Operation Cookie Monster: police shut huge cybercrime site

April 5 2023, by Jan HENNOP

Europol said the operation against Genesis Market was 'unprecedented'

A global police operation has shut down one of the world's largest online marketplaces where cybercriminals can buy stolen identities and passwords, law enforcement agencies said on Wednesday.

Dubbed "Operation Cookie Monster", the swoop targeted Genesis Market, which sold hackers the identities of over two million people for as little as $0.70, they said.

Police arrested 119 people in an international operation led by the US Federal Bureau of Investigation (FBI) and Dutch police and involving law enforcement in 17 countries, with 208 raids worldwide.

The website was based in Russia, according to the US Treasury, which said it had imposed sanctions against Genesis Market.

The "unprecedented law enforcement operation" had taken down "one of the most dangerous marketplaces selling stolen account credentials to hackers worldwide", EU police agency Europol said.

People trying to access Genesis Market on Wednesday saw a screen saying, "This website has been seized" and "Operation Cookie Monster", along with a picture of a person in an FBI hoodie in front of a computer.

A cookie is a piece of computer data that makes it easier to reopen web pages. Cookie Monster is a blue, furry character from the US children's television series "Sesame Street".

'Huge blow'

Suspects were targeted in countries including Australia, Britain, Canada, the United States and more than 10 countries in Europe.

Britain's National Crime Agency said police had arrested 24 people there over Genesis Market.

"Its removal will be a huge blow to criminals across the globe," said Rob Jones, the NCA's Director General of Threat Leadership.

Europol said the site offered "bots" for sale that had infected victims' devices through malware or other methods, attracting criminals through "accessibility and cheap prices".

Prices for bots ranged from as little as $0.70 to several hundred dollars in the case of valuable bank account information, Europol said.

"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," it said.

Unlike so-called "dark web" services, Genesis was available on the open web "although obscured from law enforcement behind an invitation-only veil", the agency said.

Another 17 people were arrested in the Netherlands, where Dutch police launched a portal so people could check whether their details were on the site.

'Most dangerous'

Ruben van Well, Dutch police cybercrime team leader based in Rotterdam, said Genesis was "one of the most dangerous" sites aiding hackers.

"For example, it was possible to order and pay for things in web shops in the name of victims or, in certain cases, even to plunder entire bank, crypto or investment accounts," Van Well said.

He gave the example of a 71-year-old man who lost almost 70,000 euros from his investment account, with items ordered from web shops in his name.

"The victim told us he felt like he was treading water in a massive swimming pool with no idea how to get out," Van Well said.

French police said officers had arrested three men on Tuesday in France near Paris and Lyon.

"They were three major clients of the platform, who had bought several hundred bots, representing several thousand accesses," added the officer, a specialist in cybercrime.

Investigators in Germany searched 62 properties connected to 58 suspects and seized several electronic data devices, the BKA federal police and prosecutors in Frankfurt said in a joint statement.

The US Treasury Department said in a statement Genesis was believed to be located in Russia.

"This action was coordinated with the U.S. Department of Justice (DOJ) and international partners from a dozen countries," it added.

© 2023 AFP