes of mitigating the effect of the bot's freshness on its price.

Geographical Findings

Now, based on the assumption that Russian Market and Genesis Market operate differently, from their initial infection method, to distribution, use, and pricing, a question would be whether their geographical targets differ? For example, we know that Genesis Market openly admits that there is higher demand for bots located in "Canada, United States, Australia, New Zealand, and all European Union countries", would this be represented in the number of available bots for sale?

Using the same 30,000 bot sample from Genesis, and a 180,000 stealer logs sample from Russian Market, we've analyzed the number of infected devices available per 6 million population and 1 million population (for Genesis Market and Russian Market, respectively). Here are our results.

	Russian Market	Genesis Market
Average number of infected devices per country	634	724
Median number of infected devices per country	485	121

Figure 15. Available infected devices per country, proportional to their population.

As you can see, both sources seem to be heavily positively skewed, leading our team to believe there is indeed some geographical targeting on their end. Let's look at which countries are more targeted by both marketplaces, once again, proportional to their respective populations.

Russian Market Most Targeted Countries		Genesis Market Most Targeted Countries	
Anguilla	2599	Portugal	15928
Brunei	2318	Hungary	9046
Portugal	2284	Romania	8210
Lithuania	2205	Croatia	5989
Dominica	2000	Italy	5679
Maldives	1939	Bulgaria	5575
Serbia	1938	Georgia	4843
Romania	1807	Slovakia	4443
Bosnia and Herzegovina	1770	Spain	4345
Hungary	1768	Greece	4196

Figure 16. Countries with the most available infected devices for sale, proportional to their population.

Surprisingly, on Genesis Market there seems to be no indication that some of what they consider "popular countries" are more targeted. However, looking specifically at the number of available infected devices in G20 countries, the data portrays a different picture.

G20 Members	Russian Market	Genesis Market
Argentina	795	2,440
Australia	211	400
Brazil	978	107
Canada	198	285
China	5	3
France	678	3,279
Germany	504	862
India	289	11
Indonesia	812	80
Italy	668	5,679
Japan	50	74
South Korea	633	200
Mexico	358	28
Russia	25	0
Saudi Arabia	602	67
South Africa	472	50
Turkey	689	1,639
United Kingdom	322	746
United States	150	153
European Union	824	3842
Average	**463**	**997**
G20 vs Global Average	73.07%	137.72%

Figure 17. G20 member countries and the number of available infected devices, proportional to their population.

Evidently, it seems Genesis Market does indeed target G20 member countries more than average, contrarily to Russian Market. As of now, our researchers aren't exactly sure why that may be. Coupled with a significant difference in Operating System distribution, it strongly suggests a vastly different approach in the malware distribution methods of both platforms.

Conclusion

Here ends our comprehensive analysis of both Markets; although offering a similar product, all things considered it appears they follow a different approach when it comes to their infection and distribution strategies.

Now, is there any way for you, the average computer user, to prevent being infected with Stealer Malware? Our team recommends taking the following measures to reduce the chances of being infected, and minimize the damage that could be done in the worst case scenario; although convenient, storing credentials in your web browser is a **security risk**, instead, use a dedicated password manager which requires a master password to unlock; whenever available, enable Multi Factor Authentication; and finally, be wary of potential **phishing** emails, always look at the sender's email address. Stay safe!

About Flare

Flare provides solutions to protect your sensitive data. Our AI-driven technology monitors the dark, deep and clear web as well as your digital footprint. It searches for data leaks, and delivers actionable intelligence. Flare constantly crawls the dark, deep and clear web. It stores, analyzes and structures billions of data points to deliver actionable intelligence through its intuitive platform and API. Flare monitors illicit markets, leaked credentials, technical leaks (API keys, SSH keys, secrets, etc.) and newly-registered domains to detect data breaches caused by human error or by malicious actors to prevent cyber fraud and damage to brand and reputation.

flare.systems • **hello@flare.systems**

flare