Brandon Buchanan
Internet and Computer Law
April 10, 2013

Internet crime has existed ever since scrupulous people recognized the important economic effects that the Internet created and how its vulnerabilities could be taken advantage of for their own gain. While some amateurs may utilize the Internet to perform crime believing that they are secured from being discovered, professional offenders often use computer programs, anonymous networks, or clever techniques in order to covertly operate and stay hidden from authorities, all while running systems that can generate massive amounts of income at the push of a button. Many laws related to cybercrime were enacted before the prevalent use of the Internet by mainstream society, leading to sometimes outrageous cases, but the majority of cases are handled appropriately.

Recently, malicious code has been spreading on the Internet via obscured executable files transmitted through Skype. Once executed by a user, the malware uses the computer's processor cycle to mine for BitCoins, a decentralized and anonymous digital currency that is generated by computers joining the BitCoin network and running proof-of-work calculations to find the next BitCoin. The value of a single BitCoin has increased greatly in a short span of time due to financial concerns in parts of the world, allowing a savvy investor to make a large return on their currency exchange or a malicious individual or entity to massively mine for new BitCoins using infected computers across the world and make a good income. Because the Internet spans across international boundaries, prosecuting offenders in some countries makes the process difficult.

Just as BitCoins have helped facilitate anonymous commerce transactions, hidden website services running in the Tor network have helped as well. The architecture of the Tor network is such that a user's traffic is encrypted and anonymous so that no node knows both endpoints of a connection or the content flowing through it. Silk Road offers a medium where

sellers can advertise goods and buyers can purchase them using BitCoins. While anything can be advertised on Silk Road, it is heavily used drug trafficking, as well other illegal activities. While it can be extremely hard for law enforcement to prosecute users of these services, it is not impossible. According to Wired, an Australian citizen plead guilty to "importing a marketable quantity of a border-controlled drug" after using Tor hidden services to have drugs delivered to his home. While the offense is not directly a cybercrime, the perpetrator relied on the encryption and anonymity of the Tor network to mask his activities in order to successfully traffic the illegal goods.

There is looming controversy over the laws that stand to prosecute cyber criminals because the laws that protect us today were implemented during a time before the Internet's expansion and involvement in everyone's daily lives. The Computer Fraud and Abuse Act has been used to harshly punish menial crimes that would have otherwise been easily decided had a computer not been involved. In *United States v. Aaron Swartz*, the government alleged that Swartz's mass downloading of white papers and intellectual material from the online database JSTOR was punishable by up to 35 years in jail, despite that the information copied was easily available to university students and researchers. Sadly, after two years of prosecution, Aaron Swartz committed suicide, leaving an enraged online community to pressure the United States to call off such prosecution attempts of others.

Outstanding

100

Malware Forces Your Computer Into The Bitcoin Mines – The Blogs at HowStuffWorks

Wednesday, April 10 2013, 11:33 AM

Malware Forces Your Computer Into The Bitcoin Mines

by **Jonathan Strickland** | April 8, 2013

Tweet 1 people like this. Be the first of your friends.

If Spielberg and Lucas were to remake *Indiana Jones and the Temple of Doom* and set it in the present, our intrepid hero might be attempting to free thousands of computers rather than children from enslavement. According to **ZDNet**, Internet security firm Kaspersky Labs discovered some malicious code — aka malware — out in the wild that forces computers to mine for bitcoins. So what does that actually mean?

Bitcoin is a digital currency, meaning it has no physical form. Instead, it's bits of code, just like any other piece of software. The code is encrypted and contains within it a hash. A hash is the end product of some sort of mathematical process (it varies from hash to hash). Basically, the way bitcoins enter circulation is through "mining." In this case, mining doesn't involve taking a pickax to a rock wall. Instead, a computer mines a bitcoin by figuring out which numbers combined to create the hash in a block of code. This involves performing millions of calculations as the computer goes through every possible combination of numbers that could have produced the hash.

