Documentation et analyse de la menace
ENSIBS, 2022-2023

Big Game Hunting

COVID-19, Ransomware et Organisations Criminelles

Ronan Mouchoux
Spécialiste en Analyse de la menace cyber

École d'ingénieurs
ensibs
Université Bretagne Sud

Présentation de l'intervenant

XRATOR
CONQUER YOUR RISK

- *Plateforme de gestion des risques*
- *Services:*
  - *Gestion des risques*
  - *Threat modeling*
  - *VAPT & Red Team*
  - *Conseil stratégique*

École d'ingénieurs ensibs : Université Bretagne Sud

Manager du module « Intelligence Cyber»

ESSEC BUSINESS SCHOOL

Manager externe du module « Security Strategy »

utt UNIVERSITÉ DE TECHNOLOGIE TROYES

Intervenant en analyse de la menace et criminologie numérique

RONINTEL
Cyber Threat Knowledge Management

2019-2021 TAL pour l'analyse de la menace

KASPERSKY lab

2017-2019 Analyse de la menace

SEKOIA

2015-2017 Analyse de la menace

AIRBUS DEFENCE & SPACE

2013-2015 Analyse de la menace

LA POSTE

2008-2013 Réseau & Sécurité

iut Saint Malo réseaux & télécoms

Réseau et Télécom (2008-2010)

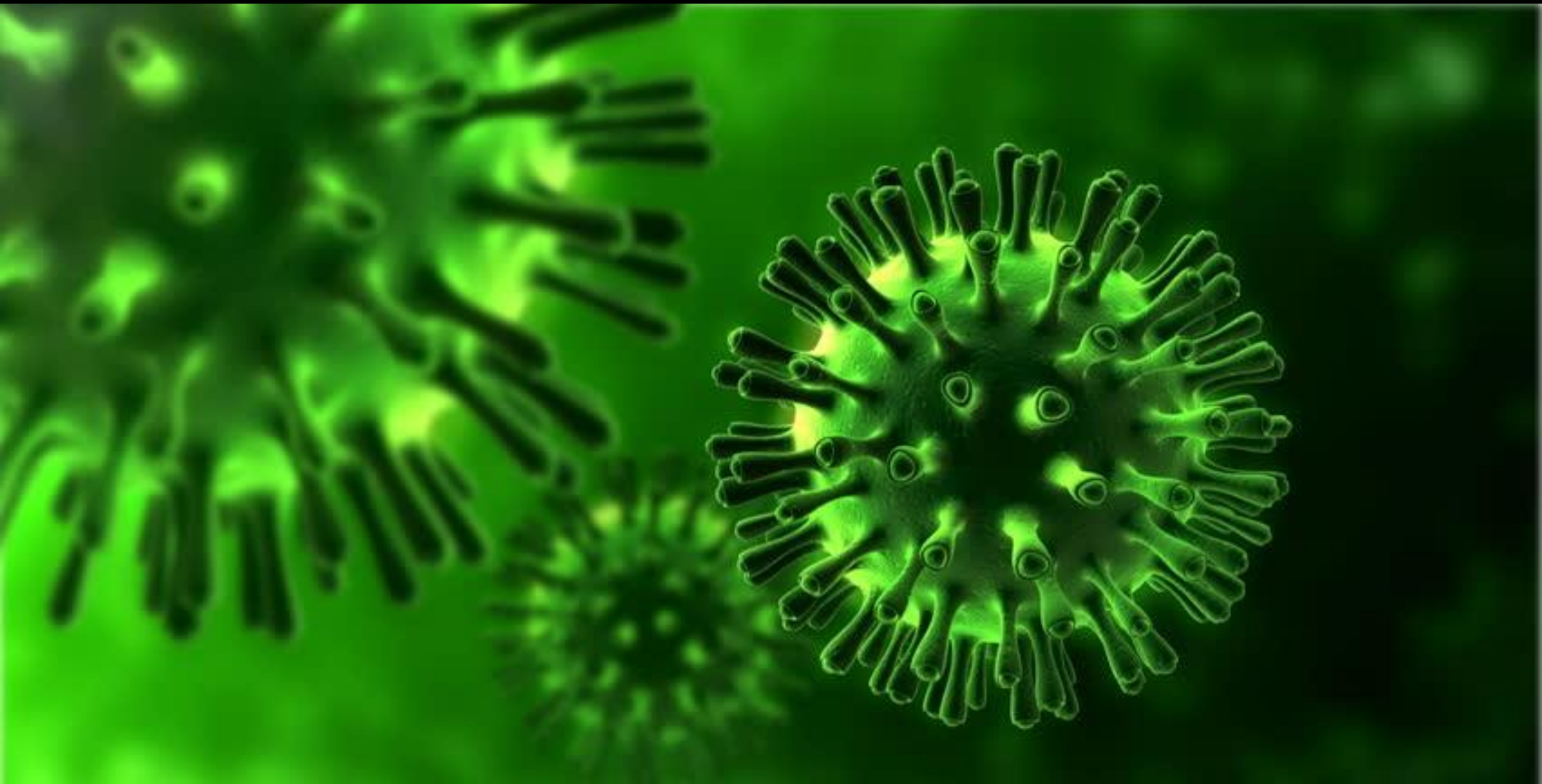
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Réseau et Télécom (2010-2013)

