Semkel
RISK & THREAT INTELLIGENCE

LE VOYAGE D'UNE MENACE

Épisode 4

Quand un fournisseur compromet votre entreprise

NEOFORMAX

LEADER EUROPÉEN DE LA BIOTECH

DEPUIS 2005

NEOFORMAX PRÉPARE LE LANCEMENT DE SA NOUVELLE GÉNÉRATION DE VACCINS. L'ENTREPRISE VA SIGNER AVEC L'OMS UN GROS CONTRAT DE DÉPLOIEMENT POUR SON VACCIN ANTI-PALUDIQUE.

POUR AMÉLIORER LEUR PRODUCTION, LES ÉQUIPES ONT SÉLECTIONNÉ UN NOUVEAU FOURNISSEUR D'ERP.

ELLES ONT SIGNÉ RÉCEMMENT UN CONTRAT AVEC DYNATRIB POUR LEUR APPLICATION DE SUIVI DE BOUT EN BOUT : DE LA PRODUCTION À LA LIVRAISON.

DYNATRIB

UN RECRUTEMENT PAS COMME LES AUTRES

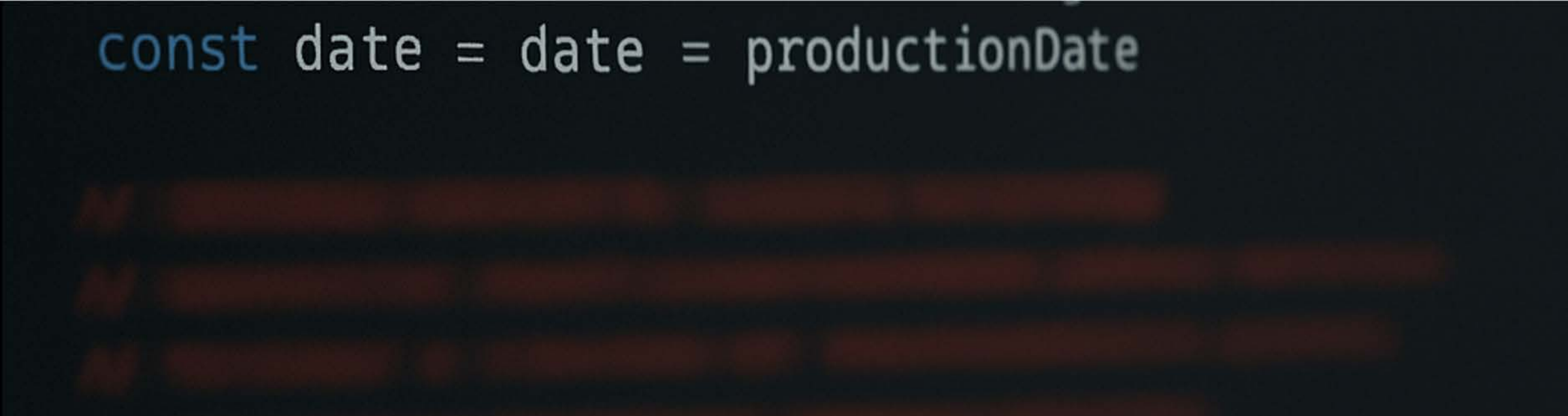
DEPUIS 2020

DYNATRIB EST UNE LICORNE INDIENNE. ELLE A RÉVOLUTIONNÉ LES ERP POUR LE MONDE DE LA PHARMA. SA NOUVELLE APPLICATION PHARE GÈRE LE TRACKING DE PRODUCTION JUSQU'À LA LIVRAISON TOUT EN FLUIDIFIANT LES PARCOURS ADMINISTRATIFS.

DANS CETTE PHASE D'ACCÉLÉRATION DYNATRIB A RECRUTÉ UN NOUVEL ARCHITECTE LOGICIEL.

AAKASH SHARMA A UN CV IDÉAL POUR PRENDRE LE LEAD SUR LE PROJET.

SEULEMENT, IL A ÉTÉ PLACÉ PAR UN GROUPE CYBERCRIMINEL, BLACKCRADLE, SPÉCIALISÉ DANS LE VOL DE PROPRIÉTÉ INTELLECTUELLE.



AAKASH

LA LIGNE DE TROP

3 MOIS PLUS TARD

LE NOUVEL ARCHITECTE LOGICIEL INTÈGRE VOLONTAIREMENT DES FAILLES LOGICIELLES DISCRÈTES (BACKDOORS).

UNE FOIS L'APP MISE À JOUR ET DÉPLOYÉE CHEZ LES CLIENTS, ELLE VA CRÉER UN CANAL D'EXFILTRATION DE DONNÉES VERS BLACKCRADLE.

