Windows 10

Avantages Et Inconvénients

Par RIGHI Sylia 4
et AKTOUCHE Sadek Rayan 6

Introduction

L'information est aujourd'hui la sève de l'entreprise. C'est ce qui fait à la fois sa force et son existence. Fichiers, bases de données, méthodes de travail et de fabrication, fiches des salariés et informations industrielles sont autant d'informations qui composent la structure et la base d'une entreprise. Il s'agit là son capital intellectuel, ou plutôt **capital informationnel**. Toute perte d'information peut porter un coup fatal à une entreprise ou même à une nation.

Si ces informations venaient à être perdues, volées ou à tomber dans les mains d'une autre entreprise, la donnée n'aurait plus de raison d'exister car **elle ne serait plus exclusive**. L'information a aujourd'hui de la valeur de par son côté unique et exclusif pour une entreprise. Il est donc dans l'intérêt de l'entreprise de protéger son patrimoine informationnel.

Le système d'exploitation est le coordinateur entre l'utilisateur et la machine, il assure la communication entre les couches logiques et physiques. Il gère les applications des utilisateurs ainsi que les différents périphériques pour un fonctionnement correct d'un ordinateur. C'est pour cette importance capitale qu'il faut impérativement protéger les systèmes d'exploitation.

Nous allons nous intéresser dans cet exposé au dernier système du leader mondial dans le domaine. Windows 10. Celui-ci, largement controversé mais aussi de plus en plus apprécié, présente un ensemble d'avantages et d'inconvénients que nous essayerons de partager avec le lecteur.

Présentation de Windows et de Windows 10

En général…

Microsoft Windows est une gamme de systèmes d'exploitation de Microsoft destiné aux ordinateurs compatibles PC. La caractéristique principale de Windows de façon générale est sa gestion cohérente, normalisée, à l'aide de symboles, menus et champs de dialogue graphiques que l'on active généralement par un clic de la souris.

Le nom « Windows », l'anglais littéral de « Fenêtres », provient du fait que la surface de travail, où se trouvent les programmes et les documents, est exploitée en fenêtres. C'est cette simplicité et ergonomie graphique qui a fait le succès de Windows.

Windows se présente sous plusieurs branches en parallèle :

- Windows NT anciennement 9x : Système d'exploitation pour PC personnel portable ou bureau.
- Windows CE : Pour les systèmes embarqués et d'autres systèmes minimalistes ou mobile.
- Windows Server : Système d'exploitation réseaux orienté serveurs.

Un peu d'histoire…

- **Tout commence en 1975** lorsque Bill Gates et Paul Allen forment un partenariat baptisé Microsoft où ils rêvent de l'idée d'un ordinateur personnel sur tous les bureaux et dans toutes les maisons.
- **En 1980**, l'entreprise commence à grandir et Microsoft se penche sur un nouveau système d'exploitation, c'est-à-dire le logiciel fait le lien entre le matériel et les programmes de l'ordinateur, comme un traitement de texte. Il s'agit de la base sur laquelle un programme informatique peut s'exécuter. Ils appellent leur nouveau système d'exploitation « MS-DOS ».

MS-DOS est efficace mais se révèle difficile à comprendre pour la plupart des gens. Il doit y avoir une meilleure façon de construire un système d'exploitation.

- **Entre 1985 et 1990** Microsoft va lancer successivement Windows 1.0, 2.0 et 2.11 Il n'est plus nécessaire de taper des commandes comme sur MS-DOS, des menus déroulants, des icônes, des boites de dialogues et les fameuses fenêtres aux quelles Windows doit son nom, font leur apparition.
- **Entre 1991 et 1995** Windows voit l'apparition des graphismes avancés. Les machines disposent d'une palette de 16 couleurs perfectionnées avec Windows 3.0 et le succès de l'OS pousse Microsoft à l'accompagner avec un SDK (kit de développement) pour les développeurs.
- **Entre 1995 et 2000** le PC arrive à maturité et Internet apparaît. Ce qui pousse Windows à intégrer des fonctionnalités adaptées aux nouveautés.
- **Entre 2000 et 2005** Windows XP est lancé avec une nouvelle ergonomie ciblée sur l'utilisabilité et le centre unifié de services d'aide et d'assistance. Il est proposé dans 25 langues. Avec un design visuel clair et simplifié c'est un vrai succès
- **Entre 2006 et 2008** Microsoft lance Windows Vista et l'équipe d'un système de sécurité renforcé surtout avec le contrôle des comptes utilisateurs.
- **Entre 2009 et 2014** Microsoft lancera Windows 7 et 8 qui sont une réaction à monde sans fil du début des années 2010. Ils introduisent l'interface tactile à Windows, et réinventent l'expérience visuelle de l'utilisateur.

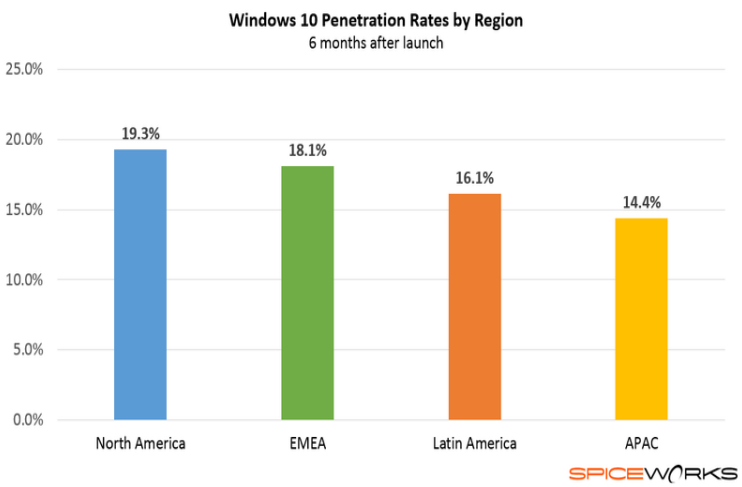
Enfin, en 2015 Microsoft lance Windows 10 disant que celui-ci est le meilleur système jamais créé. Nous allons nous intéresser un peu plus en détail à ce système. Pour ensuite exposer les avantages et inconvénients sécuritaires qu'il présente.

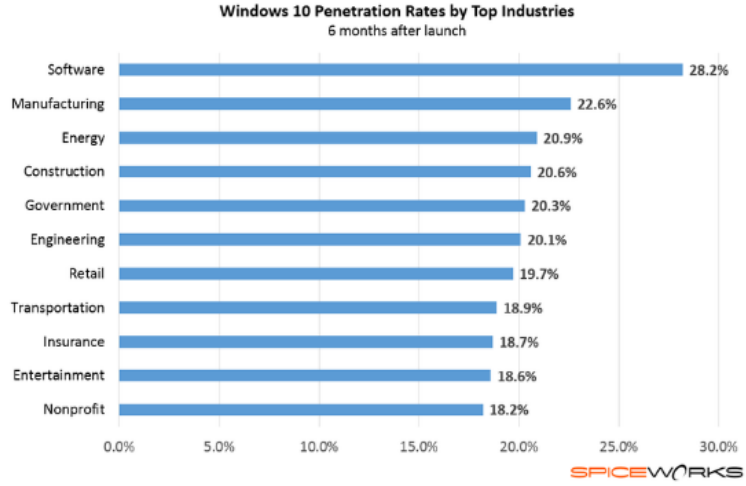
Windows 10 le lancement…

Windows 10 est lancé le 29 juillet 2015 dans une ouverture mondiale. La grande nouveauté est qu'il soit proposé gratuitement à tous les détenteurs de licence Windows 7 ou Windows 8.1. C'est la première fois qu'un système Windows et lancé gratuitement.

Ce lancement était très mitigé dans la communauté informatique cela à cause de quelques failles sécuritaires dont nous allons parler dans le volet inconvénients plus bas.

Mais le succès n'a pas tardé à amortir le lancement controversé car après 6 mois de son lancement il est largement adopté dans le monde et dans les différentes industries.





Taux de pénétration de Windows 10 dans différentes régions du monde ainsi que dans les plus grandes industries après 6 mois de son lancement

Quelque caractéristiques techniques…

Type de noyau de système : Noyau hybride (à la fois monolithique et micronoyau)

Plateforme : ordinateur de bureau, ordinateur portable, tablette tactile, smartphone, montre connectée

Architectures : Intel/AMD/x86/x64

Services supplémentaires :

Cortana : assistante personnelle virtuelle compatible avec la voix.

