SAFE&SMARTITSOLUTIONS

"Cyber Intelligence, suivre les profondeurs du web pour anticiper les cyber menaces".

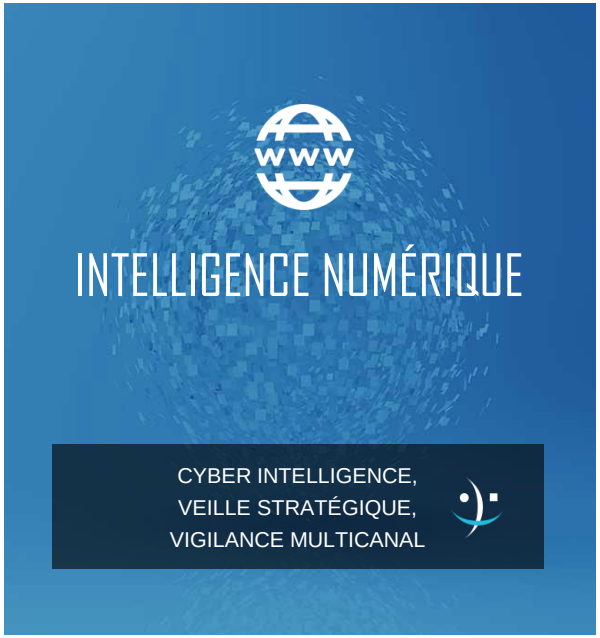
RSSIA le 16 juin

Christophe Marnat – Bertin IT - Responsable de la stratégie

© Copyright - Bertin IT 2016

GROUPE CNIM

15M€ CA 2015 ▪ 120 pers. dont 50% dédiées à la R&D
30 ans d'expérience en développement logiciel et d'ingénierie en projets complexes
France ▪ UK ▪ Allemagne ▪ Maroc



Groupe CNIM, équipementier et ensemblier industriel coté à Euronext Paris
présent dans **l'Environnement**, **l'Energie**, la **Défense** & les **Hautes Technologies**.
727 M€ de CA 2015 dont 61,3% à l'export, 3000 collaborateurs dans le monde.

www.cnim.com

Transformation numérique
Vecteur d'opportunités et de menaces

90% des données dans le monde ont été créées au cours des deux dernières années seulement.

Un périmètre de surveillance complexe

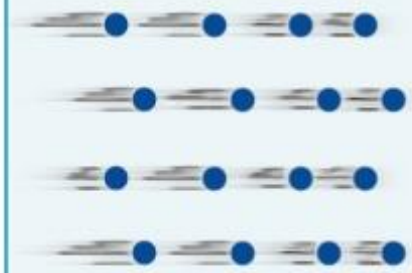
Dimensions du Big Data

Volume

Données brutes d'origine

Terabytes à exabytes de données disponibles

Vitesse



Données dynamiques

Analyse en temps réel, décision en une fraction de seconde

Variété

Données hétérogènes

Format structuré, non structuré, texte, multimédia

Véracité

Données incertaines

Cohérence, fiabilité, qualité et prédictibilité des données

© Copyright - Bertin IT 2016

Cyber Intelligence - Les enjeux

CYBER THREAT INTELLIGENCE

ANTICIPATION DES CYBER MENACES

Identifier en amont des indices de préparation de cyber attaques.

DÉTECTION DE FUITES D'INFORMATIONS

Identifier des documents confidentiels diffusés intentionnellement ou non sur le web.

DÉTECTION DE MENACES SUR LES BIENS ET LES PERSONNES

Identifier sur le web des menaces ou des revendications d'attaques physiques.

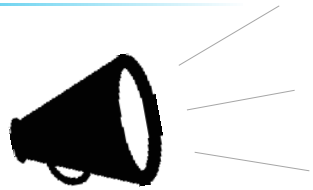
DÉTECTION DE CONTREFAÇONS

Identifier des produits contrefaits et cartographier des réseaux de distributions.

Excellence – Créativité – Engagement - Confiance

© Copyright - Bertin IT 2016

Cyber menaces : Tous concernés



IL N'EXISTE QUE DEUX SORTES D'ENTREPRISES : CELLES QUI ONT ÉTÉ PIRATÉES ET CELLES QUI NE LE SAVENT PAS ENCORE. »

MISHA GLENNY - JOURNALISTE D'INVESTIGATION BRITANNIQUE

ANTICIPER LES CYBERMENACES

90 % des grandes entreprises à travers l'Europe ont été touchées par une cyberattaque de grande ampleur au cours des cinq dernières années.
Etude Lloyds - 2016

8 attaques sur 10 en France ciblent les PME.

PROTÉGER LES SI INDUSTRIELS

L'ANSSI compte désormais faire de la sécurité des sites industriels « la priorité des priorités »
Juin 2017 - Les echos

Les exemples de piratage industriel sont plus rares que le vol de données bancaires. Mais les conséquences sont potentiellement énormes.
Juin 2017 - Les echos

Explosion des affaires de vols de données

Forte augmentation du nombre d'affaires de vols de données en 2016-2017 :

- 68 millions menacés chez Dropbox (08/16)
- 500 millions de compte chez Yahoo (09/16),
- 412 millions chez FriendFinder (10/16),
- 87 millions pour Dailymotion (10/16),
- 167 millions d'informations Linkedin à vendre.
- 17 millions de comptes sur le site Indien Zomato (Juin 17)

- 50 millions de données de citoyens en Turquie (04/16)

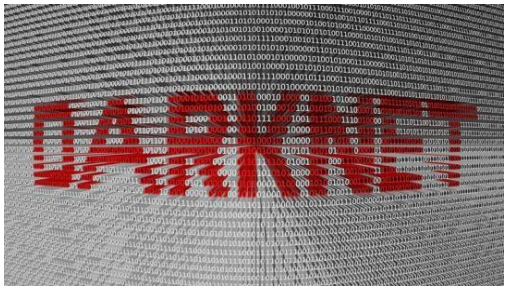
93% *des entreprises de plus de 250 employés ont été victimes d'une infraction ou d'un vol de données l'an passé. 2016 - Les Echos.*

Méthodes d'exfiltration :

- Attaque ciblée avec exploitation des failles du SI.
- Vol de données avec complice interne (idéologie, corruption)
- Vol interne d'un salarié.
- Fuite non intentionnelle (linked-in, Slideshare, Disque-dur).

© Copyright - Bertin IT 2016

Un modèle économique bien établi



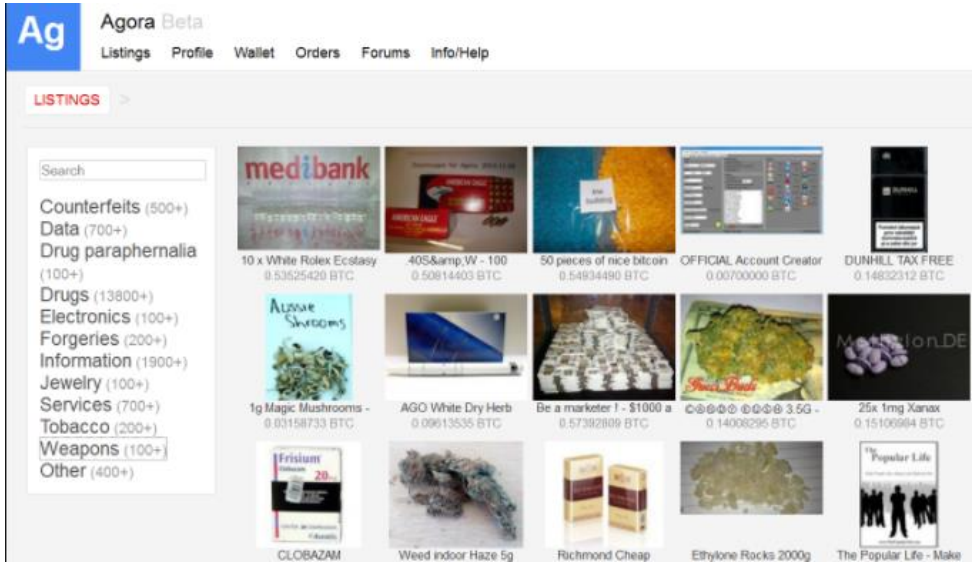
Sur le Dark Net, 40.000 escrocs réalisent un chiffre d'affaires compris entre 5 et 10 millions d'euros par mois.
Trend Micro 09/16

Une identité peut être vendue plus de 200 euros si les données bancaires sont encore valables et le plafond élevé.

Un faux passeport français sur le darknet coûte 1.500 à 3.000 euros

© Copyright - Bertin IT 2016

Cyber Intelligence & Lutte contre les contrefaçons



Identifier les réseaux de contrefacon

75 Mds $

L'impact économique de la contrefacon de médicaments.

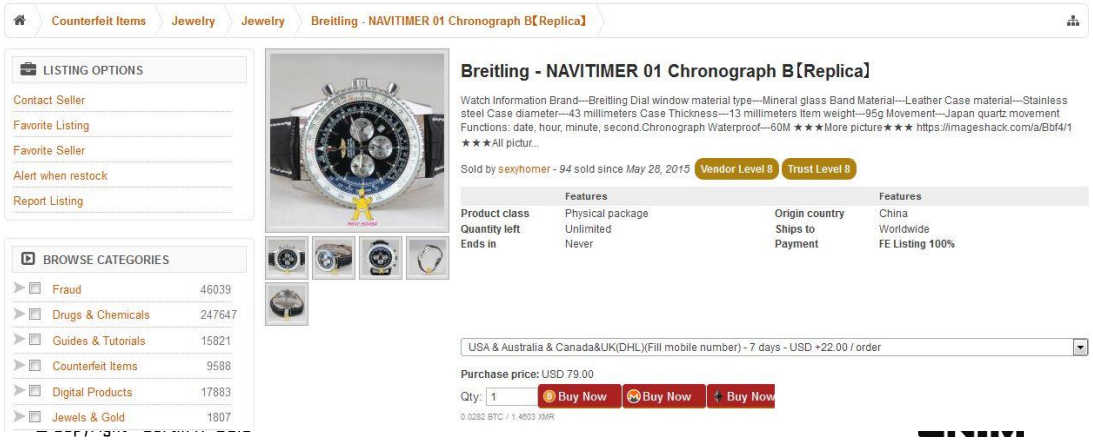
2016 – *Pharmaceutical Security Institute*

Suivre les darknet markets

+ de 30 millions de copie de montres suisses sont vendues chaque année (pour 25 millions d'unités véritables par an).

Marché en pleine croissance : 461 Mds$ en 2013 contre 250 Mds $ en 2007.

2017 - Fédération horlogère.



bertin IT
SAFE&SMARTITSOLUTIONS

Méthodologie

COLLECTION OF DATA & METADATA

[Internet]

- UGC, podcast
- Social networks , blogs, forums, Web sites, press , deep&dark web

[TV / Radio]

- Satellite & Terrestrial

ADVANCED PROCESSING OF CONTENTS

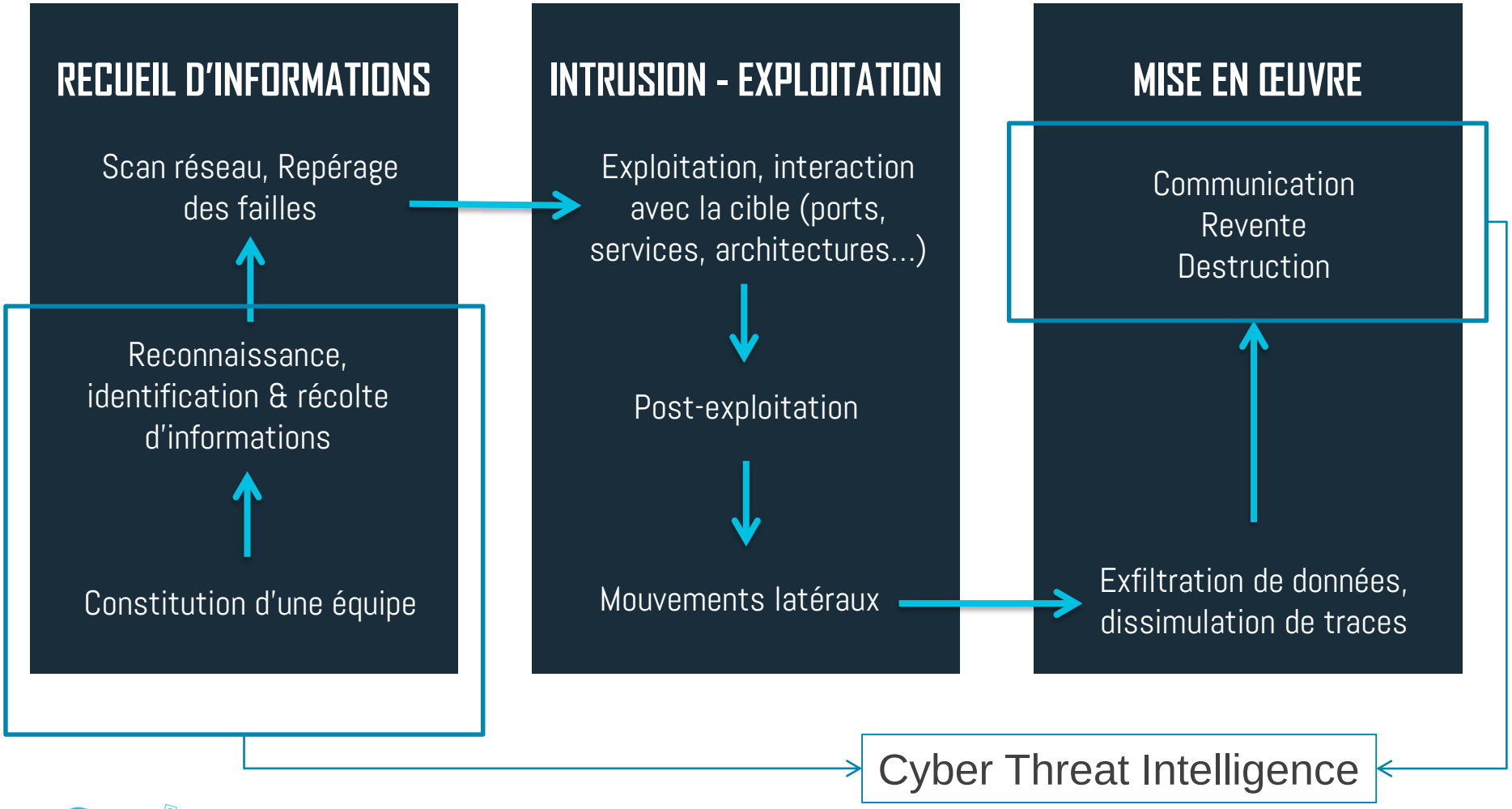
- Extraction of textual information from pictures and videos
- Special Entities extraction
- Statistical analysis
- Language identification
- Automatic Speech-to-Text
- Automatic translation

VISUALIZATION, EXPLOITATION, ANALYSIS & CAPITALIZATION

- Trend and emerging concept detection
- Cross-language & cross-media powerful indexation & search engine
- Synchronized multimedia multilingual visualization
- Dashboard & Analysis of relationship networks

© Copyright - Bertin IT 2016

Mode d'action en Cyber Threat Intelligence



© Copyright - Bertin IT 2016

INTERNET

Tous les protocoles, toutes les adresses routables (www, email, ftp…)

WORLD WIDE WEB

Internet accessible via un navigateur (Internet Explorer, Chrome, Safari…)

SURFACE WEB

> ACCESSIBLE > INDEXÉ

ou Web Public, représente **4% du contenu du web** (8 milliards de pages sont disponibles via les moteurs de recherche tel que Google)

SURFACE WEB

DEEP WEB

> ACCESSIBLE > NON INDEXÉ

ou Web Profond, représente **96% de l'univers numérique** (7,9 zettaoctets de sites non indexés par google ou autres moteurs de recherche)

PASTEBIN

DARK WEB

DARK NET

DARK NET

> RESTREINT > NON INDEXÉ

Les services incluent le web, l'email, le chat, le partage de fichiers et le routage obscurci d'int

DARK WEB

Tous les services **accessibles via un navigateur web spécifique** (TOR par exemple)

WWW.MBA-MULTIMEDIA.COM

Web

Moteurs de recherche généralistes
Réseaux sociaux
Sites de partage vidéo
Blogs

Deepweb

Moteurs de recherche spécialisés
Crawlers spécifiques
Serveurs spécifiques
Forums
Chat rooms

Darknet

Moteurs de recherche
Réseaux sociaux
Blogs
Forum
Chat room
Site de commerce illégal

Darknet

Réseau superposé (ou réseau overlay)

Protocoles spécifiques intégrant des fonctions d'anonymisation.

Du simple échange de fichiers comme RetroShare, à la construction d'un écosystème anonyme complet (web, blog, mail, irc) comme Freenet.

Quelques chiffres:

- Tor : environ 50 000 sites actifs.
- I2P : environ 6 000 sites.
- Freenet : aucunes données précises.

© Copyright - Bertin IT 2016

Outils de monitoring Dark

CANDLE:

- Recense environ 100 000 liens en mars 2016 (certainement plus maintenant)
- Projet non ouvert
- S'appuie sur les index Onion Crat (5939 onions) et Harry71

NOT EVIL :

- 22 millions de liens indexés
- Limite: censure
- Projet non ouvert

AHMIA:

- env. 5700 .onion
- Crawler I2P proposé
- Limite : censure
- Open source

© Copyright - Bertin IT 2016

Traitement multimédia – multilingue des données

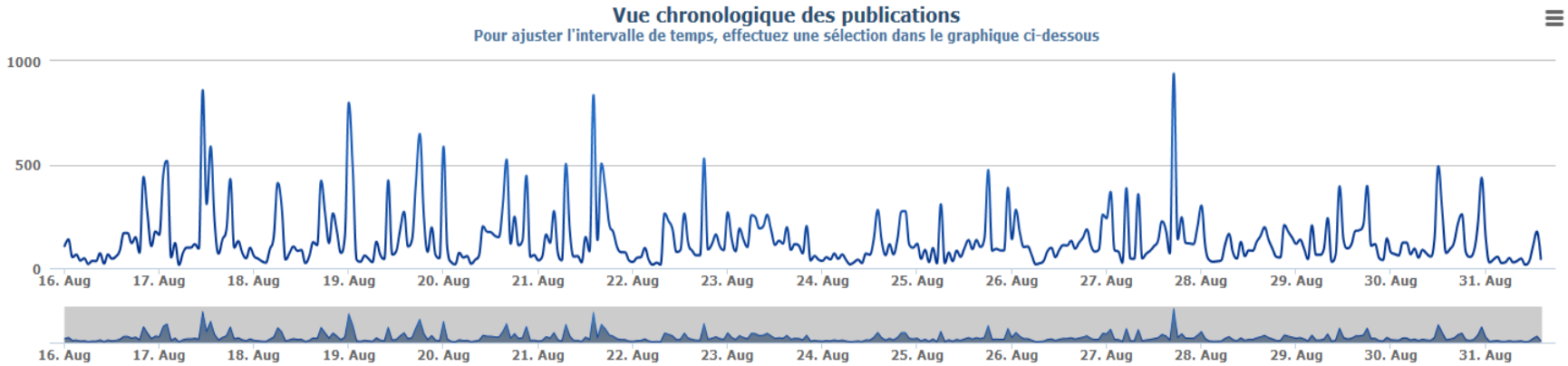
bertin SAFE&SMARTITSOLUTIONS

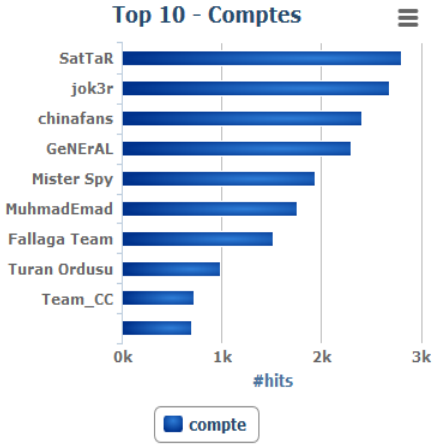
CNIM

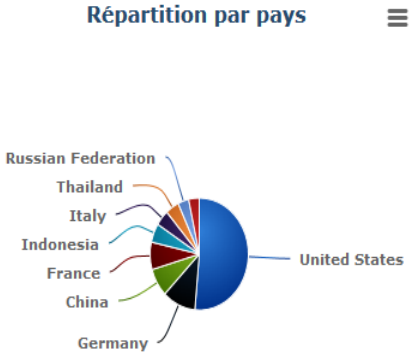
Analyse des tendances

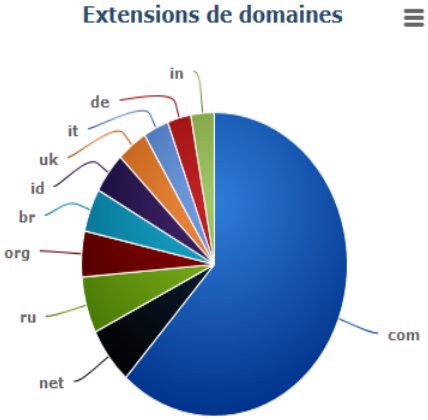
Statistiques de défacement (52771 documents)

