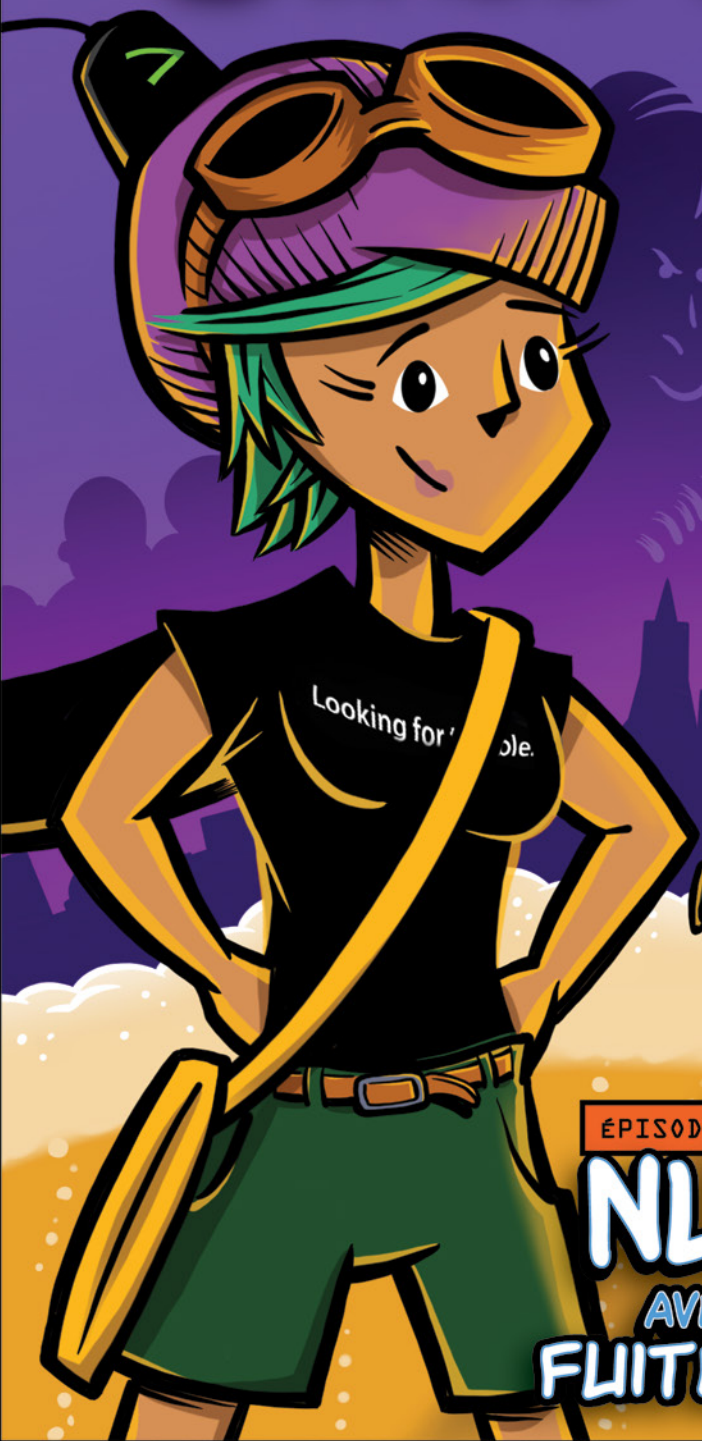


LES NOUVELLES AVENTURES D'UNE BRASSERIE ARTISANALE AUX GRANDES AMBITIONS

DE L'AUTRE CÔTÉ DE LA GLASS TABLE



ÉPISODE 2 :

NUAGEUX

AVEC RISQUE DE
FUITE DE DONNÉES



GRACE HOPPY

PDG DE FROTHLY

CETTE PASSIONNÉE A ENTIÈREMENT BÂTI LA BRASSERIE FROTHLY EN VERSANT DES PINTES DE SUEUR ET DE LARMES.



ALICE BLUEBIRD

ANALYSTE SOC

ANALYSTE ORIGINALE ET ATYPIQUE, ANCIENNEMENT CONSULTANTE POUR SWAN DAS ENTERPRISES. ELLE SAUVE LA MISE DANS L'ÉPISODE 1. ACTUELLEMENT EN CONGÉ SABBATIQUE DANS UN LIEU INCONNU.

DANS LE DERNIER ÉPISODE, FROTHLY, UNE BRASSERIE DE SAN FRANCISCO EN PLEINE CROISSANCE, DÉCOUVRIT QUE SES SYSTÈMES DE SÉCURITÉ ÉTAIENT PIRATÉS PAR UN GROUPE HOSTILE BAPTISÉ TAP'T. LE FBI AVAIT CONTACTÉ FROTHLY POUR LES AVERTIR DES AGISSEMENTS DE CETTE BANDE ORGANISÉE SOUTENUE PAR UN ÉTAT ÉTRANGER, QUI S'ÉTAIT INTRODUIT DANS LE RÉSEAU DE FROTHLY POUR EN EXFILTRER DES DONNÉES SENSIBLES. À CE MOMENT-LÀ, GRACE HOPPY, PDG DE FROTHLY, A COMPRIS QU'ELLE DEVAIT PRENDRE LES CHOSES EN MAIN.

ELLE A CONTACTÉ UN VIEIL AMI CHEZ SWAN DAS ENTERPRISES QUI LUI A RECOMMANDÉ DE FAIRE APPEL À ALICE BLUEBIRD, UNE CONSULTANTE EN SÉCURITÉ HORS PAIR, POUR OBTENIR DE L'AIDE -- CE QU'ELLE A FAIT. ALICE BLUEBIRD A MENÉ SON ENQUÊTE AVEC BRIO -- ET AVEC L'AIDE DE SPLUNK. ELLE A PRIS LE DESSUS SUR TAP'T ET SAUVÉ LA BRASSERIE.



BUD STOLL

RESPONSABLE INFORMATIQUE

REMPLACE KEVIN. BUD EST UN FAN DU CLOUD ET IL EST DÉTERMINÉ À MIGRER TOUTS LES SERVEURS LOCAUX VERS AWS ET AZURE.



MALLORY KRAUSEN

DIRECTRICE MARKETING

AUTONOME ET DÉGOURDIE, CETTE NÉOPHYTE DE LA BIÈRE ADMINISTRE LA BOUTIQUE EN LIGNE DE FROTHLY ET S'OCCUPE DES KITS DE BRASSAGE MAISON.



JACOB SMYTHE

CONSULTANT

IMPLIQUÉ DANS PLUSIEURS ENTRETIENS D'EMBAUCHE LORS DE LA RECHERCHE D'UN REMPLAÇANT POUR KEVIN.

Acte 1

BASE DE TAP'T (Taedonggang APT)

LIEU : INCONNU

HIER

"What the hell is cloud computing?"

—Larry Ellison



ÉPISODE 2 :

NUAGEUX AVEC RISQUE DE FUITE DE DONNÉES

SIÈGE DE FROTHLY

SAN FRANCISCO, CA

6 MOIS PLUS TÔT

KEVIN, COMME TU LE SAIS, L'ANNÉE DERNIÈRE A ÉTÉ DURE POUR FROTHLY. NOUS DEVONS PRENDRE UN NOUVEAU DÉPART.

TU AS L'AIR SURPRIS...

CE N'ÉTAIT PAS SI GRAVE QUE ÇA, SI ?

AS-TU OUBLIÉ TOUT CE QUI S'EST PASSÉ ?

OUI, C'EST VRAI... J'AURAIS PEUT-ÊTRE DÛ PASSER PLUS DE TEMPS À CORRIGER LES FAILLES DES SYSTÈMES

AU LIEU DE SUIVRE LA VALEUR EN BOURSE DE MES ACTIONS...

5 MOIS PLUS TÔT

GRACE fait appel à JACOB SMYTHE consultant Splunk, pour faire passer des entretiens à des informaticiens.

JACOB, NOUS SOMMES SÛRS QUE VOUS ALLEZ NOUS TROUVER UN LEADER IT D'EXCEPTION, CAPABLE DE MODERNISER NOS OPÉRATIONS ET DE GARANTIR NOTRE SÉCURITÉ.

SUR LE COUP.

PLUS TARD...

SI VOUS AVIEZ LE POSTE, QUE FÉRIEZ-VOUS DANS L'ENTREPRISE ?

JE NE VOUS LAISSERAI PAS FAIRE LA MÊME ERREUR QUE LA PIZZERIA, LE CAFÉ ET MÊME, DANS MA JEUNESSE, LE MCDO DE MON QUARTIER, QUI NE M'ONT PAS EMBAUCHÉ.

PLUS TARD...

PARLEZ-MOI UN PEU DE VOUS.

HMM... JE NE TRAVAILLE PAS AVANT MIDI. ET J'ARRÊTE À 14H.

FINALEMENT...

BUD STOLL fait son entrée. Bud s'est préparé ça se voit. Il porte un costume. Il a apporté des exemplaires de son C.V. et un dossier intitulé « Mon plan pour migrer Frothly dans le cloud. »

BUD STOLL

Il est différent
des autres candidats.
Il est compétent.
Il n'est pas un cliché.

QUELLE EST
LA PREMIÈRE CHOSE
QUE VOUS FERIEZ
SI VOUS AVIEZ
LE POSTE ?

JE MIGRERAI
FROTHLY VERS
LE CLOUD...

ET DISSIPERAI
TOUTES VOS CRAINTES
AU SUJET DE LA
TRANSFORMATION
NUMÉRIQUE !

IL A TOUT
COMPRIS, ET IL
A VRAIMENT LA
TREMPE D'UN DIRECTEUR
INFORMATIQUE...

QUAND
POUVEZ-VOUS
COMMENCER ?!

ET C'EST AINSI QUE...

SALLE DE PAUSE DE FROTHLY

Welcome to
Frothly,
Bud!

JE VOUS
PRÉSENTE NOTRE
NOUVEAU
RESPONSABLE IT..
**BUD
STOLL.**

IL NOUS REJOINT
AU TERME D'UNE
LONGUE
RECHERCHE.

IL EST LÀ POUR NOUS
PRÉPARER À UNE
CROISSANCE RAPIDE.
IL VA COMMENCER
PAR MIGRER NOTRE
INFRASTRUCTURE IT
DANS LE CLOUD.

BASE DE TAP'T

4 MOIS PLUS TÔT

C'EST TRÈS
CALME, CHEZ FROTHLY.
ILS ONT UN PETIT GÉNIE
DE LA SÉCURITÉ MAIS
NOUS AVONS FAIT QUELQUES
TESTS ET J'AI L'IMPRESSION
QUE PERSONNE NE
SUPERVISE PROACTIVEMENT
LES SYSTÈMES
CES TEMPS-LÀ.

C'EST LE
MOMENT DE
FRAPPER !

VOICI LE
NOUVEL
ORDRE DE
MARCHÉ :

LA MOITIÉ D'ENTRE
VOUS VA CONTINUER DE
TENTER D'EXFILTRER LES
DONNÉES DE FROTHLY.

L'AUTRE MOITIÉ
VA SE CONSACRER
À PAYER NOS
SALAIRES ET NOS
INFRASTRUCTURES.

IL EST
TEMPS POUR
TAP'T DE FAIRE
DU PROFIT.

ET COMMENT
ALLONS-NOUS
Y ARRIVER ?

BITCOIN !
BITCOIN !
BITCOIN !
**CRYPTO-
DÉTOURNE-
MENT
ET
MINAGE
INTENSIF !**

... ET ...
NOUS ALLONS
ASSÉCHER
FROTHLY !

12 HEURES PLUS TÔT

PENDANT CE TEMPS, NOTRE HÉROÏNE, ALICE, PREND DU BON TEMPS BIEN MÉRITÉ.

BLACK ROCK CITY, NEVADA

BURNING MAN

J'AIMERAIS VRAIMENT QU'UNE PIZZA APPARAISSE DEVANT MOI À L'INSTANT.

NE T'EN FAIS PAS, PIRANHA ÉTINCELANT. LA PLAYA TE NOURRIRA.

EN PARLANT D'APPARITION, CET APPEL EST POUR TOI.

J'AI ENFIN DU RÉSEAU...

C'EST MA LIVRAISON DE PIZZA ?

ILS N'ONT PAS PRÉCISÉ.

PIRANHA ÉTINCELANT À L'APPAREIL.

C'EST TOI ALICE ?!

!?

GRACE ?!

DÉSOLÉE, JE SAIS QUE TU ES EN CONGÉ "SABBATIQUE" EN CE MOMENT, MAIS NOUS AVONS UN GRAVE PROBLÈME.

NOUS AVONS ÉTÉ PIRATÉS...

ENCORE ??

ABSOLUMENT. JE N'ARRIVE PAS À LE CROIRE, ET NOUS AVONS VRAIMENT BESOIN DE TON AIDE.

Looking for trouble.

ÉCOUTE, J'ADORERAI VOUS AIDER, MAIS JE SUIS UN PEU OCCUPÉE, LÀ.

JE NE PEUX PAS T'OBLIGER À RACCOURCIR TES CONGÉS,

MAIS JE NE SAIS PAS VERS QUI ME TOURNER.

JE SUIS VRAIMENT DÉSOLÉE DE T'IMPOSER ÇA.

HÉ MAIS C'EST MA PIZZA !

SPÉCIALISTE EN URGENCES INFORMATIQUES, C'EST UN SACERDOCE.

TANT PIS.

