UM

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA

v.

ZACHARY BUCHTA,
also known as "pein," "@fbiarelosers," "@xotehpoodle," and "lizard," and
BRADLEY JAN WILLEM VAN ROOY,
also known as "Uchiha," "@UchihaLS," "dragon," and "fox"

CASE NUMBER:
UNDER SEAL

16CR 622

MAGISTRATE JUDGE ROWLAND

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Beginning no later than in or around November 2015, and continuing at least until in or around September 2016, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendants violated:

Code Section	*Offense Description*
Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), and 1030(c)(4)(B)(i)	Conspiring to knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, which offense caused a loss aggregating at least $5,000 in value to one or more persons during a one-year period

This criminal complaint is based upon these facts:

X Continued on the attached sheet.

ERIC T. BRELSFORD
Special Agent, Federal Bureau of Investigation (FBI)

Sworn to before me and signed in my presence.

Date: September 23, 2016

Mary M Rowland
Judge's signature

City and state: Chicago, Illinois

MARY M. ROWLAND, U.S. Magistrate Judge
Printed name and Title

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I. Introduction and Agent Background

I, Eric T. Brelsford, being duly sworn, state as follows:

1. I am a Special Agent of the Federal Bureau of Investigation and am assigned to the Chicago Field Office. I have been employed as a Special Agent with the FBI since May 2003 and have specialized in cybercrime investigations for the duration of my employment. As a Special Agent, I am charged with investigating possible violations of federal criminal law, including violations of 18 U.S.C. §§ 1030 (computer crime), 1029 (access device fraud), 875(c) (interstate transmission of threats), and 2261A(2) (cyberstalking). I have received specialized training in the investigation of cybercrime. In particular, I hold a bachelor's degree in Computer Studies and have current cybersecurity-related certifications from Global Information Assurance Certification in the fields of incident handling, web application penetration testing, and computer forensics. I have attended multiple FBI and private sector training sessions and conferences on computer intrusion, network analysis, and electronic evidence recovery.

2. This affidavit is submitted in support of a criminal complaint alleging that Zachary Buchta, also known as "pein," "@fbiarelosers," "@xotehpoodle," and "lizard," and Bradley Jan Willem van Rooy, also known as "Uchiha," "@UchihaLS," "dragon," and "fox," have conspired with each other and others to knowingly cause the transmission of a program, information, code, or command, and as a result of such

conduct, intentionally caused damage without authorization, to a protected computer, which offense caused a loss aggregating at least $5,000 in value to one or more persons during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), and 1030(c)(4)(B)(i) (the "**Subject Offense**").

3. This affidavit is also submitted in support of seizure warrants for the following domain names: shenron.lizardsquad.org (**Subject Domain 1**), lizardsquad.org (**Subject Domain 2**), stresser.poodlecorp.org (**Subject Domain 3**), and poodlecorp.org (**Subject Domain 4**) (collectively, the "**Subject Domains**"). Domains ending in ".org" are ultimately controlled by Public Interest Registry, 1775 Wiehle Avenue, Suite 200, Reston, Virginia 20190

4. The statements in this affidavit are based on my personal knowledge and from persons with knowledge regarding relevant facts. Moreover, throughout this affidavit in footnotes and in brackets I provide definitions and explanations for certain terms and phrases. Those definitions are based on my training and experience in the area of computers and my experience investigating the unauthorized access of computer systems, also known as computer hacking. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are sufficient to establish probable cause.

5. I know from my training and experience that the following definitions apply to the activity discussed in this affidavit:

a. *IP Address*: The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic to and from that computer may be properly directed from its source to its destination.

b. *Server*: A server is a computer that provides services to other computers. Examples include web servers which provide content to web browsers and e-mail servers which act as a post office to send and receive e-mail messages.

c. *VPN*: A Virtual Private Network ("VPN") is an encrypted connection between two or more computer resources over a public computer network, such as the Internet, which enables access to a shared network between those resources. A common example is an individual who purchases access to a VPN service from a VPN service provider. A VPN service provider may also be a server hosting provider or may be a customer of a server hosting provider that is using servers hosted by the server hosting provider for the VPN service. The individual would connect from the individual's computer to the VPN service at the VPN service provider over the Internet. Once connected to the VPN, the individual's subsequent computer network communications, including access to websites, would be routed through the VPN connection from the individual's computer to the VPN service at the VPN service provider, and then from the VPN service provider on to the destination website. The response from the destination website is sent back to the VPN service at the VPN service provider and then finally routed via the VPN connection to the individual's computer. In this scenario, the IP address which accesses the third party website is actually associated with the VPN service and is not the actual IP address of the individual's computer.

d. *Whois*: A "Whois" search provides publicly available information as to which entity is responsible for a particular IP address. A Whois record for a particular IP address will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range. For example, a Whois record for the IP address 10.147.53.25 might list an IP address range of 10.147.53.0 – 10.147.53.255 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the IP addresses 10.147.53.0 through 10.147.53.255.

e. *Domain Name*: A domain name is a simple, easy-to-remember way to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, "usdoj.gov" is a domain name.

f. *Domain Name System*: IP addresses generally have corresponding domain names. The Domain Name System (DNS) is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label specifies a subdivision, or subdomain, of the domain on the right. The right-most level conveys the "top-level" domain. For example, the domain name "www.example.com" means that the computer assigned that name is in the ".com" top-level domain, the "example" second-level domain, and the web server. For each top-level domain, there is a single entity, called a "registry," that determines which second-level domain resolves. Certain top-level domains have been assigned to specific countries. For example, ".de" is a top-level domain for Germany, ".mx" is a top-level domain for Mexico, and ".me" is a top-level domain for Montenegro.

g. *Registrar & Registrant*: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchaser of the domain name. The individual or business that purchases, or registers, a domain name is called a "registrant." Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Registrars typically maintain customer, billing, and contact information about the registrants who used their domain name registration services.

h. *Distributed Denial-of-service attack (DDOS)*: Based on my training and experience, I am aware that a "distributed denial-of-service" attack involves making computing or computer network resources unavailable to legitimate users. I am aware that these attacks are commonly carried out by directing large amounts of computer network traffic to a target causing that target's available resources to be consumed by the attack resulting in no or few resources left to accommodate legitimate users.

II. Facts Establishing Probable Cause in Support of the Criminal Complaint and The Seizure Warrant

A. Overview

6. The FBI has been investigating computer crimes perpetrated by members of the computer hacking groups "Lizard Squad" and "PoodleCorp." These crimes include extensive denial-of-service attacks, the trafficking of stolen payment card account information, and online account takeovers, in violation of the **Subject Offense**. Individuals associated with Lizard Squad and/or PoodleCorp include "pein," whom the FBI has identified as Zachary Buchta (who also uses the aliases "@fbiarelosers," "@xotehpoodle," and "lizard"), "Uchiha," whom the FBI has identified as Bradley Jan Willem van Rooy (who also uses the aliases "@UchihaLS," "dragon," and "fox"), "@chippyshell," whom the FBI has identified as Individual A, and "AppleJ4ck," whom the FBI has identified as Individual B.

7. As further described below, Zachary Buchta, Bradley Jan Willem van Rooy, Individual A, Individual B, and others have conspired to launch destructive cyber attacks against companies and individuals around the world. They have done so first by promoting and operating the websites "shenron.lizardsquad.org" (**Subject Domain 1**) and "stresser.ru" (hereinafter, "Shenron"), through which they provided a cyber-attack-for-hire service and trafficked stolen payment card account

information for thousands of victims. Using Shenron, Buchta, van Rooy, Individual A, Individual B, and other conspirators facilitated thousands of denial-of-service attacks targeting victims around the world, including in the Northern District of Illinois. Those denial-of-service attacks relied on a massive network of compromised computers, including computers in the Northern District of Illinois. Through Shenron, Buchta, van Rooy, Individual A, and other conspirators also sold stolen payment card information for thousands of victims.

8. As further described below, Buchta, Individual A, Individual B, and other conspirators also carried out massive denial-of-service attacks against several online gaming and entertainment companies (Victims A, B, C, and D). Finally, Buchta also operated another attack-for-hire service via the website "stresser.poodlecorp.org" (**Subject Domain 3**), which facilitated hundreds of other denial-of-service attacks. Below is a chart of the individuals and their corresponding aliases and usernames:[1]

Name	**Alias or Username**
Zachary Buchta	pein, @fbiarelosers, @xotehpoodle, lizard
Bradley Jan Willem van Rooy	@UchihaLS, @LizardLands, dragon, fox
Individual A	Chippyshell
Individual B	AppleJ4ck

[1] The evidence linking Buchta and van Rooy to their online identities is detailed later in the affidavit. *See* Part II(I) and (J).

B. Phonebomber.net

9. This investigation began in response to the launch of the website phonebomber.net, a site that enabled paying customers to select victims to receive repeated harassing and threatening phone calls from spoofed phone numbers. During October and November 2015, two Twitter accounts identified as belonging to members of Lizard Squad—@LizardLands and @UchihaLS (i.e., van Rooy)—were used to disseminate information about phonebomber.net.

10. On or about October 27, 2015, I accessed the website phonebomber.net and observed a webpage titled "Phone Bomber" that stated:

> phonebomber.net (phonebombermlyerhx.onion) is a no-registration phone bombing service. We will call your target once per hour with one of our pre-recorded messages for $20 a month. Since our calls come from random numbers, your target will be unable to block our calls. Your target will be left with only 3 options: Change their number, Bend to your whim, Deal with a ringing phone for the length of our attack :\
>
> For the extortionists amongst us we've added an option to cancel the calls at the click of a button, giving you complete control over the length of the attack. . . .
>
> Since there is no registration, all purchases are untraceable. The only data a hacker / feds would be able to exfiltrate from our database are the phone numbers currently being called, and the last 30 days of targets. Rest assured your privacy is respected here and purchase in confidence.

11. On or about October 23, 2015, @LizardLands announced that Victim O, a resident of the Northern District of Illinois, was the "first victim" of the service. Upon reviewing the hyperlink that @LizardLands tweeted and having received information from Victim O, Victim O's phone number received a phone call every hour for thirty days with the following audio recording:

> When you walk the fucking streets, Motherfucker, you better look over your fucking back because I don't flying fuck if we have to burn your fucking house down, if we have to fucking track your goddamned family down, we will fuck your shit up motherfuck.

C. Denial-of-Service Attack against Victim A

12. Soon after the launch of phonebomber.net, members of Lizard Squad began denial-of-service attacks against various victims and boasted about their attacks on Twitter. In particular, during November and December 2015, the Twitter accounts @LizardLands, @fbiarelosers (i.e., Buchta), and @chippyshell (i.e., Individual A) were used to coordinate and announce a denial-of-service attack committed against Victim A, an international digital media company. For example:

a. On or about December 3, 2015, I reviewed Twitter account @LizardLands and observed a retweet[2] of a tweet made by @chippyshell with a timestamp of November 27, 2015, at 7:33 AM PST, which stated: "[Victim A online service] #OFFLINE #CHIPPY #LIZARDSQUAD."

b. On or about December 7, 2015, I reviewed the account @chippyshell and the account description stated: "Founder of Lizard Squad / @fbiarelosers is my partner in cyber crime." I also observed the following tweets with associated timestamps:

> Tweet #1, November 27, 2015 6:40 AM PST: "put on ur fucking water boots itz bouta rain packets[3] kid"

[2] A "retweet" is the re-posting of a tweet made by another Twitter account.

[3] Based on my training and experience, I am aware that a "packet" is the terminology utilized for a unit of data that is being transmitted via digital networks. I am also aware that denial-

Tweet #2, November 27, 2015 7:33 AM PST, "[Victim A online service] #OFFLINE #CHIPPY #LIZARDSQUAD"

13. A representative of Victim A advised that Victim A was struck by a series of denial-of-service attacks that started on or about November 27, 2015, at approximately 6:40 AM PST, which had a significant impact on Victim A's online operations.

14. On or about December 7, 2015, I reviewed the account @fbiarelosers (i.e., Buchta) and observed the name listed with the account was "Pein" and the account description stated: "Leader of Lizard Squad - partner is @chippyshell." I also observed retweets posted on or about November 27, 2015 of the two tweets made by @chippyshell described above.

15. According to records from Twitter, collected through a search warrant, @fbiarelosers engaged in the following direct communications with other Twitter users, including @UchihaLS, about the denial-of-service attacks against Victim A:

Sent (UTC)	From	To	Direct Message
11/27/15 4:17 PM	Twitter User #1	@fbiarelosers	did u even lunched an attack on [Victim A online service] today, or was it just a troll?
11/27/15 4:17 PM	@fbiarelosers	Twitter User #1	we did
11/27/15 4:23 PM	Twitter User #1	@fbiarelosers	SSDP[4] again?
11/27/15 4:24 PM	@fbiarelosers	Twitter User #1	No

of-service attacks are often carried out by directing a large number of network packets to a target.

