CYBERSURVEILLANCE

Predator Files

Depuis le vendredi 6 octobre, « Le Soir » publie plusieurs épisodes des « Predator Files », enquête collaborative coordonnée par le réseau EIC (European Investigative Collaborations). Sur base de documents confidentiels, celle-ci dévoile les coulisses de l'alliance Intellexa, qui depuis l'Europe a commercialisé le logiciel espion Predator.

Les manœuvres du Vietnam pou dont la présidente du Parlement

Les « Predator Files », c'est quoi ?

L'enquête « Predator Files » à laquelle a collaboré *Le Soir* révèle comment plusieurs sociétés implantées en Europe ont développé et vendu de puissants outils de cybersurveillance à plusieurs dictatures et régimes au bilan décrié sur le plan du respect des droits humains. Et ce avec la complicité passive de plusieurs Etats membres de l'UE.

Plus spécifiquement, « Predator Files » dévoile les dessous d'une campagne commerciale atteignant son paroxysme avec l'émergence d'un consortium appelé Intellexa, au travers duquel le redoutable logiciel espion Predator a été fourni à plusieurs Etats autoritaires. Des activistes, des journalistes et des chercheurs ont depuis lors été pris pour cible par ce *spyware*, de même que des officiels européens et états-uniens.

Sur base de centaines de documents confidentiels obtenus par Mediapart et *Der Spiegel*, l'enquête a été menée durant un an sous la coordination du réseau de médias European Investigative Collaborations (EIC.network) et grâce à l'appui technique du Security Lab d'Amnesty International.

Outre *Le Soir*, les médias participant au projet sont : Mediapart (France), *Der Spiegel* (Allemagne), *De Standaard* (Belgique), *NRC Handelsblad* (Pays-Bas), InfoLibre (Espagne), *Politiken*- (Danemark), *Expresso* (Portugal), *VG* (Norvège) et *Domani* (Italie) – tous membres du réseau EIC – ainsi que *Die Wochenzeitung* (Suisse), *Reporters United* (Grèce), *Shomrim* (Israël), Daraj Media (Liban) et *The Washington Post* (Etats-Unis). A.SE

Un logiciel espion vendu par des Français aux services vietnamiens a fini par être utilisé pour tenter d'infecter les téléphones d'officiels états-uniens, asiatiques, mais aussi européens. Entre février et juin 2023, plus de 50 personnalités et institutions ont été visées. Dont la présidente du Parlement de l'UE, Roberta Metsola.

ARTHUR SENTE (AVEC L'EIC ET AMNESTY INTERNATIONAL)

Sur le réseau social X (ex-Twitter), @Joseph_Gordon16 se présente sous l'allure innocente d'un jeune homme en train de se prendre en selfie dans un miroir. Ou il faudrait plutôt dire « se présentait ». Car depuis près de deux semaines, le profil a mystérieusement disparu de la plateforme.

Entre février et juin 2023, pourtant, et en utilisant toujours la même méthode, @Joseph_Gordon16 a ciblé plus de cinquante profils de personnalités et d'institutions sur les réseaux sociaux X et Facebook, en tentant de faire en sorte que leur propriétaire clique sur un lien infectieux, vecteur d'installation du redoutable logiciel espion Predator.

C'est ce que révèle aujourd'hui l'enquête « Predator Files », menée par quinze médias internationaux (dont *Le Soir*) sous la coordination de l'European Investigative Collaborations (EIC), grâce à l'analyse technique du Security Lab d'Amnesty International qui a notamment pu se reposer sur des documents confidentiels obtenus par Mediapart et *Der Spiegel*.

Amnesty International, qui a commencé à suivre de près les activités de @Joseph_Gordon16 en avril 2023, publie ce lundi un rapport circonstancié sur le sujet.

Il ressort des analyses de son service technique que les liens infectieux partagés par ce profil portent la marque claire du logiciel espion vendu par le consortium Intellexa (au cœur des révélations des « Predator FIles ») et capable de siphonner en temps réel toutes les données d'un smartphone tout en restant invisible pour son utilisateur.

