VIRGINIA FUSION CENTER
VIRGINIA STATE POLICE
Phone (804) 674-2196
Fax (804) 674-2983
Terrorism Hotline (877) 4VA-TIPS
VFC@vsp.virginia.gov

*This is LAW ENFORCEMENT SENSITIVE information and is protected by Code of Virginia Title 52-48 and 52-49 unless otherwise noted. **Further distribution of this document outside your organization is prohibited; prior written approval shall be obtained from VFC for dissemination to other agencies.** Persons or organizations violating distribution restrictions may be prosecuted and will be prohibited from receiving future documents. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact the Virginia Fusion Center at (804) 674-2196 if you have any questions or need additional information.*

April 19, 2013
VFC Intelligence Bulletin 13-02

TOR, Bitcoins, Silk Road, and the Hidden Internet

Purpose

The purpose of this bulletin is to provide awareness and a basic understanding of the "Hidden Internet" to investigators in the field, as well as provide some examples of how the Hidden Internet can be exploited by criminal elements.

While the term "Hidden Internet" can be used in a broader context and refer to other internet terms such as the "Deep Web" or "Deepnet," for the purpose of this bulletin the term "Hidden Internet" will refer to the hidden services provided by the TOR project to internet users, specifically relating to the Silk road website and use of Bitcoins.

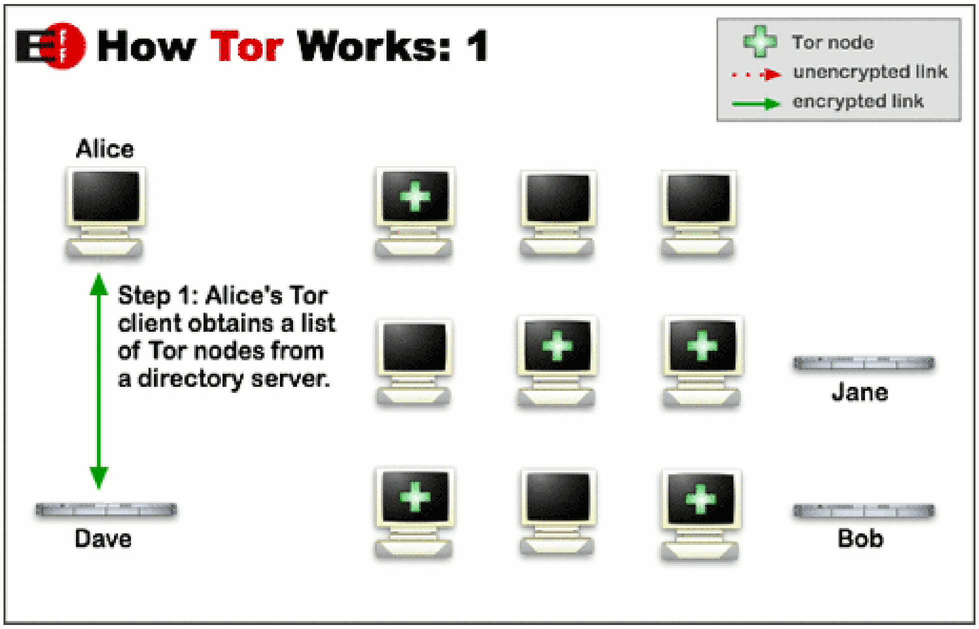
TOR Project

The TOR project was initially designed and implemented as a third generation onion routing project by the United States Naval Research Laboratory. While the inception and design was for the purpose of protecting sensitive communications for the United States Navy, today it is utilized by over 500,000 users every day for both legal and illegal activities.[1]

The TOR project's primary goal is to increase privacy and security for internet users, as stated in their own 2012 Annual Report. This is accomplished through the onion routing system that utilizes TOR volunteers which are used as relays. As users connect through TOR, their data is routed through a series of relays, is encrypted, and as a result does not provide the users location, other identifying information, or original IP address.

