NETACEA

Buying Bad Bots Wholesale: The Genesis Market

Contents

INTRODUCTION

Criminals have long used online black markets to trade illicit commodities, using the anonymity of the internet to go undetected by law enforcement. Whereas marketplaces like Silk Road famously trade in commodities like illegal drugs, a new kind of marketplace has emerged for assets perhaps even more sought after – stolen user data.

Although anti-fraud and cybersecurity systems aim to protect user data, bot operators have unearthed the signals used to detect illegitimate use of online services. Using targeted malware attacks and account takeover (ATO) bots, detailed information is collected from infected devices, allowing bots to mimic these signals exactly, bypass defences, and gain access to large amounts of private, financial or political information.

The "bots" that mimic users are often cheap, require little technical know-how to use, and can be bought wholesale on a growing number of hidden marketplaces.

The most popular marketplace of this kind, Genesis Market, is accessible from the open web but is obscured from law enforcement behind a closely guarded invitation-only veil. Although highly illegal, its operations are run in a professional and even user-friendly manner. The Genesis marketplace includes terms and conditions, an FAQ, frequently updated utility software, and even a support desk with ticket system for customer queries.

This Aladdin's cave of criminally obtained data is growing at an alarming rate. Hundreds of new "bots", or stolen digital identities, are added daily, with the total number available rising from 100,000 in April 2019 to over 350,000 in March 2021, with over 18,000 added each month. The level of access available to buyers of these bots is truly staggering. Almost anything accessed digitally by victims of these bots can be accessed by Genesis customers, including logins to online services, autofill information and even bank details.

> The number of stolen digital identities available on the Genesis Market has risen from 100,000 in April 2019 to over 350,000 in March 2021, with over 18,000 added each month.

THE GENESIS MARKET

The Genesis Market is an invite-only deep web marketplace that specialises solely in the sale of what the market owners term, bots. However, unlike the generally accepted use of the term bots, to mean the automated functioning of a task, the bots for sale on the Genesis Market instead represent the output of those tasks.

The tasks that Genesis Market bots undertake is the large-scale infection of consumer devices to steal their fingerprints, cookies, saved logins and autofill form data. That data is packaged up and put for sale on the Genesis Market. Upon purchase, consumers are provided with a custom browser to load the data into and may browse the internet masquerading as the hapless victim, use saved logins to access their accounts and where login cookies exist – continue a victim's session. All without any access to the original device.

The Genesis Market represents a significant step forward for attackers challenging client-side detection mechanisms.

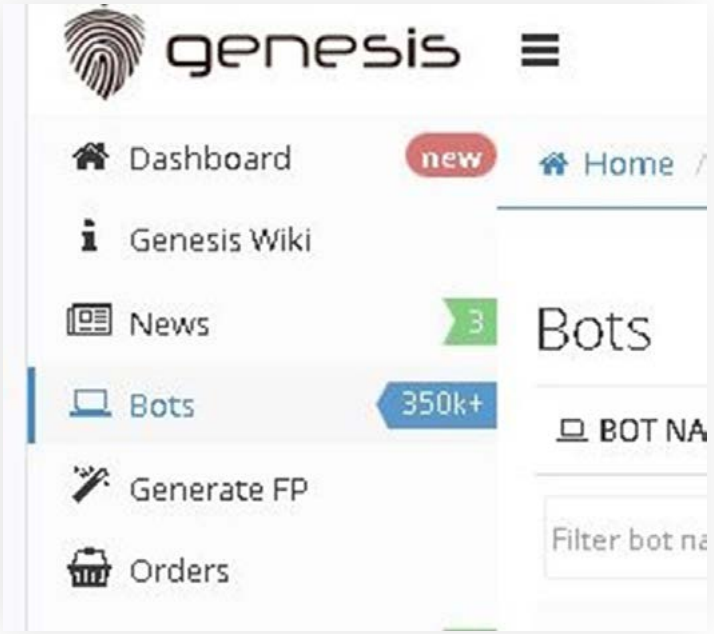
GENESIS MARKET BOTS

Each bot for sale on the Genesis Market represents the proffering of data that has been exfiltrated from a compromised consumer device, for a fee. The data may consist of any, or all of, the following types:

After purchase, the Genesis Market offers a browser for download, into which the stolen data can be loaded. Depending on how a given site handles user sessions, certain accounts may not require a login to be made and a session may be continued. For those that require re-authentication, the use of stolen credentials in combination with the device fingerprint may be enough to circumvent controls reliant on client-side signals.

