Lutte Informatique Défensive

SOC, CERT et CTI

Georges Bossert - SEKOIA
Frédéric Guihéry - AMOSSYS

8 janvier 2019 - Université Rennes 1

SEKOIA

AMOSSYS
EXPERT IN CYBERSECURITY

Comprendre la menace

Questions : quelles peuvent être les motivations d'un attaquant ?

Comprendre les motivations de l'attaquant

LUCRATIVE
Cybergangs
Cybermercenaires
Officines

POLITIQUE
Hacktivistes
Cyberpatriotes
Cyberterroristes

MILITAIRE
Unités spécialisées

LUDIQUE
Adolescent désoeuvré

TECHNIQUE
Hacker

PATHOS
Employé mécontent

Catégorisation des attaques

- Campagnes **non-ciblées**
  - Distribution massive d'un malware
  - Souvent peu évolué et peu discret
  - Objectif : toucher le plus de cibles
  - Stealer, banker, ransomware, etc.
- Campagnes **ciblées** (APT)
  - Attaque ciblée et complexe
  - Souvent très évoluée, furtive et impactante
  - Complexe à détecter et analyser
  - Objectif : rester le plus longtemps possible sur le réseau de la cible
  - Vol d'informations, compromission d'infrastructures critiques, etc.

Attaques ciblées

- **APT** : Advanced Persistent Threat, ou « Menace avancée et persistante »
  - En pratique, attaque ciblée, persistante, mais pas toujours avancée
- Attaquant structuré
  - En équipe
  - Moyens techniques et financiers importants
  - Plus ou moins discret
  - Plus ou moins efficace
- Objectifs
  - Vol d'informations
  - Destruction
  - Renseignement/espionnage

Sources d'informations sur les attaques ciblées

- Groupes d'attaquants et campagnes d'attaques
  - https://www.fireeye.fr/current-threats/apt-groups.html
  - http://cybercampaigns.net
  - https://apt.securelist.com (Kaspersky)
  - https://www.crowdstrike.com
  - APT Groups and Operations / Florian Roth et al.
    - https://airtable.com/shr3Po3DsZUQZY4we/tbljpA5wI1IaLI4Gv/viwGFVFtuu0l88e7u
- Rapports d'analyse de malware et production d'indicateurs
  - ESET
  - Kaspersky
  - Mandiant / FireEye
  - ...

La connaissance des groupes d’attaquants

Nommage des groupes d'attaquant

Country / Selector	FireEye / Mandiant	Crowdstrike	Kaspersky
Generic	APT [X]		
China		[X] Panda	[X] Dragon*
Russia		[X] Bear	[X] Duke*
North Korea		[X] Chollima	
Iran		[X] Kitten	
India		[X] Tiger	
Vietnam		[X] Buffalo	
Lebanon			
Arab Countries			[X] Falcon
Criminals / Financial	FIN[X]	[X] Spider	
Activists		[X] Jackal	
Espionage		[X] Bat	
Temporary	TEMP.[X]		
Uncategorized	UNC[X]		

Groupes d'attaquants chinois

China										
Common Name	CrowdStrike	IRL	Kaspersky	Dell Secure Wo	Mandiant	Operation 1	Operation 2	Operation 3	Toolset / Malware	Targets
Comment Crew	Comment Pand	PLA Unit 61398		TG-8223	APT 1	Shady RAT			WEBC2, BISCUIT and many others	Mainly EN speaking countries; IT/Softw
APT 2	Putter Panda	PLA Unit 61486		TG-6952	APT 2				MSUpdater	
UPS	Gothic Panda			TG-0110	APT 3	Clandestine Fox	Double Tap	Clandestine Wolf	Pirpi, PlugX, Kaba, Cookie Cutter, many 0day	Aerospace and Defence; Construction a
IXESHE	Numbered Panda			TG-2754 (tentat	APT 12	NYT Oct 2012			Etumbot, Riptide, Hightide, ThreeByte, Waterspout, Mswab, Gh0st, ShowNews, 3001	
APT 16					APT 16				ELMER backdoor	Taiwanese Media and Entertainment
Hidden Lynx	Aurora Panda				APT 17	Operation Ephemeral Hydra			BLACKCOFFEE, WEBCnC, Joy RAT, PlugX, Tr	Government, defense & aerospace, indu
Wekby	Dynamite Pand	PLA Navy		TG-0416	APT 18				HTTPBrowser, TokenControl, HcdLoader, Pis	Aerospace and Defence; Construction a
Axiom	Deep Panda		Winnti Group		APT 19	Operation SMN			Winnti, Gh0st RAT, PoisonIvy, HydraQ, Hikit, ZxShell, Deputy Dog, Derusbi, PlugX, HTR	
Shell Crew	Deep Panda		WebMasters		APT 19	Anthem	OPM		Sakula/Sakurel, Derusbi, Scanbox Framework, many Webshells including China Chop	

Source : Google doc / APT Groups and Operations / Florian Roth et al.

Groupes d'attaquants russes

Russia												
Common Name	Other Name 1	Other Name 2	Other Name 3	Other Name 4	Other Name 5	Other Name 6	Operation 1	Operation 2	Operation 3	Operation 4	Operation 5	Targets
Sofacy	APT 28	Sednit	Pawn Storm	Group 74	Tsar Team	Fancy Bear	Russian Doll	Bundestag	TV5 Monde "Cyl	EFF Attack	DNC Hack	United States government
APT 29	Dukes	Group 100	Cozy Duke	EuroAPT	Cozy Bear	CozyCar	CK					This threat actor targets government ministries and agencies in Europe, the US, Central Asia, East Africa, and the Middle East, associated with DNC attacks
Turla Group	Snake	Venomous Bea	Group 88	Waterbug	Turla Team	Krypton	Satellite Turla	Epic Turla	The 'Penquin' Tu	Witchcoven	RUAG hack	Targeting several governments and sensitive businesses such as the defense industry
Energetic Bear	Dragonfly	Crouching Yeti	Group 24	Koala Team	Berserk Bear	Anger Bear						This threat actor targets companies in the education, energy, construction, information technology, and pharmaceutical sectors for the purposes of espionage. It uses malware tailored to target industrial control systems. Energy, Middle East oil and natural gas as the goal, dedicated to gather relevant information
Sandworm	Sandworm Tea	TEMP.Noble	Electrum	TeleBots	Quedagh Grou	BE2 APT	Black Energy	Ukrenergo	NPetya, NotPetya			This threat actor targets industrial control systems, using a tool called Black Energy, associated with electricity and power generation for espionage, denial of service, and data destruction purposes.

Source : Google doc / APT Groups and Operations / Florian Roth et al.

La connaissance des techniques d’attaque

Cyber Kill Chain – Les étapes d'attaque

Base de connaissance ATT&CK du MITRE

- ATT&CK : Modèle d'attaquant
  - Tactiques d'attaques (ou étapes), s'inspirant du modèle Cyber Kill Chain
  - Techniques d'attaques (186 à ce jour)
  - Moyens de prévention des techniques d'attaques
  - Moyens de détection des techniques d'attaques

Base de connaissance ATT&CK du MITRE

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Custom Command and Control Protocol
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data from Local System	Data Transfer Size Limits	Custom Cryptographic Protocol
Change Default File Handlers	DLL Search Order Hijacking	DLL Injection	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	PowerShell	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Data Obfuscation
Component Firmware	Exploitation of Vulnerability	DLL Search Order Hijacking	Input Capture	Network Service Scanning	Remote Desktop Protocol	Process Hollowing	Data from Removable Media	Exfiltration Over Command and Control Channel	Fallback Channels
DLL Search Order Hijacking	Legitimate Credentials	DLL Side-Loading	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Regsvcs/Regasm	Email Collection	Exfiltration Over Other Network Medium	Multi-Stage Channels
Hypervisor	Local Port Monitor	Disabling Security Tools	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Regsvr32	Input Capture	Exfiltration Over Physical Medium	Multiband Communication
Legitimate Credentials	New Service	Exploitation of Vulnerability		Process Discovery	Replication Through Removable Media	Rundll32	Screen Capture	Scheduled Transfer	Multilayer Encryption
Local Port Monitor	Path Interception	File Deletion		Query Registry	Shared Webroot	Scheduled Task			Peer Connections
Logon Scripts	Scheduled Task	File System Logical Offsets		Remote System Discovery	Taint Shared Content	Scripting			Remote File Copy
Modify Existing Service	Service File Permissions Weakness	Indicator Blocking		Security Software Discovery	Windows Admin Shares	Service Execution			Standard Application Layer Protocol
New Service	Service Registry Permissions Weakness	Indicator Removal from Tools		System Information Discovery	Windows Remote Management	Third-party Software			Standard Cryptographic Protocol
Path Interception	Web Shell	Indicator Removal on Host		System Owner/User Discovery		Windows Management Instrumentation			Standard Non-Application Layer Protocol
Redundant Access		InstallUtil		System Service Discovery		Windows Remote Management			Uncommonly Used Port
Registry Run Keys / Start Folder		Legitimate Credentials							Web Service
Scheduled Task		Masquerading							
Security Support Provider		Modify Registry							
Service File Permissions Weakness		NTFS Extended Attributes							
Service Registry Permissions Weakness		Obfuscated Files or Information							
Shortcut Modification		Process Hollowing							
Web Shell		Redundant Access							
Windows Management Instrumentation Event Subscription		Regsvcs/Regasm							
Winlogon Helper DLL		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

Base de connaissance ATT&CK du MITRE

- Tactiques d'attaques
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Exfiltration
  - Command and Control

Source : https://attack.mitre.org/tactics/enterprise/

Base de connaissance ATT&CK du MITRE

- Exemples : Techniques liées à l'étape d'attaque "Initial Access"
  - Drive-by Compromise
  - Hardware Additions
  - Replication Through Removable Media
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
  - Supply Chain Compromise
  - Trusted Relationship
  - Valid Accounts

Source : https://attack.mitre.org/tactics/TA0001/

Base de connaissance ATT&CK du MITRE

- Exemples : Technique d'attaque "Spearphishing Attachment"

Spearphishing Attachment

Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

ID: T1193

Tactic: Initial Access

Platform: Windows, macOS, Linux

Data Sources: File monitoring, Packet capture, Network intrusion detection system, Detonation chamber, Email gateway, Mail server

CAPEC ID: CAPEC-163

Version: 1.0

Source : https://attack.mitre.org/techniques/T1193/

Base de connaissance ATT&CK du MITRE

- Exemples : Technique d'attaque "Spearphishing Attachment"

Mitigation

Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments in Obfuscated Files or Information.

Because this technique involves user interaction on the endpoint, it's difficult to fully mitigate. However, there are potential mitigations. Users can be trained to identify social engineering techniques and spearphishing emails. To prevent the attachments from executing, application whitelisting can be used. Anti-virus can also automatically quarantine suspicious files.

