BRYAN D. SCHRODER
United States Attorney

ADAM ALEXANDER
Assistant U.S. Attorney
Federal Building & U.S. Courthouse
222 West 7th Ave., #9, Rm. 253
Anchorage, AK 99513-7567
Phone: 907-271-5071
Email: Adam.Alexander@usdoj.gov

CATHERINE ALDEN PELKER
Trial Attorney
Computer Crime & Intellectual Property Section
1301 New York Avenue, NW, Suite 600
Washington, DC 20005
Telephone: (202) 514-1026
Facsimile: (202) 514-6113
Email: Catherine.Pelker@usdoj.gov

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA,	)	No. 3:19-cr-00109-RRB-DMS
	)	
Plaintiff,	)	COUNTS 1-3:
	)	WIRE FRAUD
vs.	)	Vio. of 18 U.S.C. § 1343
	)	
PAVEL TSURKAN, a/k/a	)	COUNTS 4-5:
"RUSSIAN8," d/b/a	)	COMPUTER INTRUSIONS
"RUSSIAN2015.RU"	)	Vio. of 18 U.S.C. § 1030(a)(5)(A)
	)	
Defendant.	)	CRIMINAL FORFEITURE
	)	ALLEGATION:
	)	18 U.S.C. §§ 981, 982, 1030;
	)	21 U.S.C. § 853; and 28 U.S.C. § 2461.

INDICTMENT

The Grand Jury Charges that:

BACKGROUND

1. At all times relevant to this indictment, PAVEL TSURKAN was an Estonian citizen residing in Estonia.

2. A proxy was an intermediary computer to which Internet users connected in order to conceal their location and identity online. In a proxy arrangement, Client A attempting to access Website C would first route the communications through Client B, the proxy. Website C would see only the traffic coming from Client B and would be unaware of the relationship between Client A and Client B. Proxies were commonly used by cyber criminals to avoid detection by a website's anti-fraud measures and apprehension by authorities.

3. A botnet was a collection of computers controlled as a group, often through infection with malicious software and without the knowledge or permission of the computers' owners.

4. Internet of Things (IoT) devices were everyday physical devices that had the capability of communicating via a network, such as the Internet. These devices commonly ran variations of the Linux operating system and were designed around a core set of features. Some examples of IoT devices included smart thermostats, DVRs, and surveillance systems.

5. A router was a device that connected different networks and made decisions about where to direct data that passed through it. Home internet routers, for example,

could connect multiple personal devices within a residence to the Internet, and could ensure that Internet traffic was routed to the correct device.

6. "Spam" referred to unsolicited e-mail communications sent in bulk with commercial, fraudulent, or malicious intent. Spam was commonly used by cyber criminals to distribute malicious software ("malware").

7. The Exploits Block List (XBL) was a database maintained by a private organization listing IP addresses of computers infected with malware hijacked computers infected by illegal third-party exploits. Many third-party mail servers used the XBL in their e-mail filtering, so that e-mail sent from IP addresses contained on the XBL would either be filtered out as "Spam" or "Junk" or would "bounce," returning to sender.

COUNTS 1-3

8. From on or about August 2015 to on or about August 2016, in the District of Alaska and elsewhere, defendant PAVEL TSURKAN devised and intended to devise a scheme to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises.

The Scheme and Artifice

9. The object of the scheme was to infect victim computer devices and misappropriate them for use as proxies by TSURKAN and his criminal clientele. TSURKAN infected IoT devices, including internet routers located in the District of Alaska, and sold access to the infected devices to his customers, who routed their internet traffic through the devices. In doing so, TSURKAN and his customers co-opted the

victim routers and their Internet bandwidth without obtaining the victims' permission or compensating them for the use of their devices and Internet service.

Manner and Means

It was part of the scheme that:

10. TSURKAN remotely gained access to computer devices, including home Internet routers, in the District of Alaska an elsewhere. In total, TSURKAN compromised over 1,000 victim devices worldwide, including at least 60 victims in the District of Alaska who were customers of ALASKA VICTIM ISP.

11. TSURKAN utilized the victim devices to build and operate an Internet of Things (IoT)-based botnet (the "Russian2015 botnet"), which utilized the domain Russian2015.ru.

12. TSURKAN modified the operation of each compromised Internet router so that it could be used as a proxy, allowing TSURKAN to transmit third-party Internet traffic through the home Internet routers without their owners' knowledge or consent.

13. TSURKAN sold access to the victim devices to cyber criminals located around the globe, who in turn routed their Internet traffic through the victims' routers.

14. At times, TSURKAN allowed dozens of his criminal clients to route their traffic through a single victim's home internet router. For example, in the case of Victim 3, a hospital located in Alaska, TSURKAN configured the victim's router to allow it to channel the traffic for over 70 different computers, designated by TSURKAN.

15. TSURKAN used a command and control (C2) server located in the Netherlands. TSURKAN accessed this C2 through his home in Estonia and sent wires to victim devices located in the District of Alaska and elsewhere.

16. The malware that infected the victim devices caused them to "check in" with the C2 every three minutes, notifying the C2 that the victim was ready for instructions. The malware also caused the infected victim devices to resolve the Russian2015 domain every three minutes, in order to determine whether the Russian2015 botnet was operating from a different C2. Collectively, this resulted in each victim device sending hundreds of additional communications each day that were not authorized by the victims and co-opted the victims' bandwidth without compensation to the victims.

17. Cyber criminals utilized the victim devices as proxies for a variety of purposes, including sending spam e-mail messages. Indeed, the IP address for Victim 2, located in the District of Alaska, was added to the Exploits Block List (XBL), meaning that mail sent from Victim 2's IP address would be returned or otherwise flagged as spam or "junk" by mail systems utilizing the XBL for spam filtering.

18. The unlawful use of the victims' routers resulted in latency in the victims' own Internet connections as well as significant data overage charges. For example, one Alaskan-based victim reported that, while his router was co-opted into the Russian2015 botnet, he consumed 3-4 gigabytes (GB) of data each day, even after he disconnected all devices from his WiFi router. Another Alaskan victim, who reported a typical consumption of less than 0.5 GB of data each day, noted a surge up to 6 GB/day while infected with TSURKAN's malware. The victims and/or their Internet Service Providers

(ISPs), including ALASKA VICTIM ISP, were left to pay for the considerable data utilized by the cyber criminals who had routed their traffic through the victims' devices. Alaska-based victims incurred data overages in the range of hundreds to thousands of dollars per victim.

Execution

19. On or about each of the dates set forth below, in the District of Alaska and elsewhere, defendant PAVEL TSURKAN, for the purpose of executing the scheme described above, caused to be transmitted by means of wire communication in interstate commerce the signals and sounds described below for each count, each transmission constituting a separate count:

COUNT	DATE	DESCRIPTION
1	March 10, 2016	Wire transmitted from TSURKAN's C2 to a router utilized by Victim 1, a rural school district in the District of Alaska
2	April 1, 2016	An executable file transferred from TSURKAN's C2 to Victim 2's router, which configured the router to operate as a Russian2015 proxy
3	April 19, 2016	Wire transmitted from TSURKAN's C2 to a router utilized by Victim 3, a hospital in the District of Alaska

COUNT 4

20. The allegations set forth in paragraphs 1-19 of this Indictment are realleged and incorporated into this Count, as if fully set forth herein.

21. Between on or about February 10, 2016 and April 5, 2016, in the District of Alaska and elsewhere, the defendant, PAVEL TSURKAN, knowingly caused the transmission of a program, information, code, and command, and as a result of such

conduct, intentionally caused damage without authorization to a protected computer, to wit, a router utilized by Victim 2, an individual in the District of Alaska; and the offense caused loss from a related course of conduct – to wit, the infection of additional devices for use in the Russian2015 proxy botnet – affecting one or more other protected computers aggregating at least $5,000 in value, and the offense caused damage affecting ten or more protected computers during a one-year period, specifically from on or about August 2, 2015 through August 1, 2016.

All of which is in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4).

COUNT 5

22. The allegations set forth in paragraphs 1-19 of this Indictment are realleged and incorporated into this Count, as if fully set forth herein.

23. Between on or about February 2, 2016 and April 5, 2016, in the District of Alaska and elsewhere, the defendant, PAVEL TSURKAN, knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, to wit, a router utilized by Victim 4, an individual in the District of Alaska; and the offense caused loss from a related course of conduct – to wit, the infection of additional devices for use in the Russian2015 proxy botnet – affecting one or more other protected computers aggregating at least $5,000 in value, and the offense caused damage affecting ten or more protected computers during a one-year period, specifically from on or about August 2, 2015 through August 1, 2016.

All of which is in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4).

NOTICE OF FORFEITURE

18 U.S.C. §§ 981, 982, 1030; 21 U.S.C. § 853; and 28 U.S.C. § 2461.

1. The allegations contained in Counts 1-4 of this Indictment are realleged and incorporated by reference for the purpose of alleging forfeiture.

The Grand Jury hereby finds that:

2. There is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.

3. Pursuant to Federal Rule of Criminal Procedure 32.2(a), the United States of America gives notice to the defendant, PAVEL TSURKAN, that, in the event of the defendant's conviction of the offense charged in Count 1 of this Indictment, the United States intends to forfeit the defendant's property as further described in this NOTICE OF FORFEITURE.

4. Upon conviction of 18 U.S.C. § 1030, as set forth in Count 1 of this Indictment, the defendant shall forfeit to the United States of America any property, real or personal, which constitutes or is derived from proceeds traceable to the violations, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c).

SUBSTITUTE ASSETS

5. If any of the property described above, as a result of any act or omission of the defendant:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(c) has been placed beyond the jurisdiction of the court;

(d) has been substantially diminished in value; or

(e) has been comingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to and intends to seek forfeiture of substitute property pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. §§ 982(b)(1), 1030(i)(2), and 28 U.S.C. § 2461(c).

//

//

//

//

//

//

//

//

//

//

//

//

//

//

All pursuant to 18 U.S.C. §§ 981, 982, 1030; 21 U.S.C. § 853; and 28 U.S.C. § 2461.

A TRUE BILL.

s/ Grand Jury Foreperson
GRAND JURY FOREPERSON

s/ Adam Alexander
ADAM ALEXANDER
United States of America
Assistant U.S. Attorney

s/ Adam Alexander for
C. ALDEN PELKER
United States of America
Trial Attorney

s/ Bryan Schroder
BRYAN SCHRODER
United States of America
United States Attorney

DATE: October 15, 2019