KASPERSKY lab

PANORAMA DES CYBER-MENACES

Guide pratique

David Emm, Principal Security Researcher
Global Research & Analysis Team, Kaspersky Lab

www.kaspersky.fr/business
#SecureBiz

Sommaire

À propos de l'auteur

David Emm, Principal Security Researcher Global Research & Analysis Team (GReAT)

David Emm est Principal Security Researcher chez Kaspersky Lab, un éditeur de solutions de gestion de la sécurité et des menaces. Il travaille pour Kaspersky Lab depuis 2004 et fait actuellement partie de la Global Research & Analysis Team de l'entreprise. Il travaille dans le secteur de la protection contre les programmes malveillants depuis 1990, à divers postes, comme ceux de Senior Technology Consultant chez Dr Solomon's Software et Systems Engineer and Product Manager pour la société McAfee. Dans le cadre de son poste actuel, David donne régulièrement des conférences sur les programmes malveillants et autres menaces informatiques, lors de salons et d'événements, en mettant en évidence ce que les organisations et les consommateurs peuvent faire pour se protéger sur Internet. Il intervient également dans la presse audiovisuelle de la cyber-sécurité et du panorama des cyber-menaces en constante évolution. David a un vif intérêt pour les programmes malveillants, le vol d'identité et le secteur de la sécurité en général. Il est un conseiller bien informé sur tous les aspects de la sécurité en ligne.

Chapitre 1 : L'évolution des programmes malveillants

Les premiers virus informatiques sont apparus il y a plus de 25 ans. Depuis, la nature de la menace a changé de manière significative et aujourd'hui, les menaces sont plus complexes que jamais.

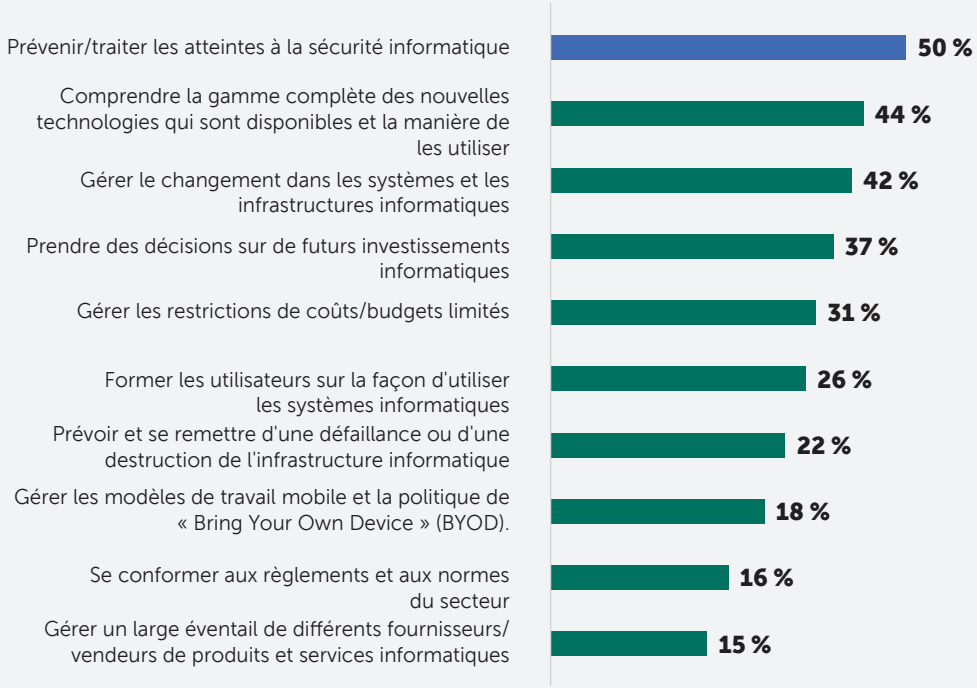
Au cours des dernières années, **l'enquête de Kaspersky Lab sur les risques informatiques mondiaux** a mis en évidence des changements dans les habitudes de travail, lesquelles ont toutes eu une incidence importante sur la sécurité de l'entreprise. Il s'agit notamment d'une mobilité croissante et de la tendance au BYOD, du stockage de données d'entreprise dans le cloud, de l'utilisation accrue de systèmes virtuels et de l'usage répandu des médias sociaux au travail.

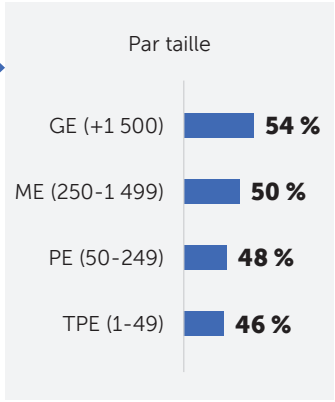
Les préoccupations en matière de sécurité autour de ces évolutions continuent de figurer très nettement dans l'enquête et, sans surprise, les résultats de 2015 soulignent que « prévenir et traiter les atteintes à la sécurité est une préoccupation primordiale pour 50 % des entreprises[1] et se prémunir contre les cyber-menaces est la première priorité en matière de sécurité pour 27 % des sociétés ».[1]

Traiter les atteintes à la sécurité est une préoccupation primordiale pour **50 %** des entreprises.[1]

PREMIÈRES PRÉOCCUPATIONS DE LA FONCTION INFORMATIQUE[1]

Traiter les atteintes à la sécurité, comprendre les nouvelles technologies et gérer les modifications apportées aux systèmes informatiques sont les principales préoccupations. Les atteintes à la sécurité sont un sujet de préoccupation pour les entreprises de toutes tailles.





1 : Global IT Risks Security Survey 2015 de Kaspersky Lab

PRIORITÉS EN MATIÈRE DE SÉCURITÉ INFORMATIQUE POUR LES 12 PROCHAINS MOIS[2]

Se prémunir contre les cyber-menaces est maintenant la priorité absolue (précédemment la troisième priorité), supplantant la prévention des fuites de données.

Des attaques à l'envergure et à la dangerosité croissantes

Le monde interconnecté signifie que les attaques peuvent être lancées sur les appareils des victimes très rapidement, et de manière aussi large ou ciblée que le requièrent les auteurs de programmes malveillants et les promoteurs d'activités criminelles clandestines.

Un code malveillant peut être intégré à un e-mail, introduit dans de faux packs logiciels, placé dans la zone grise de pages Web, ou téléchargé par un cheval de Troie installé sur un ordinateur infecté.

L'ampleur du problème a également continué de s'accroître. Le nombre d'échantillons de nouveaux programmes malveillants découverts au quotidien par Kaspersky Lab atteint plusieurs centaines de milliers.

2 : Global IT Risks Security Survey 2015 de Kaspersky Lab

Un problème de perception

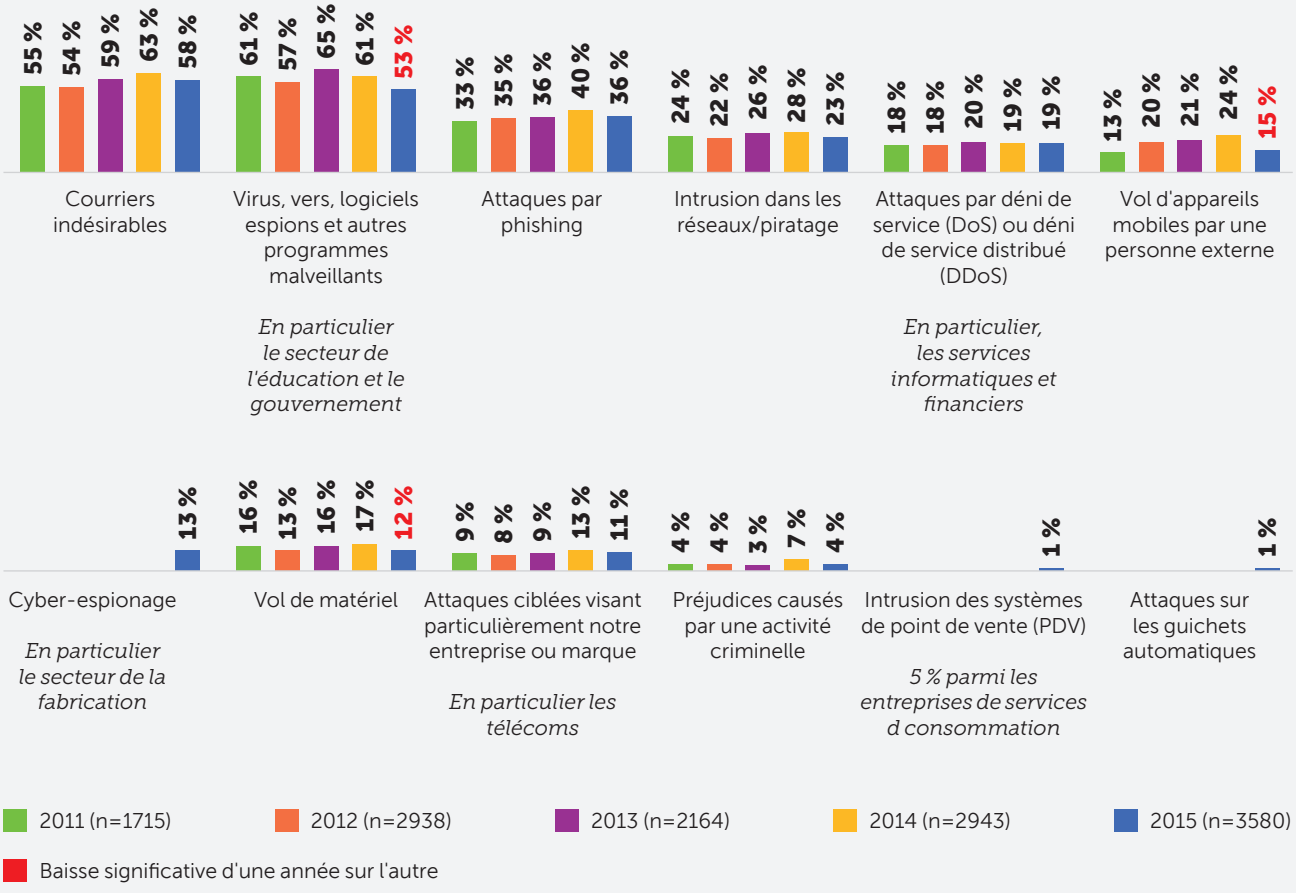
Au cours des 12 derniers mois, 90 % des entreprises ont enregistré une certaine forme d'attaque externe et 46 % des entreprises ont signalé une augmentation du nombre d'attaques[3], bien qu'il existe une perception selon laquelle il y a eu moins de cas de vol de données et d'événements dus à des programmes malveillants qui soient flagrants, en 2015.

Cependant, il existe une idée fausse selon laquelle les programmes malveillants sont à part, dans une catégorie distincte. En fait, les programmes malveillants constituent une composante essentielle de la plupart des cyber-attaques et demeurent la menace la plus importante et la plus dangereuse pour la sécurité informatique. Les attaques ciblées, le cyber-espionnage, les attaques de phishing et d'autres encore, intègrent tous des programmes malveillants. Ce n'est pas tant que les infiltrations de programmes malveillants ont baissé, c'est surtout que ces attaques ne sont pas forcément perçues comme des attaques de programmes malveillants.

90 % des entreprises ont subi une forme d'incident extérieur.[3]

MENACES EXTERNES SUBIES[3]

90 % des entreprises ont subi un incident extérieur.
Moins de cas de vol et d'événements dus aux programmes malveillants « flagrants » en 2015, par rapport aux précédentes vagues.



3 : Global IT Risks Security Survey 2015 de Kaspersky Lab

Du cyber-vandalisme à la cyber-criminalité

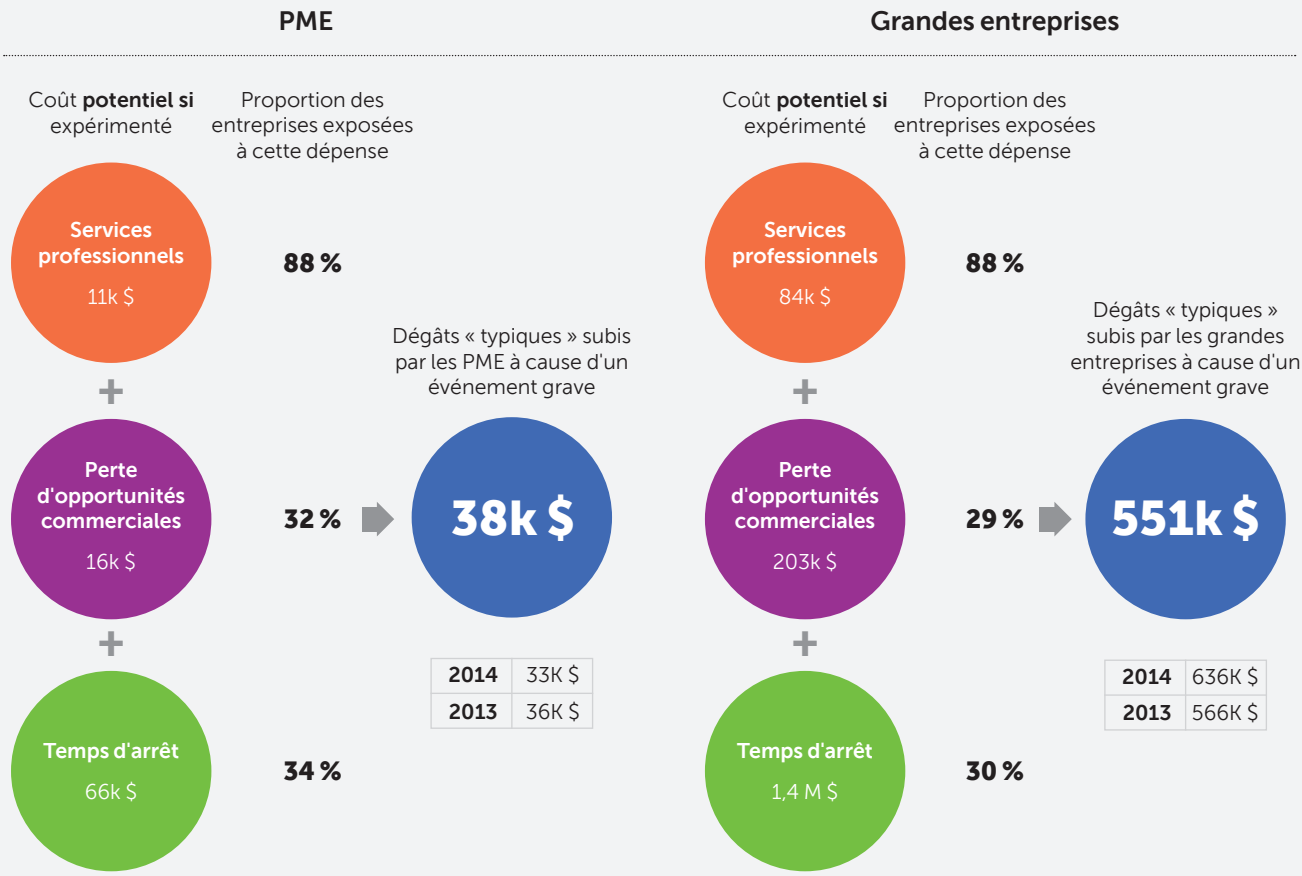
Jusqu'aux alentours de 2003, les virus et autres types de programmes malveillants comprenaient surtout des actes isolés de vandalisme informatique, un moyen d'exprimer des « idées antisociales » à l'aide de la technologie. La plupart des virus se contentaient d'infecter d'autres disques ou programmes.

