The new underbelly

Eileen Ormsby
June 1, 2012

Read later | Comments 162

The Dark Web, the parallel internet that can be found only through encrypted private networks, unknown by many and accessed by few. *Photo: Peter Riches*

It's called the Dark Web and once you are in you can buy people, drugs, guns and even have someone killed. The problem is: what can law enforcers do about it?

Deep in cyberspace is a web of private networks hosting sites that Google will never find and videos that YouTube will never play. Within this web, drugs and guns are bought and sold, hitmen advertise their services, hackers can be hired to attack an enemy's computer and pornographic images to satisfy the most depraved tastes can be downloaded.

It is a place where freedom of speech is absolute and unconstrained. It is the Dark Web, the parallel internet that can be found only through encrypted private networks, unknown by many and accessed by few.

The question being asked by law enforcement agencies is: how should they be regulated? Can they be regulated? The federal Attorney-General, Nicola Roxon, has proposed legislative changes that could lead to the web history of any device connected to the internet being logged and retained for up to two years for law enforcement purposes.

"We must stay one step ahead of terrorists and organised criminals who threaten our national security," Ms Roxon said last month.

But such measures will have no effect on those who conduct their criminal activities on the Dark Web because nothing is logged — there is no history to keep. And some argue such measures will cause more people to seek out anonymity services — the same services that provide access to the Dark Web.

"The Dark Web is the new underbelly of the internet," says Ken Gamble, chairman of the Australian chapter of the International Association of Cyber Crime Prevention. "It's seemingly uncontrollable, but of course there is a lot going on behind the scenes [by law enforcement agencies] that the public doesn't know about."

Drugs are the most common items for sale, but there are also online markets for weapons and explosives, false passports, entire new identities, counterfeit cash and fake diplomas. There are sites that claim to sell human organs that the buyer can collect from a Third World country and those that promise to procure exotic animals. Then there are the services; on offer are contract killings, hackers for hire, money laundering, theft-to-order, university papers and match-fixing.

Other sites offer porn that cannot be found on the regular internet — or "clearnet" in Dark Web speak. This includes child porn (prepubescent children), "jailbait" porn (young teens), zoophilia or bestiality and "hurt porn",' which shows children and adults being subjected to pain.

An Australian Federal Police spokesman said the ability to use technology to commit crime was a real threat. "From a law enforcement perspective, this means we need to develop new methodologies to ensure perpetrators cannot hide behind technological advances."

"Hidden services" that enable people and organisations to host or access illegal material while their identity and location remains secret come bundled with anonymity software. Tor, originally developed in conjunction with the US Navy to protect government communications, is the most widely used, with more than 36 million downloads last year and between half a million and a million daily users.

"We are pretty familiar with the Tor network, because a lot of the criminals use that," Gamble says.

Andrew Lewman, executive director of The Tor Project, says its positive applications outweigh the negative. "Tor's original design was to give users privacy and anonymity online and that's still the core of what we do.

"We produce software that we give away free [so that] anyone anywhere in the world who needs their privacy online can have it."

This includes whistleblowers (WikiLeaks recommends it for releasing sensitive information) and human rights workers in hostile regimes, but Lewman says the vast majority of Tor usage is by "normal people who are just looking to not give out all their information: who they are, where they are and every website they visit".

Tor's hidden services began as a research project by US and Norwegian militaries to determine whether an anonymous platform could be developed to help people working in hostile regimes. If nobody, including Tor, knows who runs a website or where it is hosted, that information cannot be revealed. And if a server gets confiscated, there will be no IP trails or records of traffic to compromise operations. "Of course, criminals will pick up on that too, but criminals are opportunistic. That's why they're criminals," Lewman says.

When the Tor software is downloaded, users have access to so-called "onion sites". Because the sites are not designed to be found by search engines, users must either know the exact URL they want or use one of the available gateway sites.

The best known of the onion sites is the illegal drug marketplace Silk Road. Slick, professional and thriving with a multimillion-dollar turnover, Silk Road has set the standard for online black markets.

