Le combat numérique : une approche de la lutte contre les cybermenaces

Bertrand Boyer

2017

C'est qui ?

- Saint-cyrien, diplomé de l'école de guerre et de Télécom Paris
- Membre de la chaire de cyberdéfense des Ecoles de Saint-Cyr
- Animateur du blog Cybertactique

Avertissements

- Les propos n'engagent que l'auteur et ne reflètent pas les opinions du Ministère des Armée.
- Cette présentation est pour votre usage exclusif.

La méthode de raisonnement militaire

- Analyse de l'ennemi
- Analyse des amis
- Analyse du terrain - du temps
- Analyse de la mission
- Ebauche d'une manoeuvre - modes d'action (MA)
- Confrontation des modes d'action - Révision des MA
- Décision

Cyberespace

Vous avez dit "cyber" ?

*Espace de **communication** constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.[Défense et sécurité des systèmes d'information stratégie de la France, ANSSI, 2011].*

Journal Officiel du 19 sept 2017

*Espace constitué par les **infrastructures** interconnectées relevant des technologies de l'information, notamment l'internet, et par les **données** qui y sont traitées.*

Cyberespace

Les Armées, en France

Le cyberespace est un domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont internet), des réseaux de télécommunications, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs des services en ligne.[Concept Cyberdéfense, CICDE, 2011]

Le cyberespace est à la fois **physique** (il regroupe les infrastructures réseau et de lélécommunication ainsi que les équipements connéctés) **immatériel** (il englobe également les "protocoles" et mécanismes de contrôle) et **social** (l'information transportée). Dès lors on évoque souvent les trois couches du cyberespace :
physique, logique, sociale ou sémantique.

Cyberguerre

Un concept très discuté, souvent utilisé à tort.

Wikipedia:

La cyberguerre, ou guerre cybernétique, consiste en l'utilisation d'ordinateurs et de l'Internet pour mener une guerre dans le cyberespace.

cyberattaque

*Ensemble coordonné d'actions menées dans le cyberespace qui visent des **informations** ou **les systèmes qui les traitent**, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité.*

cyberattaque persistante

Cyberattaque qui met en oeuvre des moyens humains et techniques importants pour infiltrer durablement les systèmes d'information vitaux d'une organisation.

Théâtre d'opérations ?

- Livre Blanc 2008 et 2013

le glossaire de terminologie militaire

Espace géographique délimité dans lequel une force opère pour remplir une mission fixée par l'autorité stratégique.

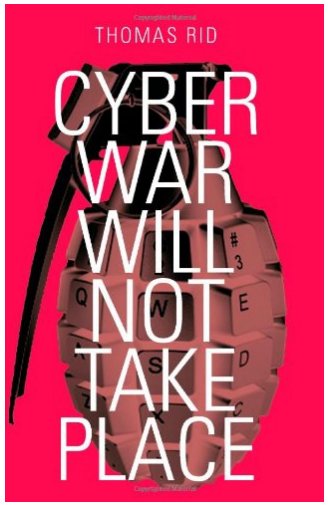
Menace sur le SI

Une menace sur un système d'information est caractérisée par:

- Un attaquant ou un groupe d'attaquants;
- Un mobile, une finalité recherchée;
- Un chemin d'attaque, avec des outils associés - une infrastructure technique;
- Une ou plusieurs victimes.

La menace s'excerce sur les trois couches du cyberespace

- Couche physique: pénétration physique de l'infrastructure cible;
- Couche logique: utilisation de vers, bombes logiques, saturation, détournement;
- Couche cognitive / sémantique: manipulation, désinformation, revendication...



- Espionnage
- Subversion
- Sabotage

Peut-on alors parler de rupture stratégique ?

Dans l'histoire militaire, les évolutions techniques ne se traduisent pas toujours immédiatement en "révolution" tactique.

sur la couche physique: le lien entre virtuel et réel

L'action vise les infrastructures réseaux, du terminal au routeur en passant par le câble et l'antenne.

- Dualité de la cible (objet civil ou militaire ?)
- Armes numériques ou classiques ?
- Effet boomerang: comment l'éviter ?

sur la couche logique: le code est partout

Les opérations sur la couche logique sont plus faciles à percevoir et à concevoir. Elles agissent sur les processus automatiques, via l'injection ou la modification d'instructions ou de données (...)
L'instruction est donc au cœur de cette couche et sa traduction littérale, le code, l'arme du combat logique.

sur la couche cognitive / sociale

Avant de conduire des opérations sur la couche cognitive, on cherche à la maîtriser pour améliorer les fonctions classiques du combat.

- Le retour de la propagande

  Les forces armées doivent pouvoir s'engager dans le cyberespace pour ne pas y laisser sans contrepoids les propagandes et les idéologies qui s'y expriment.

- Pour quels effets ?

En fait.... non!

Typologie de l'adversaire

Profils

- Étatique
- Idéologique
- Ludique
- Technique
- Pathologique - affectif
- criminels - lucratif

Les motivations

- Espionnage - renseignement politique et économique
- Sabotage - destruction - neutralisation
- Propagande - agitation
- Financière

Comprendre le message

- Un acte technique est toujours porteur d'un message
- Revendication - message vers la cible ou vers d'autres ?
- Usurpation - qui se cache derriére l'action ?
- Dissuasion ?

Cas particulier : la cybercriminalité

- Des "services" en ligne :"*Hacking as a service*".
- Des circuits de distribution: Les marchés noirs en ligne.
- Des cibles multiples: Le vol de données personnelles, secrets industriels, renseignements...

Caractéristiques

- Diversité.
- Professionalisme.
- S'appuie sur la criminalité "classique".
- Favorise la "prolifération" des outils d'attaque

Hacking Team

Alliés et alliances

La notion d'alliance est remise en cause.

Alliance classique

- Fondée sur un rapport de force mesurable
- Une alliance de force pour faire basculer le RAPFOR
- Souvent de proximité (géographique ou idéologique)

Alliance "cyber"

- Souvent à périmètre réduit
- Suppose le partage d'informations sensibles (capacités)

6 juin 2013

Vault7

Operation Socialist - 2010 - 2012

The Belgacom hack, Snowden said, is the "first documented example to show one EU member state mounting a cyber attack on another. . . a breathtaking example of the scale of the state-sponsored hacking problem."