Acte 2

"It does not do to leave
a live dragon out of
your calculations,
if you live near him."
—J.R.R. Tolkien

ALICE,
C'EST
TOI ?!

LA SEULE
ET UNIQUE !

MAIS
QU'EST-CE
QUI S'EST
PASSÉ ?

JE SUIS
RAVIE QUE TU
SOIS LÀ, PEU
IMPORTE DANS
QUEL ÉTAT.

NOUS AVONS
DES RAISONS DE
PENSER QUE NOUS
AVONS ÉTÉ PIRATÉS.

BONJOUR
ALICE, RAVI
DE TE
RENCONTRER.

GRACE A FAIT
TON ÉLOGE
ET, EUH...

NOUS
AURIONS BIEN
BESOIN
DE TON
AIDE...

NE LE PRENDS
PAS MAL BUD, MAIS
LE TEMPS C'EST
DE L'ARGENT.

OULA,
C'EST QUOI
ÇA ??

METTONS-
NOUS
AU TRAVAIL.

ET BIEN,
NOS AMIS
DU FBI NOUS ONT ENVOYÉ
UNE NOTE EXPLIQUANT
QUE CERTAINES DE NOS
DONNÉES - QUE NOUS
N'AIMERIONS PAS VOIR
DIVULGUER - ÉTAIENT
SUR INTERNET

SAVEZ-VOUS
COMMENT ELLES
SE SONT
RETROUVÉES LÀ ?

AUCUNE IDÉE,
MAIS J'AI BEAUCOUP
DÉPLACÉ LES
DONNÉES LORSQUE
NOUS SOMMES
PASSÉS DANS
LE CLOUD

MFF.

APPORTEZ-
MOI DU CAFÉ.
MAINTENANT !

TAP'T

3 MOIS PLUS TÔT

JAMAIS
VU UN
HAMEÇONNAGE
AUSSI
FACILE !

FRANCHEMENT,
CE N'ÉTAIT PAS BIEN
COMPLIQUÉ. BUD NOUS
A LAISSÉ DES TAS
D'INDICES SUR SA VIE
PERSONNELLE
EN LIGNE !

AH OUI ?

OUI ! SUR
FACEBOOK IL DIT
QU'IL EST FAN DE
TRUST, ALORS JE LUI AI
ENVOYÉ UN E-MAIL AVEC UN
PDF DE LA POCHETTE
DE « RÉPRESSION ».

ET...
IL A CLIQUÉ
SANS
RÉFLÉCHIR ?

OUI.
JE SUIS ROOT
SUR SON
MACBOOK.

TU AS FAIT DES
TROUVAILLES ?

J'AI
SES CLÉS
PEMAWS.

HOOH !
ET QU'EST-CE
QUE TU VAS
EN FAIRE ?

JE VAIS
FAIRE DE
L'ARGENT.

10H03

FROTHLY

WHUMP!

JE N'ARRIVE PAS À
CROIRE QUE NOUS AYONS
EXPOSÉ DES
DONNÉES SENSIBLES
DANS UN BUCKET
S3 OUVERT.

C'EST
GRAVE ?

OUI, TRÈS. CELA
REVIENT À METTRE
NOTRE SERVEUR
DE FICHIERS SUR
INTERNET.

UNE ERREUR
DE DÉBUTANT.

RING!

RING!

BUD

Decline Accept

ET VOILÀ
LE FAUTIF
QUI
M'APPELLE...

GRRRR

SALUT BUD,
COMMENT
ÇA VA ?

DÉSOLÉ DE TE
DÉRANGER ALICE,
MAIS NOS INSTANCES EC2
PRÉSENTENT DES CHARGES
VRAIMENT TRÈS ÉLEVÉES...

J'IMAGINE QUE
C'EST L'AGENT DE
SÉCURITÉ QUE
TU AS INSTALLÉ.

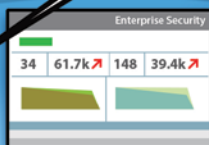
** SOUPIR
DÉSESPÉRÉ **

FROTHLY

11H25

C'EST PAS VRAI !

QUOI ?



tap tap tap

JE REGARDE LES LOGS DES SERVEURS AWS ET DE CLOUDTRAIL DANS SPLINK ENTERPRISE SECURITY DEPUIS UNE HEURE ENVIRON.

C'EST COMME SI BUD S'ÉTAIT CONNECTÉ À CHACUN DE NOS SERVEURS AWS POUR INSTALLER UN FICHIER APPELÉ « 1.JPG ».

UN JPEG ? CE N'EST PAS DRAMATIQUE ÇA, SI ?

