THE WALL STREET JOURNAL.

http://www.wsj.com/articles/more-than-70-targeted-in-global-takedown-of-hacker-forum-darkode-1436970640

U.S.

More Than 70 Targeted in Global Takedown of Hacker Forum Darkode

FBI, Europol probe focused on hackers launching attacks on companies, governments

FBI agent J. Keith Mularski, who heads a cybercrime squad, displays a screen from the Darkode site. *PHOTO: GENE J. PUSKAR/ASSOCIATED PRESS*

By **DEVLIN BARRETT**

Updated July 15, 2015 11:03 a.m. ET

U.S. officials on Wednesday said they had smashed a "hornet's nest" of hackers known as Darkode, targeting 70 alleged participants around the world and shutting down what they described as an online marketplace for malicious computer code.

Police in 20 countries charged, arrested or searched dozens of alleged Darkode members or associates, officials said—including an intern at a high-profile computer security firm that works closely with the Federal Bureau of Investigation.

Darkode's password-controlled website was seized by authorities after having allegedly served as a place where hackers bought and sold malware, or their skills, to launch cyberattacks or steal personal data.

The U.S. charges were announced in Pittsburgh, where U.S. Attorney David Hickton, who is overseeing the investigation, called Darkode "one of the gravest threats to the integrity of data on computers in the United States and around the world."

While Darkode is just one of an estimated 800 such online sites, Mr. Hickton said it was "the most sophisticated English-speaking forum for criminal computer hackers."

The prosecutor said that approximately 28 people had been arrested—12 of them in the U.S.—and more arrests were likely as a result of searches being conducted. The charges include conspiracy to commit computer fraud and conspiracy to send malicious computer code.

One suspect, 20-year-old Morgan Culbertson of Pittsburgh, was an intern at FireEye Inc., which frequently works with the FBI on hacking investigations.

Mr. Culbertson is accused of designing and selling malicious code that targets cellphones using Google Inc. 's Android operating system. A LinkedIn page in his name says his internship was centered on defending Android phones from malware.

EARLIER COVERAGE

- U.S. Agencies Conduct Cyberwar Games (http://www.wsj.com/articles/u-s-agencies-conduct-cyber-war-games-1436069213) (July 5)
- Check Point Battles to Stay at Front Line in War Against Hackers (http://www.wsj.com/articles/check-point-battles-to-stay-at-front-line-in-war-against-hackers-1435147700) (June 24)
- When Does a Hack Become an Act of War? (http://www.wsj.com/articles/when-does-a-hack-become-an-act-of-war-1434189601) (June 13)

FireEye said it learned Wednesday that Mr. Culbertson had been charged. "Mr. Culbertson's internship has been suspended pending an internal review of his activities," it said, declining to comment further.

Prosecutors said Mr. Culbertson designed Dendroid, a code to control Android phones

and steal data from them. Mr. Culbertson couldn't immediately be reached for comment and court records didn't list an attorney for him.

James Lewis, a cybersecurity expert at the Center for Strategic and International Studies, said the Darkode arrests represent "natural selection" in the world of computer criminals. "People who do this kind of thing and live in the U.S. or western Europe will end up in jail. The smart ones live in Russia," he said. Russia doesn't extradite its citizens to face charges in the U.S.

"Remaining members who have not yet been rounded up we expect will still engage in their criminal activity," said Mr. Hickton. He added that the investigation has given the FBI new insight into how such hackers operate and a better ability to pursue them.

The other countries participating in the crackdown are Australia, Bosnia and Herzegovina, Brazil, Canada, Colombia, Costa Rica, Cyprus, Croatia, Denmark, Finland, Germany, Israel, Latvia, Macedonia, Nigeria, Romania, Serbia, Sweden and the U.K.

The FBI said it spent two years on the probe, which also included Europol, the European Union's law-enforcement agency.

Europol director Rob Wainwright said the takedown "caused significant disruption to the underground economy," and sent a message that such online forums aren't beyond the reach of police.

Still, one expert said the investigation may have limited impact.

"If you look at the entire ecosystem of bad actors, this is not a major blow," said Jeffrey Carr, founder and president of Taia Global, a computer-security firm. "Is it going to make a dent in the underground market for this stuff? I don't think so."

One of those charged, a 27-year-old Swede, allegedly served as an administrator of Darkode and sold malware to take over computers. Authorities said that at times he secretly controlled more than 50,000 computers.

Authorities say another suspect, from upstate New York, used malicious code to take control of computers using Facebook and use them to send spam messages to others.

— Alexis Flynn in London contributed to this article.

Write to Devlin Barrett at devlin.barrett@wsj.com