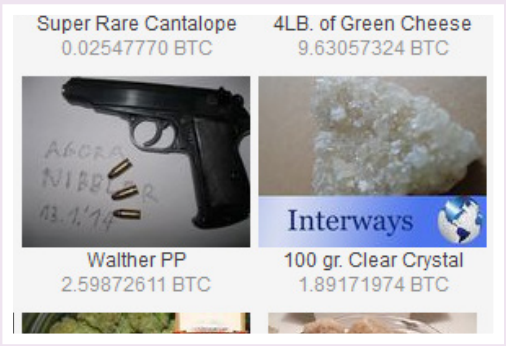
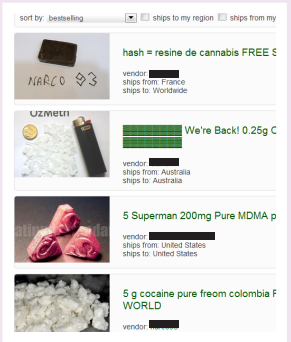
digitalcitizens alliance

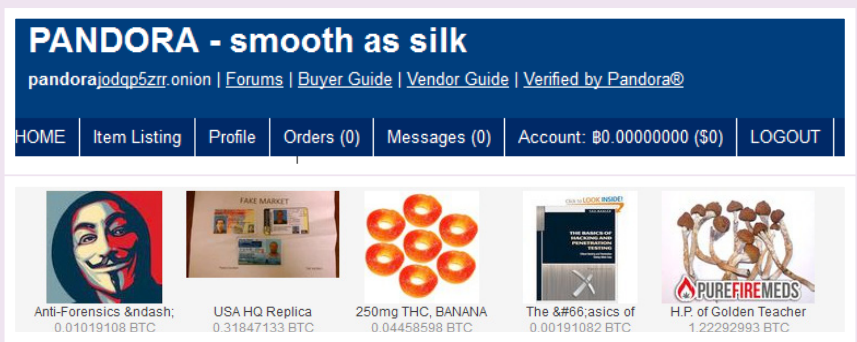
BUSTED, BUT NOT BROKEN

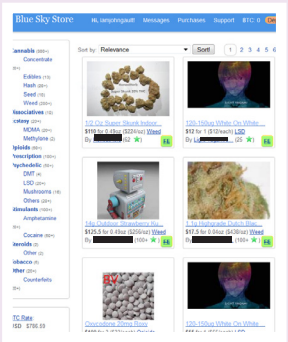
THE STATE OF SILK ROAD AND THE DARKNET MARKETPLACES

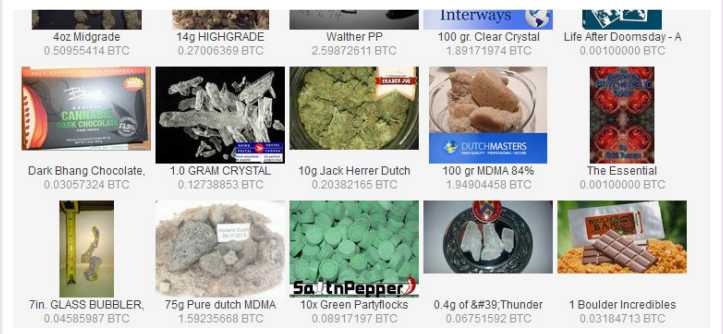
A DIGITAL CITIZENS ALLIANCE INVESTIGATIVE REPORT

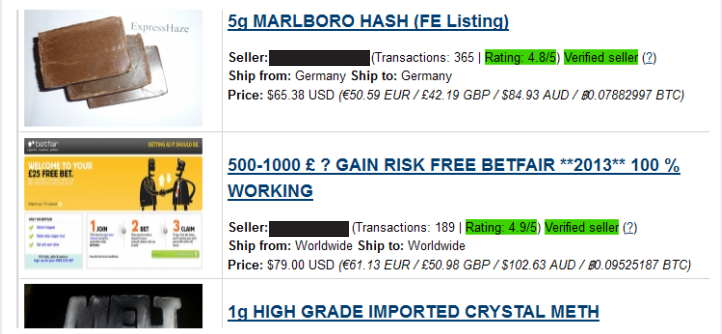


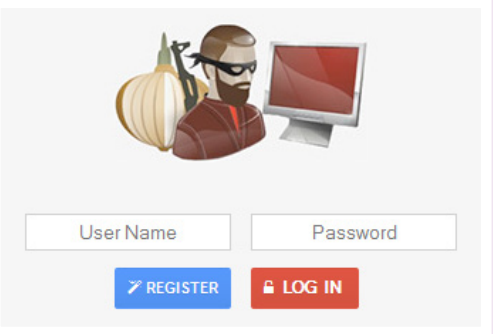












Ten months ago, the Digital Citizens Alliance began researching illicit online marketplaces, including Silk Road (pre- and post-arrest of Ross Ulbricht, accused of being Silk Road's notorious operator "Dread Pirate Roberts"). This report details the findings of Digital Citizens researchers, including the following key takeaways:

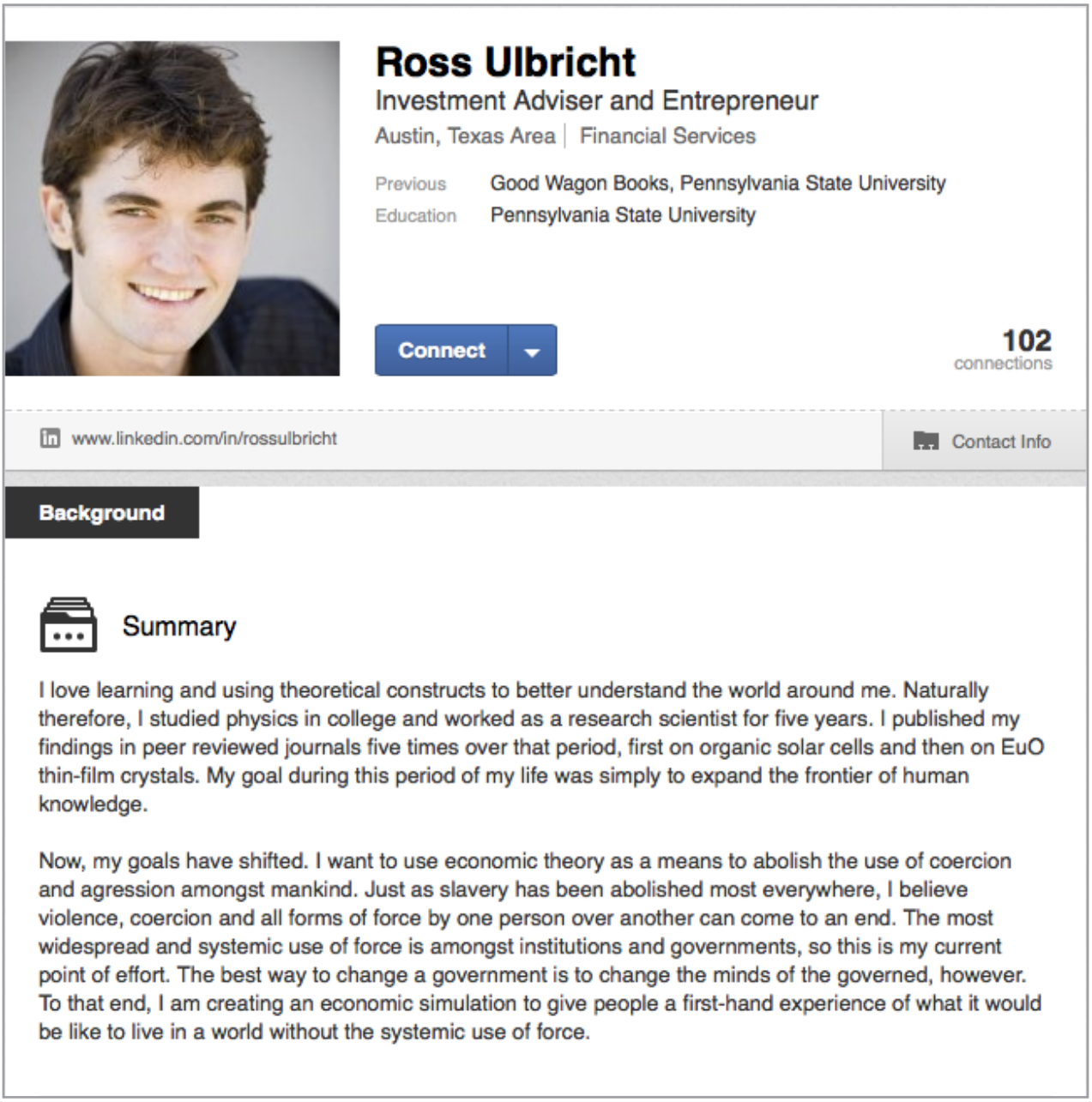
Key takeaways:

- Approximately 13,648 listings for drugs are now available on Silk Road compared to the 13,000 that were listed shortly before the FBI arrested Ulbricht and shut down the site. In comparison, Silk Road's closest competitor, Agora, has just roughly 7,400 drug listings.
- There is significantly more competition today than when the original Silk Road was seized. Silk Road 2.0 currently contains 5% more listings for drugs than its predecessor held at the time of its seizure. By comparison, the Darknet drug economy as a whole contains 75% more listings for drugs.
- Silk Road and other Darknet marketplaces continue to do steady business despite the arrests of additional alleged operators who authorities say worked for Ulbricht.
- A series of scam markets, which appeared as opportunists tried to fill the void while the original Silk Road was shut down, created distrust among customers after the operators allegedly stole tens of millions of dollars worth of bitcoin. It is speculated that the resulting distrust may be one of the factors helping Silk Road rebuild its user base so quickly.
- In chat rooms used by both operators and customers, many believe that the fallout from Ulbricht's arrest is complete. Some, who claim to be informed insiders, say that Ulbricht has surrendered as much information as he has to offer. These same individuals believe Ulbricht's information led to three high profile arrests earlier this year.
- Silk Road operators have turned a February hack, in which hundreds of thousands of bitcoins were stolen, from a crisis to an opportunity. The operators devised a plan to get bitcoins back to many customers hit in the heist. This has helped Silk Road reaffirm that it is not like the scam markets that failed customers earlier.

On October 2, 2013 law enforcement arrested the infamous "Dread Pirate Roberts," (DPR) the elusive creator and proprietor of the defunct anonymous online black market, the Silk Road (SR), who had evaded their grasp since 2011. Ross Ulbricht, a 29-year-old former engineering student from Texas, now stands accused of creating the largest, most sophisticated criminal enterprise the Internet has ever seen. An enterprise that was the platform for sales of illicit drugs, hacking wares, stolen content, forged documents, and any other illicit item a criminal could want with the exception of weapons and child pornography.

Silk Road was by far the largest and most well known online black market before its seizure. However, it was not the only one of its kind. Former, less successful competitors of DPR, were ready to reap the benefits of SR's demise and welcomed its vendors and customers with open arms. The events that have transpired since the FBI closed in on Ulbricht inside a public library in San Francisco are the focus of this report.

After months of tracking these illicit websites and their discussion boards, Digital Citizens researchers have found the online black market economy has done a complete somersault in the six months since the fall of the original Silk Road. As we will illustrate below, those competitors who initially capitalized on the fall of DPR are all gone. New players have arisen, including a second incarnation of "Dread Pirate Roberts" and a revived Silk Road (which seems to be thriving, even after law enforcement arrested and charged some of the new site's prominent figures) has replaced the original. Competition is fierce in the world of online black markets (or "Darknet Marketplaces"), and their operators give new meaning to the phrase "there is no honor among thieves." Several markets scammed their users out of millions of dollars' worth of bitcoin, which has led to a threat perhaps even greater than law enforcement: a crisis of confidence in the trustworthiness of markets, which serve as the foundation of these criminal enterprises.



Source: LinkedIn

AN ONLINE BLACK MARKET: THE BASICS

Wikipedia defines "Darknet" this way:

> *"A darknet is an anonymizing network where connections are made only between trusted peers — sometimes called "friends" (F2F)— using non-standard protocols and ports.*
>
> *"Darknets are distinct from other distributed peer-to-peer networks as sharing is anonymous (that is, IP addresses are not publicly shared), and therefore users can communicate with little fear of governmental or corporate interference.*
>
> *"For this reason, Darknets are often associated with dissident political communications and illegal activities."*[1]

Others have referred to this world as the "Deep Web" or "Dark Web."

Before discussing the recent evolution of the Darknet Marketplaces, there is background information that readers new to this world should examine. Based on our research there are three basic building blocks (outside of more advanced security protocols) that enable these Marketplaces to operate and their users to remain anonymous as they buy and sell illicit goods. They are: the Tor Network, bitcoin, and the discussion forums that are maintained by each individual market.

THE ONION ROUTER (TOR NETWORK)

We accessed Silk Road by using the Tor Network Hidden Services, which through its system of relays and nodes bounces its users from relays around the world - making a unique, and nearly impossible to trace, path. Tor, which is used by many people for socially beneficial reasons (more on that in a moment), is also the best-known pathway to the Darknet. Tor is the tool of choice for those who wish to browse the Internet anonymously for purposes both legitimate and, in this case, illegitimate. The term Tor itself can have several meanings and they are as follows:

- Tor refers to the open source software you can download for free that allows you to use the Internet anonymously.
- Tor also refers to the volunteer network of computers that makes it possible for that software to work. Each of these volunteer computers is referred to as a node or relay. There are currently an estimated 4,000 volunteers that comprise the Tor Network.[2] When you visit a site on Tor you are redirected through several of the nodes until you reach your destination. Your IP address is now that of the exit node rather than your original IP address, thus protecting your anonymity.
- Tor has become a sort of shorthand for the Darknet (this despite the fact that Tor is technology, while the Darknet is more of a concept). Tor's Hidden Services let users publish web sites and other services without needing to reveal the location of the site.[3] These services and sites, like SR, are not accessible through the regular Internet (AKA the Open Net), but through the use of Tor software.

