L'INVITÉ DU CLUSIF

RONAN MOUCHOUX (XRATOR)

Introduction

Michaël JACQUES

Comité de programme du Clusif

OSINT ET CYBERSÉCURITÉ

MAITRISER SON EXPOSITION NUMÉRIQUE POUR APPUYER LES DÉCISIONS DE PROTECTION

Ronan Mouchoux – Spécialiste en analyse de la menace - XRATOR

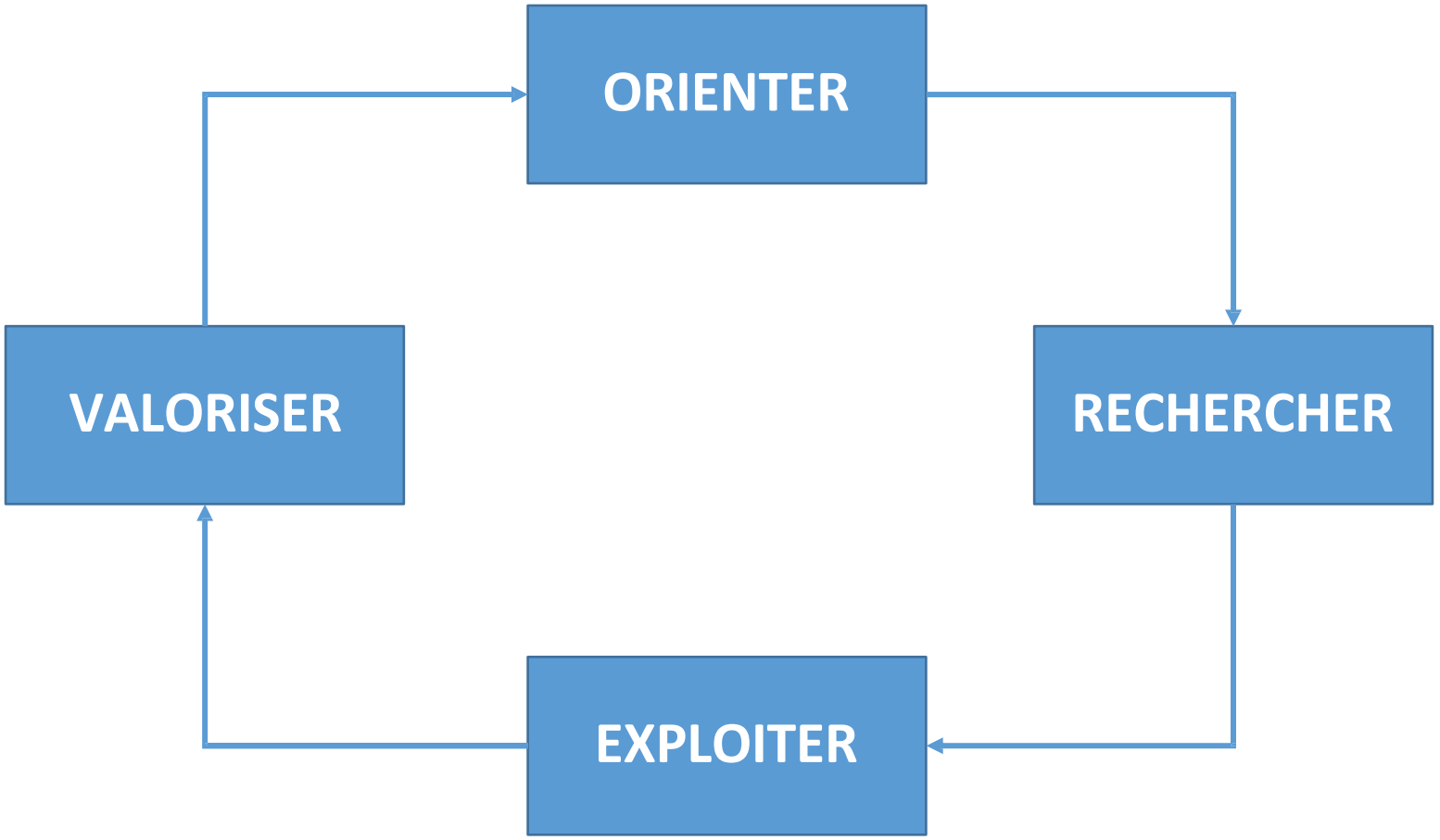
Le cyber des années 20

