IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No.
	)	
v.	)	**FILED *EX PARTE***
	)	**AND UNDER SEAL**
EVGENIY MIKHAILOVICH BOGACHEV, et al.	)	
	)	
	)	
Defendants.	)	

UNITED STATES' MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

Plaintiff, the United States of America, by and through its attorneys, David J. Hickton, United States Attorney for the Western District of Pennsylvania, Leslie R. Caldwell, Assistant Attorney General, Michael A. Comber, Assistant United States Attorney, and Ethan Arenson and David Aaron, Trial Attorneys, pursuant to 18 U.S.C. §§ 1345, 2521, and Federal Rule of Civil Procedure 65, hereby seeks an *ex parte* temporary restraining order commanding the defendants to halt a massive fraud and wiretapping scheme that is harming consumers, financial institutions, and other businesses in the United States and around the world.

I. OVERVIEW

The defendants in this case are responsible for two of the most sophisticated and destructive forms of malicious software ("malware") in existence: Gameover Zeus ("GOZ") and Cryptolocker. GOZ is a credential harvester that intercepts banking and other online credentials from infected computers and enlists those computers into a "botnet" – a network of infected computers controlled by the defendants. Cryptolocker is a form of malware known as "ransomware," which infects computers, encrypts essential files, and then demands a ransom of

hundreds of dollars in order to return the encrypted files to a readable state. Together, GOZ and Cryptolocker have infected hundreds of thousands of computers around the world and have generated direct and indirect losses to consumers and businesses that exceed $100 million.

In this action, the United States seeks injunctive relief commanding the defendants to stop using GOZ and Cryptolocker to defraud and wiretap American citizens and businesses. To give effect to this prohibition, the United States seeks permission to employ a series of technical measures designed to disrupt the defendants' malware and free victims from its grasp. Specifically, the United States seeks an Order: (1) directing four U.S. Internet Domain Registries to block access to the domain names used to control GOZ and to redirect connection requests to substitute servers established by order of this Court; (2) directing four U.S. Internet Domain Registries to block access to the domain names used to control Cryptolocker; and (3) directing the Internet Service Providers (ISPs) specified in TRO Appendix D to block their customers from connecting to the Russia-based Internet domain names listed in TRO Appendix C that are used exclusively to control computers infected with GOZ and Cryptolocker.

In addition to the civil relief sought above, the Government has also applied for a Pen Register/Trap and Trace Order that would authorize the collection of the dialing, routing, addressing, and signaling information of communications sent by the GOZ malware to the substitute servers and other infrastructure established pursuant to the TRO sought by the Government. This information would be disseminated to ISPs and other entities that would notify GOZ and Cryptolocker victims and provide instruction on how to remove these infections from their computers.

The final component of the operation will be seizures by foreign law enforcement officers of a number of computer servers that are critical to the infrastructure of GOZ and Cryptolocker. These servers are located overseas and will be disconnected from the Internet in a coordinated fashion by law enforcement agencies in a number of countries.

This action is the latest in a string of cases brought by public and private sector entities to combat malicious software, and is very similar to the successful Coreflood botnet disruption, which was initiated in the District of Connecticut in April 2011. *See United States v. John Doe 1 et al.* No. 3:11-CV-00561 (D. Conn., filed Apr. 11, 2011) ("*Coreflood*"). Coreflood, like GOZ, was a botnet used by criminals to intercept financial information and to execute fraudulent transactions. To disable Coreflood, the United States used the same authorities invoked here to deny the operators of Coreflood access to the infrastructure necessary to control the botnet. In Coreflood, the Government also received judicial authorization to establish a substitute server to replace the command and control infrastructure operated by the Coreflood defendants. These actions successfully crippled the botnet and disabled the criminal enterprise.[1]

In the years since Coreflood, the Microsoft Corporation has brought a number of civil actions against botnet operators. *See* Microsoft civil cases cited *infra* at Section VI(B). In each of these cases, Microsoft has been awarded injunctive relief – similar to the relief sought here – designed to disrupt the criminals' control over the botnet and liberate the infected computers.

The criminal enterprise responsible for GOZ and Cryptolocker is causing enormous injury in this District, in the United States, and around the world. To disrupt this criminal

---

[1] *See* Riva Richmond, "U.S. Dismantles Large Network of PCs Infected by Criminals," N.Y. Times, Apr. 15, 2011, http://query.nytimes.com/gst/fullpage.html?res=9E0DEFD8123EF936A25757C0A9679D8B63; Press Release, Department of Justice, "Department of Justice Takes Action to Disable International Botnet," (Apr. 13, 2011), http://www.justice.gov/opa/pr/2011/April/11-crm-466.html.

enterprise, and to protect American citizens and businesses from falling victim to GOZ and Cryptolocker, the United States respectfully requests that this Court enter the proposed temporary restraining order ("TRO") and order the defendants to show cause why a preliminary injunction should not be granted.

II. BACKGROUND ON GOZ AND CRYPTOLOCKER

A. Overview of GOZ

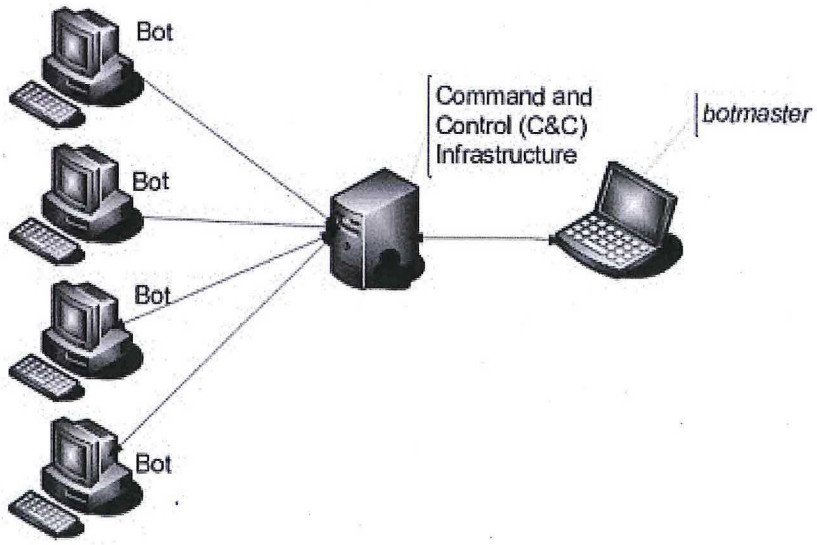
GOZ, also known as "Peer to Peer Zeus", is an extremely sophisticated malware variant that is designed to steal banking and other credentials from infected computers and to enlist them into a network of compromised computers known as a "botnet". *See* Declaration of Special Agent Elliott Peterson ("Peterson Decl.") at ¶4. GOZ is the latest incarnation of the Zeus malware, a credential stealer that first emerged in 2007. *Id.* Although earlier versions of Zeus were sold to anyone willing to pay the asking price, GOZ is tightly controlled and not distributed outside of the small, cohesive group of criminals who control the malware. *Id.* ¶¶ 20, 35.

Security researchers estimate that between 500,000 and one million computers worldwide are infected with GOZ, and that roughly 250,000 of those infected computers are active "bots" in the GOZ network at any given time. *Id.* ¶4. The remaining bots are also infected with the malware, but are "inactive" because, for example, they are not currently powered on or connected to the Internet. *Id.* Approximately 25% of the infected computers are located in the United States. *Id.*

The principal purpose of GOZ is to capture banking credentials from infected computers. *Id.* ¶5. The defendants then use those stolen credentials to initiate wire transfers to accounts controlled by the GOZ organization overseas. *Id.* ¶¶5, 14. Typical fraudulent wire transfers

initiated by the GOZ operators are in the hundreds of thousands of dollars and have reached as high as seven million dollars. *Id.* ¶¶5, 48. Total losses attributable to GOZ exceed $100 million since GOZ was first detected in September 2011. *Id.* ¶¶7, 47.

GOZ operates under a peer-to-peer framework that is designed to frustrate efforts to free infected computers from the GOZ botnet. *Id.* ¶8. Traditional botnets rely on a small number of centralized chokepoints known as command and control servers that the "botmaster" can use to push commands to, and receive information from, infected bots. *Id.* The diagram below illustrates how a traditional botnet functions:



Id.

GOZ, however, does not rely on command and control chokepoints, where control over the botnet could be compromised, instead adopting a peer-to-peer model in which the infected bots communicate with and pass along commands to one another. *Id.* ¶¶8,9. As a result of this

decentralized communications model, there is no chokepoint for law enforcement to target, which significantly complicates remediation efforts. *Id.* ¶9.