le cnam

Criminologie (2015-2016)

Virus, infection, patient-zéro, … un vocabulaire partagé



Une origine humaine

Un cycle de vie d'attaque biologique

Objectif stratégique

Arbitrage entre le but, la méthode et la gestion des risques

Définitions du ciblage

Infection ciblée ou massive
Infection direct ou indirecte
Infection bruyante ou furtive

Acquisition d'informations

Recherche sur les cibles et leurs moyen de contrer ou limiter l'impact de l'opération

Cahier des charges

Pathogénicité, virulence, incubation, létalité, transmissibilité, contre-mesures

Mise en production

Mise à l'échelle des ressources pour mener l'opération

Validation

Test de l'infection dans un environnement contrôlé

Vecteur de propagation

Méthode de diffusion aux cibles la plus adaptée pour atteinte les objectifs recherchés

Choix et mise en place des ressources

Infrastructure, personnel, agent, méthode de production

Militarisation

Combinaison de l'agent et d'un objet compatible avec le vecteur de propagation

Diffusion

Libération de l'objet chargé dans le médium de propagation

Supervision et réaction

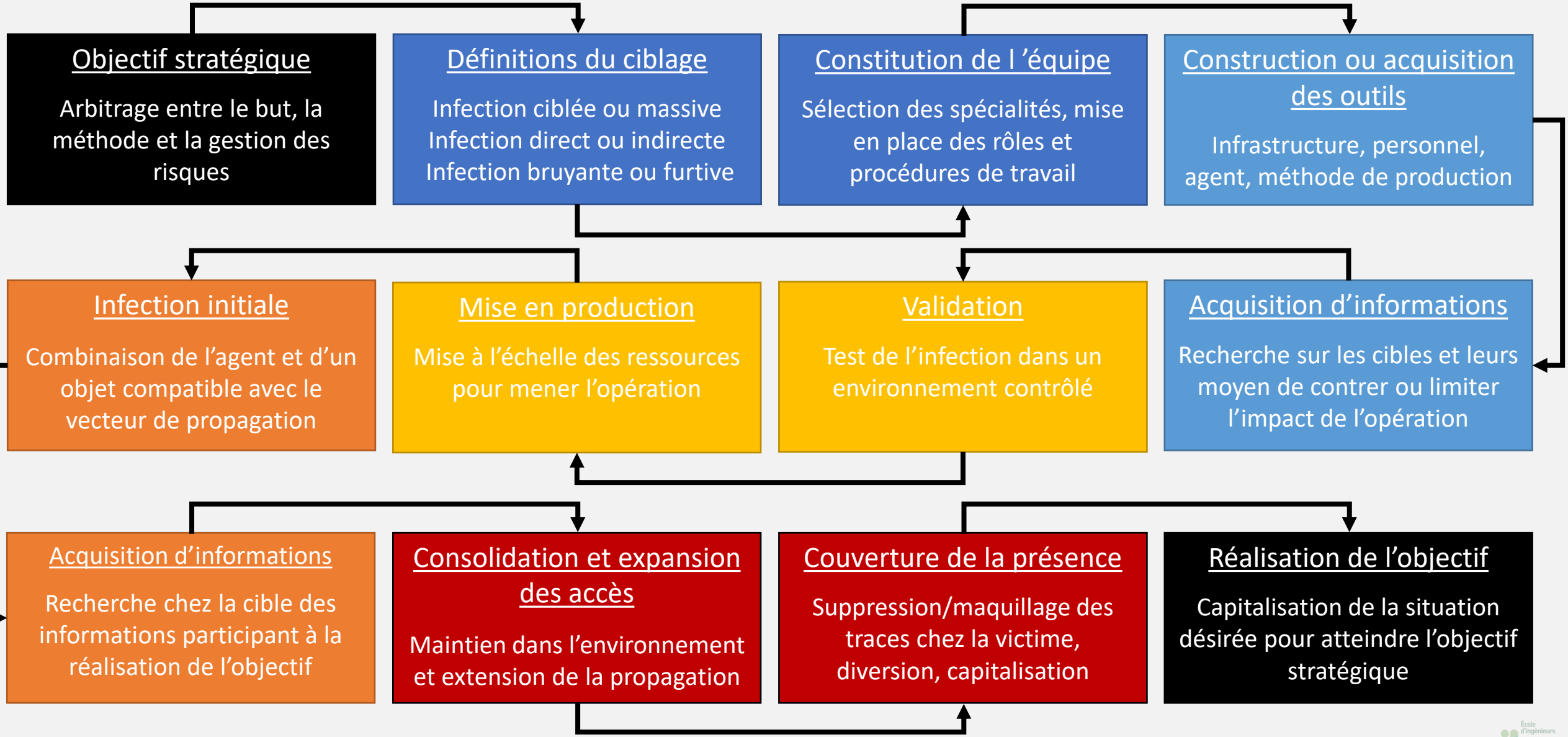
Surveillance de la propagation et éventuelle réaction en cas de contre-mesure

Réalisation de l'objectif

Capitalisation de la situation désirée pour atteindre l'objectif stratégique

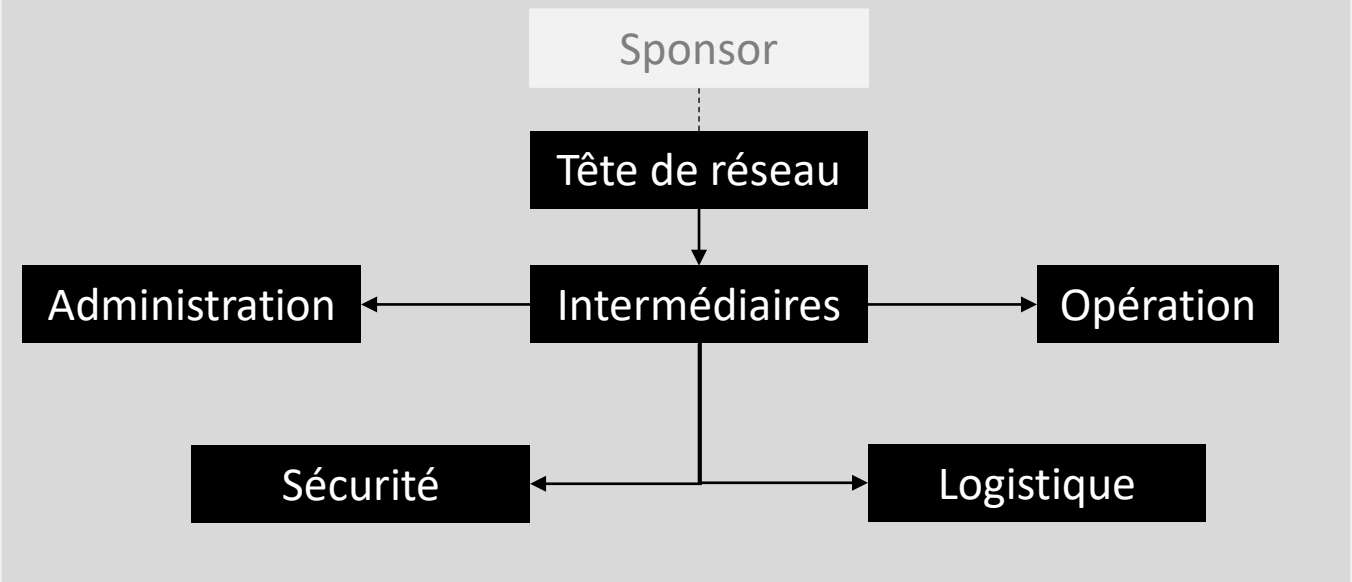
Inspiré de https://www.nti.org/newsroom/news/new-nti-tutorials-edcuate-biological-weapons-and-nuclear-testing/