Online black markets use a combination of these elements of Tor (as well as encryption software for email like PGP, code names, fictitious identities, emails from virtual privacy networks (VPNs), or anonymous mail drops) to maintain their users' anonymity. Buyers and vendors download the Tor software and then access the Tor Network in order to visit SR or one of its competitors. All of these sites were created using Tor's Hidden Services. These services hide the sites location, providing protection from law enforcement to those who create and operate the site. (For an in-depth look at Tor Hidden Services and areas where

[1] http://en.wikipedia.org/wiki/Darknet_(file_sharing)
[2] https://www.eff.org/torchallenge/what-is-tor
[3] https://www.torproject.org/about/overview.html.en

further development is expected, read the Tor Project blog post "Hidden Services, Current Events, and Freedom Hosting.")

The Tor Project's Kelley Misata told Digital Citizens' researchers: "Tor is a tool used by a wide-range of people for completely reasonable purposes. Domestic violence victims, journalists, and law enforcement use Tor any time they need some protection. But this privacy should be for everyone; it should be something all Internet users consider proactively and not just after something bad happens. Sometimes it is too late to consider your security after the fact."

BITCOIN

Silk Road operators adopted bitcoin, the decentralized, semi-anonymous digital currency, as its means of payment processing very early in its history (and without any formal blessing from bitcoin in return). Many Darknet Marketplaces and vendors view bitcoin as the perfect currency for their business. Its value is not tied to any fiat currency or backed by a bank, but maintained by a peer-to-peer network of thousands of users who run the software on their computers. Users who take the proper precautions never have to tie their bitcoins to their real identity.[4] Additionally, black markets do not have to worry about their accounts being cancelled like many rogue sites on the Open Net have by payment processors like Visa and PayPal.

Bitcoin is not completely anonymous. Every confirmed transaction is included in the bitcoin block chain. The block chain is a shared public ledger on which the entire bitcoin network relies. The block chain specifies which wallets (an individual's account) are sending and receiving the bitcoin.[5] Therefore if law enforcement knows the identity of a wallet's owner that is receiving or making payment for illegal goods, they can track down that individual once he converts his coins into fiat currency. There are, of course, services that exist to ensure complete anonymity.

Digital forms of money laundering have been created such as Bitcoin Fog. Bitcoin Fog pools the coins of a group of users together and then pays out to each member different coins from the pool.[6] At that point the link to any one specific transaction that could be used to identify an individual is eliminated. Some black markets run one automatically for each transaction ensuring anonymity and peace of mind for their customers.[7] *For more information on bitcoin, including its incredible rise in value after the arrest of DPR and the evolving view on its usefulness to criminals, please see page 10.*

BLACK MARKET DISCUSSION FORUMS

The third important trait that all anonymous online black markets have in common is the discussion forum. The forums serve multiple critical functions for all parties involved in the black market ecosystem and the last six months have certainly illustrated this point. First, they serve as the marketing, advertising, and customer service arm of the site where buyers and vendors can give and/or receive useful information. Second, in the forums black market operators and moderators (mods) such as DPR communicate with the community.

The amount of information that can be found on these forums is staggering. Categories that can be browsed include: security, legal, Silk Road discussion, customer report, product offerings, and bug reporting, among others. Vendors advertise their products and buyers report on scammers to make sure no one else falls victim and that the scammer is, ironically, black listed. Much like any site on the Open Net, there are plenty of trolls and spam to be had. These are basic functions that help to better the user experience on the markets and offer regular users the opportunity to interact with DPR and the other important mods.[8]

[4] http://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/
[5] http://bitcoin.org/en/how-it-works
[6] http://www.bitcoinfog.com/
[7] http://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/
[8] http://silkroad5v7dywlc.onion/index.php?topic=645.0

The discussion forums give users the ability to interact with those operating the site. Here Global Moderator "V" discusses what The Silk Road means to each of its users.

There are many buyers and sellers who visit anonymous marketplaces for no other reason than to buy drugs to get high or sell them for a profit. However, those who interact on forums such as SR's are diehards banded together by a likeminded libertarian "cause" that SR and its competitors are a protest against an authoritarian government that has no right to dictate what they put into their bodies. DPR and other operators use(d) the forums to foster that sense of community and strengthen it. Their effectiveness was no more apparent than when SR was seized and DPR arrested. Because the forum was on a different, undiscovered server it remained operational. Vendors were able to communicate where they were now selling, mods were able to keep up morale,[9] and instead of crumbling the community rallied.

SIX MONTHS OF PAIN AND GAIN FOR DARKNET MARKETS

A WALK DOWN MEMORY LANE

Before the arrest of DPR and the seizure of Silk Road, the Darknet drug trade was more centralized and certainly less publicized. As of late September, there were three major players: Silk Road, Black Market Reloaded (BMR), and Atlantis. The following points show an abbreviated explanation of the fate of this first wave of online markets:

- The Silk Road was widely acknowledged as the industry leader (See figure below) while BMR carved out a solid niche with its "anything goes" (including weapons) mentality and Atlantis gained attention with an aggressive marketing campaign.[10]
- In late September, the owners of Atlantis, Vladimir and Loera, closed the site due to unspecified "security concerns." The owners closed the site before users could retrieve all of their bitcoins, which led even diehard users to label it a scam.[11]

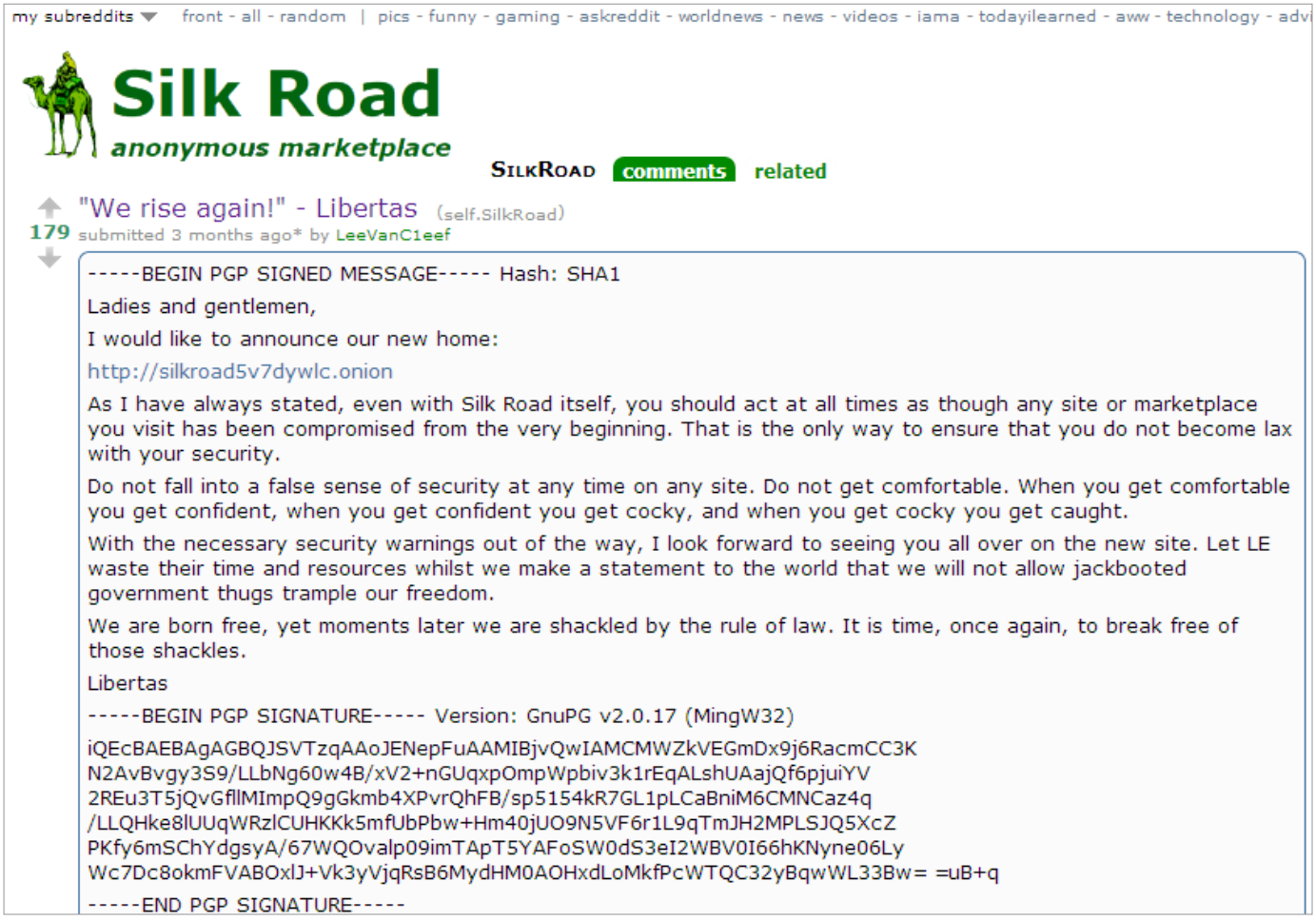
[9] http://gawker.com/a-silk-road-employees-tearful-goodbye-1440864705
[10] http://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/
[11] http://allthingsvice.com/2013/09/26/the-fall-of-atlantis-a-moderator-tells/#more-461

- With Atlantis gone, SR and BMR were unquestionably the two best-known entities for drugs and criminal wares. Less than a week later after SR was seized, BMR was the largest Darknet Marketplace left standing.
- Operated by an individual under the name "Backcopy," BMR had a reputation for scammers and interface many considered to be difficult to use.[12] Many looking for an alternative found a home with a lesser-known market called Sheep Marketplace.
- Within two weeks of Ulbricht's arrest, the sites experienced serious growth. BMR saw the number of drug listings rise from 3,075 to 5,104, representing a 70% increase, while Sheep Marketplace showed explosive growth with the number of drug listings increasing from 855 to 4,165-an almost 400% increase.[13]

For more details on the types of drugs on Silk Road and their availability after the seizure please see the Appendix on page 25.

SILK ROAD 2.0 AND THE NEW DPR

As BMR and Sheep Marketplace moved quickly to secure the business of SR vendors and customers, SR's former "mods" and "admins" were working just as diligently. Within a week of the arrest of Ross Ulbricht, former SR moderator Libertas made the following post on the original Silk Road Forums announcing their new forum home (Reddit version shown here):



my subreddits ▾ front - all - random | pics - funny - gaming - askreddit - worldnews - news - videos - iama - todayilearned - aww - technology - adv

Silk Road
anonymous marketplace

SILKROAD comments related

"We rise again!" - Libertas (self.SilkRoad)
179 submitted 3 months ago* by LeeVanC1eef

-----BEGIN PGP SIGNED MESSAGE----- Hash: SHA1

Ladies and gentlemen,

I would like to announce our new home:

http://silkroad5v7dywlc.onion

As I have always stated, even with Silk Road itself, you should act at all times as though any site or marketplace you visit has been compromised from the very beginning. That is the only way to ensure that you do not become lax with your security.

Do not fall into a false sense of security at any time on any site. Do not get comfortable. When you get comfortable you get confident, when you get confident you get cocky, and when you get cocky you get caught.

With the necessary security warnings out of the way, I look forward to seeing you all over on the new site. Let LE waste their time and resources whilst we make a statement to the world that we will not allow jackbooted government thugs trample our freedom.

We are born free, yet moments later we are shackled by the rule of law. It is time, once again, to break free of those shackles.