BLACKCRADLE AVAIT RÉPÉRÉ LES CLIENTS DE DYNATRIB GRÂCE À UNE FUITE DE DONNÉE ET PLUS PARTICULIÈREMENT NEOFORMAX.

GRÂCE AUX BACKDOORS, LES HACKERS S'INFILTRENT DANS LE SYSTÈME ET RÉCUPÈRENT LES DONNÉES CONFIDENTIELLES DE FABRICATION.

LA PANIQUE

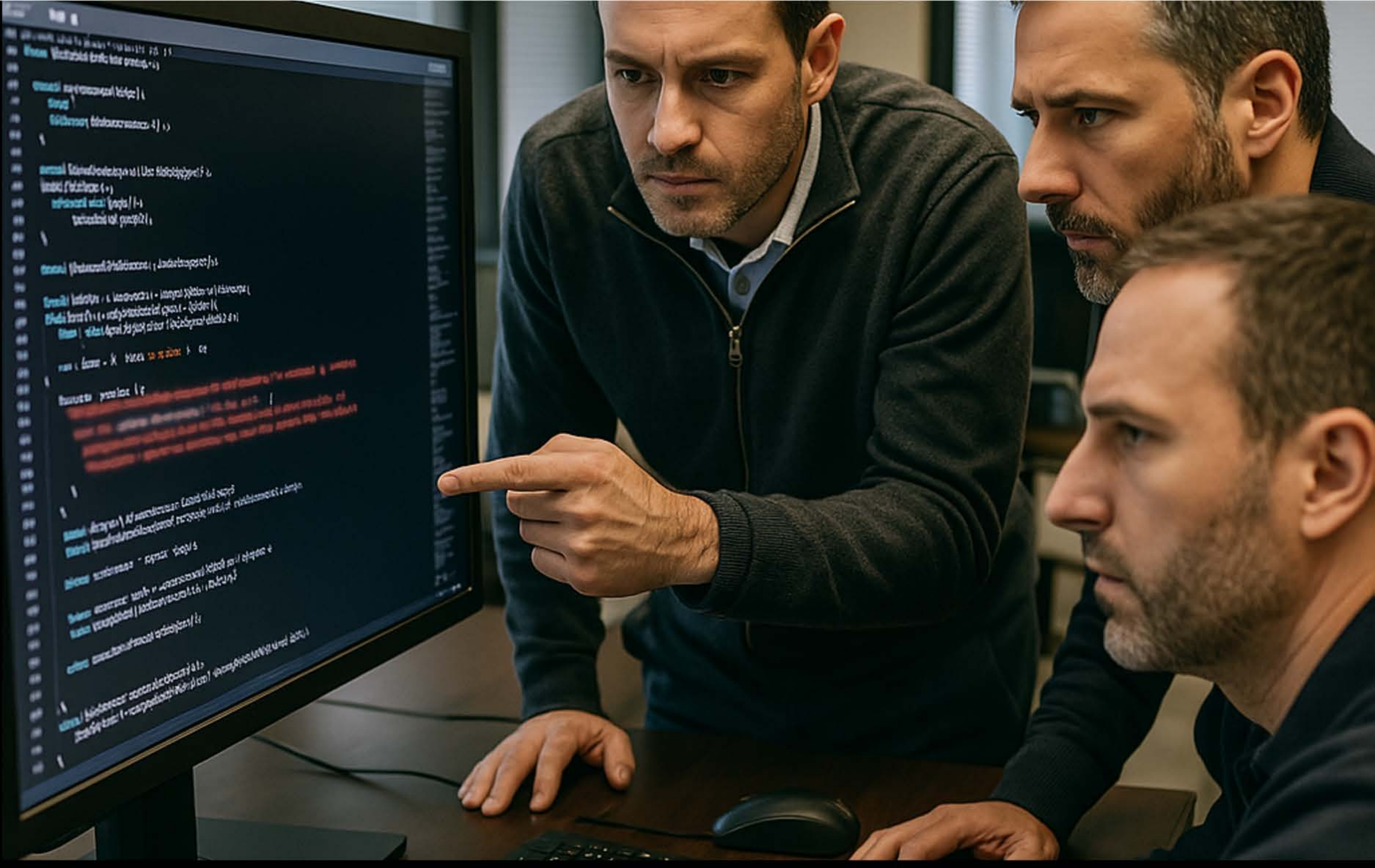
BLACKCRADLE DÉCIDE DE TOUT CASSER PENDANT 3 SEMAINES

APRÈS LEUR PASSAGE ET LA RÉCUPÉRATION DES DONNÉES, LES CYBERCRIMINELS DÉCIDENT DE COUVRIR LEUR TRACE EN SABOTANT LA PRODUCTION.