EFFECTIVEMENT, MAIS EN RÉALITÉ C'EST UN SCRIPT DE MINAGE DE CRYPTOMONNAIE.

UN QUOI ??

DU MINAGE DE CRYPTO-MONNAIE.

POUR RÉSUMER, CE FICHIER 1.JPG EST UN SCRIPT QUI EXÉCUTE UN LOGICIEL SUR NOS INSTANCES CLOUD POUR PRODUIRE DES BITCOINS.

ÇA N'A PAS L'AIR SI GRAVE QUE ÇA.

ON POURRAIT LE CROIRE, MAIS C'EST LA RAISON POUR LAQUELLE NOS SERVEURS AWS SONT À 100 % D'UTILISATION, ET ON PAYE CES SERVEURS À L'HEURE !

LA CATA.

DIS DONC BUD, EST-CE QUE, EUH, TU AURAS INSTALLÉ DES SCRIPTS DE CRYPTOMINAGE SUR TOUS LES SERVEURS CLOUD ?

QUOI ? MAIS NON, JAMAIS !

DONC J'IMAGINE QUE TU NE VOIS PAS D'INCONVÉNIENT À CE QUE JE RESTAURE LE DERNIER INSTANTANÉ NON CONTAMINÉ DE CES INSTANCES ?

OUI, FONGE !

HEUREUSEMENT, J'AI CRÉÉ UNE PROCÉDURE PHANTOM POUR ÇA DANS LE CADRE DE NOS PLANS DE RESTAURATION ET DE RÉPONSE AUX INCIDENTS.

PHANTOM ? C'EST UN GROUPE DE MUSIQUE ?

NON, JE PARLE DE SPLINK PHANTOM. C'EST UNE SOLUTION SOAR.

POUR LE DIRE SIMPLEMENT, C'EST UN OUTIL QUI AGIT À NOTRE PLACE ET NOUS ÉVITE DE DEVOIR INTERVENIR MANUELLEMENT POUR REPOUSSER LA MENACE.

JE VAIS LANCER UNE DE CES PROCÉDURES POUR DÉSACTIVER LES SERVEURS ET RÉTABLIR LEUR ÉTAT PRÉCÉDENT.

« QU'EST-CE QUE J'AI INSTALLÉ SUR LE SERVEUR ? »

PEU IMPORTE, BUD.

TAP'T

11H31

MINCE !

QUOI ?

TOUS NOS SCRIPTS
DE CRYPTOMINAGE
VIENNENT DE S'ARRÊTER
D'UN COUP.

ON DIRAIT QU'ILS
NOUS ONT VUS ET QU'ILS
ONT UTILISÉ UNE SORTE
D'AUTOMATISATION POUR
LES ÉLIMINER
SIMULTANÉMENT.

QUE
DOIT-ON
FAIRE ?

AH, NE
T'EN FAIS
PAS.

ON A
TOUJOURS
ACCÈS À LA MACHINE
DE BUD GRÂCE
À TRUST !

PASSONS
AU
PLAN B...

FROTHLY

Acte 3

20H56

"Problem solving
is hunting.
It is savage pleasure
and we are born to it."
—Thomas Harris

TIENS BUD !
JE CROIS QUE J'AI
RÉSOLU NOTRE PETIT
PROBLÈME...
POUR LONGTEMPS.

VRAIMENT ?

OUI, ON DIRAIT
QUE LE CRYPTOMINEUR
QUE JE VIENS DE
DÉSINSTALLER DEVAIT
SE CONNECTER À DES
DOMAINES AYANT
.SHOP OU .XYZ
COMME TLD.

ET ?

NOUS N'AVONS
PAS BESOIN DE ÇA
SUR NOTRE RÉSEAU...

ALORS J'AI UTILISÉ PHANTOM
POUR BLOQUER TOUS CES
DOMAINES AVEC NOTRE PARE-FEU
ET J'AI ÉCRIT UNE RECHERCHE DE
CORRÉLATION DANS *SPLUNK ES*
POUR DÉTECTER TOUT CE QUI
POURRAIT PASSER AU TRAVERS.

AH, UN
PETIT DÉTAIL
ENCORE...

J'AI FAIT UNE
RECHERCHE DANS LE
SCÉNARIO ANALYTIQUE
DE SUPERVISION DE
SPLUNK ESCU.

ON DIRAIT QUE
TU AS OUVERT UN
PDF AU SUJET D'UN
GROUPE DES
ANNÉES 80.

ALORS
C'ÉTAIT DE
MA FAUTE ?

EH BIEN...
OUI.