In place of a centralized command and control infrastructure, the GOZ operators designate thousands of infected computers within the botnet to serve as "Proxy Nodes." *Id.* Proxy Nodes have elevated status in the network and are used to relay commands from the GOZ operators to compromised computers in the network, known as "peers." *Id.* Any GOZ-infected computer can be promoted to a Proxy Node by the GOZ operators. *Id.* Also part of the GOZ botnet are "Master Drop" servers, which store stolen information for later use by the GOZ operators. *Id.*

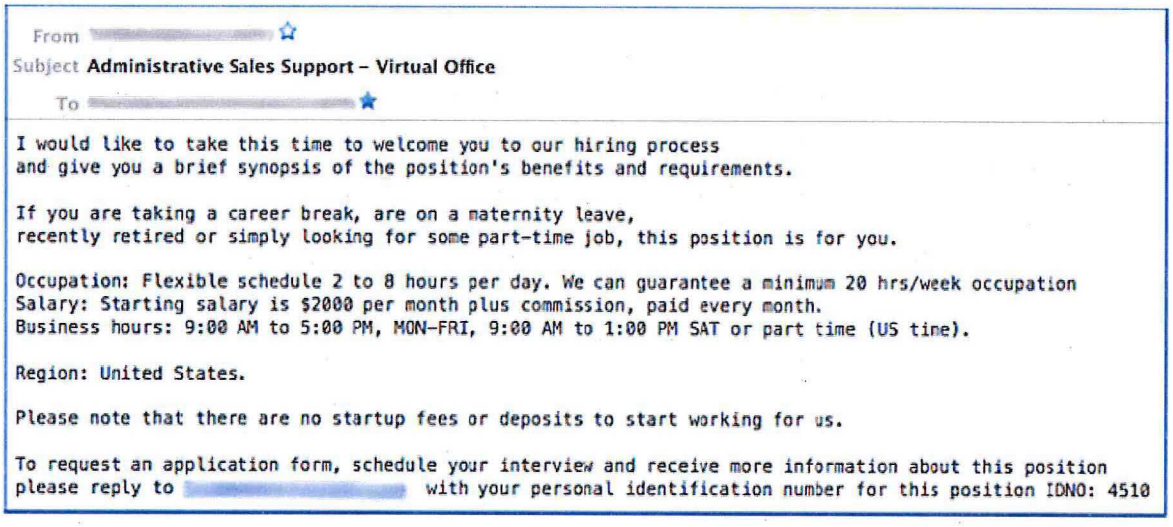
B. GOZ is Used to Wiretap Victims and to Facilitate the Theft of Funds

Once a computer is part of the GOZ botnet, the defendants have a variety of powerful options to steal sensitive information from the computer and to execute fraudulent transactions. *Id.* ¶10. The primary method used is known as a "man-in-the-middle" attack, which allows the GOZ operators to intercept communications between the victim's computer and a legitimate website, such as an online banking website. *Id.* To increase the effectiveness of the man-in-the-middle attack, GOZ is capable of changing the way a website appears to the victim computer's user. *Id.* So, for example, if a GOZ-infected user were to visit a banking website that typically requests only a username and password, the defendants could seamlessly insert additional fields into the website displayed in the user's web browser that request the user's Social Security number, credit card numbers, and other sensitive information. *Id.* Because these additional fields appear to be part of the legitimate website that the user elected to visit, the user is often

tricked into supplying the requested information, which is promptly intercepted by the GOZ malware and transmitted to the defendants. *Id.*

After stealing victims' personal information, the Defendants use the stolen credentials to log into victims' bank accounts and to initiate fraudulent electronic funds transfers from the victims' banks. *Id.* ¶13. This is most commonly done through the use of an Automated Clearing House ("ACH") payment or wire transfer sent to an accomplice known as a money "mule," who is employed for the specific purpose of retrieving the stolen money. *Id.*

Money mules are often recruited by the Defendants through spam email campaigns that promise lucrative jobs with flexible hours. *Id.* ¶14. In reality, the "job" offered to the prospective mules consists of nothing more than transferring stolen funds, which are wired to the mules after the Defendants have raided victims' bank accounts. *Id.* The Defendants instruct the money mules to keep a portion of the transferred funds as payment and then to wire the balance to a mule handler located overseas. A typical money mule recruitment email appears below:[2]



From [redacted]

Subject **Administrative Sales Support – Virtual Office**

To [redacted]

I would like to take this time to welcome you to our hiring process
and give you a brief synopsis of the position's benefits and requirements.

If you are taking a career break, are on a maternity leave,
recently retired or simply looking for some part-time job, this position is for you.

Occupation: Flexible schedule 2 to 8 hours per day. We can guarantee a minimum 20 hrs/week occupation
Salary: Starting salary is $2000 per month plus commission, paid every month.
Business hours: 9:00 AM to 5:00 PM, MON-FRI, 9:00 AM to 1:00 PM SAT or part time (US time).

Region: United States.

Please note that there are no startup fees or deposits to start working for us.

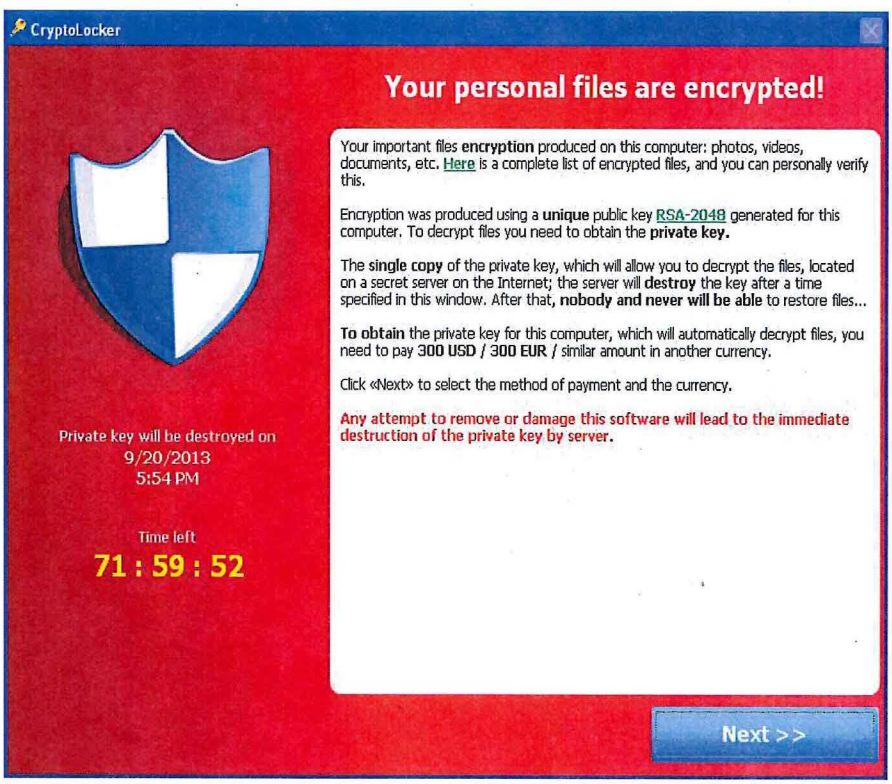
To request an application form, schedule your interview and receive more information about this position
please reply to [redacted] with your personal identification number for this position IDNO: 4510

[2] It is difficult to tie recruitment emails to specific botnets, and this email represents a general mule-recruitment solicitation.

Id. Accepting a job as a money mule typically has devastating consequences for the money mule. Not only is the money mule subject to potential criminal liability for money laundering, but mules are frequently held responsible for repaying all of the stolen money that has transited their accounts. *Id.* ¶15.

C. Cryptolocker

Cryptolocker is a malicious program designed to extract ransom payments from victims. *Id.* ¶16. After infecting a computer, Cryptolocker proceeds to encrypt files on the infected computer's hard drive. *Id.* Once the victim's files have been encrypted, Cryptolocker displays a notice on the victim's computer that demands payment of a ransom in exchange for the key that can decrypt the victim's files. *Id.* The ransom notice displayed to victims appears below:



Id. The Cryptolocker ransom, which varies in amount but can reach up to $750 or more, must be paid via anonymous, pre-paid cash vouchers like MoneyPak or via the virtual currency Bitcoin. *Id.* ¶17. Victims who refuse to pay the ransom face significant data loss, since the encryption algorithm used by the defendants is effectively unbreakable. *Id.*

Cryptolocker first emerged in mid-to-late 2013 and has infected more than 230,000 computers in the ensuing months, including more than 120,000 victims in the United States. *Id.* ¶18. Although the number of victims who have paid the Cryptolocker ransom is unknown, a reporter who studied the Bitcoin addresses used by the Cryptolocker operators estimates that $27 million in ransom payments were paid by victims between October 15 and December 18, 2013. *See id.*; Violet Blue, *Cryptolocker's Crimewave: A Trail of Millions in Laundered Bitcoin, ZDNet, Zero Day*, http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin-7000024579/.

