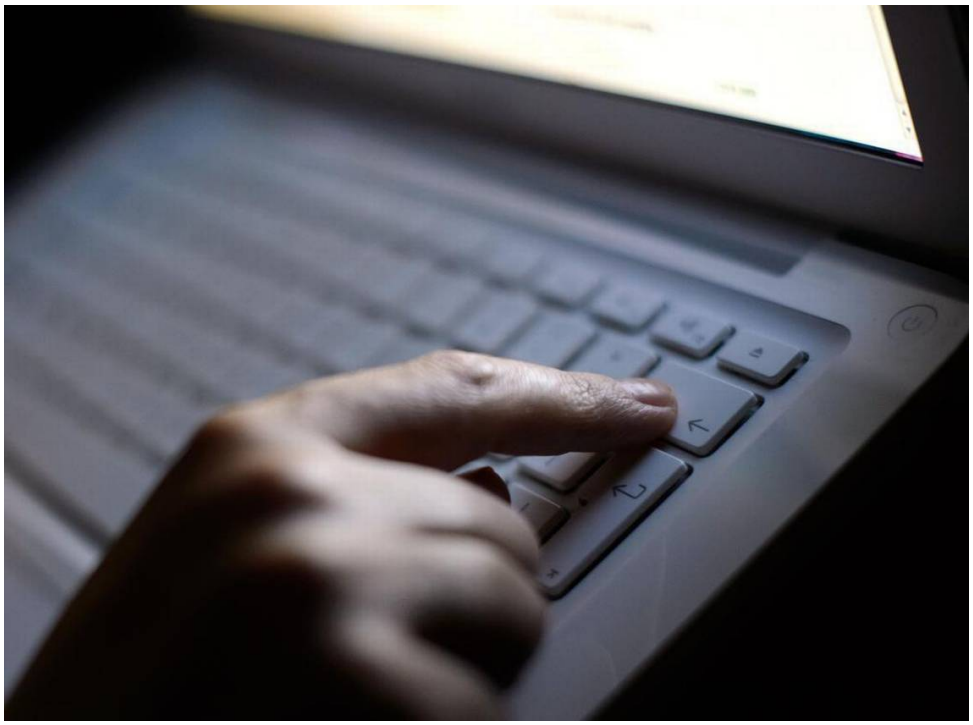

NATIONAL

Here's the 'horrible stuff' on the dark web: child snuff videos, WMD recipes, your phone number

BY TIM JOHNSON
tjohnson@mcclatchydc.com

AUGUST 02, 2017 5:00 AM

LAS VEGAS — An internet realm known as the dark web was once promoted as a safe haven for political dissidents and libertarians worldwide, and financed partly by the State Department. But it has turned into a criminal cesspool.

Rogue hackers sell stolen credit card information there, and gun runners peddle every variety of weapon. Pedophiles and malware merchants lurk in its confines alongside opioid dealers and human traffickers.

What happens on the dark web is so ugly that cybersecurity firms that comb its data routinely share the information with the FBI and other law enforcement agencies.

"All us work in partnership with law enforcement, when possible and necessary, to combat this," said Danny Rogers, chief executive of Terbium Labs, a Baltimore, Maryland, company that specializes in automated combing of the dark web.

"

AS SOON AS YOU TURN OFF THE LIGHT, THOSE COCKROACHES COME BACK.

Christian Lees of InfoArmor

A handful of U.S. cybersecurity companies focus on the dark web, primarily working for retailers, banks and other firms concerned that cybercriminal gangs are trafficking there in consumer data that they've obtained through breaches.

A small and secretive corner of the internet, the dark web cannot be accessed by traditional search engines, such as Google, Bing or Yahoo. Those visiting the dark web must employ special web software, like The Onion Router (Tor) or I2P, both of which encrypt and give anonymity to the user and hide the location of everything visited. It is a challenge to configure the software and find where one wants to browse.

That difficulty is what makes the dark web a hub for the most foul types of crime.

"When I was CEO of Tor ... law enforcement came to me my first year and said, 'Look, there's child abuse on your sites. Your technology is enabling child abusers to be far more bold,'" said Andrew Lewman, now vice president of Owl Cybersecurity, a Denver company.

In subsequent years, the complaints from the Feds grew more vigorous, saying child sex rings had been set up and were offering live streaming. Lewman, a longtime advocate and volunteer for the Tor Project who was hired fulltime as executive director in 2009, demurred over details but said one of the worst was "a sexual child abuse snuff film."

Now, Lewman serves on the Interpol Crimes Against Children Committee, and openly helps the FBI, Homeland Security and other agencies battle crimes on the dark net.

"When we crawl, we see all the amount of horrible stuff on the dark nets and the fact is that it's the majority usage. It's criminal," he said.

What is the dark web?