Fig 1 shows a selection of the 350,000 bots currently for sale on the market. There are several ways in which the marketplace may be searched, such as by the accounts accessible with the bot, price, location and how many browser fingerprints are present on a given bot. Each listing then provides an overview of the bot for sale, such as which known accounts exist on the device, the time the device was compromised, its most recent update and information on the infected device itself.

Fig 1:



PURCHASING A BOT

Bots can be purchased for as little as 70c and upwards of $370 for bots with significant amounts of data on them. The price is differentiated (and calculated automatically according to the Genesis Market's wiki) by the volume of data present on a device. It is conceivable that the most expensive data sets are due to the wealth of data that could exist on shared devices.

The summary of each bot for sale provides a good overview on what to expect from a purchase. Summaries include:

- The various browsers in use on a victim's machine
- If fingerprints for those browsers are present
- How many cookies each browser comes with and which services those cookies are from
- The victim's country of origin and their device operating system

Fig 2 shows the resources that exist on a bot in the upper price range of the market. There are multiple accounts for many well-known services and a wealth of other accounts from services unrecognised by Genesis; such as academic accounts (not shown).

Fig 2:

To access the browser into which the data may be loaded, a purchase must be made on the store. Purchases are made by loading a wallet on the store with an amount of Bitcoin and then choosing a bot to buy. Once bought, the buyer has exclusive access to the data including any updates that may come as the device remains infected.

THE GENESIS SECURITY PLUGIN AND GENESIUM BROWSER

The Genesis Market provides two options to the buyers of bots who wish to browse the internet as a victim. The first is by offering a Chromium-based browser plugin, Genesis Security, to be loaded into an attacker's existing browser setup. The second provides the Genesis Security plugin already loaded into a Chromium-based browser, Genesium. Genesium is a 'degoogled' version of Chromium maintained by the Genesis Market owners.

Either way, once a bot has been purchased and the Genesis Security plugin loaded by whatever means, the bot data may be loaded into the browser and the internet browsed as normal. The plugin does have the capability to tunnel traffic through a SOCKS5 proxy. However, this functionality is very limited. Only one SOCKS proxy may be supplied and it cannot be one that requires authentication; this can be worked around using an additional Chrome plugin.

Fig 3:

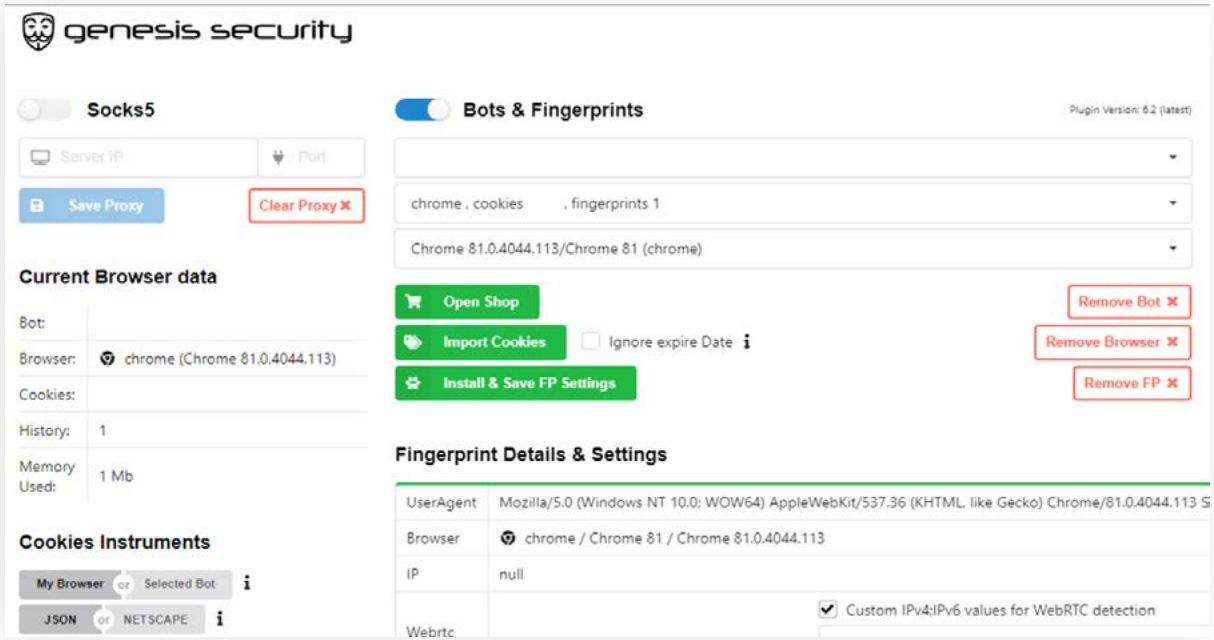
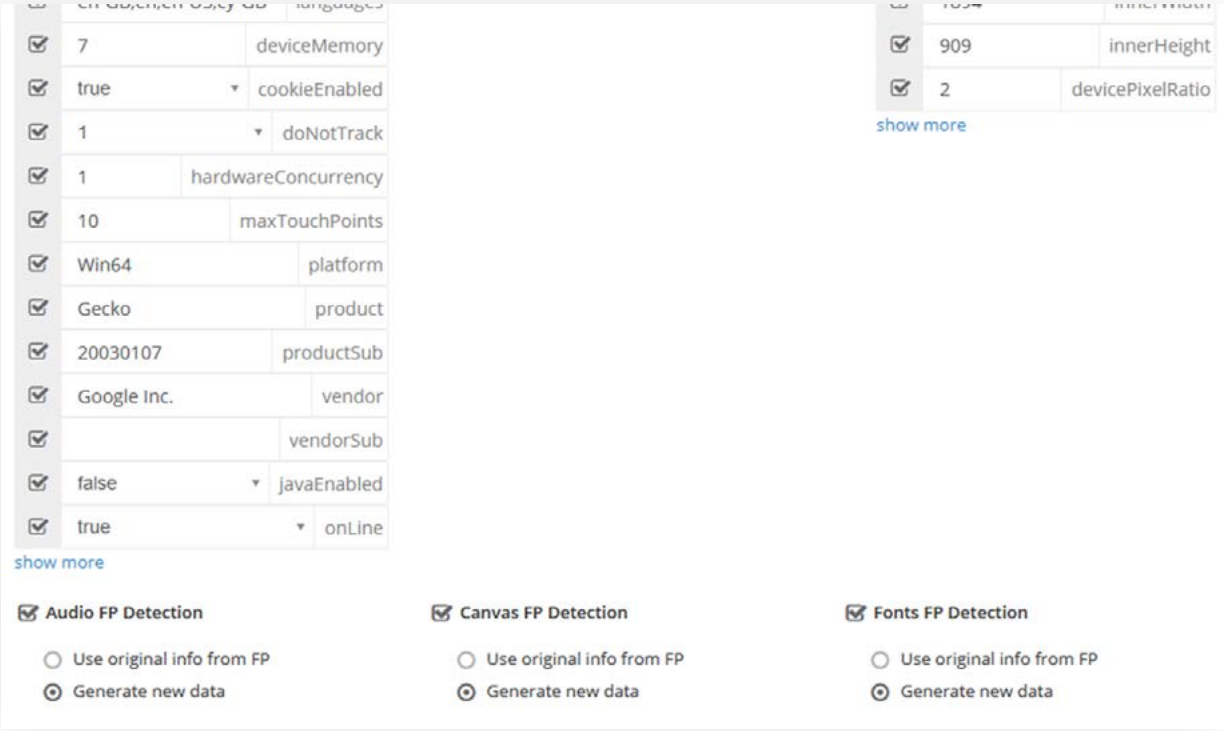


Fig 4 shows part of the final step of fingerprint generation, in which any of the generated data points may be edited and, ostensibly, validated prior to use.

