GOZNYM MALWARE: CYBERCRIMINAL NETWORK DISMANTLED IN INTERNATIONAL OPERATION

By Europol

Published: 2019-05-16 · Archived: 2026-04-05 14:06:08 UTC

An unprecedented, international law enforcement operation has dismantled a complex, globally operating and organised cybercrime network. The criminal network used GozNym malware in an attempt to steal an estimated $100 million from more than 41 000 victims, primarily businesses and their financial institutions.

A criminal Indictment returned by a federal grand jury in Pittsburgh, USA charges ten members of the GozNym criminal network with conspiracy to commit the following:

- infecting victims' computers with GozNym malware designed to capture victims' online banking login credentials;
- using the captured login credentials to fraudulently gain unauthorised access to victims' online bank accounts;
- stealing money from victims' bank accounts and laundering those funds using U.S. and foreign beneficiary bank accounts controlled by the defendants.

Over the course of the international operation, searches were conducted in Bulgaria, Georgia, Moldova and Ukraine. Criminal prosecutions have been initiated in Georgia, Moldova, Ukraine and the United States.

This operational success is a result of the international law enforcement cooperation between participating EU Member States (Bulgaria and Germany) as well as Georgia, Moldova, Ukraine and the United States (in alphabetical order). Europol, the European Agency for Law Enforcement Cooperation as well as Eurojust, the European Union's Judicial Cooperation Unit supported the case. This operation showcases how an international effort to share evidence and initiate criminal prosecutions can lead to successful operations in multiple countries.

Cybercrime as a service

The GozNym network exemplified the concept of "cybercrime as a service," with different criminal services such as bulletproof hosters, money mules networks, crypters, spammers, coders, organizers, and technical support.

The defendants advertised their specialised technical skills and services on underground, Russian-speaking online criminal forums. The GozNym network was formed when these individuals were recruited from the online forums by the GozNym leader who controlled more than 41 000 victim computers infected with GozNym malware. The leader of the GozNym criminal network, along with his technical assistant, are being prosecuted in Georgia by the Prosecutor's Office of Georgia and the Ministry of Internal Affairs of Georgia.

See the infographic

Highly Specialised and International Criminal Network

- A member of the network who encrypted GozNym malware to enable it to avoid detection by anti-virus tools and protective software on victims' computers is being prosecuted in Moldova by the Prosecutor General of the Republic of Moldova and the General Police Inspectorate of the Republic of Moldova.
- Another member from Bulgaria was already arrested by the Bulgarian authorities and extradited to the United States in December 2016 to face prosecution in Pittsburgh. His primary role in the conspiracy was that of a "casher" or "account takeover specialist" who used victims' stolen online banking credentials captured by GozNym malware to access victims' online bank accounts and attempt to steal victims' money.
- Several members of the network provided money-laundering services and were known as "cash-outs" or "drop masters." These individuals, including two from Russia and one from Ukraine, provided fellow members of the conspiracy with access to bank accounts they controlled that were designated to receive stolen funds from GozNym victims' online bank accounts.
- The five Russian nationals charged in the Indictment remain on the run. In addition to the two "drop masters" referenced above, these defendants include the developer of GozNym malware who oversaw its creation, development, management and leasing to other cybercriminals.
- Another Russian GozNym member conducted spamming operations on behalf of the conspiracy. The spamming operations involved the mass distribution of GozNym malware through "phishing" emails. The phishing emails were designed to appear legitimate to entice the victim recipients into opening them and clicking on a malicious link or attachment which facilitated the downloading of GozNym onto the victims' computers.
- Another Russian-born member of the network was a "casher" or "account takeover specialist." Like the Bulgarian defendant, he used victims' stolen online banking credentials captured by GozNym malware to access victims' online bank accounts and attempt to steal victims' money through electronic funds transfers into bank accounts controlled by fellow conspirators.

Avalanche Network

Bulletproof hosting services were provided to the GozNym criminal network by an administrator of the "Avalanche" network. The Avalanche network provided services to more than 200 cybercriminals, and hosted more than twenty different malware campaigns, including GozNym. The administrator's apartment in Poltava, Ukraine, was searched in November 2016 during a German-led operation to dismantle the network's servers and other infrastructure. Through the coordinated efforts being announced today, this alleged cybercriminal is now facing prosecution in Ukraine for his role in providing bulletproof hosting services to the GozNym criminal network. The prosecution will be conducted by the Prosecutor General's Office of Ukraine and the National Police of Ukraine.

The whole operation was conducted by the United States Attorney's Office for the Western District of Pennsylvania, the FBI's Pittsburgh Field Office, the Public Prosecutor's Office Verden (Germany), the Prosecutor's Office of Georgia, Prosecutor General's Office of Ukraine, Office of the Prosecutor General of the Republic of Moldova, Office of the General Prosecutor of Bulgaria, the Luneburg Police of Germany, Ministry of Internal Affairs of Georgia, National Police of Ukraine, General Police Inspectorate of the Republic of Moldova, and Bulgaria's General Directorate for Combatting Organized Crime. Europol and Eurojust played critical roles

in supporting this coordinated law enforcement operation. The U.S. Department of Justice’s Office of International Affairs also provided significant assistance.
