

Global law enforcement strikes deep into 'Dark Web'

7 November 2014, by Charles Onians, With Rob Lever In Washington

A global crackdown has shut down dozens of online "dark markets" selling illegal goods and services and masking their identities using the Tor encryption network, officials said Friday.

The joint operation by US and European [law enforcement](#) arrested 17 people in a massive international operation against the underground bazaars.

"It is a plain fact that criminals use advanced technology to commit their crimes and conceal evidence—and they hide behind international borders so they can stymie law enforcement," said Assistant US Attorney General Leslie Caldwell.

"But the global law enforcement community has innovated and collaborated to disrupt these 'dark market' websites, no matter how sophisticated or far-flung they have become."

Investigators from the United States and 16 European countries launched a "joint action" against the markets Thursday, the Europol police agency said in a statement.

The crackdown is part of a vast global police operation that included the seizure earlier this week of Silk Road 2.0, the new version of the [online black market](#) that sprang up after authorities shut down Silk Road a year ago.

Silk Road was the most prominent of the targeted dark markets offering a range of illicit goods and services, from firearms to computer hacking.

Officials said a total of 414 websites and hosting servers were also seized in "Operation Onymous."

"The action aimed to stop the sale, distribution and promotion of illegal and harmful items, including weapons and drugs, which were being sold on online 'dark' marketplaces," Europol said.

The operation seized virtual Bitcoins, used to carry out transactions, worth \$1 million dollars (800,000 euros), 180,000 euros in cash as well as unspecified drugs.

"We are not 'just' removing these services from the open Internet," said Troels Oerting, the head of Europol's EC3 cybercrime unit.

"This time we have also hit services on the Darknet using Tor where, for a long time, criminals have considered themselves beyond reach. We can now show that they are neither invisible nor untouchable."

Tor is an encryption service that masks a computer user's identifying IP address, allowing them to set up private web connections in what is known as the Darknet—a hidden network used for both licit and illicit ends.

Some of the dark market sites shut down were known as "Pandora," "Blue Sky," "Hydra" and "Cloud Nine," each of which sold drugs, stolen credit card data, counterfeit currency and fake identity documents.

Another site called "Executive Outcomes" specialized in firearms trafficking, selling assault rifles, automatic weapons and silencers, according to a US Justice Department statement.

'Not the end'

Cybercrime expert Lodewijk van Zwieten said: "This is not the end."

"Behind these markets sit people who earn millions of euros. It's their turn next," Van Zwieten said on the Dutch public prosecutor's website.

US prosecutors say Silk Road 2.0 enabled more than 100,000 people to buy and sell illegal drugs and other contraband anonymously over the

Internet after its predecessor was shut down last year.

Blake Benthall was arrested by the FBI in San Francisco on Wednesday and faces charges including conspiring to commit narcotics trafficking, computer hacking, traffic in forged documents and money laundering.

He faces a maximum sentence of life in prison if convicted.

The alleged original mastermind of the original Silk Road, Ross William Ulbricht, said to use the handle "Dread Pirate Roberts" to run the site, is awaiting trial in New York.

Prosecutors described Silk Road 2.0 as one of the most extensive, sophisticated and widely used criminal online marketplaces.

It was virtually identical to its predecessor and accessible only through Tor, originally an acronym for The Onion Router, which affords web anonymity by shifting the apparent identity of a user's computer.

The latest crackdown included law enforcement from 16 European countries coordinated by Europol.

Countries included Britain, Bulgaria, the Czech Republic, Finland, France, Germany, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Romania, Spain, Sweden and Switzerland.

It remained unclear how long these operations would be shuttered.

After Silk Road was shut down last year, the number of illicit listings grew at more than a dozen websites to 65,000 in August, according to the nonprofit Digital Citizens Alliance.

© 2014 AFP

APA citation: Global law enforcement strikes deep into 'Dark Web' (2014, November 7) retrieved 15 April 2021 from <https://phys.org/news/2014-11-global-law-deep-dark-web.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.