# SETEC ASTRONOMY

## Athenaeum Society

Raise your hand if you recognize the title of the paper? How many of you remember the movie Sneakers? The action/spy thriller from 1992 staring Robert Redford, Ben Kingsley, Dan Ackroyd and others involves the theft of a computer device capable of hacking into any secure computer system on Earth. At one point, when the curious band of spy experts learn this device, concealed inside an answering machine box, can tap into the Federal Reserve, the national power grid and the national air traffic control system, they simultaneously realize they have both something incredibly valuable, and something "any government on Earth" would kill them for. "SETEC ASTRONOMY" is the name of the project under which this device was developed. Redford's character while playing Scrabble discovers the name, SETEC ASTRONOMY, is actually an anagram of the phrase "Too Many Secrets."

We learn the device was created by the NSA but was stolen to break down walls and bring down corruption, a la Wikileaks, founded by Julian Assange in 2006. Where do secrets, our secrets, go when they're taken? The Dark Web.

There are 40 members of the Athenaeum Society. We each have spouses, children or parents, some of whom we loved enough to invite to this open meeting tonight. Most of us and our loved ones are carrying a modern computer on or about our person. Some of us are technology averse and refuse to bother with on/off switches, much less passwords, Facebook feeds and tweets. In fact, we all know and love people in our lives that look at us funny when we use those words. Feeds, tweets, post, share a post, like or fav a post or a tweet, and retweet.

As you all have surely learned by now, I'm eyeball deep into technology. I'm what's known as an "early adopter" of gadgets and media tools. I'm the go-to IT guy in the Westerfield family tree, and I might have even one day given my father a run for his money on technology

know-how. But for all my unabashed nerdness, a part of me can't help but believe all those people we know who refuse to embrace the digital age are the smartest ones around.

Sure they've forgone many modern conveniences, but without realizing it, they have also maintained a protection, while not impregnable, against modern intrusions into their private lives.

What intrusions am I talking about? More often than not, these intrusions aren't intrusions in the technical sense at all, but rather invitations. What do I mean? Google, Facebook, FourSquare, LinkedIn: all of these have something in common. They rely on users volunteering inconceivably large sums of data in exchange for a free service of some kind.

How many of you use Siri or Google Now for anything on an even semi-frequent basis? Does anyone here use Google Home or Amazon's Echo and Alexa? The use of these kinds of digital personal assistants is exploding, such that every major player in the technology space has ventured into that territory. We use so many devices that are far more capable than we think, and that are based on services that interconnect far more than we suspect. I believe Google is in the front here, for better or worse, by shamelessly mining its users for data and using it to allow advertisers to make highly specialized, precisely targeted ad campaigns.

Our phones and the apps they run know where we are, how long we've been there, when we leave, what the temperature is in our homes, when we're home and when we aren't, who we talk to, how often and how long we talk to them (and the NSA probably knows what we're saying), what our voices sound like, what we look like, what gender we are, what movies we watch, what we search for online, what kind of products we buy and how often we buy them, and increasingly, these modern day convenient gadgets are replacing our wallets and pocketbooks. I recall the first commercial flights whose boarding passes I stored only on my phone, the handful of occasions when I had to visit the self-serve kiosk to get a paper boarding pass printed for an airport that didn't have a scanner to read the QR code on my phone. When I

boarded a plane last week in Nashville the smartphone boarding passes far outnumbered the paper copies.

The bottom line is that we're sharing data, and pretty revealing data about ourselves and our lives at an astounding pace. We are sharing a bunch of data with the world - more data than we know. In a recent study[1] 50% of adults have shared an explicit email or text with someone else - keep looking at your neighbor - which means that if you didn't send it, the person next to you did! This is actually about 12% higher than the share of the adult population that would share bank account information, and 7% higher than the number of adults who would share a password.

Why does this matter? Well, it matters because that data is intensely personal and valuable. And just as our protagonists in Sneakers understood, where there's a valuable asset there are almost always shady, if not outright criminal actors to take advantage of it. Unfortunately, those criminals have found and thrived in a breeding ground for criminality in the digital age known as the "dark web." It is in the mysterious and bottomless pit of the dark web that our data often finds its way.

What is the "Dark Web"? It's not the web you know, but coexists with it every day. To understand the dark web let's put things into perspective. Run a Google search and see how many hits come back for a given query. The number is normally huge. Since Amanda and I are soon to be in the market again I ran a search for "baby formula" last week that brought back 79 Million search results. A search of the word "twitter" brought back 25.27 Billion results. That's an incomprehensible amount of search results, yet when you run a google search you're only hitting the "normal" web, or the internet as you know it. Those "normal" search engines don't or can't access and index what's known as the "dark web."

