VIGILANCE EXTERNE & INVESTIGATIONS EN SOURCES OUVERTES (OSINT)

La CTI* sur les Clearweb, Deepweb, Darkweb

- TRISTAN PINCEAUX
- HEAD OF CERT CWATCH - ALMOND

**CTI : Cyber Threat Intelligence*

almond

Agenda

- Les données existantes sur Internet
  - Clearweb, Deepweb, Darkweb
- Pourquoi surveiller son exposition externe
  - La démarche
  - Définir son périmètre
- Les outils de CTI et d'OSINT
  - Les modules de surveillance
  - L'analyse des résultats
- Enrichir et corréler
- Piloter l'évolution
- Que peut-on faire pour se protéger ?

MOVE FORWARD WE'LL WATCH YOUR BACK

À propos de Tristan

https://www.linkedin.com/in/tpinceaux/

Tristan Pinceaux

Incident handler / Forensic expert

Problem solver

> 12 ans d'expérience DFIR

Manager CERT

Ma vision : La sécurité ne doit pas coûter la liberté

Ma mission : Arrêter les cybercriminels avant qu'ils ne vous arrêtent

Qui sommes-nous ?

almond

AMOSSYS

Audit, conseil, formation, intégration, services managés en cybersécurité, cloud et infrastructure

Evaluation sécurité de produits et systèmes (CESTI)

Innovation et R&D cybersécurité

board of cyber

TrustHQ

Plateforme SaaS de cyber notation et de gestion du risque cyber

Groupe soutenu par seven2

(prise de participation minoritaire en juillet 2021)

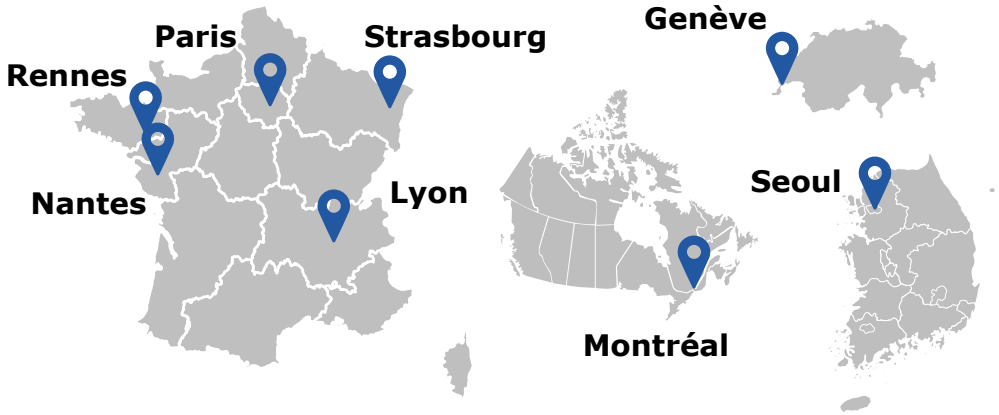
Chiffres clés

+440 collaborateurs

~60 M€ CA en 2022

+350 clients actifs

Maillage géographique



Notre offre de services

01. ANTICIPATION

Identifiez les risques, définissez les règles, préparez votre défense.

- Missions de conseil et d'audit
- Gouvernance & Risk Management
- Tests d'intrusion
- Cyber Threat Intelligence
- Conformité (PCI DSS, ISO 2700X, RGPD, DORA, NIS2, SWIFT, TISAX…)
- Plans de continuité / reprise d'activité
- Exercices de gestion de crise
- Centre de formation Almond Institute

02. PROTECTION

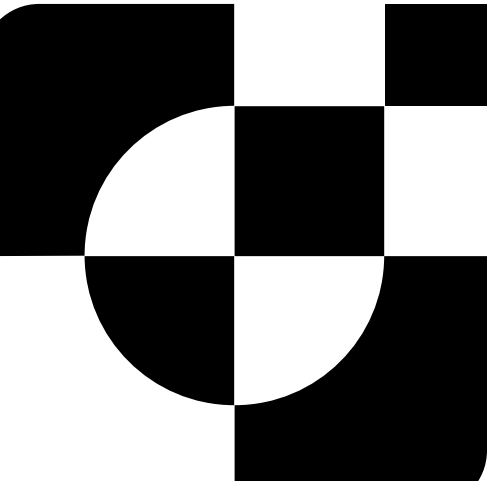
Armez-vous pour une sécurité optimale.

- Missions de conseil, AMOA et AMOE
- Intégration et supports de solutions de sécurité
- Services managés & infogérance
- Sécurité des infrastructures Cloud & IT
- Gestion des vulnérabilités
- IAM, protection des données
- Assistance technique et expertise

03. DETECTION

Repérez les incidents au plus tôt.

- Services managés MSSP : SOC + CTI + CERT
- Mission d'expertise construction services sécurité opérationnelle et déploiement de process et technologies DevSecOps
- Audit de SOC : efficacité, couverture de détection, état de l'art
- Produits venant des équipes innovation et R&D Almond et Amossys : OSINT, cyber range, adversary emulation, usecase management…



04. REACTION

Ne restez pas seul, agissez au plus vite avec nos experts.

- Mission CERT de réponse sur incident majeur
- Mission de recherche de compromission / levée de doute
- Forensic / investigations numériques
- Mission de reverse engineering logiciel et code malveillant
- Accompagnement à la gestion de crise, déploiement d'outil de gestion de crise
- Déploiement en urgence de solution de sécurité et services managés sur-mesure

05. RESTAURATION

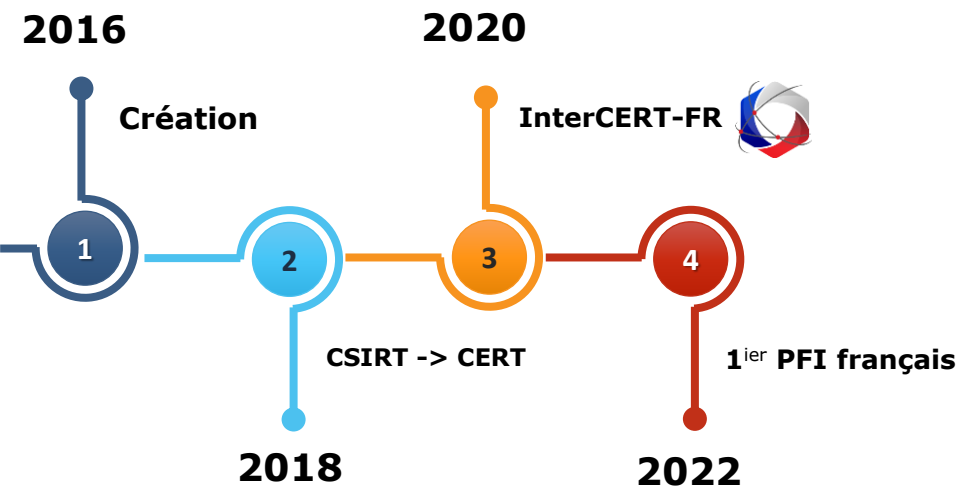
Optez pour une reconstruction efficace et un rétablissement optimal de vos opérations

- Mission de reconstruction partielle ou totale
- Transformation du système d'information et mise en place de services managés post crise
- Mission de conseil en résilience
- Assistance technique IT, Cloud et cyber sécurité

Le CERT CWATCH d'Almond

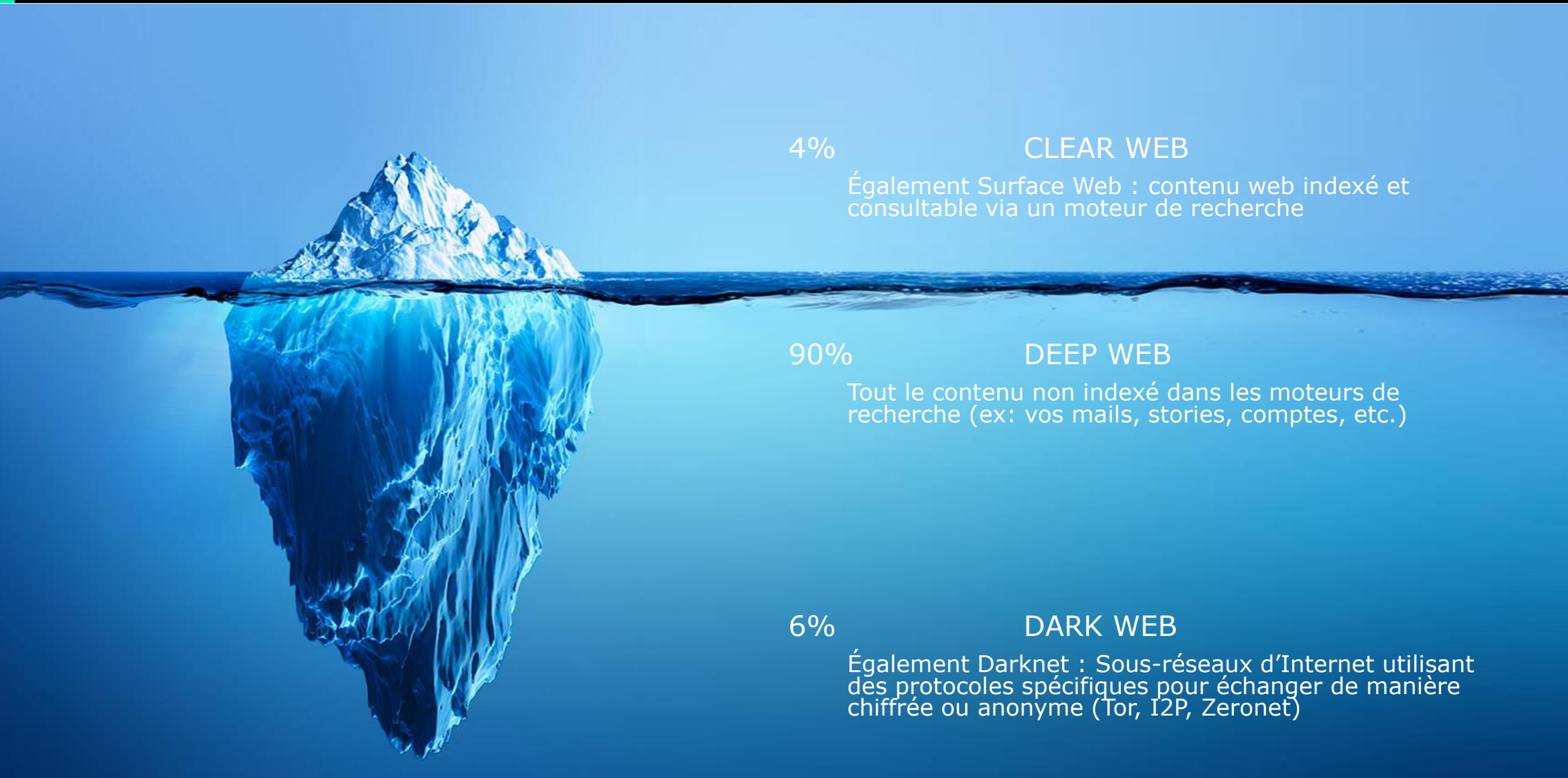
Computer Emergency Response Team

Que s'est-il passé ? → **Que devons-nous faire ?**



- **11** experts qualifiés et certifiés (PFI, GCFA, CISSP, QSA, …)
- **100+** interventions en 2022 et 2023
- ISO 27035, PRIS et NIST SP 800-61r2

Internet in a nutshell



4% CLEAR WEB

Également Surface Web : contenu web indexé et consultable via un moteur de recherche

90% DEEP WEB

Tout le contenu non indexé dans les moteurs de recherche (ex: vos mails, stories, comptes, etc.)

6% DARK WEB

Également Darknet : Sous-réseaux d'Internet utilisant des protocoles spécifiques pour échanger de manière chiffrée ou anonyme (Tor, I2P, Zeronet)

Que savez-vous vraiment du DarkWeb?

