



FATE OF GENESIS MARKET UNCERTAIN AS RUMORS OF FBI SEIZURE REMAIN UNCONFIRMED

ZEROFOX INTELLIGENCE

F-2023-04-05a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Threat Actor Activity, Infrastructure

April 5, 2023



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 8:00 AM (DST) on April 5, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Fate of Genesis Market Uncertain as Rumors of FBI Seizure Remain Unconfirmed

Key Findings

- As of this writing, longtime botnet marketplace Genesis Market forum admins have neither confirmed nor denied an alleged FBI seizure of their site but have announced forthcoming new domains in reputable dark web channels.
- Although accessing the deep web version of Genesis Market displays an alleged FBI seizure announcement, the site remains accessible, stable, and functional via the TOR address.
- ZeroFox assesses it is likely that the site admins will pivot to new domains and increase scrutiny of their users regardless of alleged law enforcement actions taken against the site.

Analyst Commentary

Botnet marketplace Genesis Market forum admins have neither confirmed nor denied the April 4, 2023, announcement of an alleged FBI seizure of its site but did recently announce forthcoming new domains in reputable dark web channels. Rumors and contradictory information about the alleged seizure continue to circulate within dark web channels, with historically reliable and well-regarded dark web actors claiming there has not been a seizure; some are even claiming this was a hoax orchestrated by the forum admins.

- Genesis Market admins took to their official personas in reputable dark web forums on April 5 to announce: "Our web-domains have been working since 2017, it's time to block. We will announce the new web-domains in the near future. We apologize for the inconvenience!"
- Ten hours later on April 5, 2023, at 5:00 AM (DST), " Web domains have been blocked, we are working at the old address in TOR: [address]. We are working on



launching the plugin via TOR. Now there will be a lot of fake shop domains, do not enter your username and passwords into unknown URLs. New web domains will be announced soon.”

- Although accessing the clear web version of the Genesis Market displays an FBI seizure announcement, the site remains accessible, stable, and functional via the TOR address, adding some heft to the argument that the seizure may have been orchestrated by the forum admins to troll law enforcement and research communities.
- Additionally, new and updated inventory, known as bots, have continued to populate the site since the seizure announcement was posted.

Over the past year, Genesis admins have been increasing scrutiny of their forum users to ban all suspected law enforcement officers and researchers from the site, shutting down completely between April and June 2022 and then reopening with the mandate for users to reassert their bonafides. Even before the announcement of the alleged seizure, Genesis required new users to contact the admins directly or buy an invite from a certified user on another dark web forum.

- In December 2022, Genesis admins began an intense campaign to ban accounts they deemed suspicious or duplicate.
- Rumors and intrigue are a staple of dark web culture, and it is likely that the site admins will pivot to new domains and increase scrutiny of their users regardless of the alleged law enforcement actions taken against the site.

What is Genesis Market

Genesis Market started in 2017 and is considered one of the most reputable and popular automated marketplaces; it has differentiated itself by making the process of exploiting stolen victim information relatively easy, thus lowering the bar to entry for lesser-skilled threat actors. This interesting business model focuses on providing high-quality data exfiltrated from single victim machines rather than larger quantities of bots in bulk. For example, the marketplace sells access to victim machines in the form of a bot that automatically updates any account changes made by the infected user—not a botnet log that only captures a snapshot in time of the victim’s computer at the moment it was offered for sale.

- Threat actors purchase the data and gain access to the entirety of a victim’s login credentials (username:password), cookies, and user agent (web browser), allowing them to imitate the victim’s browser session and a user agent to achieve unauthorized access in account takeover attacks

Additionally, the marketplace offers a proprietary browser extension on which a buyer may load the victim’s “fingerprint” (purchased bot), allowing the buyer to impersonate



the victim's digital footprint and decrease the likelihood of heightened security challenges in conducting attacks, such as account takeovers. Of note is the fact that Genesis does not broker in any victim data exfiltrated from Russia or CIS countries.



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.