Operation BlackShades

An Evaluation

April 2015

Operation BlackShades: an Evaluation

BlackShades was an organisation developing and selling malicious software (malware) that enabled buyers to infect computers and remotely take over and control the operations of the infected computers, and perform distributed denial-of-service (DDoS) cyber-attacks, among other things. An FBI investigation revealed links to several Member States. An example from the Netherlands of how the malware could be used for criminal purposes was that of an 18-year-old man who infected at least 2 000 computers, controlling the victims' webcams to take pictures of women and girls.

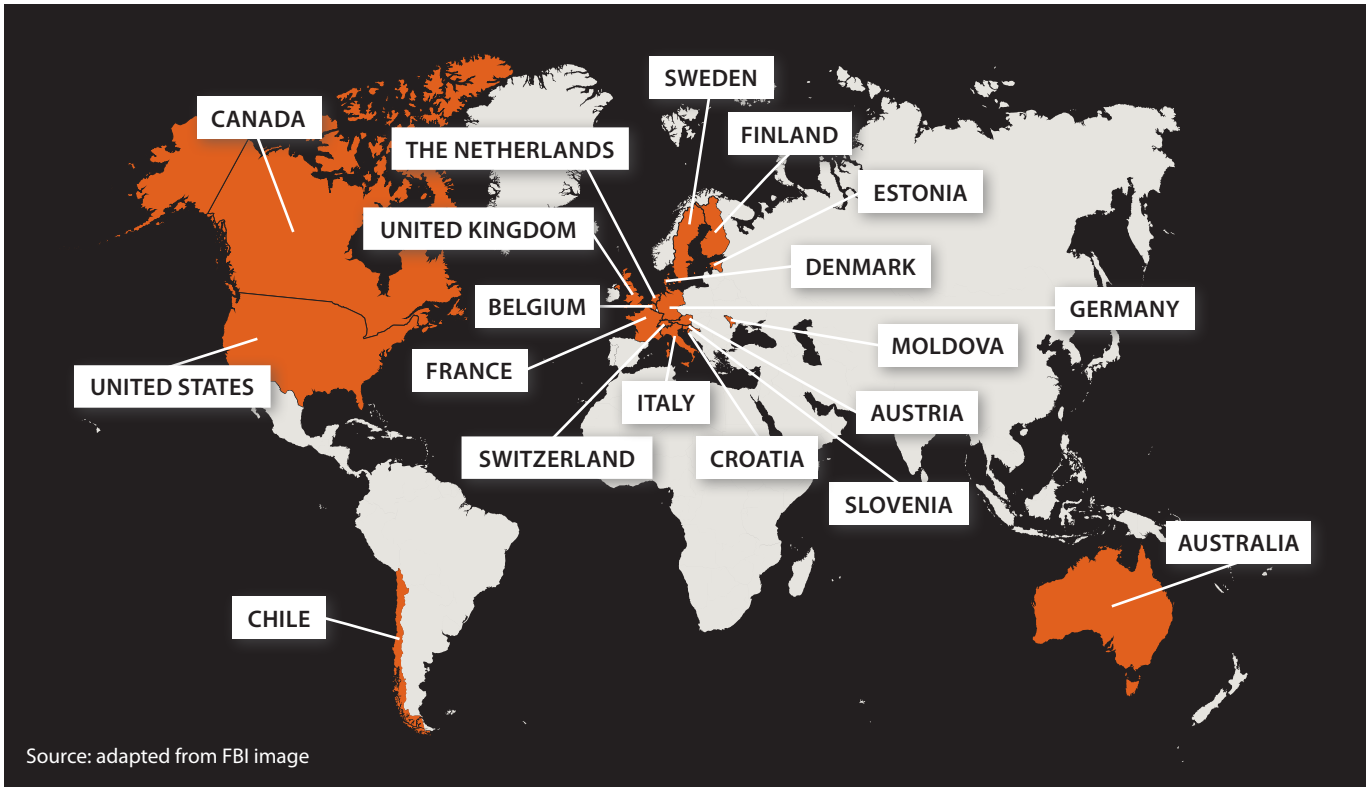
Eurojust was approached through the Dutch prosecutor who was in contact with the FBI and the US Attorney's Office regarding this investigation. While the US authorities intended to take down the BlackShades server, they did not have the intention of pursuing foreign subjects for prosecution in the USA. As creators, sellers and users of BlackShades malware were targeted by judicial and law enforcement authorities in 16 States during this worldwide investigation, the added value of judicial cooperation was apparent and the Netherlands opened a case in November 2013; a coordination meeting was convened in the same month. Three additional coordination meetings were organised in January, April and July 2014.

The objective of the initial coordination meeting was to ascertain which States could take judicial measures against identified subjects and to explore the possibility of a common judicial approach among the States involved. Although arranged on relatively short notice, authorities from the requesting State, the USA, Romania, Belgium, Germany, France and representatives from EC3 at Europol attended the meeting. Some States had been carrying out their own investigations into this malware and acknowledged the need for judicial cooperation at international level. It was evident that States other than those participating in the meeting were affected, and at subsequent meetings, these States were invited.

The US authorities were already at an advanced stage in their investigations and informed this first meeting of a two-step plan: the dismantling of the BlackShades organisation and the international takedown of the server to stop the sale of the software. The coordination meeting contributed to the US investigations through the identification of 20 customers of the BlackShades organisation.

Investigations in the participating Member States were at different stages, which inevitably meant that some time was needed to align the efforts of the various

International cooperation in the BlackShades case



national authorities. Several States indicated that while some suspects had been identified, there was a need for more information either to be able to open a case or to enrich the data already available.

