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

UNITED STATES OF AMERICA)
)
Plaintiff,) Civil Action No. 15-1315
)
v.) **FILED *EX PARTE***
) **AND UNDER SEAL**
ANDREY GHINKUL)
a/k/a Andrei Ghincul)
a/k/a "smilex,")
)
MAKSIM VIKTOROVICH YAKUBETS)
a/k/a "aqua,")
)
IGOR TURASHEV)
a/k/a "nintutu,")
)
MAKSIM MAZILOV)
a/k/a "caramba," and,)
)
ANDREY SHKOLOVOY)
a/k/a "caramba,")
)
Defendants.)

COMPLAINT

Plaintiff, the United States of America, by and through its undersigned counsel, alleges the following:

1. This is a civil action brought under Title 18, United States Code, Sections 1345 and 2521, and Federal Rule of Civil Procedure 65, to enjoin the defendants from continuing to engage in wire fraud, bank fraud, and unauthorized interception of electronic communications in violation of Title 18, United States Code, Sections 1343, 1344, and 2511, by means of malicious computer software ("malware") known as "Bugat" and its subsequent versions or adaptations known as "Cridex" and "Dridex" ("Bugat/Dridex").

2. Bugat/Dridex is malware that primarily steals user credentials that victims enter at bank websites in order to manage their funds. Once a computer is infected with Bugat/Dridex, it becomes a compromised computer, or "bot," which joins a vast network of infected computers ("botnet") that is controlled and operated by the defendants.

3. Bugat is the original multifunctional malware package that has been in use since late 2009. Bugat, like most modern malware, is specifically designed to defeat antivirus detection software and other protective measures employed by businesses and the public at large. As the individuals behind Bugat improved the malware and included additional functionality, the name of the malware changed first to Cridex, and then to Dridex. Despite the evolution of functionality, Cridex and Dridex are based upon the original Bugat source code.

4. The primary goal of the Bugat/Dridex malware is to infect computers, steal banking credentials, and then obtain money from victims' bank accounts. Bugat/Dridex malware is generally distributed through a process known as "phishing," where spam emails are distributed to victims. The emails appear legitimate and are carefully crafted to entice the victim to click on a hyperlink or to open an attached file. In the event a user clicks on a hyperlink, the user is then redirected to an exploit kit, which is a web based software program that scans the victim's computer and operating systems for vulnerabilities and, upon discovering one, forces the download of a malicious file upon the victim. In the event the victim opens an attached file, he or she is directly infected either by the Bugat/Dridex malware, or by a loader program, which then downloads the Bugat/Dridex malware.

5. The Bugat/Dridex malware accomplishes the theft of confidential financial information through the use of keystroke logging and web injects. Keystroke logging is the action of recording, or "logging," the keys struck on a keyboard. This action is usually done

surreptitiously by a computer program (i.e., keylogger) which captures the keys typed on a computer without the typist's knowledge. Malware that uses keystroke logging often will provide the captured keystrokes to those who caused the malware to be installed or to a place designated by them. Through keystroke logging, computer intruders are able to obtain online banking credentials as soon as the user of the infected computer logs into their account. After obtaining this information, these intruders can access the victim's online bank account and execute unauthorized electronic funds transfers ("EFT"), such as Automated Clearing House ("ACH") payments or wire transfers, to accounts that they control.

6. Web injects introduce, "or inject," malicious computer code into a victim's web browser while the victim browses the Internet and "hijacks" the victim's Internet session. Different injects are used for different purposes. Some web injects are used to display false online banking pages into the victim's web browser to trick the victim into entering online banking information, which is then captured by the individual employing the web inject.

7. Once a victim's computer is infected with Bugat/Dridex, it becomes a "bot" in the vast Bugat/Dridex botnet that is controlled by the defendants and other criminal actors. Approximately ten distinct Bugat/Dridex sub-botnets have been observed operating since 2014 and at least one of these sub-botnets has primarily targeted financial institutions located in the United States.[1] The sub-botnets range in number of infected machines, but security researchers identified that one sub-botnet (known as EB120) contained over 100,000 active bots during May, 2015. The infected machines are located all over the world, including a significant number in the United States.

[1] Not all of these botnets are currently operating. As of September 15, 2015, a handful of distinct Bugat/Dridex botnets were still operating worldwide.