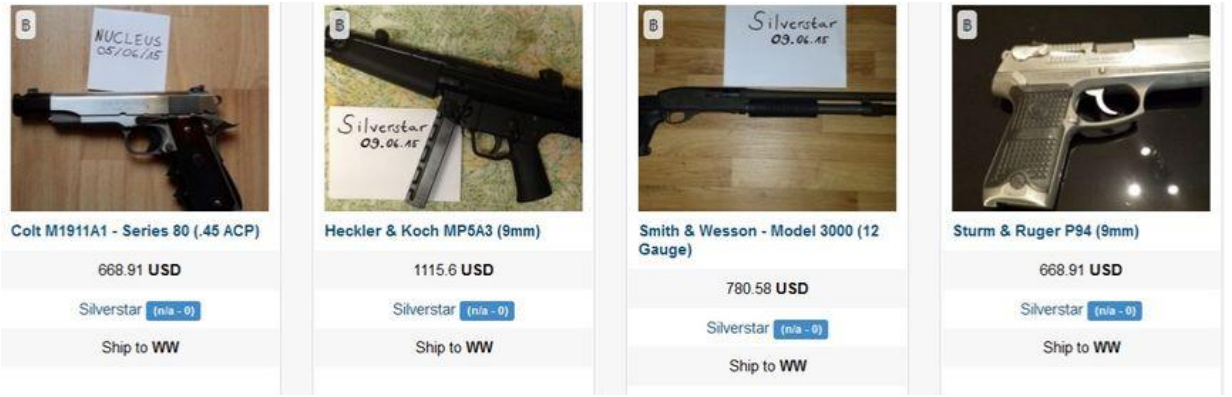
BFM TECH AVEC &CO

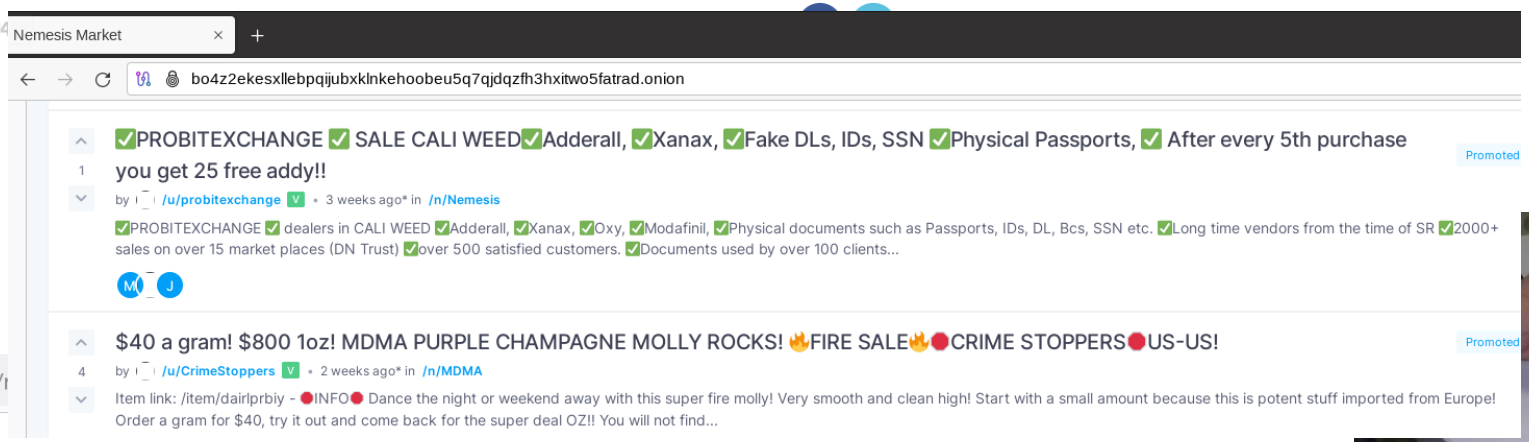
ÉMISSIONS ACTUALITÉS TESTS GUIDES ASTUCES GAMING PRODUITS SMARTPHONE ORDINATEUR ANDROID

TECH > CYBERSÉCURITÉ

20.000 DOLLARS PAR MOIS, TÉLÉTRAVAIL ET VACANCES À LA CARTE: LES OFFRES D'EMPLOI SÉDUISANTES DU DARK WEB

Julie Ragot Le 31/01/2023 à 14





https://www.francetvinfo.fr/

Rien d'illégal a priori

Se connecter au darknet n'est pas illégal en soi si l'on n'y fait rien d'illicite. C'est juste un peu compliqué techniquement. En fait, il existe plusieurs

01.

LES DONNÉES EXISTANTES SUR INTERNET

01.

Clearweb : Les données que vous souhaitez exposer (ou pas)

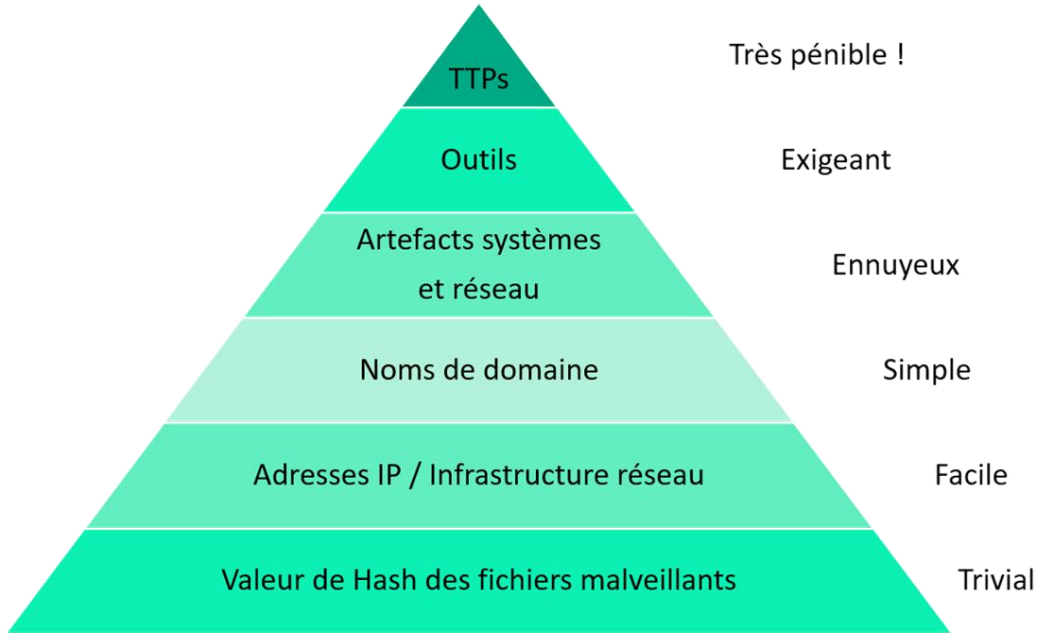
- Noms de domaines / site web
- Adresses IP
- Protocoles / services
  - Versions vulnérables ?
- Adresses mail / n° de téléphone
- Contenu déposé
  - articles, communiqués de presse
- Informations administratives
  - SIRET, siège social, capital, bilans, …
- Plans d'accès, liste des bureaux
- Les chiffres
  - CA, bilan,
  - Clients, nombre d'employés
- Appels d'offre publics
- Organigramme (ComEx, VIP)
- Employés, rôles et parcours
  - Réseaux sociaux
- Technologies utilisées et projets
  - CVs et Offres d'emploi
- Données personnelles de collaborateurs
  - nom, prénom, date de naissance
  - lieu de travail, n° de tél / mail, …
- …

Les données qui ne devraient pas être exposées

- Les données personnelles de collaborateurs
  - Nom, prénom, date de naissance
  - Numéro de téléphone, adresse de domicile
  - Rôle et lieu de travail, …
- L'activité en ligne
  - Heures de connexion
  - Géoposition, habitudes de consommation
  - Likes, commentaires, amis, centre d'intérêts, opinion
- Le résultat des fuites ou vols de données
  - Numéros de CNI, passeport, sécurité sociale
  - Mots de passe
  - Courriels et documents confidentiels (pdf, word, ppt, excel, …)
  - Token de session web (JWT, cookies, …)
  - Données financières : Portefeuilles Crypto, RIB, n° de cartes bancaires
- Sous-domaines cachés, domaines réservés ou internes
- Code source d'une application ou d'un site web
- Clés d'API ou mots de passe d'application
- Portail d'authentification exposé et/ou vulnérable
- Vulnérabilités
  - Chiffrement
  - Certificat expiré ou autosigné
  - Mauvaise configuration (service exposé / en écoute)
  - Bannière ou erreur trop verbeuse
  - Absence de patch de sécurité
- …

Les données utiles pour la surveillance des cybercriminels

- Les domaines créés lors des campagnes de phishing
- Les certificats de sites web générés
- Les identités numériques
  - Pseudo
  - Langue, jargon employé, façon de parler
  - Dates d'inscription et des posts (périodes d'activité)
  - Les forums utilisés, les sujets de prédilection
- Les posts sur les forums
  - Les demandes d'accès
  - La mention d'intérêt
  - La revente de données
  - L'hacktivisme
- Les victimes (via le Data Leak Site)
  - Les secteurs visés
  - Les revendications
  - Les rançons
- Les TTPs des précédentes attaques de l'acteur cybermalveillant
  - Mitre ATT&CK
  - Profiling / Portraits-robots
- ...



Pyramide de la douleur - David J. Bianco (01/03/13)

02.

POURQUOI SURVEILLER SON EXPOSITION EXTERNE

02.

La démarche : renforcer ses capacités de détection

- Le niveau de maturité de la vigilance interne a augmenté
  - Les petites structures sont équipées en EDR
  - Les SOC ont du succès
  - Les méthodologies d'analyse de risques sont continuellement mises en œuvre

Utiliser Internet

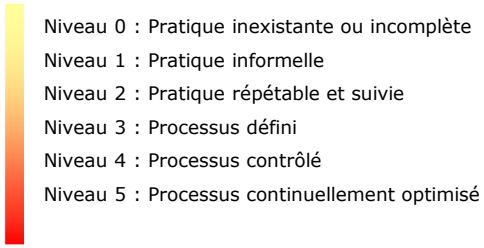
comme un atout

pour se protéger

- **Voir au-delà de son SI**
  - Qui s'intéresse à nous ?
  - Espaces publics : Quelles infos communiquent les collaborateurs ?
  - Quelle est notre réputation sur les réseaux ?
  - Y'a-t-il du Shadow IT non maitrisé ?
  - Sommes-nous la cible d'usurpation d'identité / faux profils / phishing ?
  - Que peut trouver un **attaquant** s'il souhaite pénétrer notre SI ?

L'ISO 21827 a défini 5 niveaux de maturité SSI

- https://www.ssi.gouv.fr/uploads/2009/07/maturitessi-methode-2007-11-02.pdf



Définir son périmètre

- **Prévenir plutôt que guérir**

- Quels sont mes risques ?
  - Les menaces affrontées ?
  - Les techniques employées par les criminels visant mon secteur ?
  - Les données ciblées ?

- Quels sont les moyens à disposition ?
  - Outils de scan automatique
  - Google Dorking
  - Bases de données ouvertes
  - Investigations manuelles avec des machines dédiées (stations blanches)
  - […]

« Connais ton ennemi et connais-toi toi-même. »

Sun Tzu

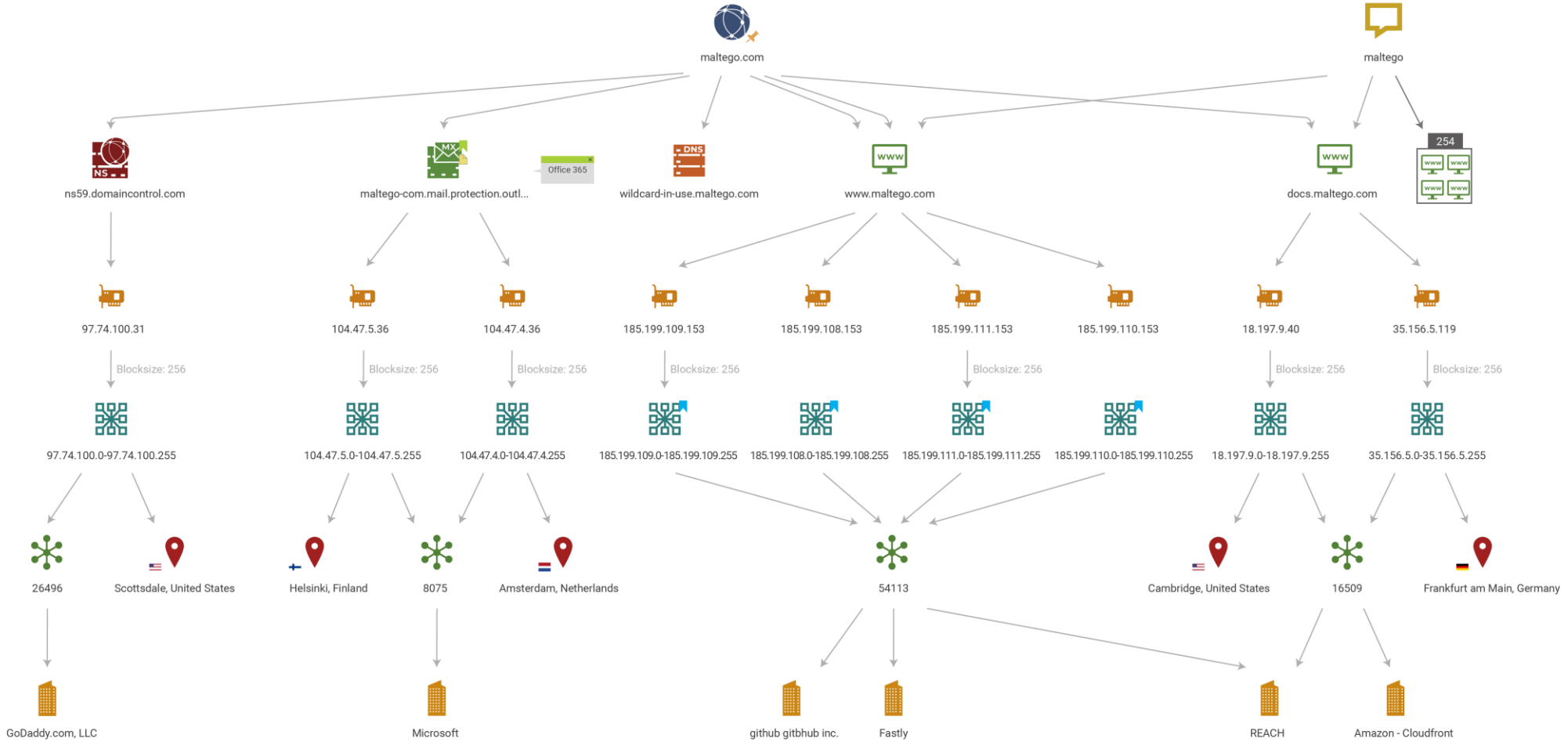
03.

COMMENT ?
LES OUTILS DE CTI ET OSINT

03.

