CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

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

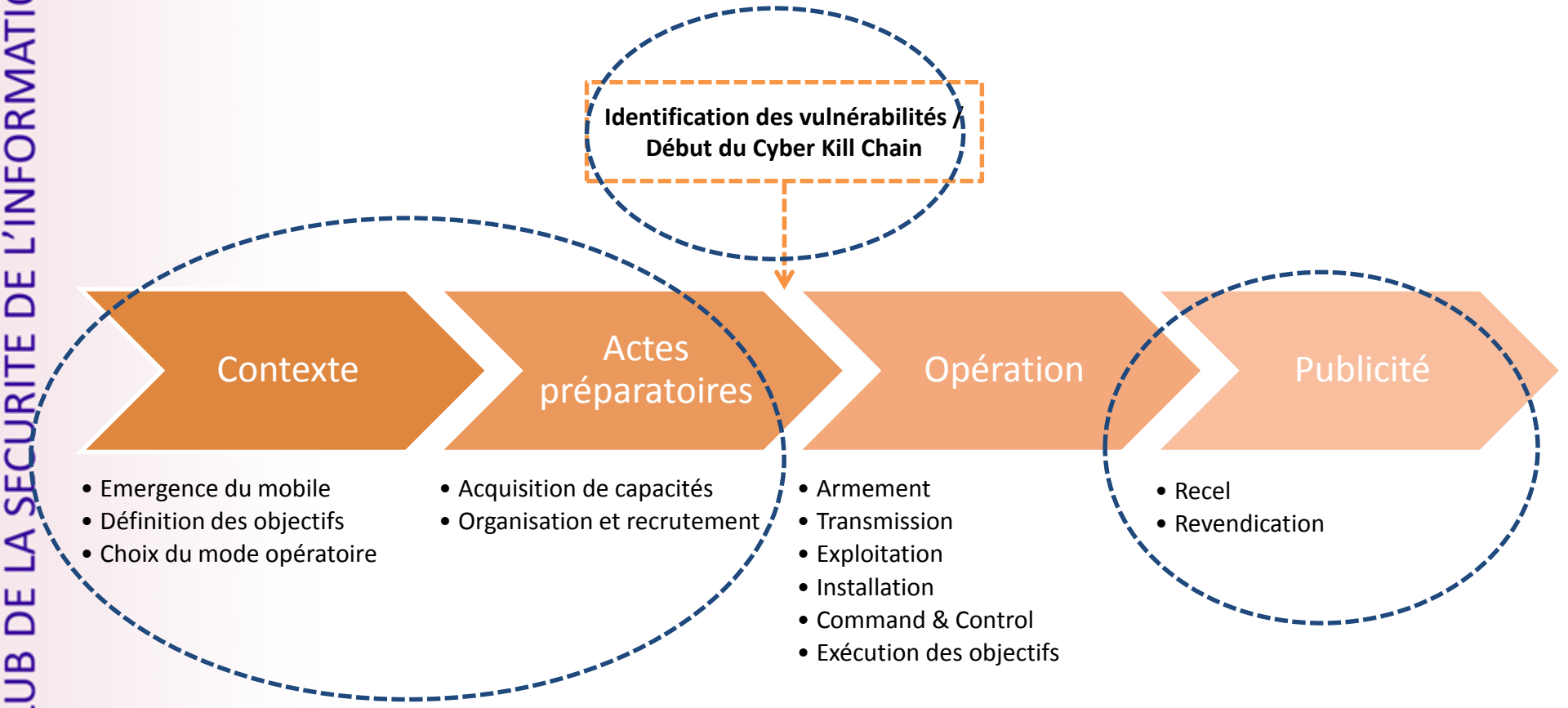
Reconnaissance	• S'informer sur la cible en utilisant de nombreuses techniques
Armement	• Combiner le vecteur d'attaque avec un contenu malicieux
Livraison	• Transmettre le contenu malicieux avec un vecteur de communication
Exploitation	• Profiter d'une faiblesse logicielle ou humaine pour activer le contenu malicieux
Installation	• Installer durablement le contenu malicieux sur un ordinateur hôte individuel
Command & Control (C2)	• Le malware appelle l'attaquant, qui en prend le contrôle
Actions prévues	• L'attaquant vole ou fait ce qu'il avait prévu de faire

