Justice Department Announces Actions to Dismantle Kelihos Botnet

justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0

April 10, 2017

The Justice Department today announced an extensive effort to disrupt and dismantle the Kelihos botnet – a global network of tens of thousands of infected computers under the control of a cybercriminal that was used to facilitate malicious activities including harvesting login credentials, distributing hundreds of millions of spam e-mails, and installing ransomware and other malicious software.

Acting Assistant Attorney General Kenneth A. Blanco of the Justice Department's Criminal Division, Acting U.S. Attorney Bryan Schroder for the District of Alaska, Assistant Director Scott Smith for the FBI's Cyber Division and FBI Special Agent in Charge Marlin Ritzman of the AnchorageDivision made the announcement.

"The operation announced today targeted an ongoing international scheme that was distributing hundreds of millions of fraudulent e-mails per year, intercepting the credentials to online and financial accounts belonging to thousands of Americans, and spreading ransomware throughout our networks. The ability of botnets like Kelihos to be weaponized quickly for vast and varied types of harms is a dangerous and deep threat to all Americans, driving at the core of how we communicate, network, earn a living, and live our everyday lives," said Acting Assistant Attorney General Blanco. "Our success in disrupting the Kelihos botnet was the result of strong cooperation between private industry experts and law enforcement, and the use of innovative legal and technical tactics. The Department of Justice is committed to combatting cybercrime, no matter the size or sophistication of the scheme, and to punish those who are engaged in such crimes."

"Cybercrime is a worldwide problem, but one that infects its victims directly through the computers and personal electronic devices that we use every day," said Acting U.S. Attorney Bryan Schroder for the District of Alaska. "Protecting the American people from such a

worldwide threat requires a broad-reaching response, and the dismantling of the Kelihos botnet was such an operation. We are lucky that we have talented FBI agents and federal prosecutors with the skillsets to help protect Americans from this pervasive cybercrime."

"On April 8, 2017, we started the extraordinary task of blocking malicious domains associated with the Khelios botnet to prohibit further infections," said FBI Special Agent in Charge Ritzman. "This case demonstrates the FBI's commitment to finding and eradicating cyber threats no matter where they are in the world."

Kelihos malware targeted computers running the Microsoft Windows operating system. Infected computers became part of a network of compromised computers known as a botnet and were controlled remotely through a decentralized command and control system. According to the civil complaint, Peter Yuryevich Levashov allegedly operated the Kelihos botnet since approximately 2010. The Kelihos malware harvested user credentials by searching infected computers for usernames and passwords and by intercepting network traffic. Levashov allegedly used the information gained from this credential harvesting operation to further his illegal spamming operation which he advertised on various online criminal forums. The Kelihos botnet generated and distributed enormous volumes of unsolicited spam e-mails advertising counterfeit drugs, deceptively promoting stocks in order to fraudulently increase their price (so-called "pump-and-dump" stock fraud schemes), work-at-home scams, and other frauds. Kelihos was also responsible for directly installing additional malware onto victims' computers, including ransomware and malware that intercepts users' bank account passwords.

As with other botnets, Kelihos is designed to operate automatically and undetected on victims' computers, with the malicious code secretly sending requests for instructions to the botnet operator. In order to liberate the victim computers from the botnet, the United States obtained civil and criminal court orders in the District of Alaska. These orders authorized measures to neutralize the Kelihos botnet by (1) establishing substitute servers that receive the automated requests for instructions so that infected computers no longer communicate with the criminal operator and (2) blocking any commands sent from the criminal operator attempting to regain control of the infected computers.
In seeking authorization to disrupt and dismantle the Kelihos botnet, law enforcement obtained a warrant pursuant to recent amendments to Rule 41 of the Federal Rules of Criminal Procedure. A copy of this warrant along with the other court orders are produced below. The warrant obtained by the government authorizes law enforcement to redirect Kelihos-infected computers to a substitute server and to record the Internet Protocol addresses of those computers as they connect to the server. This will enable the government to provide the IP addresses of Kelihos victims to those who can assist with removing the Kelihos malware including internet service providers.

The efforts to disrupt and dismantle the Kelihos botnet were led by the FBI's Anchorage Office and New Haven Office; Senior Counsel Ethan Arenson and Harold Chun, and Trial Attorney Frank Lin of the Computer Crime and Intellectual Property Section; and Assistant

U.S. Attorneys Yvonne Lamoureux and Adam Alexander of the District of Alaska. Critical assistance was also provided by foreign partners, and invaluable technical assistance was provided by Crowd Strike and The Shadow server Foundation in executing this operation.

The details contained in the civil complaint and related pleadings are merely accusations, and the defendant is presumed innocent unless and until proven guilty.

The Government has and will continue to share samples of the Kelihos malware with the internet security community so that antivirus vendors can update their programs to detect and remove Kelihos. A number of free and paid antivirus programs are already capable of detecting and removing Kelihos, including the Microsoft Safety Scanner, a free product.

The documents filed by the Government as well as the court orders entered in this case are available online at the following web address: www.justice.gov/opa/documents-and-resources-related-us-v-peter-yuryevich-levashov

Topic(s):

Cybercrime

Component(s):

Criminal Division
Press Release Number:

17-378