AccesSecurity
LE SALON EURO-MÉDITERRANÉEN
DE LA SÉCURITÉ GLOBALE
MARSEILLE CHANOT ■ 6 - 7 MARS 2019
SALON / COLLOQUE / RENDEZ-VOUS D'AFFAIRES



Les nouveaux modes opératoires cybercriminels

6 mars 2019

J.BOLONI – VP CLUSIR
Aix-Marseille

#AIX-MARSEILLE FRENCH TECH

MEMBRE DU
RÉSEAU THÉMATIQUE
FRENCH TECH
#Security #Privacy

CLUSIR PACA

Clusir Nice Côte d'Azur

Territoire ouvert en 2016

Clusir Arles Avignon

Territoire ouvert en 2018

Clusir Toulon Var

Territoire ouvert en 2017

Plus de 200 professionnels sur 3 territoires en PACA

Clusir Aix Marseille

Depuis plus de 20 ans, source du Clusir PACA

MEMBRE DU RÉSEAU THÉMATIQUE FRENCH TECH #Security #Privacy

Représentant du CLUSIF en Région

Fédère les professionnels de la Sécurité de l'Information et les Directeurs Métiers intéressés

Avec humilité face aux enjeux de la cyber sécurité

ORGANISATEUR : CLUSIR PACA

REUNIR

PARTAGER

INFORMER

REGROUPE

- des responsables gravitant autour de la Sécurité de l'Information : DG, Directeurs Métiers, DAF, Chargés de Sécurité / Responsable Sureté…
- des responsables de la Sécurité Informatique : RSSI, DSI, Responsable IT, Ingénieurs Réseaux & Systèmes, Data Protection Officer (DPO)…
- des experts offreurs de services et de solutions techniques : Avocats, Hackeurs éthiques, Experts en Gouvernance IT, Experts Techniques Réseaux, Editeurs spécialisés…

Pour ECHANGER et PARTAGER autour des thématique liée à la Sécurité de l'Information.



De nouvelles approches
Des cibles de choix

© CLUSIR PACA - 2018

Des menaces sur le « Crypto-écosystème »

Plus d'1Md$ détournés en 2018

Du plus simple avec les #GiveAway

Du plus classique : attaques des plateformes d'échange et des personnes

Au plus discret avec les cryptominer





© CLUSIR PACA - 2018

Des attaques sur les « WEARABLES »



Une montre connectée enregistre et permet la publication de parcours utilisateurs dans des lieux normalement « secret » ….
… Ou reliant des lieux connus avec des habitations
Dévoilant ainsi les localisations de bases militaires

© CLUSIR PACA - 2018

Des attaques sur les « véhicules connectés »

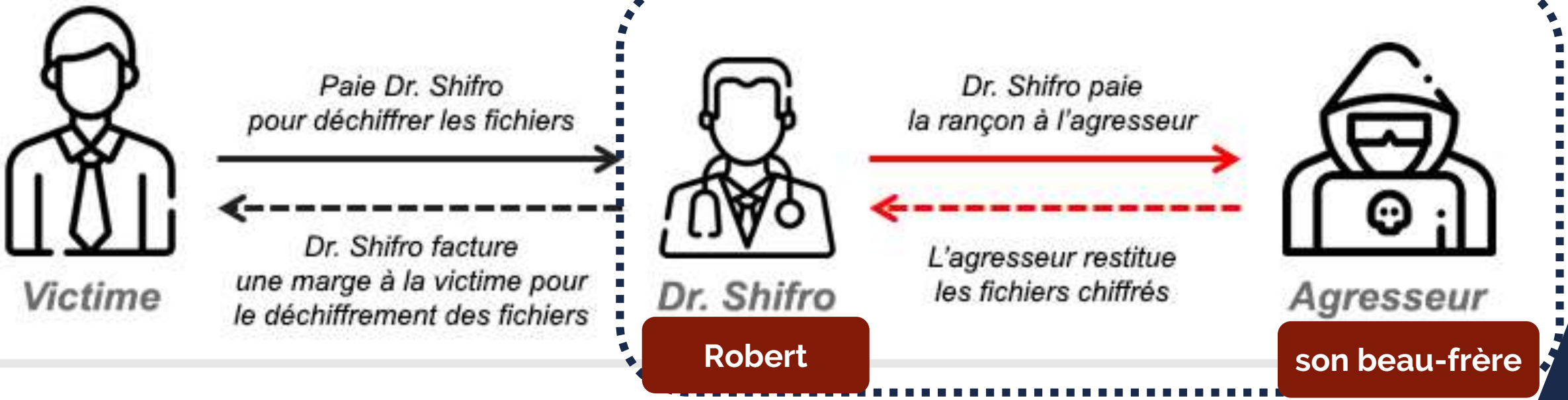


Clonage des clés Tesla en quelques secondes, pour quelques centaines de dollars d'équipement

© CLUSIR PACA - 2018

Des ransomwares, les nouvelles « techniques » de déchiffrement





© CLUSIR PACA - 2018

Des ransomwares, les nouvelles « techniques » de déchiffrement



La vraie bonne adresse c'est No More Ransom



https://www.nomoreransom.org/fr/index.html

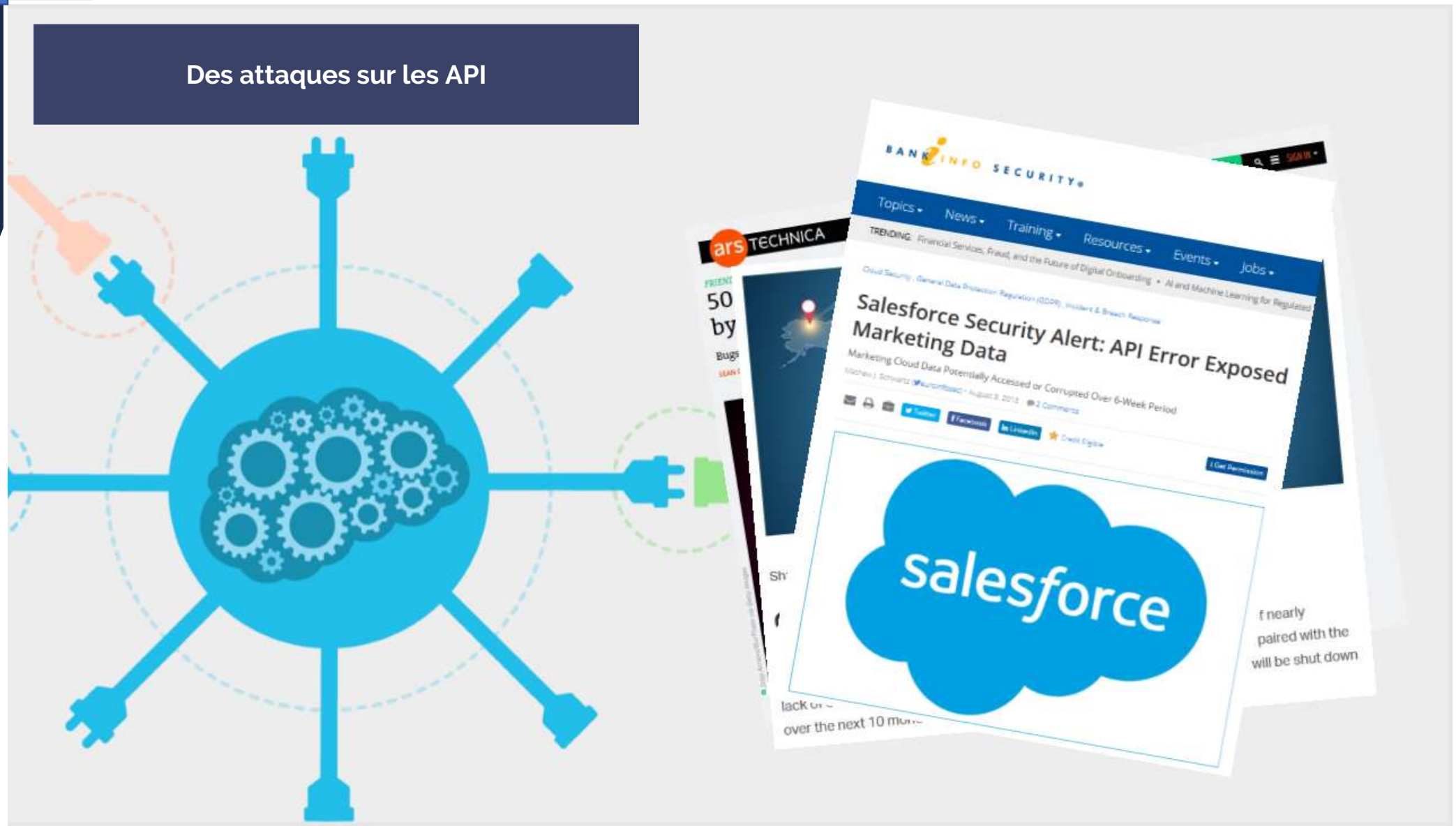
© CLUSIR PACA - 2018

Des cas de fraude au président



© CLUSIR PACA - 2018

Des attaques sur les API



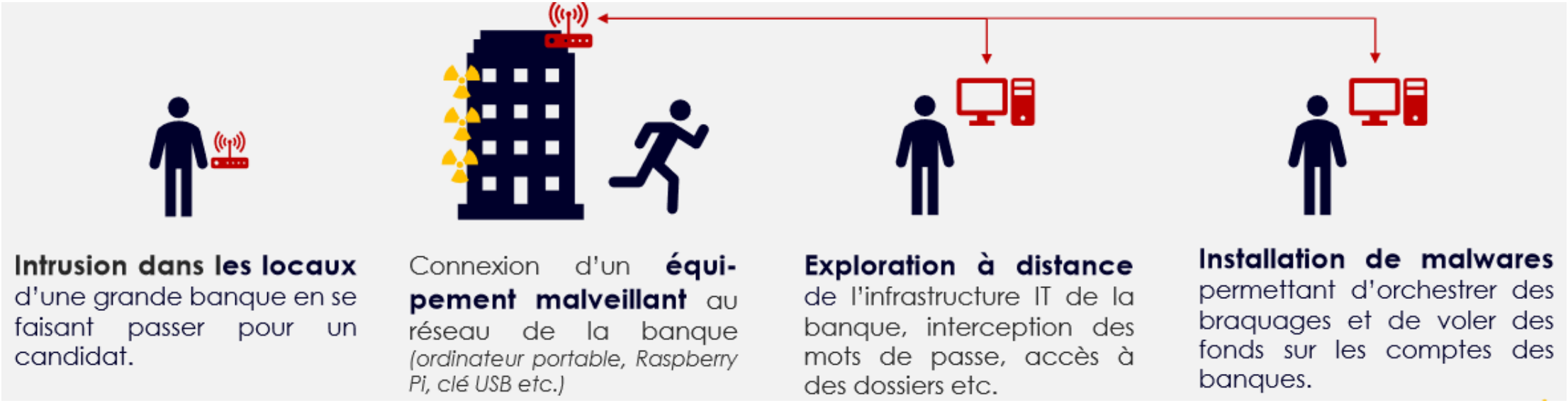
© CLUSIR PACA - 2018

Les banques toujours sources de convoitises



© CLUSIR PACA - 2018

La méthode Darkvihnya (prononcé « darkvishnya »)



Intrusion dans les locaux d'une grande banque en se faisant passer pour un candidat.

Connexion d'un **équipement malveillant** au réseau de la banque *(ordinateur portable, Raspberry Pi, clé USB etc.)*