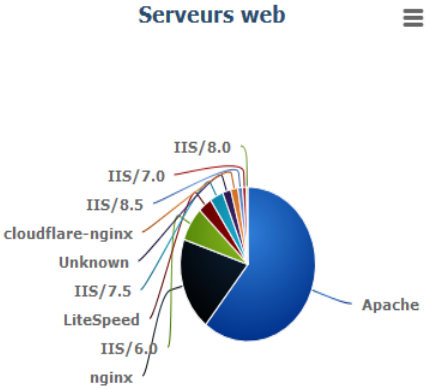
Préciser des mot-clés d'intérêt | Date minimale 16-08-2016 | Date maximale 31-08-2016 | Sélectionner la base indexée Moteur Solr | Réinitialiser











© Copyright - Bertin IT 2016

Cartographie des réseaux

Administration Basket Services Notifications (4) Current user : demo

MediaCentric® bertin TECHNOLOGIES

My Dashboards | Data sources | Information Retrieval | Networks Relation Analysis | Alerter | Request for Information

Tango_NM_... Search for a node Search in view

INFO | NODES | RELATIONSHIPS

Anonymous Venezuela

Twitter_account Tango_NM

Properties

Database Id	Followers_count
20228	46662
Friends_count	Location
14546	anonymousvenezuela.org
Statuses_count	User_account
68087	anonsghost
User_id	User_name
112715059	Anonymous Venezuela

Connections

My Notes

Console

© Copyright - Bertin IT 2016

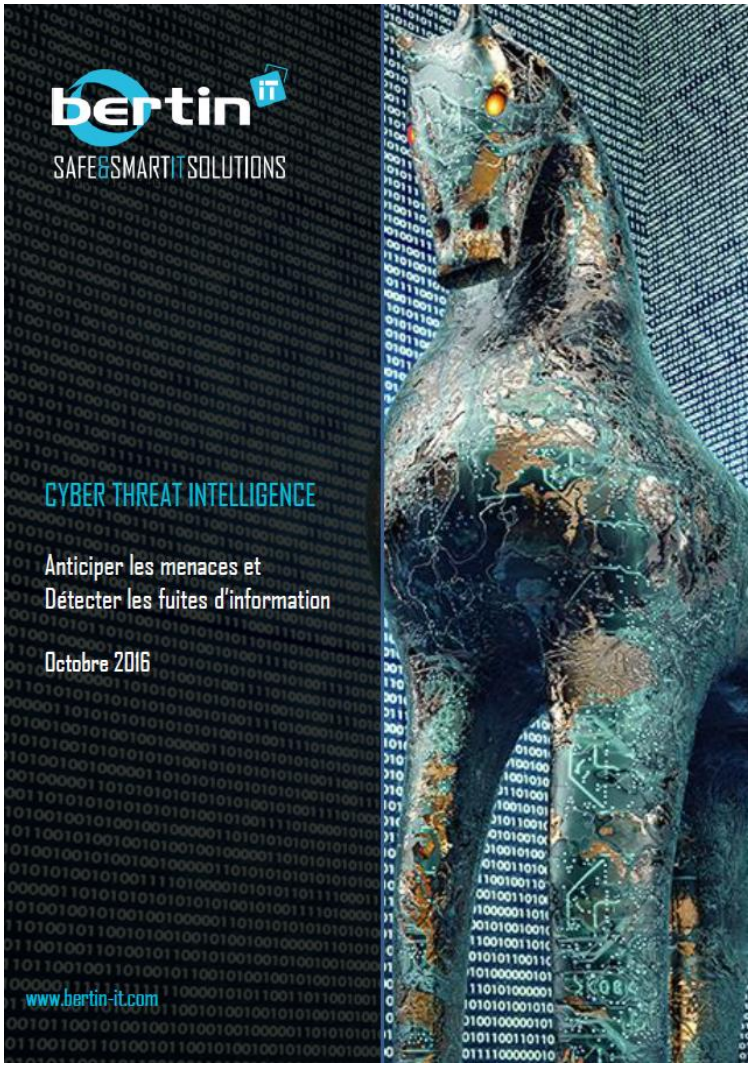
PARTAGEONS NOS EXPÉRIENCES

LIVRE BLANC

CYBER THREAT INTELLIGENCE

Anticiper les menaces et
Détecter les fuites d'information

christophe.marnat@bertin.fr



© Copyright - Bertin IT 2016

AVEZ-VOUS DES QUESTIONS ?

