BRYAN SCHRODER
United States Attorney

ADAM ALEXANDER
Assistant U.S. Attorney
Federal Building & U.S. Courthouse
222 West Seventh Avenue, #9, Room 253
Anchorage, Alaska 99513-7567
Phone: (907) 271-5071
Fax: (907) 271-1500
Email: adam.alexander@usdoj.gov

C. ALDEN PELKER
Trial Attorney
Computer Crime & Intellectual Property Section
1301 New York Avenue NW
Washington, DC 20530
Phone: (202) 514-1026
Fax: (202) 514-6113
Email: catherine.pelker@usdoj.gov

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, v. JOSIAH WHITE, PARAS JHA, and DALTON NORMAN. Defendants.	)	Case No. 3:17-cr-00165-TMB, 3:17-cr-00163-TMB, 3:17-cr-00164-TMB, 3:17-cr-00166-TMB, and 3:17-cr-00167-TMB **GOVERNMENT'S MOTION FOR DOWNWARD DEPARTURE PURSUANT TO U.S.S.G. § 5K1.1**

MOTION OF THE UNITED STATES
FOR DOWNWARD DEPARTURE PURSUANT TO U.S.S.G. § 5K1.1

The United States, through undersigned counsel, hereby moves under United States Sentencing Guideline Section 5K1.1 for a reduction in the defendants' guidelines range. The Government's position, as stated in its sentencing memorandum, is that the defendants' cooperation has been extensive and exceptional and warrants a substantial reduction in sentence of 85%.

I. Background

In 2016, the defendants, Josiah White, Paras Jha, and Dalton Norman, worked to develop and operate the Mirai botnet, an Internet of Things botnet that, at its peak, consisted of hundreds of thousands of compromised devices. White, Jha, and Norman used the botnet to conduct a number of powerful Distributed Denial of Service (DDoS) attacks. Separately, from December 2016 to February 2017, Jha and Norman created and maintained a botnet devoted to advertising fraud, particularly clickfraud. The development, operation, and use of these botnets is detailed further in the Government's sentencing memorandum.

II. Cooperation

Prior to even being charged, the defendants have engaged in extensive, exceptional cooperation with the United States Government. This cooperation, described in greater detail below, is noteworthy in both its scale and its impact. The defendants have advanced computer skills and, through years of criminal activity and academic pursuit, developed expertise in botnets and denial of service attacks. The FBI's Anchorage Field Office ("FBI Anchorage") worked closely with the defendants to apply those skills in novel ways to benefit the Government

and the cybersecurity community at large. By working with the FBI, the defendants assisted in thwarting potentially devastating cyber attacks and developed concrete strategies for mitigating new attack methods. The information provided by the defendants has been used by members of the cybersecurity community to safeguard U.S. systems and the Internet as a whole.

The defendants have each exhibited tremendous dedication to their cooperation efforts, collectively logging what the Government estimates to be well over 1,000 hours of work for the U.S. Government. Specific details regarding some of the projects undertaken by the defendants are provided below, as well as in a forthcoming sealed addendum supplementing this filing.

A. Proxy Investigations

While the defendants used the Mirai botnet to conduct DDOS attacks, other cyber criminals have found alternative ways to monetize similar IoT botnets. One such scheme involves the use of the bots as proxies, or Internet relay devices, to conduct fraud schemes. Once the victim device is infected and incorporated into the botnet, it is used by criminals to relay traffic or communications to other websites or computers. By using the bots as proxies, the criminals can conduct advertising and credit card fraud on a massive scale, with little risk of the activity being linked back to the original perpetrator.

The defendants worked exhaustively with FBI Anchorage to identify actors and networks performing these compromises and utilizing the victim devices to perpetrate criminal fraud schemes. Particularly, the defendants were able to help FBI Anchorage identify the presence of several IoT proxy networks directly affecting Alaska. FBI Anchorage was then able to notify the affected Alaskan entities and remediate the infections, freeing the Alaskan victims from the botnets' control. In some cases, these proxy networks had resulted in losses to Internet carriers

of hundreds of thousands of dollars. In multiple instances, the defendants' work prevented further localized losses. Additionally, the defendants assisted FBI Anchorage in developing tools and technologies to more rapidly identify these types of networks, which should further reduce the impact of this new type of threat on Alaska and other communities.

B. Christmas DDOS Attack Prevention

Historically, the Christmas holiday is one of the most prolific periods of large-scale DDoS attacks. This is widely attributed in part to the school holidays, as the perpetrators of the attacks are often juveniles or young adults. The intensity of the attacks is further fueled by a sense of "one upsmanship" – that is, due to past high-profile attacks during this period, each year there is renewed interest in outdoing the previous year's attacks. The highest profile targets are the major online gaming services, such as Blizzard, Xbox, and Sony, but the attacks can negatively impact broad swaths of the Internet.

Leading up to the Christmas 2017 holiday season, the defendants worked with FBI Anchorage to identify likely attack methods and volumes. FBI Anchorage worked proactively with security researchers, the online gaming industry, and hosting companies to develop proper proactive defensive measures. Partially as a result of the defendants' efforts, there were significantly fewer large or targeted DDoS attacks during the Christmas 2017 holiday period.

