IPCyb

Agence d'Information et de Protection du cyberespace

3 rue de Robien
35000 RENNES

WWW.IPCYB.COM
INFO@IPCYB.COM
+33 756 833 878

Régis Le Guennec

CEO

regis@ipcyb.com

@regisleguennec

2018

What's in an internet minute? According to data from RiskIQ and threat researchers around the world, a lot of evil.

2018 COST OF CYBER CRIME

TOTAL COST

$600 BILLION[1]

$1,138,888/minute

$171,233/minute spend by business on information security[2]

Global, the cost of cybercrime on large business ranged from **11.7 MILLION**/year[3]

Ranging from **$222**/minute

CYBERCRIME VICTIMS

2.7 MILLION/day[4]

1,861/minute

RANSOMWARE

costs to organizations

$8 BILLION/day[5]

$15,221/minute[5]

1.5 organizations/minute fall victim to ransomware attacks[6]

MALWARE

1,274 new malware variants/minute[7]

PHISHING EMAILS

22.9 attacks/minute[8]

RECORDS LEAKED

from publicly disclosed incidents

2.9 BILLION/day[9]

5,518/minute

3 familles

- **Attaque directe**
brute force, SQL/XSS, MItM, DNS

- **Attaque indirecte**
phishing, scam, président, faux virus

- **Attaque de proximité**
Epaule, tableau, postit, électromagnétique, zoom camera, piégeage de poste, amplification radio,

Panorama des menaces

- **Vol,** perte, disparition
- **Extorsion,**
- **Espionnage & écoute**
- Destruction & sabotage
- Détournement & modification
- Piégeage & déstabilisation
- Manipulation & influence

- Atteinte physique
- **Saturation** & dégradation
- **Interruption** & coupure
- **Divulgation** & diffusion
- Incendie
- Crue
- Ouragan

Attaque de masse

La plus large possible

Attaque ciblée

Complexe, préparée à l'avance

La sécurité informatique vise généralement

3 principaux objectifs

Confidentialité

Intégrité

Disponibilité

Patrimoine informationnel

Toute société qui veut se maintenir doit déployer une stratégie visant à assurer sa survie (et si possible son développement), elle doit notamment être vigilante à

- Préserver son image de marque
- Garder secret son savoir faire
- Assurer les prestations pour ses clients selon les contrats
- Assurer sa compétitivité
- Protéger ses données sensibles
- Assurer la continuité de son activité métier

Se déclare en faillite le 14 janvier 2009

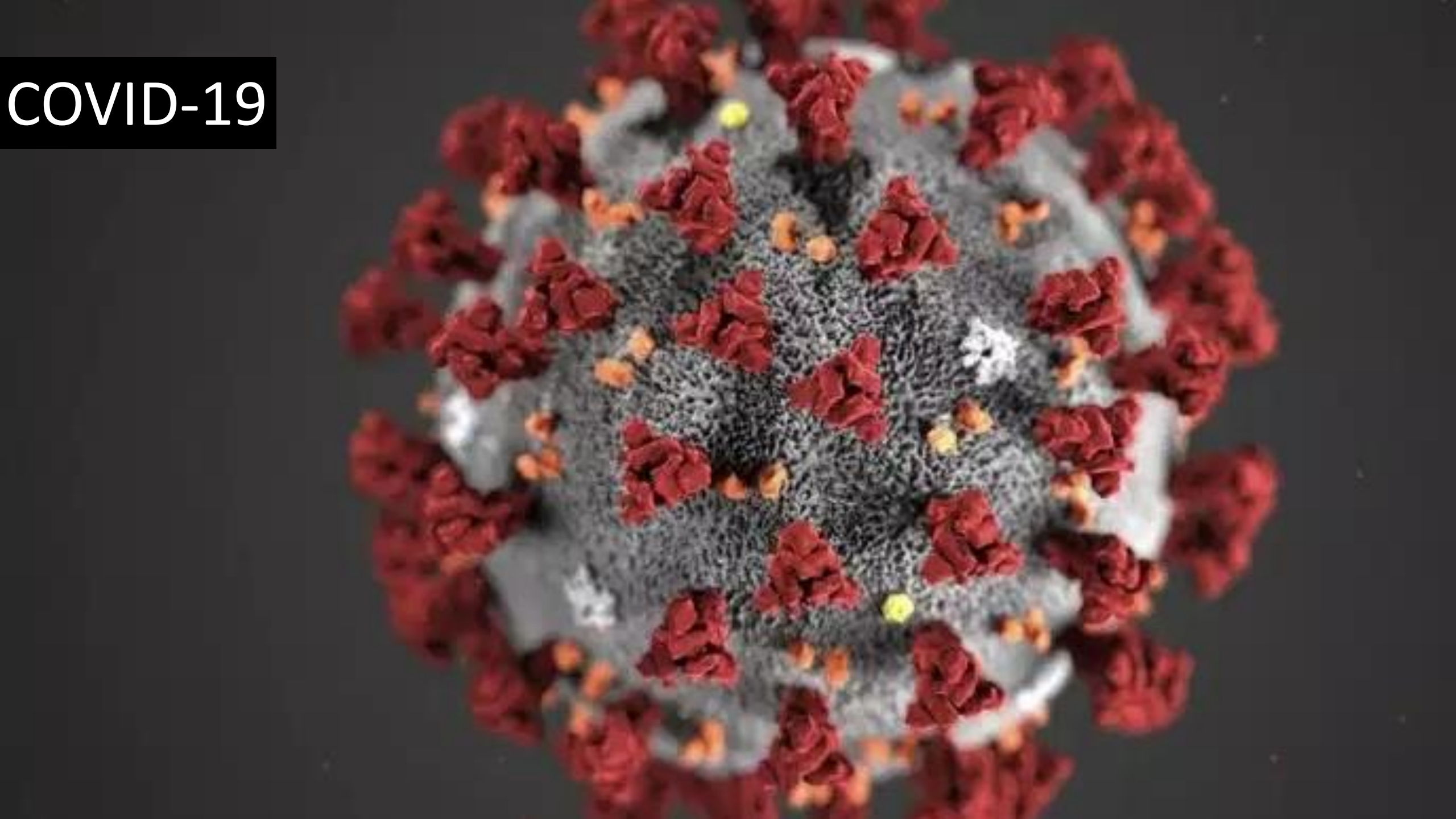
Préjudices/impacts

- L’atteinte à l’image de l’entreprise
- La perte de commande, de clientèle
- La concurrence déloyale et parasitaire
- La perte financière/économique
- Psychologique sur les collaborateurs
- Juridique & pénal

Vecteurs de menaces

- **Concurrent,**
- **Etat,**
- Service d'espionnage (NSA,..)
- Hacktiviste (Anonymous, ...)
- Collaborateur,
- Stagiaire,
- Groupe APT28,
- **Script kiddies,**
- Administrateur,
- Fournisseur,
- Co-traitant,
- Client,
- Hébergeur,
- FAI,
- **Maladie,**
- Electricité,
- Rivière,
- Feu,
- Vent
- ...