Le panorama des menaces a changé après 2003. La plupart des programmes malveillants actuels sont spécialement conçus pour pirater des ordinateurs et gagner de l'argent illégalement. En conséquence, les menaces qui pèsent aujourd'hui sur les entreprises sont bien plus complexes. Les administrateurs informatiques sont confrontés à de nombreux problèmes : les types de menace contre lesquels ils doivent défendre l'entreprise sont multiples et entraînent des préjudices qui ne se limitent plus à un simple temps d'arrêt informatique mais qui sont souvent financiers.

1 société sur 3 ayant expérimenté une violation de données a subi un arrêt temporaire de son activité. De plus, les coûts directs habituels encourus suite à un événement grave sont de **38k $** pour **les PME** et de **551k $** pour **les grandes entreprises.**[4]

ESTIMATION DES COÛTS DIRECTS ENCOURUS RÉSULTANT DE TOUT INCIDENT GRAVE DE PERTE DE DONNÉES[4]

Bien que tous les frais ne soient pas encourus par chaque entreprise, on peut néanmoins estimer une perte représentative en tenant compte de la probabilité qu'a une entreprise d'être exposée à chaque dépense.



Chaque coût potentiel est multiplié par la probabilité que ce coût soit ensuite augmenté, pour déboucher sur les coûts généraux « caractéristiques » prévus.

4 : Global IT Risks Security Survey 2015 de Kaspersky Lab

Nouvelles motivations, nouvelles tactiques

Les motivations étant différentes, les tactiques ont changé. Le nombre d'épidémies mondiales, visant une propagation aussi large et rapide que possible des programmes malveillants, a ainsi diminué. Les attaques sont devenues plus ciblées.

La principale cause de ce changement est que les attaques ont désormais des fins criminelles et visent à dérober des données confidentielles, qui peuvent ensuite être traitées avant d'être utilisées. Lorsque des millions de machines sont affectées, la détection est plus facile et s'accompagne d'une vaste opération logistique. C'est pourquoi les auteurs de codes malveillants préfèrent désormais cibler leurs attaques.

Les auteurs de codes malveillants préfèrent désormais cibler leurs attaques.

L'explosion des chevaux de Troie

Les chevaux de Troie sont aujourd'hui le type le plus commun de programmes malveillants. Ils sont classés selon leur fonction : les plus courants sont les backdoors, les voleurs de mots de passe, les téléchargeurs, et les chevaux de Troie bancaires.

Les chevaux de Troie sont utilisés pour voler des informations confidentielles (nom d'utilisateur, mot de passe, code PIN, etc.) à des fins de fraude bancaire.

Ils peuvent être utilisés pour espionner les victimes. Ils peuvent être utilisés pour installer d'autres programmes malveillants afin de répondre aux besoins des agresseurs. Ils peuvent être utilisés en attaques DDoS (déni de service distribué) sur des entreprises : ces attaques visent à extorquer de l'argent à des organisations, à l'aide d'une attaque DDoS de « démonstration », afin de donner à la victime un avant-goût de ce qui arrivera si elle ne paie pas.

Augmentation des demandes de rançon

Au cours de ces dernières années, il y a également eu une croissance constante de « ransomware ». C'est le nom donné à des programmes malveillants visant à extorquer l'argent de leurs victimes, soit en bloquant l'accès à l'ordinateur, soit en chiffrant les données qui y sont stockées. Le programme malveillant affiche un message proposant de rétablir le système en contrepartie d'un paiement.

Parfois, les cyber-criminels qui lancent l'arnaque essayent de donner de la crédibilité à leur opération en se faisant passer pour des responsables de l'application de la loi : leur message de rançon indique que l'accès au système a été bloqué, ou que les données ont été chiffrées, parce que la victime utilise un logiciel sans licence ou a eu accès à un contenu illégal, faits pour lesquels la victime doit payer une amende.

Alors que les technologies contre les programmes malveillants peuvent détecter un ransomware, il se peut qu'il ne soit pas possible de déchiffrer les données. Il est donc essentiel de faire régulièrement des sauvegardes, non seulement pour éviter la perte de données résultant de ransomware, mais aussi pour protéger les données contre toute perte en raison d'autres problèmes informatiques.

En général, les ordinateurs infectés constituent des réseaux. Les activités de ces réseaux de bots, ou botnets, sont contrôlées via des sites Web ou des comptes Twitter. Si le botnet a un seul serveur de commande et de contrôle (C2), il est possible de l'enlever une fois que son emplacement a été identifié. Mais, ces dernières années, les cyber-criminels ont développé des botnets plus complexes qui ont recours au modèle P2P pour éviter d'avoir un seul point de défaillance. C'est devenu désormais une caractéristique standard des botnets.

Une astuce GReAT : Sauvegardez régulièrement vos données

Même si vous externalisez la manipulation et le stockage de vos données, vous ne pouvez pas en externaliser la responsabilité en cas de faille de sécurité. Évaluez les risques potentiels, comme vous le feriez si vous stockiez vos données en interne. En sauvegardant vos données, vous diminuez le risque qu'un incident ne se transforme en une catastrophe.

Le phishing ou comment se faire passer pour quelqu'un d'autre

L'usage de code malveillant n'est pas la seule méthode à laquelle les cyber-criminels ont recours pour recueillir les données personnelles qu'ils utilisent pour réaliser leurs escroqueries. Le phishing consiste à piéger des individus pour les amener à divulguer leurs données personnelles (nom d'utilisateur, mot de passe, code PIN ou autres informations d'accès), lesquelles sont ensuite utilisées dans le but d'obtenir de l'argent frauduleusement.

Les spécialistes du phishing créent une réplique presque parfaite du site Web d'un établissement financier. Ensuite, ils diffusent un e-mail imitant une correspondance authentique de l'entité légitime.

Les spécialistes du phishing utilisent généralement des logos légitimes, un bon style professionnel et font même référence à des noms réels de dirigeants supérieurs de l'institution financière. Ils vont même jusqu'à reproduire l'en-tête de la vraie banque.

Les e-mails distribués par ces faussaires ont une chose en commun : ils servent d'appâts pour amener le client à cliquer sur un lien fourni dans le message. Si le client mord à l'hameçon, le lien le dirige directement vers un site imitant celui de sa banque et contenant un formulaire que la victime doit compléter. Sans le savoir, la victime fournit alors elle-même au cyber-criminel toutes les informations dont il a besoin pour accéder à son compte et lui voler de l'argent.

Rootkits et brouillage de code

Les rootkits sont utilisés pour masquer la présence de code malveillant. Ils cachent les changements qu'ils ont faits sur la machine d'une victime.

En général, l'auteur du programme malveillant obtient l'accès au système en piratant le mot de passe ou en exploitant une vulnérabilité d'application. Ensuite, il utilise cela pour obtenir d'autres informations du système, jusqu'à ce qu'il obtienne l'accès administrateur à la machine. Les rootkits sont souvent utilisés pour masquer la présence d'un cheval de Troie en dissimulant ses processus, les modifications du registre et d'autres activités du système.

