NEWSLETTERS | SEND PICS | TIPS

4 NEW YORK

25°

Search

HOME NEWS WEATHER INVESTIGATIONS ENTERTAINMENT TRAFFIC CONTESTS CONTACT US

LOCAL U.S. & WORLD SPORTS HEALTH TECH WEIRD WEATHER

LIVE VIDEO WATCH: News 4 New York Share

NEWS > LOCAL

I-Team: Identity Thieves Thrive on the "Dark Web"

By Chris Glorioso

View Comments () | Email | Print

Stolen credit card and Social Security numbers often end up on some frightening online marketplaces that law enforcement can’t always penetrate, the I-Team has found. Chris Glorioso reports. (Published Tuesday, Nov 18, 2014)

Tuesday, Nov 18, 2014 • Updated at 10:06 AM EST

Days after a federal crackdown shuttered hundreds of websites used by cyber criminals, the I-Team logged on to several anonymous Internet marketplaces and found hundreds of credit card and social security numbers up for sale again.

The thriving of those illegal marketplaces -- even after a sweeping global operation -- underscores the challenges in policing what’s become known as the “dark web.”

- **Illegal License Plate Covers Help Scofflaws Avoid Fines**

More than a dozen people were arrested in the joint operation between 16

feedback

TRENDING STORIES

Person in Custody in Deadly NYC Subway Shove: Police

NJ Homes Evacuated as Fire Consumes Building, Spreads

NYC to Test for Ebola After Apparent Heart Attack Death

WATCH: News 4 New York

WATCH: "All About That Baste" Parody Video

European countries and the United States. About 400 websites were shut down, including "Silk Road 2.0," an anonymous site where $8 million dollars a month in illegal contraband transactions changed virtual hands.

The closed sites could only be accessed using browsers like TOR, which allow users to surf the web anonymously by scrambling IP addresses and masking physical locations.

"It's been a huge deterrent effect -- showing that we have access to these 400-plus hidden websites within TOR," said Mitchell Thompson, an FBI special agent who investigates cybercrime in the New York field office.

Paul Oster, a consultant who owns Better Qualified LLC, a credit protection and repair company, said the way TOR is designed is a constant roadblock to law enforcement trying to squash illegal commerce on the "dark web."

- **Football Helmet Safety Questioned at Tri-State Schools**

"When the Silk Road closes, other roads open up," he said.

Aside from stolen identities, Oster says he continues to be alarmed by the availability of other contraband on the dark web.

- **I-Team: Cell Tower Regulations Not Followed**

"You can buy anything from a hand grenade to a handgun to an AK-47," Oster said. "Forget about drugs and prostitution and child pornography. Once I was really digging down in there, I have to be honest, I got nervous."

Designers of the TOR browser say they have worked with the FBI to thwart the "crypto markets" where identities are bought and sold. They say their browser has non-criminal uses.

- **Women Panhandling With Babies Swap Kids, Refuse Help**

Andrew Lewman, executive director of the TOR Project, said the anonymity of the TOR browser is of great value to many law-abiding people who simply want a break from constant Internet tracking and surveillance.

"We're used by millions of ordinary people just like you and me who just want to do something private, whether it's search for something or go shopping. Whatever. That's not tied to their public identity," said Lewman.

- **Section 8 Renters Turned Away Despite Legal Protections**

"We do not condone the illegal uses of TOR," he added.

Still, the prime feature of TOR, that it scrambles hides IP addresses, makes it difficult for investigators to infiltrate new illegal marketplaces as they pop up.

- **Lawyers Want Bronx DA to Name Cops in Ticket-Fix Scandal**

That's why the FBI and NYPD are intensifying efforts to cut off the supply of stolen identities before they make it to those marketplaces -- an attempt to nip the theft in the bud before the contraband arrives there

"When you look at the latest data breaches that have happened over the last 12 months, I think the number is like 600 million so that means most people have been compromised more than once," Oster said. "I mean there's a little more than 300 million people in the country."

This summer, the FBI, NYPD and MTA police formed a Financial Cyber Crimes Task Force that essentially deputizes local police officers to enforce federal identity theft law, which carries tougher penalties.

Thompson, who heads the task force, said the federal-local partnership provides more boots on the ground, allowing investigators to more quickly respond to reports of data breaches. And time is of the essence, because identity thieves look to sell stolen numbers before the cardholders realize they have been victimized.

"As soon as a credit card number is stolen, it behooves the person who stole it to get it online and sell it as quickly as possible," Thompson said. "They can put it online and they can get anywhere from $1 to $20, $30 or $40 per credit card number, depending on whether the credit card number is new."

A key objective for the task force will be to rapidly respond to reports of "skimmers" and other devices that are attached to ATMs, ticket-purchasing terminals and point-of-sale credit card readers. The skimming devices are used by criminals to peel financial data from magnetic strips, and investigators they implementing them is often the first step in an identity thief's process of creating a bundle of financial accounts that can be sold on the dark web.

The best way to protect against a skimmer is to cover PIN numbers when using ATMs or ticket-purchasing terminals, says NYPD detective Armando Coutinho, one of the 15 investigators on the task force.

Coutinho says cyber criminals use skimming devices to install a camera that records the typing in of PIN numbers, so shielding a keypad with one hand while typing the numbers in with the other is critical.

Legislators are also working to keep personal information off the dark web.

Last month, New Jersey Assemblyman Gary Schaer, (D–Passaic), introduced a bill that would force health insurers to encrypt personal health data so that it is worthless to a potential thief if it ever gets stolen. Schaer also said similar laws should apply to financial institutions.

"It's our obligation to protect people from this data being stolen and requiring those groups that collect this data -- whether they be in financial services, whether they be in health care -- that this data be protected," Schaer said.

His bill has passed through committee and is awaiting a full vote by the Assembly. A companion bill to Schaer’s has already passed the New Jersey Senate.

***Get the latest from NBC 4 New York anywhere, anytime*: iPhone/iPad App | Twitter | Facebook | Email Newsletters | Send Us News Tips | Google+ | Instagram | RSS**

View Comments () | Email | Print

Leave Comments

NEWS
Local
U.S. & World
Sports
Health
Tech
Weird
Weather

WEATHER
Forecast
Maps & Radar
Weather Alerts
School Closing Alerts
Weather News

ENTERTAINMENT
Entertainment News
The Scene
Events
In The Wings
NY Live
Your Guide 4 NY
Open House
1st Look
Talk Stoop

CONTACT US
Social Directory
About Us
Community
TV Listings
Next Step for Vets
Careers

TRAFFIC
Traffic Cameras

FCC Independent Programming Report
FCC News and Information Programming Report
NBC Non-Profit News Partnership Reports
WNBC Public Inspection File
21st Century Solutions

AdChoices

Send Feedback | Terms Of Service New | Privacy Policy