RESIST Toulouse 04 Octobre 2016

Teyssier Damien

Illustration: Yann Legendre

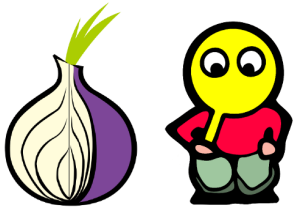
Utilisons le bon langage:

- <u>Ne confondons pas:</u>

- Deep web: tout matériel en ligne non indexé, incluant les darknet.

Darknet, iot, web privé, web dynamique

- Darknet(s): Réseaux utilisant des technologies (P2P) spécifiques, améliorant l'anonymisation, non référencés par le surface web, et très souvent liés à des outils (tor, freenet, I2P).



Quelques données

- Les darknet contiennent entre 200k et 400k sites.
- 2,5 millions d'utilisateurs journaliers (environ)
- 500 fois plus de contenu deep web que surface web
- Estimation data: 40 Zo dont 90% créés dans les 2 dernières années

Espace de dépôt d'une énorme masse d'info (vidéos, pdf,…) sur de nombreux sujets: politique, hacking,…et sur de nombreuses personnes…

En 2015, popular Science déclare que Google a indexé 16% du surface web, soit 1/3000 de tout le web (surface+deep)

- Outils et/ou OS spécifiques les plus utilisés:
- Tor, I2p, tails, freenet, subgraph OS, freepto

L’anonymat

Censé être le point central du relationnel sur le darknet.

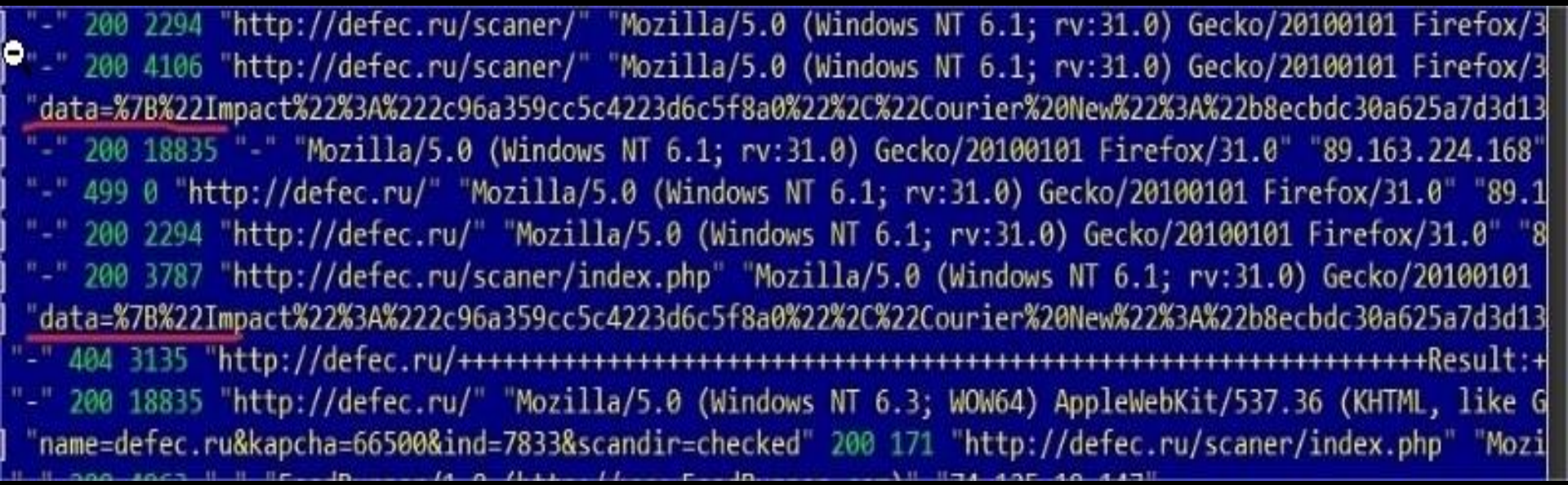
<u>En réalité, compliqué à mettre en place:</u>

machine spécifique, sécurités diverses à appliquer, nœuds tor compromis pas simples à identifier, bridges obscurcis obligatoires,…

Les moyens les plus directs d’être identifié

- Utiliser des connexions non sécurisées vers des serveurs
- Adresse IP
- Cookies, plugins,JS,
- No cookie fingerprint (browser ID)
- Nœuds Tor compromis
- Zero days …
- Ne pas être préparé (OS, plugins,…)

Fingerprint exemple



Source: securelist

Sur quoi repose le darknet?

