Semkel
RISK & THREAT INTELLIGENCE

LE VOYAGE D'UNE MENACE

Épisode 3

Quand une fuite de données impacte votre sécurité physique

ALPHAWORLD

FABRICANT D’ÉQUIPEMENTS HIGH-TECH

DEPUIS 2015

ENTREPRISE SPÉCIALISÉE DANS LA PRODUCTION D’ÉQUIPEMENTS ÉLECTRONIQUES SENSIBLES (COMPOSANTS DE DRONES, SYSTÈME DOMOTIQUE...) DONT LA RÉPUTATION GRANDIT À L’INTERNATIONAL GRÂCE À LEUR FIABILITÉ ET LEUR INNOVATION.

ILS DOIVENT RESPECTER DES EXIGENCES DRASTIQUES DE PRODUCTION.

ILS SONT SUR LE POINT DE DÉCROCHER UN GRAND CONTRAT DANS LE SECTEUR DE LA DÉFENSE. LES ÉQUIPES SONT SOUS PRESSION.

HUGO

DIRECTEUR DE L'USINE DÉDIÉE À LA DÉFENSE

DEPUIS 2019

HUGO EST UN DIRECTEUR AMBITIEUX, SOUCIEUX DE LA PRODUCTION. EXPERT DE L'INDUSTRIE, IL ADOPTE UN RYTHME SOUTENU DE PRODUCTION.

AFIN DE GARANTIR LE PLUS DE FLUIDITÉ ET DE SOUPLESSE POSSIBLE POUR LA COLLABORATION AVEC LES SOUS-TRAITANTS, IL A OPTÉ POUR UN SYSTÈME DE PARTAGE DE FICHIERS GRAND PUBLIC.

IL UTILISE AINSI UN SERVICE DE STOCKAGE NON HABILITÉ, SANS CHIFFRAGE, POUR PARTAGER DES DOCUMENTS AVEC SES FOURNISSEURS. IL N'EN MESURE PAS LES RISQUES.

LA FUITE

UN ACCÈS DIRECTEMENT AUX DOCUMENTS

DEPUIS 3 SEMAINES

PLUSIEURS FICHIERS SE RETROUVENT INDEXÉS PAR UN MOTEUR SPÉCIALISÉ DANS LES BRÈCHES DE DONNÉES. LE SYSTÈME DE PARTAGE UTILISÉ PAR HUGO N'ÉTAIT PAS CONFIGURÉ CORRECTEMENT.

BEAUCOUP DE DOCUMENTS CONFIDENTIELS SONT ACCESSIBLES.

LE FICHIER "ARCHITECTURAL SECURITY.PDF" CONTENANT LES PLANS DE SÉCURITÉ DE L'USINE, SONT EN LIBRE ACCÈS AINSI QUE D'AUTRES DOCUMENTS PERMETTANT DE MIEUX COMPRENDRE LE RÔLE DU SITE GÉRÉ PAR HUGO.