[4] Simple Service Discover Protocol (SSDP) provides a mechanism for a network connected device to locate other network connected devices offering certain services such as printers, scanners, etc. I am aware that SSDP can be leveraged to conduct denial-of-service attacks.

11/27/15 4:24 PM	@fbiarelosers	Twitter User #1	raw udp[5]
11/27/15 5:41 PM	@fbiarelosers	Twitter User #2	so
11/27/15 5:41 PM	@fbiarelosers	Twitter User #2	we took
11/27/15 5:41 PM	@fbiarelosers	Twitter User #2	[Victim A online service] offline
11/27/15 5:41 PM	@fbiarelosers	Twitter User #2	me n chippy
11/28/15 1:55 AM	@fbiarelosers	Twitter User #3	CASUALLY TAKING [Victim A online service] OFFLINE TODA
11/28/15 1:55 AM	@fbiarelosers	Twitter User #3	how was ur day?
11/28/15 1:58 AM	Twitter User #3	@fbiarelosers	Notice.... Ehh lota RL [real life] bullshit goin down... I cashed out tho finna go binge for a few days
11/28/15 1:59 AM	Twitter User #3	@fbiarelosers	How was... .errr urs?
11/28/15 1:59 AM	Twitter User #3	@fbiarelosers	Wat part about ddosing 1 of the words biggest companies is casual?
11/28/15 2:00 AM	@fbiarelosers	Twitter User #3	because it is so easy for us to do it lmfao
11/28/15 2:00 AM	@fbiarelosers	Twitter User #3	and
11/28/15 2:00 AM	@fbiarelosers	Twitter User #3	we only gave it a lil tap
11/28/15 2:00 AM	@fbiarelosers	Twitter User #3	to give the nerds a lil preview
11/28/15 2:00 AM	@fbiarelosers	Twitter User #3	of what is to come
11/28/15 3:12 PM	Twitter User #4	@fbiarelosers	y did chippy unbio me
11/28/15 3:12 PM	@fbiarelosers	Twitter User #4	because
11/28/15 3:12 PM	@fbiarelosers	Twitter User #4	hes getting serious attention rn [right now]
11/28/15 3:12 PM	@fbiarelosers	Twitter User #4	and doesnt want u to have negative attention
11/28/15 3:12 PM	@fbiarelosers	Twitter User #4	from people rn [right now]
11/28/15 3:12 PM	@fbiarelosers	Twitter User #4	becuz we took [Victim A online service] offline yesterday
11/28/15 3:12 PM	@fbiarelosers	Twitter User #4	trying to protect u ig

[5] User Datagram Protocol (UDP) is a communication protocol designed to transmit messages containing data, referred to as datagrams, between devices on a network. In this context, I believe the phrase "raw udp" refers to the tactic used in the denial-of-service attack.

11/28/15 5:32 AM	@fbiarelosers	@UchihaLS	[Victim A online service] is back offline c:

D. The Shenron Website

1. Launching of the Shenron Denial-of-Service Website

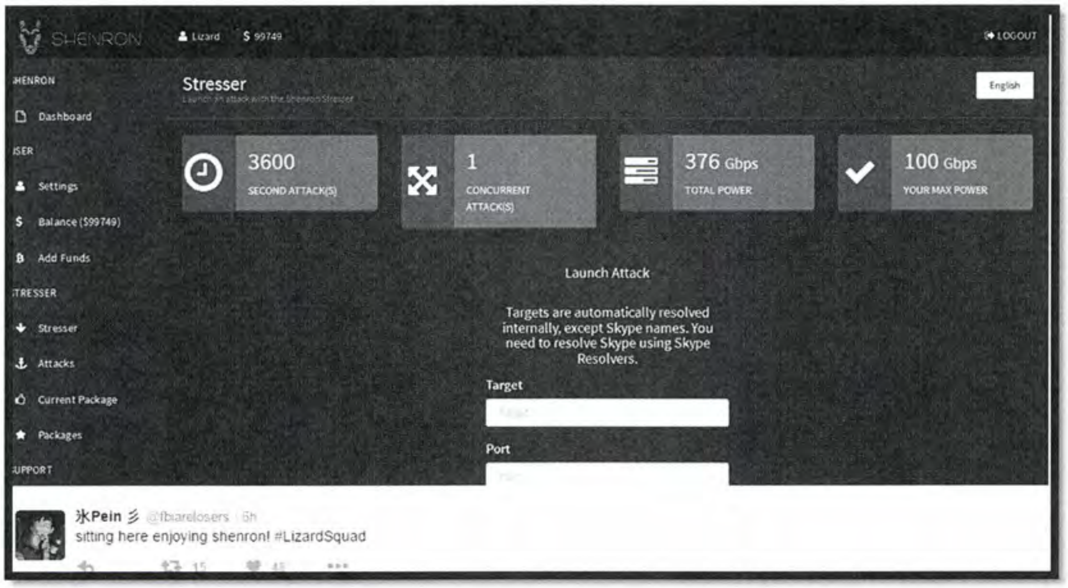
16. In or about February 2016, members of Lizard Squad, using the Twitter accounts @LizardLands, @UchihaLS (i.e., van Rooy), @fbiarelosers (i.e., Buchta), and @chippyshell (i.e., Individual A) advertised a new website named Shenron, which enabled paying customers to issue denial-of-service attacks with the click of a button against victims of their choosing.

17. On or about February 4, 2016, I reviewed the @fbiarelosers account, which had the display name "Pein," and observed a tweet dated February 4, 2016, which stated: "sitting here enjoying shenron! #LizardSquad." Also included with the tweet was a screenshot (as reflected below) of a webpage titled "SHENRON," which included a heading that invited users to "[l]aunch an attack with the Shenron Stresser." The webpage also had text boxes referring to the length, number and power of the attack (with the power reflected in gigabits per second or "Gpbs"). The webpage included a pop-up box titled, "Launch Attack."[6] The logged in user account visible in

[6] This screenshot appears to be of a website for a "stresser service." I am aware from my training and experience that stresser services, which are sometimes referred to as "booter services," typically provide denial-of-service attack capabilities on a pay-per-usage or subscription basis. Based on my training and experience, I believe "376 Gbps TOTAL POWER" refers to the maximum attack size of the service in terms of the amount of network traffic that could be directed at a target.

the upper left-hand corner of the screen was observed to be "Lizard" with an apparent account balance of $99,749.

Figure 1 – February 4, 2016 @fbiarelosers tweet

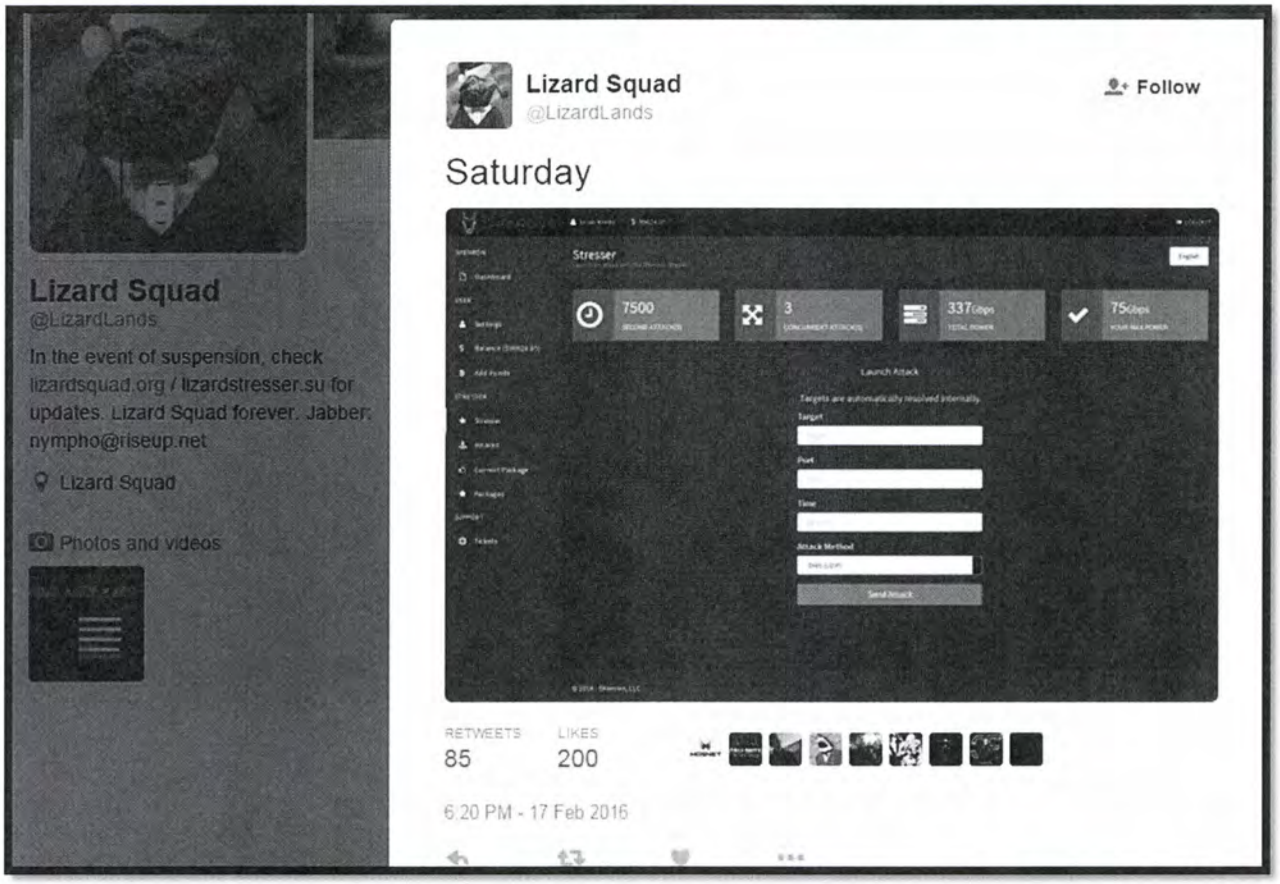


Targets are automatically resolved internally, except Skype names. You need to resolve Skype using Skype Resolvers.

氷Pein 彡 @fbiarelosers · 6h
sitting here enjoying shenron! #LizardSquad

18. On or about February 19, 2016, I reviewed the @LizardLands account and also observed a tweet dated February 17, 2016, which stated: "Saturday." Included with the tweet was a screenshot (as reflected below) of a webpage titled "SHENRON," which similarly referred to the length, number, and power of the attacks. The webpage also included a pop-up box titled, "Launch Attack," followed by fields titled, "Target," "Port," "Time," and "Attack Method." The bottom of this pop-up box included a pushbutton labeled, "Send Attack."