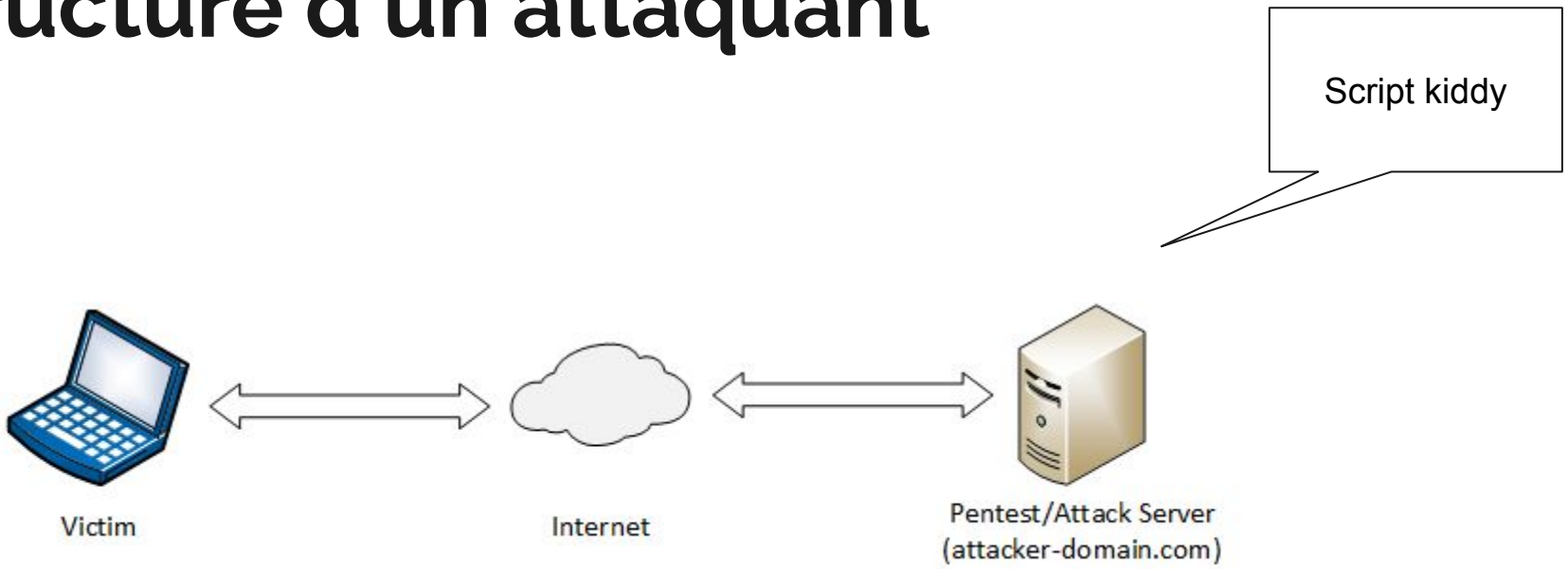
Detection

Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments in transit. Detonation chambers may also be used to identify malicious attachments. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

Anti-virus can potentially detect malicious documents and attachments as they're scanned to be stored on the email server or on the user's computer. Endpoint sensing or network sensing can potentially detect malicious events once the attachment is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning Powershell.exe) for techniques such as Exploitation for Client Execution and Scripting.

L’infrastructure d’un attaquant

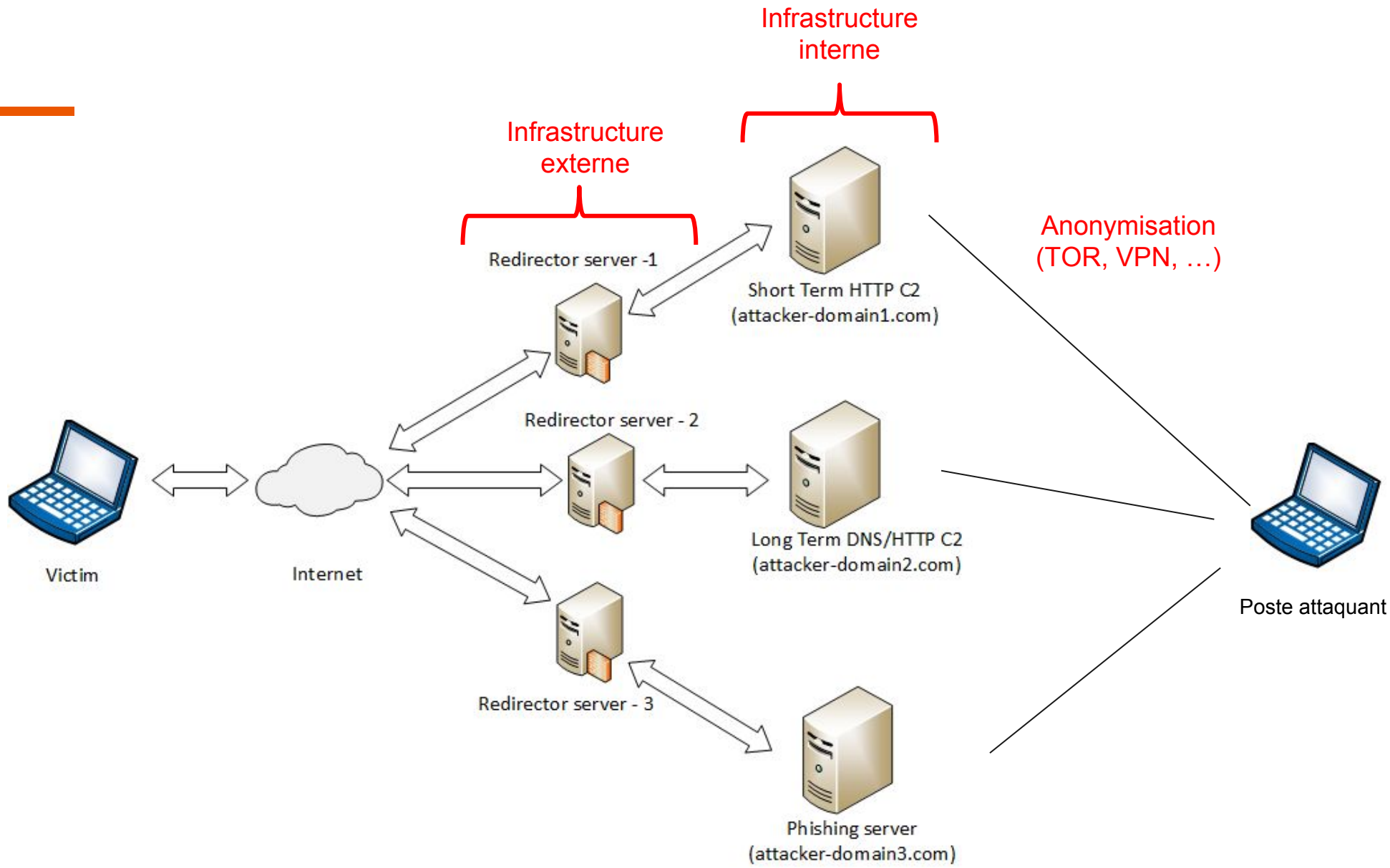
L’infrastructure d’un attaquant



Source : payatu.com

Questions : en réalité, quelle pourrait être l'infrastructure d'un attaquant ?

L'infrastructure d'un attaquant



Source : payatu.com

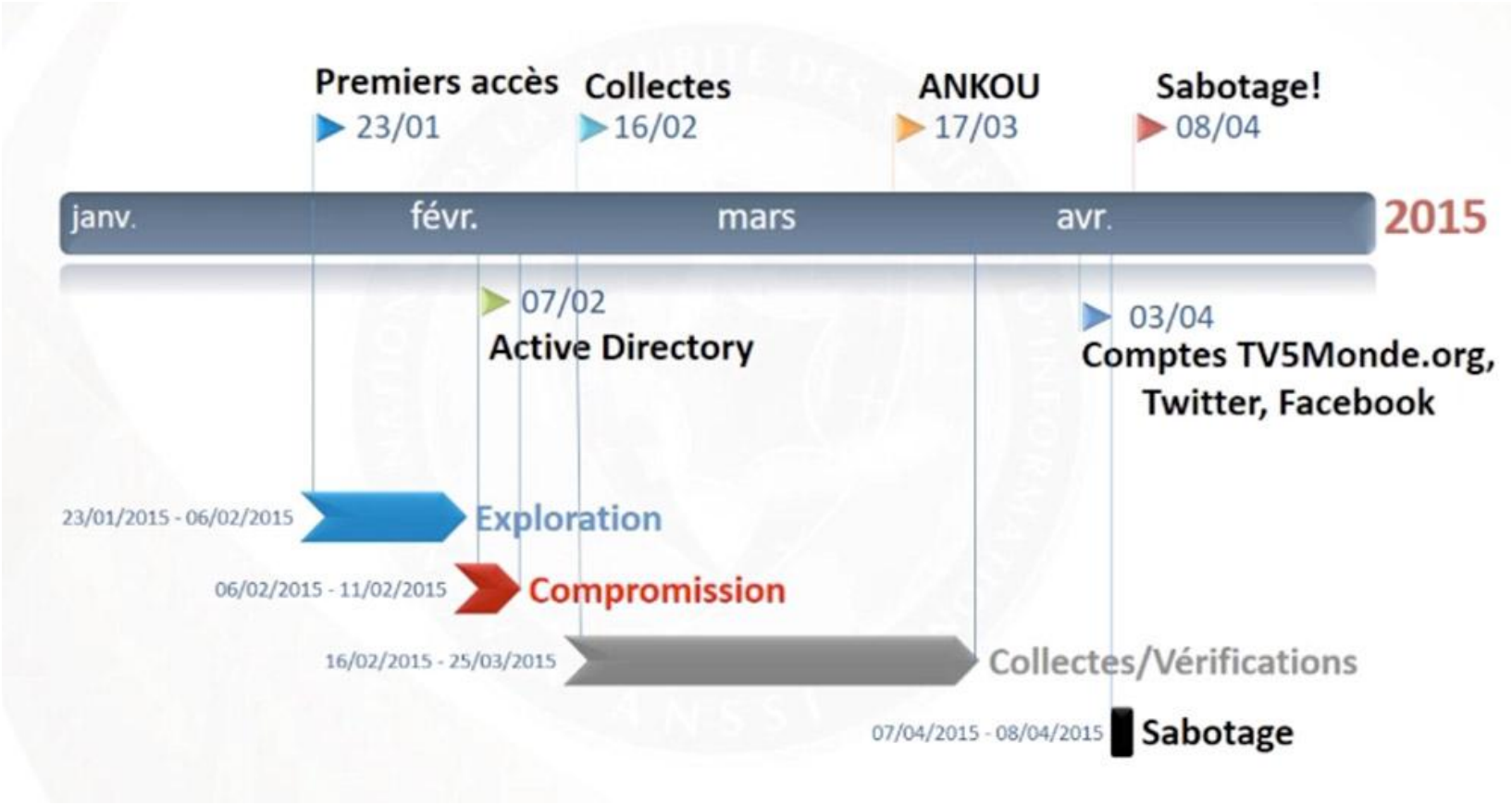
Hacker Opsec - Sécurité opérationnelle

- Un attaquant peut prendre diverses mesures pour se protéger
  - Pas d'utilisation de l'accès internet propre à l'attaquant
  - Anonymisation de l'accès à l'infrastructure d'attaque et à la cible
  - Utilisation d'un environnement dédié de préparation et de contrôle (VM)
  - Utilisation d'outils d'attaque générique
  - Utilisation de malwares spécifiques pour chaque campagne d'attaque
  - Travail sur des périodes de temps rendant difficile la localisation du fuseau horaire