COVID-19



Statistics

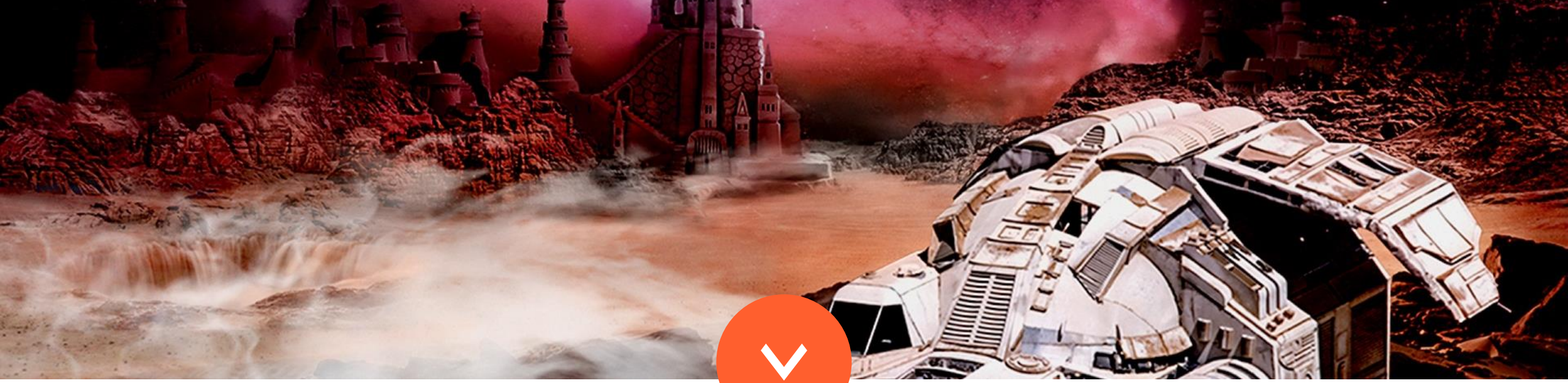
	Count	Online	Offline	Offline more than 2 days	Installed today
	31	0	31	21	5
	98	11	87	71	24
	1	0	1	1	0
	4	1	3	3	1
	70	1	69	61	8
	11	0	11	10	1
	20	1	19	11	9
	1	1	0	0	1
	5	1	4	0	4
	1	0	1	1	0
	1	0	1	1	0
	1	0	1	0	1
Total	258	16	242	189	57

Nomadisme numérique

Le nomadisme numérique désigne toute forme d'utilisation des technologies de l'information **permettant à un utilisateur d'accéder au SI de son entité** d'appartenance ou d'emploi, depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité.

FORCE BRUTE

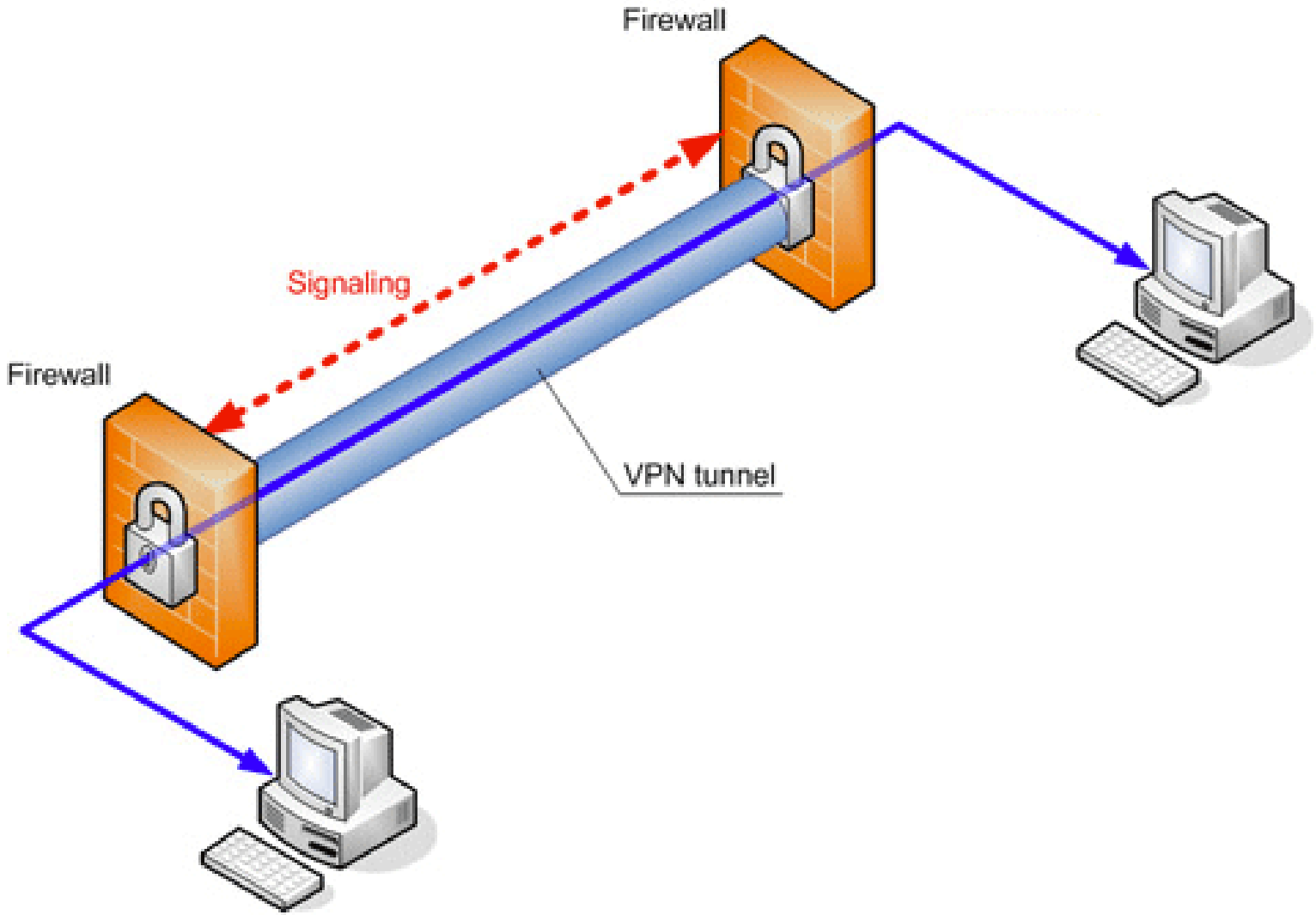
1 400 000 bruteforce RDP par jour



BYOD

BYOD, abréviation de l'anglais « Bring Your Own Device », en français, PAP pour « prenez vos appareils personnels » ou AVEC pour « apportez votre équipement personnel de communication », est une pratique qui consiste à **utiliser ses équipements personnels dans un contexte professionnel.**

VIRTUAL PRIVATE NETWORK



https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/

PHISHING

L’hameçonnage, phishing ou filoutage
est une **technique utilisée** par des fraudeurs pour
obtenir des renseignements personnels
dans le but de perpétrer une **usurpation d'identité**.

SPEAR PHISHING

Taux d’ouverture de 70 %, contre 3 % pour une campagne de scam de masse

Sujet : **Notification d'impôt**
De : République Française <lettre-info-fiscale@dgfip.finances.gouv.fr>
Date : 8:11
Pour : pc@eila.univ-paris-diderot.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DIRECTION GENERALE DES FINANCES PUBLIQUES 20/10/2009

Notification d'impôt - Remboursement

Après les derniers calculs annuels de l'exercice de votre activité, nous avons déterminé que vous êtes admissible à recevoir un remboursement d'impôt de € 178,80.

