

DE L'AUTRE CÔTÉ DE LA GLASS TABLE

PROBLÈME 1 : QUI A RENVERSÉ LES DONNÉES ?



LA PÉTILLANTE HISTOIRE D'UNE FAILLE DE SÉCURITÉ DANS
UNE BRASSERIE ARTISANALE À L'AVENIR RADIEUX.



PDG

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



STAGIAIRE

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



SCIENTIFIQUE EN CHEF

SON DUR LABEUR ET LE SUCCÈS DES CRÉATIONS DE SON LABORATOIRE FONT D'ELLE UNE DIGNE MAÎTRE-BRASSEUSE.



RESPONSABLE INFORMATIQUE

SURMENÉ ET DÉPASSÉ DERRIÈRE SES «LUNETTES DE BIÈRE», SA VISION DE LA SÉCURITÉ EST DEVENUE TRÈS FLOUE.



ANALYSTE SOC CONSULTANTE

VÉRITABLE JÉROBOAM D'INTELLIGENCE ET D'ORIGINALITÉ, CETTE CONNAISSEUSE DÉTECTE LE MOINDRE PARFUM D'ANOMALIE.

ACTE I

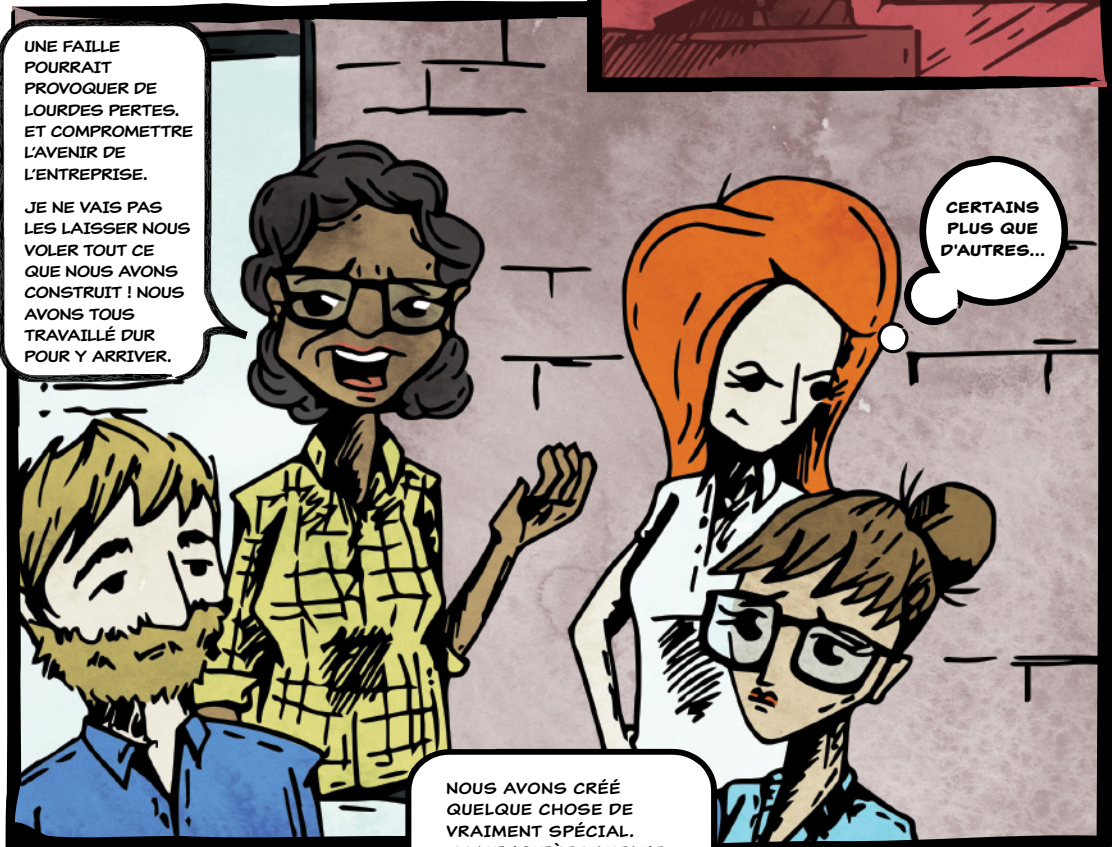
« MÉFIANCE ET PRUDENCE SONT LES
BONNES FÉES DE LA SÉCURITÉ. »