Exemples de 3 attaques

- Secteur audiovisuel : TV5 Monde
- Secteur bancaire : Carbanak
- Secteur de l'énergie : centrale en Ukraine

Chronologie de l'attaque sur TV5 Monde

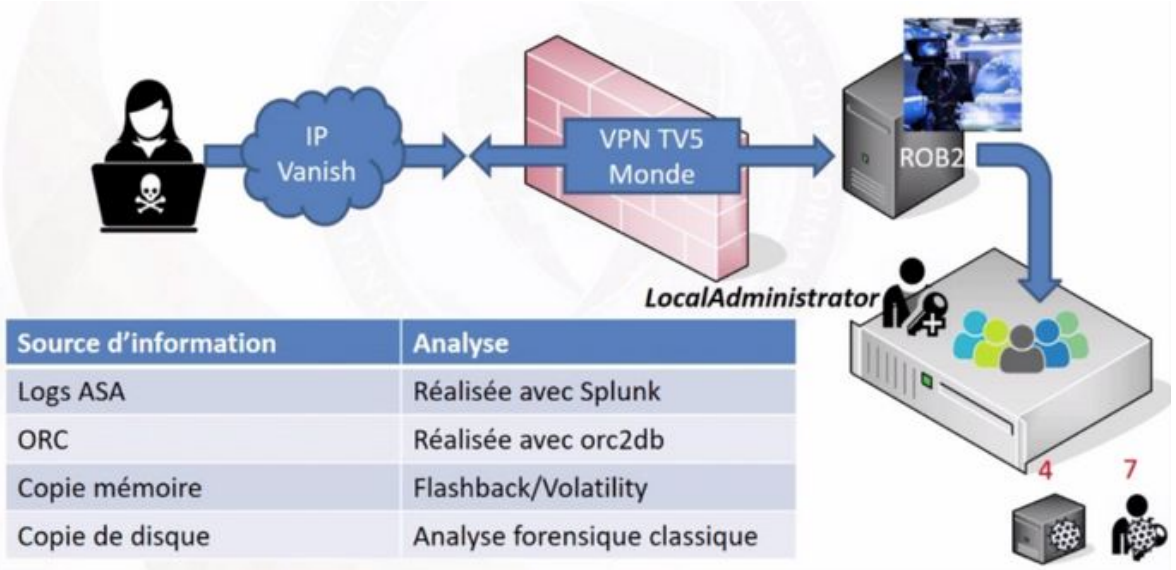


Source : ANSSI/SSTIC 2017

L’attaque sur TV5 Monde

- Phase d’exploration
  - Serveur RDP accessible sur une IP publique de TV5 Monde
    - Avec un login/mot de passe connu (lié à un service exposé)
    - Mais ne mènera nul part
  - Identification de points d’accès VPN

L’attaque sur TV5 Monde



Source d’information	Analyse
Logs ASA	Réalisée avec Splunk
ORC	Réalisée avec orc2db
Copie mémoire	Flashback/Volatility
Copie de disque	Analyse forensique classique

- Phase de compromission
  - Accès VPN avec un compte d’un sous-traitant
    - Utilisation d’un proxy anonymisant l’IP de l’attaquant
  - Scan du réseau interne de TV5 Monde
  - Identification de deux machines utilisées comme robot de caméra sur le plateau
    - Avec login/mot de passe par défaut, livré par un intégrateur
  - Dépôt d’un RAT (Remote Access Tool) sur ces machines
  - Obtention d’un compte administrateur de domaine, issu d’un prestataire
  - Connexion à l’AD et création d’un compte dédié d’administrateur de domaine
    - Afin de ne pas être dépendant du compte du prestataire

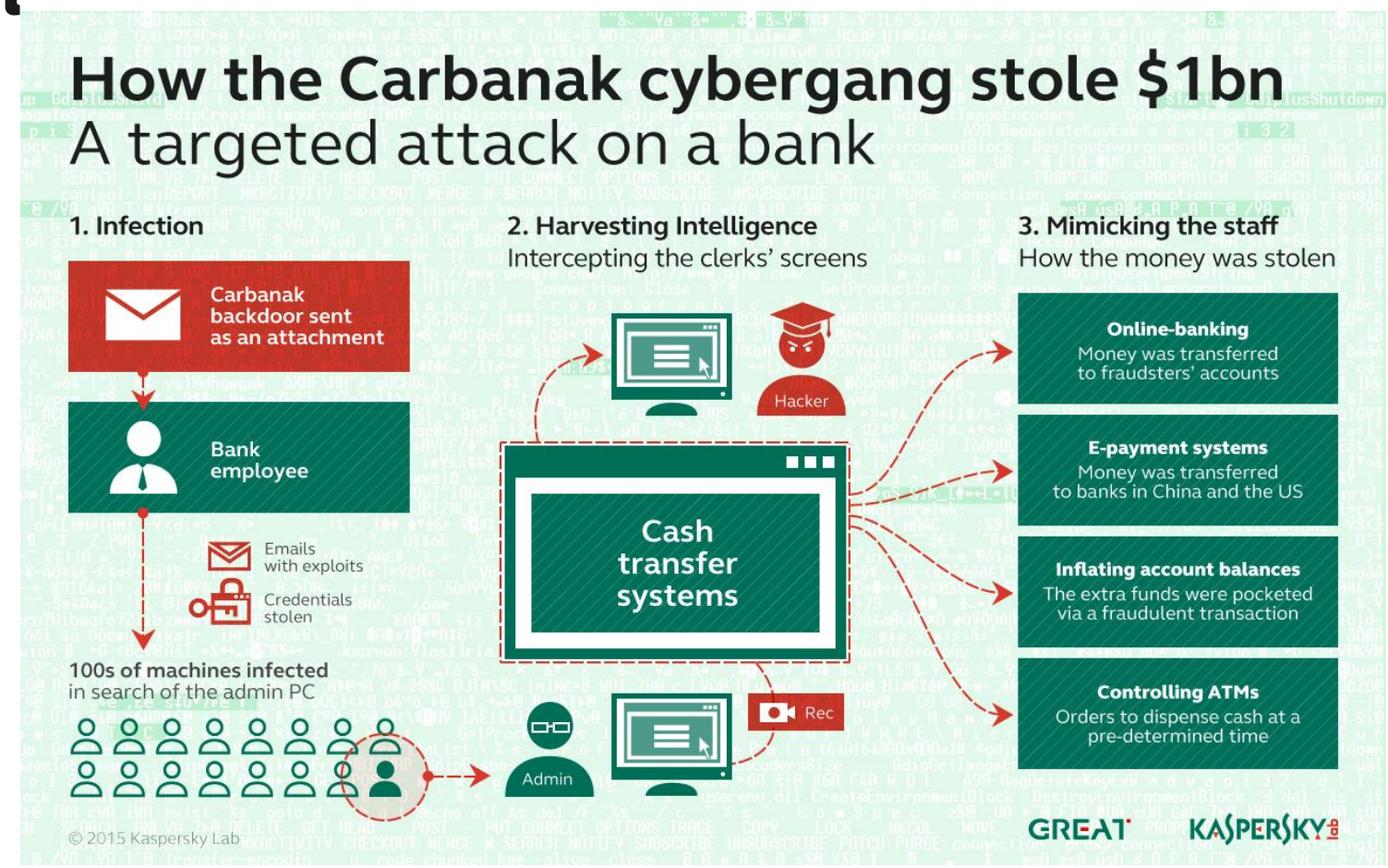
L’attaque sur TV5 Monde

- Phase de collecte
  - Accès au wiki et récupération d’informations techniques sur le SI
    - Schémas d’architecture
    - IP des équipements réseau
    - Comptes de management
  - Accès aux mails et réalisation de recherches
  - Récupération de logins et mots de passe
  - Vérification des informations techniques et des logins/mots de passe
    - Pour être sur qu’ils soient fonctionnels
  - Dépôt d’un Connect-Back sur le poste d’un administrateur

L’attaque sur TV5 Monde

- Phase de sabotage (le 8 avril)
  - Accès au VPN, puis vérification que les comptes sont toujours fonctionnels
  - Activation du Connect-Back sur le poste admin afin de ne plus être dépendant du VPN
  - Reconfiguration d’équipements vidéo (encodeurs/multiplexeurs)
  - Altération des comptes de médias sociaux (Youtube, Twitter et Facebook)
  - Altération du site web de TV5 Monde
  - Suppression des firmwares de switchs et routeurs
    - Résultats : écran noir sur la la chaine de diffusion

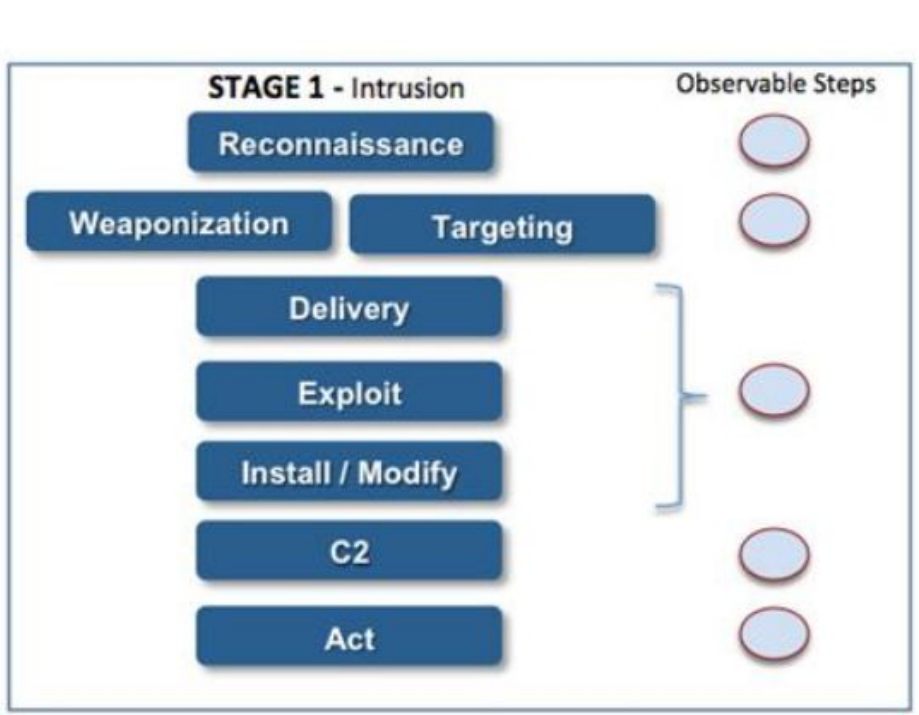
L’attaque Carbanak dans le secteur bancaire

