FBI: BlackShades Infected Half Million Computers

Larry Neumeister and Toby Sterling, Associated Press

NEW YORK (AP) — More than a half million computers in over 100 countries were infected by sophisticated malware that lets cybercriminals take over a computer and hijack its webcam, authorities said as charges were announced May 19, 2014, against more than 100 people worldwide.

The FBI described its investigation in criminal complaints unsealed in Manhattan federal court against five individuals. Meanwhile, police worldwide said they had recently arrested 97 people in 16 countries suspected of using or distributing the malicious software called BlackShades.

"This case is a strong reminder that no one is safe while using the Internet," said Koen Hermans, an official representing the Netherlands in the European Union's criminal investigation coordination unit, Eurojust. "It should serve as a warning and deterrent to those involved in the manufacture and use of this software."

The FBI said the BlackShades Remote Access Tool has been sold since at least 2010 to several thousand users. The agency said one of the program's co-creators is now cooperating with the government and had provided extensive information.

The malware lets hackers steal personal information, intercept keystrokes and hijack webcams to make secret recordings of users. BlackShades also can be used to encrypt and lock a computer's data files, blocking the rightful owners from regaining access unless they pay a ransom.

Security experts have linked the program to attacks on Syrian dissidents in 2012 and attempts to steal data from more than a dozen French organizations last year. The low cost of the hacking tool has made it increasingly popular across the hacker underground, where variants have been circulating online for years.

Last year, security firm Symantec said that use of BlackShades was going up, with licenses for the program going for $40 to $100.

French officials said raids occurred last week after the FBI arrested two BlackShades developers and distributed a list of customers who had purchased the malware.

Law enforcement coordination agencies Europol and Eurojust, based in The Hague, Netherlands, said that police in 13 European countries — Austria, Belgium, Britain, Croatia, Denmark, Estonia, Finland, France, Germany, Italy, Moldova, the Netherlands and Switzerland — as well as in the United States, Canada and Chile raided 359 properties and seized cash, firearms, drugs and more than 1,000 data storage devices.

The two European agencies declined to provide country-by-country breakdowns of arrests, details of items seized or the specific days when the raids occurred.

In Paris, the state prosecutor's office said French detectives arrested more than two dozen people during May 13 raids and described the global nature of the arrests and searches as an unprecedented "new form of judicial action." It said those arrested were identified by the FBI as French "citizens who had acquired or used this software."

In a BlackShades-related investigation before the latest global arrests, Dutch police earlier this year arrested an 18-year-old man for using the malware to take pictures of women and girls using about 2,000 computers.

Sterling reported from Amsterdam. Associated Press writers Jamey Keaten in Paris, Raphael Satter in London and Tom Hays in New York contributed to this report.