Operation Avalanche

A closer look

April 2017

Operation Avalanche: a closer look

Key threats

A German investigation into an OCG called Avalanche involved in malware, phishing and spam activities commenced in 2012, after a wave of encryption ransomware infected a substantial number of computer systems, blocking users' access. The investigation exposed the existence of a highly sophisticated technical infrastructure that was used to infect millions of private and business computer systems with malware (e.g. banking Trojans and ransomware), enabling the criminals operating the network to harvest bank and e-mail passwords.

With this information, the criminals were able to perform bank transfers from the victims' accounts. The proceeds were then redirected to the criminals through an infrastructure specifically created to secure the proceeds of the criminal activity. In addition to launching and managing mass global malware attacks, the Avalanche network was used for money mule recruiting campaigns. The Avalanche infrastructure was set up in a way that was highly resilient against takedowns and law enforcement action (through so-called 'double fast-flux' technology).

Eurojust and Europol

The need for broad international cooperation arose in 2015. The German prosecution and law enforcement authorities approached Eurojust and Europol for support. While at this point in time certain actions against parts of the network had taken place, wide-ranging cooperation had not been established, nor had the perpetrators been identified.

Several operational and coordination meetings, which brought together a large number of Member States and third States, including the USA and Azerbaijan, were held at Europol and Eurojust, with both agencies cooperating closely. Prior to the final coordination meeting, a level II meeting, attended exceptionally by German and US prosecutors and law enforcement officers, was held at Eurojust, with a limited group of countries that would not be present during the following coordination meeting. The operational and coordination meetings served to plan a global joint action day and to clarify legal issues and concepts related to this form of cybercriminality.

Eurojust supported the work of the involved judicial authorities by mapping out the legal requirements to effectuate the necessary interventions, as well as facilitating the drafting and timely execution of letters of request.

EC3 supported the investigation by facilitating secure information exchange, providing in-depth analysis and advanced digital forensic support, and fostering cooperation between law enforcement and private partners.

Impact

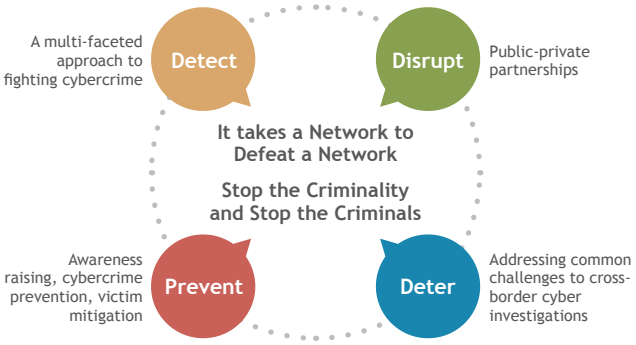
The Avalanche infrastructure had been used since 2009, causing an estimated EUR 6 million in damages in concentrated cyberattacks on online banking systems in Germany alone. In addition, the monetary losses associated with malware attacks conducted over the Avalanche network were estimated to be in the hundreds of millions of euros worldwide, although exact calculations were difficult due to the large number of malware families managed through the platform. Initially, an action day was foreseen for 2015. This action day was postponed to late 2016 to allow for an identification of the perpetrators, through close cooperation with the US authorities.

While initial sovereignty concerns were raised by the fact that servers subject to takedown were located in various jurisdictions, discussions among the relevant authorities resolved the matter. Similarly, concerns were raised that, under various participating countries' legislation, the seizure of so-called unborn domains was not possible. Eurojust's Seconded National Expert on Cybercrime was able to inform the national authorities that in this case the problem would not arise, as the status of the domains in question would change from unborn to born by the time the actions took place. His advisory role towards the National Desks and national authorities continued throughout the investigation. Additionally, he provided contact details of judicial authorities in countries outside of Eurojust's contact network.

Private sector

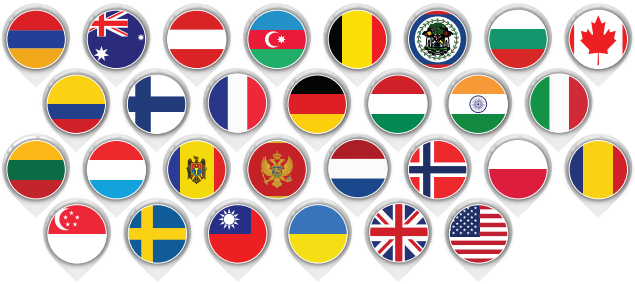
Cooperation with several non-profit and private sector partners was initiated to allow for the analysis of over 130 TB of captured data and identification of the server structure of the botnet, leading to the shutdown of servers and the collapse of the entire criminal network.

The partners included the German *Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie*, the Shadowserver Foundation, Registrar of Last Resort and the Internet Corporation for Assigned Names and Numbers (ICANN). Other partners, such as INTERPOL and the Ibero-American Network for International Legal Cooperation (IberRed), also played an important role, particularly in preparation of the joint action day. IberRed served as a liaison to Spanish-speaking countries, mainly in South America.



Results

On the action day in November 2016, Europol hosted a command post, in which Eurojust participated and provided immediate support to the judicial authorities involved in the action day. At the command post, the German prosecutor and police officers worked together with representatives of the involved countries and private industry partners to ensure the success of such a large-scale operation. This global effort to take down the network involved the crucial support of prosecutors and investigators from 29 countries.



As a first result, five individuals were arrested, 37 premises were searched, and 39 servers were seized. Victims of malware infections were identified in over 180 countries. In addition, 221 servers were put offline through abuse notifications sent to the hosting providers. Over 800 000 domains associated with the criminal infrastructure were sinkholed, and dedicated webpages were created for the public to assist in removing the malware from their computers and to prevent further illegal access.

Lessons learned

To help the involved countries with their investigations, close cooperation between Eurojust and Europol in organising joint meetings saved both time and money.

This operation showed that only when public and private entities collaborate as a team can a large and sophisticated criminal network be taken down. Cybercrime truly is a global phenomenon and requires cooperation between authorities, which is sometimes most efficiently established by tapping into regional networks of practitioners.

A business model lies behind every successful cybercrime venture. By targeting the business model of the Avalanche network and devising ways of interfering with the perpetrators and the technical infrastructure, as well as identifying and supporting the victims, one of the most sophisticated cybercrime networks of the past years was effectively shut down. The operations yielded valuable insights into the cybercriminal business model. At the same time, the trust built among the cooperating public and private entities will prove to be an invaluable asset in the future fight against cybercrime. Since the action day, the approach in the case has been regarded as best practice amongst cybercrime investigators and prosecutors.


© ZKI Lüneburg

The lead prosecutor, Mr **Frank Lange**, said:

Having trustworthy and quick international cooperation, beyond the traditional means of legal assistance, was essential to Avalanche's success. Eurojust and EC3 played an important role in establishing the atmosphere for cooperation between judicial participants and police. The organisation of coordination meetings at Eurojust and operational meetings at Europol, as well as their further support by forwarding information and letters of request to the correct recipients, laid the groundwork for a truly multinational approach. We are really grateful.

Eurojust, Johan de Wittlaan 9, 2517 JR The Hague, Netherlands
Phone: +31 70 412 5000 - E-mail: info@eurojust.europa.eu - Website: www.eurojust.europa.eu

Catalogue number: QP-01-17-801-EN-N • *ISBN*: 978-92-9490-158-3 • *Doi*: 10.2812/816706