SOPHOS

Les bonnes pratiques de la sécurité informatique en entreprise

Ce que vous ne pouvez pas ne pas savoir

A Sophos Whitepaper July 2015

SOPHOS

Sommaire

1. Sécurité et produits de sécurité

Votre vie personnelle et professionnelle est remplie d'incertitudes. C'est notamment le cas lorsque vous prenez votre voiture, lorsque vous bricolez, ou encore lorsque vous prenez les transports en commun.

Dans chacun de ces cas de figure, des éléments techniques et technologiques visent à augmenter votre confort, assurer votre sécurité, ou rendre l'objet utilisé plus accessible.

L'élaboration des matériels que vous employez inclut la plupart du temps des mécanismes de sécurité, tels que la ceinture de sécurité pour la voiture, les messages d'annonce de l'arrivée d'un train, des gants et lunettes de protection pour un outil de bricolage.

Bien que votre voiture dispose de freins, ABS, airbags et ceintures de sécurité, ces éléments ne suffisent pas à garantir votre sécurité, et le comportement du conducteur doit être responsable afin de ne pas mettre en péril sa sécurité ainsi que celle de ses passagers. Il en va de même pour les produits de sécurité informatique qui à eux-seuls, ne suffisent pas à garantir votre sécurité et l'attention de l'utilisateur est donc requise.

Ce n'est pas parce que vous disposez de produits de sécurité antivirus qu'aucune infection ne peut subvenir, et ce n'est pas parce que vous disposez de pare-feu protégeant les frontières de votre entreprise qu'aucune intrusion ne peut aboutir, la non vigilance de l'utilisateur et les techniques d'ingénierie sociale faisant partie de l'attirail dont bénéficient les attaquants afin de vous atteindre.

Les conséquences d'une attaque réussie peuvent être multiples, et peuvent par exemple résulter en une perte ou un vol d'informations, une indisponibilité de votre messagerie d'entreprise ou encore de votre chaine de production.

Nous verrons dans ce document les fausses idées les plus fréquentes et les moyens humains et technologiques permettant de réduire le niveau de risque auquel votre organisation est confrontée au quotidien, souvent sans que vous-même ou vos utilisateurs n'en soient conscients.

Nous espérons que la lecture de ce document vous permettra d'y voir plus clair sur les menaces et comment réduire le facteur de risque induit par ces dernières.

Sophos et ses partenaires peuvent vous accompagner afin de mettre en œuvre des stratégies de défense efficaces qui amélioreront encore votre niveau de sécurité et réduiront le risque auquel votre organisation est exposée au quotidien.

2. En bref dans ce document

Négligence des mobiles

(plus de détails en page 7)

Risques	Vol de données, conséquences financières, perte de productivité
Vecteurs d'attaque	Codes malveillants (+1800% ces 12 derniers mois), Ingénierie sociale, négligence utilisateur
Moyens de s'en prémunir	Utilisez une solution de MDM pour assurer la conformité des terminaux incluant une solution anti-malware

Menaces sur les Mac

(plus de détails en page 10)

Risques	Infection virale, perte et vol de données, indisponibilité de service
Vecteurs d'attaque	Code malveillant, ingénierie sociale
Moyens de s'en prémunir	Installez une solution de protection (antivirus) y compris sur les Mac, appliquez-leur le même filtrage web que les autres machines

Réseaux Wifi non sécurisés

(plus de détails en page 13)

Risques	Espionnage des réseaux, usurpation d'identité, atteinte aux données
Vecteurs d'attaque	Accès trop permissif, WiFi ouvert, WiFi mal sécurisé
Moyens de s'en prémunir	Séparation des réseaux invités des réseaux d'entreprise, identification des utilisateurs, vérification de la conformité des terminaux

Pare-feu défaillant

(plus de détails en page 15)

Risques	Contournement des protections, intrusion, espionnage, ralentissement ou perte de productivité
Vecteurs d'attaque	Multiples
Moyens de s'en prémunir	Installez un pare-feu de nouvelle génération et utilisez ses fonctions avancées

Documents et correspondances non chiffrées

(plus de détails en page 20)

Risques	Divulgation d'informations sensibles, atteinte aux données, pénalités financières
Vecteurs d'attaque	Vol de machine, vol de documents, interception d'email
Moyens de s'en prémunir	Chiffrement d'emails, de disque et de fichiers

Pratique de surf sur Internet

(plus de détails en page 25)

Risques	Infections des machines, vol d'information, usage inapproprié du web
Vecteurs d'attaque	Site légitime piraté, ingénierie sociale, spam, phishing
Moyens de s'en prémunir	Solution de filtrage web complète avec filtrage HTTPS et prise en compte des URLs malveillantes

3. Eventail des menaces

3.1. Négligence des mobiles

Pour aller à l'essentiel	
Risques	**Vol de données, conséquences financières, perte de productivité**
Vecteurs d'attaque	**Codes malveillants (+1800% ces 12 derniers mois), Ingénierie sociale, négligence utilisateur**
Moyens de s'en prémunir	**Utilisez une solution de MDM pour assurer la conformité des terminaux incluant une solution anti-malware**

3.1.1. Les risques

La négligence des mobiles est une problématique qui devient de plus en plus importante et ce pour deux raisons principales.

Premièrement, la pratique montre que les utilisateurs de mobiles ont tendance à laisser leurs données exposées. Il est facile, sans le vouloir, de fournir un point d'accès aux pirates et aux voleurs de données en « jailbreakant » son iPhone, en téléchargeant des applications Android depuis un store non officiel ou encore en laissant son écran déverrouillé (fr3.securityreflex.net) .

La deuxième raison est la forte croissance des malwares sur les mobiles. Les SophosLabs ont observé une croissance exponentielle de 1 800% des malwares ciblant les systèmes Android au cours des 12 derniers mois (soit 18 fois plus aujourd'hui qu'il y a un an).

Les conséquences liées à cette négligence sont:

- **Le vol de données:** si un téléphone est volé ou infecté par un malware, des données sensibles de l'entreprise sont susceptibles de se retrouver entre de mauvaises mains.
- **Conséquences financières:** les frais liés aux spams de SMS surtaxés, les appareils devant être remplacés et les coûts occasionnés par les violations de données sont quelques exemples de l'impact financier potentiel.
- **Perte de productivité:** les utilisateurs et le personnel informatique peuvent perdre un temps précieux face aux conséquences d'un appareil compromis: la récupération de l'appareil, le nettoyage de l'infection, les problèmes de performances...

En résumé, la négligence des mobiles peut avoir de profondes répercussions.

3.1.2. Les vecteurs d'attaque

Prenons l'exemple d'une variante de malware Android connue sous le nom de ***NotCompatible***, qui a été découverte en 2012 mais qui est devenue plus active et dangereuse récemment. Dans les premiers jours, elle a simplement agi comme un proxy sur les systèmes infectés, ne causant aucun dommage direct.

La dernière variante – ***NotCompatible.C*** – a placé la barre encore plus haute en termes de sophistication et de complexité opérationnelle des malwares mobiles. Elle a créé l'un des botnets mobiles les plus longs jamais vus auparavant. C'est un parfait exemple qui illustre comment les malwares mobiles gagnent en complexité et empruntent des techniques jusqu'alors réservés aux PC. C'est une pratique très sophistiquée, mature et résiliente. Par exemple, les serveurs de Command and Control (C&C) se régénèrent, se protègent eux-mêmes avec la redondance et le chiffrement, donc si un serveur est éliminé par les autorités, de nouveaux apparaitront automatiquement.

