Emotet takedown is not like the Trickbot takedown

intel471.com/blog/emotet-takedown-2021

On Wednesday, January 27, U.S. and European law enforcement agencies announced that they had seized control of Emotet, the notorious botnet that's been used by cybercriminals all over the world for the past decade.

Based on the information available to Intel 471, the law enforcement operation took place Jan. 26, 2021, resulting in the arrest of several Ukrainian nationals allegedly responsible for running the botnet's infrastructure.

Only time will tell if the takedown will have a long-term impact on Emotet operations. The groups who run these botnets are sophisticated and resilient, and will most likely have some sort of inherent recovery in place. Emotet itself does not appear to have any sort of recovery mechanism, but a lot of the infected machines will have other malware installed as well, such as Qbot, Trickbot or something else. That could be leveraged to rein in the infected machines and put them back under their control. Yet, right now, those bots are talking to servers controlled by the good guys.

Additionally, oftentimes groups like this tend to be composed of members spread across different countries, some of which may not be so open to cooperating with international law enforcement. This leaves open the possibility that someone will simply take the code and rebuild.

A rebuild or recovery won't be hard to detect, however.

Those scenarios aside, what was announced on Wednesday is very promising. The effort is a shining example of what needs to be done in order to have any real impact on these organized cybercrime groups. The difference between disruption and takedown boils down to criminals being put in handcuffs. It's the pinnacle of a takedown operation and the only way to have a long term impact on the health and safety of the internet.