

Corruption de données

Réflexions des établissements financiers du **Forum des Compétences**



Une étude menée avec



Sommaire

Étude des scénarios de corruption de données	3
I. Objectifs	3
II. Participants	4
III. Typologie des techniques d'attaques	5
Introduction	6
IV. Définition et cadre	6
V. Typologie de corruption accidentelle	6
VI. Typologie de corruption malveillante	7
VII. Motivations principales d'une corruption de données malveillante	8
Description des conséquences d'une corruption de données	10
VIII. Les macro-scénarios de corruption de données	10
1. Les scénarios accidentels	10
2. Les scénarios de malveillance logique	13
3. Scénario de malveillance physique	19
IX. Conséquences	20
1. Impacts financiers	20
2. Impacts d'image	21
3. Impacts réglementaires	22
Protection des données	23
X. Bonnes pratique en matière de résilience	23
ANNEXE 1	24
ANNEXE 2	25

Étude des scénarios de corruption de données

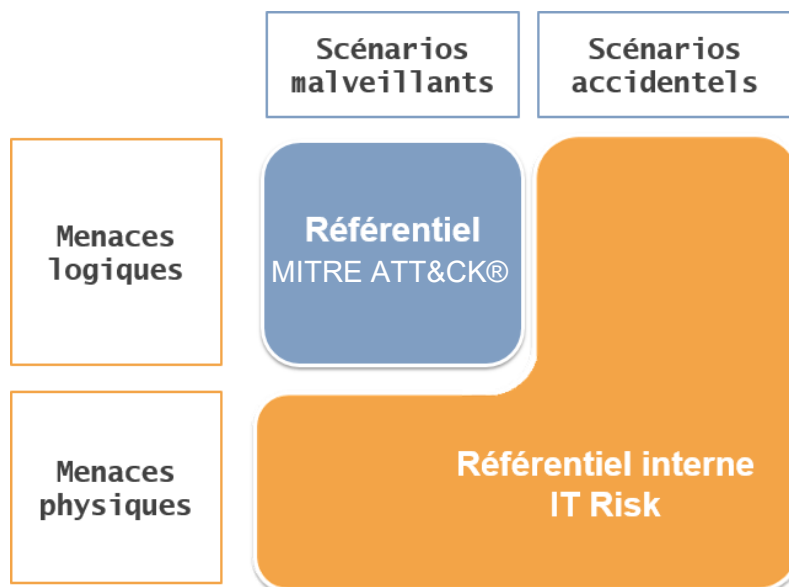
I. Objectifs

Ce document a pour objectifs d'identifier des scénarios représentatifs d'une corruption de données, et de les regrouper par typologie de causes et d'impacts.

Les scénarios génériques identifiés permettent d'établir une cartographie des menaces relatives à la corruption, à la fois macroscopique mais suffisamment exhaustive pour nourrir les réflexions d'entreprise en matière de stratégie de résilience ou de *Cyber Threat Intelligence*.

À l'issue de cette étape intermédiaire, ces travaux sont amenés à se poursuivre. La suite logique consistera à établir des réponses aux scénarios génériques présentés dans ce document au travers d'un autre groupe de travail.

Le rapprochement des scénarios avec le référentiel MITRE ATT&CK® a permis de standardiser davantage la catégorisation des causes et des impacts. En revanche, ce dernier se limitant aux techniques logiques couplées à des actes de malveillances, un référentiel générique complémentaire a été élaboré pour traiter des menaces physiques et scénarios accidentels source de corruption de données.



L'altération et la destruction de données peut être un dommage collatéral à une chaîne d'attaque, voire être l'objectif principal des assaillants au regard de leurs motivations.

Ce document liste des scénarios de corruption de données, en se focalisant sur les vecteurs initiaux de ces chaînes d'attaques.

II. Participants

- Wilfrid GHIDALIA (Forum des Compétence)
- Romain ELIOT (Crédit Agricole SA)
- Emmanuel ZANON (Crédit Agricole SA)
- Carlos GARCIA (Allianz)
- Eddy NABTI (COVEA)
- Mathieu DOIDY (Gras-Savoie)
- Xavier MIGAUD (AG2R La Mondiale)
- Laurence HERROU (IEDOM)
- Jeremy MARTINVILLE (Banque de France)
- Fabien DAVID (Banque de France)

- Jérôme CONSIGNY (AXA)
- Frank VAN CAENEGEM (CNP)
- Lionel SANTAL (CNP)
- Marc DEVALLIER (La Banque Postale)
- Laurent CHAILLEY (Banque de France)
- Xavier PERNOT (Generali)
- Nicolas BURTIN (Generali)
- Alexandre CHOPIN (BNP Paribas)
- Pierre LEDERER (Gras-Savoie)
- Magdalena DERYLO (Forum des Compétence)

Les membres du GT dédient ce présent document à la mémoire de Wilfrid qui a personnellement suivi l'avancement des travaux.

III. Typologie des techniques d'attaques

Les scénarios de corruption de données peuvent s'appuyer sur une multitude de techniques. L'analyse du référentiel MITRE ATT&CK® permet d'identifier un ensemble de techniques susceptibles d'altérer le SI.

Pour gagner en lisibilité, celles-ci ont été regroupées par cible d'attaques :