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

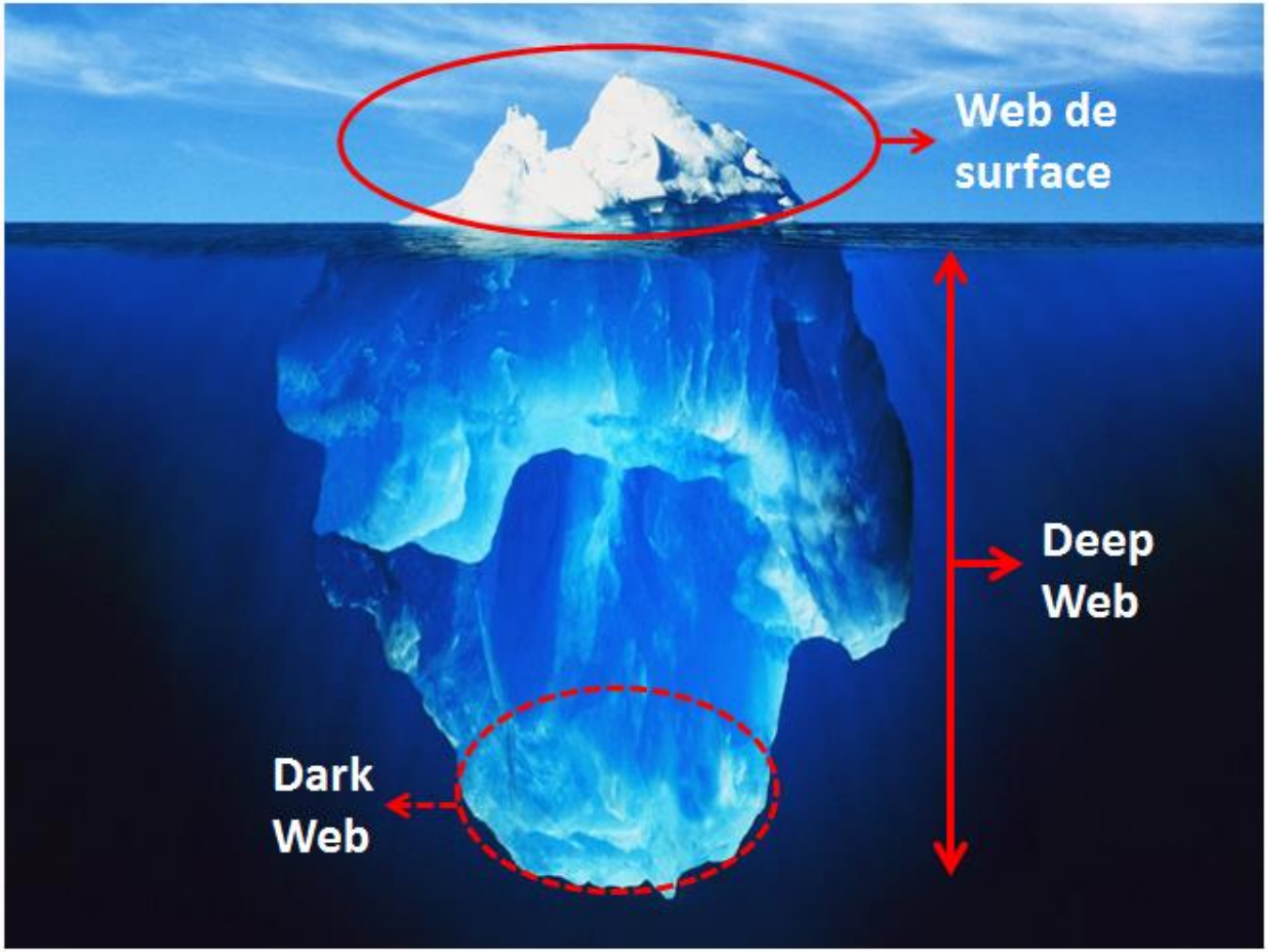
Comment réagir ?

	Technologie	Couverture	Limite des outils
Web de surface	Outils sur étagère	- Réseaux sociaux - Sites de partage - Sites de diffusion - Sites de stockage - Forums	Flux de données brutes sans analyse
Deep Web	Outils sur étagère + Développement d'outils spécifiques		
Dark Web	Développement d'outils spécifiques	- Wikis - Forums - IRC - Blackmarkets	Difficultés pour acquérir l'information à forte valeur ajoutée

Humain
- Présence proactive sur les canaux de communication - Analyse thématique (technique, géopolitique, etc.) - Analyse de tendance - Vision prospective

