

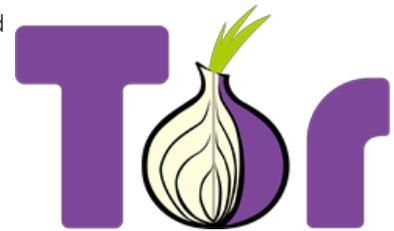
# Security Sidebar: Is Tor No Longer Safe?



John Wagnon, 2014-26-11

The "Dark Web" (sometimes called the "Dark Net") is a collection of thousands of websites that use anonymity tools (like [Tor](#) or [I2P](#)) to hide their IP address and physical location. These websites are notorious for conducting illegal activity like drug trade, money laundering, prostitution, etc. This Dark Web is fascinating because it seemingly allows all this illegal activity to happen in plain sight. A user who loads one of the anonymity tools and knows the site's URL can easily visit one of these illegal online marketplaces. Take Tor, for instance (it's the most commonly used anonymity software). Tor will encrypt web traffic in layers and route it through randomly-chosen computers around the world. Each computer removes one of the encryption layers before passing it to the next hop point. Because of this, it's extremely difficult (and many times impossible) to match the traffic's origin with its destination. This provides a safe haven for illegal activity to take place in plain sight. Imagine being a law enforcement official who watches all this illegal activity take place right in front of your face every day. You know you can arrest someone for it, but who? You can never trace the activity back to a known location/person.

It's easy to understand that law enforcement officials around the world are interested in taking down some of the sites on this Dark Web network...sites like Silk Road 2, Cloud 9, Cannabis Road, and Cash Machine to name just a few. Of course, the problem has always been knowing who and where to strike.



"We can now show that they are neither invisible nor untouchable"

Welcome to "Operation Onymous." Europol's Cybercrime Centre, the Federal Bureau of Investigations, the US Immigrations and Customs Enforcement, and the Department of Homeland Security [announced earlier this month](#) that they had formed a Joint Cybercrime Action Team and spent six months preparing to take down many of these illegal sites on Tor. Troels Oerting (head of the Cybercrime Centre) said "we have demonstrated that we are able to efficiently remove vital criminal infrastructures that are supporting serious organised crime. And we are not 'just' removing these services from the open Internet; 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."

Many reports disagree on the actual number of sites that were taken down, but even the lowest estimates leave us doubting whether or not the feds were able to crack the secure foundation of the Tor network. If only one or two sites had been compromised, you could reasonably believe poor OPSEC contributed to the problem. But, when approximately 50 sites were taken down, it makes you wonder if the entire foundation of Tor anonymity was compromised. When the feds were finished with their operation, 17 people were arrested including Blake Benthall who is said to have managed and administered the online drug marketplace Silk Road 2.0.

The Silk Road site once looked like this:

---

silkkroadvb5piz3r.onion

Welcome **OzFreelancer!**  
 messages(0) | orders(0) | account(\$0.00) | settings | log out

**Silk Road**  
anonymous marketplace

search | (0)

**Shop by category:**

- Drugs(1582)
  - Cannabis(271)
  - Dissociatives(33)
  - Ecstasy(217)
  - Opioids(106)
  - Other(65)
  - Prescription(274)
  - Psychedelics(306)
  - Stimulants(190)
- Apparel(37)
- Art(1)
- Books(300)
- Computer equipment(9)
- Digital goods(218)
- Drug paraphernalia(33)
- Electronics(13)
- Erotica(165)
- Fireworks(1)
- Food(1)
- Forgeries(34)
- Hardware(1)
- Home & Garden(5)
- Lab Supplies(5)
- Medical(3)
- Money(89)
- Musical instruments(2)
- Parkinson(1)

**News:**

- The gift that keeps on giving
- Who's your favorite?
- Acknowledging Heroes
- A new anonymous market **The Armory!**
- State of the Road Address

<p>10 Grams high grade MDMA 80+% <b>\$61.17</b></p>	<p>Amphetamines sulfate / Speed freebase... <b>\$28.59</b></p>	<p>2g Jack Frost (weed) *420 SALE**** <b>\$8.54</b></p>
<p>5 Grams of pure MDMA crystals <b>\$42.04</b></p>	<p>100 red Y tablets 111mg (lab tested)... <b>\$97.77</b></p>	<p>Michael Jackson Discography 1971-2009... <b>\$2.52</b></p>
<p>3.5g Albino Rhino (weed) <b>\$12.37</b></p>	<p>10mg Flexeril (muscle relaxant)... <b>\$3.22</b></p>	<p>***10gr. Amphetamine Sulphate... <b>\$33.19</b></p>

...but now looks like this:

U.S. Immigration and Customs Enforcement

**THIS HIDDEN SITE HAS BEEN SEIZED**

as part of a joint law enforcement operation by  
 the Federal Bureau of Investigation, ICE Homeland Security Investigations,  
 and European law enforcement agencies acting through Europol and Eurojust

In accordance with the law of European Union member states  
 and a protective order obtained by the United States Attorney's Office for the Southern District of New York  
 in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section  
 issued pursuant to 18 U.S.C. § 983(j) by the  
 United States District Court for the Southern District of New York

As you can imagine, Tor is none too pleased. A recent post relayed this message: "Tor is most interested in understanding how these services were located and if this indicates a security weakness in Tor hidden services that could be exploited by criminals or secret police repressing dissents."

I guess you always run the risk of law enforcement involvement when you provide an anonymous service and knowingly allow illegal activity to be so pervasive.

Tor is hoping that, when these convicts face trial, the police will have to explain how they broke in. The police offered a different sentiment when they said “this is something we want to keep for ourselves. The way we do this, we can’t share with the whole world, because we want to do it again and again and again.”

Despite this global force crackdown, many Tor (and Silk Road) users remain cautiously optimistic (Silk Road has been [taken down before](#), by the way). One user said “I predict that we will bounce back, stronger than before, but at this point I’m pretty freaked out.”

I guess no matter how you slice it or how you go about accomplishing it, crime doesn't pay.

---

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | [f5.com](http://f5.com)

F5 Networks, Inc.  
Corporate Headquarters  
[info@f5.com](mailto:info@f5.com)

F5 Networks  
Asia-Pacific  
[apacinfo@f5.com](mailto:apacinfo@f5.com)

F5 Networks Ltd.  
Europe/Middle-East/Africa  
[emeainfo@f5.com](mailto:emeainfo@f5.com)

F5 Networks  
Japan K.K.  
[f5j-info@f5.com](mailto:f5j-info@f5.com)