Figure 2 – February 17, 2016 @LizardLands tweet



Lizard Squad
@LizardLands
In the event of suspension, check lizardsquad.org / lizardstresser.su for updates. Lizard Squad forever. Jabber: nympho@riseup.net
Lizard Squad
Photos and videos

Lizard Squad
@LizardLands

Saturday

RETWEETS 85
LIKES 200

6:20 PM - 17 Feb 2016

19. On or about February 20, 2016, and February 21, 2016, I reviewed the @LizardLands account and observed the following tweets:

> February 20, 2016 10:07 AM PST: "shenron.lizardsquad.org" [**Subject Domain 1**]
>
> February 20, 2016 11:45 AM PST: "@TRAITORTR8R Tool for taking down internet connections." This tweet was observed to have been sent in response to the following tweet by @TRAITORTR8R: "@LizardLands what's a stresser lol."
>
> February 20, 2016 12:18 PM PST: "Shenron Booter has been released - shenron.lizardsquad.org" [**Subject Domain 1**]

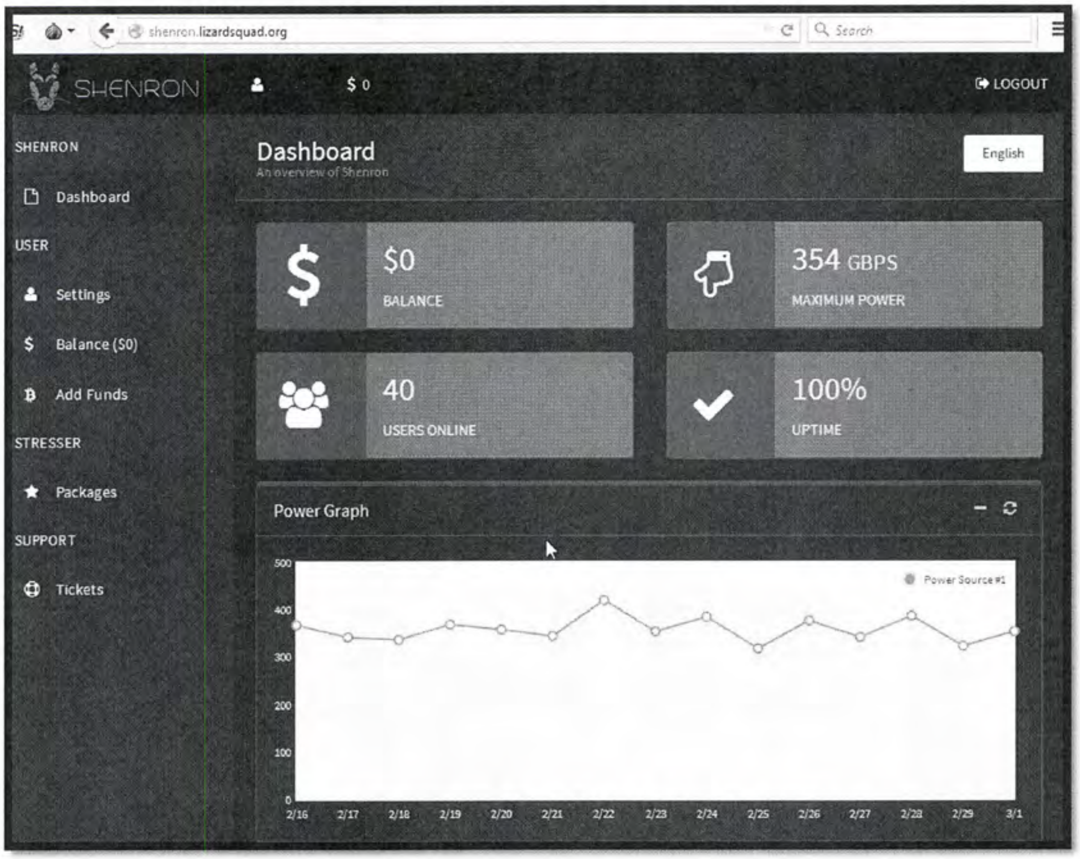
> February 20, 2016 1:03 PM PST: "PayPal Payments are now being accepted on shenron.lizardsquad.org [**Subject Domain 1**], limited time!"
>
> February 20, 2016 1:41 PM PST: "@DominicAero1 Its a monthly subscription with unlimited attacks." This tweet was observed to have been sent in response to the following tweet by @DominicAero1: "@LizardLands Do we have to add 20$ and get the 20$ package to be able to ddos [distributed denial-of-service] or can we add 2$ and do 1 attack?"

20. On or about February 20, 2016, I reviewed the @fbiarelosers account and observed a tweet with a timestamp of February 20, 2016, at 12:10 PM PST, which stated: "shenron.lizardsquad.org," i.e., **Subject Domain 1**.

21. On or about February 21, 2016, I reviewed the @chippyshell account and observed a tweet with a timestamp of February 20, 2016, at 6:01 pm PST, which stated "shenron.lizardsquad.org," i.e., **Subject Domain 1**.

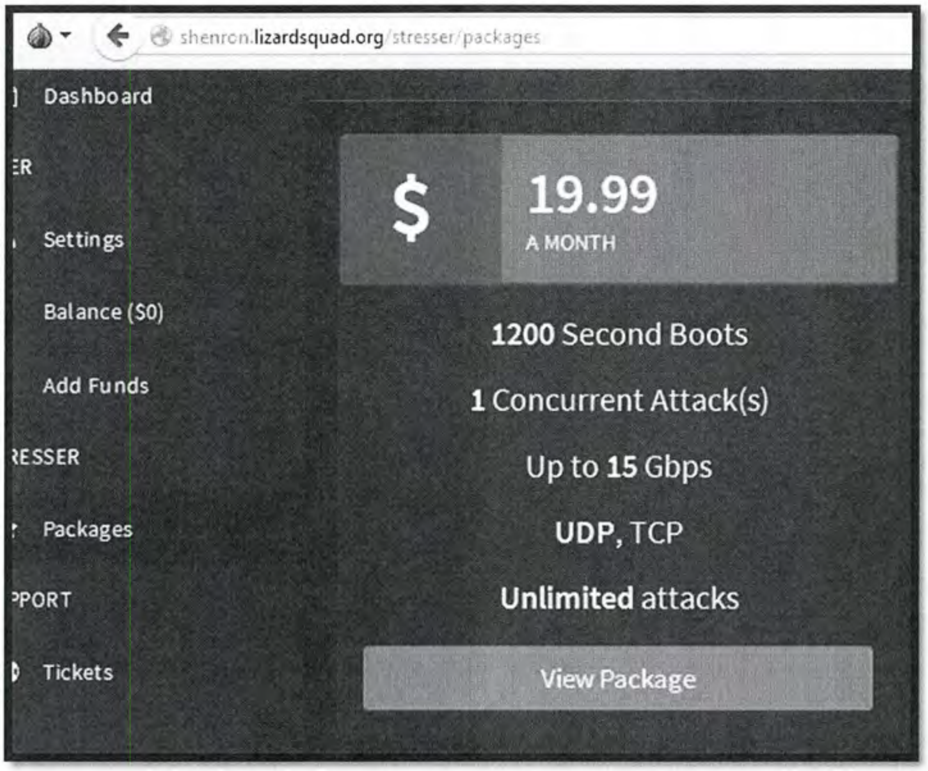
22. On or about March 1, 2016, I accessed the website **Subject Domain 1**. After creating a user account, I was presented with a webpage (as reflected below) titled "Dashboard: An overview of Shenron," which had text boxes reflecting the user balance, the maximum power of an attack, the number of users online, and the percentage of time the website was available.

Figure 3 – March 1, 2016 FBI access to ***Subject Domain 1***



23. During the March 1, 2016 review of **Subject Domain 1**, I also observed (as reflected below) a "Packages" webpage that listed several packages for sale, including a package priced at $19.99 per month which would purchase the ability to carry out attacks for 1,200 seconds at a time with a power of up to "15Gbps," and "Unlimited Attacks."

*Figure 4 – March 1, 2016 FBI access to **Subject Domain 1***



shenron.lizardsquad.org/stresser/packages

$ **19.99**
A MONTH

1200 Second Boots

1 Concurrent Attack(s)

Up to **15** Gbps

UDP, TCP

Unlimited attacks

2. Testing of the Shenron Denial-of-Service Capability

24. After the launch of the Shenron website, a confidential source ("Source A")[7] paid for a subscription on Shenron and tested each of the denial-of-service attack capabilities against a consenting party that logged the attack traffic. One of the attack methods tested was labeled on the Shenron site as "SNMP (UDP)."[8] Source A

[7] Source A is involved in computer security and is in direct and indirect online communications with individuals involved in computer hacking activities, including individuals involved in this investigation. Source A has provided information to the FBI since 2014 for multiple computer hacking related investigations. Information provided by Source A in this investigation has been corroborated. Source A has no criminal history and has not received monetary compensation from the FBI apart from certain expenses.

[8] Simple Network Management Protocol (SNMP) is a communication protocol for management and monitoring of network devices. SNMP operates using User Datagram Protocol (UDP) packets.

has provided the FBI a copy of the results of the testing, including the Simple Network Management Protocol ("SNMP") attack, which I have reviewed.

25. The SNMP attack was found to be composed of approximately 6,000 unique IP addresses, each of which was transmitting SNMP responses to the targeted IP address and port. Based on my training and experience, this attack traffic appeared to be consistent with an SNMP amplification attack.[9]

26. I reviewed the IP addresses reflected in the logs as sending the SNMP responses and identified one of these as an IP address associated with Company T ("Company T IP address"). Company T is located in Arlington Heights, Illinois, and the Company T IP address was assigned to a computer network device running the SNMP service from a location in Arlington Heights.

27. On or about March 17, 2016, Company T provided consent for the FBI to monitor computer trespasser traffic to and from the Company T IP address, which commenced on or about March 22, 2016, and continued until on or about May 31, 2016. The monitoring reflected hundreds of instances in which a single IP address appeared to issue large numbers of SNMP requests to the Company T IP address, resulting in the Company T IP address sending SNMP responses to the IP address

[9] I am aware from my training and experience that an SNMP amplification attack is a type of denial-of-service attack in which the attacker sends SNMP requests to Internet-accessible devices running SNMP, with the source IP address in the request being falsified (also known as "spoofed") to appear to be the IP address of the target of the denial-of-service attack. This results in the SNMP responses from these Internet accessible devices to be directed to that target IP address instead of back to the IP address of the attacker that sent the request. The size of the SNMP response is typically much larger than the size of the request resulting in the "amplified" size of the attack.

that appeared to be submitting the requests.[10] Based on my training and experience, I found this to be consistent with an SNMP amplification attack in which the attack "spoofs" the source IP address in the SNMP request to cause the responses to be directed to the intended target IP address.

3. Further Investigation of the Shenron Website

28. On or about March 4, 2016, I reviewed the publicly accessible portion of @LizardLands and observed a tweet explaining that Shenron had a "new domain," which was listed as "stresser.ru."

29. On or about March 4, 2016, I accessed the website "stresser.ru" and it appeared to be the same website previously accessed via **Subject Domain 1**, offering identical denial-of-service attack packages. I also was able to successfully login to the website using the username and password combination for the account I had created on March 1, 2016, when accessing **Subject Domain 1**.

30. On or about April 12, 2016, I reviewed the @LizardLands and @fbiarelosers accounts and observed a tweet by @LizardLands dated April 11, 2016, which advertised stresser.ru. For the @fbiarelosers account, the "bio" section stated that the user was a "Leader of Lizard Squad" and that one may direct message (or "DM") the account about obtaining the services of a "5 star botnet."[11]

[10] There were some instances in which the Company T IP address received SNMP requests, but for an unknown reason did not send the corresponding SNMP responses.

[11] A "botnet" refers to a collection of computers or other Internet-connected devices that have been compromised, typically with malicious software, enabling an attacker to exercise some

31. I re-reviewed the Shenron website via "stresser.ru" approximately eight times between on or about March 11, 2016, and May 16, 2016, and observed that it continued to offer denial-of-service attack packages for purchase. The maximum denial-of-service attack size advertised during this time was "Up to 500 Gbps" for packages that cost $999.99 a month.

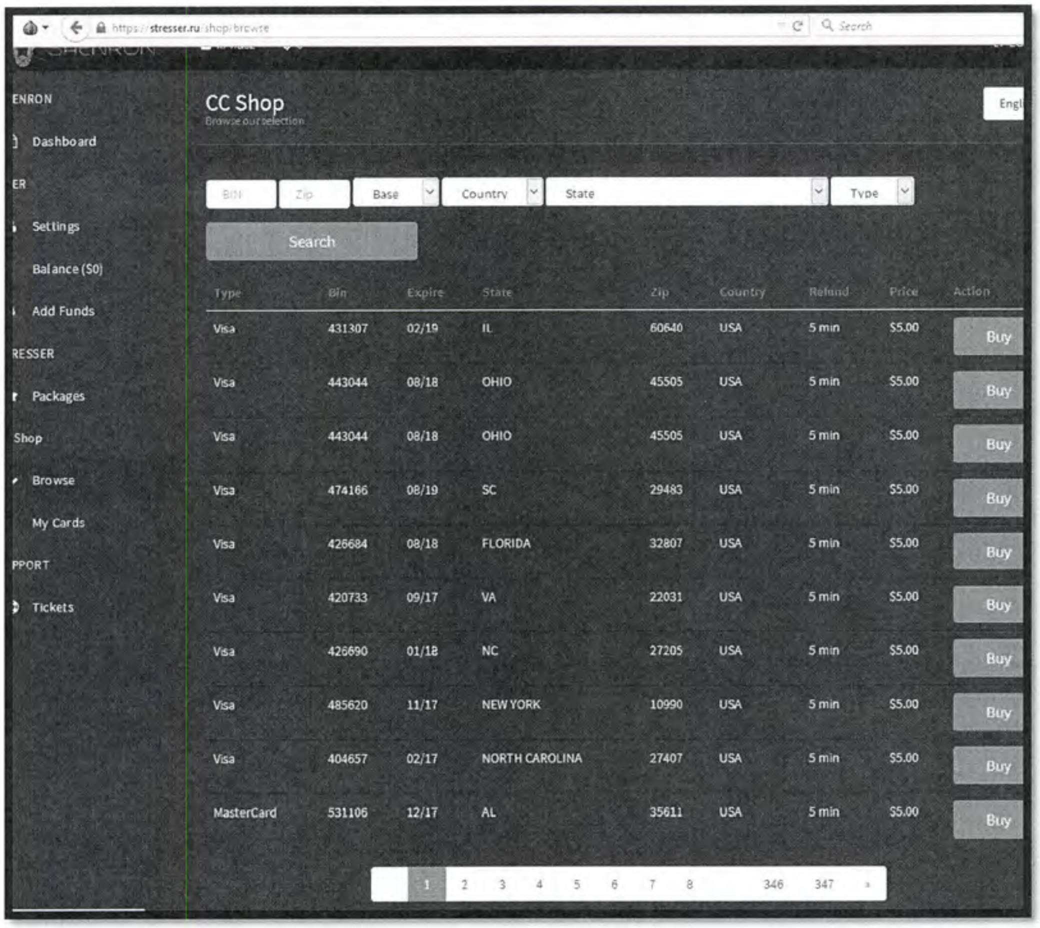
32. On or about May 24, 2016, I accessed the Shenron website via "stresser.ru" and found that in addition to offering denial-of-service attack packages, the website also contained a section named "CC Shop" that offered for sale credit card information. The section had a comment that stated:

> Welcome to the newest addition to the shenron family: the card shop! We have uploaded a very small batch for testing purposes. The valid rate is 60-80%. Please note it's still under development so expect issues. If you have any questions submit a ticket. More coming soon. ~ shenron team.