Libertas

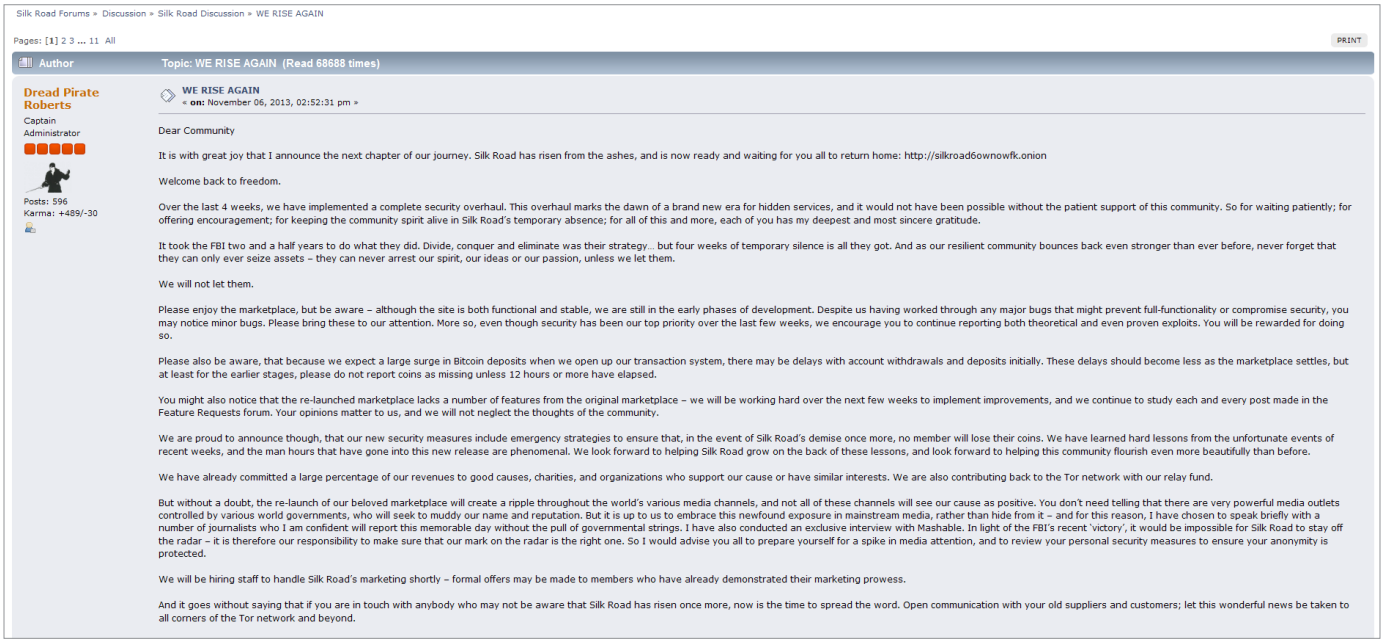
-----BEGIN PGP SIGNATURE----- Version: GnuPG v2.0.17 (MingW32)

iQEcBAEBAgAGBQJSVTzqAAoJENepFuAAMIBjvQwIAMCMWZkVEGmDx9j6RacmCC3K
N2AvBvgy3S9/LLbNg60w4B/xV2+nGUqxpOmpWpbiv3k1rEqALshUAajQf6pjuiYV
2REu3T5jQvGfllMImpQ9gGkmb4XPvrQhFB/sp5154kR7GL1pLCaBniM6CMNCaz4q
/LLQHke8lUUqWRzlCUHKKk5mfUbPbw+Hm40jUO9N5VF6r1L9qTmJH2MPLSJQ5XcZ
PKfy6mSChYdgsyA/67WQOvalp09imTApT5YAFoSW0dS3eI2WBV0I66hKNyne06Ly
Wc7Dc8okmFVABOxlJ+Vk3yVjqRsB6MydHM0AOHxdLoMkfPcWTQC32yBqwWL33Bw= =uB+q

-----END PGP SIGNATURE-----

[12] http://webcache.googleusercontent.com/search?q=cache:Y7ihm-TWt-kJ:atlantisblog.org/191/+&cd=3&hl=en&ct=clnk&gl=us
[13] Id.

The rumors of a new Silk Road started and were confirmed by the new Dread Pirate Roberts. On November 6, just 34 days after the arrest of Ross Ulbricht and the seizure of SR, the new DPR announced Silk Road 2.0 was open for business:


Silk Road Forums » Discussion » Silk Road Discussion » WE RISE AGAIN

Pages: [1] 2 3 ... 11 All

PRINT

Author | Topic: WE RISE AGAIN (Read 68688 times)

Dread Pirate Roberts
Captain
Administrator
Posts: 596
Karma: +489/-30

WE RISE AGAIN
« on: November 06, 2013, 02:52:31 pm »

Dear Community

It is with great joy that I announce the next chapter of our journey. Silk Road has risen from the ashes, and is now ready and waiting for you all to return home: http://silkroad6ownowfk.onion

Welcome back to freedom.

Over the last 4 weeks, we have implemented a complete security overhaul. This overhaul marks the dawn of a brand new era for hidden services, and it would not have been possible without the patient support of this community. So for waiting patiently; for offering encouragement; for keeping the community spirit alive in Silk Road's temporary absence; for all of this and more, each of you has my deepest and most sincere gratitude.

It took the FBI two and a half years to do what they did. Divide, conquer and eliminate was their strategy.. but four weeks of temporary silence is all they got. And as our resilient community bounces back even stronger than ever before, never forget that they can only ever seize assets – they can never arrest our spirit, our ideas or our passion, unless we let them.

We will not let them.

Please enjoy the marketplace, but be aware – although the site is both functional and stable, we are still in the early phases of development. Despite us having worked through any major bugs that might prevent full-functionality or compromise security, you may notice minor bugs. Please bring these to our attention. More so, even though security has been our top priority over the last few weeks, we encourage you to continue reporting both theoretical and even proven exploits. You will be rewarded for doing so.

Please also be aware, that because we expect a large surge in Bitcoin deposits when we open up our transaction system, there may be delays with account withdrawals and deposits initially. These delays should become less as the marketplace settles, but at least for the earlier stages, please do not report coins as missing unless 12 hours or more have elapsed.

You might also notice that the re-launched marketplace lacks a number of features from the original marketplace – we will be working hard over the next few weeks to implement improvements, and we continue to study each and every post made in the Feature Requests forum. Your opinions matter to us, and we will not neglect the thoughts of the community.

We are proud to announce though, that our new security measures include emergency strategies to ensure that, in the event of Silk Road's demise once more, no member will lose their coins. We have learned hard lessons from the unfortunate events of recent weeks, and the man hours that have gone into this new release are phenomenal. We look forward to helping Silk Road grow on the back of these lessons, and look forward to helping this community flourish even more beautifully than before.

We have already committed a large percentage of our revenues to good causes, charities, and organizations who support our cause or have similar interests. We are also contributing back to the Tor network with our relay fund.

But without a doubt, the re-launch of our beloved marketplace will create a ripple throughout the world's various media channels, and not all of these channels will see our cause as positive. You don't need telling that there are very powerful media outlets controlled by various world governments, who will seek to muddy our name and reputation. But it is up to us to embrace this newfound exposure in mainstream media, rather than hide from it – and for this reason, I have chosen to speak briefly with a number of journalists who I am confident will report this memorable day without the pull of governmental strings. I have also conducted an exclusive interview with Mashable. In light of the FBI's recent 'victory', it would be impossible for Silk Road to stay off the radar – it is therefore our responsibility to make sure that our mark on the radar is the right one. So I would advise you all to prepare yourself for a spike in media attention, and to review your personal security measures to ensure your anonymity is protected.

We will be hiring staff to handle Silk Road's marketing shortly – formal offers may be made to members who have already demonstrated their marketing prowess.

And it goes without saying that if you are in touch with anybody who may not be aware that Silk Road has risen once more, now is the time to spread the word. Open communication with your old suppliers and customers; let this wonderful news be taken to all corners of the Tor network and beyond.

On the surface Silk Road 2.0 looks identical to the original by design. In order to appeal to the loyal fan base of the original Silk Road, the new DPR has maintained the look and feel of SR on the new website.

Dr. Nicolas Christin is an Assistant Research Professor in Electrical and Computer Engineering at Carnegie Mellon University in Pittsburgh and is affiliated with the University's security lab, CyLab. In 2013, he published "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace."[14] It is still the most exhaustive and complete analysis of Silk Road. In an email response to Digital Citizens, Christin answered questions regarding the newest Silk Road and how it compares to the original. He made several observations:

- "The features are still a subset of the original Silk Road. On the other hand they have seemingly beefed up their security."
- "The original Silk Road had a number of financial features that made it very convenient for people to transact on it. The new Silk Road is slowly building these features."
- "Silk Road has history since a number of old vendors have re-appeared on the new marketplace—and with history you can build reputation, which is paramount in the commerce of illicit goods, be it online or offline."

Professor Christin's findings speak to the reasons that SR 2.0 was able to have early success and reestablish itself as a major competitor so quickly. However, recent weeks have tested the resolve of the new site along with the black market community as a whole, as scams and arrests have rocked the online underworld.

Originally on SilkRoad	Available on new SR?	Found on other TOR market	Found on open web
Forged official documents	Y	Y	Y
Secret Bank Accounts/Money Laundering	Y	Y	Y
Hacking Techniques	Y	Y	Y
Phishing/Spam Services	Y	Y	Y
Anonymous Mail Drops	Y	Y	Y
Access to other Darknets	Y	Y	Y
Hard drugs	Y	Y	Y

The table above shows a comparison of items that were available on the original Silk Road and those available on the new Silk Road, other Darknet Marketplaces, and Open Net websites. For the larger, more detailed list please see the Appendix on page 25.

[14] Nicolas Christin. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In Proceedings of the 22nd International World Wide Web Conference (WWW'13), pages 213-224. Rio de Janeiro, Brazil. May 2013.

COMPARISON OF THEN AND NOW:
PRODUCT AVAILABILITY AND PRICE

While Silk Road grabbed the headlines, there is no shortage of underground markets on Tor. What helped set Silk Road apart was its diversity of products, efficiency, and transaction secrecy. Here we have selected a number of products sold on the old Silk Road to check their current availability. Are they still available? Did the price change? Can they be found in other black markets on the Darknet or even on the Open Net?

Our in-depth analysis of Silk Road and related topics captured available product lists from July 2013 to its first shutdown in October 2013. During this period, the value of bitcoins fluctuated, but the average price was approximately US$ 100 (bitcoins jumped in value through December 2013). For the purposes of this discussion $100 is the equivalent we will use. In our follow-up comparison, we pulled 32 Silk Road products examined in our first report to see their price and availability after the Ulbricht arrest. These 32 items include drugs and other illicit items the marketplace is known for, but the overall most expensive category is an eye-opener. While the brazen sales of heroin and crystal meth attract attention, the real money is in underground financial transactions. At a staggering 34.22 bitcoins, worth $3,422 at the time of our initial research, an anonymous German bank account wins the prize as the most expensive item on our list. The next two most expensive items are an Australian secret bank account ($1,198/Btc11.98) and anonymous credit cards originating from Germany ($854.41/Btc8.5441). The true value of Silk Road in the criminal underground is more than drugs; it is the further enabling of secret illicit activity.

In general, the prices have not changed for the list of products examined. If all the illicit sales occurred only within Silk Road, why didn't prices appear to adjust with the wild changes in bitcoin value and remain constant regardless of Silk Road's uptime? The reason is that the vendors on Silk Road operate independently from the marketplace and also sell their wares on other sites so are not directly part of the takedowns and arrests. It is likely due to the fact that vendors price their products in local currency and then convert to bitcoin. This leads us to the next part of the analysis concerning the availability of the products outside of Silk Road. For example, heroin of various kinds was easily found on the Darknet site Pablo Escobar, but this site does not have the other kinds of products found on Silk Road. There are other Tor sites that specialize in secret bank accounts, money laundering, and currency exchange but these sites do not sell drugs. Again, there are sites that offer vast arrays of forged identification and documents, but do not offer other illicit products. Silk Road is one-stop-shopping; a true nexus of secret illicit activity.

The 32 products we examined fell into six broad categories: forged official documents, secret financial transactions, hacking services, anonymous mail drops, hard drugs, and access to other Darknet Marketplaces. All six categories were prominently featured in the new Silk Road even if specific products or vendors were gone. There were some specific items no longer available on the new Silk Road. For example, Scopolamine, the so-called "Devil's Breath" powder used as an offensive zombification drug, could not be found. However, the directory for it was available waiting for a new vendor. It is difficult to tell if the unavailability of certain products is directly attributable to the Silk Road takedown or if it would have happened over time anyway as the marketplace changed.

As far as the Open Web is concerned, nearly all of the products found on Silk Road can be found for purchase in the normal domain name system. There are two major differences, one being the lack of anonymity and the other is how far and wide illicit consumers must crawl to find their contraband.

In reviewing from this perspective, Silk Road's special place is almost architectural. The products can be found elsewhere, but with difficulty and a lack of trust or stability. The shopping mall convenience and cultish dedication of its operators provide something not found elsewhere.

WHY BITCOIN THRIVED AS SILK ROAD 1.0 DIED

The Dread Pirate Roberts made no secret of Silk Road's reliance on the virtual currency bitcoin. Roberts/ Ulbricht told Forbes's Andy Greenberg: "We've won the State's War on Drugs because of bitcoin."

Some of the data recovered after the arrest made one wonder if bitcoin needed Silk Road just as much. As Ulbricht headed off to jail last October, the online magazine Quartz reported Silk Road had collected 9.5 million bitcoins – at a time when only 11.75 million bitcoins existed. Numbers like this supplied naysayers' reason to forecast a crash for the cryptocurrency.

But in fact the value jumped from $99 on the day of the DPR arrest to $1,000 for just a single bitcoin – in less than two months.[15] Make no mistake, only roller coasters would envy the kind of ups and downs we see tracking bitcoin. Yet while there have been peaks and valleys since the bust, the prices have stayed well above the levels seen prior to the FBI's takedown of Silk Road.

While some may have thought the government seizure would doom bitcoin's prospects, this may have in fact caused a shortage increasing value of the remaining currency and sparking a race to create more. Others might argue that Silk Road helped bitcoin find a foothold, but the currency has found mainstream acceptance from Capitol Hill to Wall Street. Whatever you believe about bitcoin's beginnings, increasingly, concern has turned into curiosity and even - in some cases - confidence.

WHY?

First, there is increasing sentiment that bitcoin is not as helpful to criminals as first believed. The initial belief that bitcoin can be used anonymously and leave no trail has been debunked.

