Phishing, Spear-phishing

Piratage Informatique, comment les hackers déjouent votre vigilance ?

Présenté par
Simon Vidogue| Solution Architect

VadeSecure
Predictive Email Defense

Qui sommes-nous ?

600 millions

de boites aux lettres protégées

Clients :

Accident Fund INSURANCE COMPANY OF AMERICA · Boys & Girls Clubs of Puerto Rico · Eakes office solutions · KVC Health Systems people matter · Dubuque Community Schools · Volkswagen · LADURÉE Paris · smartsheet

Partenaires :

Microsoft* · Cisco · mimecast · SONICWALL · INTERMEDIA · DreamHost · OVH.com

* One Commercial Partner (OCP) Program

Fournisseurs d'accès :

COMCAST · BT · orange · TELSTRA · vodafone · Spark NZ · eastlink · IIJ Internet Initiative Japan

Clients

COMCAST

Porcher industries

Domaines Barons de Rothschild Lafite

Groupama Asset Management

Paris Habitat OPH vivre ensemble la ville

Gironde Le Département gironde.fr

Nestlé

Bordeaux Métropole

Norauto

Région Aquitaine

Latécoère

Stelia Reliability. Performance.

msa santé famille retraite services

Council of Europe

Conseil de l'Europe

Le Mans Métropole Communauté urbaine

Centre Hospitalier Antibes Juan-les-Pins

Centre Hospitalier Blois Simone Veil

Nantes Métropole Communauté urbaine

Groupe Hospitalier du Havre

Sapeurs Pompiers Paris

Apec

Vade Secure for Office 365 Wins Prestigious Cybersecurity Awards

Vade Secure Office 365

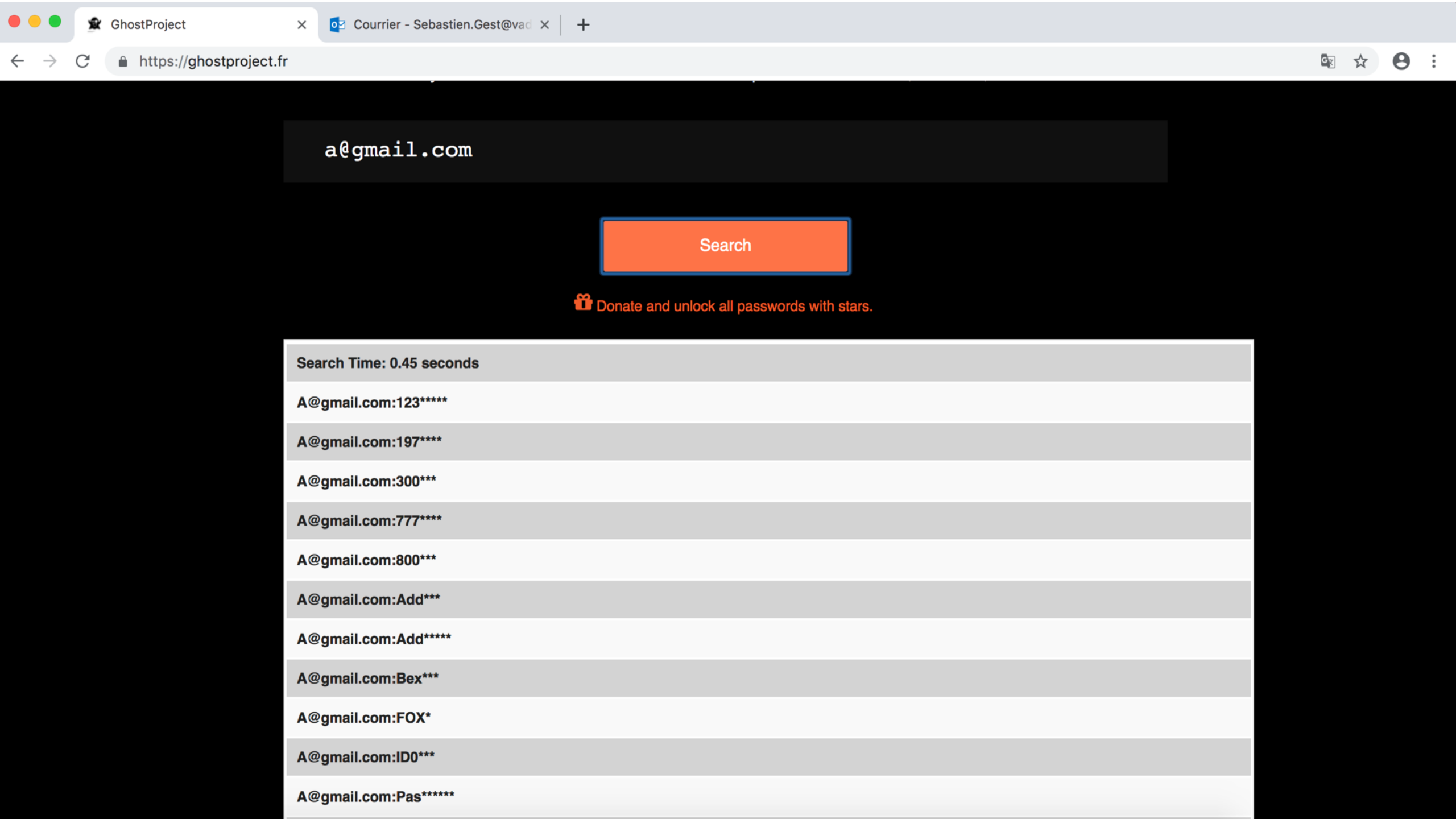
Les données de mes ami(e)s sont mes ….

LES DONNÉES DE 130 000 GENDARMES FRANÇAIS EXPOSÉES PAR UN PRESTATAIRE

Bastien L 3 septembre 2019 Sécurité Ecrire un commentaire

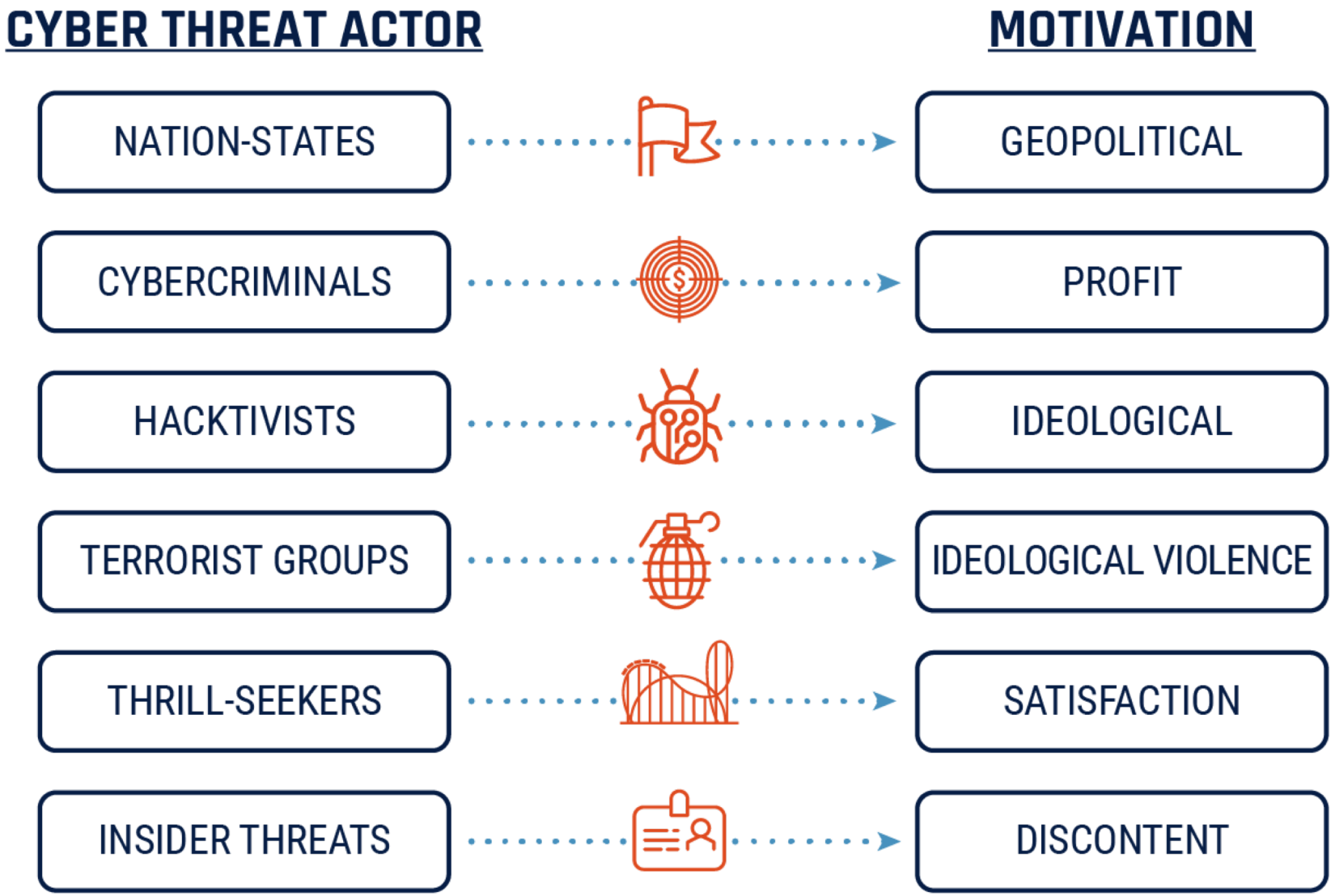
Yves Rocher : un prestataire provoque la fuite de données de 2,5 millions de clients

Bastien L 2 septembre 2019 Sécurité Ecrire un commentaire


GhostProject
Courrier - Sebastien.Gest@vad
https://ghostproject.fr
a@gmail.com
Search
Donate and unlock all passwords with stars.
Search Time: 0.45 seconds
A@gmail.com:123*****
A@gmail.com:197****
A@gmail.com:300***
A@gmail.com:777****
A@gmail.com:800***
A@gmail.com:Add***
A@gmail.com:Add*****
A@gmail.com:Bex***
A@gmail.com:FOX*
A@gmail.com:ID0***
A@gmail.com:Pas******

Woodie, Data everywhere!

Oubliez le hacker dans sa chambre.



Oubliez le hacker dans sa chambre.

Actualités ▸ Internet ▸ Divers

Les cyberattaques auraient rapporté 2 milliards de dollars à la Corée du Nord

Le mardi 06 Août 2019 à 15:10 par Jérôme G. | 9 commentaire(s)

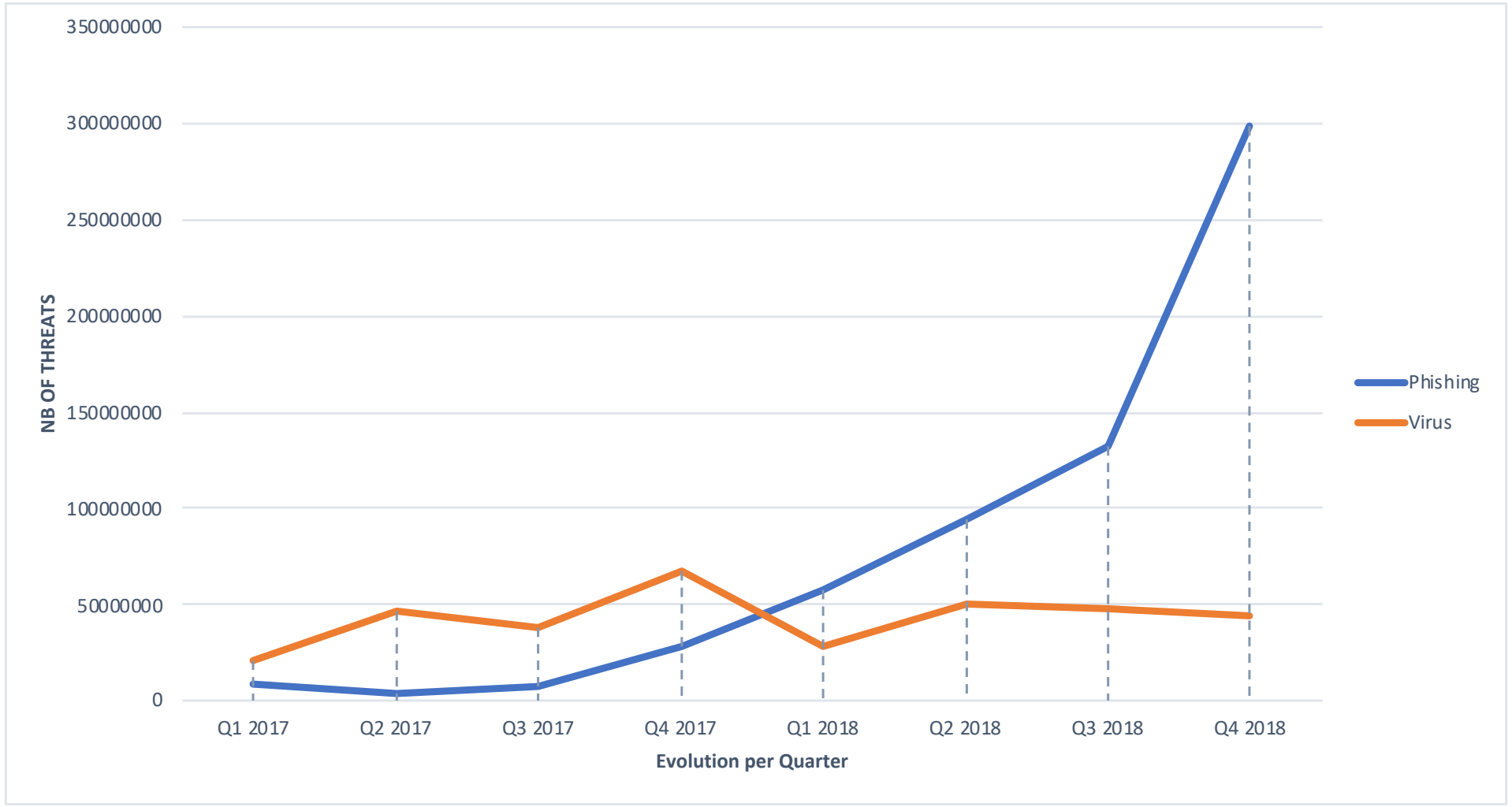
D'après un rapport des Nations unies, la Corée du Nord a financé ses programmes d'armement via des cyberattaques ayant visé des banques et des plateformes de cryptomonnaies.

Vade Secure
Predictive Email Defense

Focus sur l’email

RETOUR

Un changement de paradygme



“New Phishing Attack Targets 550M Email Users Worldwide”