S'il vous plaît soumettre la demande de remboursement d'impôt et nous permettre de 10 jours ouvrables pour le traitement.

Pour accéder au formulaire pour votre remboursement d'impôt, cliquez ici

Un remboursement peut être retardé pour diverses raisons. Par exemple la soumission des dossiers non valides ou inscrivez après la date limite.

Le Conciliateur fiscal adjoint

Philippe BERGER

http://www.capitalhouse.com.mx/.secure/

https://leboncoln.fr/promo/

ZATAZ.com DataSecurityBreach.fr zataz.tv Damienbancal.fr Q S MG S TweetDeck ANY.RUN T TW D M MJ Emoji Saucisse Aligo

leboncoin ACCUEIL DÉPOSER UNE ANNONCE OFFRES DEMANDES MES FAVORIS BOUTIQUES Se connecter

Trouvez la bonne affaire parmi 27 776 142 petites annonces sur leboncoin.

Déposer une annonce

Rechercher autour de moi

Alsace
Aquitaine
Auvergne
Basse-Normandie
Bourgogne
Bretagne
Centre
Champagne-Ardenne
Corse
Franche-Comte
Haute-Normandie
Ile-de-France
Languedoc-Roussillon
Limousin
Lorraine
Midi-Pyrenees
Nord-Pas-de-Calais
Pays de la Loire
Picardie
Poitou-Charentes
Provence-Alpes-Cote d'Azur
Rhone-Alpes

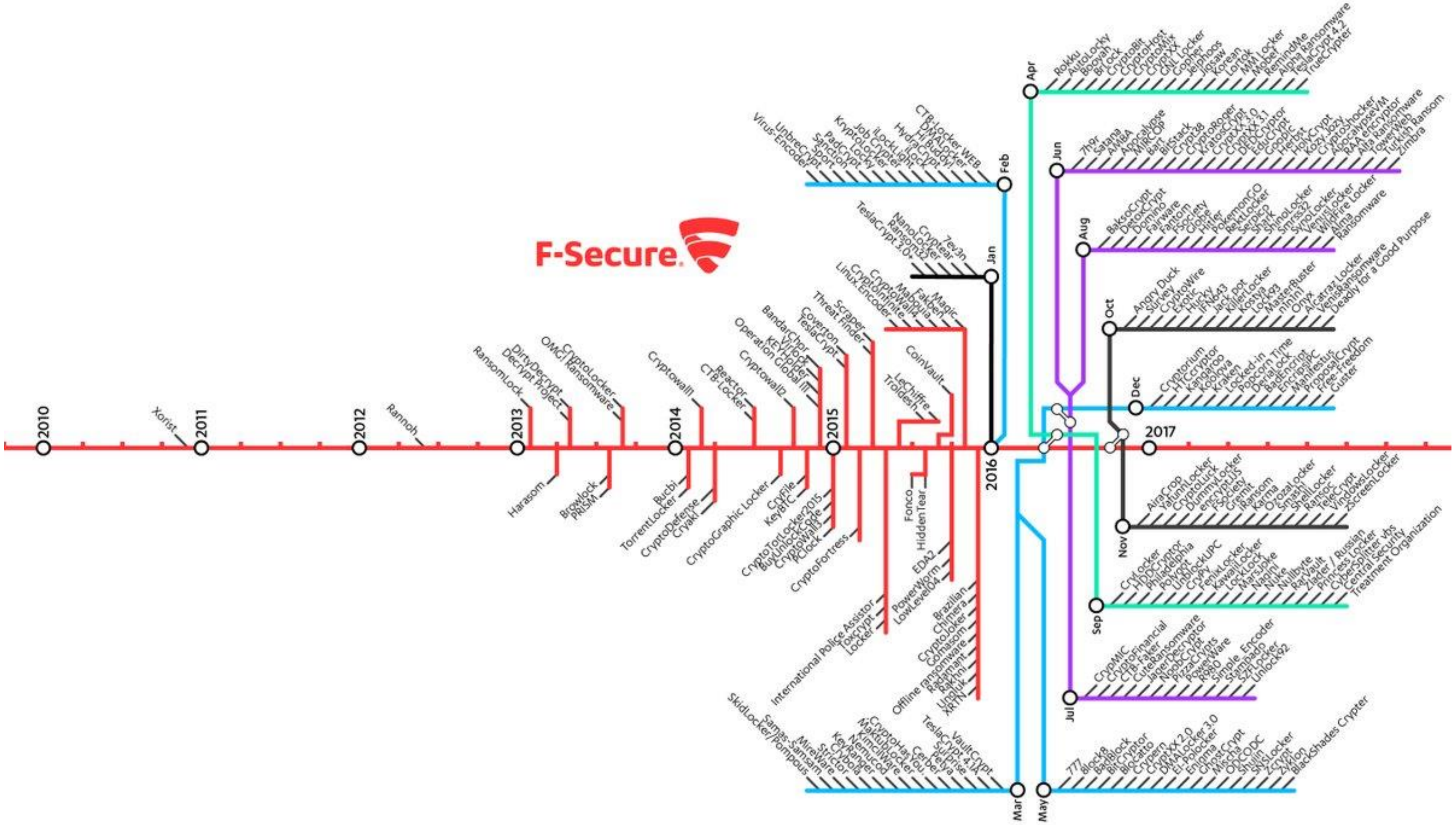
Guadeloupe
Martinique
Guyane
Reunion

Sur le site leboncoin.fr, passez des annonces gratuites et sans commission. Vous pouvez consulter des petites annonces de particuliers et de professionnels partout en France, que vous cherchiez des annonces immobilières, des voitures d'occasion, des offres d'emploi, des meubles, du matériel électronique ou tout autre type de produits d'occasion. 92829

EMPLOI VACANCES MULTIMEDIA MATERIEL PROFESSIONNEL

RANSOMWARE

« Le but est d’extorquer de l’argent à l’utilisateur »



