**What’s Lurking in the Deep End of the Internet?**

Last month, a jury convicted Ross Ulbricht as the ringleader of the notorious Silk Road website. The largest online black market, until it was shutdown by the Federal government in 2013, was the poster child of the so-called “Deep Web” and was best known as a platform for selling illegal drugs. Meanwhile, Darpa unveiled on *60 Minutes* recently that the agency is developing a new search engine (Memex) that aims to make it easier for law enforcement and government to track illegal activity on the Deep Web. So what exactly is the Deep Web?

Like an iceberg, the vast majority of the Internet is obscured from easy view. This unindexed section of the Internet is dubbed “the Deep Web.” Experts agree that it is impossible to accurately gauge the exact size and scope of the Deep Web, but some dare to put the figure at hundreds of times the size of the visible or “surface” Internet.  While most of this content is innocuous, more and more criminal activity is moving away from the light of day and into to the shadowy corners.

Accessing the Deep Web requires specialized knowledge and tools, as well as an anonymity network to guarantee privacy protection for users. Tor is an example of such a vehicle. Developed by the U.S. Navy more than ten years ago, Tor (The Onion Router) was designed to prevent browsing activity from being traced back to the user. Silk Road was operated as a Tor hidden service, enabling users to browse it anonymously and securely.

In addition to the skill and infrastructure needed to access a deep web presence, black market operators generally take additional security procedures to ensure their sites are not found and shut down by the authorities, and that users’ identities are protected. These measures may include hosting sites with bullet-proof servers, where the host agrees not to reveal information about the people using the platform, regardless of the circumstances.

The underground markets have long become gathering points for hackers wanting to buy and sell information, while enjoying anonymity and escrow services from operators.  These markets continue to grow more sophisticated every day, and are developing into a “supply chain” for all kinds of illegal activities, where each party within the chain specializes in their unique piece of a nefarious puzzle.

For example, hackers who are skilled enough to breach a network and extract information may not have the interest or the resources to then use those credentials to steal actual funds. Instead, they are increasingly finding it more profitable to go into the Deep Web and find a buyer for the information (credit card numbers, Social Security Numbers, other personal data) and sell it to them.

Today, the Deep Web has evolved and has turned into an immense information-sharing tool that is making it easier for criminals to do their job more thoroughly. For example, someone may purchase your Social Security Number from one data broker. Then, in order to buy a car under your name, they may need to know information such as your physical and email addresses, phone numbers, current and historical career history, and answers to security questions. Putting the information together from multiple data brokers (typically from multiple breaches) can provide these criminals a comprehensive, credible dossier that makes it far easier to impersonate someone.

The recent evolution of the Deep Web has allowed fraud to become increasingly commoditized and easier to do, simply because there are many ways to monetize the fraud process itself. As it continues to mature, we expect to see increasingly sophisticated fraud based on the ability to mine the Deep Web for a variety of information. The Darpa Memex project is a great first step in leveling the playing field. But it will take a coordinated effort between government and the private sector to catch up to the very large lead that the hacker community has been building.

Daniel Ingevaldson is Chief Technology Officer of Easy Solutions.

https://www.wired.com/insights/2015/03/whats-lurking-deep-end-internet/

# The disturbing world of the Deep Web, where contract killers and drug dealers ply their trade on the internet

Hiring a hitman has never been easier. Nor has purchasing cocaine or heroin, nor even viewing horrific child pornography.

Such purchases are now so easy, in fact, that they can all be done from the comfort of one's home at the click of a button... and there's almost nothing the police can do about it.

This worrying development of the criminal black market is down entirely to the Deep Web - a seething matrix of encrypted websites - also known as Tor - that allows users to surf beneath the everyday internet with complete anonymity.

The Deep Web has existed for more than a decade but came under the spotlight last month after police shutdown the Silk Road website - the online marketplace dubbed the 'eBay of drugs' - and arrested its creator.

But experts warn this has done next to nothing to stem the rising tide of such illicit online exchanges, which are already jostling to fill the gap now left in this unregulated virtual world.

So for those looking to bump off a difficult acquaintance, all they have to do is enter the Deep Web - known also as the 'Dark Web' or the 'Undernet' - and search 'hitman for hire'.

There they are presented with lists of willing assassins touting their wares to anyone who will pay.

And like The Silk Road, transactions are all made using the mysterious online currency Bitcoin. One site, whose name MailOnline has chosen not to publish, offers an assassination in the US or Canada for $10,000 and one in Europe for $12,000.

'I do not know anything about you, you do not know anything about me,' crows one self-styled assassin, according to The Daily Dot. 'The desired victim will pass away. No one will ever know why or who did this. On top of that I always give my best to make it look like an accident or suicide.'

'I have gained endless experience(s) in this [sic] 7 years,' he goes on. 'It has changed me a lot. I don't have any empathy for humans anymore.

'This makes me the perfect professional for taking care of your problems and makes me better than other hitmen. If you pay enough I'll do ANYTHING to the desired victim. If I say anything I mean anything.'

Many of the sites even use slogans and marketing techniques that, if it weren't for their macabre subject matter, could be as at home on the website of a legitimate retail website.

'The best place to put your problems is in a grave,' boasts one.

Some even seem to offer others the chance to profit from their killing by allowing users to bet on when a victim will die by putting money in a pool. The closest guess takes home the pot.

And while many appear every inch the cold-blooded killer one would expect from a gun-for-hire, there is also apparently the odd humanitarian hitman.

'Killing is in most cases wrong, yes,' writes one. 'However, as this is an inevitable direction in the technological evolution, I would rather see it in the hands of me than somebody else.'

'By providing it cheaply and accurately I hope that more immoral alternatives won't be profitable or trusted enough. This should primarily be a tool for retribution.'

Adding that murder should always be committed for 'good reason', he writes: 'Bad reasons include doctors for performing abortions and Justin Bieber for making annoying music.'

The Silk Road's creator, Ross Ulbricht, was arrested last month after allegedly hiring an undercover FBI agent to murder a member of the site who was apparently blackmailing him. He allegedly also tried to have an employee killed who he thought might blow his identity to police.

Meanwhile, even as the Silk Road was trundling to a halt, already hundreds of other websites were springing up in its place, peddling anything from drugs to stolen identities, illegal weapons to sickening child pornography and even explosives.

In June it emerged one such site, called Atlantis, was even offering its wares in an advert posted on YouTube.

Looking like an advert for a well-funded Silicon Valley start-up, the slick promo video for Atlantis boasts that it is 'the world's best anonymous online drug marketplace'.

It comes as the site's backers announced the launch of a 'big social media campaign' that seems intended to make a play for the market share of the better-known Silk Road.

But while experts say police are all but powerless to shut down websites selling illicit products, authorities claim they are making inroads in their bid to stifle the Deep Web's growth.

The U.S. federal government appears to have been forcing the shut down of pedophiles communities on the shady underbelly of the Internet by targeting sites hiding within the Deep Web.

August saw the arrest of Irishman Eric Eoin Marques, who the FBI has called 'the biggest facilitator of child pornography on the planet'.

Marques is accused of running Freedom Hosting, a web hosting service that operates on the anonymous Tor network. Forums on Freedom Hosting allegedly allowed pedophiles to anonymously share horrific child pornography and trade tips on how to sexually abuse children without getting caught

http://www.dailymail.co.uk/news/article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html