The Intercept

Les modèles d'attaque

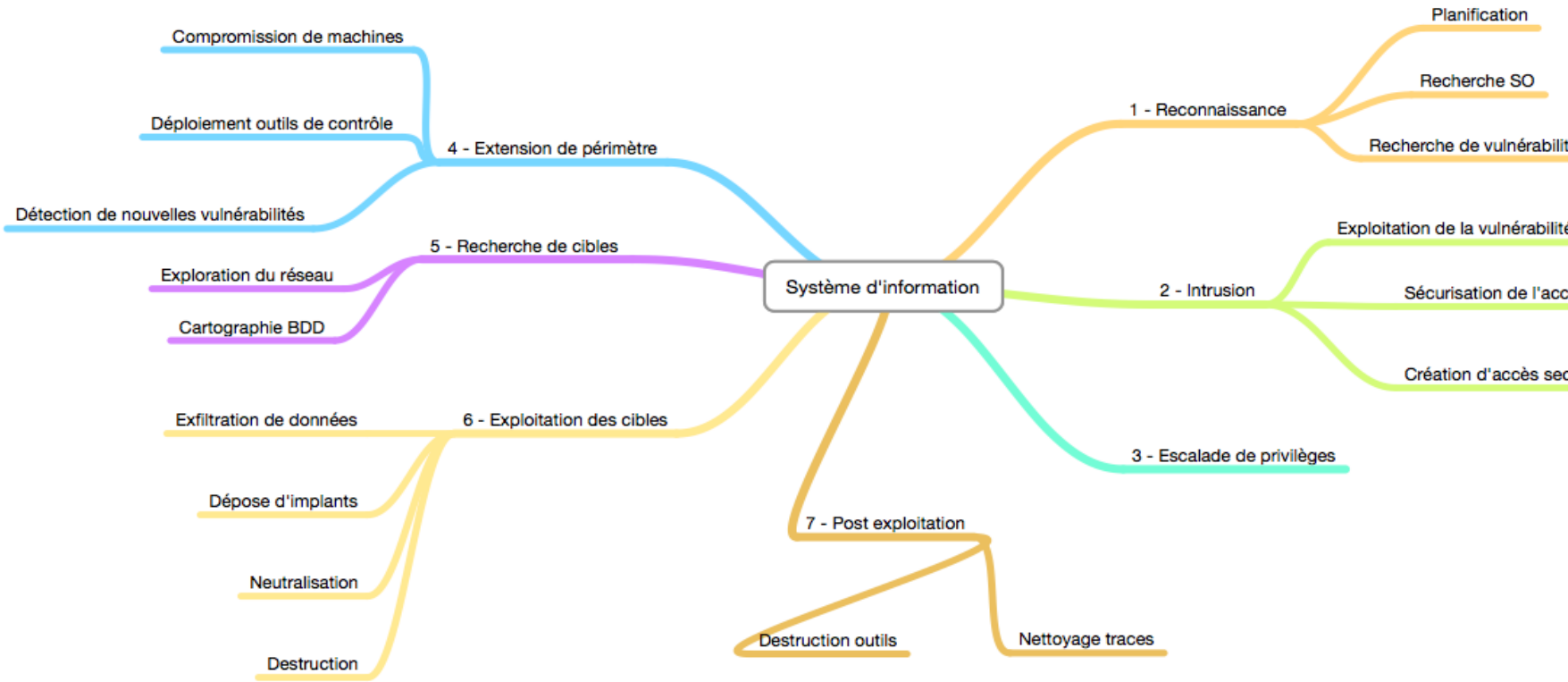
Attaques directes

- Intrusions
- DDoS
- Ransomware / cryptolockers

Attaques indirectes

- Attaques / infections via clients et/ou prestataires
- "Insider"
- Attaques informationnelles (e-reputation)

Les composants de l'attaque



Cyberespionnage

Multiplications des cas d'espionnage informatique sur l'ensemble du tissu économique. De la PME au CAC 40. De la sous-préfecture au ministère.

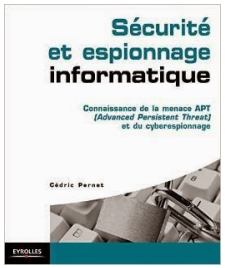
Priorité des services

- Mode d'action indolore;
- Difficulté d'attribution;
- Impacts (politique, stratégique, économique)
- Vulnérabilités nombreuses.

Advanced Persistent Threat, une définition ?

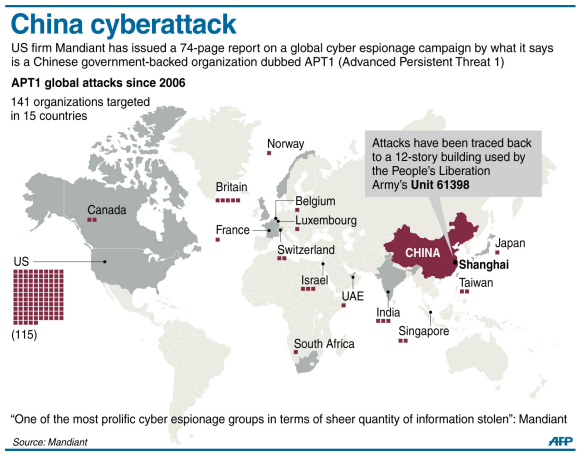
Terme d'origine US (2006) pour désigner des **attaquants étatiques**.

> *Une attaque informatique persistante ayant pour but une collecte d'information sensibles d'une entreprise publique ou privée ciblée, par la compromission et le maintien de portes dérobées sur le système d'information.*[1]



[1] Pernet, Sécurité et espionnage informatique, Eyrolles 2014.

Advanced Persistent Threat



La nature organisée des attaques APT est ce qui les rend avancées et c'est cet attribut combiné avec le ciblage d'une entreprise spécifique qui les rend différents des autres scénarios de menaces. Les APT ne sont pas nécessairement "sophistiquées".

Advanced **Persistent** Threat

Une APT, par nature cherche à se maintenir sur le système cible. Il y a contrôle en profondeur du SI par l'attaquant. Une APT peut rester plusieurs années sur sa cible.

Advanced Persistent **Threat**

Terme complexe à cerner, et s'il peut paraître lié au code mis en œuvre, il fait plutot référence á l'intelligence qu'il y a derrière. La menace ce n'est pas le malware, c'est le groupe qui cherche à l'utiliser dans un but précis.

