SIMULATION STRATÉGIQUE : **ET SI INTERNET S'EFFONDRAIT ?**

DANS LE CADRE DE LA 3e ÉDITION DE L'ÉVÉNEMENT **CYBERDÉFENSE ET STRATÉGIE** DU 2 JUILLET 2019, UN EXERCICE DE SIMULATION DE CRISE SUR LE THÈME "ET SI INTERNET S'EFFONDRAIT" A PERMIS AUX PARTICIPANTS DE RÉFLÉCHIR COLLECTIVEMENT AUX MESURES À PRENDRE FACE À UNE ATTAQUE MASSIVE.

PRÉSENTATION DE L'EXERCICE :

DURÉE : ENVIRON 1H

DÉROULEMENT : 2 phases de jeu de 20 mn chacune, chacune lancée par un spot vidéo en format « JT ».

OBJECTIF : chaque groupe travaille de son côté sur les réponses à imaginer face à la crise. Un rapporteur est ensuite désigné au sein de chaque groupe pour présenter à l'ensemble des participant en quelques minutes les réponses qui ont été imaginées.

DÉROULÉ :

PHASE 1 :

Introduite par un spot TV dont l'objectif est de lancer la simulation, à un stade où peu d'information est encore disponible sur le détail des attaques

EXEMPLE : « Vous êtes le conseiller à la sécurité nationale. Le Premier ministre intervient ce soir au JT, vous êtes chargé de lui préparer des éléments de langage. »

JT de lancement de l'exercice. Interviews de Stéphane Bortzmeyer (AFNIC) et Nicolas Arpagian (Orange) par Julia Sieger.

VOICI LES QUESTIONS AUXQUELLES IL DEVRA RÉPONDRE :

- S'agit-il d'une guerre informatique ?
- Peut-on attribuer ces attaques ?
- Que fait le gouvernement lorsqu'une telle attaque survient ?
- Quels moyens de réponse pouvez-vous/comptez-vous mettre en œuvre ?
- Doit-on craindre que les particuliers soient touchés à leur tour ? Auquel cas que peuvent/doivent faire les particuliers et les entreprises pour se protéger et limiter les dégâts ?

PHASE 2 :

Introduite par un spot TV dont l'objectif est de montrer la progression de l'attaque et de permettre aux participants de travailler sur un plan de réaction face à une attaque qui touche maintenant le cœur du réseau Internet.

EXEMPLE : « Vous êtes toujours le conseiller à la sécurité nationale. Cette fois, le président de la République a décidé de réunir un conseil de défense. Vous êtes chargé de lui préparer un ordre du jour détaillé listant toutes les questions à aborder et proposant pour chacune quelques orientations clés. »

2e émission TV animée par Julia Sieger autour d'Alix Desforges (Institut Français de Géopolitique) et Grégoire Germain (Harfang Lab).

PARMI LES POINTS À ABORDER :

- L'évaluation des impacts de l'attaque ;
- Les mesures de réaction à engager pour limiter ces impacts ;
- La communication à l'égard des citoyens ;
- La coopération internationale etc.

SIMULATION STRATÉGIQUE : SCÉNARIO DE CRISE

CONTEXTE

15 OCTOBRE 2024 :
Suite aux ravages d'un typhon sur les infrastructures de son voisin insulaire Cataracte, la Sabanie décide d'envoyer une mission militaire de 10 000 hommes pour assister les autorités de Cataracte.

25 OCTOBRE 2024 :
Suite à une montée des tensions, la France prend position contre ce qui semble être une invasion de Cataracte par la Sabanie.

DÉCEMBRE 2024 :
Un groupe de hackers dénommé CosyRooster (plus connu sous le nom de code APT144) est secrètement financé par la Sabanie pour orchestrer une cyber-attaque contre la France.

LE GROUPE COSYROOSTER

Le groupe CosyRooster a plusieurs faits d'armes à son actif : employé par différents groupes ou pays, ces cyberattaquants se comportent en mercenaires. D'obédience anarcho libertaires, le groupe a effectué plusieurs opérations de décrédibilisation de symboles étatiques, comme l'arrêt partiel des transports en Kratovie par le biais du ransomware B4kounin3, pour protester contre le contrôle croissant de la population par le gouvernement kratovien.

Leurs *Tactics, Techniques and Procedures (TTP)* ont été reconnues dans plusieurs attaques de types DDoS, APT, création et diffusion de malwares. La Sabanie décide de faire appel à nouveau à ce groupe en raison de ses compétences et sa réputation.

PROGRESSION DE L'ATTAQUE

2024

OCTOBRE

NOVEMBRE

DÉCEMBRE

DÉCEMBRE 2024 : (DIVERSION)
Tentatives d'exploitation de vulnérabilités récentes sur des OS Windsoft 12 de PME françaises.

FÉVRIER 2025 :
Tentatives de pénétration sur les serveurs frontaux des principaux FAI, Kiwi et Liberté.

FÉVRIER 2025 : (ENFOUISSEMENT)
- CosyRooster Découvre une vulnérabilité de type 0day sur le protocole RDP de Windsoft, qui permet une exécution de code à distance sans interaction de l'utilisateur.
- CosyRooster Installe le programme malveillant R4V4CH0L (type « bombe logique ») sur toutes les machines exposées à la faille 0day.

1ER MARS 2025 : (MISE À FEU)
- CosyRooster active R4V4CH0L contre des Opérateurs d'Importance Vitale (OIV) et des ministères ;
- 1er message de revendication.

6 MARS 2025 : (AMPLIFICATION)
- CosyRooster réalise un hijack BGP qui provoque une panne totale des AS pivots de deux FAI français.
- Nouveau message de revendication.

10 MARS 2025 :
- CosyRooster lance une campagne de phishing par RCS (Rich Communication Services) sur les Android et Iphone.
- Nouveau message de revendication.

2025

JANVIER

FÉVRIER

MARS

AVRIL

MAI

RÉPONSE

20 DÉCEMBRE 2024 :
- L'Agence de sécurité nationale appelle les entreprises à la vigilance et les encourage à effectuer toutes les mises à jour sur leurs SI.
- Windsoft patch les exploits.

1ER MARS 2025 :
- Déploiement sur site des experts Windsoft et des équipes de l'Agence de sécurité nationale
- Mobilisation de la réserve opérationnelle cyber

2 MARS 2025 : Le Président de la République s'exprime à la télévision et présente le plan d'action du gouvernement. (cf script et spots).

4 MARS 2025 : Waltersky Lab identifie des marqueurs techniques similaires à ceux utilisés lors d'attaques menées par CosyRooster pour le compte de la Sabanie.

5 MARS 2025 : Les Opérateurs d'Importance Vitale (OIV) tentent de fonctionner en mode dégradé et sur des systèmes alternatifs.

IMPACT

1ER MARS 2025 : Des données sensibles sont perdues, des programmes de recherches disparaissent, les banques bloquent l'intégralité des transactions. Les cours en bourse de plusieurs entreprises du CAC 40 s'effondrent.

6 MARS 2025 : perte de connectivité à l'Internet pour les AS français . Les réseaux de communication sont fortement perturbés.

10 MARS 2025 : Les appareils sont désormais contrôlés et enrôlés sur les serveurs C & C de CosyRooster.