Security researchers believe that GOZ is one of the primary methods criminals use to infect a computer with the Cryptolocker malware. Peterson Decl. ¶19. Among the features built into GOZ is a "user_execute" command that permits the defendants to install additional software onto any GOZ-infected machine. *Id.* The Defendants have used this capability to install Cryptolocker onto numerous computers already infected with GOZ, thereby adding another stream of revenue to their credential theft operation. *Id.*

III. THE DEFENDANTS

A multi-year investigation by the Federal Bureau of Investigation (FBI) has revealed that a tightly knit group of cybercriminals based in Russia and Ukraine is responsible for GOZ and Cryptolocker. *Id.* ¶20. Operating from computers located half-way around the world, these

individuals have deliberately targeted their malicious software at U.S. individuals and companies, with devastating effect. *Id.* Although the full scope of harm caused by the defendants is impossible to calculate, the best evidence available suggests that the defendants' malicious software has cost U.S. businesses and individuals more than $100 million. *Id.*

The defendants have gone to great lengths to conceal their identities and hide from law enforcement. Among other tactics, the defendants use false identities and online monikers, anonymous Internet-based payment systems, and an extensive network of money mules to launder the funds stolen during their high tech bank robberies. *Id.* ¶21. Despite these tactics, the FBI has identified an individual at the top of the criminal enterprise responsible for GOZ and Cryptolocker. That individual is Evgeniy Mikhailovich Bogachev of Anapa, Russia. *Id.*

Bogachev was indicted in the Western District of Pennsylvania on May 19, 2014 for violations of 18 U.S.C. §§ 371 (Conspiracy), 1030(a)(2) (Unauthorized access to a protected computer), 1343 (Wire Fraud), 1344 (Bank Fraud); 1956 (Money Laundering) and 1957 (Engaging in monetary transactions in property derived from specified unlawful activity) arising from his leadership role in the GOZ conspiracy. The indictment against Bochachev is currently under seal, but will be unsealed on or about June 3, 2014, if the Court grants the TRO sought by the Government. Bogachev will also be added to the FBI's list of most wanted cyber criminals and a substantial reward will be offered for information leading to his arrest. *Id.* ¶22.

In addition to Bogachev, the FBI has identified a number of other individuals who are part of the criminal enterprise responsible for GOZ and Cryptolocker. These individuals are known by the online monikers "Temp Special", "Ded", "Chingiz 911", and "mr. kykypky", and have also been named as defendants in this action. *Id.* ¶23.

A. Evgeniy Mikhailovich Bogachev

In the course of its GOZ investigation, the FBI obtained via a Mutual Legal Assistance Treaty (MLAT) request a copy of a server in the United Kingdom (UK) that was believed to serve as a communications hub for the operators of GOZ. *Id.* ¶24. Subsequent FBI analysis of the UK server revealed that the server played a much larger role than initially believed. *Id.*

1. *visitcoastweekend.com*

Among other content, the UK server hosted a website called *visitcoastweekend.com,* which was accessible only to authorized users with a username and password. *Id.* ¶25. The Frequently Asked Questions page for that website, translated from the original Russian below, detailed the website's function:

> Starting on September 19, 2011, we are beginning to work through the panel where you now find yourselves. [Fraudulent] Money transfers and drop [money mule] managers are synchronizing their work through our panel, which enables a much greater optimization of the work process and increase in the productivity of our work. Starting from this moment, all drop [money mule] managers with whom we are working and all [fraudulent] money transferors who work with us are working through this panel. We wish you all successful and productive work.[3]

Id.

Among other content, the *visitcoastweekend.com* website hosted a detailed ledger of hundreds of financial transactions that include dates, company names, amounts, and an indicator whether the transaction was an ACH payment or a wire transfer. *Id.* ¶26.

One of the company names in the *visitcoastweekend.com* ledger is of a composite materials company in the Western District of Pennsylvania (Victim Company #1). *Id.* ¶27. The

[3] The terms in brackets are not the actual words used on the webpage; however, the actual word used was slang and the implied meaning of the term is what the translator has provided in brackets.

ledger lists a wire transfer of $198,234.93, the date October 21, 2011, and a bank account number. *Id.*

The FBI has confirmed that Victim Company #1 was the target of a bank account intrusion that caused $198,234.93 to be wired from its account to an account at another U.S. bank on October 20, 2011. *Id.* ¶28. The unauthorized wire transfer was initiated using the credentials of two employees at Victim Company #1, both of whom denied any knowledge of the transfer. *Id.* Subsequent FBI analysis confirmed that the employee credentials used in the theft were stolen from a computer at Victim Company #1 that was infected with GOZ. *Id.*

The FBI has interviewed a number of the victims listed in the ledger and studied fraud reports submitted by banks that match the transactions in this ledger. *Id.* ¶29. This analysis has led the FBI to conclude that the entries in the ledger are victims of GOZ, and that the ledger was used by the GOZ operators to track their bank account intrusion activity and subsequent money laundering efforts. *Id.*

2. Businessclub Website

In addition to the *visitcoastweekend.com* website, the UK server also contained data related to the website *work.businessclub.so* (the "Businessclub website"). *Id.* ¶30. FBI analysis of the Businessclub website revealed a ticket system where technical issues and upgrades to the GOZ botnet and infrastructure were posted and assigned to be performed by registered members of the website. *Id.* ¶30-31. The website also tracked the status of assigned projects. *Id.*

B. Bogachev's ties to the UK Server, *visitcoastweekend.com* and the Businessclub website

During the course of the FBI's investigation of GOZ, a source advised the FBI that a GOZ administrator was using an email address hosted by a Russian provider. *Id.* ¶32. To pursue

this lead, a search warrant was issued to a U.S. Service Provider (the "Service Provider") for records related to this email address. *Id.* The records produced in response to the search warrant revealed an account in the name of Evgeniy Bogachev. *Id.* Importantly, the Service Provider's response also contained a comprehensive log of IP addresses that were used to access Bogachev's account from 2010 through October 2013. *Id.*

The FBI compared the IP addresses from Bogachev's account with a series of server logs obtained from the UK GOZ server. *Id.* ¶33. Specifically, the FBI compared the IP data from the Service Provider with three other sources: the logs from the Administrative Panel for the UK server, the logs for *visitcoastweekend.com*, and the logs for the Businessclub website. *Id.* This analysis revealed hundreds of instances in which the same IP address was used to access Bogachev's account with the Service Provider, the Administrative Panel for the UK Server, *visitcoastweekend.com*, and the Businessclub website within a short period of time. *Id.*

Further analysis of the UK server logs revealed compelling evidence linking the Bogachev-connected IP addresses used to access the Administrative Panel of the UK Server and the Businessclub website to the same computer. *Id.* ¶34. The FBI made this connection by studying a digital footprint known as a "user agent string." *Id.* When connecting to a website, the user's web browser transmits a user agent string – information about the computer on which the browser is running. This information typically includes the computer's operating system and version, as well as information about the browser itself, including the version number. *Id.* The FBI compared the user agent string information for numerous logins to the Administrative Panel of the UK Server and the Businessclub website from IP addresses previously tied to Bogachev.

Id. This analysis confirms that the same user agent string appears again and again connected to these logins. *Id.*

This consistent pattern of overlapping IP addresses and user agent strings establishes that Bogachev was the individual utilizing and managing the GOZ infrastructure. *Id.* ¶35. Moreover, the fact that Bogachev had elevated Administrative access to the critical UK GOZ server establishes that he is not only a participant in the GOZ conspiracy, but a leader. *Id.*

C. Bogachev's Use of the "Pollingsoon" Moniker

A user known as "Pollingsoon" has participated for years in an underground hacking forum known as Cardingworld. *Id.* ¶36. Using the IP data from Bogachev's account with the Service Provider, the FBI has been able to link Bogachev to the Pollingsoon moniker. *Id.*

On multiple occasions, Pollingsoon has claimed to be the author of the Zeus malware in private messages sent to other members of the Cardingworld forum. *Id.* ¶37. In other private messages, Pollingsoon has stated that he is "Slavik" and provided ICQ numbers[4] registered to the moniker Slavik. *Id.* Slavik's central role in the development and sale of the original Zeus malware led the Microsoft Corporation to name Slavik as a defendant in its March 2012 civil suit brought against numerous online monikers that Microsoft alleged to be the perpetrators of Zeus. *See Microsoft Corp. v. John Does 1-39*, No. 1:12-CV-01335 (E.D.N.Y. 2013). That suit concluded on November 29, 2012, when Judge Sterling Johnson of the Eastern District of New York entered a permanent injunction against Slavik and other aliases ordering them to, *inter alia*, stop infecting Microsoft Windows customers with malicious software and to stop enlisting

[4] ICQ is an instant messaging platform that allows participants to communicate with each other in near real time. Each ICQ subscriber has a unique ICQ number, which is the rough equivalent of a telephone number. A user seeking to communicate with another ICQ subscriber must know the ICQ number of that subscriber in order to communicate with that user. Petersen Decl. ¶37.