Filiale de Bertin Technologies
Groupe CNIM

HEAD OFFICE

Parc d'Activités du Pas du Lac
10 bis avenue Ampère
78180 Montigny-le-Bretonneux

T. +33(0)1 39 30 62 50
E. contact@bertin-it.com

www.bertin-it.com

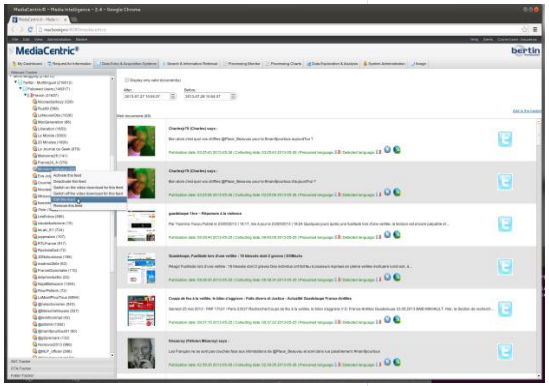
CNIM

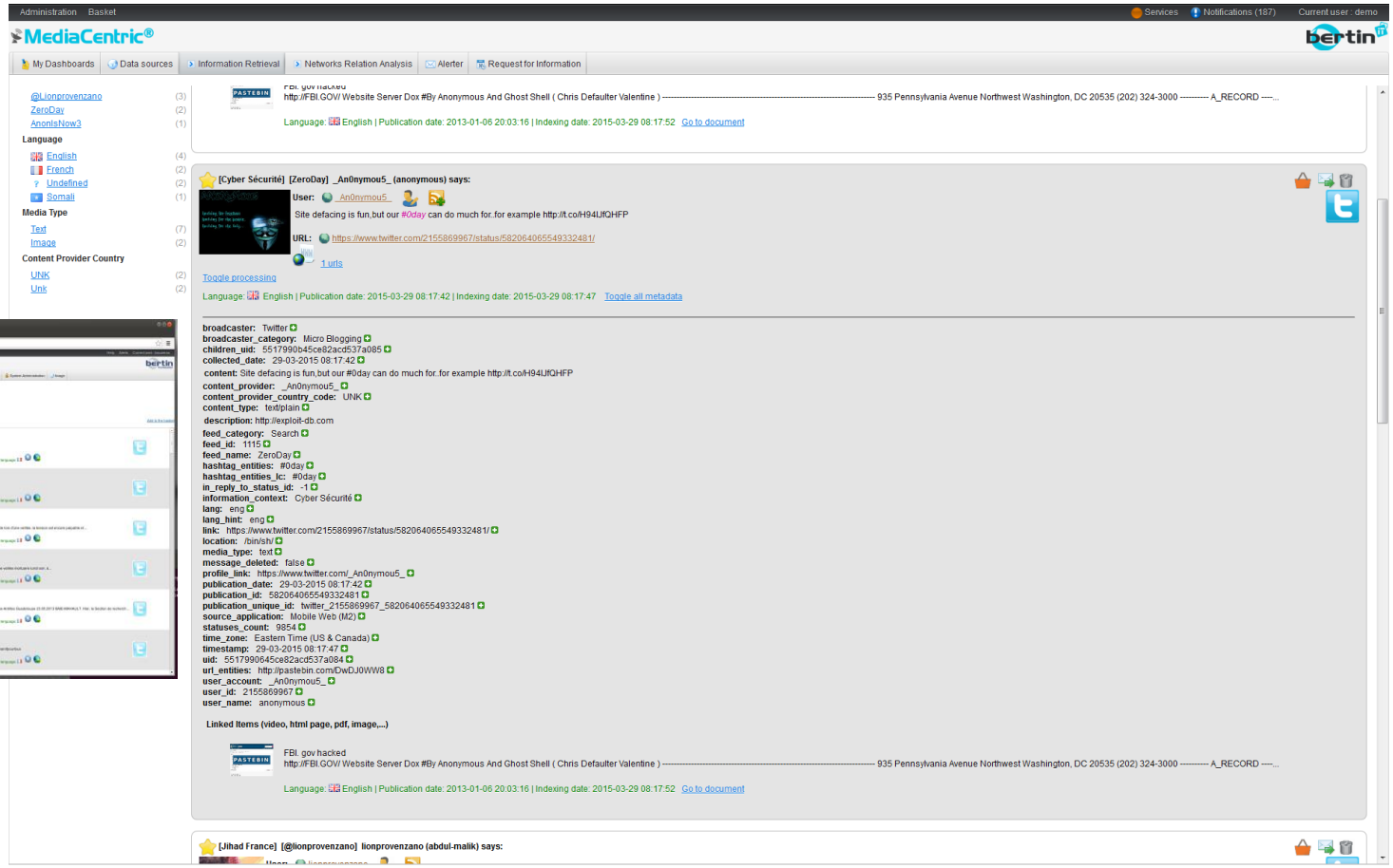
B.T.D46.D

Exemple 1 : de Twitter vers…

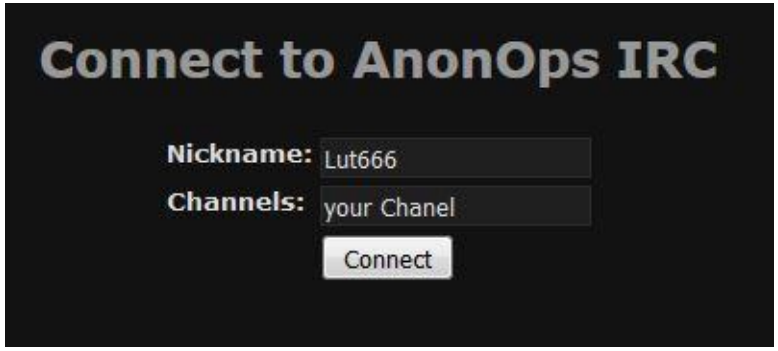
Monitoring deTwitter par User et/ou mots-clefs

- Par l'API
- Avec un historique des données collectées et/ou des métadonnées.





...une liste privée - Chan List...