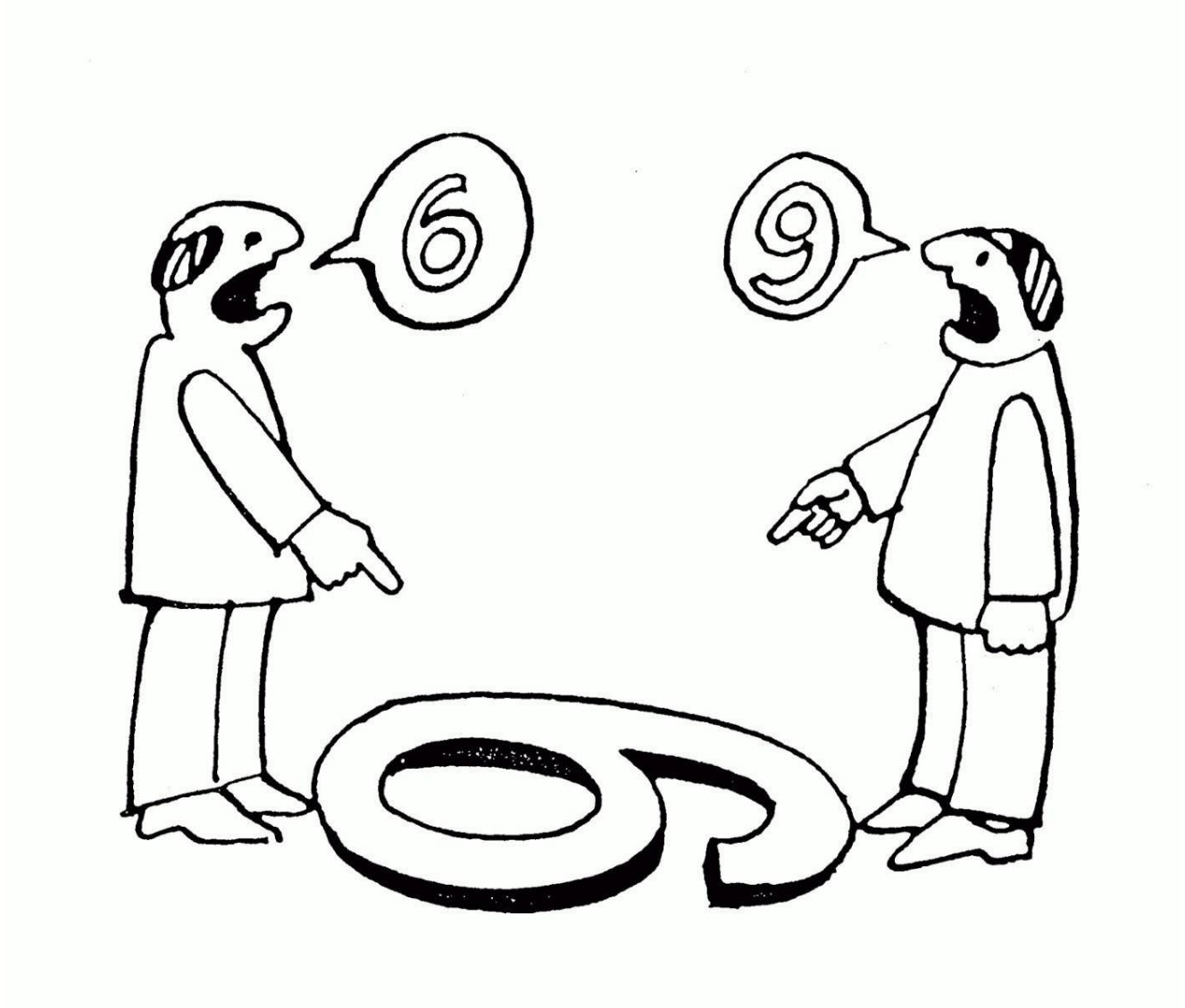
Un vecteur de rééquilibrage des relations asymétriques du monde physique

ENISA Threat Landscape 2022

Attaquer et défendre sont des projets

… qui commencent par une collecte des informations nécessaires à l'atteinte des objectifs




6
9

OSINT

La capacité à créer de la valeur à partir d'informations disponibles à tout le monde.