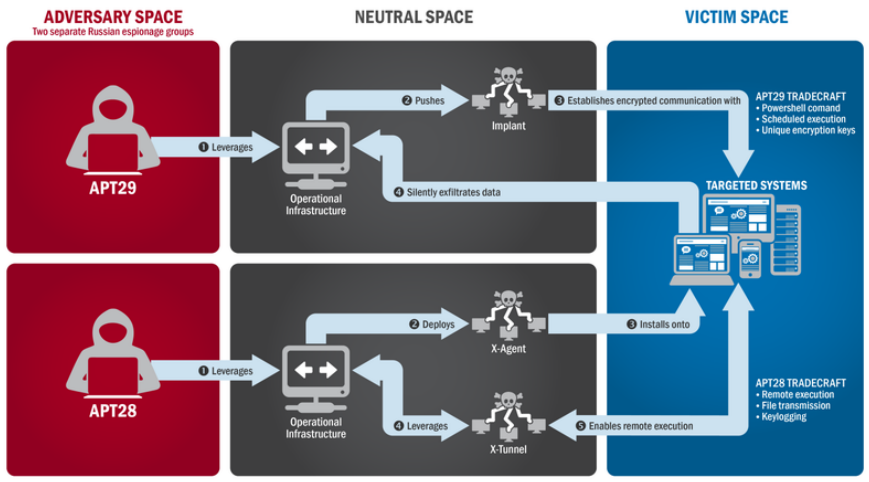
exemples d'APT

Chine ?

- APT 1, PLA 61398;
- APT 4, "Nitro Gang", suivi depuis 2012, existerait depuis 2011;
- APT 14, cible le secteur de l'aéronautique, utilise le "water hole".

Russie ?

- APT 2, découvert en 2013, cible le secteur de l'énergie;
- APT 28 "Fancy Bear", Vaste infrastructure d'attaque, cibles politiques et militaires;
- APT 29 "Cosy Bear", Pentagon UN email (2015), DNC (2016)...



Premier exemple documenté d'utilisation de l'outil informatique à des fins de sabotage, Stuxnet utilise un code malveillant qui leure les systèmes de protection et les capteurs physiques afin d'induire en erreur les opérateurs des installations d'enrichissement d'uranium en Iran.

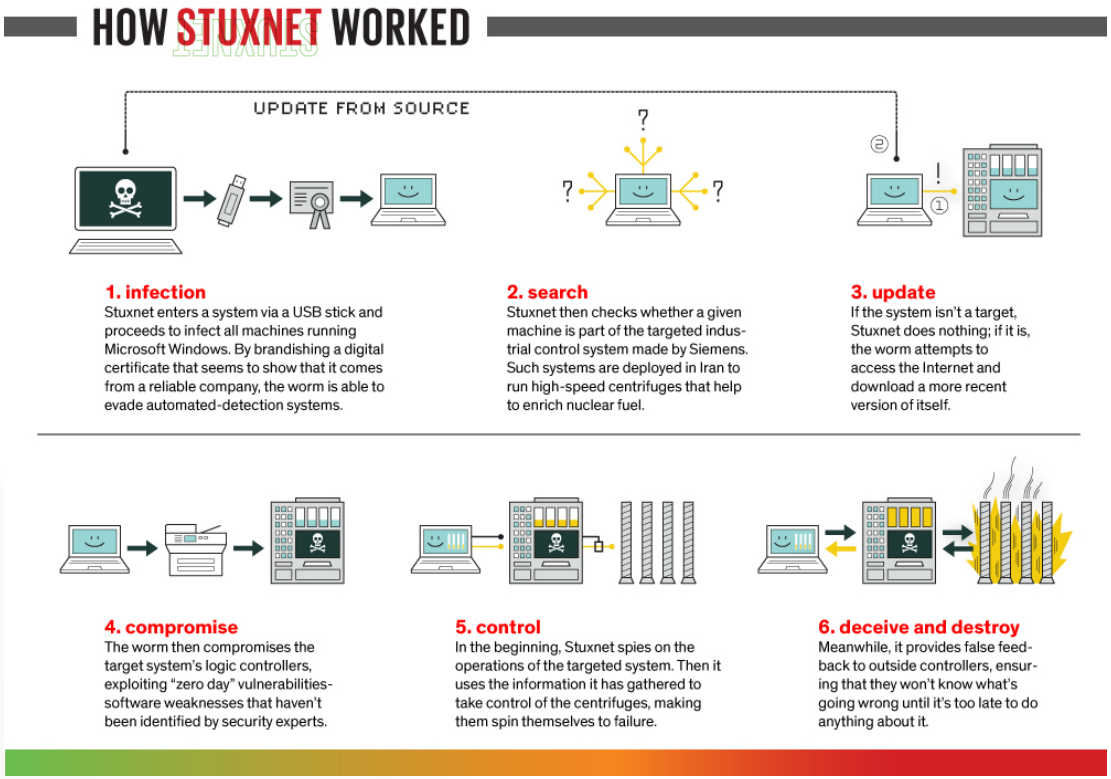
Stuxnet

- Exploite plusiuers failles zero-day.
- Découvert en 2010 le programme aurait débuté en 2006.
- Utilise des certificats de sécurité dérobés.
- Furtif et assez résistant.

L'opération semble avoir atteint son objectif stratégique :

- Ralentir le programme nucléaire iranien.

une petite vidéo ;-)