BRIGADE RED HAWK

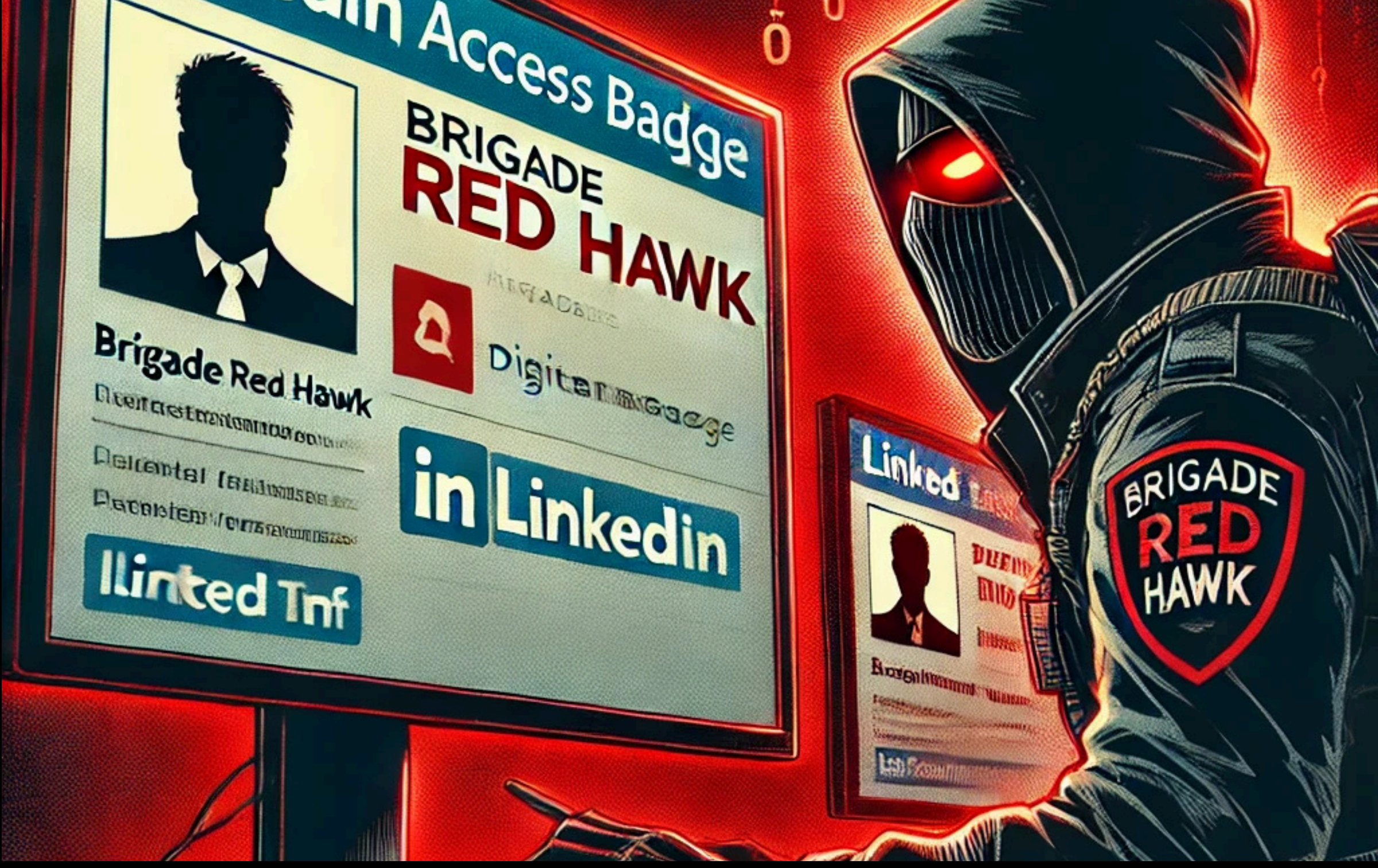
GROUPUSCULE ACTIVISTE

DEPUIS 2018

LES MEMBRES DES RED HAWK S'OPPOSENT À TOUS LES INTÉRÊTS LIÉS À LA DÉFENSE. ILS CHERCHENT TOUS LES MOYENS POUR DÉNONCER ET SABOTER LES PROJETS MILITAIRES.

ILS EXPLOITENT TOUTES LES MÉTHODES POSSIBLES : HACKING, SABOTAGE PHYSIQUE, PRESSION MÉDIATIQUE...

UNE DES BRIGADES DES RED HAWK DÉCOUVRE LES DOCUMENTS CONFIDENTIELS DE ALPHAWORLD. ILS DÉCOUVRENT QUE CETTE SOCIÉTÉ EST SUR LE POINT DE LANCER UN NOUVEAU DRONE D'INFILTRATION EN TERRAIN HOSTILE.
ILS DÉCIDENT D'AGIR.