Ronan Mouchoux – Spécialiste en analyse de la menace - XRATOR

VALEUR

Décision à prendre

COÛT

Moyen mobilisé

Attaquant et reconnaissance

Collecte active et passive d'informations sur les technologies, les personnes et l'organization pour préparer une attaque

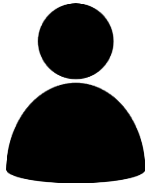
Reconnaissance
10 techniques

Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (3)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (3)
Search Victim-Owned Websites

Source : https://attack.mitre.org/matrices/enterprise/pre/

ACTIF

Contact direct avec la cible



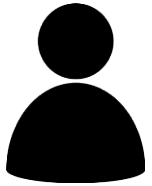
Echanger avec une personne sur Linkedin

Scanner les ports d'une IP publique

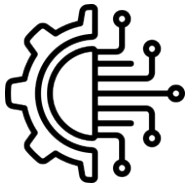
Visiter le site vitrine d'une organisation

PASSIF

Contact indirect avec la cible



Visiter le profil public d'une personne sur Linkedin



Rechercher sur Onyphe une IP publique

Consulter le registre du commerce

Nous devons nous faire

Tout ce que l'attaquant peut nous faire.

MITRE ID	Technique	CIS Safeguard (example)
T1595	Active Scanning	• Inventory and Control of Enterprise Assets Continuous Vulnerability Management
T1592	Gather Victim Host Information	• Secure Configuration of Enterprise Assets and Software • Email and Web Browser Protections
T1589	Gather Victim Identity Information	• Security Awareness and Skills Training • Account Management
T1590	Gather Victim Network Configuration	• Network Infrastructure Management • Network Monitoring and Defense
T1591	Gather Victim Org Information	• Security Awareness and Skills Training • Data Protection
T1596	Search Open Technical Database	X
T1593	Search Open Websites/Domains	X
T1594	Search Victim-Owned Websites	• Security Awareness and Skills Training • Data Protection

DE L'OSINT

La capacité à créer de la valeur à partir d'informations disponibles à tout le monde.

A L'OPSEC

La capacité à réussir ses opérations même en divulguant des informations critiques à l'adversaire.

