UNITED STATES ATTORNEY'S OFFICE
Southern District of New York

U.S. ATTORNEY PREET BHARARA

FOR IMMEDIATE RELEASE
Wednesday, February 18, 2015
http://www.justice.gov/usao/nys

CONTACT: James Margolin, Jennifer Queliz,
Betsy Feuerstein
(212) 637-2600

CO-CREATOR OF "BLACKSHADES" MALWARE PLEADS GUILTY IN MANHATTAN FEDERAL COURT

"Blackshades" Used To Secretly And Remotely Control Victims' Computers

Preet Bharara, the United States Attorney for the Southern District of New York, announced that ALEX YÜCEL, the co-creator of malicious software known as the Blackshades Remote Access Tool, or "RAT," which has been sold and distributed through YÜCEL's Blackshades organization to thousands of people in more than 100 countries, pled guilty today in Manhattan federal court to one count of distribution of malicious software. U.S. District Judge P. Kevin Castel presided over the plea proceedings.

Manhattan U.S. Attorney Preet Bharara said: "Through his creation and sale of the Blackshades RAT, Alex Yücel enabled anyone, for just $40, to violate the property and privacy of his victims. With his guilty plea today, Yücel will now have to pay for his conduct. This Office will continue to work with our law enforcement partners at the Federal Bureau of Investigation and around the world to find and prosecute those who create, market, and employ malicious software."

According to the allegations in documents filed in Manhattan federal court, and statements made at today's plea and other court proceedings:

Beginning in at least 2010, the "Blackshades" organization, which Yücel owned and controlled, sold and distributed malware to thousands of cybercriminals throughout the world. Blackshades' flagship product was the RAT – a sophisticated piece of malware that enabled cybercriminals secretly and remotely to gain control over a victim's computer. After installing the RAT on a victim's computer, a user of the RAT had free rein to, among other things, access and view documents, photographs, and other files on the victim's computer, record all of the keystrokes entered on the victim's keyboard, steal the passwords to the victim's online accounts, and even activate the victim's web camera to spy on the victim – all of which could be done without the victim's knowledge. A Blackshades user could also exploit victims' computers for Distributed Denial of Service ("DDoS") attacks by commanding Blackshades-infected computers to overwhelm websites or computer servers with traffic, and thereby disable them.

The RAT was typically advertised on forums for computer hackers and marketed as a product that conveniently combined the features of several different types of hacking tools. Copies of the Blackshades RAT were available for sale, typically for $40 each, on a website maintained by Blackshades. After purchasing a copy of the RAT, a user had to install the RAT on a victim's computer – i.e., "infect" a victim's computer. The infection of a victim's computer could be accomplished in several ways, including by tricking victims into clicking on malicious links or by hiring others to install the RAT on victims' computers.

Once a computer was infected with the RAT, the user of the RAT had complete control over the computer. The user could, among other things, remotely activate the victim's web camera. In this way, the user could spy on anyone within view of the victim's webcam inside the victim's home or in any other private spaces where the victim's computer was used. The RAT also contained a "keylogger" feature that allowed users to record each key that victims typed on their computer keyboards. To help users steal a victim's passwords and other log-in credentials, the RAT also had a "form grabber" feature. The "form grabber" automatically captured log-in information that victims entered into "forms" on their infected computers (*e.g.*, log-in screens or order purchase screens for online accounts).

YÜCEL co-created the Blackshades RAT with Michael Hogue and operated the Blackshades organization with the help of several employees. The RAT was purchased by at least several thousand users in more than 100 countries and used to infect more than half a million computers worldwide.

* * *

YÜCEL, 24, a Swedish national, was arrested in Moldova in November 2013. He was the first defendant ever to be extradited from Moldova to the United States. His guilty plea to distribution of malicious software carries a maximum sentence of 10 years in prison. He is scheduled to be sentenced by Judge Castel on May 22, 2015, at 11:00 a.m. The maximum potential sentences are prescribed by Congress, and are provided here for informational purposes only, as any sentencing of the defendant will be determined by the judge.

Michael Hogue, the co-creator of the RAT, pled guilty before Judge Castel in January 2013 and is awaiting sentencing.

Brendan Johnston, an administrator for the Blackshades organization, pled guilty on November 21, 2014, before U.S. District Judge Jesse M. Furman to conspiracy to commit computer hacking, which carries a maximum sentence of 10 years in prison. He is scheduled to be sentenced by Judge Furman on May 27, 2015, at 3:30 p.m.

Marlen Rappa, a customer of Blackshades who purchased the RAT and used it to infect victims' computers, spy on those victims using their web cameras, and steal personal files from their computers, pled guilty on October 31, 2014, before U.S. District Judge Valerie E. Caproni. He is scheduled to be sentenced by Judge Caproni on March 13, 2015, at 3:00 p.m.

Kyle Fedorek, a customer of Blackshades who purchased the RAT and used it to steal financial and other account information from more than 400 victims, pled guilty on August 19, 2014, before U.S. Magistrate Judge Gabriel W. Gorenstein and is scheduled to be sentenced by U.S. District Judge Vernon S. Broderick on February 19, 2015, at 10:00 a.m.

Mr. Bharara praised the outstanding investigative work of the Federal Bureau of Investigation.

The case is being prosecuted by the Office's Complex Frauds and Cybercrime Unit. Assistant U.S. Attorneys Sarah Lai and Daniel Noble are in charge of the prosecution. Assistant U.S. Attorney Paul Monteleoni is in charge of the forfeiture aspects of the case.

15-045 ###