Police make 5 arrests in 'unprecedented' cybercrime takedown

December 1 2016, by Raphael Satter

German Interior Minister Thomas de Maiziere speaks about the arrest of heads of a group called Avalanche, in Berlin, Thursday Dec. 1, 2016. Also Europol says five key suspects have been arrested in connection with a massive operation aimed at knocking out a cybercrime group accused of inflicting hundreds of millions of euros in losses worldwide. The European Union police agency said the sweep was "unprecedented in its scale" and resulted in the seizure of 39 servers and hundreds of thousands of internet domains used by the group, nicknamed Avalanche. (Kay Nietfeld/dpa via AP)

U.S. and European officials say they've knocked out a cybercrime group accused of inflicting hundreds of millions of dollars in losses worldwide, putting five key suspects in custody.

The European Union police agency said Thursday the sweep was "unprecedented in its scale" and resulted in the seizure of 39 servers and hundreds of thousands of internet domains used by the Avalanche network, a major player in the market for cybercrime services.

Unlike some past seizures—which grabbed crooks' infrastructure while leaving the masterminds free to reorganize their networks—officials say they're confident they've struck a fatal blow this time.

"We have arrested the top, the head of the snake," Fernando Ruiz, the head of operations at Europol's Cybercrime Center, told The Associated Press ahead of the announcement. "We are sure that this will have a very huge impact."

Ruiz called Avalanche "the perfect example of crime as a service," saying the massive network was rented out by players across the underworld to send spam, direct malicious software and to recruit money mules.

As a cybercriminal, Ruiz said, "you will contact this organization, and this organization will give you all you need."

He said the arrests Wednesday followed months of preparation and years of investigation by law enforcement agencies. In a separate statement , the U.S. Department of Justice said 40 different countries were involved and accused the network of hosting some of the world's most pernicious malware as well as several money laundering campaigns.

German Interior Minister Thomas de Maiziere speaks about the arrest of heads of a group called Avalanche, in Berlin, Thursday Dec. 1, 2016. Also Europol says five key suspects have been arrested in connection with a massive operation aimed at knocking out a cybercrime group accused of inflicting hundreds of millions of euros in losses worldwide. The European Union police agency said the sweep was "unprecedented in its scale" and resulted in the seizure of 39 servers and hundreds of thousands of internet domains used by the group, nicknamed Avalanche.(Kay Nietfeld/dpa via AP)

German Interior Minister Thomas de Maiziere told reporters at a press conference in the town of Lueneburg that the size of the operation was "unique."

The network came into focus in 2012 after German officials began looking into the spread of fake police ransomware—an early form of extortion software designed to trick users into thinking their computers had been locked down by law enforcement—according to Orla Cox, the director of security intelligence at Symantec Corp., a California-based

security firm which participated in the investigation. That inquiry eventually widened to include dozens of other law enforcement agencies investigating a wide array of misdeeds.

German authorities alone would eventually record 1,336 crimes in connection with the group. Neither U.S. or European officials would issue precise figures but both said losses connected to the gang's activities reached into the hundreds of millions.

German officials suggested other, potentially lower-ranking members of the gang appear to have escaped the global dragnet.

Lutz Gaebel, press officer at the German Federal Prosecutor's Office, right, speaks at a press conference in Lueneburg, Germany, Thursday Dec. 1, 2016. Police announced the discovery and neutralization of a massive online fraud network. Also Europol says five key suspects have been arrested in connection with a massive operation aimed at knocking out a cybercrime group accused of inflicting hundreds of millions of euros in losses worldwide.The European Union

police agency said the sweep was "unprecedented in its scale" and resulted in the seizure of 39 servers and hundreds of thousands of internet domains used by the group, nicknamed Avalanche. (Philipp Schulze/dpa via AP)

Prosecutors there said they were able to identify 16 people at the group's "leadership level" and a court in the German town of Verden had issued arrest warrants for seven of them. It's not clear how many, if any, of the seven people being sought by German authorities overlap with the five individuals arrested Wednesday.

Ruiz, of Europol, declined to give any details of those arrested or even say where they had been detained, saying the countries where the arrests took place had asked not to be identified.

Cox, with Symantec, confirmed that some suspects were still at large but said law enforcement was still pretty sure they'd beaten Avalanche, given the sheer scale of what they'd seized.

"We can never say it's completely done but confidence levels are high this time around," Cox said.

Lutz Gaebel, press officer at the German Federal Prosecutor's Office, right, speaks at a press conference in Lueneburg, Germany, Thursday Dec. 1, 2016. Police announced the discovery and neutralization of a massive online fraud network. Also Europol says five key suspects have been arrested in connection with a massive operation aimed at knocking out a cybercrime group accused of inflicting hundreds of millions of euros in losses worldwide.The European Union police agency said the sweep was "unprecedented in its scale" and resulted in the seizure of 39 servers and hundreds of thousands of internet domains used by the group, nicknamed Avalanche. (Philipp Schulze/dpa via AP)

This is a Friday Jan. 11, 2013 file photo of a member of the Cybercrime Center as he turns on the light in a lab during a media tour at the occasion of the official opening of the Cybercrime Center at Europol headquarters in The Hague, Netherlands. Europol said Thursday Dec. 1, 2016, that five arrests have been made in connection with a massive operation aimed at knocking out a cybercrime group accused of inflicting hundreds of millions of euros in losses worldwide. (AP Photo/Peter Dejong, File)

This is Friday, Jan. 16, 2015 file photo of the European police agency Europol in The Hague, Netherlands. Europol said Thursday Dec. 1, 2016, that five arrests have been made in connection with a massive operation aimed at knocking out a cybercrime group accused of inflicting hundreds of millions of euros in losses worldwide. (AP Photo/Peter Dejong, File)

Citation: Police make 5 arrests in 'unprecedented' cybercrime takedown (2016, December 1) retrieved 20 April 2024 from https://phys.org/news/2016-12-police-unprecedented-cybercrime-takedown.html