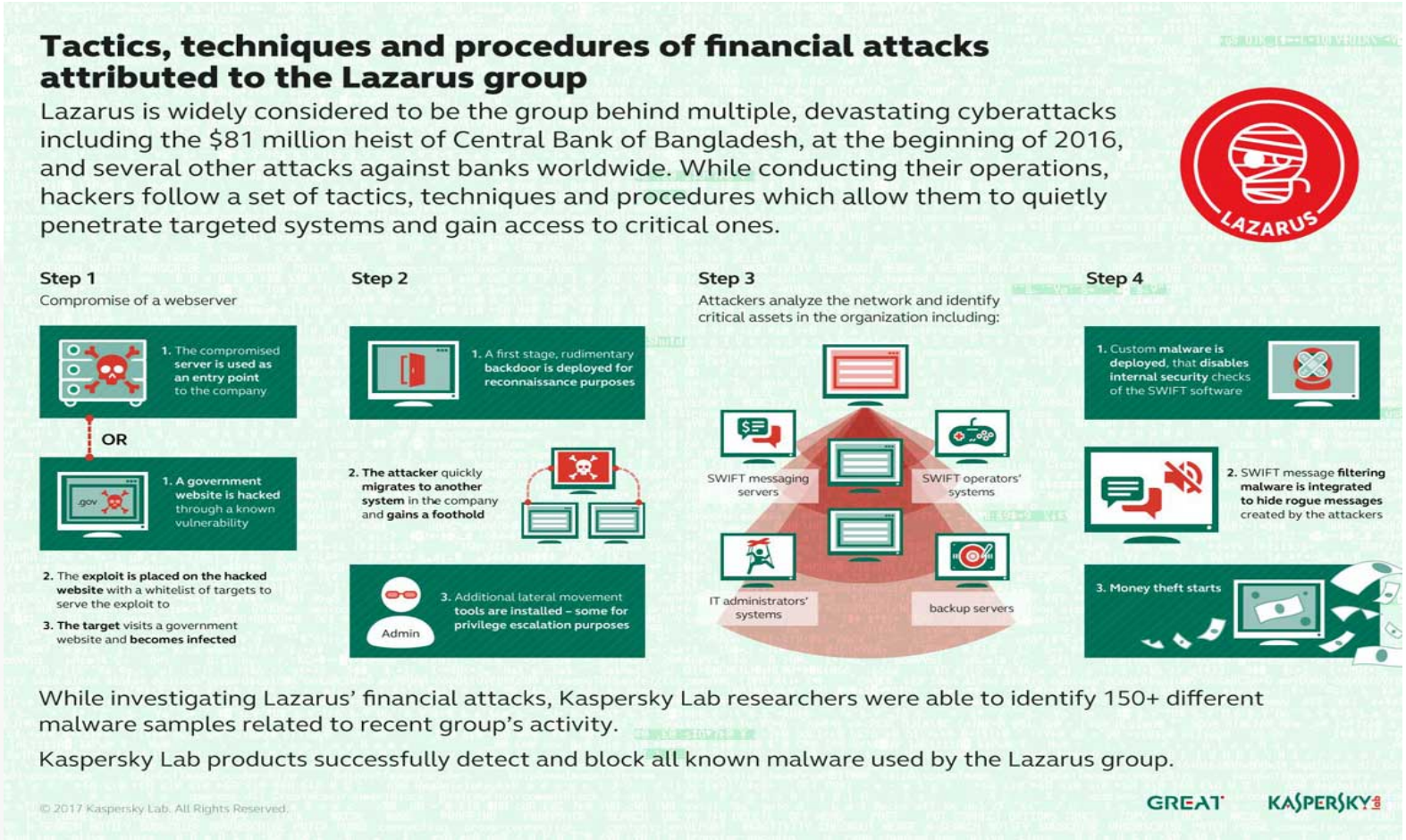


Au mois d'aout 2012, la réponse ?

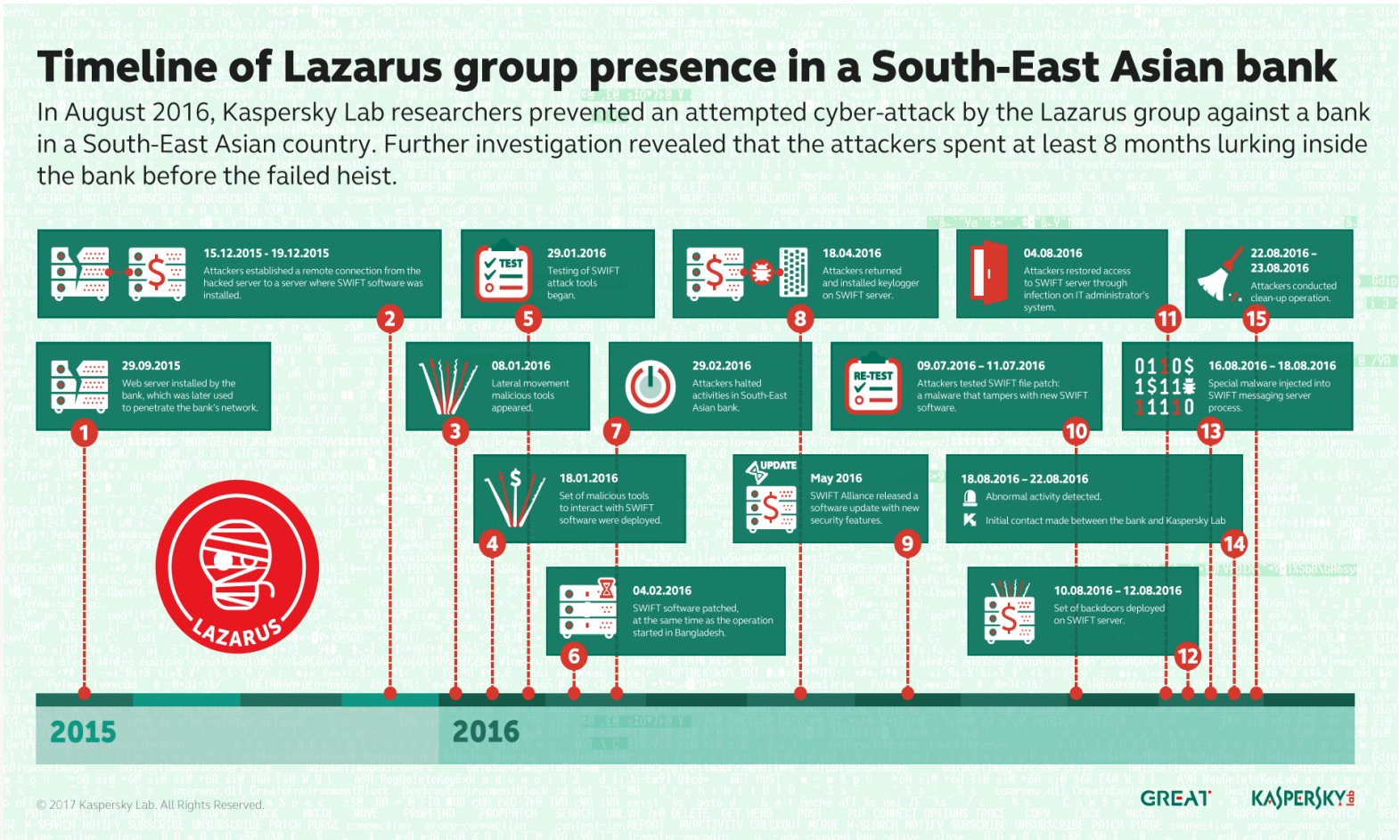
30 000 ordinateurs infectés.

