GLOBAL LAW ENFORCEMENT ACTION AGAINST VENDORS AND BUYERS ON THE DARK WEB

26 Mar 2019

Press Release

Buying on the dark web? You are on the menu!

Law enforcement from Europe, Canada and the United States joined forces early 2019 to target vendors and buyers of illegal goods on dark web marketplaces. During the course of this operation, international law enforcement agencies made 61 arrests and shut down 50 dark web accounts used for illegal activity. Law enforcement executed 65 search warrants, seizing 299,5 kg of drugs, 51 firearms, and over €6,2 million (almost €4 million in cryptocurrency, €2,2 million in cash, and €35 000 in gold). They also conducted 122 interviews.

By coordinating efforts and acting simultaneously, a strong signal has been sent to those active in selling and buying drugs, counterfeit goods, firearms, etc. on the dark web. This coordinated hit shows that if you are conducting illegal activities on the dark web, you can and will be tracked down by law enforcement.

The dark web is a part of the internet that is only accessible through special software such as Tor (The Onion Router). While it provides a safe environment for personal privacy and freedom, it is also a fertile environment for criminals and individual illegal activities. Investigating these illegal activities online has become a priority for law enforcement all over the world. While you may have a higher level of anonymity on the dark web, you still have an identity; dark web applications are not an invisibility cloak or an immunity vaccine against the law.

CYBER PATROL ACTION WEEK

These global actions were launched during last year's Cyber Patrol Action Week at Europol's headquarters in The Hague. Between 2 and 5 July 2018, the second coordinated action week brought together a diverse group of online investigators and subject matter experts to patrol the surface web and dark web. Overall, 60 experts from 19 countries[1], Eurojust and Europol looked for the illegal sale and signs of counterfeit goods and money, drugs, cybercrime, document fraud, non-cash payment fraud, trafficking in human beings and trafficking in firearms and explosives. The experts identified 247 high-value targets and developed intelligence packages that were disseminated to the concerned countries for further handling. Based on this information, hundreds of investigations are currently underway. Today we can already announce some results of recent law enforcement successes.

Police and customs authorities in Germany have started investigations against 39 dark web users who were active on 21 different dark web markets. The 19 vendors and 20 buyers were trading illicit goods such as narcotics, firearms, counterfeit money, documents and pharmaceuticals and child sexual abuse material. These investigations are currently still ongoing.

On 13 February, as part of a larger investigation, the State Police of Saxony-Anhalt and the Prosecutors Office of Halle arrested several suspects of drugs trafficking. They were selling their merchandise via the dark web. This led to the seizure of 36 kg of marijuana, amphetamines, cocaine and ecstasy tablets and packaging material and firearms. Large amounts of cash and cryptocurrencies were also seized.

On 1 February 2019, in a joint operation, the German Public Prosecutor's Office in Münster, the German Customs' Investigation Office, the Dutch Specialised Prosecution Office for Fraud and Environmental Crime in Zwolle and the Dutch Fiscal Intelligence and Investigation Service dismantled an organised crime group involved in international drug trafficking and money laundering. The suspects in the Netherlands prepared parcels or envelopes with drugs, which were sent to Germany. The perpetrators in Germany used various mailboxes and post offices to ship the packages on to recipients around the world. The orders were made online through the dark web, using cryptocurrency.

In November 2018, the Austrian Federal Criminal Police Office (Bundeskriminalamt, .BK), special intervention units Cobra and Wega and the Vienna State Criminal Police Office arrested young men living a luxurious lifestyle, suspected of selling over 1 800 parcels of cocaine, heroin, amphetamine, methamphetamine and cannabis to customers all over the world, under the name Pablos Kitchen. The drugs were ordered through a dark web market and then sent by post. Considerable amounts of cash and drugs were seized during the house searches. A few weeks later, in December 2018, a group of Serbian perpetrators was halted who had been selling ecstasy tablets from Vienna to the US and Europe for almost ten years. The investigation revealed the main suspect received the profits of the dark web shop in the form of virtual currencies for almost €13 million. In total, 91 000 tablets were seized during the arrest of the main suspect.

The Portuguese Judiciary Police have opened 13 new investigations which have led to five arrests and nine house searches so far. Ecstasy tablets, raw MDMA and LSD stamps and dark web market account details were also discovered.

French Customs (Direction générale des douanes et droits indirects) was able to identify a vendor of firearms and 9 mm ammunition on a French dark web marketplace. Further investigations, as well as information received from Europol, led to the identification of the user. The perpetrator admitted to having sold between 350 and 400 9 mm cartridges.

Several US agencies (FBI, DEA, HSI, CBP, USPIS, DOJ, DOD), with the support of Europol, conducted Operation SaboTor, a coordinated international effort targeting dark web drug trafficking organisations operating on the dark web. The operation aimed to detect and disrupt the most prolific opioid vendors on the dark web and dismantle the criminal enterprises facilitating their opioid trafficking. This was the second coordinated action of J-CODE, the Joint Criminal Opioid and Darknet Enforcement team.

Europol's Executive Director, Catherine De Bolle, commented: "The dark web is not as dark as you think. When you buy or sell illegal goods online, you are not hidden from law enforcement and you are putting yourself in danger. This international coordinated approach demonstrates law enforcement's determination to tackle crime on the dark web and to reduce the number of people who fall victim to criminals selling life endangering products or scamming them for their own gain."

