U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

April 28, 2016

Honorable Kimba M. Wood
United States District Judge
Southern District of New York
500 Pearl Street
New York, New York 10007

Re: *United States* v. *Nikita Kuzmin*, 11 Cr. 387 (KMW)

Dear Judge Wood:

The Government respectfully submits this letter in advance of the sentencing of defendant Nikita Kuzmin, which is currently scheduled for May 2, 2016, at 10 a.m. In its Presentence Report ("PSR"), the United States Probation Office ("Probation") correctly calculates that the defendant's Guidelines range is 151-188 months' imprisonment. Probation recommends a non-Guidelines sentence of 84 months, noting that its position does not take into account any assistance Kuzmin has provided in this case.

The Government writes to advise the Court of the relevant facts regarding the defendant's offense and substantial assistance to the Government in this case. In light of the facts set forth below, and assuming that the defendant continues to comply with the terms of his cooperation agreement and commits no additional crimes before sentencing, the Government intends to move at sentencing, pursuant to Section 5K1.1 of the Guidelines and Section 3553(e) of Title 18, United States Code, for the Court to sentence the defendant in light of the factors set forth in Section 5K1.1(a) of the Guidelines.

A. The Investigation of Gozi and 76 Service

In approximately 2007, computer network security experts identified, for the first time, a form of malicious software, or malware, that was stealing victims' personal bank account information on a widespread basis. The malware, which the experts named "Gozi," infected the victim's computer, among other ways, when the victim received and opened a .pdf document that was designed to appear innocuous and relevant to the victim. Opening the .pdf caused the Gozi malware to be downloaded onto the victim's computer secretly where it generally remained undetectable by anti-virus software. Once downloaded, the malware collected bank account-related data from the victim's computer, including the username and password to access the victim's bank account online. The malware transmitted that data to the individuals who controlled the malware, which they used to fraudulently transfer money out of victims' bank

accounts. The network security experts subsequently identified a server that contained certain data stolen by Gozi, including 10,000 account records belonging to over 5200 personal computer users. The records included login information for accounts at over 300 companies, including leading global banks and financial services firms.

For years, Gozi was the subject of law enforcement investigations and analysis by network security experts and financial institutions. Coordinated efforts between the Government and law enforcement in multiple countries ultimately led to the identification of the defendant, Nikita Kuzmin, a Russian national, as the individual who controlled the malware.

In addition to creating Gozi (as described below), Kuzmin developed an innovative means of distributing and profiting from it. Unlike many cybercriminals at the time, who profited from malware solely by using it to steal money, Kuzmin rented out Gozi to other criminals, pioneering the model of cybercriminals as service providers for other criminals. For a fee of $500 a week paid in WebMoney, a digital currency widely used by cybercriminals, Kuzmin rented the Gozi "executable," the file that could be used to infect victims with Gozi malware, to other criminals. Kuzmin designed Gozi to work with customized "web injects" created by other criminals that could be used to enable the malware to target information from specific banks; for example, criminals who sought to target customers of particular American banks could purchase web injects that caused the malware search for and steal information associated with those banks. Once Kuzmin's customers succeeded in infecting victims' computers with Gozi, the malware caused victims' bank account information to be sent to a server that Kuzmin controlled where, as long as the criminals had paid their weekly rental fee, Kuzmin gave them access to it. Kuzmin, who used the online identity "76," advertised this cybercriminal business, which he called "76 Service," on underground cybercriminal forums.

In the course of the investigation, Gozi was found to have infected over 1,000,000 computers across the United States, Germany, Great Britain, Poland, France, Finland, Italy, Turkey, and other countries. U.S. victims include individuals, companies, and others, including the National Aeronautics and Space Administration. While the losses attributable to Gozi are difficult to determine precisely, based on certain institutions' loss estimates, the Government believes Gozi has caused at least tens of millions of dollars in losses to the individuals, businesses, and government entities whose computers were infected with it.

In November 2010, Kuzmin traveled to a conference in the United States and was arrested on a complaint in this case. He began cooperating immediately.