Une version « améliorée » du rootkit a également été développée : le « bootkit ». Le premier bootkit, détecté en 2008, s'appelait Sinowal (également connu sous le nom de Mebroot). Le but des bootkits est le même que celui des rootkits : masquer la présence de programmes malveillants dans le système. La différence, c'est que le bootkit s'installe lui-même sur le secteur d'amorçage maître (MBR) pour se charger le plus tôt possible (le MBR est le premier secteur physique du disque dur et le code inscrit dans ce secteur est chargé immédiatement après que les instructions dans le BIOS soient chargées). Depuis, les bootkits n'ont cessé de se développer, y compris dans les versions 64 bits.

Une astuce GReAT : Développer une stratégie de sécurité

Votre stratégie de sécurité doit être adaptée à votre entreprise et ne pas reposer uniquement sur des « bonnes pratiques » et des « estimations » génériques. Une évaluation approfondie est nécessaire pour déterminer les risques auxquels votre entreprise est exposée.
Vous aurez besoin de mesurer l'efficacité de vos outils de sécurité et vous devrez prévoir de mettre en place un process de mise à jour de votre stratégie, afin de répondre aux nouvelles menaces.

Chapitre 2 : Mode de propagation des programmes malveillants

Les cyber-criminels ont recours à diverses techniques pour infecter l'ordinateur de leurs victimes. En voici la description ci-dessous :

Téléchargement intempestifs

Voici une des principales méthodes utilisées pour propager les programmes malveillants. Les cyber-criminels recherchent des sites Web non sécurisés et dissimulent leur code dans une des pages de ce site : lorsque quelqu'un affiche cette page, le programme malveillant peut être transféré automatiquement et de manière invisible sur son ordinateur avec le reste du contenu demandé. C'est ce qu'on appelle le téléchargement intempestif, car il ne nécessite pas d'autre intervention de la victime que la simple consultation de la page Web infectée.

Les cyber-criminels introduisent un script dans la page Web, qui installe un programme malveillant sur l'ordinateur de la victime ou, plus souvent, prend la forme d'une redirection IFRAME vers un site contrôlé par les cyber-criminels.
La victime est infectée si le système d'exploitation ou les applications de son ordinateur ne sont pas corrigées.

Les cyber-criminels introduisent un script dans la page Web, qui installe un programme malveillant sur l'ordinateur de la victime ou, plus souvent, prend la forme d'une redirection IFRAME vers un site contrôlé par les cyber-criminels.

Réseaux sociaux

À l'instar des pickpockets, les cyber-criminels opèrent là où il y a du monde. Certains réseaux sociaux disposent d'une base d'utilisateurs de la taille d'un pays, qui constitue une réserve de victimes potentielles toutes trouvées. Les cyber-criminels utilisent les réseaux sociaux de différentes manières.

- Tout d'abord, ils utilisent des comptes piratés pour propager des messages qui contiennent des liens vers un code malveillant
- Deuxièmement, ils développent de fausses applications qui récoltent les données personnelles de la victime (celles-ci peuvent ensuite être vendues à d'autres cyber-criminels) ou installent des programmes malveillants (par exemple, de faux logiciels anti-virus)
- Enfin, ils créent de faux comptes qui réunissent des « amis », recueillent des informations personnelles et les vendent à des publicitaires.

Messageries électroniques et instantanées

Environ 3 % des e-mails contiennent des logiciels malveillants, sous la forme de pièces jointes ou de liens vers des sites Web malveillants. En plus des campagnes de phishing en vrac, conçues pour voler les données confidentielles de quiconque se laisse prendre par l'escroquerie, l'e-mail est également utilisé dans des attaques ciblées, comme moyen d'obtenir un point d'ancrage initial dans les organisations cibles.
Dans ce cas, l'e-mail est envoyé à une personne spécifique dans une organisation, dans l'espoir qu'elle ouvrira la pièce jointe ou cliquera sur le lien et déclenchera le processus par lequel les attaquants peuvent accéder au système. Cette approche est connue sous le nom de harponnage.

Pour maximiser leurs chances de réussite, les cyber-criminels envoient généralement leurs e-mails au personnel en relation directe avec le public (souvent non-technique), tels que les managers marketing et vente. L'e-mail s'adresse à la personne par son nom, l'adresse d'expédition est usurpée pour donner l'impression qu'elle vient d'une personne de confiance interne à l'organisation et le contenu de l'e-mail est adapté aux intérêts de l'organisation, afin de paraître légitime.

Généralement, les auteurs de campagnes d'attaques ciblées adaptent le contenu en fonction de la nature spécifique de l'entreprise qu'ils veulent pirater. Les cyber-criminels utilisent également la messagerie instantanée pour répandre des liens vers des programmes malveillants.

Pour maximiser leurs chances de réussite, les cyber-criminels envoient généralement leurs e-mails au personnel en relation directe avec le public (souvent non-technique), tels que les managers marketing et vente.

Supports amovibles

Les supports de stockage physique sont idéaux pour propager des programmes malveillants. Ainsi, les cyber-criminels utilisent des clés USB pour étendre la pénétration des programmes malveillants au sein d'une organisation, une fois l'infection initiale lancée.

Elles sont également utilisées pour aider les programmes malveillants à parcourir l'« espace d'air virtuel » entre un ordinateur connecté à Internet et un réseau de confiance qui est isolé d'Internet.

Les programmes malveillants utilisent souvent les vulnérabilités des clés USB pour lancer automatiquement un code une fois insérées dans un ordinateur.

Vulnérabilités et exploitation des failles

Pour installer des programmes malveillants sur les ordinateurs des victimes, les cyber-criminels exploitent souvent les vulnérabilités non corrigées des applications. Cette méthode repose sur l'existence de vulnérabilités et sur le fait que les individus ou entreprises ne corrigent pas leurs applications.

De telles vulnérabilités, ou failles, peuvent être trouvées dans un système d'exploitation ou les applications fonctionnant sur l'ordinateur. Les cyber-criminels se concentrent généralement sur les applications les plus courantes, susceptibles de ne pas être corrigées avant un long moment, ce qui leur donne une marge suffisante pour atteindre leurs objectifs.

Vulnérabilités zero-day

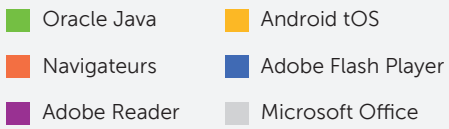
Mais ils ne se contentent pas de compter sur le fait que les utilisateurs ne corrigent pas leurs applications :

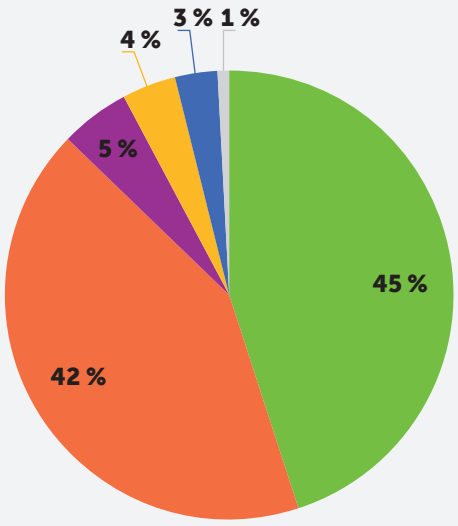
Parfois, ils sont même en mesure d'identifier les vulnérabilités avant qu'un fournisseur d'application ne le fasse et d'écrire un code de vulnérabilité pour profiter de la faille.