- Les états
- Les cybercriminels
- Les hackers
- Les défenseurs des libertés
- Les crypto-monnaies
- Le Blackmarket

Les états et la géopolitique cachée

Le « darknet » est un remarquable moyen de renseignement protéiforme

Cybint, osint, assistance au humint,...

Exemple: memex (darpa), spiderfoot et autres progs d'acquisition automatique d'intel.

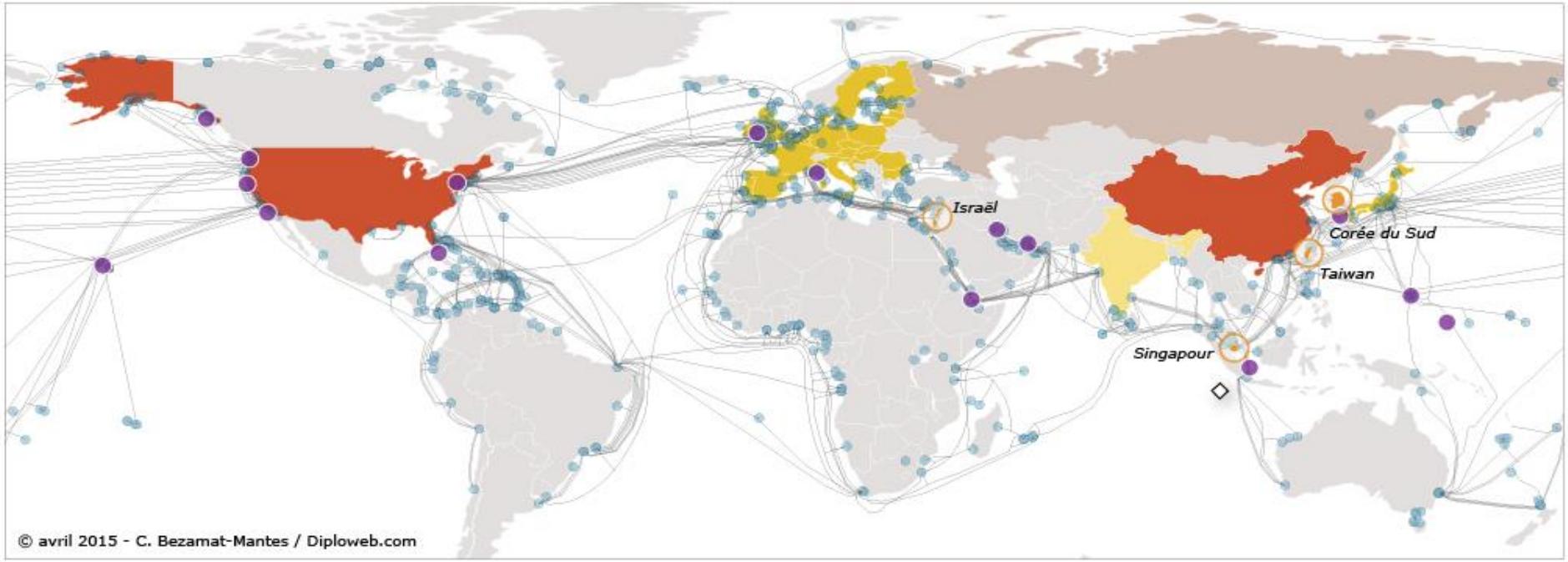
Pourquoi la NSA finance Tor de 600 000$ par an sur un budget total de 2Millions $?

Pourquoi la Russie possède (directement ou indirectement)

60% des nœuds Tor ?

Rapport force surface web

Géopolitique de l'Internet : quelle hiérarchie des puissances ?



I. Des acteurs inégaux ...

- Les cyber-puissances : Etats-Unis et Chine
- 4 cyber-dragons : Israël, Singapour, Taiwan, Corée du Sud
- Les déserteurs du cyber-espace : Union européenne et Japon
- Un acteur secondaire : l'Inde
- Un quasi-absent : la Russie (sauf pour les virus, antivirus et attaques cyber)

II. ... et de remarquables moyens de renseignement

- Câbles sous-marins
- Points d'entrée des câbles (stations d'atterrage)
- Points d'accès majeurs de la NSA aux stations d'atterrage des câbles
- Sous-marin américain capable de faire des branchements secrets sur les câbles immergés

Sources : La Documentation Photographique, n° 8104, Antoine Frémont et Anne Frémont-Vanacore, *Géographie des espaces maritimes*, Documentation française - DILA, mars-avril 2015 ; L. Bloch.
Conception de la carte et de la légende : C. Bezamat-Mantes, L. Bloch, P. Verluise. Réalisation : C. Bezamat-Mantes.

Cybint and Cyberwarfare

- Délégation d'une partie du cybint et du cyberwarfare
- Réduction de la trace étatique et des sphères d'influence marquées
- Achat d'informations à bas prix (on ne parle pas que d'argent mais aussi de jeux d'influence publique ou non, de shadow intel sur les alliés,…)
- Possibilité d'actions tous types non revendiquées,…

Les « Liberty » friends

- Journalistes
- Cyber-activistes
- Oppressés ou minorités d’état (exemples Turquie, Tibet)
- Whistleblowers

Les crypto-monnaies

- Bitcoin 
- Escrow 

- Litecoin 

- Dogecoin 
- Perfect money, Webmoney (russie) 

- Ethereum ? 

- Monero ? 

NB: L'impact des blockchains dans tous les types de relations transactionnelles

Les hackers

On en rencontre de tous types, du « fun boy »
au cybercriminel endurci, solitaire ou non.

On trouve BCP de littérature et d'échanges divers
liés au piratage sur ces réseaux.

Votre avatar possède souvent une image de marque,
et les portes qu'on vous ouvre (contrats, sites,…)
dépendent de votre réputation.

Des bourses d'emploi existent pour des contrats uniques.

De nombreux services sont disponibles, pas forcément illicites

PROFESSIONAL **HACK GROUP** QUICKLY HELPS TO SOLVE YOUR NEEDS

BASIC SERVICES THAT WE PROVIDE:

Hacking

- Have you been hacked?
- Do you want to find out if your website, computer or network can be or has been hacked?
- Would you like to hack into a computer, website or network?

Social Media Threats

- Has your Facebook, Twitter or Google+ account been hacked? We can help get it restored and track the person who did it in many cases.

Computer Spying and Surveillance

- Do you want to install spyware on a cellphone or computer?
- Do you want to know if you have spyware on your computer?

Remove A Link

- Mugshot Picture Removed
- Blog Link Removed
- Google Link Removed

Locate Missing People

- Find and reconnect with family, old friends, relatives just about anyone! People Search reports include phone numbers, address history, ages, birthdates, household members and more.

Background Checks

- Background reports include, when available, a criminal check, lawsuits, judgments, liens, bankruptcies, property ownership, address history, phone numbers, relatives & associates, neighbors, marriage/divorce records and more.

SSN Trace

- Address History
- 7-Year National Criminal Database Search
- Courthouse Verification of Criminal Database Records (up to 3)
- National Sex Offender Registry Check

Online Dating Scams

- Have you been scammed because all you were looking for was love? We can help you in 2 ways.
- Verify the person's identity before meeting the person and moving to the next step.
- If you have been scammed online and would like to track the person's location so you can proceed with some type of action.