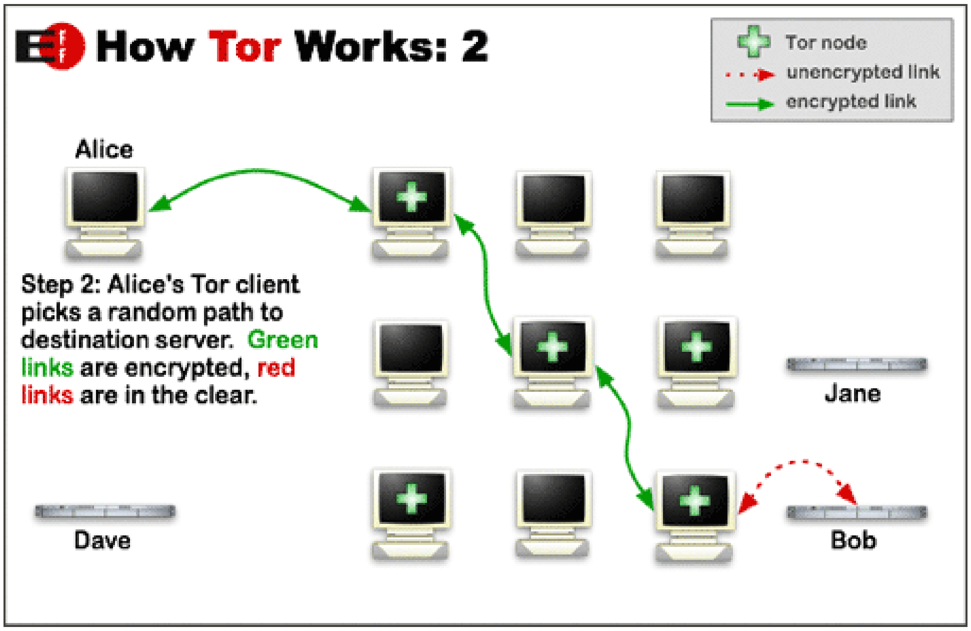
The following diagrams can be seen on the TOR project's website and provide an explanation of how TOR works.

[1] (OS) TOR Project: *Annual Report,* 2012



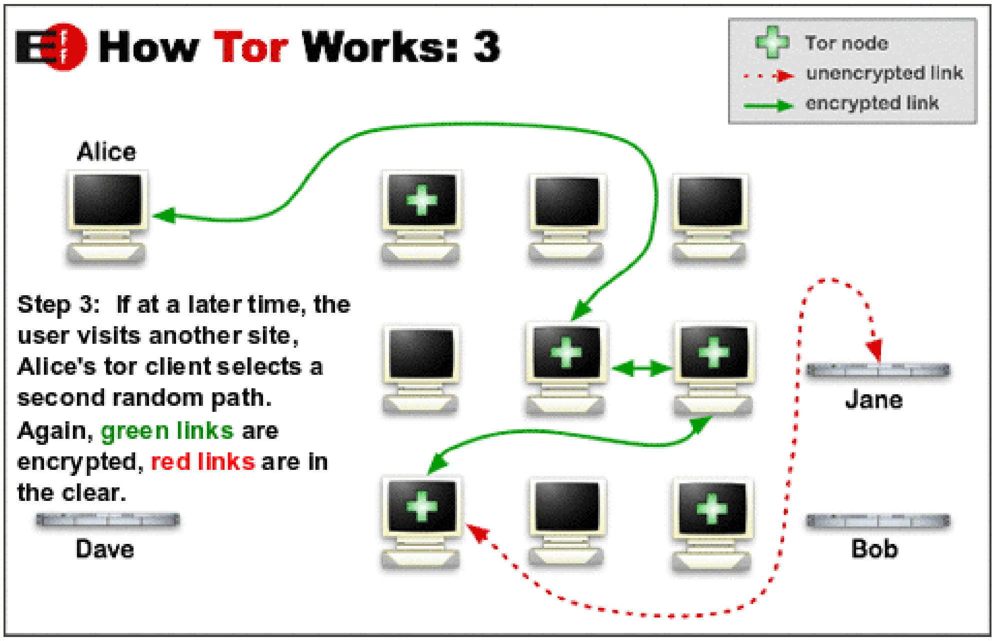
How Tor Works: 1

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.



How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.


How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
Dave
Bob

It is important to note that the use of TOR is not illegal in and of itself. Further, the use of TOR provides a service that can be a useful tool both to individuals personally, for governments, and law enforcement personnel. For example, TOR can provide an investigator a level of anonymity while conducting investigations covertly on the internet, such as attempting to monitor a suspect’s Facebook or Myspace account without the risk of identifying the investigators location or IP address.

If electronic evidence is seized and subsequently searched for digital evidence during an investigation, the discovery of the TOR software on a computer **may** be an indicator that not all of the individual’s internet browsing history will be obtainable through traditional means, i.e. subpoena, to the individual’s internet service provider.

Bitcoins

While TOR provides individuals the ability to remain anonymous on the internet, it would not be possible to establish a cyber black market without the ability to exchange currency. Bitcoins are a virtual currency traded online over peer-to-peer networks allowing both the providing and receiving parties to remain anonymous to one another.

A Bitcoin is "a digital currency, a protocol, and a software that enables; Instant peer to peer transactions, and Worldwide payments[2]" which allows users to conduct online transactions without the use of standard regulated world currencies. For law enforcement, the use of Bitcoins in conjunction with the Hidden Internet, poses a great challenge.

Bitcoins can be purchased several ways, including online exchanges (Mt. Gox being the most common), private companies, or individuals who have Bitcoin holdings already. To begin trading in Bitcoins all a user needs to do is choose a wallet and install it on a computer or smartphone/tablet. Once the user has the wallet they are able to send and receive Bitcoins.

