Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE
Monday, December 5, 2016

Avalanche Network Dismantled in International Cyber Operation

The Justice Department today announced a multinational operation involving arrests and searches in four countries to dismantle a complex and sophisticated network of computer servers known as "Avalanche." The Avalanche network allegedly hosted more than two dozen of the world's most pernicious types of malicious software and several money laundering campaigns.

Assistant Attorney General Leslie R. Caldwell of the Justice Department's Criminal Division, Acting U.S. Attorney Soo C. Song of the Western District of Pennsylvania and Assistant Director Scott S. Smith of the FBI's Cyber Division made the announcement.

"For years, sophisticated cyber criminals have used our own technology against us—but as their networks have grown more complex and widespread, criminals increasingly rely on an international infrastructure as well," said Assistant Attorney General Caldwell. "Avalanche is just one example of a criminal infrastructure dedicated to facilitating privacy invasions and financial crimes on a global scale. And now a multinational law enforcement coalition has turned the tables on the criminals, by targeting not just individual actors, but the entire Avalanche infrastructure. Successful operations like this one can disrupt an entire criminal ecosystem in one strike."

"The takedown of Avalanche was unprecedented in its scope, scale, reach and cooperation among 40 countries," said Acting U.S. Attorney Song. "This is the first time that we have aimed to and achieved the destruction of a criminal cyber infrastructure while disrupting all of the malware systems that relied upon it to do harm."

"We are committed to halting cybercriminal activity against the United States," said Assistant Director Smith. "Cybercriminals can victimize millions of users in a moment from anywhere in the world. This takedown highlights the importance of collaborating with our international law enforcement partners against this evolution of organized crime in the virtual."

The Avalanche network offered cybercriminals a secure infrastructure, designed to thwart detection by law enforcement and cyber security experts, over which the criminals conducted malware campaigns as well as money laundering schemes known as "money mule" schemes. Online banking passwords and other sensitive information stolen from victims' malware-infected computers was redirected through the intricate network of Avalanche servers and ultimately to backend servers controlled by the cybercriminals. Access to the Avalanche network was offered to the cybercriminals through postings on exclusive, underground online criminal forums.

The operation also involved an unprecedented effort to seize, block and sinkhole – meaning, redirect traffic from infected victim computers to servers controlled by law enforcement instead of the servers controlled by cybercriminals – more than 800,000 malicious domains associated with the Avalanche network. Such domains are needed to funnel information, such as sensitive banking credentials, from the victims' malware-infected computers, through the layers of Avalanche servers and ultimately back to the cybercriminals. This was accomplished, in part, through a temporary restraining order obtained by the United States in the Western District of Pennsylvania.

The types of malware and money mule schemes operating over the Avalanche network varied. Ransomware such as Nymain, for example, encrypted victims' computer files until the victim paid a ransom (typically in a form of electronic currency) to the cybercriminal. Other malware, such as

GozNym, was designed to steal victims' sensitive banking credentials and use those credentials to initiate fraudulent wire transfers. The money mule schemes operating over Avalanche involved highly organized networks of "mules" who purchased goods with stolen funds, enabling cybercriminals to launder the money they acquired through the malware attacks or other illegal means.

The Avalanche network, which has been operating since at least 2010, was estimated to serve clients operating as many as 500,000 infected computers worldwide on a daily basis. The monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of dollars worldwide, although exact calculations are difficult due to the high number of malware families present on the network.

Several victims of Avalanche-based malware attacks are located in the Western District of Pennsylvania. A local governmental office was the victim of a Nymain malware attack in which computer files were encrypted until the victims paid a Bitcoin ransom in exchange for decrypting the files. Two companies, based in New Castle and Carnegie, Pennsylvania, and their respective banks were victims of GozNym malware attacks. In both attacks, employees received phishing emails containing attachments designed to look like legitimate business invoices. After clicking on the links, GozNym malware was installed on the victims' computers. The malware stole the employees' banking credentials which were used to initiate unauthorized wire transfers from the victims' online bank accounts.

The U.S. Attorney's Office of the Western District of Pennsylvania, the FBI and the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) conducted the operation in close cooperation with the Public Prosecutor's Office Verden; the Luneburg Police of Germany; Europol; and Eurojust, located in The Hague, Netherlands; and investigators and prosecutors from more than 40 jurisdictions, including India, Singapore, Taiwan and Ukraine.

Other agencies and organizations partnering in this effort include the Department of Homeland Security's U.S.-Computer Emergency Readiness Team (US-CERT), the Shadowserver Foundation, Fraunhofer Institute for Communication, Registry of Last Resort, ICANN and domain registries from around the world. The Criminal Division's Office of International Affairs also provided significant assistance.

Assistant U.S. Attorney Charles Eberle of the Western District of Pennsylvania and CCIPS Senior Trial Attorney Richard D. Green are prosecuting the case. Assistant U.S. Attorney Michael A. Comber of the Western District of Pennsylvania and CCIPS Senior Trial Attorney Green are handling the civil action to disrupt the malware operating over the Avalanche network.

Individuals who believe that they may have been victims of malware operating over the Avalanche network may use the following webpage created by US-CERT for assistance in removing the malware: www.us-cert.gov/avalanche.

Anyone claiming an interest in any of the property seized or actions enjoined pursuant to the court orders described in this release is advised to visit the following website for notice of the full contents of the orders: https://www.justice.gov/opa/documents-and-resources-december-5-2016-announcement-takedown-international-cybercriminal.