Typologie de cible d'attaques	Description
Hardware & pré OS	Attaque modifiant des données de Firmware, Bios ou UEFI des systèmes ou de leurs périphériques.
Système	Techniques ciblant toutes les composantes et fonctionnalités avancées d'un système d'exploitation : <ul style="list-style-type: none"> • Tâches planifiées / exécution sur événement, • Librairies, binaires du système, • Système de gestion des process et des services, registre de clés, • Gestion de la mémoire, • Exécution automatique, gestion des comptes systèmes, • Fonctionnalités de développement, • Boot, image système, et outil de restauration ...
Infrastructure	Altération d'éléments d'infrastructure : <ul style="list-style-type: none"> • Progiciel ou suite de développement, • Service BITS (service de transfert intelligent en arrière-plan Windows), • Images de systèmes ou de conteneurs (utilisées par des outils de provisionning automatique de plateforme Cloud ou de Containeur), • Stratégie sécurité de groupe (GPO), • Dispositif de mise à jour des logiciels, • Composants Cloud (instances, virtual machines, and snapshots).
Référentiel des comptes	Manipulation des bases de comptes, des informations d'identification, des propriétés de verrouillage, ou des groupes d'autorisation.
Mesure de sécurité	Corruption des mécanismes de défense (antivirus, firewall personnel...), des capacités de chiffrement (désactivation, manipulation de clés ou de leurs caractéristiques...) , des journaux d'investigation comportant des traces de sécurité, ou des dispositifs d'agrégation et d'analyse d'évènements (SIEM).
Session	Attaques ciblant le dispositif de gestion des sessions : <ul style="list-style-type: none"> • Login et process d'authentification, • script d'initialisation local ou réseau...
Environnement utilisateur	Techniques s'appuyant sur l'altération d'éléments en environnement utilisateur : <ul style="list-style-type: none"> • Site Web intégrant un code malicieux infectant les internautes lors de leur navigation, • Navigateurs altérés (ou leurs modules d'extension), • Documents compromis (intégrant des macros malveillantes), • Usage malicieux de fonctionnalités de la messagerie Outlook (gestion des règles, formulaires, page d'accueil, modules d'extension...), • Clés de registre altérées ...

Introduction

IV. Définition et cadre

La corruption de données (ou altération de données) est la conséquence d'une atteinte à l'intégrité d'un ensemble cohérent de données par l'action d'une ou plusieurs actions accidentelles, ou malveillantes.

Elle peut intervenir durant l'écriture, la lecture, le stockage ou la transmission des données.

La corruption peut être totale (le fichier clients), ou partielle : seuls certains enregistrements (la fiche client de Mr Blanc) ou attributs (toutes les adresses du fichier clients) sont affectés.

L'intégrité peut être atteinte par

- une modification incertaine et non reproductible,
- par l'intermédiaire de fonctions réversibles,
- par perte
- par soustraction de la donnée.

Dans la majeure partie des cas, la conséquence d'une corruption de données est l'impossibilité d'interpréter correctement les données ou l'exécution de programmes modifiés frauduleusement par l'assaillant. Cependant des dispositifs (contrôle d'intégrité, dispositif de scellement ou de cohérence) peuvent être en place pour pallier aux défaillances élémentaires.

L'impact de la corruption de données peut être :

- Temporaire : La réinitialisation du système permet généralement le retour à la situation nominale,
- Persistant : existence d'une copie non corrompue... à l'exception de certains cryptolockers qui affectent également le système de sauvegarde les rendant plus persistant.

La détection d'une corruption de données est détectée soit par les utilisateurs soit par le dispositif de surveillance mis en place (SOC,...). Une fois l'évènement détecté, il est qualifié et peut déclencher l'activation d'une cellule de crise en fonction des impacts.

La corruption de données fait l'objet d'investigations destinées entre autre à qualifier si son origine est accidentelle ou malveillante. Dans ce dernier cas le RSSI est mobilisé.

V. Typologie de corruption accidentelle

Les principales causes de corruption accidentelle de données découlent de la complexité des architectures logicielles actuelles. Historiquement, les composants électroniques pouvaient représenter un point de faiblesse des ressources et provoquer des corruptions de données accidentelles. La technologie physique a progressé (RAID, Code correcteur d'erreur, etc...). Cependant les incidents imputables à une panne du hardware sont encore présents.

1. Défaillance matérielle :

Elle a pour origine une défaillance électronique, une panne mécanique ou une surtension électrique qui affecte tout type de support de stockage (disque dur, clé USB, bandes magnétiques, etc...). Cette défaillance provoque une perte partielle ou totale d'accès aux données.

2. Perte du matériel :

Elle est causée par la perte physique du support du stockage. Les données contenues sur le support sont, par voie de conséquence, perdues.

3. Panne logicielle :

Elle est causée par une défaillance du logiciel (bug) ou de la synchronisation des données (architecture multi-tiers, réplication de données entre 2 sites). Elle provoque une altération ou une perte partielle ou totale de données.

4. Mauvaise manipulation / Mauvaise pratique :

Elle trouve son origine en une mauvaise utilisation liée à une erreur humaine ou à des modes opératoires erronés.

5. Partie Tierce :

Les entreprises déportent une partie de leur SI et services informatiques chez des prestataires (externalisation). Ces prestataires peuvent faire l'objet d'attaques ou de malveillances visant les données qui, par dommage collatérale, peuvent impacter l'entreprise donneuse d'ordre.

VI. Typologie de corruption malveillante

La corruption de données malveillante est multiforme et peut provenir de multiples vecteurs. Elle est catégorisée de manière suivante :

1. Corruption logicielle :

Modification d'un système applicatif par l'ajout de code non légitime. L'objectif est de porter atteinte à l'intégrité du système hébergeur en s'exécutant dans le contexte du système applicatif.

Les conséquences recherchées de cette corruption logicielle peuvent être multiples :

- L'ouverture et le maintien d'accès au système hébergeur (attaque Sunburstⁱ,...),
- L'exfiltration de données (keylogger, copies d'écrans...),
- Le téléchargement, l'exécution et la prolifération de code malveillant (NotPetyaⁱⁱ...)

2. Corruption matérielle :

Altération du fonctionnement nominal d'un équipement matériel :

- Directement par l'intermédiaire d'une mise à jour de firmware (ie EquationDrug ou GrayFishⁱⁱⁱ), d'un driver ou par un code malveillant (stuxnet^{iv}),
- Indirectement (serveurs endommagés suite au déclenchement du système anti incendie).

L'objectif étant de porter atteinte à l'intégrité d'un matériel servant de support à un système applicatif.

Les conséquences recherchées de cette corruption matérielle peuvent être multiples :

- Le détournement de l'usage,
- La génération de désordre,
- La destruction...

3. Corruption d'un référentiel de sécurité :

Atteinte à l'intégrité d'un référentiel de sécurité (annuaire Active Directory, LDAP, ...) en :

- Créant des comptes non légitimes,
- Ajoutant des privilèges à un compte existant,
- Modifiant les attributs de comptes existants (mots de passe, statuts, privilèges, ...)
- Supprimant des comptes.