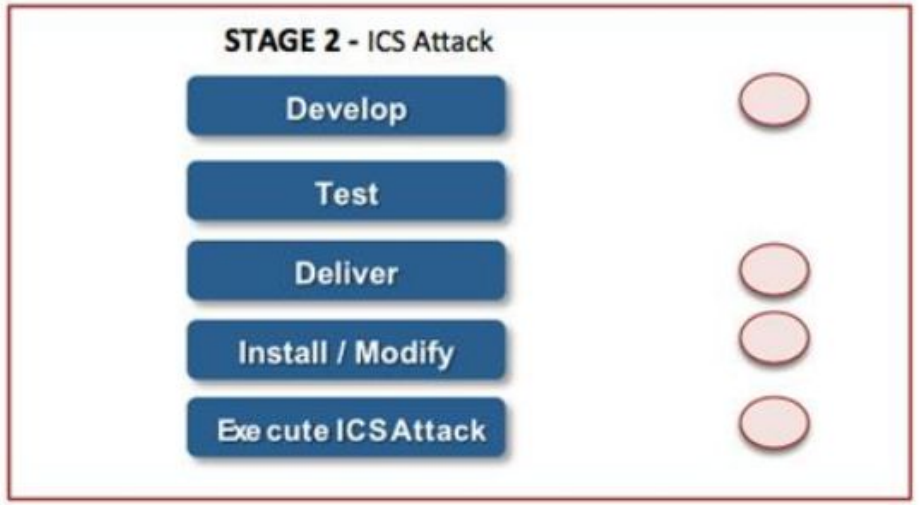


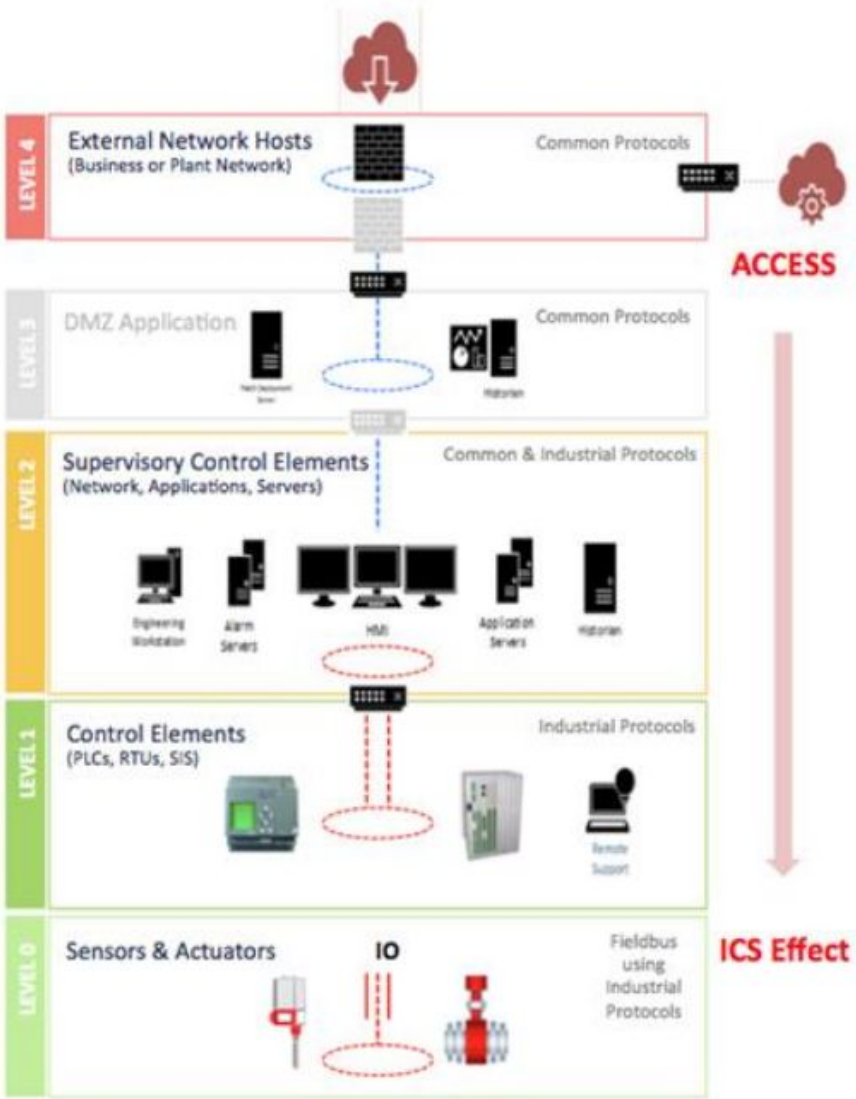
L’attaque de 2015 sur une centrale en Ukraine

- 225.000 personnes sans électricité pendant plusieurs heures
- Attribuée à la Russie

Modèle de kill chain spécifique au domaine ICS







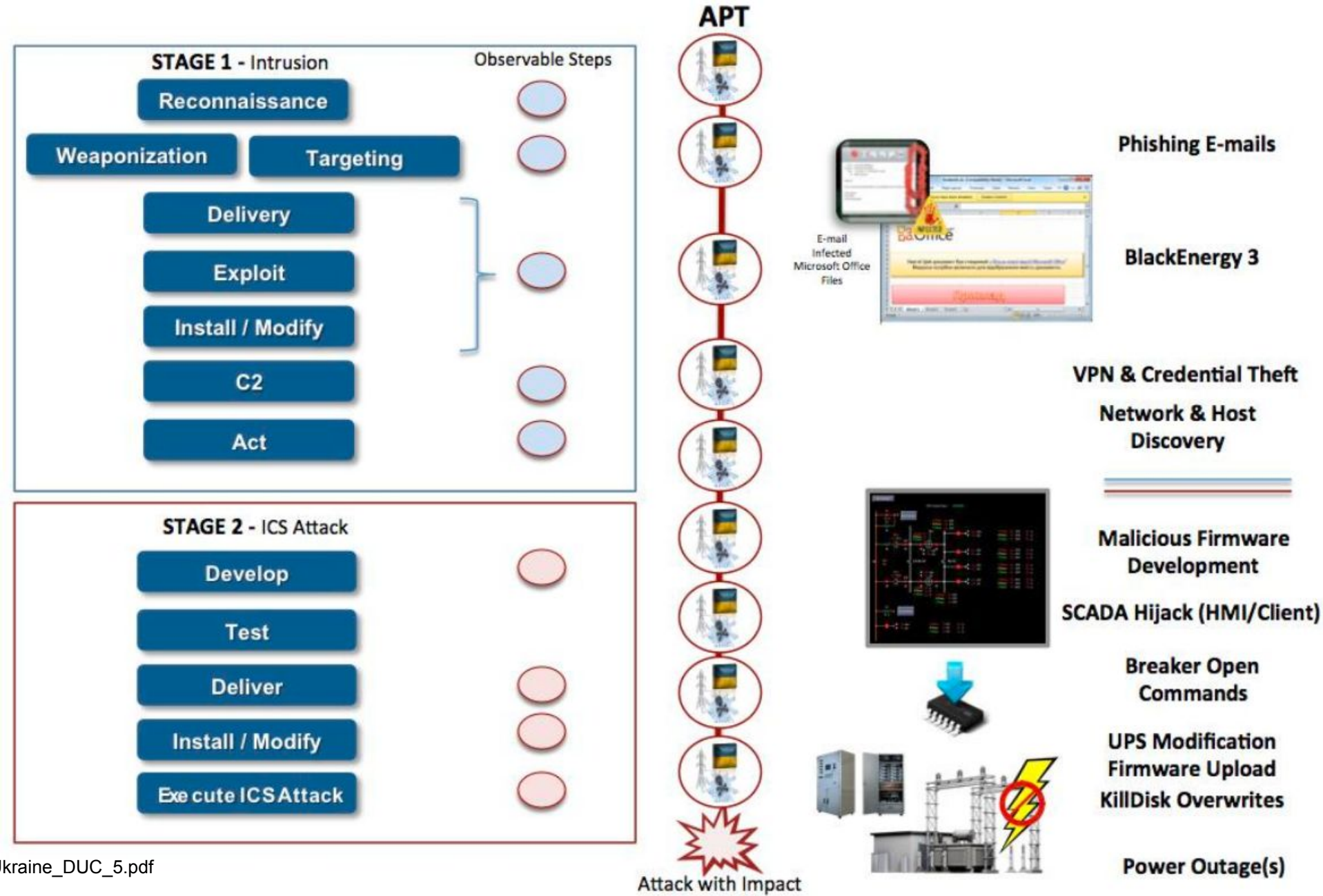
Source : https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

L'attaque de 2015 sur une centrale en Ukraine

- Déroulement
  - Spear phishing to gain access to the business networks of the oblenergos
  - Identification of existing BlackEnergy 3 presence (RAT)
  - Theft of credentials from the business networks
  - The use of virtual private networks (VPNs) to enter the ICS network
  - The use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator HMI
  - Serial-to-ethernet communications devices impacted at a firmware level
  - The use of a modified KillDisk to erase the master boot record of impacted organization systems as well as the targeted deletion of some logs
  - Utilizing UPS systems to impact connected load with a scheduled service outage
  - Telephone denial-of-service attack on the call center

Source : https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

L’attaque de 2015 sur la centrale ukrainienne Kyivoblenergo



Source : https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

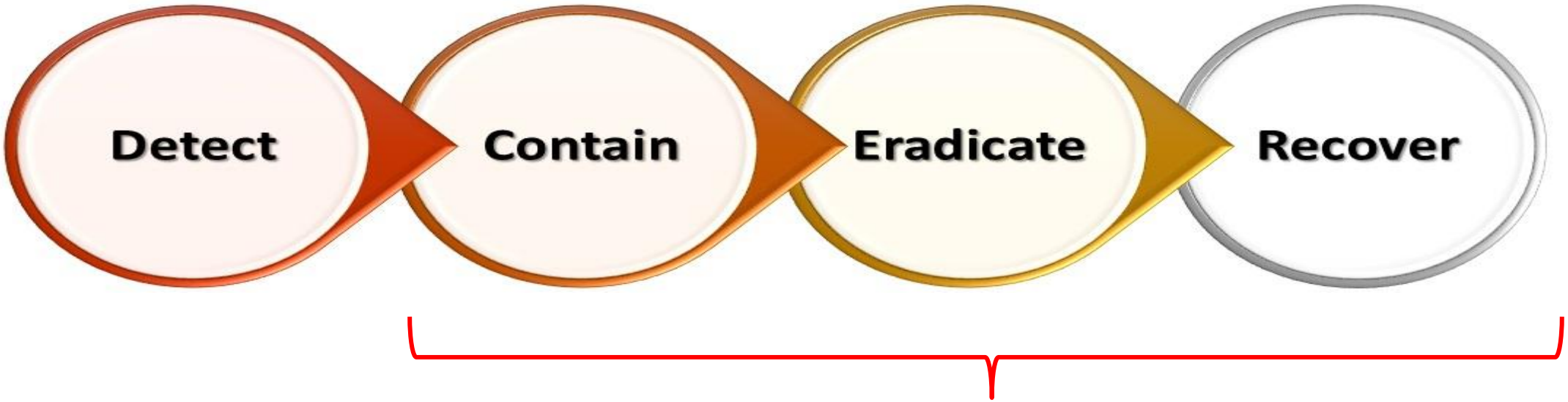
Un peu de lecture...