Lazarus, vol à grande échelle

Lazarus : TTP

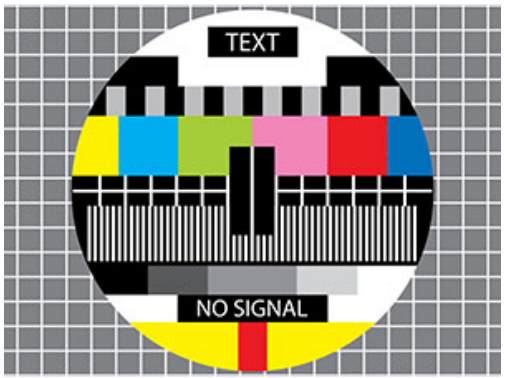

Tactics, techniques and procedures of financial attacks attributed to the Lazarus group
Lazarus is widely considered to be the group behind multiple, devastating cyberattacks including the $81 million heist of Central Bank of Bangladesh, at the beginning of 2016, and several other attacks against banks worldwide. While conducting their operations, hackers follow a set of tactics, techniques and procedures which allow them to quietly penetrate targeted systems and gain access to critical ones.
LAZARUS
Step 1
Compromise of a webserver
1. The compromised server is used as an entry point to the company
OR
1. A government website is hacked through a known vulnerability
2. The exploit is placed on the hacked website with a whitelist of targets to serve the exploit to
3. The target visits a government website and becomes infected
Step 2
1. A first stage, rudimentary backdoor is deployed for reconnaissance purposes
2. The attacker quickly migrates to another system in the company and gains a foothold
Admin
3. Additional lateral movement tools are installed – some for privilege escalation purposes
Step 3
Attackers analyze the network and identify critical assets in the organization including:
SWIFT messaging servers
SWIFT operators' systems
IT administrators' systems
backup servers
Step 4
1. Custom malware is deployed, that disables internal security checks of the SWIFT software
2. SWIFT message filtering malware is integrated to hide rogue messages created by the attackers
3. Money theft starts
While investigating Lazarus' financial attacks, Kaspersky Lab researchers were able to identify 150+ different malware samples related to recent group's activity.
Kaspersky Lab products successfully detect and block all known malware used by the Lazarus group.
© 2017 Kaspersky Lab. All Rights Reserved.
GREAT
KASPERSKY

Lazarus : Timeline



Une attaque terroriste ?

Entre le 8 et le 9 avril 2015, une cyberattaque visant TV5 Monde entraîne l'arrêt de la diffusion des programmes. Première du genre, l'attaque est revendiquée par le groupe *Cybercaliphate* et se réclame de l'Etat Islamique.



fiml ?


OUR
DEMOCRACY
HAS BEEN
HACKED
MR. ROBOT
6|24
usa

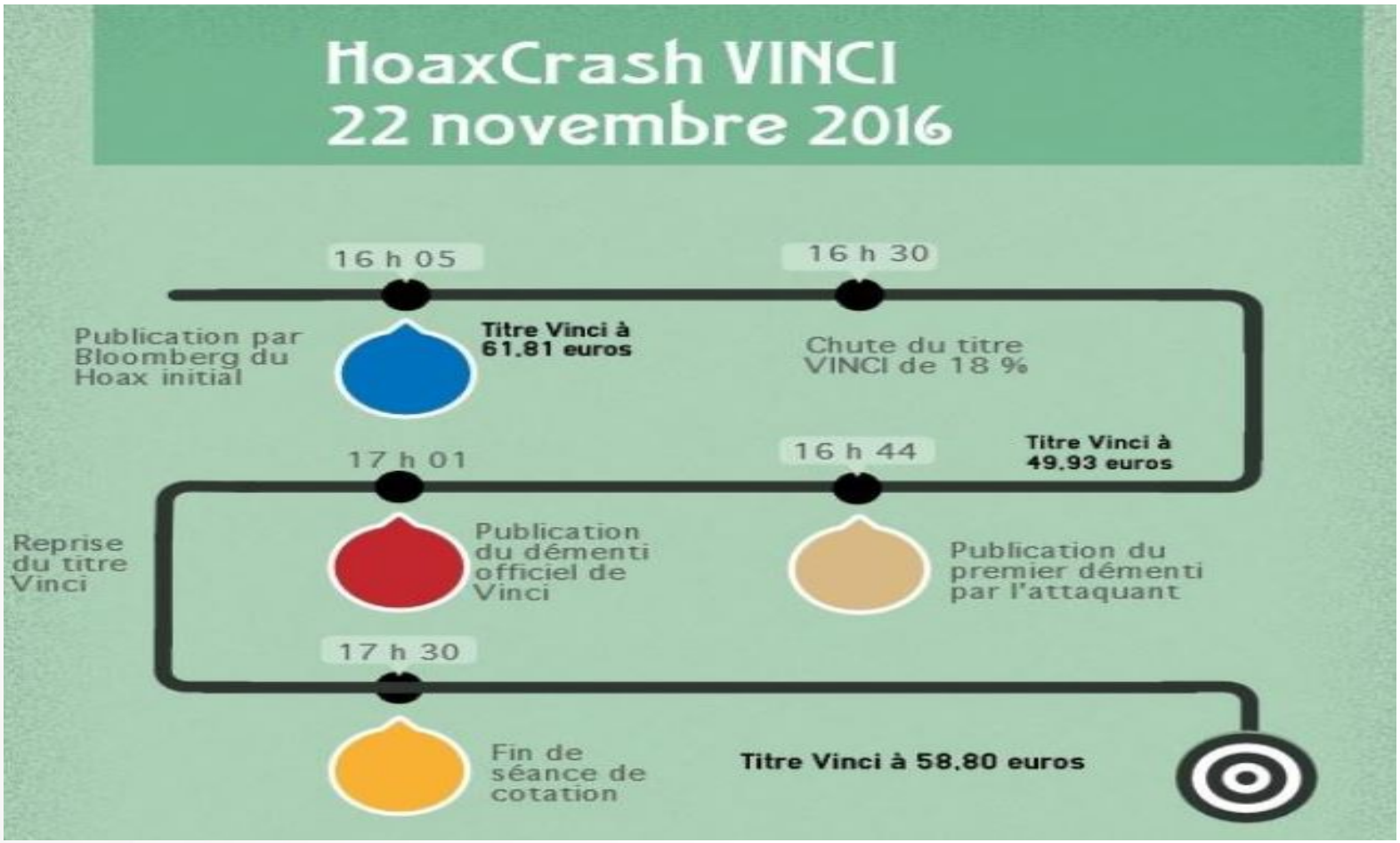
Propagande - Désinformation - Agitation

L'information un enjeu stratégique

- Une nouvelle tribune pour des groupes organisés (entreprises, associations, groupes politiques).
- Modification des formes politiques et des rapports hierarchiques dans la société.
- La libération de la parole: l'individu au centre du cyberespace.

L'attaquant ne cible pas directement le SI de la cible. La surface d'attaque ne se limite pas au périmètre "contrôlé" par le défenseur.