Its owner, known as Dread Pirate Roberts, claims to take a "high moral ground" when it comes to what it will sell; it refuses to list any items or services the intent of which is to defraud or cause harm to another person.

Black Market Reloaded (BMR), has no such pretences of conscience. Run on a similar platform to Silk Road, it sells not only drugs, but firearms and explosives, stolen Paypal accounts and credit card numbers, online banking account numbers and passwords, and contract killing services.

There are several offers of Australian bank account details for a percentage of the balance amount. The vendor offering Australian bank account details has good feedback for most transactions, but three claim the seller is a scammer.

Scammers and law enforcement are the main concerns of users of the black-market sites — in that order. Although buyers have the protection of an escrow and dispute resolution service on the larger sites, sellers sometimes persuade buyers to transact out of escrow. Or they plan a long con, as happened recently on Silk Road when the site's top-rated and most trusted seller of cocaine and heroin disappeared with an estimated $250,000 of Silk Road customers' money.

Identity items are another high-demand black-market product. These range from $5 driving licence copies that are good for nightclub entry but not much else, to passports that are "genuinely generated from within the IPS system of the UK government and guaranteed good for travel" for $4000.

The black markets and services almost exclusively use the virtual online currency Bitcoin. An April 2012 report apparently by America's FBI (marked for official use only but leaked to the internet in early May) claims that the unique features of Bitcoin present distinct challenges for deterring illicit online activity.

While Bitcoin has legitimate uses, it is likely to continue to attract cyber criminals due to the ability to transact anonymously. "Since Bitcoin does not have a centralised authority, law enforcement faces difficulties detecting suspicious activity, identifying users and obtaining transaction records," the report says. It estimates the Bitcoin economy to be worth between $35 million and $40 million.

Some Dark Web sites seem to be a form of dark parody or perhaps the demented fantasies of a disturbed mind. Some, which Fairfax Media has chosen not to name, offer tips about the type of female a cannibal should target, depending on how they want to cook their prey, while others claim to detail illegal laboratory experiments conducted on homeless people.

Other sites are incomprehensible to mere mortals — these are the hangouts of the hackers and phreakers (people who study, explore or experiment with telecommunications systems and who often work with hackers) doing whatever it is they do in their own impenetrable language.

But it is a cost of having a completely free anonymous web that the most unpalatable also get an equal voice. The most persistently disturbing aspect of the Dark Web is the child porn services. The Dark Web allows offenders to chat openly in online forums, download under-age porn and swap images without fear of identification or censorship.

One site, a smaller anonymity provider than Tor, but one that is known for its population of child abuse sites, says: "The true test of someone who claims to believe in freedom of speech is whether they tolerate speech which they disagree with or even find disgusting."

Seeing chat rooms in which offenders graphically describe sex acts with prepubescent children in the same terms you might expect to hear about adult porn stars is certainly disturbing.

Dr William Glaser, a psychiatrist who specialises in the assessment and treatment of sex offenders, says: "Offenders who only use child porn without going on to assault children seem to have a higher level of deviant sexual fantasies and an increased tendency to hold distorted views of children as sexual beings, compared to those offenders who actually assault kids." But he concedes it might be possible that, for some, contact with other offenders over the internet could help to normalise and validate their experiences.

Even in the underground world of the Dark Web, most participants consider this stuff unacceptable. Dark markets that allow under-age porn to be listed for sale soon find their customers boycotting their shops.

Members of vigilante hacktivist collective Anonymous continually attempt to frustrate child abuse sites by crashing their hosts' servers and those of sites they believe to be supportive of child porn.

Last October members of the group launched "Operation Darknet", crashing the server of the host of the largest collection of child pornography on the internet and using a form of trickery to expose a list of IP addresses they claimed had accessed a child porn site.

"We will continue to not only crash [their] server, but any other server we find to contain, promote, or support child pornography," Anonymous said.

But the successes of Anonymous have amounted to little more than a slight inconvenience to their targets; servers are restored within hours, if not minutes, the owners and whereabouts of the child abuse sites remain secret and images continue to be downloaded.