Le Web de surface: passerelle vers le Dark Web

Le Web de surface: passerelle vers le Dark Web

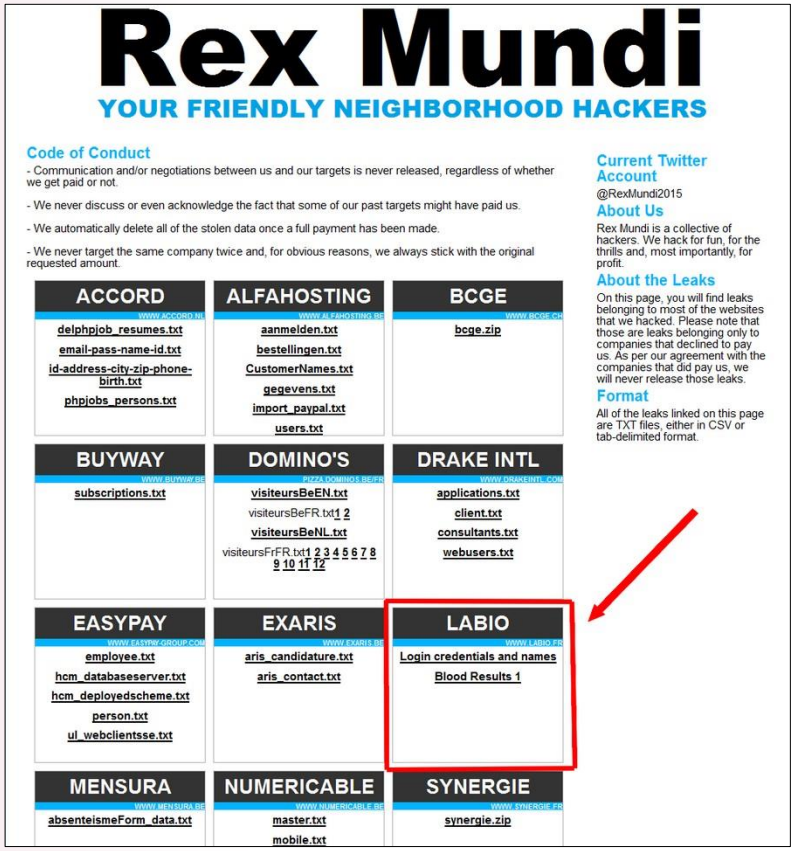


Le Web de surface: passerelle vers le Dark Web

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

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.

ACCORD
WWW.ACCORD.NL
delphpjob_resumes.txt
email-pass-name-id.txt
id-address-city-zip-phone-birth.txt
phpjobs_persons.txt

ALFAHOSTING
WWW.ALFAHOSTING.BE
aanmelden.txt
bestellingen.txt
CustomerNames.txt
gegevens.txt
import_paypal.txt
users.txt

BCGE
WWW.BCGE.CH
bcge.zip

BUYWAY
WWW.BUYWAY.BE
subscriptions.txt

DOMINO'S
PIZZA.DOMINO'S.BE/FR
visiteursBeEN.txt
visiteursBeFR.txt1 2
visiteursBeNL.txt
visiteursFrFR.txt1 2 3 4 5 6 7 8 9 10 11 12

DRAKE INTL
WWW.DRAKEINTL.COM
applications.txt
client.txt
consultants.txt
webusers.txt

EASYPAY
WWW.EASYPAY-GROUP.COM
employee.txt
hcm_databaseserver.txt
hcm_deployedscheme.txt
person.txt
ui_webclientsse.txt