The "CC Shop" section contained what appeared to be approximately 347 pages of payment card data available for purchase with each page appearing to contain approximately ten records per page.

degree of control over these compromised devices. I am aware from my training and experience that botnets are commonly utilized to conduct denial-of-service attacks.

Figure 5 – March 24, 2016 Shenron CC Shop



CC Shop
Browse our selection

Type	Bin	Expire	State	Zip	Country	Refund	Price	Action
Visa	431307	02/19	IL	60640	USA	5 min	$5.00	Buy
Visa	443044	08/18	OHIO	45505	USA	5 min	$5.00	Buy
Visa	443044	08/18	OHIO	45505	USA	5 min	$5.00	Buy
Visa	474166	08/19	SC	29483	USA	5 min	$5.00	Buy
Visa	426684	08/18	FLORIDA	32807	USA	5 min	$5.00	Buy
Visa	420733	09/17	VA	22031	USA	5 min	$5.00	Buy
Visa	426690	01/18	NC	27205	USA	5 min	$5.00	Buy
Visa	485620	11/17	NEW YORK	10990	USA	5 min	$5.00	Buy
Visa	404657	02/17	NORTH CAROLINA	27407	USA	5 min	$5.00	Buy
MasterCard	531106	12/17	AL	35611	USA	5 min	$5.00	Buy

33. On or about May 27, 2016, an FBI agent connected to the Shenron website via "stresser.ru" and purchased six credit cards from the Shenron card shop. The purchased information included the card holder's name, address, full credit card number, security code, and expiration date. The FBI has confirmed with the issuer of these six cards that the purchased information was accurate card data. The FBI has interviewed two of the associated cardholders and they confirmed they had not authorized anyone to sell their payment card information. One of these individuals, Victim E, is a resident of the Northern District of Illinois.

34. I have re-reviewed the Shenron website via "stresser.ru" approximately ten times between on or about June 27, 2016, and or about September 15, 2016, and have observed that it has continued to offer payment cards for sale during each of these instances.

35. On or about September 15, 2016, I also reviewed the website lizardsquad.org, i.e., **Subject Domain 2**, which displayed the title "Lizard Squad Hub" with the only additional text on the page stating: "If you were looking for the lizard squad twitter click [https://twitter.com/lizardlands] Stresser: [**Subject Domain 1**]." I then accessed **Subject Domain 1** and logged in with the same account I used to access Shenron via "stresser.ru." I found that it displayed the same information I observed during my September 15, 2016 review via "stresser.ru."

36. I reviewed the IP addresses associated with both **Subject Domain 1** and stresser.ru and found them to be associated with the U.S.-based website proxy service provider CloudFlare, Inc.[12]

37. Records provided from CloudFlare reflected that it was providing proxy services to access the websites **Subject Domain 1** and stresser.ru and that the actual

[12] CloudFlare is a U.S.-based internet service company that provides proxy services for its customers' websites which results in internet traffic destined for those websites to be routed through CloudFlare's network. As a result, the publicly listed IP addresses associated with a CloudFlare customer's website would be a CloudFlare controlled IP address. CloudFlare maintains records of the true IP address on which the corresponding website is actually hosted in order to properly route the traffic to and from that website via CloudFlare's network.

IP address associated with both **Subject Domain 1** and stresser.ru was an IP address ending in 247.

38. I performed a Whois search for the IP address ending in 247 and found it was allocated to an internet service provider in the Netherlands.

4. Court-Authorized Wiretap of the Shenron Website

39. Pursuant to both a mutual legal assistance request from the United States and a parallel investigation initiated by Dutch authorities, a court in the Netherlands authorized a wiretap of the computer assigned to the IP address ending in 247, which began on or about May 24, 2016. United States authorities received a copy of the wiretap data covering the period of approximately on or about May 24, 2016, through approximately on or about June 8, 2016, and I have reviewed that data. The data reflects, among other things, that during that time period:

a. Users of the Shenron website purchased over 100 payment cards.

b. Over 600 apparent denial-of-service attacks were initiated by users of the Shenron website, including SNMP denial-of-service attacks.

40. The payment card data purchased via the Shenron website included card data for Victim E[13] and F, both of whom are residents of the Northern District of Illinois. Victim E and F were both interviewed by the FBI and they confirmed that they had not authorized anyone to sell their payment card information.

[13] The card data for Victim E was associated with the previously described FBI purchase on or about May 27, 2016.

41. The wiretap data reflected that several purchases of payment card data were made by a Shenron user whose connection to the Shenron website was routed through a CloudFlare data center associated with the identifier "ORD."[14] These included purchases from on or about May 27, 2016, through on or about June 2, 2016, of payment card information for Victims G through J. Victims G, H, and I have been interviewed by the FBI. Victims G and H and each confirmed that they had not authorized anyone to sell their payment card information. Victim I confirmed that he/she was aware that his/her card information had been compromised without his/her authorization.

42. I compared the SNMP denial-of-service attacks reflected in the wiretap data with the SNMP requests that were identified by the computer trespasser monitoring of the Company T IP address. The first SNMP denial-of-service attack reflected in the wiretap had a date of on or about May 23, 2016, at 8:52 AM UTC.[15] The wiretap data reflected approximately 62 SNMP denial-of-service attacks initiated between this date and time, and on or about May 31, 2016.[16]

43. Based on my review, 32 of the 62 SNMP denial-of-service attacks had corresponding matches in the computer trespasser monitoring of the Company T IP

[14] Information provided by CloudFlare reflects that the data center associated with "ORD" is physically located in Chicago, Illinois.

[15] Based on an analysis of the wiretap data, it appears that Shenron displays recent attack history to a user. As a result, I was able to obtain information on some attacks performed via the site prior to the start of the wiretap.

[16] As stated previously, the computer trespasser monitoring of the Company T IP address ended on or about May 31, 2016.

address. Specifically, for each of these 32 matches, at the date and time a Shenron user submitted a SNMP denial-of-service attack against a specified target IP address and target port, a series of SNMP requests began to be received by the Company T IP address which had a source IP address and source port that matched the target IP address and target port specified in the Shenron attack.

44. I reviewed the IP addresses that were targeted by the denial-of-service attacks reflected in the wiretap data and identified several IP addresses associated with Comcast that appeared to be located in the Northern District of Illinois. Records from the wiretap data and Comcast reflect the following date and time of the cyber attack, the victim, and the victim's location:

Date and Time	Victim	Location
5/24/16 at 9:44 PM UTC	K	Belvidere, Illinois
5/24/16 at 1:40 PM UTC	L	Rockford, Illinois
5/30/16 at 10:49 PM UTC	M	Maywood, Illinois
6/08/16 at 1:39 AM UTC	N	Chicago, Illinois

E. April Denial-of-Service Attack Against Victim B

45. On or about April 14, 2016, I reviewed the @LizardLands account and observed the following tweets made by @LizardLands on April 13, 2016 (PDT):

> 6:44 PM PDT: "Get ready!"
>
> 6:49 PM PDT: "US [Victim B] #Offline – [Victim B game #1] #Offline, [Victim B game #2] #Offline, [Victim B game #3] #Offline, [Victim B game #4] #Offline @fbiarelosers @AppleJ4ckxoxo"
>
> 6:53 PM PDT: A retweet of an April 13, 2016 6:53pm PDT tweet by @[Victim B]CS, which stated "We are currently monitoring a DDOS attack against network providers which is affecting connections to our games"

7:09 PM PDT: "EU [Victim B] #Offline – [Victim B game #1] #Offline, [Victim B game #2] #Offline, [Victim B game #3] #Offline, [Victim B game #4] #Offline @fbiarelosers @AppleJ4ckxoxo"

7:20 PM PDT: "Arrest us."

7:55 PM PDT: "More to come."

46. On or about April 14, 2016, I reviewed the @fbiarelosers account and observed the bio section stated mentioned "PEiN" and that the user was a "Member of @LizardLands." I also observed that @fbiarelosers had retweeted the April 13, 2016, 7:09 PM PDT @LizardLands tweet which stated: "EU [Victim B] #Offline – [Victim B game #1] #Offline, [Victim B game #2] #Offline, [Victim B game #3] #Offline, [Victim B game #4] #Offline @fbiarelosers @AppleJ4ckxoxo"

47. On or about April 14, 2016, I reviewed the @UchihaLS account and observed the following tweet made by @UchihaLS on April 14, 2016 at 3:54 AM PDT: "You can't arrest a lizard."

48. Victim B is a U.S.-based company that produces video games, among other things. Representatives of Victim B confirmed that Victim B sustained significant denial-of-service attacks on or about April 13, 2016, which targeted both its United States and European region online gaming platforms. The denial-of-service attack against Victim B's United States region online gaming platform specifically targeted a particular IP address, Victim B IP address #1. This IP address is associated with the authentication servers for Victim B's United States region and is used to allow players to access Victim B's online games. The representatives

identified over 60,000 IP addresses involved in the attacks. Moreover, according to representatives of Victim B, the denial-of-service attacks had a significant impact on its operations in the United States and European region and that its damages were well in excess of $5,000.

49. According to records from Twitter, collected through a search warrant, the accounts @fbiarelosers (i.e., Buchta) and @AppleJ4ckxoxo (i.e., Individual B) had the following direct communications during the denial-of-service attacks against Victim B:

Sent (PDT)	From	To	Direct Message
4/13/16 6:04 PM	@AppleJ4ckxoxo	@fbiarelosers	[Victim B IP address #1] 1119[17]
4/13/16 6:06 PM	@AppleJ4ckxoxo	@fbiarelosers	done
4/13/16 6:07 PM	@AppleJ4ckxoxo	@fbiarelosers	logged out
4/13/16 6:08 PM	@fbiarelosers	@AppleJ4ckxoxo	hacker
4/13/16 6:08 PM	@fbiarelosers	@AppleJ4ckxoxo	kk
4/13/16 6:48 PM	@fbiarelosers	@AppleJ4ckxoxo	ok its loldongs123 for the [first four letters of Victim B] account
4/13/16 6:53 PM	@AppleJ4ckxoxo	@fbiarelosers	oh
4/13/16 6:53 PM	@fbiarelosers	@AppleJ4ckxoxo	what
4/13/16 6:53 PM	@fbiarelosers	@AppleJ4ckxoxo	u have the email right
4/13/16 6:53 PM	@fbiarelosers	@AppleJ4ckxoxo	dont paste it here
4/13/16 6:54 PM	@fbiarelosers	@AppleJ4ckxoxo	but input email and loldongs123 as password and switch region to eu
4/13/16 6:54 PM	@AppleJ4ckxoxo	@fbiarelosers	yaya I'm done buddy
4/13/16 6:54 PM	@fbiarelosers	@AppleJ4ckxoxo	oh wait u might need to make a eu account not sure
4/13/16 6:54 PM	@fbiarelosers	@AppleJ4ckxoxo	ok

[17] Representatives of Victim B have indicated that the port used to access its authentication servers is 1119.