Bitcoins are not regulated or insured by any government or banking system. As such, the use of Bitcoins, the terminology, and execution are extremely technical and will not be covered in this bulletin but the explanations and descriptions are widely available on the Internet.

Since the inception of Bitcoins in 2009 there has been a continuous rise in the usage and total value of Bitcoins in circulation. There are over 50,000 Bitcoin transactions daily equaling millions of U.S. dollars. The total value of all Bitcoins in circulation is over 1.3 billion[3].

As is the case with the use of TOR, the purchase, receipt, and use of Bitcoins is not illegal in and of itself and perfectly legitimate transactions are made such as paying for clothing, hotels, restaurants, and allowing individuals or groups to make anonymous donations[4]. However, with the limited exposure to detection and high potential for profit, the use of TOR and Bitcoins has laid the foundation for the exploitation of these services by criminal elements.

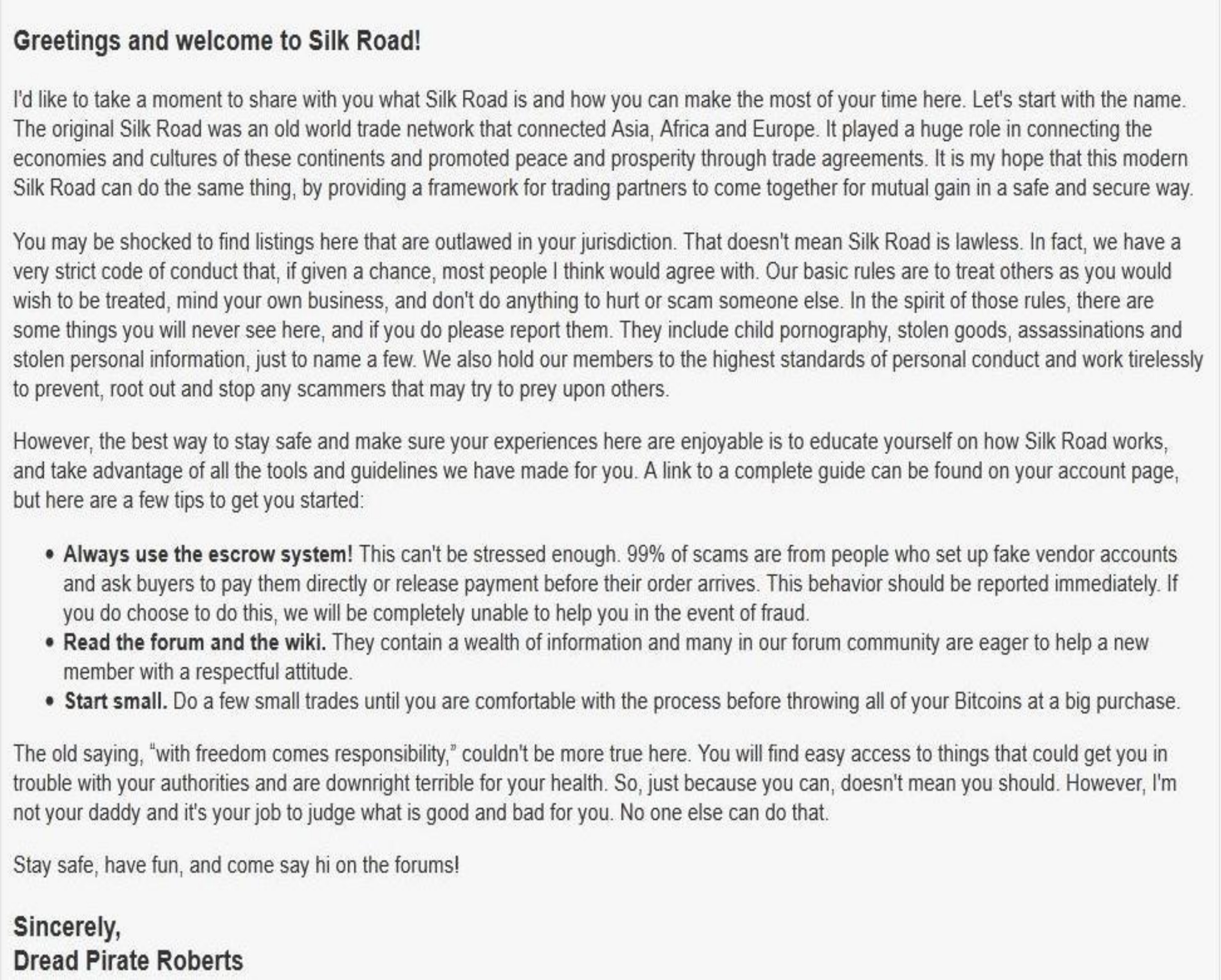
Silk Road

The Silk Road is a hidden website that can only be accessed using TOR or other services (such as Onion.to) that will route through TOR. The hidden net address for The Silk Road Anonymous Marketplace is: http://silkroadv5p5cbl6.onion/.