GLOUPS

TRUST ?!
ILS M'ONT
EU COMME
ÇA ?

DÉSOLÉE.

ET
MAINTENANT ?

JE VAIS
UTILISER
SPLUNK LBA POUR
RECHERCHER
LES MENACES.

splunk - User Behavior Analytics

23 122 225 14

TAP'T

21H30

RHAAA,
ILS ONT
DÉSACTIVÉ LES
SERVEURS.

TU VEUX
DIRE QUE
C'EST LA FIN ?

SURTOUT PAS.
NOUS SOMMES ENCORE
DANS LEUR SYSTÈME,
NOUS AVONS SIMPLEMENT
PERDU L'ACCÈS...
POUR LE MOMENT.

QUAND NOUS
AVONS INFILTRÉ
LA MACHINE DE BUD,
NOUS AVONS ÉVOLUÉ
LATÉRALEMENT DANS
TOUT LE RÉSEAU. NOUS
AVONS DES OUTILS
D'ACCÈS À DISTANCE
DANS TOUS LES
SYSTÈMES
DE FROTHLY.

TAP'T commence à examiner les données de l'enregistreur de frappe provenant de leurs agents malveillants et découvre le nom d'utilisateur et le mot de passe de Bud pour la console amazon.com/EC2...

TAP'T se connecte au compte de BUD et commence à lancer des instances.
Des centaines d'instances.

CETTE FOIS,
C'EST UNE AFFAIRE
PERSONNELLE.

SI NOUS N'ARRIVONS
PAS À TIRER LE MOINDRE
SOU DE CETTE AFFAIRE,
AU MOINS NOUS FERONS
EXPLOSER LEUR
FACTURE AWS !

ON VA LES
ESSORER !