[1] Jason Thomas: https://www.youtube.com/watch?v=Z1tFPtWhT8c&feature=youtu.be

In fact, the internet we know is incomprehensibly large, and growing at an exponential rate.[2]

- 1 billion sites
- 3 Billion users
- 3.5 Billion searches are run daily
- 500 Million tweets sent out everyday
- 150,000 HOURS of video uploaded to YouTube everyday

But as the so-called "surface" web grows, the deep and dark webs grows even faster. The dark web is a place built for anonymity, and, unfortunately, the most vile and upsetting conduct and content you can fathom.

The "dark web" isn't accessible through the apps your currently have, You can't get there using Windows' Internet Explorer, Apple's Safari or Google's Chrome browser. But it is freely available, and, within a few minutes, you could be surfing the internet's underbelly just as swiftly as you surf its surface. The dark web is accessible through various programs, but the most popular client to use is called the TOR Browser (The Onion Router, torproject.org). TOR, formerly a product of funding from the U.S. Naval Research Laboratory in order to protect government communication, uses a distinct protocol and encryption process. This encryption actually conceals your IP address, which is like the fingerprint of your computer, so that your browsing habits and history are nearly impossible to track.

Listen to this description offered by the folks behind TOR:

> *The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you — and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going.*
>
> *To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way*

[2] https://www.thenakedscientists.com/podcasts/naked-scientists/internet-good-bad-and-ugly

> *knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.*
>
> *Because each relay sees no more than one hop in the circuit, neither an eavesdropper nor a compromised relay can use traffic analysis to link the connection's source and destination.*

The best example of the "dark web" would be the infamous "Silk Road" investigation from a few years ago. This modern "Silk Road" refers to the name of a dark web marketplace that was launched around 2011 by a young dark web entrepreneur, Ross William Ulbricht. He was in his mid-twenties at the time. Ulbricht went by the online persona of "Dread Pirate Roberts" (a referenced to "The Princess Bride") in his role as founder and administrator of Silk Road. However, in 2015 he was convicted of multiple felonies and is currently serving a life sentence without the possibility of parole. Ironically, he was caught by, among other things, soliciting a hitman using the Silk Road site. The hitman he was communicating with was actually an undercover federal agent.[3]

Interestingly, the trial of young Mr. Ulbricht revealed chat logs showing conversations with another character in the Silk Road tapestry, Variety Jones. Those chat logs actually indicate it was Jones that suggested Ulbricht embrace the fanciful pseudonym.[4]. I cannot locate any current information on the whereabouts of Mr. Jones.

Silk Road, in its short run, still managed to draw in approximately 1 Million users, nearly a third of which were located in the United States. Ulbricht's indictment claimed the site had generated over 9.5 Million Bitcoins in revenue, and over 600,000 Bitcoins in commissions for Ulbricht himself.[5] The value of the nascent bitcoin cryptocurrency have fluctuated wildly since

---

[3] U.S. v. Ross William Ulbricht, Criminal No. CCB-13-0222, INDICTMENT, https://www.ice.gov/doclib/news/releases/2013/131002baltimore.pdf

[4] https://www.wired.com/2015/02/ross-ulbricht-didnt-create-silk-roads-dread-pirate-roberts-guy/

[5] https://www.wired.com/2015/02/ross-ulbricht-didnt-create-silk-roads-dread-pirate-roberts-guy/

its creation, but the FBI's cyber crime investigator leading the Silk Road case, estimated the site generated about $1.2 Billion in sales, good enough for $80 Million in commissions for Ulbricht. Bitcoin was a currency built for TOR and the Dark Web, allowing owners to remain anonymous. The technology itself is worthy of another stand alone paper. There are no, and can be no, more than 21 Million Bitcoins in existence because of the limitations of the code. The currency is not managed or backed by any government, and the transactions are all recorded in a publicly accessible ledger. However, there is not way to connect a Bitcoin account number with any specific person, hence the anonymity and the allure to the vendors and customers of places like Silk Road.

If you happen to have a Bitcoin wallet, and by chance were an early adopter of the currency, you have a substantial fortune in today's dollars. As of earlier this week, 1 Bitcoin is valued at approximately $1448.48.

The Silk Road is certainly the highest profile marketplace on the Dark Web. The site was shut down by the FBI following Ulbricht's arrest, only to be relaunched by some of Ulbricht's lieutenants, only to be shut down again. The site was "the amazon.com of vice" according to a blogger from Wired. Ulbricht's indictment was a smorgasbord of the offerings of Silk Road. Guns, hackers or hitmen for hire, counterfeit money and government documents (passports) and drugs of literally all kinds were the most popular items. Unfortunately, the dark web gets still darker.

Simply put, the anonymous TOR network has fostered marketplaces of some of the most vile, evil content one can imagine. Dealing with trafficking in drugs is bad enough, but the dark web sees the *sale of people*, the intentional and violent assaults of others for sport. It reminds me of the citizens of The Capitol in the series, "The Hunger Games." People seem to take such pleasure and delight, without remorse or sympathy, in the pain and suffering of others.