A federal judge on Friday refused to make public details of the FBI's actions in a 'dark web' internet sting raising the question about what is on the dark web. By Susan Ardis

Susan Ardis

Not all on the dark web is sinister. Advocates say it was designed as a refuge for dissidents and outcasts who reside in oppressive countries, like Syria and China. Over the years, the State Department offered more than $3 million in funding, largely from its Democracy and Human Rights branch but sometimes through third parties. The Tor Project was seen as a vehicle to promote freedom of speech, allow access to blocked news and research sensitive topics. More than a million people access Facebook through the dark web, where the social media site has a presence, among the 5,000 to 7,000 sites that are available through Tor.

“Over half of those sites themselves are benign, people’s personal blogs, conspiracy websites, pictures of cats,” Rogers said.

The other half is where nasty stuff happens.

> **THE SHEAR AMOUNT OF DRUGS IS ASTOUNDING.**
>
> Dan Palumbo, Digital Citizens Alliance

Two weeks ago, the FBI and law enforcement agents from six other countries took down the dark web’s biggest criminal marketplace, AlphaBay, which it called “the largest criminal marketplace on the internet.”

Joining the FBI in the global takedown were law enforcement authorities in Thailand, the Netherlands, Lithuania, Canada, Britain and France.

Prior to the action, Thai authorities arrested a Canadian, Alexandre Cazes, 26, on a U.S. petition. On July 12, Cazes, the founder of AlphaBay, was found dead in his cell, and news reports said he hung himself with a piece of cloth. Prosecutors in California July 19 filed a civil forfeiture complaint against Cazes’ estate seeking control of a Lamborghini, a Porsche and properties in Thailand, Cyprus, Lichtenstein, and Antigua & Barbuda.

Other criminal platforms are ready to take AlphaBay’s place.

“As soon as you turn off the light, those cockroaches come back, don’t they?” said Christian Lees, chief information security officer at InfoArmor Inc., a Scottsdale, Arizona, cybersecurity firm that analyzes the dark web.

Those who scour the dark web often come away stunned.

“The shear amount of drugs is astounding,” said Dan Palumbo, research director of the Digital Citizens Alliance, a Washington-based coalition of consumers, internet businesses and experts seeking to make the internet safer.

Palumbo said he has seen sites offering black tar heroin, cocaine, and synthetic drugs like fentanyl, a powerful addictive opioid driving a sweeping U.S. drug epidemic.

Vendors sell varieties of ransomware and malicious hacking tools on dark web storefronts, as well as military-grade weapons, and what Rogers called “recipes for making WMD” – weapons of mass destruction.

“It’s varying degrees of shocking,” he said.

The dark web, sometimes also called the dark net, is a hive for cybercriminals involved in buying and selling stolen personal information.

“Your identity, social security number, Visa numbers, phone, address, email, passwords, all that, is already on the dark net,” said Lewman of Owl Cybersecurity.

> **WHAT’S $10 BILLION? IT’S SMALL PEANUTS.**
>
> Danny Rogers, cofounder of Terbium Labs

“The market for stolen data is very robust,” said Rogers, of Terbium Labs. “If the data is monetizable, this is where it will end up.”

When hackers steal credit card data or other personal data, they advertise it on digital underground storefronts. Fraudsters buy the data and make phony purchases, launder money or commit other acts.

Hundreds of millions of stolen records and credit card numbers are believed to have passed through the dark net, and criminal gangs routinely finance activities through card theft. While growing as a menace, the $10 billion a year in credit card losses have yet to alarm banks.

“Compared to the $4 trillion a year or more that’s spent on credit cards in the U.S., what’s $10 billion? It’s small peanuts,” Rogers said.

Former federal agents say it is a huge task to suppress dark web criminal activity.

“Thanks to the Russian-speaking underground, they’ve created this crime-as-a-service model that is very robust,” said Eduardo E. Cabrera, chief cybersecurity officer at Trend Micro, and a former cyber official at the U.S. Secret Service.

Increasingly, though, the private cybersecurity firms that sift through the dark web – either with automated “crawl” systems or using human analysts – collaborate with the FBI.

“We simply cooperate with them,” Lees said.

Tim Johnson: 202-383-6028, @timjohnson4

Andrew Lewman, vice president of Owl Cybersecurity, a Denver-based firm, stands before a monitor that registers data from the dark corners of the internet. Lewman was attending the Black Hat hackers convention in Las Vegas July 26, 2017. **Tim Johnson** - McClatchy

1 of 2

SUGGESTED FOR YOU

COMMENTS

SUBSCRIPTIONS

Newsletters

SITE INFORMATION

Customer Service

Contact Us

SOCIAL, MOBILE & MORE

Text News Alerts

Mobile & Apps

Beyond The Bubble Podcast

The ACC Now Podcast

ADVERTISING

Advertise With Us

MORE

Copyright

Privacy Policy

Terms of Service