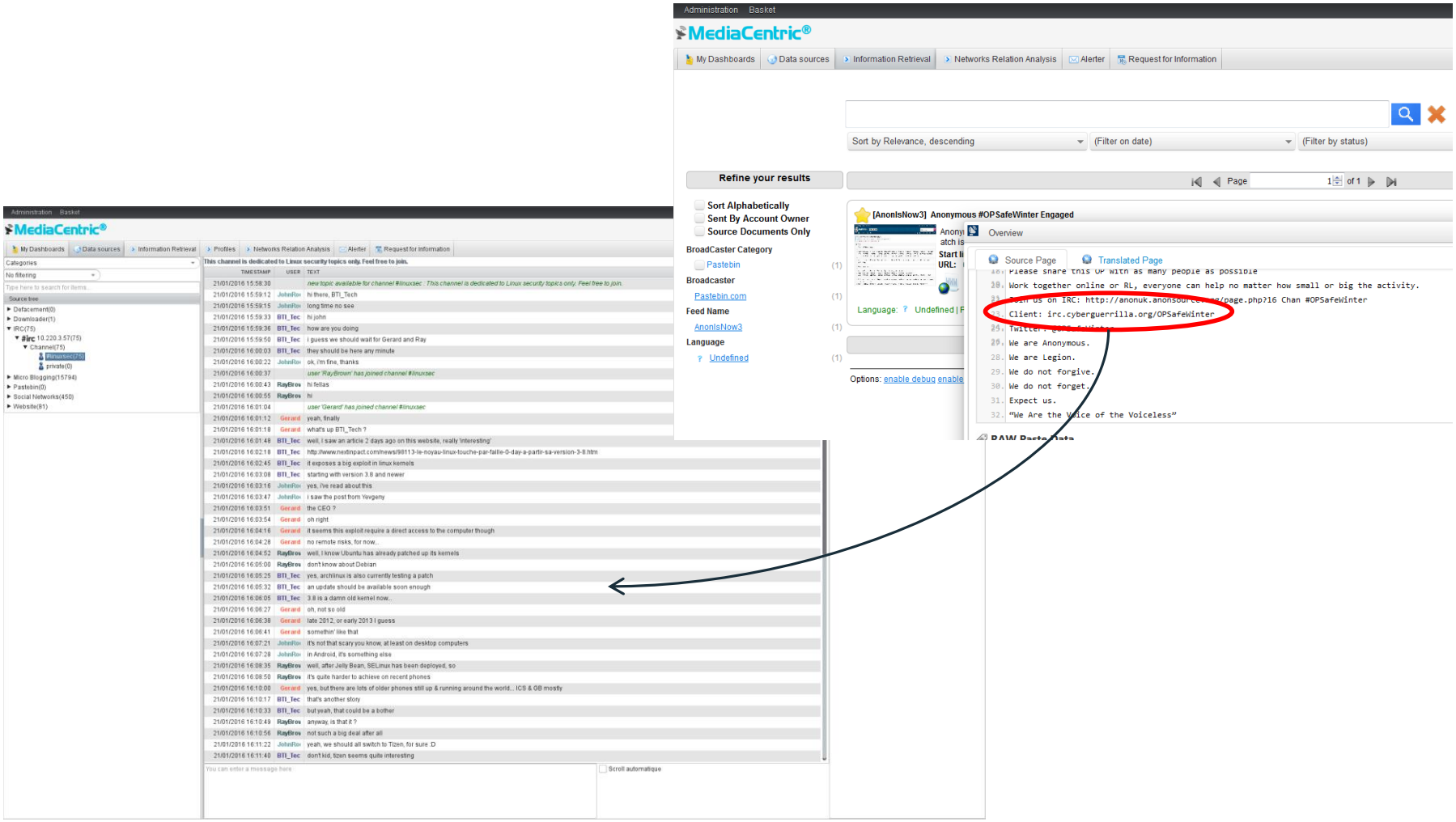



```
[11:15] == * 8
[11:15] == #opsafewinter 10 [+Cnrt] URGENT! /join #opnsa and help us fight rule 41. This effects all of usWelcome to Operaton Safe Winter: Channel in construction. Help is welcome. Promote if
you can! https://pad.riseup.net/p/opsafewinter2016
[11:15] == #OpIstanbul 1 [+Cnrt] Blog: opturkey.com | Mail: info@opturkey.com | PGP Fingerprint: E38A CCDF D6A6 6125 7688 A09A B688 1AD4 92BE 8824
[11:15] == #AntiMogul 5 [+Cnrt] Who is Mogul? Mogul is Domestic Overlord Trump. #AntiMogul will be the thorn in his side for at least the next 4 years | Twitter @AntiMogul |
http://pastebin.com/N2S2vPEf https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government || **#RULE41 Video** http://youtu.be/9WuJupWcobM
|| https://i.imgur.com/N3bBSHd.jpg
[11:15] == #livestreams 9 [+Cnrt] Thanks to everyone who tuned in and watched UFC 205! Our homepage: https://ghostbin.com/paste/t9oj7 , Put this channel on your autojoin list and keep an
eyeout for future events! Sister channel: #Televison
[11:15] == #operationitaly 2 [+Cnrt]
[11:15] == #czsk 4 [+Cnrt] Obnoveny kanal CZSK, pre vase napady pouzite pad: https://pad.riseup.net/p/czsk -- miki pre tor musis poziadat pristup v #help, viac info v pade
[11:15] == #ophungary 6 [+Cnrt] Welcome #opHungary | Üzenjük, hogy ők is Same in English!
[11:15] == #news.fr 7 [+Cmnrt] Nouvelles RSS Francophones - leparisien, clubic, cnetfrance, journaldunet, korben, lemonde, generationnt, lemondeinformatique, silicon, nextinpact, itpro, zdnet,
01net, france24, nouvelobs, rfi, developpez, & undernews
[11:15] == #blackhat 17 [+CRnrt] Welcome to Blackhat ~ Home of The Divine Order of Kek ~ *Actually Use 7 Proxies* ~ THIS IS NOT A DRILL ~ Rooting shit since 2600 B.C. #oppizza || #oppizza -
pizzagate.press || http://kekchanaymdxjuh6.onion/ || keksec.com || empire of the rooted shell REFLASH ALL YOUR SHIT TODAY || | BLEACHBIT || wipe with a cloth || dont idle
[11:15] == #italy 7 [+Cnrt] FB https://www.facebook.com/AnonymousItalyOperation
[11:15] == #TheAccountG 1 [+Cnt]
[11:15] == #lounge 25 [+CNPRnrt] Now life has killed the dream... I dreeeeeamed || it's a mad world || https://www.youtube.com/watch?v=GLG9g7BcjKs || use a hoe || https://www.youtube.com
/watch?v=vYyUb_MI7to
[11:15] == #bots 15 [+Cnrt] IRC Bot Channel || Read the rules before bringing your own bot on this network! || % = user bot owners + = user bots || Anonops Bot Rules: https://anonops.com
/bots.html || CONTACT A STAFF MEMBER BEFORE YOU JOIN A BOT ON THIS NETWORK || If you are not a bot owner GET THE FUCK OUT
[11:15] == #OpTurkey 1 [+Cnrt] Blog: opturkey.com | Mail: info@opturkey.com | PGP Fingerprint: E38A CCDF D6A6 6125 7688 A09A B688 1AD4 92BE 8824
[11:15] == #OpFerguson 2 [+Cnt]
[11:15] == #learninghub 22 [+Cnrt] Sick porn & hardcore IT training || Goldmine: www.ghostbin.com/paste/bjywz || Course count: 125
[11:15] == #OpIndiaPress 2 [+Cnrt] PRESS CHANNEL for #OpIndia
[11:15] == #ophungarygames 4 [+Cnrt]
[11:15] == #turkish 1 [+Cnrt] Blog: opturkey.com | Mail: info@opturkey.com | PGP Fingerprint: E38A CCDF D6A6 6125 7688 A09A B688 1AD4 92BE 8824
[11:15] == #opSyria 3 [+CTnrt] Guides & Links: https://anonops.com/sy/ :: Intro: http://tinyurl.com/lsf479g :: Other Channels: #opnewblood #news :: This is NOT the chan for conspiracy
theories. Please don't discuss them here. :: DDOS or Defacement? DISCUSS
[11:15] == #rawr 0 [+CPnt] .
[11:15] == #francophone 10 [+CKTnrt] Communauté Francophone IRC AnonOps || #Francophone sert à la discussion concernant les sujets sur Anonymous et les opérations de cet IRC. || Autres Canaux
FR: #Hackers.Fr #Linux.Fr #News.Fr #OpGraffiti || Discussion tout genre: #Random.Fr || Nouveaux pour votre sécurité et de l'aide IRC = /join #OpNewBlood.Fr
[11:15] == #OpBlackFlare 12 [+CJfnrt 60 *5:5] Fight POLICE BRUTALITY! | Channel focus: North Dakota Pipeline Protests | Add info to: https://pad.riseup.net/p/HTwfyURz2UGR
```