DirectX 12 : Bibliothèques pour la programmation d'application multimédia et jeux.

Avantages sécuritaires de Windows 10

Les principaux avantages sécuritaires de Windows 10 proviennent d'une batterie de nouvelles fonctionnalités incorporées dans le système afin de mieux protéger les informations des utilisateurs.

Ceux-ci viennent s'ajouter aux fonctionnalités déjà existantes lors des précédentes versions comme BitLocker pour le chiffrement des données, ou Windows Defender qui existent déjà depuis Windows 7.

Nous allons nous intéresser à ces nouvelles fonctionnalités qui apportent un plus au système de sécurité de Windows. Ces fonctionnalités sont classées selon le type d'utilisateur ciblé. Essentiellement il y a deux types. Les fonctionnalités destinées aux entreprises qui utilisent Windows 10 et les autres qui sont destinées aux utilisateurs d'ordinateurs personnels. Intéressons-nous de plus près à ces fonctions.

Avantages Entreprises :

Device Guard

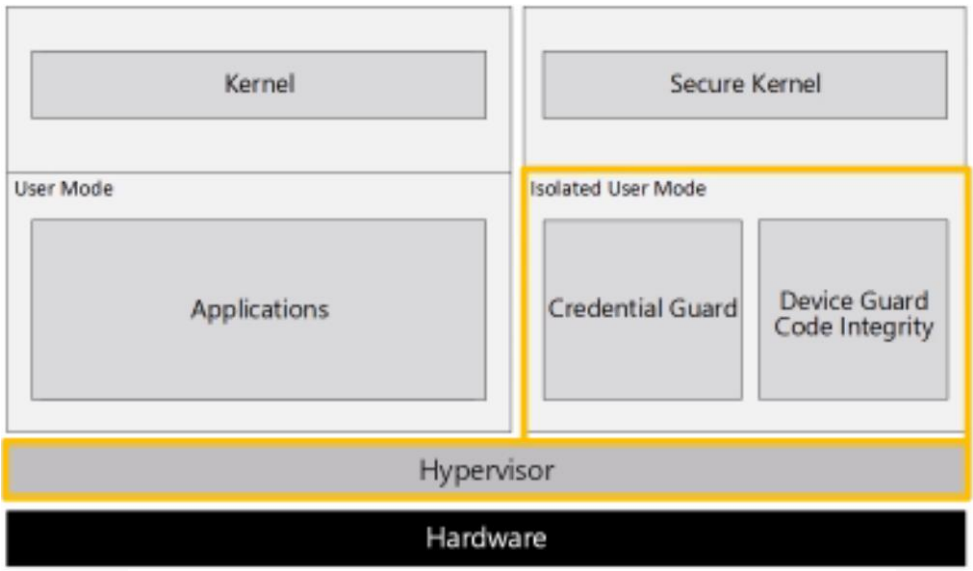
Device Guard est une nouvelle fonctionnalité de Windows 10 exclusive à l'édition entreprise. Il vise à lutter contre les malwares de manière efficace il s'agit d'un formidable complément aux outils de sécurité traditionnels.
Lors du lancement d'une application Windows 10 se charge de déterminer si elle est approuvée ou non par la politique d'entreprise et en avertit l'utilisateur. Device Guard donne le contrôle sur les applications autorisés à s'exécuter ainsi seul les logiciels, applications, scripts et drivers approuvés par l'entreprise sont utilisables sur un appareil ou Device Guard est configuré.

Le mode le plus robuste de Device Guard repose sur la virtualisation. Ainsi des prérequis matériels spécifiques doivent être présents pour prendre en charge les fonctions de virtualisation Hyper-V.
Le mode de lancement UEFI Secure Boot est également requis pour le bon fonctionnement.

Le processus basé sur la virtualisation va isoler les processus critiques et la mémoire associée, du reste du système d'exploitation. Lorsque la protection est activée, les processus critiques s'exécutent alors dans un mode utilisateur isolé.

Le composant qui détermine si l'application est approuvée se nomme Code Integrity. Celui-ci est configurable à partir d'un fichier de politique qui est chargé au démarrage de l'appareil.