- Ensemble de rapports de campagnes d'attaques de type APE
  - https://github.com/kbandla/APTnotes
- Rapport de l'attaque de la société Hacking Team, par l'attaquant lui-même
  - https://pastebin.com/0SNSvyjJ
- D'autres techniques d'intrusions, par le même auteur
  - http://pastebin.com/raw/cRYvK4jb

La réponse à incidents

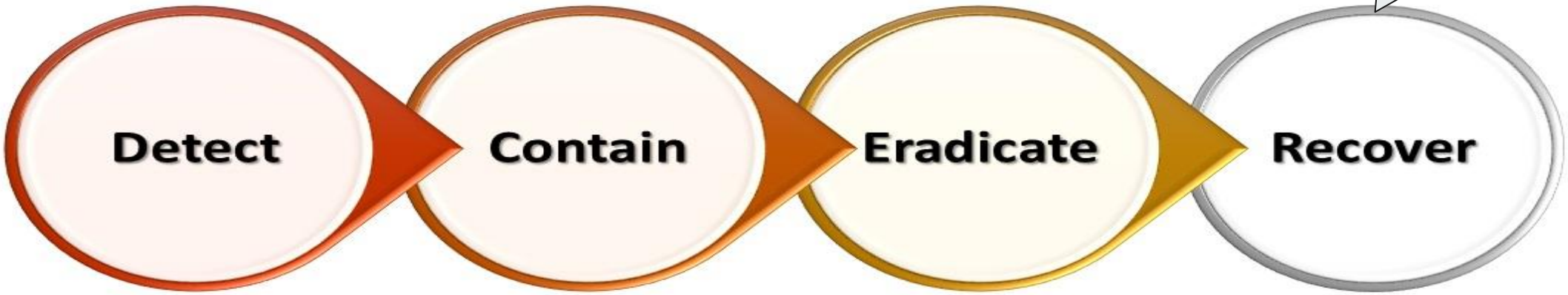
Questions : après la phase de détection, quelles peuvent être les prochaines étapes ?

Les grandes étapes

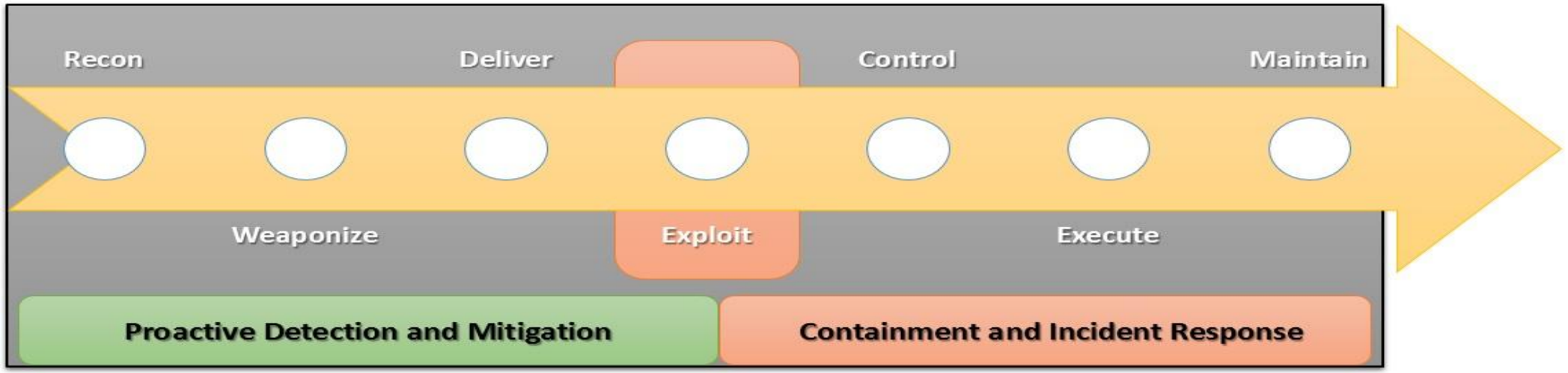


Les grandes étapes

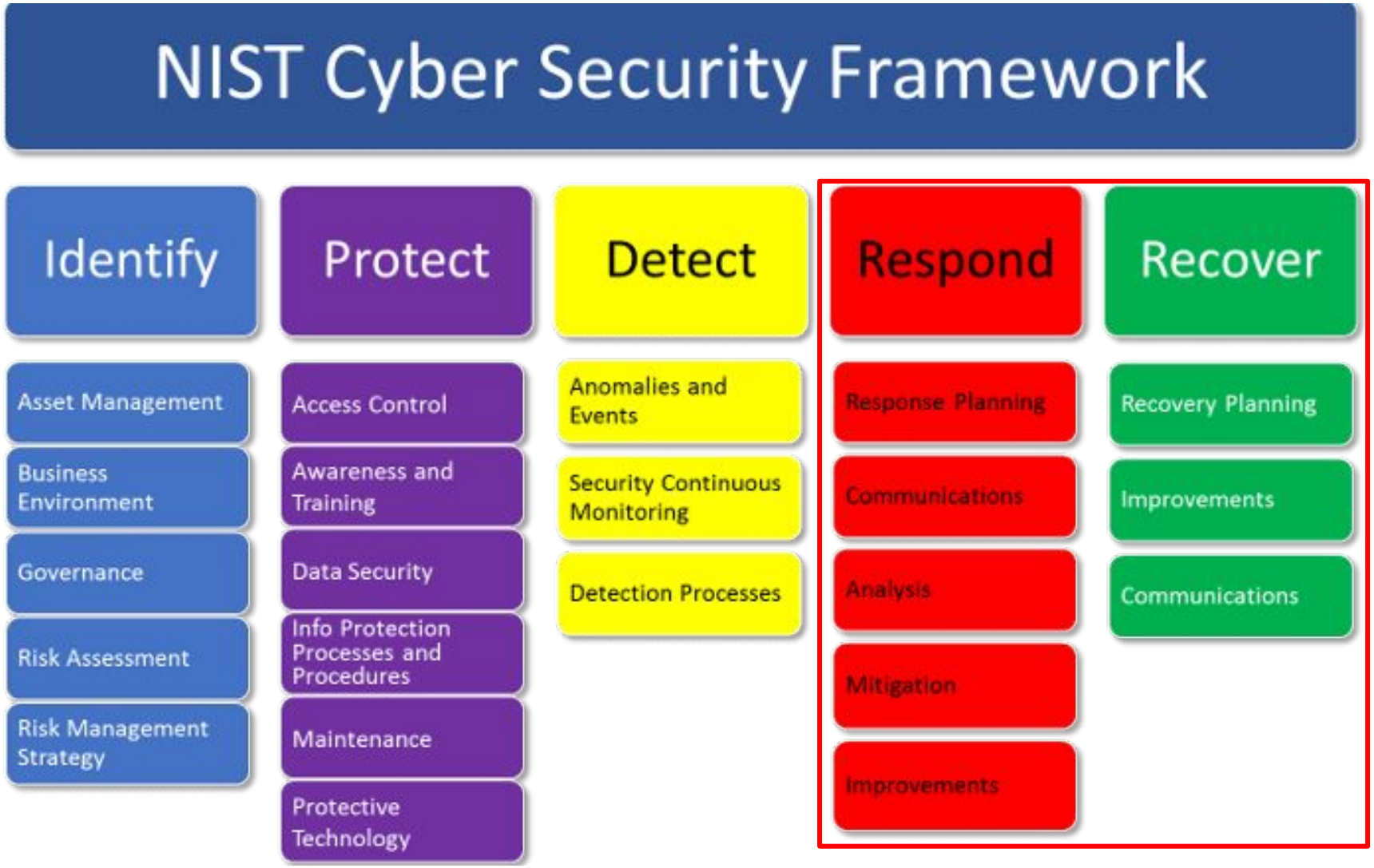
En général, l'équipe CERT s'arrête à des préconisation de remédiation



Cyber Kill Chain – La vision défensive



Le framework du NIST



Durées moyennes d'attaque et de découverte

In 60% of breaches, data is stolen in hours

54% of breaches are not discovered for months

Timespan of events by percent of breaches

Source: 2013 Data Breach Investigations Report

Durées moyennes d’attaque et de découverte

- Une compromission est souvent détectée plusieurs mois après
  - 224 jours d'après Mandiant
- D'où la nécessité de pouvoir scanner les logs historisés à la recherche de compromissions nouvellement connues

Le confinement de l’incident

Le confinement de l'incident

- Objectifs
  - Limiter la propagation sur le SI
  - Limiter les capacités de contrôle un attaquant interne/externe

Le confinement de l'incident

- Approches envisageables
  - Mise en quarantaine sur le réseau (NAC, etc.)
  - Coupure réseau de la machine infectée
  - Extinction de la machine infectée

L’analyse de l’incident

L’analyse de l’incident

- Dans un premier temps
  - Etablir un journal de bord
  - Collecter un maximum d’information
    - Copie des disques
    - Traces réseau/netflow
    - Évènements remontés au SIEM

Les questions que l'on se pose face à un incident

- Quel est le vecteur d'infection initiale ?

Source : Allain Sullam

Les questions que l'on se pose face à un incident

- Quels fichiers ont été accédés, créés, supprimés ?
  - Importance de pouvoir tracer les accès aux fichiers

Source : Allain Sullam

Les questions que l'on se pose face à un incident

- Y-a-t-il eu des communications réseau ?
  - Internes (rebond latéral ? dump de serveur de fichier ?)
  - Externes (exfiltration de données ? ...)
  - Ponctuelles (peut laisser penser à une attaque opportuniste)
  - Permanentes (peut laisser penser à une attaque ciblée)

Source : Allain Sullam

Les questions que l'on se pose face à un incident

- En cas de communications réseau, quels sont leurs buts ?
  - Spamming
  - (D)DOS
  - Exfiltration de données
  - ...
- Quelles sont leurs destinations ?

Source : Allain Sullam

Les questions que l'on se pose face à un incident

- Quel est le périmètre de compromission ?
- Comment s'est propagé l'attaquant ?

Source : Allain Sullam

L’éradication des éléments d’attaque

L’éradication des éléments d’attaque

- Objectifs
  - Nettoyer les machines infectées

L’éradication des éléments d’attaque

- Principes
  - Suppression des comptes frauduleux
  - Désactivation des comptes usurpés / changement du mot de passe
  - Suppression des portes dérobées, RAT, et autres malwares
  - Mise en place des correctifs vis à vis des vulnérabilités exploitées

La remise en état

La remise en état

- Objectifs
  - Permettre au activités métier de fonctionner de nouveau

La remise en état

- Principes
  - Réalisation d'un plan d'action
  - Réinstallation de postes/serveurs OU mises à jour systèmes
  - Déploiement d'un domaine Active Directory propre
  - Mise en place de règles réseau (VLAN, pare-feu, etc.) saines
  - Déploiement de nouveaux mécanismes de sécurité
  - Suivi dans le temps des logs système et réseau
  - Dans certaines situations, la réponse à incident doit être effectuée en parallèle du maintien du service

Contre attaquer ?

Contre attaquer ?