4/13/16 6:54 PM	@fbiarelosers	@AppleJ4ckxoxo	going bac on
4/13/16 6:59 PM	@fbiarelosers	@AppleJ4ckxoxo	this is weird last time we hit [Victim B] [Twitter shortened URL which resolved to Victim B's gaming platform website] went offline
4/13/16 6:59 PM	@fbiarelosers	@AppleJ4ckxoxo	now its not offline
4/13/16 6:59 PM	@fbiarelosers	@AppleJ4ckxoxo	but [Victim B] is offline
4/13/16 6:59 PM	@fbiarelosers	@AppleJ4ckxoxo	odd
4/13/16 7:00 PM	@fbiarelosers	@AppleJ4ckxoxo	[Twitter shortened URL which resolved to a Twitter.com search for “[Victim B]CS”]
4/13/16 7:04 PM	@AppleJ4ckxoxo	@fbiarelosers	done
4/13/16 7:04 PM	@AppleJ4ckxoxo	@fbiarelosers	EU down as well
4/13/16 7:04 PM	@fbiarelosers	@AppleJ4ckxoxo	ok
4/13/16 7:50 PM	@fbiarelosers	@AppleJ4ckxoxo	ay
4/13/16 7:50 PM	@fbiarelosers	@AppleJ4ckxoxo	ay
4/13/16 7:50 PM	@fbiarelosers	@AppleJ4ckxoxo	ay
4/13/16 7:50 PM	@fbiarelosers	@AppleJ4ckxoxo	ay
4/13/16 7:50 PM	@fbiarelosers	@AppleJ4ckxoxo	u done?
4/13/16 7:50 PM	@AppleJ4ckxoxo	@fbiarelosers	Yep

50. I have reviewed the IP addresses identified by Victim B as participating in the denial-of-service attacks and many of them have service addresses located in the Northern District of Illinois.

F. PoodleCorp

51. Beginning in or about June 2016, a new computer hacking group operating under the name “PoodleCorp” emerged, which, as further described below, involved individuals associated with the group Lizard Squad. The “official” Twitter account for this group as identified on the group’s website, poodlecorp.org (**Subject Domain 4**), used the screen name @PoodleCorp.

52. Between approximately or about June 29, 2016, and July 6, 2016, FBI personnel reviewed the publicly-accessible content of @LizardLands and @PoodleCorp, and observed the following tweets:

a. A tweet by @PoodleCorp on or about June 23, 2016, at 2:15 AM UTC, which stated "Soon ;) #PoodleCorp #Summer2016";

b. A retweet by @LizardLands of the preceding tweet by @PoodleCorp.

c. A tweet by @LizardLands on or about June 28, 2016, at 5:35 AM UTC, which stated "Lizards and Poodles. #Summer2016";

d. A tweet by @LizardLands on or about June 30, 2016, at 5:14 AM UTC, which stated "[**Subject Domain 2**] & [**Subject Domain 4**] #Summer2016"; and

e. A tweet by @PoodleCorp on or about July 4, 2016, at 7:45 AM UTC, which stated "poodlecorp.org," i.e., **Subject Domain 4**.

1. Review of Subject Domain 4

53. On or about July 6, 2016, I reviewed **Subject Domain 4** and observed that it contained a section titled "Members," which listed six monikers and a corresponding hyperlink to the associated Twitter account. These included in part, the moniker "xo" with a hyperlink to twitter.com/xotehpoodle ("@xotehpoodle"), the moniker "shadowpoodle" with a hyperlink to twitter.com/shadowpoodle ("@shadowpoodle"), and the moniker "appleJ4ck" with a hyperlink to twitter.com/applej4ckxoxo. The website also contained a section titled "Used &

Abused," which listed seven entries corresponding to a purported victim of a cyber-attack from PoodleCorp and the date for that attack, including an entry for an attack on Victim C on June 26, 2016, and on Victim B on June 28, 2016. Victim C is also a U.S.-based company that produces, among other things, video games. Representatives from Victim C and Victim B have confirmed that their company each sustained a denial-of-service attack on June 26 and 28, 2016, respectively, and that the attack had an impact on their company's online gaming platform, blocking online access for tens of thousands of customers.

54. The "Used & Abused" section described in the previous paragraph also included an entry for Victim S and a link to a YouTube channel operated by Victim S.

55. On or about September 1, 2016, I reviewed the publicly-accessible portion of the YouTube channel for Victim S. The channel had over 12 million listed subscribers. I also reviewed the Twitter account for Victim S and located a tweet dated June 22, 2016, which stated: "We are aware of the hack on our youtube channel and we're working with YouTube to fix the changes."

56. On or about September 1, 2016, I performed an internet search for the Victim S YouTube channel compromise and located a video posted on a separate YouTube channel documenting the compromise of Victim S. All of the posted videos visible in Victim S's channel were observed to have the title "HACKED BY OBNOXIOUS AND PEIN twitter.com/poodlecorp." The video also displayed a tweet

from Victim S's Twitter account made on June 22, 2016, which stated "HACKED BY @fbiarelosers and @BLADER."

2. Launch of the PoodleStresser Service

57. Between approximately July 6, 2016, and July 31, 2016, FBI personnel reviewed the @PoodleCorp and @xotehpoodle (i.e., Buchta) accounts and observed the following tweets regarding "PoodleStresser":

a. A tweet by @PoodleCorp on or about July 19, 2016, at 6:08 PM PDT, which stated "Going to be doing a giveaway for PoodleStresser (stresser.poodlecorp.org [**Subject Domain 3**]) soon. RT to be eligible.";

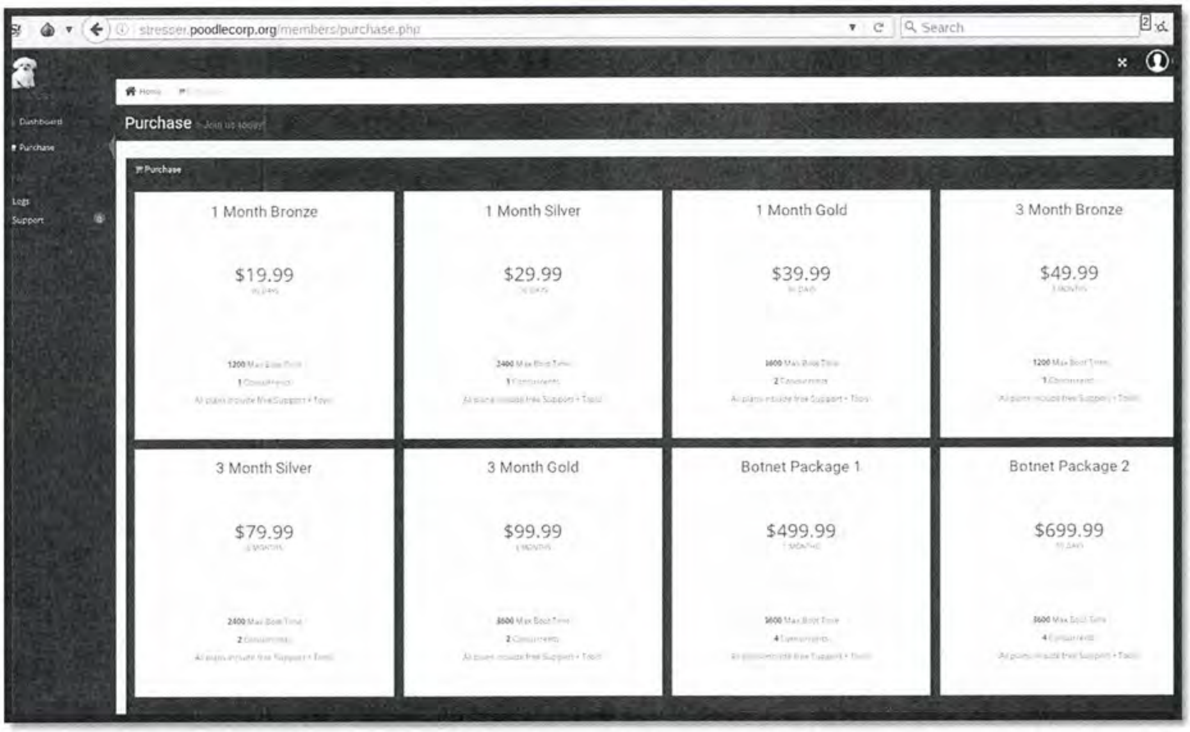
b. A retweet by @xotehpoodle of the July 19, 2016, 6:08 PM PDT tweet by @PoodleCorp; and

c. A tweet by @xotehpoodle on or about July 19, 2016, at 6:36 PM PDT, which stated "All user boots hit minimum of 10Gbps and the gold package does 20Gbps+ Also the botnet packages both hit at least 400Gbps at any time."

58. On or about July 22, 2016, an FBI employee accessed **Subject Domain 3**, and after creating a user account, was presented with a dashboard view web page (as reflected below), which stated "361 Total Attacks" and "1776 Total Users." The website also contained a section titled "Purchase," which listed eight options for purchase which included in part the following choices:

- 1 Month Bronze; $19.99 for 30 days; 1200 Max Boot Time, 1 Concurrents
- 1 Month Silver; $29.99 for 30 days; 2400 Max Boot Time, 1 Concurrents;
- 1 Month Gold; $49.99 for 30 days; 3600 Max Boot Time, 2 Concurrents;

Figure 6 – July 22, 2016 FBI access to ***Subject Domain 3***



Purchase - Join us today!

Purchase

1 Month Bronze	1 Month Silver	1 Month Gold	3 Month Bronze
$19.99 30 DAYS 1200 Max Boot Time 1 Concurrents All plans include free Support + Tools	$29.99 30 DAYS 2400 Max Boot Time 1 Concurrents All plans include free Support + Tools	$39.99 30 DAYS 3600 Max Boot Time 2 Concurrents All plans include free Support + Tools	$49.99 3 MONTHS 1200 Max Boot Time 1 Concurrent All plans include free Support + Tools
3 Month Silver	**3 Month Gold**	**Botnet Package 1**	**Botnet Package 2**
$79.99 3 MONTHS 2400 Max Boot Time 2 Concurrents All plans include free Support + Tools	$99.99 3 MONTHS 3600 Max Boot Time 2 Concurrents All plans include free Support + Tools	$499.99 1 MONTHS 3600 Max Boot Time 4 Concurrents All plans include free Support + Tools	$699.99 30 DAYS 3600 Max Boot Time 4 Concurrents All plans include free Support + Tools

3. The Leak of the PoodleCorp Database

59. On or about August 2, 2016, the Twitter account @LeakedSource (Twitter.com/LeakedSource) tweeted "PoodleCorp's DDOS [distributed denial-of-service] tool was hacked and all user data leaked. Search for yourself on #LeakedSource."[18] On or about the date of this tweet, **Subject Domain 3** was no longer accessible.

[18] The website leakedsource.com states that "Leaked Source is a collaboration of data found online in the form of a search engine. The purpose of the tool is to give users the ability to search each and find whether their data is available online or not." The site further states "We've accumulated hundreds of databases, not through a miraculously successful spate of hacking attempts, but by scouring the internet and dark web for data."

60. On or about August 10, 2016, a confidential source ("Source B")[19] provided the FBI a copy of what is believed to be the leaked Poodle Stresser database.[20] I have reviewed the contents of this database and found it to contain several database tables including those named "users" which appeared to reflect usernames, encrypted passwords, and email addresses, "loginlogs" which appeared to reflect user account login activity, "logs" which appeared to reflect attacks carried out, and "payments" which appeared to reflect payment details. To corroborate the authenticity of this information, I observed that the "loginlogs" table contained a login from the test account created by the FBI on July 22, 2016. I made the following observations during the review of these tables:

a. The first two accounts listed in the "users" table were "test123" and "admin." There were in excess of 1,500 user accounts overall listed in this table.

b. The "payments" table reflected sixteen entries with each entry listing in part an email address, a paid amount, an apparent PayPal transaction ID, and an apparent payment method. The first entry listed in the table had a listed email address of ThomasTaylor0707@hotmail.com (discussed later) and an apparent PayPal transaction ID of 8AF147362X797261U.

[19] Source B is in direct online communications with individuals involved in computer hacking activities. Source B has provided information to the FBI since 2012 as part of multiple computer hacking related investigations. Source B has a prior conviction for reckless driving. Source B has received approximately $6,000 from the FBI in return for assistance in this and other investigations.

[20] Source B obtained the database from a third party individual with whom Source B was in online communication.