C. Memcache Attack Mitigation

In March 2018, a new DDoS attack method emerged known as Memcache. Memcache is a legitimate protocol utilized for speeding up websites and networks by maintaining a cache of large, important, or frequently requested items. In DDoS attacks using Memcache, the attackers themselves loaded large amounts of extraneous data on servers that had the Memcache protocol

enabled. The attackers then fraudulently misrepresented themselves as the intended victims and requested the extraneous data from these servers and many others. The resulting DDoS attacks were some of the largest ever recorded. The impact on the stability and resiliency of the broader Internet could have been profound.

FBI Anchorage worked with the defendants and others within the security industry to identify the Memcache servers vulnerable to abuse by attackers. FBI Anchorage then provided this information to those companies principally affected by Memcache, either because they hosted servers vulnerable to abuse of the protocol or because they were operating system vendors for which the Memcache protocol was enabled in their default builds. Due to the rapid work of the defendants, the size and frequency of Memcache DDoS attacks were quickly reduced such that within a matter of weeks, attacks utilizing Memcache were functionally useless and delivering attack volumes that were mere fractions of the original size.

D. Work with Security Researchers

On many occasions, the defendants volunteered to collaborate with researchers and representatives of Internet security companies in order to assist with ongoing projects or investigations. The defendants have provided briefings to companies and cybersecurity researchers. During these presentations defendants would discuss past and current tactics employed by criminal groups as well as novel mitigation techniques. Further, defendants assisted various researchers with establishing "attribution," that is, determining the true or suspected identities associated with a given criminal nickname.

In one noteworthy incident, defendants were able to provide expert assistance to a private researcher actively investigating an Advanced Persistent Threat (APT) group, an industry term

used to denote malware or Internet activities suspected of being associated with a country's military or intelligence services. Similarly, the defendants worked closely with certain researchers to accurately describe and categorize the various IoT threats that were affecting platforms for which the researcher was assigned to defend.

E. Coding Projects

The defendants have assisted FBI Anchorage with a number of projects related to the development or review of computer code. This included examining the source code of other botnets and cyber criminal tools, a process which included limited reverse engineering as well as diagraming and documentation of their associated analysis. The defendants also wrote several pieces of code for the FBI to support cases and cybersecurity programs. Of particular note, the defendants, who have extensive cryptocurrency knowledge, developed a program that allowed law enforcement to examine cryptocurrency private keys in a variety of formats. This program was designed to derive information utilizing different input variables, including the wallet "seed." This program and the features devised by defendants can greatly reduce the time needed by Law Enforcement to do initial cryptocurrency analysis as the program automatically determines a path for a given wallet. By displaying in a graphical user interface form critical wallet information and associated public and private keys, the program also reduces the difficulty associated in conducting an initial analysis of a cryptocurrency wallet.

F. Kelihos Victim Notification

In 2017, the FBI's Anchorage and New Haven offices executed a takeover of the Kelihos botnet to coincide with the arrest of the botnet operator. For a decade, Kelihos had been one of the Internet's top spam and malware delivery platforms, negatively affecting

individual users and corporations alike. Upon conclusion of the botnet takeover operation in 2018, FBI Anchorage had the responsibility to notify victims of the Kelihos botnet who had been infected with the virus at the time of the takeover operation. FBI Anchorage possessed vast logs containing the technical details of daily interaction between the victim computers and the sink-holed botnet, but the information did not include identifying information for the victims beyond their IP addresses. Parsing this data into a format usable for individual ISPs to provide notification to their customers, the victims, was a challenging undertaking. The Mirai cooperators devoted significant time to assisting FBI Anchorage with engineering a series of scripts which would parse the sinkhole data into a usable format. FBI Anchorage was then able to expeditiously begin the process of notifying the many botnet victims via their Internet Service Providers.

G. Meetings with Targets

As the FBI Anchorage office investigated other criminal groups associated with conducting large-scale DDoS attacks, various opportunities arose in which defendants offered to travel to meet with and surreptitiously record the activities of known investigative subjects. These actions significantly increased the speed by which FBI Anchorage could conduct complex DDoS investigations and resulted in significant judicial outcomes relative to these criminal groups. FBI Anchorage continues to investigate multiple groups responsible for large-scale DDoS attacks and seeks to continue to work with defendants.

The defendants similarly assisted with international investigations, at one point assisting foreign law enforcement by ensuring a given target was actively utilizing a computer during the execution of a physical search. Their actions directly contributed to significant material evidence

seized by the respective law enforcement agency. The defendants also assisted other FBI Field Offices with ongoing cyber investigations, either directly, or through data passed from FBI Anchorage to the respective investigating agents.

III. Conclusion

The United States respectfully asks the Court to consider the defendants' exceptional and extensive cooperation in imposing its sentence.

RESPECTFULLY SUBMITTED this 11th day of September, 2018, in Anchorage, Alaska.

BRYAN SCHRODER
United States Attorney

s/ Adam Alexander
ADAM ALEXANDER
Assistant U.S. Attorney

C. Alden Pelker
Trial Attorney
Computer Crime & Intellectual Property Section
U.S. Department of Justice

CERTIFICATE OF SERVICE

I hereby certify that on September 11, 2018, a copy of the foregoing was served electronically on:

Rich Curtner, Federal Public Defender
Robert Stahl, Esq.
David Nesbett, Esq.

s/ Adam Alexander
Office of the U.S. Attorney