LOGICIELS RANÇONNEURS : MENACES, RISQUES ET CONTRÔLES

J.-M. KUBEK & É. CARAYOL

23 MAI 2017

Contexte relatif aux logiciels rançonneurs ; présentation des menaces associées, étude de risques et mesures préconisées en cas de non-acceptation de ces risques.

Guide de lecture Le résumé opérationnel s'adresse plus particulièrement aux instances de décision, le contexte et l'étude aux personnes intéressées par une analyse des logiciels de rançon, la présentation des mesures envisageables est destinée aux personnels du service en charge du numérique.

Résumé opérationnel (TL ;DR)

Lors du W.-E. des 13 et 14 mai 2017[1], [2] de nombreux médias ont rapporté l'existence et les dommages créés par un logiciel de rançon, dénommé `WannaCry`. Ciblant les environnements `Windows`, ce logiciel s'est rapidement répandu dans de nombreux pays en affectant la bonne marche de plusieurs entreprises importantes et sans doute de nombreuses autres, plus petites, ou de particuliers.

1. Cert-FR. *Propagation d'un rançongiciel exploitant les vulnérabilités MS17-010*. Mai 2017. URL : `http://www.cert.ssi.gouv.fr/site/CERTFR-2017-ALE-010/index.html`.
2. Microsoft. *Customer Guidance for WannaCrypt attacks*. Mai 2017. URL : `https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/`.

Ransomware : Logiciel de rançon ou logiciel rançonneur parfois contracté en rançongiciel.

La propagation du virus `WannaCry` sous sa forme actuelle semble stoppée mais l'on peut sans doute s'attendre à la création de multiples versions alternatives qui constitueront elles-mêmes rapidement un danger.

Ver (Worm) : Programme malveillant pouvant se propager de manière autonome en exploitant les vulnérabilités d'un autre logiciel

Les logiciels de rançon ne sont pas une source de menace récente malgré ce que pourrait laisser croire l'exposition médiatique de `WannaCry`. Ces logiciels sont apparus au début de la décennie et différentes générations se sont répandues depuis cette date (cf tableau 1 à la page 8). On peut alors tenter d'expliquer la popularité de `WannaCry` par les particularités suivantes :

— il peut se propager de manière autonome, alors que la diffusion des générations précédentes de ransomwares nécessitait des actions volontaires des utilisateurs (activations de pièces jointes dans la messagerie, accès inconsidérés à des fichiers internet) ;

— il utilise un moteur de recherche de vulnérabilités subtilisé à l'agence U.S. du renseignement (National Security Agency (nsa)).

— il s'attaque, entre autres, à d'anciens systèmes dont l'utilisation est toujours répandue Windows XP mais qui ne bénéficient plus de mises à jour de sécurité de la part du fabricant (MicroSoft).

Du point de vue de l'établissement, indépendamment de la réputation[3] du virus en cause, la possibilité de dissémination en mode autonome des logiciels de rançon constitue une menace dont les conséquences pourraient être graves :

1. l'exploitation d'une vulnérabilité présente sur de nombreux postes de travail ou serveurs pourraient rapidement rendre indisponibles un volume important de données ;

3. Cert-FR. *Campagne de messages électroniques non sollicités de type Jaff*. Mai 2017. URL : `http://www.cert.ssi.gouv.fr/site/CERTFR-2017-ALE-011.pdf`.

2. Le paiement effectif de la rançon ne garantit pas que les criminels fourniront effectivement en échange les moyens de retrouver un accès au données.
3. l'indisponibilité définitive des données entraînerait alors, avec certitude, des situations de blocage d'activités pouvant porter préjudice aux intérêts de l'établissement, de ses personnels ou de ses partenaires.

Mesures de sécurité : mesures techniques ou organisationnelles permettant de diminuer la gravité d'un risque en *prévenant*, *en détectant*, ou *en répondant à* un évènement redouté

LE PROPOS DE CETTE NOTE PUBLIQUE EST d'exposer les principales menaces associées aux ransomwares, les risques qu'ils font courir à l'établissement ainsi que les mesures qui permettent de réduire ces risques. Cette note ne contient donc aucune information relative à la situation de l'établissement ou de ses composantes vis-à-vis de ces risques ou de ces mesures.

CERTAINES DES MESURES PRÉSENTÉES PEUVENT MODIFIER les habitudes de travail des utilisateurs, d'autres peuvent nécessiter l'acquisition de nouveaux matériels ou logiciels et donc demander des efforts supplémentaires en exploitation. Les décisions relatives à la mise en place effective de ces mesures devraient donc être prises dans le cadre d'une évaluation mettant en regard le désir de prise de risque de l'établissement d'une part et l'effort de mise en œuvre des mesures d'autre part.

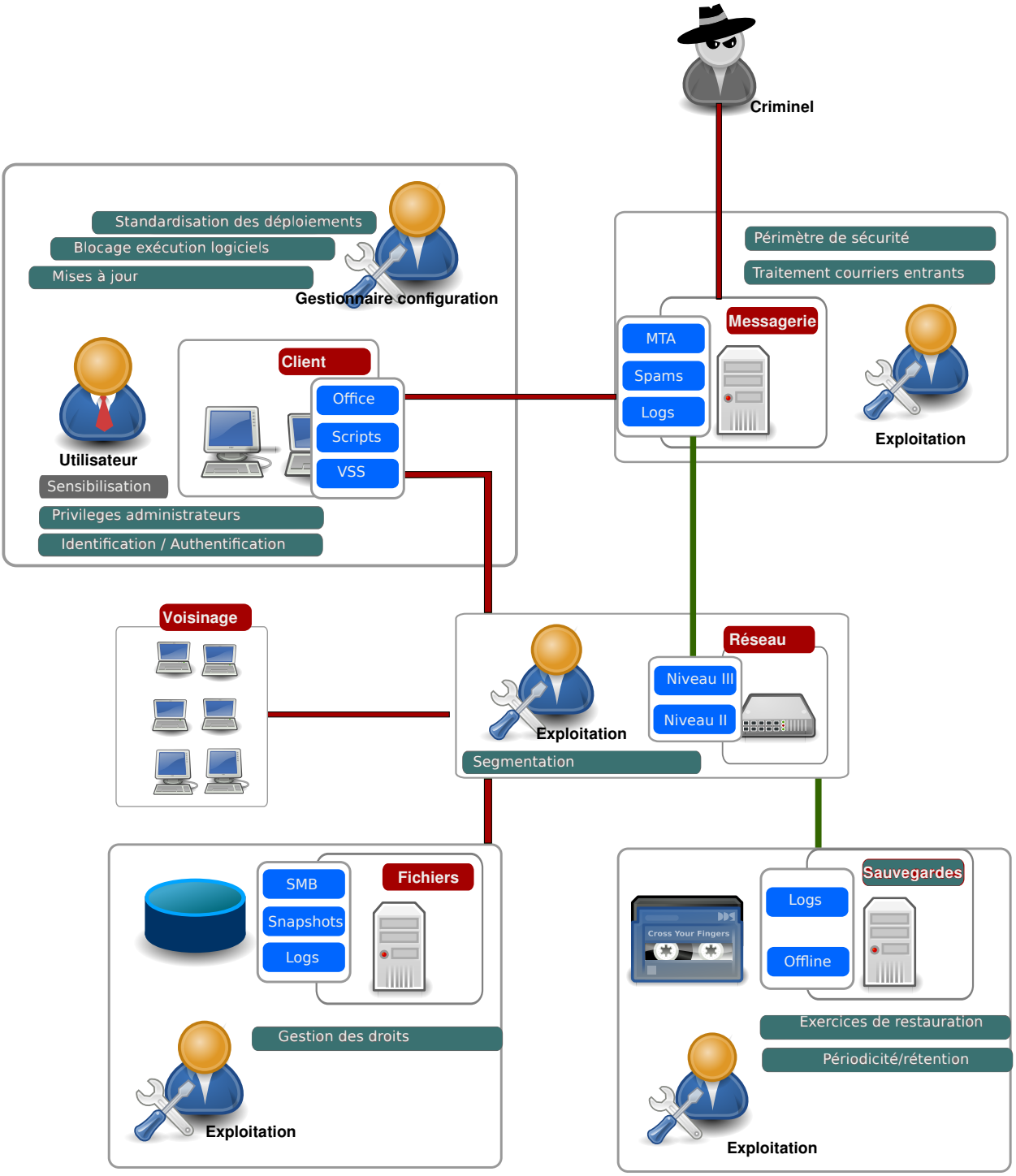

FIGURE 1 – Technologies et Rôles impliqués dans l'étude de risque relative aux ransomwares. Les canaux de communication en rouge explicitent les moyens qui peuvent être utilisés pour rendre indisponibles les données : Criminel – serveur de messagerie ; serveur de messagerie – poste de travail ; poste de travail – serveur de fichier

Acronymes utilisés

ADW (ADW) Application Directory Whitelisting. 17
DKIM (DKIM) DomainKeys Identified Mail. 14
DMARC (DMARC) Domain-based Message Authentication. 14
DNS (DNS) Domain Name Service. 14
ESR (ESR) Enseignement supérieur recherche. 13
IP (IP) Internet Protocol. 15
MBR (MBR) Master Boot Record. 17
NSA (NSA) National Security Agency. 1
SMS (SMS) Short Message Service. 8, 10
SPF (SPF) Sender Policy Framework. 14
USB (USB) Universal Serial Bus. 9
VBS (VBS) Visual Basic Script. 14
VPN (VPN) Réseau Privé Virtuel. 15
VSS (VSS) Volume Shadow Copy. 9, 18
WSH (WSH) Windows Scripting Host. 14

Types de fichiers mentionnés

.7z .7z sur Wikipédia. 14
.bas .bas sur Wikipédia. 14
.bat .bat sur Wikipédia. 14
.chm .chm sur Wikipédia. 14
.cmd .cmd sur Wikipédia. 14
.com .com sur Wikipédia. 14
.doc .doc sur Wikipédia. 11
.docm .docm sur Wikipédia. 11
.docx .docx sur Wikipédia. 11
.dot .dot sur Wikipédia. 11
.exe .exe sur Wikipédia. 11, 14
.hta .hta sur Wikipédia. 14
.jar .jar sur Wikipédia. 14
.js .js sur Wikipédia. 11, 14
.jse .jse sur Wikipédia. 14
.lnk .lnk sur Wikipédia. 14
.msi .msi sur Wikipédia. 14
.pdf .pdf sur Wikipédia. 11
.pdf.js .pdf.js sur Wikipédia. 11
.ps1 .ps1 sur Wikipédia. 11
.pse .pse sur Wikipédia. 14
.rar .rar sur Wikipédia. 11, 14
.scf .scf sur Wikipédia. 14
.scr .scr sur Wikipédia. 14
.vb .vb sur Wikipédia. 14
.vbe .vbe sur Wikipédia. 14
.vbs .vbs sur Wikipédia. 11, 14
.ws .ws sur Wikipédia. 14
.wsf .wsf sur Wikipédia. 11, 14
.xls .xls sur Wikipédia. 11
.xslx .xlsx sur Wikipédia. 11
.zip .zip sur Wikipédia. 11, 14
.zipx .zipx sur Wikipédia. 14

Produits

`Android` Famille de système d'exploitation pour smartphones de Google. 10, 12

`Apple iStore` Boutique dématérialisée d'Apple. 8, 10

`Applocker` Utilitaire de gestion des droits d'exécution de programmes sur les plates-formes `windows`. 14

`Browlock` Logiciel rançonneur. 8

`Explorateur windows` Gestionnaire de fichiers des environnements windows. 14
`Gnu/Linux` Famille de système d'exploitation sous licence GPL. 10, 12
`MacOS` Famille de système d'exploitation équipant les ordinateurs de marque Apple. 10
`Notepad` Éditeur de fichiers texte intégré aux plate-formes windows. 14
`PowerShell` Environnement d'exécution de programmes de script. 14
`WannaCry` Logiciel rançonneur. 1, 10
`Windows` Famille de système d'exploitation Microsoft. 1, 10, 12
`Wordpad` Éditeur permettant une mise en forme minimale de documents intégré aux plates formes windows. 14
bitcoin Monnaie numérique. 10
botnet Réseau d'ordinateurs piratés sous le contrôle de criminels. 11, 15
clients de messagerie Logiciels clients de messagerie. 15
Flash (Adobe) Lecteur multimédia propriétaire. 15
Java (Oracle) Environnement d'exécution d'application. 15
Javascript Langage de programmation initialement conçu pour le web. 14
navigateurs web Logiciels permettant d'utiliser des serveurs web. 15
Office Applications dites de productivité : traitements de texte ; tableurs ; présentations ; bases de données. 14
Silverlight Environnement propriétaire Microsoft de publication d'applications web. 15
snapshot Historique de système de gestion de fichiers. 18
visualbasicscript Langage de script conçu pour la création d'applications Web en sous environnement Windows. 14
Windows XP Versions de l'environnement Windows commercialisée à partir de 2001 ; non supportées depuis 2014. 1

Entreprises mentionnées

Amazon Amazon. 8, 10
MicroSoft Microsoft. 1, 10
Paysafe Paysafe. 8
Ukash Ukash. 8

Table des matières

Introduction

LES LOGICIELS DE RANÇON sont des programmes malveillants qui empêchent l'accès aux données stockées sur un ordinateur et bloquent toute tentative de retour à une situation normale tant qu'une rançon n'a pas été payée par la victime.
Pour communiquer avec la victime, le logiciel, installé sur l'ordinateur, affiche à l'écran un message d'information sur le blocage du système et invite l'utilisateur à verser une somme d'argent sur un compte dématérialisé.

LES RANSOMWARES MODERNES rendent inaccessibles les données en les chiffrant. Le résultat de ce traitement rends illisible ces données et la complexité des algorithmes utilisés ne permet pas d'envisager leur décryptage .

> La seule solution permettant de récupérer les données repose donc sur la restauration d'une sauvegarde préalable.

Chiffrer transformer un message clair en message incompréhensible afin d'assurer la confidentialité de son contenu
Décrypter Obtenir un message en clair sans être en possession du code (clef) de chiffrement/déchiffrement
Déchiffrer utiliser une clef (ou un code) pour transformer un message chiffré en message clair

La plupart des ransomwares actuels chiffrent aussi bien les données des disques locaux que celles des disques distants (partages réseaux) auxquels ils ont accès. Les dégâts de ce type de logiciel peuvent donc être importants lorsque les espaces disques sont partagés sans précaution au sein d'une organisation.
Les grandes lignes de défense suivantes permettent de minimiser les risques ou les dégâts liés à l'installation d'un ransomware :

- mesures contre le vecteur d'attaque ; blocage à la périphérie des pourriels, utilisation contrôlée des macros ou des scripts contenus dans les documents office et la gestion des correctifs (patch) systèmes ou applicatifs ;
- contrôle et limitation des possibilités de communication des équipements autorisés à se connecter sur le réseau ;
- sauvegarde, à l'échelle de l'institution des données pertinentes pour son fonctionnement ;
- sensibilisation des utilisateurs du S.I. aux techniques actuelles d'attaques, qu'elles soient du domaine technique ou humain (ingénierie sociale) ;
- mesures supplémentaires visant à faciliter la restauration des données ou à limiter les dégâts en cas de compromission d'un poste de travail.

Historique

Le tableau 1 présente un aperçu historique des logiciels malveillants de type ransomware. On pourra se reporter au site `https://id-ransomware.malwarehunterteam.com/` pour une liste plus complète.

Période	Évènement	Cible
2000	Concepts initiaux	
2006	Premières dissémination	Windows
2010	Utilisation courante	
2010	Winlock	Windows
2012	Reveton	Windows
2012	Browlock	Windows
2013	CryptoLocker	Windows
2013	Android Defender	Android
06/2014	Simplocker	Android
05/2014	Koler	Android
06/2014	FileCoder	MacOSX
05/2015	LinuxEncoder	GNU/Linux
02/2015	CTB-Locker	Windows
01/2015	TeslaCrypt	Windows
11-2015	CryptoWall	Windows
01/2016	Locky	Windows
03/2016	Petya	Windows
02/2016	CTB-Locker	GNU/Linux
03/2016	KeRanger	MacOS X
05/2017	Jaff	Windows
05/2017	WannaCry	Windows

TABLE 1 – Historique des grandes familles de ransomwares

Fonctionnement des logiciels de rançon

Logiciels bloquant l'accès au système

Les ransomwares peuvent être classés en deux catégories :

— logiciels qui bloquent l'accès au système,

— logiciels qui chiffrent les données

LES LOGICIELS QUI BLOQUENT l'accès au système se dissimulent au sein du système d'exploitation infecté de manière a être lancé à chaque redémarrage de la machine. Toute action de l'utilisateur sur le clavier ou la souris est interceptée et ignorée afin de réaliser le blocage.
Le bureau du poste de travail est remplacé par une image ou une page web qui informe l'utilisateur que l'accès au système ne lui sera rendu qu'après paiement d'une somme d'argent. Le moyen de paiement demandé peuvent être du type « cartes de paiement prépayées » (Ukash, Paysafe), Short Message Service (SMS) surtaxé ou «carte cadeaux» (Amazon, `Apple iStore`, ...).
Les causes invoquées pour le blocage sont souvent relatives à une opération de police ou autre organisation d'état. La demande est renforcée par l'affichage de logo ou de symboles officiels et parfois l'adjonction d'une image pornographique ou d'un écran de webcam.

FIGURE 2 – Exemple d'écran d'information consécutif au blocage de l'accès à un ordinateur (`Browlock`).Cliquer pour zoomer.

CETTE FORME DE RANSOMWARE se limite au blocage des actions utilisateur sans porter atteinte aux données de l'ordinateur il est donc possible de le contrer en utilisant un moyen alternatif de dé-

marrage du poste informatique (clef USB, disque dur alternatif, …).

Logiciels chiffrant le disque dur

LES LOGICIELS QUI CHIFFRENT les informations des disques durs sont plus difficiles à contrer que les ransomwares bloquants.

> Il est impossible de restaurer les données sans la ou les clefs appropriées si les mécanismes cryptographiques du ransomware sont bien implémentés.

Le logiciel rançonneur recherche ensuite d'autres données de l'utilisateur sur les disques secondaires (périphériques Universal Serial Bus (USB)) et les partages réseaux accessibles.
Le logiciel utilisé pour réaliser le chiffrement n'est plus nécessaire à la fin de l'opération, il s'efface donc en général lui-même.

FIGURE 3 – Copie d'écran Wanna Cry.Cliquer pour zoomer.

Le chiffrement peut concerner tous les fichiers ou se limiter à certains types, considérés d'une grande valeur pour les utilisateurs, tels que les documents ou feuilles de calcul, les images, les vidéos, …. Les fichiers nécessaires au fonctionnement du système ne sont toutefois pas chiffrés afin que cet ordinateur puisse toujours redémarrer et afficher le message d'avertissement.
Le ransomwares peut ensuite tenter de chiffrer un certain nombre d'autres données présentes sur les disques dur des postes de travail :

- Sauvegardes cachées Volume Shadow Copy (VSS) et zone de restauration système
- Chiffrement de certains fichiers systèmes non indispensables au redémarrage de la machine.

Incitation au paiement

Ces caractéristiques techniques sont associées à des outils d'ingénierie sociale visant à mettre l'utilisateur sous pression pour le paiement de la rançon :

- montant demandé peu élevé ;
- augmentation graduelle de la rançon au cours du temps ;
- menace de destruction de la clef de chiffrement (rendant impossible toute récupération) après un certain délai ;
- destruction périodique de certain fichiers du disque dur.

Paiement

L'extorsion de rançon est un modèle économique criminel bien établi. Son intérêt principal réside en un transfert financier direct entre la victime et le criminel.

Dans le domaine numérique les criminels demandent à ce que les transferts financiers soient réalisés anonymement. Ils peuvent par exemple exiger l'utilisation d'une des méthodes suivantes :

— acquisition de cartes de paiement prépayées,

— utilisation d'une devise numérique de type bitcoin,

— expédition de SMS vers des numéros surtaxés,

— acquisition de « bons cadeaux » disponibles auprès de certains marchands numériques : Amazon, `Apple iStore`, …

Plates formes visées

En général les criminels cherchent un bénéfice rapide, ils visent pour cela les plates-formes les plus répandues : celles basées les systèmes d'exploitation de MicroSoft.
Il existe toutefois (cf tableau 1, à la page 8) un certain nombre de logiciels visant d'autre familles : `MacOS`, `Gnu/Linux` ou `Android`. En particulier les logiciels ayant eu un certain succès sous `Windows` sont parfois portés par d'autres plates-formes.

Chiffrement

En général, pour des raisons d'efficacité (rapidité du traitement), le chiffrement est réalisé en deux temps : chiffrement symétrique pour les fichiers, puis chiffrement de la clef symétrique par une algorithme asymétrique.
Pour la partie asymétrique, la clef publique utilisée pour le chiffrement peut être incluse dans le programme malicieux ou obtenue dynamiquement à partir d'un serveur sur internet.

Chiffrement symétrique une même clef est utilisée pour chiffrer puis pour déchiffrer les données
Chiffrement asymétrique deux clefs sont utilisées l'une permet de chiffrer les données l'autre clef permet seulement de déchiffrer. Ainsi une clef peut rester secrète et l'autre peut-être rendue publique

> Dans certain cas, une infection pourrait être stoppée en déconnectant la machine du réseau et une analyse post-mortem pourrait permettre de retrouver la clef symétrique.

Outils de déchiffrement

Les virus contiennent parfois des erreurs de codage qui permettent de retrouver les clefs utilisées pour le chiffrement des données,

Catalogue de ransomwares : `https://id-ransomware.malwarehunterteam.com/index.php`

> Toutefois, en raison de la grande variabilité des clefs de chiffrement l'existence actuelle d'une solution pour certaines familles de ransomwares n'assure pas qu'il sera possible de déchiffrer une version améliorée d'un tel logiciel.

Méthodes de compromission

Les données récentes montrent que les logiciels bloqueurs ont quasiment disparu et que les dernières vagues de compromission ont toutes utilisé des logiciels de chiffrement.
La plupart de ces attaques sont des attaques de masse qui ne ciblent pas particulièrement un pays, une organisation ou un groupe de personnes.

Le moyen d'attaque préféré pour les ransomwares est identique à ceux des autres virus : il utilise principalement une diffusion par envoi en masse de courriels (pourriels), le logiciel `WannaCry` a complété cette méthode classique par un outil de propagation autonome basé sur une vulnérabilité des systèmes `Windows`.

Propagation par envoi massif d'emails

Les pièces jointes aux courriers électroniques constituent à ce jour la méthode préférée de propagation des ransomwares.
Afin de capter l'attention de la victime, ces courriers mentionnent des sujets potentiellement attractifs : factures, confirmations de commande, notifications de livraison, documents numérisés (scannés), lettres de candidature, messages relatifs aux impôts, ou photographies.
Les adresses d'expéditions de ces courriers peuvent être des personnes, des institutions ou des entreprises connues ou inconnues de la victime.
Ces fichiers contenus dans les pièces jointes peuvent par exemple être les suivants :

— des documents offices ou des modèles de documents (.doc, .xls, .docx, .xslx, .docm, .dot) contenant des macros ;
— des fichiers archives avec ou sans protection par mot de passe ((.zip, .rar)
— des fichiers de code en langage de script : javascript, visualbasicscript, powershell -.js, .vbs, .ps1, .wsf)
— des fichiers exécutables (.exe)

Ces formats peuvent bien entendu être combines (un code javascript contenu dans une archive .zip, par exemple) et les types de fichiers concernés sont en constante évolution.
Enfin, de nombreuses pièces jointes utilisent des doubles suffixes (document..pdf.js) afin que les systèmes d'exploitation n'informent l'utilisateur que sur le premier de ces suffixes (.pdf) et masque ainsi le caractère exécutable et donc dangereux du fichier joint.

Les macros incluses dans les documents office peuvent déclencher l'affichage d'avertissements sur le caractère potentiellement dangereux de la manipulation ; dans ce cas les documents contiennent des instructions en clair indiquant à l'utilisateur de ne pas tenir compte de ces avertissements.
Dans la plupart des cas, le code malicieux inséré dans les pièces jointes ne constitue pas le code du virus, il est plutôt utilisé pour télécharger ce code dangereux à partir d'un site web.
L'utilisation d'un code de script comme code de téléchargement permet une certaine flexibilité dans l'architecture des attaquants puisqu'elle lui permet de ne pas utiliser systématiquement le même type de programme malveillants.

Les machines expédiant les pourriels sont la plupart du temps des machines appartenant à un botnet, c'est-à-dire des machines qui ont été piratées afin d'être utilisées à l'insu de leurs propriétaire comme outils criminels.

Kits d'exploitation de vulnérabilité

Les kits d'exploitation de vulnérabilités sont des programmes qui tentent de détecter une ou plusieurs vulnérabilités (connue ou non connue publiquement) afin de les exploiter. Ces kits sont constamment mis à jour afin d'intégrer les dernières vulnérabilités connues. Ils peuvent tenter d'exploiter les vulnérabilités de la machine locale mais aussi celles des machines voisines.
Ces kits sont souvent installés sur la machine cible par utilisation de iframes au sein d'une page ou en détournant la cible d'une image publicitaire. Lorsqu'ils sont installés, ces programmes recherchent, sans que l'utilisateur ne s'en aperçoive, les vulnérabilités qu'ils connaissent.
Les postes de travail ou serveurs sous `Windows` ne sont pas les uniques cibles de ces kits d'exploitation, il en existe aussi pour `Android` et pour `Gnu/Linux`.

Dommages

Les conséquences d'une attaque réussie par un logiciel de rançon moderne sont importantes. Dans le secteur domestique, les personnes auront tendances à payer la somme exigée afin de pouvoir retrouver des données qui ont souvent une charge sentimentale forte (photos, musiques, vidéos) ou représentent des documents importants (scans de titres de propriétés, documents financiers, …).
En ce sens, le modèle économique du ransomware est attirant pour les criminels et les attaques de ce type vont sans doute perdurer un long moment.
Les dommages principaux dans les organisations sont en général décomposés de la manière suivante :

La défense principale qui repose sur les sauvegardes doit donc être systématiquement appliquée dans les organisations.

— Atteintes aux personnes,
— Atteintes aux biens,
— Atteintes à l'image,
— Atteintes aux tierces parties,

Une attaque par ransomware peut avoir des conséquences dans chacun des composants précédent. L'étendue des dommages dépend de mesures techniques ou organisationnelle dans les domaines suivants : prévention, détection, réaction.
En général les mesures à appliquer pour les ransomwares ne sont pas différentes de celles, plus générales, visant à protéger l'établissement des autres virus. Ces mesures sont basées sur les principes suivants :

— les défauts de sensibilisation du personnel ou la mise en place de mesures techniques non normalisées accroissent les risques d'attaques réussies par pourriels,

— les défauts dans la mise à jour des systèmes et l'application retardée de correctifs accroissent les risques en cas de présence de kits d'exploitation de vulnérabilités,
— les défauts de segmentation réseau, des mots de passe administrateurs faibles augmentent les risques de dissémination d'une attaque initiale réussie.
— des sauvegardes manquantes, non à jour ou non testées rendent la restauration des données impossible et augmente le volume de données perdues.

Prospective

Le succès du modèle économique des logiciels de rançons va sans doute rendre de plus en plus banal les kits de piratage prêts à l'emploi.

Risques de banalisation des tentatives d'extorsion

Cette banalisation risque de faciliter la réalisation d'attaques ciblées vers une organisation ou plusieurs organisations du même type à certaines de leurs périodes clefs (par exemple les établissements Enseignement supérieur recherche (ESR) lors des périodes d'inscription ou d'examen). Les tentatives de rançon seront d'autant plus réussies que les attaquants sont proches de l'organisation qu'ils tentent d'extorquer.

Risques de non-détection des attaques

Des attaquants distants peuvent toutefois être dangereux s'ils peuvent agir sur le long terme : une infiltration non détectée de programme malveillant peut précéder une attaque par ransomware. Cette infiltration éventuelle fournirait à l'attaquant un poste d'observation du S.I. de l'organisation, poste d'observation qui pourrait lui permettre par exemple de cartographier les infrastructures de stockage ou de sauvegarde, …. Les dégâts relatifs à une attaque de ransomware pourraient aussi être ensuite largement amplifiés en perturbant le réseau de communication interne de l'établissement. Une fois l'infiltration réussie, les attaquants auraient tout le temps nécessaire pour la réalisation de leurs futurs méfaits, qu'il s'agisse d'espionnage, de sabotage ou d'extorsion.

Mesures de protection

Protection des postes de travail contre les logiciels malveillants

Exec.1 prévenir l'exécution des codes malveillants (Javascript, visualbasicscript, `PowerShell`, …).

Exec.1.1 invalider Windows Scripting Host (WSH) cf[4] ;

Exec.1.2 restreindre ou interdire l'exécution des Visual Basic Script (VBS) cf[5]

Exec.1.3 invalider `PowerShell` en utilisant `Applocker` ou activation de la journalisation `PowerShell` avec les politiques de groupes.

> Il ne suffit pas d'activer la politique d'exécution restreinte car ce paramètre peut être contourné.

Exec.1.4 modifier les associations de fichier par défaut pour les scripts (.js, .vbs, …) pour empêcher leur exécution et faire en sorte qu'ils s'ouvrent plutôt dans un éditeur de texte (`Notepad`/`Wordpad`).

Exec.2 prévenir l'exécution de macros dans les documents Office

Exec.2.1 désactiver l'exécution de macro dans les produits Office, cf[6]

Exec.2.2 activer le mode de visualisation protégé pour les produits Office cf[7]

Exec.2.3 adapter les mesures précédentes si les activités opérationnelles nécessitent l'utilisation de macros.

Exec.2.4 définir un espace de confiance pour les documents contenant des macros : cf[8]

Exec.2.5 utiliser des macros signées

Exec.2.6 configurer l'`Explorateur windows` pour qu'il affiche les extensions complètes de fichier afin que les utilisateurs puissent reconnaître la nature des fichiers qu'ils activent.

4. MICROSOFT. *Disabling Windows Script Host*. Mai 2017. URL : `https://technet.microsoft.com/fr-fr/library/ee198684.aspx`.
5. MICROSOFT. *Restricting the Ability to Run Scripts*. Mai 2017. URL : `https://technet.microsoft.com/fr-fr/library/ee198679.aspx`.
6. MICROSOFT. *Désactiver Visual Basic*. Mai 2017. URL : `https://technet.microsoft.com/de-de/library/ee857085.aspx#changevba`.
7. MICROSOFT. *Planifier les paramètres de vue protégée pour Office 2013*. Mai 2017. URL : `https://technet.microsoft.com/fr-fr/library/ee857087.aspx`.
8. MICROSOFT. *Create, remove, or change a trusted location for your files*. Mai 2017. URL : `https://support.office.com/en-us/article/Create-remove-or-change-a-trusted-location-for-your-files-f5151879-25ea-4998-80a5-4208b3540a62`.

Protection contre les messages malveillants sur les serveurs de messagerie

SpamAV.1 filtrer au plus tôt les messages non sollicités envoyés en masse (pourriels)

SpamAV.2 bloquer les types de fichiers potentiellement dangereux :

SpamAV.2.1 Formats de fichiers exécutables : .bat, .com, .chm, .cmd, .exe, .hta, .jar, .js, .jse, .lnk, .msi, .pse, .scf, .scr, .ws, .wsf

SpamAV.2.2 fichiers archives ou chiffrés : .7z, .zip, .zipx, .rar

SpamAV.2.3 fichiers de macro : .bas, .vb, .vbs, .vbe

SpamAV.2.4 marquer les messages comme dangereux s'il n'est pas possible de bloquer les messages suspects

SpamAV.2.5 utiliser les moyens d'infrastructure spécifiques à la lutte anti-spam :

SpamAV.2.5.1 Domain Name Service (DNS) : Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication (DMARC)

SpamAV.2.5.2 listes grises, bases de données de détection de botnets

SpamAV.2.5.3 détection distribuée d'envois en nombre

Protection contre les kits d'intrusions

Intrus.1 mettre à jour et gérer les applications de correctifs aux postes de travail, une politique de mise à jour prenant en compte les aspects suivants devrait être définie :

Intrus.1.1 mettre à jour régulièrement les postes de travail

Intrus.1.2 mettre à jour immédiatement les correctifs de sécurité dès leur publication.

en particulier en ce qui concerne les navigateurs web ou leurs extensions (plugins), clients de messagerieles applications pdf ou les programmes office utilisés pour visualiser ou ouvrir du contenu en provenance de l'extérieur.

Intrus.2 favoriser une utilisation sûre des navigateurs et réduire leur surface d'attaque

Intrus.2.1 désinstaller de l'image initiale les extensions des navigateurs ou des programmes de messagerie qui ne sont pas utilisés : Flash (Adobe), Java (Oracle), Silverlight ;

Intrus.2.2 restreindre l'utilisation automatique de ces extensions si elles sont nécessaires aux activités de l'établissement (fonction «click to play» ou activation automatique uniquement à partir de zones de confiance).

Intrus.2.3 plus généralement : minimiser le nombre de programmes utilisés pour accéder à du contenu distant en désinstaller les programmes qui ne sont pas nécessaires aux activités de l'établissement.

Protection contre les autres modes d'attaque

Extern.1 sécuriser les accès distant et des accès à partir de systèmes externes

Extern.1.1 sécuriser les serveurs permettant l'accès externe : Réseau Privé Virtuel (VPN), authentification à double facteur, filtrage par source Internet Protocol (IP), détection active des tentatives d'intrusion par force brute, supervision des systèmes.

Extern.1.2 gérer les mises à jour et appliquer rapidement les correctifs de sécurité : l'intrusion puis l'installation d'un ransomware peut provenir de vulnérabilités dans les programmes exécutés sur les serveurs (serveur web, serveur d'applications).

Extern.1.3 réaliser des tests d'intrusion

Extern.1.4 documenter les systèmes accessibles de l'extérieur ainsi que leur surface d'exposition aux attaques.

Mesures générales de protection

Gen.1 sauvegarder les données ou les systèmes de fichiers

cette mesure est la mesure principale à prendre pour contrer une attaque réussie de ransomware. Les sauvegardes doivent être stockées indépendamment du réseau informatique. Les restaurations doivent être régulièrement testées.

> L'exigence sur la mise hors ligne des sauvegardes est particulièrement importante pour les sources de menaces ransomwares.

Gen.2 utilisation de programme anti-virus

Gestion centralisée, mise à jour des programmes aussi bien que des signatures, cependant les nouvelles versions d'un virus sont rarement détectées, l'utilisation d'IDS ou de bases de données en ligne peut permettre de renforcer les activités de détection.

L'utilisation de listes noires peut permettre de bloquer les connexions à des URLs dangereux.

Le fournisseur de l'anti-virus devrait de plus être consulté sur les possibilités de ses produits vis-à-vis des ransomwares.

Gen.3 sensibiliser le personnel.

La sensibilisation ou la formation du personnel doit l'amener à se méfier sainement des données en provenance de l'internet tout en mettant en perspective les connexions dématérialisée avec des contacts extérieurs.

De plus, les personnels devraient être périodiquement informés sur les deux principaux vecteurs de propagation des ransomwares ou autres virus : l'infection par l'ouverture de fichiers joints et l'infection par consultation de sites compromis.

Les courriers devraient toujours être lus avant que les pièces jointes ne soient ouvertes. Les expéditeurs douteux ou les messages incompréhensibles ne doivent pas être ouverts. En cas de doutes le service en charge du numérique (ou du S.I.) devrait être averti.

Les utilisateurs devraient être alertés sur les attaques en cours, les types de messages envoyés, les types de pièces jointes ainsi que les macros présentes dans les documents

Protection contre la dissémination de code malveillant

Dis.1 restreindre les droits d'accès aux partages réseau

L'accès entre les différentes machines des réseaux de site. Les accès en écriture doivent être limités, les restrictions de droits doivent être appliquées selon le principe du besoin d'en connaître.

Les droits devraient être gérés en fonction de la position professionnelle des personnes, les modifications de ses positions devraient être répercutées sur ces droits.

Ces droits devraient être revus périodiquement.

Dis.2 restreindre les communications directes entre ordinateurs de sites

Les virus se répandent en exploitant des vulnérabilités des ordinateurs qu'ils peuvent joindre. Mettre en place une segmentation réseau permet de restreindre la visibilité commune des postes de travail et donc de limiter les possibilités d'exploitation des vulnérabilités ;

La segmentation peut-être mise en oeuvre plus ou moins finement, en fonction des capacités humaines et technologiques des sites :

- segmentation par grandes fonctions : étudiants, enseignants, personnels administratifs,
- segmentation organique prenant en compte les différentes structures ou composantes d l'établissement ; services fonctionnels, ufrs ou départements, structures de recherche.
- utilisation de «private vlans» disponible sur certains matériels.

Dis.3 limiter l'utilisation avec des droits administrateurs

Les activités classiques, lecture de mail, navigation internet ne doivent pas être effectuées avec un compte possédant des privilèges d'administration.

Idéalement l'administration devrait se faire en utilisant différents compte, chaque compte correspondant à une activité. Chaque système ne devrait avoir qu'un seul mot de passe administrateur. Les accès administrateurs devraient utiliser une identification à double facteur.

Pour les ransomwares, la séparation «utilisateur, administrateur» permet d'éviter l'effacement des copies fantômes du système de fichier, effacement impossible lorsque les droits administratifs sont positionnés par défaut. Il en est de même pour l'accès au Master Boot Record (MBR).

Dis.4 prévenir l'exécution indésirable de programmes

Dis.4.1 La mise en liste blanche des applications pouvant s'exécuter est une opération lourde, il est préférable d'utiliser les fonctions d'Application Directory Whitelisting (ADW) ou les applications pouvant s'exécuter doivent appartenir à certains répertoires. Les répertoires concernés ne doivent pas pouvoir être écrits par l'utilisateur.

> En particulier les fichiers contenus dans le répertorie %TEMP% ne doivent pas être exécutables.

Dis.5 restreindre des types permis de fichiers sur un serveur de fichiers,

Dis.6 rechercher périodiquement des points de vulnérabilité et tests d'intrusion,

Dis.7 mettre en oeuvre des exercices de sécurité ;

Détection des compromissions

Detect.1 centraliser et analyser des journaux d'activité,

Detect.2 détecter les transferts réseaux vers les serveurs de contrôle attaquants

Réponse aux incidents

Resp.1 répondre immédiatement

Resp.1.1 déconnecter la machine du réseau

Resp.1.1.1 réseau filaire : invalidation du port du switch de connexion de la machine

Resp.1.1.2 réseau wifi : déconnexion forcée du réseau Wifi

Resp.1.2 interrompre le processus de chiffrement par arrêt de l'alimentation électrique ou démontage de la batterie pour les portables

> l'arrêt brutal d'une machine peut laisser le processus de chiffrement dans un état aléatoire, ce qui va sans doute rendre impossible tout déchiffrement même en cas de paiement de la rançon ; il est cependant préférable d'interrompre le processus et d'envisager une restauration des sauvegardes plutôt que d'espérer un retour à la situation initiale après paiement.

Resp.1.3 analyser les journaux d'activité pour retrouver la trace d'autres machines infectées : activité réseau, activités des partages, journaux d'activités des autres postes de travail ;

Resp.1.4 se renseigner sur le virus : utiliser le site `https://id-ransomware.malwarehunterteam.com/` pour identifier le logiciel et vérifier l'éventuelle existence d'une méthode de déchiffrement ;

Resp.1.5 limiter des effets : restreindre temporairement l'accès aux serveurs de fichiers, aux serveurs utilisés pour les sauvegardes, a l'Internet.

Resp.1.6 préserver le contenu des disques durs chiffrés afin de rendre possible une analyse/expertise post-mortem (forensics).

Resp.2 signaler le problème au cert renater pour expertise externe ;

Resp.3 porter plainte et (ou) renseigner une pré-plainte sur le site dédié ;

Resp.4 vérifier l'état des logiciels embarqués sur la machines : bios, uefi.

> l'idéal serait de remplacer le poste de travail de l'utilisateur afin de conserver en l'état la machine infectée.

Resp.5 restaurer les données chiffrées sur le poste de travail après avoir vérifié l'innocuité des sauvegardes existantes.

Resp.6 appliquer l'une des solutions suivantes après avoir vérifié l'innocuité des données associées : VSS, snapshot de machine virtuelle, snapshot serveurs de fichiers ;

Resp.7 planifier des mesures préventives manquantes pour éviter d'autres infections.

Resp.8 décliner le paiement de la rançon

Le paiement est déconseillé, il est préférable d'appliquer les mesures ci-dessus. Le paiement ne garantit en rien la remise d'une clef de déchiffrement et elle augmente la confiance des criminels dans ce type d'attaque. Le risque est enfin grand qu'une première attaque réussie soit suivie d'une seconde attaque plus ciblée.