8. Bugat/Dridex initially utilized a botnet infrastructure whereby the infected victim machines, or "bots," communicated with, and received messages directly from, a multi-layered network of command and control ("C&C") servers. A C&C server is a centralized computer that issues commands to a botnet and receives reports back directly from the compromised computers. The outermost group of servers in the Bugat/Dridex C&C communication architecture (Layer 3) is made up hundreds of servers which have been compromised by the perpetrators. The Layer 3 servers, which are also referred to as "admin nodes," forward traffic upstream to a smaller group (Layer 2) of approximately 15 servers that are directly owned by the Bugat/Dridex group. This intermediate layer forwards traffic to the innermost section (Layer 1) of the infrastructure, which is comprised of about two dozen servers and operates as the back-end infrastructure that is controlled directly by the perpetrators.[2] The Bugat/Dridex C&C servers were operated by the defendants and were used to control and push out commands to the botnet.

9. Beginning in approximately November 2014, the defendants added peer-to-peer[3] (P2P) functionality to make the botnet infrastructure more resilient to countermeasures by law enforcement. In the P2P botnet, each infected bot (a "peer") maintains a list of other infected peers. The list maintained by the peer consists of routing information that includes IP addresses and port numbers of other peers on the network. To ensure that this list remains active, the peers regularly request new updated bot routing information from "super-peers" on the network. The super-peers get the most updated information directly from the C&C servers that are controlled

[2] There appears to be virtual private network (VPN) communication between the Layer 2 and Layer 1 servers, probably via a common VPN tunnel to the level 2 devices, creating an internal network for the perpetrators that is accessible via VPN.

[3] "Peer-to-peer" refers to a means of networking computers such that they communicate directly with each other, rather than through a centralized management point.

by the perpetrators. Upon receiving the new routing information from the super-peers, the bots update their lists of peers accordingly. In this way, the super-peers serve as relay points for commands coming from the Bugat/Dridex operators and for encrypted data stolen from victim computers to be sent to the perpetrators. Bugat/Dridex operators can promote any Bugat/Dridex-infected computer to super-peer status.

10. On or around September 4, 2015, the National Crime Agency in the United Kingdom undertook action to collectively disable the C&C servers that formed the backbone of the Bugat/Dridex botnets. Because the C&C servers have been disabled, the super-peers and peers have no centralized mechanism to take direction from and are awaiting new commands and peer lists. Thus, Bugat/Dridex has been temporarily disabled but could be reestablished at any time by the defendants and their criminal associates, who will simply register new C&C servers to issue commands to the botnet.

11. It is believed that Bugat/Dridex has infected hundreds of thousands of computers worldwide. Although it is difficult to precisely quantify the extent of the financial loss associated with Bugat/Dridex, largely because of the technical hurdles of directly attributing a given financial fraud directly with a specific malware strain, through interviews with victims, information provided by foreign law enforcement partners, technical monitoring of Bugat/Dridex botnet activities, and examining the records kept by Bugat/Dridex operators, it is likely that total losses associated with Bugat/Dridex exceed $10 million in the United States and significantly more than that worldwide.

Parties

12. Plaintiff is the United States of America.

13. Defendant Andrey Ghinkul is citizen of Moldova currently in custody of the

authorities in Cyprus awaiting extradition to the United States to answer criminal charges filed in the United States District Court for the Western District of Pennsylvania in case number: CR 15-198 (under seal). Ghinkul is a leader of the criminal enterprise responsible for Bugat/Dridex.

14. Defendants Yakubets, Turashev, Mazilov, and Shkolovoy are individuals, believed to be located in Russia, who participate in the deployment of the Bugat/Dridex malware and the criminal proceeds generated therefrom.

Jurisdiction and Venue

15. Subject matter jurisdiction lies pursuant to Title 18, United States Code, Sections 1345(a)(1) and 2521 and Title 28, United States Code, Sections 1331 and 1345.

16. The defendants are subject to the personal jurisdiction of this Court, having infected computers, used infected computers in furtherance of their scheme to defraud, initiated fraudulent money transfers, and engaged in unauthorized wiretapping, all within the Western District of Pennsylvania.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2).

The Bugat/Dridex Scheme to Defraud and Unauthorized Interception

18. A botnet is a collection of compromised computers that are controlled, without the knowledge of the victims, by an unauthorized third party. A botnet can be used for many criminal purposes, including sending spam, stealing data, and committing financial fraud.

19. The Bugat/Dridex botnet has been used for the commission of fraudulent financial activity. The principal purpose of Bugat/Dridex is to capture banking credentials from infected computers. One means by which Bugat/Dridex accomplishes this is through "man-in-the-

middle" attacks, in which Bugat/Dridex intercepts sensitive information victims transmit from their computers.

20. To increase the effectiveness of such attacks, the defendants use Bugat/Dridex to inject additional code into victims' web browsers that changes the appearance of the websites victims are viewing. For example, if a Bugat/Dridex-infected user were to visit a banking website that typically requests only a username and password, the defendants could seamlessly inject additional form fields into the website displayed in the user's web browser that also request the user's social security number, credit card numbers, and other sensitive information. Because these additional fields appear to be part of the legitimate website users elected to visit, users are often defrauded into supplying the requested information, which is promptly intercepted by Bugat/Dridex and transmitted to the defendants.