F-Secure
2010
2011
2012
2013
2014
2015
2016
2017
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Xorist
Rannoh
RansomLock
DirtyDecrypt
Decrypt Project
OMG! Ransomware
CryptoLocker
Harasom
Browlock
PRISM
Cryptowall
Reactor
CTB-Locker
Cryptowall2
Bucbi
TorrentLocker
CryptoDefense
Cryaki
CryptoGraphic Locker
CryFile
KeyBTC
CryptoTorLocker2015
BuyUnlockCode
CryptoWall3
PClock
CryptoFortress
BandarChor
Virlock
KEYHolder
Operation Global III
Coverton
TeslaCrypt
Threat Finder
Scraper
Linux.Encoder
CryptoWall4
CryptoApp
Mabouia
Fakben
Magic
CoinVault
LeChiffre
Troldesh
Fonco
HiddenTear
EDA2
PowerWorm
LowLevel04
International Police Assistor
Toxcrypt
Locker
Brazilian
Chimera
CryptoJoker
Gomasom
Offline ransomware
Radamant
Rakhni
Unlock
XRTN
TeslaCrypt 3.0+
Ransom32
NanoLocker
Cryptear
7ev3n
Virus-Encoder
UmbreCrypt
Sport
Sanction
PadCrypt
KryptoLocker
Job Crypter
iLock
HydraCrypt
Hi Buddy!
DMALocker
CTB-Locker WEB
SkidLocker/Pompous
Samas-Samsam
MireWare
Strictor
Cryptobola
Kenger
Nemucod
Maktub Locker
CryptoHasYou.
Cerber
TeslaCrypt 4.1A
Petya
Surprise
VaultCrypt
Rokku
AutoLocky
Booyah
BrLock
CryptoBit
CryptoHost
CryptoMix
CryptXXX
Coverton
Gopher
Jeiphoos
Jigsaw
Korean
Lortok
MM Locker
Mobef
RemindMe
Alpha Ransomware
TeslaCrypt 4.2
TrueCrypter
777
Blocker
BadBlock
BitCryptor
Blocatto
Crypren
CryptXXX 2.0
DMALocker 3.0
El-Polocker
Enigma
GhostCrypt
Mischa
ODCODC
Shujin
SNSLocker
Zcrypt
Zyklon
BlackShades Crypter
7h9r
Satana
AMBA
Apocalypse
MIRCOP
Bart
BitStack
Crypto28
CryptoRoger
KratosCrypt
CryptXXX 3.0
CryptXXX 3.1
DEDCryptor
EduCrypt
Goopic
Herbst
HolyCrypt
Kozy.Jozy
CryptoShocker
ApocalypseVM
RAA encryptor
Alfa Ransomware
TowerWeb
Turkish Ransom
Zimbra
CrypMIC
CryptoFinancial
CTB-Faker
CuteRansomware
JagerDecryptor
NoobCrypt
PizzaCrypts
PowerWare
R980
Simple_Encoder
Stampado
ZLocker
Unlock92
BaksoCrypt
DetoxCrypt
Domino
Fairware
Fantom
FSociety
Globe
Hitler
PokemonGO
RektLocker
Serpico
Shark
ShinoLocker
Smrss32
SyncLocker
VenusLocker
Wildfire Locker
Alma Ransomware
CryLocker
HDDCryptor
Philadelphia
Polyglot
UnlockUPC
Cry
FenixLocker
KawaiiLocker
LockLock
MarsJoke
Nagini
Nuke
Nullbyte
RarVault
Zlader / Russian
Princess Locker
CyberSplitter vbs
Central Security
Treatment Organization
Angry Duck
Survey
CryptoWire
Exotic
Flucky
HCrypt
iRansom
Jack.Pot
KillerLocker
Kostya
Lock93
MasterBuster
nin1n1
Onyx
Alcatraz Locker
VenisRansomware
Deadly for a Good Purpose
AiraCrop
YafunnLocker
CryptoLuck
DummyLocker
encryptJJS
FSociety
Gremit
iRansom
Karma
OzozaLocker
Smash!
ShellLocker
Ransoc
TeleCrypt
VindowsLocker
ZScreenLocker
Cryptorium
HTCryptor
Kangaroo
Koolova
Kraken
Locked-In
Popcorn Time
DeriaLock
BadEncript
EncryptJPC
Manifestus
ProposalCrypt
Free-Freedom
Guster


Wana Decrypt0r 2.0
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49
Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


ABUS 6,31
ROBIN
TÔLERIE INDUSTRIELLE - DÉCOUPE LASER

Cyber attack on Hydro

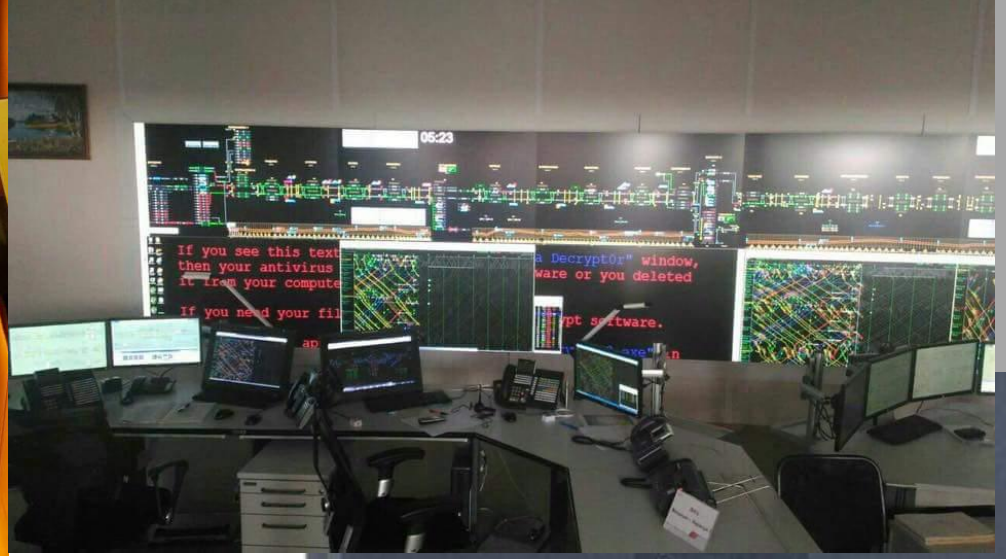
Hydro was the target of a serious cyber-attack on March 19. We are providing updates on the situation regularly.

«You hacked, ALL Data Encrypted»

Hollywood Presbyterian Medical Center de Los Angeles

WannaCry


Abfahrt
Linie
Ziel
Gleis
Nach
Gleis
Zeit
Über
22:10 RB81 Flöha - Pockau-Lengefeld Olbernhau 8
22:30 RB30 Flöha - Fre Hbf 11
Hohenstein (S) Hbf 10
22:31 RB30 Flöha - Zsc g-B. Süd 8
22:36 RB80 9
22:36 RB45 Geithain - B Hbf 5
22:44 RE6 Einsiedel - Thalheim (Erzgeb) Aue (Sachs) 14
22:45 RB89 Flöha - Freiberg (Sachs) - Tharandt Dresden Hbf 11
23:30
Fährt heute von Gleis 11
BMG | MIS


05:23
If you see this text
then your antivirus
If you need your fil
a Decryptor" window,
ware or you deleted
pt software.


Desigual


Ooops, your important files are
u see this text, but don't see the "Wan
your antivirus removed the decrypt soft
om your computer.
u need your files you have to run the d
find an application file named "@Wanna
older or restore from the antivirus qua
Bhumibol Adulyadej


Telefonica


RENAULT
La vie, avec passion


NHS
choices
www.nhs.uk


KPMG


PT
PORTUGAL
TELECOM


China National
Petroleum Corporation


HITACHI
Inspire the Next

IBERDROLA


MEGAFON

SHAHEEN AIR


UNIVERSITÀ DEGLI STUDI DI MILANO
BICOCCA

СБЕРБАНК
Всегда рядом

Mardi 27 juin 2017

me doc

APRIL 14, 2017
01.175-10.01.176 version of MeDoc is released with a backdoor.

MAY 15, 2017
01.180-10.01.181 version of MeDoc is released with a backdoor.

JUNE 22, 2017.
01.188-10.01.189 version of MeDoc is released with a backdoor

JUNE 27TH, 2017

8:59:14 UTC
Malicious actor used stolen credentials and "su" to obtain root privileges on the update server.

BETWEEN 9:11:59 UTC AND 9:14:58 UTC
The actor modifies the web server configuration to proxy to an OVH server.

