Source: https://americansecuritytoday.com/guilty-pleas-computer-crime-cases-involving-massive-ddos-attacks-videos/

Guilty Pleas in Computer Crime Cases Involving Massive DDoS Attacks (Videos)

By **AST Administrator** - December 13, 2017

Millions of IoT devices that have been deployed with default credentials, programmed backdoor accounts, open access ports etc and are wide open to be taken over by the Mirai malware.

The Justice Department have announced today the guilty pleas in three high-profile cybercrime cases.

In the District of Alaska, defendants pleaded guilty to creating and operating two botnets, which targeted “Internet of Things” (IoT) devices, and in the District of New Jersey, one of the defendants also pleaded guilty to launching a cyber attack on the Rutgers University computer network.

Acting Assistant Attorney General John P. Cronan of the Justice Department's Criminal Division, U.S. Attorney Bryan D. Schroder of the District of Alaska, Acting U.S. Attorney William E. Fitzpatrick of the District of New Jersey and Assistant Director Scott Smith of the FBI Cyber Division made the announcement.

On Dec. 8, Paras Jha, 21, of Fanwood, New Jersey; Josiah White, 20, of Washington, Pennsylvania; and Dalton Norman, 21, of Metairie, Louisiana, pleaded guilty to criminal Informations in the District of Alaska charging them each with conspiracy to violate the Computer Fraud & Abuse Act in operating the Mirai Botnet.

In the summer and fall of 2016, White, Jha, and Norman created a powerful botnet – a collection of computers infected with malicious software and controlled as a group without the knowledge or permission of the computers' owners.

The Mirai Botnet targeted IoT devices – non-traditional computing devices that were connected to the Internet, including wireless cameras, routers, and digital video recorders.

(Learn More. Between 500,000 and 550,000 hacked devices around the world are now part of the Mirai botnet, and about 10% of those were involved in the October 2016 attack. 'Hacked: Who's Responsible for Today's Web-Host Siege?' Courtesy of Bloomberg)

The defendants attempted to discover both known and previously undisclosed vulnerabilities that allowed them to surreptitiously attain control over the victim devices for the purpose of forcing the devices to participate in the Mirai Botnet.

At its peak, Mirai consisted of hundreds of thousands of compromised devices.

The defendants used the botnet to conduct a number of powerful distributed denial-of-service, or "DDOS" attacks, which occur when multiple computers, acting in unison, flood the Internet connection of a targeted computer or computers.

The defendants' involvement with the original Mirai variant ended in the fall of 2016, when Jha posted the source code for Mirai on a criminal forum.

Since then, other criminal actors have used Mirai variants in a variety of other attacks.

On Dec. 8, Paras Jha and Dalton Norman also pleaded guilty to criminal Informations in the District of Alaska charging each with conspiracy to violate the Computer Fraud & Abuse Act.

From December 2016 to February 2017, the defendants successfully infected over 100,000 primarily U.S.-based computing devices, such as home Internet routers, with malicious software.

(Learn More. The Mirai malware is seen as a milestone in the threat landscape, showing that IoT botnets can be used in distributed denial-of-service (DDoS) attacks and can deal significant blows. Courtesy of Bitdefender BOX and YouTube. Posted on Apr 13, 2017)

That malware caused the hijacked home Internet routers and other devices to form a powerful botnet.

The victim devices were used primarily in advertising fraud, including “clickfraud,” a type of Internet-based scheme that makes it appear that a real user has “clicked” on an advertisement for the purpose of artificially generating revenue.

On Dec. 13, Paras Jha pleaded guilty in the District of New Jersey to violating the Computer Fraud & Abuse Act.

Between November 2014 to September 2016, Jha executed a series of attacks on the networks of Rutgers University.

Jha’s attacks effectively shut down Rutgers University’s central authentication server, which maintained, among other things, the gateway portal through which staff, faculty, and students delivered assignments and assessments.

Acting Assistant Attorney General John P. Cronan

At times, Jha succeeded in taking the portal offline for multi-day periods, harming Rutgers University, its faculty, and its students.