Un cycle de vie d'attaque informatique



Inspiré de https://en.wikipedia.org/wiki/Advanced_persistent_threat#/media/File:Advanced_persistent_threat_lifecycle.jpg/

Structure abstraite d'un groupe criminel organisé



Pour plus d'informations : https://www.europol.europa.eu/socta/2017/defining-serious-and-organised-crime.html

Affaire Colonial Pipeline : une illustration du modèle d'affaire

7 mai 2021

About the latest news. 10.05.2021

We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined goverment and look for other our motives.
Our goal is to make money, and not creating problems for society.
From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future.

Développeur

BLACK MARKET

Accès initial au réseau

(« Partenaire »)
Expansion des accès

(« Opérateur »)
Localisation, Chiffrement, Négociation des données

Echec rançon

Accès
Données

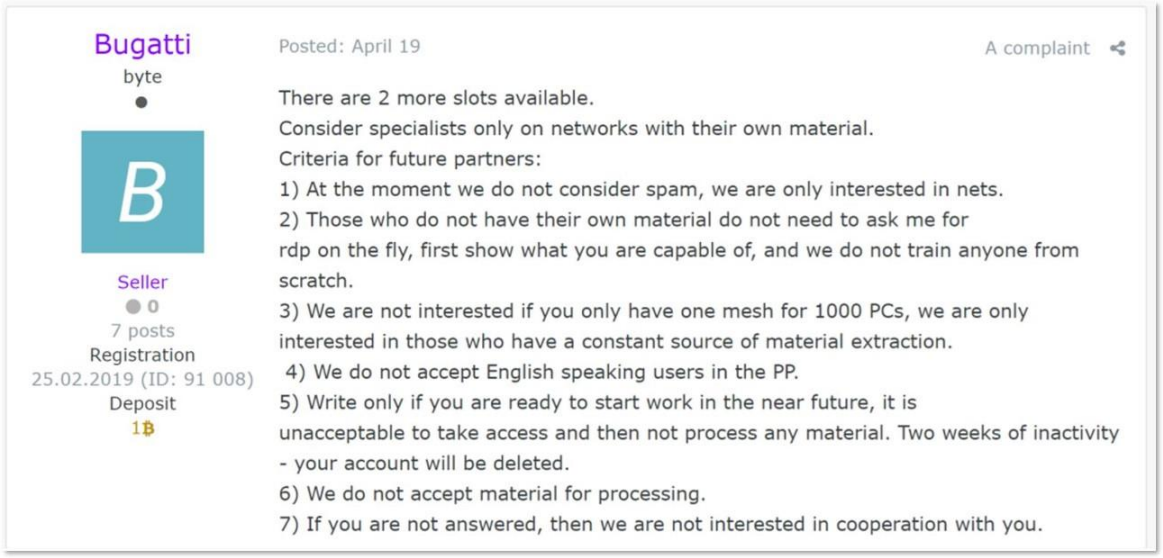
Rançon
Accès
Données

Succès rançon

Blanchiment

Plus d'informations sur les rançongiciels : *https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf*

