Quand la manifestation cache une intrusion

Kehl, frontière franco-allemande. Une manifestation pacifique devant Galvaris Armor Systems…Quand la foule fait écran pour laisser place à un sabotage.

Le Voyage d’une menace

Épisode 8

Semkel
RISK & THREAT INTELLIGENCE

GAS

Galvaris Armor Systems (GAS) est un acteur central du secteur de la défense. Il fournit la quasi-totalité des industriels spécialisés dans les véhicules militaires. Sa spécialité : les châssis blindés, entre autres.

Compte tenu du réarmement européen, son usine principale en Allemagne, à la frontière avec la France, ne chôme pas et suit des cadences infernales imposées par ses clients.

LA COALITION

Un groupe d'activistes antiguerre, **No Army No Blood (NANB)**, entend enrayer « cette marche vers la mort », comme il le clame dans ses manifestes. Pour atteindre son objectif, le mouvement cherche des alliances pour décupler sa capacité d'action.

Il rencontre **Peace Patriot Network (PPN)**, des cyberactivistes qui se revendiquent « pour la paix ».

Les deux groupes veulent mutualiser leurs ressources pour démontrer leur détermination aux autorités et aux industriels.

LA PRÉPARATION

PPN et NANB décident de cibler l'un des sites industriels majeurs de l'armement en Europe : l'usine de **GAS** à Kehl (Allemagne). Leur idée : combiner action physique et action numérique.

PPN analyse le versant numérique : recherche des failles des infrastructures, ingénierie sociale sur le personnel et la direction, etc. En quelques semaines, ils élaborent une cartographie des vulnérabilités humaines et numériques.

De son côté, **NANB** repère les lieux et établit un plan pour manifester au plus près de l'usine.

LE PLAN

Volet cyber (PPN) :

- Exploitation des vulnérabilités du système de vidéosurveillance pour aveugler la sécurité.
- Déverrouillage de la première grille via la compromission du système de contrôle.

Volet terrain (NANB) :

- Rassemblement d'autres associations amies via les forums privés Telegram.
- Logistique dédiée (bus, voitures, vélos) pour parvenir rapidement devant le site et éviter d'être bloqués si les forces de l'ordre sont présentes.

JOUR J

En moins d’une heure, 500 personnes se massent devant les grilles de l’usine.

Arrivés en nombre et répartis autour de Kehl, les manifestants se présentent en ordre dispersé mais efficace : bus loués, vélos, voitures… Aucune autorité n’est sur place ; l’information ne semble pas avoir fuité.

Le service de sécurité tente de joindre les autorités : **les communications sont fortement perturbées (fixe et mobile).**

+30 MINUTES

La manifestation change de nature lorsque la première grille s’ouvre, sous les yeux ébahis des gardes.

La direction ordonne l’évacuation du site et concentre les agents de sécurité à l’intérieur pour protéger le personnel.

C’est la panique chez les agents de sécurité et le personnel car de nombreux manifestants sont en train d’escalader la deuxième grille.

H+2

Les forces de l’ordre arrivent une heure après le début de la manifestation. Les communications restent dégradées.

Des bus sont positionnés de manière à entraver leur progression vers la foule.

À 14 h, un départ de feu est constaté dans le bâtiment principal, celui de la plus grande ligne de production.

Les forces de l’ordre et les agents de sécurité sont débordés.

CONSÉQUENCES

Un blessé grave parmi le personnel lors de l’incendie, et des blessés légers lors de l’évacuation des manifestants.

Le principal bâtiment est fortement endommagé. L’usine restera paralysée de nombreux mois, c’est toute une chaîne d’approvisionnement de la défense européenne qui se retrouve à l’arrêt.

LES FAITS

Peace Patriot Network (PPN) n'est pas forcément antiguerre ; le collectif choisit ses combats. En tant que cyberactivistes, ils semblent agir pour la paix mais la plupart du temps ils sont en mission commandée pour une des 2 belligérants.

PPN est composée d'hackers mercenaires qui souhaitent avant tout faire fructifier leur savoir-faire. **Et en son sein, d'anciens officiers du GRU (renseignement militaire russe).**

Ces derniers vont ainsi décider d'organiser une opération d'intrusion et de sabotage au moment de la manifestation.

Leur plan fonctionne parfaitement : alors que la sécurité repousse les premiers manifestants ayant franchi la première grille, un individu, portant le même uniforme que les agents de sécurité, pénètre le corridor sans heurt. Il suit d'autres agents chargés d'organiser l'évacuation.

Il parvient à pénétrer dans le bâtiment principal et il a tout son temps pour provoquer un court-circuit généralisé qui endommagera la plupart des machines et provoquera l'incendie détruisant une partie du bâtiment.

L'opération a-t-elle été orchestrée par la Russie à travers PPN ? S'agit-il de l'initiative de quelques patriotes ? Certains chez No Army No Blood étaient-ils au courant ? Peu importe : le mal est fait.

COMMENT GAS AURAIT PU ÉVITER OU ATTÉNUER LA MENACE

Galvaris Armor Systems est un modèle industriel : machines-outils de pointe et processus robustes. Mais sa sûreté n'est pas suffisamment robuste et à jour face aux nouvelles menaces numériques et à des modes d'action plus pernicieux. En complément d'un renforcement de sa gouvernance sûreté et de son dispositif de sécurité physique, **GAS** aurait dû notamment :

1 Surveiller l'ensemble de ses infrastructures

L'attaque est rendue possible par des vulnérabilités d'équipements installés et gérés par le prestataire de sécurité. Ces équipements auraient dû entrer dans le périmètre de supervision de son équipe cyber. La présence d'équipes SOC et CTI est indispensable pour suivre les événements (mineurs/majeurs) et les vulnérabilités susceptibles d'entraîner des dommages critiques.

2 Ne pas négliger la surveillance du cyberespace

L'activisme se joue dans le monde physique mais également numérique. La veille du cyberespace (sites, blogs, réseaux sociaux, forums...) doit faire partie du continuum de sûreté pour anticiper et détecter les préparatifs de manifestation, les campagnes de dénigrement, les fuites d'informations...

Semkel
RISK & THREAT INTELLIGENCE

Avec SEMKEL, GAS aurait été protégée et conseillée :

Veille du cyberspace (clear, deep et dark web) dans un double objectif : anticiper vos risques cyber (vulnérabilités, fuite de données, vol d'identifiants...) et détecter les menaces contre votre sûreté (criminels, activisme, fraude...).

Experts en intelligence du risque et de la menace, nous proposons un accompagnement sur les 3 champs d'actions des menaces hybrides : économique, informationnel et cyber.

“ NE SUBISSEZ PLUS, ANTICIPEZ ”
Julien Lopizzo PDG de Semkel

Investigations et surveillance 24/7 de vos risques et menaces

Informations sur
semkel.com ou au +33 (0) 4 78 51 13 79