XRATOR CONQUER YOUR RISK

Ronan Mouchoux – Spécialiste en analyse de la menace - XRATOR

CLUSIF #ConfClusif

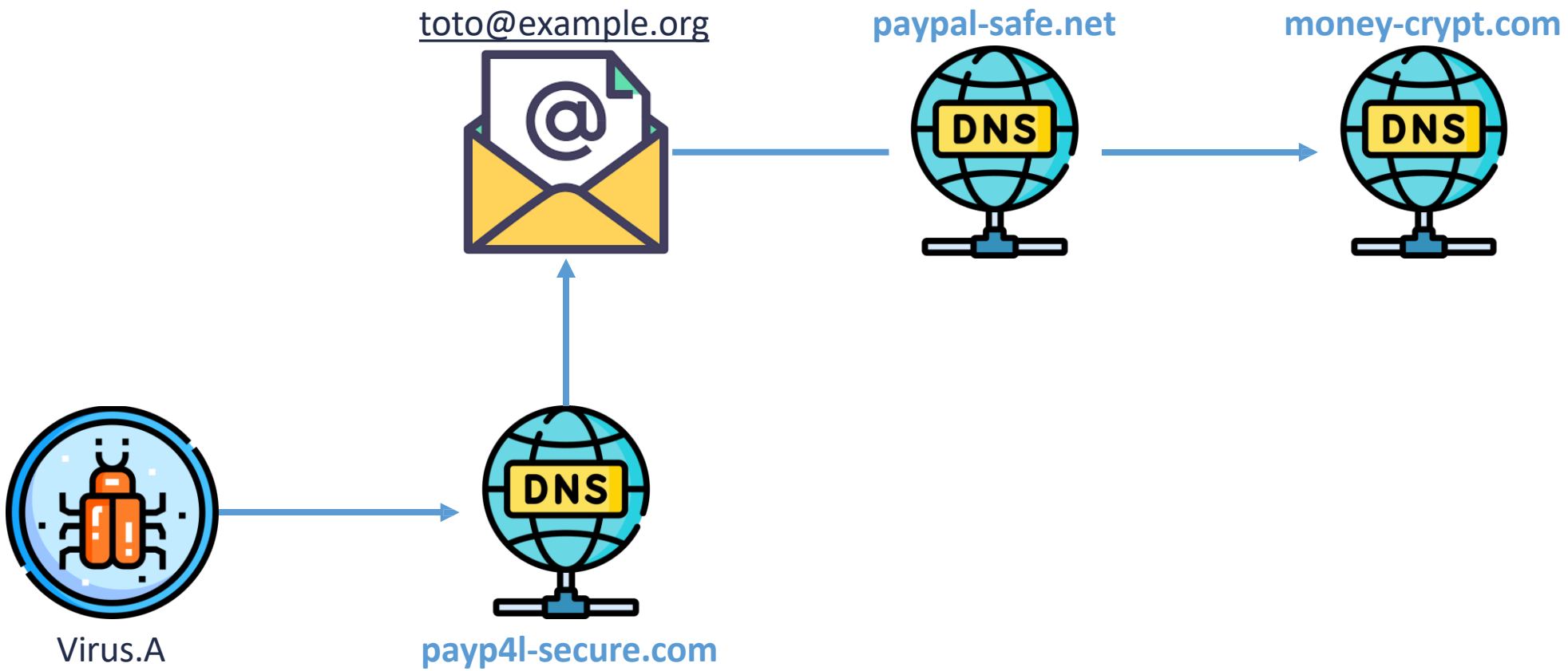
Nous devons nous renseigner sur l’adversaire

Tout autant qu’il se renseigne sur nous *.