Fig 4:



PRIVACY, ANONYMITY AND ANTIDETECT BROWSERS

With focus applied to circumventing client-side signals, Genesium and the Genesis Security plugin fall under the category of antidetect browsers. These browsers are, according to their developers, designed with privacy in mind. But it's plain to see the intention is to avoid tracking and detection of antifraud technology.

The Genesis Market's solution to avoid entrapment by sending insufficient, contradictory or no signals is to infect legitimate devices so that genuine fingerprints and associated browser data may be purchased and used at low cost. This is an interesting model as it addresses two potential problems that other solutions may face.

The first is cost. Currently version 7.7 of the eponymous antidetect browser 'Antidetect' costs $600 to buy outright or can be used on a subscription basis for $100 a month. The latest version of Antidetect, version 8, costs $2999 along with a monthly $100 service and support fee. This cost is prohibitive to many, potentially as a means to be less accessible to researchers and tinkerers, reserved for those serious about its intended use.

The second is on the fingerprints themselves. The Genesis Market offers genuine fingerprints for sale (with a mechanism to generate fingerprints should a bot come without). It is understood that competing antidetect browsers come only with the functionality to dynamically generate fingerprints, or in some cases, derive fingerprints from legitimately owned machines which presents its own limitations in the face of a botnet that has, at the time of writing, infected upwards of 350,000 machines.

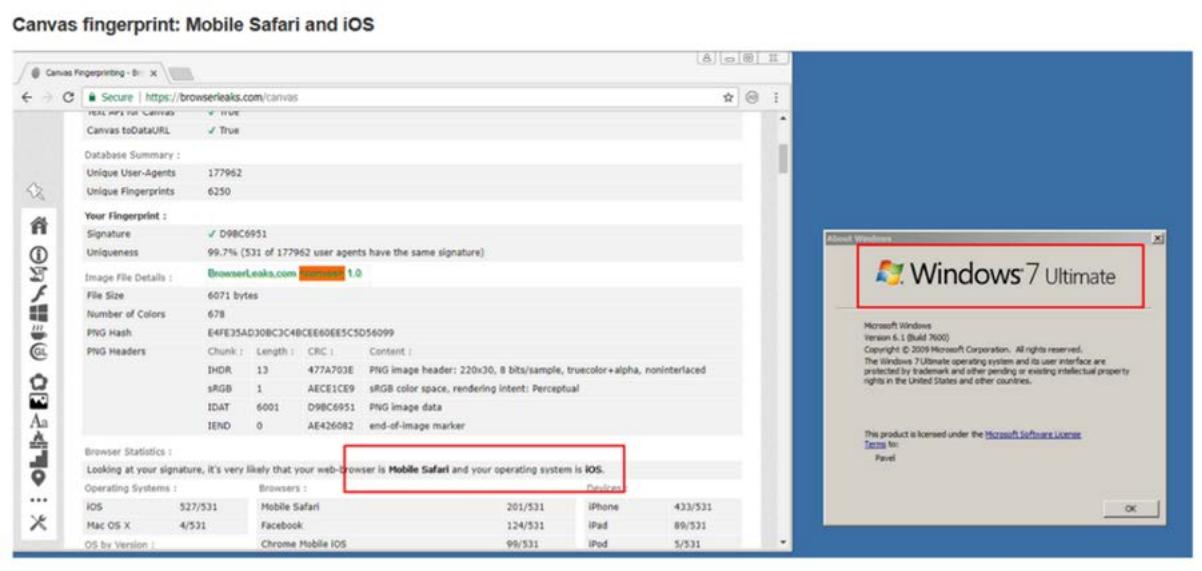
Considering the nature of antidetect browsers more broadly, many antidetect browser developers posit themselves as privacy advocates, concerned only that mainstream browsers can be subject to invasive examination which reveals more than is necessary about a user and their device to simply view a webpage. Those statements by antidetect browser developers are half-truths at best, their solution works to defend against fingerprinting, but the circumvention of controls is the objective regardless of any seemingly well-intentioned means.