Microsoft Windows customers into botnets. *See* Order for Permanent Injunction, *id.* (Nov. 29, 2012).

There is evidence that the Slavik moniker and the Slavik ICQ addresses may have been shared between two or more individuals, and it is possible that others had substantial roles in developing and marketing earlier versions of Zeus as well as GOZ. Peterson Decl. ¶39. Nonetheless, the evidence against Bogachev summarized above and described in more depth in the Declaration of Special Agent Peterson establishes clear probable cause to believe that Bogachev has been involved with the Zeus malware for more than four years and is a senior member of the criminal enterprise that developed and deployed the earlier versions of Zeus as well as GOZ.

D. Bogachev's Ties to Cryptolocker

In the course of its investigation of Cryptolocker, the FBI located a server located in Luxembourg that served as a critical part of the Cryptolocker infrastructure. *Id.* ¶40. Pursuant to a Mutual Legal Assistance Treaty request, the FBI obtained a copy of the Luxembourg server. *Id.* ¶41. FBI analysis of the server showed that the server was accessed on numerous occasions in May 2013 via an Administrator account utilizing an IP address in Switzerland. *Id.*

Aware of the close ties between Cryptolocker and GOZ, the FBI compared the IP address used to access the Luxembourg Cryptolocker server with the IP addresses used to access Bogachev's account with the Service Provider. The comparison revealed that on multiple occasions in May 2013, the same IP address was used to access Bogachev's account with the Service Provider and the Luxembourg Cryptolocker server within a short period of time. *Id.* For

example, on May 29, 2013, the same IP address accessed the Luxembourg Cryptolocker server and Bogachev's account with the Service Provider within a window of less than three hours. *Id.*

The fact that an IP address tied to Bogachev repeatedly accessed a critical server in the Cryptolocker infrastructure, and had full administrative access to that server, is yet more evidence of Bogachev's leadership role in the criminal enterprise responsible for GOZ and Cryptolocker.

E. The Nickname Defendants

The FBI's review of the data associated with the Businessclub website revealed a list of registered users with the authority to access the site, as well as their assigned roles. *Id.* ¶42. The user list does not include real names, but rather lists online monikers. *Id.* Based on this information, the FBI has concluded that four individuals are likely to have sufficient control over the GOZ botnet to enable them to comply with a TRO from this Court ordering them to halt the scheme. *Id.* These individuals use the monikers "Temp Special", "Ded", "Chingiz 911", and "mr. kykypyky". *Id.* Each has been named as a defendant in this action. *Id.*

IV. GOZ AND CRYPTOLOCKER HAVE HARMED VICTIMS IN THIS DISTRICT AND THROUGHOUT THE UNITED STATES

GOZ and Cryptolocker have caused enormous injury in this District and throughout the United States. *Id.* ¶46. Although it is impossible to fully quantify the losses these two malicious programs have caused, the paragraphs below provide the court with an overview of the scope of injury at issue.

A. GOZ

Based on its investigation to date, the FBI estimates that GOZ has caused more than $100 million in direct loss since GOZ was first detected in September 2011. *Id.* ¶47. These

estimates are based on victim reporting and undoubtedly underestimate the actual losses that GOZ has caused, since victims are rarely able to connect their losses to the theft of their banking credentials by GOZ. *Id.*

GOZ is programmed to defeat the added safeguards that banks place on corporate bank accounts, including one-time authorization codes. *Id.* ¶48. Accordingly, the defendants often use GOZ to target lucrative corporate bank accounts, especially those belonging to small and mid-sized businesses. *Id.* The impact of these attacks on these organizations is often devastating, as illustrated by the cross-section of GOZ victims discussed below:

- In October 2011, a composite materials company in the Western District of Pennsylvania had more than $198,000 wired from its bank account. Although the bank's records show that the wire was authorized by two company employees, the employees denied initiating or approving the wire transfer. Subsequent FBI investigation revealed that an employee at the materials company had unknowingly infected a company computer with GOZ by clicking on a link in an email. GOZ was then used to steal the credentials of two company employees authorized to approve wire transfers. Those credentials were then used to initiate the fraudulent wire transfer.

- In February and March 2012, an Indian tribe in Washington State had more than $277,000 wired from its bank account to overseas accounts. Subsequent FBI investigation revealed that a computer at the tribe's accounting firm was infected with GOZ and that the fraudulent wire transfers were initiated using credentials stolen from the accounting firm.

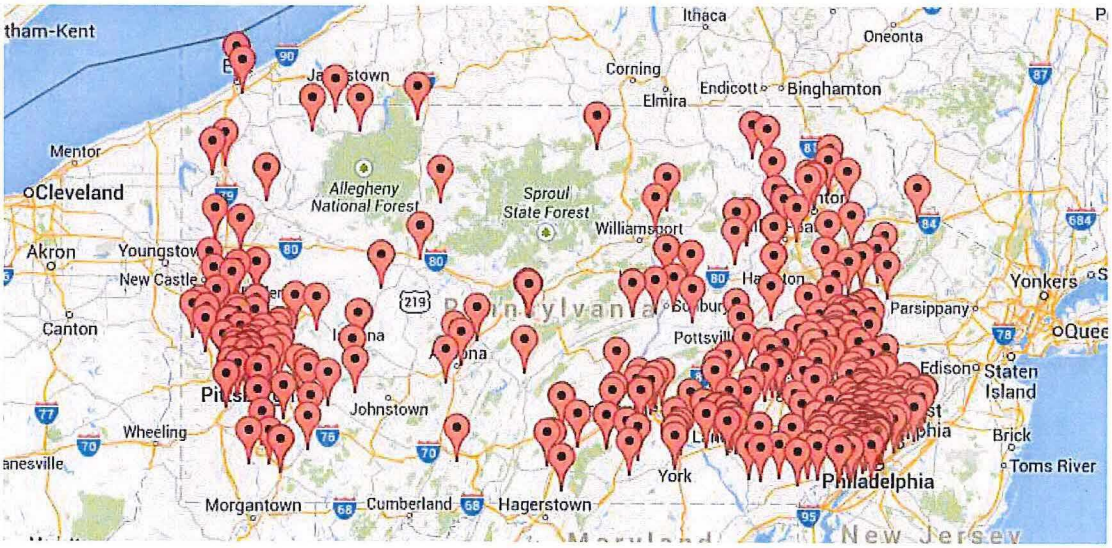
- In April 2012, the Director of Finance for three assisted living facilities in eastern Pennsylvania unknowingly infected his computer with GOZ via a malicious email. Shortly thereafter, a total of $190,800 in fraudulent ACH transfers were initiated from the facilities' corporate bank account.

- In November 2012, a regional bank in northern Florida had nearly seven million dollars fraudulently wired out of one of its accounts. The bank maintained an account at a larger correspondent bank – a bank that provides services to other banks rather than to businesses or individuals. On November 6, 2012, a fraudulent wire in the amount of $6,984,672 was initiated from the correspondent bank account to an account in Switzerland. Although the correspondent bank's records show that the wire was initiated by an employee of the Florida bank, that

> employee denied initiating or authorizing the wire transfer. Subsequent FBI investigation confirmed that a computer at the Florida bank was infected with GOZ, and that the infected computer was used to steal the credentials that were used to initiate the fraudulent transfer.

Id.

Additional insight about the impact of GOZ on this District, and the Commonwealth of Pennsylvania as a whole, can be gained by studying GOZ infection data. *Id.* ¶49. The infection map below was created by a private security researcher who has extensively studied the GOZ botnet and was able to plot the IP addresses of GOZ infected computers on a single day in May 2013. *Id.* The map shows a large number of GOZ infections in this District, and in Pennsylvania as a whole.



Id. ¶50.