Attaque contre Vinci



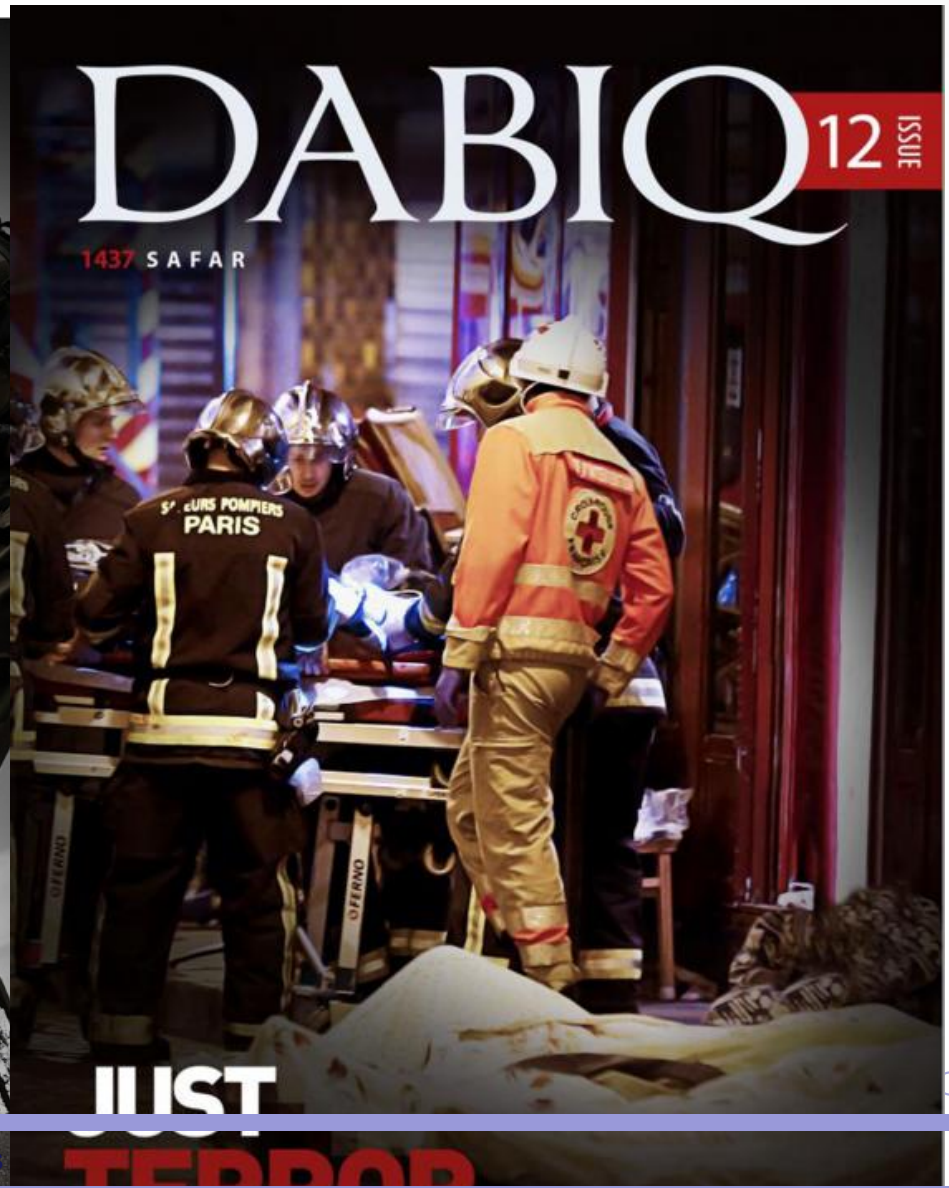

WE ARE ANONYMOUS.
WE ARE LEGION.
WE DO NOT FORGIVE.
WE DO NOT FORGET.
EXPECT US.

Le cas des "Cyber Army"

You are fake news

Agir contre la propagande ?