Elle a pour objectif soit de prendre pied durablement dans le SI, soit d'occasionner la paralysie partielle ou totale d'un SI

La corruption de référentiel de sécurité est fréquemment combinée avec la corruption ou la destruction des systèmes de sauvegarde (ie Ragnar Locker^v) pour accentuer la pression sur la victime.

4. Corruption système :

Altération du fonctionnement nominal d'un système informatique par la modification des programmes de bas niveau (ou de fichiers de configuration) lui permettant de gérer les différentes ressources à sa disposition. Exemple avec la modification de bibliothèques systèmes d'une application (les fichiers DLL d'Internet Explorer par exemple) permettant ensuite d'altérer la mémoire, et par voie de conséquence de modifier certaines données dont l'emplacement est connu ou de faire exécuter des commandes.

5. Corruption des données Métier :

Pour une partie non négligeable de l'économie, la disponibilité et l'intégrité des données métiers sont essentielles au bon fonctionnement de l'entreprise (Banques et assurances, sociétés financières, ...). La corruption de ces données, structurées ou bureautiques, porte un fort préjudice à l'entreprise victime, dégradant ou stoppant ses processus opérationnels le temps que ces données soient à nouveau disponibles. La corruption d'origine malicieuse des données nominales peut également s'accompagner de la corruption des données sur les sauvegardes afin d'augmenter le rapport de force entre le cybercriminel et l'entreprise.

6. Corruption de données volatiles :

Les environnements d'exécution et d'authentification présentent de multiples opportunités de corruption. En effet, les systèmes ou applications exécutent une série de commandes ayant pour objet de personnaliser l'environnement utilisateur : l'altération des commandes exécutées permet d'augmenter le champ des possibles. A titre d'exemple, une faille XSS (pour cross-site scripting^{vi}) permet, en ajoutant des instructions supplémentaires dans une page web, de les faire s'exécuter dans le contexte utilisateur d'un visiteur de cette page. La corruption peut aussi se matérialiser par le vol de session avec des techniques par exemple de « Cookie poisoning » ou « Session Hijacking ^{vii} » permettant de falsifier les cookies de session ou d'altérer la communication entre deux systèmes pour s'insérer dans les échanges et ultimement usurper l'identité d'un des participants.

VII. Motivations principales d'une corruption de données malveillante

Pour l'ANSSI, une cyber-attaque est une atteinte à des systèmes informatiques réalisée dans un but malveillant. Une cyber-attaque peut émaner d'une personne isolée ou d'un groupe organisé. La corruption de données peut être la finalité de la cyber-attaque, ou un dommage collatéral. Une cyber-attaque peut avoir des impacts sur l'image, la stabilité, voire la pérennité de l'entreprise à travers plusieurs objectifs :

1. Pour récupérer illicitement des données :

Il y a dans un premier temps les attaques **à des fins crapuleuses**, pour récupérer des données en vue de les exploiter ou de les revendre. Il peut s'agir de données bancaires, de fichiers clients, d'outils internes, ou d'identifiants de connexion.

2. Pour espionner :

On parle ensuite des attaques **à des fins d'espionnage**, pour capter les informations importantes des entreprises. Ces attaques de cyber-espionnage sont conçues pour le vol de propriété intellectuelle. Elles touchent de plus de plus le secteur industriel.

3. Pour déstabiliser :

Les **attaques à des fins de déstabilisation**, par exemple par le vol d'informations puis leur publication. Ce type de cyber-attaques nuit directement à l'image de marque de l'entreprise touchée. Elle révèle sa défaillance en matière de sécurisation des données et entame la confiance des clients ou des partenaires de l'entreprise victime.

4. Pour saboter :

On notera pour les attaques **à des fins de sabotage**, qu'elles visent à altérer ou à détruire les données d'une entreprise ce qui aura pour conséquence de considérablement ralentir, voire de stopper complètement l'activité ou d'engendrer des pertes importantes.

Description des conséquences d'une corruption de données

VIII. Les macro-scénarios de corruption de données

Les macro-scénarios sont regroupés en 3 catégories :

- L'accident
- La malveillance logique
- La malveillance physique

1. Les scénarios accidentels

Les scénarios accidentels (logique comme physique) ne sont pas couverts par MITRE ATT&CK®. Le GT a, par conséquent, défini sa propre nomenclature pour compléter celle du MITRE ATT&CK®.

Désastre physique

Type	Code	Scénario	ID GT	Description GT
Désastre physique	ADP1	Une défaillance technique déclenche une détonation d'un équipement au sein d'un centre de données qui génère une onde de choc (ex: système d'extinction d'incendie) provoquant un dysfonctionnement des équipements de stockage de données (dysfonctionnement, arrêt et perte de données).	Z0010	Data loss
	ADP2	Une impulsion électromagnétique d'origine externe (impact de foudre, bombe IEM) endommage les installations électriques et/ou génère un champs électromagnétique provoquant la perte de données.	Z0010	Data loss
	ADP3	Lors d'une opération de déménagement de datacenters des supports de stockage sont perdus.	Z0010	Data loss
	ADP4	Un utilisateur branche un dispositif de stockage externe (clés USB, disques durs externes, DVD/CDROM...) qui demeure inerte et n'est pas reconnu par le système. Après vérification, il s'agit d'une défaillance physique entraînant une perte de données.	Z0010	Data loss
	ADP5	Un utilisateur exécute le script de mise à jour du bios fourni par son administrateur. Pendant le processus, la carte mère flashée devient inerte et la puce TPM est rendue inutilisable. Or le chiffrement des données s'appuie sur la puce TPM : les données sur le disque ne peuvent plus être lues.	Z0020	Data unavailable

Mauvaise pratique

Type	Code	Scénario	ID GT	Description
Mauvaise pratique	AMP1	Un technicien introduit un matériel électromagnétique générant un champs magnétique provoquant une altération des supports magnétiques (mauvaise pratique)	Z0010	Data loss
	AMP2	Un technicien met en production une application (ou mise à jour) sans avoir effectué de recette. Suite à un bug non identifié, la mise en production provoque une altération de données (directe ou par effet de bord).	Z0050	Data corrupted
	AMP3	Les équipes techniques réalisent plusieurs migrations successives sur un système de stockage (sens large), aboutissant à une corruption des données ou à une incapacité à restaurer des données	Z0050	Data corrupted
	AMP4	Les équipes techniques réalisent des sauvegardes itératives sans jamais les tester complètement. Elles finissent par devenir incohérentes. L'absence de test de restauration n'a pas permis de détecter la corruption des données.	Z0050	Data corrupted