Il est distribué via le spam et des sites Web piratés et infectés, il utilise des astuces d'ingénierie sociale pour se propager sur les appareils des utilisateurs.

Cela a été observé sur 1 à 2% des appareils... et lorsque vous pensez au nombre d'appareils qui sont en circulation sur votre réseau mais aussi en dehors de votre réseau, c'est largement trop.

Une fois sur un appareil, le malware peut utiliser celui-ci au gré des pirates... comme pour envoyer du spam ou acheter des billets en ligne et les revendre à profit.

Mais les pirates et les auteurs de ce malware réalisent qu'ils n'ont pas encore exploité tout son potentiel, notamment en termes d'espionnage industriel et de vol de données...

Le malware peut facilement identifier le réseau sur lequel il se trouve et relayer cette information aux serveurs C&C, qui peuvent ensuite utiliser l'appareil comme plate-forme pour lancer une attaque ATP ciblée en l'utilisant comme un proxy pour d'autres systèmes.

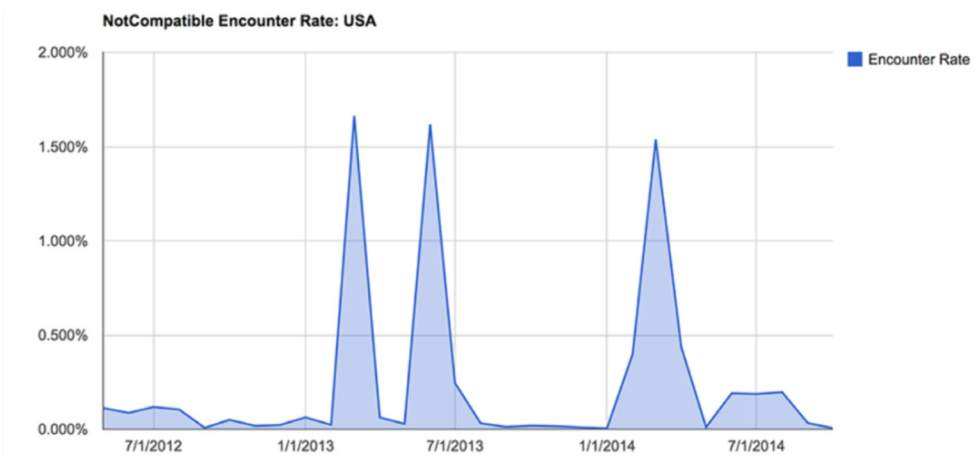

Figure 1: Présence du malware NotCompatible aux Etats Unis sur les dernières années.

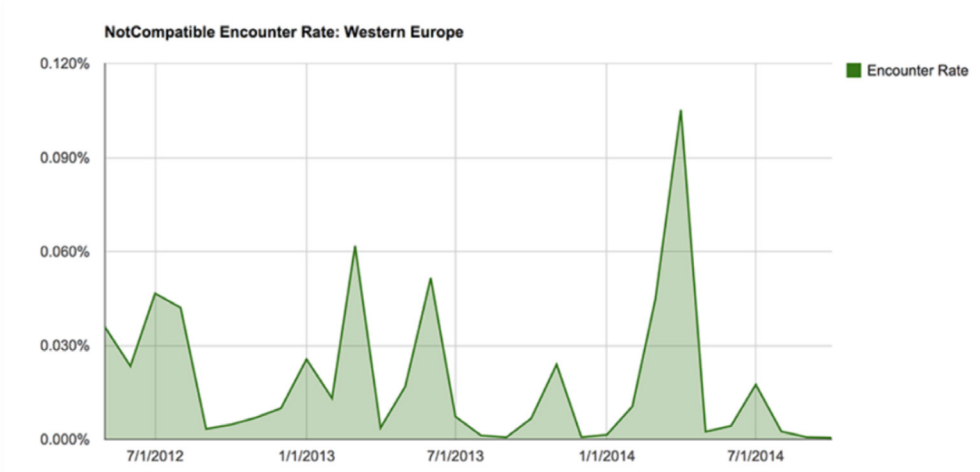

Figure 2: Présence du malware NotCompatible en Europe de l'Ouest sur les dernières années.

3.1.3. Les moyens de s'en prémunir

Vous avez besoin d'une solution qui vous permette de gérer et de sécuriser vos mobiles s'intégrant parfaitement à la sécurité de votre réseau d'entreprise afin de laisser vos employés accéder aux ressources de l'entreprise partout sans mettre en péril ces données sensibles.

Assurez-vous que vous avez une solution de type MDM qui puisse vous aider à:

- Appliquer des mots de passe sécurisés et à effacer les appareils ayant été perdus.
- Contrôler les applications indésirables et bloquer les malwares Android.
- Prévenir ou identifier les appareils jailbreakés.

Et assurez-vous également que votre solution mobile s'intègre à votre pare-feu next-gen pour:

- Empêcher les appareils non conformes ayant été jailbreakés ou infectés de rejoindre votre réseau d'entreprise.
- Identifier les appareils ayant été infectés par des menaces persistantes avancées (APT) ou communiquant avec les serveurs command and control.

3.1.4. Pour aller plus loin

Si vous êtes intéressé pour en savoir plus, plusieurs livres blancs sur les mobiles, leur sécurité et la gestion du BYOD en entreprise sont à votre disposition depuis notre site web.

blog.SophosFrance.fr est un blog de sécurité dédié aux utilisateurs et responsables IT. Découvrez chaque semaine plusieurs alertes et astuces pour garder en sécurité les données de votre entreprise. Non seulement les données d'entreprise mais surtout vos données à caractère personnel. Abonnez-vous gratuitement à la newsletter.SophosFrance.fr, garantie zero spam.

3.2. Menaces sur les Mac

Pour aller à l'essentiel

Risques	**Infection virale, perte et vol de données, indisponibilité de service**
Vecteurs d'attaque	**Code malveillant, ingénierie sociale**
Moyens de s'en prémunir	**Installez une solution de protection (antivirus) y compris sur les Mac, appliquez-leur le même filtrage web que les autres machines**

3.2.1. Les risques

Les gens ont l'habitude de dire que les Mac sont parfaitement sûrs et qu'il n'existe pas de malwares sur Mac. Mais nous savons tous que le paysage a changé. Justement parce que les Mac gagnent en popularité... ils sont devenus une cible majeure pour les pirates. Mais bon nombre d'entre eux ne sont pas correctement protégés contre les malwares et la perte de données.

Les menaces sont réelles et vous ne pouvez pas vous permettre de faire l'impasse sur cette plate-forme:

- Les Mac peuvent être infectés par des malwares et la menace grandit. Le malware ***Flashback***, en 2012, a compromis 600 000 Mac. Et les ransomwares sur Mac sont un autre problème, nous le verrons par la suite.
- Les SophosLabs ont également vu une augmentation inquiétante des malwares signés avec un identifiant Apple Developer actif et donc permettant au logiciel d'être installé.
- Les Mac peuvent également héberger des malwares Windows et les propager à travers votre réseau sur tous vos ordinateurs Windows.
- Ne laissez pas les Mac devenir le maillon faible dans votre dispositif de sécurité.