UN MATIN, TOUTE L'ACTIVITÉ S'ARRÊTE

NEOFORMAX DÉCLENCHE UNE CELLULE DE CRISE. L'OMS SUSPEND LE CONTRAT FAUTE D'AVOIR PU RÉALISER LA VISITE DE CONFORMITÉ.

EN EFFET L'ENSEMBLE DU SITE DE PRODUCTION EST OUT. PLUS DE DONNÉES ET PLUS AUCUN APPAREIL NE FONCTIONNE.



L’ENQUÊTE

REMONTÉE VERS LA SOURCE

PENDANT 1 MOIS

LES EXPERTS MANDATÉS MÈNENT L’ENQUÊTE. ILS ARRIVENT D’ABORD À RELANCER L’ENSEMBLE DU SYSTÈME EN 15 JOURS GRÂCE À DE NOUVEAUX OUTILS DE PRODUCTION COMMANDÉS ET DES SAUVEGARDES NON COMPROMISES.

MAINTENANT RESTE À SAVOIR CE QU’IL S’EST PASSÉ.

APRÈS AVOIR RÉCUPÉRÉ DES LOGS RÉSEAUX INTERNES OUBLIÉS PAR LES HACKERS, ILS DÉCOUVRENT DES FLUX DE DONNÉES ÉTRANGES QUI SEMBLENT REMONTER VERS DYNATRIB.

ILS SONT DÉPÊCHÉS SUR PLACE.

DYNATRIB

LE MAILLON INVISIBLE

DYNATRIB REFUSE AU DÉPART DE CROIRE À SA RESPONSABILITÉ.

LES EXPERTS DE NEOFORMAX ONT L'AUTORISATION D'ENQUÊTER ET REMONTENT JUSQU'À LA BACKDOOR DANS LES SERVEURS DE DYNATRIB.

ILS DÉCOUVRENT ALORS QUE L'APPLICATION PHARE EST COMPROMISE.

1 SEMAINE PLUS TARD

GRÂCE À DES RECHERCHES APPROFONDIES, LES DÉVELOPPEURS DE DYNATRIB REMONTENT LE FIL DES MISES À JOUR ET RÉVÈLENT LES BACKDOORS MISES PAR AARASH.

L'ARCHITECTE LOGICIEL A DISPARU ENTRE TEMPS.

LE PROCÈS DÉMARRE

CONSÉQUENCES

NEOFORMAX ET DYNATRIB EN DIFFICULTÉ

12 MOIS

NEOFORMAX PREND DU RETARD SUR SON PROGRAMME DE NOUVEAUX VACCINS. L'OMS S'IMPATIENTE ET LE COURS DE BOURSE DE LA BIOTECH A ÉTÉ DIVISÉ PAR 2 EN 3 MOIS.

DYNATRIB VOIT SA RÉPUTATION ENTÂCHÉE ET PERD DE NOMBREUX CLIENTS.

LEUR FUTURE RELATION SERA AU TRIBUNAL.

CONSÉQUENCES :

- **LES SECRETS DE FABRICATION ONT ÉTÉ VOLÉS.**
- **PERTE DE CHIFFRE D'AFFAIRES À CAUSE DE L'INACTIVITÉ ET DU DÉPART DES CLIENTS.**
- **RÉPUTATION ENTACHÉE.**
- **RISQUES SYSTÉMIQUES : D'AUTRES CLIENTS ONT PEUT-ÊTRE ÉTÉ INFECTÉS.**

QU’AURAIT DÛ FAIRE DYNATRIB AVANT L’ATTAQUE

- FAIRE DES BACKGROUND CHECKS SUR LE RECRUTEMENT DE COLLABORATEURS CLÉS.
- METTRE EN PLACE UNE SURVEILLANCE PROACTIVE DE SA SURFACE D’ATTAQUE ET DE SON EMPREINTE NUMÉRIQUE (CLEAR / DEEP / DARKWEB).
- METTRE EN PLACE UNE ANALYSE RÉGULIÈRE DU CODE SOURCE DE SES APPLICATIONS PAR UNE TIERCE PARTIE.

QU'AURAIT DÛ FAIRE NEOFORMAX AVANT L'ATTAQUE

- CARTOGRAPHIER LES LOGICIELS ET LES INTERCONNEXIONS DE DONNÉES AVEC L'EXTÉRIEUR.
- METTRE EN PLACE UNE SURVEILLANCE PROACTIVE DE SES FOURNISSEURS CRITIQUES (CLEAR / DEEP / DARK WEB, FUITE DE DONNÉES, VULNÉRABILITÉS...).
- DEMANDER UNE CERTIFICATION DE SÉCURITÉ POUR LES APPLICATIONS TIERCES CRITIQUES.

Semkel
RISK & THREAT INTELLIGENCE

Avec SEMKEL, Neoformax & Dynatrib auraient été protégées et conseillées :

- 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
  - Background check.
  - 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