Profiler les groupes cybercriminels

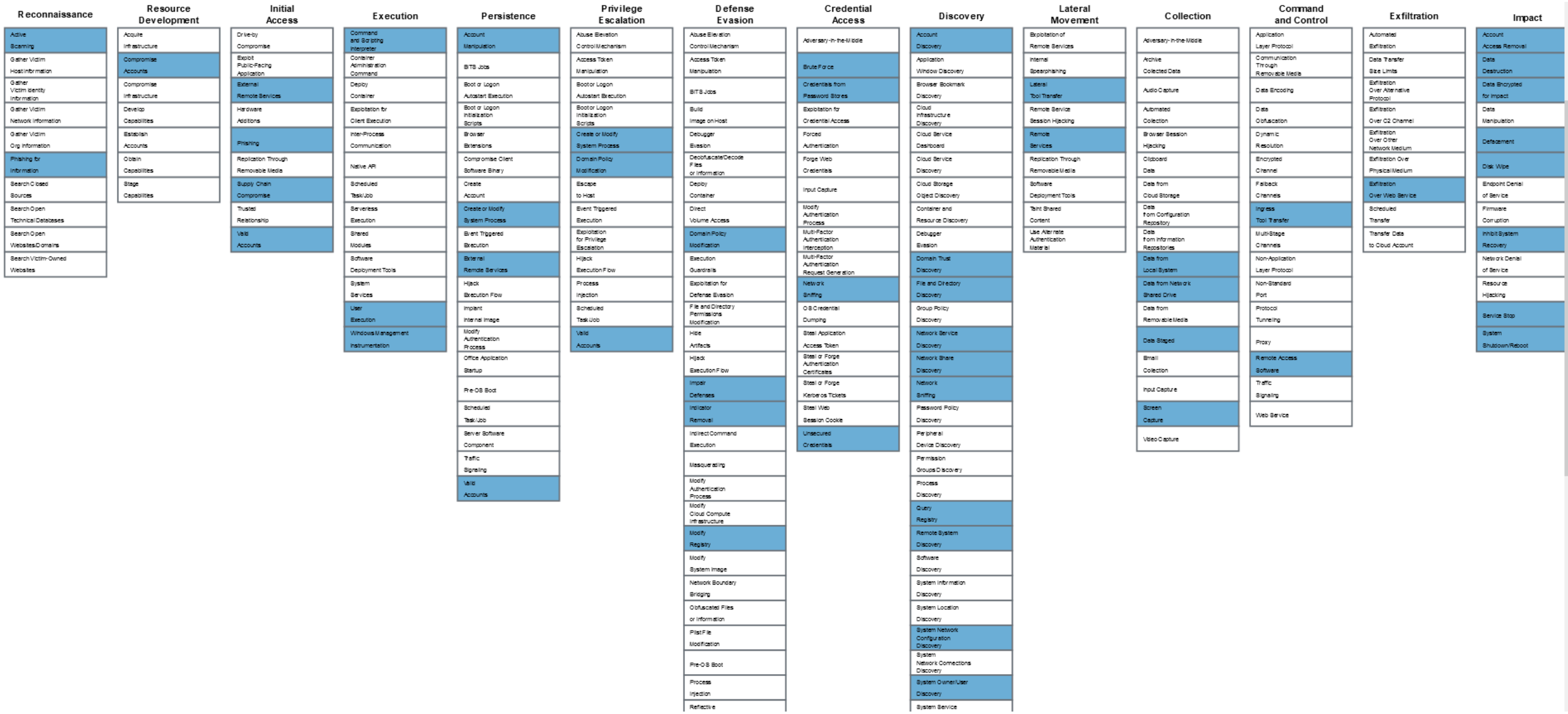
- Représentation des actions d'un attaquant sur un tableau blanc



Utilisation de l'outil Maltego

Framework Mitre ATT&CK et les heatmaps

almond



Présentation des outils de CTI

Des **crawlers** :
Robots d'indexation qui explorent le Web, conçus pour collecter les ressources

Des **scrapers** :
Scripts d'extraction du contenu de sites Web

Des **parsers** :
Analyseurs syntaxiques mettant en évidence la structure d'un texte

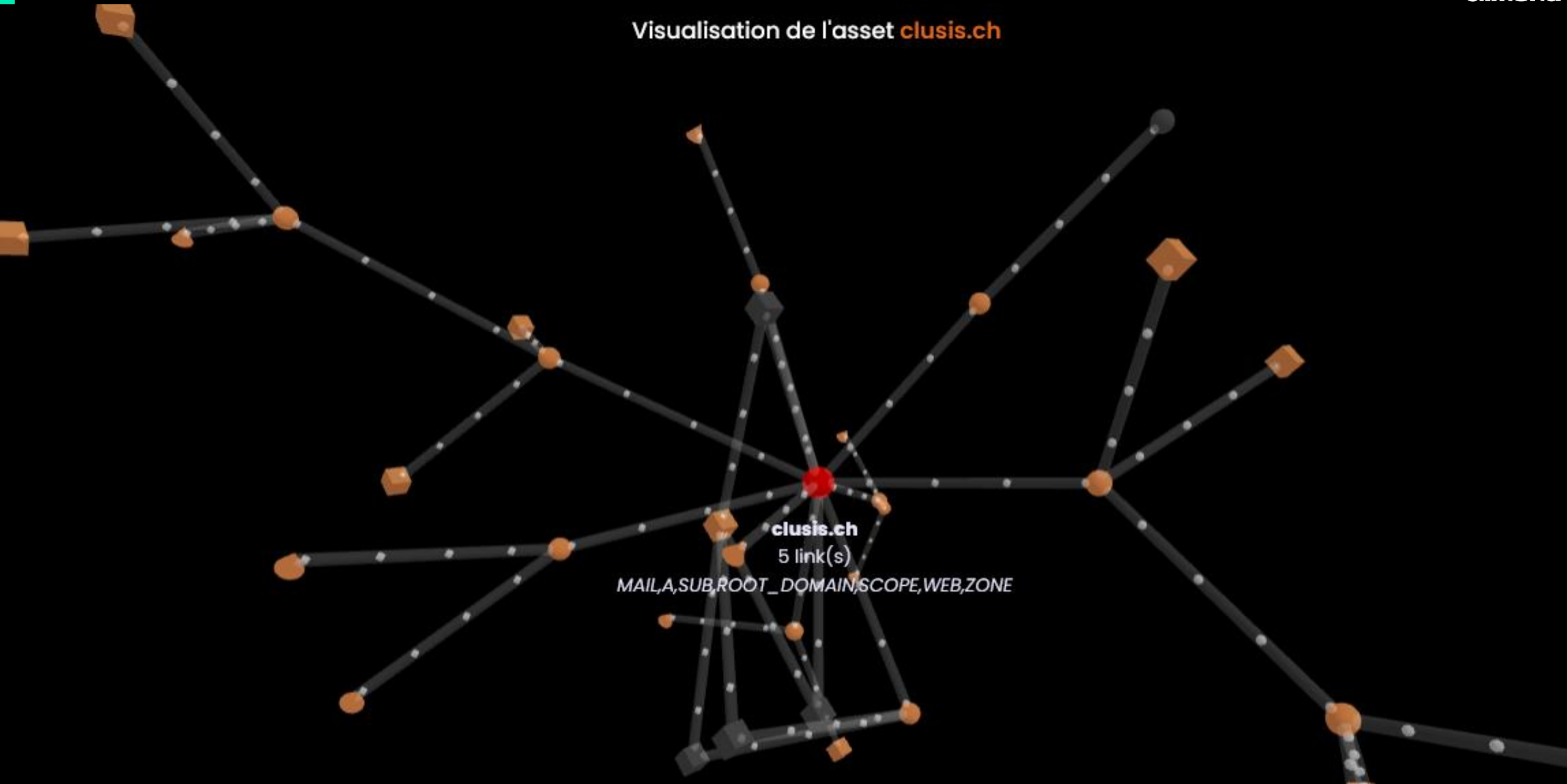
Des **bases de données** :
Pour stocker ces informations et garder un historique

Des infiltrations dans les forums (HUMINT)

Module	Icon	Goal of the module
Credentials		Retrieve stolen credentials from botnets and detect infections.
Credit Cards		Retrieve stolen credit cards from infected POS and blackmarkets.
Malware		Locate malware samples targeting your assets and analyze malware.
Data Leakage		Locate confidential or sensitive information in repositories or P2P networks (docs, source code, etc.)
Hacktivism		Identify hacktivism attacks, mentions, defacements or vulnerabilities.
Social Media		Locate brand abuse threats or negative comments, protect your VIPs.
Mobile App		Locate brand abuse in apps or non-authorized app distribution as well as mobile phishing or rogue apps
Domain Protection		Identify Phishing or Cybersquatting threats or counterfeiting.
Dark Web		Locate information in the Dark Web from onion URLs, documents or sensitive and confidential data
Threat Context		Monitor threat actors, TTPs, campaigns and perform threat hunting as well as investigations

Cartographie

almond



Domaines similaires

Utilisation d'un outil de DNS twister (distance de Levenshtein) pour détecter des sites de phishing

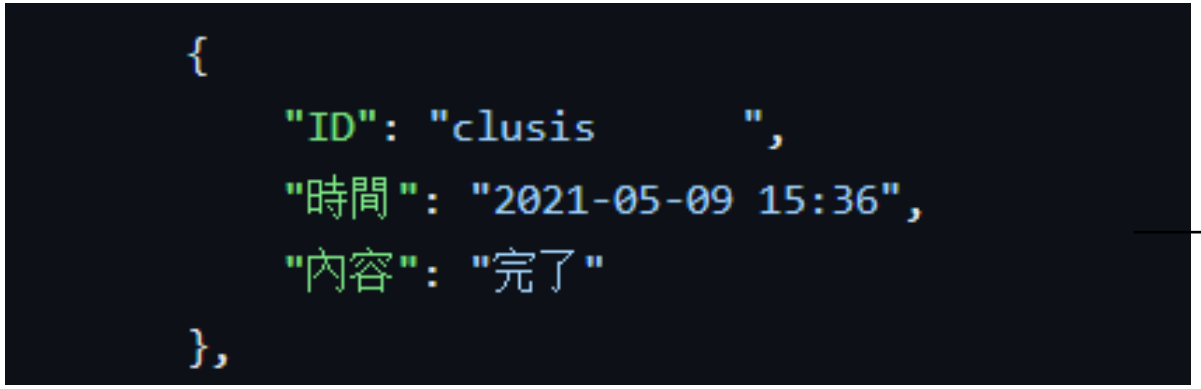
Domain	IP Address / A record	MX record?
alusis.com	185.46.40.47	✓
elusis.com	13.248.169.48	✗
clusis.com	83.166.138.38	✗
klusis.com	172.67.209.30	✓
clousis.com	149.50.132.80	✓
clesis.com	52.71.57.184	✗
cl.usis.com	192.157.56.139	✗
clasis.com	64.190.63.111	✓
clisis.com	207.148.248.143	✗
clsis.com	72.167.76.150	✓

Domain	IP Address / A record	MX record
glusis.ch	185.230.63.107	✓
clusis.ch	141.101.62.153	✓
clusis.com	83.166.138.38	✗
cludis.ch	52.211.184.61	✓
clusius.ch	3.33.130.190	✓

INTERNET ARCHIVE

Qui parle de vous ?

Détecter des campagnes d' « Hacktivisme »



Mention du Clusis dans des listes d'entreprise sur github : https://github.com/ji08kk44/BDSE26_TEAM3

Correspond à un cours de Big Data dans une université à Taipei

We need the people to get educated. I think that, on this topic, we do have a lot of associations and projects which are doing a great job: I think about APWG, ENISA, CLUSIT in Italy (and, CLUSIF in France, CLUSIS in Switzerland, etc), many EU-funded research projects such as ACDC and Cyberoad, and a lot of so-called "underground" conferences, such as Hack in the Box AMS, CONFidence, St.Hack, ATHCon, just to mention some of the biggest and smallest we have in Europe. On the other hand, security needs sacrifices, it isn't an easy mission to accomplish. We must give up on something, if we

Article de « Security Affairs » mentionnant le Clusis

Investigation Telegram

almond

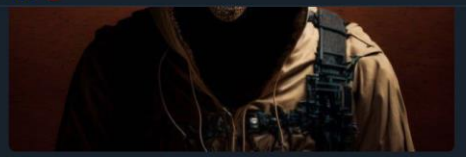
Rechercher des signes d’attaques sur des channels semi-public

❗ Next target: France

Because of the offensive caricature of the Prophet Muhammad

Anonymous Sudan
11438 subscribers

Pinned message



❗ Мы все будем атаковать через 15 минут | We'll all attack After 15 Min from now

Airports:

https://www.parisaeroport.fr/

https://www.annecy-airport.com/

https://www.parisvatry.com/

https://www.euroairport.com/

https://www.pau.aeroport.fr/

http://www.brest.aeroport.bzh/

Hospitals:

https://www.american-hospital.org/

https://www.aphp.fr/

https://pitiesalpetriere.aphp.fr/

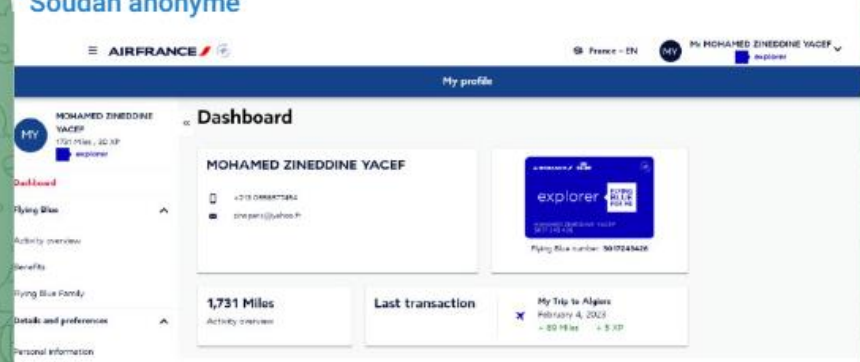
https://hopital-necker.aphp.fr/

https://hopital-georgespompidou.aphp.fr/

https://hopital-bichat.aphp.fr/

#AnonymousSudan

Soudan anonyme



❗ La compagnie aérienne française: airfrance a été piratée

Une grande partie de leurs données a été consultée, certaines seront divulguées pour preuve

#AnonymousSudan

2.8K édité 12:46

Soudan anonyme

Soudan anonyme

❗ La compagnie aérienne française: airfrance a été piraté...