EMBARCADERO

SAN FRANCISCO, CA

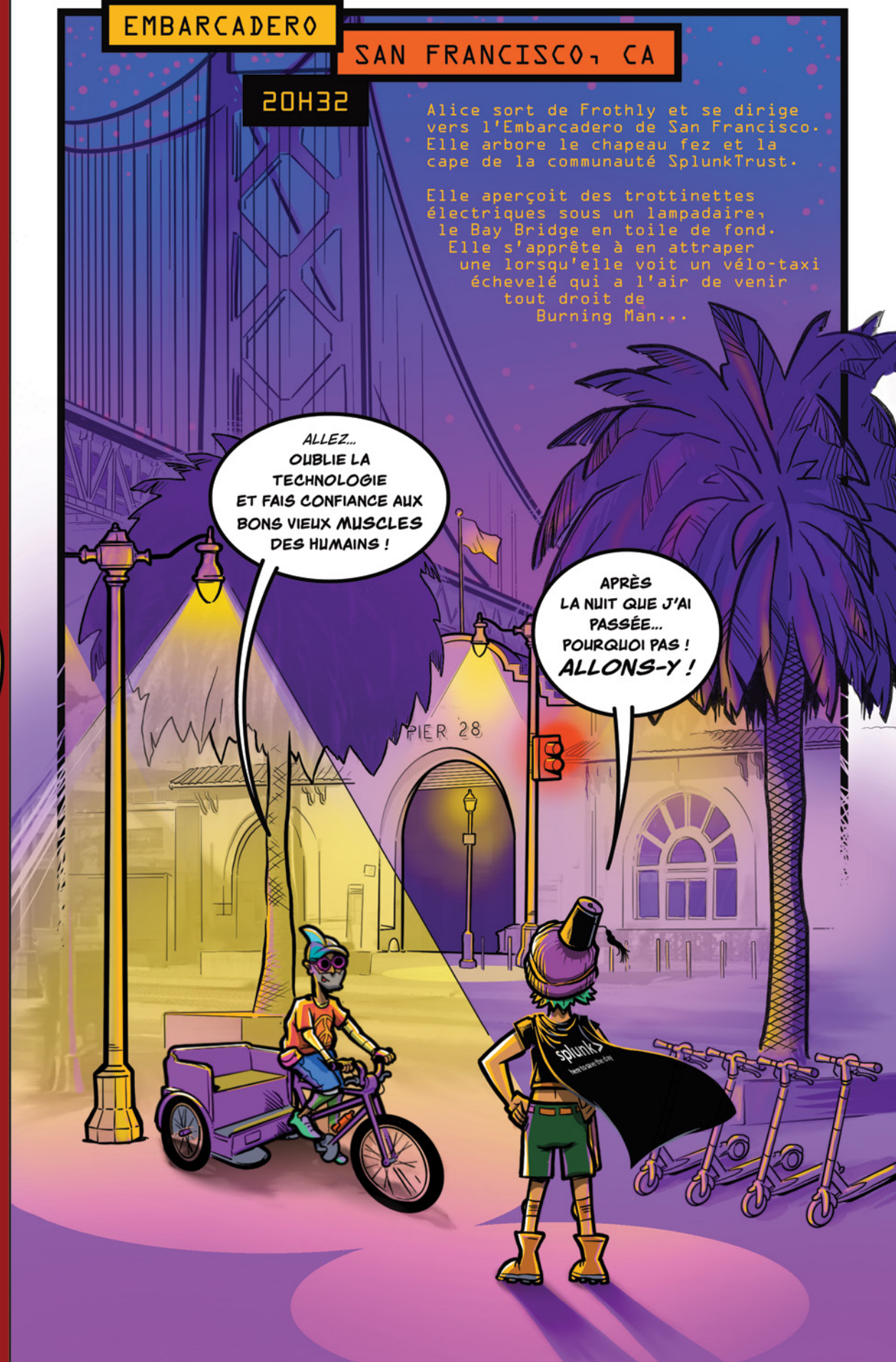
20H32

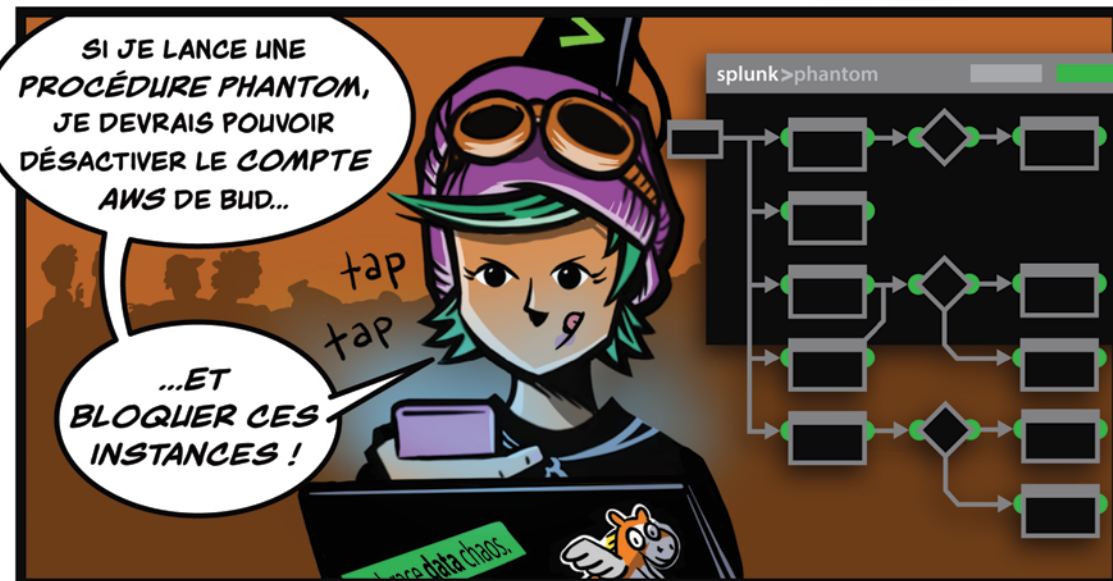
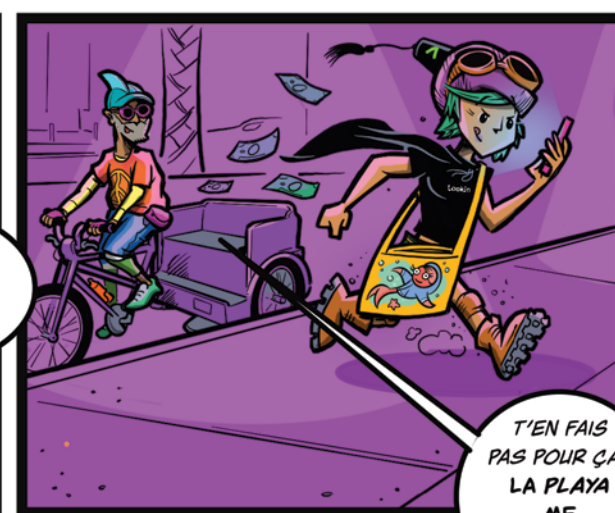
Alice sort de Frothly et se dirige vers l'Embarcadero de San Francisco. Elle arbore le chapeau fez et la cape de la communauté SplunkTrust.

Elle aperçoit des trottinettes électriques sous un lampadaire, le Bay Bridge en toile de fond. Elle s'apprête à en attraper une lorsqu'elle voit un vélo-taxi échevelé qui a l'air de venir tout droit de Burning Man...