Bitcoin is not the virtual currency of choice for criminal syndicates – according to the Secret Service's Ed Lowrey[16] in his testimony at a November Senate Hearing focused on bitcoin, titled "Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies." Lowrey told the Senate panel, "within what we see in our investigations that the online cyber criminals - the high level international cyber criminals - have not by in large gravitated towards the peer to peer cryptocurrency such as bitcoin."

At the same hearing, Jennifer Shasky Calvery, Director of the Financial Crimes Enforcement Network, said "Any financial system can be exploited. Cash is probably still the best medium for laundering money."[17] We don't forecast that anyone will campaign for Americans to stop using the dollar because it is useful to criminals.

At the same hearing, U.S. Assistant Attorney General Mythili Raman said "…virtual currency is not necessarily synonymous with anonymity. A convertible virtual currency with appropriate anti-money laundering and know-your-customer controls, as required by U.S. law, can safeguard its system from exploitation by criminals and terrorists in the same way any other money services business could."[18]

In fact, there are many who say the breadcrumbs left behind from a bitcoin purchase are quite easy to follow. Michael Nielsen, author of the blog DDI, says "someone who bought drugs on Silk Road in 2011 will still be identifiable on the basis of the block chain in, say, 2020." He speculates that he "would not be at all surprised if the NSA and other agencies have already de-anonymized many users" and calls bitcoin "the most open and transparent financial instrument the world has ever seen."[19]

David Woo, Bank of America Merrill Lynch's head of currencies research, echoed that sentiment. In December, Woo wrote, "the fact that all bitcoin transactions are publically available and that every bitcoin has a unique transaction history that cannot be altered may ultimately limit its use in the black market/ underworld."

---

[15] http://www.coindesk.com/price
[16] http://www.businessweek.com/articles/2013-11-19/currency-cops-want-congress-to-steer-clear-of-bitcoin-thanks
[17] http://www.businessweek.com/articles/2013-11-19/currency-cops-want-congress-to-steer-clear-of-bitcoin-thanks
[18] http://upstart.bizjournals.com/news/technology/2013/11/19/7-quotes-from-congress-bitcoin-hearing.html?page=2
[19] http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/
[20] http://www.businessinsider.com/baml-initiates-coverage-on-bitcoin-2013-12

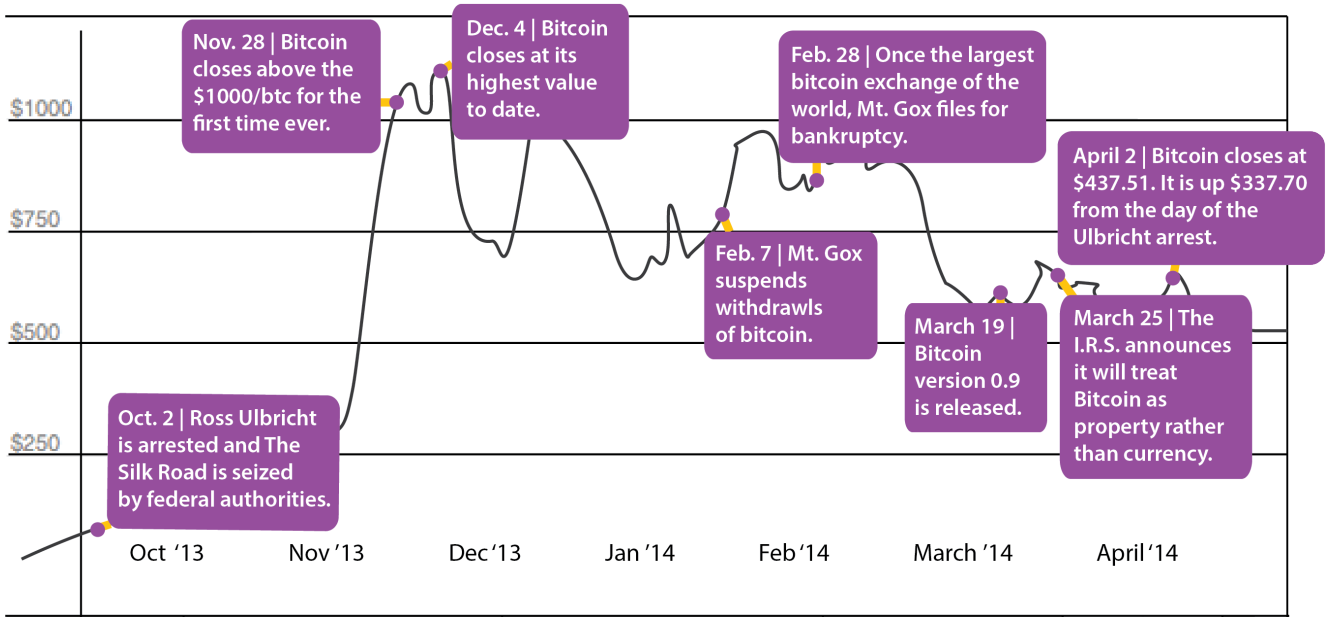
In the same December letter to Bank of America clients, Woo produced one of the positive assessments about bitcoin's potential to date saying, "As a medium of exchange, bitcoin has clear potential for growth." Second, there is a whole other community that sees bitcoin as an instrument for social good. Some are motivated by strong political beliefs. Others see bitcoin having potential to be a currency to a portion of the world that still has no access to banks and fiat currencies.

Patrick Murck, the General Counsel for the Bitcoin Foundation, told Digital Citizens researchers that he could see a psychological change in the perception of bitcoin almost instantaneously: "There was this assumption that if Silk Road was taken down, of course bitcoin would topple. If the only purpose for bitcoin is illicit transactions, it has no value in a world where there aren't any black markets. Then it was taken down, and people had this instant panic, because that function just dropped out of the system. But within 24 hours, the price had actually gone up. It showed people must think there's a useful purpose for this thing that has nothing to do with illicit transactions. The illicit transactions experiment failed."

But since soaring its all-time high in December, bitcoin has gone back to the more familiar rollercoaster-like track we saw before the Silk Road arrest. The collapse of Mt. Gox, once the world's largest bitcoin exchange, and the IRS decision to tax bitcoin as property instead of currency might have scared off some investors. Even the rollout of version 0.9, which included changes designed to prevent hackers from stealing bitcoins by changing the unique ID before it is confirmed on the network, might have actually caused a short term dip. Still, it is notable that these things hurt bitcoin, but Silk Road's issues have not. It does seem that bitcoin's value is effected by criminal activity, but usually because it is a target of criminals, not a tool.

The IRS decision marks a critical moment for the currency. It could create an interesting dilemma for those who flocked to bitcoin because of its perceived anonymity. However, many bitcoin advocates see the decision creating certainty for bitcoin believers. Now, the IRS has recognized bitcoin and treats it as a tangible commodity. Tax returns do have a category for property, but not for currency. Clearly, listing bitcoin as property will make it easier for the IRS to track – and that much less appealing to shoppers on Silk Road 2.0.

For tips on bitcoin safety, go to: http://bitcoin.org/en/secure-your-wallet.



Source: coindesk.com

LEADING THE SHEEP TO THE SLAUGHTER

With the rise of SR 2.0 there were again three major anonymous online drug markets open for business. SR 2.0 joined Black Market Reloaded and Sheep Marketplace as the three most well-known criminal bazaars. It took no longer than three weeks for that to change as the owners of Sheep Marketplace committed the largest scam in the history of anonymous drug markets stealing at least $40 million (some estimates are as high as $100 million) worth of bitcoin.

THE FACTS:

- Sheep Marketplace went permanently offline the last weekend in November, claiming that it had been robbed of $6 million in bitcoins by one of its sellers who found a security vulnerability in the site.
- Sheep's owners used that theft to justify closing the market without returning the bitcoins stored in the market by users, despite claiming that they would redistribute those coins to users' "emergency addresses."(Very similar to what occurred with Atlantis when it shut down.)
- Administrators blocked withdrawals of bitcoins from the site for more than a week in advance of shuttering the site. That same weekend they absconded with as much as $44 million from the site's users, indicated by a movement of 39,900 bitcoins visible in the public record of bitcoin transactions known as the blockchain.[21]
- A separate transfer of 96,000 stolen bitcoins was viewed that following Monday from the same address used to steal the 39,900 over the weekend giving rise to the $100 million figure.[22]

THE FALLOUT FROM SHEEP MARKETPLACE'S DEMISE

The Sheep Marketplace scam has had a major impact on the world of Darknet Marketplaces. One could argue that the owners of Sheep Marketplace did just as much, if not more damage to the community than law enforcement did when they arrested DPR and seized the original Silk Road. The fallout includes:

- More than 135,000 bitcoins stolen (estimates put the amount seized by the FBI in the DPR arrest at 173,000 bitcoins).[23]
- Sheep Marketplace, one of the two biggest Darknet Marketplaces at the time, shut down.
- Black Market Reloaded, at the time the largest anonymous market for contraband online with nearly 7,000 product listings, went offline indefinitely, worried that the site wouldn't be able to handle the influx of new customers and sellers leaving their security vulnerable.[24]
- Silk Road 2.0 shut down for several days to updates its servers to make sure it could properly handle the increase in traffic it was expecting after BMR and Sheep shutdown.[25]
- The heist did a tremendous amount of damage to the psyche of the Darknet drug community. They were now getting it from all angles as they have to worry about market operators just as much, if not more, than law enforcement.

[21] http://www.forbes.com/sites/andygreenberg/2013/12/01/silk-road-competitor-shuts-down-and-another-plans-to-go-offline-after-6-million-theft/
[22] http://mashable.com/2013/12/03/sheep-marketplace-shutdown-100-million-bitcoin/
[23] http://www.wired.com/wiredenterprise/2013/12/fbi_wallet

[redacted] 2 points 1 month ago

Ok guys with the amount of people getting [redacted] by the sheep we should hunt these [redacted] down. I know everyone thinks it might be Tomas the [redacted] perv czech, but for now its all speculation. I have a suggestion. If we organize and use each others skills i dont c why we cant find the admins to the site. We got to approach like a le investigation. What we know it is most unlikely we will be able to track down this guy through tor. What we do know is we can follow the btc. So y dont we do that...people have posted that the stolen coins are being cashed at Mt. Gox...only if a group of hackers could hack the gox and follow the money to the bank accounts. Once we get that its a flight and a few water boardings to get this [redacted] done. I know some of the users have to have some balls using the site and if we think about if we organized we would be a formidable force. For those with the skills, is this plan feasible? Personally I lost over 5k which is nothing compared to the stories of 100k plus loses. I am not a hacker but i am huge [redacted] if an identity is found i know the right people to make those [redacted] suffer I personally would like to torture and melt them in nice warm lye bath. Thoughts and comments are appreciated. By the way if it is the czech mob i dont really give a [redacted] and people who i roll with dont give a [redacted] A 9mm hollow point to the back of the head will ruin anyone's disposition

An example of the reaction to the Sheep Marketplace heist. This was by no means the only post seeking an identity to inflict physical harm on the person responsible.

The closures of BMR and Sheep Marketplace left an enormous void much like Atlantis and the Silk Road did when they went offline. Silk Road 2.0, still relatively new, stood to gain significantly from the lack of competition. Two other markets, Pandora Openmarket and Tormarket, looked to capitalize. Not surprisingly, there has been no shortage of drama and speculation along the way.

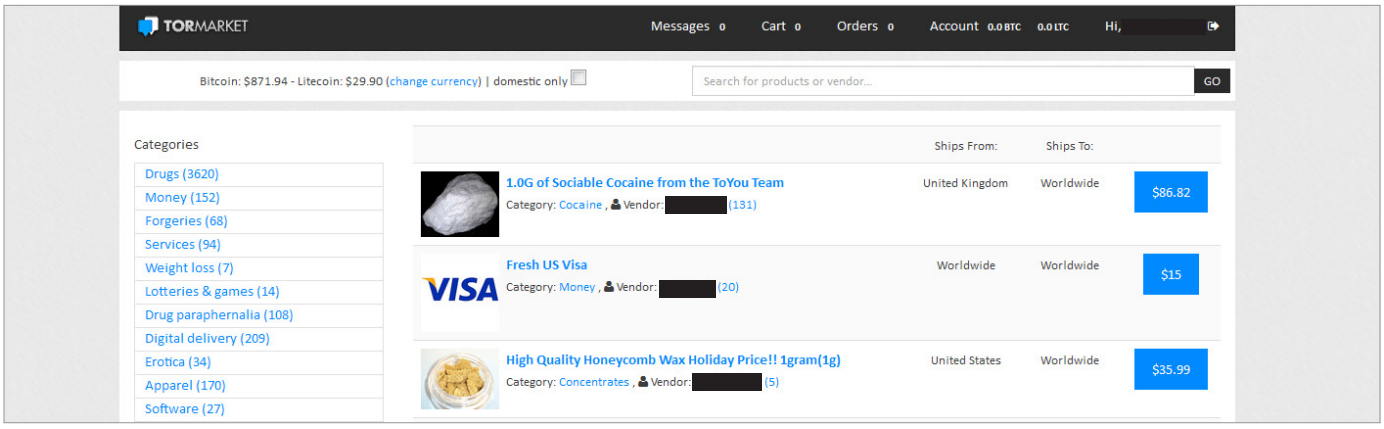
TRACKING THE CHATTER:
THE CONVERSATIONS BETWEEN ADMINS, MODS, AND CUSTOMERS

In at least one respect, the criminals in the world of Darknet Marketplaces are much different than say those you'd see on mob movies and TV. In shows like The Sopranos, everyone knew who the gangsters were, the challenge for law enforcement was finding a way to get them talking about it. Sopranos fans will remember the episode in which a carefully placed FBI microphone, hidden on a desk lamp, was whisked off in a packing frenzy by Tony's college-bound daughter.