And note there's always a sense of nobility concealing a true financial motivation. Ulbricht and the team at torproject.org alike maintain noble reasons for pursuing the technology they're behind. Ulbricht wrote on his LinkedIn page, ""I want to use economic theory as a means to abolish the use of coercion and agression (sic) amongst mankind."[6] If you take a few minutes to read the FAQs for the TOR browser you'll get a sense of the honor its proprietors feel in maintaining a secure platform that allows "journalists…to communicate more safely with whitleblowers and dissidents," or "individuals…use TOR for socially sensitive communication." The browser is billed as a safe method to "speak and read freely online." And while those are arguably legitimate reasons to use TOR, the bulk of the traffic through the network is nefarious and felonious.

That brings us back to the data we share so freely, and usually unknowingly, and the inherent risks involved in expanding our digital lives. In short, the potential exposure to data breaches for most people is enormous, and the Dark Web is where much of our data goes.

Once you load the TOR browser you can pull up a site known as "the hidden wiki" which pulls up a plain list of linked sites, separated by category. Finance, Official Documents, Drugs, Weapons, Pornography and a host of others.

One such site, called "PayPal Center," allows one to browse hacked PayPal accounts like you were picking out songs in iTunes, showing the account balance for each account, and the price to buy those credentials, in Bitcoin, no less.

On another, you can scroll through long lists of stolen credit cards, with credit balances and localities provided, along with a price in Bitcoin to purchase them. We hardly go a couple weeks without hearing about a massive data breach that exposes tens of millions of user accounts, filled with Personally Identifiable Information, to this criminal community.

Other examples of Dark Web sites include:

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

- EuroArms sells and delivers weapons (without ammunition).
- You can hire assassins through a service called "White Wolves."
- Child pornography is readily available through countless sites.
- The Human Experiment details medical experiments performed on people against their will[7]

And we thought scummy websites like Topix were bad.

An expert in this field that I've had an opportunity to hear speak on the subject will often run a live demo from a machine he uses specifically and exclusively for TOR browsing. He's able to pull up stolen credit cards by geographic location. On another site, much like eBay, he's able to purchase radioactive material. I have no desire to install the TOR browser on any computer. As it is, with the various web searches I performed in researching this paper, I'm now reasonably confident I'm on some sort of government watchlist.

Just this week a hacker, or group of hackers, known as The Dark Overlord, tried to extort Netflix with the threat of releasing stolen episodes of a heretofore unreleased production. On Monday the hackers made good on their threats, releasing several episodes in an unreleased season of "Orange is the NW Black." The group claims it has additional unaired content from ABC, NBC, Fox, FX, IFC and National Geographic. The video content was stolen from a production studio whose network security was compromised sometime last year.[8]

To offer some perspective on the scope of the problem I want to share some key findings from a study done by Bitglass, a data security firm, that created a "complete digital identity for an employee of a fictitious retail bank, a functional web portal for the bank, and a Google Drive account, complete with seemingly real corporate and personal data. Among the files in the Google Drive were documents containing real credit card numbers, work-product, and more.

[7] http://www.businessinsider.com/tor-silk-road-deep-web-2013-3#the-hidden-wiki-catalogs-several-tor-sites-that-would-otherwise-be-impossible-to-find-it-shows-you-a-number-of-sites-offering-things-for-sale-both-legal-and-illegal-1

[8] http://variety.com/2017/digital/news/netflix-hackers-additional-shows-movies-1202404171/

The team then leaked the employee's "phished" Google Apps credentials to the Dark Web. What the hackers didn't know was that each file in the Google Drive was embedded with a watermark and all activities, from logins to downloads, were being tracked by Bitglass, deployed in monitor-only mode."

*Bitglass Study findings*

- *Over 1,400 hackers viewed the leaked credentials.*
- *One in 10 hackers attempted to use the leaked creds at the bank web portal.*
- *There were five attempted bank logins within the first 24 hours.*
- *Visitors to the bank site came from over 30 countries across six continents.*
- *68 percent of the attempts on either the Google Drive account or bank account were from Tor-anonymized IP addresses.*
- *12 percent of those hacking the Google Drive account attempted to download files with sensitive content.*
- *There were three attempted Google Drive logins within the first 24 hours.*
- *94 percent uncovered and attempted to log into other accounts.*

The dark web shows no signs of slowing down, and the methods by which bad actors obtain data, or share it anonymously become more sophisticated by the day. Public policy is woefully behind, as it often is, and I have little hope it will ever catch up, much less keep pace. That means the burden is largely on our own shoulders to be more informed about the realities of the world we live in, especially as we continue to live and operate in the digital space.