3.2.2. Les vecteurs d'attaque

Pendant des années, les utilisateurs de Windows ont été victimes de ransomware exigeant plusieurs centaines de dollars pour déverrouiller leurs ordinateurs.

Et bien, les cybercriminels savent qu'il existe un marché croissant d'utilisateurs d'Apple qui, pour la plupart, se sentent en sécurité pour naviguer sur Internet avec un Mac sans avoir besoin d'une protection.

Les cybercriminels, bien connus pour ne pas réinventer la roue à chaque fois, ont décliné le dernier ransomware sur OS X, non pas en utilisant un exploit compliqué mais en exploitant le navigateur et sa fonctionnalité de «récupération sur incident».

Des avertissements semblant provenir du FBI informent la victime: *"Votre navigateur a été bloqué... vous avez été consulté ou distribué du contenu illicite et interdit. Pour déverrouiller votre ordinateur et éviter toute implication juridique, vous êtes obligé de payer un montant de 300 dollars ".*

Le plus triste est que beaucoup de gens vont soit tomber dans le piège de ce type d'escroquerie, soit être tellement embarrassés qu'ils n'oseront pas en informer leur administrateur système. Ils accepteront de payer la rançon, remplissant les poches des pirates et devenant une cible idéale pour une attaque future.

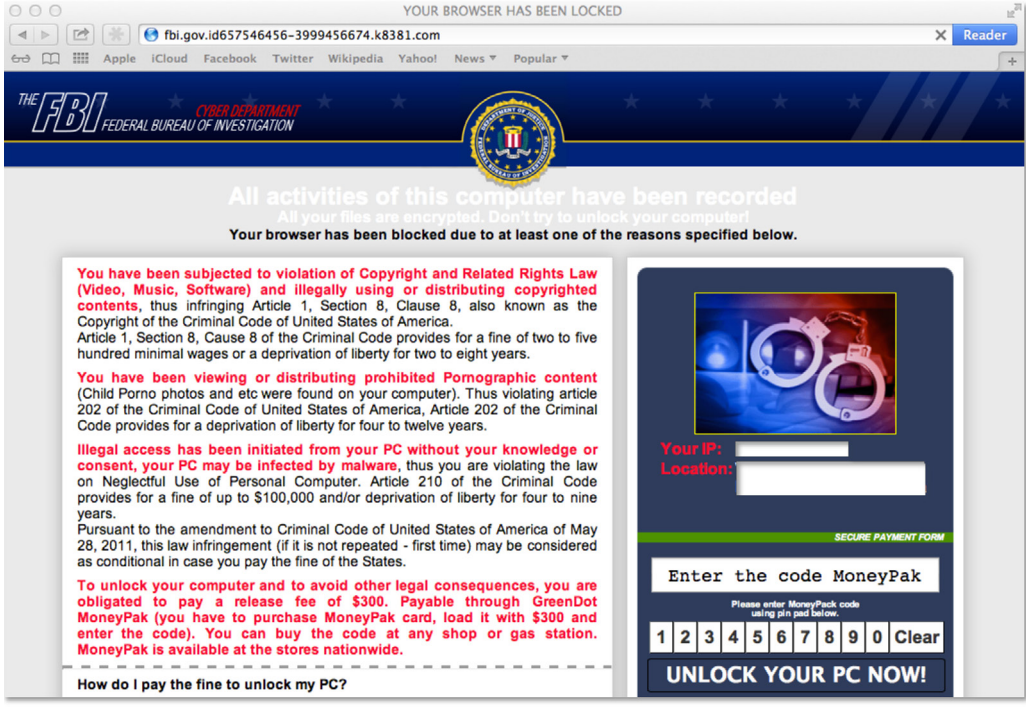

Figure 3: Exemple de ransomware se faisant passer pour le FBI.

3.2.3. Les moyens de s'en prémunir

Heureusement, il est assez facile de montrer à vos Mac que vous les aimez. Si c'est un péché que votre entreprise a besoin de corriger, voici trois étapes simples pour y parvenir:

1. Réduisez le risque que vos utilisateurs introduisent des applications malveillantes. Configurez vos systèmes Mac de telle manière que seules les applications signées puissent être installées.
2. Trop souvent, les solutions de sécurité Mac n'offrent pas le même niveau de protection que celles des PC, ce qui occasionne des failles de sécurité pour l'ensemble de votre organisation. Tout comme pour vos PC Windows, assurez-vous que vos Mac bénéficient d'une solution de protection Endpoint de très haut niveau, mise à jour en permanence.
3. Naturellement, vous ne voulez pas résoudre votre problème Mac et réaliser plus tard qu'une autre plate-forme est votre nouveau maillon faible. C'est pourquoi vous devriez opter pour une solution qui vous permette de gérer toutes vos plates-formes ensemble. Elle garantira que vos politiques de sécurité sont appliquées de manière homogène sur l'ensemble des plates-formes et des systèmes, réduisant de manière significative vos risques et votre charge administrative.

3.2.4. Pour aller plus loin

Sur le blog sécurité de Sophos France vous pourrez lire les billets suivants à propos de la sécurité sur Mac:

- Les Macs en entreprise: les 4 choses à savoir
- Pourquoi protéger un Mac?

3.3. Réseaux Wifi non sécurisés

Pour aller à l'essentiel

Risques	**Espionnage des réseaux, usurpation d'identité, atteinte aux données**
Vecteurs d'attaque	**Accès trop permissif, WiFi ouvert, WiFi mal sécurisé**
Moyens de s'en prémunir	**Séparation des réseaux invités des réseaux d'entreprise, identification des utilisateurs, vérification de la conformité des terminaux**

3.3.1. Les risques

Dans une étude intitulée Projet Warbike, Sophos a utilisé un seul homme, un vélo, un ordinateur, un GPS, deux dynamos et des panneaux solaires dans les rues de Londres (et beaucoup d'autres villes dans le monde entier) pour déterminer le nombre de réseaux Wi-Fi non sécurisés.

Sur les quelques 107 000 réseaux Wi-Fi étudiés, 27% avaient une mauvaise sécurité ou pas de sécurité du tout. La plus forte densité de réseaux mal sécurisés se trouvait dans les rues ayant un nombre élevé de petites entreprises.

Et bien sûr, l'intérêt de tout cela est que, sans aucun contrôle d'accès approprié, n'importe qui peut accéder à votre réseau et mettre vos données – le Saint Graal pour les pirates – en grand danger. Et les petites entreprises ne devraient jamais présumer que les pirates ne s'intéressent pas à elles. Car ils s'y intéressent de très près!

3.3.2. Les vecteurs d'attaque

Il existe deux grands types d'attaques...

Les attaques passives sont parfaitement indétectables car le pirate espionne le réseau en utilisant un sniffer de paquets qui analyse le trafic et examine les emails non chiffrés.

Les attaques actives signifient que le pirate se connecte au réseau, ce qui est très simple à réaliser avec n'importe quel réseau non sécurisé et tout à fait possible avec certains réseaux sécurisés grâce à des points d'accès ou des routeurs grand public.