Un écosystème spécialisé



Bugatti
byte
B
Seller
0
7 posts
Registration
25.02.2019 (ID: 91 008)
Deposit
1฿

Posted: April 19 — A complaint

There are 2 more slots available.
Consider specialists only on networks with their own material.
Criteria for future partners:
1) At the moment we do not consider spam, we are only interested in nets.
2) Those who do not have their own material do not need to ask me for rdp on the fly, first show what you are capable of, and we do not train anyone from scratch.
3) We are not interested if you only have one mesh for 1000 PCs, we are only interested in those who have a constant source of material extraction.
4) We do not accept English speaking users in the PP.
5) Write only if you are ready to start work in the near future, it is unacceptable to take access and then not process any material. Two weeks of inactivity - your account will be deleted.
6) We do not accept material for processing.
7) If you are not answered, then we are not interested in cooperation with you.

Annonce de recrutement

drumrlu
килобайт
Платная регистрация
1

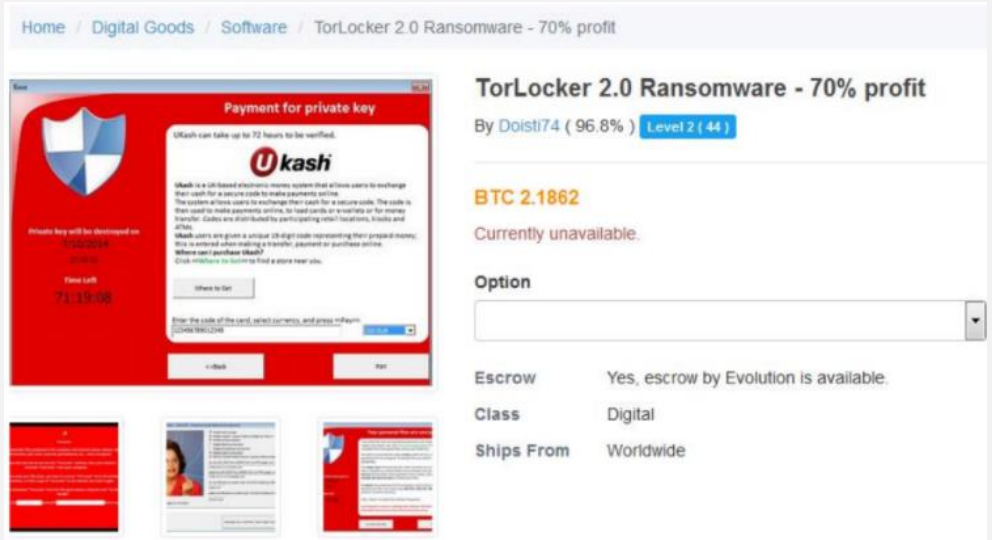
Опубликовано: 6 июля — Жалоба

Electric Power Company - Amman, Jordan - Employees:8,150 Revenue: $719 Million (Domain Admin+NTDS+Full internall netwrok info) Price: 3200$

German Hospitals - Saudi Arabia - Employees: 7,400 Revenue: $1 Billion (Domain Admin+NTDS+Full internall netwrok info) Price: 3500$

Insurance - Thailand - Employees: 520 Revenue: $131 Million (Domain Admin+NTDS+Full internall netwrok info) Price: 1000$

Vente d'accès pirate à des réseaux avec analyse financière



Home / Digital Goods / Software / TorLocker 2.0 Ransomware - 70% profit

Payment for private key
Ukash

TorLocker 2.0 Ransomware - 70% profit
By Doisti74 (96.8%) Level 2 (44)
BTC 2.1862
Currently unavailable.
Option
Escrow — Yes, escrow by Evolution is available.
Class — Digital
Ships From — Worldwide