The Silk Road is the largest, most utilized, and most well-known website dealing in illegal items on the Hidden Internet. The Silk Road is known for the sale and distribution of illegal drugs and substances. The Silk Road's founder/owner is known as "The Dread

[2] (OS) Bitcoin.org: *An open source P2P digital currency,* April 2013
[3] (OS) Bitcoin.org: *About Bitcoin,* April 2013
[4] (OS) Scottish Police College, *Interview, April 3, 2013*

Pirate Roberts," and once into the site he provides an overview of the Silk Road, its history, and its purpose as laid out below:



Greetings and welcome to Silk Road!

I'd like to take a moment to share with you what Silk Road is and how you can make the most of your time here. Let's start with the name. The original Silk Road was an old world trade network that connected Asia, Africa and Europe. It played a huge role in connecting the economies and cultures of these continents and promoted peace and prosperity through trade agreements. It is my hope that this modern Silk Road can do the same thing, by providing a framework for trading partners to come together for mutual gain in a safe and secure way.

You may be shocked to find listings here that are outlawed in your jurisdiction. That doesn't mean Silk Road is lawless. In fact, we have a very strict code of conduct that, if given a chance, most people I think would agree with. Our basic rules are to treat others as you would wish to be treated, mind your own business, and don't do anything to hurt or scam someone else. In the spirit of those rules, there are some things you will never see here, and if you do please report them. They include child pornography, stolen goods, assassinations and stolen personal information, just to name a few. We also hold our members to the highest standards of personal conduct and work tirelessly to prevent, root out and stop any scammers that may try to prey upon others.

However, the best way to stay safe and make sure your experiences here are enjoyable is to educate yourself on how Silk Road works, and take advantage of all the tools and guidelines we have made for you. A link to a complete guide can be found on your account page, but here are a few tips to get you started:

- **Always use the escrow system!** This can't be stressed enough. 99% of scams are from people who set up fake vendor accounts and ask buyers to pay them directly or release payment before their order arrives. This behavior should be reported immediately. If you do choose to do this, we will be completely unable to help you in the event of fraud.
- **Read the forum and the wiki.** They contain a wealth of information and many in our forum community are eager to help a new member with a respectful attitude.
- **Start small.** Do a few small trades until you are comfortable with the process before throwing all of your Bitcoins at a big purchase.

The old saying, "with freedom comes responsibility," couldn't be more true here. You will find easy access to things that could get you in trouble with your authorities and are downright terrible for your health. So, just because you can, doesn't mean you should. However, I'm not your daddy and it's your job to judge what is good and bad for you. No one else can do that.

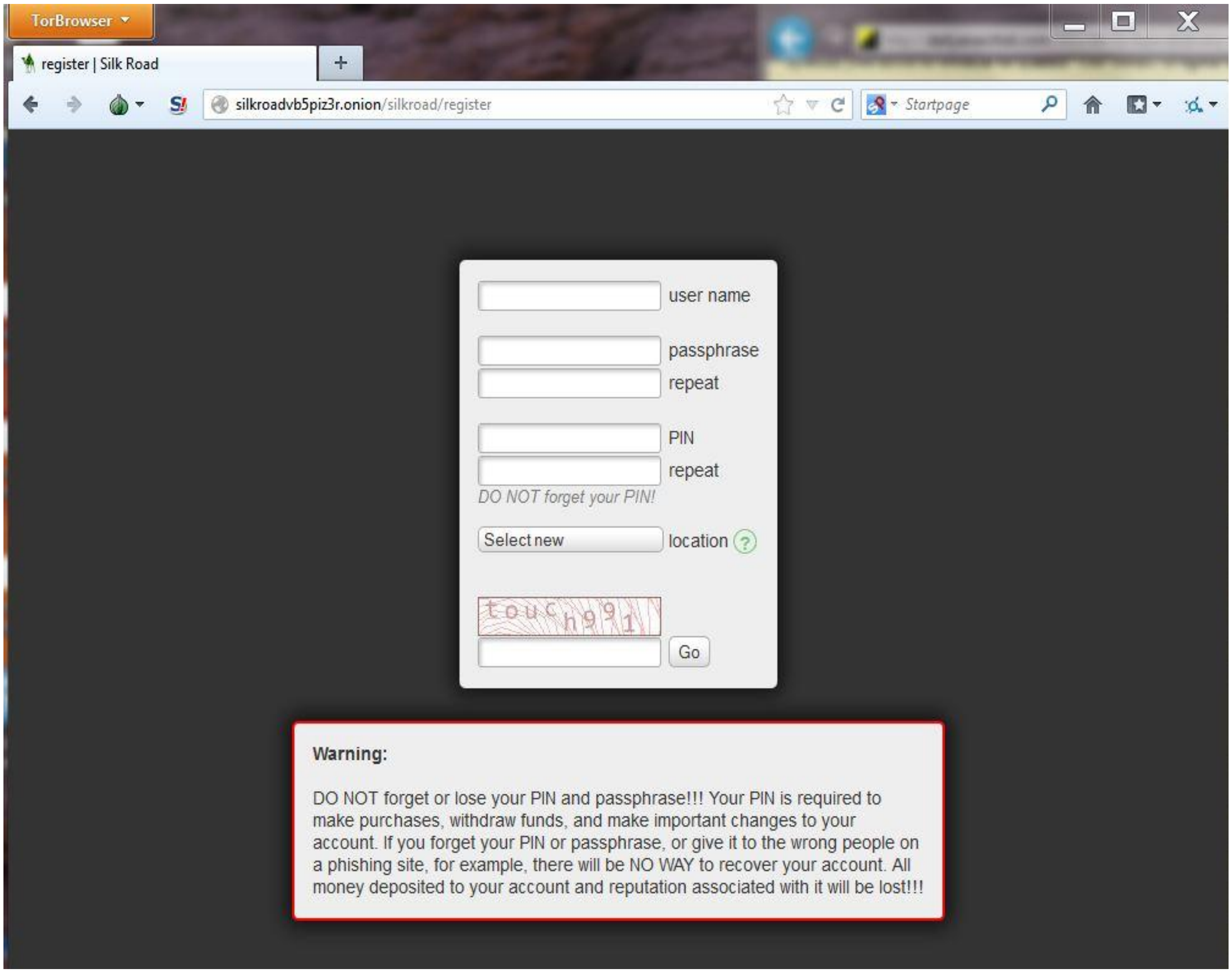
Stay safe, have fun, and come say hi on the forums!