Cyber bully - Cyber Stalked

Computer Security Training

Cyber Extortion

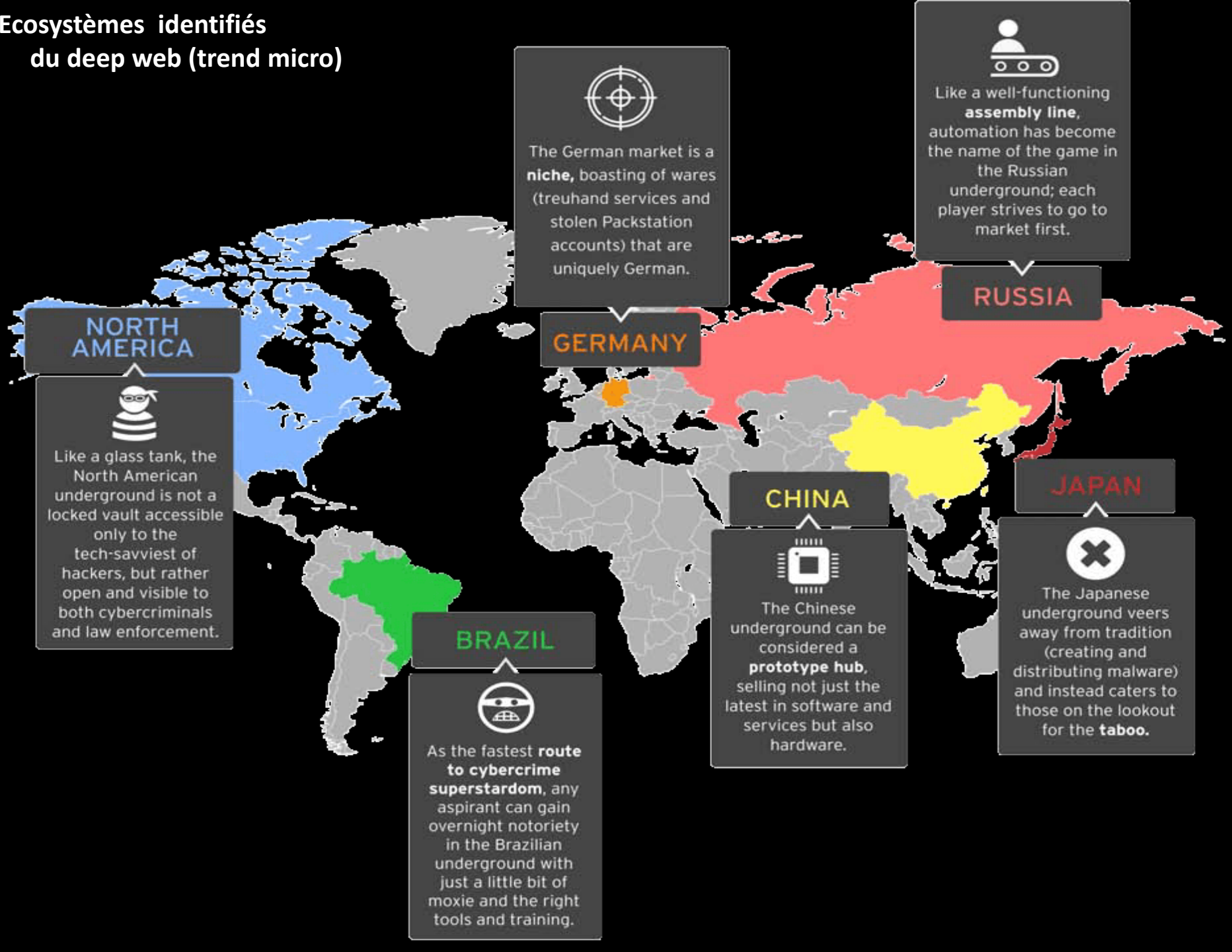
Relationships

La cybercriminalité

- La cybercriminalité est courante, diverse, plus ou moins malsaine…
- Pédophilie, vente d'armes, de drogues, d'êtres humains, de service de tueurs à gages (pas tous vrais^^), ….

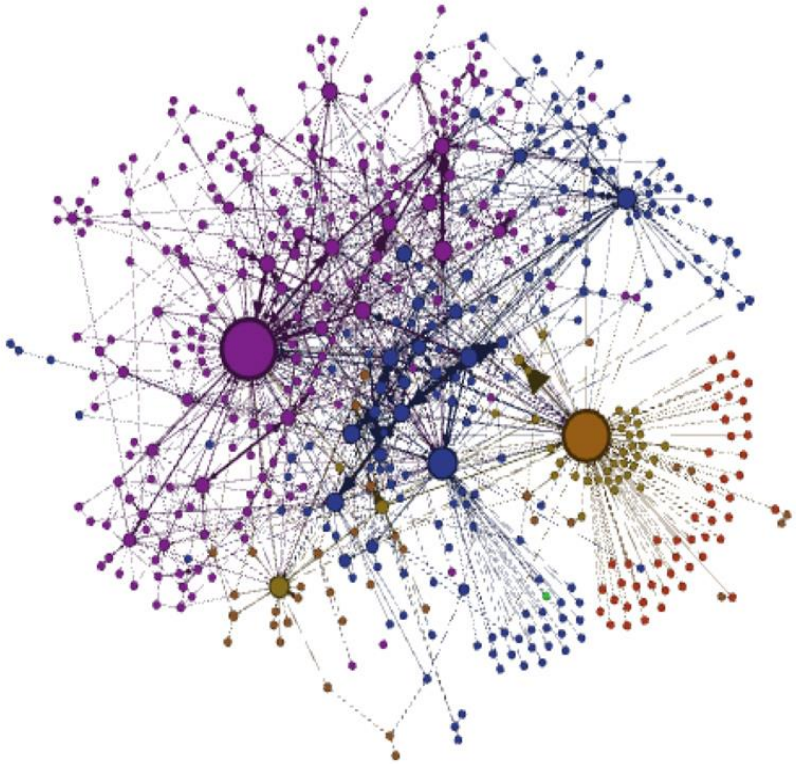
- Mais aussi de renseignements sur des entités ou des individus, de services d'action technique ou de vente de programmes divers,…

