Feds say they have shut down Darkode malware marketplace

July 15 2015, byJoe Mandak

FBI Supervisory Special Agent J. Keith Mularski, who heads the cybercrime squad at the agency's Pittsburgh field office, displays a screen shot from the Darkcode website, top left, an English-language "marketplace for cybercriminals", at the National Cyber-Forensics & Training Alliance in Pittsburgh, Tuesday, July 14, 2015. The Justice Department announced Wednesday that investigators have shut down what they call the world's largest-known English-language malware forum, called Darkode where cybercriminals bought and sold hacked databases, malicious software and other products that could cripple or steal information from computer systems. (AP Photo/Gene J. Puskar)

The Justice Department shut down an online "criminal bazaar" where computer hackers bought and sold stolen databases, malicious software and other products that could cripple or steal information from computers and cellphones, authorities said Wednesday.

Roughly 70 alleged cybercriminals in the United States and 19 other countries were targeted in the 18-month probe of Darkode.com. The secretive, members-only site was the largest-known English language malware forum in the world until the FBI got a court order to shut it down, investigators said.

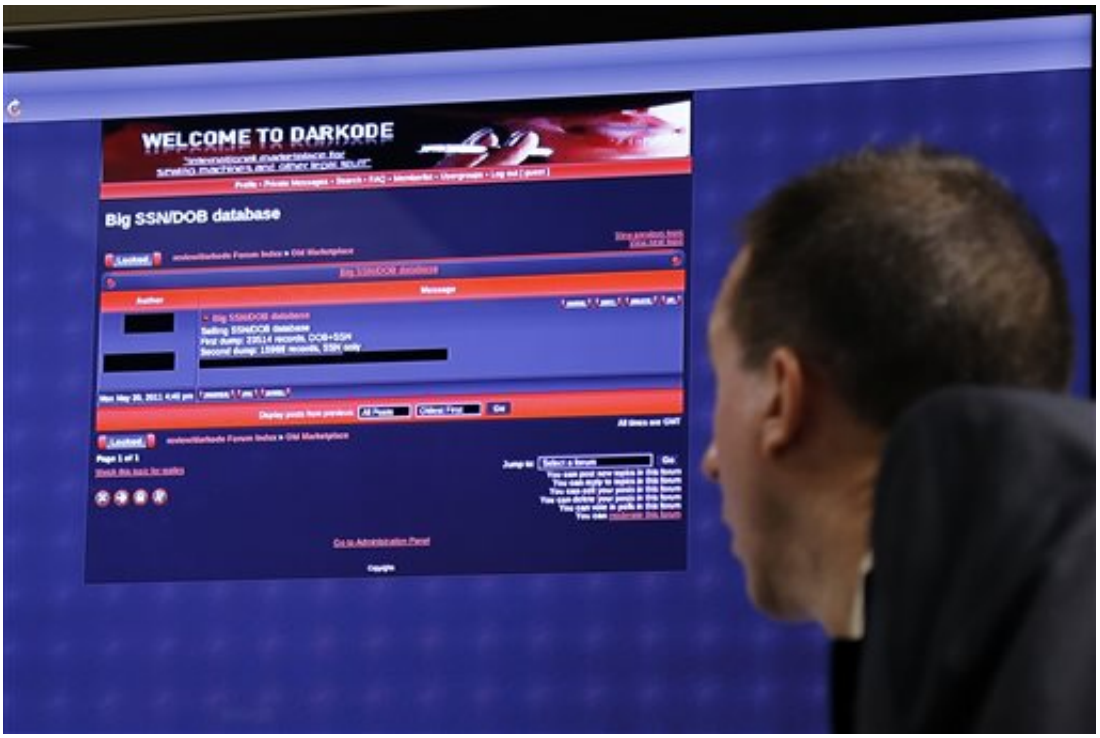
"We have dismantled a cyber-hornets' nest of criminal hackers which was believed by many to be impenetrable," U.S. Attorney David Hickton said.