61. The "logs" table reflected over 500 entries with each entry containing a username, an IP address, an apparent port number, an apparent attack duration, and an apparent attack method. I reviewed the IP addresses that were targeted by the denial-of-service attacks reflected in the "logs" table and identified several IP addresses associated with Comcast that appeared to be located in the Northern District of Illinois. Records from the "logs" table and Comcast reflect the following date and time of the cyber attack, the victim, and the victim's location:

Date and Time	Victim	Location
7/21/16 5:04 PM UTC	P	Plainfield, Illinois
7/21/16 8:02 PM UTC	Q	Oswego, Illinois
7/24/16 4:11 AM UTC	R	Aurora, Illinois

4. The Re-Launching of PoodleStresser (August 2016)

62. On or about August 24, 2016, I reviewed the @PoodleCorp and @xotehpoodle accounts and observed the following tweets regarding the re-launching of the "PoodleStresser" website:

a. A tweet by @PoodleCorp on or about August 24, 2016, at 4:45 AM PDT, which stated "stresser.poodlecorp.org [**Subject Domain 3**] back online! Upgraded power as well"; and

b. A retweet by @xotehpoodle of the @PoodleCorp August 24, 2016 4:45 AM PDT tweet.

63. On or about August 24 2016, I accessed **Subject Domain 3**, and after creating a user account was presented with a dashboard view web page, which displayed summary statistics for the use of the website which included 203 registered

users, 0 total global attacks launched, and 3 users listed as "Upgraded" with the sub-description "users that have active plan." A section of the website titled "upgrade" was found to allow individuals to purchase attack packages. This section stated in part: "All packages are delivered instantly upon payment confirmation – for obvious reasons we do not accept PayPal! However you can exchange PayPal to BitCoin via LocalBitcoins." This section also stated "Available Attack Methods: DNS, SSyN, Home, xSyn, TCP-FIN, TCP-RST, TCP-ACK, TCP-AMP, VSE, Dominate."[21] Six different attack packages were observed to be listed for purchase. These included in part the following:

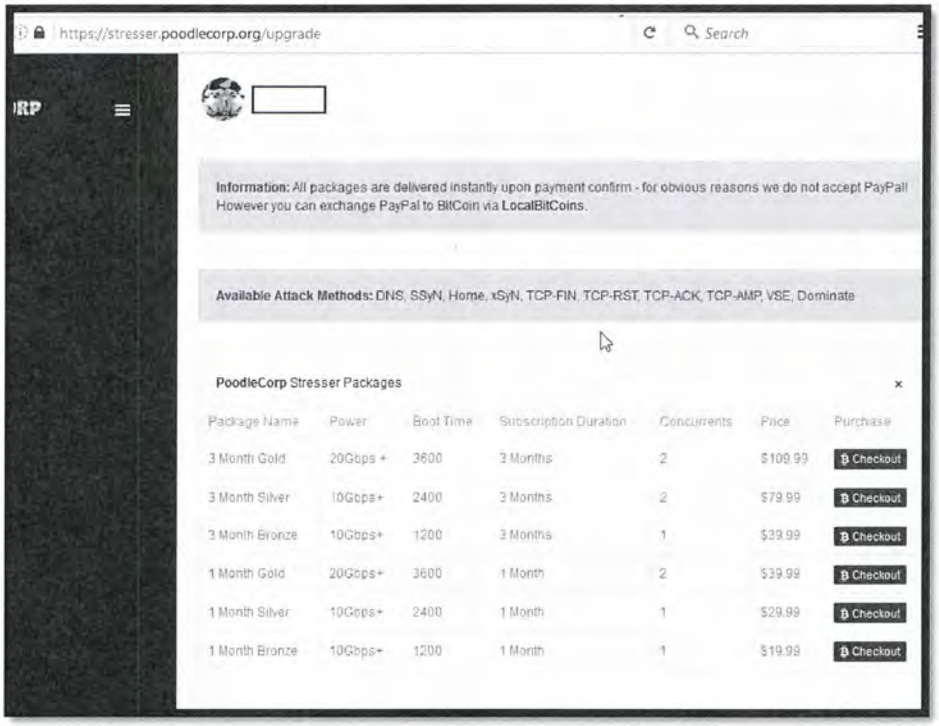
- 1 Month Bronze: $19.99 for 1 month; 10Gbps+ Power; 1200 Boot Time; 1 Concurrents;

- 1 Month Silver: $29.99 for 1 month; 10 Gbps+ Power, 2400 Boot Time; 1 Concurrents;

- 1 Month Gold; $39.99 for 1 month; 20Gbps+ Power; 3600 Boot Time; 2 Concurrents;

[21] Based on my training and experience, I am aware that the "attack methods" listed ("DNS," "SSyN," etc.) refer to different types of denial-of-service attacks.

Figure 7 – August 24, 2016 review of ***Subject Domain 3***



Information: All packages are delivered instantly upon payment confirm - for obvious reasons we do not accept PayPal! However you can exchange PayPal to BitCoin via **LocalBitCoins**.

Available Attack Methods: DNS, SSyN, Home, xSyN, TCP-FIN, TCP-RST, TCP-ACK, TCP-AMP, VSE, Dominate

PoodleCorp Stresser Packages ×

Package Name	Power	Boot Time	Subscription Duration	Concurrents	Price	Purchase
3 Month Gold	20Gbps +	3600	3 Months	2	$109.99	Ƀ Checkout
3 Month Silver	10Gbps+	2400	3 Months	2	$79.99	Ƀ Checkout
3 Month Bronze	10Gbps+	1200	3 Months	1	$39.99	Ƀ Checkout
1 Month Gold	20Gbps+	3600	1 Month	2	$39.99	Ƀ Checkout
1 Month Silver	10Gbps+	2400	1 Month	1	$29.99	Ƀ Checkout
1 Month Bronze	10Gbps+	1200	1 Month	1	$19.99	Ƀ Checkout

64. On or about August 26, 2016, I re-reviewed **Subject Domain 3** and observed the "dashboard" page reflected updated summary statistics for the use of the website, which reflected 2,526 registered users, 151 total global attacks launched, and 11 users listed as "Upgraded" with the sub-description "users that have active plan."

65. On or about August 28, 2016, I re-reviewed **Subject Domain 3** and observed the "dashboard" page reflected updated summary statistics for the use of the website, which reflected 3,321 registered users, 238 total global attacks launched, and 12 users listed as "Upgraded" with the sub-description "users that have active plan."

G. August 2016 Denial-of-Service Attack Against Victim B

66. Beginning on or about August 4, 2016, FBI personnel reviewed the account @PoodleCorp and observed the following Twitter activity pertaining to a denial-of-service attack against Victim B:

a. A tweet by @PoodleCorp on or about August 2, 2016, at approximately 4:33 PM PDT, which stated "(US) [Victim B] #Offline #PoodleCorp #Lubed"; and

b. A tweet by @PoodleCorp on or about August 2, 2016, at approximately 5:20 PM PDT, which stated "(EU & US) [Victim B] #Offline #PoodleCorp @[Victim B]CS @Gh0stPoodle @PoodlesInBlack."

67. A representative of Victim B confirmed to the FBI that Victim B sustained a denial-of-service attack on or about August 2, 2016, which had an impact on its online gaming platform.

H. August 2016 Denial-of-Service Attack Against Victim D

68. Victim D is a U.S.-based company that produces video games, among other things.

69. Beginning on or about September 1, 2016, I reviewed the publicly-accessible contents of @PoodleCorp and observed the following Twitter activity pertaining to a denial-of-service attack against Victim D:

a. A tweet by @PoodleCorp on or about August 31, 2016, at 11:58 AM PDT, which stated: "The upcoming attacks are powered by stresser.poodlecorp.org [**Subject Domain 3**] #PoodleCorp"; and

b. A tweet by @PoodleCorp on or about August 31, 2016, at 12:33 PM PDT which stated: "We are responsible for the downtime of @[Victim D] & @[Victim D game]#PoodleCorp."

70. A representative of Victim D has confirmed that a significant denial-of-service attack was experienced by Victim D beginning on or about August 31, 2016 at approximately 11:00 AM PDT, which had an impact on Victim D's operations and caused damages well in excess of $5,000.

5. Common access between @fbiarelosers, @PoodleCorp, and @xotehpoodle accounts

71. Records from Twitter, collected through a search warrant, subpoenas, and pen register data, reflect times in which Twitter accounts @fbiarelosers, @PoodleCorp, and @xotehpoodle were accessed from a common IP address in close time proximity. Specifically:

a. There were eight instances between on or about June 24, 2016, and on or about June 27, 2016, in which @fbiarelosers, @PoodleCorp, and @xotehpoodle were all logged into from the same IP address within three hours or less. This occurred on four different days and involved six different IP addresses used to log into all three accounts. A review of these IP addresses found them to be associated with the Tor network.[22]

[22] Tor (or The Onion Router) is an international software project to anonymize Internet traffic that allows individuals to use software to encrypt their communications and route them through a series of computers before they reach their destination thereby concealing the true origin point of the communication.

b. There were thirty-three instances between on or about June 24, 2016, and on or about September 2, 2016, in which @PoodleCorp and @xotehpoodle were logged into from the same IP address within three hours or less.

I. Identification of Zachary Buchta as User of @fbiarelosers and as an Operator of the Shenron and PoodleCorp Websites

72. As described below, the FBI first identified Buchta in this investigation based in part on text messages he appeared to exchange with @chippyshell near the time of the November 27, 2015, denial-of-service attack against Victim A (which attack is mentioned in ¶12). This led the FBI to identify and monitor Buchta's internet traffic and compare that to traffic accessing the @fbiarelosers account and the Shenron and PoodleCorp websites. As further described below, it appears that Buchta frequently accessed the @fbiarelosers account and the Shenron and PoodleCorp websites, often through an intermediary Virtual Private Network (VPN) based overseas.

73. Regarding the text messages, records obtained from Twitter reflect that @chippyshell had a telephone number ending in 1065 listed as a registered device for this account as of July 31, 2015, at 5:08 AM UTC. The records list the service carrier for this telephone number as "us.googlevoice." Records obtained from Google reflect that telephone number ending in 1065 was a Google Voice telephone number and that the underlying telephone number associated with the account was a number ending in 7297.

74. Records obtained from AT&T for the number ending in 7297 reflect a total of four SMS text messages sent between the number ending in 7297 and a Sprint telephone number ending in 9229 between November 27, 2015, at 4:28 PM UTC, and November 28, 2015, at 5:24 AM UTC, i.e., near the time of the denial-of-service attack against Victim A. Records from Sprint for telephone number ending in 9229 reflect that it is associated with mobile telephone service and that on November 27, 2015, the subscriber had a billing address in Fallston Maryland, where Zachary Buchta resides (the "Buchta Residence").

75. Comcast records obtained February 9, 2016, reflect that Comcast account number 0951967050805 (the "Buchta Comcast Account") is associated with Internet service provided to the Buchta Residence.

1. Internet Usage of the Buchta Comcast Account

76. On or about February 12, 2016, a pen register order for the Buchta Comcast Account was issued in the Northern District of Illinois, and thereafter renewed three times. The pen register collection reflected extensive communications between the Buchta Comcast Account and IP addresses ending in 218, 194, 138, 235, 58, and 42, all through UDP 443 and/or TCP port 22.[23] There were also extensive communications between the Buchta Comcast Account and the IP address ending in

[23] As described below, connections to these particular IP addresses and ports were determined to be consistent with usage of a particular VPN service based overseas.

92 through TCP port 3389.[24] In particular, the table below reflects the IP address, date range, days of communications between the IP address and the Buchta Comcast Account, and the cumulative size of data transmitted in gigabytes:

IP	Date Range	Days	Size
*218	2/24/16 – 6/22/16	63	150 GB
*194	4/1/16 – 9/5/16	83	300 GB
*138	4/2/16 – 9/5/16	93	400 GB
*235	2/25/16 – 5/30/16	37	100 GB
*58	5/23/16 – 5/24/16	2	10 GB
*42	7/4/16 – 9/3/16	18	30 GB
*92	7/4/16 – 8/29/16	25	1 GB

77. I performed Internet searches for the IP addresses above and found references indicating that, other than the *92 address, they were associated with a particular VPN service based overseas.

78. On or about June 30, 2016, I tested that VPN service observed that it supports establishing remote VPN sessions via UDP to port 443 and via TCP to port 22. I used the software to connect with servers identified as being located in the United States. Upon successful connection, the VPN service provided information about the connection, including the entry IP address and exit IP address, as well as the "Protocol" and "Port." I repeated this process again on or about September 20, 2016, and found that each VPN server had a consistent IP address when connecting

[24] These communications went to destination port TCP 3389. I am aware from my training and experience that Remote Desktop Protocol ("RDP") is a form of remote computer administration that allows an individual to establish a connection to a remote computer and have the equivalent of desktop access on the remote computer. I am also aware that RDP typically operates on TCP port 3389.

to VPN service and a corresponding IP address for connections exiting from the service, as follows:[25]

Server	IP Entry	IP Exit
1	*218 "Entry IP Address 1"	*219 "Exit IP Address 1"
2	*194 "Entry IP Address 2:	*195 "Exit IP Address 2"
3	*138 "Entry IP Address 3"	*139 "Exit IP Address 3"
4	*235 "Entry IP Address 4"	*236 "Exit IP Address 4"
5	*58 "Entry IP Address 5"	*59 "Exit IP Address 5"
6	*42 "Entry IP Address 6"	*43 "Exit IP Address 6"

79. As previously described, the entry IP addresses in the table above correspond to IP addresses with which the Buchta Comcast Account engaged in extensive communications.