AirFrance.txt
380 B

https://wwws.airfrance.fr/ #AnonymousSudan

Credentials leaks

almond

Utilisation de bases de données historiques ou provenant de botnets d'infostealers

EXCLUSIVE USE - HIGHLY CONFIDENTIAL

Reported At	Username	Password/Hash	Portal URL	Type	Bot IP	Bot City	Bot Country	Bot Lat	Bot Lon
2023-02-27 08:14:45	646253 REDACTED	12349876	REDACTED	ARKEI					
2023-02-01 23:43:05	518323 REDACTED	navidiwu	REDACTED	REDLINE	82.65.187.32	Coignieres	France	48.7501	1.9146
2023-03-26 19:20:17	LMASSU REDACTED	Murmuratil1984	REDACTED	REDLINE	41.248.138.87	Rabat	Morocco	34.0123	-6.8484
2023-02-03 20:47:29	754687 REDACTED	ROubaix1@	REDACTED	REDLINE	90.45.55.12	Lille	France	50.624	3.0511
2022-12-19 10:42:56	475474 REDACTED	25081967	REDACTED	RACCOONSTEALER	196.127.109.198	Casablanca	Morocco	33.5922	-7.6184
2023-03-08 11:46:52	vincent REDACTED	lferkij81A	REDACTED	ARKEI					
2022-12-19 10:42:57	475474 REDACTED	25081967	REDACTED	RACCOONSTEALER	196.127.109.198	Casablanca	Morocco	33.5922	-7.6184
2023-03-08 11:47:01	vanessa REDACTED	Magnolia76	REDACTED	ARKEI					
2022-06-20 07:30:14	825166 REDACTED	AgcTls31	REDACTED	REDLINE					
2023-01-21 21:53:07	herman REDACTED	hermand2019	REDACTED	REDLINE	41.141.164.149	Casablanca	Morocco	33.5922	-7.6184
2023-03-23 14:35:26	523255 REDACTED	osehtilx	REDACTED	RACCOONSTEALER	41.230.81.207	Tunis	Tunisia	36.8232	10.1701
2022-12-19 10:43:07	marcleg REDACTED	oMARCH91	REDACTED	RACCOONSTEALER	196.127.109.198	Casablanca	Morocco	33.5922	-7.6184
2023-02-01 23:43:12	518323 REDACTED	navidiwu	REDACTED	REDLINE	82.65.187.32	Coignieres	France	48.7501	1.9146
2022-04-29 21:26:28	877514 REDACTED	lamiaomc82	REDACTED	REDLINE					
2023-02-03 20:46:49	754687 REDACTED	rOUBAIX1	REDACTED	REDLINE	90.45.55.12	Lille	France	50.624	3.0511
2023-03-23 14:35:26	482446 REDACTED	celinealves2017	REDACTED	RACCOONSTEALER	41.230.81.207	Tunis	Tunisia	36.8232	10.1701
2022-10-27 16:20:53	532646 REDACTED	Nrab19	REDACTED	RACCOONSTEALER	41.249.147.77	Marrakesh	Morocco	31.6298	-8.0101
2022-06-27 09:48:16	813311 REDACTED	wchgabbq	REDACTED	REDLINE	91.164.184.4	Épinay-sur-Seine	France	48.9512	2.3144
2023-02-03 07:07:14	124162 REDACTED	rockito94	REDACTED	RACCOONSTEALER	88.123.126.137	Beton-Bazoches	France	48.7004	3.241
2022-04-29 21:26:27	745666 REDACTED	omc82290	REDACTED	REDLINE					
2023-02-03 12:08:27	Adam35 REDACTED	coulibaly35	REDACTED	REDLINE	41.141.163.152	Casablanca	Morocco	33.5922	-7.6184
2022-12-19 10:43:07	781834 REDACTED	ghait1001	REDACTED	RACCOONSTEALER	196.127.109.198	Casablanca	Morocco	33.5922	-7.6184
2023-03-31 02:28:08	737445 REDACTED	pedtlmhv	REDACTED	RACCOONSTEALER	41.250.202.136	Casablanca	Morocco	33.5922	-7.6184

Investigation des documents publics CLUSIS

CLUSIS

[redacted]

facture -00093

date:	18.01.2021	payable à:	16.02.2021
période de prestation :	01.01-31.12.2021	numéro de client :	[redacted]

Nouvelles coordonnées bancaires !

Banque Cantonale Vaudoise : IBAN [redacted]
Compte numéro: [redacted]
Communication : Cotisation 2021

Nous vous remercions par avance de vous acquitter de ce montant sur le compte du Clusis.

Afin d'éviter des frais financiers, veuillez utiliser de préférence l'e-banking et le compte IBAN.
Si vous payez au guichet de la poste, merci d'ajouter CHF 2.35 au montant de la cotisation.

description	prix net CHF
Cotisation annuelle - membre entreprise	500.00
Membre entreprise	
montant de la facture défiscalisé	**500.00**

Facture d'un adhérant disponible sur internet

Data Leak

Cas réels de fuites de données sensibles et du secteur de la défense

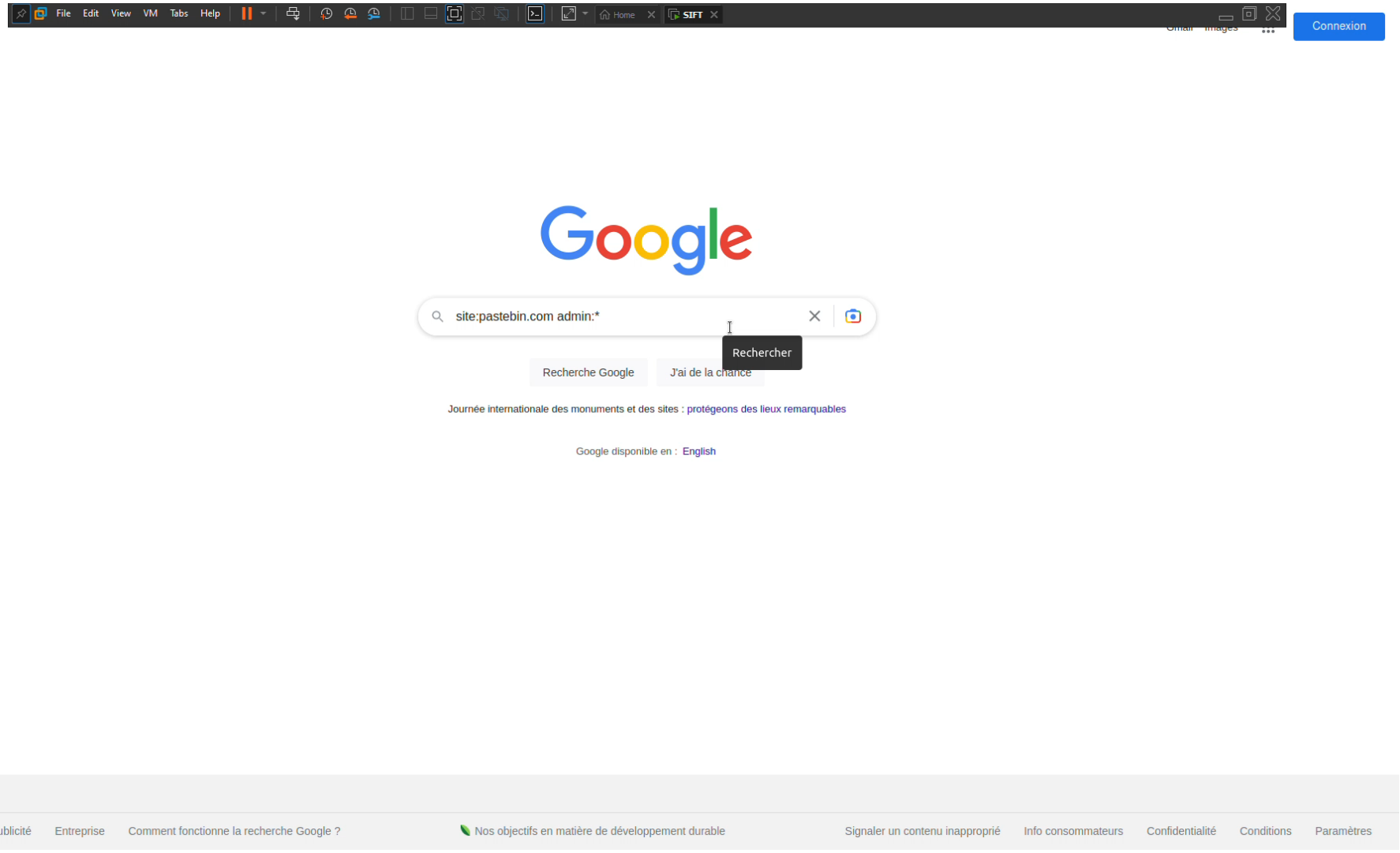
```
8002 Edmund Halley Drive
Reston, VA 20191
CoreSite's facility is on the left when you turn into the parking lot.

IAD54
Contact: iad-logistics@amazon.com
43791 Devin Shafron Dr.
Ashburn, VA 20147

IAD55
Contact: iad-logistics@amazon.com
15395 John Marshall Hwy
Haymarket, VA 20169

IAD56
Contact: iad-logistics@amazon.com
45210 Prologis Plaza, Sterling, VA 20166

IAD57 - Prologis building 10
Contact: iad-logistics@amazon.com
22755 Relocation Drive
Sterling, VA 20166

IAD58
22745 Relocation Drive,
Sterling, VA 20166

IAD59
Contact: iad-logistics@amazon.com
7600 Doane Drive
Manassas, VA 20109

IAD60
Contact: iad-logistics@amazon.com
21267 Smith Switch Rd
Ashburn, VA 20147

IAD66 (Equinix DC11)
Do not ship directly to this location without emailing iad-management@ first. Redirect
shipment to IAD6.
- Exceptions are made under certain circumstances for DWDM. Tracking numbers need to be
provided prior to the equipment showing up, or else Equinix WILL reject the shipment.
Contact: iad-logistics@amazon.com
21721 Filigree Court
Ashburn, VA 20147
```

```
INSERT INTO "afg" VALUES('FFQLVQ','14 EXP ASO (FFQLVQ)','FA6537','5865015337406','COUNTERMEASURES SET-(WARLOCK DUK','
INSERT INTO "afg" VALUES('FH00B0','AFOSI EDET 2405 (FH00B0)','AC0001','582001V090070','ACORN IED JAMMER','V','TPE','N
INSERT INTO "afg" VALUES('FH00B0','AFOSI EDET 2405 (FH00B0)','FA6537','5865015337406','COUNTERMEASURES SET-(WARLOCK D
INSERT INTO "afg" VALUES('FHXFX0','755 ESFS-CC (FHXFX0)','J85705','8470015207370','INSERTS,ENHANCED SM','N','TPE','N'
INSERT INTO "afg" VALUES('FHXFX0','755 ESFS-CC (FHXFX0)','J85705','8470015207373','INSRTS ENHNCD SM MED','N','TPE','N
INSERT INTO "afg" VALUES('FHXFX0','755 ESFS-CC (FHXFX0)','J85705','8470015207382','INSRTS ENHNCD SM XLG','N','TPE','N
INSERT INTO "afg" VALUES('FHXFX0','755 ESFS-CC (FHXFX0)','J85705','8470015207385','INSRTS ENHNCD SM LG','N','TPE','N'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','70169N','582000K046777','MOTOROLA ASTRO/SPECTR','N','TP
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','70169N','582000X242630','RADIO MOTOROLA 2WAY','N','TPE'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','70169N','582001C022615','RADIO 2 WAY VOICE ACTIVATED 1/
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','A26852','4120012834096','AIR CONDITIONER','H','LTT','N'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','A27104','6515014491423','ANALYZER NONINVAS BLD','H','LT
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','A55800','6630014151593','ANALYZER CLIN CHEM','H','LTT',
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','A79381','5985010631574','ANT GRP OE-254()/GRC','H','LTT
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','A83433','6515014491420','ANALYZER DEFIB & TRAN','H','LT
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','A84342','6630014689142','ANALYZER HEMATOLOGY','H','LTT'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','C05701','6665013578502','IMPROVED CHEM AGT MON','H','LT
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','C19266','6625012713012','CNTR E R: AN/USM-459A','H','LT
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','D78555','5810013931973','D T D ANCYZ-10 V3','H','LTT','
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','D89418','8470015269163','DELTOID AND AXILLAR','N','TPE'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','DA708G','8470015367227','INSERT,SMALL ARMS P','N','TPE'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','DA709B','8470015370504','CARRIER ASSEMBLY,UN','N','TPE'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','E98103','5810010269618','ELEC KEY KYK-13/TSEC','H','LTT
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','FA0501','580501D046877','MODULE VOICE, SECURE: 9505 IRI
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','FA0510','580501C007687','TELEPHONE SATELLITE: HNS-7100
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','FA2008','582001C011976','RADIO SET : XTS 3000 MOTOROLA'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','FA956S','589501C025322','RECEIVER SCANNER: IC-R3','N','
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','FJ258N','702501C042780','MULTI-MODAL BIOMETRIC COLLECTI
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','J35801','6115011340165','GEN ST 100KW PU495B/G','H','LT
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','J85705','8470015207370','INSERTS,ENHANCED SM','N','TPE'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','J85705','8470015207373','INSRTS ENHNCD SM MED','N','TPE
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','J85705','8470015207382','INSRTS ENHNCD SM XLG','N','TPE
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','J85705','8470015207385','INSRTS ENHNCD SM LG','N','TPE'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','K47623','5810013910187','KY 99A MINTERM','H','LTT','N',
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','L63833','6520000000158','LIGHT SET DENT 115V','H','LTT'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','L67964','5815011877844','LTWT DIG FAC AN/UXC-7','H','LT
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','M23954','6625011452430','MULTIMTR AN/USM-486','H','LTT'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','M30817','6525014802199','COMPUTER RADIOGRAPHY','H','LTT
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','M30817','6525015045002','COMPUTED RADIOGRAPHY','H','LTT
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','M60449','6625012656000','MULT DIGIT AN/PSM-45A','H','LT
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','M66626','6515014322707','VITAL SIGNS MONITOR','H','LTT'
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','M72868','6545011823798','MMS ORTHO CAST CLINIC','H','LT
INSERT INTO "afg" VALUES('FM6924','455 EMDG TF MED (FM6924)','M72936','6545011823786','MMS OPERATING ROOM','H','LTT',
```