RABÎ' ATH-THÂNÎ 1436
DAR AL-ISLAM
NUMERO 2
QU'ALLAH عزوجل
MAUDISSE LA FRANCE


DABIQ
12 ISSUE
1437 SAFAR
PARIS
JUST
TERROR

Propagande - Désinformation - Agitation

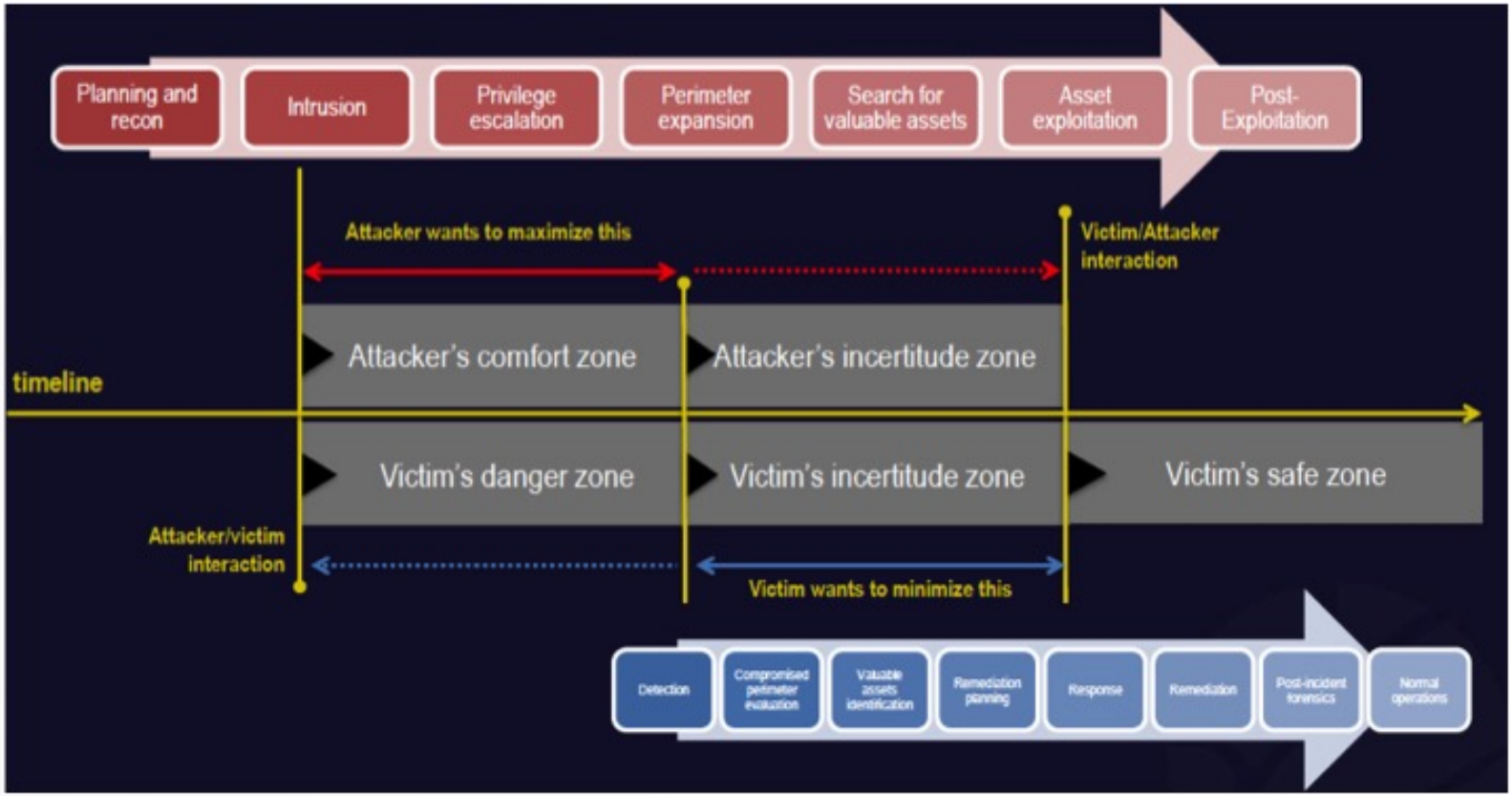
Les guerres de l'information

La "militarisation" de l'espace numérique

- Le cyberespace comme un "théâtre d'opération".
- L'organisation du commandement : USCybercom,etc.
- Hybridation avec le concept d'influence.

Les modèles défensifs

Défendre ou protéger ?



Les différents temps de la cyberdéfense

- Détection.
- Caractérisation.
- Attribution.
- Réponse.

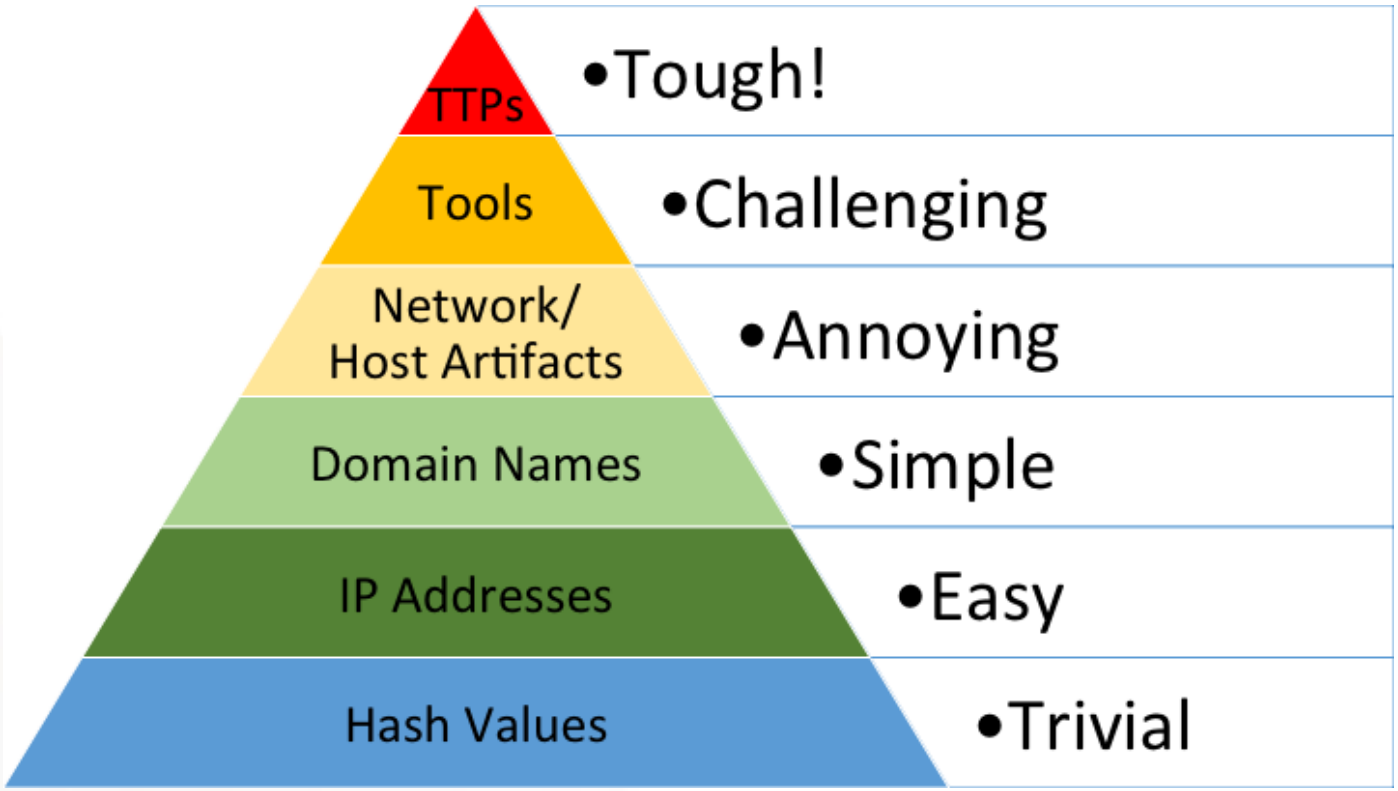
La **détection** est au centre du dispositif de cyberdéfense.

Comment répondre ?

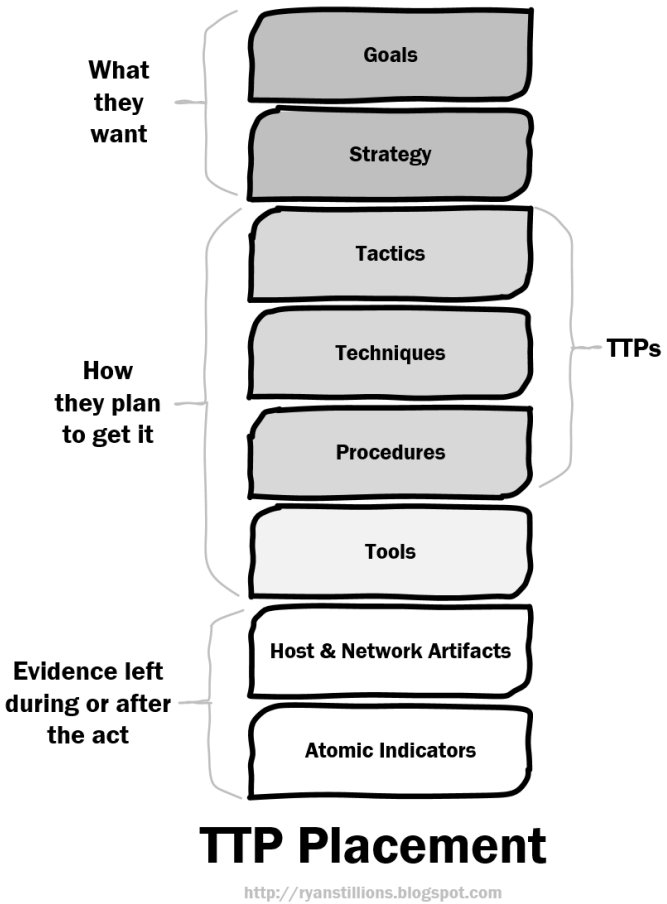
- Pénale.
- Politique/médiatique (rapports techniques).
- Technique.

