2017-12-04

4 December 2017

On 29 November 2017, the Federal Bureau of Investigation (FBI), in close cooperation with the Luneburg Central Criminal Investigation Inspectorate in Germany, Europol's European Cybercrime Centre (EC3), the Joint Cybercrime Action Task Force (J-CAT), Eurojust and private-sector partners, dismantled one of the longest running malware families in existence called Andromeda (also known as Gamarue).

This widely distributed malware created a network of infected computers called the Andromeda botnet (1). According to Microsoft, Andromeda's main goal was to distribute other malware families. Andromeda was associated with 80 malware families and, in the last six months, it was detected on or blocked an average of over 1 million machines every month. Andromeda was also used in the infamous Avalanche network, which was dismantled in a huge international cyber operation in 2016. Steven Wilson, the Head of Europol's European Cybercrime Centre said: *"This is another example of international law enforcement working together with industry partners to tackle the most significant cyber criminals and the dedicated infrastructure they use to distribute malware on a global scale. The clear message is that public-private partnerships can impact these criminals and make the internet safer for all of us."*

One year ago, on 30 November 2016, after more than four years of investigation, the Public Prosecutor's Office Verden and the Luneburg Police in Germany, the United States Attorney's Office for the Western District of Pennsylvania, the Department of Justice, the FBI, Europol, Eurojust and global partners, had dismantled the international criminal infrastructure Avalanche. This was used as a delivery platform to launch and manage mass global malware attacks such as Andromeda, and money mule recruitment campaigns.

Insights gained during the Avalanche case by the investigating German law enforcement entities were shared, via Europol, with the FBI and supported this year's investigations to dismantle the Andromeda malware last week.

Jointly, the international partners took action against servers and domains, which were used to spread the Andromeda malware. Overall, 1500 domains of the malicious software were subject to sinkholing (2). According to Microsoft, during 48 hours of sinkholing, approximately 2 million unique Andromeda victim IP addresses from 223 countries were captured. The involved law enforcement authorities also executed the search and arrest of a suspect in Belarus. Simultaneously, the German sinkhole measures of the Avalanche case have been extended by another year. An extension of this measure was necessary, as globally 55 per cent of the computer systems originally infected in Avalanche are still infected today.

The measures to combat the malicious Andromeda software as well as the

extension of the Avalanche measures involved the following EU Member States: Austria, Belgium, Finland, France, Italy, the Netherlands, Poland, Spain, the United Kingdom, and the following non-EU Member States: Australia, Belarus, Canada, Montenegro, Singapore and Taiwan.

The operation was supported by the following private and institutional partners: Shadowserver Foundation, Microsoft, Registrar of Last Resort, Internet Corporation for Assigned Names and Numbers (ICANN) and associated domain registries, Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), and the German Federal Office for Information Security (BSI).

The operation was coordinated from the command post hosted at Europol's HQ.

1. Botnets are networks of computers infected with malware, which are under the control of a cybercriminal. Botnets allow criminals to harvest sensitive information from infected computers, such as online banking credentials and credit card information. A criminal can also use a botnet to perform cyberattacks on other computer systems, such as denial-of-service attacks.

2. Sinkholing is an action whereby traffic between infected computers and a criminal infrastructure is redirected to servers controlled by law enforcement authorities and/or an IT security company. This may be done by assuming control of the domains used by the criminals or IP addresses. When employed at a 100% scale, infected computers can no longer reach the criminal command-and-control computer systems and criminals can therefore no longer control the infected computers. The sinkholing infrastructure captures victims' IP addresses, which can subsequently be used for notification and follow-up through dissemination to National CERTs and network owners.