Mauvaise manipulation

Type	Code	Scénario	ID GT	Description
Mauvaise manipulation	AMM1	Un administrateur exécute une commande système erronée détruisant des données de production (disques durs, partitions, dossiers, fichiers, base de données, index de données).	Z0030	Data erased
	AMM2	Un technicien intervient sur une baie de stockage d'un SAN pour effectuer une maintenance. Il applique par erreur une mauvaise configuration et provoque la perte des données.	Z0030	Data erased
	AMM3	Un technicien disposant de droits légitimes fait une mauvaise manipulation sur la console d'administration provoquant un effacement par erreur d'une forêt OU d'un domaine AD	Z0030	Data erased
	AMM4	Un technicien disposant de droits légitimes fait une mauvaise manipulation sur la console d'administration effectue une mauvaise restauration des données.	Z0030	Data erased
	AMM5	Un technicien intervient pour modifier les flux (ajout ou mise à jour) d'une application. L'application n'est pas correctement arrêtée ce qui provoque une rupture / désynchronisation de la base de données.	Z0050	Data corrupted
	AMM6	Un technicien disposant de droits légitimes effectue une mauvaise manipulation dans la base de données (requête SQL mal forgée) ou sur le serveur applicatif d'un progiciel et provoque une corruption de données.	Z0050	Data corrupted
	AMM7	Un utilisateur lance par erreur le formatage d'un dispositif de stockage ce qui entraîne une perte de données.	Z0030	Data erased

Panne logiciel / logique

Type	Code	Scénario	ID GT	Description
Panne logiciel	APL1	Une application est répartie sur une infrastructure partagée entre deux centres informatiques distants. Un incident technique (perte de serveurs, perte de réseau, perte de lien entre les centres) sur le premiers centre provoque une désynchronisation des SAN avec le 2 ^{ème} centre de données.	Z0040	Data out of sync
	APL2	Un lot de disques durs livrés avec un micrologiciel buggé est installé dans une baie de stockage. Ces disques corrompent silencieusement les données qu'ils stockent sans alerte au niveau de la console du SAN.	Z0050	Data corrupted

Parties tierces

Type	Code	Scénario	ID GT	Description
Partie tierce	APT1	Un fournisseur est victime d'une attaque et voit les données de l'organisation altérée	Z0050	Data corrupted
	APT2	Un opérateur SAAS multi-tenant subit une attaque sur sa base de données, affectant tous ses clients (tenant)	Z0050	Data corrupted
	APT3	Un fournisseur de contenu Web ou de bandeaux publicitaires, intégré au sein de pages d'un site Web de l'organisation, est victime d'une attaque et voit son contenu altéré. Par rebond, l'image de l'organisation est impactée	Z0050	Data corrupted
	APT4	Un fournisseur héberge des données dans un pays étranger. Suite à un incident géopolitique, l'état où réside le fournisseur décide de fermer les flux internet entrant et sortant. L'entreprise n'a plus accès à ses données externalisées chez le fournisseur.	Z0020	Data unavailable
	APT5	Un fournisseur de données financières (scoring, valeurs...) livre un fichier de données financières tronquées ou corrompues provoquant des erreurs dans les traitements métier (back et front office).	Z0050	Data corrupted
	APT6	Un attaquant injecte dans un système de fausses données, ou des données altérées (ex : mauvaise devise pour les opérations financières)	Z0050	Data corrupted

2. Les scénarios de malveillance logique

Les scénarios de malveillance logiques s'appuient sur la nomenclature du MITRE ATT&CK® (version du 27 avril 21).

La couverture jointe en annexe précise dans quel cas la corruption de données est possible et son origine (code couleur).

Les scénarios ci-dessous sont regroupés par origine.

Hardware & pré OS

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Hardware & pré OS	MHO1	Un attaquant prend le contrôle d'un système et installe un rootkit BIOS/UEFI ou un firmware corrompu sur un équipement via une installation physique ou à distance.	T1542	Pre-OS Boot
	MHO2	Un attaquant installe un rootkit BIOS/UEFI ou un firmware corrompu sur un équipement via la corruption d'un firmware dont la signature est usurpée et publiée en ligne, à partir duquel les administrateurs vont faire leur mise à jour.	T1542	Pre-OS Boot
	MHO3	Le démarrage du système est rendu inopérant par l'intermédiaire d'une mise à jour malicieuse du BIOS déjouant les contrôles d'intégrité mis en place par le constructeur et exécutée par l'intermédiaire d'une mise à jour applicative contrefaite (mise à jour ADOBE, CHROME, ...)	T1495	Firmware Corruption

Système

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Système	MSY1	Un attaquant prend la main sur un serveur puis altère ses traces applicatives ou système, dans le but de dissimuler une activité (fraude, cyberattaque).	T1564	Hide Artifacts
	MSY2	Un attaquant injecte un code malveillant sur une des pages d'un site web légitime. Le code malveillant enregistre la frappe et les mouvements à l'écran permettant la récupération d'informations sensibles (moyen de paiement)	T1564	Server Software Component
			T1190	Exploit Public-Facing Application
			T1210	Exploitation of Remote Services
MSY3	Un attaquant exploite une faille de sécurité connue non corrigée lui permettant de réinitialiser le mot de passe administrateur d'un CMS (Content Management Server). Il prend le contrôle du site et modifie à loisir les informations.	T1491	Defacement	
MSY4	Un malware se rend persistant par la création d'un service s'exécutant au démarrage de la machine pour miner de la crypto monnaie	T1569	System Services	