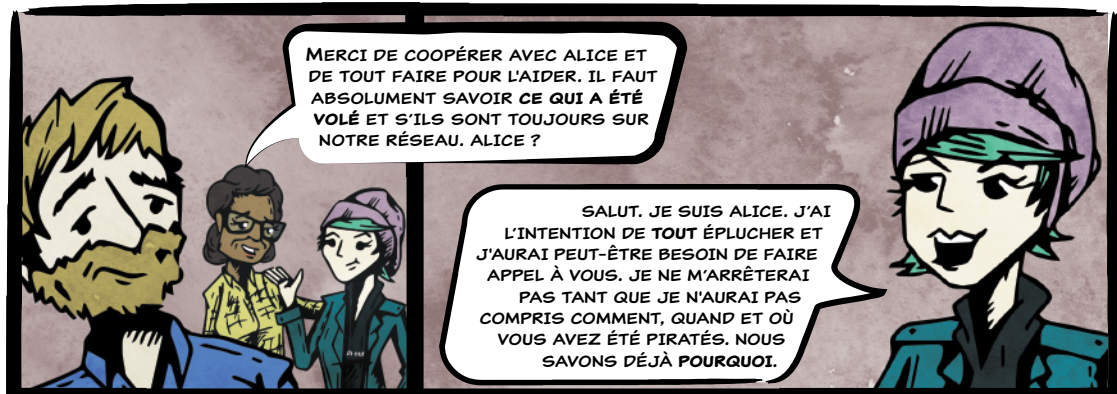
— BENJAMIN FRANKLIN





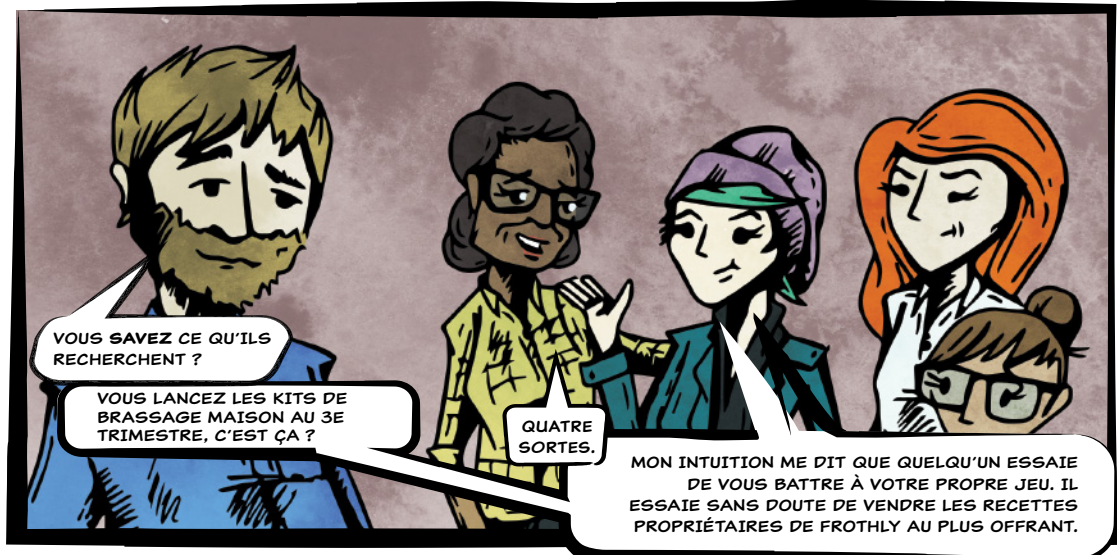






MERCI DE COOPÉRER AVEC ALICE ET DE TOUT FAIRE POUR L'AIDER. IL FAUT ABSOLUMENT SAVOIR CE QUI A ÉTÉ VOLÉ ET S'ILS SONT TOUJOURS SUR NOTRE RÉSEAU. ALICE ?

SALUT. JE SUIS ALICE. J'AI L'INTENTION DE TOUT ÉPLUCHER ET J'AURAI PEUT-ÊTRE BESOIN DE FAIRE APPEL À VOUS. JE NE M'ARRÊTERAI PAS TANT QUE JE N'AURAI PAS COMPRIS COMMENT, QUAND ET OÙ VOUS AVEZ ÉTÉ PIRATÉS. NOUS SAVONS DÉJÀ POURQUOI.



VOUS SAVEZ CE QU'ILS RECHERCHENT ?

VOUS LANCEZ LES KITS DE BRASSAGE MAISON AU 3E TRIMESTRE, C'EST ÇA ?

QUATRE SORTES.

MON INTUITION ME DIT QUE QUELQU'UN ESSAIE DE VOUS BATTRE À VOTRE PROPRE JEU. IL ESSAIE SANS DOUTE DE VENDRE LES RECETTES PROPRIÉTAIRES DE FROTHLY AU PLUS OFFRANT.

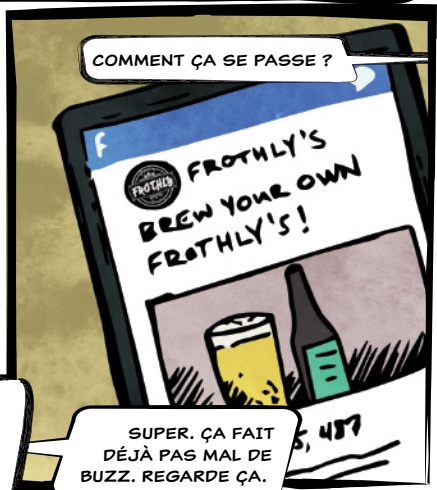


APRÈS LA RÉUNION

SALUT KEVIN. C'EST D'INGUE, HEIN ?

C'EST CLAIR. ELLE VA AVOIR ACCÈS À L'INTÉGRALITÉ DE NOTRE RÉSEAU.

OUAIS. AU FAIT, MERCI ENCORE POUR CE MACBOOK, MÊME SI SA LICENCE D'OFFICE EST SUR LE POINT D'EXPIRER. IL ME PERMET DE METTRE À JOUR LA BOUTIQUE EN LIGNE, ET C'EST LA PRIORITÉ NUMÉRO UN !



COMMENT ÇA SE PASSE ?

