

**Federal Bank of Atlantis Ltd.**

FBA Bank Towers  
Atlantis     123456  
Tél : +1123.456.789  
Fax : +1123.456.987

Date : 2 octobre 2017

Atlantis

**Service des technologies de l’information**

**Déclaration de Neo Matrix**

Je suis employé par la Federal Bank of Atlantis en qualité de chef du Service informatique.

Le 29 septembre, dans le courant de l’après-midi il me semble, j’ai été informé d’une anomalie lors d’un virement entre nous et la société UBP. Apparemment, quelqu’un avait eu accès à l’échange de courriels entre des personnes impliquées dans cette opération.

J’ai commencé immédiatement l’analyse des logs entre le 20 septembre et le 1er octobre, en particulier pour les appareils dont les adresses IP étaient celles de Nicos Nikolakis, Georgos Atlantis, Yorgos Yorgos et Artemida Olimpiakos.

Ce qui nous a semblé d’emblée très bizarre est qu’il semblait que tous leurs ordinateurs avaient des connexions avec un ordinateur spécifique dans le Service DLO sur certains ports normalement non utilisés pour une communication normale. De plus, le type de données transférées utilisait un format étrange que nous ne connaissons pas.

Lors du contrôle de cet appareil spécifique, les choses sont devenues encore plus bizarres, puisqu’après chaque communication entre ces ordinateurs, le serveur du courrier électronique enregistrait l’envoi de mails courts entre l’ordinateur qui « collectait » et un ou des ordinateurs communiquant vers l’extérieur, dont un sur des ports et selon des protocoles très similaires aux serveurs ouverts SMTP.

Nous avons examiné plus profondément l’ordinateur en question et avons trouvé des traces d’interface de contrôle et de logs d’un programme espion très similaire aux logiciels FlexiSpy ou Spytech. L’ordinateur collecteur a été identifié comme étant utilisé par un employé récemment arrivé à la DLO, du nom de Hermes Novas.

Nous avons extrait des logs du trafic et des serveurs de courrier électronique et avons copié la boîte mail de l’ordinateur de Hermes Nova. Nous avons également placé tous les ordinateurs susmentionnés sous scellés et préservé les données sur notre ordinateur principal après en avoir informé notre Conseil de direction qui nous y a autorisé en attendant que les autorités reprennent l’affaire.

Le Chef du Service informatique de la FBA

Neo Matrix