EXARIS
WWW.EXARIS.BE
aris_candidature.txt
aris_contact.txt

LABIO
WWW.LABIO.FR
Login credentials and names
Blood Results 1

MENSURA
WWW.MENSURA.BE
absenteismeForm_data.txt

NUMERICABLE
WWW.NUMERICABLE.BE
master.txt
mobile.txt

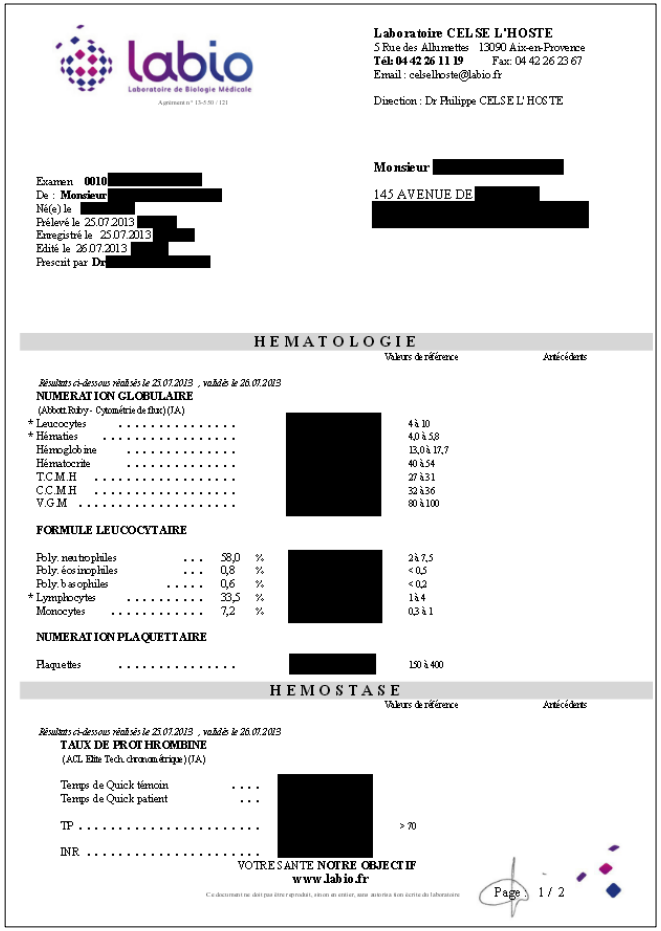
SYNERGIE
WWW.SYNERGIE.FR
synergie.zip

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.



labio
Laboratoire de Biologie Médicale

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**[redacted]
De : **Monsieur**[redacted]
Né(e) le [redacted]
Prélevé le 25.07.2013
Enregistré le 25.07.2013
Edité le 26.07.2013
Prescrit par **Dr**[redacted]

Monsieur[redacted]
145 AVENUE DE[redacted]

HEMATOLOGIE

	Valeurs de référence	Antécédents
Résultats ci-dessous réalisés le 25.07.2013 , validés le 26.07.2013		
NUMERATION GLOBULAIRE		
(Abbott Ruby - Cytométrie de flux) (JA)		
* Leucocytes	4 à 10	
* Hématies	4,0 à 5,8	
Hémoglobine	13,0 à 17,7	
Hématocrite	40 à 54	
T.C.M.H	27 à 31	
C.C.M.H	32 à 36	
V.G.M	80 à 100	
FORMULE LEUCOCYTAIRE		
Poly. neutrophiles ... 58,0 %	2 à 7,5	
Poly. éosinophiles ... 0,8 %	< 0,5	
Poly. basophiles ... 0,6 %	< 0,2	
* Lymphocytes ... 33,5 %	1 à 4	
Monocytes ... 7,2 %	0,3 à 1	
NUMERATION PLAQUETTAIRE		
Plaquettes	150 à 400	

HEMOSTASE

	Valeurs de référence	Antécédents
Résultats ci-dessous réalisés le 25.07.2013 , validés le 26.07.2013		
TAUX DE PROTHROMBINE		
(ACL Elite Tech. chronométrique) (JA)		
Temps de Quick témoin ...		
Temps de Quick patient ...		
TP	> 70	
INR		

VOTRE SANTE **NOTRE OBJECTIF**
www.labio.fr
Ce document ne doit pas être reproduit, même en entier, sans autorisation écrite du laboratoire
Page 1 / 2

Le Web de surface: passerelle vers le Dark Web

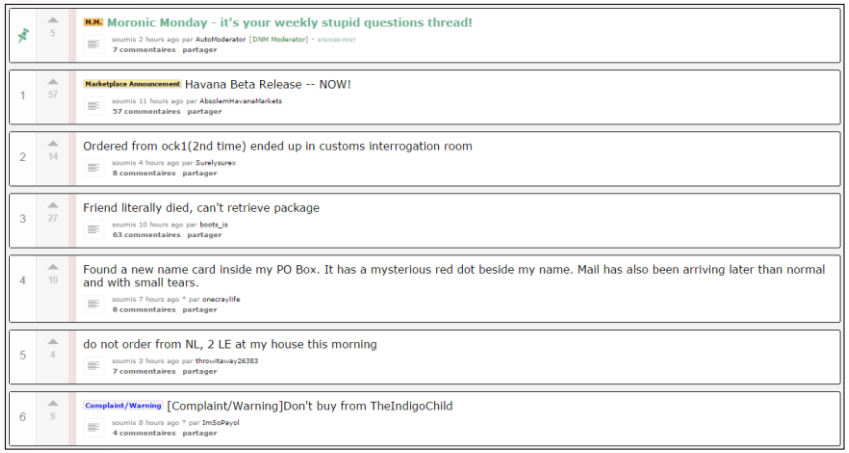
- Bases de données de pasties (Pastebin.com – Justepaste.it – etc.)
  - Instructions d'attaque DDoS (Anonymous)
  - Fuites de données (Carding)

```
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
```