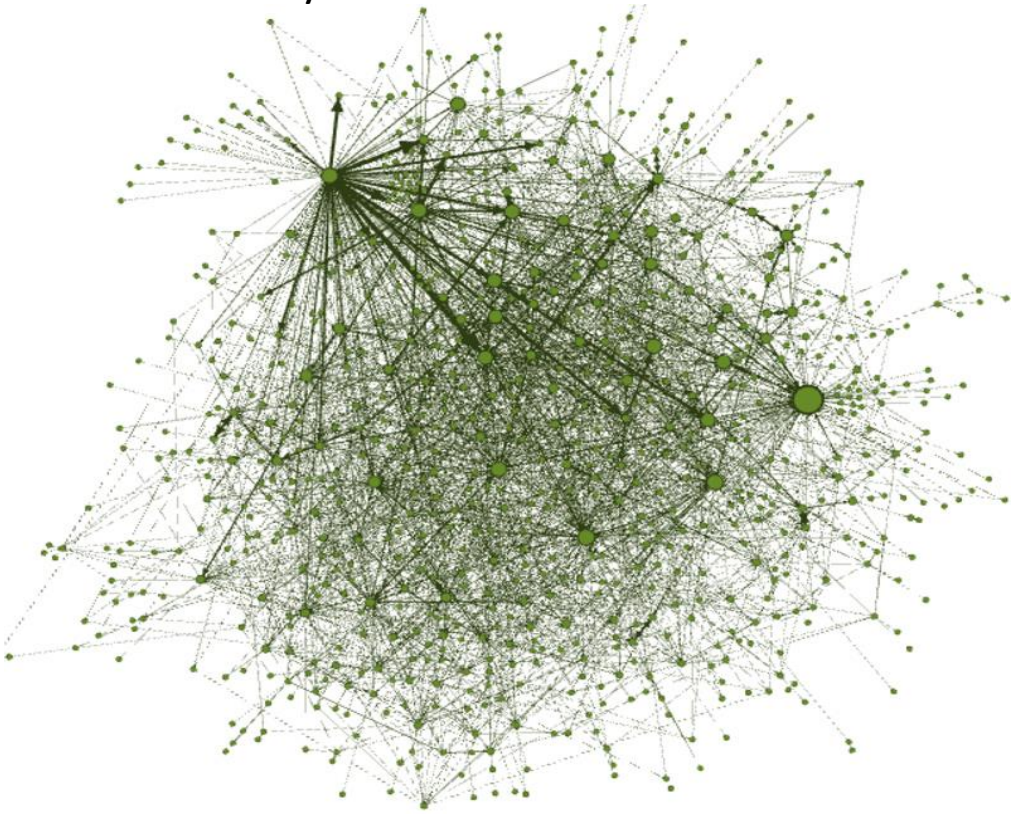
Ecosystèmes identifiés du deep web (trend micro)



La cybercriminalité (L'organisation)

Deux organisations courantes des cybercriminels:





Fonctionnement type « GANG » :

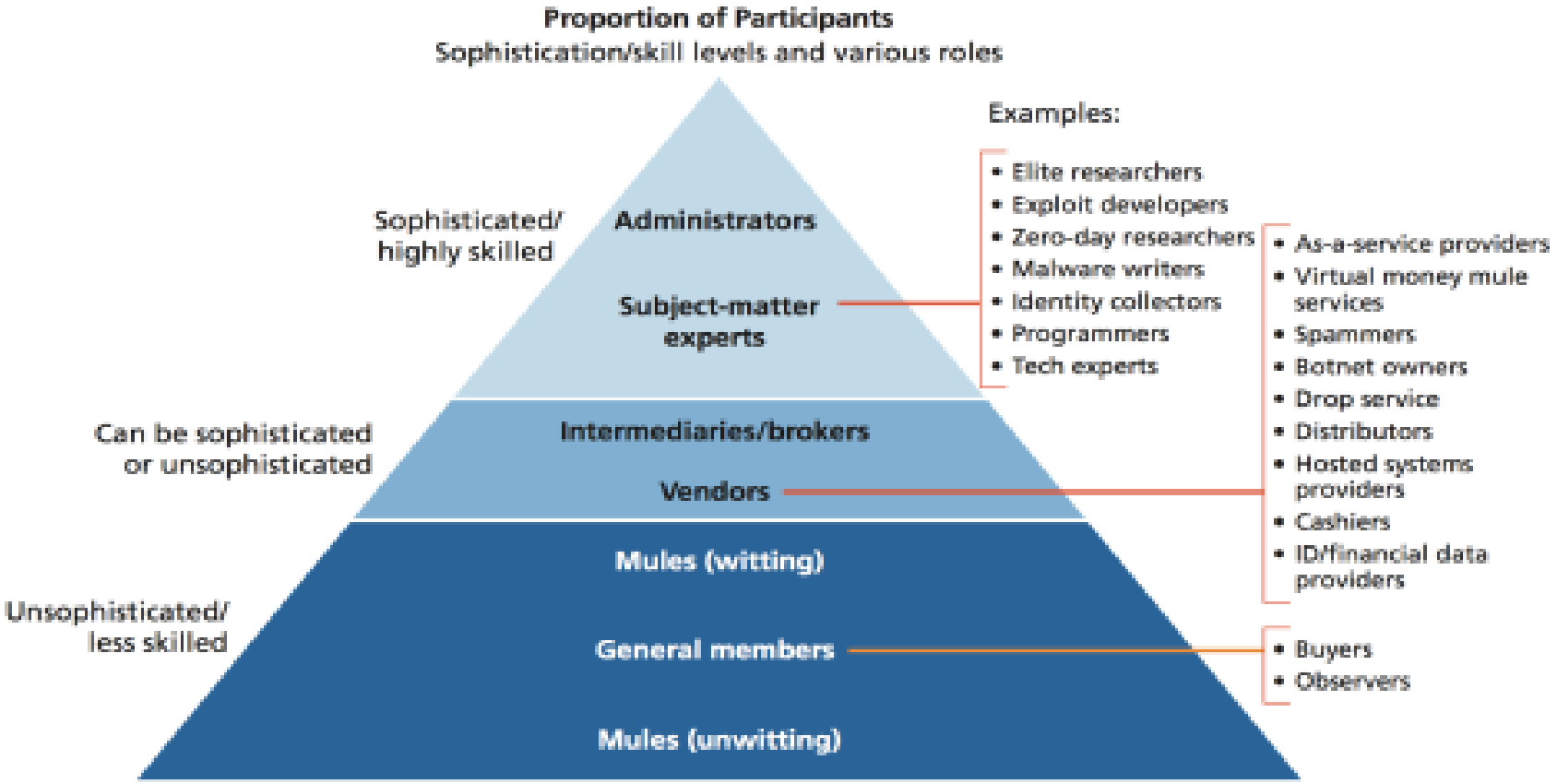
Un chef, des lieutenants, action pyramidale et peu structurée, attaque tout ce qui leur tombe sous la main, …