Bitcoin's design is clever in that the difficulty of the mining process depends entirely upon how much computing power is being directed at mining. If a lot of processors are trying to find that next bitcoin, the difficulty ramps up. If people get discouraged and quit, the difficulty decreases. This way, the flow of bitcoins into circulation remains steady. There's also a cap on how many bitcoins will ever be in circulation, which I suppose is to prevent the currency from becoming worthless due to an endless supply.

The value of bitcoins — the **Washington Post** reported a couple of days ago that the currency hit an all-time high exchange rate of $147 per bitcoin — means that a lot of people are interested in mining them. But how do you have a chance of mining a digital currency that gets harder to find the more people look for it? A single computer — even one with a decent **GPU** parallel processor — doesn't stand a chance against the more powerful mining rigs out there. Enter the malware.

The malicious code Kaspersky Labs detected pulls computers into a botnet, also known as a **zombie computer army**. The code allows hackers to repurpose a compromised computer's processor to mining for bitcoins. Corrupt enough computers and you've got a huge amount of processing power you can use to find new bitcoins out there. Meanwhile, the victim sees his or her computer performing under par. It may also leave the computer vulnerable to future attacks or manipulation.

The ZDNet story mentions that hackers are distributing the malware with file names that tempt people into opening them. An example might be "is this you in this video." The hackers are counting on our curiosity to trick us into installing malicious code. The best advice is to always be suspicious of any files you come across online. Verify that the file is legitimate before opening it.

While all this is interesting, I still wonder if bitcoins are ever going to be a widely-accepted currency. At the moment, I'd say they're more of a commodity. People want bitcoins because they're worth a lot of "real" money. There's not a large enough marketplace to spend bitcoins to make them worthwhile as an actual currency. I'm skeptical that there ever will be.

Study: Online marketplace Silk Road sells £1m worth of drugs each month

According to a report in The Age Paul Leslie Howard used Silk Road to buy and import the illicit drugs on 11 different occasions. Australian Customs and Border Protection Service officers in Melbourne and Sydney examined mail -- most of which came from the Netherlands and Germany -- destined for his home. They found 46.9 grammes of MDMA and 14.5 grammes of cocaine. The federal police then raided his house in July 2012 and found digital scales, ziplock bags, $2,300 (£2,000) in cash, 35 stun guns disguised as mobile phones and a money counter. They also found two working mobile phones, and forensically analysed more than 20,000 text messages. In amongst them were incriminating texts such as "I got five grand worth if you want" and "promote the LSD I got more in. I sold 200 cubes last week".

Howard has pleaded guilty to two charges of "importing a marketable quantity of a border-controlled drug", which carries a maximum jail term of 25 years. He also pleaded guilty to possessing controlled weapons. During the trial he said that he had been drawn to the site after reading an article by a journalist called Eileen Ormsby, who regularly covers the Silk Road in Australian newspapers. Since Howard's conviction, the Silk Road has warned its users via its Twitter account not to follow their feed nor the feed of Ormsby with their real names.

Prosecutor Morgan Brown made it clear that the authorities had a lot of information about Howard from the Silk Road, including access to his profile, which he registered under the name Shadh1 in April 2012. He set up a vendor's account offering up cocaine and speed and saying that he is looking to "branch into more as I get more coin back in my pocket".

At the time of Howard's arrest, the Australian Federal Police and the Customs and Border Protection Service issued a warning to any would-be drug traders using supposedly anonymous marketplaces such as the Silk Road saying they could be identified by police techniques.

AFP manager of crime operations Peter Sykora said in a statement: "Criminals are attempting to exploit the international mail system through online networks, but the recent arrest demonstrates that we are one step ahead of them. The AFP will continue to identify, investigate and prosecute individuals or groups importing narcotics into Australia, including via illicit ecommerce platforms such as Silk Road."

Australian police aren't the only ones to crack down on the Silk Road. The DEA in the United States is also on the warpath, targeting similar sites such as the Farmer's Market. In July 2012 the organisation told a US news station KXAN that it was investigating the Silk Road and in November 2012, DEA spokesperson Rusty Payne told