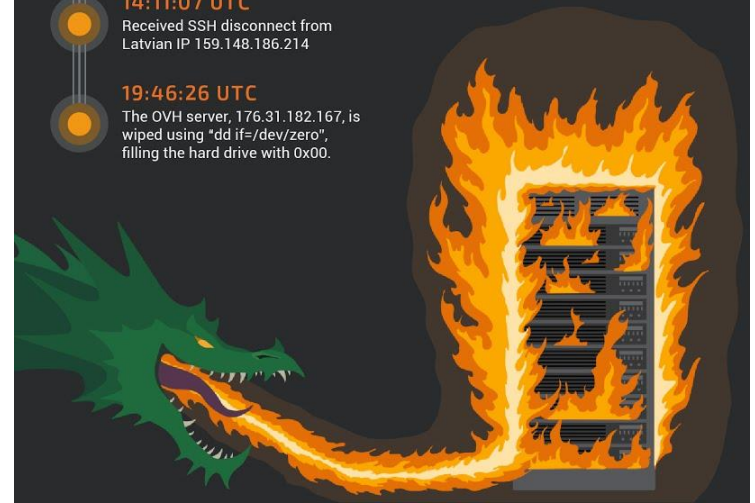
9:14:58 UTC
Logs confirm proxied traffic to OVH.

12:31:12 UTC
The last confirmed proxy connection to OVH is observed. This marks the end of the active infection period.

12:33:00 UTC
The original server configuration is restored.

14:11:07 UTC
Received SSH disconnect from Latvian IP 159.148.186.214

19:46:26 UTC
The OVH server, 176.31.182.167, is wiped using "dd if=/dev/zero", filling the hard drive with 0x00.




NotPetya : 300 millions de dollars
MAERSK LINE

NEED HELP unlocking your digital life without paying your attackers*?

YES NO

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

GOOD NEWS

Prevention is possible. Following simple cyber security advice can help you to avoid becoming a victim of ransomware.