Twelve people have been charged in the United States by federal prosecutors in Pittsburgh, Wisconsin, Louisiana and the District of Columbia, including Daniel Placek, 27, of Glendale, Wisconsin, and Matjaz Skorjanc, of Maribor, Slovenia.

They allegedly created Darkode in 2007 "for the purpose of bringing together the most talented computer hackers and cybercriminals on the Internet," court documents said.

Skorjanc is jailed in Slovenia and must be brought to Pittsburgh to face charges including racketeering conspiracy and wire, bank and computer fraud. He doesn't have an American attorney.

Placek, charged with conspiracy to commit computer fraud, will surrender once a federal judge in Pittsburgh orders him to appear. His attorney didn't immediately return a call.



FBI Supervisory Special Agent J. Keith Mularski, who heads the cybercrime squad at the agency's Pittsburgh field office, displays a screen shot from the Darkcode website, top left, an English-language "marketplace for cybercriminals", at the National Cyber-Forensics & Training Alliance in Pittsburgh, Tuesday, July 14, 2015. The Justice Department has targeted more than 70 alleged cybercrimals in 20 countries who've been using Darkcode, a members-only online marketplace to buy and sell hacked databases, malicious software and other "products" that can cripple or steal information from computer systems. U.S. Attorney David J. Hickton of the Western District of Pennsylvania announced Wednesday in Pittsburgh that the computer hacking forum known as Darkcode was dismantled Wednesday, and criminal charges have been filed against 12 individual associated with the forum. (AP Photo/Gene J. Puskar)

Twenty-eight others have been arrested by foreign authorities.

Roughly 30 more are the targets of search warrants, which are necessary

because some countries require evidence to be seized before criminal charges can be brought. In other cases, computers must be searched so investigators can connect online personas with real people.

The number of victims and the amount of their losses can't readily be calculated, Hickton said. John Lynch, the chief of the Justice Department's Criminal Division's Computer Crime and Intellectual Property Section, estimated it at hundreds of millions of dollars.

Rob Wainwright, director of the European Union's law enforcement agency, Europol, said shutting down Darkode significantly disrupted the underground economy. He called it "a stark reminder that private forums are no sanctuary for criminals."

One 20-year-old Pittsburgh man is charged with designing Dendroid, a piece of malware that lets someone remotely control infected Android cellphones. Information from those phones could be stolen and the phones themselves used to take pictures and videos, make calls and send text messages without the owner's knowledge.

Dendroid was sold for as much as $65,000 to outsiders, but $300 to other Darkode members.

U.S. Attorney David J. Hickton of the Western District of Pennsylvania, left, and Deputy Director Mark F. Giuliano of the FBI, announce that the computer hacking forum known as Darkcode was dismantled, and criminal charges have been filed in the Western District of Pennsylvania and elsewhere against 12 individuals associated with the forum, Wednesday, July 15, 2015 in Pittsburgh. (AP Photo/Gene J. Puskar)

A Binghamton, New York, man infected computers with something called Facebook Spreader, used to send out spam messages on the social media site, authorities said.

Among those still at-large is Johan Anders Gudmunds, 27, of Sollebrunn, Sweden. He took over administering Darkode in 2010 and operated his own botnet, which illegally took control of more than 50,000 computers and stole data from them more than 200 million times, authorities said.

Hackers could also sell the fruits of their labor: stolen email and personal

information databases that others could use in identity theft and other schemes. Lists for sale included customers who participated in an automobile auction; personal information from 39,000 people on a Social Security database; and 20 million email and usernames stolen in another scheme.

One target, an 18-year-old man arrested in England in January, is allegedly responsible for hacking into Sony's PlayStation Network and Microsoft's Xbox Live services last year around Christmas.

Those targeted for arrest or searches live in the United States, United Kingdom, Australia, Bosnia-Herzegovina, Brazil, Canada, Colombia, Costa Rica, Croatia, Cyprus, Denmark, Finland, Germany, Israel, Latvia, Macedonia, Nigeria, Romania, Serbia and Sweden. There are victims in all of those countries, and others, authorities said.

"The FBI has effectively smashed the hornets' nest and we are in the process of rounding up and charging the hornets," Hickton said.