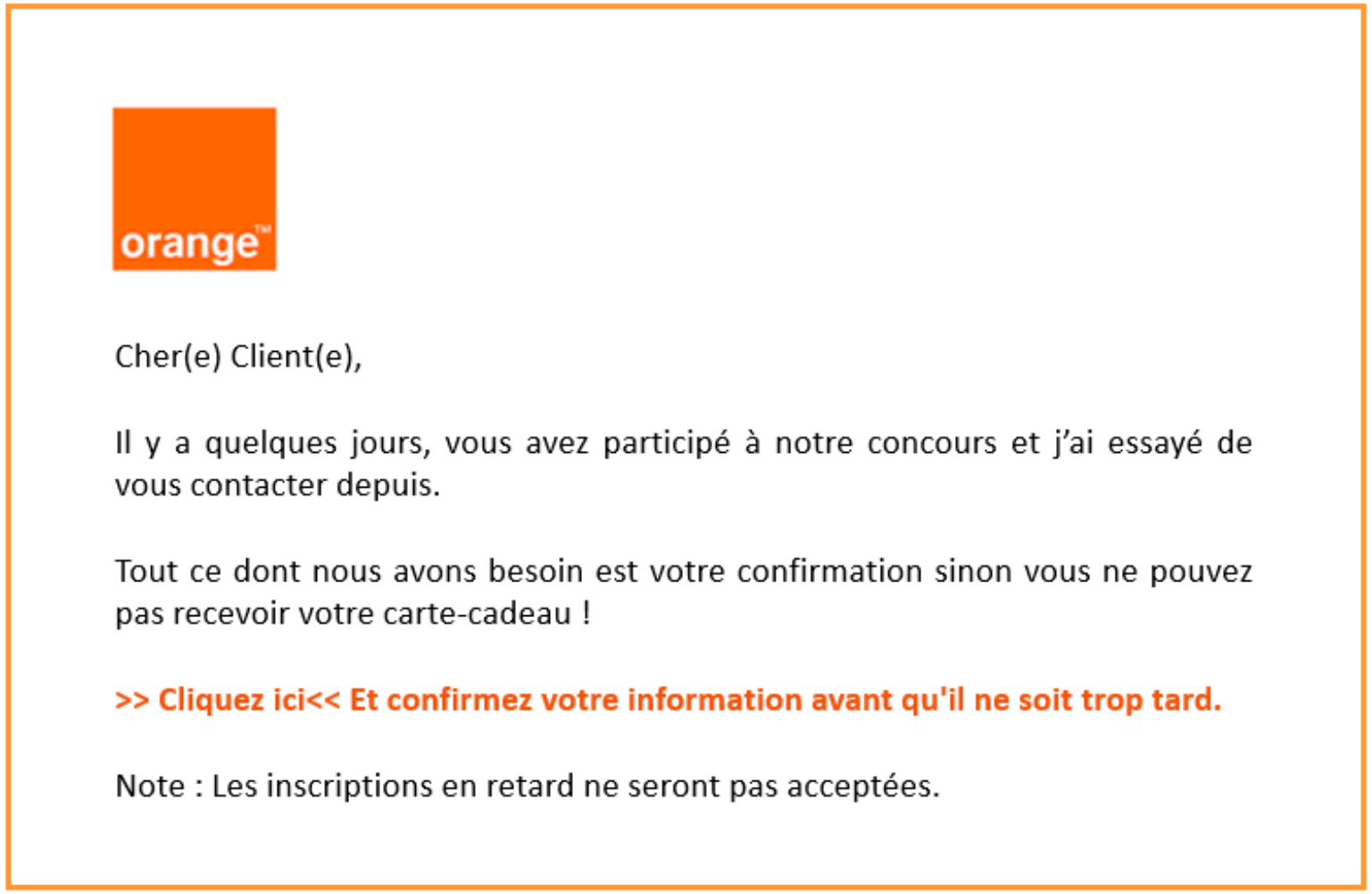
DARKReading

Vade Secure
Predictive Email Defense

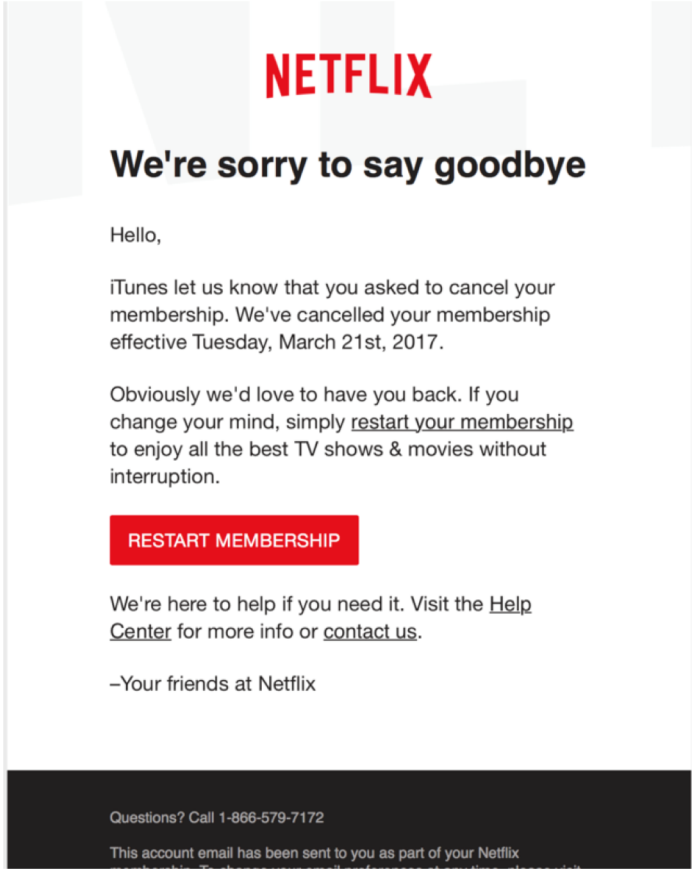
Le Phishing a évolué

RETOUR

A quoi ressemblent ces emails ?



A quoi ressemblent ces emails ?



NETFLIX

We're sorry to say goodbye

Hello,

iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we'd love to have you back. If you change your mind, simply restart your membership to enjoy all the best TV shows & movies without interruption.

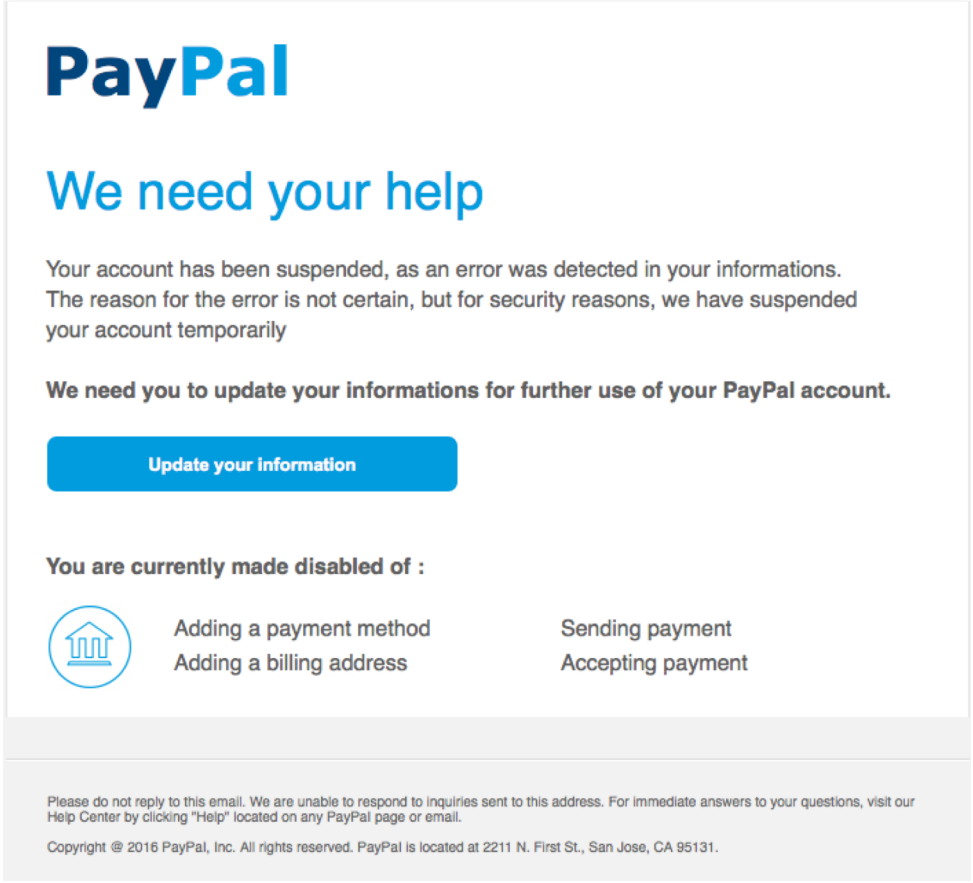
RESTART MEMBERSHIP

We're here to help if you need it. Visit the Help Center for more info or contact us.

–Your friends at Netflix

Questions? Call 1-866-579-7172

This account email has been sent to you as part of your Netflix



PayPal

We need your help

Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

Update your information

You are currently made disabled of :

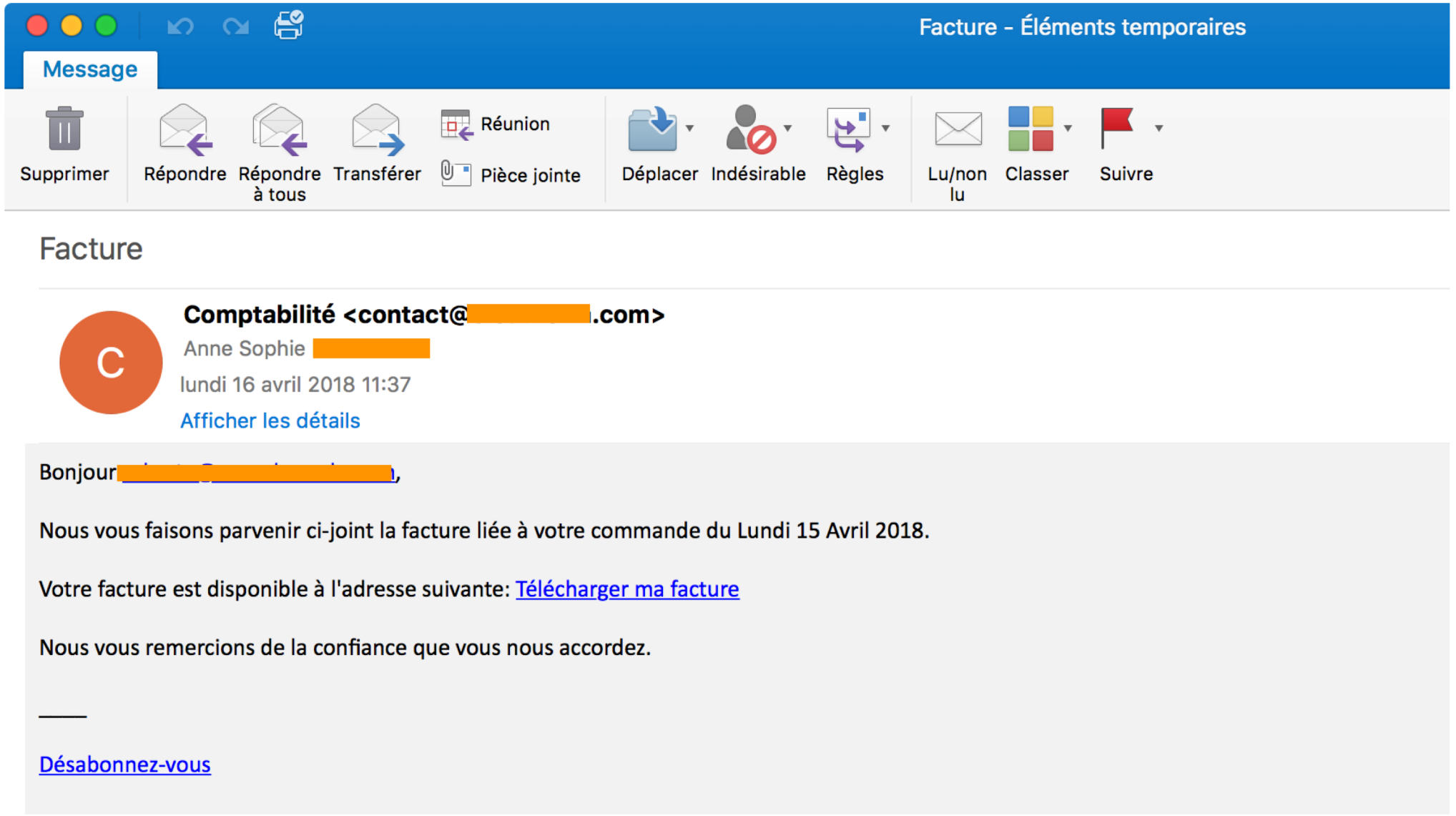
Adding a payment method
Adding a billing address
Sending payment
Accepting payment

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

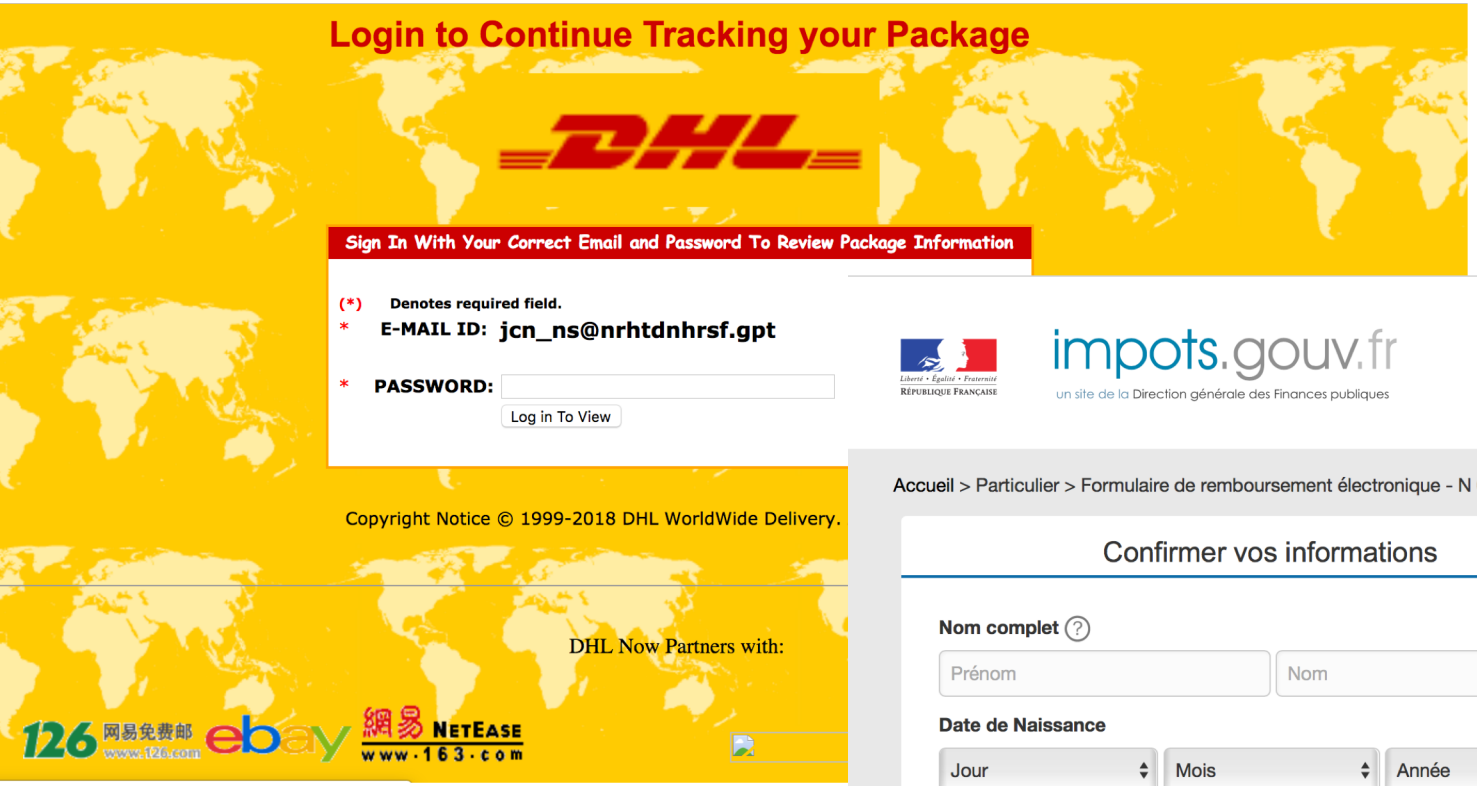
Copyright @ 2016 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