In the Darknet, you struggle to find who the bad guys are, but much of what they say is in plain sight for anyone using Tor to see. Chatrooms are filled with conversation about what "management" is doing. Some of it is speculation; other discussions may be important dictates from on high.

We've tracked those conversations. Not every word seen should be taken as truth – in fact, some of conversations may be deliberate lies, designed to threaten or intimidate. But you can see some patterns and trends from the tenor of the talk. It's impossible to pull every compelling example, but we found a few that demonstrate what we've seen.

BATTLE OF THE CLONES



The opening listing page of Tormarket before it was shutdown.

[24] http://www.forbes.com/sites/andygreenberg/2013/12/01/silk-road-competitor-shuts-down-and-another-plans-to-go-offline-after-6-million-theft/
[25] http://silkroad5v7dywlc.onion/index.php?topic=5248.0

Competition has always been fierce among Darknet Marketplaces going back to when it was just SR, Black Market Reloaded, and Atlantis. According to DPR himself, the competition from these sites pushed him to make improvements. He claimed to be happy to have competition because that meant the cause was being furthered.[26]

Under the new DPR, that has changed. Beginning on December 9, Silk Road 2.0, Pandora Openmarket, and Tormarket all came under DDOS attack that shut down access to the websites. SR 2.0 was the first to come under attack and the new DPR believed it to be the work of Tormarket's owners. He assured his vendors that he had proof, but never produced any. Days later Tormarket was under its own DDOS attack, albeit a different type.[27] It has not been proven if these two sites attacked each other or if a third party is responsible. There is no doubt, however, about who launched the most important attack that followed.

On December 14, DPR made the below post on the Silk Road 2.0 forums. In it he claims that he was able to steal Tormarket's entire database which included private messages, orders, addresses, vendor and buyer statistics, purchasing histories, and the entire user list. According to his post, DPR did so in order to protect the sites user's and make sure it was secure, which clearly it was not. DPR's aggressive maneuver was a marked change from the previous regime and was met with mixed reactions.[28]

Author | Topic: Security: Why claims are dangerous to believe (Read 13720 times)

Dread Pirate Roberts
Captain
Administrator
Posts: 596
Karma: +490/-30

Security: Why claims are dangerous to believe
« on: December 14, 2013, 02:23:54 am »

To start, I would like to make this clear to everyone involved that Silk Road does not have malicious intentions or an anti-competition attitude, we actually require competition to keep us motivated and for the diversity of the network but in order to fulfill that function the competition must be a safe one which does not put people in harms way or subject to possible exploit. This post I hope will demonstrate to you why claims a market makes does not correlate to the true story and we would like to demonstrate this with Tormarket.

At this moment in time, I also want to clarify in light of recent events the full disclosure everyone deserves to know. This investigation started under the suspicion that Tormarket was behind the ongoing DDOS against Silk Road but has since taken another turn when we looked below the surface a little more. I have no conclusive proof Tormarket did or did not order the DDOS currently hitting us and personally I don't believe I ever will so I won't go on about this much more as it is actually not something that matters any more since we are definitely en route to fixing it if you have watched our recent developments, but over Tor such attacks are not trivial to correct. All of this is done in the name of safety and I hope the owners of Tormarket can take this seriously, go away and rethink their strategies because as I will discuss later we didn't even put much effort in to extracting this data.

What is it I am attempting to prove?

To take it from the home page of Tormarket, I wish to publicly overturn the rumors and falsehoods of some of the below:

Quote from: [redacted]

Darknet Market done right

Secure codebase, competent operators, and common sense.

Common sense I will allow that to pass as a subjective matter and how they wish to operate their market is none of my business. Competent operators - again it would depend on your individual definition of that. Secure codebase - let us put that to the test.

Let's start with the basics

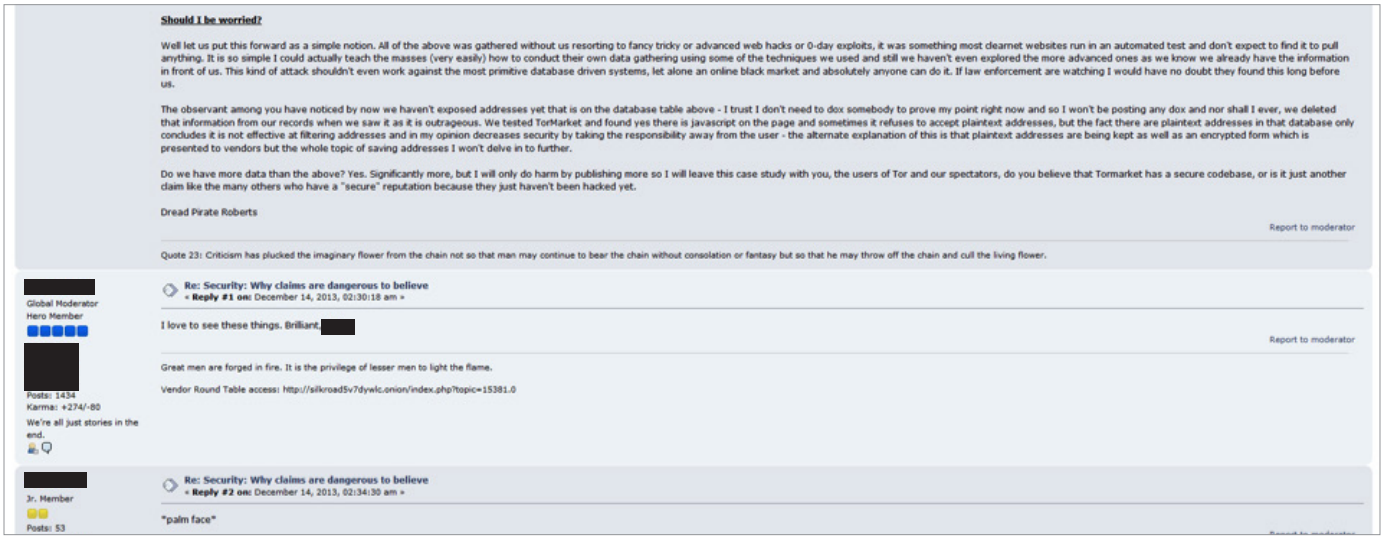
One of the most valuable pieces of any website is the database. It controls so many parts of the site and without it there could be no effective market, so we started trying to extract the information from that. Surprise surprise, it didn't take long to grab the structure:

Code: [Select]

```
  - address
  - notes
  - crypto_currency_id
  - buyer_id
  - buyer_username
  - vendor_username
  - vendor_id

vendor table
  - id
  - username
  - banned
  - currency
  - location
  - messages_id
  - messages_body
```

Now we've had a sneak peak at their table structure, it was decided to have a trawl through the messages that vendors had sent to customers. We will list a little segment below, some vendors here might recognize their own messages with of course sensitive information removed from below.



Should I be worried?

Well let us put this forward as a simple notion. All of the above was gathered without us resorting to fancy tricky or advanced web hacks or 0-day exploits, it was something most clearnet websites run in an automated test and don't expect to find it to pull anything. It is so simple I could actually teach the masses (very easily) how to conduct their own data gathering using some of the techniques we used and still we haven't even explored the more advanced ones as we know we already have the information in front of us. This kind of attack shouldn't even work against the most primitive database driven systems, let alone an online black market and absolutely anyone can do it. If law enforcement are watching I would have no doubt they found this long before us.

The observant among you have noticed by now we haven't exposed addresses yet that is on the database table above - I trust I don't need to dox somebody to prove my point right now and so I won't be posting any dox and nor shall I ever, we deleted that information from our records when we saw it as it is outrageous. We tested TorMarket and found yes there is javascript on the page and sometimes it refuses to accept plaintext addresses, but the fact there are plaintext addresses in that database only concludes it is not effective at filtering addresses and in my opinion decreases security by taking the responsibility away from the user - the alternate explanation of this is that plaintext addresses are being kept as well as an encrypted form which is presented to vendors but the whole topic of saving addresses I won't delve in to further.

Do we have more data than the above? Yes. Significantly more, but I will only do harm by publishing more so I will leave this case study with you, the users of Tor and our spectators, do you believe that Tormarket has a secure codebase, or is it just another claim like the many others who have a "secure" reputation because they just haven't been hacked yet.

Dread Pirate Roberts

Report to moderator

Quote 23: Criticism has plucked the imaginary flower from the chain not so that man may continue to bear the chain without consolation or fantasy but so that he may throw off the chain and cull the living flower.

[redacted]
Global Moderator
Hero Member
[redacted]
Posts: 1434
Karma: +274/-80
We're all just stories in the end.

Re: Security: Why claims are dangerous to believe
« Reply #1 on: December 14, 2013, 02:30:18 am »

I love to see these things. Brilliant.[redacted]

Report to moderator

Great men are forged in fire. It is the privilege of lesser men to light the flame.

Vendor Round Table access: http://silkroad5v7dywlc.onion/index.php?topic=15381.0

[redacted]
Jr. Member
Posts: 53

Re: Security: Why claims are dangerous to believe
« Reply #2 on: December 14, 2013, 02:34:30 am »

palm face

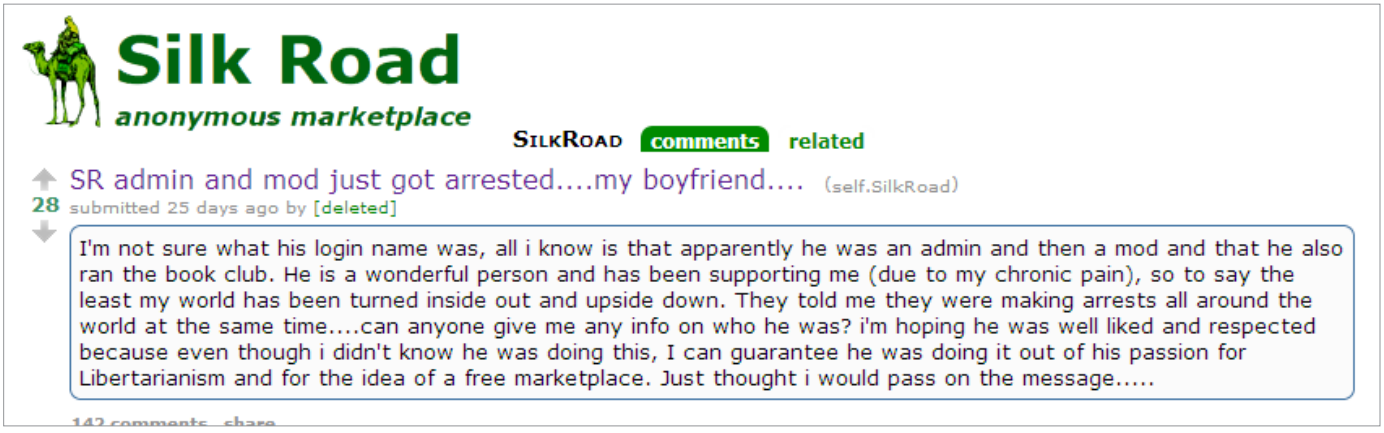
[26] http://www.forbes.com/sites/andygreenberg/2013/08/14/meet-the-dread-pirate-roberts-the-man-behind-booming-black-market-drug-website-silk-road/
[27] http://www.dailydot.com/business/cyberwar-deep-web-silk-road-2/
[28] Ibid 25

Within two weeks of DPR's hack, the owners of Tormarket closed shop and disappeared. It is not clear whether they did so in response to the attack, but according to forum posts they did so without returning users bitcoin or any communication:

Tormarket was the third major site (including Atlantis and Sheep Marketplace) that made off with users' bitcoin - a fact that is not lost on Darknet Marketplace dwellers. Understandably, they have become increasingly wary of operators who might want to make off with their bitcoin or any law enforcement activity that might threaten the Marketplaces themselves. No one is immune to these scares - especially those doing business on the new Silk Road.