2. Access to @fbiarelosers from VPN Servers With Corresponding Access from the Buchta Comcast Account

80. On or about December 29, 2015, a pen register order for @fbiarelosers was issued in the Northern District of Illinois, and renewed four times thereafter. The pen register collection, as well as login records obtained via search warrants of @fbiarelosers, reflected several logins from Exit IP Addresses 1, 2, and 4. Similarly,

[25] On September 20, 2016, VPN Server 1 was found to no longer be an available option and the results reflected here are from the June 30, 2016 testing only. VPN Servers 2 – 6 were tested on both June 30, 2016 and September 20, 2016 with identical Entry IP and Exit IP results between the two tests.

the login records for @fbiarelosers reflect logins from the *92 IP address, which was also accessed extensively from the Buchta Comcast Account.

81. Indeed, there are many instances in which the Buchta Comcast Account was communicating with one of the Entry IP Addresses at the same time that @fbiarelosers was accessed from the corresponding Exit IP Address. For example:

a. On or about April 14, 2016 at 2:48 AM UTC, Exit IP Address 4 logged into @fbiarelosers. The Buchta Comcast Account was communicating with Entry IP Address 4 at the same time.

b. On or about April 17, 2016 at 6:59 AM UTC, Exit IP Address 2 logged into @fbiarelosers. The Buchta Comcast Account was communicating with Entry IP Address 2 at the same time.

c. On or about April 17, 2016 at 10:31 PM UTC, Exit IP Address 4 logged into @fbiarelosers. The Buchta Comcast Account was communicating with Entry IP Address 4 at the same time.

d. On or about April 27, 2016 at 3:56 AM UTC, Exit IP Address 4 logged into @fbiarelosers. The Buchta Comcast Account was communicating with Entry IP Address 4 at the same time.

e. On or about May 14, 2016 at 5:53 AM UTC, Exit IP Address 1 logged into @fbiarelosers. The Buchta Comcast Account was communicating with Entry IP Address 1 at the same time.

82. Moreover, records indicate that the Buchta Comcast Account was used to access @fbiarelosers when that account was used to discuss the ongoing denial-of-service attack against Victim B, as described in ¶49. In particular, Twitter records reflect a login to @fbiarelosers from Exit IP Address 4 on or about April 13, 2016, at 7:48 PM PDT. The pen register for the Buchta Comcast Account reflects that the account was communicating with Entry IP Address 4 at the same time.

3. Access to the Shenron Website from VPN Servers With Corresponding Access from the Buchta Comcast Account

83. The wiretap data also reflected that the exit IP addresses for the VPN service were used to operate and use the Shenron website, such as reviewing and handling customer support tickets, initiating denial-of-service attacks, and purchasing a payment card. The wiretap data reflected that two different user accounts, "support" and "lizard," were used to perform this activity.

84. There are many instances in which the Buchta Comcast Account was communicating with entry IP address for the VPN service at the same time that the Shenron website was accessed from the corresponding exit IP addresses. For example:

a. On or about May 24, 2016, from 2:04 PM UTC to 2:06 PM UTC, Exit IP Address 5 accessed the Shenron website using the account "support"[26] and proceeded to review and close open support tickets (i.e., handle customer complaints

[26] At the time of this access, the user appears to have already been logged into the "support" account as there was no corresponding login reflected in the wiretap data.

or issues). The Buchta Comcast Account was communicating with Entry IP Address 5 at the same time.

b. On or about May 24, 2016, from 8:54 PM UTC to 9:02 PM UTC, Exit IP Address 1 accessed the Shenron website using the already logged in account "support" and proceeded to purchase a payment card and review the open support tickets. The Buchta Comcast Account was communicating with the corresponding Entry IP Address 1 at the same time.

c. On or about May 25, 2016, from 1:16 PM UTC to 1:18 PM UTC, Exit IP Address 1 accessed the Shenron website using the already logged in account "support" and proceeded to initiate two denial-of-service attacks with a specified duration of 7,500 seconds each. The Buchta Comcast Account was communicating with Entry IP Address 1 at the same time.

d. On or about May 25, 2016, from 2:32 PM UTC to 2:33 PM UTC, Exit IP Address 1 accessed the Shenron website and logged into the "lizard" account using a twenty-two-character password. The account balance was listed as $86,233.57 and the maximum power available to the "lizard" account was listed as 500 Gbps.[27] The "lizard" user then initiated a denial-of-service attack against a particular IP address with a specified duration of 18,000 seconds. The Buchta Comcast Account was communicating with Entry IP Address 1 at the same time.

[27] As previously stated, the prior reviews of the Shenron website identified the largest advertised attack size as "up to 500 Gbps" for a package which cost $999.99 per month.

e. On or about May 25, 2016, at 11:01 PM UTC, Exit IP Address 1 accessed the Shenron website and logged into the "support" account. The "support" user then reviewed and closed a support ticket. The Buchta Comcast Account was communicating with Entry IP Address 1 at the same time.

f. On or about May 26, 2016, at 9:32 AM UTC, Exit IP Address 1 accessed the Shenron website using the already logged in account "support" and reviewed a support ticket. The Buchta Comcast Account was communicating with Entry IP Address 1 at the same time.

g. On or about May 29, 2016, from 9:36 PM UTC to 9:37 PM UTC, Exit IP Address 4 accessed the Shenron website using the already logged in account "support" and reviewed support tickets. The Buchta Comcast Account was communicating with Entry IP Address 4 at the same time.

h. On or about June 3, 2016, from 4:45 PM UTC to 4:50 PM UTC, Exit IP Address 1 accessed the Shenron website, logged into the "support" account, and accessed the support tickets. The Buchta Comcast Account was communicating with Entry IP Address 1 at the same time.

i. On or about June 3, 2016, from 6:24 PM UTC to 6:25 PM UTC, Exit IP Address 3 accessed the Shenron website using the already logged in account "support" and reviewed an open support ticket. The Buchta Comcast Account was communicating with Entry IP Address 3 at the same time.

j. On or about June 4, 2016, at 12:15 AM UTC, Exit IP Address 2 accessed the Shenron website using the already logged in account "support" and accessed the support tickets. The Buchta Comcast Account was communicating with the Entry IP Address 2 at the same time.

k. On or about June 4, 2016, from 1:29 PM UTC to 1:33 PM UTC, Exit IP Address 1 accessed the Shenron website and logged into the "lizard" account. The account user then changed the "lizard" account password. The Buchta Comcast Account was communicating with Entry IP Address 1 at the same time.

l. On or about June 5, 2016, at 12:45 PM UTC, Exit IP Address 1 accessed the Shenron website using the already logged in account "lizard." The "lizard" user then initiated a denial-of-service attack with a specified duration of 18,000 seconds. The Buchta Comcast Account was communicating with Entry IP Address 1 at the same time.

m. On or about June 6, 2016, from 4:39 PM UTC to 4:40 PM UTC, Exit IP Address 2 accessed the Shenron website, logged into the "support" account, and accessed the support tickets. The Buchta Comcast Account was communicating with Exit IP Address 2 at the same time.

4. Access to the PoodleCorp Website from VPN Servers With Corresponding Access from the Buchta Comcast Account

85. As described above, I reviewed the leaked PoodleCorp database. With respect to the "loginlogs" table entries reflecting logins to the accounts "test123" and "admin," I identified many instances in which the Buchta Comcast Account was

communicating with an entry IP address for the VPN service at the same time there was access to the "admin" account for the PoodleCorp website with a corresponding exit IP addresses. For example:

a. Exit IP Address 2 was listed for twenty-two logins to the "admin" account and five logins to the "test123" account between on or about July 21, 2016 at 10:28 AM UTC, and on or about July 24, 2016 at 7:21 PM UTC. The Buchta Comcast Account was communicating with Entry IP Address 2 during the times listed for each of these twenty-seven combined logins.

b. Exit IP Address 6 was listed for three logins to the "admin" account and two logins to the "test123" account on or about July 24, 2016, between approximately 10:01 AM UTC and 8:01 PM UTC. The Buchta Comcast Account was communicating with Entry IP Address 6 during the times listed for each of these five combined logins.

c. Exit IP Address 3 was listed for five logins to the "admin" account on or about July 25, 2016, between 9:48 AM UTC and 5:13 PM UTC. The Buchta Comcast Account was communicating with Entry IP Address 3 during the times listed for each of these five logins.

86. With respect to the "payments" table for the PoodleCorp database, PayPal records were obtained for the accounts associated with the transaction ID 8AF147362X797261U, which was the first transaction listed in the table. These records show that PayPal transaction 8AF147362X797261U occurred on July 20,

2016, at 12:08 AM UTC and was a $1.00 payment from the PayPal account associated with the email address ThomasTaylor0707@hotmail.com (which was reflected in the leaked database, see ¶60(b)) made to the PayPal account associated with the email address 495081505855@protonmail.com. The subject of the payment was "1 Month Bronze."

87. PayPal records for the account associated with the email address 495081505855@protonmail.com reflected the following information:

a. The account holder is listed as Zachary Buchta, along with his date of birth. The Buchta Residence is listed as an address for the account, and a mobile telephone number ending in 9229 is listed for the account.[28] A bank account held at Aberdeen Proving Ground Federal Credit Union with an account number ending in 7176 was also associated with the account.

b. The records reflect 69 logins to the account, including:

i. Twenty-five logins to the account from the Buchta Comcast Account between April 9, 2016, and July 30, 2016.

ii. Fifteen logins to the account from Exit IP Address 2 between June 16, 2016, and July 28, 2016.

iii. Fifteen logins to the account from Exit IP Address 3 between April 7, 2016, and July 20, 2016.

[28] The telephone number associated with this PayPal account was the same telephone number previously described in this affidavit as exchanging text messages with the AT&T telephone number ending in 7297, and which had a billing address of the Buchta Residence.

iv. Two logins to the account from Exit IP Address 1 between June 8, 2016, and June 14, 2016.

88. PayPal records for the account associated with the email address ThomasTaylor0707@hotmail.com reflected the following information:

a. The account received sixteen payments between July 19, 2016, and July 20, 2016 with values of $19.99, $29.99, or $39.99 with corresponding descriptions of "1 Month Bronze," "1 Month Silver," and "1 Month Gold."

b. The records showed sixty-nine logins to the account between July 6, 2016, and July 28, 2016 which included:

i. Two logins to the account from Exit IP Address 3 on July 19, 2016.

ii. Two logins to the account from Exit IP Address 2 on July 20, 2016

89. Aberdeen Proving Ground Federal Credit Union records reflect that the account holder of the account ending in 7176 is Zachary Buchta with the Buchta Residence listed as the account holder address.

5. Previous Interview of Buchta

90. As part of a separate FBI investigation into a denial-of-service attack, on or about July 17, 2014, Buchta was interviewed by FBI agents at the Buchta Residence. During the interview, Buchta provided his mobile telephone number as the same telephone number ending in 9229 as has been previously described. The interview was prompted by a report received by the FBI alleging that an individual

named "Zach" residing at the Buchta Residence had been involved in a denial-of-service attack. During the interview, Buchta denied any involvement with denial-of-service attacks, and stated that he had been chatting online with a group of individuals, but that Buchta eventually stopped associating with them.

91. As part of a separate FBI investigation into swatting calls,[29] on or about November 5, 2015, Individual C[30] was interviewed by the FBI in connection with Individual A's alleged involvement in making swatting calls. Individual A stated that "Zach Buchta" was his/her friend and also responsible for making swatting calls. Individual C stated that Zach Buchta lived at the Buchta Residence, and that Buchta utilized the Twitter account @fbiarelosers and the moniker "Pein." Individual C also stated that Buchta was the "co-leader" of Lizard Squad. Individual C also stated that a Facebook account he/she was questioned about was also used by an individual with the moniker "vamp."

92. During the review of the search warrant results for @fbiarelosers, I observed Twitter direct messages sent on or about November 6, 2015, at 5:56 AM UTC from @fbiarelosers to another Twitter user which stated, "oh I also found out I got snitched on by vamp so I cant have anything illegal or do anything illegal."