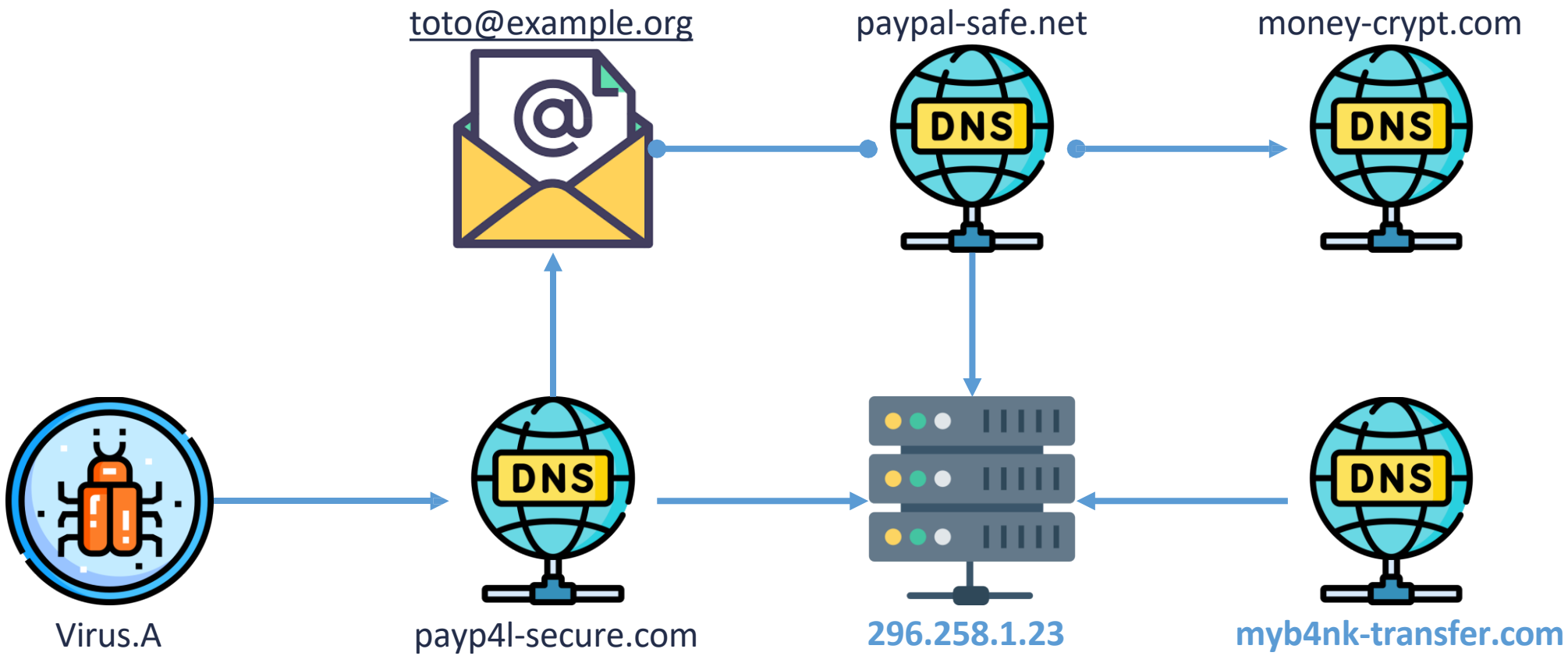
** Dans les limites du cadre légal*

1	**Ma sandbox détecte un maliciel.**	L'analyse comportemental indique qu'il communique avec un nom de domaine.	payp4l-secure.com
2	**Je réalise une recherche WHOIS.**	Le nom de domaine est enregistré avec un email non anonymisé.	toto@example.org
3	**J'inverse la recherche WHOIS.**	L'email a servi à enregistré deux autres noms de domaines.	paypal-safe.net money-crypt.com
4	**Analyse et valorisation**	Les trois domaines semblent suspicieux. Je vérifie qu'ils sont bloqué dans mon parc.	payp4l-secure.com paypal-safe.net money-crypt.com

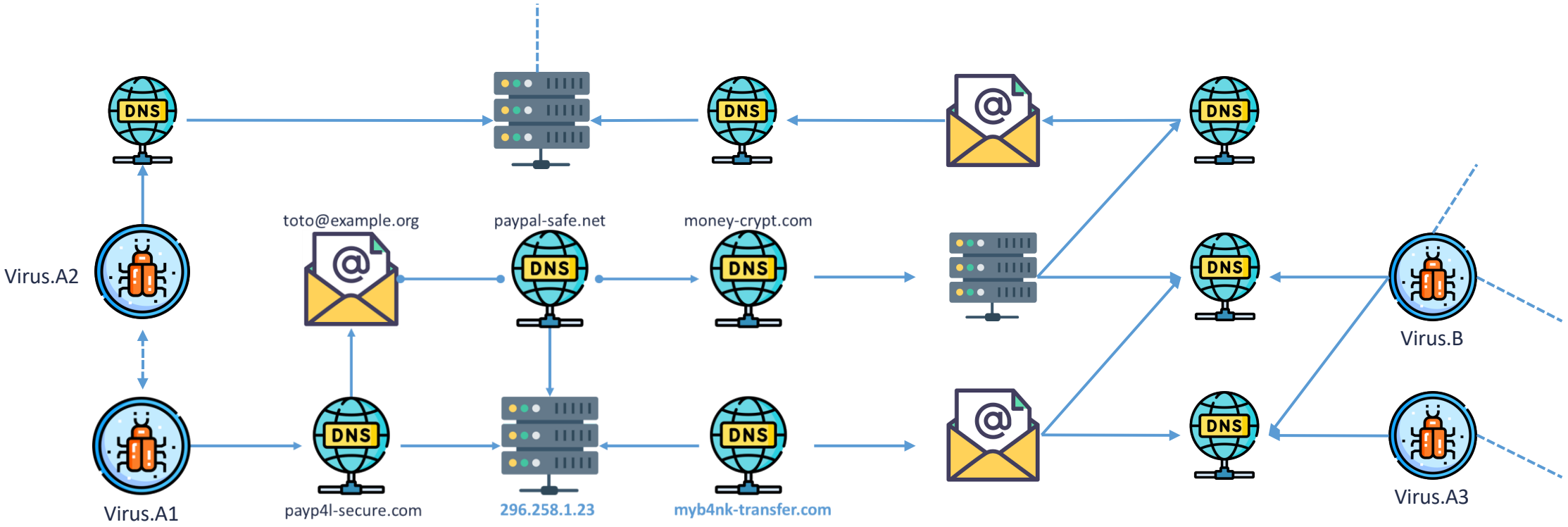
Exemple d'OSINT d'une infrastructure malveillante (WHOIS)