ALLEZ...
OUBLIE LA
TECHNOLOGIE
ET FAIS CONFIANCE AUX
BONS VIEUX MUSCLES
DES HUMAINS !

APRÈS
LA NUIT QUE J'AI
PASSÉE...
POURQUOI PAS !
ALLONS-Y !







ON DIRAIT QUE
LES MACHINES DE FROTHLY
SONT INFECTÉES PAR
UN OUTIL DE PIRATAGE
POWERSHELL ET CONTRÔLÉES
À DISTANCE PAR TAP'T.

EN GROS,
C'EST COMME ÇA
QU'ILS SE SONT
INFILTRÉS !



SAIS-TU OÙ
ILS SE
CACHENT ?

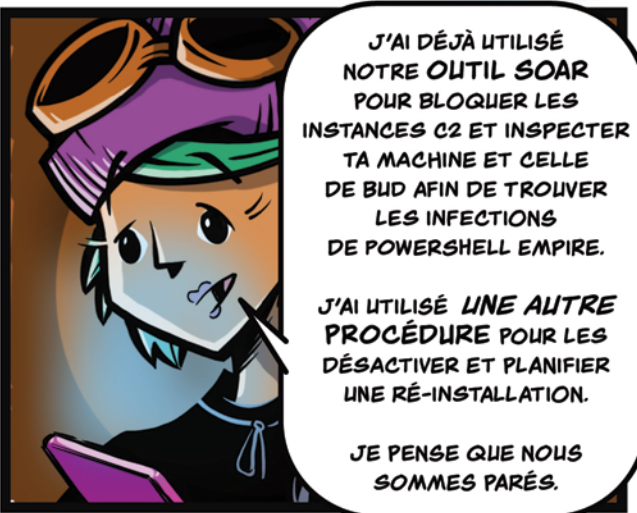


J'AI VU DES
SIGNAUX PROVENANT
DE TA MACHINE ET
CELLE DE BUD.



LES
CRAPULES

ET TU PEUX Y
FAIRE QUELQUE
CHOSE ?



J'AI DÉJÀ UTILISÉ
NOTRE OUTIL SOAR
POUR BLOQUER LES
INSTANCES C2 ET INSPECTER
TA MACHINE ET CELLE
DE BUD AFIN DE TROUVER
LES INFECTIONS
DE POWERSHELL EMPIRE.

J'AI UTILISÉ UNE AUTRE
PROCÉDURE POUR LES
DÉSACTIVER ET PLANIFIER
UNE RÉ-INSTALLATION.

JE PENSE QUE NOUS
SOMMES PARÉS.



C'EST
INCROYABLE !
TU AS DÙ NOUS FAIRE
ÉCONOMISER UNE
SACRÉE SOMME !



OUI,
C'EST BIEN
POSSIBLE.



PARFAIT !
OÙ TE TROUVES-TU,
ET AS-TU PU
PRENDRE UNE
DOUCHE ?



PAS
ENCORE.



ALORS RENTRE VITE
CHEZ TOI !
JE T'ATTENDS DÈS DEMAIN À LA
PREMIÈRE HEURE POUR DISCUTER
DE NOTRE PROCHAIN
GRAND PROJET.



ENCORE
UN GRAND
PROJET ?!

NOUS ESSAYONS
DE RACHETER UNE
BRASSERIE, ET J'AI
BESOIN DE TOI POUR
SAISIR CETTE
HOP-PORTUNITÉ !
TU SAISIS ?



OUI OUI.



VOUS ÊTES
PIRANHA
ÉTINCELANT ?



J'AI UNE
PIZZA POUR
VOUS.

C'EST
MOI.....
EH BIEN LA PLAYA
TIENT SES
PROMESSES.

TAP'T

LE LENDEMAIN

NOUS AVONS
ENCORE
PERDU !

tap

tap
tap

PAS SI
VITE...

J'AI UN
NOUVEAU
COMPTE
UTILISATEUR SUR
LE DOMAINE
DE FROTHLY
ET J'AI ACCÈS
À LEUR
SERVEUR.

GÉNIAL !
ON VA LEUR
MONTRER.

N'OUBLIE PAS,
TAP'T C'EST
D'ABORD
ET AVANT TOUT
DU GÉNIE !

ET LE COMBAT
CONTINUE...



PAS DE REPOS POUR LES BRAVES



Pour en savoir plus sur la manière dont Frothly garde une longueur d'avance sur les cybermenaces, rendez-vous sur le site :
www.splunk.fr