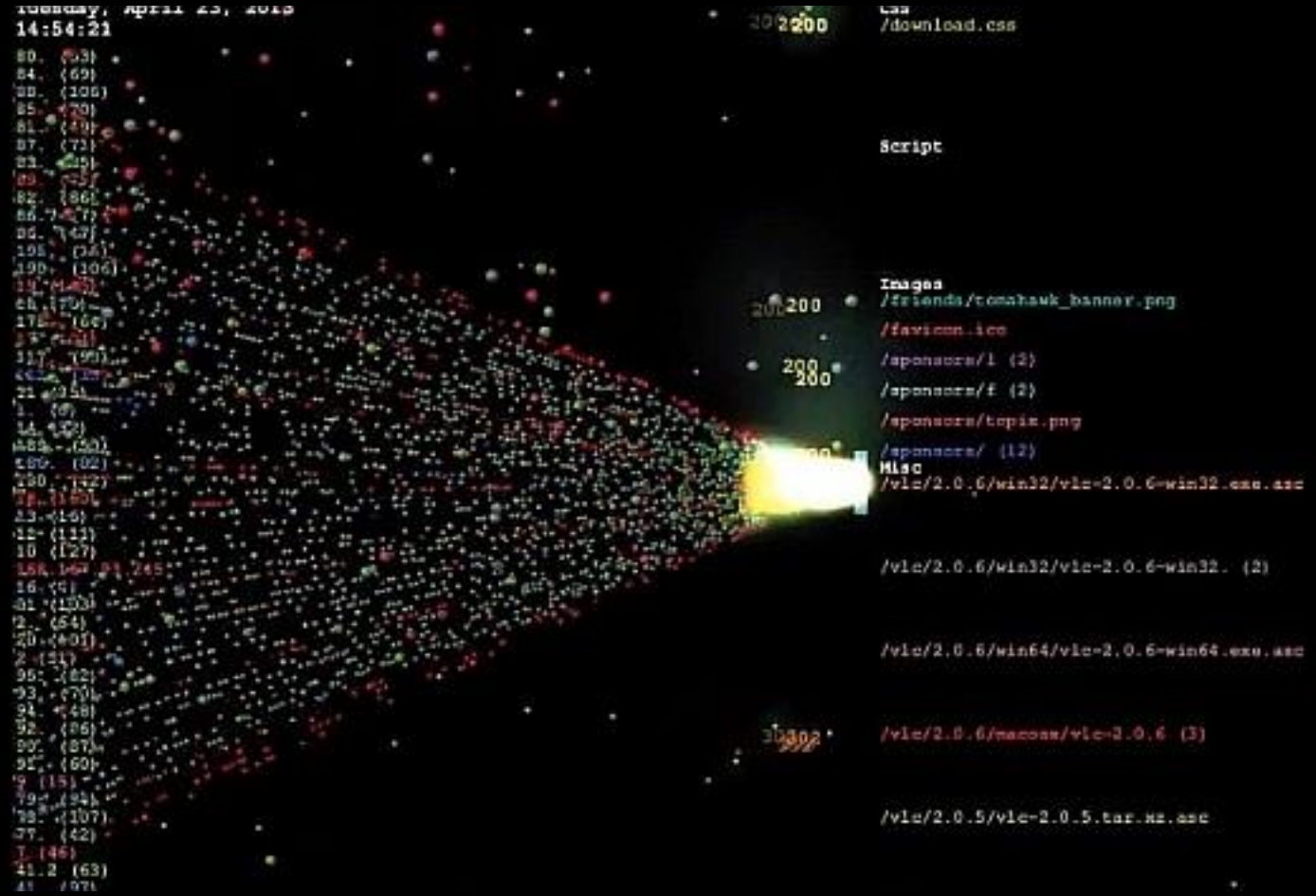
BAD NEWS

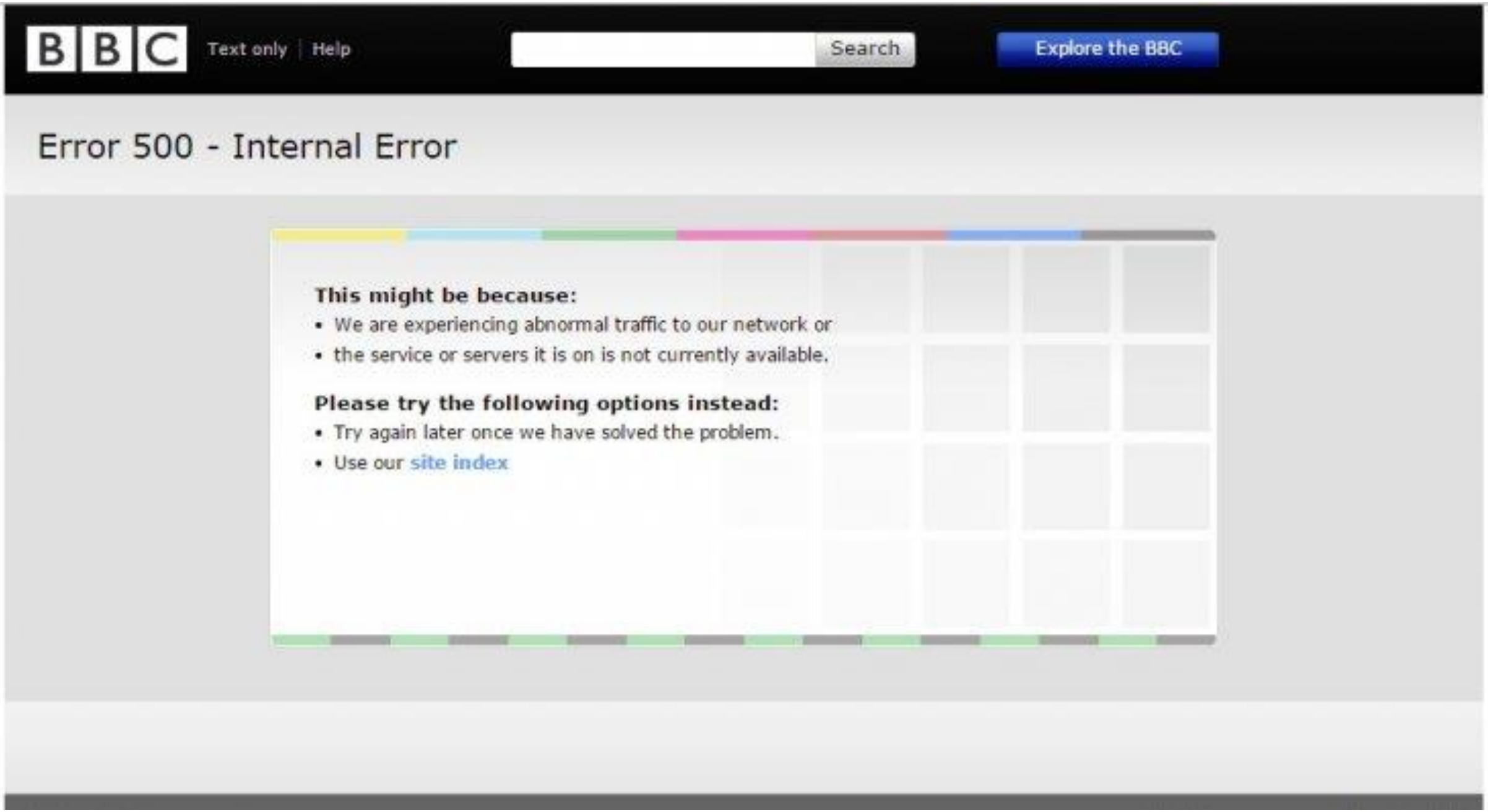
Unfortunately, in many cases, once the ransomware has been released into your device there is little you can do unless you have a backup or security software in place.

GOOD NEWS

Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay. We have created a repository of keys and applications that can decrypt data locked by different types of ransomware.

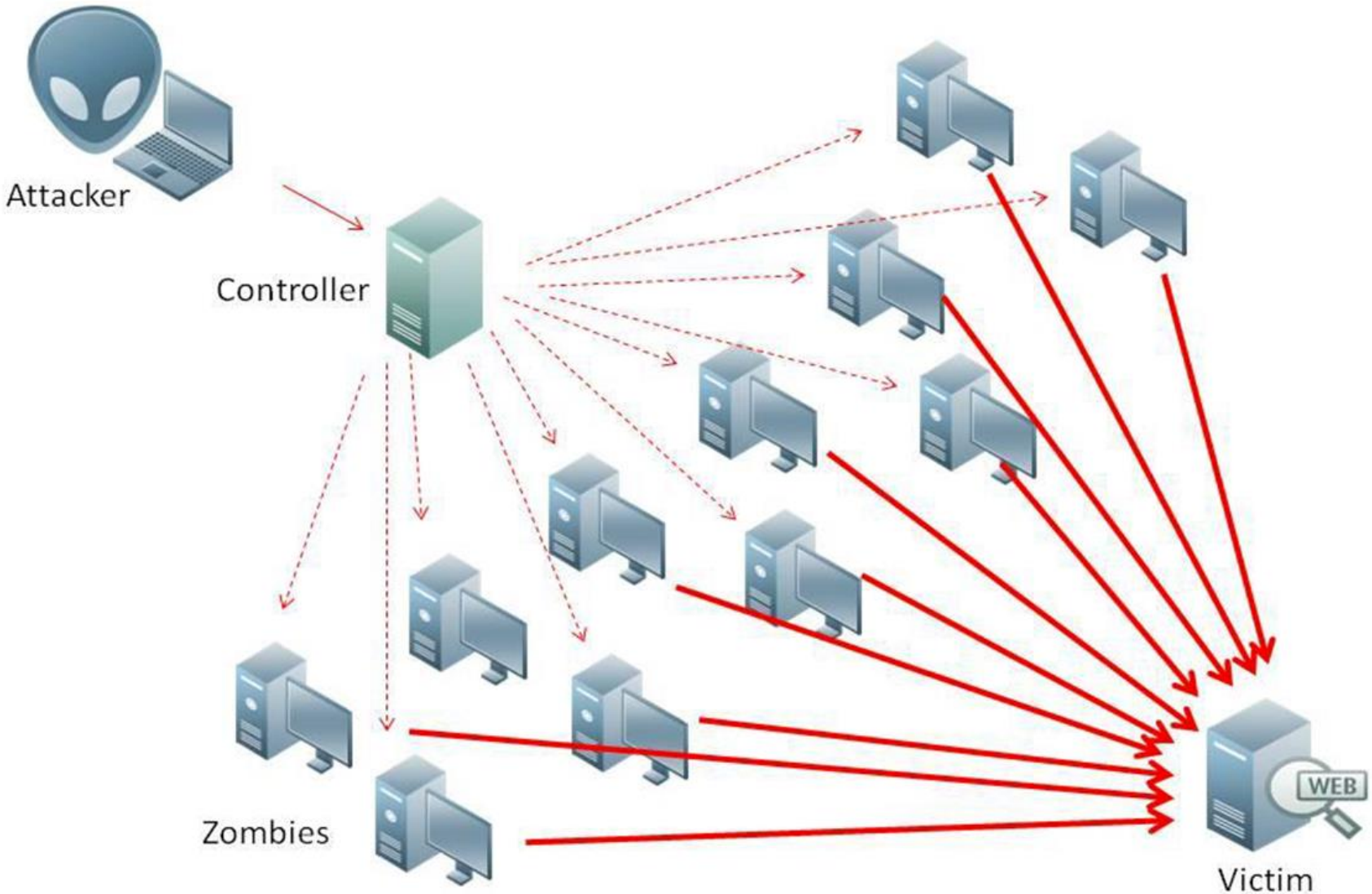
Distributed Denial-Of-Service




BBC
Text only
Help
Search
Explore the BBC
Error 500 - Internal Error
This might be because:
• We are experiencing abnormal traffic to our network or
• the service or servers it is on is not currently available.
Please try the following options instead:
• Try again later once we have solved the problem.
• Use our site index

BOTNET

Acronyme de Bot (Robot) et Net (Réseau)


Attacker
Controller
Zombies
WEB
Victim

PLANS

Plan length and concurrents are fully customizable when purchasing.