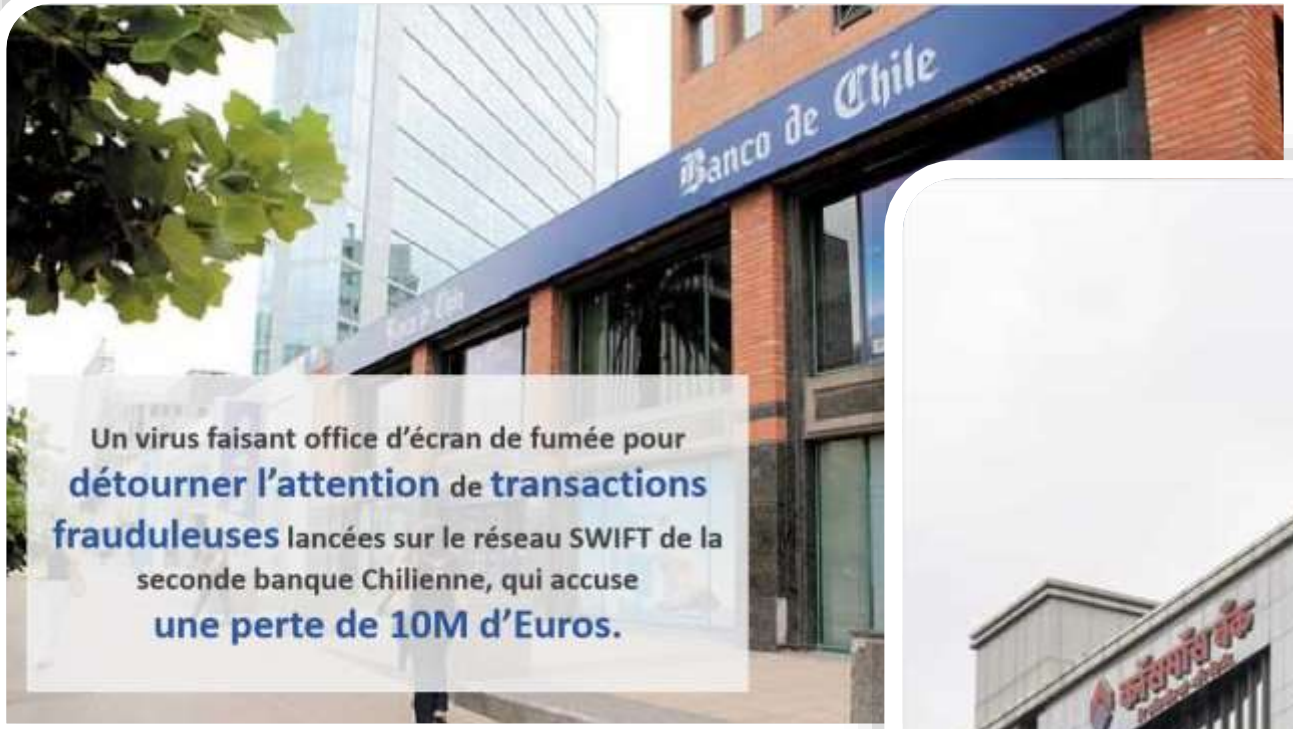
Exploration à distance de l'infrastructure IT de la banque, interception des mots de passe, accès à des dossiers etc.

Installation de malwares permettant d'orchestrer des braquages et de voler des fonds sur les comptes des banques.

Testé avec succès sur les banques
Applicable à toutes les entreprises …

© CLUSIR PACA - 2018

Mais aussi





© CLUSIR PACA - 2018

Et enfin des formes de menaces plus personnelles

MENU **Le Point**

Actualité > Société > Faits divers

Escroquerie : « sextorsion » la nouvelle menace sur Internet

Une nouvelle arnaque se répand sur Internet. Des escrocs font croire aux internautes qu'ils possèdent des vidéos compromettantes, menaçant de les diffuser.
Source AFP

Publié le 11/08/2018 à 14:46 | Le Point.fr





Les jeunes sont vulnérables à la cyberintimidation. Photo : iStock

Gare à la cyberintimidation

Selon M. Côté, même si le défi Momo n'a pas causé de suicide, il n'est pas inoffensif pour autant. Des cyberprédateurs peuvent créer des profils avec l'avatar du personnage de Momo, puis s'en servir pour intimider des jeunes ou tenter d'obtenir leurs informations personnelles.