Fonctionnement type « Cartel » :

Gestion par spécialisation, but d'optimisation et rentabilisation, éclatement des fonctions pour mieux s'étendre,…

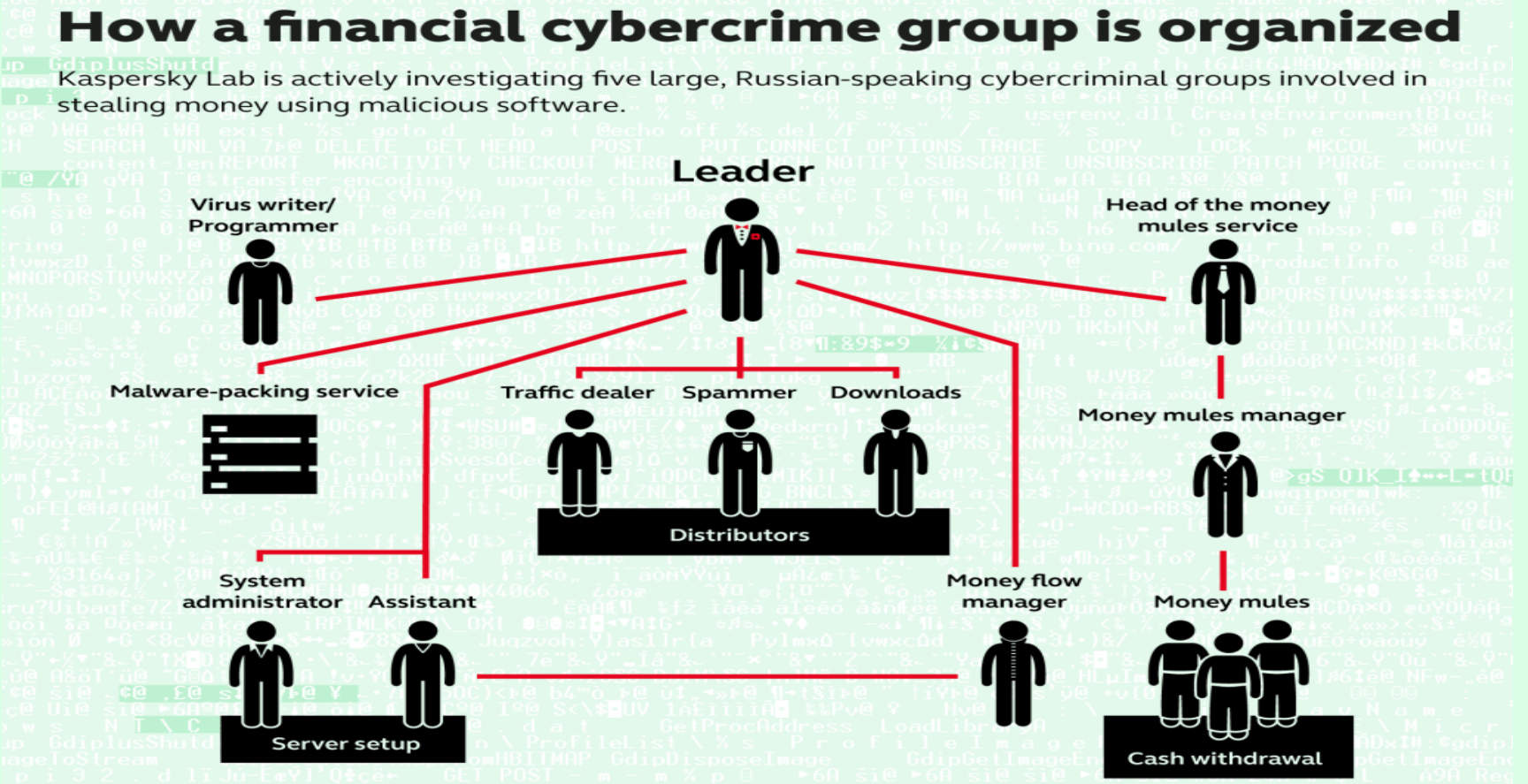
La cybercriminalité (L'organisation)