Leak avec toutes les coordonnées de gérant de DC Amazon hébergeant des données du D&D
Base SQL contenant une liste de tous les équipements militaires utilisés en Irak et en Afghanistan

Investigation manuelle

Utilisation de Google Dorking pour rechercher des mots de passe fuités

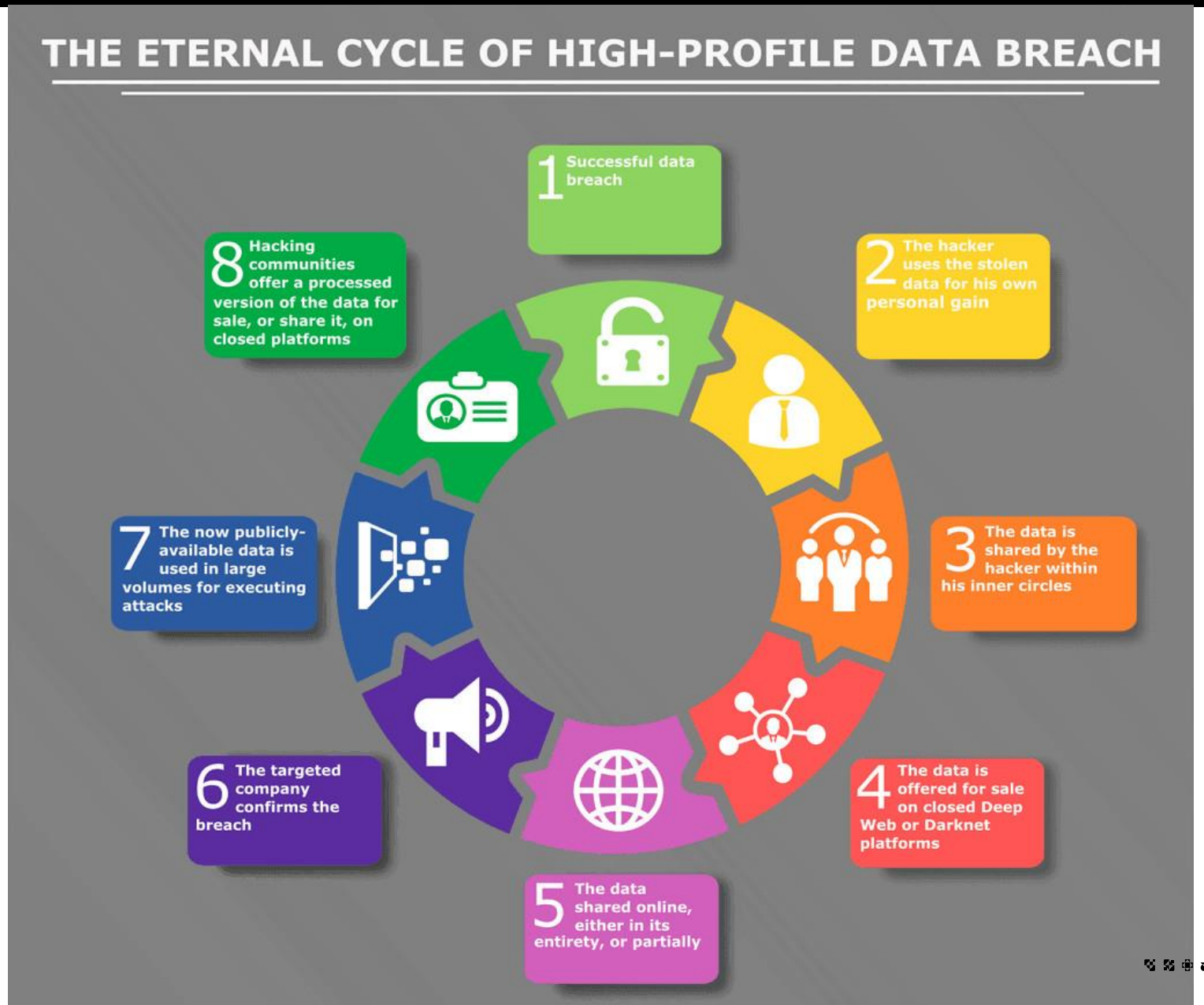


04.

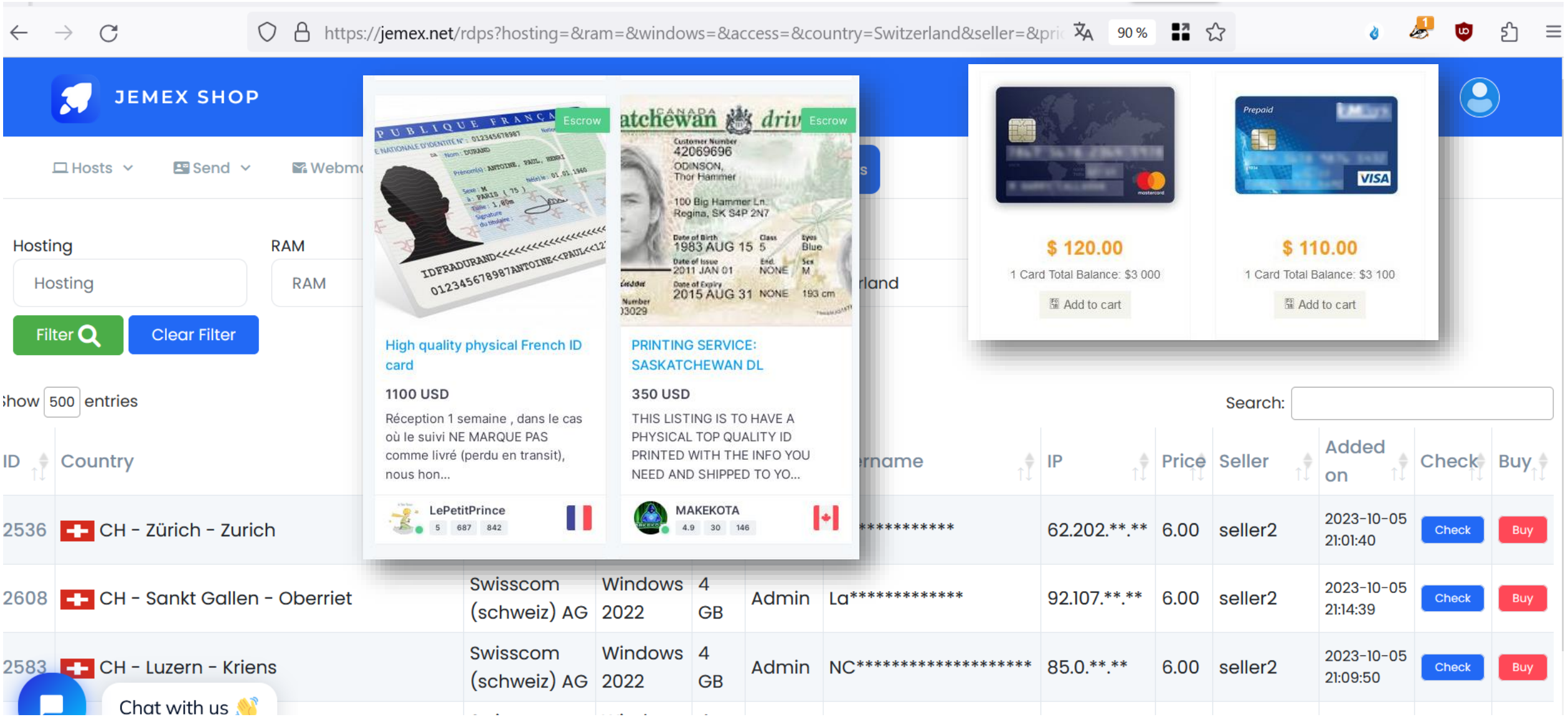
ENRICHIR ET CORRELER

04.

Cycle de vie de la donnée

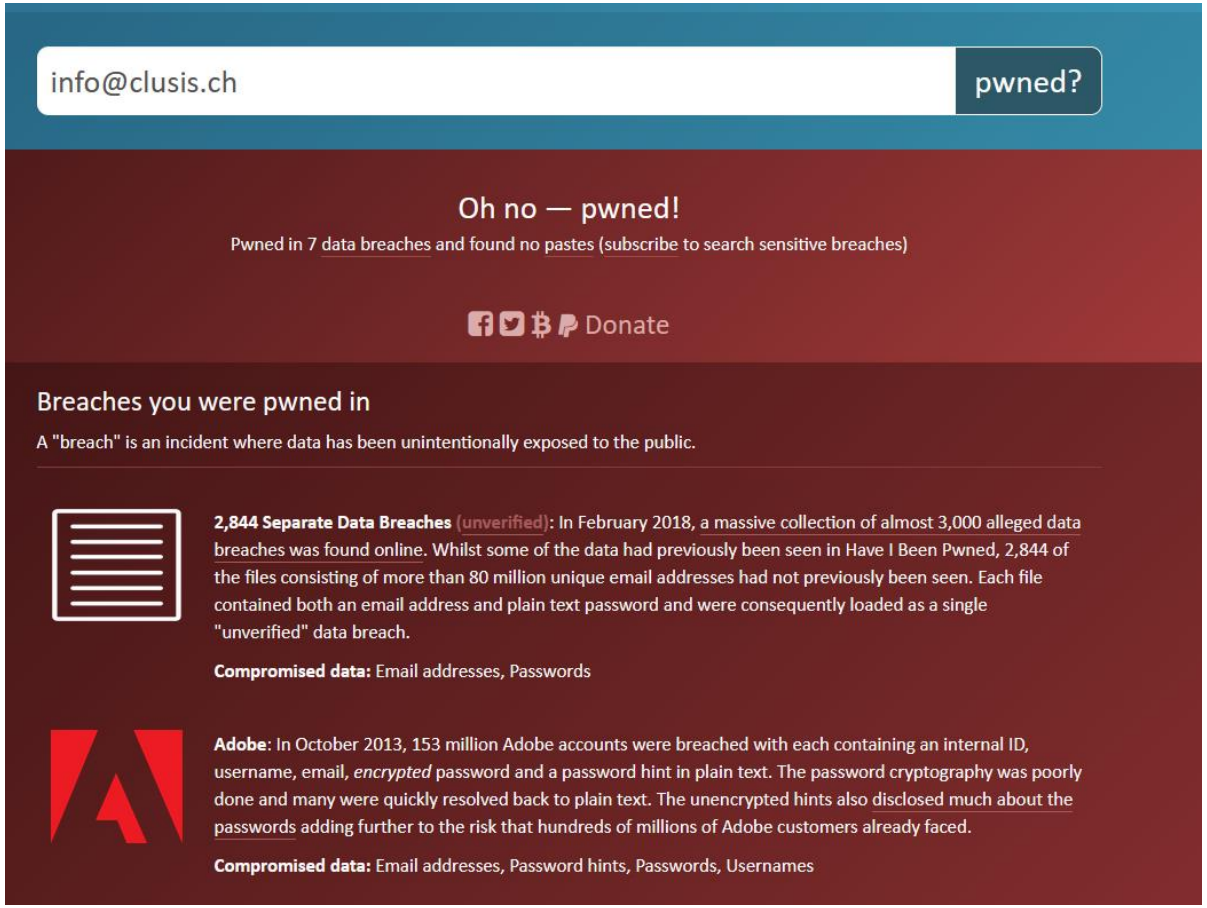


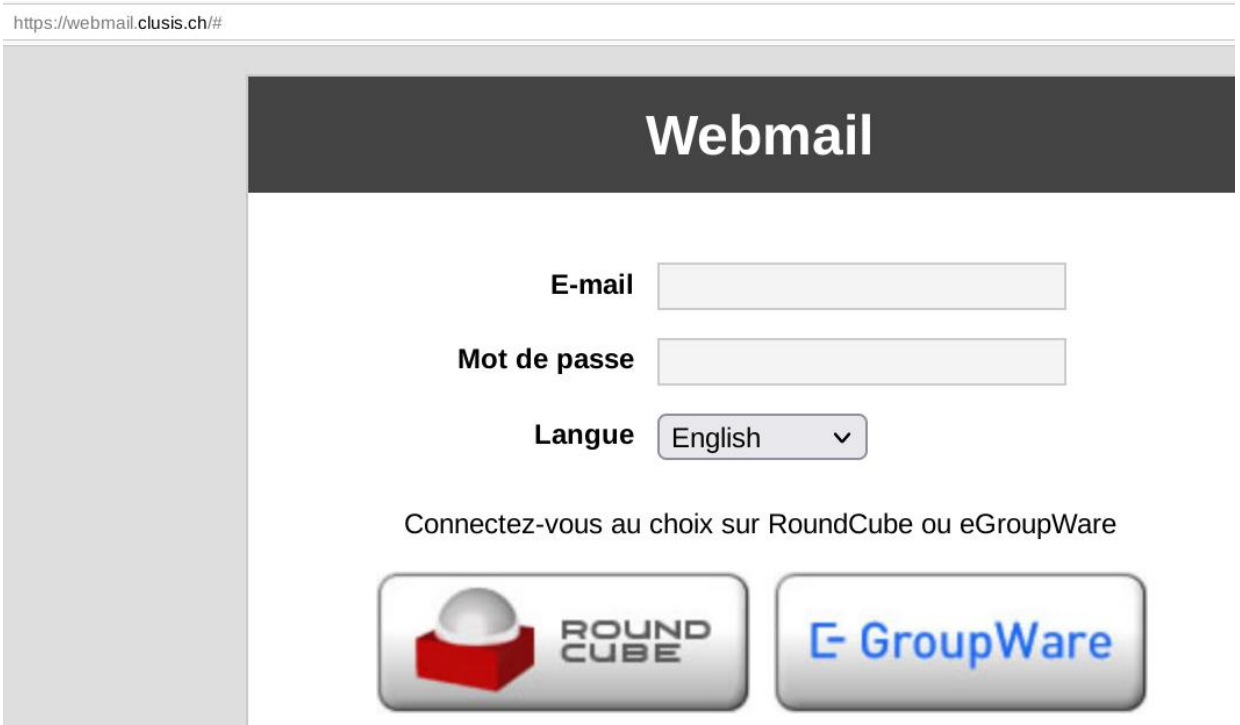
La donnée vaut de l'argent



Analyse manuelle – Pivot avec des nouvelles données

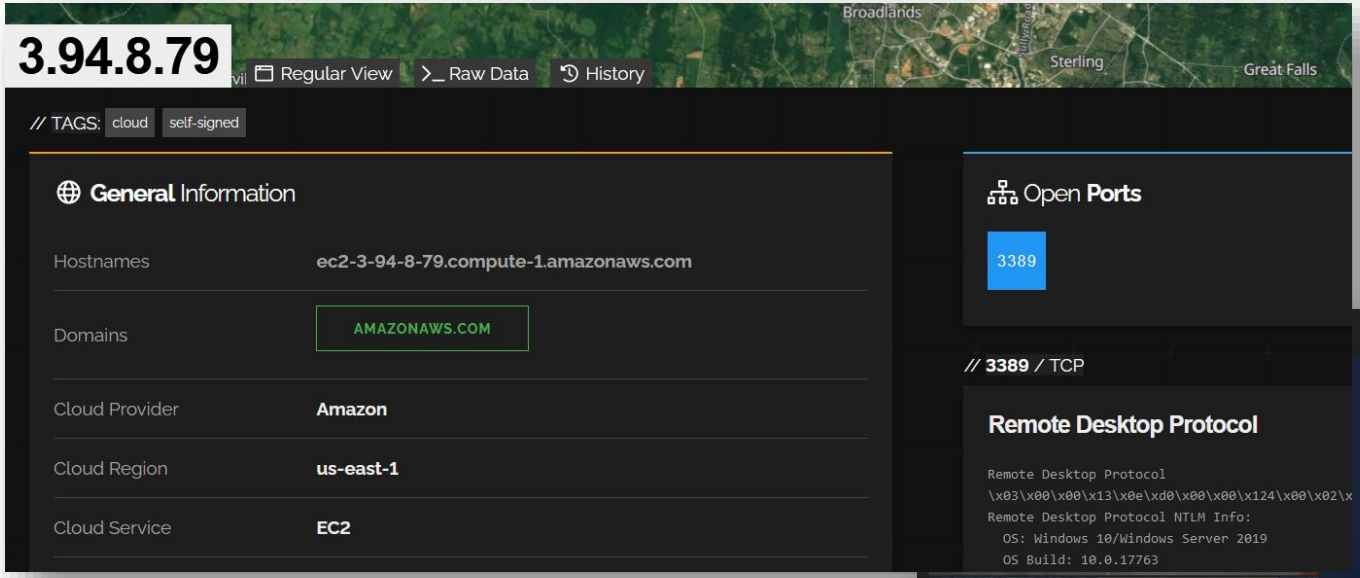
Exemple : Intégration des nouvelles données dans les outils automatique – Cas d'un compte « info »

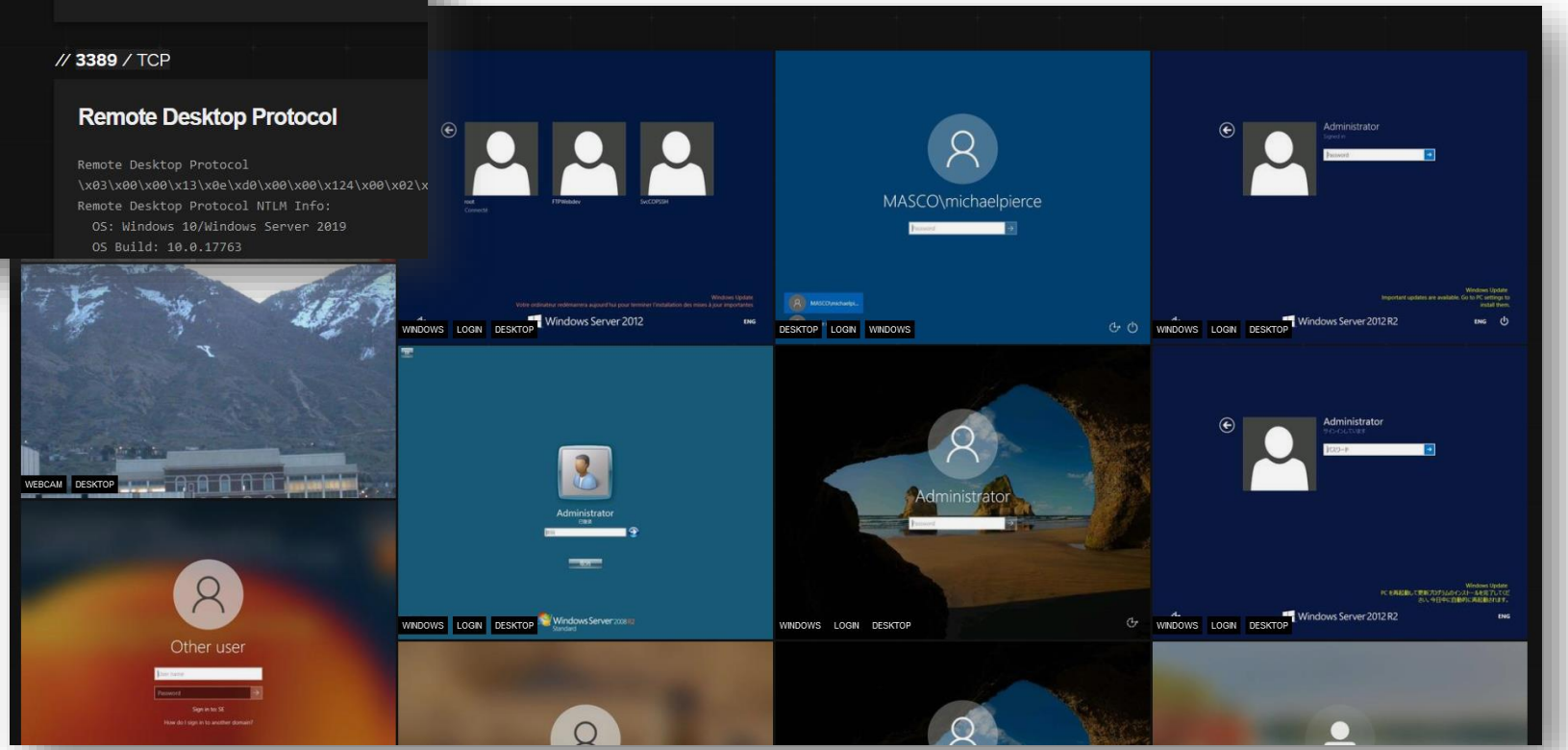




Utiliser les bases ouvertes pour enrichir le contexte

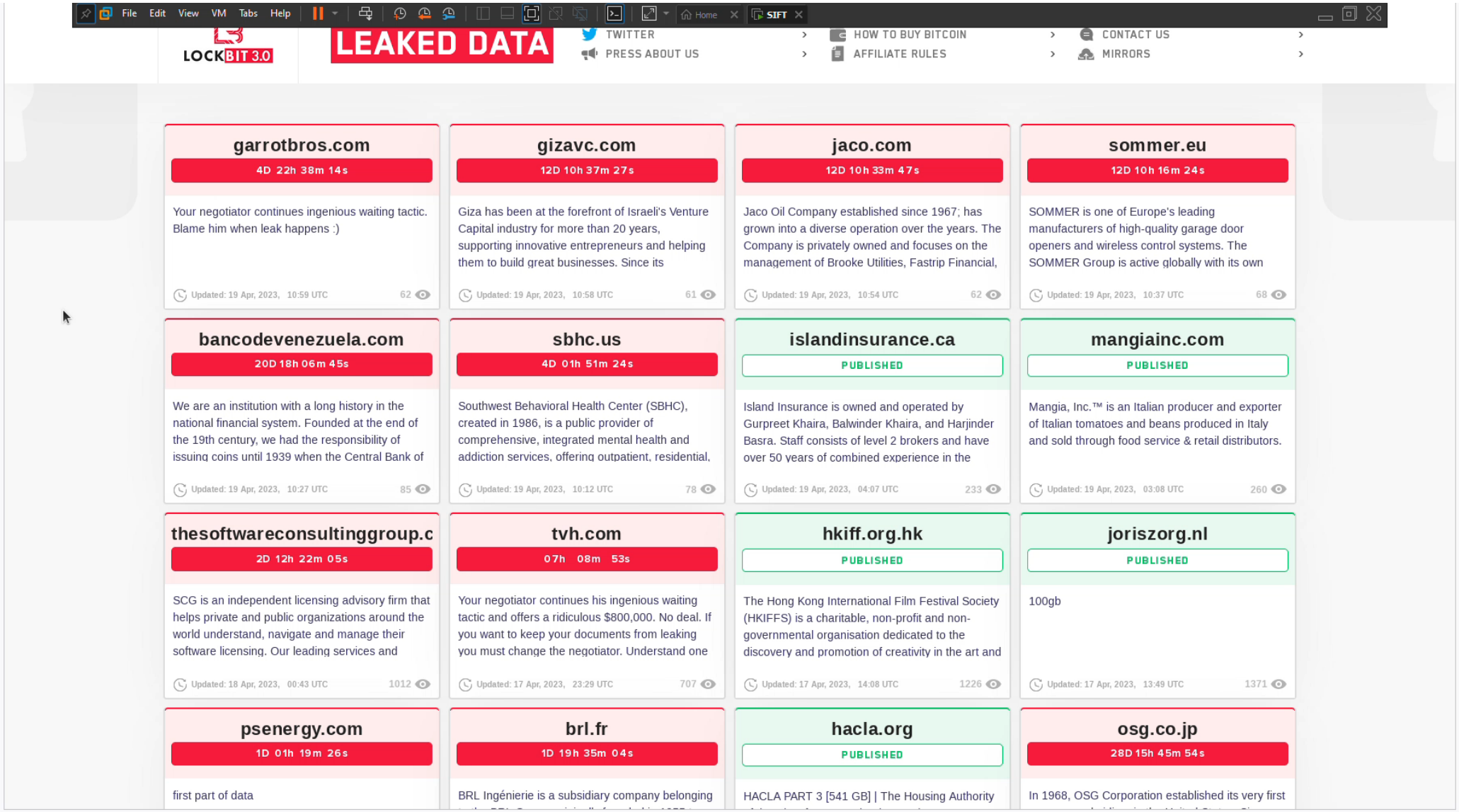
Vérifier que ça appartient bien à l'entité





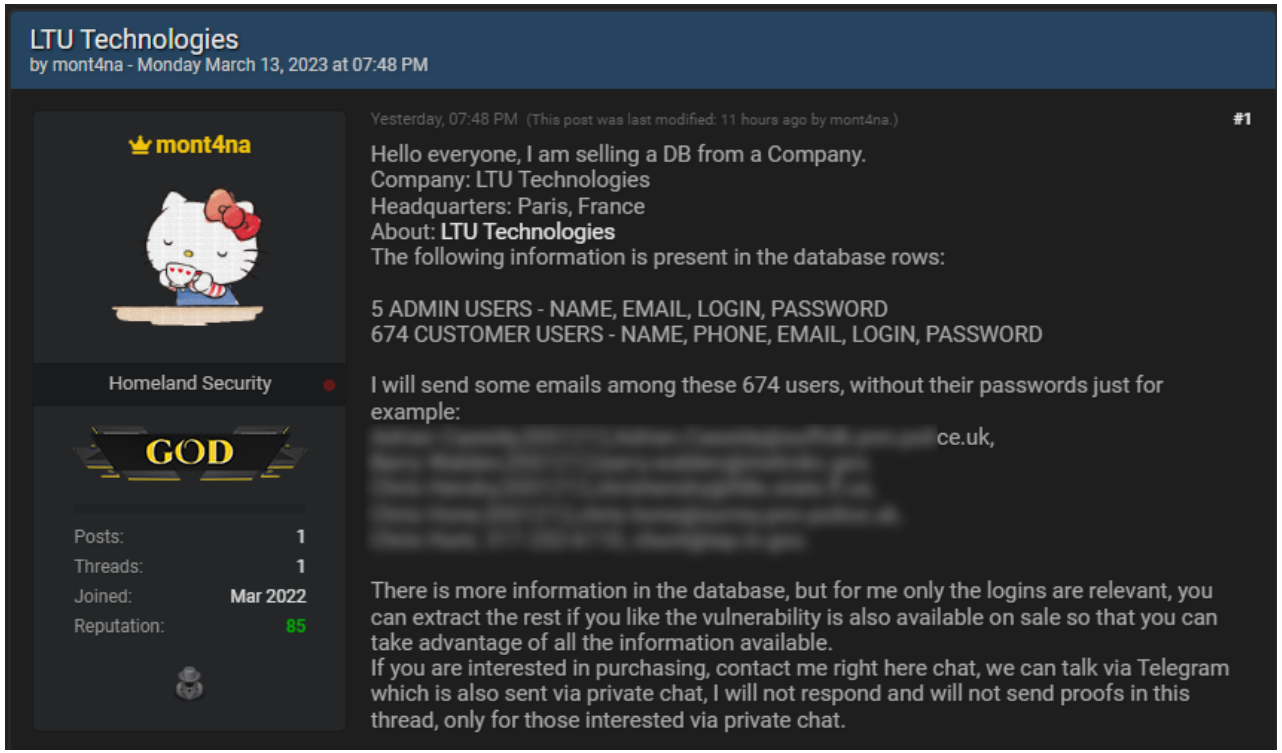
Fuites de données de victimes de ransomware

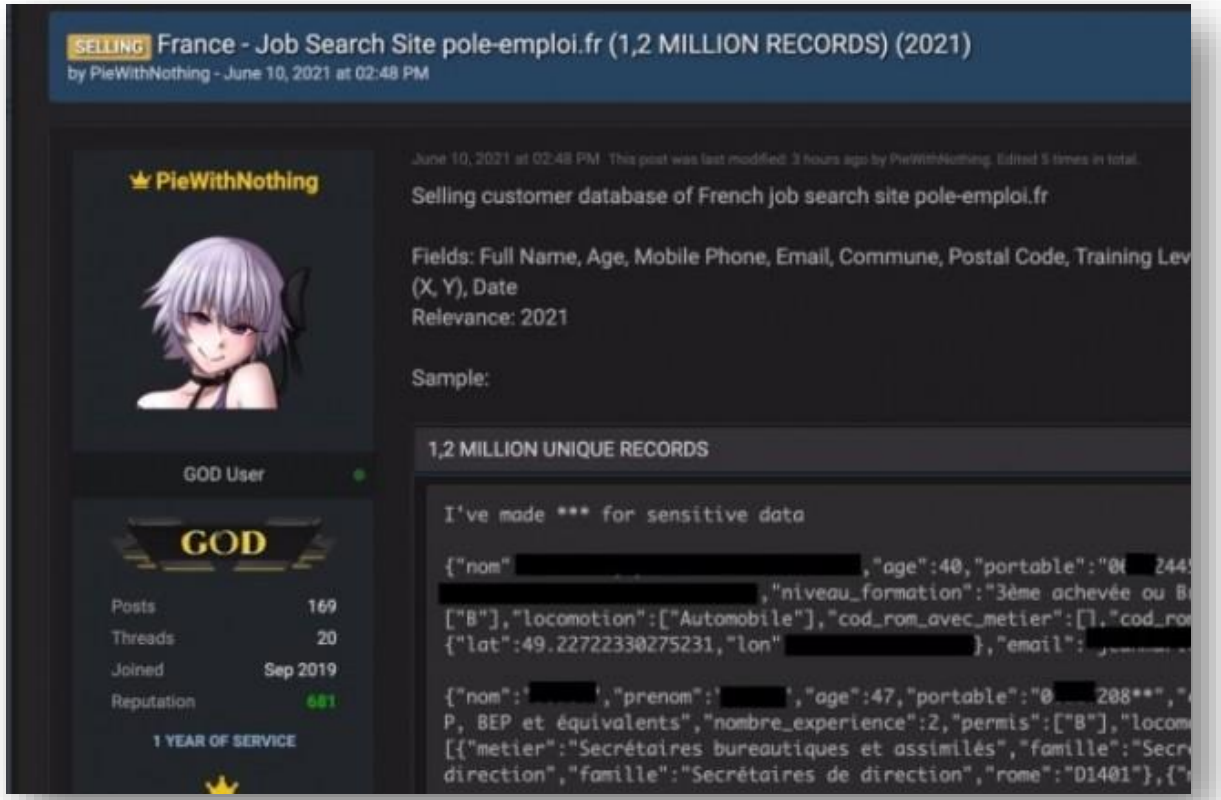
Exemple : Forum du ransomware « Lockbit »



Investigation sur des forums de fuites de données

Exemple : Forum « Valid Market »

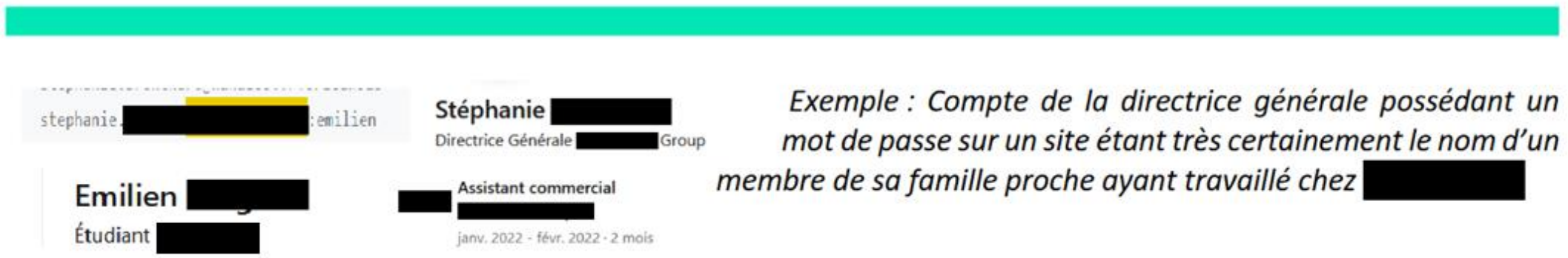




Analyse manuelle – interpréter et filtrer les résultats

Fuite de mots de passe et fuites de données

L’analyste interprète les résultats, exemple sur un grand groupe international :



Exemple : Compte de la directrice générale possédant un mot de passe sur un site étant très certainement le nom d’un membre de sa famille proche ayant travaillé chez [redacted]

L’analyste récupère des données fuitées et en estime la sensibilité, exemple après un rançongiciel :

- Document de comptabilité
- Document RH ainsi que pièce d’identité de collaborateur

Potentielle compromission d’un serveur de paye / facturation interne par un cyber attaquant

05.

LIMITES

05.

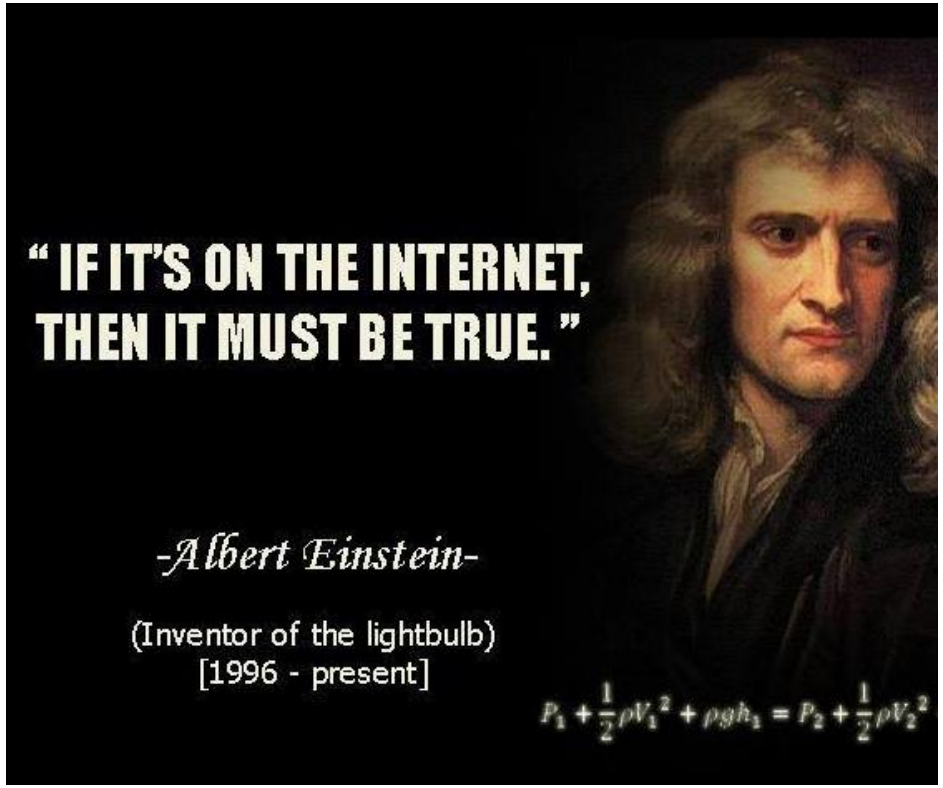
Les limites et les risques de l'OSINT

A vos risques et périls

- Légales et juridiques
  - Réutiliser des données « leakées » est illégal (même si publiques)
  - Toute intrusion dans un SI est passible d'emprisonnement
  - Aller sur le Darkweb : **OK**
  - Acheter de la drogue sur le Darkweb : **KO**

- Exposition
  - Attention aux traces que vous laissez (OPSEC)
  - Contre-renseignement
  - TOR + VPN mais pour visiter un site avec un compte ?
    - Webeacon, logs de VPN / sites web / cache CDN, DNS, …
  - Soumission sur VT

- Pertinence de la donnée
  - Fausses revendications Lockbit
  - Fausse vente de BDD pour mettre la pression
  - Attribution
    - Si je refais la recette d'un chef, je ne suis pas le chef pour autant



Victime collatérale

- Fuite de données personnelles via brèche d’une entreprise
- Fuite de données économiques / base client
- Impact sur l’image
- …

PILOTER L'EVOLUTION

06.

Livrables

Avoir un premier aperçu de son exposition

[redacted]

Analyse OSINT

Périmètre

L'analyse a été réalisé sur le périmètre suivant :

Nom de la société	Site Web	Adresses IP
[redacted]		

Contexte

Dans le cadre d'une mission de sécurisation, [redacted] souhaite sensibiliser l'ensemble des entreprises pour lesquelles [redacted] devra être déployé. Afin de partager de manière efficace l'état de santé de Cybersécurité de ces entreprises, Almond a réalisé une analyse OSINT sur les données exposées pour indiquer si d'éventuelles fuites d'information ou de documents, de compromissions d'identifiants/mots de passes, d'usurpation de site internet... sont connues.

Vérification des erreurs de configuration sur le chiffrement du site WEB :

Pas de recommandations nécessaires supplémentaires

Surveillance des tentatives d'attaques :

La surveillance mise en place n'a pas permis de relever la présence de la société [redacted] dans des sites connus pour de l'activité récurrente d'attaque. Nombre d'occurrence : **0**

Il est recommandé de monitorer ce type de communications publiques en permanence pour identifier de potentielles actions malveillantes à l'encontre des services de PMA.

Détection de compte de collaborateurs compromis :

Nous avons observé **5** comptes de collaborateur de [redacted] avec des informations d'identification ayant fuitées. Les informations d'identification volées ou divulguées peuvent être utilisées à des fins de fraude, de vente clandestine, de chantage, d'atteinte à la réputation, d'usurpation d'identité et d'espionnage.

Exemple : Mot de passe possible de deux comptes [redacted]
Un attaquant pourrait réutiliser ces mots de passe en essayant d'essayer le schéma qui se répète pour le compte « qualite » : [redacted]

Il est recommandé de surveiller régulièrement les fuites de mots de passe des collaborateurs afin de s'assurer que ces derniers ont été modifiés ou ne permettent pas d'identifier un schéma se répétant (Exemple : NomEnfant1_NomEnfant2_DateDeNaissance).

Trace de données sur le Dark Web :

Un nombre élevé de référence à la société [redacted] sur le Dark Web pourrait indiquer une attaque en cours. Le Dark Web est régulièrement utilisé par des groupes d'attaquants organisés pour du partage d'informations et d'outils. Nombre d'occurrences : **7**

Exemple : IP présente dans un fichier nommé « wordpress attack - ip addresses 17 Nov 2019 » pouvant indiquer une utilisation malveillante d'une ressource

Il est recommandé de régulièrement vérifier le Dark Web afin d'identifier les premières traces d'une attaque sur le système d'information et de réagir en conséquence.

Possible fuite de données :

La société [redacted] possède actuellement **884** documents exposés publiquement. Certains de ces documents pourraient contenir des informations ne devant pas être accessibles au public.

Il est recommandé de vérifier régulièrement la liste des documents pouvant être accessible via internet. Si un document ne doit pas être exposé publiquement, il faut s'assurer de modifier son exposition.

Protection de domaine :

La protection de domaine monitore les noms de domaines proches de [redacted] afin d'identifier de l'hameçonnage ou des infractions à la propriété intellectuelle. Nombre d'occurrences : **655**

[redacted]

Exemple de domaines à surveiller : [redacted]

Dans le cadre de la découverte d'un nom de domaine frauduleux, il est nécessaire de lancer une procédure de demande de suppression.

Vérification des réseaux sociaux :

La vérification des réseaux sociaux permet de recueillir des informations sur le sentiment des utilisateurs à l'égard d'une marque, d'une société ou d'un produit. Nombre d'occurrences : **1132**

Il est important de surveiller les réseaux sociaux afin de découvrir des potentiels abus de marque

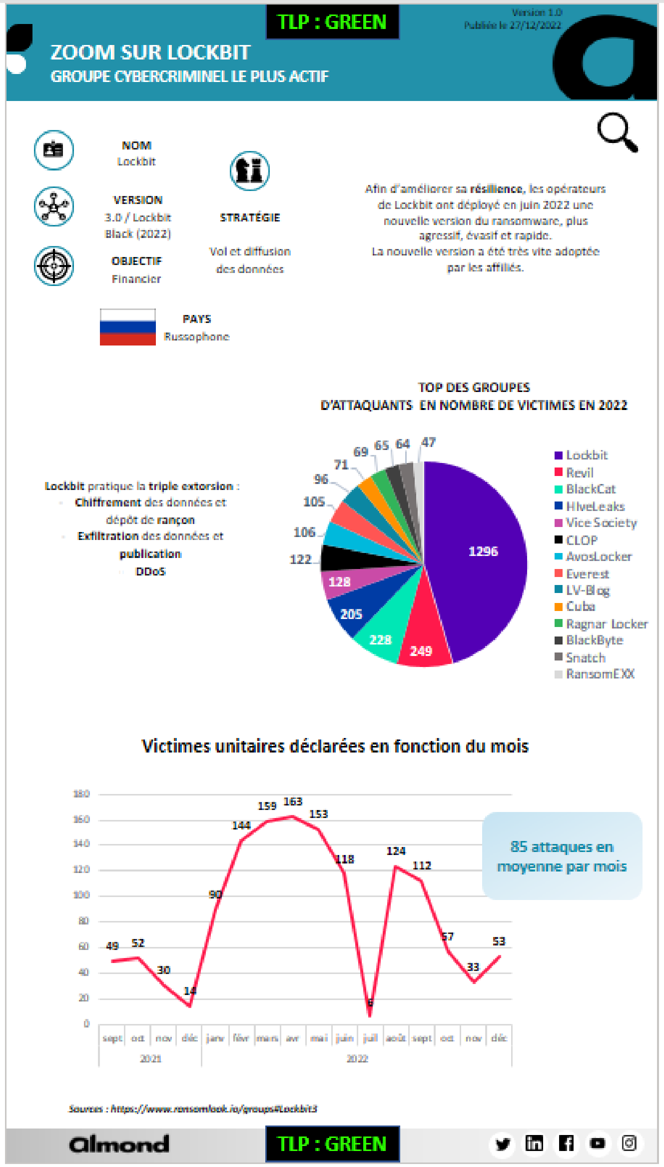
Vulnérabilités :

L'analyse des vulnérabilités sur la base des entêtes et bannières de serveur permet d'identifier des versions d'applicatif obsolètes, non à jour et présentant des vulnérabilités plus ou moins critiques. Nombre d'occurrence : **0 vulnérabilités identifiées**.

Livrables

Rapport d'OSINT complet sur une structure

Portraits Robot de groupes criminels



ZOOM SUR LOCKBIT
GROUPE CYBERCRIMINEL LE PLUS ACTIF
TLP : GREEN
Version 1.0
Publiée le 27/12/2022

NOM
Lockbit

VERSION
3.0 / Lockbit Black (2022)

OBJECTIF
Financier

STRATÉGIE
Vol et diffusion des données

PAYS
Russophone

Afin d'améliorer sa résilience, les opérateurs de Lockbit ont déployé en juin 2022 une nouvelle version du ransomware, plus agressif, évasif et rapide. La nouvelle version a été très vite adoptée par les affiliés.

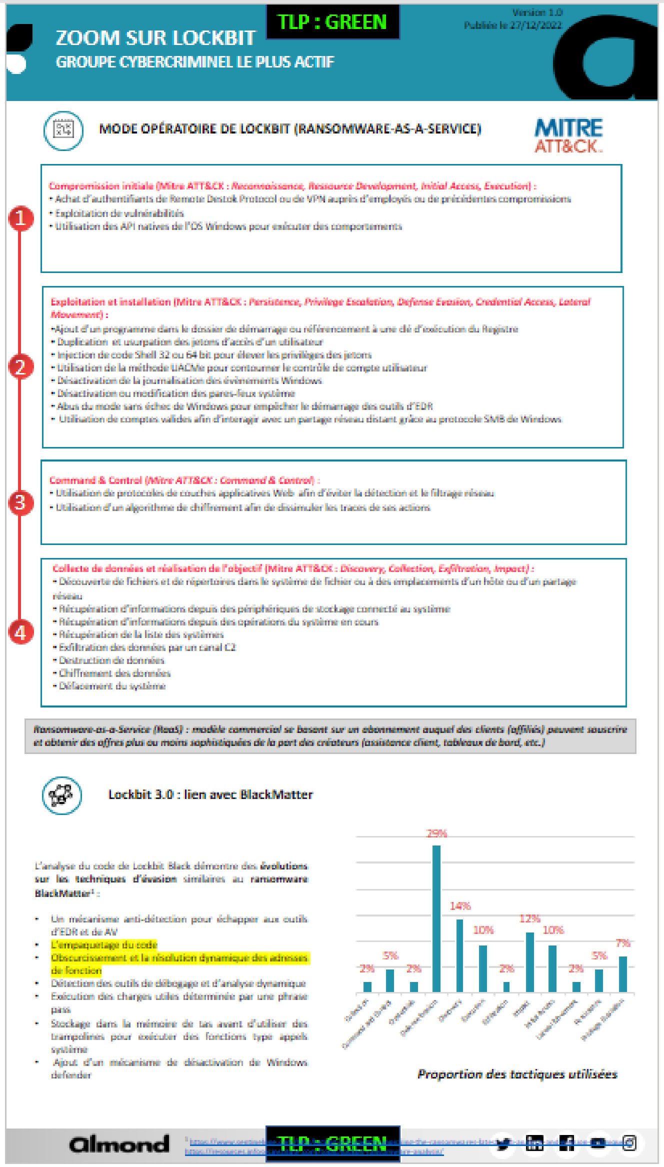
Lockbit pratique la triple extorsion :
Chiffrement des données et dépôt de rançon
Exfiltration des données et publication
DDoS

TOP DES GROUPES D'ATTAQUANTS EN NOMBRE DE VICTIMES EN 2022

Victimes unitaires déclarées en fonction du mois

Sources : https://www.ransomlook.io/group/Lockbit3

Almond TLP : GREEN



ZOOM SUR LOCKBIT
GROUPE CYBERCRIMINEL LE PLUS ACTIF
TLP : GREEN
Version 1.0
Publiée le 27/12/2022

MODE OPÉRATOIRE DE LOCKBIT (RANSOMWARE-AS-A-SERVICE)
MITRE ATT&CK

1 Compromission initiale (Mitre ATT&CK : Reconnaissance, Ressource Development, Initial Access, Execution) :
- Achat d'authentifiants de Remote Destok Protocol ou de VPN auprès d'employés ou de précédentes compromissions
- Exploitation de vulnérabilités
- Utilisation des API natives de l'OS Windows pour exécuter des comportements

2 Exploitation et installation (Mitre ATT&CK : Persistence, Privilege Escalation, Defense Evasion, Credential Access, Lateral Movement) :
- Ajout d'un programme dans le dossier de démarrage ou référencement à une clé d'exécution du Registre
- Duplication et usurpation des jetons d'accès d'un utilisateur
- Injection de code Shell 32 ou 64 bit pour élever les privilèges des jetons
- Utilisation de la méthode UACMe pour contourner le contrôle de compte utilisateur
- Désactivation de la journalisation des événements Windows
- Désactivation ou modification des pares-feux système
- Abus du mode sans échec de Windows pour empêcher le démarrage des outils d'EDR
- Utilisation de comptes valides afin d'interagir avec un partage réseau distant grâce au protocole SMB de Windows

3 Command & Control (Mitre ATT&CK : Command & Control) :
- Utilisation de protocoles de couches applicatives Web afin d'éviter la détection et le filtrage réseau
- Utilisation d'un algorithme de chiffrement afin de dissimuler les traces de ses actions

4 Collecte de données et réalisation de l'objectif (Mitre ATT&CK : Discovery, Collection, Exfiltration, Impact) :
- Découverte de fichiers et de répertoires dans le système de fichier ou à des emplacements d'un hôte ou d'un partage réseau
- Récupération d'informations depuis des périphériques de stockage connecté au système
- Récupération d'informations depuis des opérations du système en cours
- Récupération de la liste des systèmes
- Exfiltration des données par un canal C2
- Destruction de données
- Chiffrement des données
- Défacement du système

Ransomware-as-a-Service (RaaS) : modèle commercial se basant sur un abonnement auquel des clients (affiliés) peuvent souscrire et obtenir des offres plus ou moins sophistiquées de la part des créateurs (assistance client, tableaux de bord, etc.)

Lockbit 3.0 : lien avec BlackMatter

L'analyse du code de Lockbit Black démontre des évolutions sur les techniques d'évasion similaires au ransomware BlackMatter[1] :
- Un mécanisme anti-détection pour échapper aux outils d'EDR et de AV
- L'empaquetage du code
- Obscurcissement et la résolution dynamique des adresses de fonction
- Détection des outils de débogage et d'analyse dynamique
- Exécution des charges utiles déterminée par une phrase pass
- Stockage dans la mémoire de tas avant d'utiliser des trampolines pour exécuter des fonctions type appels système
- Ajout d'un mécanisme de désactivation de Windows defender

Almond TLP : GREEN

ZOOM SUR LOCKBIT
GROUPE CYBERCRIMINEL LE PLUS ACTIF
TLP : GREEN
Version 1.0
Publiée le 27/12/2022

FOCUS SUR LES TECHNIQUES UTILISEES
MITRE ATT&CK

Utilisation majoritaire de la technique Impair Defenses [T1562] lors de l'étape de Defense Evasion.

Comme évoqué, Lockbit cherche à d'échapper à la détection en contournant/désactivant les dispositifs de sécurité.

La second technique utilisée Valid Accounts [T1078] lors des étapes d'Initial Access et de Defense Evasion rejoint le point précédemment. L'utilisation d'identifiants de comptes valides permet d'éviter la détection.

Ces comptes sont achetés auprès d'employés suite à des annonces sur le dark web ou obtenus par les affiliés lors d'attaques de reconnaissance.

FOCUS SUR LES OUTILS UTILISES

AMADEY bot
Logiciel malveillant qui permet de voler des données et d'installer d'autres logiciels malveillants en recevant des commandes de l'attaquant. Il peut être déployé soit en utilisant un fichier Word malveillant ou via un exécutable sous la forme d'une icône de fichier Word. Il est installé par le malware SmokeLoader. Pour en savoir plus sur les TTPs.

Cobalt Strike
Outil offensif, très fréquemment utilisé par les attaquants, il facilite la prise en main à distance sur des machines compromises. Il déploie un agent afin d'effectuer des actions de latéralisation, en réalisant des rebonds d'une machine à l'autre (Lateral Movement). Il permet de faire des énumérations réseau, c'est-à-dire qu'il va collecter des informations sur un réseau tel que des hôtes, des noms d'utilisateurs, etc. Il exploite aussi les capacités d'autres outils tels que Mimikatz. Pour en savoir plus sur les TTPs.

Mimikatz
Outil largement utilisé par les attaquants et à multiples usages, il permet de récupérer des informations de connexions et des mots de passe de comptes Windows (Privilege Escalation). Pour en savoir plus sur les TTPs.

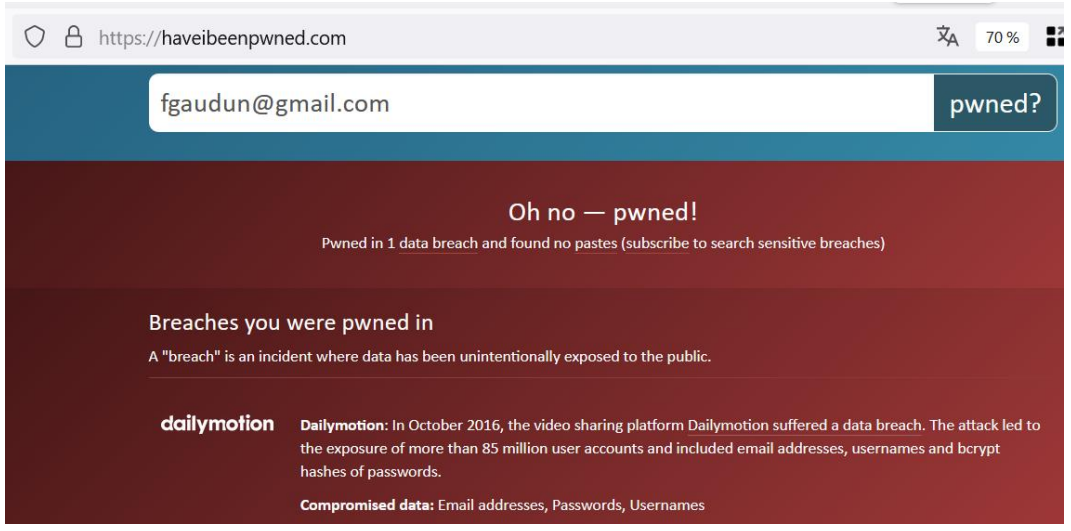
Almond TLP : GREEN

CALL TO ACTION

07.

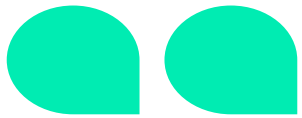
Que pouvez-vous faire dès aujourd'hui

- Prendre conscience des traces que vous laissez
- Sensibiliser votre entourage
- Changer vos mots de passe selon les services
  - Mots de passe longs, gestionnaire type KeePass
- Vous stalker vous-même
  - Se googler
  - HIBP
- Déréférencer / désindexer le contenu
  - Supprimer ce qui peut être gênant
- Réfléchir à 2 fois
  - avant de publier ou commenter



Questions

?



Almond

PARIS_
STRASBOURG_
NANTES_
RENNES_
LYON_
GENÈVE_

Contact

Tristan PINCEAUX
HEAD Of CERT CWATCH
tpinceaux@almond.eu

Almond Suisse : +41 (0)22 588 96 98

alerte@cwatch.almond.eu

MERCI