Source: http://www.ktuu.com/content/news/Cybercriminal-ring-botnet-developers-plead-guilty-to-powerful-cyberattacks.html

Alaska spearheads investigation into 'one of the most powerful cyberattacks in history'

By Beth Verge | Posted: Wed 11:38 AM, Dec 13, 2017 | Updated: Thu 12:38 AM, Dec 14, 2017

ANCHORAGE (KTUU) - Three young men who reportedly met online and are credited with creating and operating massive botnet schemes have officially pleaded guilty to criminal charges surrounding the original and subsequent cyberattacks, according to U.S. officials with the Dept. of Justice.

Much like other global-scale cybercrimes, the attack reached far and wide, including up to Alaska, where the criminals also seem to have met their downfall.

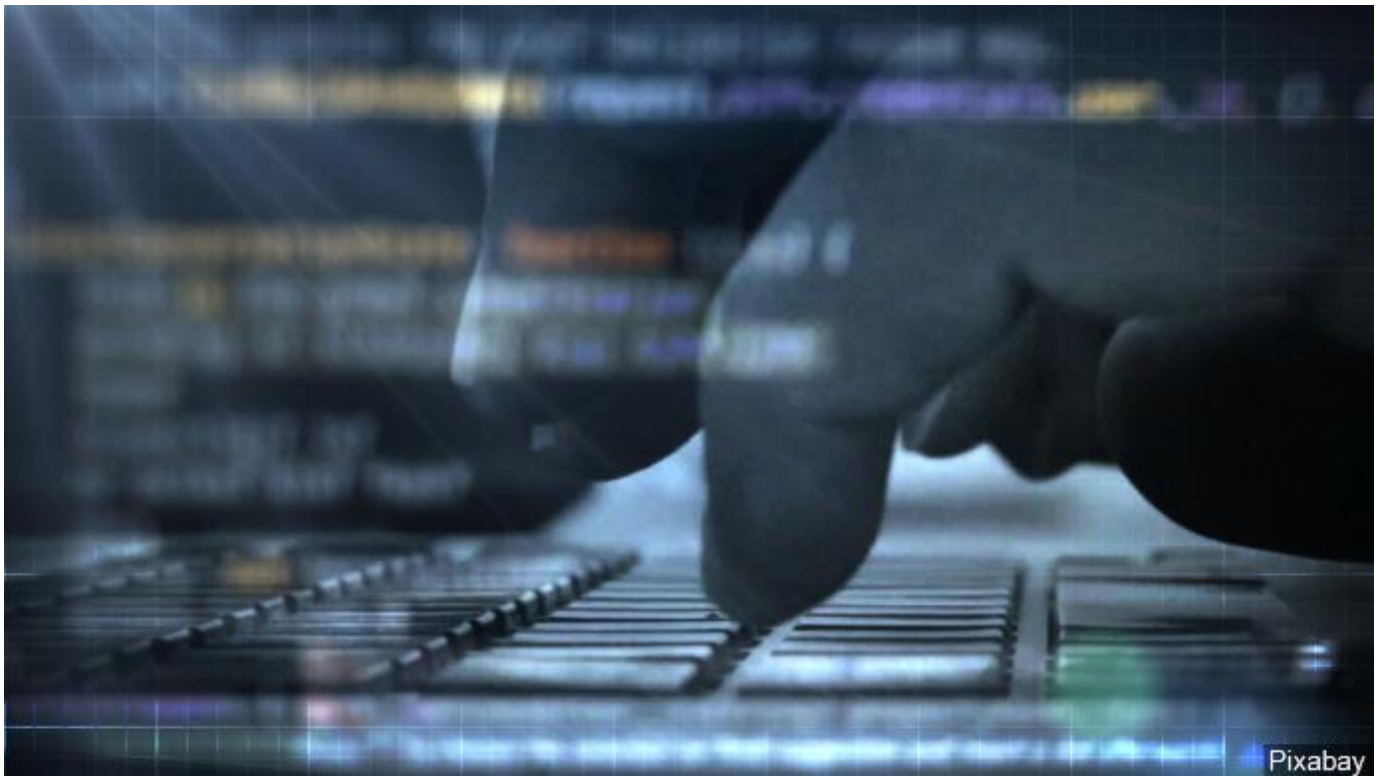
"There are victims that are in Alaska whose devices were compromised by these individuals," said Asst. U.S. Attorney Adam Alexander, "to comprise these botnets to then use for additional other related criminal activity.

"One was," he continued, "to attack targets here in the United States and abroad. That was comprised of hijacked devices, including victims here in Alaska."

Paras Jha, 21, of Fanwood, New Jersey; Josiah White, 20, of Washington, Penn.; and Salton Norman, 21, of Metairie, Louisiana, pleaded guilty in the District of Alaska to creating and operating the botnets, which specifically targeted Internet of Things devices. The men have each been charged in Alaska with conspiracy to violate the Computer Fraud & Abuse Act, also known as the CFAA, a hacking statute which prohibits unauthorized access to networks, computer and other devices.

Jha and Norman were additionally charged in the District of Alaska with conspiracy to violate the Computer Fraud & Abuse Act for infecting more than 100,000 primarily U.S.-based devices, including home Internet routers, with malware that allowed the victims to be utilized in advertising fraud known as "clickfraud." Users would click on an advertisement but it would generate artificial revenue for the hidden source.

Jha also pleaded guilty to launching a cyberattack on Rutgers University, where he was enrolled at the time.



In operating the Mirai Botnet, Jha, White and Norman had harnessed a massively powerful collection of computers infected with malware that allowed the group to control them without the knowledge of the devices' owners.

"A botnet is a series of devices that have been compromised by a cybercriminal," said Supervisory Special Agent William Walton of the FBI Anchorage Division, "who is then able to control them from a remote location and cause them to respond to his commands."

The three hackers used Mirai, named after an anime series, to conduct distributed denial-of-service (DDoS) attacks in order to flood and in turn disrupt the Internet connection of the targeted devices. At its peak, according to the DOJ, Mirai "consisted of hundreds of thousands of compromised devices," many of them located across Alaska.

"Why is it that we think this is a particularly significant case?" said Acting Deputy Assistant Attorney General of the Criminal Division Richard W. Downing by phone Wednesday morning. "The Mirai Botnet emerged in late 2016 and the source code was later posted. The Mirai Botnet, though, was the first to specifically target IoT devices, those non-traditional devices that are connected to the internet.

"At its peak, it was one of the largest IoT botnets ever recorded," he said.

DOJ officials said Jha posted the source code for Mirai on a criminal forum in the fall of 2016, triggering the end of his, White's and Norman's involvement with the original Mirai variant, though other criminals have used pieces of it in other attacks.

While the FBI helped spearhead the campaign, the Mirai Botnet and Clickfraud Botnet cases are now primarily in the hands of prosecutor and Assistant U.S. Attorney Adam Alexander of the District of Alaska, and Trial Attorney C. Alden Pelker of the Computer Crime and Intellectual Property Section of the Criminal Division.

All in all, though, according to Special Agent in Charge Marlin Ritzman of the FBI Anchorage Division, it was a load of teamwork that took down this dangerous ring of cybercriminals.

"Part of our ability to conduct investigations is through some of our outstanding liaison and partnership with local, private and public businesses, too," he said. "When companies identify issues or problems with systems early, they allow us to get in at the ground level on these investigations."