B. Cryptolocker

By monitoring connection attempts to domain names used by Cryptolocker, security researchers are able to estimate the total number of Cryptolocker infections. *Id.* ¶51. This data

shows that as of April 2014, Cryptolocker has infected more than 234,000 computers, and that more than half of those infections – nearly 120,000 – occurred in the United States. *Id.*

It is estimated that tens of millions of dollars in ransom payments have been paid by Cryptolocker victims. *Id.* ¶52. Although this figure is substantial, it is a small fraction of the actual losses caused by Cryptolocker. *Id.* FBI interviews with numerous Cryptolocker victims demonstrate that many victims are either unable or unwilling to pay the ransom demanded by the Defendants. *Id.* As a result, these victims often end up losing their data. *Id.* While it is difficult to assign a dollar value to these losses, the victim narratives below help illustrate the magnitude of the loss:

- In November 2013, an employee at an insurance company in Pittsburgh, Pennsylvania opened an attachment to an email that purported to originate from a major U.S. bank. The attachment infected the employee's work computer with Cryptolocker. Cryptolocker encrypted the files on the employee's computer and displayed a splash screen demanding that a ransom be paid in order to return the encrypted files to a readable state. The employee subsequently learned that because his computer was connected to the company's network at the time of infection, Cryptolocker was able to access the company's network and encrypt critical business files. The company was able to repair the damage by using backup files, but was forced to send employees home while the repair work was completed. The company estimates its total loss at $70,000.

- In October 2013, an employee of a restaurant operator in Florida opened an attachment to an email that appeared to originate from inside the company. The attachment infected the employee's work computer with Cryptolocker, which encrypted the files on her computer as well as a shared network drive. More than ten thousand files were encrypted, including the contents of the company's team training, franchise, and recipe folders. The company's head of Information Technology estimates that remediating the Cryptolocker infection has cost the company $30,000.

- In November 2013, a computer at the Swansea Police Department in Massachusetts ("SPD") was infected with Cryptolocker. Because the infected computer was connected to the SPD's network, Cryptolocker was able to encrypt the SPD's main file server. Files encrypted on this server included administrative documents, investigative materials, and seven years' worth of digital photo mug shots. To recover these critical files, the SPD was forced to pay the $750 ransom demanded by Cryptolocker.

- On April 4, 2014, an employee at a pest control company in North Carolina unwittingly infected the company's computers with Cryptolocker after opening an email attachment. Cryptolocker promptly traversed the company's network and encrypted the company's most critical files, including its customer database and schedule of appointments. Cryptolocker also encrypted the company's backup server. The company hired a computer forensics firm to recover the encrypted data, but no data could be saved. The owner of the company estimates that the Cryptolocker infection has cost his company approximately $80,000 to date and is contemplating whether the losses incurred will force him to lay off employees.

Id.

V. THE UNITED STATES IS PREPARED TO DISRUPT THE GOZ BOTNET AND CRYPTOLOCKER

The FBI has developed a comprehensive technical plan to disrupt both the GOZ botnet and Cryptolocker. *Id.* ¶53. A detailed review of the technical disruption effort and subsequent remediation campaign is provided below.

A. GOZ

The GOZ botnet is widely believed to be the most advanced in existence and one of the most difficult to remediate. *Id.* ¶54. This is primarily due to the botnet's decentralized command and control infrastructure, which makes the GOZ botnet impervious to traditional disruption techniques such as seizing key command and control servers or domain names. *Id.*

To successfully disrupt the GOZ botnet requires a comprehensive technical approach that severs the three separate communications channels used by the defendants to control the infected computers within the botnet. *Id.* ¶55. The technical operations planned against each of these three communications channels – the Peer Layer, the Proxy Layer, and the Domain Generation Algorithm – are discussed below. *Id.*

[REDACTED **]**

3. The DGA Domains

The final step to liberating infected computers from the GOZ botnet is to control the Internet domains generated by GOZ's Domain Generation Algorithm ("DGA"). *Id.* ¶67. The DGA is yet another failsafe built into the GOZ code that is designed to harden the GOZ network against communications failures and disruption efforts. *Id.* The DGA generates a list of 1,000 domain names, which consist of lengthy combinations of letters – acawktkhtdfqfumnttoaydwckn, for example – combined with one of six top level domains ("TLDs"): .com, .net, .org, .biz, and .info, which are controlled by Registries in the United States and .ru, which is TLD for the Russian Federation. *Id.*

At least once every week,[5] the GOZ code picks a random starting point on the list of 1,000 domain names generated by the DGA and attempts to connect to that domain. *Id.* ¶68. If no response is received, the GOZ code will move to the next domain and proceed sequentially through the list until a successful connection attempt is made. *Id.* If attempts to reach all 1,000 of the domains fail, the GOZ code will try again the next week using a fresh list of 1,000 domains generated by the DGA. *Id.* After connecting to a DGA domain, GOZ requests a Peer List – a list of other infected bots in the GOZ network. *Id.* Once the Peer List is received, GOZ appends a select number of the new Peers to the existing list of Peers maintained on each infected computer. *Id.*

In order to prevent the defendants from using the DGA to recapture Peers at the substitute servers, it is essential that the domains generated by the DGA be kept out of the defendants'

[5] In addition to the weekly check-in, a Peer will seek a Peer List from the DGA domains whenever there are fewer than 25 peers on its Peer List or the Peer fails to learn of any new Peers during Peer verification. *Id.* ¶68 n.9.

control.[6] *Id.* ¶69. The TRO sought as part of this action denies the defendants these domains through two provisions: 1) an Order to the Domain Registries that administer the U.S.-based TLDs requiring them to redirect connection attempts to DGA-generated domains to the substitute servers; and 2) an Order directing the largest domestic ISPs to block connection requests to the malicious .ru domains generated by the DGA. *Id.*

As discussed in more depth in the legal section below, blocking criminals from obtaining domain names and requiring Domain Registries to redirect traffic inbound to those domains has been authorized in a series of injunctions entered in other botnet disruption cases, including the Coreflood disruption. Requiring ISPs to block outbound connections to malicious botnet domains has also been ordered before. *See, e.g., Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction at 1, 8, 11, *Microsoft Corp. v. John Does 1-8 Controlling a Computer Botnet Thereby Injuring Microsoft and its Customers*, No. A13 CV 1014 (W.D. Tx. Nov. 25, 2013) (hereinafter "*ZeroAccess*"). The Government has consulted with the ISPs that would be impacted by the TRO and none have raised technical or legal objections.

B. Cryptolocker

The technical operation against Cryptolocker bears much in common with the operation against GOZ, but is far less complex. There are three essential elements. *Id.* ¶70.

The first step will be to seize key servers in the Cryptolocker infrastructure, which are located overseas. On or about May 30, 2014, the FBI's foreign law enforcement partners will seize these servers in coordination with the FBI's operation. *Id.* ¶71.

[6] The DGA has been reverse engineered by security researchers and as a result, the FBI is able to accurately predict which domains will be generated for each week. *Id.* ¶69 n.10.

The second and third steps in the operation target the DGA used by Cryptolocker. *Id.* ¶72. Like GOZ, Cryptolocker uses a DGA, although in a slightly different fashion. *Id.* The Cryptolocker DGA generates 1,000 domain names per day across seven TLDs. *Id.* Immediately upon infecting a computer, Cryptolocker attempts to connect to domains that are hardcoded into the malware. *Id.* If that connection attempt fails, Cryptolocker runs the DGA and attempts to connect to the domains generated by the DGA. *Id.* Testing of Cryptolocker has shown that Cryptolocker must connect to one of these command and control domains before it will encrypt files on the infected computer. *Id.* If these domains are blocked, Cryptolocker should not be able to initiate its encryption function. *Id.*

To add to the disruption caused by the infrastructure disruptions, this action seeks a TRO that prevents the defendants from registering and using the hardcoded domains and the Cryptolocker DGA domains. *Id.* ¶73. To keep these domains out of the defendants' hands, the requested TRO contains two provisions: 1) an order to the Domain Registrars responsible for the U.S.-based TLDs used by Cryptolocker that prohibits the Registrars from allowing these domains to be registered and used; and 2) an order directing the largest domestic ISPs to block connection requests to the .ru domains generated by the Cryptolocker DGA.[7] *Id.*

---

[7] There is one downside to disrupting the Cryptolocker infrastructure and blocking the Cryptolocker DGA domains: once the operation commences, computers that have already been infected and encrypted by Cryptolocker will be cut off from the network. *Id.* ¶73 n.11. As a result, it will be impossible for these users to pay the Cryptolocker ransom and obtain the private key to decrypt their computers. *Id.*

Although it is difficult to estimate the number of users that will be negatively impacted by the Cryptolocker disruption, the Government believes the number will be small. *Id.* After encrypting victim computers, Cryptolocker informs its victims that the ransom must be paid within 72 hours. *Id.* To highlight the urgency, Cryptolocker displays a countdown clock on victims' screens warning of the deadline. *Id.* It is reasonable to assume that the overwhelming majority of victims take this warning at face value and decide whether or not to pay the Cryptolocker ransom within the 72 hour period. *Id.* Accordingly, the pool of victims that wish to pay the Cryptolocker ransom but will be blocked from doing so because of the technical operation will be limited to those who have been infected

The injunctive relief sought against Cryptolocker is nearly identical to the relief sought against GOZ, and consistent with relief granted in other malware disruption efforts detailed in the legal argument section below. The Government has consulted with the ISPs that would be impacted by the TRO and none have raised technical or legal objections.