Figure 2.1
Different Levels of Participants in the Underground Market



SOURCES: Drawn from interviews; Schipka, 2007; Panda Security, 2011; Fortinet, 2012; BullGuard, undated.
NOTE: Almost any participant can be a ripper; see text for discussion.
RAND RR610-2.1

Exemple russe



Le blackmarket en France

Environ 40000 personnes satellites de ce milieu en France en 2015 (clients, vendeurs,fournisseurs)

Comme les Russes et les allemands, nous travaillons bcp en tierce partie

Schéma Buyer/escrow/seller

L'escrow sert d'intermédiaire et prend 7% des transactions de moins de 500$ et 5% au dessus (4% sur Intelligence Black Market)

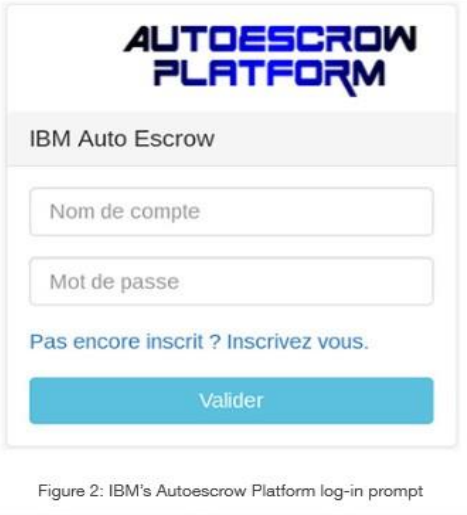


Figure 2: IBM's Autoescrow Platform log-in prompt

méthodes de vente et particularités

- <u>3 méthodes:</u>

- Publicité sur les marketplace connus
- Approche directe client par profilage
- Autoshop (quasiment existant qu'en France et au Japon):
  petit magasin en ligne géré directement par le vendeur

On a parfois des frais d'inscription au market, souvent associé à une authentification (pas existante dans tous les pays).

400 euros l'autoshop prêt à servir.

Deux paiements acceptés uniquement en France: bitcoin et cartes prépayées.

Quelques prix et produits fr?

