

FBI: BlackShades infected half-million computers (Update)

May 19 2014, by Larry Neumeister



Preet Bharara, U.S. Attorney for the Southern District of New York, discusses arrests in the malware BlackShades Remote Access Tool, during a news conference in New York, Monday, May 19, 2014. 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 Monday against more than 100 people worldwide. (AP Photo/Richard Drew)

More than a half-million computers in over 100 countries were infected by sophisticated malware that lets cybercriminals remotely hijack a computer and its webcam, authorities said as charges were announced Monday against nearly 100 people worldwide.

Authorities said 97 people suspected of using or distributing the malicious software called BlackShades have been arrested in 16 countries, including the software's owner, a 24-year-old Swedish man.

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

U.S. Attorney Preet Bharara called BlackShades a "frightening form of cybercrime," saying a cybercriminal could buy a \$40 malicious program whose capabilities were "sophisticated and its invasiveness breathtaking." FBI Agent Leo Taddeo said people suspecting they are BlackShades victims should visit FBI.gov to learn how to check computers.

Authorities said the BlackShades Remote Access Tool or "RAT" has been sold since 2010 to several thousand users, generating sales of more than \$350,000. The agency said one of the program's co-creators is cooperating and had provided extensive information.



Preet Bharara, U.S. Attorney for the Southern District of New York, discusses arrests in the malware BlackShades Remote Access Tool, during a news conference in New York, Monday, May 19, 2014. 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 Monday against more than 100 people worldwide. (AP Photo/Richard Drew)

BlackShades owner, Alex Yucel, arrested in Moldova last November, is facing extradition to the United States. Michael Hogue, 23, of Maricopa, Arizona—the program's co-creator—had pleaded guilty in New York after his June 2012 arrest and is cooperating, Bharara said.

The malware lets hackers steal personal information, intercept keystrokes and hijack webcams to secretly record computer users. BlackShades also can be used to encrypt and lock computer data files,

forcing people to pay a ransom to regain access.

The hacking tool's low cost has boosted its popularity across the hacker underground, where variants have long circulated online.

Last year, security firm Symantec said use of BlackShades was rising, with program licenses costing \$40 to \$100.

French officials said raids last week followed the FBI's arrest of two BlackShades developers and its distribution of a list of the malware's customers.



Leo Taddeo, special agent-in-charge, Federal Bureau of Investigation, Special Operations and Cyber Division, discusses arrests in the malware BlackShades Remote Access Tool, during a news conference in New York, Monday, May 19, 2014. 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 Monday against more

than 100 people worldwide. (AP Photo/Richard Drew)

Law enforcement coordination agencies Europol and Eurojust, based in The Hague, Netherlands, said Monday 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.

In Paris, the state prosecutor's office said more than two dozen people were arrested during May 13 raids. It said those arrested were identified by the FBI as French "citizens who had acquired or used this software."



Preet Bharara, U.S. Attorney for the Southern District of New York, discusses

arrests in the malware BlackShades Remote Access Tool, during a news conference in New York, Monday, May 19, 2014. 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 Monday against more than 100 people worldwide. (AP Photo/Richard Drew)

In a previous BlackShades-related investigation, Dutch police this year arrested an 18-year-old man for using the malware to take pictures of women and girls within view of webcams on about 2,000 computers.

A Southern California man who was sentenced in March to prison for hacking the computers of a future Miss Teen USA and other young women was not part of the case. Although authorities say that he had BlackShades on his computer, but that it wasn't clear whether he used it or another program.

© 2014 The Associated Press. All rights reserved.

Citation: FBI: BlackShades infected half-million computers (Update) (2014, May 19) retrieved 22 September 2024 from <https://phys.org/news/2014-05-raids-blackshades-hackers.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.