Vente de logiciel malveillant

CRÉATION DE FAKE DOCUMENTS

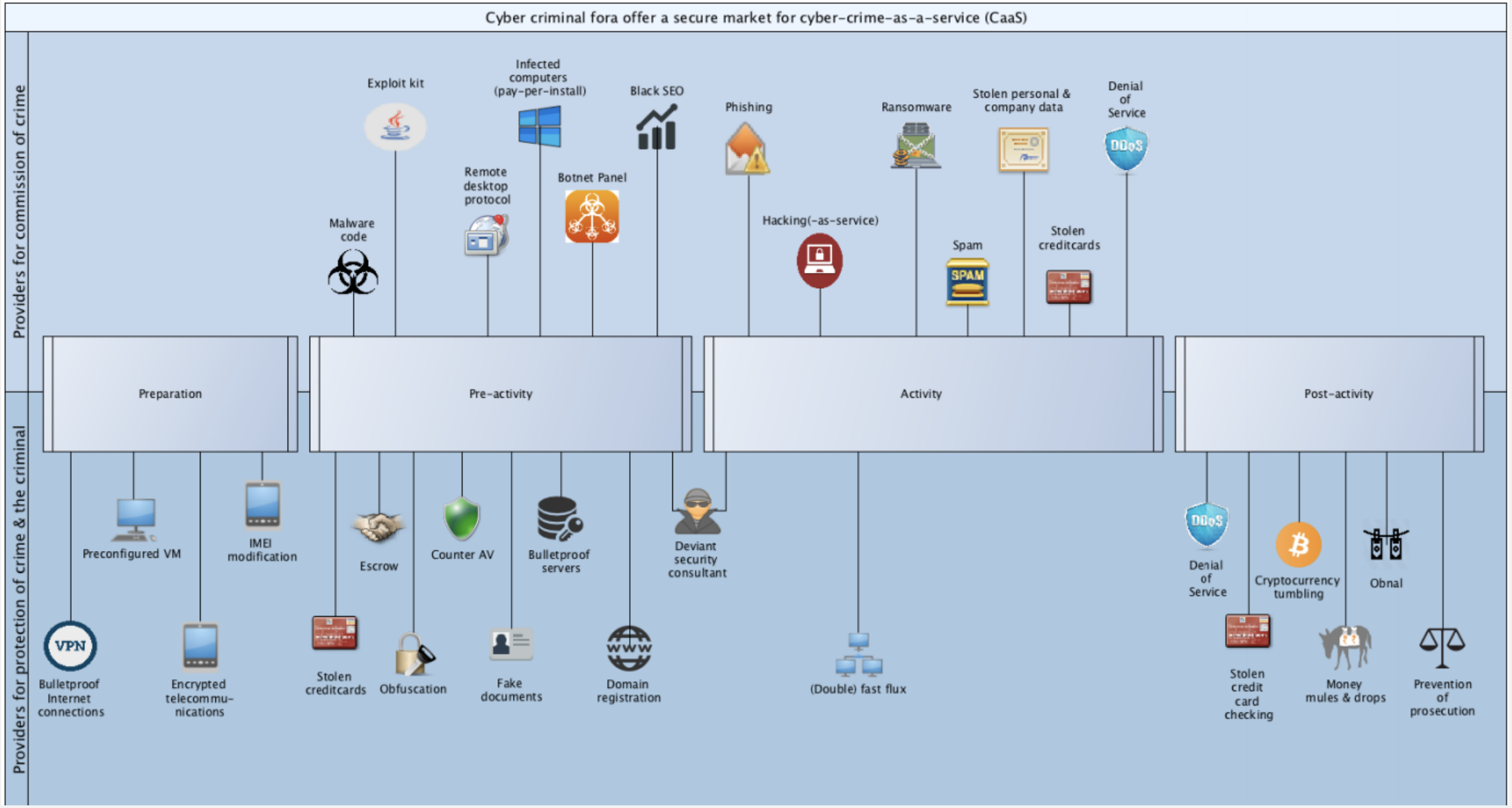
CRÉATIONS DE FAUX DOCUMENTS :