A quoi ressemblent ces emails ?

A quoi ressemblent ces emails ?



Des landing page réalistes



Cette attaque de phishing contournait les systèmes de vérification de la réputation des adresses IP

Serveurs de fournisseurs d'hébergement légitimes

Plus de 100 000 adresses IP

Machines sans antécédents suspects

Volume très faible envoyé depuis chaque machine/adresse IP de façon à se mêler au « bruit » ambiant d'Internet

RETOUR

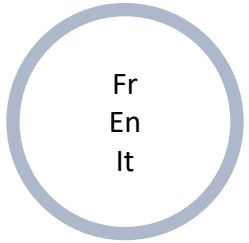
L'attaque de phishing a berné les utilisateurs

Outil de raccourcissement permettant de masquer la véritable URL

Les internautes sont habitués à voir des URLs classiques au format raccourci et estiment que le lien est sans danger.

Abus de liens de redirection officiels

Des hackers utilisent des noms de domaine légitimes pour faire croire aux internautes que le lien est authentique.



Pages Web localisées

Les hackers créent des pages qui paraissent légitimes.

Homoglyphes

En utilisant des caractères spéciaux, les hackers parviennent à utiliser des noms de domaine quasi identiques aux domaines authentiques.

RETOUR

Vade Secure
Predictive Email Defense

Spear Phishing (BEC)

RETOUR

Spear-Phishing: Le mode opératoire classique

1. Le pirate espionne Paul pour usurper l'identité d'un membre de son réseau: John

2. Le pirate utilise l'identité de John pour envoyer un email à Paul l'invitant à réaliser une action sensible

3. Paul agit selon les instructions de son correspondant qu'il pense être John

4. Le pirate a pénétré le réseau et peut maintenant effectuer les actions souhaitées

Vous avez reçu un e-mail de Georges, votre PDG

Répondre à tous | Supprimer Courrier indésirable | •••

Contrat Urgent

AF [redacted]

lun. 17/09, 16:04

[redacted]

Répondre à tous

Boîte de réception

Cher Directeur des finances
Pourriez-vous vous assurer que le montant du closing du contrat de Paris soit versé?
Pour rappel, les coordonnées bancaire ci-dessous:
IBAN FR[redacted] A12
Merci à vous
Georges
Président Directeur Général

RETOUR

Vous avez reçu un e-mail de Georges, votre PDG

Répondre à tous | Supprimer Courrier indésirable | •••

Contrat Urgent

AF [redacted]

lun. 17/09, 16:04

[redacted]

Répondre à tous

oîte de réception

Cher Directeur des finances
Pourriez-vous vous assurer que le montant du closing du contrat de Paris soit versé?
Pour rappel, les coordonnées bancaire ci-dessous:
IBAN FR[redacted] A12
Merci à vous
Georges
Président Directeur Général

RETOUR

Sauf qu'en réalité, il ne vient pas de Georges !

Les e-mails de spear phishing contournent les systèmes traditionnels

Utilisation visible d'un alias

Les hackers changent l'alias visible des comptes de messagerie pour tromper les systèmes qui ne vérifient que la correspondance exacte des domaines.

Domaines voisins

Les hackers utilisent des domaines voisins pour tromper les systèmes qui ne vérifient que la correspondance exacte des domaines.

Aucun contenu malveillant

Les hackers envoient des e-mails ponctuels ne contenant ni lien ni pièce jointe.

RETOUR

Spear-phishing : Il n’a jamais été aussi simple de mettre la pression sur un employé.

SECURITYWEEK NETWORK: Information Security News | Infosec Island | CISO Forum — Security Experts: WRITE FOR US

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CISO Forum 2018 | ICS Cyber Security Conference | Contact Us

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture | Security Strategy | IoT Security | SCADA / ICS

Home › Fraud & Identity Theft

YouPorn Users Warned to Change Passwords After Data Leak

By Brian Prince on February 23, 2012

Share | G+ | Tweet | Recommend 0 | RSS

It hasn’t been the greatest couple of weeks for the Internet porn industry.

Last week, a hacker claimed to have stolen personal information belonging to 350,000 users from the hardcore porn company Brazzers. On Wednesday, The H **reported** the user database of videosz.com porn portal was publicly available on the Internet, exposing hundreds of thousands of data records of customers and affiliate partners, including credit card details and password information.

Now it seems thousands of YouPorn users may have had their password information compromised due to a programmer of the YP Chat service leaving log information publicly available on the Internet. Though YP Chat is not owned or run by YouPorn, the situation touched off concerns because many users may use the same password for both the site and the service.