Système	MSY5	Une DLL malveillante portant un nom légitime est chargée dans le système dans un répertoire reconnu. Au lancement du programme, le chemin est modifié pour appeler la DLL corrompue.	T1129	Shared Modules
	MSY6	Un attaquant a pris le contrôle d'un ordonnanceur métier sur les systèmes en production. Il programme une tâche pour se créer un accès persistant	T1053	Scheduled Task/Job
	MSY7	Un attaquant contrôle les logiciels de démarrage d'un PC par l'usage d'un Rootkit et met en place une charge malveillante tout en masquant ses activités. Ce point d'accès corrompu peut permettre des mouvements latéraux dans le SI.	T1014 T1564	Rootkit Hide Artifacts
	MSY8	Par l'intermédiaire d'un mail de phishing, une copie compromise du programme bloc-notes est téléchargée sur le poste de travail est l'association du programme d'exécution modifiée en conséquence dans le registre. Lors de la prochaine ouverture d'un fichier texte, le bloc note compromis sera exécuté, libérant ainsi la charge malicieuse.	T1546	Event Triggered Execution
	MSY9	L'exécution d'un programme malveillant par un usager altère les entrées de démarrage automatique de la base de registre du système, dans l'objectif de persister dans celui-ci tout en maintenant des privilèges élevés.	T1547	Boot or Logon Autostart Execution
	MSY10	Après avoir corrompu une plate-forme centralisant les ressources logicielles de référence d'une entreprise, des binaires et bibliothèques altérés sont déployés sur des serveurs afin de tirer parti de leur puissance de calcul dans le cadre d'une mission frauduleuse de minage de cryptomonnaie.	T1554	Compromise Client Software Binary
	MSY11	L'altération d'un agent logiciel vulnérable sur un poste de travail exécuté sous une forme de service Windows, contribue à la réalisation d'une opération malveillante, de façon persistante y compris après des reboots de la machine.	T1543	Create or Modify System Process
	MSY12	L'attaquant modifie le chemin des logs des serveurs et des postes de travail pour corrompre les traces permettant la détection d'une attaque, ainsi que l'identification de malwares ou de virus.	T1070	Indicator Removal on Host
	MSY13	Un attaquant s'introduit sur un poste de travail et se sert du protocole SMB pour transférer du code malveillant et pour inonder l'attaque sur d'autres sites.	T1570	Lateral Tool Transfer
	MSY14	Un attaquant installe son code malveillant sur la DLL GINA puis récupère les comptes et mots de passe de tous les utilisateurs de l'entreprise qui se sont connectés.	T1556	Modify Authentication Process
	MSY15	Un utilisateur surfe sur internet et récupère un code malveillant qui s'exécute et supprime des informations sur la base de registre pour se dissimuler.	T1112	Modify Registry
	MSY16	Un attaquant modifie l'image du firmware des routeurs afin de récolter les données transitant par celui-ci et les envoyer vers un site externe.	T1601	Modify System Image
	MSY17	Suite à son licenciement, un administrateur dépose une bombe logique dans le SI pour se venger. Elle se déclenche après son départ. Elle corrompt les données de production et les sauvegardes.	T1078 T1124	System Service Discovery Valid Accounts

Infrastructure

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Infrastructure	MIF1	Suite à l'observation du fonctionnement du système, un attaquant pollue (infection ou modification) une base de données nécessaire au fonctionnement d'une Intelligence Artificielle pour en changer le comportement et influencer sur les résultats/prise de décision du métier qui en découle à son avantage.	T1565	Data Manipulation
	MIF2	Un attaquant prend pied dans le SI. Il détourne les protocoles réseau pour dérouter les flux sur une infrastructure qu'il contrôle (ARP poisoning, TCP hijacking)	T1557	Man-in-the-Middle
	MIF3	Un attaquant prend pied dans le SI et altère les tables de routage pour rerouter un trafic réseau (DNS Spoofing, Pharming/DNS cache poisoning) vers une infrastructure qu'il contrôle.	T1557.001	LLMNR/NBT-NS Poisoning and SMB Relay
	MIF4	Un exploitant informatique modifie la liste de transactions bancaires (ajout d'opérations, modification des bénéficiaires...), par abus de droits, directement auprès des applications internes spécialisées ou dans les tables de bases de données afin de détourner des fonds.	T1565	Data Manipulation
	MIF5	Un attaquant prend le contrôle de l'outil de déploiement de l'entreprise. L'attaquant crée un compte administrateur sur chaque poste local.	T1072	Software Deployment Tools
	MIF6	Dans le cadre d'une attaque plus globale, et suite à la compromission d'une compte d'administration de l'AD, une GPO est modifiée pour abaisser le niveau de traçabilité des opérations réalisées sur les systèmes du domaine Active Directory et réduire la période de rétention à quelques secondes.	T1484	Domain Policy Modification
	MIF7	Un utilisateur est infecté par un code malveillant en surfant sur Internet, dont la charge utile est téléchargée sur son poste de façon transparente, en s'appuyant sur le service BITS de Windows permettant le transfert de données en arrière-plan.	T1197	BITS Jobs
	MIF8	Un attaquant modifie un Master sur le Cloud pour introduire un nouveau compte d'admin ou un code malveillant pour ensuite voler des données ou chiffrer les serveurs ou les postes de travail quand il le souhaite.	T1525	Implant Container Image
	MIF9	Un attaquant installe une porte dérobée dans la partie système des machines virtuelles sur des infrastructures Cloud accessible par l'utilisateur au moyen d'un code malveillant ou de droits d'administration	T1578	Modify Cloud Compute Infrastructure

Système et infrastructure

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Système / Infrastructure	MSI1	Un attaquant prend pied sur un serveur et réalise des opérations malveillantes. Au terme de son action, il génère un incident de production pour forcer la restauration d'une version de la base de données antérieure ne comportant pas de trace des actions illégitimes.	T1485 T1564	Data Destruction Hide Artifacts
	MSI2	Un attaquant désactive / détruit les fonctionnalités de récupération de données altérant voire rendant impossible leur restauration.	T1490 T1485 T1486	Inhibit System Recovery Data Destruction Data Encrypted for Impact
	MSI3	Un malware corrompt un système de sauvegarde et le système primaire	T1490 T1485 T1486	Inhibit System Recovery Data Destruction Data Encrypted for Impact
	MSI4	Un utilisateur reçoit un mail de phishing, clique sur un lien le dirigeant vers un site web malveillant pour télécharger un ransomware, qui chiffre l'intégralité de ses données sur son poste et les partages bureautiques auxquels il a accès	T1486	Data Encrypted for Impact
	MSI5	Un code malveillant se propage sur le réseau à l'aide d'un compte valide en ciblant exclusivement les machines serveurs. Le malware utilise des fonctions d'accès direct au disque pour dans un premier temps corrompre aléatoirement et progressivement des fractions limitées des disques (et ainsi permettre sa latéralisation sans donner l'alerte), puis en altérant sa structure.	T1561	Disk Wipe
	MSI6	Un attaquant modifie les droits d'accès contenus dans le DACL de Windows afin d'accéder aux fichiers/répertoires protégés et établir une persistance d'accès.	T1222	File and Directory Permissions Modification

