GozNym Cyber-Criminal Network Operating out of Europe Targeting American Entities Dismantled in International Operation

justice.gov/opa/pr/goznym-cyber-criminal-network-operating-out-europe-targeting-american-entities-dismantled

May 16, 2019

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, May 16, 2019

Network Formed by Individuals Who Advertised their Specialized Technical Skills and Services on Underground Russian-Language Online Criminal Forums

A complex transnational organized cybercrime network that used GozNym malware in an attempt to steal an estimated $100 million from unsuspecting victims in the United States and around the world has been dismantled as part of an international law enforcement operation. GozNym infected tens of thousands of victim computers worldwide, primarily in the United States and Europe. The operation was highlighted by the unprecedented initiation of criminal prosecutions against members of the network in four different countries as a result of cooperation between the United States, Georgia, Ukraine, Moldova, Germany, Bulgaria, Europol and Eurojust.

United States Attorney Scott W. Brady of the Western District of Pennsylvania made the announcement at Europol, located in The Hague, Netherlands, along with his international partners.

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

"International law enforcement has recognized that the only way to truly disrupt and defeat transnational, anonymized networks is to do so in partnership," said U.S. Attorney Brady. "The collaborative and simultaneous prosecution of the members of the GozNym criminal conspiracy in four countries represents a paradigm shift in how we investigate and prosecute cybercrime. Cybercrime victimizes people all over the world. This prosecution represents an international cooperative effort to bring cybercriminals to justice."

Earlier today, the U.S. Attorney's Office for the Western District of Pennsylvania unsealed an Indictment returned by a federal grand jury in Pittsburgh charging 10 members of the GozNym criminal network with conspiracy to commit computer fraud, conspiracy to commit wire fraud and bank fraud, and conspiracy to commit money laundering. An eleventh member of the conspiracy was previously charged in a related Indictment. The victims of these crimes were primarily U.S. businesses and their financial institutions, including a number of victims located in the Western District of Pennsylvania.

> "This takedown highlights the importance of collaborating with our international law enforcement partners against this evolution of organized cybercrime," said FBI Pittsburgh Special Agent in Charge Robert Jones. "Successful investigation and prosecution is only possible by sharing intelligence, credit and responsibility. Our adversaries know that we are weakest along the seams and this case is a fantastic example of what we can accomplish collectively."

According to the Indictment, the defendants conspired to:

- infect victims' computers with GozNym malware designed to capture victims' online banking login credentials;
- use the captured login credentials to fraudulently gain unauthorized access to victims' online bank accounts; and,
- steal money from victims' bank accounts and launder those funds using U.S. and foreign beneficiary bank accounts controlled by the defendants.

The defendants reside in Russia, Georgia, Ukraine, Moldova and Bulgaria. The operation was an unprecedented international effort to share evidence and initiate criminal prosecutions against members of the same criminal network in multiple countries.

At the request of the United States, Krasimir Nikolov, aka “pablopicasso,” “salvadordali,” and “karlo,” of Varna, Bulgaria, was searched and arrested by Bulgarian authorities and extradited to the United States in December 2016 to face prosecution in the Western District of Pennsylvania. Nikolov’s 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 through electronic funds transfers into bank accounts controlled by fellow conspirators. Nikolov is named as a GozNym conspirator in the newly unsealed indictment, although he is charged in a related Indictment filed in the Western District of Pennsylvania. Nikolov entered a guilty plea in federal court in Pittsburgh on charges relating to his participation in the GozNym conspiracy on April 10, 2019. He is scheduled to be sentenced on Aug. 30, 2019.

Five of the named defendants reside in Russia and remain fugitives from justice. However, to overcome the inability to extradite the remaining defendants to the United States for prosecution, an unprecedented effort was undertaken to share evidence and build prosecutions against defendants in the remaining countries where they reside, including Georgia, Ukraine and Moldova. The prosecutions are based on shared evidence acquired through coordinated searches for evidence in Georgia, Ukraine, Moldova and Bulgaria, as well as from evidence shared by the United States and Germany from their respective investigations.

The GozNym network exemplified the concept of “cybercrime as a service.” According to the Indictment, the defendants advertised their specialized technical skills and services on underground, Russian-language, online criminal forums. The GozNym network was formed when these individuals were recruited from the online forums and came together to use their specialized technical skills and services in furtherance of the conspiracy.

According to the Indictment, Alexander Konovolov, aka “NoNe,” and “none_1,” age 35, of Tbilisi, Georgia, was the primary organizer and leader of the GozNym network who controlled more than 41,000 victim computers infected with GozNym malware. Konovolov assembled the team of cybercriminals charged in the Indictment, in part by recruiting them through the underground online criminal forums. Marat Kazandjian, aka “phant0m,” age 31, of Kazakhstan and Tbilisi, Georgia, was allegedly Konovolov’s primary assistant and technical administrator. Konovolov and Kazandjian are being prosecuted in Georgia for their respective roles in the GozNym criminal network.