Elles sont connues comme les failles zero-day et fournissent aux cyber-criminels l'occasion de diffuser leurs programmes malveillants sur tout ordinateur où se trouve l'application vulnérable. Il n'y a simplement aucun correctif disponible pour bloquer la faille.

APPLICATIONS VULNÉRABLES UTILISÉES PAR LES FRAUDEURS

Le graphique des applications vulnérables montré ci-contre est fondé sur les informations concernant les « exploits » bloqués par nos produits. Ces failles ont été utilisées par des pirates informatiques dans des attaques Internet et lorsqu'elles compromettaient des applications locales, y compris celles installées sur des appareils mobiles.





La distribution des « exploits » utilisés par les fraudeurs, par type d'application attaquée, 2014

Source : Kaspersky Lab

Certificats numériques

Nous avons tous tendance à faire confiance aux sites Web disposant d'un certificat de sécurité émis par une autorité de certification authentique ou à une application possédant un certificat numérique valide.

Malheureusement, non seulement les cyber-criminels ont pu émettre de faux certificats pour leur programmes malveillants, à l'aide de soi-disant certificats auto-signés, mais ils ont également réussi à violer les systèmes de diverses autorités de certification et à utiliser des certificats volés pour signer leur code.

Cela leur permet d'inspirer confiance et d'optimiser leurs chances de réussite : les entreprises et les individus sont évidemment plus susceptibles de faire confiance à un code signé.

Une astuce GReAT : Déployez une protection complète et intégrée contre les programmes malveillants

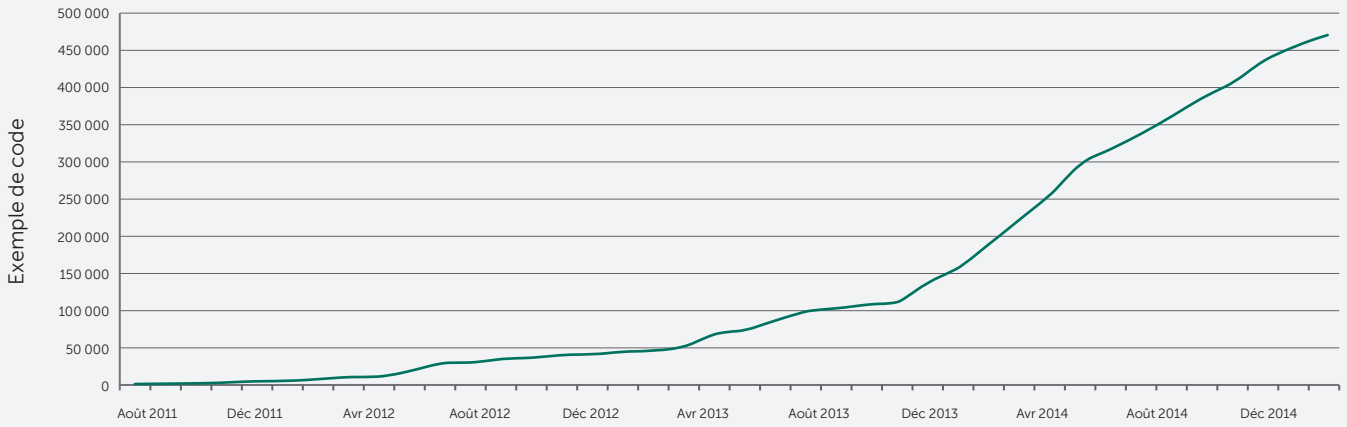
Veillez à toujours exécuter le logiciel de sécurité le plus récent, à appliquer les mises à jour lorsqu'elles sont disponibles et à supprimer les logiciels qui ne sont plus utiles.

Chapitre 3 : Hausse des programmes malveillants contre les appareils mobiles

Les cyber-criminels se concentrent désormais sur les appareils mobiles. Les premières menaces sont apparues en 2004, mais les attaques contre les appareils mobiles ne constituent des menaces importantes que depuis quelques années. L'accélération a eu lieu en 2011 : il y a eu le même nombre de menaces détecté en 2011 que sur l'ensemble de la période 2004-2010. Cette croissance explosive a continué depuis. À la fin 2014, on recensait 470 000 échantillons de codes de programmes malveillants différents sur appareils mobiles.

CODES MALVEILLANTS SUR LES APPAREILS MOBILES

14 643 582 packs d'installation



Source : Kaspersky Lab

En 2014, plus de 295 000 échantillons sont apparus. Ces échantillons de code sont souvent réutilisés et reconditionnés de nombreuses fois, le nombre de packs d'installation malveillants dépasse ainsi de loin le nombre d'échantillons de code : à la fin 2014, le nombre total de packs d'installation de programmes malveillants sur appareils mobiles était de près de 15 millions. Au cours de l'année 2014, Kaspersky Lab a bloqué plus de 1,3 million d'attaques et 19 % des personnes utilisant des appareils Android ont rencontré au moins une menace de programme malveillant mobile. Malgré la croissance spectaculaire des programmes malveillants sur appareils mobiles, de nombreuses entreprises ignorent encore le danger potentiel et, en conséquence, de nombreux appareils mobiles ne sont pas protégés.

La plus grande part des programmes malveillants sur appareils mobiles est ciblée sur les appareils Android. La principale raison est qu'Android fournit un environnement ouvert pour les développeurs d'applications et cela a conduit à la création d'une grande et vaste sélection d'applications. Il existe peu de restrictions concernant l'emplacement d'origine où sont téléchargées les applications, ce qui augmente l'exposition des utilisateurs aux applications malveillantes. En revanche, le système iOS est un système de fichiers fermé et restreint, qui permet le téléchargement et l'utilisation d'applications en provenance d'une seule source, l'App Store. Cela signifie un risque plus faible pour la sécurité : afin de distribuer le code, les aspirants auteurs de programmes malveillants doivent trouver une façon de falsifier le code dans l'App Store ou limiter leurs attaques aux appareils iOS « débridés ». Il est donc probable que, pour le moment du moins, Android reste le principal centre d'intérêt des cyber-criminels.

À la fin 2014, le nombre total de packs d'installation de programmes malveillants sur les appareils mobiles était de près de 15 millions.

Banque mobile : la prochaine proie des cyber-criminels ?

L'utilisation de smartphones pour les services bancaires en ligne est grandissante et il est clair que les cyber-criminels tournent leur attention vers elle.

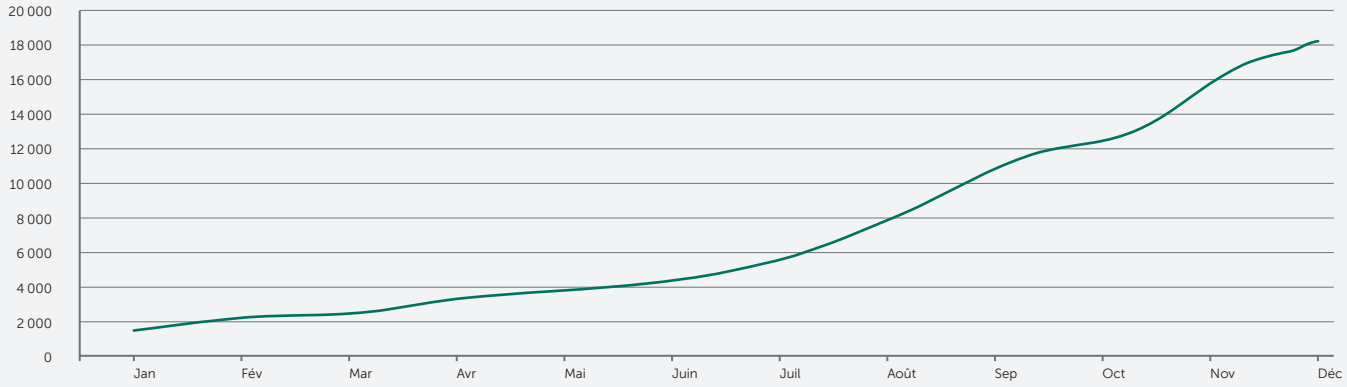
Il est déjà courant d'utiliser des appareils mobiles dans le cadre de l'authentification double des transactions bancaires réalisées sur un ordinateur de bureau ou un ordinateur portable. La banque envoie sur le smartphone du client un SMS contenant un mot de passe temporaire nécessaire à l'exécution d'une transaction.