> *« Le phénomène, ce n'est pas le Momo Challenge ou le Blue Whale Challenge. Le phénomène, c'est un adulte qui est un prédateur et qui rentre en contact avec un jeune et qui le fait chanter. Ça peut être de la sextorsion, ça peut être des menaces ou des trucs comme ça, et c'est ça, le réel phénomène. On parle de cybercriminalité. »*
>
> — *Louis-Philippe Côté, membre du Centre de recherche et d'intervention sur le suicide, enjeux éthiques et pratiques de fin de vie, à l'Université du Québec à Montréal*

© CLUSIR PACA - 2018



Les habitudes des cybercriminels changent également …

© CLUSIR PACA - 2018

L'éternel jeu du chat et de la souris



Hacker domain

Hacker domain

Hacker V2 domain

Hacker V2 domain

Etc .....

© CLUSIR PACA - 2018

Tendance à la décentralisation des services

- **Période de transition** : les groupes cybercriminels changent leurs habitudes et quittent leurs plateformes traditionnelles

- Forums centralisés
- Canaux IRCs
- Darknet Markets

BLOCAGE(S) / FERMETURE(S)



Conséquence des opérations de police menées en 2017 ayant abouties à la fermeture de 2 Darknet Market : AlphaBay et Hansa

Opération BAYONET

© CLUSIR PACA - 2018

Malgré tout des forums existe toujours

HACK FORUMS

RAIDFORUMS

MagBO

eXploit.in

HPC

MERRY CHRISTMAS NULLED EXPECT LAZY STAFF

Commonwealth of independant States



Situation	
Création	8 décembre 1991
Type	Organisation intergouvernementale
Siège	Minsk[1]
Langue	Russe, arménien, azéri, biélorusse, kazakh, kirghize, roumain, ouzbek, tadjik et turkmène.

Organisation	
Membres	Azerbaïdjan Arménie Biélorussie Kazakhstan Kirghizistan Moldavie Ouzbékistan Russie Tadjikistan Turkménistan (État associé)

- **Hébergés dans des républiques membres du « CIS »**
  - Bénéficiant d'un certain niveau d'impunité
    - Pour l'hébergement
    - Pour les actions des cyber criminels

© CLUSIR PACA - 2018

Les méthodes actuelles

- Proxy/VPN pour masquer l'infrastructure de commande
- Hébergement « BulletProof »
- Infrastructure TOR
- Algorithme de génération de domaine

```
def generate_domain(year, month, day):
    """Generates a domain name for the given date."""
    domain = ""

    for i in range(16):
        year = ((year ^ 8 * year) >> 11) ^ ((year & 0xFFFFFFF0) << 17)
        month = ((month ^ 4 * month) >> 25) ^ 16 * (month & 0xFFFFFFF8)
        day = ((day ^ (day << 13)) >> 19) ^ ((day & 0xFFFFFFFE) << 12)
        domain += chr(((year ^ month ^ day) % 25) + 97)

    return domain
```

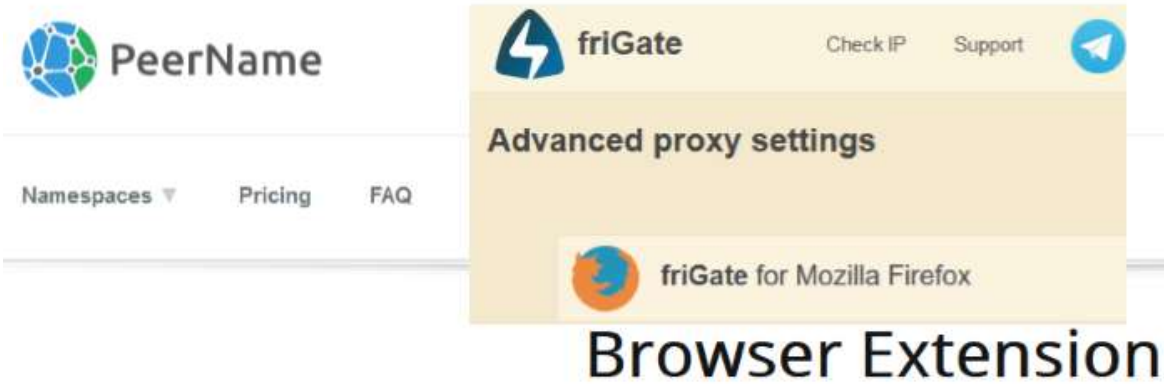
Objectifs :
Masquer l'infrastructure malveillante
Stocker les informations volées
Conserver l'efficacité des dispositifs le plus longtemps possible

