Two Romanian Cybercriminals Convicted of All 21 Counts Relating to Infecting Over 400,000 Victim Computers with Malware and Stealing Millions of Dollars

Published: 2019-04-11 · Archived: 2026-04-10 03:02:22 UTC

A federal jury today convicted two Bucharest, Romania, residents of 21 counts related to their scheme to infect victim computers with malware in order to steal credit card and other information to sell on dark market websites, mine cryptocurrency and engage in online auction fraud, announced Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division and U.S. Attorney Justin E. Herdman of the Northern District of Ohio.

Bogdan Nicolescu, 36, and Radu Miclaus, 37, were convicted after a 12-day trial of conspiracy to commit wire fraud, conspiracy to traffic in counterfeit service marks, aggravated identity theft, conspiracy to commit money laundering and 12 counts each of wire fraud. Sentencing has been set for Aug. 14, 2019 before Chief Judge Patricia A. Gaughan of the Northern District of Ohio.

According to testimony at trial and court documents, Nicolescu, Miclaus, and a co-conspirator who pleaded guilty, collectively operated a criminal conspiracy from Bucharest, Romania. It began in 2007 with the development of proprietary malware, which they disseminated through malicious emails purporting to be legitimate from such entities as Western Union, Norton AntiVirus and the IRS. When recipients clicked on an attached file, the malware was surreptitiously installed onto their computer.

This malware harvested email addresses from the infected computer, such as from contact lists or email accounts, and then sent malicious emails to these harvested email addresses. The defendants infected and controlled more than 400,000 individual computers, primarily in the United States.

Controlling these computers allowed the defendants to harvest personal information, such as credit card information, user names and passwords. They disabled victims' malware protection and blocked the victims' access to websites associated with law enforcement.

Controlling the computers also allowed the defendants to use the processing power of the computer to solve complex algorithms for the financial benefit of the group, a process known as cryptocurrency mining.

The defendants used stolen email credentials to copy a victim's email contacts. They also activated files that forced infected computers to register email accounts with AOL. The defendants registered more than 100,000 email accounts using this method. They then sent malicious emails from these addresses to the compromised contact lists. Through this method, they sent tens of millions of malicious emails.

When victims with infected computers visited websites such as Facebook, PayPal, eBay or others, the defendants would intercept the request and redirect the computer to a nearly identical website they had created. The defendants would then steal account credentials. They used the stolen credit card information to fund their

criminal infrastructure, including renting server space, registering domain names using fictitious identities and paying for Virtual Private Networks (VPNs) which further concealed their identities.

The defendants were also able to inject fake pages into legitimate websites, such as eBay, to make victims believe they were receiving and following instructions from legitimate websites, when they were actually following the instructions of the defendants.

They placed more than 1,000 fraudulent listings for automobiles, motorcycles and other high-priced goods on eBay and similar auction sites. Photos of the items were infected with malware, which redirected computers that clicked on the image to fictitious webpages designed by the defendants to resemble legitimate eBay pages.

These fictitious webpages prompted users to pay for their goods through a nonexistent “eBay Escrow Agent” who was simply a person hired by the defendants. Users paid for the goods to the fraudulent escrow agents, who in turn wired the money to others in Eastern Europe, who in turn gave it to the defendants. The payers/victims never received the items and never got their money back.

This resulted in a loss of millions of dollars.

The Bayrob group laundered this money by hiring “money transfer agents” and created fictitious companies with fraudulent websites designed to give the impression they were actual businesses engaged in legitimate financial transactions. Money stolen from victims was wired to these fraudulent companies and then in turn wired to Western Union or Money Gram offices in Romania. European “money mules” used fake identity documents to collect the money and deliver it to the defendants.

The FBI investigated the case, with assistance from the Romanian National Police. Senior Counsel Brian Levine of the Criminal Division’s Computer Crime and Intellectual Property Section (CCIPS) and Assistant U.S. Attorneys Duncan T. Brown and Brian McDonough of the Northern District of Ohio prosecuted the case. The Office of International Affairs also provided assistance in this case.
