naJustin Sullivan
Wednesday, December 14th, 2016
Computer Security
Ming Chow

The Darknet and it's Dangerous and "Invincible" Illegal Bazaars

Whether its original users like it or not, the Darknet has become engrained into the global popular culture. As the internet and its use has managed to pervade almost every aspect of life at an exponential rate, it's shady underbelly was bound to expose itself to the world. With dozens of Law and Order storylines, the world's fascination with hacker culture and cyber security becoming a buzzword for every politician, something that was once shrouded in "darkness" has now been brought into the light. In late 2002, the U.S. Naval Research Laboratory released a new software called that had been in development since the mid-nineties called "The Onion Router" or Tor[1]. Tor is an internet browsing resource that conceals IP address by redirecting internet traffic through several thousand relays along with "onion" routing which is used to encrypt the data passed through these channels. Initially built as a security tool for the US government it was eventually released to the public. This marked the creation of the deep web, the portion of the internet hidden from search engines and traditional web users. As one would expected, this anonymity and safety was soon employed for less benign uses. Following in the footsteps of Ian Clarke, creator of illegal file sharing network Freenet, hackers began to exploit Tor and the deep web to create a place where illegal activity could be conducted under the blanket of safety that these tool provided[1]. This was the start of the Darknet.

Just as advertisers and business began to see the uses of the internet not long after its invention, It wasn't long before people began looking for ways to profit from the Darknet. As in any society, once you move away from subsistence and exploration the next logical evolution is trade. That is what happened with Darknet. The early Darknet could be seen as a hunter-gathering society, small tribes hackers doing smaller trades, deals and attacks. It takes the invention of currency to push these societies towards what we consider a semi-modern economy. This step was a complicated one to make within the Darknet because whatever currency would be used has to not only had to be digital but also had to be totally protected like the rest of the Darknet. There were several attempts to develop this digital currency, but they ended up being far too hackable.

Then in 2009, a new cryptocurrency, Bitcoin, was introduced. It was a nearly perfect solution. Along with being totally untraceable, Its value was "based only on market factors, unattached to any central bank" and there was a public anonymous ledgering system that would make hacking quite difficult[2]. It was with Bitcoin that the Darknet was able to move from a nomadic tribal existence to centralized communities based around bazaars. However these bazaars were not physical town squares filled with exotic spices and textiles, they were large, black marketplaces trading illegal wares, contraband and services. In an interview with Milwaukee Magazine, George Ledin a Sonoma State University computer science professor who tracks malware said most of these forums aim "serve their purpose without being overtly accessible or visible to too many"[3]. However, with Bitcoin and the exchanges gaining further exposure in the media and in pop culture thus bringing in more customers, a select few marketplaces were able to break this trend and become huge ventures with thousands of listings and users. These new “professional” exchanges now provide anyone with access to a Tor browser with opportunity to pursue that were too expensive, hard to find and highly illegal things like narcotics, hacking services, child porn and more. These networks are usually referred to as bazaars and I think that is a particularly apt name because, like a burgeoning society, the Darknet economy reached the point where there a markets and “trade routes” open to a large but still select group of people. It is only logical to assume that the next step is the corporatization of these forums.

Before these marketplaces became maintained, highly used services, the threat of deals made on the Darknet was far more abstract and hard to perceive because they were not centralized and few people were aware they were happening. However with the user bases and awareness of these exchanges growing the direct danger they pose to our community become far more clear.

In our web-obsessed culture, we are constantly reminded of the effects that the anonymity of internet can have on individuals. People are far more likely to not consider the real life consequence of their online actions when protected even by a totally traceable tweet or instant message. The Darknet provides an even higher and “real” level of protection to its users. Under the guise of the Darknet protection, individuals believing that they are safe to proport themselves in anyway they seem fit have direct access to these exchanges offering drugs, DDOS attacks and contracts for murder. If people behind the protection of their computer screen feel safe to send death threats to a fellow Twitter user, what is going to keep that person, within a few keystrokes, ordering a hit on them. Not only does a person using these networks pose a threat to other but it endanger the person themselves. A drug bought through the darknet could advertized as LSD but in reality be something far more potent or harmful. Hackers can be hired to do something and in the process, gain access to the buyers computer and systems.

