Smooth as Silk: The Story of the Internet's Largest Drug Marketplace

Krzysztof Danielewicz

krys.danielewicz@gmail.com

Mentor: Ming Chow

Abstract

On October 2 2013, the largest illegal online marketplace in the world was shut down by the FBI, and its founder arrested. Ross William Ulbricht, the "Dread Pirate Roberts" and founder of Silk Road, had spent 2½ years escaping the efforts of the United States Government to take down his creation, with great success. During this time, Silk Road offered the ability to solicit and purchase a staggering number of blatantly criminal substances and services within minutes, from practically anywhere in the world: it was well known as "the Amazon.com of illegal drugs." Silk Road was run through Tor, a service which offers online anonymity and security. Which brings the question: how did the FBI manage to take down a supposedly anonymous online drug empire, arrest its owner, and seize over $3 million in Bitcoin? Will these actions by the United States Government make a significant difference in the online proliferation of illegal goods, or do the alternatives to Silk Road (already in full swing) make their efforts fruitless? And do these alternatives suffer from the same vulnerabilities that took down Ulbricht? This paper will explore the above questions and discuss the implications of this take down on illegal trade over the internet and, more generally, the anonymity and potential flaws of the Tor network as it exists today.

To The Community

Silk Road and Tor showcase a side of the Internet that is not well known to the general public, but is nonetheless a growing force in the proliferation of illegal goods worldwide. The tools that allow internet anonymity are growing in number, ease-of-access, and sophistication. As these programs and their user bases grow, so do the security risks and pitfalls. They are not bulletproof- although Bitcoin and Tor do offer some protection over traditional browsing and money transfer methods, government action against illegal activity online has increased significantly over the last several years. Being aware of these dangers and knowing where on the internet to tread lightly is a crucial part of being a well informed, aware, and safe Internet user.

Applications

From a security standpoint, the stories of Silk Road and its counterparts expose the type of vulnerabilities that are actively exploited every day. Becoming aware of and learning good practices for website development (both Tor-based and not) is integral to becoming an effective developer. The methods described in this paper and the accompanying video could be used to purchase drugs or other illegal goods online. However, especially with the volatility in these market over the last few months, every such transaction is under the very real danger of being recorded by federal authorities, or scammed by either party. Therefore, the methods and steps described in this paper should be viewed as an academic analysis, not a practical guide to be followed.

Introduction

Since its creation, the Internet has undoubtedly been used to facilitate illegal transactions. However, until the last few years, the barrier to entry has been significant. After all, you could not search for “drug dealer” or “buy a gun online” in a search engine and expect to find any reliable results. Transactions took place through 'private' communication channels, such as e-mail or instant message, or through small, publicly inaccessible websites. After all, if a website grew enough, the servers hosting it could be subpoenaed by the government, and quickly shut down. The introduction of Tor changed all that. Tor introduced a way to get to the internet anonymously, which seemed to remove much of the danger of being tracked and prosecuted for illegal activity. “.onion” domains, which are unaccessible through regular internet browsing, further provided an avenue to mask both the host, administrator, and user of a website. The first well known 'hidden site' to take advantage of this anonymity was dubbed “The Farmer's Market”. This online marketplace laid the foundation for bringing the world of illegal transactions into the open, of which Silk Road quickly became the most prominent.

The Farmer's Market

The Farmer's Market was not nearly as popular as Silk Road eventually became, for several reasons. It facilitated illegal transactions largely through one-to-one correspondence- a seller would list a product, and a buyer would contact him and purchase it. The interface was not intuitive or easy to navigate through, which hampered the number of users and media attention it received. Many transactions in The Farmer's Market were done in Paypal, mailed cash transactions, or other online payment services, which made it easier for scammers to operate on the site. To their credit, the owners of the website were relatively careful about the way transactions were handled- random Americans would receive Paypal payments, and then route them through a digital currency based in Panama.