Référentiel des comptes

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Référentiel des comptes	MRC1	Un attaquant prend le contrôle d'un poste de travail et élève ses droits pour en devenir administrateur local. Après avoir exploré le SI et collecté des mots de passe, l'attaquant prend le contrôle d'autres postes de travail et serveurs. Il analyse et exploite les failles de l'AD pour prendre le contrôle des émissions de ticket Kerberos.	T1558	Steal or Forge Kerberos Tickets
	MRC2	Un attaquant injecte un code SQL (SQL Injection ou par abus de droits SGBD), pour modifier des tables de données stockant des authentifiants et se créer un compte permanent.	T1098 T1136	Account Manipulation Create Account
	MRC3	Un attaquant, après avoir acquis des tables de comptes et de mots de passe parvient à entrer dans le SI via un compte légitime. Il en modifie le mot de passe afin de prendre le contrôle dudit compte ou d'envisager une attaque sur un dispositif 2FA.	T1098	Account Manipulation
	MRC4	Un attaquant, après avoir eu accès à des informations secrètes, génère ses propres informations d'identification pour accéder aux ressources SI exposées sur Internet.	T1606	Forge Web Credentials
	MRC5	Via un programme malveillant exécuté par l'utilisateur d'un système, une vulnérabilité d'exécution arbitraire par le noyau est exploitée permettant d'obtenir des tickets d'authentification légitimes persistants.	T1212	Exploitation for Credential Access
	MRC6	Un code malveillant corrompt un système d'exploitation, puis tente de s'étendre sur le réseau d'entreprise, après avoir élevé ses privilèges locaux en manipulant et usurpant les contextes de sécurité des processus systèmes Windows (access token).	T1134	Access Token Manipulation
	MRC7	La base des comptes utilisateur légitimes est altérée pour ne conserver que des comptes compromis, les autres étant verrouillés ou détruits, provoquant une paralysie du système.	T1531	Account Access Removal

Mesure de sécurité

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Mesure de sécurité	MMS1	Un attaquant prend le contrôle d'un élément de chiffrement réseau (VPN, outil d'administration de chiffrement...) en exploitant les techniques d'élévation de privilège, ce qui permet de dégrader le protocole de chiffrement utilisé afin de pouvoir dérober les données échangées.	T1600	Weaken Encryption
	MMS2	Un code malveillant désactive les copies de sauvegardes des données bureautiques (Shadow Copies) et écrase les instances existantes avant de chiffrer les fichiers bureautiques accessibles.	T1562	Impair Defenses

Environnement utilisateur

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Environnement utilisateur	MEU1	Un attaquant exploite une vulnérabilité d'une API exposée sur Internet afin d'établir un canal d'accès illégitime.	T1190	Exploit Public-Facing Application
	MEU2	Un attaquant envoie un spearphishing avec un document office modifié avec un lien vers un site extérieur. A son ouverture, le document télécharge une charge malveillante qui se déclenche sur le poste de l'utilisateur et sur les serveurs dont il a accès.	T1221	Template Injection
	MEU3	Un site d'actualités affinitaire est compromis et un script recherchant la présence d'un nombre réduit et identifié de vulnérabilités est systématiquement exécuté lors de la connexion des visiteurs. Lorsque qu'une des vulnérabilités est présente via le browser de l'utilisateur, elle est exploitée dans le but d'obtenir un accès à la machine du visiteur.	T1189	Drive-by Compromise
	MEU4	Un utilisateur installe une extension à son navigateur Web, alléché par les fonctionnalités innovantes promues par celle-ci, et altère l'intégrité de son système, qui lui affiche à l'écran des publicités intempestives et qui exfiltre les mots de passe, les cookies stockés dans son navigateur, ainsi que les adresses Web consultées.	T1176	Browser Extensions
	MEU5	Un attaquant envoie un mail avec un fichier Excel avec une macro contenant du code malveillant. A l'ouverture du fichier, le code ajoute une macro complémentaire pour maintenir sa persistance à chaque ouverture d'Excel.	T1137	Office Application Startup

Infrastructure et environnement utilisateur

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Infrastructure / environnement utilisateur	MIU1	Un attaquant envoie un spearphishing avec un document office malveillant comportant un ver. A son ouverture, le malware remplace des fichiers office sur les partages réseaux avec son propre contenu pour se propager sur les postes des utilisateurs qui ouvriront ce fichier.	T1080	Taint Shared Content

Systeme et Session

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Systeme / Session	MSS1	Un serveur assure une persistance dans un système, en altérant un script de logon.	T1037	Boot or Logon Initialization Scripts