The cultural stigmas and lessons about the dangers of illegal activity seem to go out the window when people feel a certain level of protection. This recklessness and lack of awareness that has allowed these marketplaces to gain popularity exponentially. With this growth in use it now becomes important for our society to think about how to handle and mitigate the effects of these marketplaces. With a concerted effort to analyze and observe these sites, we as a society may be able to curb their possibly detrimental effects.

In order to best investigate these Darknet exchanges it will be beneficial to focus on some practical examples. Two of the most famous marketplaces are Silk Road and Dark0de. These two sites reflect two specific categories of Darknet bazaar, one specializing in contraband and illegal services, Silk Road, and the other trading in hacker services, Dark0de. They are both the epitome of the these networks that started small and amateur and grew into strong and formidable platforms. Both were started by individuals who felt a combination of two things: a want to generate a good deal of profit and a general disillusionment or resentment for the “man” and the system.

Ross Ulbricht was one of these resentful individuals. In his LinkedIn page he wrote that he wanted “to use economic theory as a means to abolish the use of coercion and agression [sp] amongst mankind”[4]. In other words, Ulbricht was sick of corporations and governments straggling the rights of man. After many failed attempts to start businesses, Ulbricht discovered Bitcoin and hatched the idea of a digital black market where, safe for a few ground rules, anyone could sell whatever they wanted in a safe and protected environment. In 2011, under the pseudonym the Dread Pirate Roberts, Ulbricht released the first version of the Silk Road[2]. The site would become known specifically for drug sales and was popularized by a Gawker written in June of that year. Since then Silk Road has become synonymous with the online drug trade.

In interface it is very similar to Amazon or Ebay, “product descriptions and user ratings amounted to an encyclopedic information source”[2] and transactions were completed seamlessly with Bitcoin transaction and vacuum sealed protective shipping.The platform has become so popular that I know people personally, individuals who have little to no experience in programming or coding, who downloaded a Tor browser to utilize the exchange to both buy and sell wares. Silk Road is an example of a Darknet marketplace that has transcended the trope of only being able to a handful of hackers in poorly lit rooms. Preppy college students, Brooklyn hipsters and middle-aged suburbanites are gaining access to an unmediated, uncontrollable platform to partake in the purchasing and selling of illegal contraband. Silk Road is the prototypical example of how powerful a service can be when ingenuity, commitment to obtaining illegal goods and services and the Darknet are combined.

Slightly before this in the mid-aughts, Daniel Pacek, along with a few friends he had made on the internet, created an invite-only, online hacker community on his parents computer in Milwaukee called Dark0de[5]. It was a site hosted on the standard web where hackers deemed "good enough" could exchange their projects and opinions. Quickly, however, these hackers began to offer each other money to use each others botnets, which during that time were at best made up of only thousands of computers as opposed to today's millions[6]. Dark0de soon became a hacking services exchange, and just as with Silk Road, one that relied on Bitcoin and Tor. Unlike Silk Road however this is still a community that remains relatively "in the dark" to the general public. That does not mean, however, that is any less dangerous. In fact, Europol describe the exchange as "the most prolific English-speaking cybercriminal forum to date"[7]. It provides a community to thousands of blackhat hackers who have intention to harm individuals, corporations and governments. Considering the current climate and accusations of international cybercriminal activity, the danger that a community where incredibly skilled hackers can collaborate with and work for each other becomes even more clear.

With these two examples and the fear they may instill, the next logical question becomes how do we stop them? The short answer is no. The longer answer is that the FBI and other international agencies have tried to shut down just these two marketplaces on *several* occasions and were either unsuccessful or the community was able to reappear quickly. This can largely be attributed to the organization and strength of these communities themselves. Dark0de and the most recent iteration of Silk Road, Silk Road 3.0, like many other Darknet markets use bulletproof hosting described by

Brian Krebs as “the online equivalent of offshore havens where shady dealings go ignored”[8]. This along with other precautions make these sites very hard to dismantle or infiltrate. That being said, both sites have been shut down by the FBI at different times. However like any good programmer, the administrators of both sites quickly learn of the bugs in their systems, patch them, improve them and put them back online shortly afterward. Most recently in July of 2015 Dark0de was seized by the FBI and several members were arrested as part of Operation Shrouded Horizon[6]. *Two weeks later,* Dark0de was back online with higher levels of security and utilizing Bitcoin Blockchains[9]. Similarly Silk Road has gone through several major iterations due to seizures and hacks, with one going strong today.