PLAN 1

$5/mo

1 Concurrent Attack

300 Second Attack Time

PURCHASE

PLAN 2

$10/mo

1 Concurrent Attack

600 Second Attack Time

PURCHASE

PLAN 3

$15/mo

1 Concurrent Attack

1200 Second Attack Time

PURCHASE

PLAN 4

$25/mo

1 Concurrent Attack

3600 Second Attack Time

PURCHASE

PLAN 5

$45/mo

1 Concurrent Attack

7200 Second Attack Time

PURCHASE

PLAN 6

$60/mo

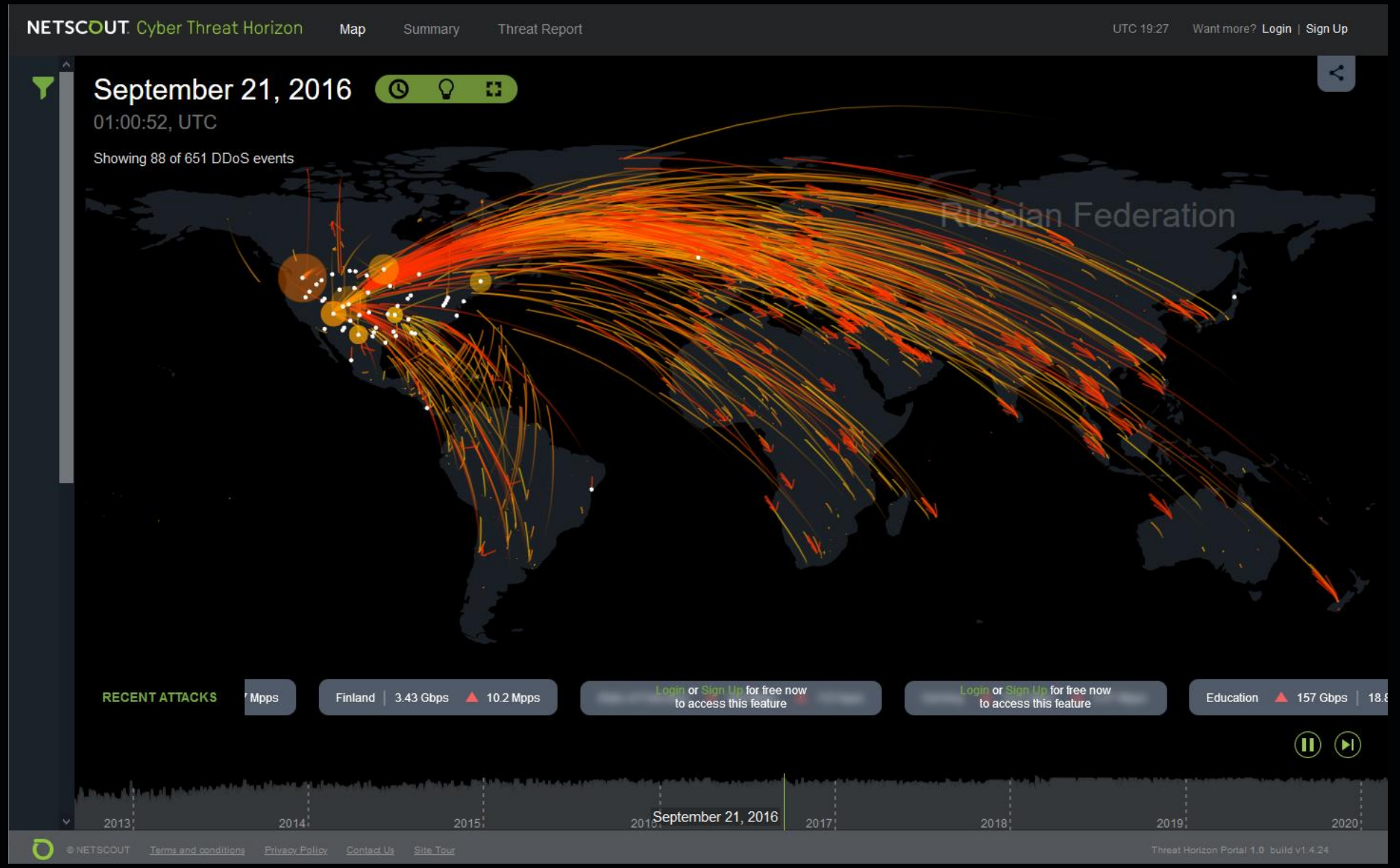
1 Concurrent Attack

10800 Second Attack Time

PURCHASE

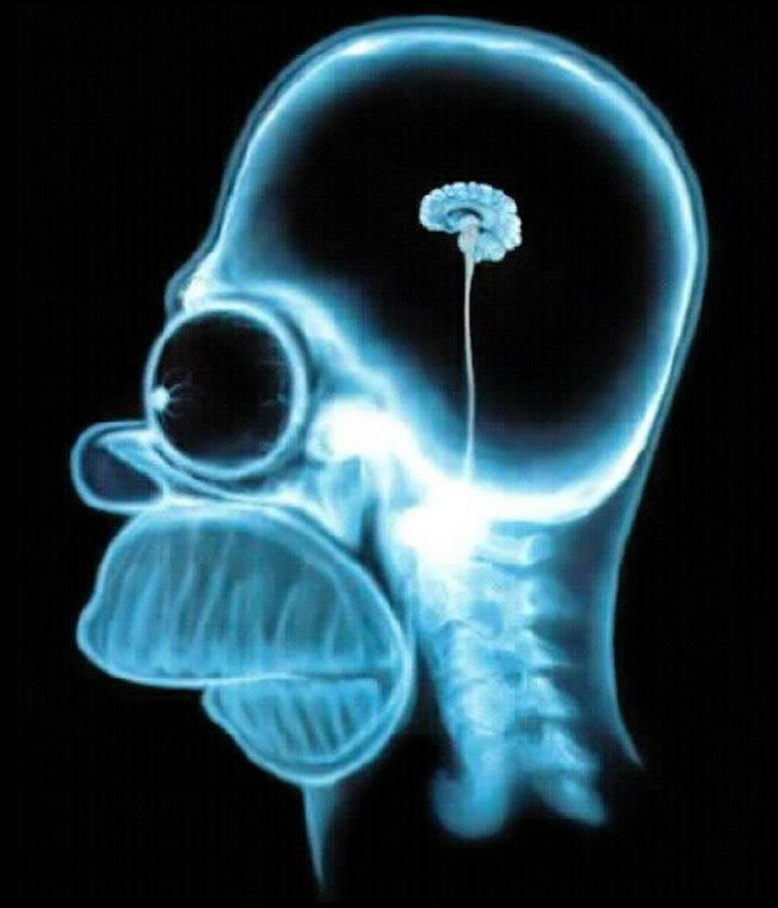
GROUPE DD4BC

DD4BC signifie littéralement *DDoS for Bitcoin*


NETSCOUT Cyber Threat Horizon
Map
Summary
Threat Report
UTC 19:27
Want more? Login | Sign Up
September 21, 2016
01:00:52, UTC
Showing 88 of 651 DDoS events
Russian Federation
RECENT ATTACKS
Mpps
Finland | 3.43 Gbps 10.2 Mpps
Login or Sign Up for free now to access this feature
Login or Sign Up for free now to access this feature
Education 157 Gbps
2013
2014
2015
2016
September 21, 2016
2017
2018
2019
2020
© NETSCOUT
Terms and conditions
Privacy Policy
Contact Us
Site Tour
Threat Horizon Portal 1.0 build v1.4.24

3 POSTURES

- Comportementale
- Organisationnelle
- Technique



On réfléchit d'abord, on clique ensuite

Tous les droits-privilèges, tout le temps !!