Sincerely,
Dread Pirate Roberts

For the purposes of this bulletin, the Virginia Fusion Center (VFC) established, through the use of TOR, a Silk Road account. The following are screen shots of the site from initial logon, to browsing. For any individual who is comfortable with the internet the entire process can take only minutes.

The following screenshots show the initial account set up screen, login screen, as well as browsing screen shots of items that could be purchased from the site. For the purposes of this bulletin, a covert screen name was utilized. The screenshots are simply samples of the items listed on the site, and in no way are all inclusive.

Screenshot 1: Registration/Account set up



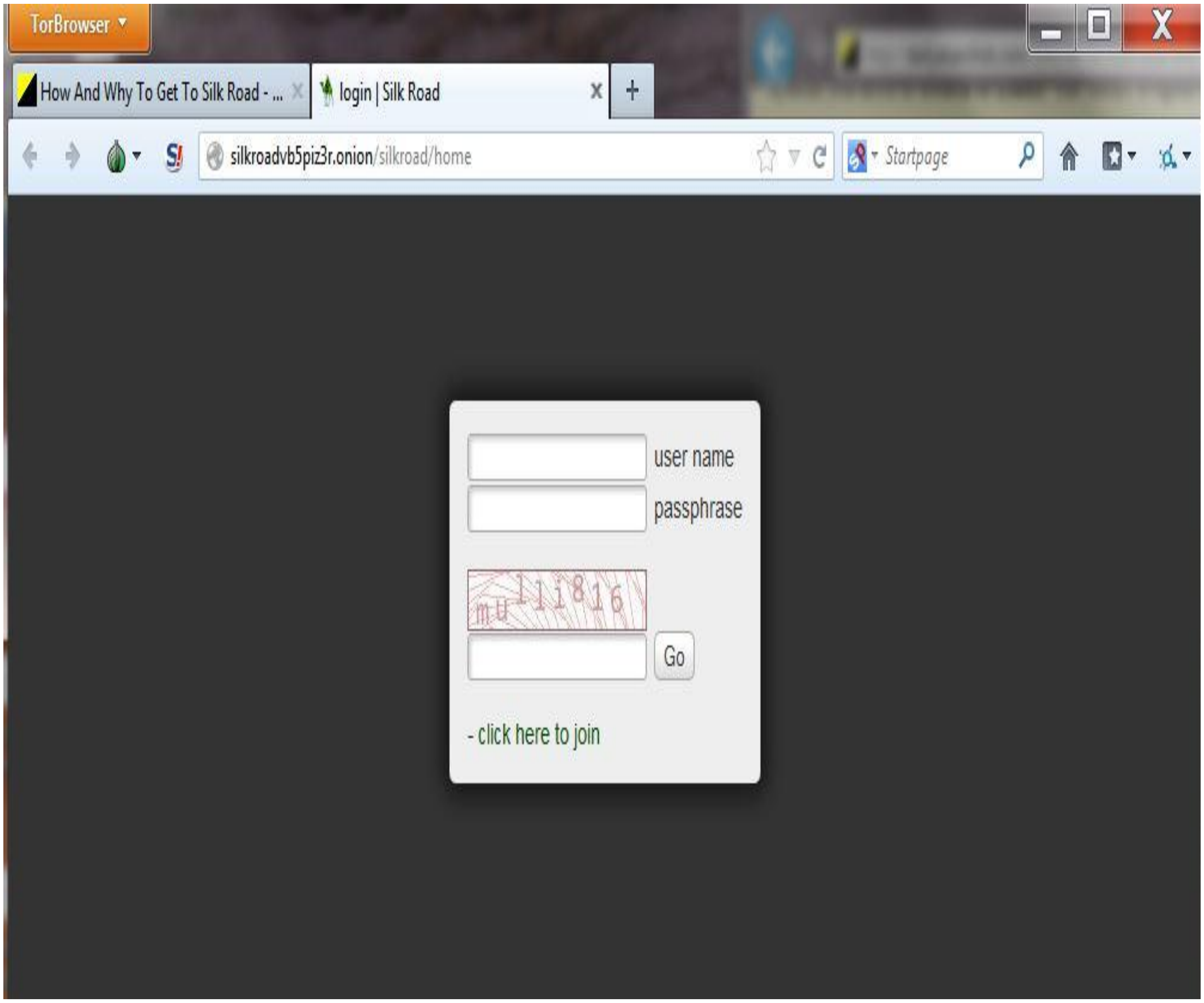
DO NOT forget your PIN!

