2019-05-16

16 May 2019

In an unprecedented, international law enforcement operation, a complex, globally operating and organised cybercrime network was dismantled. The criminal network used GozNym malware 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, charged 10 members of the GozNym criminal network with conspiracy to commit the following:

- infect victims' computers with GozNym malware designed to capture victims' online banking login credentials;
- use the captured login credentials to fraudulently gain unauthorised access to victims' online bank accounts;
- steal money from victims' bank accounts and laundering those funds using US and other beneficiary bank accounts controlled by the defendants.

The international law enforcement operation initiated criminal prosecutions against members of the network in four different countries. During the course of the 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 results in multiple countries.

Cybercrime as a service

The GozNym network exemplified the concept of 'cybercrime as a service' with different criminal services, such as cyberattacks, bulletproof 'hosters', money mule networks, 'crypters', spammers, coders, organisers, 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 and his technical assistant are being prosecuted in Georgia by the Prosecutor's Office of Georgia and the Ministry of Internal Affairs of Georgia.

Highly specialised and international criminal network

- A member of the network who encrypted GozNym malware to enable it to avoid detection by antivirus tools and protective software on victims' computers is being prosecuted in Moldova by the Prosecutor General 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. 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 their victims.
- 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, which were designated to receive stolen funds from GozNym victims' online bank accounts.
- Five Russian nationals charged in the indictment remain on the run. In addition to the two 'drop masters' referenced above, the group of these defendants includes the developer of the GozNym malware who oversaw its creation, development, management and leasing to other cybercriminals.
- One of the Russian GozNym members conducted spamming operations on behalf of the network. The spamming operations involved the mass distribution of GozNym malware through 'phishing' emails. Those emails were designed to appear legitimate to entice the recipients to open them and click on a malicious link or attachment that facilitated the downloading of GozNym onto the victims' computers.
- Another Russian-born member of the network was a 'casher' or 'account takeover specialist' who resided in Ukraine at the time of the attacks. 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 fund 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 service known as the 'Avalanche' network. The Avalanche network provided hosting services to more than 200 cybercriminals, and hosted more than twenty different malware campaigns, including GozNym. At the request of the United States and Germany, the administrator's apartment in Poltava, Ukraine, was searched in November 2016, during an operation led by Germany to dismantle the network's servers and other infrastructure. Through the coordinated efforts being announced today, this notorious cybercriminal will now face 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 (PGO) and the National Police of Ukraine.

The operation was conducted by the United States Attorney’s Office for the Western District of Pennsylvania, the Federal Bureau of Investigation (FBI)’s Pittsburgh Field Office, the Public Prosecutor’s Office (PPO) Verden (Germany), the PPO of Georgia, PGO of Ukraine, the Office of the Prosecutor General of the Republic of Moldova, the PGO of Bulgaria, the German Lüneburg Police, the Ministry of Internal Affairs of Georgia, the National Police of Ukraine, the General Police Inspectorate of the Republic of Moldova, and Bulgaria’s General Directorate for Combatting Organised Crime. Europol and Eurojust played a critical role in supporting this coordinated law enforcement operation. The Office of International Affairs of the US Department of Justice provided significant assistance.

Eurojust, the EU’s Judicial Cooperation Unit, facilitated the investigations by holding coordinating meetings, helping with the exchange of information and judicial best practice, and providing financial support and translation services. The successful result of the operation was also due to the active role of the Liaison Prosecutors from the United States and Ukraine appointed to Eurojust, as well as to the experience and expertise of the European Judicial Cybercrime Network, which is hosted at Eurojust since 2016.