© CLUSIR PACA - 2018

De nouvelles orientations : Block-Chain DNS

- Extensions ‘Blockchain-DNS’ navigateur







Echapper au contrôle et au blocage

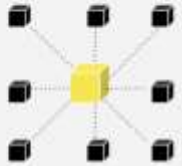
© CLUSIR PACA - 2018

De nouvelles orientations : Block-Chain DNS

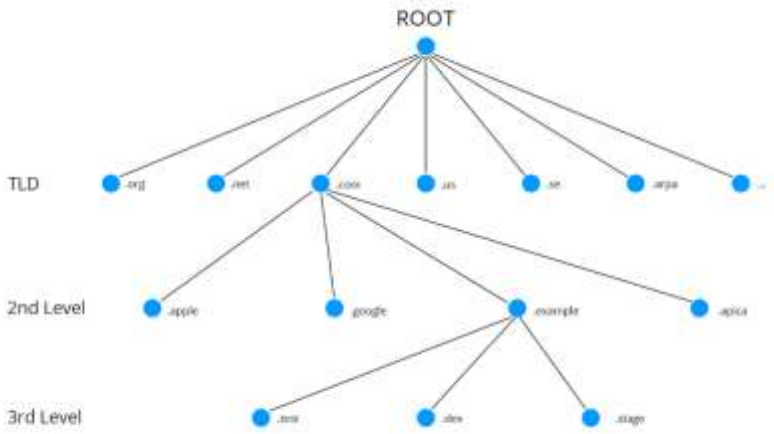
TOP Level Domain
Organisation hiérarchisée & goubvernée

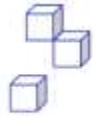
DNS

Domain Name Service



DNS is governed by centralized organization, and can be the website entry point, branding, identity.





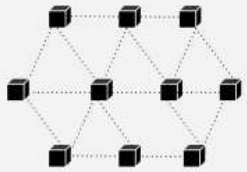
www.christopher.com

- WEBSITE ENTRY POINT
- BRANDING

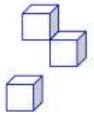
Block Chain DNS
Organisation décentralisée

BNS

Blockchain Name Service



BNS is decentralized and governed by smart contract, and is the website entry point, branding, identity, login account.



christopher.eth

- WEBSITE ENTRY POINT
- BRANDING
- IDENTITY
- LOGIN ACCOUNT

MORE...