Select new location

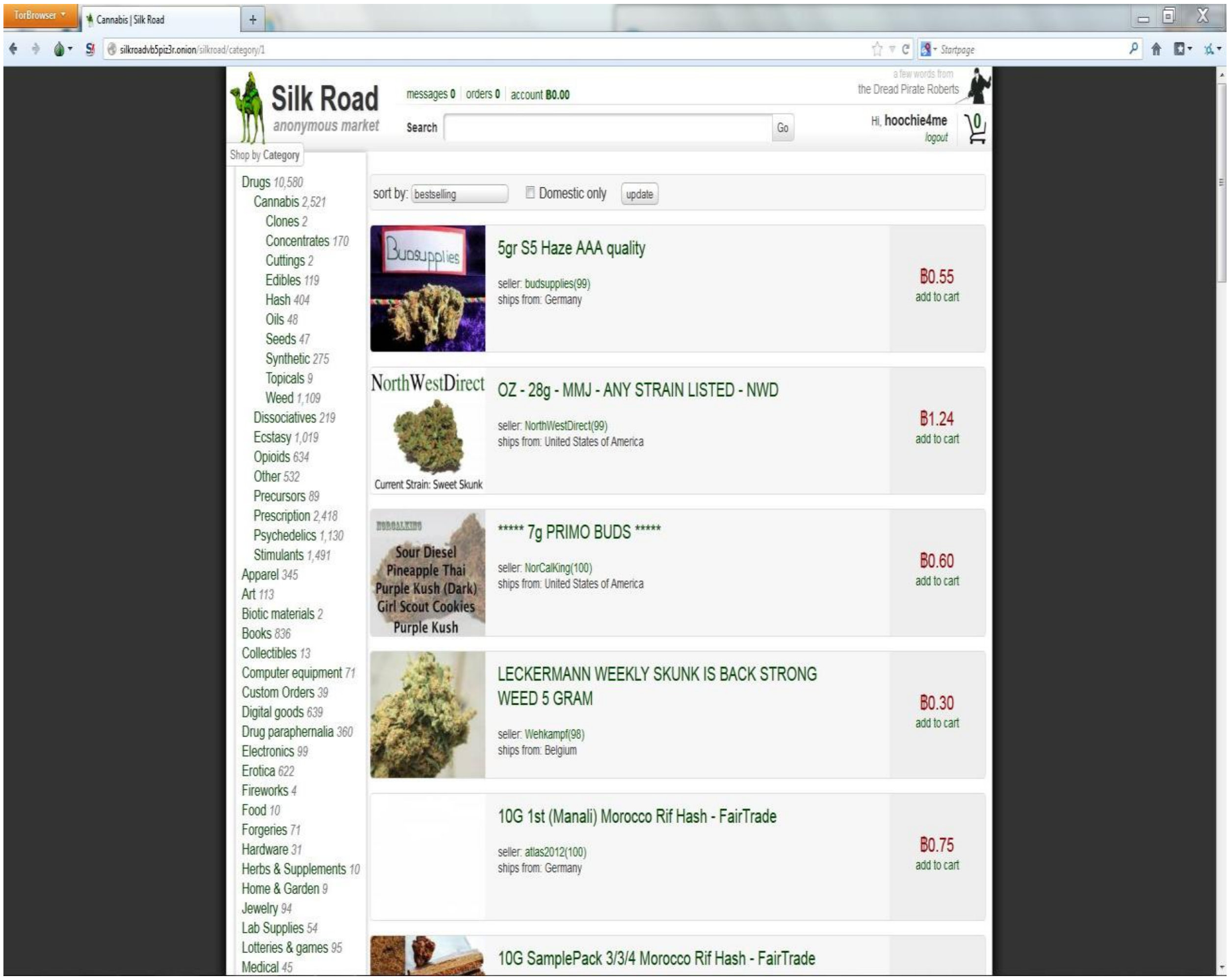
Warning:

DO NOT forget or lose your PIN and passphrase!!! Your PIN is required to make purchases, withdraw funds, and make important changes to your account. If you forget your PIN or passphrase, or give it to the wrong people on a phishing site, for example, there will be NO WAY to recover your account. All money deposited to your account and reputation associated with it will be lost!!!

Screenshot 2: Initial login/user password



Screenshot 3: Marijuana/Cannabis Listings



sort by: bestselling □ Domestic only

- Drugs 10,580
  - Cannabis 2,521
    - Clones 2
    - Concentrates 170
    - Cuttings 2
    - Edibles 119
    - Hash 404
    - Oils 48
    - Seeds 47
    - Synthetic 275
    - Topicals 9
    - Weed 1,109
  - Dissociatives 219
  - Ecstasy 1,019
  - Opioids 634
  - Other 532
  - Precursors 89
  - Prescription 2,418
  - Psychedelics 1,130
  - Stimulants 1,491
- Apparel 345
- Art 113
- Biotic materials 2
- Books 836
- Collectibles 13
- Computer equipment 71
- Custom Orders 39
- Digital goods 639
- Drug paraphernalia 360
- Electronics 99
- Erotica 622
- Fireworks 4
- Food 10
- Forgeries 71
- Hardware 31
- Herbs & Supplements 10
- Home & Garden 9
- Jewelry 94
- Lab Supplies 54
- Lotteries & games 95
- Medical 45

Budsupplies

5gr S5 Haze AAA quality

seller: budsupplies(99)
ships from: Germany

B0.55
add to cart

NorthWestDirect
Current Strain: Sweet Skunk

OZ - 28g - MMJ - ANY STRAIN LISTED - NWD

seller: NorthWestDirect(99)
ships from: United States of America

B1.24
add to cart

NORCALKING
Sour Diesel
Pineapple Thai
Purple Kush (Dark)
Girl Scout Cookies
Purple Kush

***** 7g PRIMO BUDS *****

seller: NorCalKing(100)
ships from: United States of America

B0.60
add to cart

LECKERMANN WEEKLY SKUNK IS BACK STRONG WEED 5 GRAM

seller: Wehkampf(98)
ships from: Belgium

B0.30
add to cart

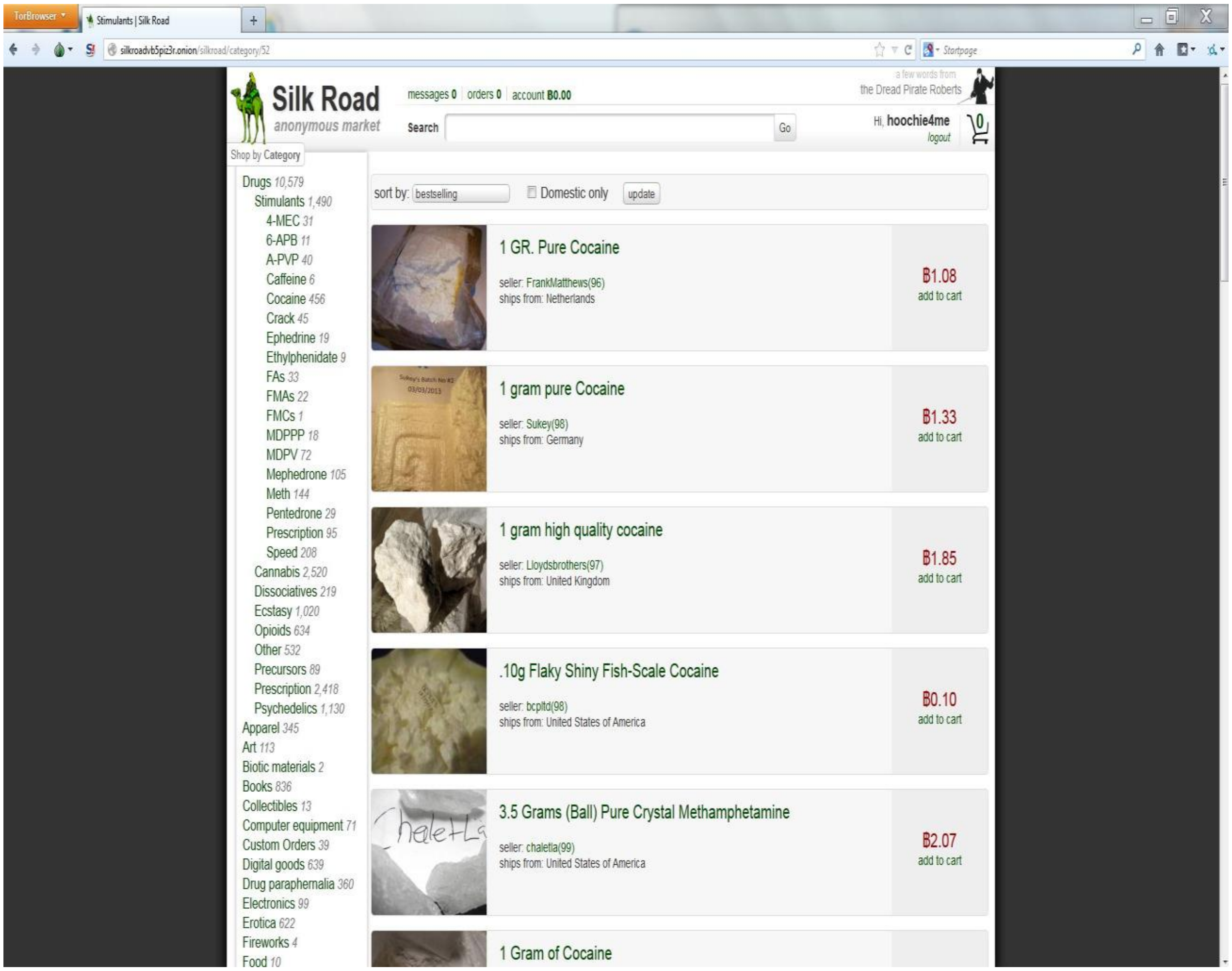
10G 1st (Manali) Morocco Rif Hash - FairTrade

seller: atlas2012(100)
ships from: Germany

B0.75
add to cart

10G SamplePack 3/3/4 Morocco Rif Hash - FairTrade

Screenshot 4: Stimulants/Cocaine Listings



- Drugs 10,579
  - Stimulants 1,490
    - 4-MEC 31
    - 6-APB 11
    - A-PVP 40
    - Caffeine 6
    - Cocaine 456
    - Crack 45
    - Ephedrine 19
    - Ethylphenidate 9
    - FAs 33
    - FMAs 22
    - FMCs 1
    - MDPPP 18
    - MDPV 72
    - Mephedrone 105
    - Meth 144
    - Pentedrone 29
    - Prescription 95
    - Speed 208
  - Cannabis 2,520
  - Dissociatives 219
  - Ecstasy 1,020
  - Opioids 634
  - Other 532
  - Precursors 89
  - Prescription 2,418
  - Psychedelics 1,130
- Apparel 345
- Art 113
- Biotic materials 2
- Books 836
- Collectibles 13
- Computer equipment 71
- Custom Orders 39
- Digital goods 639
- Drug paraphernalia 360
- Electronics 99
- Erotica 622
- Fireworks 4
- Food 10

1 GR. Pure Cocaine
seller: FrankMatthews(96)
ships from: Netherlands
฿1.08
add to cart

1 gram pure Cocaine
seller: Sukey(98)
ships from: Germany
฿1.33
add to cart

1 gram high quality cocaine
seller: Lloydsbrothers(97)
ships from: United Kingdom
฿1.85
add to cart

.10g Flaky Shiny Fish-Scale Cocaine
seller: bcpltd(98)
ships from: United States of America
฿0.10
add to cart

3.5 Grams (Ball) Pure Crystal Methamphetamine
seller: chaletia(99)
ships from: United States of America
฿2.07
add to cart

1 Gram of Cocaine

Note: All listings are in Bitcoins only

With the launch of the Silk Road website in 2011, use has increased. By some accounts, it is believed that the Silk Road conducts approximately $2,000,000 per month in transactions believed to net “The Dread Pirate Roberts” approximately $140,000 per month, all in Bitcoins.

While the Silk Road is believed to be the largest and most well-known of the hidden sites, there are others such as “Black Market Reloaded”, “Deep Web Weapons”, “Gun Guys Den”, and “Behind Bloodshot Eyes”, amongst others.

VIRGINIA FUSION CENTER
VIRGINIA STATE POLICE
Phone (804) 674-2196
Fax (804) 674-2983
Terrorism Hotline (877) 4VA-TIPS
VFC@vsp.virginia.gov

Conclusion
The VFC believes this will be an escalating challenge for law enforcement as awareness in the general public increases about these services. The VFC will continue to analyze and attempt to identify the impact of the hidden internet and its services in Virginia. It is requested that any information related to the TOR, use of Bitcoins, and the Silk Road or other hidden internet sites that are seen as a result of investigations or official duties be forwarded to the Virginia Fusion Center at vfc@vsp.virginia.gov.

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu