Vending on Dark Net Markets

Collin Berman
cmb5nh

December 8, 2015

1 Introduction

Dark net markets (DNMs) have been extensively researched from an economic standpoint, but they also pose interesting implmentation questions in terms of software design and user experience. In addition, most reporting on DNMs has focused on the buying side. To this end, I looked at the process of setting up a shop on DNMs, with special attention payed to novel uses of bitcoin.

2 Background

Although the internet has been used to sell drugs since it was still ARPANET [3], Silk Road emerged as the first marketplace to leverage both TOR and bitcoin in 2011 [2]. The most extensive analysis of Silk Road can be found at [1], but it does not focus on newer bitcoin technologies and does not get into vending. In fact, the essay is critical of multisignature escrow, which it calls "intrinsically hard to use".

3 Methods

In order to look at the process of becoming a vendor, I selected two DNMs to become a merchant on.

The first marketplace I chose was Darknet Heroes League, due to its lack of a vendor fee. However, this market is fairly new and low quality. There

are only 60 vendors on the site, most of whom have under 10 reviews. The forums went down while I was researching the site, and when they came back up at a different domain, all the accounts had been deleted. The site itself has numerous bugs and is hard to use. That being said, the market did take advantage of some interesting features of bitcoin.

To get more of a representative feel of DNMs, I also looked at East India Company. While this market is also new, it's already fairly large, with over 3000 listings. This site looks a lot cleaner, and the DNM community says it has the best customer support. The downside was that this market required a vendor fee, but it was only ฿0.2, much less than some of the other big-name marketplaces.

4 Results

As we would expect, both marketplaces offer strong security settings for accounts, and have secure ways for customers to communicate with vendors. This is accomplished using PGP keys. These keys can be used as a second authentication factor for login, by requiring the user to decrypt a message before logging in. While PGP itself is notoriously hard to use, simply decrypting a message is not hard if one's keyring is properly configured. The same PGP keys used for authentication are also used to encrypt communications between customers and vendors. A user's public PGP key is available on their public profile.

Although the marketplace is unable to read messages encrypted with users' public keys, they could perform a man-in-the-middle attack to expose messages. Instead of providing a customer with a vendor's real public key, they could provide their own. After decrypting the message, they could reencrypt it using the vendor's actual public key. Communications would appear encrypted to both parties, but they have actually lost all confidentiallity.

Outside of public-key encryption, both marketplaces I looked at used features of bitcoin to provide other assurances of security.

4.1 Darknet Heroes League

The best service Darknet Heroes League (DHL) had to offer was their use of hierarchical deterministic (HD) wallets, defined in BIP 0032. By uploading your HD wallet's master public key, DHL is able to generate a new address for

you every time they need to send you bitcoin. By using the public key, DHL is not able to generate the private key corresponding to each new address. This is a great way to add anonymity without compromising security.

Although HD wallet support is a good idea in theory, DHL's implementation leaves much to be desired. After uploading your master public key, they require you to sign it with your PGP key. They expect a detached signature but don't indicate this anywhere. I couldn't tell if I was signing the key incorrectly, or if the site was buggy. Eventually I got it to work, but more documentation would be useful.

4.2 East India Company

Although I set up vendor accounts on both DHL and East India Company (EIC), I only created a product listing and made purchases on EIC. On EIC, vending is almost as straightforward as purchasing. The site is incredibly easy to use, and the store options are surprisingly modular. Product images can be uploaded and shipping methods can be created, and both of these can be attached to multiple product listings. Item listings can be grouped together, and there is an inventory system that automatically deactivates a listing when you run out of stock.

To try out vending, I created a listing for a potato, setting the price at 10 cents. I was easily able to buy it from other accounts I created, and left myself multiple positive reviews. Because the price was only 10 cents, I didn't get much credit for my sales. However, it would be possible to repeat this process with higher-valued listings, since I'm paying myself for the product.

In addition to vendor ratings, EIC also gives customers ratings. This lets vendors determine whether a customer is trustworthy before they decide to ship them products. Buyers increase reputation the same way vendors do, by making many transactions.

One big feature that sets EIC apart from other DNMs is their implementation of multisig. Multisig escrow is an alternative to conventional escrow that utilizes special locking scripts to create transactions that require multiple signatures. In the escrow system, the multisig transaction that is created knows the marketplace's, vendor's and customer's public keys, and needs two out of three possible signatures to spend the coins. If the marketplace transaction goes smoothly, the marketplace and vendor can sign a trandaction giving the vendor the money. If the vendor scams the customer, then

the marketplace and customer can sign a transaction giving the customer the money. Multisig escrow also offers distinct advantages over conventional escrow, in that it insures that funds are released even if the market is not around to release funds. It does this by signing timelocked transactions and releasing them to the customer and merchant. If the marketplace has not signed an escrow transaction paying the vendor 31 days after the product was shipped, the vendor can sign the timelocked transaction to get their money anyway.

Generally, multisig escrow is seen as hard to use, especially for the customer. But with pay to script hash transactions, creating a multisig transaction is just as easy as sending bitcoin to any standard address. The customer never has to sign a multisig transaction unless they are scammed by a vendor. On the other hand, vendors using multisig escrow need to know how to sign and broadcast multisig transactions in order to receive any payments. Current wallets do not make this easy to do (the DNM community recommends saving an ofline version of the coinb.in website instead of using a wallet), but as wallet software improves, multisig will be easy even for merchants.

5 Conclusion

Although DNMs are generally viewed as hotbeds of criminal activity, using bitcoin for payments allows them to implement features that are beneficial to users outside of providing anonymity. Dark net markets have learned how to create user-friendly marketplaces from conventional ecommerce sites; conventional ecommerce sites could also stand to learn from dark net markets.

References

[1] G. Branwen. Silk road: Theory and practice. *Gwern*, July 2011.

[2] A. Chen. The underground website where you can buy any drug imaginable. *Gawker*, June 2011.

[3] M. Power. Online highs are old as the net: the first e-commerce was a drugs deal. *The Guardian*, Apr. 2013.