Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of “Bugat” Malware

Published: 2019-12-05 · Archived: 2026-04-06 15:44:28 UTC

The United States of America, through its Departments of Justice and State, and the United Kingdom, through its National Crime Agency (NCA), today announced the unsealing of criminal charges in Pittsburgh, Pennsylvania, and Lincoln, Nebraska, against Maksim V. Yakubets, aka online moniker, “aqua,” 32, of Moscow, Russia, related to two separate international computer hacking and bank fraud schemes spanning from May 2009 to the present. A second individual, Igor Turashev, 38, from Yoshkar-Ola, Russia, was also indicted in Pittsburgh for his role related to the “Bugat” malware conspiracy. The State Department, in partnership with the FBI, announced today a reward of up to $5 million under the Transnational Organized Crime Rewards Program for information leading to the arrest and/or conviction of Yakubets. This represents the largest such reward offer for a cyber criminal to date.

Assistant Attorney General Brian A. Benczkowski of the Justice Department’s Criminal Division, U.S. Attorney Scott W. Brady for the Western District of Pennsylvania, U.S. Attorney Joseph P. Kelly for the District of Nebraska, FBI Deputy Director David Bowdich, Principal Deputy Assistant Secretary James A. Walsh of the State Department’s Bureau of International Narcotics and Law Enforcement Affairs (INL), and Director Rob Jones of the Cyber Crime Unit at the United Kingdom’s National Crime Agency (NCA) made the announcement.

“Maksim Yakubets allegedly has engaged in a decade-long cybercrime spree that deployed two of the most damaging pieces of financial malware ever used and resulted in tens of millions of dollars of losses to victims worldwide,” said Assistant Attorney General Benczkowski. “These two cases demonstrate our commitment to unmasking the perpetrators behind the world’s most egregious cyberattacks. The assistance of our international partners, in particular the National Crime Agency of the United Kingdom, was crucial to our efforts to identify Yakubets and his co-conspirators.”

“For over a decade, Maksim Yakubets and Igor Turashev led one of the most sophisticated transnational cybercrime syndicates in the world,” said U.S. Attorney Brady. “Deploying ‘Bugat’ malware, also known as ‘Cridex’ and ‘Dridex,’ these cybercriminals targeted individuals and companies in western Pennsylvania and across the globe in one of the most widespread malware campaigns we have ever encountered. International cybercriminals who target Pennsylvania citizens and companies are no different than any other criminal: they will be investigated, prosecuted and held accountable for their actions.”

“The Zeus scheme was one of the most outrageous cybercrimes in history,” said U.S. Attorney Kelly. “Our identification of Yakubets as the actor who used the moniker ‘aqua’ in that scheme, as alleged in the complaint unsealed today, is a prime example of how we will pursue cyber criminals to the ends of justice no matter how long it takes, by tracking their activity both online and off and working with our international partners to expose their crimes.”

"Today's announcement involved a long running investigation of a sophisticated organized cybercrime syndicate," said FBI Deputy Director Bowdich. "The charges highlight the persistence of the FBI and our partners to vigorously pursue those who desire to profit from innocent people through deception and theft. By calling out those who threaten American businesses and citizens, we expose criminals who hide behind devices and launch attacks that threaten our public safety and economic stability. The actions highlighted today, which represent a continuing trend of cyber-criminal activity emanating from Russian actors, were particularly damaging as they targeted U.S. entities across all sectors and walks of life. The FBI, with the assistance of private industry and our international and U.S. government partners, is sending a strong message that we will work together to investigate and hold all criminals accountable. Our memory is long and we will hold them accountable under the law, no matter where they attempt to hide."

"Combatting cybercrime remains a top national security priority for to the United States," said INL Principal Deputy Assistant Secretary of State Walsh. "The announcements today represent a coordinated interagency effort to bring Maksim Yakubets to justice and to address cybercrime globally."

"This is a landmark for the NCA, FBI and U.S. authorities and a day of reckoning for those who commit cybercrime," said NCA Director Jones. "Following years of online pursuit, I am pleased to see the real world identity of Yakubets and his associate Turashev revealed. Yakubets and his associates have allegedly been responsible for losses and attempted losses totaling hundreds of millions of dollars. This is not a victimless crime, those losses were once people's life savings, now emptied from their bank accounts. Today the process of bringing Yakubets and his criminal associates to justice begins. This is not the end of our investigation, and we will continue to work closely with international partners to present a united front against criminality that threatens our prosperity and security."

Yakubets and Turashev Indicted in Relation to "Bugat" Malware

A federal grand jury in Pittsburgh returned a 10-count indictment, which was unsealed today, against Yakubets and Turashev, charging them with conspiracy, computer hacking, wire fraud, and bank fraud, in connection with the distribution of "Bugat," a multifunction malware package designed to automate the theft of confidential personal and financial information, such as online banking credentials, from infected computers. Later versions of the malware were designed with the added function of assisting in the installation of ransomware.

According to the indictment, Bugat is a malware specifically crafted to defeat antivirus and other protective measures employed by victims. As the individuals behind Bugat improved the malware and added functionality, the name of the malware changed, at one point being called "Cridex," and later "Dridex," according to the indictment. Bugat malware was allegedly designed to automate the theft of confidential personal and financial information, such as online banking credentials, and facilitated the theft of confidential personal and financial information by a number of methods. For example, the indictment alleges that the Bugat malware allowed computer intruders to hijack a computer session and present a fake online banking webpage to trick a user into entering personal and financial information.