© Copyright - Bertin IT 2016

...monitorée en temps réel...

- Real time crawling, monitoring and archiving



...partageant des comptes d'un réseau


```
We are trying to stop a Terrorist Organization
from advancing any further.
Please understand that, and thank you.

Intel to add? PM: (last updated: 24.04.16)
- Vennox (Bitmessage: BM-2cTwwTDZw8vQwrqspKAR6V6iqnBdeR8svu)
- Darkshark


---------------------------------------------- ------------------------------ |
News:

New Information (24.04.16):
https://docs.google.com/document/d/1YeR8aS0_2d8qxP5myJskiT3OE5PX8JHLZIblhHANbC4/edit?pref=2&pli=1

---------------------------------------------- ------------------------------ |



---------------------------------------------- ------------------------------ |

#OPBrussels Information Pad / Informações Pad

---------------------------------------------- ------------------------------ |


https://twitter.com/opbrussels

#TogetherBrussels
```

```
==== START OF TARGETS ====

=================================================================
[ Twitter Accounts: ]
=================================================================


https://twitter.com/shirwan_k

https://mobile.twitter.com/uwaysT

https://twitter.com/sltan72648391

https://twitter.com/tbtytty

https://twitter.com/usjenkamasablji

https://twitter.com/0_jmaale2

https://twitter.com/_Wolfex_x

https://twitter.com/6309c843fecd40b

https://twitter.com/WESAM50016

https://twitter.com/6288Abo

https://twitter.com/wwwwkjhlasuepo2

https://twitter.com/L_L_016
```

```
================================================ ================
[Facebook Profiles:]
================================================ ================

https://www.facebook.com/zineb.amg.12

https://www.facebook.com/Djadiste-958694864154772/timeline?__mref=message_bubble

https://www.facebook.com/abelk.karim

https://www.facebook.com/elias.myl.5

https://www.facebook.com/profile.php?id=100011454576582
```

Source : GhostBin