Toutes origines possibles

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Toutes origines possibles	MTO1	Un attaquant ajoute un code malveillant au code d'une application mobile légitime et publie cette nouvelle version sur le store d'applications. Un utilisateur télécharge la nouvelle version : ses données sont aspirées par l'attaquant.	T1195.002	Compromise Software Supply Chain
	MTO2	Un attaquant injecte un code malveillant dans une nouvelle version légitime d'un logiciel. La mise à jour s'effectue de façon automatique à l'insu des exploitants.	T1195.002	Compromise Software Supply Chain
	MTO3	Un attaquant injecte un code malveillant dans un code source non protégé et non sauvegardé. Outre la charge malveillante, l'entreprise perd également l'intégrité du code initial.	T1195	Supply Chain Compromise
	MTO4	Un attaquant injecte un code malveillant dans le binaire d'une application portable et la diffuse aux utilisateurs. L'application est exécutée de façon autonome sans besoin d'élévation de privilège.	T1195	Supply Chain Compromise
	MTO5	Un attaquant injecte un code malveillant dans des développements internes qui sont ensuite déployés dans l'entreprise.	T1195.002	Compromise Software Supply Chain
	MTO6	Un attaquant prend le contrôle sur le système de gestion de code source de l'entreprise (ex: github / gitlab, Visual SourceSafe) ce qui lui permet d'injecter du code malveillant dans les applications.	T1195.002	Compromise Software Supply Chain
	MTO7	Un poste corrompu par un malware dont la fonction est de déverser une charge malveillante dès connexion de support amovible. Les supports amovibles deviennent à leurs tours corrompus.	T1091	Replication Through Removable Media

3. Scénario de malveillance physique

Les scénarios de malveillance physique ne sont pas couverts par MITRE ATT&CK®. Le GT a, par conséquent, défini sa propre nomenclature.

Type	Code	Scénario	ID GT	Description GT
Malveillance physique	MPH1	Un technicien (interne ou externe) ayant accès à une zone protégée vole des disques durs au sein d'une baie de stockage.		Perte de données

IX. Conséquences

1. Impacts financiers

La valorisation des scénarios de risque cyber s'appuie sur la valorisation de 2 **familles de coûts** :

- Coûts de traitement de la crise,
- Coûts métier.

Ces familles de postes de coût sont-elles même subdivisées en **postes de coûts**. Le tableau de synthèse ci-dessous donne une vue d'ensemble du modèle :

Intitulé des postes de coûts	
Coûts de traitement de la crise	P1 - Frais d'expertise IT des systèmes endommagés 1.1 – Mobilisation cellule(s) de crise (coûts interne) 1.2 – Investigation numérique (coûts externes) 1.3 – Remise à niveau SSI 1.4 – Coûts complémentaires SSI
	P2 - Frais de notification et de communication liés à la violation de données à caractère personnel 2.1 – Notification des collaborateurs 2.2 – Notification des clients 2.3 – Communication externe
	P3 - Frais de gestion commerciale 3.1 - Prise en charge des réclamations 3.2 – Prise en compte des gestes commerciaux 3.3 – Dédommagement agents/partenaires
	P4 - Frais juridiques & règlementaires 4.1 – Charge interne de réalisation d'une enquête 4.2 – Frais d'avocat 4.3 – Dommages & intérêts clients 4.4 – Amendes (Solvency II, RGPD, OSE, ...)
Coûts métier	P5 - Frais opérationnels de gestion de renforts 5.1 – Renfort interne 5.2 – Renfort externe
	P6 - Manque à gagner 6.1 – Perte « sur portefeuille » : - IARD Sinistre - processus dommages & responsabilités : particuliers, pros, entreprises - Prévoyance 6.2 – Perte « sur flux » : - Flux clients/ prospects (canal web) - Flux clients/ prospects (canaux tel/web/agences)
	P7 – autres coûts 7.1 - Heures travaillées perdues (du fait de l'indisponibilité des ressources SI)

- postes de coûts utilisés pour le cycle 2019-20 -

Ces postes de coût représentent des impacts financiers bruts associés aux scénarios Cyber étudiés, tels qu'ils pourront être provisionnés lors de la déclaration d'incident du risque opérationnel. Les corruptions de données ne sont pas forcément instantanées. Le temps de détection et de réaction influe sur l'impact.

Aussi, cette valorisation est généralement revue lors d'une étape postérieure à la crise, pour évaluer « l'impact net » n'intégrant que les éléments réels ou ayant permis de réduire des coûts (assurances). Sur le plan comptable, celle-ci pourra permettre de réaliser des reprises sur provision.

Les principaux postes de coûts peuvent fortement varier en fonction des incidents et de leurs impacts :

- **Sanction publique ou non** exemple Amende RGPD (frais juridiques & réglementaires – poste P4)
- Manque à gagner sur **flux prospects ou clients** (poste P6)
- **Heures** travaillées **perdues** (poste P7)

Il convient également d'ajouter à ces coûts, les coûts liés au traitement de la crise :

- Frais d'expertise des systèmes endommagés – « forensics » - (poste P1)
- Frais de notification et de communication (poste P2)
- Frais de gestion commerciale (poste P3)
- Coûts induits de non-respect des délais contractuels
- Temps passé à reconstruire des fichiers corrompus
- Charges induites pour le nettoyage des données
- Délai nécessaire au lancement de plusieurs batchs

2. Impacts d'image

En cas de cyberattaque, la réputation de l'entreprise ne sera pas épargnée. Il sera pertinent d'anticiper et d'intégrer ces risques aux dispositifs de communication de crise.

1. Atteinte à l'Image de l'entreprise :

La réputation d'une entreprise, qui est construite sur de nombreuses années d'efforts et de valorisations, peut être facilement menacée par des comportements imprévisibles et sournois, à la limite de la légalité ou voir totalement illégaux, mis en œuvre pour attaquer la crédibilité de l'entreprise.

Dans le monde de la finance, l'image de l'entreprise est liée à la fiabilité, à la disponibilité du SI et à l'intégrité des données.

2. E-réputation (Wikipedia):

L'**e-réputation**, parfois appelée **web-réputation**, **cyber-réputation**, **réputation numérique, sur le Web, sur Internet** ou **en ligne**, est l'opinion commune (informations, avis, échanges, commentaires, rumeurs...) sur le Web d'une entité (marque), personne morale (entreprise) ou physique (particulier), réelle (représentée par un nom ou un pseudonyme) ou imaginaire. Elle correspond à l'identité de cette marque ou de cette personne associée à la perception que les internautes s'en font.

Cette notoriété numérique, qui peut constituer un facteur de différenciation et présenter un avantage concurrentiel dans le cas des marques, se façonne par la mise en place d'éléments positifs et la surveillance des éléments négatifs. L'e-réputation peut aussi désigner sa gestion, via une stratégie globale et grâce à des outils spécifiques (activité à l'origine de nouveaux métiers) pour la pérennité de l'identité numérique.

