

Operation Cookie Monster: Feds seize “notorious hacker marketplace”

Enlarge / Domain seizure message at genesis.market.

reader comments

22 with

Share this story

An international law enforcement operation shut down a “notorious hacker marketplace” that sold access to infected devices and stolen account credentials, the US Department of Justice and Europol announced today. The operation targeting Genesis Market involved 17 countries, seized the platform’s infrastructure, and resulted in “119 arrests, 208 property searches, and 97 knock-and-talk measures,” Europol said.

The now-shuttered Genesis Market “advertised and sold packages of account access credentials—such as usernames and passwords for email, bank accounts, and social media—that had been stolen from malware-infected computers around the world,” the Justice Department said. The so-called “Operation Cookie Monster” seized 11 domain names pursuant to a warrant authorized by the US District Court for the Eastern District of Wisconsin.

While Genesis Market’s public website was taken down, its .onion domain was still accessible on the dark web using Tor today. Law enforcement is apparently still looking for at least some of the people behind the platform, as the domain

seizure message seeks tips from anyone who's been in contact with Genesis Market administrators. The US Treasury Department said Genesis Market "is believed to be located in Russia."

Europol said that "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."

Genesis Market reportedly had about 59,000 registered users. According to Europol, the market's "main criminal commodity was digital identities" or "what the market owners referred to as 'bots' that had infected victims' devices through malware or account takeovers."

Operation Cookie Monster was led by the FBI and Dutch National Police, with coordination by Europol.

Advertisement

"Custom browser" mimicked victims' devices

Genesis Market emerged in March 2018 and since then "has offered access to data stolen from over 1.5 million compromised computers around the world containing over 80 million account access credentials," the Justice Department said.

Upon purchasing a bot from Genesis Market, "criminals would get access to all the data harvested by it such as fingerprints, cookies, saved logins and autofill form data," Europol said. The cheapest bots sold for less than a dollar each but others fetched hundreds of dollars and provided access to online banking accounts.

Europol said that Genesis Market shoppers were "provided with

a custom browser which would mimic the one of their victim," letting them access victims' accounts "without triggering any of the security measures from the platform the account was on. These security measures include recognizing a different log-in location, a different browser fingerprint or a different operating system."

A Brian Krebs report described the Genesis offering as "a custom Web browser plugin which can load a Genesis bot profile so that the browser mimics virtually every important aspect of the victim's device, from screen size and refresh rate to the unique user agent string tied to the victim's web browser."

The DOJ said it accessed Genesis Market's user database. "The database contained the purchase and activity history on all users, which the feds say helped them uncover the true identities of many users," Krebs wrote.

Three big takedowns in the past year

The Genesis Market takedown follows similar actions against Hydra Market in April 2022 and BreachForums in March 2023. The DOJ claims it has "dismantled the darknet's largest marketplaces" due to those three operations over the last year.

The Justice Department said victim credentials obtained during Operation Cookie Monster were provided to HaveIBeenPwned.com, which helps you check whether you've been involved in a data breach.

The Treasury Office of Foreign Assets Control (OFAC) said it designated Genesis Market, meaning that "all property and interests in property of the entity that are in the United States or in the possession or control of US persons must be blocked and reported to OFAC." Additionally, anyone who

“engage[s] in certain transactions with the entity designated today may themselves be exposed to sanctions.”

<https://arstechnica.com/?p=1929514>