B. The Information, Kuzmin's Guilty Plea, and the Guidelines Calculation

In May 2011, the defendant appeared before the Honorable Leonard Sand and pled guilty pursuant to a cooperation agreement to the above-referenced seven-count Information charging him with conspiracy and substantive counts of bank fraud, access device fraud, and computer intrusion (the latter of which included substantive counts of computer intrusion to obtain information in a financial record, and to further a fraud), in violation of 18 U.S.C. §§ 1349, 1344,

1029(b)(2), 1029(a)(5) and (c)(1)(A)(2), 1030(b), 1030(c)(2)(B)(i)-(iii), and 1030(c)(3)(A), respectively. The cooperation agreement provided that, if Kuzmin rendered substantial assistance in the investigation and prosecution of others, and otherwise complied with the obligations imposed by the agreement, the Government would request that the Court sentence him in light of the factors set forth in Section 5K1.1(a) of the United States Sentencing Guidelines which, as set forth above, it intends to do. Pursuant to his cooperation agreement, and during his plea allocution, Kuzmin admitted to the forfeiture allegations with respect to the counts in the Information and consented to the entry of a consent order of forfeiture in an amount to be determined by the Court.

The Probation Department correctly calculates the total adjusted offense level attributable to the defendant's conduct is 34, and that the defendant is in Criminal History Category I because he has no criminal history, yielding a Guidelines range of 151 to 188 months' imprisonment. PSR at ¶ 47 and p.18. The Probation Office recommends a sentence of 84 months' imprisonment, noting that it takes no position on whether the sentence should be adjusted in connection with any motion made by the Government under Section 5K1.1 of the Guidelines. PSR at Sentencing Recommendation.

C. Kuzmin's Cooperation

1. Kuzmin's Criminal Conduct

Kuzmin admitted, immediately upon his arrest, that he engaged in the charged criminal conduct. In a series of proffers with the Government, Kuzmin provided detailed information on how he created and disseminated the Gozi malware. Kuzmin also admitted engaging in uncharged criminal conduct, as set forth below, which the Government would not have known about but for his admissions.

a. Gozi and 76 Service

Kuzmin attended two major engineering universities in Russia beginning at age 16 and graduated with a computer science degree. He conceived of the idea of Gozi and 76 Service around 2005, when he was 18 years old. According to Kuzmin, he had initially purchased and attempted to use various forms of malware to steal money from bank accounts in the United States, Australia, and several Western European countries. When those attempts proved largely unsuccessful, Kuzmin decided develop his own malware to steal banking information.

Kuzmin developed a list of technical specifications for the malware he envisioned. Even with his advanced computer science skills, Kuzmin did not have sufficient technical skills to write the source code necessary to meet his specifications for the malware, so he hired another person (the "Coder") to write it. Kuzmin paid the Coder about $2000 a month in WebMoney for ten months to write and revise the source code to meet Kuzmin's specifications.

Soon after the Coder developed Gozi, Kuzmin began operating "76 Service," the cybercrime-as-a-service scheme through which he rented the malware to others. Kuzmin did not use the malware himself because, according to him, cashing out bank accounts could be difficult and required, among other things, depending upon people in the countries where the bank accounts were located to act as "money mules," receiving and transferring back the stolen funds.

Kuzmin stopped operating 76 Service around 2009 because it had begun to attract public attention, including by the network security experts whose work is described above. Thereafter, Kuzmin sold the Gozi source code – thereby enabling the purchaser to operate and disseminate the malware freely – to certain individuals for approximately $50,000 each. As to some of these individuals, Kuzmin retained a right to receive a share of their future profits from using the malware. Kuzmin knew that certain of these individuals planned to target and steal from victims in the United States, and based on information he later learned from them, he believes that they were successful. By Kuzmin's estimate, he made at least approximately a quarter of a million dollars renting and selling Gozi to other criminals.

b. Uncharged Criminal Conduct

Kuzmin admitted that he engaged in uncharged criminal conduct, most of which pre-dated his development of Gozi. The Government would not have known this conduct about but for his admissions.

According to Kuzmin, his first criminal scheme, which began about five years prior to his arrest in this case, involved the sale of stolen "ICQ" numbers. ICQ is an instant messaging service which, at the time, was owned by America Online; an ICQ number designates a particular ICQ user. Kuzmin estimated that he made approximately $20,000 selling stolen ICQ numbers.

When Kuzmin was approximately 18, he acted as a middleman in the sale of a database containing logs of stolen financial account data and earned approximately $2,000. However, Kuzmin also kept a copy of that database and, over the course of a year, attempted to use the stored usernames and passwords to withdraw money over the internet from over 100 bank accounts located abroad, including in the United States. Kuzmin hired people in the countries where the bank accounts were located to withdraw money from the victims' bank accounts and forward the funds to accounts he controlled. Through this scheme, Kuzmin attempted to transfer approximately $150,000 out of accounts using the stolen data, but was successful in transferring only about $50,000.

