MENU

Dark net dealers dragged into the light

A security firm boss with police clients and an NHS worker are among those caught up in our investigation

Robin Henry, Louis Goddard and the Sunday Times Data Team

February 12 2017, 12:01am, The Sunday Times

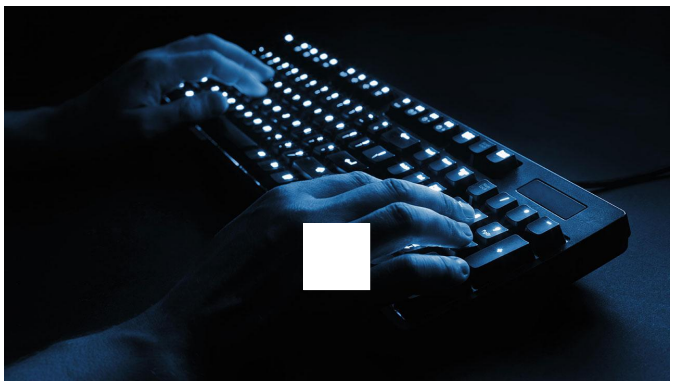
Wheeley: claims his account was hacked

Share Save

Dozens of people in Britain, including company bosses, NHS workers and suburban professionals, are linked to the sale and purchase of illegal goods ranging from stolen identities to lethal drugs on the “dark net”, an investigation by The Sunday Times has discovered.

In one case, a dark net account trading in devices to hack the electronic locks on cars had been set up by the director of a security company, which boasts of ties to the military and the Metropolitan police.

In another, links were found between a computer engineer at an NHS hospital and a vendor who had sold prescription medication and steroids worth tens of thousands of pounds.



What is the dark net?

In total, The Sunday Times found more than 50 individuals in

Past six days

The discovery comes after George Cottrell, 22, a former public-school boy and close aide to Nigel Farage, the former leader of Ukip, admitted running a fraudulent operation to launder drug money on the dark net.

The dark net is the name given to a network of websites, messageboards and forums that can be accessed via a browser called The Onion Router, or Tor. It grants anyone who uses it almost total anonymity by disguising their location, and the network has proved popular with criminals to buy and sell illegal goods, including weapons and child pornography.

However, a combination of security flaws has led some dark net users to expose their personal details unwittingly, including their emails and home addresses.

This year, The Sunday Times obtained an archive of dark net activity from between 2013 and 2015, compiled by a security researcher who uses the name Gwern Branwen. We analysed this archive for hidden markers that could identify people.

One dark net account, Autosafe, advertised on a marketplace called Agora. This included a guide to ripping off the gambling site Betfair for up to £1,000 and a tool for bypassing gas meters to “stop those robbing utility people”.

Autosafe also advertised a device that would allow car thieves to hack the electronic lock on a Ford car. The user was selling the lock-cracker for hundreds of pound in bitcoins, the anonymous cryptocurrency used on the dark net.

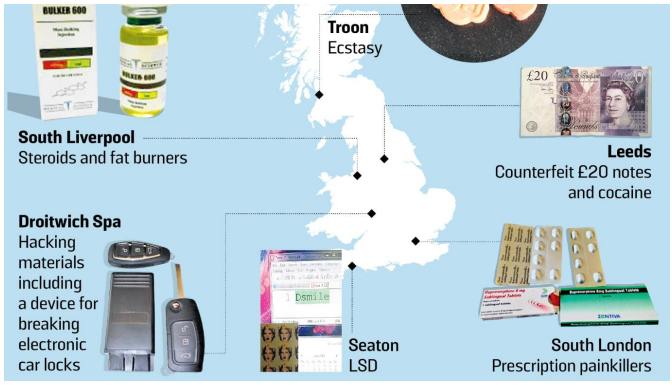
Autosafe wrote: “If you want to discreetly open Ford cars quickly, without worrying about alarms or locks this is the tool you need . . . This is very new technology . . . police don’t understand how cars are being broken into.”

Alongside the advertisement was a photograph of the homemade device. However, a security flaw in the Agora marketplace meant the photograph still contained metadata, which revealed where and when it was taken. According to the metadata, the photograph was taken on December 30, 2013, in a cul-de-sac in Droitwich Spa, Worcestershire.

Two more photographs of Autosafe products, taken in February 2014, narrowed the location down to the detached home of Darren Wheeley, who claims to be a former senior officer with the government’s Defence Science and Technology Laboratory.