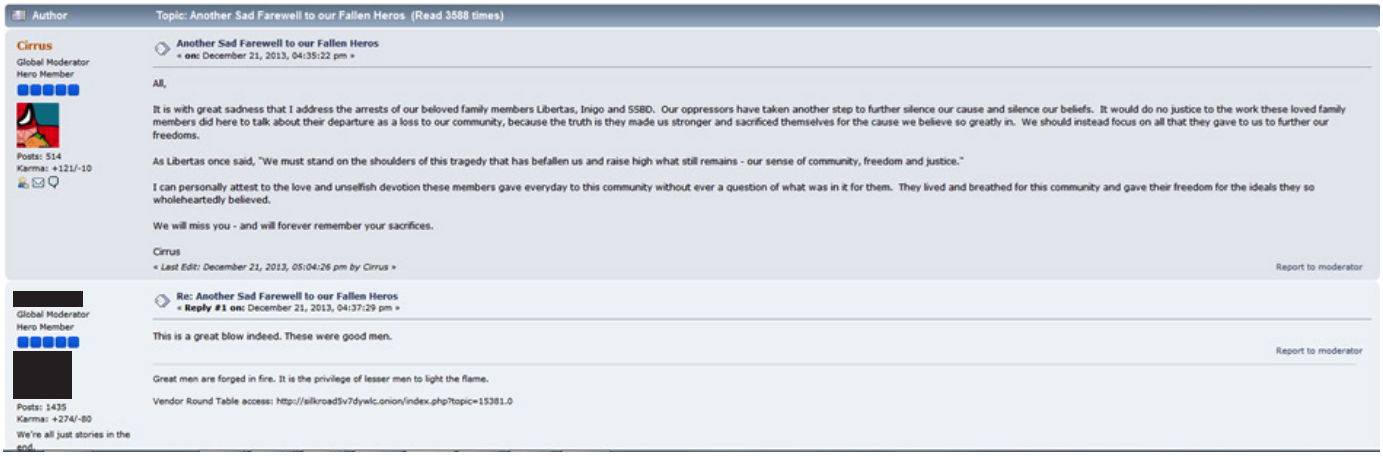
TRAVELLING ON THE NEW SILK ROAD? WATCH YOUR STEP

As the battle with Tormarket was seemingly coming to a close, Silk Road 2.0 found itself facing a familiar threat, law enforcement. Initial rumblings of arrests began when the girlfriend of an apparent Silk Road employee made the following post on Reddit:[29]



[29] http://www.reddit.com/r/SilkRoad/comments/1tb2yl/sr_admin_and_mod_just_got_arrestedmy_boyfriend/)

Quickly word spread on Silk Road 2.0's forums and news outlets began to report that three of the original Silk Road's employees had been arrested. The next day the U.S. States Attorney announced that Andrew Jones AKA "Inigo", Gary Davis AKA "Libertas", and Peter Nash AKA "Samesamebutdifferent," AKA "Batman 73, AKA "Symmetry" and "Anonymousasshit" faced charges including conspiracy to engage in narcotics trafficking, computer hacking, and money laundering by the U.S. Attorney for the Southern District of New York.[30]


Author | Topic: Another Sad Farewell to our Fallen Heros (Read 3588 times)

Cirrus
Global Moderator
Hero Member
Posts: 514
Karma: +121/-10

Another Sad Farewell to our Fallen Heros
« on: December 21, 2013, 04:35:22 pm »

All,

It is with great sadness that I address the arrests of our beloved family members Libertas, Inigo and SSBD. Our oppressors have taken another step to further silence our cause and silence our beliefs. It would do no justice to the work these loved family members did here to talk about their departure as a loss to our community, because the truth is they made us stronger and sacrificed themselves for the cause we believe so greatly in. We should instead focus on all that they gave to us to further our freedoms.

As Libertas once said, "We must stand on the shoulders of this tragedy that has befallen us and raise high what still remains - our sense of community, freedom and justice."

I can personally attest to the love and unselfish devotion these members gave everyday to this community without ever a question of what was in it for them. They lived and breathed for this community and gave their freedom for the ideals they so wholeheartedly believed.

We will miss you - and will forever remember your sacrifices.

Cirrus
« Last Edit: December 21, 2013, 05:04:26 pm by Cirrus »

Report to moderator

[redacted]
Global Moderator
Hero Member
Posts: 1435
Karma: +274/-80
We're all just stories in the end.

Re: Another Sad Farewell to our Fallen Heros
« Reply #1 on: December 21, 2013, 04:37:29 pm »

This is a great blow indeed. These were good men.

Report to moderator

Great men are forged in fire. It is the privilege of lesser men to light the flame.

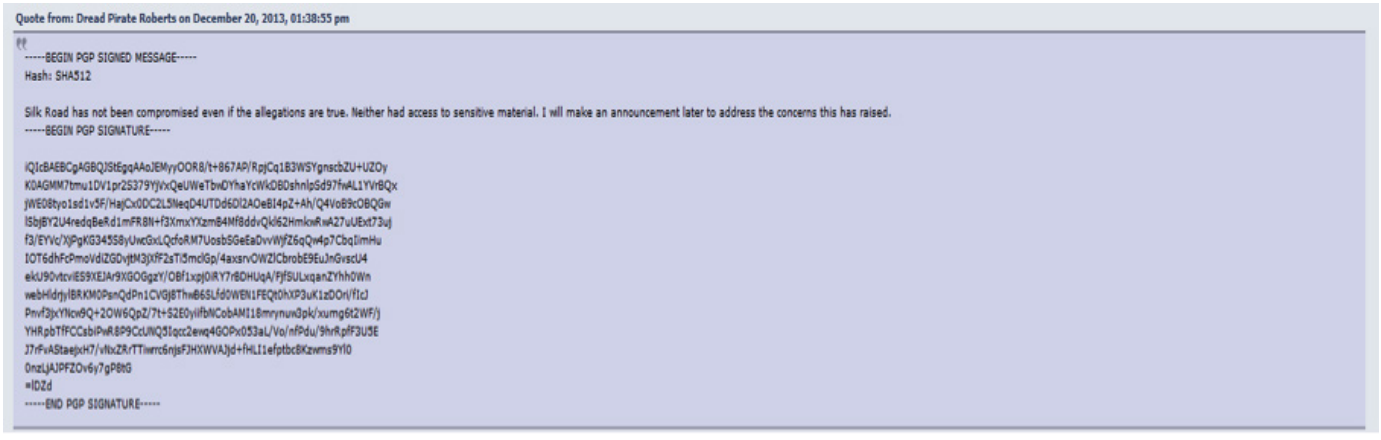
Vendor Round Table access: http://silkroad5v7dywlc.onion/index.php?topic=15381.0

Global Moderator "Cirrus" discusses the arrest of three Silk Road employees.)

Jones, 24 of Virginia, and Davis, 25 of Ireland, acted as site administrators for Silk Road, while Nash, 40 of Australia, was the primary moderator for the website's discussion forums.[31] Many speculate that law enforcement came across these individuals during their investigation of Ross Ulbricht. The theory being that they had given Ulbricht their identities in order to work on the original Silk Road.[32]

In a business where the threats to survival include federal agencies, rival markets, and the potential of an operator running off with all of your bitcoin, there is a certain level of paranoia required to avoid complacency. The arrests of Inigo, Libertas, and Samesamebutdifferent (SSBD) sent the paranoia into hyperdrive and the users were looking to their fearless leader for news and instruction. Just one minor problem-the new DPR had abandoned them.

NEW DPR UNDERGROUND AND THE RISE OF "DEFCON"


Quote from: Dread Pirate Roberts on December 20, 2013, 01:38:55 pm

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Silk Road has not been compromised even if the allegations are true. Neither had access to sensitive material. I will make an announcement later to address the concerns this has raised.
-----BEGIN PGP SIGNATURE-----

iQIcBAEBCgAGBQJStEgqAAoJEMyyOOR8/t+867AP/RpjCq1B3WSYgnscbZU+UZOy
K0AGMM7tmu1DV1pr2S379YjVxQeUWeTbnOYhaYcWkDBDshnlpSd97fwAL1YVrBQx
jWE08tyo1sd1v5F/HajCx0DC2L5NeqD4UTDd6DI2AOeBI4pZ+Ah/Q4VoB9cOBQGw
l5bjBY2U4redqBeRd1mFR8N+f3XmxYXzmB4Mf8ddvQkl62HmkwRwA27uUExt73uj
f3/EYVc/XjPgKG345S8yUwcGxLQcfoRM7UosbSGeEaDvvWfjZ6qQw4p7CbqIimHu
IOT6dhFcPmoVdiZGDvjtM3jXfF2sTi5mclGp/4axsrvOWZlCbrobE9EuJnGvscU4
ekU90vtcviES9XEJAr9XGOGgzY/OBf1xpjOiRY7r8DHUqA/FjfSULxqanZYhh0Wn
webHIdrjyIBRKMOPsnQdPn1CVGj8ThwB6SLfd0WEN1FEQt0hXP3uK1zDOn/f1cJ
Pnvf3jxYNcw9Q+2OW6QpZ/7t+S2E0yiifbNCobAMI18mrynuw3pk/xumg6t2WF/j
YHRpbTfFCCsbiPwR8P9CcUNQ5Iqcc2ewq4GOPx053aL/Vo/nf9du/9hrRpfF3U5E
J7rFvAStaejxH7/vNxZRrTTiwrc6njsFJHXWVAJjd+fHLI1efptbcBKzwms9YI0
0nzLjAJPFZOv6y7gP8tG
=IDZd
-----END PGP SIGNATURE-----

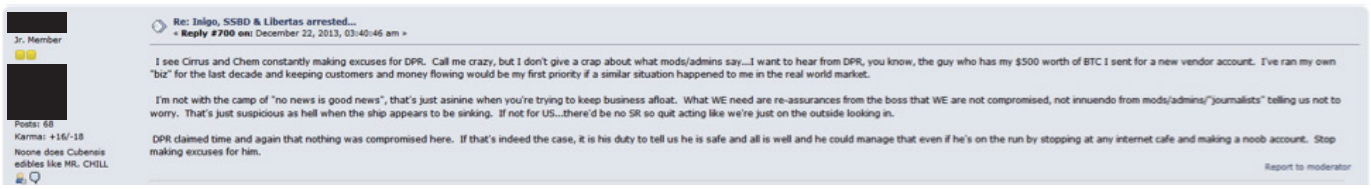
The last known forum post from the new DPR before he went underground following the most recent arrests.

[30] http://mashable.com/2013/12/20/fbi-silk-road-arrests/
[31] http://usnews.nbcnews.com/_news/2013/12/20/21990649-three-more-arrested-in-silk-road-online-drug-market-case?lite
[32] http://arstechnica.com/tech-policy/2013/12/feds-indict-three-alleged-silk-road-forum-moderators-and-administrators/

After the arrests of former Silk Road employees and moderators of SR 2.0, the new DPR responded with the following message:

> "Silk Road has not been compromised even if the allegations are true. Neither (of those arrested) had access to sensitive material. I will make an announcement later to address the concerns this has raised."[33]

The follow up message, however, never came and SR 2.0 loyalists were left wondering whether DPR had been compromised or abandoned them:



Jr. Member

Posts: 68
Karma: +16/-18
Noone does Cubensis edibles like MR. CHILL

Re: Inigo, SSBD & Libertas arrested...
« **Reply #700 on:** December 22, 2013, 03:40:46 am »

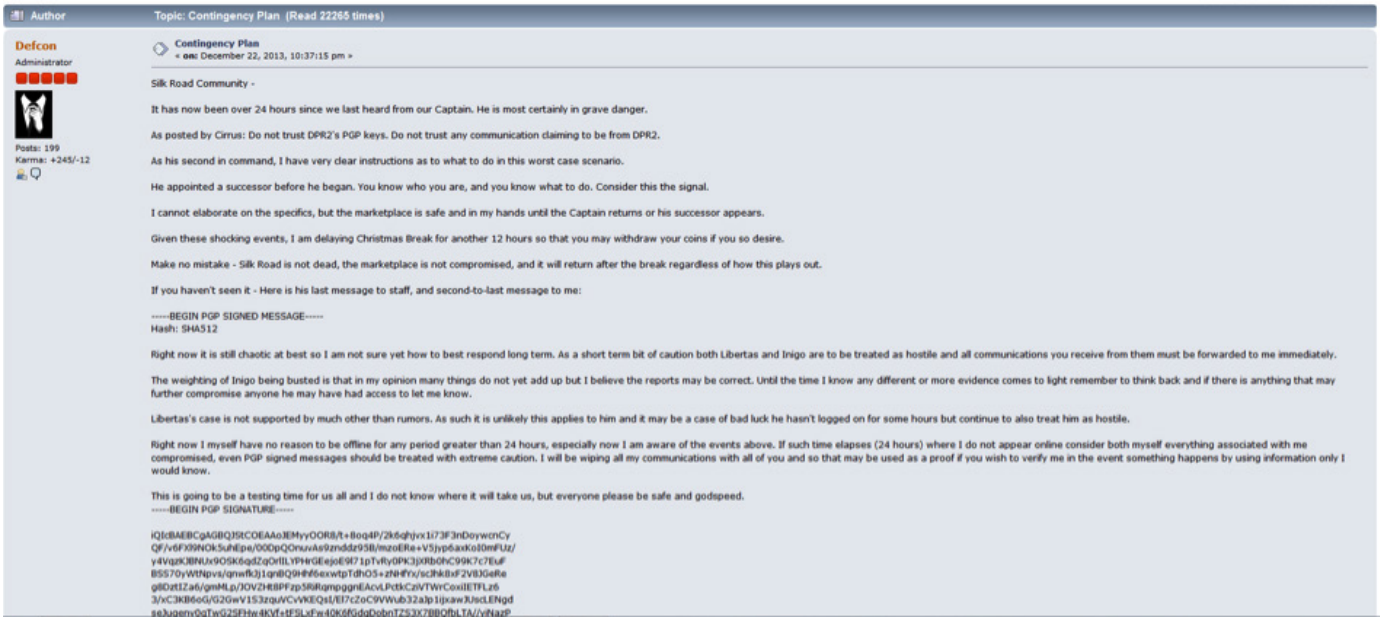
I see Cirrus and Chem constantly making excuses for DPR. Call me crazy, but I don't give a crap about what mods/admins say...I want to hear from DPR, you know, the guy who has my $500 worth of BTC I sent for a new vendor account. I've ran my own "biz" for the last decade and keeping customers and money flowing would be my first priority if a similar situation happened to me in the real world market.