[29] The term "swatting" refers to false emergency calls placed to law enforcement agencies typically alleging scenarios such as an active shooter at a residence. The purpose of the "swatting" call is to incite a law enforcement response, often times a SWAT team, to the targeted address.

[30] Individual C was a minor at the time this interview was conducted.

J. Identification of Bradley Jan Willem van Rooy as the User of Uchiha and as an Operator of the Shenron Website

93. According to records from Twitter, collected through subpoenas and a search warrant, there were extensive logins to both @LizardLands and @UchihaLS from the same IP address 86.89.127.163 ("the '163 IP Address").[31] The records also reflected that the @LizardLands account was registered on or about January 28, 2015 from the '163 IP address. The records reflected that from on or about February 3, 2013, through on or about April 12, 2015, the email address associated with the @UchihaLS account was lil_jon@hotmail.nl. On or about April 12, 2015, the email address was changed to uchihals@mail.ru.

94. The Twitter records also reflect the following direct communications by @LizardLands in which the user indicated that he lived near a police station:

Date/Time (UTC)	From	To	Direct Message
2/1/15 10:47:57 PM	Twitter User #5	@LizardLands	Feds lurkin, be careful bro.
2/1/15 10:48:09 PM	Twitter User	@LizardLands	I could be an informant
2/1/15 10:50:08 PM	Twitter User #5	@LizardLands	You make me wanna start harassing twitch streamers again
2/1/15 10:50:37 PM	@LizardLands	Twitter User #5	God etc follow you you aint shit bruh
2/1/15 10:50:51 PM	Twitter User #5	@LizardLands	Lmao
2/1/15 10:50:55 PM	@LizardLands	Twitter User #5	Once the feds over here ill throw my laptop off my balcony 101
2/1/15 10:51:17 PM	Twitter User #5	LizardLands	Eat the hard drive

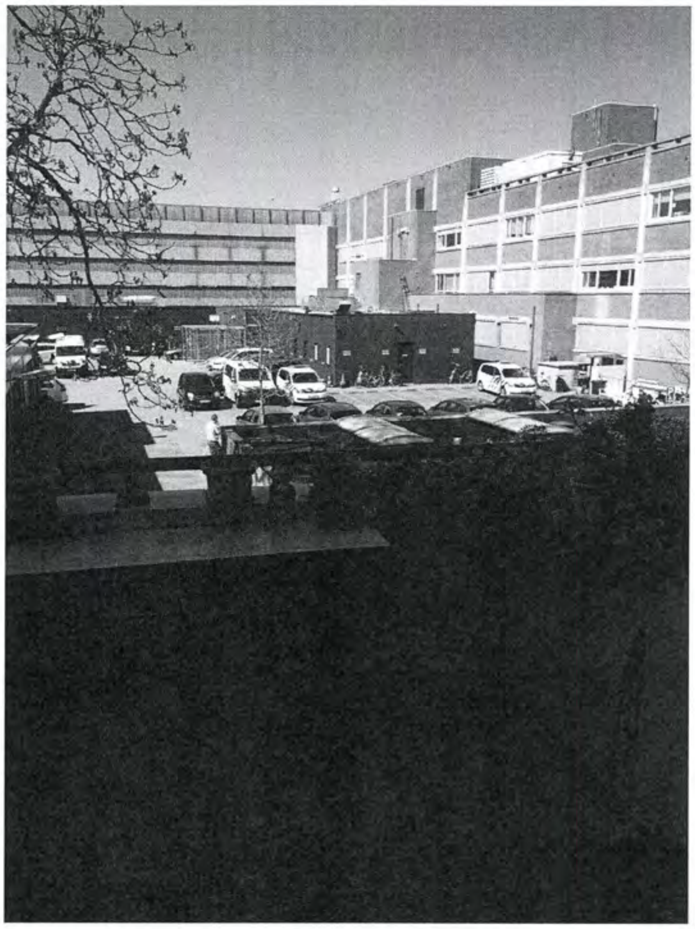
[31] Whois records reflected the IP address 86.89.127.163 to be associated with KPN, an internet service provider located in the Netherlands.

2/1/15 10:51:19 PM	@LizardLands	Twitter User #5	Wouldn’t be the best idea on second thoughts
2/1/15 10:51:32 PM	Twitter User #5	LizardLands	Just magnet it
2/1/15 10:51:37 PM	@LizardLands	Twitter User #5	Well there's a small problem
2/1/15 10:51:48 PM	@LizardLands	Twitter User #5	Nearest fed to me atm [at the moment] is approx 50 meters l0l
2/1/15 10:52:00 PM	Twitter User #5	@LizardLands	LOL
2/1/15 10:52:08 PM	@LizardLands	Twitter User #5	Living above a police station, they'll never swat/raid me l0l
2/1/15 10:52:50 PM	@LizardLands	Twitter User #5	Even if they would trace down my shit, they’d leave the address cuz of that reason ^^
2/1/15 10:52:50 PM	Twitter User #5	@LizardLands	Lmao
2/1/15 10:52:57 PM	@LizardLands	Twitter User #5	they won’t take it serious lol
2/1/15 10:53:12 PM	Twitter User #5	@LizardLands	ik they would think it was a hoax
2/1/15 10:53:37 PM	@LizardLands	Twitter User #5	Yeah but if i look outside my window right now i can see undercover cars etc lmao

95. The Twitter records also reflect the following direct communications by @UchihaLS:

Date/Time (UTC)	**From**	**To**	**Direct Message**
4/15/2015 10:41:06 AM	@UchihaLS	Twitter User #6	[photo sent via direct message – *see Figure 8*]
4/15/2015 10:41:11 AM	@UchihaLS	Twitter User #6	Feds

Figure 8 – April 15, 2015 direct message photo from @UchihaLS



96. Pursuant a mutual legal assistance request from the United States, subscriber records obtained from the Netherlands for the '163 IP address reflect the subscriber is an individual with the last name Van Rooy with a service address listing a residence located in Leiden, the Netherlands ("the Leiden Address").

97. Netherlands authorities have confirmed that the Leiden Address backs up to the parking lot of a police station. I have personally been in the parking lot of

this police station and found it to be the parking lot and building depicted in the above photograph.

98. According to records from Microsoft, collected through subpoena and a search warrant, the lil_jon@hotmail.nl email account was logged into over 400 times from the '163 IP address between November 2014 and November 2015. These records also reflect an email message sent on or about August 2, 2015, from lil_jon@hotmail.nl to lil_jon@hotmail.nl, which contained the photo of a Netherlands passport for Bradley Jan Willem van Rooy. The same email also contained a photo of a bank statement from Rabobank for a bank account ending in account number 4264 with what appears to be an abbreviation of the Leiden Address listed for the account address.

1. Investigation of PayPal Payments to Shenron

99. As previously stated, on or about February 20, 2016, at approximately 1:03 PM PST, @LizardLands tweeted: "PayPal Payments are now being accepted on shenron.lizardsquad.org [**Subject Domain 1**], limited time!"

100. PayPal records for an account associated with the email address uchihals@mail.ru reflected that:

a. The account was registered on or about May 22, 2015, from the '163 IP address, and the account holder is listed as Bradley van Rooy with the Leiden Address listed as an address and an associated bank account at Rabobank with the account number ending in 4264.

b. There were over 400 logins to the account from the '163 IP address between on or about May 22, 2015, and on or about March 4, 2016.

c. The records also reflect a series of login and account administration activity that occurred on or about February 20, 2016, immediately preceding the @LizardLands tweet announcing the acceptance of PayPal payments at 1:03 PM PST. This included an event at 12:46 PM PST in which the '163 IP address was used to remove the Leiden Address from the account.

d. On or about February 20, 2016, at approximately 1:01 PM PST (two minutes prior to the tweet announcing the acceptance of PayPal), there was a $1.00 payment made to the uchihals@mail.ru PayPal account from a PayPal account associated with the email address JackMarrowz@outlook.com. PayPal records for the JackMarrowz@outlook.com account reflect that it was logged into from the '163 IP Address on or about February 20, 2016, at approximately 12:56 PM PST, and the uchihaLS@mail.ru PayPal was logged into from the '163 IP Address on February 20, 2016 at approximately 12:58 PM PST.

e. On or about February 20, 2016, at approximately 1:09 PM PST, a payment of $19.99 was received with a description of "Add funds – 19.99 USD." Between the time of this payment, and on or about March 1, 2016, there were a total of 46 additional payments received with a total value of approximately $1,046. The majority of the payment amounts were observed to be consistent with the prices for the packages listed on the Shenron website.

2. Access to the Shenron Website from '163 IP Address

101. The wiretap data also reflected that the '163 IP Address was used to access the Shenron website and perform a variety of functions, including in part reviewing customer support tickets and purchasing payment cards. The wiretap data reflected that three different user accounts, "support" and "fox," and "dragon," were used by the '163 IP Address. For example:

a. On or about May 24, 2016, at 9:39 PM UTC, the '163 IP Address accessed the Shenron website and logged into the account "dragon" and proceeded to review an already purchased payment card.

b. On or about May 24, 2016, at 9:40 PM UTC, the '163 IP Address accessed the Shenron website and logged into the account "fox" and proceeded to purchase a payment card. The account balance for "fox" was listed as $89,999.

c. On or about May 27, 2016, between 7:58 PM UTC and 8:57 PM UTC, the '163 IP Address accessed the Shenron website using the already logged in account "fox" and proceeded to purchase approximately five payment cards.

d. On or about May 29, 2016, at 2:54 AM UTC, the '163 IP Address accessed the Shenron website using the already logged in "fox" account and proceed to review the current stresser package for this account. The current package was listed as having a twelve-month duration from April 2, 2016 through April 2, 2017 with a cost of $9,999. The listed attack length for the package was 18,000 seconds.

e. On or about June 2, 2016, at 2:15 PM UTC, the '163 IP Address accessed the Shenron website and logged into the account "support" and proceeded to review and respond to open support tickets.

III. SEIZURE OF THE DOMAIN NAMES

A. Statutory Basis

102. Title 18, United States Code, Sections 1030(i)(1)(A) and 1030(j) provides, in relevant part, that any property used, or intended to be used, to commit or facilitate an offense under Title 18, United States Code, Section 1030, is subject to criminal forfeiture to the United States government. Section 1030(i)(2) further provides that the "forfeiture of property under this section, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by [21 U.S.C. § 853], except for subsection (d) of that section."

103. To protect the ability of the United States to exercise its right of forfeiture, Title 21, United States Code, Section 853(e), empowers courts to enter restraining orders and injunctions to preserve the availability of property that is subject to forfeiture under Section 853(a). However, if there is probable cause to believe that the property to be seized is subject to forfeiture and that an order pursuant to Section 853(e) may not be sufficient to assure its availability for forfeiture, a district court may issue a warrant authorizing the seizure of such property. 21 U.S.C. § 853(f). Section 853(f) provides that:

> The Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that

> there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

B. The Subject Domains

104. There exists probable cause that the **Subject Domains** are property used or intended to be used to commit or facilitate violations of Title 18, United States Code, Section 1030(a)(5)(A). Moreover, given the nature of the **Subject Domains** and the fact that they have been used to facilitate ongoing violations of the **Subject Offense** by third parties, neither a restraining order nor an injunction is sufficient to guarantee the availability of the **Subject Domains** for forfeiture and prevent ongoing criminal activity. By seizing and locking the **Subject Domains**, the United States will prevent third parties from using the **Subject Domains** to commit additional crimes.

C. Seizure Procedure

105. Upon execution of the seizure warrants for the **Subject Domains**, Public Interest Registry, the registry for the ".org" top-level domain, shall be directed to restrain and lock the domains or otherwise suspend the **Subject Domains**, pending transfer of all right, title, and interest in the domains to the United States upon completion of forfeiture proceedings, to ensure that changes to those domains cannot be made absent court order or, if forfeited to the United States, without prior consultation by FBI.

IV. CONCLUSION

106. Based on the above information, I respectfully submit that there is probable cause to believe that Zachary Buchta, also known as "pein," "@fbiarelosers," "@xotehpoodle," and "lizard," and Bradley Jan Willem van Rooy, also known as "Uchiha," "@UchihaLS," "dragon," and "fox," have committed the **Subject Offense** and that the **Subject Domains** constitute personal property used or intended to be used to commit or facilitate the **Subject Offense** and are therefore subject to seizure.

FURTHER AFFIANT SAYETH NOT.

E T

Eric T. Brelsford
Special Agent
Federal Bureau of Investigation

Subscribed and sworn
before me on September 23, 2016

Mary M Rowland

Honorable Mary M. Rowland
United States Magistrate Judge