MINISTÈRE
DE LA JUSTICE
Liberté
Égalité
Fraternité

PARQUET DU TRIBUNAL JUDICIAIRE DE PARIS

Paris, le 29 août 2023

Communiqué de presse de la procureure de la République

Le 26 août 2023, une opération internationale impliquant les autorités policières et judiciaires des Etats-Unis, de l'Allemagne, des Pays-Bas et de la France a permis le démantèlement de l'infrastructure du réseau malveillant Qakbot (aussi appelé Qbot, ou Pinkslipbot), ainsi que la saisie de 8,6 millions de dollars en crypto-monnaies. La section de lutte contre la cybercriminalité de la Juridiction Nationale de Lutte contre la Criminalité Organisée (JUNALCO) du parquet de Paris a supervisé la partie française.

Le principe d'action des cybercriminels consistait dans un premier temps à déployer leur logiciel malveillant Qakbot au moyen de cyberhameçonnage sur des ordinateurs ciblés, puis d'y implanter d'autres malwares, par exemple de rançongiciels. L'ensemble des machines infestées étaient connectées ensemble sous forme de réseau (botnet), pouvant être vendu comme tel à d'autres cybercriminels. C'est alors seulement que ceux-ci ont pu exiger des rançons en cryptomonnaies, sans même que les victimes aient eu préalablement conscience d'être infectées.

La sous-direction de la lutte contre la cybercriminalité a travaillé en coopération avec les enquêteurs des autres pays, sous la direction des parquets de Paris, Los Angeles, Francfort, et Rotterdam, à l'identification de cette infrastructure. Au total, les enquêteurs ont établi que plus de 700 000 machines dans le monde, dont 26 000 en France, ont à un moment ou un autre été infectées, et que près de 58 millions de dollars de rançons en sont l'effet. Six serveurs sur les 170 à l'origine du bot se trouvaient sur le territoire français.

Dans la nuit du 26 août 2023, le FBI a procédé à la redirection de l'ensemble du trafic vers des serveurs sous son contrôle, libérant toutes les machines du botnet, et rendant celui-ci tout à fait inopérant. L'opération a conduit en outre à la coupure d'une cinquantaine de serveurs répartis entre les quatre pays partenaires, puis à la mise hors opération du reste de l'infrastructure.

Comment savoir si on fait partie des victimes ?

Le site https://politie.nl/checkyourhack, mis en ligne par la Police Néerlandaise, permet, en s'y connectant, de savoir si sa machine est infectée. Si votre opérateur vous contacte, c'est que vous avez à un moment été infecté.

Que faire si on est victime ?

Si vous figurez sur ces listes de victimes, vous pouvez vous rendre sur le site de Cybermalveillance.gouv.fr où les démarches à suivre vous seront indiquées :

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/victimes-qbot

Laure BECCUAU

Procureure de la République

Contact presse :

01 44 32 68 10
scom.parquet.tj-paris@justice.fr