However, despite the intention with which antidetect browsers are developed and used, their recognition that browser fingerprinting impacts user privacy resonates with others who differ far from the obscure user base of antidetect browsers. In recent years, the adoption of delivering content over HTTPS has increased significantly, with the GDPR ensuring the removal of personal data from whois records and the user agent string being depreciated in favour of client hints. As these measures take effect, a balance must be struck between protecting user privacy and allowing for the detection of malicious actors.

Apple's November 2019 'Safari Privacy Overview' describes, amongst many privacy improvements, how the development of Safari seeks to 'combat fingerprinting' by having the browser present '… a simplified version of the system configuration to trackers so more devices look identical, making it harder to single one out'. This effective immunisation of the herd of Safari users was not to be overlooked by the developers of antidetect browsers.

Fig 5 shows an Antidetect promotional image of their browser running on Windows 7, signalling itself as a Safari on iOS, with fingerprints to boot. This development is a boon to privacy advocates and antidetect browser developers, but of little solace to mechanisms reliant on what a client says about itself.

Fig 5:



The implementations of browser technology differ, but the overall direction has always been heterogeneous. Features are developed, adopted and become entangled into what a user expects of any browser regardless of its name. The development of browser technology is the communal decision of what is deemed good. Tabs are good, private browsing is good, exiling Java and Flash was good, ad-blocking is good - but is browser fingerprinting good? If other browser vendors follow suit, they may be less damning. It's possible that future browser development could see fingerprinting consigned to asking for user permission. Either way, with Safari users immune by herd, increasingly privacy aware users and the imposition of privacy law that has teeth leads us to wonder - could the death knell of browser fingerprinting soon begin to toll?

CONCLUSION

The market for sites like Genesis, which sell bots that impersonate legitimate users to allow access to compromised accounts, is booming; hundreds of thousands of bots are readily available and easy to use. Given the number of bots available at any one time, Genesis Market alone represents millions of dollars of illegal transactions passing from criminal to criminal.

The prevalence of stolen browser fingerprints, cookies, sessions and other identifiers is evidence that these signals are not enough to distinguish malicious users from genuine ones. This means that more sophisticated, AI-driven defences will become more and more crucial against the rising tide of sophisticated bot attacks.

Talk to Netacea today about our unique and patented approach to bot detection and mitigation. Our server-side approach and Intent Analytics™ engine asks what each user is doing and identifies suspicious activity in real-time. Because we are focused on behaviour rather than signals like fingerprinting and cookies, we stay one step ahead of the bots whilst staying invisible to legitimate users.

To find out more about Netacea's unique approach to stopping sophisticated bot threats, visit www.netacea.com/why-netacea or talk to our team today at hello@netacea.com.

GLOSSARY

Antidetect

A type of web browser designed to protect the privacy and anonymity of its users by either spoofing, repurposing or removing fingerprints and other identifying information

ATO (Account Takeover)

An attack making use of bots to gain access to user accounts with techniques such as credential stuffing and card cracking

Bots

Automated programs that carry out repetitive tasks on websites or applications

Client-side

Actions taken as a user attempts to access a website – Anything on the client-side is exposed to users and can be reverse-engineered

Dark web

Web content only accessible through specific software or authorisation, usually anonymously

Deep web

The part of the internet not accessible by traditional web search engines

Fingerprints

The unique identifiers left behind by browsers and devices when visiting websites, for example browser version, screen resolution, IP address or operating system

Malware

Malicious software that infects target devices unknowingly, passing information from or control of the device to the attacker remotely

Open web

The part of the internet indexed and accessible via traditional search engines, e.g. Google