Gennady Kapkanov, aka “Hennadiy Kapkanov,” “flux,” “ffhost,” “firestarter,” and “User 41,” age 36, of Poltava, Ukraine, was an administrator of a bulletproof hosting service known by law enforcement and computer security researchers as the “Avalanche” network. This network provided services to more than 200 cybercriminals, including Konovolov and Kazandjian, and it hosted more than 20 different malware campaigns, including GozNym. Kapkanov’s apartment in Poltava, Ukraine was searched in November 2016 during a German-led operation to dismantle the network’s servers and other infrastructure. Kapkanov was arrested for shooting an assault rifle through the door of his apartment at Ukrainian law

enforcement officers conducting the search. Through the coordinated efforts being announced today, Kapkanov is now facing prosecution in Ukraine for his role in providing bulletproof hosting services to the GozNym criminal network.

Alexander Van Hoof, aka “al666,” age 45, of Nikolaev, Ukraine, was a “cash-out” or “drop master” who provided fellow members of the conspiracy with access to bank accounts he controlled that were designated to receive stolen funds from GozNym victims’ online bank accounts.

Eduard Malanici, aka “JekaProf,” and “procryptgroup, age 32, of Balti, Moldova, provided crypting services to cybercriminals. Malanici crypted GozNym malware in furtherance of the conspiracy to enable the malware to avoid detection by anti-virus tools and protective software on victims’ computers. Malanici, along with two associates, is being prosecuted in Moldova.

Victims of the GozNym malware attacks include:

- An asphalt and paving business located in New Castle, Pennsylvania;
- A law firm located in Washington, DC;
- A church located in Southlake, Texas;
- An association dedicated to providing recreation programs and other services to persons with disabilities located in Downers Grove, Illinois;
- A distributor of neurosurgical and medical equipment headquartered in Freiburg, Germany, with a U.S. subsidiary in Cape Coral, Florida;
- A furniture business located in Chula Vista, California;
- A provider of electrical safety devices located in Cumberland, Rhode Island;
- A contracting business located in Warren, Michigan;
- A casino located in Gulfport, Mississippi;
- A stud farm located in Midway, Kentucky; and
- A law office located in Wellesley, Massachusetts;

Five Russian nationals charged in the Indictment who remain fugitives from justice include:

Vladimir Gorin, aka “Voland,” “mrv,” and “riddler,” of Orenburg, Russia. Gorin was a malware developer who oversaw the creation, development, management, and leasing of GozNym malware, including to Alexander Konovolov.

Konstantin Volchkov, aka “elvi,” age 28, of Moscow, Russia, provided spamming services to cybercriminals. Volchkov conducted spamming operations of GozNym malware 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 the emails and clicking on a malicious link or attachment, which facilitated the downloading of GozNym onto the victims’ computers.

Ruslan Katirkin, aka “stratos,” and “xen,” age 31, of Kazan, Russia, resided in Khmelnytskyi, Ukraine, during the time frame of the charged conspiracy. Katirkin, like Krasimir Nikolov, was 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 through electronic funds transfers into bank accounts controlled by fellow conspirators.

Viktor Vladimirovich Eremenko, aka “nfcorpi,” age 30, of Stavropol, Russia, and Farkhad Rauf Ogly Manokhin, aka “frusa,” of Volgograd, Russia, were “cash-outs” or “drop masters” on behalf of the GozNym criminal network. Like Alexander Van Hoof, Eremenko and Manokhin 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. Manokhin was arrested at the request of the United States while visiting Sri Lanka in February 2017. Following his arrest, Manokhin was released on bail but was required to remain in Sri Lanka pending the outcome of his extradition proceedings to the United States. In December 2017, Manokhin unlawfully absconded from Sri Lanka and successfully fled back to Russia prior to the conclusion of the extradition proceedings.

Other agencies and organizations partnering in this effort include the United States Secret Service, the National Cyber-Forensics and Training Alliance (NCFTA) in Pittsburgh and the Shadowserver Foundation. The Justice Department’s Office of International Affairs provided significant assistance throughout the investigation and spearheaded the efforts to enable the United States to request searches, arrests, and extraditions in the foreign countries as well as the sharing of evidence with those countries through Mutual Legal Assistance Treaty requests.

The case is being prosecuted by Assistant U.S. Attorney Charles A. “Tod” Eberle, Chief of National Security and Cybercrime for the Western District of Pennsylvania.

Updated May 16, 2019