VI. ARGUMENT

A. Jurisdiction and Venue Are Proper in This Court

Sections 1345 and 2521 of Title 18 authorize the United States to "commence a civil action in any Federal court" to enjoin fraud, and to "initiate a civil action in a district court of the United States" to enjoin illegal interception of communications. As detailed above, and in the Complaint filed herewith, the defendants are engaged in fraud and wiretapping against U.S. citizens and businesses on a massive scale. Accordingly, subject matter jurisdiction is proper in this Court. This Court may also exercise personal jurisdiction over the defendants, who are foreign nationals that have deliberately targeted victims in this District. Venue is proper under 28 U.S.C. § 1391(b)(2), for the reasons discussed below in relation to personal jurisdiction.

1. The Defendants Are Subject to Personal Jurisdiction in This Court Because They Have Defrauded and Engaged in Unauthorized Wiretapping of Victims in this District

At the complaint stage, a *prima facie* case by the plaintiff of personal jurisdiction is sufficient. *Eurofins Pharma US Holdings v. BioAlliance Pharma SA*, 623 F.3d 147, 155 (3d Cir. 2010). For claims arising under federal law, serving a summons or filing a waiver of service establishes personal jurisdiction over a defendant who is subject to the jurisdiction of a court of general jurisdiction in the state where the district court is located. Fed. R. Civ. P. 4(k)(1); *see*

---

within 72 hours of the operation. *Id.* Some of the victims within this pool will have already paid the ransom, which will further reduce the number of impacted victims.

Provident Nat'l Bank v. California Federal Sav. & Loan Ass'n, 819 F.2d 434, 437 (3d Cir.1987) ("A federal district court may assert personal jurisdiction over a nonresident of the state in which the court sits to the extent authorized by the law of that state."). Pennsylvania law provides for jurisdiction "to the fullest extent allowed under the Constitution of the United States" and "based on the most minimum contact with [the] Commonwealth allowed under the Constitution of the United States." 42 Pa. Cons.Stat. Ann. § 5322(b); *see Marten v. Godwin*, 499 F.3d 290, 296 (3d Cir. 2007).

Pursuant to the Pennsylvania long-arm statute, this Court may assert personal jurisdiction if the defendants have sufficient "minimum contacts" with this forum and if subjecting the defendants to the court's jurisdiction comports with "traditional notions of fair play and substantial justice." *International Shoe Co. v. Washington*, 326 U.S. 310, 316-17 (1945); *Pinker v. Roche Holdings Ltd.*, 292 F.3d 361, 368-69 (3d Cir. 2002). Where, as here, the cause of action is related to the defendant's contacts with the forum, it is sufficient if the contacts show "purposeful availment" by the defendant of an opportunity to conduct activity in the forum state. *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985) ("Jurisdiction is proper . . . where the contacts proximately result from actions by the defendant *himself* that create a "substantial connection" with the forum).

Defendants' victims include many individuals and businesses within Pennsylvania. Defendants have not only infected countless computers in Pennsylvania with GOZ and Cryptolocker, but have intentionally caused enormous harm in this Commonwealth through bank account intrusions and extortion attempts. In so doing, the defendants have purposefully directed their conduct at Pennsylvania. Accordingly, the defendants' conduct readily satisfies the "minimum contacts" requirement of due process, and personal jurisdiction is consistent with the Pennsylvania long-arm statute, quoted above.

2. The Court Should Authorize Service of Process by Internet Publication and Delivery to Defendants' Last-Known Addresses

Unless otherwise prohibited by federal law or international agreement, an individual outside the United States may be served "as the court orders." Fed. R. Civ. Pro. 4(f)(3). The method of service selected must be "reasonably calculated, under all circumstances, to apprise interested parties of the pendency of the action" and afford them an opportunity to be heard." *Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306, 314 (1950).

Here, defendant Bogachev is located in Anapa, Russia. The remaining defendants are believed to reside in Russia or Ukraine, but their precise locations are not known. In order to ensure that these defendants are notified of the pendency of this action, the Government purposes to provide notice of this action through a number of methods.

First, the Government will serve the Complaint, Summons, TRO, and related filings ("Court Filings") via overnight delivery upon defendant Bogachev at his home address in Anapa, Russia.

Second, the Government will provide notice to defendants Bogachev and Chingiz 911 through email. Through the course of the FBI's investigation, the Government has uncovered

email addresses used by these two defendants. The Government will email the Court Filings to these e-mail addresses, which should provide these two defendants with notice of this suit.

Third, the Government will send the Court Filings to the e-mail addresses provided for every active GOZ and Cryptolocker domain name. Domain name registrants are required to provide accurate contact information when they register a domain name. Although cybercriminals often use incomplete or inaccurate contact information during these registrations, they frequently provide at least one accurate email address in order to ensure that they receive important communications about the domain. Accordingly, sending the Court Filings to the postal and email addresses listed in the domain registrations should serve to notify the defendants of this case.

Fourth, the Government's will post copies of the Court Filings on the websites of the Department of Justice and the FBI. If the TRO is granted, all press releases issued by the Department of Justice and the FBI with respect to this matter will direct the defendants to the websites where those pleadings can be accessed. Moreover, because the Government's plan to assist victims of GOZ and Cryptolocker includes substantial media engagement, it is likely that the defendants will learn that the Department of Justice and FBI are involved in the disruption of their infrastructure. There is therefore good cause to believe that the defendants will seek additional information by visiting the public Internet sites of the Department of Justice and FBI and will thereby be notified of this action.

The service plan outlined above is very similar to what was proposed and ultimately approved by the court in Coreflood. In fact, the methods of service proposed above are even more likely to provide notice to the defendants in this suit as compared to the Coreflood

defendants because – unlike in Coreflood – the Government knows the true name of the lead defendant and will serve him at his home address. Moreover, the Government is not aware of any international agreement that prohibits the methods of service proposed above. Accordingly, pursuant to Rule 4(f)(3), the Court should approve the Government's plan for service of process.

B. The Court May Authorize the United States to Implement the Technical Disruption Described Above to Stop the Ongoing Fraud and Unlawful Interception of Communications Perpetrated by the GOZ Botnet and Cryptolocker

As described in more detail above, the TRO sought by the Government would: (1) direct four U.S. Internet Domain Registries to block access to the domain names used to control GOZ and to redirect connection requests to the substitute servers established pursuant to this Court's Order; (2) direct four U.S Internet Domain Registries to block access to the domain names used to control Cryptolocker; and (3) direct the ISPs specified in Appendix D to block their customers from connecting to a list of Russia-based Internet domain names that are used exclusively to control computers infected with GOZ and Cryptolocker. By ordering this relief, the Court will halt the defendants' use of GOZ and Cryptolocker to defraud and wiretap U.S. citizens and businesses, and will preserve the status quo while private-sector partners identify and notify victims and assist in removing the defendants' malicious software from their computers.

District Courts generally have broad discretion in deciding whether to grant injunctive relief. *See General Instrument Corp. of Delaware v. Nu-Tek Elecs. & Mfg., Inc.*, 197 F.3d 83, 90 (3d Cir. 1999). As courts of equity, District Courts "'may, and frequently do, go much farther both to give and withhold relief in furtherance of the public interest than they are accustomed to go when only private interests are involved.' . . . This is especially the case where the public interest in question has been formalized in a statute." *Instant Air Freight Co. v. C.F. Air Freight,*

Inc., 882 F.2d 797, 803 (3d Cir. 1989) (quoting *Virginian Ry. Co. v. System Fed'n No. 40*, 300 U.S. 515, 552 (1937)). In particular, the Third Circuit has noted that injunctive relief is "in the broadest sense for the discretion of the trial court which is best qualified to form a judgment as to the likelihood of a repetition of the offense." *U.S. v. Article of Drug Designated B-Complex Cholinos Capsules*, 362 F.2d 923, 928 (3d Cir. 1966).

Sections 1345 and 2521 of Title 18 enhance the Court's traditional powers at equity by allowing the Court to promptly enjoin ongoing fraudulent or unauthorized interception upon a suit by the Government. These statutes confer broad authorization for courts to enter restraining orders "at any time," or to "take such other action, as is warranted to prevent a continuing and substantial injury." 18 U.S.C. §§ 1354(b), 2521. In particular, Section 1345

> authorizes broad injunctive relief . . . for any violation of chapter 63 [and is] a powerful weapon in the government's anti-fraud arsenal. In addition to authorizing injunctive relief . . . the statute empowers courts to enter restraining orders, prohibitions, and "take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of person for whose protection the action is brought." . . . As a result, civil suits under § 1345 are often used to preserve the status quo during a lengthy parallel criminal probe.