One gateway site that provides links to many Dark Web sites, including child porn, carries the message: "To Anonymous: [this site] is simply a wiki. Anti-paedo? Attack the paedo sites. You didn't attack Wikipedia for hosting information about your enemies. Wake up."

Ken Gamble believes Tor and other anonymity providers need to take responsibility for the content they enable. "Any organisation or infrastructure that operates as part of the global internet machine needs to take accountability," he says.

Andrew Lewman disagrees. "We don't host the content and therefore have no control over it. Would he expect Ford or Toyota to 'take responsibility' for those who steal, kidnap, speed, and otherwise break laws with their automobiles?"

Most of Tor's funding comes from the US government, non-profit organisations and research programs. Around 5 per cent of its funding comes from donations, including anonymous donations. Some Dark Web sites claim to anonymously direct a percentage of their profits to Tor and encourage their customers to do the same. However, Tor does not accept Bitcoin donations, directing them instead to an unrelated entity that offers "a faster, larger Tor Network".

Lewman says Tor has turned down sizeable donations from organisations known or suspected to be involved with terrorism or organised crime. But its acceptance of anonymous donations means it is reasonable to assume that part of Tor's funding may come from the criminals who have a vested interest in the work carried out in conjunction with some of the world's top university research departments. "It concerns us, yes," Lewman says.

But no matter how advanced the technology, users can never have 100 per cent guaranteed anonymity. "As a research project, we're far more honest than others about this," Lewman says. "We do not magically encrypt the internet. Anyone who says they do is lying."

But he says it is operator rather than software error — users log into a site that knows their identity or publish information that inadvertently identifies them. "Tor will protect your traffic over the network — what you do with that is up to you."

One thing Gamble and Lewman agree on is that old-fashioned police work is still the most effective way to catch those who would use the Dark Web for illegal activities. And the Australian Federal Police has this warning for anyone contemplating online crimes: "Anyone engaging in illegal activity through these websites cannot be guaranteed of remaining anonymous and they might be prosecuted. The Australian Crime Commission, AFP and Customs and Border Protection are committed to targeting and combating illicit e-commerce platforms.

"The AFP will continue to work closely with international partner agencies to combat serious and organised crime, including high-tech crime and technology-enabled crime."

162 comments

❝»«

»What a trashy piece. This kind of moral panic article is up there with "Reefer Madness" in the credibility stakes. Quotes like this:«

»"hackers and phreakers doing whatever it is they do in their own impenetrable language"«

»don't belong in a broadsheet newspaper. If you were trying to scare me into supporting more internet censorship and powers for law enforcement, ooh because of the scary hackers and paedos - sorry, you failed.«

»«

kosh | Melbourne June 01, 2012, 8:21AM

> ❝»«
>
> *»I din't think that was the aim. He was merely saying those in the IT world and especially those into hacking speak a whole jargon that most of us would never understand. It takes a smarter mind than average to come up with these viruses and hacking techniques.
What is written here is consistent with what the enforcement agencies have been saying around areas such as child porn. Unfortunately they cannot win the battle for now. But I'm sure that at some point the technology will come to track this part of the internet.«*
>
> *»«*
>
> chillout | June 01, 2012, 8:50AM
>
> ❝»«
>
> *»Boy, there sure are a lot of scary freaks out there. And to think we live, walk and share our world with these demented individuals.«*
>
> *»«*
>
> chrissy | June 01, 2012, 8:58AM
>
> ❝»«
>
> *»Deepnet, darknet, onion ...its very very very old news thats being sensationalised.. yeah the majority of content is amazingly brutal and disturbing..and funny how that "net filter" was supposed to keep the pedos away.. yet anyone with a bit of knowledge knew that it bypasses all of it and its been/continues to be a pedo hideout/share frenzy for years!!....I'm sure youve succeeded to shock 25% of the readers but as with most of the others I'm dissapointed.«*
>
> *»«*
>
> johnson | syd June 01, 2012, 9:14AM
>
> ❝»«
>
> *»A puff piece supporting more internet censorship! No more, no less.«*
>
> *»«*

More comments

Vic | Melbourne June 01, 2012, 9:24AM

Comments are now closed

“»«