- CARTE NATIONAL D'IDENTITÉ (SCANS 15€ + PHYSIQUE 400€)
- FAUX DERMIS DE CONDUIRE (SCANS 15€)
- JUSTIFICATIF DE DOMICILE (SCANS 15€ + PHYSIQUE 50€)
- FAUX PAPIERS (PM SUR CEUX QUE VOUS VOULEZ ~ PRIX À NÉGOCIER)

Service de fraude documentaire

Pour plus d'information : *https://www.trendmicro.com/vinfo/us/security/news/cybercriminal-underground-economy-series*

(Cyber) Crime as a Service



https://researchinformation.bris.ac.uk/ws/portalfiles/portal/194364696/DEVIANT_SECURITY_EHAVANDESANDT.pdf

Les facteurs COVID

Opportunité psychologique

La peur est un levier de manipulation efficace pour engendrer un comportement.

Le seuil général de tolérance au risque est augmenté, relativisant les menaces antérieures.

Les méthodes et technologies utilisées par les pirates restent stables.

Télétravail et Télécole

Extension subite et souvent improvisée des accès des organisations depuis l'extérieur.

Mélange des habitudes personnels et professionnels avec parfois du désœuvrement.

Soif d'information

Les états, organisation et individus sont dans un flou informationnel accroissant le besoin en acquisition d'information.

Les facteurs Hôpitaux Publiques

Le patient avant le PC

La mission de l'hôpital est tournée vers le soin de patients. L'urgence de situations critiques s'accommode mal avec certaines mesures de sécurités.

Il n'y a pas de sanctuaire en cyberguerre.

Double levier

L'hôpital doit assurer à la fois la disponibilité du système de soin et la confidentialité des informations du patient. C'est un double levier pour le succès d'un rançonnage.

Triple récompense

Les hôpitaux sont à la fois des mannes de données sur une situation sanitaire locale et sur l'état de la recherche médicale. C'est de plus une cible intéressante pour le rançonnage.

Les acteurs COVID

Pirate criminel

Monétisation direct

Vulnérabilité psychologique

Perte d'emploi et désœuvrement

Pirate institutionnel

Besoin en information stratégique

Perturbation de concurrents

Course au vaccin

Les avantages du rançongiciel

Monétisation directe

L'opération criminelle résulte sur une demande de rançon qu'il ne reste plus qu'à blanchir.

Cela réduit les étapes de transformations du résultat du crime en argent.

Un écosystème ergonomique

Les opérations de rançonnage peuvent s'appuyer sur une base industrielle criminelle compétente et expérimentée fournissant des services clés en main.

C'est la rencontre des vendeurs de pioches et des chercheurs d'or.

Sur fond de la démocratisation des législations sanctionnant les fuites de données personnelles (RGPD, PDPA, …)

Hausse cyclique des cryptomonnaies

Bitcoin (BTC) et Monero (XMR) sont devenues les deux principales valeurs utilisées pour la rançon. La période 2020-2021 était anticipée comme haussière pour leur conversion en monnaie fiduciaire.

Poly-monétisation

L'implantation et l'activation d'un rançongiciel, comment finalité ou moyen de couverture, requière une opération générant de nombreux produits pouvant être revendu en plus de la rançon (accès, documents, …)