Pour évaluer un préjudice d'image, cela reste une tâche difficile. Bien souvent, ces préjudices d'image sont réparés par l'allocation de dommages et intérêts symboliques qui ne couvrent que partiellement le dommage subi. Difficile ne veut pas dire impossible et, dans certains cas, les tribunaux allouent des sommes conséquentes pour réparer ces préjudices.

Pour obtenir une juste réparation de ces préjudices immatériels, il faut :

- Être en mesure d'explicitier le rôle et les incidences de l'image et de la réputation pour l'entreprise.
- Démontrer l'existence d'un préjudice d'image et évaluer son étendue, en construisant un modèle permettant d'évaluer la valeur économique que représente l'image de l'entreprise et la perte de valeur engendrée par les actes litigieux.

L'indemnisation des dommages économiques subis par les entreprises se fait par l'intervention d'experts financiers, et d'experts de justice.

Remarque : le préjudice d'image ou de réputation reste mal reconnu, et mal indemnisé. Les propositions d'évaluation de ce préjudice sont difficiles à appréhender.

3. Impacts réglementaires

Une corruption de données peut entraîner une non-conformité réglementaire et exposer sa victime à un risque de sanction (remise en cause d'agrément, interdiction d'exercer, sanctions financières, ou pénales).

Protection des données

Dans un contexte d'accroissement des menaces, les dernières réglementations (NIS, RGPD, Arrêté du 3 novembre 2014...) ont poussé les entreprises à renforcer la sécurité et la résilience de leurs systèmes d'informations, et la protection de leurs données.

Les menaces évoluent vers la chaîne de sous-traitance et les acteurs majeurs du numérique. Les futures réglementations renforceront notamment les exigences pour faire face à ces dernières.

Des bonnes pratiques ont émergé et contribuent à l'atteinte des objectifs de sécurité et de continuité d'activité que se sont fixés les entreprises afin de maîtriser leurs risques.

X. Bonnes pratique en matière de résilience

Il est essentiel pour toute entreprise de disposer d'un système d'information résilient en cas de cyberattaque afin de s'assurer de l'intégrité des données et de sa disponibilité.

Cette résilience peut s'opérer à travers :

- **Des moyens IT :**
 - **Des sauvegardes (et des bonnes pratiques) :**
Elles doivent être en permanence surveillées, supervisées et contrôlées périodiquement.
Il est conseillé de les tester périodiquement (ex : chaque année). La robustesse (capacité, disponibilité, performance) du processus de restauration est essentielle dans le traitement des crises portant atteinte à l'intégrité et à la disponibilité des données.
 - **Un « jeu de recours » :**
Il est conseillé d'avoir des sauvegardes à froid déconnectées du réseau de l'entreprise (air-gapped). Celles-ci ne couvrent généralement pas la totalité des activités des organisations, mais se limitent sur aux processus, activités et données critiques.
- **Des processus :**
 - **Le PCA :**
Il va permettre la continuité d'activité sans perte de donnée et rétablir l'accès aux applications et aux données de l'entreprise
 - **Le PRA :**
C'est un Plan de Reprise d'Activité qui va permettre une bascule sur un site distant et mettre à disposition les applications et données de l'entreprise. Il est opportun qu'il soit testé périodiquement (ex : chaque année)

ANNEXE 1 Couverture par le MITRE ATT&CK®

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (12)	Boot or Logon Autostart Execution (12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Daofuscatw/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Scheduled Task/Job (6)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Displacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)		Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (7)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (2)
				Hijack Execution Flow (11)	Scheduled Task/Job (6)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Data Staged (2)	Non-Standard Port		Resource Hijacking
				Implant Container Image	Valid Accounts (4)	Impair Defenses (7)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (3)	Protocol Tunneling		Service Stop
				Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (4)	Proxy (4)		System Shutdown/Reboot
				Pre-OS Boot (5)		Indirect Command Execution	Unsecured Credentials (6)	Permission Groups Discovery (3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (6)		Masquerading (6)		Process Discovery		Man-in-the-Middle (2)	Traffic Signaling (1)		
				Server Software Component (3)		Modify Authentication Process (4)		Query Registry		Screen Capture	Web Service (3)		
				Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)		Remote System Discovery		Video Capture			
				Valid Accounts (4)		Modify Registry		Software Discovery (1)					
						Modify System Image (2)		System Information Discovery					
						Network Boundary Bridging (1)		System Network Configuration Discovery					
						Obfuscated Files or Information (5)		System Network Connections Discovery					
						Pre-OS Boot (5)		System Owner/User Discovery					
						Process Injection (11)		System Service Discovery					
						Rogue Domain Controller		System Time Discovery					
						Rootkit		Virtualization/Sandbox Evasion (3)					
						Signed Binary Proxy Execution (1)							
						Signed Script Proxy Execution (1)							
						Subvert Trust Controls (4)							
						Template Injection							
						Traffic Signaling (1)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							

Typologies

- Hardware & pré OS
- Système
- Infrastructure
- Référentiel des comptes
- Mesure de sécurité
- Session
- Environnement utilisateur
- Tous

ANNEXE 2
Références bibliographiques

ⁱ Sunburst (SolarWind)

https://fr.wikipedia.org/wiki/Cyberattaque_de_2020_contre_les_%C3%89tats-Unis

ⁱⁱ Notpetya :

https://fr.wikipedia.org/wiki/Cyberattaque_NotPetya

ⁱⁱⁱ EquationDrug et GrayFish :

https://fr.wikipedia.org/wiki/Equation_Group

^{iv} Stuxnet :

<https://fr.wikipedia.org/wiki/Stuxnet>

^v Ragnar Locker :

<https://www.lemondeinformatique.fr/actualites/lire-ragnar-locker-un-ransomware-camoufle-en-machine-virtuelle-79185.html>

<https://www.pcrisk.fr/guides-de-suppression/9587-ragnar-locker-ransomware>

<https://www.silicon.fr/ragnar-ransomware-vm-340269.html>

^{vi} Cross-site scripting

https://fr.wikipedia.org/wiki/Cross-site_scripting

^{vii} Cookie Poisoning ou Session Hijacking :

https://en.wikipedia.org/wiki/Session_hijacking