Nonetheless, the Farmer's Market was eventually shut down. Rumors quickly spread that Paypal had been responsible for the downfall. However, it's demise was not due to Tor, or Paypal. Surprisingly, the shut down was caused by the owners' use of hushmail.com, an online private, supposedly secure email service. Although they did eventually move away from hushmail, the DEA was able to subpoena the website and acquire the contents of early emails the owners of the market sent to each other. From those emails, the government was able to identify the men behind the Farmer's Market and quickly took it down, arresting the men responsible. Now, the online drug scene was in need of an anonymous, easy to use, and well populated marketplace. Enter Silk Road.

The Rise of Silk Road

In February of 2011, Silk Road was officially launched. It was pioneered by an online entity under the pseudonym “Dread Pirate Roberts,” later identified as Ross William Ulbricht. A few important features led to its rapid success and growth. Firstly, it operated on Tor, which alleged to guarantee a certain level of anonymity, as long as it was used correctly. Transactions were done only in Bitcoin, which could be purchased and spent without any personally identifiable information connected to the money itself or the 'wallet' which stored the virtual currency. Silk Road operated on an escrow

system for payments, which meant that drug dealers were not paid until the users actually received their products and left a review on the website (except for well established and reputable sellers, who could insist that buyers 'finalize' a transaction early before shipment). Silk Road's payment system was a complex route designed to hide the originator and receiver of the Bitcoin accounts. Since all Bitcoin transactions are published publicly in the blockchain, Silk Road ran the money through several nodes that attempted to disguise the identity of the buyer and seller, making it even harder to trace any given transaction in the system. Lastly, Silk Road was structured with an Amazon-like interface. Drugs and illegal merchandise were listed under different categories, with pictures and reviews for every item. Silk Road quickly took off as a massive success. How big was it? There were over a million documented transactions that took place on the site before it was taken off-line, with approximately 150,000 buyer accounts, and just shy of 4,000 vendor accounts. Approximately 10 million Bitcoin in revenue was made in the two years of its operation- a sum roughly equivalent to a billion USD. Silk Road was undoubtedly the leader in its sector.

The Fall

On October 2, 2013, Silk Road was taken off-line by the US Government. The take-down was made possibly through a series of mistakes made by the "Dread Pirate Roberts." Ulbricht's first mistake was his lack of anonymity on the internet. The FBI, by searching for references to silk road on the internet, found a forum where a user named "altoid" was searching for "an IT pro in the Bitcoin community". The post mentioned an email address where inquires should be sent- "rossulbricht at gmail dot com". This online handle was traced to other posts on Bitcoin forums, and several drug-oriented sites, where "altoid" was trying to drum up interest in Silk Road. Through a subpoena to Google, investigators found that the Gmail account was connected to a man named Ross Ulbricht. By itself, this was not enough evidence to carry out a conclusive report. Further evidence came when a user with the above email created a Stack Overflow post asking for help accessing a Tor hidden server

using curl, in PHP. At this point, the investigators had a strong lead on the owner of the site, and started a serious investigation into Ulbricht.

Meanwhile, authorities had tracked down and arrested a Silk Road administrator, who sold cocaine to an undercover US agent. The administrator had used his real return address on the package. Shortly after, authorities arrested Curtis Green, a 47 year old man from Utah. Through Green's computer and access to private messages on Silk Road, they were able to find Ulbricht's account, which led to a scheme designed to trap him in an online assassination attempt. Ulbricht contacted an undercover agent disguised as a drug dealer, with the intent to set up a hit on Curtis. The undercover agent accepted, and ultimately sent staged images of the murder, which Ulbricht allegedly believed to be real. On July 10, 2013, another piece of the puzzle came together. A package was intercepted coming in from Canada, containing 9 fake driver's licenses, each with a picture of Ulbricht. After compiling all of the evidence, authorities finally came down on Ulbricht in October of 2013: he was arrested in San Francisco. Along with Ulbricht himself, the government seized over 5 million dollars in cash and over 40 million dollars in Bitcoin from Ulbricht and the users of Silk Road. At the same time, they gained access to the servers running Silk Road and shut it down.