Analysis also uncovered that Wheeley’s personal email had been used to set up an anonymous encrypted messaging key used by the Autosafe account.

Past six days



Wheeley is now the director of D2 Technology, a company that provides security and surveillance services. Its website listed clients including aerospace companies and the Metropolitan police. D2's website has now been taken down.

Wheeley confirmed he had set up the Autosafe account but said it was hacked by another dark net user, who he claims was responsible for uploading the ads offering illegal goods and services.

He said: "I have no involvement in this. We are a reputable business. I was purely looking for technology that we could possibly utilise to use against criminal activities, not to aid them."

Wheeley suggested the metadata may have been fabricated by the same person he claimed had hacked his account.

The security flaws that allowed this metadata to leak out were exposed by Harvard researchers Paul Lisker and Michael Rose in September 2016. They analysed the same archive used in our investigation and found hundreds of accounts could have been affected.

> "
> **Some dark net users have exposed their personal details unwittingly, including home addresses**

Although metadata can be falsified, the Harvard researchers believe this was unlikely because of natural "cluster" patterns in the data and instead concluded that dark net users had genuinely been exposed in a "security oversight" by the markets on which they were selling.

Our investigation found 14 accounts on the dark net that had posted photographs of their illegal wares taken at UK locations ranging from Troon in Scotland to the seaside town of Seaton, Devon, according to the metadata.

This included a vendor selling cocaine and counterfeit money, who posted a photo of a fake £20 note that was taken in a luxury tower block in Leeds. The account also contained a

Another drug dealer, calling themselves “Heizenberg”, a misspelling of the pseudonym used by the central character in the television series Breaking Bad, posted photos of the opiate buprenorphine, taken at two different addresses in south London.

One of the locations was a £1m house, owned by a professional woman in her fifties who lives there with her teenage sons. She said they had taken in a male lodger around the time the photo was taken. The man had stayed for a few months and left no forwarding address.

A cluster of 10 photos of steroid and prescription medication was taken in the vicinity of a detached house in suburban Liverpool, which were posted by a dealer who calls himself “Cerberus”.

Cerberus has boasted that his drugs, which include the DNP “fat burners” that have been linked to a string of deaths, could “kill you” and has also claimed to have “access to morphine and painkillers”.

In 2013 Cerberus may have revealed details about himself while seeking business on a body-building forum, including that he was 29 and lived in Liverpool.

In another post in December 2016, he revealed he had just been to see a surgeon because of a shoulder problem.

One of the listed occupants of the house in South Liverpool at the time the medication photos were taken, is a 32-year-old bodybuilder who until recently worked as an IT engineer for an NHS hospital trust. In mid-December 2016 he was seen by a specialist about his shoulder problem.

The man admitted there were “a lot of coincidences” linking him to Cerberus but said his position at the hospital did not give him “access to meds whatsoever”. He said he was shocked because he had little knowledge of the dark net.

The Sunday Times has passed a file to the hospital where he worked.

Our investigation also identified dozens of email addresses linked to customers trying to buy illegal goods. This included “MrKhan” who at one point tried to enlist someone to hack Essex University in 2014 after he was kicked off his business course.

“I am looking to employ the services of a hacker to get me the password for . . . a senior staff member at the uni so I can [be] back on the register in time for the finals without her knowledge,” he wrote.

The account was linked to Arjun Chowdhury, 23, who attended Essex University in 2014. It is understood he did not graduate.

Past six days

4 comments

Kremlin Troll No9 Feb 12, 2017

"close aide to Nigel Farage, the former leader of Ukip, admitted running a fraudulent operation to launder drug money on the dark net." Kippers involved in fraudulent activity? Surely not, who'd have thunk it!

6 Recommend Reply

RGT Feb 12, 2017

@Kremlin Troll No9 And the other "more than 50" were members of what? Surely not the Labour Party, Conservatives, Liberal Democrats, SNP or just unaffiliated. Who'd have thought it - a cross section of the UK population. Oh dear, how disappointing - you can't trust anyone it seems.

2 Recommend Reply

Martin Scotson Feb 12, 2017

Excellent work. It's good to see proper investigative journalism still be done in the UK. I hope that our security services, with their huge resources, are working at least as hard and as smart as you.

38 Recommend Reply

Oldflo Feb 12, 2017

@Martin Scotson I hope this superb investigatory journalism has been passed on to Technoplod!

6 Recommend Reply