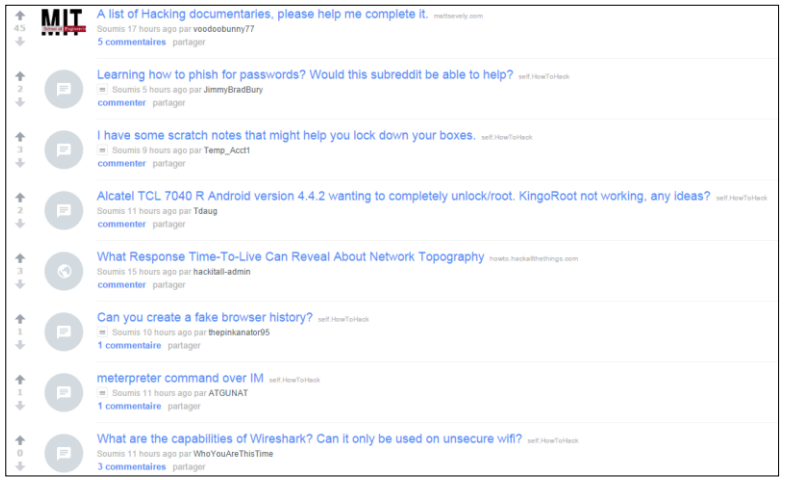
Le Web de surface: passerelle vers le Dark Web

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

Subreddit /r/DarkNetMarkets



Subreddit /r/HowToHack



Le Web de surface: passerelle vers le Dark Web

- Abraxas
- Agora
- Alphabay
- BlackBank
- Bloomsfield
- Crypto Market
- Dream Market
- French Dark Net
- French Dark Place 2
- French Marketplace
- GotMilk Pharmacy
- HonestCocaine
- IDC
- KISS
- LONDON UNDERGROUND
- MIDDLE EARTH MARKETPLACE
- Mr Nice Guy
- Nucleus Market
- Outlaw Market
- Ramp (Russian Anonymous Marketplace)
- Silkkitien
- SwissShop

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

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

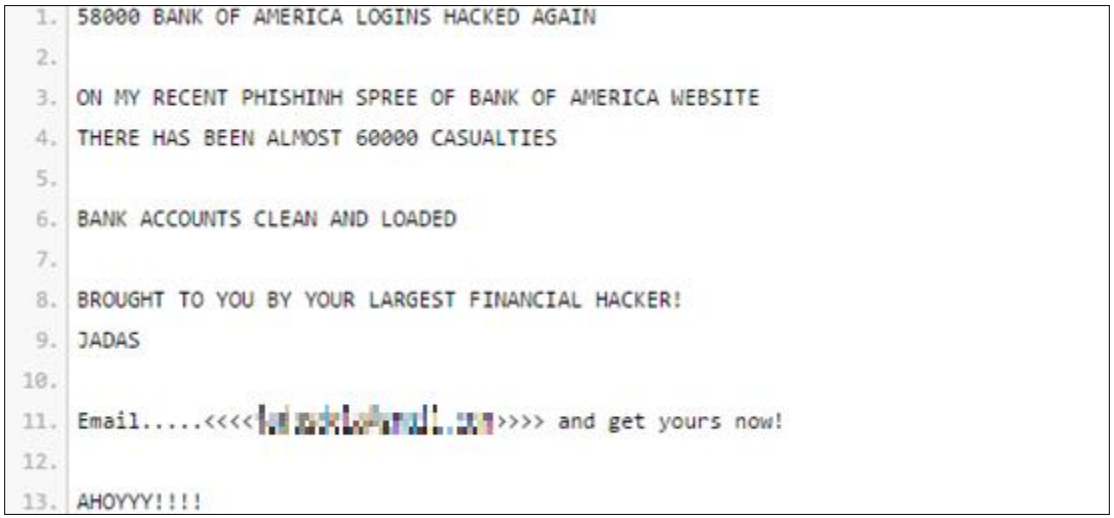
- Double présence des cybercriminels sur le Web de surface et Dark Web