Il n'est donc pas surprenant que l'on ait constaté l'apparition d'attaques spécialement conçues pour capturer les numéros mTAN (mobile Transaction Authentication Numbers, numéros d'authentification des transactions mobiles). Elles sont connues sous le nom d'attaques « Man-in-the-Mobile » et de nombreuses menaces spécifiques ont été développées à cet effet : ZeuS-in-the-Mobile (ou ZitMo), SpyEye-in-the-Mobile (ou SpitMo) et Carberp-in-the-Mobile (ou CitMo).

Le nombre de chevaux de Troie bancaires a considérablement augmenté au cours de 2014, passant de moins de 2 000 au début de l'année à plus de 18 000 à la fin de l'année. Ces chevaux de Troie, qui visaient auparavant presque exclusivement des victimes russes, se trouvent maintenant dans de nombreux pays du monde entier.

CHEVAUX DE TROIE CIBLANT LES DONNÉES BANCAIRES SUR MOBILE

Croissance spectaculaire en 2014



Source : Kaspersky Lab

Une astuce GReAT : Mettez en place une politique de sécurité de type « follow me »

Assurez-vous que vos solutions de sécurité sont flexibles et reflètent les évolutions des méthodes de travail pour que tous vos employés soient protégés sur leur lieu de travail et en dehors, quels que soient les appareils qu'ils utilisent.

Chapitre 4 : Êtes-vous particulièrement visé ? Une nouvelle ère d'attaques ciblées

Les attaques et les attaques ciblées

Le panorama des menaces continue d'être dominé par des attaques spéculatives et aléatoires conçues pour voler les informations personnelles des malchanceux qui en sont victimes. De telles attaques affectent non seulement les consommateurs individuels, mais également les entreprises. Souvent, l'objectif est d'utiliser des données d'identification volées pour accéder à des comptes financiers et dérober de l'argent. Toutefois, le nombre d'attaques ciblées sur des organisations est en nette augmentation et ce type de menace est à présent bien ancré dans le paysage.

Les attaques ciblées cherchent à pénétrer une entreprise cible, à voler ses données ou à nuire à sa réputation. Aussi, nous sommes maintenant dans une ère où le code malveillant peut être utilisé comme une cyber-arme : alors qu'une entreprise particulière pourrait ne pas être dans la ligne de mire directe, elle pourrait devenir un « dommage collatéral » si elle n'est pas adéquatement protégée.

À lire les gros titres des médias sur les attaques ciblées, on peut avoir tendance à conclure que les attaques ciblées ne concernent que les grandes entreprises, en particulier celles qui gèrent les systèmes d'infrastructures stratégiques d'un pays. En réalité, toute entreprise peut un jour ou l'autre en être victime. Toutes les entreprises détiennent des données qui peuvent être utiles aux cyber-criminels et toutes sont susceptibles de servir de passerelles pour atteindre d'autres entreprises.

Cyber-armes

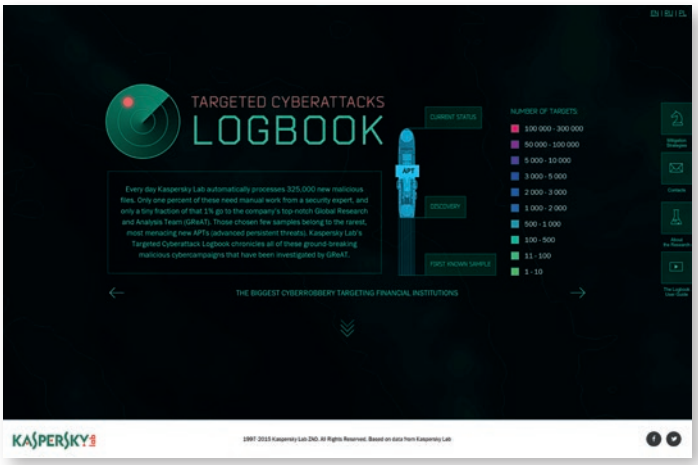
Stuxnet a été le premier programme malveillant hautement sophistiqué utilisé pour réaliser des attaques ciblées contre des sites de production stratégiques. En outre, l'apparition d'autres attaques commanditées par un État (Duqu, Flam, Gauss, Careto, Regin, Equation et Dudu 2.0) a clairement fait savoir que ce type d'attaque est loin d'être un incident isolé.

Nous vivons désormais dans une ère de « cyber-guerre froide » où les nations ont la possibilité de combattre les unes contre les autres sans être entravées par les limites des guerres « réelles ». À l'avenir, on peut s'attendre à ce que davantage de pays développent des cyber-armes conçues pour dérober des informations ou saboter des systèmes : en effet, le niveau de base requis pour développer ce genre d'armes est bien inférieur à celui nécessaire au développement d'armes physiques.

Il est également possible que l'on voie apparaître des attaques du même genre commanditées par des acteurs autres que les nations, auquel cas il y aura un risque plus élevé de « dommages collatéraux », c'est-à-dire de victimes autres que celles visées.
Parmi les cibles potentielles de ce genre de cyber-attaques, on peut citer les installations de contrôle de l'approvisionnement énergétique et du transport, les systèmes financiers et de télécommunications, ainsi que d'autres installations d'infrastructures stratégiques.

Registre des cyber-attaques ciblées

Le Registre des cyber-attaques ciblées de Kaspersky Lab décrit toutes les cyber-campagnes malveillantes innovantes qui ont été étudiées par le GReAT.



Visitez https://apt.securelist.com/ pour obtenir plus d'informations

Chapitre 5 : Le facteur humain en matière de sécurité

Le facteur humain

L'être humain est généralement le maillon faible de la chaîne de sécurité. Il existe plusieurs raisons à cela :

- De nombreuses personnes ne sont pas conscientes des ruses utilisées par les cyber-criminels
- Les escroqueries successives ne se ressemblent jamais tout à fait, ce qui rend difficile aux particuliers de savoir à quels éléments il faut faire attention

Le problème peut être pire dans le cas de smartphones et tablettes. Leur taille et leur portabilité peut être un grand avantage, mais ils sont également facilement perdus ou volés. S'ils tombent entre de mauvaises mains, un code PIN ou code d'accès faible (voire inexistant) devient un point de faille unique : la seule chose entre une personne non autorisée et les données stockées sur l'appareil.

De même, alors que c'est un avantage d'avoir du personnel connecté en permanence, cela devient dangereux si le personnel effectue des transactions confidentielles sur des réseaux wifi non fiables ou s'il se connecte par inadvertance à une fausse borne wifi (le réseau wifi appelé « café » pourrait être légitime, mais celui nommé « café-vite » pourrait appartenir à un criminel qui cherche à recueillir des données à partir d'une personne peu méfiante).

Parfois, les utilisateurs passent outre les procédures pour se simplifier la vie et ne sont pas conscients des conséquences de leur comportement en termes de sécurité. Cela vaut notamment pour les mots de passe. Beaucoup de gens utilisent le même mot de passe pour tout : souvent quelque chose qui est aussi facile à retenir que « mot de passe », « 123456 », « qwerty » ou « football » !

Il est alors d'autant plus facile pour un cyber-criminel de deviner leur mot de passe. Si la sécurité d'un compte est compromise, elle offre un accès facile à d'autres comptes. Même lorsqu'on les informe du danger potentiel, la plupart des individus ne voient pas d'alternative réalisable, car ils pensent ne pas être en mesure de mémoriser un grand nombre de mots de passe différents et complexes.

Une astuce GReAT : Protégez tous vos mots de passe

Pour obtenir plus d'informations sur la sécurité de votre mot de passe, lisez le blog de David EMM sur The Huffington Post.

Ingénierie sociale

L'ingénierie sociale est la manipulation de la psychologie humaine : convaincre quelqu'un de faire ce que vous voulez. Dans le contexte de la sécurité informatique, cela signifie piéger une personne pour qu'elle fasse quelque chose qui nuise à sa sécurité, ou à la sécurité de l'entreprise dans laquelle elle travaille. Les e-mails de phishing sont un bon exemple d'ingénierie sociale. Elle prend généralement la forme de courriers indésirables envoyés à un grand nombre de personnes, bien que le harponnage soit une version ciblée conçue pour tromper les victimes dans des organisations spécifiques. Elle imite les vrais e-mails d'une entreprise réelle. Elle imite le logo, la police de caractères et le style de la véritable entreprise, dans l'espoir qu'un nombre suffisant de personnes recevant l'e-mail croira qu'il s'agit d'une communication authentique. Lorsque la victime clique sur le lien, elle est redirigée vers un faux site Web où elle est invitée à divulguer des informations personnelles (noms d'utilisateur, mots de passe, codes PIN et autres informations pouvant être utiles aux cyber-criminels).

L'utilisation généralisée des réseaux sociaux a simplifié la tâche des cyber-criminels. En effet, ils peuvent y recueillir les données que les gens publient en ligne et les utiliser pour rendre un e-mail de phishing plus crédible.

Une astuce GReAT : Sensibiliser

Les cyber-criminels utilisent de plus en plus des données publiques pour lancer des attaques ciblées contre des entreprises. Informez vos collègues des risques associés au partage en ligne d'informations personnelles et professionnelles.

Pour obtenir plus de conseils sur la façon de diffuser le message à vos collaborateurs, consultez les 10 meilleurs astuces à la fin de ce guide.

Chapitre 6 : Technologies de défense contre les programmes malveillants

Technologies actuelles de défense contre les programmes malveillants
Des centaines de milliers de programmes malveillants apparaissent chaque jour. L'augmentation impressionnante de ces dernières années exige de bloquer les menaces de façon proactive : les signatures seules ne suffisent plus. Certaines des principales technologies de protection contre les programmes malveillants utilisées aujourd'hui sont présentées ci-dessous.

Analyse heuristique
Analyse utilisée pour détecter de nouvelles menaces inconnues. Elle fait appel à une signature qui identifie des instructions malveillantes connues, plutôt qu'un programme malveillant en particulier.
Elle peut également faire appel à une sandbox (environnement virtuel sécurisé créé dans une mémoire) afin d'étudier le comportement du code dans l'environnement réel de l'ordinateur.

Analyse des vulnérabilités et gestion des correctifs
Les cyber-criminels ayant tendance à profiter des vulnérabilités des applications, il est utile de pouvoir identifier sur un système les applications qui sont vulnérables face aux attaques, afin de permettre aux entreprises ou aux individus de mettre en place des actions réparatrices avec une gestion des correctifs. Certaines solutions sont également dotées d'une fonction d'analyse en temps réel des ordinateurs pour bloquer l'utilisation des vulnérabilités zero-day.

Signatures
En général, il s'agit de séquences caractéristiques d'octets utilisées pour identifier un programme malveillant en particulier. Mais les solutions de protection contre les programmes malveillants ont souvent recours à des signatures génériques pour détecter de grands nombres de programmes malveillants appartenant à la même famille.

Analyse comportementale
Cette démarche consiste à surveiller le système en temps réel pour voir comment un code agit avec l'ordinateur. Les dispositifs les plus sophistiqués n'examinent pas uniquement le code de manière isolée : ils suivent également ses activités sur différentes sessions et observent comment le code interagit avec d'autres processus sur l'ordinateur. Pour se protéger contre les cryptovirus, Kaspersky Lab utilise deux technologies : **System Watcher**, qui fait partie d'une protection proactive et **Application Privilege Control**, qui peut restreindre les droits d'une application.
Par exemple, il peut interdire aux applications d'apporter des modifications aux fichiers du système.

Listes blanches
Jusqu'à présent, les solutions de protection contre les programmes malveillants étaient basées sur l'identification de codes connus pour être malveillants, les programmes de « liste noire ». Les programmes de liste blanche et le blocage par défaut procèdent de manière inverse en bloquant les codes qui ne figurent pas sur la liste des programmes acceptables.

Services de réputation
Actuellement, de nombreuses solutions ont très souvent recours à une infrastructure basée sur le cloud, qui permet de bénéficier d'une protection quasi en temps réel contre une menace récemment découverte.

Les métadonnées des programmes s'exécutant sur un ordinateur protégé sont chargées sur les ordinateurs basés sur le cloud d'un éditeur de sécurité, où leur réputation globale est évaluée : sont-elles bonnes ou mauvaises, leur quantité est-elle connue, à quelle fréquence les a-t-on observées, où les a-t-on observées, etc. Le système fonctionne comme un système global de surveillance de quartier, surveillant les programmes exécutés sur des ordinateurs du monde entier et fournissant une protection à tout ordinateur protégé si un élément malveillant est détecté.

Kaspersky Security Network
Kaspersky Security Network (KSN), est le service assisté par cloud de Kaspersky Lab. Il apporte de la valeur ajoutée aux clients, les protégeant même de menaces encore inconnues, en surveillant constamment la réputation des applications exécutées et des URL consultées. Si la réputation du fichier passe soudainement de « bonne » à « mauvaise », les clients KSN en sont informés en quelques minutes et les ressources de leur entreprise sont immédiatement protégées contre lui.

Les programmes malveillants évolués nécessitent une solution évoluée : l'émergence des plates-formes intégrées

Les programmes malveillants continuent de se développer en termes de volume et de sophistication. C'est pourquoi les entreprises sont actuellement exposées à un nombre croissant de vecteurs d'attaque.

Le maintien à jour et le contrôle de l'utilisation du Web, l'accroissement de la mobilité du personnel (et des données), la mise à jour d'une série de plus en plus complexe d'applications, etc. font que les équipes informatiques en manque de ressources doivent souvent faire des compromis en termes de sécurité informatique.

Face à la complexification de l'environnement, la solution peut être d'ajouter de nouvelles technologies permettant de gérer et de protéger les différents domaines de risque, mais cela accroît la charge de travail de l'équipe informatique, les coûts et même les risques.

Le nouveau paysage des menaces a entraîné la création de la première plate-forme de sécurité unique véritablement intégrée, développée par Kaspersky Lab. Cette plate-forme sous forme de console de gestion est le meilleur moyen de rassembler toutes les technologies et de permettre leur visualisation, gestion et protection.