Ses cibles, identifiées par l'ONG, étaient loin d'être choisies au hasard.

On retrouve parmi elles la présidente du Parlement européen, Roberta Metsola, la présidente de Taïwan, Tsai Ing-Wen, l'eurodéputé français Pierre Karleskind (du parti présidentiel français Renaissance et membre du groupe Renew au Parlement européen) ou encore Emily Haber, alors ambassadrice d'Allemagne auprès des Etats-Unis.

Le compte X de la Commission européenne de même que ceux de plusieurs institutions placées sous l'autorité de celle-ci ont également été visés. Tout comme trois sénateurs et un député états-uniens, dont le Démocrate Chris Murphy (président du sous-comité Moyen-Orient et Asie de la commission des affaires étrangères du Sénat) et le Républicain Michael McCaul (président de la commission des affaires étrangères de la Chambre des représentants).

Le mode opératoire du profil @Joseph_Gordon16 est le suivant : il s'attache à publier en « réponse » à un tweet de sa cible un lien renvoyant vers un site internet, dont l'URL imite souvent celui d'un média reconnu et légitime.

Le 1er juin 2023, il écrira ainsi sous une publication de Roberta Metsola : « Alors que de plus en plus de nations s'opposent à la Chine, à quel point le monde prend-il Pékin au sérieux ? », en joignant à cette question provocatrice un lien vers un site imitant celui du journal South China Morning Post, quotidien de référence à Hong Kong. Le même message sera envoyé en réponse sous une publication du compte X officiel de la Commission européenne.

La marque du Vietnam

Pour Amnesty, il y a certainement lieu de penser que ces tentatives d'infection portent la marque du Vietnam. Un régime communiste connu pour ne tolérer aucune opposition.

Pour l'ONG, en effet, le fait que certains des noms de domaines utilisés dans le cadre des attaques « ont été conçus pour imiter des sites web vietnamiens légitimes suggère un lien avec des acteurs liés au Vietnam, ce qui est étayé par des preuves significatives fondées sur une analyse du compte X de l'attaquant et des antécédents des cibles. »

Dans son rapport, Amnesty note ainsi que « le premier tweet du compte, en 2020, est rédigé en vietnamien ». Et ajoute qu'un compte visé par des tweets contenant des liens infectieux n'est autre que celui « de Thò'i Báo, un site d'information sur le Vietnam basé en Allemagne. »

Khoa Le Trung, activiste et journaliste vivant à Berlin, est le propriétaire de ce site critique du régime, visé par cette attaque menée le 9 février 2023. Contacté par l'EIC, il indique ne pas avoir cliqué sur le lien infectieux mais demeure très préoccupé. « Si le gouvernement vietnamien avait accès à mon téléphone et savait qui sont mes sources et mes employés, leurs vies seraient en danger », s'inquiète-t-il en précisant employer actuellement douze personnes signant leurs articles sous pseudonyme et avoir déjà fait l'objet de menaces liées à ses activités.

Ce n'est d'ailleurs pas le seul journaliste visé par @Joseph_Gordon16. Sur son tableau de chasse, on retrouve notamment le compte de CNN Philippines ainsi que trois journalistes de la chaîne d'information états-unienne, dont deux basés à Taïwan.

Le mobile ? Le sujet de la pêche

Que le régime vietnamien puisse vouloir cibler des journalistes établis en Asie ou des voix critiques basées à l'étranger paraît suivre une certaine logique. Mais pourquoi une telle énergie dépensée pour viser autant d'institutions et de personnalités européennes ? Une thèse soulevée par Amnesty International, étayée par de multiples éléments, est que ces tentatives d'espionnage trouvent leur origine dans des tensions qui opposent le régime vietnamien avec l'Union européenne au sujet de la pêche.

En effet, l'Union européenne a délivré en 2017 une « carte jaune » au Vietnam, estimant que le pays, dont la pêche est l'une des premières sources de revenus, ne luttait pas suffisamment contre l'exploitation illégale des ressources halieutiques.

Un avertissement qui représente l'ultime étape avant l'attribution d'une