United States v. Payment Processing Ctr., 435 F. Supp.2d 462, 464 (E.D. Pa. 2006); *see also id.* at 466 (citing *United States v. Cen-Card Agency/C.C.A.C.*, No. 88-5764, 1989 WL 30653 (3d Cir. March 23, 1989) (discussing past use of Section 1345 to stop fraud)). Indeed, Congress enacted Section 1345 specifically "to allow the Attorney General to put a speedy end to a fraud scheme by seeking an injunction in federal District Court whenever he determines he has received sufficient evidence of a violation of Chapter 63 to initiate such an action," and intended the District Court "to grant such action as is warranted to prevent a continuing and substantial injury to the class of persons designed to be protected by the criminal statute." S. Rep. No. 98-225, at

402 (1984). The use of similar statutory language in Section 2521, enacted after Section 1345, suggests a similar Congressional intent to permit the Attorney General to "put a speedy end" to ongoing unlawful interceptions. *See also* S. Rep. No. 99-541, at 34 (1986). The Government seeks the relief set forth herein for precisely those purposes.

Civil injunctive relief, such as that sought in this application, has been used in several Districts to accomplish large-scale disruptions of widespread computer hacking. In some cases, the United States Government has been the plaintiff, and in others, a private party has sought the injunctions. In all cases, injunctions have enabled the plaintiffs to halt hackers' schemes without infringing upon the privacy or property interests of victims or other parties.

For example, in Coreflood, the United States District Court for the District of Connecticut, pursuant to 18 U.S.C. §§ 1345 and 2521, enjoined a series of John Doe defendants from running the Coreflood botnet software.[8] The court based its ruling on the Government's showing that the John Doe defendants were using Coreflood to commit wire and bank fraud and to engage in unauthorized electronic surveillance, that the defendants' conduct was causing a continuing and substantial injury, and that the requested restraining order would prevent or ameliorate that injury. The Coreflood order authorized the FBI to establish a substitute server to replace the botnet command and control server formerly run by the defendants and compelled the

[8] 18 U.S.C. § 1345, combined with the court's inherent equitable authority, was also the basis upon which the U.S. District Court for the Eastern District of Missouri entered a temporary restraining order enjoining individuals from transferring domain names and ordering registrars and registries not to change registration for specified domains, and subsequently entered a permanent injunction with the additional requirement that the registration of defendants' domain names be transferred to non-U.S. registrars. *United States v. Betonsports PLC*. No. 4:06CV01064, 2006 WL 3257797, at *8-9 (E.D. Mo. Nov. 9, 2006); Temporary Restraining Order, *United States v. Betonsports PLC*, No. 4:06CV01064 (E.D. Mo. July 17, 2006).

Domain Registries and Registrars responsible for the domain names used by the Coreflood malware to redirect to the substitute server all traffic intended for the Coreflood domains.

Similarly, in Microsoft's recent action against the ZeroAccess botnet, the Western District of Texas entered an injunction granting very similar relief to the relief sought here. Specifically, the Court ordered Domain Registries to redirect traffic from ZeroAccess domains to a substitute command and control server, and ordered 45 U.S. ISPs to block their customers from connecting to a series of malicious IP addresses specified by Microsoft. *See Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, *ZeroAccess*, *supra*. Microsoft has obtained similar injunctions in a number of courts throughout the country. *See, e.g.*, *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, *Microsoft Corp. v. Patti et al.*, 1:11 CV 01017 (Sep. 22, 2011); Second Amended *Ex Parte* Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction, *Microsoft Corp. v. John Does 1-11 Controlling a Computer Botnet Thereby Injuring Microsoft and its Customers*, 2:11 CV 00222 (Mar. 9, 2011); *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction, *Microsoft Corp. v. John Does 1-27, Controlling a Computer Botnet Thereby Injuring Microsoft and its Customers*, No. 1:10 CV 156 (E.D.Va. Feb. 22, 2010).

1. Statutory Framework

Section 1345 of Title 18 authorizes the Attorney General to commence a civil action for injunctive relief whenever "a person is violating or about to violate this chapter." 18 U.S.C. § 1345(a)(1)(A). The referenced chapter of Title 18 includes Sections 1343 (Fraud by wire, radio, or television) and 1344 (Bank fraud), statutes the defendants are fragrantly violating through the

use of GOZ and Cryptolocker. Section 1345 further provides that a "permanent or temporary injunction or restraining order shall be granted," and that the "court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought." 18 U.S.C. § 1345(a)(3), (b).

Section 2521 of Title 18 similarly authorizes injunctions against illegal interception of communications in violation of 18 U.S.C. § 2511:

> Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought.

Because GOZ harvests user credentials by illegally intercepting the communications between infected computers and Internet websites, Section 2521 also empowers the Government to seek the injunctive relief proposed in this action.

2. The United States May Obtain an Injunction Under 18 U.S.C. § 1345 and 18 U.S.C. § 2521 Without Demonstrating the Traditional Prerequisites for Injunctive Relief

Where, as here, the United States seeks an injunction pursuant to federal statutes enacted to protect the public interest that provide for injunctive relief, the Court is authorized to issue the injunction if the statutory conditions are satisfied. *See United States v. Nutrition Serv., Inc.*, 227 F. Supp. 375, 388–89 (W.D. Pa. 1964), *aff'd* 347 F.2d 233 (3d Cir. 1965) ("There is sufficient

showing [for an injunction], where as here, the Government presents evidence of violations of the provisions of a statute enacted for the protection of the public. . . . Nor is it necessary to demonstrate the precise way in which violations of the law might result in injury to the public interest. It is sufficient to show only that the threatened act is within the declared prohibition of Congress."); *United States v. Sene X Eleemosynary Corp.*, 479 F. Supp. 970, 980 (S.D. Fla. 1979) ("Where an injunction is authorized by statute, it is proper to issue such an order to restrain violations of the law if the statutory conditions are satisfied."). The United States thus is not required to demonstrate the traditional prerequisites for a TRO or preliminary injunction, such as irreparable harm or sufficient public interest. *See United States v. Livdahl*, 356 F.Supp.2d 1289, 1290-91 (S.D. Fla. 2005); *Sene X Eleemosynary Corp.*, 479 F. Supp. at 980–81 ("It is sufficient to show only that the threatened act is within the declared prohibition of Congress."); *Nutrition Serv., Inc.*, 227 F. Supp. at 388–89; *see also Government of the Virgin Islands v. Virgin Islands Paving*, 714 F.2d 283, 286 (3d Cir. 1983) (superseded on other grounds by statute, *see Edwards v. Hovensa*, 497 F.3d 355, 359 (3d Cir. 2007); *United States Postal Service v. Beamish*, 466 F.2d 804, 806 (3d Cir. 1972); *CSX Transp., Inc. v. Tennessee Bd. Of Equalization*, 964 F.2d 548, 551 (6th Cir. 1992).[9]

3. The United States Is Authorized to Obtain Injunctive Relief Under 18 U.S.C. § 1345 and 18 U.S.C. § 2521 Because Defendants Are Committing Bank and Wire Fraud and Are Illegally Intercepting Electronic Communications

As detailed in Special Agent Peterson's Declaration, and summarized above, the defendants are engaged in wire fraud, bank fraud, and illegal interception of communications on

[9] In passing a statute authorizing injunctive relief, Congress implicitly finds that a violation of the law will irreparably harm the public interest. *See Nutrition Serv., Inc.*, 227 F. Supp. at 388–89.

a massive scale through the use of GOZ and Cryptolocker. The United States is therefore fully authorized to obtain an injunction under both 18 U.S.C. § 1345 and 18 U.S.C. § 2521.