- Synonymes
  - *hack-back*
  - *Counter-CNE (Computer network exploitation)*
  - Riposte numérique
  - Contre attaque numérique
- Principe : traquer et identifier l'attaquant et son infrastructure

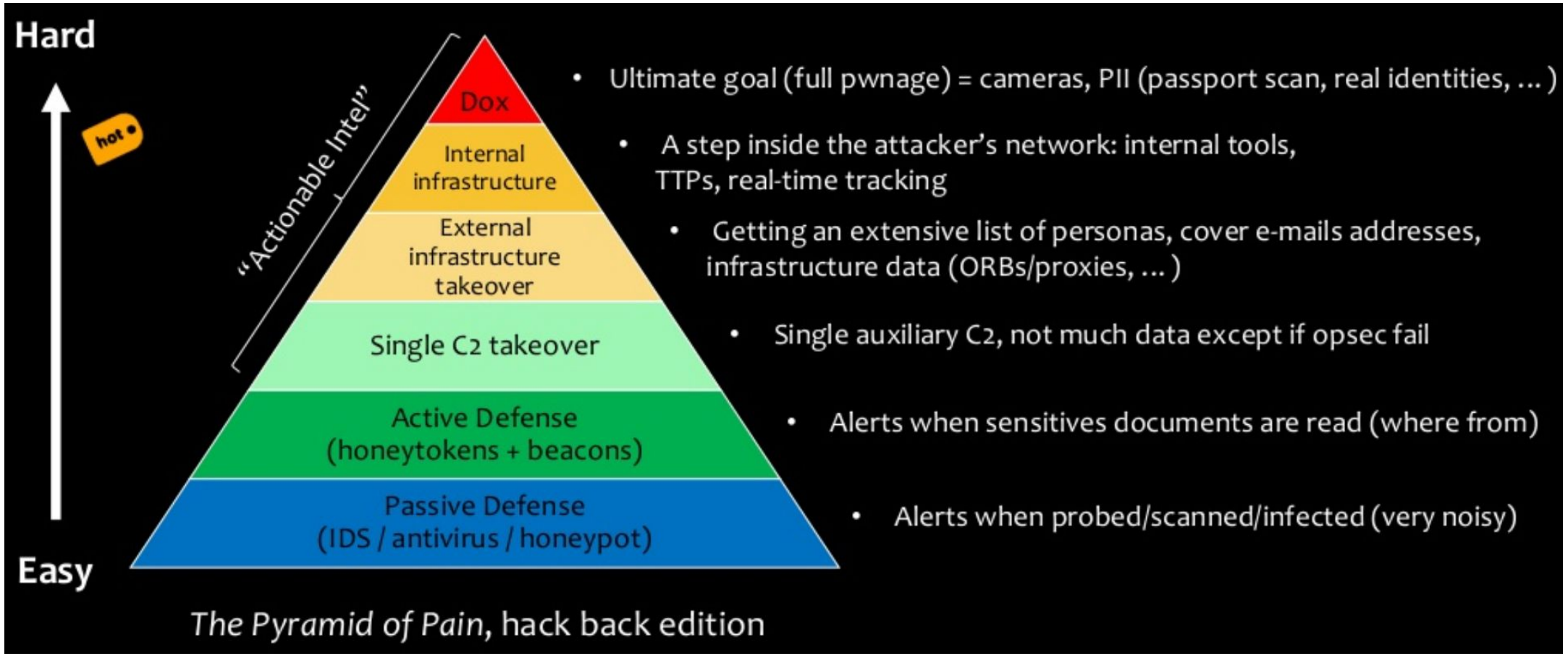
Questions : pourquoi et comment contre-attaquer ?

Contre attaquer ?

- Dans quels buts ?
  - Caractériser plus finement l'étendue de l'attaque (ex : ensemble des machines infectées)
  - Neutraliser l'adversaire (botnet, C&C, etc.)
  - Attribuer l'attaque
  - Décourager l'adversaire
  - Récupérer les outils de l'adversaire

Source : @xorz

Différents niveaux de contre attaque



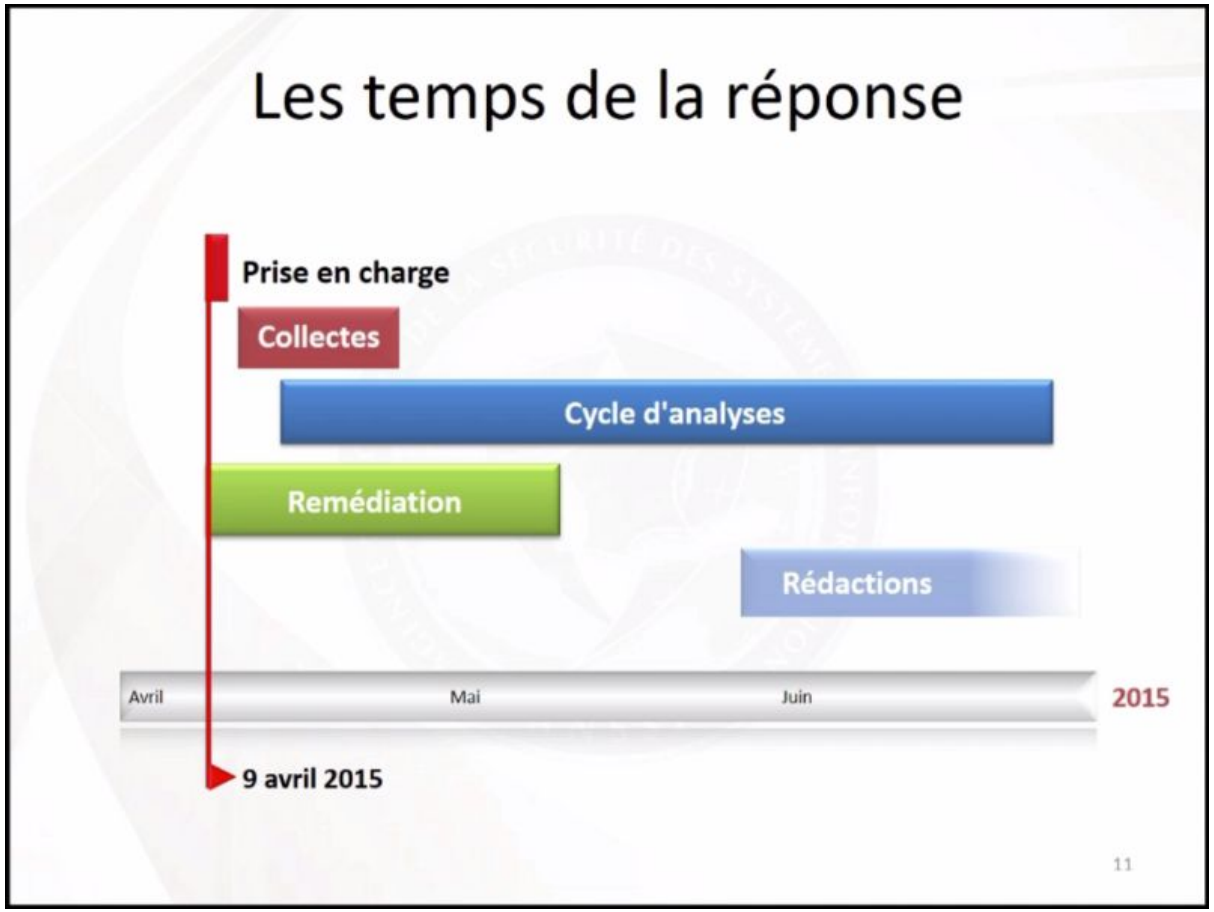
Source : @xorz

Contre attaquer ?

- Le cadre légal
  - Aux US : proposition de loi en 2017 *“Active Cyber Defense Certainty Act”*
    - Donnerait la possibilité aux entreprises d’*« accéder à l’ordinateur de l’attaquant sans son autorisation […] pour récolter des informations afin de constater une activité criminelle et la partager avec les forces de l’ordre ou de perturber l’activité non autorisée »*
  - En France, l’ANSSI s’y oppose :
    - Risque de se tromper en termes d’attribution
    - Risque de profiter d’un cadre légal laissant la porte ouverte à l’attaque de concurrents