La criminalité est un reflet de la société

Q1 2020

- ***Phase*** : Alerte
- ***Réaction*** : Confinement
- ***Cible*** : Entreprise

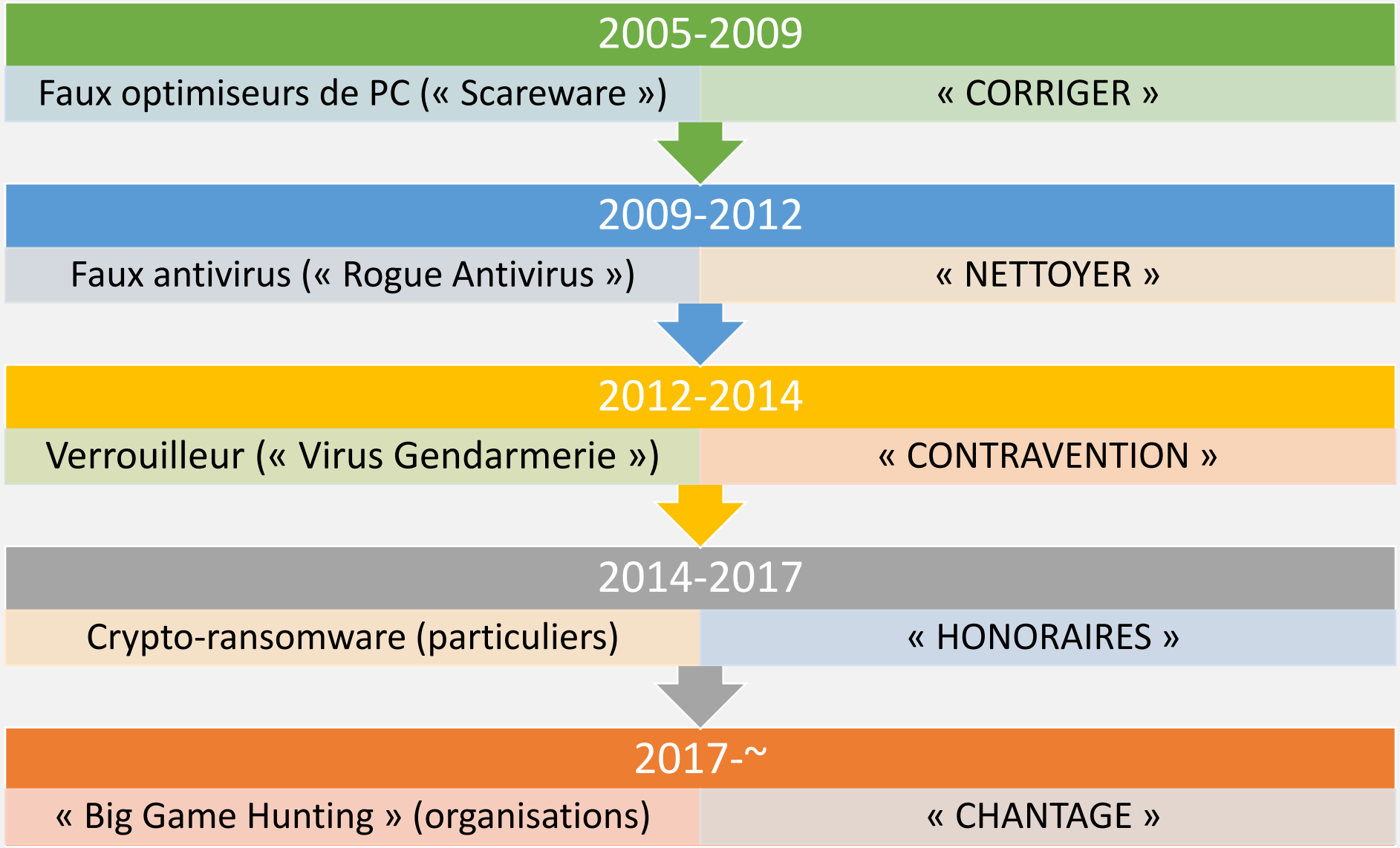
Q2-3 2020

- ***Phase*** : Accélération
- ***Réaction*** : Course au vaccin
- ***Cible*** : Laboratoire

Q4 2020

- ***Phase*** : Aggravation
- ***Réaction*** : Urgence sanitaire
- ***Cible*** : Hôpitaux

Les attaques ne disparaitront pas avec le COVID



Inspiré de Anatomy of a ransomware attack, Symantec, 2015


École
d'ingénieurs
ensibs :
Université Bretagne Sud