Device Guard ne s'active pas à l'appui d'un bouton. En effet il nécessite la signature électronique de l'entreprise le désirant, du code de confiance, et une configuration au préalable adaptée à chaque politique de sécurité de chaque entreprise.



Structure du noyau système en utilisant Device Guard

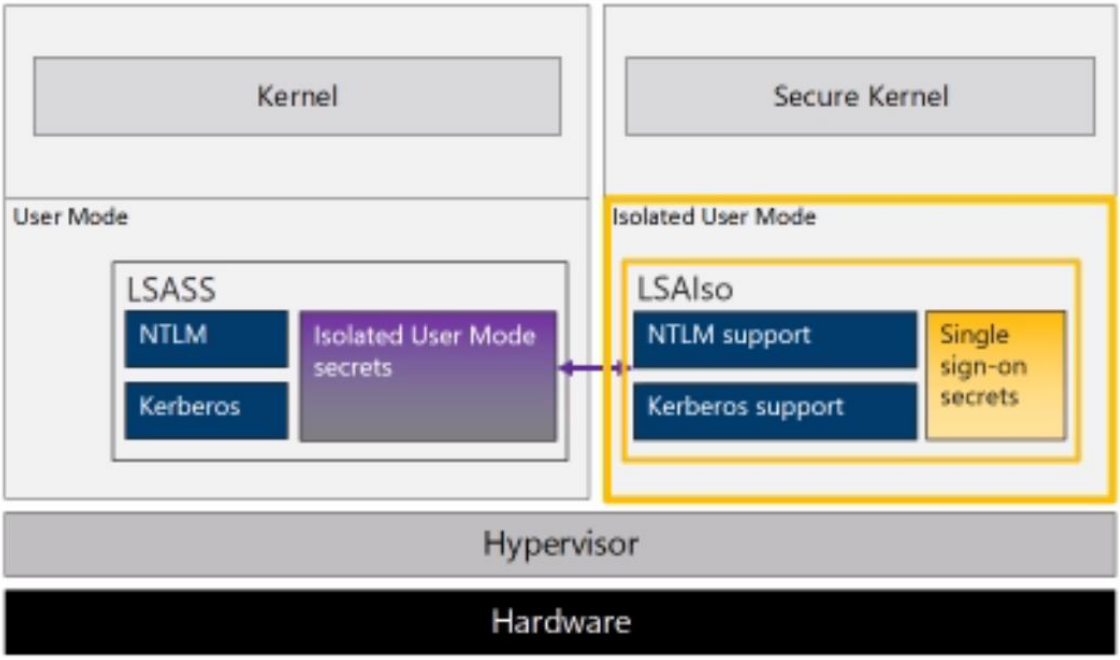
Credential Guard

Il s'agit d'une autre nouveauté de Windows 10 en termes de sécurité exclusive à l'édition entreprise. Le rôle principal de Credential Guard est de protéger contre le vol d'information d'authentification en rendant inopérant les outils de type Mimikatz[1] qui sont fréquemment utilisés lors des cyber-attaques.

Comme l'outil précédent Credential Guard utilise l'environnement d'exécution Hyper-V basé sur la virtualisation, pour isoler les secrets d'authentification du reste du système d'exploitation au niveau du noyau virtuel. Ainsi même des malwares s'exécutant avec des privilèges élevés ne peuvent plus extraire en mémoire les credential NTLM[2] et Kerberos[3]. C'est une excellente protection contre les attaques de type pass-the-hash (contournement de hachage), ou pass-the-ticket (contournement de ticket).

Les attaques visant les informations d'authentifications sont très répandues dans le milieu des entreprises et cela peut concerner des enjeux majeurs. Credential Guard a l'avantage de ne nécessiter aucun prérequis matériel.

1 : Des outils qui extraient de la mémoire de données d'authentification comme les mots de passe, les codes PIN, et les tickets Kerberos tout en contournant les hachages.
2 : Un protocole d'authentification utilisé dans les réseaux de machines utilisant un système Windows.
3 : Microsoft Kerberos et un paquet de sécurité composé de protocole d'authentification et de mécanismes de protection basé sur un système de tickets avec des niveaux de confiance.



Fonctionnement : LSASS est le service d'authentification dans Windows qui permet de déterminer l'identité d'un utilisateur sur Windows qui se sert d'un mot de passe ou d'une autre méthode d'authentification, Credential Guard isole les données de sécurité précédemment stockées dans l'autorité de sécurité locale LSA en utilisant la sécurité basée sur le noyau virtuel sécurisé. Le processus LSASS (à gauche) communique alors avec le processus LSA Isolé en utilisant des appels de procédures externes. Les données stockées en utilisant la sécurité basée sur la virtualisation ne sont plus extractibles à partir du système d'exploitation.

Entreprise Data Protection

Une nouvelle fonctionnalité de Windows 10 orientée données. Destinée aux entreprises.

A quoi sert EDP ?

Un scénario classique en entreprise est quand un appareil est utilisé de façon mixte c'est-à-dire à la fois personnelle et professionnelle, l'utilisateur va manipuler des données privées et des données d'entreprise. L'objectif est d'être capable de différentier ces deux types de données et bien sûr d'apporter une protection aux données de l'entreprise. On veut également éviter les fuites d'informations involontaires par exemple un copier/coller un peu rapide de l'utilisateur depuis un document tagué entreprise vers un document non-protégé ou une application non-autorisée.
Quand on parle de protection on parle de **chiffrement**. Le point important c'est que les données sont chiffrées au niveau du fichier, l'utilisateur n'est donc pas restreint à utiliser des fichier spéciaux conteneurs et d'applications capables d'accéder à ces fichier conteneurs. L'interface doit permettre à l'utilisateur d'identifier facilement les fichiers protégés. Et enfin la protection doit être conservée lors de la copie du fichier par exemple sur une clé USB.

Comment protéger les données ?

EDP nous offre la possibilité de protéger un document. Tout simplement par un clic droit sur le fichier et en choisissant « Encrypt To » on sélectionne ensuite l'entité de l'entreprise. Le fichier sera aussi tôt marqué comme fichier entreprise protégé.

Quelles applications peuvent manipuler les données protégées de l'entreprise ?

Il y a deux catégories d'applications :

Les applications éclairées : adaptées pour prendre en compte la notion de données d'entreprise. Celles-ci sont capable d'ouvrir et de modifier les fichiers protégés et de conserver la protection si elle existait initialement.

Les applications non-éclairées : doivent être paramétrées par l'administrateur pour pouvoir manipuler les données chiffrées.

Dans ces deux catégories l'administrateur a le choix d'autoriser ou non des applications à manipuler les données d'entreprise protégées par chiffrement.

Qui décide de ce qui est protégé ou pas ?

L'utilisateur peut définir si un fichier sur lequel il travaille est classé entreprise ou non. L'administrateur aussi peut définir des politiques concernant les emplacements et les sources des fichiers.
Par exemple : Tout les fichiers qui proviennent de l'intranet sont sécurisés et classés comme fichiers entreprise.

EDP en conclusion ?

Entreprise data protection est un outil de sécurité additionnel qui vient s'ajouter à la ceinture des utilisateurs de Windows 10 au niveau de l'entreprise et sa simplicité et son efficacité vient accentuer l'avantage qu'il représente et la valeur sécuritaire ajoutée au système d'exploitation.

Avantages Utilisateurs

Authentification renforcée par « Windows Hello » et « Windows Passport » :

L'ère du simple mot de passe pour accéder à son ordinateur est révolue. Pour rendre plus difficile l'accès à un ordinateur en cas de perte ou de vol, et plus généralement mieux protéger le terminal, Windows 10 intègre un système de double authentification.

L'utilisateur et la machine c'est-à-dire ordinateur, tablette ou smartphone, deviennent les deux composants nécessaires au bon fonctionnement de l'appareil grâce aux deux modules « Hello » et « Passeport ».

Windows Hello :

Windows Hello est un système d'authentification biométrique qui permet de reconnaître l'utilisateur grâce à son iris, son visage ou son empreinte digitale.

Pour pouvoir utiliser et mettre en œuvre la reconnaissance faciale il faut que le pc, la tablette ou le smartphone soient équipés d'un capteur.

Pour que Windows Hello puisse fonctionner sur notre machine, cette dernière doit disposer de trois éléments :

- L'élément central qui est une caméra haute définition qui travaille en lumière visible.
- Un émetteur laser qui émet de l'infrarouge.
- Le récepteur équivalent qui va recevoir la lumière infrarouge.

Les deux derniers éléments combinés vont pouvoir être capable de donner une image en 3D de la scène et donc du visage qui va se présenter.

Remarque : si l'utilisateur n'est pas à l'aise avec cette technologie, il peut la remplacer par un code PIN ou le mot de passe classique.

Windows Passeport :

Il s'agit d'un système d'authentification qui permet à un smartphone par exemple, d'agir comme une smartcard pour déverrouiller l'accès à la machine, à des sites web, services ou applications.

Sur Windows 10, Microsoft Passeport remplace les mots de passe par une authentification forte à deux facteurs se composant d'un appareil inscrit et d'un Windows Hello (biométrique) ou d'un code confidentiel.

Microsoft Passeport contribue à protéger l'identité de l'utilisateur et ses informations d'identification, vu qu'il remplace les mots de passe par une authentification forte à deux facteurs se composant d'un appareil inscrit et d'un Windows Hello ou d'un code confidentiel, et comme aucun mot de passe n'est utilisé, cela permet de contourner les attaques d'hameçonnage et en force brute.

Cela permet également d'empêcher les violations de serveur, car les informations d'identification Microsoft Passeport sont une paire de clés asymétriques, ce qui empêche les attaques par relecture lorsque ces clés sont générées dans des environnements isolés de modules de plateforme sécurisée (TPM).

Démarrage sécurisé (secure boot):

Windows 10 bloque les voies qui permettent aux logiciels malveillants de ne pas être vus par le système d'exploitation en démarrant en premier. Avec la virtualisation au niveau matériel, les processus clés sont également isolés du système pour ne pas être falsifiés.

Confidentialité :

Windows 10 peut être amené à sauvegarder de très nombreuses informations, certaines pour des statistiques et diagnostique, et d'autres pour des raisons personnelles.

Géolocalisation, évènements du calendrier, frappes au clavier, identifiant de publicité, données de navigation, rapports d'erreurs et autres ont tous une option qui permet de contrôler soigneusement ce que l'on souhaite envoyer.

Remarque : Toutes ces options sont activées par défaut.

Toutes les options reliées à l'envoi de données sont paramétrables, il suffit de cliquer sur « paramètres de personnalisation » et entrer dans une phase de réglage à deux écrans qui nous permet de, couper complétement la géolocalisation, désactiver certaines options liées aux données de navigation et au partage des accès Wi-Fi …etc.

Synthèse des avantages

On peut déduire de ces avantages que Microsoft a très clairement fourni un effort considérable sur la sécurité surtout que celle-ci représente un argument de vente et de publicité important. Les systèmes doivent être de plus en plus sécurisés pour faire face à la menace de malveillance qui est de plus en plus présente.

La réaction rapide de Microsoft aux changements de l'environnement sécuritaire des systèmes est un atout considérable. On trouve que chacune de ces fonctionnalités ciblent un problème donné qui aurait apparu récemment. Cette réactivité permet à Windows de rester compétitif et leader du marché.

En guise de gage de confiance et de preuve de qualité de la sécurité de Windows 10 ; on peut mentionner que très récemment le Département de Défense des états unis a pris la décision en Février 2016 de passer à Windows 10 à partir de 2017 dans ses systèmes. Le DoD prévoit de déployer le système sur 4 millions de machines durant l'année en cours.

Cette décision témoigne de la qualité sécuritaire de Windows 10, ceci-étant que le Department of Defense est considéré comme une référence en termes de sécurité sur tous les domaines.

Inconvénients de Windows 10 :

Télémétrie :

Microsoft définit la télémétrie de la manière suivante : il s'agit de « données systèmes qui sont téléchargées par le composant Connected User Experience et Telemetry », également connu sous le nom de Universal Telemetry Client, ou service UTC. Des analystes interprètent ce fait comme étant un espionnage et une violation de la vie privée de l'utilisateur.

Des études ont montré que Windows 10 est un système d'exploitation qui collecte plusieurs informations sur nos habitudes devant nos Ordinateurs, et il est possible en revanche de supprimer une partie de ces informations en utilisant un logiciel Open Source bien conçu pour cet usage. Mais la question qui se pose est la suivante : est-t-il suffisant pour réduire l'étendue de l'espionnage mis en place par Microsoft ?

Des spécialistes ont effectué une analyse réseau, qui a montré que l'utilisation du cloud de Windows10 transforme cet OS en sorte de terminal communiquant constamment avec les serveurs de Windows.

En analysant le trafic réseau d'un ordinateur sous Windows 10 voici les informations collectées :

Le texte tapé au clavier :

Tout le texte qui est tapé sur le clavier de l'ordinateur (informations confidentielles, mots de passe, identifiants bancaires …) est stocké dans des fichiers temporaires à l'aide d'un enregistreur de frappes et envoyés après toutes les 30 minutes aux serveurs suivants :

```
oca.telemetry.microsoft.com.nsatc.net
pre.footprintpredict.com
reports.wes.df.telemetry.microsoft.com
```

Remarque : Ceci est inévitable, même lors de l'utilisation du clavier virtuel.

Les numéros de téléphones tapés sur le navigateur :

Lors d'une recherche d'un numéro sur internet, un processus se déclenche et envoie ce numéro aux serveurs suivants :

```
vortex.data.microsoft.com
vortex-win.data.microsoft.com
telecommand.telemetry.microsoft.com
telecommand.telemetry.microsoft.com.nsat
c.net
oca.telemetry.microsoft.com
oca.telemetry.microsoft.com.nsatc.net
sqm.telemetry.microsoft.com
sqm.telemetry.microsoft.com.nsatc.net
```

La liste des fichier audio et vidéos de l'ordinateur :

Lors d'une recherche locale c'est-à-dire sur l'ordinateur et non pas sur internet, un processus liste tous les fichiers médias qui existe sur l'ordinateur et une fois connecté, ce même processus se chargera de transmettre cette liste sur les serveurs suivants :

```
df.telemetry.microsoft.com
reports.wes.df.telemetry.microsoft.com
cs1.wpc.v0cdn.net
vortex-sandbox.data.microsoft.com
pre.footprintpredict.com
```

Un extrait des sessions Webcam :

Lors de l'activation de la webcam, 35 Mo de données sont envoyés aux serveurs suivants :

```
oca.telemetry.microsoft.com
oca.telemetry.microsoft.com.nsatc.net
vortex-sandbox.data.microsoft.com
i1.services.social.microsoft.com
i1.services.social.microsoft.com.nsatc.n
```

Tout ce qui est dit au Micro est transmis à Microsoft :

Est ceci arrive même si Cortana (l'assistant à reconnaissance vocale de Microsoft) n'est pas activée, ou complétement désinstallé.

Les échantillons de voix sont envoyés aux serveurs suivants :

```
oca.telemetry.microsoft.com
oca.telemetry.microsoft.com.nsatc.net
vortex-sandbox.data.microsoft.com
pre.footprintpredict.com
i1.services.social.microsoft.com
i1.services.social.microsoft.com.nsatc.n
et
telemetry.appex.bing.net
telemetry.urs.microsoft.com
cs1.wpc.v0cdn.net
statsfe1.ws.microsoft.com
```

Lorsque Cortana est activée, ce qu'elle collecte est également retranscrit sous format textuel et envoyé aux serveurs suivants :

```
pre.footprintpredict.com
reports.wes.df.telemetry.microsoft.com
df.telemetry.microsoft.com
```

Remarque : Si Windows est laissé sans activité pendant plus de 15 minutes, une grande quantité de données est envoyée aux serveurs de Microsoft.

Des inquiétudes fortes sur la sécurité sur Wi-Fi Sense :

Avec Wi-Fi Sense, Windows 10 propose de partager une connexion Wi-Fi d'un utilisateur du nouvel OS de Microsoft avec ses contacts Skype, Outlook.com ou encore Facebook. Les utilisateurs de ces applications pourront ainsi partager leurs mots de passe de connexion de manière transparente. Cette fonctionnalité a pour but de rendre plus simple l'accès à une connexion Internet en mode nomade, et ce en connectant automatiquement les appareils à des hotspots Wi-Fi.

Même si le mot de passe n'est pas révélé, le fait qu'il soit sauvegardé par Microsoft et par extension la diffusion aux contacts, constitue selon les spécialistes un potentiel problème de sécurité et de confidentialité.

C'est une « méthode de piratage pas chère » mentionne Craig Mathias, de FairPoint Group, dans PCWorld, qui précise que selon lui « personne ne devrait laisser un accès Wi-Fi grand ouvert ».

En guise de réponse, Microsoft mentionne que le partage de connexion via Wi-Fi Sense ne doit permettre que d'accéder à Internet, et en aucun cas au réseau local, Et que les identifiants de connexions sont, selon une FAQ de Microsoft, « envoyés via une connexion chiffrée et stockés dans un fichier sécurisé sur un serveur Microsoft puis retournés toujours à travers une communication chiffrée sur le téléphone de vos contacts s'ils utilisent la fonction WiFi Sense et s'ils sont à portée du réseau Wi-Fi partagé ».

Synthèse sur les inconvénients

Bien que Windows 10 apporte une protection à la vulnérabilité traditionnelle des malwares et des attaques externes avec son ensemble d'outil, la menace principale provient de Microsoft eux-mêmes.

En effet l'analyse du trafic de données a révélé que Windows 10 ne peut pas s'arrêter d'envoyer des informations à Microsoft. La sortie de ses données porte atteinte à la confidentialité des utilisateurs qui ne désirent pas que leurs données voyagent à travers le monde pour tomber entre les mains d'inconnus d'une part. Et d'autre part ceci crée une vulnérabilité, car comme nous le savons toute donnée transmise sur le réseau est susceptible d'être interceptée par des individus malveillants.

De plus, les données personnelles sont susceptibles d'être vendues par Microsoft à des gens qui seraient prêts à mettre le prix pour savoir ce que nous faisons et avoir accès à nos navigations, fichiers, recherches, webcam, micro…

Ils existeraient deux types d'acheteurs à nos informations :

- Les organismes de renseignements tels que la CIA ou le FBI ou encore le MOSSAD Israélien.
- Les compagnies publicitaires qui ça arrangerait de connaitre les préférences du public pour pouvoir toujours lui proposer des offres de plus en plus attirantes.

Ces risques sont réels. Peut-être est-ce de la paranoïa de tirer ces conclusions sans preuves, mais les soupçons sont de plus en plus grands. Et les enjeux bien vraisemblables.

Conclusion

Le système d'information d'une entreprise peut être vital à son fonctionnement. Il est donc nécessaire d'assurer sa protection, afin de lutter contre les menaces qui pèsent sur l'intégrité, la confidentialité et la disponibilité des ressources.

La malveillance informatique est souvent à l'origine de ces menaces, qu'il s'agisse de vol d'information ou de sabotage, n'importe qui pouvant s'improviser pirate informatique avec des outils adaptés.

Le choix du système d'exploitation des machines joue un rôle primordial dans la sécurité et nous avons vu que Windows 10 bien qu'imparfait et controversé, propose un tas d'outils de sécurité très efficaces.

Cependant, les soupçons et la controverse portée sur Microsoft sur son dernier OS pousse tout de même à se méfier et à ouvrir l'œil sur ce qui se fait. Et ne pas être dupe.

Nous espérons que cet exposé a pu nous éclairer sur le volet sécurité primordial dans le système que beaucoup d'entre nous utilisent déjà, et d'autres pas, Windows 10.

Notre travail incitera-t-il peut être quelque uns à adopter ce système et d'autre à y renoncer éventuellement ?

Références Bibliographiques

Outils de sécurité : Travaux et vidéos de Arnaud Jumelet de la Direction Technique et Sécurité de Microsoft France

Articles inconvénients :

- Peter Bright pour ARS Technica http://arstechnica.com/information-technology/2015/08/even-when-told-not-to-windows-10-just-cant-stop-talking-to-microsoft/
- Simon Rockman pour The Register http://www.theregister.co.uk/2015/06/30/windows_10_wi_fi_sense/

Analyse trafic réseau : Analyse du bloggeur spécialiste en sécurité Nikopik http://www.nikopik.com/2015/08/une-analyse-de-trafic-reseau-de-windows-10-devoile-lincroyable-etendue-de-lespionnage-mis-en-place-par-microsoft.html

Department of Defense Windows 10: https://blogs.windows.com/windowsexperience/2016/02/17/us-department-of-defense-commits-to-upgrade-4-million-seats-to-windows-10/