- 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

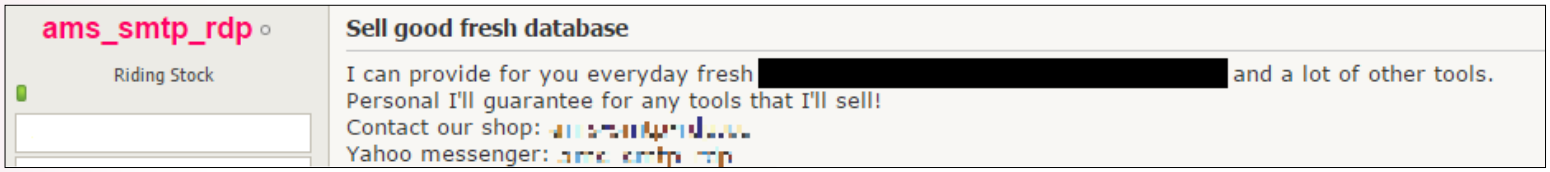


```
58000 BANK OF AMERICA LOGINS HACKED AGAIN

ON MY RECENT PHISHINH SPREE OF BANK OF AMERICA WEBSITE
THERE HAS BEEN ALMOST 60000 CASUALTIES

BANK ACCOUNTS CLEAN AND LOADED

BROUGHT TO YOU BY YOUR LARGEST FINANCIAL HACKER!
JADAS

Email.....<<<<[redacted]>>>> and get yours now!

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)

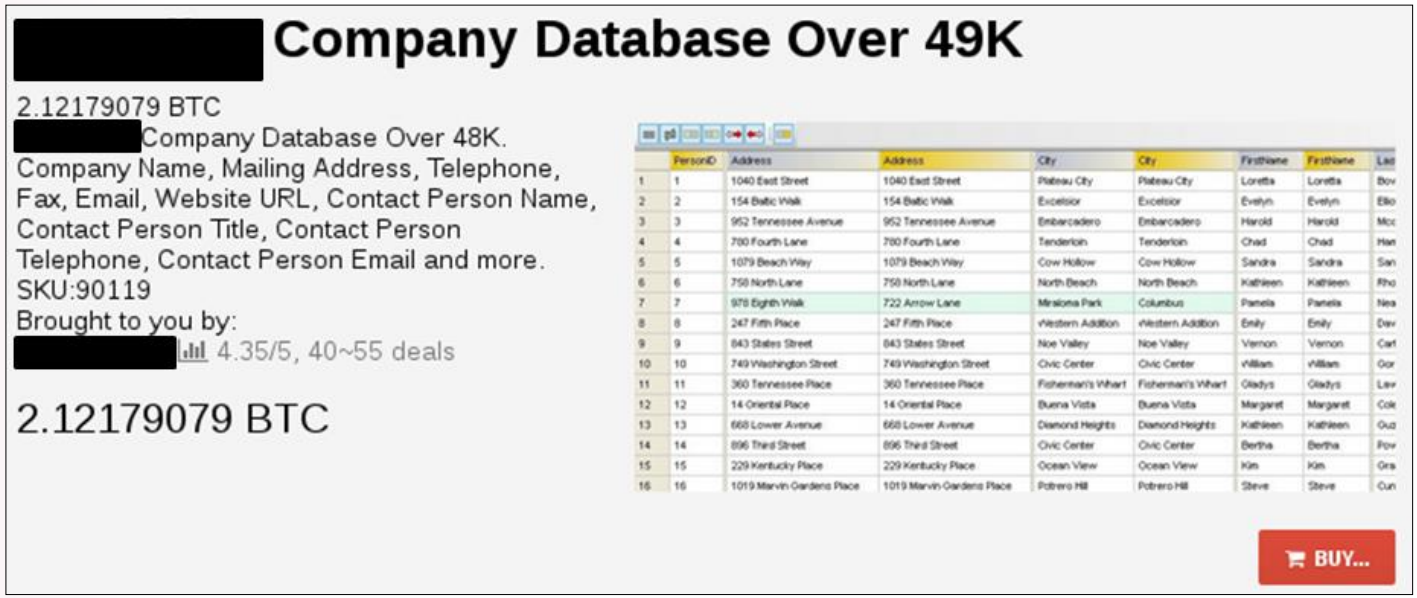


- En fonction de la demande client, échanges avec le cybercriminel
  - Prise de contact
  - Demande d'informations complémentaires
  - Négociation

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



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

- 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

Merci pour vote attention