The Hague, June 2013

Intelligence Notification 004-2013

CYBER BITS

Hackers deployed to facilitate drugs smuggling

What happened?

On 17 June Belgian and Dutch authorities reported on arrests made in a drugs investigation. The members of the criminal group smuggled drugs through the harbour of Antwerp to The Netherlands. A dozen suspects have been arrested and 1 044 kilos of cocaine as well as 1 099 kilos of heroin have been seized. What's interesting is that the criminal group used hackers to access the computer systems of harbour companies and container terminals.

How does it work?

Using hackers, the criminals took control of the computers of two container terminals and of a harbour company. The approach was twofold:

- Classic intrusion by sending mails with attachments containing Trojans to staff members;
- Breaking into offices to install key logging devices to capture passwords.

Once the computers were under their control, the group could follow "their" container and upon arrival, unload it to a location and at a time of their choosing. This in return enabled the criminal group's drivers to access the container before the normal harbour staff would.

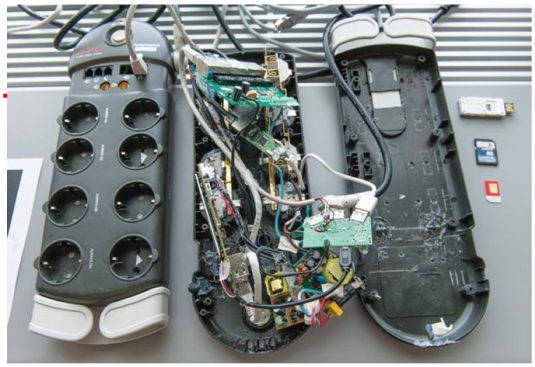
The investigation discovered that the intrusion mails were sent from a Dutch IP address. The stolen data were forwarded to a server owned by the criminal group.

Why do you need to know?

- It's one of the first times this modus operandi has been revealed;
- The criminal group was professional and well-connected as demonstrated by the amounts of drugs seized. It can be assumed that their modus operandi has been shared with other criminal groups who will try to do the same in other ports and airports;
- Europol currently has no view on the cyber resilience of cargo companies and container terminals in harbours. We suggest evaluating the cyber security situation for the various companies involved in cargo handling, especially in the big harbours. The focus should be on the risks and vulnerabilities of the different actors involved. Awareness has to be raised that for instance signs of a burglary should not be ignored. The use of short term contractors from different companies might also increase the risk of infiltration.
- EC3 would welcome reactions on this note. Please mail to O31@europol.europa.eu.

CYBER BITS

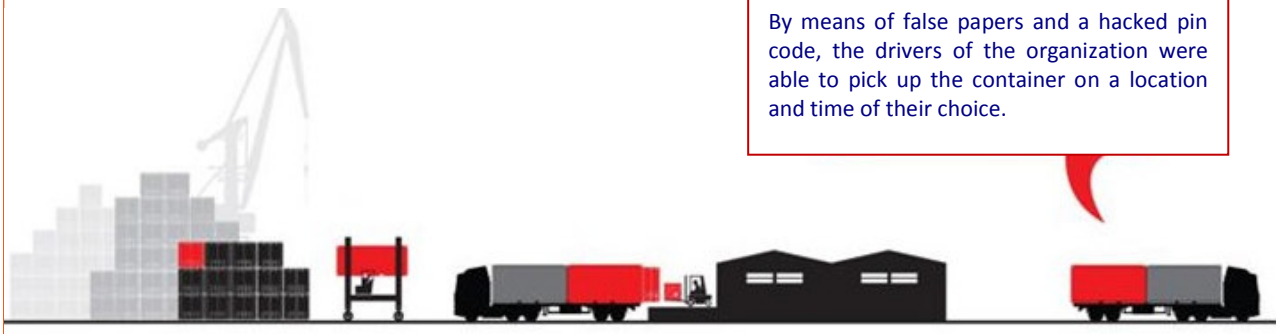
By breaking into the offices of a harbour company, the criminals could install key logger devices to take control of the computers.



Computers of container terminals were hacked so the containers containing drugs could be monitored.

Modus Operandi

By means of false papers and a hacked pin code, the drivers of the organization were able to pick up the container on a location and time of their choice.



Copyright: "De Standaard"