PORTAL NETWORK

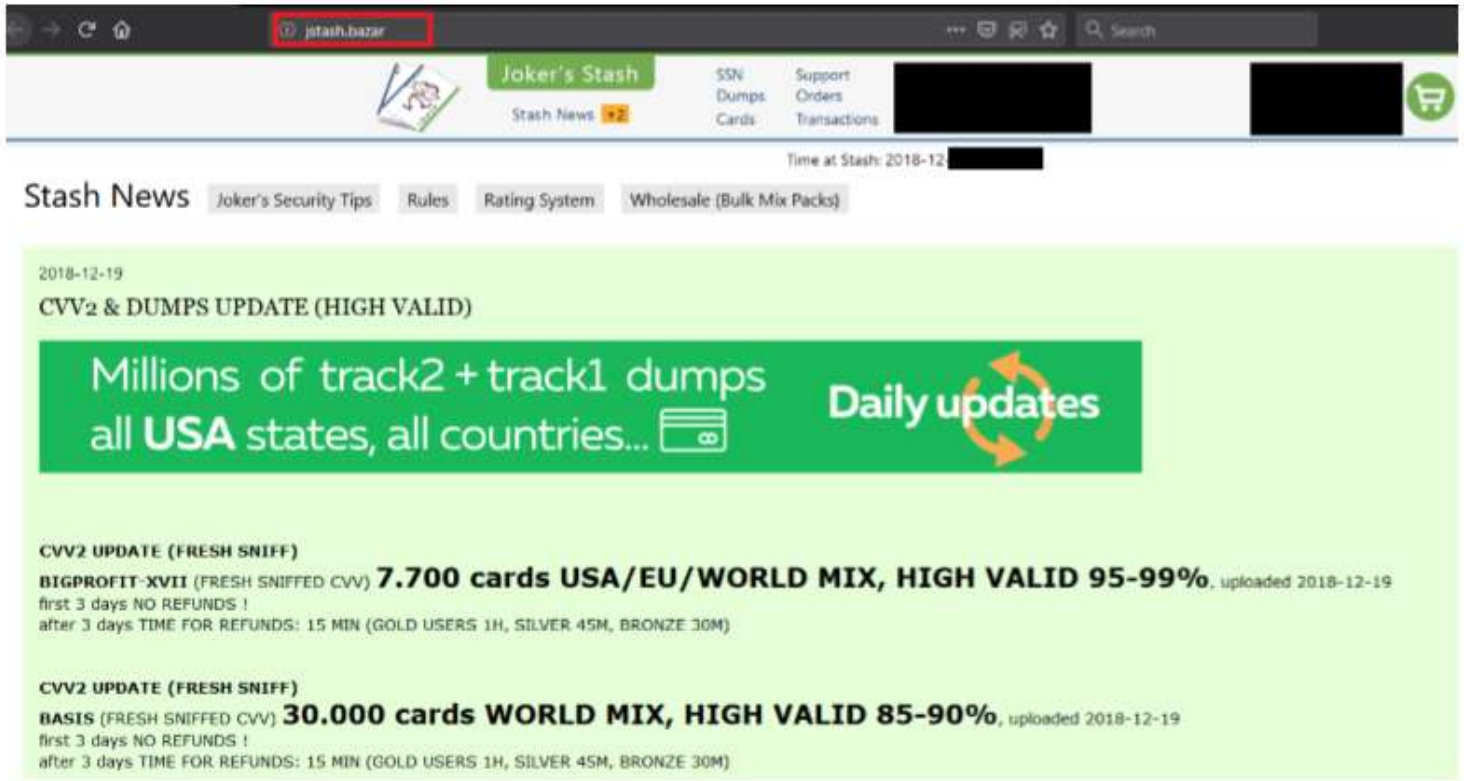
© CLUSIR PACA - 2018

Cas d'usage Services : Joker Stash

- Site spécialisé dans la vente de numéro CB utilisant un nom de domaine .bazar

- Carding





la Block Chain DNS Permet au site d'échapper au blocage

© CLUSIR PACA - 2018

Cas d'usage malwares







- Trinity / FBOT
  - Botnets android
  - Smartphone, smartTV, …
- Spécialité : miner cryptojacking

- GandCrab
- Spécialité : Ransomware

- Azorult
- Spécialité : Vols de données
  - Mots de passe
  - Cartes de crédit

la Block Chain DNS aide les cybercriminels à masquer l'infrastructure et à conserver l'efficacité des dispositifs

© CLUSIR PACA - 2018

Les « autoshops »



des pages où sont regroupés un grande nombre d'offre de service. Et pour lesquels chaque bannière amène l'utilisateur vers une messagerie instantanée afin de procéder au transactions.

© CLUSIR PACA - 2018

L'apprentissage du passé (de la prison ?)

- Moins de traces écrites sur les forums
  - Moins de visibilité = Moins de risques d'identifications

- Explosion des messageries instantanées (IM) type ICQ/Jabber/QQ
  - Transactions directes
  - Traçabilité réduite







© CLUSIR PACA - 2018

Pour conclure

- Les cyber criminels restent maitres pour retourner les moyens / solutions / outils à leur avantage …

- Aujourd'hui, c'est la blockChain ….

Et Demain l'IA ?