Google™ Custom Search — Search

SECURITYWEEK DAILY BRIEFING

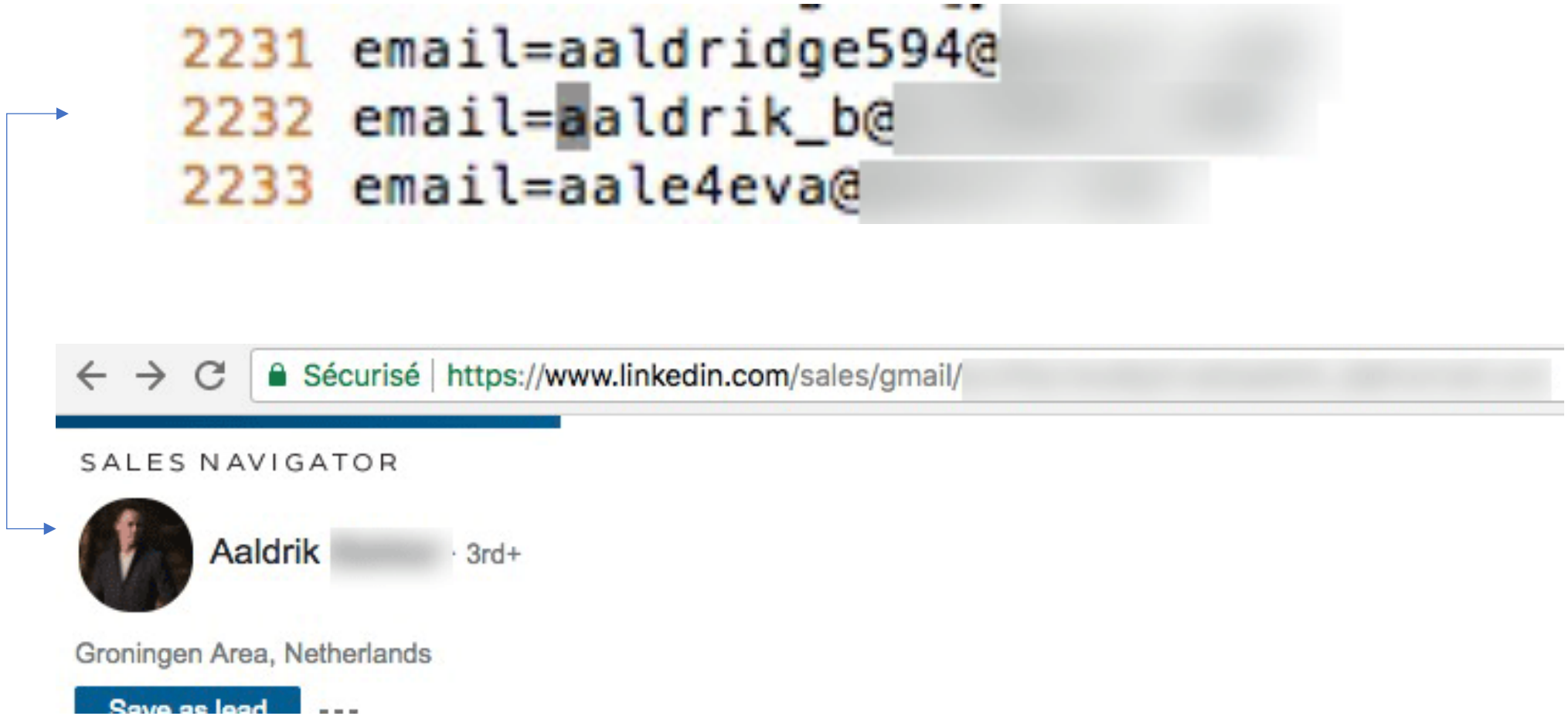
BRIEFING

Business Email Address — SUBSCRIBE

Most Recent | Most Read

- Chrome 66 Distrusts Older Symantec Certificates
- Rockwell Automation Switches Exposed to Attacks by Cisco IOS Flaws
- Few RSA Conference Exhibitors Implemented DMARC
- The Kiss of Death for Passwords: Machine Learning?

Spear-phishing : grâce au « social engineering »



Le spear-phishing est un mécanisme des FOVI

Le Cottage social des Flandres à Dunkerque a été victime d'une arnaque aux faux ordres de virements. Près de 10 millions d'euros ont été détournés au profit d'un compte situé en Slovaquie. Le bailleur social a porté plainte.

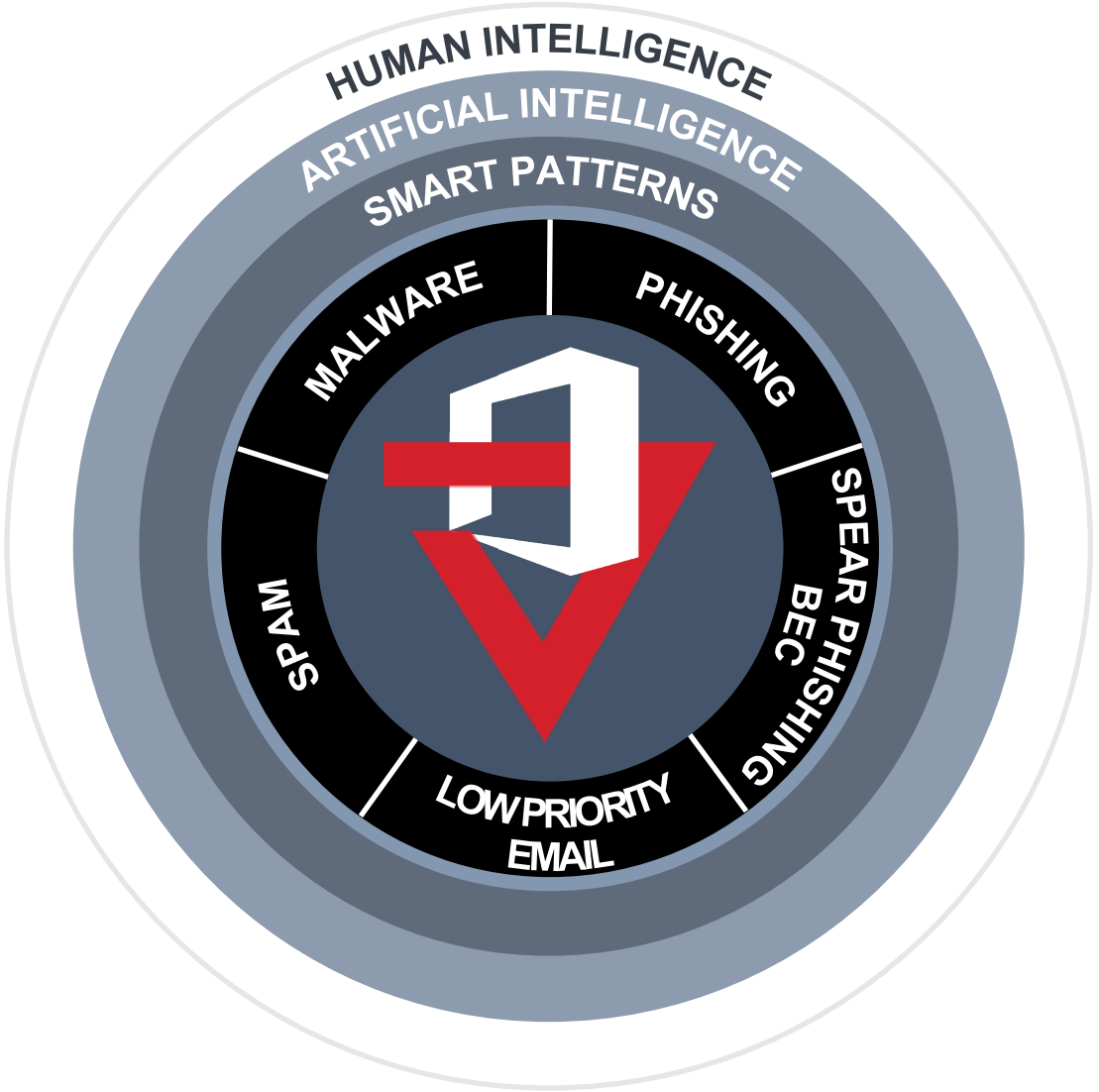
Le spear-phishing est un mécanisme des FOVI