When, as here, a federal statute empowers the Government to obtain an injunction prohibiting further violations of criminal law, courts are split on whether the United States must show that there is probable cause to believe the defendant is violating or is about to violate any of the enumerated offenses, or must demonstrate such violations by a preponderance of the evidence. *Compare United States v. Luis,* 966 F.Supp.2d 1321, 1326 (S.D. Fla. 2013) (probable cause; collecting cases) and *United States v. Payment Processing Ctr., LLC*, 461 F. Supp. 2d 319, 323 & n.4 (E.D. Pa. 2006) (probable cause) with *United States v. Brown*, 988 F.2d 658, 663 (6th Cir. 1993) (preponderance) and *United States v. Williams*, 476 F.Supp.2d 1368, 1374 (M.D.Fla.2007) (preponderance). This issue has not been decided by the Third Circuit. In any event, given the overwhelming evidence of criminal conduct presented in Special Agent Peterson's Declaration, the United States easily meets its burden of proof under 18 U.S.C. § 1345 and 18 U.S.C. § 2521 regardless of which evidentiary standard is applied.

a. The Defendants Are Committing Wire Fraud (18 U.S.C. § 1343)

The elements of wire fraud are: (1) a scheme to defraud; (2) use of the wires for the purpose of executing the scheme; and (3) fraudulent intent. *Devon IT, Inc. v. IBM Corp.*, 805 F. Supp. 2d 110, 123 (E.D. Pa. 2011) (citing *United States v. Pharis*, 298 F.3d 228, 234 (3d Cir. 2002)); *see National Sec. Systems, Inc. v. Iola,* 700 F.3d 65, 105 (3d Cir. 2012). The defendants' conduct readily establishes all of these elements. The defendants operate the GOZ botnet for the sole purpose of stealing online credentials and using those credentials to gain unauthorized access to financial accounts. Once these credentials are harvested, the defendants use the

credentials to pose as their victims and log into their bank accounts over the Internet. The defendants then initiate fraudulent wire and ACH transfers in order to empty the bank accounts they have compromised.

The defendants further violate 18 U.S.C. § 1343 through the use of Cryptolocker. The defendants encrypt victims' computers and then, to create a sense of urgency, make a series of false statements, including that: (1) the private key needed to unlock the computer will be destroyed in 72 hours, and (2) that any attempt to remove Cryptolocker from the computer will result in the destruction of the private key. The defendants then demand that victims pay the Cryptolocker ransom by transferring anonymous payments to them via the Internet.

Moreover, as noted above, the defendants keep a close hold on the GOZ malware, and GOZ is one of the primary means by which Cryptolocker is installed on victims' computers. Accordingly, Cryptolocker is part of the overall GOZ scheme to defraud.

b. The Defendants are Committing Bank Fraud (18 U.S.C. § 1344)

The elements of bank fraud are: (1) a scheme to defraud a federally insured financial institution; (2) the defendant participated in the scheme by means of false pretenses, representations, or promises that were material; and (3) the defendant acted knowingly. *United States v. Goldblatt*, 813 F.2d 619, 624 (3d Cir. 1987); *McCoy-McMahon v. Godlove*, No. 08-CV-05989, 2011 WL 4820185, at *12 (E.D. Pa. Sept. 30, 2011). The defendants' criminal conduct satisfies each of these elements. First, the defendants use the GOZ botnet to conduct fraudulent financial transfers from federally insured banks, as exemplified by the specific GOZ attacks described above. Second, the defendants make materially false representations to both the bank and the victim to perpetrate their fraudulent scheme, both in tricking victims into installing

malware and in impersonating victims to conduct the fraudulent transfers. Finally, the defendants act knowingly and intentionally, as demonstrated by their operation of highly sophisticated botnet software to accomplish their fraud.

c. The Defendants are Unlawfully Intercepting Electronic Communications (18 U.S.C. § 2511)

It is a violation of the Wiretap Act to:

> intentionally intercept, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> [or to]
>
> intentionally use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.

18 U.S.C. § 2511(1)(a), (d); (4)(a). As described in the Declaration of Special Agent Peterson, GOZ is a highly advanced communications interception platform that exists to harvest online credentials by intercepting communications between infected computers and financial websites. Through the use of GOZ's "man-in-the-middle" attack, these credentials are harvested in real time as they are transmitted from the victim's computer. This conduct clearly violates 18 U.S.C. § 2511(1)(a) and (d).

4. The Proposed Disruption Is Neither A Fourth Amendment Search nor Seizure and Does Not Require the Issuance of a Warrant

The Government's planned disruption of GOZ and Cryptolocker is neither a search nor a seizure under the Fourth Amendment. Accordingly, this court may authorize the proposed disruption without the issuance of a warrant.

In order to constitute a Fourth Amendment search, the government's actions must either invade an individual's reasonable expectation of privacy, or constitute a physical trespass upon property for the purpose of obtaining information. *See United States v. Jones*, 132 S.Ct. 945, 951 (2012); *Ware v. Donahue*, 950 F.Supp. 2d 738, 744 (D. Del. 2013) (differentiating between a Fourth Amendment search and seizure, and explaining that a "search occurs when an individual's reasonable expectation of privacy is infringed").

Nothing in the planned operation constitutes a Fourth Amendment search. If approved, the only information gathered by the Government during the operation will be dialing, addressing, routing, and signaling information that will be recorded by the Government when infected computers check in at the substitute servers. There is no reasonable expectation of privacy in this information, which will be collected pursuant to a Pen/Trap Order. *See, e.g. United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010) ("no reasonable expectation of privacy exists in an IP address"); *United States v. Forrester*, 512 F.3d 500, 510-12 (9th Cir. 2008) (holding that Government surveillance techniques that reveal non-content information, including the to/from addresses of e-mail messages, the IP addresses of websites visited, and the total amount of data transmitted to or from an account, do not constitute a Fourth Amendment search).

The planned disruption also does not constitute a seizure. A seizure occurs when the Government meaningfully interferes with an individual's possessory interests in property. *Soldal*

v. Cook Cnty., 506 U.S. 56, 61 (1992). Here, the proposed operation would cause no meaningful interference with the victims' possessory interests in their computers, or any other possessory interest. If the Court grants the TRO, computers infected with GOZ will stop communicating with computers controlled by the defendants, and will begin exchanging routing information with the substitute servers established by this Court's Order. This transition will be completely transparent to the user, whose computer will perform all authorized functions exactly as it has before. This imperceptible change does not constitute a meaningful interference with the user's possessory interests.

5. *Ex Parte* Relief is Appropriate

The purpose of a temporary restraining order is to preserve the status quo until the Court has an opportunity to pass on the merits of a preliminary injunction. *See Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers Local No. 70*, 415 U.S. 423, 439 (1974); *Garcia v. Yonkers Sch. Dist.*, 561 F.3d 97, 107 (2d Cir. 2009). A District Court may grant a temporary restraining order without notice to defendants if "specific facts in an affidavit or verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition," and the movant "certifies in writing any efforts made to give notice and the reasons why it should not be required." Fed. R. Civ. P. 65(b)(1).

The relief sought herein would preserve the status quo by preventing the defendants from defrauding additional individuals and financial institutions. In addition, the TRO would prevent further extortion of Cryptolocker victims. As discussed herein, the ongoing and aggressive fraud the Government seeks to stop will continue to cause irreparable injury and loss until it is halted.

Prior notice to the defendants would render futile the Government's efforts to stop the defendants' ongoing criminal acts. If notified in advance of the Government's intended actions, Defendants could change their malware, shift their domains, change IP addresses, or take other technical steps – which would not require substantial time or effort – to avoid the planned disruption of their operations. *See* Peterson Decl. ¶43. The requested *ex parte* relief is necessary to prevent such evasion of the Government's remedial measures. *See* 18 U.S.C. §§ 1345(b) (the "court shall . . . take such other action as is warrant to prevent a continuing and substantial injury"), 2521 (same); Fed. R. Civ. P. 65(b)(1).

6. A Sealing Order Should be Entered in this Case

As set forth in the Government's request for leave to file under seal, the Government respectfully requests leave to file this memorandum, the Complaint, the proposed TRO and all associated documents under seal. The Government further requests leave to file redacted versions of these documents at the time they are unsealed in order to protect an ongoing law enforcement investigation in this case and similar law enforcement investigations in the future.

Conclusion

For the foregoing reasons, the Government respectfully requests the Court grant the Temporary Restraining Order requested by the Government.

Respectfully submitted,

DAVID J. HICKTON

United States Attorney

By: /s/ Michael A. Comber
MICHAEL COMBER
Assistant U.S. Attorney
Western District of PA
U.S. Post Office & Courthouse
700 Grant Street, Suite 4000
Pittsburgh, PA 15219
(412) 894-7485 Phone
(412) 644-6995 Fax
PA ID No. 81951
Michael.Comber@usdoj.gov

LESLIE R. CALDWELL

Assistant Attorney General

By: /s/ Ethan Arenson
ETHAN ARENSON
DAVID AARON
Trial Attorneys
Computer Crime and Intellectual Property Section
1301 New York Avenue, NW
Washington, DC 20530
(202) 514-1026 Phone
(202) 514-6113 Fax
DC Bar No. 473296 (Arenson)
NY Bar No. 3949955 (Aaron)
Ethan.Arenson@usdoj.gov
David.Aaron@usdoj.gov