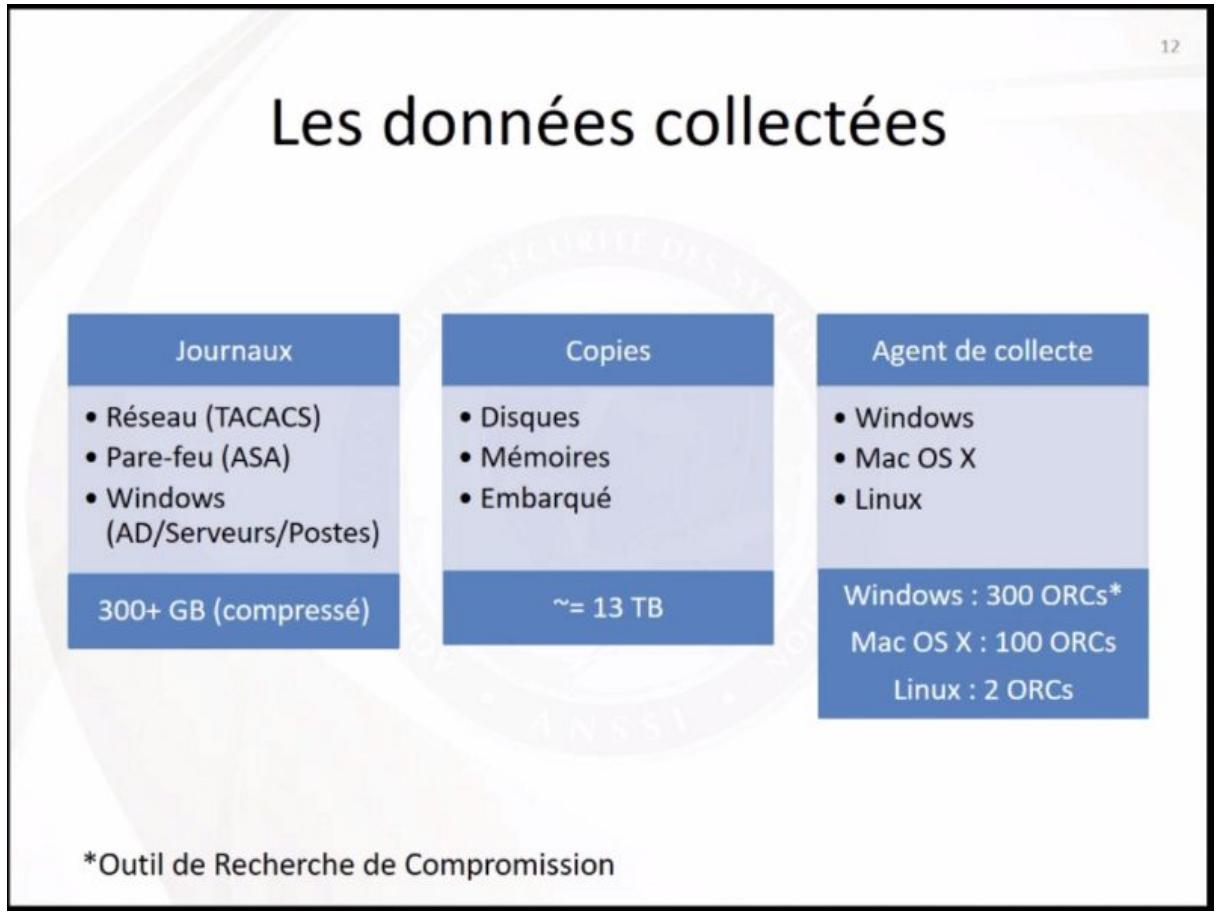
Réponse sur l'incident TV5 Monde

Chronologie de réponse



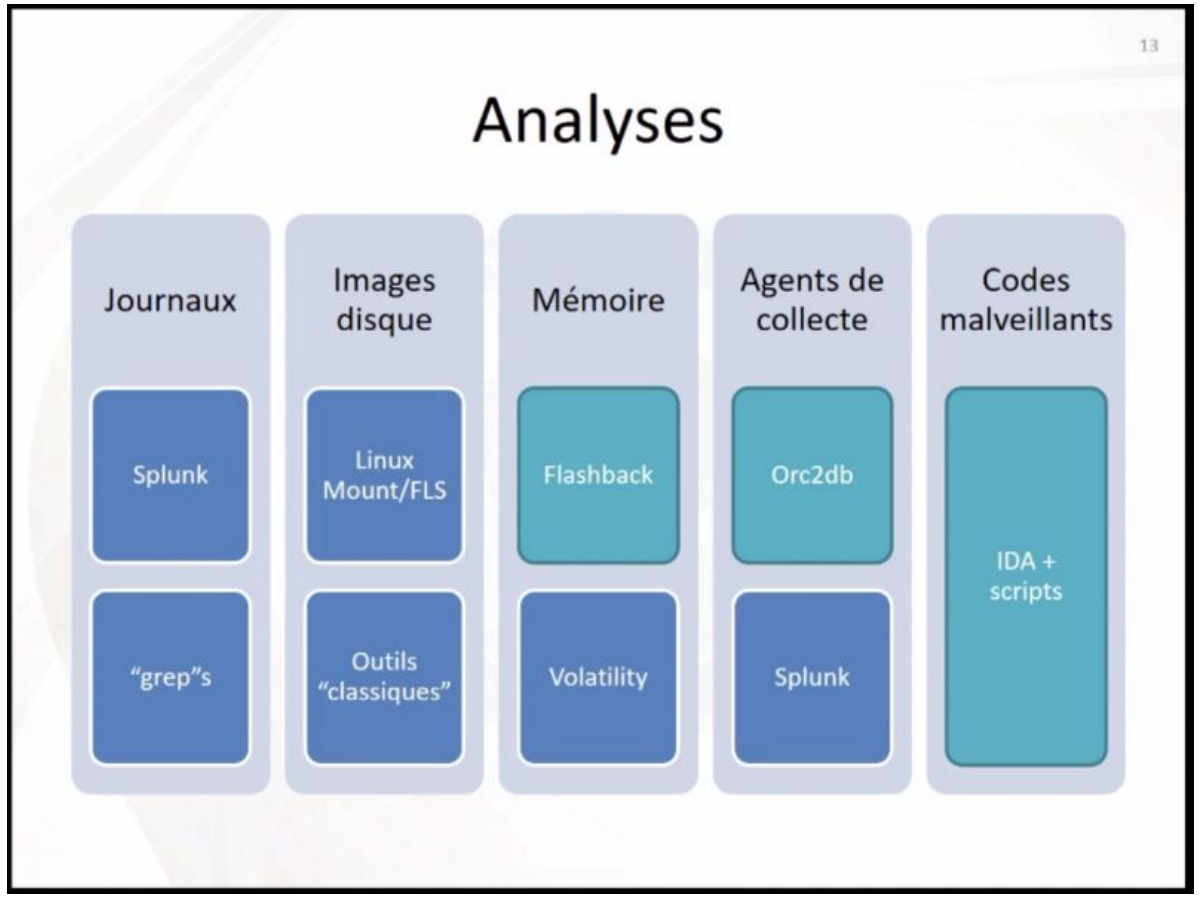
Source : SSTIC 2017

Données collectées



Source : SSTIC 2017

Moyens d'analyse



Source : SSTIC 2017

Organisation du SOC

Les profils d'une équipe SOC

- Level 1 analyst, first responder, real-time analyst
  - Inspect alerts and the associated traffic to eliminate false positives (triage analysis)
- Level 2 analyst
  - Escalation analysis, investigate suspicious activity received from triage analysis
- Correlation analyst
  - Search for patterns and trends in current and historical data
- Threat analyst
  - Gain insight into the identity, motives and sponsorship of attackers and forecast upcoming attack
- Incident handler, incident responder
  - Implement a course of action in reaction to a confirmed incident
- Forensic analysts
  - Work in support of a law enforcement investigation

Source : The real work of computer network defense Analysts

Quelques bonnes pratiques

- Pas d’organisation type
- Importance de la collaboration avec les équipes SI et NOC
- Utilisation fiches réflexes pour l'analyse et la remédiation
- Ne pas tomber dans la routine
- Eviter la hiérarchisation des équipes
    - Faire tourner les postes
    - Chacun peut participer à l’ensemble des tâches

Fiches réflexe

- Utilisé par les analyses pour savoir comment réagir face à un incident
- Une fiche par catégorie d'attaque
- Chaque étape est décrite
  - Détection
  - Isolation
  - Suppression de la menace
  - Remise en état
- Capitalisation et amélioration continue des fiches

Fiches réflexe

- Exemple : les fiches du CERT Société Générale
  - IRM-1: Worm Infection
  - IRM-2: Windows Intrusion
  - IRM-3: Unix Intrusion
  - IRM-4: DDoS
  - IRM-5: Malicious Network Behaviour
  - IRM-6: Website Defacement
  - IRM-7: Windows Malware Detection
  - IRM-8: Blackmail
  - IRM-9: Smartphone Malware
  - IRM-10: Social Engineering
  - IRM-11: Information Leakage
  - IRM-12: Insider Abuse
  - IRM-13: Phishing
  - IRM-14: Scam
  - IRM-15: Trademark Infringement
  - IRM-16: Not public
  - IRM-17: Ransomware

Source : https://github.com/certsocietegenerale/IRM

Exemple : Fiche réflexe ransomware

Preparation 1

- A good knowledge of the usual operating systems security policies is needed.
- A good knowledge of the usual users' profile policies is needed.
- Ensure that the endpoint and perimetric (email gateway, proxy caches) security products are up to date
- Since this threat is often detected by end-users, raise your IT support awareness regarding the ransomware threat
- **Make sure to have exhaustive, recent and reliable backups of local and network users' data**

Identification 2

General signs of ransomware presence

Several leads might hint that the system could be compromised by ransomware:

- Odd professional emails (often masquerading as invoices) containing attachments are being received
- A ransom message explaining that the documents have been encrypted and asking for money is displayed on user's desktop

Figure 1 - Cryptowall ransom message

Identification 2

Host based identification

- Look for unusual executable binaries in users' profiles (%ALLUSERSPROFILE% or %APPDATA%) and %SystemDrive%
- Look for the aforementioned extensions or ransom notes
- Capture a memory image of the computer (if possible)
- Look for unusual processes
- Look for unusual email attachment patterns
- Look for unusual network or web browsing activities; especially connections to Tor or I2P IP, Tor gateways (tor2web, etc) or Bitcoin payment websites

Network based identification

- Look for connection patterns to Exploit Kits
- Look for connection patterns to ransomware C&C
- Look for unusual network or web browsing activities; especially connections to Tor or I2P IP, Tor gateways (tor2web, etc) or Bitcoin payment websites
- Look for unusual email attachment patterns

Source : https://github.com/certsocietegenerale/IRM

Exemple : Fiche réflexe ransomware

Containment 3

- Disconnect all computers that have been detected as compromised from the network
- If you cannot isolate the computer, disconnect/cancel the shared drives (NET USE x: \\unc\path\ /DELETE)
- Block traffic to identified ransomware's C&C
- Send the undetected samples to your endpoint security provider
- Send the uncategorized malicious URL, domain names and IP to your perimetric security provider

Remediation 4

- Remove the binaries and the related registry entries (if any) from compromised profiles (%ALLUSERSPROFILE% or %APPDATA%) and %SystemDrive%
- If the above step is not possible reimage the computer with a clean install

Recovery 5

Objective: Restore the system to normal operations.

1. Update antivirus signatures for identified malicious binaries to be blocked
2. Ensure that no malicious binaries are present on the systems before reconnecting them
3. Ensure that the network traffic is back to normal
4. Restore user's documents from backups

All of these steps shall be made in a step-by-step manner and with technical monitoring.

Aftermath 6

Report

An incident report should be written and made available to all of the stakeholders.

The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve malware and network intrusion detection processes should be defined to capitalize on this experience.

Source : https://github.com/certsocietegenerale/IRM

Processus d’un SOC

Processus liés à une prestation

- Initialisation d'une prestation
- Suivi de la prestation
- Construction de la liste des incidents redoutés
- Construction d'une échelle de gravité
- Construction de la stratégie de collecte
- Construction de la stratégie d'analyse
- Construction de la stratégie de notification

Processus liés à la gestion des règles

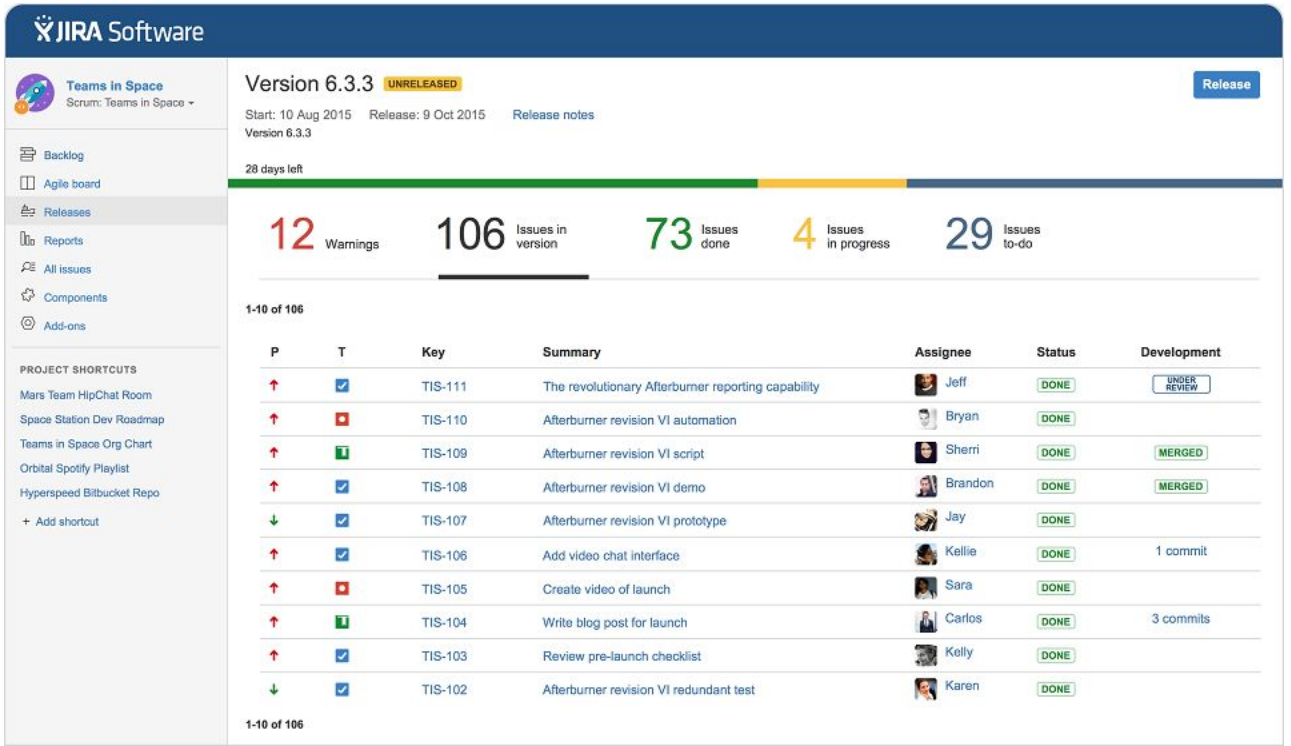
- Création de règles de détection
- Création et la mise à jour d'une liste de règles de détection
- Implémentation des règles de détection dans les outils techniques d'analyse