21. The defendants also use a feature of the Bugat/Dridex malware to log all of the keystrokes on an infected computer to capture an individual's banking credentials as they are typed by that victim.

22. The defendants use the intercepted credentials for fraudulent purposes, such as initiating or re-directing wire transfers from victims' accounts to accounts controlled by the Bugat/Dridex organization overseas.

23. Victims of the Bugat/Dridex scheme to defraud and unauthorized interception include, among others:

a. A petroleum company in the Western District of Pennsylvania, which lost more than $3,500,000 after unauthorized wire transfers were initiated from its bank account using credentials stolen by the defendants through the use of Bugat/Dridex;

b. A school district in the Western District of Pennsylvania learned from their bank that a wire transfer of $999,000 was about to be executed. This

> unauthorized wire was canceled. Subsequent FBI investigation revealed that a computer at the school district was infected with Bugat/Dridex malware at a time before the attempted transfer of funds. The analysis also revealed that the infection was the result of a spam email received on November 8, 2011.

24. Since Bugat/Dridex first emerged in late 2009, total losses attributable to Bugat/Dridex are estimated to be in excess of 25 million dollars worldwide.

COUNT I
(Injunctive Relief under 18 U.S.C. § 1345)

25. The United States of America alleges and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

26. The Defendants are engaging in wire fraud, in violation of Title 18, United States Code, Section 1343, in that the defendants, having devised a scheme or artifice to defraud and for obtaining money by means of false or fraudulent pretenses, are transmitting and causing to be transmitted, by means of wire communication in interstate and foreign commerce, writings, signs, and signals for the purpose of executing such scheme or artifice.

27. Pursuant to Title 18, United States Code, Section 1345(a) and (b), the United States of America requests the issuance of a temporary restraining order, preliminary injunction, and permanent injunction against the defendants and their agents in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers in the Bugat/Dridex botnets.

COUNT II
(Injunctive Relief under 18 U.S.C. § 1345)

28. The United States of America alleges and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

29. The defendants are engaging in bank fraud, in violation of Title 18, United States Code, Section 1344, in that the defendants are knowingly executing a scheme or artifice to defraud financial institutions insured by the Federal Deposit Insurance Corporation and to obtain moneys under the custody and control of these institutions by means of false and fraudulent pretenses and representations.

30. Pursuant to Title 18, United States Code, Section 1345(a) and (b), the United States of America requests the issuance of a temporary restraining order, preliminary injunction, and permanent injunction against the Defendants and their agents in order to prevent a continuing and substantial injury to the owners and legitimate users of the infected computers in the Bugat/Dridex botnets.

COUNT III

(Injunctive Relief under 18 U.S.C. § 2521)

31. The United States of America alleges and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

32. The defendants are engaging in the unauthorized interception of electronic communications, in violation of Title 18, United States Code, Section 2511, in that the defendants are intentionally intercepting electronic communications, and are intentionally using and endeavoring to use the contents of electronic communications knowing that the information is obtained through the unauthorized interception of electronic communications.

33. Pursuant to Title 18, United States Code, Section 2521, the United States of America requests the issuance of a temporary restraining order, preliminary injunction, and permanent injunction against the defendants and their agents in order to prevent a continuing and

substantial injury to the owners and legitimate users of the infected computers in the Bugat/Dridex botnets.

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays that the Court:

A. Enter judgment in favor of the Government and against the defendants;

B. Pursuant to Title 18, United States Code, Sections 1345(b) and 2521, enter a preliminary injunction and and permanent injunction against the defendants and their agents, servants, employees, and all persons and entities in active concert or participation with them from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity from engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;

C. Pursuant to Title 18, United States Code, Sections 1345(b) and 2521, enter a preliminary injunction and permanent injunction authorizing the Government to continue the malware disruption plan specified in the Government's Memorandum of Law in Support of Motion for Temporary Restraining Order, Order to Show Cause, and Other Ancillary Relief for a period of six months, and requiring the entities specified in the Temporary Restraining Order to continue take the actions specified in the Temporary Restraining Order for a period of sixty days.

D. Order such other relief that the Court deems just and proper.

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/ Richard D. Green
RICHARD D. GREEN
Senior Trial Attorney
Computer Crime and Intellectual
Property Section
1301 New York Avenue NW
Washington, DC 20530
(202) 514-1026 Phone
(202) 514-6113 Fax
PA Bar No. 43758
Richard.Green@usdoj.gov