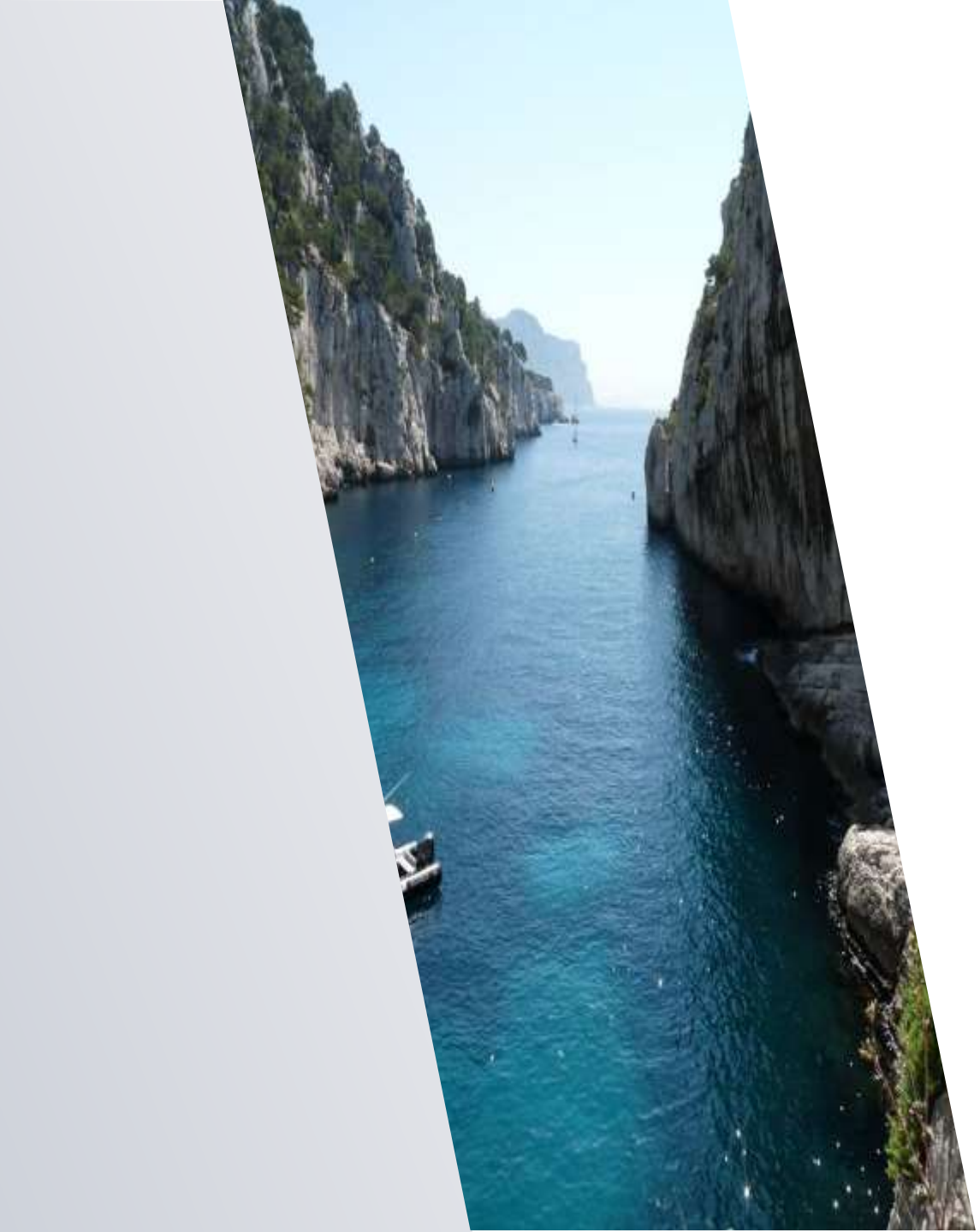


© CLUSIR PACA - 2018

Source

- Panocrim 2019 – CLUSIF
  - https://clusif.fr/conferences/panorama-de-la-cybercriminalite-annee-2018/

© CLUSIR PACA - 2018



MERCI POUR VOTRE ATTENTION

CLUSIR PACA

100%

Sécurité de l'Information

100%

Professionnels et experts

© CLUSIR PACA - 2018