Photo: zataz

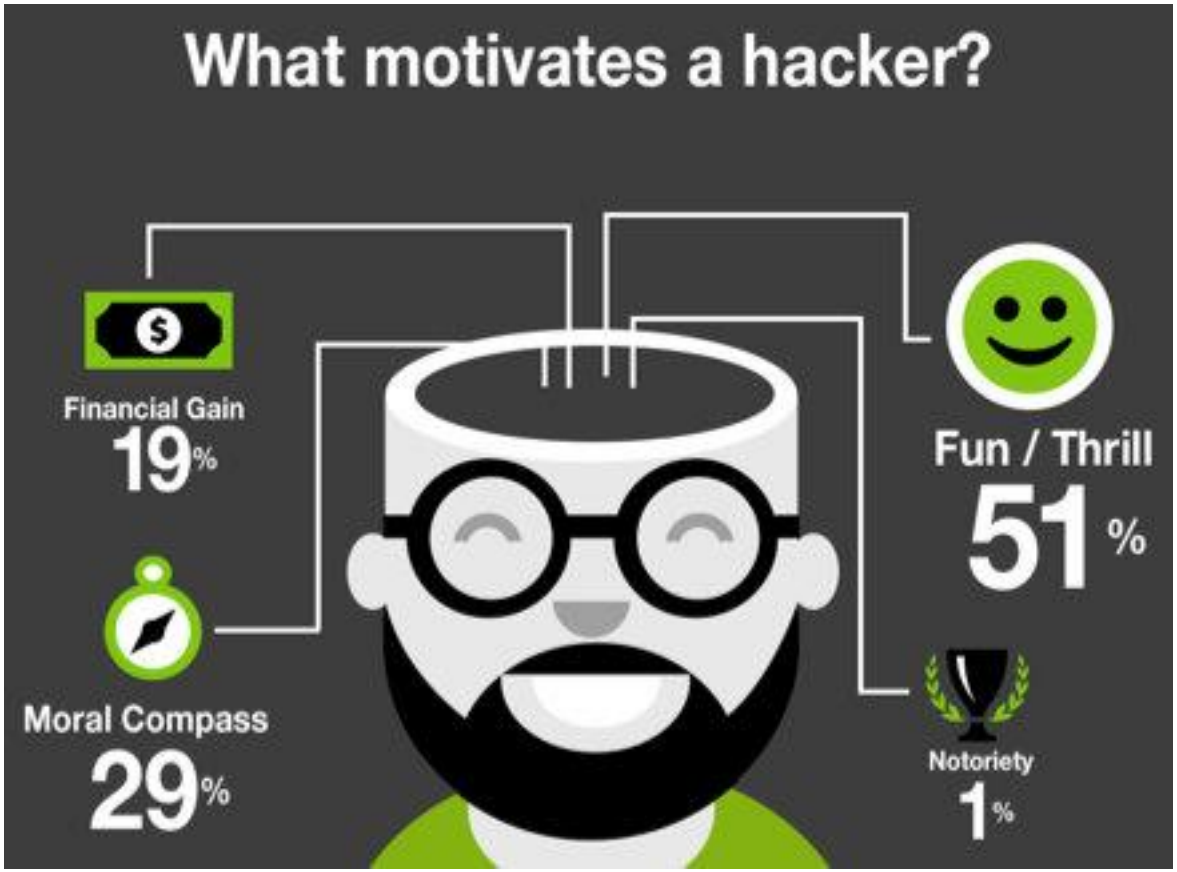
Product/Service	Price
Fully undetectable (FUD) crypting service	€4–100
Bulletproof-hosting service	€10
Phishing kit	€100–500
Phishing page	€5
Phishing-website-creation service	€299
Botnet rental (100–150 bots/day)	€95
Fake national ID card	€60
Fake disabled ID card	€40
Fake document pack (ID and proof of identity)	€50–100
Teslin paper (used to create national/government ID cards; 200 sheets)	€167
Portable Document Format (PDF) file-editing service (including metadata modification)	€8
Fake money (€300 in €20 bills)	€135–150
Fake checks made out to specific recipients (10 pieces)	€70–100
Vulnerable website log (100 sites vulnerable to SQL injection attacks)	€30
Access to vulnerable website	€1–2
Software-vulnerability-scanning service (via source code analysis)	€219
Stolen credit card credentials (depending on limit/available balance)	€9–23
Automated teller machine (ATM) skimmer	€800
Credit card clone (depending on limit)	€40–110
Access to compromised PayPal account	€5–10
Access to compromised Amazon account	€10

Product/Service	Price
Fake shop gift card	50% of the card's amount
Access to compromised Facebook account	€0.50
Access to compromised Gmail/French Webmail service, Spotify, or Netflix account	€1
Access to compromised Leboncon, Wi-Fi Internet service provider (ISP), Cdiscount, Pixmania, LDLC, Zalando, Auchan, or 3Suisses account	€2
Access to compromised PlayStation account (+20 games)	€3
Stolen data dump	€400
Stolen banking website config files	€50

Training/Tutorial Topic	Price
How to open bank accounts for use in fraud	€450
How to convert credit card balances into BTC	€250
Carding	€29–150
How to convert PayPal balances into BTC	€100
SQL injection	€60
How to monetize access to compromised PayPal accounts	€60
How cybercrime affiliation works	€30
How to make an unlimited amount of Amazon refunds	€25
How to use a RAT	€20
How to send and receive illicit goods and payment anonymously	€10
How to spread malware	€2

Source darknet France : trend micro

Nous sommes tous des cibles (de valeur)



Pourquoi ?

Je sais que je suis paranoïaque, mais ce n'est pas parce que je suis paranoïaque qu'ils ne sont pas tous après moi ….

sources

- Wilson Center,
- House of parliament (UK),
- Batblue company ,
- University of Luxembourg,
- Cryptopolitic of the darknet (issn 0039-6338) Rid and Moore,
- Nsa documents,
- Securelist
- Kaspersky
- Trend Micro
- RAND
- Divers blogs spécialisés, lectures diverses, j'espère n'oublier personne ;)
- Sources personnelles

Merci de votre attention, des questions ?