U.S. Dept. of Justice: Genesis Market disrupted in international cyber operation

Posted on Wednesday, Apr 5, 2023

U.S. Attorney Gregory J. Haanstad for the Eastern District of Wisconsin joined the Attorney General and other Justice Department officials in announcing a coordinated international operation that resulted in the dismantlement of Genesis Market, a criminal marketplace accessible on the dark web and clear web that 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.

“Working across 45 of our FBI Field Offices and alongside our international partners, the Justice Department has launched an unprecedented takedown of a major criminal marketplace that enabled cybercriminals to victimize individuals, businesses, and governments around the world,” said Attorney General Merrick B. Garland. “Our seizure of Genesis Market should serve as a warning to cybercriminals who operate or use these criminal marketplaces: the Justice Department and our international partners will shut down your illegal activities, find you, and bring you to justice.”

“Yesterday, the Department of Justice and its partners dismantled the Genesis Market and arrested many of its users around the world,” said Deputy Attorney General Lisa O. Monaco. “Genesis falsely promised a new age of anonymity and impunity, but in the end only provided a new way for the Department to identify, locate, and arrest on-line criminals. The Department of Justice is shining a light on the internet’s darkest corners – in the last year alone, our agents, prosecutors, and partners have dismantled the darknet’s largest marketplaces – Hydra Market, BreachForums, and now Genesis. Each takedown is yet another blow to the

cybercrime ecosystem."

Since its inception in March 2018, Genesis Market has offered access to data stolen from over 1.5 million compromised computers around the world containing over 80 million account access credentials. Account access credentials advertised for sale on Genesis Market included those connected to the financial sector, critical infrastructure, and federal, state, and local government agencies. Genesis Market was also one of the most prolific initial access brokers (IABs) in the cybercrime world. IABs attract criminals looking to easily infiltrate a victim's computer system. Genesis Market offered for sale the type of access sought by ransomware actors to attack computer networks in the United States and around the world and published private-sector reports indicate that they indeed were used by ransomware actors to attack such systems.

Genesis Market was user-friendly, providing users with the ability to search for stolen access credentials based on location and/or account type (e.g., banking, social media, email, etc.). In addition to access credentials, Genesis Market obtained and sold device "fingerprints," which are unique combinations of device identifiers and browser cookies that circumvent anti-fraud detection systems used by many websites. The combination of stolen access credentials, fingerprints, and cookies allowed purchasers to assume the identity of the victim by tricking third party websites into thinking the Genesis Market user was the actual owner of the account.

Genesis Market users were located all over the world. Federal law enforcement has worked to identify prolific users of Genesis Market who purchased and used stolen access credentials to commit fraud and other cybercrimes. This effort resulted in hundreds of leads being sent to FBI field offices throughout the United States, as well as to foreign law enforcement partners. Further, as part of this operation, law enforcement seized, pursuant to court order, 11 domain names used to support Genesis Market's infrastructure.

"The operation being announced today is the direct result of the hard work, dedication, and exceptional collaborative efforts of the FBI and its partners around the globe," stated U.S. Attorney Haanstad. "Along with investigative partners and our Justice Department colleagues, my office remains committed to using all available tools to protect individuals from cybercriminals like those who operate these types of online marketplaces."

“Today’s takedown of Genesis Market is a demonstration of the FBI’s commitment to disrupting and dismantling key services used by criminals to facilitate cybercrime,” said FBI Director Christopher Wray. “The work in this case is a great example of the FBI’s ability to leverage our technical capabilities and work shoulder-to-shoulder with our international partners to take away the tools cyber criminals rely on to victimize people all across the world.”

As alleged in a domain seizure warrant authorized by the U.S. District Court for the Eastern District of Wisconsin, Genesis Market offered for sale victim credentials associated with the White House, Department of State, Justice Department, IRS, Department of Energy, U.S. Postal Service, National Aeronautics and Space Administration, and the Department of Defense.

The FBI Milwaukee Field Office investigated the case, with assistance from the U.K. National Crime Agency, Italy’s Polizia de Stato, Police of Denmark, Australian Federal Police, Royal Canadian Mounted Police, Canada’s Sûreté du Québec, Romanian Police, French Police Cybercrime Central Bureau, Spain’s Policia Nacional, Spain’s Guardia Civil, Germany’s Federal Criminal Police Service, Swedish Police Authority, Poland’s Central Bureau for Combating Cybercrime, Dutch National Police, Finland’s National Bureau of Investigation, Switzerland’s Office of the Attorney General, Swiss Federal Police, Estonia’s Prosecutor General’s Office, Iceland’s Metropolitan Police, and Eurojust.

The department appreciates the assistance provided by authorities in Bulgaria and Latvia in response to Mutual Legal Assistance requests.

Trial Attorneys Benjamin Proctor and Jessica Peck of the Criminal Division’s Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Farris Martini for the Eastern District of Wisconsin are handling the investigation. The Justice Department’s Office of International Affairs provided significant assistance.

Victim credentials obtained over the course of the investigation have been provided to the website Have I Been Pwned, which is a free resource for people to quickly assess whether their access credentials have been compromised (or “pwned”) in a data breach or other activity. Victims can visit HaveIBeenPwned.com to see whether their credentials were compromised by Genesis Market so that they can know whether to change or modify passwords and other authentication credentials that may have been compromised.

If you have been active on Genesis Market, in contact with Genesis Market administrators, or have been a victim and have a need to report, please email the FBI at FBIMW-Genesis@fbi.gov.