I'm not with the camp of "no news is good news", that's just asinine when you're trying to keep business afloat. What WE need are re-assurances from the boss that WE are not compromised, not innuendo from mods/admins/"journalists" telling us not to worry. That's just suspicious as hell when the ship appears to be sinking. If not for US...there'd be no SR so quit acting like we're just on the outside looking in.

DPR claimed time and again that nothing was compromised here. If that's indeed the case, it is his duty to tell us he is safe and all is well and he could manage that even if he's on the run by stopping at any internet cafe and making a noob account. Stop making excuses for him.

Report to moderator

Eventually, the SR 2.0 admin "Defcon" let it be known that DPR's account might indeed be comprised according to DPR himself, but the site was not:



Author | Topic: Contingency Plan (Read 22265 times)

Defcon
Administrator

Posts: 199
Karma: +245/-12

Contingency Plan
« **on:** December 22, 2013, 10:37:15 pm »

Silk Road Community -

It has now been over 24 hours since we last heard from our Captain. He is most certainly in grave danger.

As posted by Cirrus: Do not trust DPR2's PGP keys. Do not trust any communication claiming to be from DPR2.

As his second in command, I have very clear instructions as to what to do in this worst case scenario.

He appointed a successor before he began. You know who you are, and you know what to do. Consider this the signal.

I cannot elaborate on the specifics, but the marketplace is safe and in my hands until the Captain returns or his successor appears.

Given these shocking events, I am delaying Christmas Break for another 12 hours so that you may withdraw your coins if you so desire.

Make no mistake - Silk Road is not dead, the marketplace is not compromised, and it will return after the break regardless of how this plays out.

If you haven't seen it - Here is his last message to staff, and second-to-last message to me:

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Right now it is still chaotic at best so I am not sure yet how to best respond long term. As a short term bit of caution both Libertas and Inigo are to be treated as hostile and all communications you receive from them must be forwarded to me immediately.

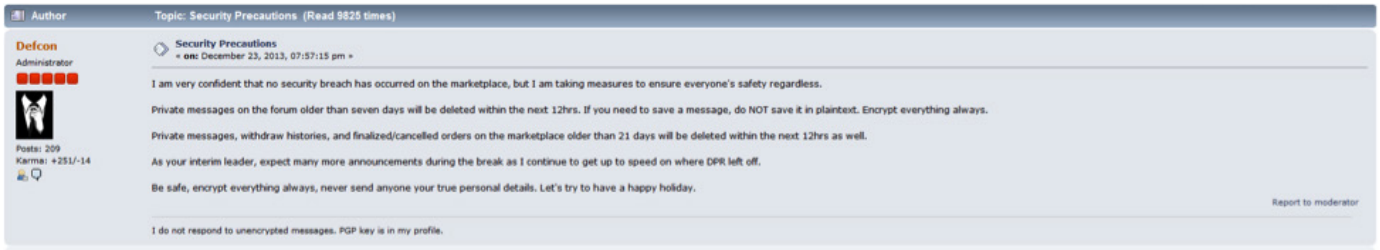
The weighting of Inigo being busted is that in my opinion many things do not yet add up but I believe the reports may be correct. Until the time I know any different or more evidence comes to light remember to think back and if there is anything that may further compromise anyone he may have had access to let me know.

Libertas's case is not supported by much other than rumors. As such it is unlikely this applies to him and it may be a case of bad luck he hasn't logged on for some hours but continue to also treat him as hostile.

Right now I myself have no reason to be offline for any period greater than 24 hours, especially now I am aware of the events above. If such time elapses (24 hours) where I do not appear online consider both myself everything associated with me compromised, even PGP signed messages should be treated with extreme caution. I will be wiping all my communications with all of you and so that may be used as a proof if you wish to verify me in the event something happens by using information only I would know.

This is going to be a testing time for us all and I do not know where it will take us, but everyone please be safe and godspeed.
-----BEGIN PGP SIGNATURE-----

iQIcBAEBCgAGBQJStCOEAAoJEMyyOOR8/t+8oq4P/2k6qhjvx1i73F3nDoywcnCy
QF/v6FX9NOk5uhEpe/00DpQOnuvAs9znddz95B/mzoERe+V5jyp6axKo30mFUz/
y4VqzKJBNUx9O5K6qdZqOrIILYPHrGEejoE9f71pTvRyOPK3jXRb0hC99K7c7EuF
BS570yWtNpvs/qnwfkDj1qnBQ9Hf66exwtpTdhO5+zNHfYx/scJhk8xF2V8JGeRe
g8DztIZa6/gmMLp/JOVZHt8PFzp5RRqmpggnEAcvLPctkCzlVTWrCoxiIETFLz6
3/xC3KB6oG/G2GwV1S3zquVCvVKEQsI/El7cZoC9VWub32a3p1ijxawJUscLENgd
seJugemv0qTwG2SFHw4KVfxtF5LxFw40K6fGdqDobnTZ53X7BBOfbLTA//viNazP



Author | Topic: Security Precautions (Read 9825 times)

Defcon
Administrator

Posts: 209
Karma: +251/-14

Security Precautions
« **on:** December 23, 2013, 07:57:15 pm »

I am very confident that no security breach has occurred on the marketplace, but I am taking measures to ensure everyone's safety regardless.

Private messages on the forum older than seven days will be deleted within the next 12hrs. If you need to save a message, do NOT save it in plaintext. Encrypt everything always.

Private messages, withdraw histories, and finalized/cancelled orders on the marketplace older than 21 days will be deleted within the next 12hrs as well.

As your interim leader, expect many more announcements during the break as I continue to get up to speed on where DPR left off.

Be safe, encrypt everything always, never send anyone your true personal details. Let's try to have a happy holiday.

Report to moderator

I do not respond to unencrypted messages. PGP key is in my profile.

With the deadline passed and DPR out of contact, Defcon took control of SR 2.0 until the appointed successorof DPR stepped forward. However, as of the writing of this report, no such person has stepped forward and Defcon is still running SR 2.0. Since Defcon took control of SR 2.0, there is no sign of it being compromised by law enforcement. However, in February the resolve of Defcon and the SR 2.0 community were again put to the test as the news broke that the site had been hacked.

[33] http://silkroad5v7dywlc.onion/index.php?topic=10209.msg185499#msg185499

TROUBLE AT THE TOP: SR 2.0 AND PANDORA HACKED

On February 13 Silk Road users logged onto their beloved drug haven to find their worst nightmares had become reality. Defcon wrote:

> "I am sweating as I write this… I must utter words all too familiar to this scarred community: We have been hacked. Our initial investigations indicate that a vendor exploited a recently discovered vulnerability in the Bitcoin protocol known as "transaction malleability" to repeatedly withdraw coins from our system until it was completely empty."[34]

Author | Topic: IMPORTANT: Humbled and Furious (Read 46444 times)

[redacted]
Global Moderator
Hero Member
[redacted]
Posts: 2658
Karma: +503/-228
We're all stories in the end.

IMPORTANT: Humbled and Furious
« on: February 15, 2014, 07:54:25 pm »

Reposting this in it's entirety due to the issue with the forum filters:

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

I am sweating as I write this.

Christmas brought grave news. I cannot adequately express how deeply honored I was by your unconditional support of my staff.

I do not expect the same reaction to today's revelations. This movement is built on integrity, and I feel obligated to be forthright with you.

I held myself to a high standard as your leader, yet now I must utter words all too familiar to this scarred community:

We have been hacked.

Nobody is in danger, no information has been leaked, and server access was never obtained by the attacker.

Our initial investigations indicate that a vendor exploited a recently discovered vulnerability in the Bitcoin protocol known as "transaction malleability" to repeatedly withdraw coins from our system until it was completely empty.

Despite our hardening and pentesting procedures, this attack vector was outside of penetration testing scope due to being rooted in the Bitcoin protocol itself.

This attack hit us at the worst possible time. We were planning on re-launching the new auto-finalize and Dispute Center this past weekend, and our projections of order finalization volume indicated that we would need the community's full balance in hot storage.

In retrospect this was incredibly foolish, and I take full responsibility for this decision.

I have failed you as a leader, and am completely devastated by today's discoveries. I should have taken MtGox and Bitstamp's lead and disabled withdrawals as soon as the malleability issue was reported. I was slow to respond and too skeptical of the possible issue at hand. It is a crushing blow. I cannot find the words to express how deeply I want this movement to be safe from the very threats I just watched materialize during my watch.

A moderator reposted Defcon's announcement of the hack several days later.[35]

Estimates put the total theft at approximately 4,400 bitcoin, worth around $2.6 million at that time.[36] Defcon and SR 2.0's staff pointed to three possible attackers and much like those scorned by the Sheep MarketPlace scam they are out for justice writing "Stop at nothing to bring this person to your own definition of justice."

However, many users were unwilling to put their faith in Defcon's explanation. More than a few accused Defcon and his team of admins of perpetrating the heist themselves and using the Bitcoin protocol as the scapegoat. The hack has further eroded the credibility of Defcon and his team of admins, but SR 2.0 caught a break a little over a month later as their main competition, Pandora MarketPlace, faced similar difficulties.

After the Sheep and Tormarket scams that saw all users lose their bitcoin, Pandora stood as the only sizeable competitor to SR 2.0 remaining. With the hack to SR 2.0, Pandora stood to gain significantly.[37] However, just over a month later," Alice," the admin of Pandora, announced that Pandora had been hacked and lost half of its bitcoin. Two vendors were able steal an estimated 425 bitcoins ($250,000 at that time) thanks to a "leak in the system," according to "Alice."[38] The chaos that has engulfed the Darknet market economy in the last six months finally caught up to Pandora and cost the market a chance at catching SR 2.0 as the market leader.

[34] http://www.forbes.com/sites/andygreenberg/2014/02/13/silk-road-2-0-hacked-using-bitcoin-bug-all-its-funds-stolen/
[35] http://silkroad5v7dywlc.onion/index.php?topic=26366.0
[36] http://www.forbes.com/sites/andygreenberg/2014/02/13/silk-road-2-0-hacked-using-bitcoin-bug-all-its-funds-stolen/
[37] Ibid
[38] http://www.deepdotweb.com/2014/03/20/pandora-hacked-losing-50-btc/

Alice
Administrator
Full Member
Posts: 241
Karma: +106/-23
[applaud] [smite]

THE TRUTH & PLAN
« **on:** March 19, 2014, 10:40:24 am »

First of all sorry, but i didn`t had to much for choice if i didn`t wanted to close pandora market and hope at least some of you will understand situation, but i know i am going to burn and lost all of my karma, but there is whole truth with my plan.

What happened:
1) Last week pandora market got shaved of large portions of BTC by 2 vendors used to be small-time scammers, they were able to steal about 1/2 of BTC pandora total holdings (basically everything, that was not on cold storage), they found the leak in system.
2) I stopped all withdrawals, found leak and fix the bug in system and also were checking any signle money operation programming, that is the reason why everyone withdrawals were stopped for about 12 hours.

What were my options back then, when i found bitcoin lost:
1) I could make market to disapear and just close it down, everyone will think then, i scammed oll of you.
2) I will apply solution to cover losses and continue operations.
3) **I choose number 2)**

Why I didn`t told truth before:
1) **That would probably lead only to instant panic and market closure week before that day**. All money would be probably lost - all vendors and customers money.
2) I didn`t informed and pandora were able to make withdrawals of more than 1000BTC since steal of bitcoins discovered to vendors - **all of that would not be possible if i would not take this drastic measurements**.
3) All my actions was made to safe pandora market and continue operation, time will tell if that was good move.
4) **Only what i am sure about is if i didn`t made this drastic measurements, i can only close down the market and be remembered as scammer.**

Current situation:
1) I partly covered loss from my profits (*this is probably very stupid move from me* as everybody will probably blame me, i should closed market i think now) - **i covered about 1/3 of losses from my own money** (hard desicion for me).
2) Market and almost all BTC will be recovered during this week by aplying very high tax on all transactions.

Actions made:
1) Currently only max 2/10 pandora holdings are held on main server so possible loss is limited to 2/10 of total pandora holdings.
2) Many security updates to the system, leak fixed.
3) If pandora will survive that, in future if that ever happen again, loss is limited to 2/10 of BTC holdings.

Pandora Admin "Alice" announces hack on the market's forum.[39]

MAKING THINGS "RIGHT"?

The hacks of SR 2.0 and Pandora are similar in several ways:

1. They were hacked in a very similar fashion with vendors taking advantage of a flaw in the Bitcoin protocol and a "leak in the system" of Pandora.
2. They are the first two marketplaces to get their bitcoin stolen and remain open. All previous site operators who faced similar hacks, if they were ever even hacked, proceeded to make off with user funds. This was the case with Sheep MarketPlace.
3. Most importantly, both Defcon and Alice devised systems to repay all of the bitcoin that was stolen to their users in an attempt to make things "right." By doing so these two markets, SR 2.0 especially, have a chance to convince users that they are different from the failed Darknet markets of the past.