VOLS ET CAMBRIOLAGES

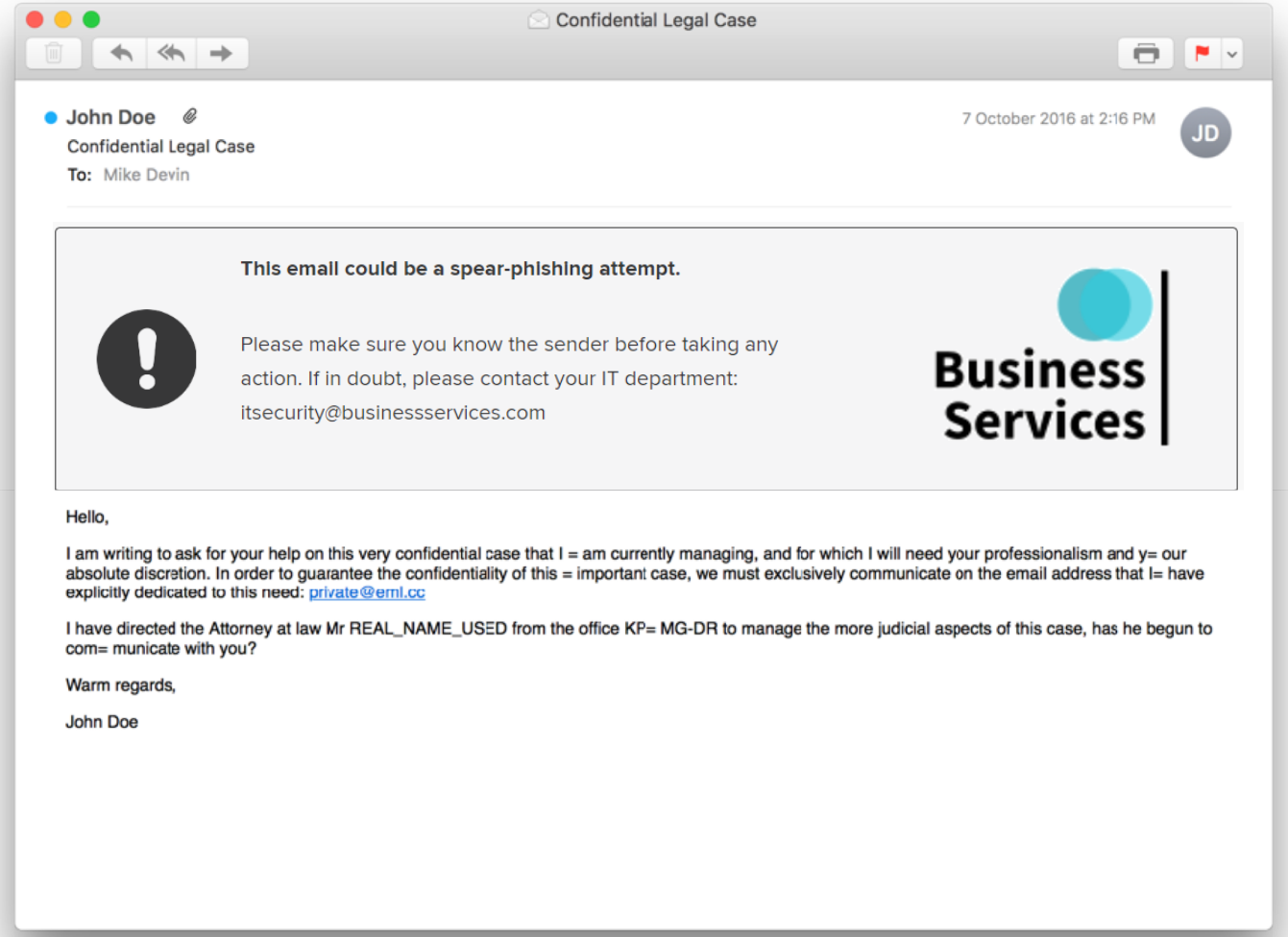
Une grande surface d'Orthez victime d'une "fraude au président" pour 180000 €


vevo

Protection à 360° contre toutes les menaces liées aux emails



Alertes entièrement personnalisables au sein des messages



RETOUR

Qui a la première question ?

Présenté par
Simon Vidogue| Solution Architect

VadeSecure
Predictive Email Defense