FINAL PRESS RELEASE
5 April 2023, 14:00 CEST

Takedown of notorious hacker marketplace selling your identity to criminals

Genesis Market listed for sale the identities of over 2 million people when it was shut down

An unprecedented law enforcement operation involving 17 countries has resulted in the takedown of Genesis Market, one of the most dangerous marketplaces selling stolen account credentials to hackers worldwide. As a result of an action day on 4 April, this illegal service was shut down and its infrastructure seized.

Simultaneous actions were also carried out across the globe against the users of this platform, resulting in 119 arrests, 208 property searches and 97 knock and talk measures.

This international sweep was led by the U.S. Federal Bureau of Investigation (FBI) and the Dutch National Police (*Politie*), with a command post set-up at Europol's headquarters on the action day to coordinate the different enforcement measures being carried out across the globe.

Genesis Market was considered one of the biggest criminal facilitators, with over 1.5 million bot listings totalling over 2 million identities at the time of its takedown.

Why was Genesis Market so dangerous?

Genesis Market's main criminal commodity was digital identities. This marketplace would offer for sale what the market owners referred to as 'bots' that had infected victims' device through malware or account takeovers attacks.

Upon purchase of such a bot, criminals would get access to all the data harvested by it such as fingerprints, cookies, saved logins and autofill form data. This information was collected in real time – the buyers would be notified of any change of passwords, etc.

The price per bot would range from as little as $0.70 up to several hundreds of dollars depending on the amount and nature of the stolen data. The most expensive would contain financial information which would allow access to online banking accounts.

The criminals buying these special bots were not only provided with stolen data, but also with the means of using it. Buyers were provided with a custom browser which would mimic the one of their victim. This allowed the criminals to access their victim's account without triggering any of the security measures from the platform the account was on. These security measures include recognising a different log-in location, a different browser fingerprint or a different operating system.

In addition, unlike other criminal marketplaces, Genesis Market was accessible on the open web, although obscured from law enforcement behind an invitation-only veil. Its accessibility and cheap prices greatly lowered the barrier of entry for buyers, making it a popular resource among hackers.

The law enforcement response

The takedown of Genesis Market was a priority for law enforcement given the platform’s ability to facilitate all types of cybercrime.

Europol’s European Cybercrime Centre (EC3) has been supporting this investigation since 2019 by coordinating the international activity with the help of the Joint Cybercrime Action Taskforce (J-CAT) hosted at Europol. EC3’s support included data analysis, the organisation of operational meetings and the facilitation of the information exchange. A command post was also set-up at Europol’s headquarters in The Hague, the Netherlands to ensure the smooth running of the action day across the world.

Eurojust actively facilitated the cross-border judicial cooperation between the national authorities involved. The Agency hosted a coordination meeting in March 2023 to prepare for this week’s operation and hosted a command center on 4 April to resolve any legal issues arising during the parallel operations in 13 countries.

Commenting on this operation, the Head of Europol’s European Cybercrime Centre, Edvardas Šileris, said: “*Through the combined efforts of all the law enforcement authorities involved, we have severely disrupted the criminal cyber ecosystem by removing one of its key enablers. With victims located across the globe, the strong relationships with our international partners were critical in the success of this case*.”

How to tell whether your data was stolen

With over 1.5 million bots listed on Genesis Market, chances are that your credentials have already ended up for sale on this criminal marketplace.

The Dutch Police has developed a portal to check whether your information has been compromised. Visit https://www.politie.nl/checkyourhack and fill in your email address to control whether it is part of a Genesis Market leak.

If your digital identity has been stolen, here are the steps you should take:

1. **Run your antivirus programme.** In most cases, your antivirus will catch the malware and remove it. Only then should you change all your passwords – not before if you do not want the cybercriminals getting their hands on them.
2. **Notify relevant stakeholders.** Your bank, insurance company and any other important third party should be made aware of your identify theft.

Remember that cybercriminals are quick adapting their techniques to benefit from any opportunity. There are simple preventive actions you can take to make it more difficult for them to access your devices and data:

- If available, use antivirus software on all your electronic devices.
- Keep your software updated, including your browser, antivirus and operating system.
- Browse and download only official versions of software and always from trusted websites.
- Be wary while browsing the internet and do not click on suspicious links, pop ups or dialogue boxes.
- Think twice before clicking on links or attachments within unexpected emails.
- Set up unique passwords. Generate strong passwords or passphrases for each individual website and service. This is where the use of a password manager comes in handy.
- Activate multifactor authentication functionality whenever possible for all of your accounts.

The following law enforcement authorities took part in this investigation:

- **Australia:** Australian Federal Police (AFP), State and Territory Police Forces
- **Canada:** 25 Law Enforcement Agencies supported by Sûreté du Québec (SQ) & Royal Canadian Mounted Police (RCMP)
- **Denmark:** National Police (Politi)
- **Estonia:** Police and Border Guard Board (Politsei ja Piirivalveamet)
- **Finland**: National Bureau of Investigation (Keskusrikospoliisi/ Centralkriminalpolisen)
- **France:** National Police (Police Nationale)
- **Germany:** Federal Criminal Police Office (Bundeskriminalamt)
- **Italy:** National Police (Polizia di Stato)
- **Netherlands:** National Police (Politie)
- **New Zealand:** New Zealand Police - Ngā Pirihimana o Aotearoa
- **Poland:** Central Cybercrime Bureau (Centralne Biuro Zwalczania Cyberprzestępczości)
- **Romania:** National Police (Poliția Română)
- **Spain:** National Police (Policia Nacional) and Civil Guard (Guardia Civil)
- **Sweden:** Swedish Police Authoirity (Polisen)
- **Switzerland:** Federal Police (fedpol), Cantonal Police of Zurich (Kantonspolizei Zürich)
- **United Kingdom:** National Crime Agency (NCA)
- **United States**: Federal Bureau of Investigation (FBI)

Involved countries and partners

United States

EuroJust
Europe

Europol
Europe

The Netherlands

Canada

Australia

United Kingdom

Germany

Denmark

Poland

Sweden

Spain

France

Italy

Romania

Switzerland

Estonia

New Zealand

Finland

Partners

Trellix
The Netherlands

Computest
The Netherlands

Microsoft
USA