The Pyramid of Pain

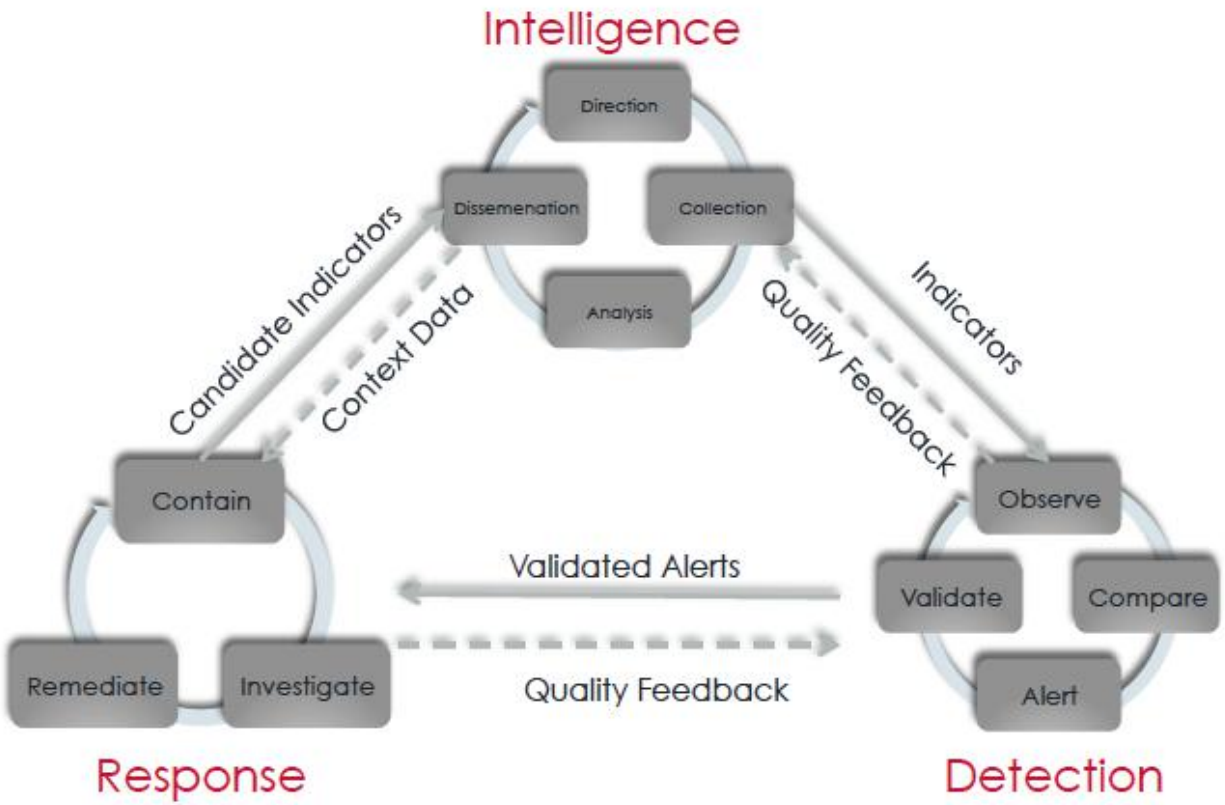
Comment le défenseur peut "faire mal" à l'attaquant ?



Les TTP ? Comprendre l'attaquant



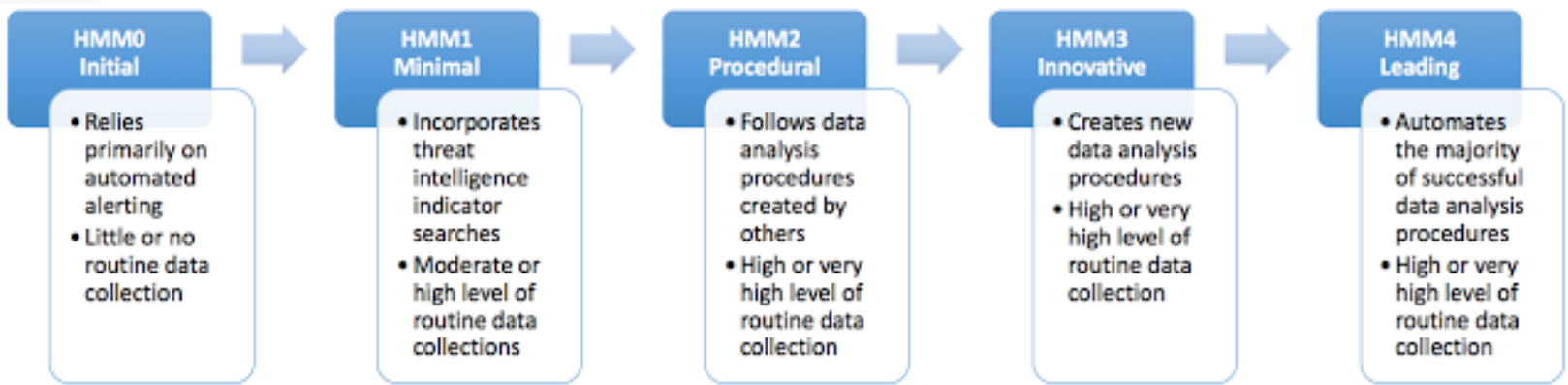
Le cycle de la défense



L' *Active Response* et *Hunting Team*

Des concepts qui dépendent du **niveau de maturité** de votre entreprise[2].

> *I usually define hunting as the collective name for any **manual** or **machine-assisted** techniques used to detect security incidents.*



[2] Voir David Bianco : http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html

Le *Hunting Maturuty Model*: Connais toi toi-même

- **HMM0** : L'organisation repose principalement sur des outils de détection automatiques (IDS, SIEM).
- **HMM1**: Collecte des données, fonde la dection sur le renseignement dont il dispose.
- **HMM2**: L'organisation est capable d'apprendre et d'appliquer des procédures externes et de les modifier à la marge.
- **HMM3**: Organisations qui produisent des procédures, disposent de compétences analytiques. Face aux menaces peuvent avoir un problème de "passage à l'échelle"
- **HMM4**: Capable d'automatiser la détection fondée sur les process qu'elle a développé.

Le combat numérique : une approche de la lutte contre les cybermenaces

Bertrand Boyer

2017