Processus liés à la gestion des incidents

- Qualification des incidents de sécurités
- Récupération des évènements liés à un incident de sécurité
- Récupération des évènements sur demande du commanditaire
- Récupération de l'incident lié à une notification

Processus liés au ticketing

- Administration et exploitation d'un outil de gestion des tickets d'incident de sécurité
- Construction des tickets d'incident



Processus liés au stockage

- Processus de stockage des évènements
- Processus de stockage des notifications
- Processus de stockage des incidents de sécurité

Processus liés à la collecte

- Collecte des sources de collecte
- Implémentation des sources de collecte
- Implémentation des collecteurs
- Administration des collecteurs

Processus liés à la notification

- Processus pour implémenter et utiliser les moyens de notification
- Processus pour utiliser les moyens de notification
- Processus d'implémentation du portail Web

Les indicateurs de suivi

Indicateurs techniques

- Suivi de la capacité de stockage des évènements
- Suivi de la capacité de stockage des incidents de sécurité
- Suivi de la capacité de stockage des notifications
- Délai de prise en charge des évènements sur les collecteurs

Indicateurs liés aux règles de détection

- Le nombre de règles de détection créées, modifiées ou retirées des outils d'analyse
- L'identifiant et la description de chaque règle créée, modifiée ou retirée des outils d'analyse
- Le motif de la création, de la modification ou du retrait de la règle de sécurité (ex. : création, modification ou retrait à la demande du commanditaire, etc.)

Indicateurs sur la gestion des évènements (activité)

- Le nombre de sources de collecte
- Le nombre de collecteurs
- Le nombre d'évènements collectés par jour / par mois
- Le nombre d'évènements collectés par collecteur par jour / par mois
- Le nombre d'évènements transmis aux outils techniques d'analyse par jour / par mois
- Le taux de remplissage de chaque système de stockage des évènements, y compris les collecteurs dans l'enclave si ces derniers sont sous la responsabilité du prestataire
- La capacité de stockage restante de chaque système de stockage des évènements, y compris les collecteurs dans l'enclave si ces derniers sont sous la responsabilité du prestataire

Indicateurs sur la gestion des évènements (efficacité)

- La durée minimale / moyenne / maximale entre la génération d'un évènement par la source de collecte et son stockage dans les systèmes de stockage des évènements
- La durée minimale / moyenne / maximale entre la génération d'un évènement par la source de collecte et l'envoi aux outils techniques d'analyse
- La durée minimale / moyenne / maximale de traitement d'une recherche d'évènement dans les systèmes de stockage des évènements
- Le taux de disponibilité de chaque dispositif de gestion des évènements, y compris les collecteurs dans l'enclave si ces derniers sont sous la responsabilité du prestataire

Indicateurs liés à la gestion des incidents (activité)

- Le nombre d’incidents détectés par mois
- Le nombre d’incidents avérés suite à une qualification par mois
- Le nombre de règles de détection implémentées dans les outils techniques d’analyse
- Le nombre de règles de détection créées, modifiées ou retirées par mois en fonction de l’origine (activité de veille, demande du commanditaire, etc.)
- Le taux de disponibilité des outils techniques d’analyse
- Le nombre de règles de détection déclenchées par mois
- Le taux de remplissage des systèmes de stockage des incidents
- La capacité restante des systèmes de stockage des incidents
- La liste des règles de détection jamais déclenchées

Indicateurs liés à la gestion des incidents (efficacité)

- Le délai maximal de qualification d'un incident
- Le délai moyen de qualification d'un incident de sécurité selon son niveau de gravité
- Le délai moyen de mise à jour des règles de détection suite à une demande du commanditaire
- La durée moyenne d'une recherche unitaire d'incident
- Le nombre d'erreurs de qualification d'incident
- Le taux d'erreurs de qualification d'incidents
- Le nombre d'évènements non reconnus et donc non pris en compte par les outils techniques d'analyse
- Le taux d'évènements non reconnus et donc non pris en compte par les outils techniques d'analyse

Indicateurs sur la gestion des notifications (activité)

- Le taux de disponibilité du portail Web
- Le taux de disponibilité du serveur de messagerie
- Le nombre de notifications transmises au commanditaire par mois selon le niveau de gravité de l'incident de sécurité
- Le nombre de tickets d'incident de sécurité ouverts par mois
- Le nombre de tickets d'incident de sécurité clos par mois
- La durée minimale / moyenne / maximale entre la création d'un ticket et sa clôture
- Le nombre de comptes autorisés à accéder au portail Web
- Le nombre de comptes d'accès au portail Web créés par mois
- Le nombre de comptes d'accès au portail Web supprimés par mois
- Le nombre d'authentifications au portail Web réussies par mois
- Le nombre d'authentifications au portail Web en échec par mois

Indicateurs sur la gestion des notifications (efficacité)

- La durée minimale / moyenne / maximale entre la détection d'un incident de sécurité et la notification, selon le niveau de gravité
- Le nombre de notifications erronées (faux positifs, etc.)

Indicateurs stratégiques

- La consolidation des indicateurs opérationnels
- Le taux de disponibilité du service de détection
- Le taux de disponibilité des dispositifs techniques du service de détection
- Le nombre d’incidents avérés sur le système d’information du prestataire par mois pour le périmètre du service de détection du commanditaire
- Le taux de conformité avec le niveau de qualité exigé par le commanditaire

L'entraînement des équipes

L'entraînement d'une équipe SOC

- Objectifs
  - Former les analystes
  - Tester l'efficacité et la réaction des équipes SOC/CERT (i.e. les compétences intrinsèques des personnes et leur maîtrise des processus)
  - Valider l'architecture de défense face à des modèles d'attaquant

Plusieurs approches pour l'entraînement

- Plateforme Cyber Range
  - Airbus
  - Diateam
  - Cyberbit
  - Ravello Systems
  - Sypris
  - Simspace

Plusieurs approches pour l'entraînement

- Plateforme de génération de trafic de fond et d’attaque
  - Ixia / BreakingPoint
  - Cyber Test System

Plusieurs approches pour l'entraînement

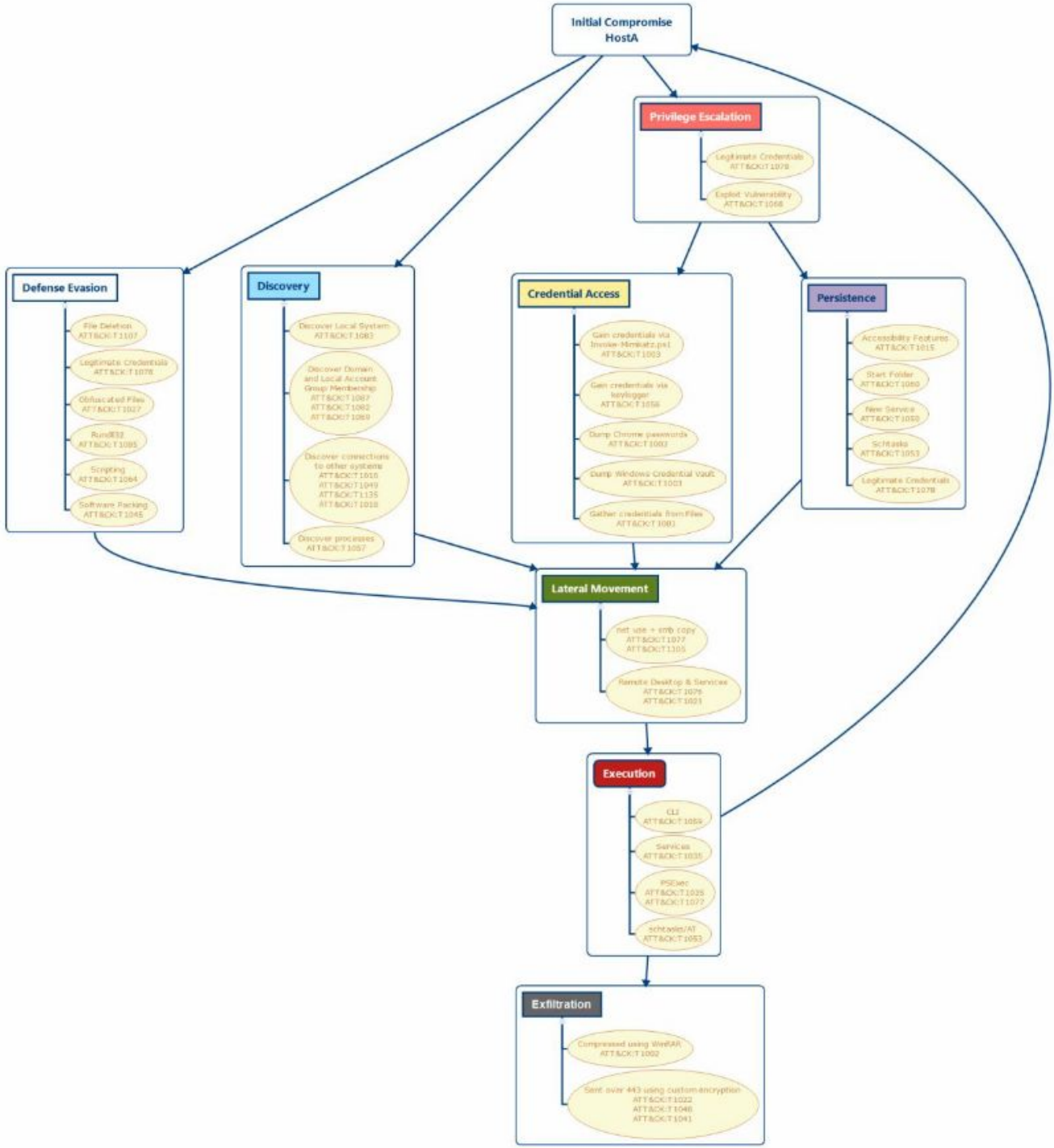
- Outils de simulation d’attaquant - RTA (*Red Team Automaton*)
  - Redcanary
  - Red Team Automation
  - Metta
  - APT Simulator
  - Caldera

Scénarios possibles

- Red team face à une architecture de défense qui évolue et qui réagit automatiquement
- Blue team (défense) face à des scénarios d'attaque joués automatiquement
- Red team vs Blue team
- ...

Simulation de groupes d'attaquants

- *Adversary Emulation Plans* du MITRE
- Simulation des TTP de groupes d'attaquants
  - Sur la figure : groupe chinois APT3



Source : https://attack.mitre.org/resources/adversary-emulation-plans/