*(**Privilèges** : faveurs, avantages particuliers accordés à un individu)*

Invité (très peu de privilège)

Utilisateur (privilège restreint)

Administrateur (privilège total accès)

Double authentification


HTTPS://
EVERYWHERE

Guides de l'ANSSI

01 **Guide d'hygiène informatique**

Il vous présente les 42 mesures d'hygiène informatique essentielles pour assurer la sécurité de votre système d'information et les moyens de les mettre en œuvre, outils pratiques à l'appui.

02 **Recommandations pour la sécurisation des sites web**

Les sites web sont par nature des éléments très exposés du système d'information. Leur sécurisation revêt une grande importance, et ce à plusieurs titres.

03 **PSSI : Guide d'élaboration de politiques de sécurité des systèmes d'information**

La PSSI reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration…) en matière de sécurité des systèmes d'information (SSI).

04 **Recommandations sur le nomadisme numérique**

L'importance croissante de la mobilité et du télétravail dans le monde professionnel crée de nouveaux risques sur les systèmes d'information.

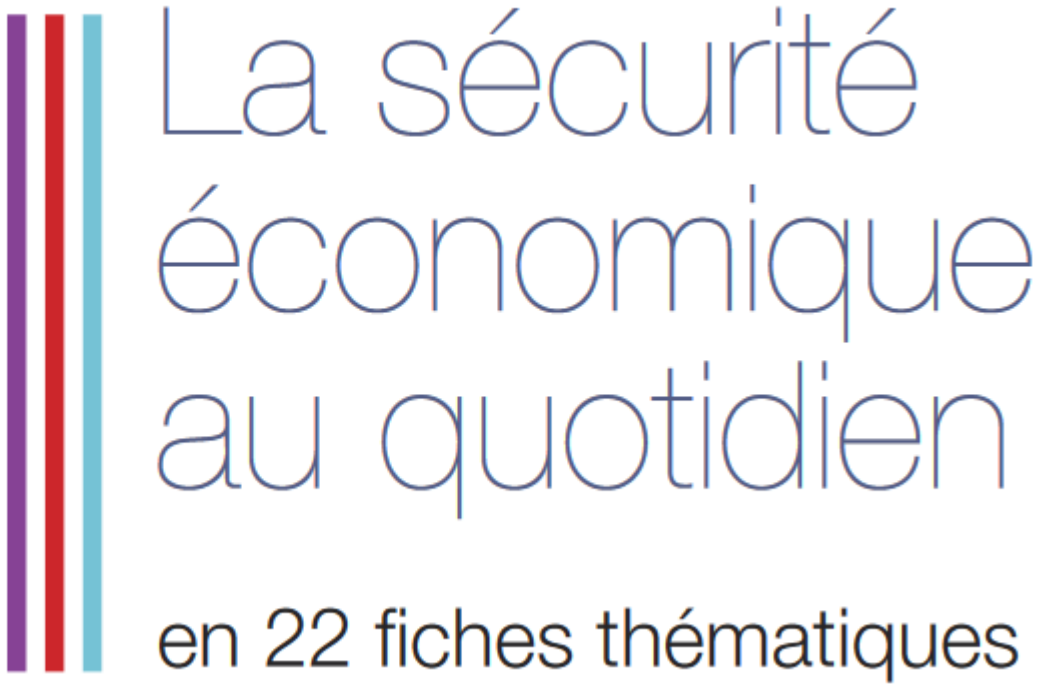
05 **Sécuriser son ordiphone**

Ce document a pour objectif de sensibiliser le lecteur aux principaux risques de sécurité des terminaux mobiles et d'indiquer des recommandations de sécurité génériques à appliquer pour les limiter.

06 **Sécuriser les accès Wi-Fi**

Plusieurs aspects de configuration sont à prendre en compte. L'objet de ce document est donc de guider le lecteur dans le choix des meilleurs paramètres pour la bonne sécurisation d'un réseau Wi-Fi.

https://www.ssi.gouv.fr/administration/bonnes-pratiques/



https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/outils/fiches/22-fiches-rassemblees.pdf

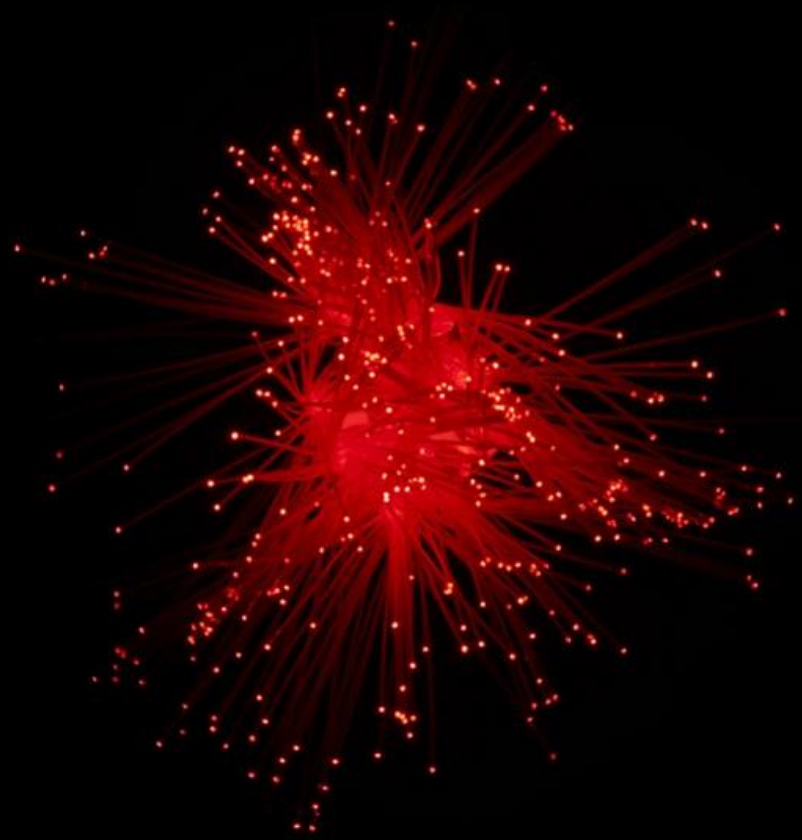
L'ANSSI et l'Association pour le Management des Risques et des Assurances de l'Entreprise (AMRAE) s'associent dans la « Maîtrise du risque numérique – l'atout confiance» pour proposer aux dirigeants et aux risk managers une démarche progressive pour construire étape par étape une politique de gestion du risque numérique au sein de leur organisation.

https://www.ssi.gouv.fr/uploads/2019/11/anssi_amrae-guide-maitrise_risque_numerique-atout_confiance.pdf

HISCOX

Calculateur d'Exposition aux Cyber-Risques

Êtes-vous exposé ? Comprendre et gérer vos cyber-risques



https://www.hiscox.fr/garantie-cyberclear

RGPD

Règlement Général sur la Protection des Données

GDPR *(General Data Protection Regulation)*

Avoir des règles communes dans tous les pays de l’Union

FIN / MERCI

KEEP
CALM
AND
ASK
QUESTIONS

IPCyb

Agence d'Information et de Protection du cyberespace

3 rue de Robien
35000 RENNES

WWW.IPCYB.COM
INFO@IPCYB.COM
+33 756 833 878