Participants of the meeting were informed that not only suspects in the USA, but also in Member States, were already known for, or could be linked to, other cybercrime offences. For one Member State, the possession of a copy of the malicious software itself was important, while for another Member State, the mere possession of the software was not enough, and it had to be shown that the software was created predominantly for illegal use.

The investigation culminated in a common action lasting two days in May 2014, coordinated by Eurojust through a coordination centre at Eurojust, supported by EC3. During the two action days, 359 house searches were carried out worldwide, and 97 people were arrested. Over 1 100 data storage devices suspected of being used in illegal activities were seized, including computers, laptops, mobile telephones, routers, external hard drives and USB memory sticks. Substantial quantities of cash, illegal firearms and drugs were seized. Authorities also succeeded in seizing the domain of the BlackShades website. States that undertook actions were the Netherlands, Belgium, France, Germany, the UK, Finland, Austria, Estonia, Denmark, Italy, Croatia, the USA, Canada, Chile, Switzerland and Moldova.

Eurojust assisted the involved States by delivering overviews of the status of the investigations in each State and by providing judicial assistance. Representatives of Europol and the FBI were present at the coordination centre set up at Eurojust, and EC3 provided real-time analytical support. EC3 was also committed to supporting the follow-up and identification of victims, as well as to promoting technical solutions to protect computers against this malware.

The Dutch prosecutor in charge of the case and the Assistant to the National Member for the Netherlands jointly commented on the success achieved: '*Operation BlackShades is a fine example of cross-border judicial cooperation in practice. The Internet is not a safe environment for criminals. This case, involving so many Member States and third States, with the common goal of stopping further cyber-attacks, shows the potential of worldwide joint actions and points the way to future common efforts. We are very pleased with the outcome.*'

Based on meeting reports and the evaluation performed in the aftermath of the common action days, it was possible to detect some legal and practical challenges that had an impact on the timeframe and the outcome of the case. A number of lessons learned and the best practice in this case were identified.

Legal and practical issues

- A challenge throughout the case was the fact that the investigations were at different stages in the participating States: at the first coordination meeting, it became clear that some States needed an additional period of up to two months to receive additional information regarding the alleged criminal acts.

- The advantages of extending the case to a large number of States and coverg as many criminal acts as possible had to be weighed against the disadvantages of delays and loss of momentum in States in which the investigations were at a more advanced stage.

- At the beginning of the Eurojust case, some States needed to enrich their data through MLA to have enough evidence to pursue the case at national level.

- Some States were limited by the fact that possession of the software alone was not sufficient to commence judicial proceedings against the suspect, that there was a need to prove the malware had caused damage and that victims had been identified. Others needed to prove that the software had been created for predominantly illegal use.

- Several States indicated that information for their investigations was needed quickly to comply with data retention terms, which varied among the States and depended on whether the term concerned IP addresses only or also other data.

- In some States, several cases concerning BlackShades were opened, which added complexity to the coordination of the case. For instance in France, where no national cyber prosecutor exists, coordination had to be ensured between the eight interregional specialised jurisdictions, which represent cz1 prosecution districts.

Investigation culminates in a two-day coordination centre held at Eurojust in May 2014. Photo © Eurojust

- In some instances, authorisation to publish a press release is required from more than one authority. Awareness of the accurate contact points and early communication ensured timely publication of the press release.

Lessons learned

- Two common action days appeared at the time to be the method of delivering the best possible result. However, as news on the internet spreads swiftly, synchronising the timing of searches, seizures and arrests in future operations is to be preferred, particularly when large-scale operations are involved.

- The importance of collecting information on the victims and financial loss caused by the malware was emphasized, as sentencing in cybercrime cases, particularly in the USA, is victim- and loss-driven.

- Instead of focusing solely on repressive measures, the UK undertook high-volume preventative activity to deter lower-level purchasers of BlackShades from becoming involved in cybercrime. This activity involved sending warning e-mails and letters to approximately 500 purchasers and warning visits by the National Crime Agency (NCA) and police staff to approximately 100 purchasers.

Best practice

- During the first coordination meeting, participants pointed to the positive effects of having a meeting at judicial level at an early stage of the case, as in most Member States decisions regarding searches, seizures and arrests are taken at judicial level. Early coordination at judicial level also made it possible to find a unified approach among the Member States to ensure sufficient information for convictions in several Member States.

- The distribution of points of discussion prior to the coordination meeting was seen as very advantageous to the productivity and concrete outcome of the meeting.

- To streamline and simplify the house searches and interviews regarding the malware in question, an FBI Interview/Search Guide was circulated by Europol via its Secure Information Exchange Network Application (SIENA) to the participating authorities. Due to the complications involved in securing evidence in cybercrime cases, this guide was considered very useful.

- To hold a debriefing after the coordination centre was valuable in identifying the added value of this coordination tool and drawing lessons from the cooperation during the common action days.

- The evaluation of the case at the final meeting showed that Eurojust's analysis of the judicial situation in the participating States at the early stages of the case was advantageous to the results of the case, as this analysis allowed the national authorities to come prepared to the coordination meetings.

- A letter from the Dutch authorities, which was transmitted through Eurojust and which confirmed that the information provided in this case could be used as evidence in judicial proceedings, was seen as welcome support for the ongoing proceedings in various participating States.

- Willingness to share information between the participating States largely contributed to the impressive results of the case and was seen as a key factor in future cybercrime cases.

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-02-17-914-EN-N • *ISBN*: 978-92-9490-164-4 • *Doi*: 10.2812/048221