[39] http://www.deepdotweb.com/2014/03/20/pandora-hacked-losing-50-btc/

SILK ROAD'S PLAN TO PAY BACK CUSTOMERS

The Plan for Moving Forward as of Feb 15

1. This administration will not earn any commissions until everyone is completely paid back, and will be very transparent about the progress towards this goal.
2. The marketplace will relaunch as no-escrow. We will not re-implement escrow unless it is multi-signature and decentralized to multiple escrow providers (trusted mediators with feedback just like vendors). Never buy from a market which uses centralized escrow again. You will only get hurt no matter how honest the team is.
3. All items will be priced at a flat 5% commission which will go directly into victims' balances upon purchase.
4. Vendors who lost funds: Commissions from your items will go directly into your wallet until you are completely repaid, then will be distributed to other vendors until they are repaid. Vendor bonds are considered lost funds, and we also commit to paying these back.
5. All vendors can opt-in to give a higher percentage back on their listings, and all buyers will be presented with a "Donate" box on the shopping cart. Vendors' donation percentage will be publicly visible.
6. We will launch the support system immediately. Resubmit any open support requests you had which are still applicable. All previous messages will be ignored due to our inbound message volume. I have received over 1000 private messages over the past 24 hours, for example. This fresh start will allow us to stay on top of the support queue, rather than paying down a large debt incurred by previous administrators.
7. We will still handle dispute resolution for existing escrow orders until all balances site-wide are in "Pending Balance" category. Your stolen balances and escrows will display as "Pending balance" and "Pending escrow". Yes, like Christmas. I hoped to never have to take this approach again. All unshipped orders have been cancelled. To the vendors who have shipped orders despite no access to the portal: you are beautiful people. Try to resolve with your buyer directly, and file a support ticket if you do not receive a refund to your pending escrow balance within a month.

Defcon's orginal plan to pay back all bitcoin to those affected by the hack.[40]

PANDORA'S PLAN TO PAY BACK CUSTOMERS

Recovery scheme & Buyback:

1) For save pandora market i had to make very drastic measurements – commission (operating tax) of 24% during 23.3.

1.2) commission paid from all transaction scheme:

1.3) 24% by 23.3. (16% recovery tax if your item have add commission to item instead of deduct)

1.4) 16% 23.3. – 31.3. (8% recovery tax if your item have add commission to item instead of deduct)

1.5) 8% from 31.3. until 1.4.

1.6) If you have option to add commission to item price as vendor, you are not charged full 24% but customer pay commission of 8% and after you are cahrged 16%.

Alice's original plan to payback those vendors affected by the hack.[41]

Both payment plans are essentially taxes on all future purchases. In the case of Pandora, the tax is more significant at 24% than SR 2.0's 5%. Regardless of the amount, the very fact that there IS a repayment plan is a stark contrast to previous markets whose customers have lost all of their money. Defcon and Alice appear to be doing everything in their power to make it "right," in the eyes of their vendors and customers. In doing so, they have to opportunity to rebuild the trust of their users and further their brands as two of the bigger names in the business.

[40] http://www.reddit.com/r/SilkRoad/comments/1y27ha/the_sewage_ship_sails_on_another_post_from_defcon/
[41] http://www.deepdotweb.com/2014/03/20/pandora-hacked-losing-50-btc/

AN EVEN DARKER WEB

WHERE INTERNET LIBERTARIANISM CROSSES INTO REVOLUTION

Readers of Darknet news are aware of murderers for hire in the cryptoworld and the role they played in the Silk Road saga. While the contract killer services are usually offered on a specific basis, there is a more general political assassination market ongoing. This Tor site professes, "Anonymous, safe, secure, crowdfunded assassinations." The site collects bitcoins to fund murders of political figures, and the figure accruing the most money so far is telling.

It is no surprise that the list includes world leaders, including the President of United States as well as prime ministers of France, Sweden and Finland. The target that had "amassed" the biggest bounty surprised us. That person is not an elected official. We decided to not include that person's name here, so as not to bring additional attention to a specific threat to this person's life. We will say that the fund to assassinate this person was up to 124.22 bitcoins, or around $124,220. Whether or not this is serious, that is certainly enough money to motivate some unhinged people to act.

The owner of this site makes his motivation completely clear: "A deep-rooted hate against oppressive regimes." The person who calls him or herself "Kuwabatake Sanjuro" insists "Once you're on the list you're on it until you die."

THE CURRENT STATE OF THE DARKNET ECONOMY

The last six months have tested the wherewithal of the Darknet Marketplaces. Arrests, site seizures, scams from small to massive, and an ever-increasing amount of paranoia have challenged those who buy and sell illicit goods online. The Marketplaces have proven resilient and as one closes or disappears, several others pop up to take its place. Here is a current look at the Darknet Marketplaces that are currently on top and others looking to make some noise:

Marketplaces (Today)	Drug Listings	Total Listings	Weapons
Silk Road 2.0	13,648	17,192	No
Agora	7,400	9,158	Yes
Pandora Openmarket	5,249	5,812	No
Evolution	2,623	5,523	Yes
BlueSky Marketplace	1,740	1,833	No
New Markets			
Dark Bay	292	329	No
The Pirate Market	247	367	Yes
Outlaw Market	230	246	No
Tor Bazaar Alpha	205	252	Yes
Black Bank Market	201	239	No
White Rabbit Anonymous MarketPlace	194	256	Yes
TOTAL LISTINGS	32,029	41,207	

Darknet sites at the time of the Silk Road seizure (10/2/13)	Drug Listings
The Silk Road	13,000
Black Market Reloaded	3,567
Sheep Marketplace	1,407
DeepBay	200
TOTAL	18,174

The current state of the Darknet drug economy, despite the turmoil, is not all that different six months after the arrest of DPR if one looks strictly at the numbers (these numbers are as of January 29, 2014):

- The current number of total drug listings is 176% of pre-TSR take down levels. This growth has come with increased competition, as there are now five marketplaces that have more listings than Sheep Marketplace did at the time of the original Silk Road seizure.
- Silk Road 2.0 is the market leader with a 43% market share. TSR had 71% at the time of its seizure.

- Silk Road 2.0 currently contains 105% of the drug listings that TSR had listed at the time of its seizure.
- Agora currently carries 26% of drug listings and has seen major growth in listings, as well as credibility, since the hacks of Silk Road 2.0 and Pandora. Agora further differentiates itself from Silk Road 2.0, Pandora, and BlueSky by offering weapons.
- Pandora Marketplace, thanks in large part to the Tormarket shutdown, occupied the number two slot for several months, but has since been overtaken by Agora. Pandora currently represents 19% of drug listings among major marketplaces.
- There are several newer markets looking to get in on the action. These sites pop up quickly and usually fade away or are quickly identified as scammers, but some become viable option for those seeking drugs online. The markets listed above are worth keeping an eye on in the months to come.[42]

REVIEW OF GOVERNMENT POLICY INITIATIVES CONCERNING THE DARKNET

Bitcoin, Tor and Darknet Markets are related topics, but they are not the same thing. While Colorado and the state of Washington have legalized sales of marijuana, there is no sign that the U.S. government will legitimize the sale of various illicit products. While bitcoin and Tor are highly decentralized and may not have official voices, interested organizations with sway have met with both lawmakers and regulators in Washington. Executives from the Bitcoin Foundation testified in a Senate Homeland Security Committee hearing late last year on Silk Road and were generally given positive reviews. Regulators have also advised bitcoin exchanges to require identification. As far as Tor policy goes, government has the conflicting position of simultaneously trying to use Tor for its own clandestine operations while also working to crack Tor.

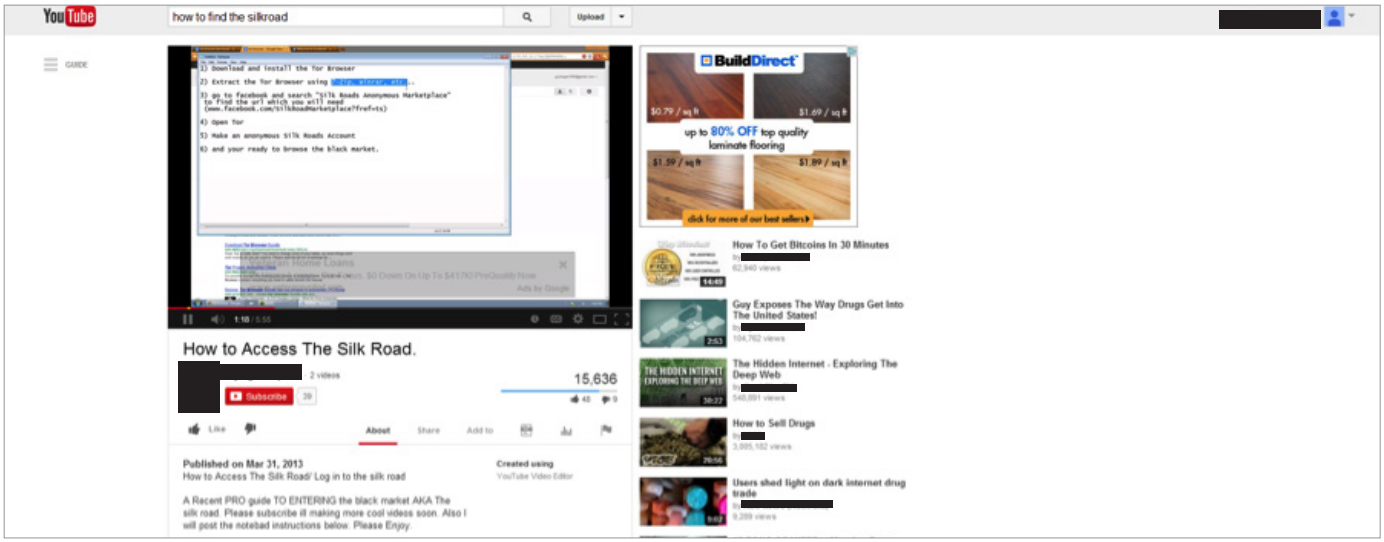
Even if there is motivation to develop policy, the development will emerge from different areas. The Treasury Department has examined bitcoin while the other two topics have been the province of law enforcement. The government in general struggles with developing any Internet policy, and the cryptonet debate seems even more fraught with apathy.

Both bitcoin and Tor proponents are pushing for normalization and engaging government directly. That's clearly not the case for black market operators and vendors. In short, the policy development areas for Tor, bitcoin, and Darknet Marketplaces are wide open. U.S. states may see the need to create their own policies or recommend federal ones. States may see the need to regulate bitcoin exchanges in their own jurisdictions or require Internet service providers to block Tor use locally, regardless of how technically implausible it might be. This is a brave new world of policy analysis.

[42] http://blueskyplzv4fsti.onion/

CONCLUSION

We want to end our report with a mention of where we began our research. Getting onto Silk Road using bitcoin to make a purchase and getting there through the Tor Network is a bit like going into Wonderland. Of course, Alice's journey began with sipping from a bottle marked "drink me." We didn't even have to work that hard. Every step to get to Silk Road can be found on videos contained in YouTube. Some pages included advertising that produces revenues for both YouTube and the producers of the videos.



Just because it sounds complicated doesn't mean it is for kids and young adults who've grown up with the Internet. In fact, many of those teens have taken to social media sites to share news about their purchases.[43] This may sound like a long, strange trip, but the path is all too easy to find.

A few tips for concerned parents:

- Check to see if the Tor software has been downloaded on your child's computer, tablet, or smartphone. Without it they will not be able to access marketplaces like Silk Road and other nefarious corners of the Darknet.
- If your child mentions the use of bitcoin or asks you for money to convert to bitcoin, be sure to discuss the purpose for using the digital cryptocurrency.
- While the order is made with a computer, the delivery still comes through the mail. Check all packages to see what is coming into your house. At least one parent in Fishers, Indiana did just that and may have saved her 14-year-old's life.
- Don't allow teens to keep PO Boxes. If you find your child has one it could be a red flag.

[43] http://www.dailydot.com/crime/tumblr-teens-silk-road-drug-deals/

APPENDIX

Seller	BCPrice(Summer 2013)	DollarPrice(Then) 1BC=100US	On new SR?	Found on other TOR market
YourCannabisProvider	0.2506	$25.06	N	Y
DrugsAndCash	8.5441	$854.41	Y	Y
aldog25	0.1106	$11.06	Y	Y
sniffsniff	0.0982	$9.82	Y	Y
UK Stealth	0.376	$37.60	N	Y
fake	0.4908	$49.08	Y	Y
druqks	5.0477	$504.77	Y	Y
DoctorFreedom	0.0491	$4.91	Y	Y
High Carts	0.0981	$9.81	Y	Y
optiman	2.458	$245.80	Y	Y
optiman	0.1513	$15.13	Y	Y
fake	0.1571	$15.71	N	Y
thesimguy	0.9629	$96.29	N	Y
optiman	0.1358	$13.58	Y	Y
DoctorFreedom	0.2945	$29.45	N	Y
optiman	0.1241	$12.41	Y	Y
everythingman	0.3366	$33.66	Y	Y
tucksh0p	11.98	$1,198.00	Y	Y
namedeclined	0.5171	$51.71	Y	Y
aldog25	0.2209	$22.09	Y	Y
fake	0.4908	$49.08	Y	Y
namedeclined	0.3186	$31.86	Y	Y
Red Bull	34.22	$3,422.00	Y	Y
TehStore	0.0318	$3.18	Y	Y
namedeclined	0.2775	$27.75	Y	Y
fake	0.4205	$42.05	Y	Y
Asession1	5.5312	$553.12	N	Y
frock952	0.2168	$21.68	N	Y
Dr. Earnhardt	0.1307	$13.07	N	Y
XXXX	6.2459	$624.59	Y	Y
the company	1.6046	$160.46	Y	Y
theanchor	0.7311	$73.11	Y	Y

Note: *Digital Citizens has located several of the sites where these products are being sold on the Open Net. If you are a journalist interested in seeing the list, please contact the Digital Citizens Alliance for that information.*


digitalcitizens
alliance