Ransomwares et Rançongiciels : Définition et comment s’en protéger

Un page concernant les Crypto-Ransomwares, des menaces malveillantes, qui sont des menaces informatiques très importantes depuis fin 2015.
En français, vous pouvez traduire Ransomware par Rançongiciel.

Les ransomwares sont des logiciels malveillants qui prend en otage un ordinateur ou les données de l’ordinateur et demandent de payer une somme d’argent (souvent sous la forme de bitcoin, ou précédemment en Paysafecard et Ukash pour les Trojan Winlock).
Les crypto-ransomwares portent aussi len om de cryptolocker ou Trojan FileCoder.
Les sommes d’argent demandées tournent autour de centaines d’euros.
Depuis fin 2015, le ransomware chiffre les documents à travers des chiffrements asymétriques, la somme d’argent permet d’acheter la clé de déchiffrement.

Historique des ransomwares

Contrairement aux Ransomwares Fake Police (Virus Gendarmerie) qui bloquaient l'accès au PC en affichant une page se faisant passer pour les autorités et vous demandant de payer une amende imaginaire.

Les crypto-ransomwares sont des ransomwares qui chiffrent les documents afin d'empêcher leurs accès.
Les fichiers touchés par le ransomware ont souvent l'extension modifée.
Une fois vos fichiers chiffrés, on vous demande de payer une rançon pour récupérer l'accès à ces documents.
Pour se faire, ces crypto-ransomwares créés des fichiers texte ou pages WEB dans différents dossiers afin de vous informer

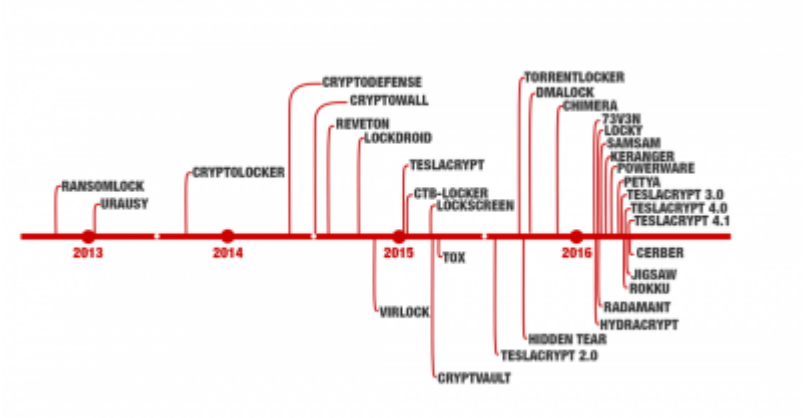
des modalités pour payer la dite rançon.
Ainsi le but est de gagner de l'argent en prenant en otage vos données.

Différentes familles de crypt-ransomwares ont succédés avec des pics d'activités.

Voici les Crypto-Ransomware les plus actifs qui ont ou visent la France :

- ~~Cryptowall (n'est plus actif)~~
- ~~TeslaCrypt fin 2015/2016 (n'est plus actif)~~
- ~~CryptXXX – Ransomware RSA-4096 .crypt~~
- ~~Ransomware Jaff etLocky Ransomware)~~
- ~~Cerber Ransomware et Ransomware Cerber~~
- ~~CTB-Locker (Critroni.A)~~
- Spora ransomware
- WannaCry
- GandCrab ransomware

Voici une timeline qui regroupent les différentes familles de ransomwares.



(source endgame.com)

Entre 2015 et 2016, d'après (Décembre 2016), en terme de prévalence, CTB-Locker se place loin devant les autres Ransomwares, suivi par Locky puis TeslaCrypt.
Ce dernier n'étant plus actif depuis courant mai 2016).

	Name	Verdict*	% of attacked users**
1	CTB-Locker	Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion	25.32
2	Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7.07
3	TeslaCrypt	Trojan-Ransom.Win32.Bitman	6.54
4	Scatter	Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan-Dropper.JS.Scatter	2.85
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2.79
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2.36
7	Shade	Trojan-Ransom.Win32.Shade	1.73
8	(generic verdict)	Trojan-Ransom.Win32.Snocry	1.26
9			1.15
10			0.90

Statistique répartition des ransomwares

Ces statistiques de répartition des familles de ransomwares, Cryptowall place devant Wannacry, Cerber et Locky.

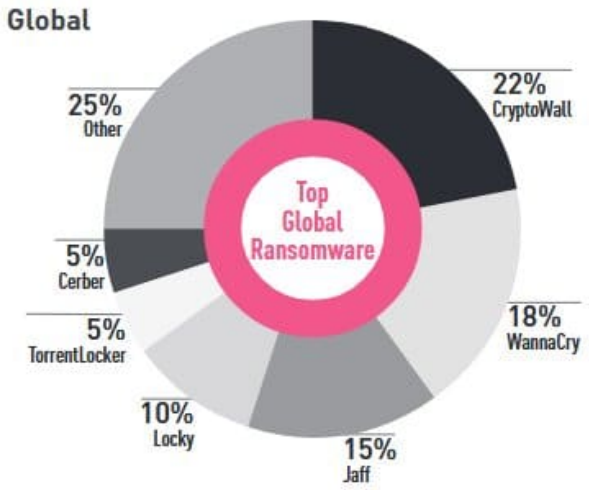


Figure 8: Most Prevalent Ransomware Globally

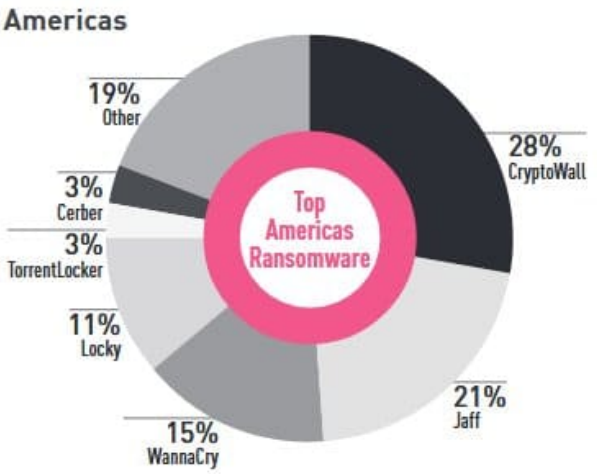


Figure 9: Most Prevalent Ransomware in the Americas

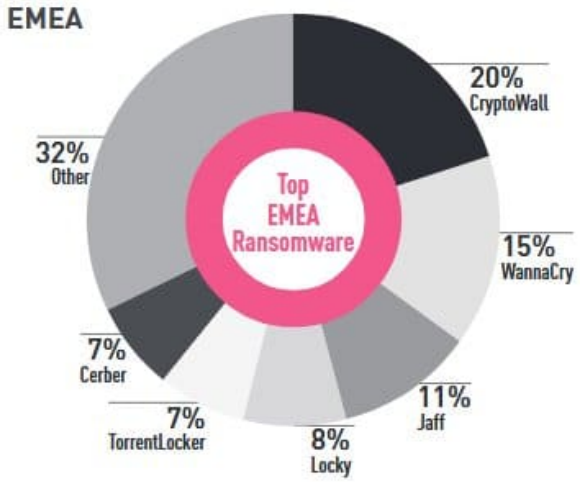


Figure 10: Most Prevalent Ransomware in EMEA

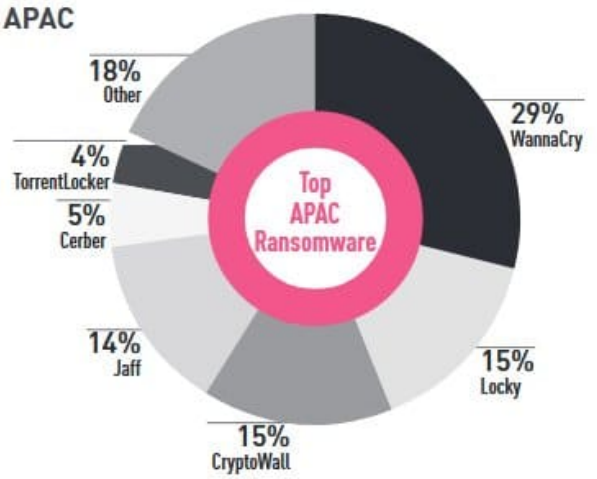


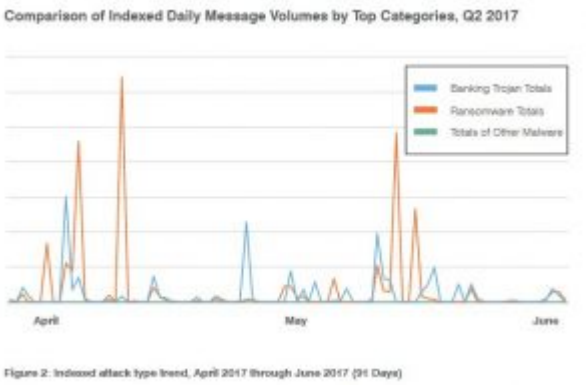
Figure 11: Most Prevalent Ransomware in APAC

Statistique répartition des ransomware

En 2018, le ransomware Grandcrab qui tire son épingle du jeu en devenant la menace la plus importante.
En effet, les autres ransomwares devenant beaucoup moins actifs et beaucoup ont même disparu.

Le ransomware GrandCrab

Enfin, ces dernières statistiques qui montrent qu'en 2016 détrônent les trojan banker comme menace la plus importante :



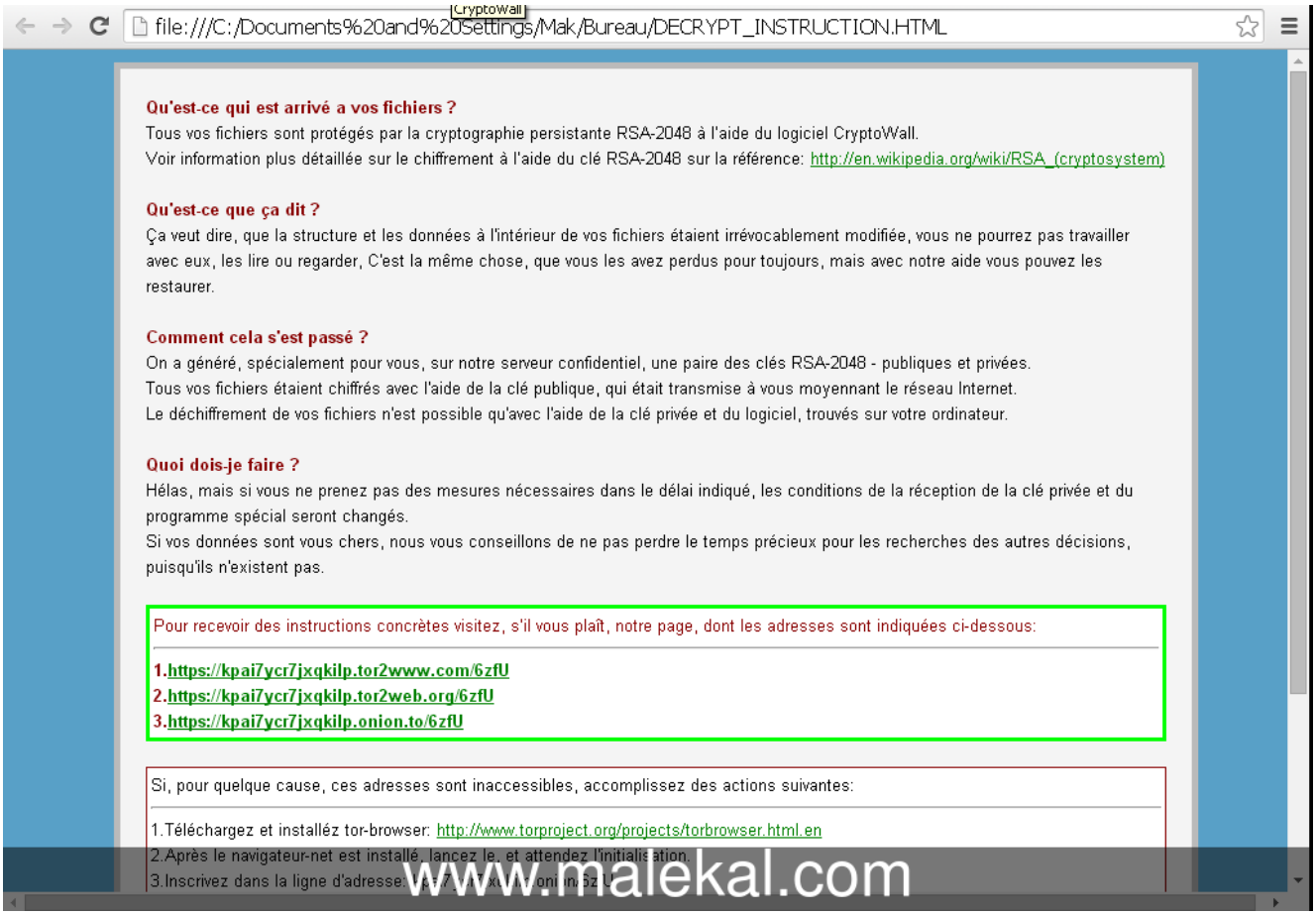
Statistique répartition des ransomwares

Quelques exemples de ransomwares

Voici quelques exemples de ransomwares et leurs fonctionnements.

Par exemple CryptoWall après avoir frappé créé un fichier **HELP_FILE** qui contient les explications sur le paiement.

En général, ces derniers expliquent que vous ne pouvez pas récupérer vos données sauf en payant la rançon.
Tout est pensé pour vous faire payer afin de récupérer la clé de déchiffrement.



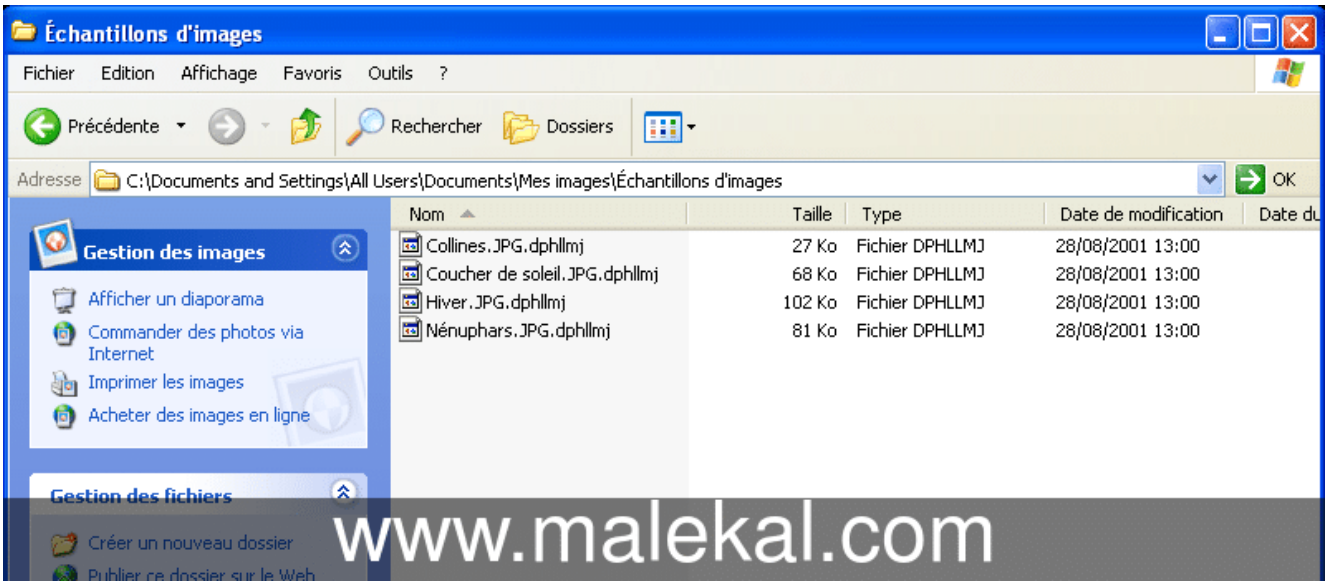
Instruction de paiement de CryptoWall

Cet autre exemple avec CTB-Locker qui affiche un message : **Your personal files are encrypted.**
Certaines variantes modifient le fond d’écran avec un message indiquant qu’un ransomware a infecté l’ordinateur.

CTB-Locker (Critoni.A)

Ce dernier ajoute une extension à 7 caractères aléatoires aux fichiers chiffrés.
Les extensions utilisées diffèrent d’un ransomware à l’autre.
On peut avoir le nom du ransomware, des lettres aléatoires.
Au sein d’une même famille, les extensions utilisées changent selon la variante et version.

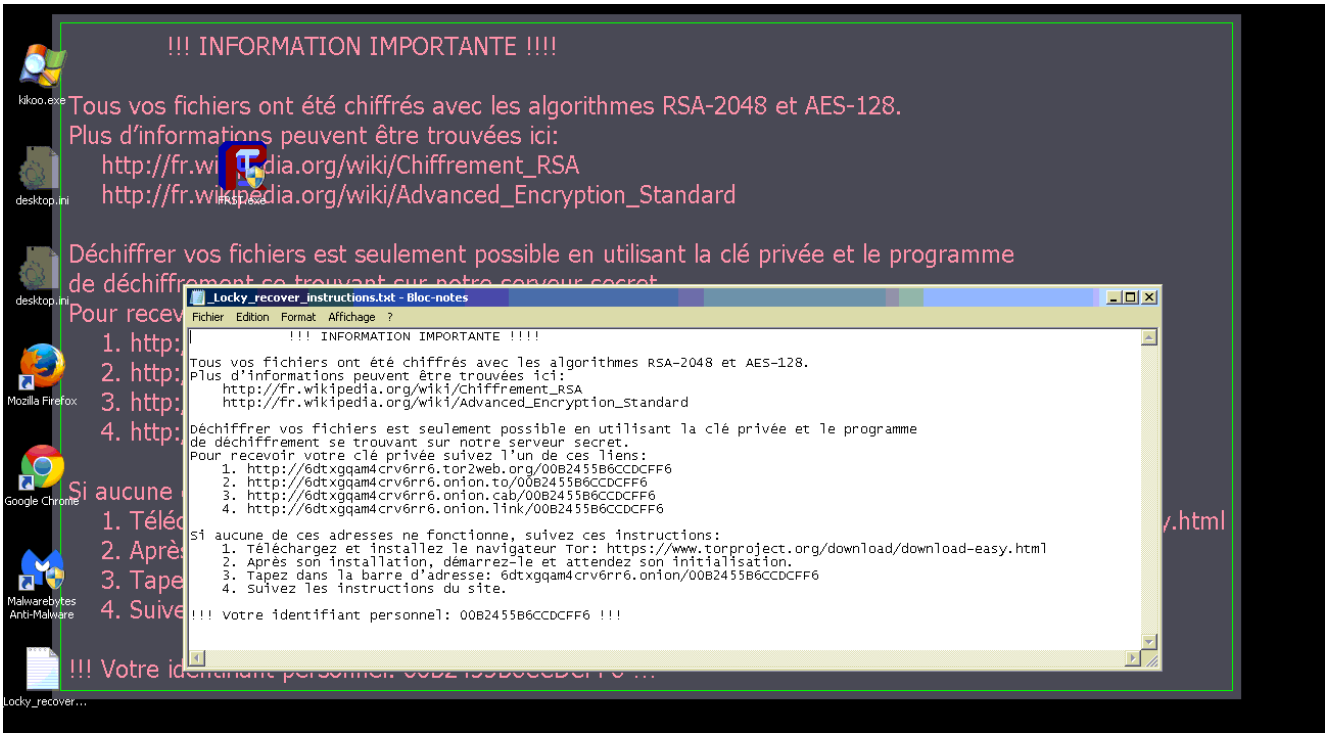
Le rançongiciel CTB-Locker



Le rançongiciel CTB-Locker

Enfin même comportement avec [Locky Ransomware]() qui modifie le

fond d’écran et ouvre les instructions de paiement avec toutes les explications.



Les Ransomwares en vidéo

Pour mieux comprendre le fonctionnement de ces logiciels malveillants, voici quelques vidéos.

Le ransomware Jaff en vidéo :

Locky Ransomware en vidéo :

Le Ransomware CryptXXX en vidéo :

TeslaCrypt Crypto-Ransomware en action :

Cerber en vidéo :

Comment se propagent et se protéger des ransomwares ?

Plusieurs méthodes principales sont utilisées pour diffuser les ransomwares.

- Les WebExploit qui tirent parti de vulnérabilités présentes sur l'ordinateur pour installer un ransomware à la simple visite d'une page WEB. Exemple avec Ransomware : Vulnérabilité Flash (CVE-2016-1019) et Magnitude Exploit Kit
- Des campagnes de virus par emails, voici quelques exemples de campagnes d'emails malicieux :
    - Email malicieux – Ransomware Locky
    - Mail malicieux : TeslaCrypt Ransomware (virus RSA 4096)
    - Sujets connexes à ces campagnes d'emails malicieux JS/TrojanDownloader.Nemucod : Ransomware et Trojan Dridex – Mail malicieux Macro Office

- Piratage à distance via le protocole RDP (Terminal Serveur), VNC, etc
- Plateforme de PUP.

Les virus par mail

Les virus par mail sont un grand classique dans les méthodes de distribution.
Depuis fin 2015, grâce aux scripts et aux documents Word, ils ont fait un grand retour.

Exemple ci-dessous d'un mail malicieux VoiceMail et Invoice qui poussent le ransomware Cerber

Dans le cas des pièces jointes malicieuses, il suffit de bien faire attention aux emails que vous ouvrez et surtout aux fichiers qui y sont joints. Prenez bien le temps de lire.
Généralement, ces emails reprennent des services connus (UPS, Service de Fax, Banque etc) avec une pièce jointe zip mais dernièrement, de plus en plus de campagnes en langue française

copiant des emails existants (site de vente, des avocats, des comptables etc)
En cas de doute sur une pièce jointe, vous pouvez soumettre [cette dernière sur VirusTotal](VirusTotal).

Voici un exemple d'email malicieux, comme vous pouvez le voir, ils ne font pas beaucoup d'efforts.

Du côté des protections, nous vous conseillons de désactiver Windows Script Host, comme l'explique cette vidéo.
Se reporter à la page : [Comment se protéger des scripts malicieux sur Windows]
Notamment le programme [Marmiton] permet de filtrer les scripts malveillants.

Les documents Word permettent aussi d'infecter l'ordinateur, plus d'informations, se reporter à l'actualité : Vulnérabilité (?) DDE sur Word et mails malveillants et cette vidéo illustrative :

Les Web Exploit

Un exploit sur site WEB tire parti de la présence de logiciels non à jour sur l'ordinateur, notamment les plugins des navigateurs WEB (Java, Flash, etc) qui vont permettre l'infection automatique à la simple visite d'un site WEB.
Soit le site a été piraté et permet une redirection vers un exploit, soit une publicité malicieuse a été déposée sur des régies publicitaire afin de provoquer la redirection vers l'exploit.
Exemple de campagne de WebExploit poussant des ransomwares : Ransomware : Vulnérabilité Flash (CVE-2016-1019) et Magnitude Exploit Kit

Exemple avec : Exploit Java et en vidéo :

Les web exploits : comment infecter son ordinateur automatiquement

Il faut donc impérativement maintenir vos logiciels à jour afin de ne pas voir ces portes d'entrée sur ton système.
Tant que ces logiciels ne seront pas à jour, ton PC est vulnérable et les infections peuvent s'installer facilement.

Maintenez vos logiciels à jour c'est important, des programmes peuvent vous y aider : Logiciels pour maintenir ses programmes

à jour.

Voici les pages pour sécuriser vos navigateurs WEB :

- Google Chrome (paragraphe Plugin) : Sécuriser Google Chrome
- Internet Explorer (paragraphe plugin Java) : Sécuriser Internet Explorer
- Mozilla Firefox : Sécuriser Mozilla Firefox

Plus globalement pour sécuriser son ordinateur, suivre les bonnes habitudes, se reporter à la page : Comment Sécuriser son ordinateur ?

Terminal Server

Les serveurs Windows peuvent être piratés à travers Terminal Serveur (l'accès du bureau à distance).
Il s'agit d'attaque brute-force, énumérer les utilisateurs Windows et tenter de se connecter à travers des tentatives successives de mot de passe.
Si un compte Windows est présent avec un mot de passe faible, l'attaquant pourra se connecter au serveur et aura la main dessus.

L'accès en administrateur peut permettre de désactiver l'antivirus, si celui-ci n'est pas protégé par un mot de passe.

Plus d'informations : Piratage de serveur Windows par Terminal Server.

Particularité avec les ransomwares Wana Decryptor et Petya

Wanna Decrytpor et Petya sont des ransomwares particuliers, non pas par la partie ransomware, mais par le mode d'attaque.
Wana Decryptor / WannaCry et Petya utilise les mêmes principes que les vers informatiques en exploitant une vulnérabilité à distance et ayant donc des capacités d'auto-propagation propre afin d'infecter des ordinateurs d'un même raison.
L'attaque WannaCry a été lancée à l'aveugle, à savoir des ordinateurs sur internet ont été infectés et envoyés des trames sur la toile afin d'infecter d'autres ordinateurs.
WannaCry s'est ainsi propagé assez rapidement sur internet.

Petya est aussi encore plus particulier, car il a visé plutôt les entreprises à travers une pré-attaque pour pirater un ordinateur de l'entreprise, le but étant de rentrer dans le réseau de celle-ci.
Il semblerait qu'une mise à jour du logiciel de comptabilité MeDoc ait été corrompu pour charger des outils pour voler les

mots de passe du réseau et lancer la partie d'auto-propagation qui attaque des ordinateurs vulnérables au sein du réseau. Tous les ordinateurs du réseau vulnérables seront donc touchés, ce qui peut être très pénalisant pour une entreprise. L'attaque de Petya est donc plus ciblée.

La fiche ransomware Petya donne plus d'informations sur ce dernier et son mode d'attaque : [FAQ – Ransomware Petya]

Les Anti-Ransomwares

Il existe des logiciels de protection dédiés à ce type de menaces, des anti-ransomwares, mon avis et commentaires sur ces programmes. A lire : [Anti-Ransomware]

Windows 10 incorpore aussi son anti-ransomware, pour plus d'informations, rendez-vous sur la page : Comment activer la protection Anti-Ransomware de Windows 10

Solutions pour récupérer les fichiers attaqués par un ransomware

La page suivante donne quelques solutions, si vos documents ont été pris en otage par un ransomware : Ransomware : solutions pour récupérer fichiers chiffrés (cryptés)

Liens autour des logiciels malveillants

Résumer tout le monde des trojans et logiciels malveillants serait très compliqués.
Il existe divers types et de familles plus ou moins évolués selon le but recherché par les pirates, voler des infos bancaires, mot de passe ou permettre le contrôle de l'ordinateur.
Vous trouverez une liste des familles de trojan sur la page : Index des menaces et programmes malveillants/Malwares

Les liens généraux sur les menaces informatiques :

- Les virus informatiques
- Comment les virus informatiques sont distribués.
- Les botnets : réseau de machines infectées

- Business malwares : le Pourquoi des infections informatique
- Comment les virus informatiques sont distribués.
- La sécurité de son PC, c’est quoi ?