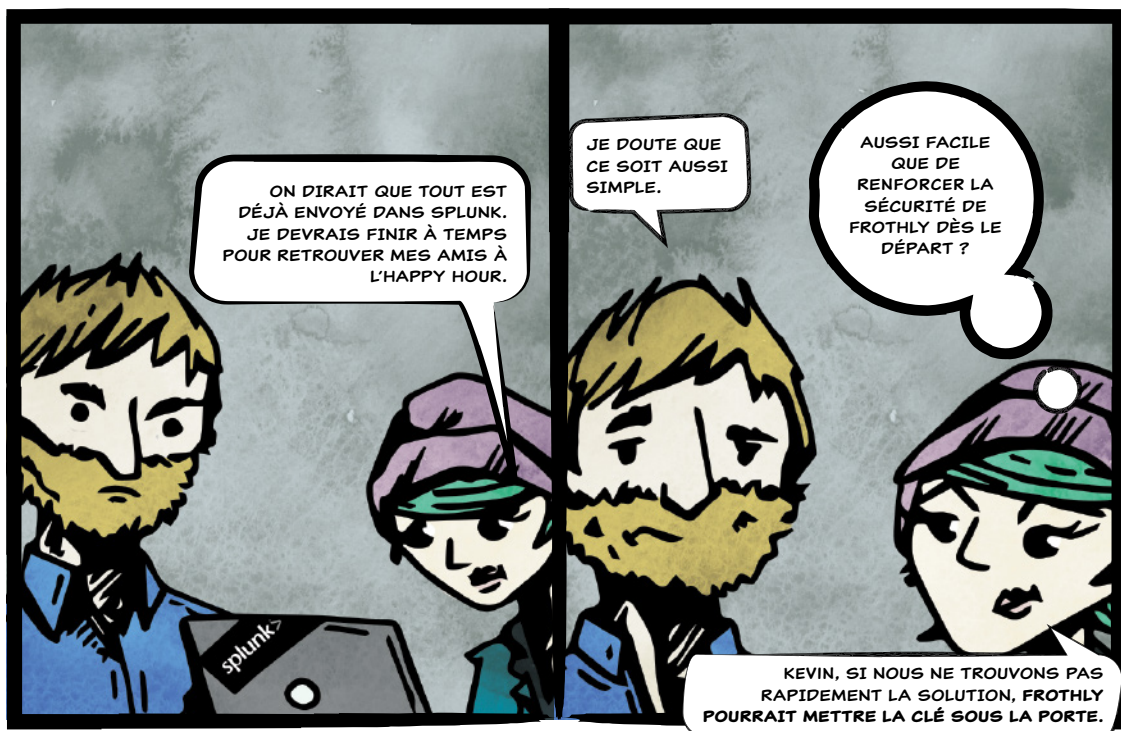
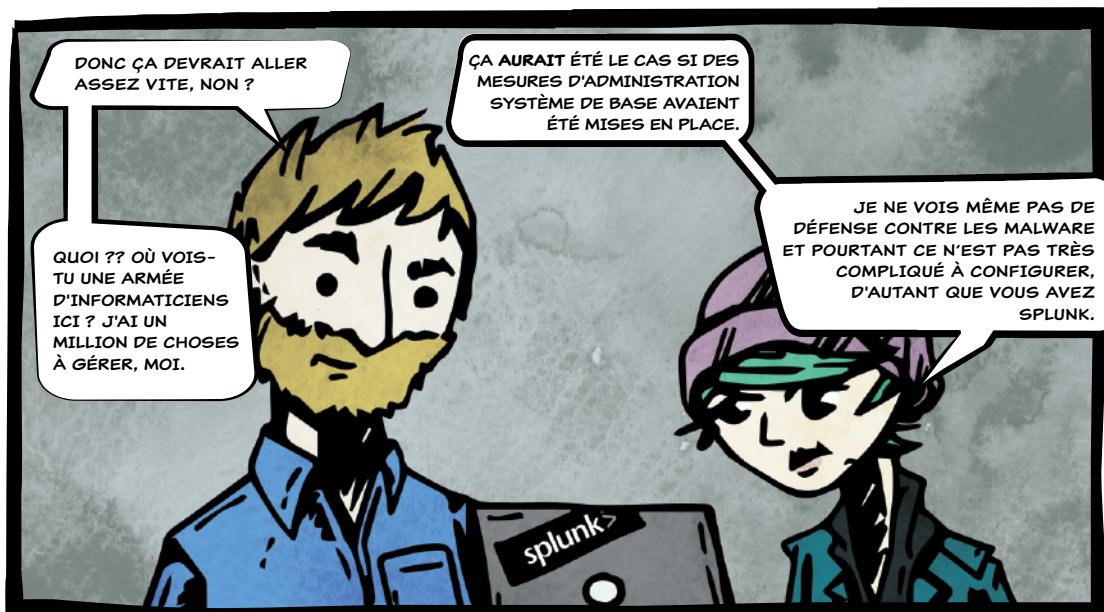
SUPER. ÇA FAIT DÉJÀ PAS MAL DE BUZZ. REGARDE ÇA.



PLUS TARD

TU DOIS AVOIR PAS MAL D'ANECDOTES À RACONTER AVEC TOUTE TON EXPÉRIENCE EN RÉPONSE AUX INCIDENTS. JE SÉRAIS CURIEUX D'ENTENDRE ÇA DEVANT UNE BIÈRE !

AVEC MON ÉQUIPE, ON VOIT ÇA COMME UN JEU. Y A TOUJOURS DES RIGOLOS PRÊTS À TE POSER UNE NOUVELLE ÉNIGME.



ACTE II

« LA LUNE NE DISPARÂÎT PAS QUAND
NOUS CESSONS DE LA REGARDER. »

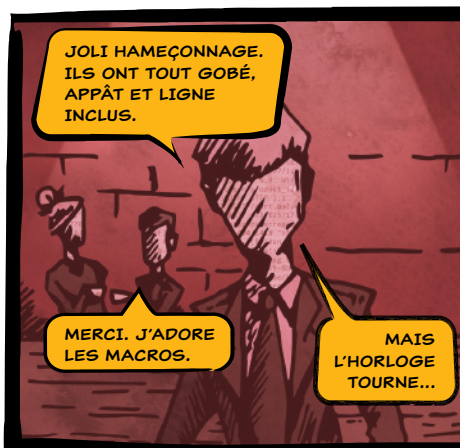
— ALBERT EINSTEIN

TAE-DONGGANG APT

DÈS QUE NOUS AURONS LES RECETTES DE FROTHLY, NOUS POURRONS LES VENDRE AU PLUS OFFRANT !

J'AI LE GOÛT DE LA VICTOIRE DANS LA BOUCHE.

NE VENDS PAS LA PEAU DE L'OURS. L'EXFILTRATION DES DONNÉES DE FROTHLY EST EN COURS, MAIS NOUS AVONS ENCORE BEAUCOUP À FAIRE POUR OBTENIR TOUT CE QU'IL NOUS FAUT.



JOLI HAMEÇONNAGE.
ILS ONT TOUT GOBÉ,
APPÂT ET LIGNE
INCLUS.

MERCI. J'ADORE
LES MACROS.

MAIS
L'HORLOGE
TOURNE...



ILS UTILISENT SPLUNK, ÇA COMPLIQUE
LES CHOSSES MAIS COMME LEUR ÉQUIPE
IT EST COMPLÈTEMENT DÉPASSÉE, IL
N'Y A MÊME PAS D'ANTIVIRUS SUR
CERTAINS POSTES DE TRAVAIL.

ÇA NOUS LAISSE
UNE FENÊTRE.

MAIS ELLE EST
ÉTROITE ET NOUS
RISQUONS D'ÊTRE
DÉTECTÉS.

ALLONS-Y.