PRÉPARATION

DU VIRTUEL AU RÉEL

EN 2 SEMAINES

RED HAWK DÉCOUVRE LES PLANS DE SÉCURITÉ AINSI QUE LA GESTION DES CONTRÔLES D'ACCÈS.

UN QR CODE DANS UN DOCUMENT PERMET AUX FOURNISSEURS DE DEMANDER L'ACCÈS À UN BADGE VIA UN EXTRANET.

LA BRIGADE SÉLECTIONNE UN FOURNISSEUR ET USURPE L'IDENTITÉ DE 2 DE LEURS COLLABORATEURS TROUVÉS SUR LINKEDIN.
ILS COMMUNIQUENT PAR MAIL AVEC ALPHAWORLD ET OBTIENNENT 2 BADGES D'ACCÈS VIA LA PLATEFORME.

INFILTRATION

UN LUNDI MATIN TOUT BASCULE

3 MAI

RED HAWK PASSE À L'ACTION. SOUS PRÉTEXTE D'UNE MAINTENANCE, 2 PERSONNES DE LA BRIGADE UTILISENT DES BADGES AUTHENTIQUES SOUS DE FAUSSES IDENTITÉS POUR PÉNÉTRER DANS L'USINE.

AUCUN PROBLÈME AU POINT DE SÉCURITÉ.

GRÂCE AUX DIFFÉRENTS DOCUMENTS, ILS SAVENT OÙ ALLER ET QUOI CHERCHER:

- **ILS SABOTENT LES RÉGLAGES DE L'ALIMENTATION DES MACHINES-OUTILS, DES CLIMS ET DU CENTRE SERVEUR**
- **ILS DÉROBENT UN PROTOTYPE DE DRONE.**

CONSÉQUENCES

UNE USINE À L’ARRÊT ET UN GROUPE EN DIFFICULTÉ

DÈS LE 4 MAI

DÈS LE LENDEMAIN : L’USINE EST EN STAND-BY COMPTE TENU DES DÉGÂTS. AU 20H, RED HAWK REVENDIQUE LE SABOTAGE ET LE VOL DU DRONE.

L’ENSEMBLE DES SITES D’ALPHAWORLD SONT À L’ARRÊT EN ATTENDANT DE COMPRENDRE COMMENT L’INFILTRATION S’EST DÉROULÉE. LE CONSEIL D’ADMINISTRATION SE RÉUNIT POUR ÉTABLIR UN PLAN DE GESTION DE CRISE.

CONSÉQUENCES :

- **PERTE DE CONFIANCE DU CLIENT POTENTIEL**
- **DES ÉQUIPES ÉBRANLÉES PAR LA SITUATION**
- **REMISE EN QUESTION DES PERSPECTIVES FINANCIÈRES GLOBALES**
- **L’INCIDENT D’ALPHAWORLD EST COUVERT PAR TOUS LES MÉDIAS**

QU’AURAIT DÛ FAIRE ALPHAWORLD AVANT L’ATTAQUE

- CARTOGRAPHIER LES OUTILS UTILISÉS PAR L’ENSEMBLE DES COLLABORATEURS
- ADOPTER UNE PLATEFORME SÉCURISÉE D’ÉCHANGE
- SENSIBILISER LE PERSONNEL ET LA DIRECTION AUX ENJEUX DE SÛRETÉ NUMÉRIQUE
- METTRE EN PLACE UNE POLITIQUE GLOBALE DE SÛRETÉ AVEC DE LA SURVEILLANCE CONTINUE ET DES AUDITS RÉGULIERS

Semkel
RISK & THREAT INTELLIGENCE

Avec SEMKEL, Alphaworld aurait été protégée et conseillée :

- Surveillance des menaces externes :
  - Détection des brèches et des fuites des données
  - Surveillance du darkweb et du deep web
  - Identifications des menaces
- Accompagnement et conseil sur la posture de sûreté
  - Contrôle des accès
  - Sensibilisation du personnel
- Mise en place d’un plan d’actions en cas de menaces identifiées

Surveillance 24/7 de vos risques et menaces

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