PERCEPTION VERSUS REALITY

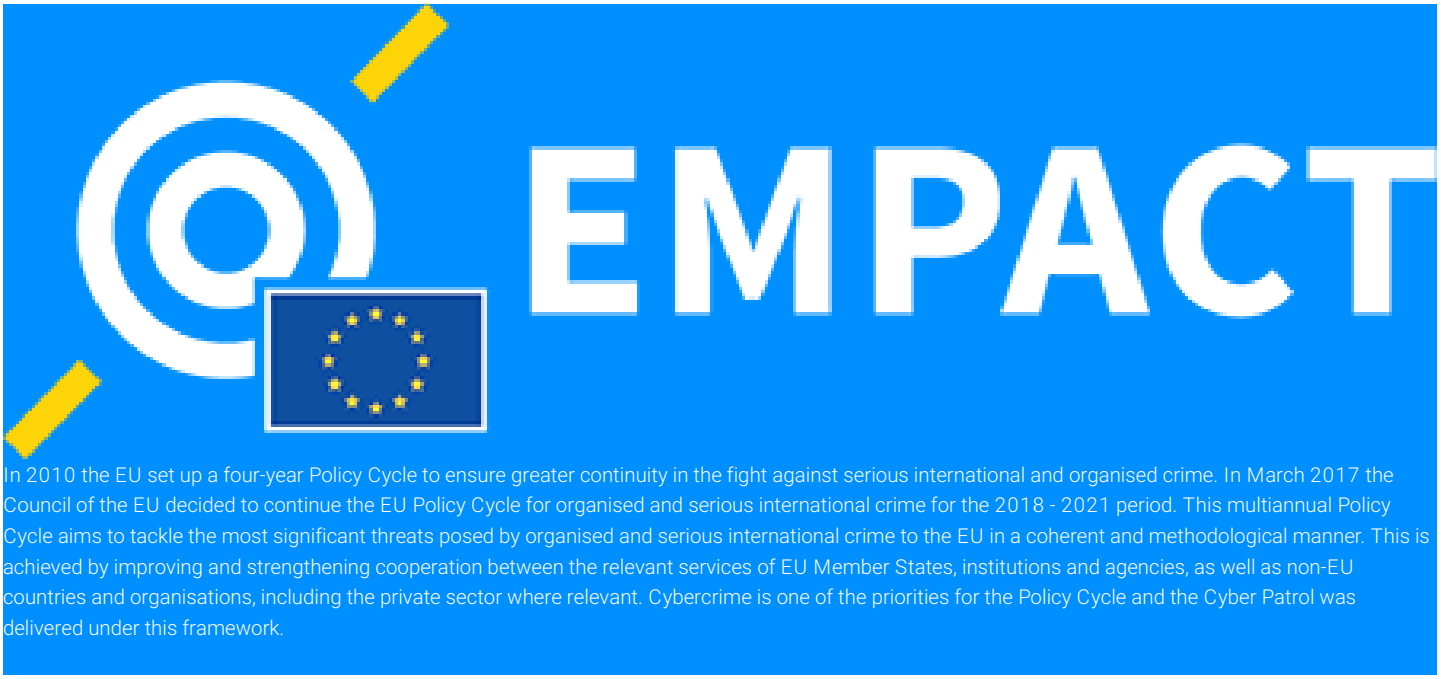
Do you access hidden services on the dark web because you want to buy illegal goods anonymously? Then you should know that the risks are actually higher than those on the surface web.

What actually happens after pressing the buy button from the comfort of your own home?

- You expose your sensitive data to scammers who are only after your money and your personal details.
- You expose your device to some of the most damaging malware around.
- You may receive counterfeited products or nothing at all: drugs that could kill you, malfunctioning weapons, or cybercrime services that work against you.

If you fall victim to a scam on the dark web, you have no one to turn to. Criminals don't have a customer service department. Your usual digital consumer rights do not apply on the dark web.

Dark web criminals know more about you than you know about them when you place an order. You give them personal information, while they remain hidden behind avatars. Any dispute can put your life in danger.



In 2010 the EU set up a four-year Policy Cycle to ensure greater continuity in the fight against serious international and organised crime. In March 2017 the Council of the EU decided to continue the EU Policy Cycle for organised and serious international crime for the 2018 - 2021 period. This multiannual Policy Cycle aims to tackle the most significant threats posed by organised and serious international crime to the EU in a coherent and methodological manner. This is achieved by improving and strengthening cooperation between the relevant services of EU Member States, institutions and agencies, as well as non-EU countries and organisations, including the private sector where relevant. Cybercrime is one of the priorities for the Policy Cycle and the Cyber Patrol was delivered under this framework.

[1]*Austria, Belgium, Canada, Czech Republic, Finland, France, Germany, Greece, Hungary Italy, Latvia, the Netherlands, Poland, Portugal, Romania, Spain, Sweden, the United Kingdom, the United States.*

CRIME AREAS	Drug Trafficking • Cybercrime
TARGET GROUPS	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
COUNTRIES	Austria • Canada • France • Germany • Portugal • United States of America
ORGANISATIONS	Drug Enforcement Administration (DEA) • Eurojust • Federal Bureau of Investigation (FBI)
SUPPORT & SERVICES	Operational coordination • Operational support • Information exchange

---

Source URL: https://www.europol.europa.eu/newsroom/news/global-law-enforcement-action-against-vendors-and-buyers-dark-web