In addition, in about 2007, an individual approached Kuzmin online about stealing money from debit cards for which personal identification numbers had been stolen. Kuzmin negotiated a deal to participate in this fraud, and heard that the fraud had some success, but never received any money from it. He heard that the co-conspirator with whom he communicated was killed in a car accident.

Finally, several years ago, through co-conspirators he met on an internet forum, Kuzmin became involved in a fraud scheme that targeted victims in Italy. Kuzmin's partners used malware that caused victims' computer modems to make unauthorized, automated telephone calls to 1-900 telephone numbers that charged the victims—and paid Kuzmin and his co-conspirators—fees for the calls. Kuzmin earned $10,000-$15,000 from this scheme over a period of approximately two months.

2. Substantial Assistance

Kuzmin provided substantial assistance to the Government, as set forth in a separate letter which the Government has submitted and respectfully requests to file under seal.

D. Offense Conduct Discussion

As set forth above, Gozi malware has victimized countless people in the United States and across Europe, resulting in an estimated tens of millions of dollars in loss. The loss amount is difficult to quantify only because the malware is not readily detectable by victims. Illustrating the significance of the malware in the view of law enforcement, FBI identified the prosecution of Kuzmin as one of its top 10 most significant non-terrorism cases of the year.

Yet the significance of Kuzmin's offense reaches beyond the large dollar amount of loss that Kuzmin caused. Unlike most crimes, Kuzmin's crime – the creation and distribution of harmful malware - cannot be stopped simply by capturing the perpetrator, as the Government has done here. Because Kuzmin sold the Gozi source code to others, Gozi can be used by others, and it is in fact still in wide use by criminals today. In fact, through alterations to Gozi by others who have used it, new variants of Gozi have emerged that are also currently in use. As this illustrates, the seriousness of Kuzmin's crime, and the need for general deterrence, are heightened in this case by the difficulty of eradicating Gozi and other types of destructive malware once they are disseminated.

Kuzmin's offense is particularly significant for another reason, namely, that in perpetrating this crime, Kuzmin developed the model of cybercrime as a service. As noted above, instead of using Gozi solely for his own benefit, Kuzmin enabled other criminals to use it for a fee. This innovation (which was not solely Kuzmin's, though Kuzmin was a notable proponent of it) has contributed to the increase in the incidence of cybercrime in recent years. In renting the malware to others, Kuzmin made it widely accessible to criminals, in other words, to criminals who do not or need not have sophisticated computer science skills like Kuzmin and his Gozi co-creators. Since that time, cybercrime-as-a-service has become common; for example, ordinary criminals rent malware and destructive botnets to perpetrate criminal schemes of all kinds, and "hackers for hire" advertise their services on criminal internet forums. From this perspective, Kuzmin's crime is particularly significant.

Finally, in terms of Kuzmin's personal history and characteristics, while his malware victimized people indiscriminately, Kuzmin committed this crime purely out of greed. Kuzmin had an excellent education and valuable skills, graduating with a computer science degree from a

prominent engineering university in Russia. Kuzmin also had legitimate business interests, including in a start-up social media site in Russia called Youdo, among other things. But none of that was enough for him. Kuzmin used his talent and skills to create malware with the single purpose of stealing other people's money, and when he succeeding in doing that, he spent lavish sums on luxury sports cars, and extravagant travel and entertainment in Europe and Russia.

E. Forfeiture and Restitution

As set forth above, the actual losses attributable to Gozi are difficult to determine. The Government has received loss figures from three small banks, two in the United States and one in Europe, reflecting actual losses attributable to Gozi malware. Those losses total $6,934,979. Therefore, the Government respectfully requests that the Court enter a forfeiture order, and order restitution, in that amount. The Government will provide the Court with a proposed order of forfeiture for its consideration.

F. Conclusion

For the reasons discussed above, and assuming that Kuzmin continues to comply with all of the terms of his cooperation agreement, the Government intends to move at sentencing, pursuant to Section 5K1.1 of the Sentencing Guidelines, for the Court to sentence Kuzmin in light of the factors set forth in Section 5K1.1(a)(1) (5) of the Guidelines.

Respectfully submitted,

PREET BHARARA
United States Attorney

By: 
Nicole Friedlander
Assistant United States Attorney
(212) 637-2211

cc: Mr. Alan Futerfas, Esq.
Ms. Michelle Greer Bambrick, U.S. Probation Officer