Back From the Ashes

The story doesn't end there. In early November of 2013, Silk Road made a comeback. The twitter handle “DreadPirateSR” announced the re-opening of the site, on a small invite only basis. In early December, the site was re-opened to public registration. The new “Dread Pirate Roberts” announced that encrypted portions of the source code behind Silk Road, along with cryptographic keys to decrypt those portions, were sent to more than 500 locations around the world. This move was orchestrated in order to ensure the survival of Silk Road through the survival of its source. If the current version of Silk Road is taken down by authorities, the source code of the website could be theoretically re-hosted through the Tor network, and kept alive. Like its predecessor however, “Silk

Road 2.0" has already run into problems. As the time of this paper's publishing, the second iteration of Silk road had been off-line for several days, as a result of a crippling denial of service attack form an unknown source. Rumors pointing to the US government as the source of the attack have proliferated over the internet, while others point out that the federal government may be using the second iteration of Silk Road as a 'honeypot' to capture information about both the buyers and sellers using the site. Regardless, it remains to be seen whether the rebirth of Silk Road will prosper as its predecessor did, or stumble and fall.

An Unsaturated Market

Silk road has not been the only online drug market. In the time before and shortly after Silk Road was taken down, several other markets opened up. However, these alternatives have not fared well. Atlantis Marketplace, which opened in the summer of 2013 with a slick, professionally produced marketing video advertising its services. However, in September, Atlantis went down, with "security concerns" specified as the reason behind the close, with many allegations of the administrators shutting down to steal the money stored in the site at the time. Another Tor site, Sheep Marketplace, shut down in the first week of December, after over six million dollars in Bitcoin was allegedly stolen from the website and its users.

Black Market Reloaded, another marketplace based in Tor, has faced security issues as well, albeit smaller ones. After several thousands dollars in Bitcoin were stolen, the administrators of Black Market Reloaded decided to shut down the site, because the influx of users from Silk Road put the market "in the edge of the blade, Tor can't support any site to be too big." Another online drug store, known simply as "The Marketplace" has made an appearance in the last few months. Unlike the other failed attempts mentioned above, The Marketplace is not based on Tor. Instead, it uses I2P, another anonymizing protocol, to hide its website and transactions. It remains to be seen whether I2P can be competitive with the Tor-based markets that have come before, but it currently operates with the

advantage of obscurity. The numerous online markets will certainly challenge the government. Over the next few years, we will find out whether law enforcement will be able to cut the heads of the hydra before they have time to regrow.

Conclusion

A serious question emerges from the accounts examined in this paper: is the online illegal transaction marketplace a viable business model? Thus far, the majority of these marketplaces have fallen due to relatively simple security flaws and loopholes. As the minds behind the marketplaces learn more sophisticated techniques and improve upon the websites they use, we might see an iteration of Silk Road that becomes much more difficult to take down. Work is already in progress on an open-source Bitcoin based marketplace. If successful, an open source project could be difficult to take down or penetrate- if the user base becomes large enough, users skilled in cryptography and internet security could see it as a worth cause to contribute to. An open source release of such a website would greatly increase transparency, which could also make the process of finding a willing host more difficult. If the relatively small security flaws that have taken down the drug empires on-by-one are avoided, an anonymous online marketplace may be viable in the near future. We are undoubtedly in a critical period for the development of anonymity on the Internet, the results of which remain to be seen.

References

http://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/

http://www.bbc.co.uk/news/technology-24371894

http://www.wired.com/threatlevel/2013/11/silk-road/

http://www.businessinsider.com/silk-road-alternatives-2013-10

http://www.businessinsider.com/silk-road-2-2013-11

http://mashable.com/2013/10/04/silk-road-by-the-numbers/

https://twitter.com/DreadPirateSR

http://www.i2p2.de/how_networkcomparisons

http://www.forbes.com/sites/andygreenberg/2013/12/01/silk-road-competitor-shuts-down-and-another-plans-to-go-offline-after-6-million-theft/

http://www.ibtimes.co.uk/articles/514988/20131018/black-market-reloaded-silk-road-alternative-online.htm

http://www.ibtimes.com/atlantis-illegal-online-drug-marketplace-forced-shut-down-due-security-reasons-outside-our-control

http://www.slate.com/blogs/crime/2013/10/17/black_market_reloaded_silk_road_s_biggest_competitor_shuts_down_after_site.html