In the web's hidden darknet, criminal enterprise is thriving

October 3 2014, by Daniel Prince

Credit: AI-generated image (disclaimer)

Criminals have always done their best to use new technology to their advantage and the rapid development of new digital technologies and online markets has provided the criminal entrepreneur with as much opportunity for innovation as their legitimate counterpart.

Europol's recent Internet Organised Crime Threat Assessment (iOCTA) report spells this out in no uncertain terms, revealing how entire criminal enterprises have developed around using the internet to hawk criminal services to anyone with the cash.

Broadly cybercrime can be broken down into two categories:

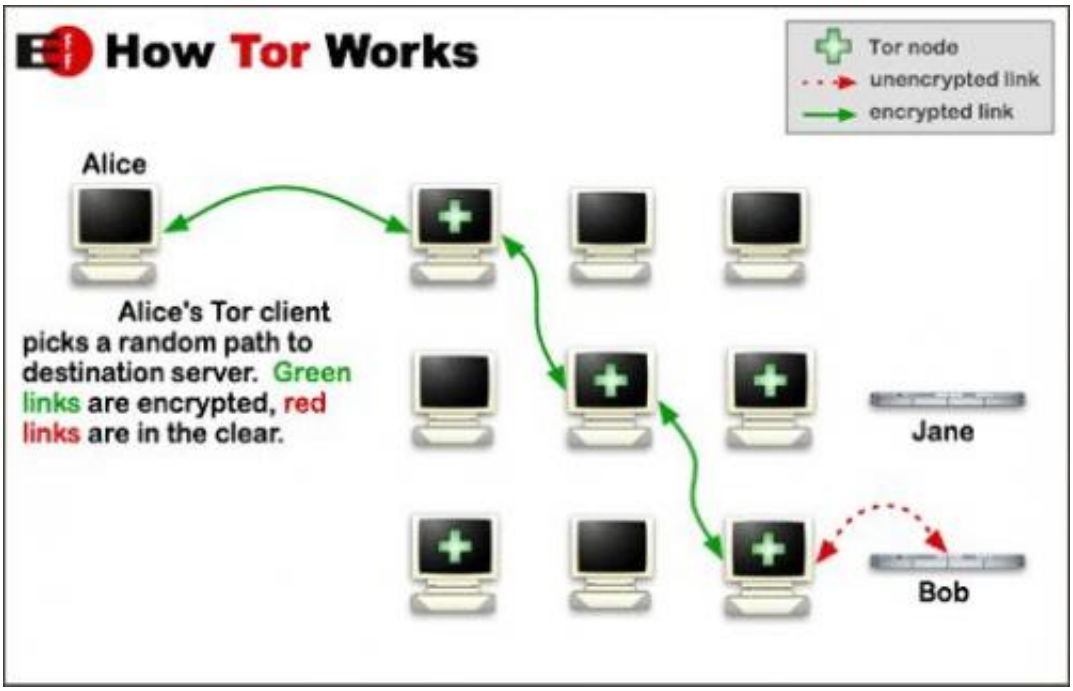
Cyber-dependent crime: a criminal act that only exists because of the computer, such as writing and releasing malware or efforts to hack and penetrate computer or network security.

Cyber-enabled crime: a criminal act that is enhanced through the use of technology, such as Ponzi schemes or credit card fraud.

The bulk of cybercrime is computer-enabled crime, predominantly economic in nature such as fraud, financial scams, and so on. This is why Action Fraud, the lead cybercrime reporting mechanism in the UK, has joined the National Fraud Intelligence Bureau (NIFB) of the City of London Police. Reports of cybercrime are analysed and then passed on to local police forces, or the National Crime Agency which deals with serious and organised crime.

Crime is getting easier

However these classifications hide a very concerning trait: the extent to which technology makes it easy to commit crime at a distance, in anonymity, and with worldwide reach. Committing a crime of potentially equivalent financial return in person, such as a bank robbery, might require getting hold of a gun – a significant barrier of entry for the average person.



How Tor anonymises the web. Credit: Electronic Frontier Foundation, CC BY

On the other hand the tools to conduct cybercrime – hacking software, scanning scripts, keyloggers – can be downloaded freely, if you know where to look. There are even step-by-step video instructions online that explain how to use them. We can see from looking at standard consumer technology that it only takes a few iterations of a product for it to become straightforward to use. So the barrier to entry for cybercrime is very low.

What the iOCTA report highlights is the extent to which crime as a service has matured, as facilitated by the hidden internet.

The concept of a "dark market" where cybercriminals trade their skills and ill-gotten gains was brought to the world's attention in 2011 through Misha Glenny's book DarkMarket: Cyberthieves, Cybercops and You, in which how he explains how cybercriminal networks trade their services.

A hacker discovers a bug, a vulnerability in a software program. This is sold to another, who writes a program that exploits this vulnerability in order to take control of a computer. Now compromised, this machine – perhaps someone, somewhere's home PC – is sold on to yet another hacker who might group it with other compromised machines to form a botnet of remotely controlled computers. The botnet becomes a platform – also for sale – from which cybercriminals can launch attacks against websites or networks, for financial, political or even military ends. This criminal market has developed sophisticated systems to establish trust and guarantee financial transactions, while minimising the risk of being traced.

Self-supporting crime

In the past these types of systems would have only been available only to technology-savvy cybercriminals. Now such criminal services can be bought and used by anyone, regardless of their technical skills. What this evolution has revealed is the extent to which other criminal activities, beyond economic crime, are now being supported by these infrastructures.

The drug trade has shifted significantly online in the form of the Silk Road illegal marketplace (which has been shut down) and its many successors. These marketplaces use anonymity software such as Tor to hide the location of the servers and identities of those involved in the transactions, while Bitcoin and other cryptocurrencies allow anonymous financial transactions. It's not just drugs on offer, with reports of anything from credit card details, to gold, guns and even hit-man services.

The business of supporting online criminality has become a truly global enterprise, with help desks, regular software updates and platform development road-maps created to service the needs of their users. In

fact having imitated the very best enterprise approaches and unbound by legislative requirements, they have become innovative and agile businesses.

The thin blue line

This creates a two-tiered, organised criminal enterprise: those committing crimes that directly victimise and those that are automating and supporting the businesses of crime. The question becomes where should law enforcement's limited resources be allocated: the criminals that carry out the crime, or those that provide the infrastructure that make it possible?

A key issue is the the shortage of technical skills, highlighted by a National Audit Office report which suggests it will take 20 years to ensure the development of sufficient skills – it's a problem found worldwide. With this demand for skills – and the private sector's capacity to pay more than the public sector – it's debatable whether law enforcement will be able to recruit the right people. A recent NSPCC report reiterates this, highlighting the shortage of skilled police staff to deal with the number of seized child abuse images requiring review.

Another complication is that many of the technologies criminal enterprises use have legitimate uses. For example, Tor provides a means to communicate anonymously that is vital for groups living under repressive regimes, or whistleblowers. Society has to find a way of balancing the use of privacy technology with the need to investigate criminal activity.

The iOCTA report recommendations for greater collaboration between international law enforcement and improving business cybersecurity are not enough – a step change is needed in the way police agencies deal with the impact of technology. The worry is that, given the skills

shortage and ingrained, institutional approaches to enforcement, this step change is still generations away.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation