



# Le « Dark Web » : enjeux et mesures

Comment réagir, quelles mesures appliquer ?

# Intervenants

- Pôle Management des Risques de CEIS
    - ❖ Benoit Mercier – Manager
    - ❖ Adrien Petit – Consultant en cybercriminalité
- Retour d'expérience d'une cellule de type  
« **Cyber Threat Intelligence** »

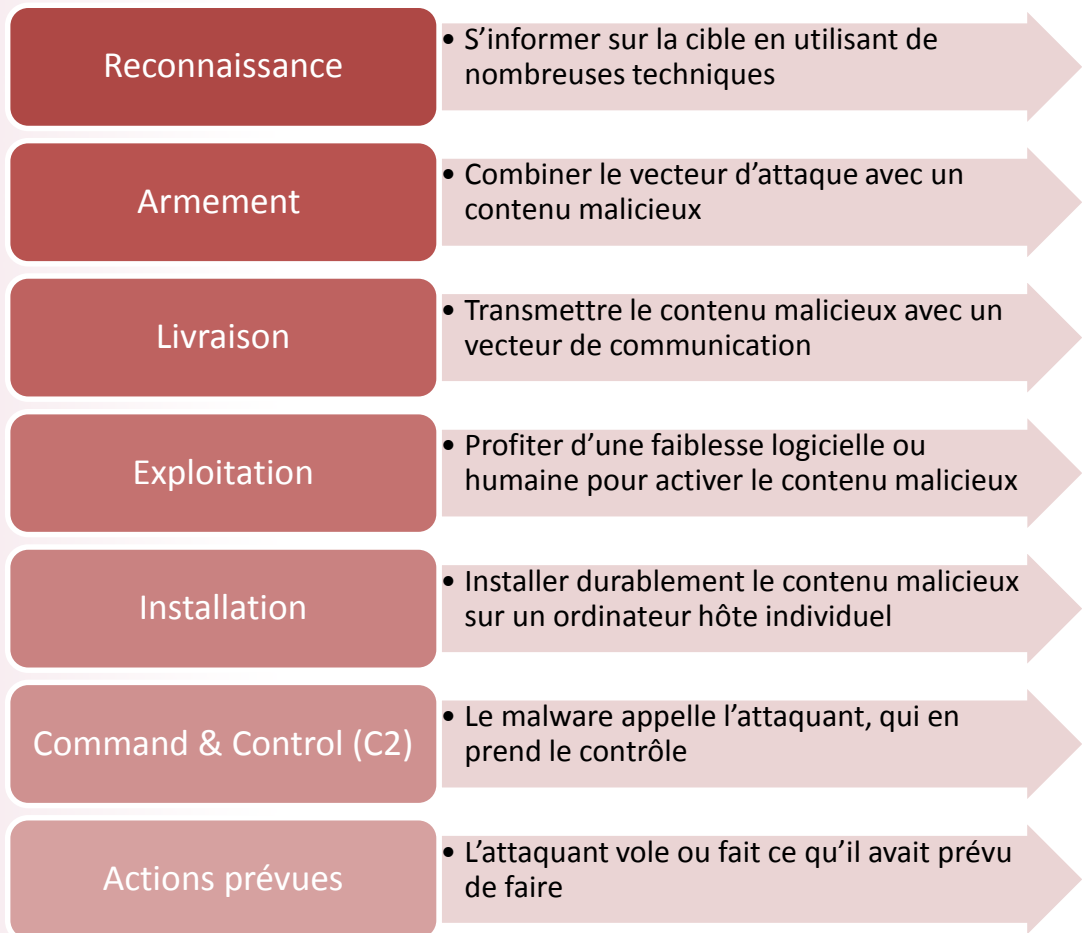
# Comment réagir ?

# Comment réagir ?

- Se mettre à la place d'un cyber-attaquant
  - ❖ Cyber Kill Chain
    - Concept introduit par Lockheed Martin en mars 2011
    - Décrit le modèle d'une cyber-attaque
    - 7 étapes majeures

# Comment réagir ?

## 7 étapes de la Cyber Kill Chain

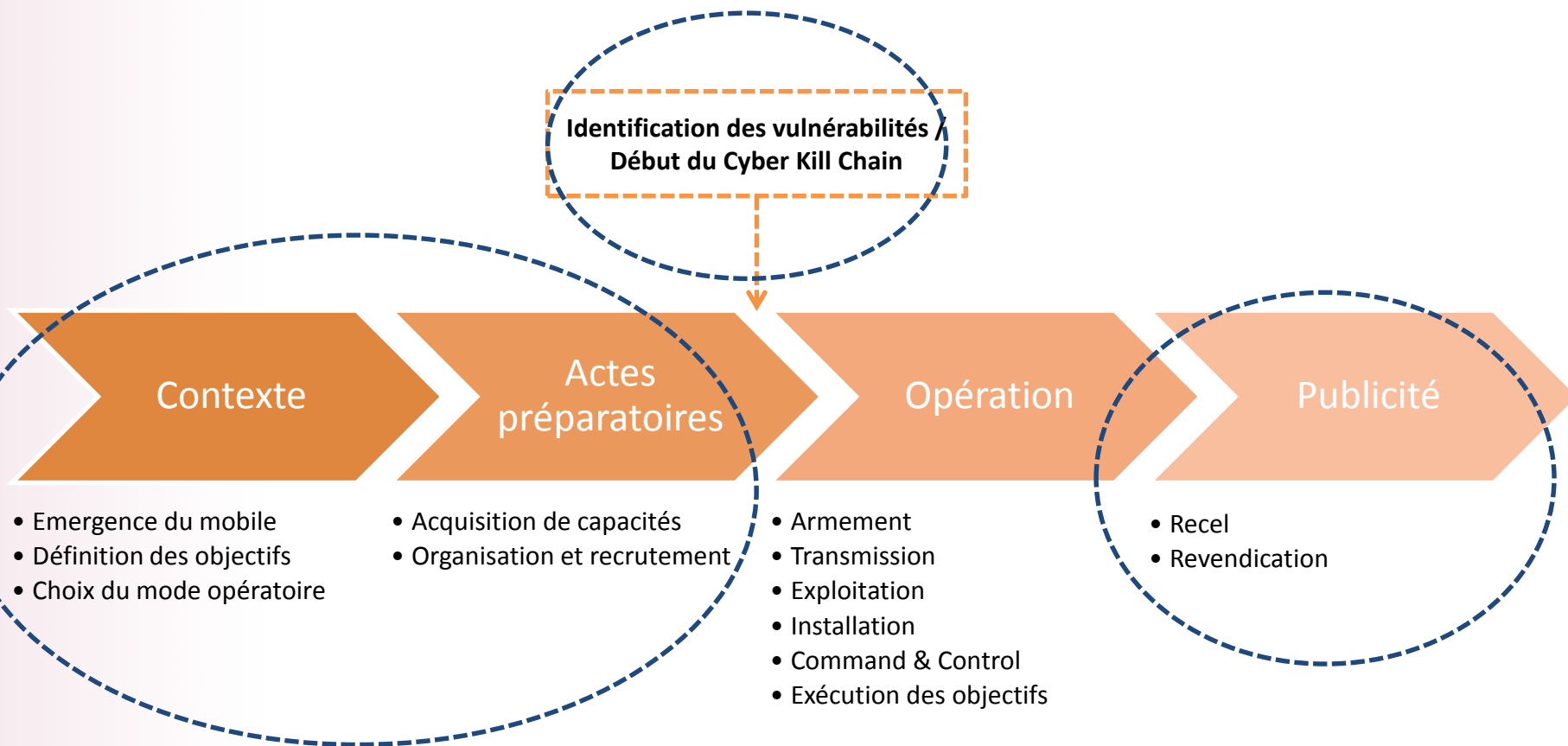


### Limites :

- Adaptée à certains types d'attaque (APT)
- Manque des étapes cruciales

# Comment réagir ?

- Cyber Kill Chain et Threat Intelligence



# Comment réagir ?

- Mettre en place une cellule CTI
  - ❖ Approche technologique
    - Outils sur étagère
    - Développement d'outils spécifiques
  - ❖ Approche humaine
    - Equipe multilingue
    - Profils variés

# Comment réagir ?

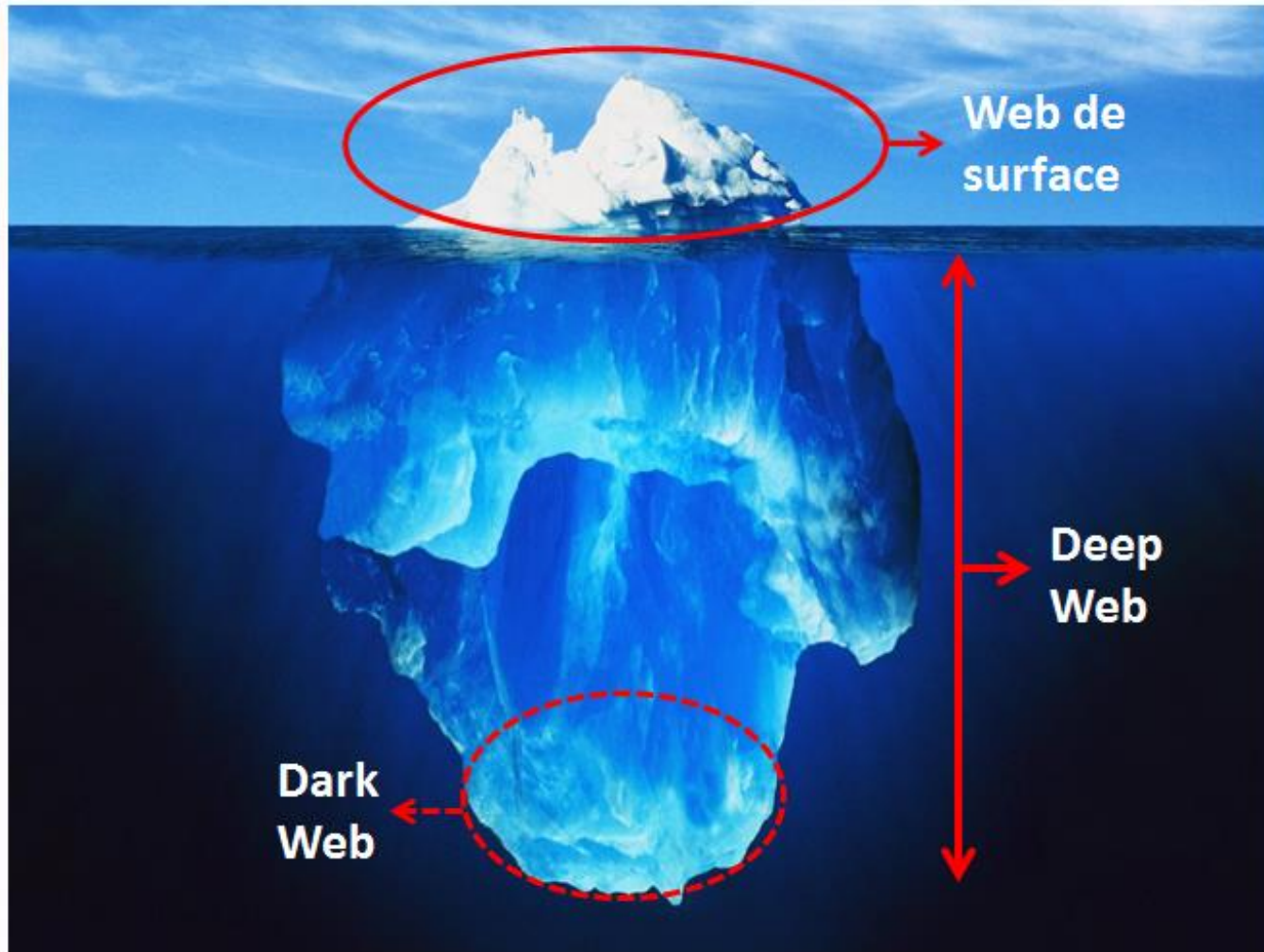
	Technologie	Couverture	Limite des outils
<b>Web de surface</b>	Outils sur étagère	<ul style="list-style-type: none"> <li>- Réseaux sociaux</li> <li>- Sites de partage</li> <li>- Sites de diffusion</li> <li>- Sites de stockage</li> <li>- Forums</li> </ul>	Flux de données brutes sans analyse
<b>Deep Web</b>	Outils sur étagère + Développement d'outils spécifiques		
<b>Dark Web</b>	Développement d'outils spécifiques	<ul style="list-style-type: none"> <li>- Wikis</li> <li>- Forums</li> <li>- IRC</li> <li>- Blackmarkets</li> </ul>	Difficultés pour acquérir l'information à forte valeur ajoutée

Humain
<ul style="list-style-type: none"> <li>- Présence proactive sur les canaux de communication</li> <li>- Analyse thématique (technique, géopolitique, etc.)</li> <li>- Analyse de tendance</li> <li>- Vision prospective</li> </ul>



# Le Web de surface: passerelle vers le Dark Web

# Le Web de surface: passerelle vers le Dark Web



# Le Web de surface: passerelle vers le Dark Web

- Réseaux sociaux
  - ❖ Rex Mundi : cybercriminels spécialisés dans le rançonnage
  - ❖ Victimes récentes : Domino's Pizza et Labio



 **Rex Mundi** @RexMundi2015 · 13 mars  
Labio.fr hacked last week. 100's of blood test results in our possession. #infosec #hack #piratage #Labio

# Le Web de surface: passerelle vers le Dark Web

❖ Documents disponibles sur le site .onion de Rex Mundi

## Rex Mundi

**YOUR FRIENDLY NEIGHBORHOOD HACKERS**

**Code of Conduct**

- Communication and/or negotiations between us and our targets is never released, regardless of whether we get paid or not.
- We never discuss or even acknowledge the fact that some of our past targets might have paid us.
- We automatically delete all of the stolen data once a full payment has been made.
- We never target the same company twice and, for obvious reasons, we always stick with the original requested amount.


**Current Twitter Account**  
@RexMundi2015

**About Us**  
Rex Mundi is a collective of hackers. We hack for fun, for the thrills and, most importantly, for profit.

**About the Leaks**  
On this page, you will find leaks belonging to most of the websites that we hacked. Please note that those are leaks belonging only to companies that declined to pay us. As per our agreement with the companies that did pay us, we will never release those leaks.

**Format**  
All of the leaks linked on this page are TXT files, either in CSV or tab-delimited format.

<b>ACCORD</b> <a href="#">delphjob_resumes.txt</a> <a href="#">email-pass-name-id.txt</a> <a href="#">id-address-city-zip-phone-birth.txt</a> <a href="#">phjobs_persons.txt</a>	<b>ALFAHOSTING</b> <a href="#">aanmelden.txt</a> <a href="#">bestellingen.txt</a> <a href="#">CustomerNames.txt</a> <a href="#">gegevens.txt</a> <a href="#">import_paypal.txt</a> <a href="#">users.txt</a>	<b>BCGE</b> <a href="#">bcge.zip</a>
<b>BUYWAY</b> <a href="#">subscriptions.txt</a>	<b>DOMINO'S</b> <a href="#">visiteursBeEN.txt</a> <a href="#">visiteursBeFR.txt1 2</a> <a href="#">visiteursBeNL.txt</a> <a href="#">visiteursFRFR.txt1 2 3 4 5 6 7 8 9 10 11 12</a>	<b>DRAKE INTL</b> <a href="#">applications.txt</a> <a href="#">client.txt</a> <a href="#">consultants.txt</a> <a href="#">webusers.txt</a>
<b>EASYPAY</b> <a href="#">employee.txt</a> <a href="#">hcm_databaseserver.txt</a> <a href="#">hcm_deployedscheme.txt</a> <a href="#">person.txt</a> <a href="#">ul_webclientsse.txt</a>	<b>EXARIS</b> <a href="#">aris_candidature.txt</a> <a href="#">aris_contact.txt</a>	<b>LABIO</b> <a href="#">Login credentials and names</a> <a href="#">Blood Results 1</a>
<b>MENSURA</b> <a href="#">absenteismeForm_data.txt</a>	<b>NUMERICABLE</b> <a href="#">master.txt</a> <a href="#">mobile.txt</a>	<b>SYNERGIE</b> <a href="#">synergie.zip</a>



Labio  
Laboratoire de Biologie Médicale  
Avenue n° 145-00 / 121

**Laboratoire CELSE L'HOSTE**  
5 Rue des Allumettes 13090 Aix-en-Provence  
Tél: 04 42 26 11 19 Fax: 04 42 26 23 67  
Email: celselhoste@labio.fr

Direction : Dr Philippe CELSE L'HOSTE

Examen **0010**  
De : **Monsieur**  
Né(e) le **25.07.2013**  
Enregistré le **25.07.2013**  
Éché le **26.07.2013**  
Prescrit par **Dr**

Monsieur **[REDACTED]**  
**145 AVENUE DE [REDACTED]**

HEMATOLOGIE		Unités	Antécédents
		Unités	Antécédents
<i>Résultats ci-dessous validés le 25.07.2013 - validés le 26.07.2013</i>			
<b>NUMERATION GLOBULAIRE</b> (Abit. Etm. Dyan. (micro. tripa)) (TA)			
* Leucocytes	[REDACTED]	4 à 10	
* Hématies	[REDACTED]	4.0 à 5.8	
Hémoglobine	[REDACTED]	13.0 à 17.7	
Hématocrite	[REDACTED]	40 à 54	
T.C.M.H	[REDACTED]	27 à 31	
C.C.M.H	[REDACTED]	32 à 36	
V.G.M	[REDACTED]	80 à 100	
<b>FORMULE LEUCOCYTAIRE</b>			
Poly. neutrophiles	[REDACTED] 59,0 %	28,7,5	
Poly. éosinophiles	[REDACTED] 0,8 %	< 0,5	
Poly. basophiles	[REDACTED] 0,6 %	< 0,2	
* Lymphocytes	[REDACTED] 33,5 %	18,4	
Monocytes	[REDACTED] 7,2 %	0,3 à 1	
<b>NUMERATION PLAQUETTAIRE</b>			
Plaquettes	[REDACTED]	150 à 400	
HEMOSTASE		Unités	Antécédents
		Unités	Antécédents
<i>Résultats ci-dessous validés le 25.07.2013 - validés le 26.07.2013</i>			
<b>Taux de Prothrombine</b> (ACL Etm. Tech. chromatron tripa) (TA)			
Temps de Quick témoin	[REDACTED]		
Temps de Quick patient	[REDACTED]		
TP	[REDACTED]	> 70	
INR	[REDACTED]		

VOTRE SANTÉ NOTRE OBJECTIF  
[www.labio.fr](http://www.labio.fr)

Page 1 / 2

# Le Web de surface: passerelle vers le Dark Web

- Bases de données de pasties (Pastebin.com – Justepaste.it – etc.)
  - ❖ Instructions d'attaque DDoS (Anonymous)
  - ❖ Fuites de données (Carding)

```
10. 6011361029565298=161010110000391
11. (101)
12. DISCOVER
13. BANK OF [REDACTED]361029565298^SIMON/HILDA^16101011000000655
14.
15.
16. 6011361151337128=160910110000919
17. (101)
18. DISCOVER
19. BANK OF [REDACTED]361151337128^FLOYD/CASSIE^1609101100000065600
```

# Le Web de surface: passerelle vers le Dark Web

- Autres outils traditionnels :
  - ❖ Channels IRC
  - ❖ Sites de diffusion
  - ❖ Forums

Subreddit /r/DarkNetMarkets

5	<b>Moronic Monday - it's your weekly stupid questions thread</b>	submitted 2 hours ago par AutoModerator [DNM Moderator] · 7 commentaires · partager
1	<b>Marketplace Announcement: Havana Beta Release -- NOW!</b>	submitted 11 hours ago par Alacemiravanalarkats · 57 commentaires · partager
2	Ordered from ock1(2nd time) ended up in customs interrogation room	submitted 6 hours ago par Sarelystures · 8 commentaires · partager
3	Friend literally died, can't retrieve package	submitted 10 hours ago par boote_is · 63 commentaires · partager
4	Found a new name card inside my PO Box. It has a mysterious red dot beside my name. Mail has also been arriving later than normal and with small tears.	submitted 7 hours ago * par oncraylife · 8 commentaires · partager
5	do not order from NL, 2 LE at my house this morning	submitted 3 hours ago par throulaway2633 · 7 commentaires · partager
6	<b>Complaint/Warning</b> [Complaint/Warning]Don't buy from TheIndigoChild	submitted 5 hours ago * par 3m5pPayol · 4 commentaires · partager

Subreddit /r/HowToHack

45	<b>MIT</b> A list of Hacking documentaries, please help me complete it. <a href="#">mathwvety.com</a>	submitted 17 hours ago par voo00obunny77 · 5 commentaires · partager
7	Learning how to phish for passwords? Would this subreddit be able to help?	submitted 5 hours ago par JimmyBradbury · commenter · partager
3	I have some scratch notes that might help you lock down your boxes.	submitted 9 hours ago par Temp_Acct1 · commenter · partager
2	Alcatel TCL 7040 R Android version 4.4.2 wanting to completely unlock/root. KingoRoot not working, any ideas?	submitted 11 hours ago par Tdaug · commenter · partager
3	What Response Time-To-Live Can Reveal About Network Topography	submitted 15 hours ago par hacktail-admin · commenter · partager
1	Can you create a fake browser history?	submitted 10 hours ago par thepinkahor95 · 1 commentaire · partager
1	meterpreter command over IM	submitted 11 hours ago par ATGUNAT · 1 commentaire · partager
0	What are the capabilities of Wireshark? Can it only be used on unsecure wifi?	submitted 11 hours ago par WhoYouAreThisTime · 3 commentaires · partager



# Le Web de surface: passerelle vers le Dark Web

	Market	Monitored	By Registration	Multisig	2FA	Vendor PGP Enforced	FE Allowed	Prior Security Flaws	Commission	Vendor Fee	Uptime	Status
↑ Abraxas	Agora	11 months and 16 days	By Referral	No	Ok	No	Ok	No	4%	btc0.60	82.44%	↑
↑ Agora	BlackBank	11 months and 16 days	Open	Ok	Ok	Ok	No	No	3%	\$200	98.53%	↑
↑ Alphasbay	Bloomsfield	1 month and 27 days	?	Ok	Ok	Ok	Ok	No	1%	.3 btc	99.58%	↑
↑ BlackBank	Crypto Market	1 month and 27 days	open	Ok	Ok	Ok	Ok	No	na	0	97%	↑
↑ Bloomsfield	Dream Market	8 months and 17 days	open	Ok	Ok	Ok	Ok	No	5%	Free	96.3%	↑
↑ Crypto Market	French Dark Net	21 days	na	No	No	No	No	No	na	na	99.53%	↑
↑ Dream Market	French Dark Place 2	21 days	na	No	No	No	No	No	na	na	72.4%	↓
↑ French Dark Net	French Dark Net	21 days	na	No	No	No	No	No	na	na	98.89%	↑
↓ French Dark Place 2	KISS	15 days	Open	No	Ok	Ok	Ok	No	?	.4	93.25%	↑
↓ French Marketplace	LONDON UNDERGROUND	16 days	open	No	No	No	Ok	No	0	na	99.31%	↑
↑ GotMilk Pharmacy	MIDDLE EARTH MARKETPLACE	9 months and 18 days	?	?	?	?	?	?	?	?	97.11%	↑
↑ HonestCocaine	Mr Nice Guy	9 months and -2 day	Open	No	Ok	Ok	Ok	No	3%	btc0.50	22.88%	↑
↑ IDC	Nucleus Market	7 months and 4 days	Open	No	Ok	?	Ok	No	4%	Free	97.95%	↑
↑ KISS	Outlaw Market	11 months and 16 days	Open	No	Ok	Ok	Ok	No	0%	?	92.69%	↑
↑ LONDON UNDERGROUND	Ramp (Russian Anonymous Marketplace)	10 months and 21 days	?	?	?	?	?	?	?	?	98.16%	↑
↑ MIDDLE EARTH MARKETPLACE	Silkkitien	9 months and 25 days	?	?	?	?	?	?	?	?	95.67%	↑
↑ Mr Nice Guy	The Armory	10 months and -1 day	?	?	?	?	?	?	?	?	98.73%	↑
↑ Nucleus Market	The Hub	11 months and 16 days	?	?	?	?	?	?	?	?	92.88%	↑
↑ Outlaw Market												
↑ Ramp (Russian Anonymous Marketplace)												
↑ Silkkitien												
↑ SwissShop												

# Le Web de surface: passerelle vers le Dark Web

- Moyens de communication sur le Web de surface
  - ❖ *Réseaux sociaux - Sites de partage – IRC – Sites de diffusion – Forums*
    - Utilisés massivement par les cybercriminels
    - Recel, publicité, revendications et recrutement
  - **Modus Operandi des cybercriminels plus facile d'accès**
  - **Rebond vers le Dark Web**



# Le Web de surface: passerelle vers le Dark Web

- Outils et services utilisés sur le Dark Web

- ❖ *Wikis*
- ❖ *Moteurs de recherche*
- ❖ *Forums*
- ❖ *IRC*
- ❖ *Blackmarkets*
- ❖ *E-mails anonymes*

→ **Déplacements transverses sur le Dark Web par de l'investigation digitale et humaine (HUMINT et DIGINT)**

# Le Web de surface: passerelle vers le Dark Web

- Double présence des cybercriminels sur le Web de surface et Dark Web
- Actions de l'équipe de type CTI :
  - ❖ Anticipation en amont
  - ❖ Détection opérationnelle
  - ❖ Investigation en aval

# Etude de cas : Fuite de données

# Etude de cas : Fuite de données

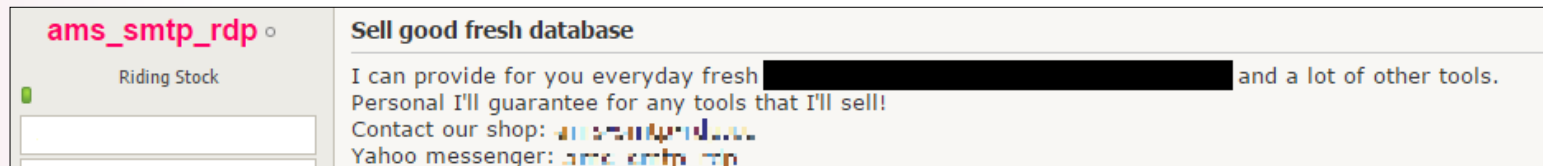
- Détection d'un signal faible sur un site de pasties

```
1. 58000 BANK OF AMERICA LOGINS HACKED AGAIN
2.
3. ON MY RECENT PHISHING SPREE OF BANK OF AMERICA WEBSITE
4. THERE HAS BEEN ALMOST 60000 CASUALTIES
5.
6. BANK ACCOUNTS CLEAN AND LOADED
7.
8. BROUGHT TO YOU BY YOUR LARGEST FINANCIAL HACKER!
9. JADAS
10.
11. Email.....<<<<[redacted]>>>> and get yours now!
12.
13. AHOYYY!!!!
```

- Présence d'un point de contact ou URL vers un forum du Dark Web

# Etude de cas : Fuite de données

- Diffusion d'un message du pirate sur un forum indiquant le moyen de le contacter (ICQ, MP, Jabber)



- En fonction de la demande client, échanges avec le cybercriminel
  - ❖ Prise de contact
  - ❖ Demande d'informations complémentaires
  - ❖ Négociation

# Etude de cas : Fuite de données

- Redirection vers un black market pour finaliser l'achat
- Demande d'un échantillon puis acquisition de l'intégralité des documents

**Company Database Over 49K**

2.12179079 BTC  
 Company Database Over 48K.  
 Company Name, Mailing Address, Telephone, Fax, Email, Website URL, Contact Person Name, Contact Person Title, Contact Person Telephone, Contact Person Email and more.  
 SKU:90119  
 Brought to you by:  
 4.35/5, 40~55 deals

2.12179079 BTC

PersonID	Address	Address	City	City	Firstname	Firstname	Last
1	1040 East Street	1040 East Street	Plateau City	Plateau City	Loretta	Loretta	Bov
2	154 Batic Walk	154 Batic Walk	Excelsior	Excelsior	Evelyn	Evelyn	Eko
3	952 Tennessee Avenue	952 Tennessee Avenue	Embarcadero	Embarcadero	Harold	Harold	Moc
4	700 Fourth Lane	700 Fourth Lane	Tenderlon	Tenderlon	Chad	Chad	Han
5	1079 Beach Way	1079 Beach Way	Cow Hollow	Cow Hollow	Sandra	Sandra	San
6	750 North Lane	750 North Lane	North Beach	North Beach	Kathleen	Kathleen	Rho
7	978 Eighth Walk	722 Arrow Lane	Mirafloa Park	Columbus	Pamela	Pamela	Nea
8	247 Fifth Place	247 Fifth Place	Western Addition	Western Addition	Emily	Emily	Dev
9	843 States Street	843 States Street	Noe Valley	Noe Valley	Vernon	Vernon	Carl
10	749 Washington Street	749 Washington Street	Civic Center	Civic Center	William	William	Oor
11	360 Tennessee Place	360 Tennessee Place	Fisherman's Wharf	Fisherman's Wharf	Gladys	Gladys	Lav
12	14 Oriental Place	14 Oriental Place	Buena Vista	Buena Vista	Margaret	Margaret	Cole
13	660 Lower Avenue	660 Lower Avenue	Diamond Heights	Diamond Heights	Kathleen	Kathleen	Oud
14	896 Third Street	896 Third Street	Civic Center	Civic Center	Bertha	Bertha	Pov
15	229 Kentucky Place	229 Kentucky Place	Ocean View	Ocean View	Kim	Kim	Grs
16	1019 Marvin Gardens Place	1019 Marvin Gardens Place	Potrero Hill	Potrero Hill	Steve	Steve	Cun

 BUY...

# Etude de cas : Fuite de données

- En se déplaçant de façon transverse sur le Dark Web, identification de nouvelles sources pouvant impacter directement le client :
  - ❖ 0-day
  - ❖ Malware
  - ❖ Fuite de bases de données

# Etude de cas : Fuite de données

## Over 28 Million Malaysia Telco Database - Maxis, DIGI & Celcom

254.61489497 BTC  
 Over 28 Million Malaysia Telco Database -  
 Maxis, DIGI & Celcom. Name, Address & Mobile  
 Phone Number. SKU:90142  
 Brought to you by:

[GreatGalaxy](#)  4.35/5, 40~55 deals

254.61489497 BTC

PersonID	Address	Address	City	City	Firstname	Firstname	Last
1	1040 East Street	1040 East Street	Padang City	Padang City	Loretha	Loretha	Bov
2	154 Batu Hah	154 Batu Hah	Ecublery	Ecublery	Evelyn	Evelyn	Bo
3	962 Tennessee Avenue	962 Tennessee Avenue	Embarradero	Embarradero	Harold	Harold	Mic
4	700 Fourth Lane	700 Fourth Lane	Tenderon	Tenderon	Chad	Chad	Hat
5	1079 Beach Way	1079 Beach Way	Cow Hollow	Cow Hollow	Sandra	Sandra	Sai
6	750 North Lane	750 North Lane	North Beach	North Beach	Kathleen	Kathleen	Rho
7	978 Eighth Walk	722 Ancon Lane	Malama Park	Columbus	Patella	Patella	Nea
8	247 Fifth Place	247 Fifth Place	Western Addition	Western Addition	Emily	Emily	Dev
9	843 States Street	843 States Street	Nov Valley	Nov Valley	Vernon	Vernon	Carl
10	749 Washington Street	749 Washington Street	Civic Center	Civic Center	William	William	Oor
11	360 Tennessee Place	360 Tennessee Place	Fisherman's Wharf	Fisherman's Wharf	Gedys	Gedys	Ler
12	14 Oriental Place	14 Oriental Place	Buena Vista	Buena Vista	Margaret	Margaret	Col
13	668 Lower Avenue	668 Lower Avenue	Diamond Heights	Diamond Heights	Kathleen	Kathleen	Out
14	696 Third Street	696 Third Street	Civic Center	Civic Center	Bertha	Bertha	Por
15	229 Kentucky Place	229 Kentucky Place	Ocean View	Ocean View	Kim	Kim	Ora
16	1019 Marvin Gardens Place	1019 Marvin Gardens Place	Pobrero Hill	Pobrero Hill	Steve	Steve	Out

BUY...

- Client alerté de la fuite de données
  - ❖ Sensibilisation des futures victimes potentielles
  - ❖ Mise en place de garde-fous
    - Ex: actions pour se prémunir d'une attaque de type spear-phishing