Exemple d'OSINT d'une infrastructure malveillante (DNS)

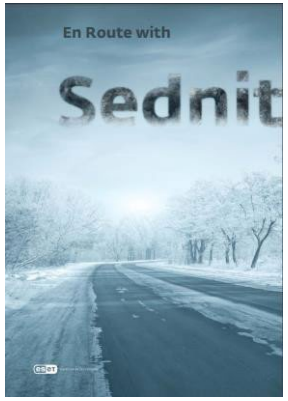


Exemple d'OSINT d'une infrastructure malveillante (etc…)



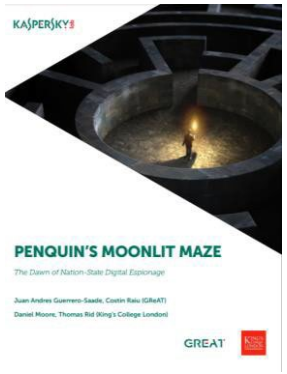
Contexte et mode opératoire

https://www.cert.ssi.gouv.fr/cti/



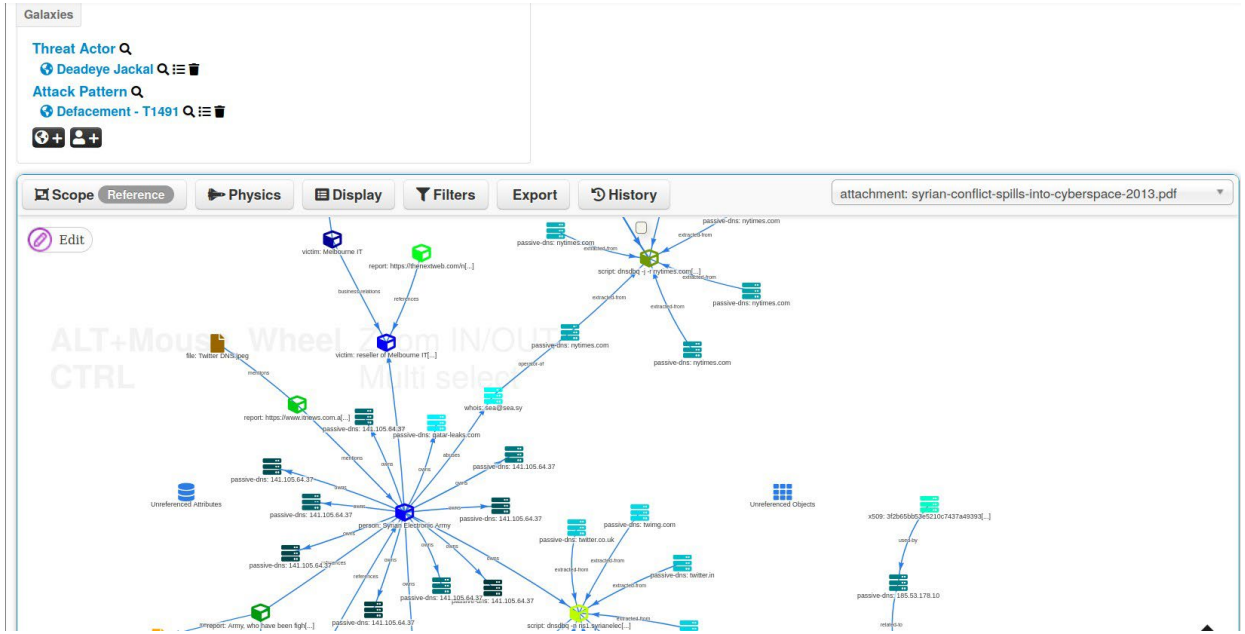
https://www.welivesecurity.com/

https://www.mandiant.com/resources/blog



https://securelist.com/

Infrastructure et outillage adverse



https://www.misp-project.org/

A VOS QUESTIONS !

Ronan MOUCHOUX (XRATOR) – Michaël JACQUES (Clusif)

Rendez-vous le 26 janvier prochain pour Panocrim !