The indictment further alleges that Yakubets and Turashev used captured banking credentials to cause banks to make unauthorized electronic funds transfers from the victims' bank accounts, without the knowledge or consent of the account holders. They then allegedly used persons, known as "money mules," to receive stolen funds into

their bank accounts, and then move the money to other accounts or withdraw the funds and transport the funds overseas as smuggled bulk cash. According to the indictment, they also used a powerful online tool known as a botnet in furtherance of the scheme.

Yakubets was the leader of the group of conspirators involved with the Bugat malware and botnet, according to the indictment. As the leader, he oversaw and managed the development, maintenance, distribution, and infection of Bugat as well as the financial theft and the use of money mules. Turashev allegedly handled a variety of functions for the Bugat conspiracy, including system administration, management of the internal control panel, and oversight of botnet operations.

According to the indictment, Yakubets and Turashev victimized multiple entities, including two banks, a school district, and four companies including a petroleum business, building materials supply company, vacuum and thin film deposition technology company and metal manufacturer in the Western District of Pennsylvania and a firearm manufacturer. The indictment alleges that these attacks resulted in the theft of millions of dollars, and occurred as recently as March 19, 2019.

Yakubets Charged in Relation to "Zeus" Malware

A criminal complaint was also unsealed in Lincoln today charging Yakubets with conspiracy to commit bank fraud in connection with the "Zeus" malware. Beginning in May 2009, Yakubets and multiple co-conspirators are alleged to have a long-running conspiracy to employ widespread computer intrusions, malicious software, and fraud to steal millions of dollars from numerous bank accounts in the United States and elsewhere. Yakubets and his co-conspirators allegedly infected thousands of business computers with malicious software that captured passwords, account numbers, and other information necessary to log into online banking accounts, and then used the captured information to steal money from victims' bank accounts. As with Bugat, the actors involved with the Zeus scheme were alleged to have employed the use of money mules and a botnet.

Yakubets and his co-conspirators are alleged to have victimized 21 specific municipalities, banks, companies, and non-profit organizations in California, Illinois, Iowa, Kentucky, Maine, Massachusetts, New Mexico, North Carolina, Ohio, Texas, and Washington, identified in the complaint, including multiple entities in Nebraska and a religious congregation. According to the complaint, the deployment of the Zeus malware resulted overall in the attempted theft of an estimated $220 million USD, with actual losses of an estimated $70 million USD from victims' bank accounts. According to the complaint, Yakubets' role in the Zeus scheme was to provide money mules and their associated banking credentials in order to facilitate the movement of money, which was withdrawn from victim accounts by fraudulent means.

An individual charged as John Doe #2, also known as "aqua," was indicted in District of Nebraska in case number 4:11-CR-3074. The indictment in that case charges that individual and others with conspiracy to participate in racketeering activity, conspiracy to commit computer fraud and identity theft, aggravated identity theft, and multiple counts of bank fraud related to the Zeus scheme. As alleged, the complaint unsealed today associates use of the moniker "aqua" in the Zeus scheme to Yakubets.

In case number 4:11-CR-3074, two of the co-conspirators of "aqua," Ukrainian nationals Yuriy Konovaleko and Yevhen Kulibaba, were extradited from the United Kingdom to the United States. Konovalenko and Kulibaba both pleaded guilty in 2015 to conspiracy to participate in racketeering activity and have completed prison

sentences that were imposed. Konovalenko and Kulibaba were previously convicted in the United Kingdom, after an investigation conducted by the Metropolitan Police Service, for their role in laundering £3 million GBP on behalf of the group responsible for the Zeus malware.

State Department $5 million USD Reward

The U.S. Department of State's Transnational Organized Crime (TOC) Rewards Program is offering a reward of up to $5 million for information on Yakubets. Cyber threats are a top national security threat to the United States, and the Department of State's TOC Rewards Program is one of the many tools used by U.S. authorities to bring significant cybercriminals to justice. Congress established the TOC Rewards Program in 2013 to support law enforcement efforts to dismantle transnational criminal organizations and bring their leaders and members to justice. The U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs manages the program in coordination with other U.S. federal agencies.

In addition to NCA, the law enforcement actions taken related to these two prosecutions were assisted by the efforts of law enforcement counterparts from The Netherlands, Germany, Belarus, Ukraine, and the Russian Federation.

The FBI's Pittsburgh and Omaha Field Offices led the investigations of Yakubets and Turashev with assistance by the FBI's Major Cyber Crimes Unit and Global Operations and Targeting Unit. The prosecution in Pittsburgh is being handled by Assistant U.S. Attorney Shardul S. Desai of the Western District of Pennsylvania, and the prosecution in Lincoln is being handled by Senior Counsel William A. Hall, Jr., of the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and Assistant U.S. Attorney Steven A. Russell of the District of Nebraska. The Criminal Division's Office of International Affairs provided significant assistance throughout the criminal investigations. The Department's National Security Division also provided investigative assistance.

The details contained in the indictment, criminal complaint and related pleadings are merely accusations, and the defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.