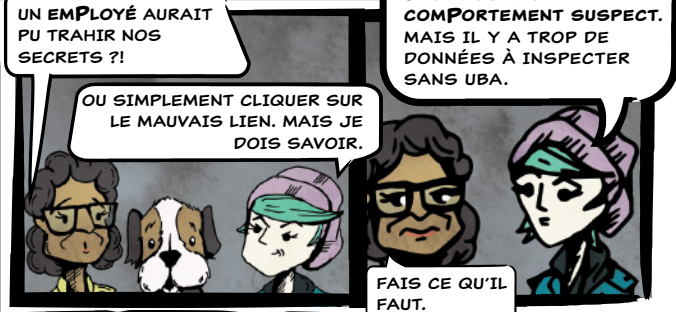
UNE QUESTION.

J'ÉCOUTE.

ES-TU D'ACCORD POUR
QUE JE LANCE L'UBA ?

JE LE SERAIS
CERTAINEMENT SI JE
SAVAIS CE QUE C'EST.

C'EST L'ANALYSE DES
COMPORTEMENTS DES UTILISATEURS,
UN PRODUIT SPLUNK QUI UTILISE LE
MACHINE LEARNING POUR DÉTECTER
LES MENACES INTERNES.



UN EMPLOYÉ AURAIT
PU TRAHIR NOS
SECRETS ?!

OU SIMPLEMENT CLIQUER SUR
LE MAUVAIS LIEN. MAIS JE
DOIS SAVOIR.

EN CHERCHANT TAP'T,
J'AI TROUVÉ UN
COMPORTEMENT SUSPECT.
MAIS IL Y A TROP DE
DONNÉES À INSPECTER
SANS UBA.

FAIS CE QU'IL
FAUT.



EN FIN D'APRÈS-MIDI

JE PEUX ?

UN CARACTÈRE. UN CLIC.
VRAIMENT, ÇA PEUT
SUFFIRE.

ÉCOUTE, JE VEUX BIEN
T'AIDER. MAIS JE NE
PEUX PAS ME PASSER
DE MON ORDINATEUR. JE
PEUX TE CERTIFIER QUE
CETTE MACHINE EST UNE
IMPASSE.

JE NE SUIS PAS.



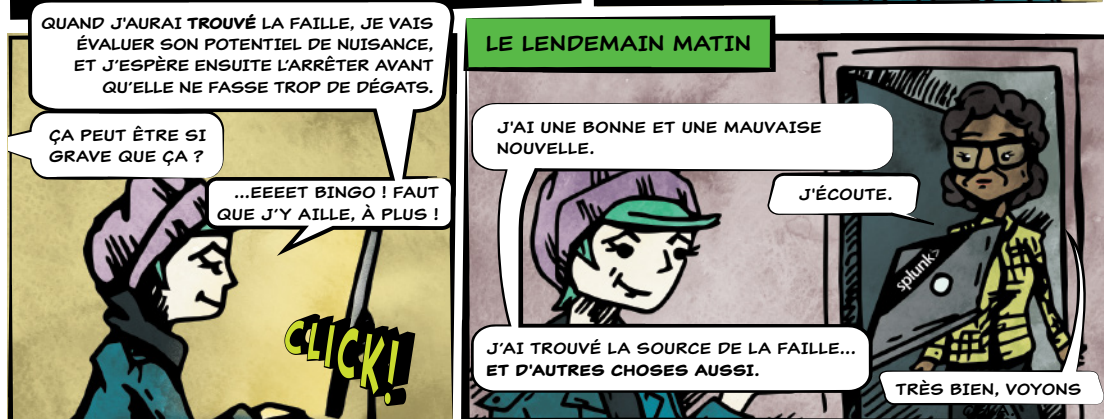
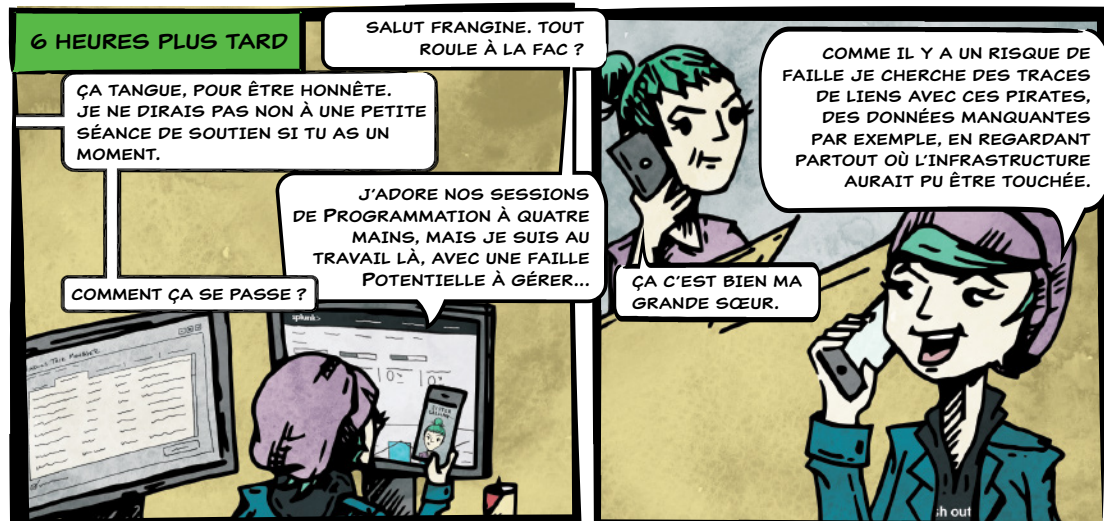
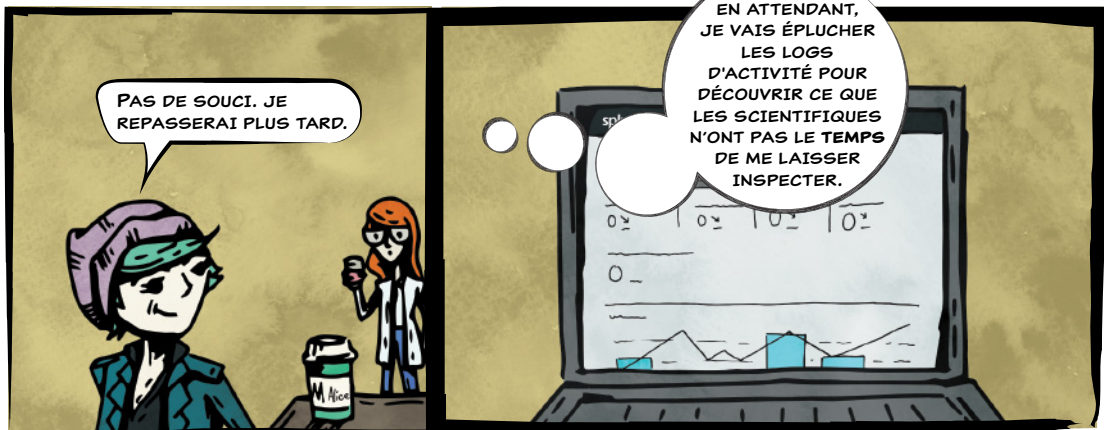
CES RECETTES SONT UNE MINE D'OR
ENTRE DE MAUVAISES MAINS.

ET JE VAIS TROUVER QUI S'EST SALI
LES MAINS.

OUAIS. JE SAIS.
C'EST MON LABO
QUI LES A CRÉÉES.

VRAIMENT ? JE PENSais QUE
CE SERAIT TROP COMPLIQUÉ.

TOUTE ACTION LAISSE UNE TRACE, AMBER.
IL SUFFIT D'AVOIR L'OUTIL CAPABLE DE LA
FLAIRER.





UN CLIC A SUFFI POUR ACTIVER LE MALWARE. C'EST COMME ÇA QUE TAP'T A EU ACCÈS AUX DONNÉES.

QUAND J'AI TROUVÉ PAR OÙ ILS ÉTAIENT ENTRÉS, J'AI PU LES EXPULSER DU RÉSEAU AVANT QU'ILS NE RÉCUPÈRENT PLUS D'INFORMATIONS ET LEUR METTRE LES POINTS SUR LES I.

BON, TRÈS BIEN. AU MOINS TU AS RÉSOLU LE MYSTÈRE. ET LA MAUVAISE NOUVELLE ?

QUAND J'AI LANCÉ UBA, J'AI DÉCOUVERT QU'IL NE S'AGISSAIT PAS SEULEMENT D'UNE ATTAQUE PAR HAMEÇONNAGE. J'AI TROUVÉ DES TRACES DE MENACE INTERNE. ALORS J'AI CREUSÉ...



J'AI DÉCOUVERT UNE EXFILTRATION DE DONNÉES SUSPECTE DU CÔTÉ D'UN EMPLOYÉ DE FROTHLY. CERTAINES DONNÉES QUE TAP'T RECHERCHAIT, AU MOMENT OÙ LA FAILLE S'EST PRODUITE. JE NE SAIS PAS ENCORE SI TOUT CELA EST LÉGAL, IL FAUT LAISSER MACÉRER UN PEU PLUS LONGTEMPS.

À CE STADE, NOUS DEVONS AGIR AVEC UNE PRUDENCE ET UNE RAPIDITÉ EXTRÊMES.

JE VEUX SAVOIR QUI C'EST.

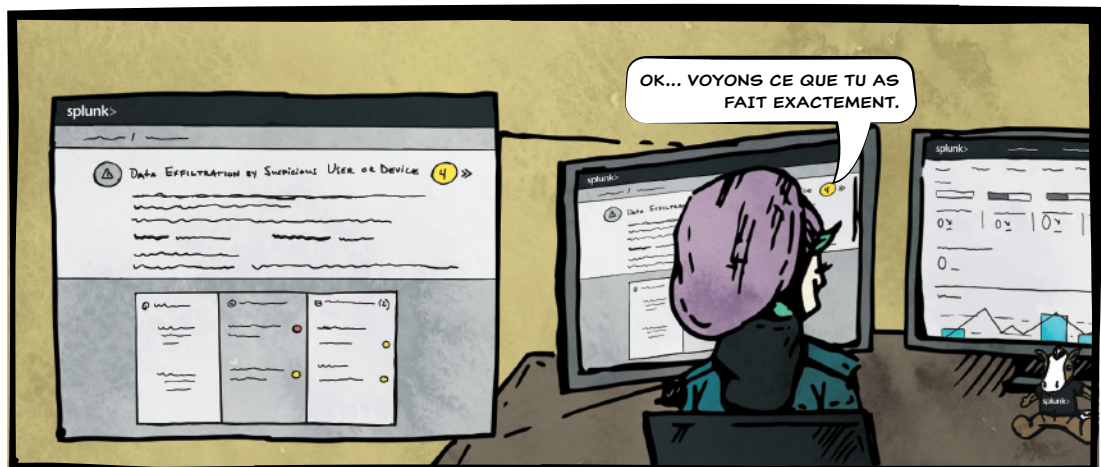
LA **PRIORITÉ**, C'EST D'ÉVALUER LES DÉGÂTS ET DE VOIR S'IL EST ENCORE POSSIBLE D'ARRÊTER LA FUITE. JE NE VEUX PAS PRENDRE LE RISQUE DE DÉTRUIRE LA CARRIÈRE DE QUELQU'UN SANS ÊTRE SÛRE À 100 %.



DÈS QUE J'AURAI CONFIRMÉ MES SOUPÇONS, NOUS APPELLERONS LE FBI POUR QU'ILS MÈNENT UNE ENQUÊTE EN BONNE ET DUE FORME.

QU'EST-CE QUE VOUS ATTENDEZ ?





36 HEURES PLUS TARD



TAP'T A ENVOYÉ UN E-MAIL DE HAMEÇONNAGE AVEC UNE PIÈCE JOINTE, FACTURE.ZIP. QUAND MALLORY L'A OUVERT, ILS ONT INFECTÉ SA MACHINE AVEC UN CHEVAL DE TROIE.

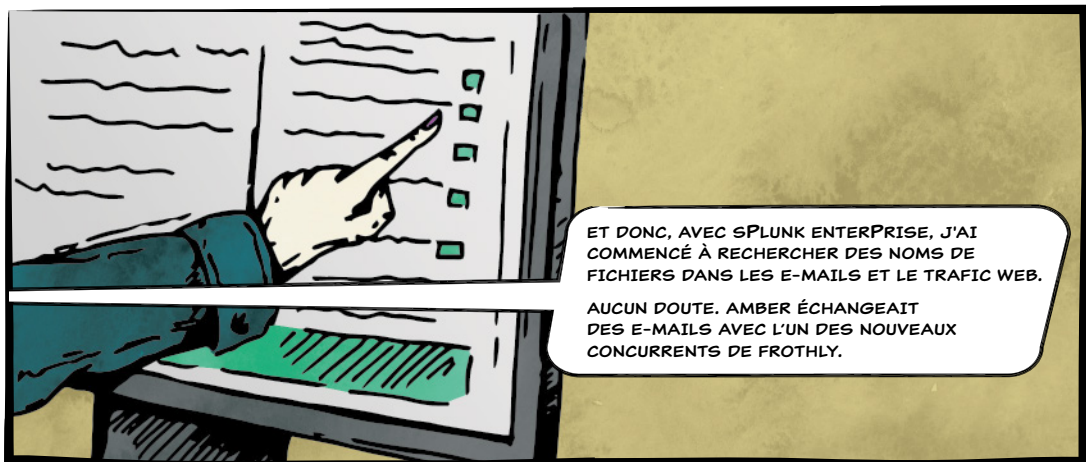
HEUREUSEMENT, VOTRE INSTANCE DE SPLUNK NE REÇOIT PAS SEULEMENT LES LOGS DE LA MESSAGERIE ET DES POSTES DE TRAVAIL.



EFFECTIVEMENT. QUAND J'AI LANCÉ L'OUTIL D'UBA, J'AI TROUVÉ PLEIN D'ALERTE « EXFILTRATION DE DONNÉES PAR DES UTILISATEURS SUSPECTS » QUI MONTRAIENT AMBER EN TRAIN DE SORTIR DES BREVETS DU SERVEUR DE FICHIERS...

QUOI ?! MAIS LES BREVETS NE SONT ABSOLUMENT PAS CENSÉS QUITTER CE SERVEUR !

EXACTEMENT. ET COMME C'ÉTAIT INHABITUEL, L'UBA L'A DÉTECTÉ ET GÉNÉRÉ DES ALERTES. MAIS JE DEVAIS M'ASSURER QUE CET ACTE ÉTAIT MALVEILLANT. ELLE AURAIT PU VOULOIR TRAVAILLER SUR CES FICHIERS AVEC SON ORDINATEUR.



ET DONC, AVEC SPLUNK ENTERPRISE, J'AI COMMENCÉ À RECHERCHER DES NOMS DE FICHIERS DANS LES E-MAILS ET LE TRAFIC WEB.

AUCUN DOUTE. AMBER ÉCHANGEAIT DES E-MAILS AVEC L'UN DES NOUVEAUX CONCURRENTS DE FROTHLY.

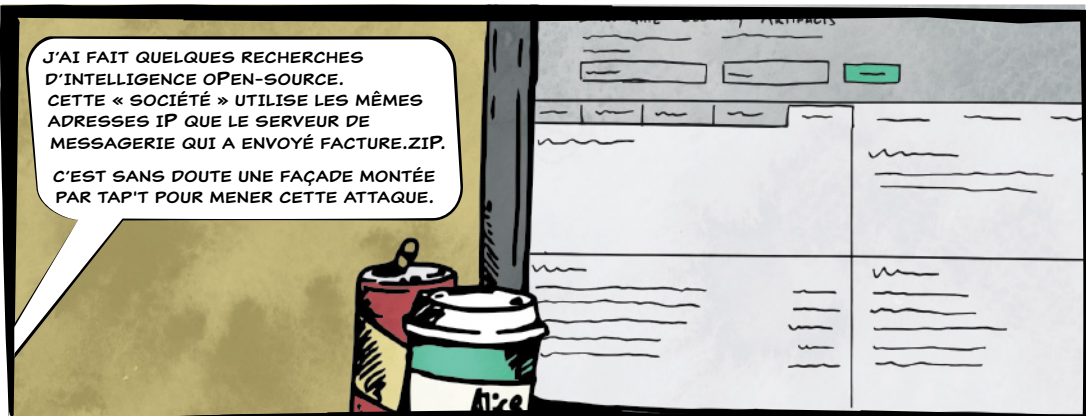


ON PENSE CONNAÎTRE QUELQU'UN...

ELLE MONTRAIT DES CAPTURES D'ÉCRAN DE CE DOCUMENT POUR PROUVER QU'ELLE ÉTAIT SÉRIEUSE ET POUVAIT « FOURNIR LE RESTE ».

OH C'EST BAS. VRAIMENT C'EST HONTEUX.

ATTENDS, LE PIRE ARRIVE.



J'AI FAIT QUELQUES RECHERCHES D'INTELLIGENCE OPEN-SOURCE. CETTE « SOCIÉTÉ » UTILISE LES MÊMES ADRESSES IP QUE LE SERVEUR DE MESSAGERIE QUI A ENVOYÉ FACTURE.ZIP. C'EST SANS DOUTE UNE FAÇADE MONTÉE PAR TAP'T POUR MENER CETTE ATTAQUE.



SI NOUS NE L'AVIONS PAS COINCÉE AVEC UBA, ELLE AURAIT PU TOUT LEUR ENVOYER !

LE LENDEMAIN

ALLEZ VOIR ALICE !

ALICE!!!

ELLE A ÉTÉ JUSQU'AU FOND DES CHOSSES, À NOUS DE FAIRE DE MÊME !

MERCI À TOUS. ÇA FAIT PLAISIR DE VOIR LES MÉCHANTS SE FAIRE PRENDRE DE TEMPS À AUTRE.

ET MAINTENANT LES CHOSSES PEUVENT REPRENDRE LEUR COURS NORMAL !

PAS VRAIMENT, KEVIN. FROTHLY A EU DE LA CHANCE !

L'INSTANCE QUE TU AS INSTALLÉE NE FAISAIT QU'EFFLEURER LES POSSIBILITÉS DE SPLUNK. PHANTOM AUTOMATISE TES WORKFLOWS : C'EST COMME SI TU AVAIS UNE PLUS GROSSE ÉQUIPE ET ÇA RÉDUIT LE DÉLAI D'INTERVENTION.

IL TE RESTE BEAUCOUP DE PAIN SUR LA PLANCHE ! INSTALLER DES CORRECTIFS ET DES ANTIVIRUS SUR TOUS LES SYSTÈMES, LIMITER POWERSHELL, MIEUX PROTÉGER LES E-MAILS, INTÉGRER L'INTELLIGENCE DES MENACES. ET CE N'EST QUE LE DÉBUT.

BON, J'AI VRAIMENT BIEN FAIT DE VOUS ENVOYER CETTE PROPOSITION DE POSTE À PLEIN TEMPS, MOI.

COMMENT ?

DANS LA SOIRÉE

PAS DE REPOS POUR LES BRAVES.



TRAFIC GANG APT

SI VOUS AVEZ RATÉ, PAS GRAVE, HACHEZ,
HACHEZ ET ENCORE HACHEZ...

LE PREMIER INFILTRÉ
PAYE SA TOURNÉE.

ÇA MARCHE.



666 130.253.37.97 - - [07/Jan 18:10:55:187] "GET /oldlink?item_id=EST-6&SESSIONID=SD0SL8FF9ADFF9 HTTP/1.1" 200
B-02"Opera/9.01 (Windows NT 5.1; U; en)" 553 62.216.64.19 - - [07/Jan 18:10:55:111] "GET /category.screen?category
t.do?action=remove&itemId=EST-15&product_id=FL-DSH-01"Opera/9.01 (Windows NT 5.1; U; en)" 695130.253.37.97 - - [0
P/1.1" 404 474 "http://buttercup-shopping.com/oldlink?item_id=EST-21"Mozilla/4.0 (compatible; MSIE 6.0; Windows N
15&product_id=AV-SB-02&JSESSIONID=SD4SL1FF7ADFF7 HTTP/1.1" 200 205 "http://buttercup-shopping.com/cart.do?action=rem
t." 163 131.178.233.243 - - [07/Jan 18:10:54:171] "GET /oldlink?item_id=EST-17&JSESSIONID=SD1SL9FF9ADFF1 HTTP/1.1" 20
CW-01"Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.37
emId=EST-7&product_id=FI-SW-01&JSESSIONID=SD10SL3FF1ADFF4 HTTP/1.1" 404 2258 "http://buttercup-shopping.com/cart.do?
5.1; SV1)" 189 82.245.228.36 - - [07/Jan 18:10:54:165] "GET /category.screen?category_id=TEDDY&JSESSIONID=SD1SL1FF8A
27&product_id=FL-DLH-02"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 969 128.241.2
RP-SN-01&JSESSIONID=SD7SL8FF3ADFF2 HTTP/1.1" 200 1901 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST
37.97 - - [07/Jan 18:10:54:121] "GET /category.screen?category_id=BOUQUETS&JSESSIONID=SD10SL1FF4ADFF10 HTTP/1.1" 406
B-02"Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375
SURPRISE&JSESSIONID=SD7SL3FF9ADFF10 HTTP/1.1" 200 1361 "http://buttercup-shopping.com/category.screen?category_id=SU
53;104] "POST /category.screen?category_id=BOUQUETS&JSESSIONID=SD7SL3FF9ADFF2 HTTP/1.1" 200 2567 "http://buttercup
5.1)" 920 130.253.37.97 - - [07/Jan 18:10:52:111] "GET /category.screen?category_id=TEDDY&JSESSIONID=SD8SL2FF5ADFF
lebot/2.1 (http://www.googlebot.com/bot.html) " 302 125.17.14.100 - - [07/Jan 18:10:51:197] "POST /category.screen
/category.screen?category_id=BOUQUETS"Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (K
97] "GET /product.screen?product_id=FL-DLH-02&JSESSIONID=SD6SL2FF3ADFF4 HTTP/1.1" 200 363 "http://buttercup-shopping
81 131.178.233.243 - - [07/Jan 18:10:51:127] "GET /oldlink?item_id=EST-12&JSESSIONID=SD7SL1FF9ADFF6 HTTP/1.1" 200 33
MSIE 6.0; Windows NT 5.1; SV1)" 876 128.241.220.82 - - [07/Jan 18:10:50:198] "GET /category.screen?product_id=RP-SN-01&
en?product_id=RP-SN-01"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 876 128.241.220.82 - - [07/Jan 18:10:50:198]
B "http://buttercup-shopping.com/product.screen?product_id=RP-SN-01&JSESSIONID=SD7SL1FF9ADFF6 HTTP/1.1" 200 33
&product_id=FL-DSH-01&JSESSIONID=SD1SL6FF3ADFF7 HTTP/1.1" 200 2139 "http://buttercup-shopping.com/product.screen?pro
80 195.80.144.22 - - [07/Jan 18:10:50:178] "GET /category.screen?category_id=RP-LI-02&JSESSIONID=SD7SL1FF9ADFF6
RP-LI-02"Opera/9.20 (Windows NT 6.0; U; en)" 473 125.17.14.100 - - [07/Jan 18:10:50:136] "POST /cart.do?action=pur
200 3778 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"Mozilla/4.0 (compatible; MSIE 6.0; Wind
=EST-11&JSESSIONID=SD8SL1FF3ADFF2 HTTP/1.1" 404 1418 "http://buttercup-shopping.com/oldlink?item_id=EST-11"Mozilla
me/5.0.375.38 Safari/533.4" 443 12.130.60.4 - - [07/Jan 18:10:49:128] "GET /cart.do?action=purchase&itemId=EST-14&pr
duct.screen?product_id=RP-SN-01"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 298 128.241.220.82 - - [07/Jan
FF10ADFF7 HTTP/1.1" 200 1409 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"Mozilla/5.0 (Windows
7/Jan 18:10:48:143] "GET /product.screen?product_id=K9-BD-01&JSESSIONID=SD8SL1FF3ADFF2 HTTP/1.1" 200 844 "http://but
3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4" 629 212.235.92.150 - - [07/Jan 18:1
99] "http://buttercup-shopping.com/category.screen?category_id=FLOWERS"Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10
6 125.17.14.100 - - [07/Jan 18:10:48:102] "POST /category.screen?category_id=GIFTS&JSESSIONID=SD4SL7FF6ADFF6 HTTP/1.
I-FW-02"Opera/9.01 (Windows NT 5.1; U; en)" 294 202.164.25.24 - - [07/Jan 18:10:48:102] "GET /category.screen?cate
t.do?action=view&itemId=EST-21&product_id=AV-CB-01"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 473 12.130.
0FF3ADFF10 HTTP/1.1" 200 3718 "http://buttercup-shopping.com/product.screen?product_id=FI-FW-02"Mozilla/4.0 (compa
9] "POST /category.screen?category_id=GIFTS&JSESSIONID=SD5SL3FF6ADFF9 HTTP/1.1" 200 672 "http://buttercup-shopping.c
t/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4" 265 91.205.40.22 - - [07/Jan 18:10:46:111] "GET /cart.do
" 200 1371 "http://buttercup-shopping.com/category.screen?category_id=BOUQUETS"Mozilla/5.0 (Macintosh; U; Intel Ma
7 142.162.221.28 - - [07/Jan 18:10:45:145] "GET /cart.do?action=addtocart&itemId=EST-7&product_id=AV-CB-01&JSESSIONI
I-02"Opera/9.01 (Windows NT 5.1; U; en)" 103 131.178.233.243 - - [07/Jan 18:10:45:142] "POST /category.scre
/cart.do?action=view&itemId=EST-13&product_id=FI-FW-02"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 403 141
FF2ADFF9 HTTP/1.1" 200 2982 "http://buttercup-shopping.com/category.screen?category_id=BOUQUETS"Mozilla/5.0 (Wind
3 - - [07/Jan 18:10:45:114] "GET /oldlink?item_id=EST-14&JSESSIONID=SD1SL1FF4ADFF4 HTTP/1.1" 406 364 "http://butter
ot.html) " 310 27.101.11.11 - - [07/Jan 18:10:44:197] "GET /cart.do?action=addtocart&itemId=EST-21&product_id=RP-S
?category_id=TEDDY"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 801 141.146.8.66 - - [07/Jan 18:10:44:180]
739 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
&JSESSIONID=SD5SL10FF8ADFF4 HTTP/1.1" 404 3842 "http://buttercup-shopping.com/product.screen?product_id=FL-DSH-01" "
147] "POST /product.screen?product_id=RP-SN-01&JSESSIONID=SD5SL7FF6ADFF5 HTTP/1.1" 404 2023 "http://buttercup-shoppi
t/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4" 154 141.146.8.66 - - [07/Jan 18:10:44:101] "GET /product
opping.com/product.screen?product_id=K9-CW-01"Googlebot/2.1 (http://www.googlebot.com/bot.html) " 234 12.130.60.5
FF8 HTTP/1.1" 200 1763 "http://buttercup-shopping.com/oldlink?item_id=EST-26"Opera/9.01 (Windows NT 5.1; U; en)" 5
product_id=AV-SB-02&JSESSIONID=SD3SL1FF9ADFF10 HTTP/1.1" 404 2824 "http://buttercup-shopping.com/category.screen?cate
]"GET 12.130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SL4FF10ADFF10 HT
FI-SW-01"Opera/9.20 (Windows NT 6.0; U; en)" 559 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?pro
gory.screen?category_id=GIFTS"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 317 27.160.0.0 - - [07/Jan 18:1
18 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01"Mozilla/4.0 (compatibl
147] "POST /category.screen?category_id=SURPRISE&JSESSIONID=SD9SL4FF4ADFF7 HTTP/1.1" 200 2423 "http://buttercup-sho
I-02"Opera/9.20 (Windows NT 6.0; U; en)" 564 130.253.37.97 - - [07/Jan 18:10:55:189] "GET /cart.do?action=changequ
FF6ADFF10 HTTP/1.1" 404 3860 "http://buttercupshopping.com/oldlink?item_id=EST-18"Opera/9.20 (Windows NT 6.0; U
SL8FF2ADFF9 HTTP/1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-6&product_id=AV-SB-0
gory?category_id=FLOWERS&JSESSIONID=SD8SLBFF1ADFF6 HTTP/1.1" 200 3971 "http://buttercup-shopping.com/cart.do?ac
53.37.97 - - [07/Jan 18:10:55:108] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD1SL9FF9ADFF9 HTTP/1.1" 40
; Windows NT 5.1)" 606 195.69.160.22 - - [07/Jan 18:10:54:192] "GET /cart.do?action=remove&itemId=EST-15&product_id=FI
t.do?action=remove&itemId=EST-15&product_id=AV-SB-02"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 163
SL9FF9ADFF1 HTTP/1.1" 200 1976 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-17&product_id=K9-CW
ko) Chrome/5.0.375.38 Safari/533.4" 544 86.9.190.90 - - [07/Jan 18:10:54:166] "POST /cart.do?action=addtocart&itemi
g.com/cart.do?action=addtocart&itemId=EST-7&product_id=FI-SW-01"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
&JSESSIONID=SD1SL1FF8ADFF2 HTTP/1.1" 200 408 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-27&pr
69 128.241.220.82 - - [07/Jan 18:10:54:145] "GET /cart.do?action=view&itemId=EST-13&product_id=RP-SN-01&JSESSIONID=SD
EST-13&product_id=RP-SN-01"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 393 130.253.37.97 - - [07/Jan
1" 406 1437 "http://buttercup-shopping.com/cart.do?action=addtocart&itemId=EST-27&product_id=AV-SB-02"Mozilla/5.0 (W
38 Safari/533.4" 571 141.146.8.66 - - [07/Jan 18:10:54:118] "GET /category.screen?category_id=SURPRISE&JSESSIONID=SD
id=SURPRISE"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 932 141.146.8.66 - - [07/Jan 18:10:53:104] "POST /
p-shopping.com/product.screen?product_id=AV-SB-02"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 210 130.253
FF2 HTTP/1.1" 200 1649 "http://buttercup-shopping.com/category.screen?category_id=TEDDY"Googlebot/2.1 (http://www
lebot/2.1 (http://www.googlebot.com/bot.html) " 302 125.17.14.100 - - [07/Jan 18:10:51:197] "POST /category.screen?
/category.screen?category_id=BOUQUETS"Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (K



Pour découvrir comment Frothy garde une longueur
d'avance sur les cybermenaces, rendez-vous sur
splunk.com/frothy