Department of Justice

U.S. Attorney's Office

Southern District of New York

FOR IMMEDIATE RELEASE Tuesday, April 26, 2016

Estonian Cybercriminal Sentenced For Infecting 4 Million Computers In 100 Countries With Malware In Multimillion-Dollar Fraud Scheme

Preet Bharara, the United States Attorney for the Southern District of New York, announced today that VLADIMIR TSASTSIN was sentenced in Manhattan federal court to more than seven years in prison for perpetrating a massive internet fraud scheme by infecting more than four million computers in over 100 countries with malware. The malware secretly altered the settings on infected computers, enabling TSASTSIN and his co-conspirators to digitally hijack users' Internet searches and re-route their computers to certain websites and advertisements. As a result, the defendants received millions of dollars in fees from advertisers who paid the defendants to bring customers to their websites or ads, but were unaware that the defendants did so by digitally hijacking victims' computers. The malware also prevented the installation of anti-virus software and operating system updates on millions of infected computers, leaving those computers and their users unable to detect or stop the malware, and exposing them to attacks by other malware. On July 8, 2015, TSASTSIN pled guilty to one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer intrusion. U.S. District Judge Lewis A. Kaplan sentenced TSASTSIN earlier today.

U.S. Attorney Preet Bharara said: "Vladimir Tsastin was sentenced today to 87 months in prison for his role in a massive fraud scheme, which victimized more than four million Internet users in 100 countries. By falsely collecting advertising fees for every 'click' their victims made, Tsastsin and his co-conspirators collected over $14 million. Together with our law enforcement partners all over the globe, this Office will continue to investigate and prosecute sophisticated cyber frauds."

According to the Indictment and other court documents previously filed in the case and statements made in court proceedings:

From 2007 until October 2011, TSASTSIN and co-defendants Andrey Taame, Timur Gerassimenko, Dmitri Jegorov, Valeri Aleksejev, Konstantin Poltev, and Anton Ivanov controlled and operated various companies that masqueraded as legitimate publisher networks (the "Publisher Networks") in the Internet advertising industry. The Publisher Networks entered into agreements with ad brokers under which they were paid based on the number of times Internet users clicked on the links for certain websites or advertisements, or based on the number of times certain advertisements were displayed on certain websites. Thus, the more traffic that went to

the advertisers' websites and display ads, the more money the defendants earned under their agreements with the ad brokers. The defendants fraudulently increased the traffic to the websites and advertisements that would earn them money and made it appear to advertisers that the Internet traffic came from legitimate "clicks" and ad displays on the defendants' Publisher Networks when, in actuality, it had not.

To carry out the scheme, the defendants and their co-conspirators used dozens of "rogue" Domain Name System ("DNS") servers and malware ("the Malware") designed to alter the DNS server settings on infected computers. Victims' computers became infected with the Malware when they visited certain websites or downloaded certain software to view videos online. The Malware altered the DNS server settings on victims' computers to route the infected computers to rogue DNS servers controlled and operated by the defendants and their co-conspirators. The re-routing took two forms that are described below: "click hijacking" and "advertising replacement fraud" (together, "click fraud"). The Malware also prevented the infected computers from receiving anti-virus software updates or operating system updates that otherwise might have detected the Malware and stopped it. In addition, the infected computers were left vulnerable to infections by other malware.

Click Hijacking

When the user of an infected computer clicked on a search result link displayed through a search engine query, the Malware caused the computer to be re-routed to a different website. Instead of being brought to the website to which the user asked to go, the user was brought to a website designated by the defendants. Each "click" triggered payment to the defendants under their advertising agreements. This click hijacking occurred for clicks by users on unpaid links that appeared in response to a user's query as well as clicks on "sponsored" links or advertisements that appeared in response to a user's query – often at the top of, or to the right of, the search results – thus causing the search engines to lose money. For example, when the user of an infected computer clicked on the domain name link for the official website of Apple-iTunes, the user was instead taken to a website for a business unaffiliated with Apple Inc. that purported to sell Apple software. The advertisers who paid for such Internet traffic to their websites were never told that the traffic consisted of hijacked clicks and that the visitors had not intended to visit their websites.

Advertising Replacement Fraud

In the advertisement replacement scheme, using their DNS Changer Malware and rogue DNS servers, the defendants replaced legitimate advertisements on websites, without the paying advertisers' knowledge or consent, with substituted advertisements that triggered payments to themselves. For example, when the user of an infected computer visited the home page of *The Wall Street Journal*, a featured advertisement for American Express had been fraudulently replaced with an ad for "Fashion Girl LA," which triggered a payment to the defendants from another advertiser.

To acquire the online infrastructure for the fraudulent scheme, enter into contracts to sell Internet traffic, and launder the proceeds from the fraudulent scheme, Tsastsin and his co-defendants created and controlled over a dozen front companies located and/or registered in the United States, Estonia, Russia, Denmark, the Republic of Seychelles, England, and Cyprus. At the time of his arrest, TSASTSIN, assisted by his co-defendants, operated approximately 50 rogue DNS servers located in New York City and additional ones at a data center in Chicago. Each of the rogue servers contained approximately two hard drives; the larger hard drives received as many as 3,000 fraudulent "clicks," or DNS resolution requests, per second, while the smaller servers received several hundred requests per second.

* * *

In addition to the 87-month prison term, TSASTSIN, 35, of Tartu, Estonia, was sentenced to one year of supervised release and ordered to forfeit $2.5 million and pay a $200 special assessment. In imposing sentence, Judge Kaplan described TSASTSIN's crimes as "brazen, sophisticated, and outrageous."

On July 27, 2015, Gerassimenko, Jegorov, and Poltev were sentenced to 48 months, 44 months, and 40

months in prison, respectively. Aleksejev was sentenced on October 30, 2013, to 48 months in prison. Ivanov was sentenced on July 25, 2014, to time served. Judge Kaplan also entered orders against each defendant forfeiting his criminal proceeds and the electronic and online infrastructure used to perpetrate their fraudulent scheme. The last defendant, Taame, who is a Russian national, remains at large.

Mr. Bharara praised the outstanding investigative work of the Federal Bureau of Investigation, National Aeronautics and Space Administration-Office of the Inspector General, and the Estonian Central Criminal Police. He also thanked the U.S. Department of Justice's Office of International Affairs for its assistance with the extraditions.

This case is being handled by the Office's Complex Frauds and Cybercrime Unit. Assistant U.S. Attorney Sarah Lai is in charge of the prosecution. Alexander Wilson, Deputy Chief of the Asset Forfeiture Unit, is in charge of the forfeiture aspects of the case.

16-098 USAO - New York, Southern

Topic:
Cyber Crime

Updated April 26, 2016