“The Mirai and Clickfraud botnet schemes are powerful reminders that as we continue on a path of a more interconnected world, we must guard against the threats posed by cybercriminals that can quickly weaponize technological developments to cause vast and varied types of harm,” said Acting Assistant Attorney General Cronan.

“The Criminal Division will remain constantly vigilant in combating these sophisticated schemes, prosecuting cybercriminals, and protecting the American people.”

U.S. Attorney Bryan D. Schroder of the District of Alaska

“Our world has become increasingly digital, and increasingly complex,” said U.S. Attorney Schroder.

“Cybercriminals are not concerned with borders between states or nations, but should be on notice that they will be held accountable in Alaska when they victimize Alaskans in order to perpetrate criminal schemes. ”

“The U.S. Attorney’s Office, along with our partners at the FBI and Department of Justice’s Computer Crime and Intellectual Property Section (CCIPS), are committed to finding these criminals, interrupting their networks, and holding them accountable.”

“Paras Jha has admitted his responsibility for multiple hacks of the Rutgers University computer system,” said Acting U.S. Attorney Fitzpatrick.

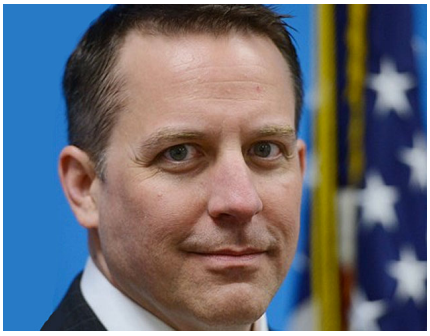
Acting US Attorney for the District of NJ William E. Fitzpatrick

“These computer attacks shut down the server used for all communications among faculty, staff and students, including assignment of course work to students, and students’ submission of their work to professors to be graded.”

“The defendant’s actions effectively paralyzed the system for days at a time and maliciously disrupted the educational process for tens of thousands of Rutgers’ students.”

“Today, the defendant has admitted his role in this criminal offense and will face the legal consequences for it.”

“These cases illustrate how the FBI works tirelessly against the actions of criminals who use malicious code to cause widespread damage and disruptions to the general population,” said FBI Assistant Director Smith.



Assistant Director Scott Smith of the FBI Cyber Division

“The FBI is dedicated to working with its domestic and international partners to aggressively pursue these individuals and bring justice to the victims.”

For additional information on cybersecurity best practices for IoT devices, please visit: https://www.justice.gov/criminal-ccips/page/file/984001/download.

All three cases were investigated by the FBI’s Anchorage, Alaska and Newark, New Jersey Field Offices.

The Mirai Botnet and Clickfraud Botnet cases are being prosecuted by 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.

The Rutgers University case is being prosecuted by Assistant U.S. Attorney Shana Chen of the District of New Jersey.

Additional assistance was provided by the FBI's New Orleans and Pittsburgh Field Offices, the U.S. Attorney's Office for the Eastern District of Louisiana, the United Kingdom's National Crime Agency, the French General Directorate for Internal Security, the National Cyber-Forensics & Training Alliance, Palo Alto Networks Unit 42, Google, Cloudflare, Coinbase, Flashpoint, Yahoo and Akamai.

Former Department of Justice prosecutors Ethan Arenson, Harold Chun, and Yvonne Lamoureux provided invaluable support during their previous tenure at DOJ.

Attachment(s):
Download Dkt 5 Jha Clickfraud Plea Agreement
Download Dkt 5 Jha Mirai Plea Agreement
Download Dkt 5 Norman Clickfraud Plea Agreement
Download Dkt 5 Norman Mirai Plea Agreement
Download Dkt 5 White Mirai Plea Agreement
Download Jha, Paras Information NJ
Download Jha, Paras Plea Agreement NJ
Download Dkt 1 Jha Clickfraud Information
Download Dkt 1 Jha Mirai Information
Download Dkt 1 Norman Clickfraud Information
Download Dkt 1 Norman Mirai Information
Download Dkt 1 White Mirai Information