Whether we like it or not, these marketplaces are here to stay. So now the question becomes, if we cannot eliminate these exchanges, how can we mitigate their effects? Clearly law enforcement agencies need to continue their attempts to quell these marketplaces and even shut them down for good. Until then however the quickest way to weaken these marketplaces is to minimize or eliminate the user base. This can and should be done through an organized and concerted effort, either by governments or an NGO to raise awareness of the threat of use Darknet use and specifically Darknet marketplaces. Throughout my adolescence and childhood I was exposed to nuanced and effective programs that warned me against reckless use of alcohol and drug abuse. However, the only lessons I had about safe computer and internet use were taught in 2 or 3 health classes during middle school. As internet and technology use becomes further ingrained in our lives and children are given larger access at a younger age, it becomes important to create a global movement to educate people, particularly from a young age, about the dangers of reckless computer use. This will cover a multitude of things including privacy, cyberbullying and use of the Darknet. Different types of curriculums could be taught to younger children, high schoolers and college students. As described above, when on the internet, individuals tend to forget the consequences of real life. If students are shown from a young age, consistently and creatively that these actions have true repercussions to themselves and other, they will be far less motivated to enter the void that is the Darknet. Seeing that these marketplaces keep returning and evolving, it unfortunately seems that awareness of their danger seems to be the only true way to weaken these institutions.

Like anything that creeps into the general culture of the world, it enters unchecked and without much context. Use of the Darknet is becoming less stigmatized and easier than ever, compound that with a general lack of awareness and knowledge of its true danger things like the Silk Road and Dark0de pose a daunting threat. Tools of anonymity like Tor and Bitcoin allow people to feel that they are hidden from the eyes of authority and without a consideration for repercussions, act in extreme and illegal ways. However like most things that enter global consciousness, a perspective and cynicism will grow that will help to curb the amount of people unknowingly entering this possibly destructive space. I believe truly one of the base ways to spur this is by organizing a movement that will promote awareness about the Darknet and inspire intelligent internet usage.

Bibliography

1. Mccormick, Ty. "The Darknet: A Short History." Foreign Policy. Foreign Policy, 9 Dec. 2013. Web. 14 Dec. 2016. <http://foreignpolicy.com/2013/12/09/the-darknet-a-short-history>.

2. Bearman, Joshua, and Tomer Hanuka. "The Untold Story of Silk Road." Wired. Conde Nast, Apr. 2015. Web. 14 Dec. 2016. <https://www.wired.com/2015/04/silk-road-1/>.

3. Hrodey, Matt. "Dark Side: The Rise and Fall of a Suburban Hacker." Milwaukee Magazine. Milwaukee Magazine, 12 Oct. 2015. Web. 14 Dec. 2016. <https://www.milwaukeemag.com/2015/10/12/dark-side-darkode-fbi/>.

4. Ulbricht, Ross. "Ross Ulbricht LinkedIn." LinkedIn. LinkedIn, n.d. Web. 14 Dec. 2016. <https://www.linkedin.com/in/rossulbricht>.

5. Poplin, Cody M. "The Lawfare Podcast: Daniel Placek on Darkode." Lawfare Blog. Lawfare, 13 Feb. 2016. Web. 14 Dec. 2016. <https://www.lawfareblog.com/lawfare-podcast-daniel-placek-darkode>.

6. Abumrad, Jad, and Robert Krulwich. Audio blog post. RadioLab. RadioLab, 21 Sept. 2015. Web. 14 Dec. 2016. <http://www.radiolab.org/story/darkode/>.

7. "Cybercriminal Darkode Forum Taken down through Global Action." Europol. Europol, 15 July 2015. Web. 14 Dec. 2016. <https://www.europol.europa.eu/newsroom/news/cybercriminal-darkode-forum-taken-down-through-global-action>.

8. Krebs, Brian. "Krebs on Security." Krebs on Security. Brian Krebs, 20 May 2013. Web. 14 Dec. 2016. <http://krebsonsecurity.com/2013/05/conversations-with-a-bulletproof-hoster/>.

9. Clark, Liat. "Hacker Forum Darkode Is Back and More Secure than Ever." WIRED UK. Wired, 23 May 2016. Web. 14 Dec. 2016. <http://www.wired.co.uk/article/darkode-back-and-more-secure>.