- Souvent elles permettent de lancer des attaques de l'homme du milieu (man in the middle), comme indiqué ici, où elles compromettent les ordinateurs clients pour intercepter les communications et accéder ainsi au reste du réseau ou à Internet. Cela leur permet d'inspecter et d'intercepter tout le trafic, de rediriger les navigateurs vers des sites malveillants, de réutiliser des identifiants pour authentifier les serveurs d'entreprise et voler des données, ou encore de déployer des attaques par déni de service pour nuire à votre réseau.
- Il s'agit là de pratiques très frauduleuses.

3.3.3. Les moyens de s'en prémunir

Heureusement, nous avons un programme simple en 7 étapes pour vous aider à sécuriser votre Wi-Fi:

- Utilisez des points d'accès Wi-Fi pour entreprises... On ne compte plus les fois où l'on voit dans une petite ou moyenne entreprise l'utilisation de routeurs grand public pour accéder au Wi-Fi.
- Appliquez sur votre réseau Wi-Fi les mêmes politiques de sécurité réseau que sur votre LAN.
- Y compris le contrôle de tout le trafic réseau entrant et sortant.
- Bloquer l'accès aux systèmes que votre solution de MDM (gestion des mobiles) a identifié comme jailbreakés ou tout simplement non conformes.
- Fournissez des profils de connexion à vos utilisateurs mobiles pour vos réseaux Wi-Fi pour qu'ils ne se connectent pas à un réseau Wi-Fi usurpé.
- Utilisez une solution Wi-Fi qui vous permette de maintenir vos réseaux invités séparés de votre réseau d'entreprise sur vos points d'accès.
- Choisissez une solution qui soit simple à gérer et qui s'intègre facilement au reste de votre sécurité réseau.

Lorsque vous évaluez plusieurs solutions de sécurité Wi-Fi, Forrester Research recommande cinq mots d'ordre: extensible, partagée, simple, standardisée et sécurisée.

3.3.4. Pour aller plus loin

Vous pouvez consulter quelques exemples sur le blog sécurité de Sophos France concernant les risques liés au Wi-Fi:

- Wi-Fi gratuit: au revoir la confidentialité!
- Tunnel VPN: synonyme de sécurité?
- Cryptage OpenPGP pour les emails de notifications Facebook

3.4. Pare-feu défaillant

Pour aller à l'essentiel

Risques	**Contournement des protections, intrusion, espionnage, ralentissement ou perte de productivité**
Vecteurs d'attaque	**Multiples**
Moyens de s'en prémunir	**Installez un pare-feu de nouvelle génération et utilisez ses fonctions avancées**

3.4.1. Les risques

Les menaces et les règles ont changé sans que vous ne vous en aperceviez. Votre ancien pare-feu est devenu défaillant sans que cela ne soit votre faute.

Qu'est ce qui a rendu la plupart des pare-feu défaillants? Beaucoup de choses ont changé ...

- Avec autant d'applications et de services mobiles transférés dans le Cloud, les besoins en matière de bande passante et de performances ont explosé.
- D'une part, les employés utilisent les réseaux sociaux sur leur lieu de travail à des fins personnelles, d'autre part, les réseaux sociaux sont aussi devenus un outil très utilisé dans les entreprises pour les opérations de marketing et de relation clients.
- De plus, les menaces sont de plus en plus avancées, furtives et sophistiquées...ce que nous allons voir bientôt.
- Pour la plupart des entreprises, tout cela s'ajoute à un pare-feu défaillant offrant des performances limitées, qui a du mal à gérer les besoins actuels de mise en réseau ou avec des fonctionnalités manquantes, et le pire de tout, une visibilité limitée de sorte que vous ne pouvez même pas identifier vos zones à problèmes.

Le pire, c'est que votre pare-feu défaillant limite les possibilités de croissance de votre organisation, ralentissant la productivité, aboutissant à des sous-performances du personnel et augmentant l'exposition aux menaces.

3.4.2. Vecteurs d'attaque

Regardons maintenant les menaces avancées ou les menaces persistantes avancées (APT) car elles sont souvent responsables de rendre la plupart des pare-feu défectueux.

Au cœur de ces attaques, il y a souvent une organisation de pirates ou de cybercriminels qui gère l'attaque et la collecte de données avec une infrastructure de serveurs *Command and Control* qu'ils utilisent pour communiquer avec les machines infectées.

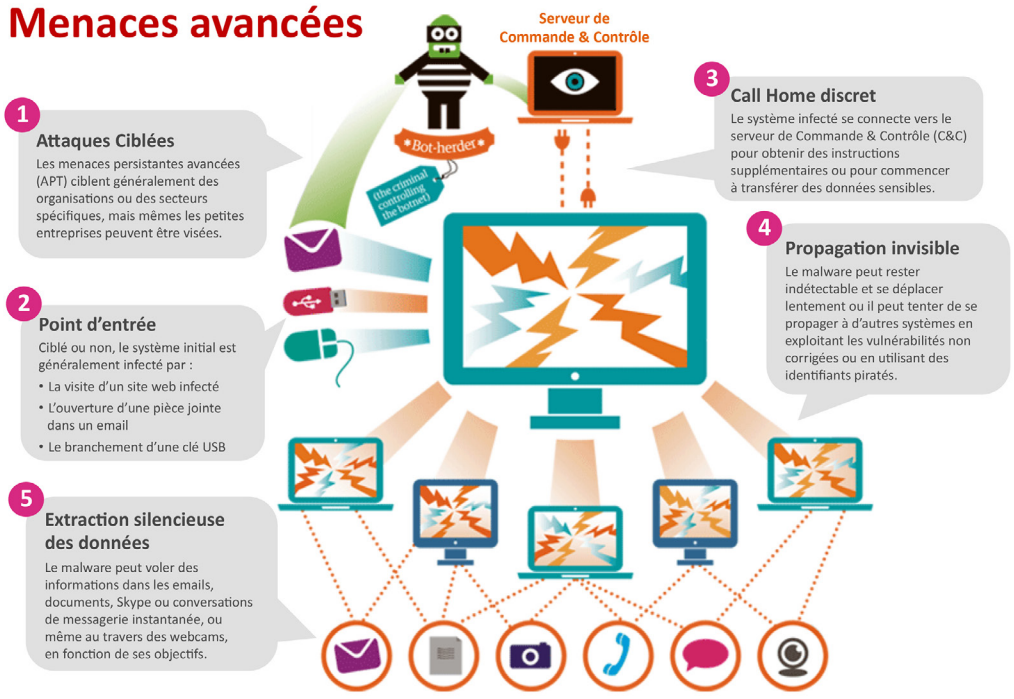

Figure 4: Fonctionnement d'un APT.

1. Ce qui rend les menaces persistantes avancées (APT) uniques et particulièrement efficaces, c'est que ce sont souvent des attaques ciblées. Elles peuvent cibler des secteurs ou des organisations spécifiques... par exemple des institutions financières, des organismes de santé ou encore des chaînes de distribution. Mais même les petites entreprises sont exposées à ce genre d'attaques.

2. Celles-ci consistent à propager des malwares qui permettent de créer un point d'entrée. Cela peut être un système Android infecté, comme nous avons vu plus tôt, ou un site infecté, une attaque de phishing par email ou même un support aussi banal qu'une clé USB contenant des malwares et volontairement abandonnée sur le parking d'une organisation cible, dans l'espoir qu'un utilisateur non averti la prenne et la connecte à son poste de travail pour voir ce qu'elle contient.

3. Une fois que la menace s'est introduite sur le réseau, elle effectue un *call* home (ou appel à domicile en cachette), mais peut attendre des heures, des jours, voire des semaines, avant de faire quoi que ce soit. Ce genre de menaces avancées se montrent souvent très discrètes et agissent lentement.

4. À un moment donné, elles peuvent obtenir des instructions pour se propager secrètement en exploitant des vulnérabilités sur d'autres systèmes ou en utilisant des identifiants volés pour accéder aux autres systèmes.

5. Enfin, que la menace soit rapide ou lente et persistante, son objectif reste le même: extraire silencieusement des données hors de l'entreprise par tous les moyens possibles. Elle peut obtenir les informations souhaitées en analysant les emails, les documents, les échanges sur Skype ou IM, voire en utilisant clandestinement dans l'environnement des micros ou des webcams pour surveiller les conversations en direct. Toutes ces actions ont déjà été observées par le passé.

3.4.3. Les moyens de s'en prémunir

Comment un pare-feu next-gen peut vous aider grâce à l'identification, au blocage et au sandboxing de ces types de menaces afin de fournir la protection dont vous avez besoin pour les arrêter? Cela commence par...

1. Une protection multi-couches – Les fonctionnalités intégrées de protection du Web, de la messagerie et des systèmes d'extrémité empêchent les infections de pénétrer le réseau en tout premier lieu.

2. Vous avez notamment besoin d'une fonction avancée de détection des malwares Web qui peuvent émuler du JavaScript pour identifier les menaces polymorphes et obscurcies – même les plus sophistiquées.

3. Votre pare-feu next-gen et l'IPS doivent bloquer les attaques réseau et empêcher les violations au niveau de la passerelle réseau.

4. Il doit également bloquer les appels à domicile ou calls-home, en vérifiant les différents vecteurs de trafic réseau pour identifier les récurrences de trafic C&C et pour les bloquer.

5. Votre pare-feu doit également identifier les systèmes infectés et signaler tous les hôtes infectés qui tentent de communiquer avec les serveurs C&C et les empêcher de le faire.

6. Enfin, il devrait avoir une fonction de sandboxing sélectif... pour envoyer des échantillons suspects représentant des menaces inconnues potentielles à un sandbox pour analyse. Les nouvelles informations sur ces menaces devraient être transmises au pare-feu.

Ce dont vous avez besoin

Prévenir, bloquer, identifier, sandboxing – Sophos simplifie la sécurité

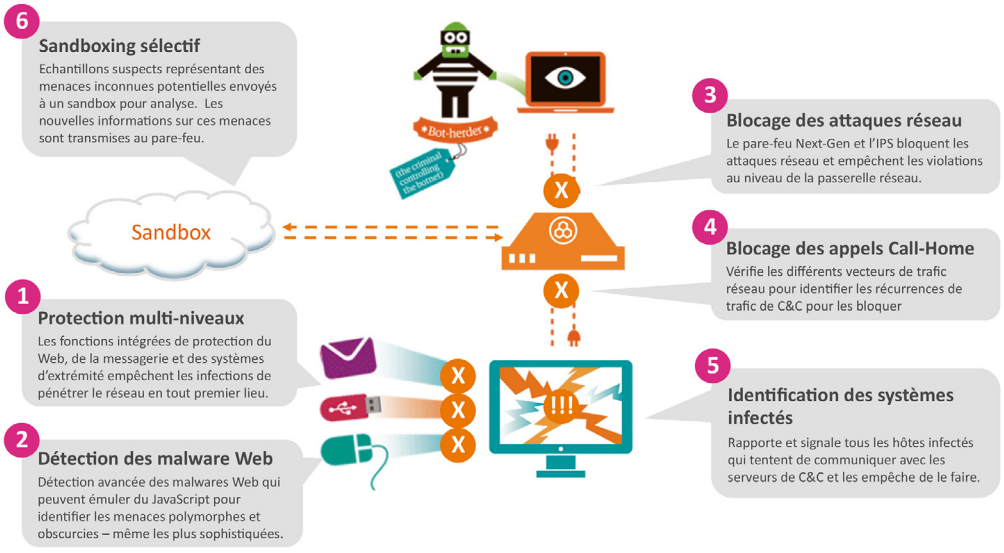

Figure 5: Protection contre les APT.

Si votre pare-feu n'est pas à la hauteur, vous devez le remplacer et en choisir un qui soit efficace aujourd'hui, et qui saura également répondre aux exigences de demain. Lorsque vous évaluez plusieurs offres de pare-feu next-gen, prenez en considération les cinq points suivants:

1. **Facilité d'utilisation.** Vous devez pouvoir utiliser votre pare-feu de manière efficace! Assurez-vous de bien comprendre le fonctionnement du pare-feu avant de vous engager pour les trois prochaines années. Vous pouvez effectuer un essai, regarder des vidéos de démonstration pour les tâches courantes, lire les commentaires et avis indépendants sur des sites comme SpiceWorks.

2. **Performances.** Chaque éditeur – y compris Sophos – dispose de données sur les performances de leur pare-feu dans des conditions idéales. Mais vous ne travaillez pas dans un laboratoire de test réseau. Vous travaillez dans un environnement d'entreprise réel. C'est pourquoi vous devriez regarder comment le pare-feu fonctionne en situation réelle, lorsqu'il exécute les tâches classiques devant être réalisées quotidiennement. Si des tests en situation réelle et indépendants sont disponibles, n'hésitez pas les consulter également.

3. **Fonctions de protection.** Identifier ce dont vous avez besoin et vérifiez bien que votre pare-feu next-gen possède ces fonctionnalités! Pour rester protégé contre les menaces actuelles que nous venons de voir, vous devriez mettre la fonction Protection avancée contre les menaces en haut de votre liste. Et aller au-delà des fonctions basiques pour choisir un pare-feu qui protège non seulement les messageries, le Web, les systèmes d'extrémité, les mobiles et les applications, mais qui facilite aussi l'intégration pour que toutes ces fonctions travaillent ensemble à identifier les menaces, gérer les mobiles, et ce grâce à une seule solution.

4. **Expertise en sécurité.** Assurez-vous que le vendeur auquel vous faites confiance pour votre pare-feu soit vraiment un expert en sécurité, qu'il garde toujours une longueur d'avance sur les menaces qui évoluent constamment et auxquelles nous sommes tous confrontées.
5. **Rapports.** Vous ne pouvez pas régler vos problèmes si vous ne savez pas qu'ils existent. Assurez-vous que votre prochain pare-feu vous offre les rapports dont vous avez besoin pour prendre des décisions éclairées, en temps réel.

3.5. Documents et correspondances non chiffrées

Pour aller à l'essentiel

Risques	**Divulgation d'informations sensibles, atteinte aux données, pénalités financières**
Vecteurs d'attaque	**Vol de machine, vol de documents, interception d'email**
Moyens de s'en prémunir	**Chiffrement d'emails, de disque et de fichiers**

L'absence de chiffrement est une bombe à retardement pour de nombreuses entreprises. Malheureusement, la plupart d'entre elles savent qu'elles ont besoin de faire quelque chose à ce sujet, mais elles reportent sans cesse parce qu'il est généralement très difficile de résoudre ce problème avec élégance.

3.5.1. Emails non chiffrés – Les risques

Un nombre considérable d'emails sont envoyés chaque jour dans le monde: plus de 144 milliards. Un grand nombre d'entre eux contiennent des informations sensibles, et pour la plupart elles ne sont pas chiffrées, ce qui facilite grandement l'espionnage mais aussi la fuite de données.

Nous sommes en proie à une épidémie d'espionnage des messageries. Toute personne équipée d'un "renifleur de paquets" (packet sniffer) ou d'un analyseur peut lire votre courrier non chiffré.

Et naturellement, les FAI et les fournisseurs de messageries Web tels que Google, Microsoft ou Yahoo ont admis qu'ils analysaient votre courrier à des fins publicitaires ou autres...

3.5.2. Emails non chiffrés – Les vecteurs d'attaque

La capture d'écran ci-après montre un renifleur de paquets freeware pouvant être installé par n'importe qui sur son ordinateur portable pour afficher le trafic de messagerie échangé sur un réseau donné. Souvenez-vous de ces attaques de l'homme du milieu dont nous avons parlé auparavant qui espionnent des réseaux Wi-Fi non sécurisés ... et bien c'est exactement le genre d'outils qu'elles utilisent pour lire vos emails.

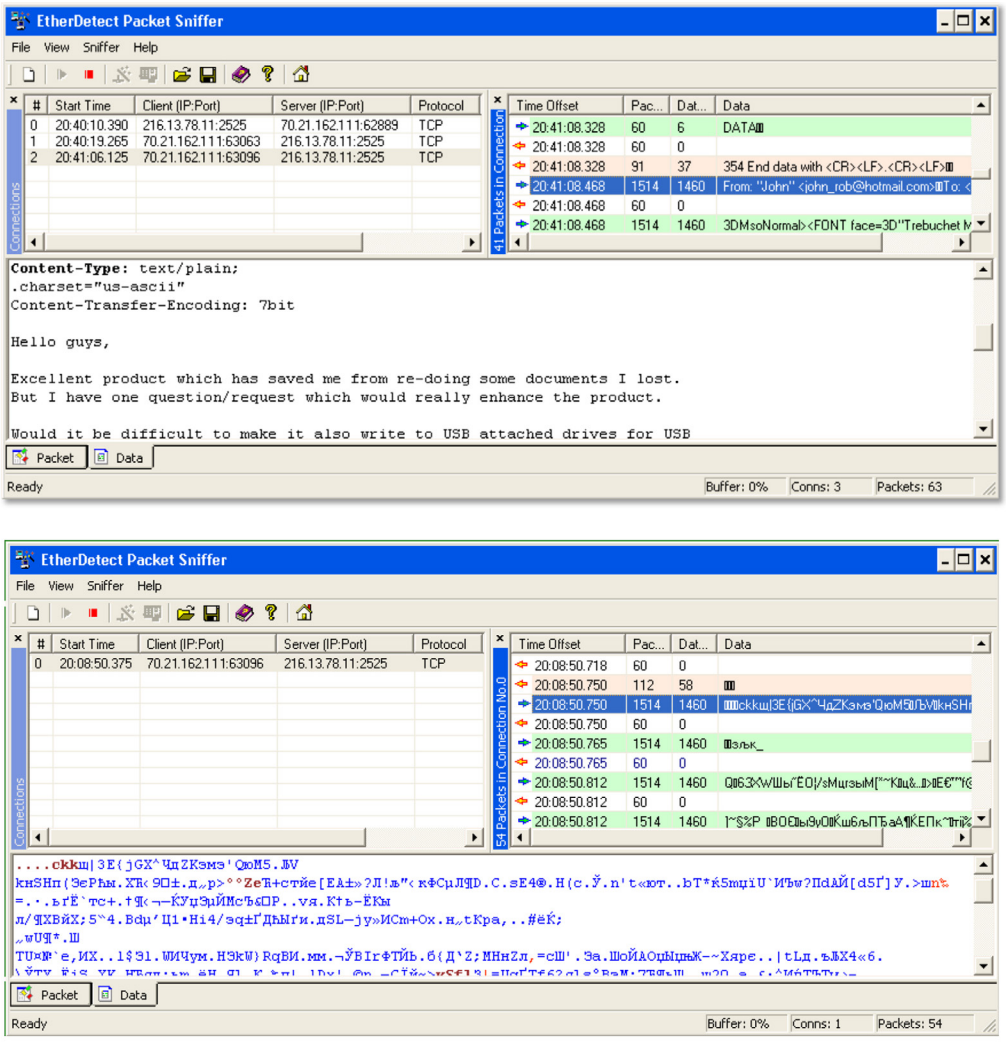

Figure 6: Exemple de sniffer afin d'intercepter les emails.

Mais sans parler des pirates... combien de personnes ont accidentellement envoyé un courrier électronique à la mauvaise personne? Que faire si ce courrier contenait des données sensibles? Les pertes de données peuvent aussi survenir suite à des erreurs humaines.

3.5.3. Emails non chiffrés – Les moyens de s'en prémunir

Les temps ont changé – ne reportez plus à plus tard le DLP et le chiffrement des emails. Il existe aujourd'hui des solutions très simples, intelligentes et tout à fait abordables sur le marché. Vous pouvez maintenant obtenir un DLP et un chiffrement de votre messagerie de façon simple, qui s'intègrent à votre budget antispam et qui peut être opérationnel en quelques minutes.

Voici votre liste de contrôle pour sécuriser votre messagerie... Créer une politique, informer les utilisateurs sur l'importance du chiffrement et faciliter son utilisation... Simplifiez-vous la tâche, à vous et à vos utilisateurs, en mettant en œuvre une solution qui s'intègre à votre passerelle de messagerie et qui permette de détecter automatiquement les données sensibles dans les emails sans impacter les utilisateurs, puis de les bloquer ou de les chiffrer automatiquement sans besoin de clé ni de certificats.

Le chiffrement des emails n'est pas une fin en soi, il n'existe pas vraiment de bonne raison de ne pas chiffrer vos fichiers.

3.5.4. Documents non chiffrés – Les risques

On estime qu'un dixième des ordinateurs portables professionnels seront volés avant même d'arriver à la fin de leur cycle de vie. En d'autres termes, cela arrive tout le temps. Maintenant tous les vols ou pertes d'ordinateurs n'aboutissent pas nécessairement à une débâcle de pertes de données, mais pour beaucoup c'est le cas.

En voici quelques exemples.

Figure 7: Perte de données médicales.

Stolen Laptops, Hard Drives Expose Over 100,000 People's Personal Data

The data potentially exposed includes names, addresses, phone numbers and Social Security numbers.

By **Jeff Goldman** | Posted February 25, 2015 Share

Several thefts of unencrypted laptops and hard drives recently exposed a significant number of people's personal information.

The Boston Baskin Cancer Foundation recently acknowledged that 56,694 patients' and employees' personal information may have been exposed when an unencrypted external hard drive was stolen from an employee's home on December 2, 2014 (h/t DataBreaches.net).

The drive contained patient demographic information, birthdates, Social Security numbers, phone numbers and first and last dates of clinic visits for patients seen between 2008 and July 2014. For employees, the drive held titles, office locations, Social Security numbers, birthdates, pay rates, and dates of employment.

Figure 8: Perte de données personnelles d'une fondation contre le cancer.

Coca-Cola Says 74,000 Affected After Company Laptops Stolen

Coca-Cola's shares fell 1 percent to $38.84 at the close in New York and added 14 percent last year.
Photographer: Dario Pignatelli/Bloomberg

Figure 9: Perte de données chez Coca Cola.

3.5.5. Documents non chiffrés – Les vecteurs d'attaque

Tous ces ordinateurs portables étaient confiés aux employés et ils ont été volés dans leur voiture, dans un aéroport, ou malheureusement dans un centre de déchets comme cela fut le cas pour Coca Cola qui a envoyé cinq ordinateurs portables au centre de déchet pour y être détruits sans d'abord effacer le contenu des disques... ou vérifier qu'ils étaient chiffrés, et quelqu'un en a profité. Bien que cela soit difficile à imaginer, cela arrive tous les jours.

Une recherche rapide sur Google avec les termes "ordinateurs portables volés" vous fournira 40 millions de résultats!

Il existe d'innombrables exemples comme ceux-ci, pour lesquels des entreprises, organismes de santé ou société financière conservent les données de leur clients sur des ordinateurs portables sans chiffrement.

3.5.6. Documents non chiffrés – Les moyens de s'en prémunir

Il y a deux types de données dont vous devez vous préoccuper.

Le premier, ce sont les données personnelles. Autrement dit tout ce qui vous permet d'identifier un individu. Cela comprend les dossiers du personnel, les bases de données clients ou encore les dossiers des patients (DMP: Dossier Médical Patient).

Dans la plupart des pays, il existe des lois qui exigent des organisations de maintenir ces informations protégées et imposent des sanctions financières sévères en cas de violation ainsi que l'obligation de divulguer ces faits. Ce qui peut entrainer des dommages irréparables à votre image de marque et une perte d'activité.

Le second, ce sont les données d'entreprise. Ce sont les informations stratégiques à l'entreprise et que vous ne voulez pas voir tomber entre de mauvaises mains. Il s'agit notamment des dossiers financiers, des données de R & D, des opportunités commerciales futures.

Malheureusement, ce problème ne devrait pas exister. La solution est si simple, et elle est intégrée à tous les ordinateurs portables. C'est ce qu'on appelle le chiffrement complet du disque. Sur Windows, il est appelé Bitlocker (intégré dans toutes les licences Microsoft sans surcoût à partir de Windows 8) et sur Mac il est appelé FileVault.

Mais vous devez aussi regarder au-delà de vos ordinateurs portables, aux autres endroits qui stockent des données sensibles... vos données sur serveurs de fichiers partagés, votre messagerie, le Cloud, vos appareils mobiles, en adoptant une solution de chiffrement qui vous permette également de maintenir les fichiers sensibles chiffrés, peu importe l'endroit où ils sont stockés: sur vos serveurs de fichiers, sur vos serveurs de fichiers Cloud, ou même sur vos mobiles.

Enfin, assurez-vous que la solution que vous choisissez offre les outils de rapports, de gestion et d'audit dont vous avez besoin.

3.6. Pratiques de surf sur Internet

Pour aller à l'essentiel

Risques	**Infections des machines, vol d'information, usage inapproprié du web**
Vecteurs d'attaque	**Site légitime piraté, ingénierie sociale, spam, phishing**
Moyens de s'en prémunir	**Solution de filtrage web complète avec filtrage HTTPS et prise en compte des URLs malveillantes**

3.6.1. Les risques

Avant le filtrage Web était facile: il suffisait de bloquer les sites de pornographie, de jeu et les sites à contenu extrémiste, le filtrage était suffisant.

Aujourd'hui, cela ne suffit plus pour maintenir vos employés protégés contre les sites dangereux. Aujourd'hui, 80% de l'ensemble des malwares Web sont hébergés sur des sites légitimes ayant été compromis. Ce tableau montre les 10 catégories de sites les plus infectées et comme vous pouvez le constater, les sites pour adultes occupent la dernière place sur la liste.

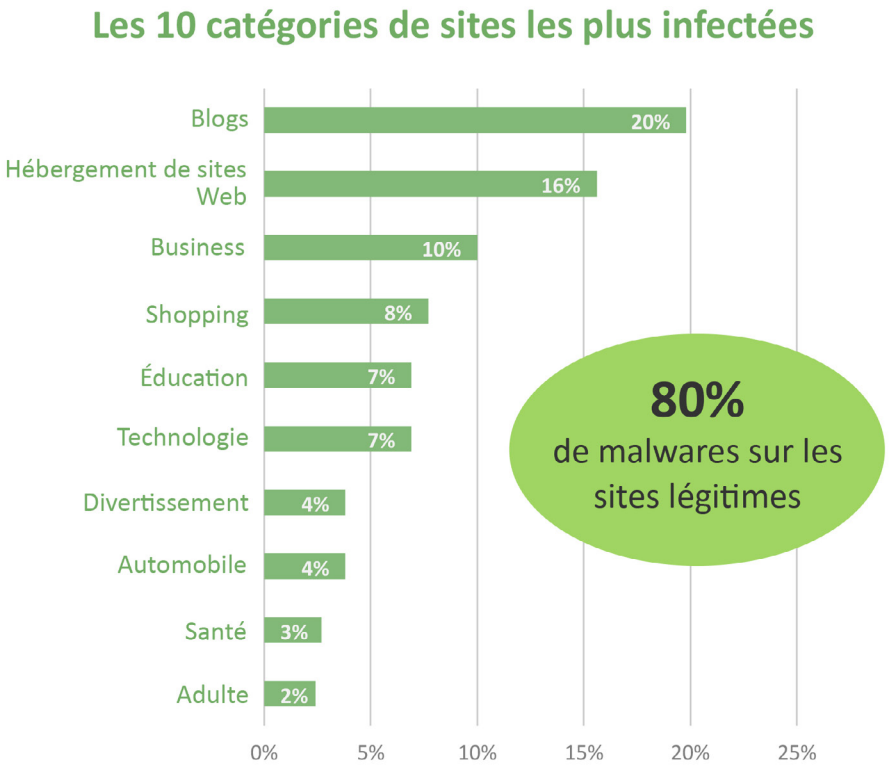

Figure 10: Les catégories de sites web les plus infectées

En revanche, les sites que vous êtes susceptibles de visiter quotidiennement sont au sommet. Vous pouvez être infecté par un malware simplement en naviguant sur un site piraté qui pouvait très bien être sûr la veille, sans même le savoir.

3.6.2. Les vecteurs d'attaque

Vos employés sont confrontés à 40 000 nouvelles menaces Web chaque jour, c'est donc un défi quotidien à relever.

Les implications réelles de ces menaces Web ne doivent pas être sous-estimées. Elles peuvent se nicher silencieusement sur votre ordinateur pour collecter vos identifiants bancaires et les autres données saisies dans les formulaires de votre navigateur, verrouiller votre ordinateur ou chiffrer vos données et exiger un paiement pour en rétablir l'accès.

1. La première étape d'une attaque consiste à avoir un point d'entrée...soit un téléchargement passif depuis un site piraté, soit un email renfermant un lien malveillant.
2. Maintenant, si vous vous trouvez sur un site piraté qui charge des scripts malveillants, la première chose qu'il va faire est d'évaluer le type de système que vous avez... utilisez-vous un Windows ou un Mac, IE ou Safari, avez-vous Java, est-ce une ancienne version, etc. Une fois qu'il aura récupéré toutes ces informations, il tentera de vous rediriger vers l'un des milliers de sites de distribution de malwares en utilisant ce qu'on appelle un réseau de distribution du trafic.
3. La prochaine étape d'une attaque Web classique est que le pack d'exploits téléchargé depuis le serveur de distribution tente d'exécuter un grand nombre d'exploits pré-installés contre les vulnérabilités connues dans le navigateur ou les plugins associés tels que Java, les lecteurs de PDF, les lecteurs de médias, etc. Le Blackhole Exploit Kit est un exemple notoire... il est disponible pour 500$ par mois et il est hébergé sur leurs serveurs avec un support de 9 à 19h chaque jour. Dans cet aperçu-ci, nous pouvons voir que l'exploit le plus efficace se fait avec Java avec un taux de réussite de 96% et plus de 1900 infections.

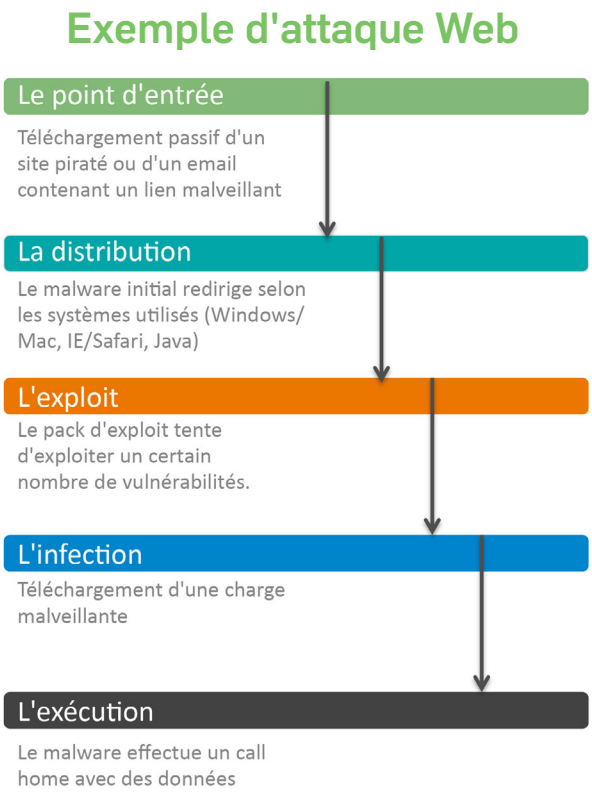

Figure 11: Exemple d'une attaque Web.

Dès qu'une vulnérabilité a été exploitée, la machine peut être infectée par une charge malveillante. Le ransomware, comme indiqué précédemment, est particulièrement redoutable car il chiffre vos données, verrouille votre ordinateur ou votre compte utilisateur, et vous empêche d'y accéder jusqu'à ce que vous leur reversiez une somme d'argent (généralement environ 300 USD par incident). Mais il existe bien d'autres types de malwares furtifs qui peuvent se dissimuler sur un ordinateur afin de recueillir des informations bancaires saisies dans les formulaires ou de faire de l'espionnage d'entreprise.

3.6.3. Les moyens de s'en prémunir

Vous avez besoin d'une protection à chacun de ces niveaux d'attaque, parce que la nature des attaques web fait que les pirates et les criminels sont constamment en train de changer leurs tactiques à tous les niveaux. Il est donc très important d'avoir une défense multi-couches:

- Aux niveaux du point d'entrée et de la distribution, vous avez besoin d'un filtrage du spam et d'un filtrage en temps réel de la réputation des URLs qui doivent être assurés par un fournisseur qui surveille en permanence les derniers réseaux de distribution, les réputations des DNS et les sites infectés.
- Vous avez besoin d'un contrôle sophistiqué des malwares Web avec émulation JavaScript et analyse comportementale pour inspecter et bloquer les dernières menaces polymorphes et obscurcies.

- Vous avez également besoin d'une analyse HTTPS pour inspecter le trafic chiffré qui est un vecteur croissant. Et comme nous l'avons vu plus tôt dans ce document, recherchez aussi une solution dotée d'une fonction avancée de détection des menaces (APT) pour pouvoir identifier les machines infectées sur votre réseau.
- Comme nous le savons tous, la protection est efficace seulement si les dernières mises à jour sont appliquées alors ne vous contentez pas de mises à jour fréquentes (chaque jour ou même chaque heure). Trouvez une solution capable d'effectuer des recherches en temps réel dans le Cloud pour collecter les dernières informations sur les menaces. Et assurez-vous d'avoir un antivirus professionnel avec HIPS pour détecter les infections au fur et à mesure qu'elles sont téléchargées et exécutées dans la dernière phase de l'attaque (en supposant qu'elles y parviennent).

Enfin, assurez-vous que vos utilisateurs soient protégés partout où ils vont ... pas seulement quand ils sont sur votre LAN derrière le pare-feu, mais aussi quand ils surfent sur le Web à la maison ou en déplacement.

3.6.4. Pour aller plus loin

Le blog sécurité de Sophos France a publié un article et une vidéo expliquant comment détecter les sites web frauduleux.

En effet nous n'avons pas parlé des sites frauduleux dans cette section mais ils représentent des risques importants pour les utilisateurs/internautes. La plupart du temps ce sont des sites e-commerces affichant des tarifs improbables, douteux pour vous pousser à passer commande. Les escrocs utilisent ces sites d'arnaque pour récupérer vos informations bancaires comme votre numéro de carte de crédit ou votre compte PayPal.

Abonnez-vous à la newsletter.SophosFrance.fr, nous écrivons régulièrement au sujet des arnaques sur le web.

4. Conclusion

Nous avons passé en revue dans ce document les différentes menaces auxquelles vous devez faire face que vous soyez dans une grande entreprise ou une plus petite structure.

Les cyber-attaquants sont malins et perfectionnent régulièrement leurs attaques afin de trouver et d'exploiter les brèches dans vos systèmes.

Un système de sécurité efficace à un instant T ne le sera pas dans 100% des cas de figure, et nécessitera des ajustements au fil du temps afin de continuer à vous fournir le niveau de protection que vous attendez de lui.

Vous avez maintenant plus de cartes en main pour réduire le risque induit par ces différents types de menaces. Outre les moyens techniques et les stratégies de sécurité mis en place, la réduction du risque passe également par l'éducation de vos utilisateurs.

Sophos et ses partenaires peuvent vous accompagner afin de mettre en œuvre des stratégies de défense efficaces qui amélioreront encore votre niveau de sécurité et réduiront le risque auquel votre organisation est exposée au quotidien.

Nous serons heureux de vous aider conjointement dans cette démarche, n'hésitez pas à faire appel à nous!

Essais gratuits

Demandez des évaluations gratuites de nos solutions sur sophos.fr/products

Équipe Commerciale France
Tél: 01 34 34 80 00
Email: info@sophos.fr

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

2015-07-20 WP-FR (RG)

SOPHOS