Une astuce GReAT : Utilisez des technologies proactives

Déployez des solutions de protection contre les programmes malveillants rassemblant différentes technologies pour bloquer des menaces connues, inconnues et avancées en temps réel, au lieu de dépendre d'une simple protection à base de signatures.

L'équipe GReAT

Les informations contenues dans ce rapport sont fournies par l'équipe Global Research and Analysis de Kaspersky Lab (GReAT).
Depuis 2008, l'équipe GReAT ouvre la voie en matière d'informations, de recherche et d'innovation sur la protection contre les menaces, au sein de Kaspersky Lab et en externe.

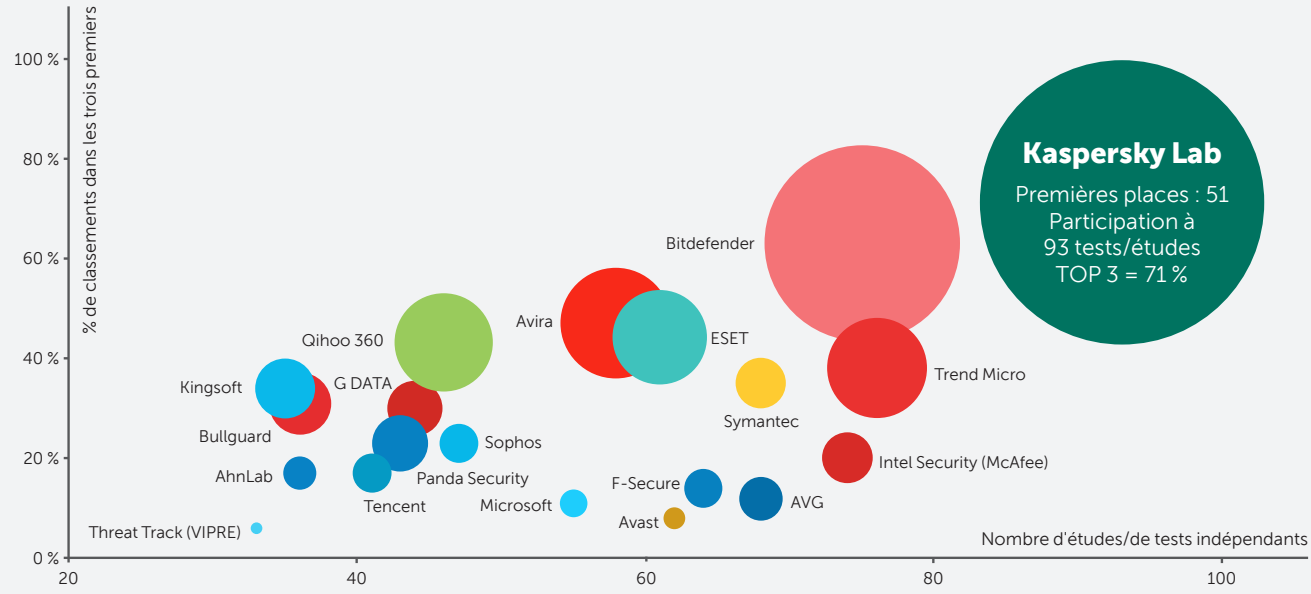
Le GReaT a été à l'avant-garde de l'analyse de certaines des menaces les plus sophistiquées au monde, y compris Stuxnet, Duqu, Flame, Red October, NetTraveler, Careto, Equation, Carbanak et Duqu 2.0. En 2013, le GReAT a remporté le titre d'« **Équipe dédiée à la sécurité des informations de l'année** » aux SC Awards.

Pourquoi Kaspersky Lab ?

Classé parmi les quatre plus grands spécialistes mondiaux de la sécurité, Kaspersky Lab est l'un des fournisseurs de solutions de sécurité informatique enregistrant la croissance la plus rapide au monde. Présents dans près de 200 pays et territoires à travers le monde, nous fournissons une protection à plus de 400 millions d'utilisateurs et plus de 270 000 entreprises clientes de toutes tailles, des petites et moyennes entreprises aux grandes organisations gouvernementales et commerciales.

Nos solutions de sécurité intégrées et avancées permettent aux entreprises de contrôler de manière inégalée l'utilisation des applications, du Web et des périphériques : vous définissez les règles et nos solutions vous aident à les gérer. Kaspersky Endpoint Security for Business est spécifiquement conçue pour combattre et bloquer les menaces persistantes sophistiquées d'aujourd'hui. Déployée parallèlement à Kaspersky Security Center, cette solution donne aux équipes de sécurité la visibilité et le contrôle dont elles ont besoin, quelles que soient les menaces auxquelles elles font face.

En 2014, les produits Kaspersky Lab ont fait l'objet de 93 études et tests indépendants. Nos produits ont figuré 51 fois en première position et 66 fois parmi les trois premiers.[5]



** Remarques : D'après le résultat synthétisé d'un test indépendant réalisé en 2014 pour les produits d'entreprise, grand public et mobiles.*

La synthèse comprend les tests effectués par les laboratoires et les magazines indépendants suivants : Laboratoires de test : AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin. La taille de la bulle correspond au nombre de premières places.

5 : http://www.kaspersky.com/TOP3/

10 conseils pour sensibiliser vos collaborateurs à la sécurité informatique

Vous avez peut-être du mal à sensibiliser vos collaborateurs à l'importance de la sécurité informatique dans votre entreprise. C'est pourquoi nous avons rassemblé dix conseils pour vous aider à communiquer plus facilement sur les problèmes de sécurité que rencontre votre entreprise.

1
Adressez-vous adéquatement à votre public
Évitez d'appeler quiconque « utilisateurs » : c'est impersonnel et cela peut donner à votre auditoire le sentiment d'être un peu dissocié de ce que vous dites. Préférez des mots comme « employé », « collaborateur », « collègue » ou « personne ».

2
Utilisez le ton de voix approprié
Un ton accessible et amical vous aidera à communiquer avec votre auditoire plus efficacement, vous garantissant d'instruire vos collaborateurs sur ce que chacun peut faire pour protéger l'entreprise.

3
Obtenez l'appui des équipes RH et juridique
Lorsque cela est nécessaire, elles peuvent mettre en place des politiques réelles et apporter leur soutien en cas d'atteinte à la sécurité informatique.

4
Tenez vos collaborateurs informés
Réfléchissez à la fréquence et au moment adéquats pour communiquer vos informations. Veillez à ce qu'ils soient réguliers et marquent les esprits.

5
Faites preuve d'imagination
Il existe de nombreux moyens de rendre des informations plus accrocheuses. Plus elles sont créatives et intéressantes, plus elles ont de chances d'être lues. Essayez des bandes dessinées, des affiches et des quiz.

6
Faites le bilan
Vos informations ont-elles été bien comprises ? Testez vos collègues et déterminez ce qu'ils ont retenu et ce qu'ils ont oublié. Vous pouvez par exemple commencer par leur soumettre un questionnaire sur les cinq problèmes majeurs de sécurité informatique.

7
Soulignez les conséquences pour chacun
Puiser dans les propres intérêts de vos collaborateurs les aidera à acquérir une meilleure compréhension de l'importance et du contexte de la sécurité informatique. Par exemple, parlez de la façon dont les atteintes à la sécurité pourraient affecter leurs appareils mobiles.

8
Proscrivez le jargon
La plupart des gens n'auront pas la même expertise que vous, donc assurez-vous de tout expliquer d'une manière qui soit facile à comprendre.

9
Encouragez les échanges
Veillez à ce que vos collègues comprennent les conséquences d'une atteinte à la sécurité et sachent à quel point il est important de vous en informer. Certains pourraient craindre d'être sanctionnés s'ils cliquent sur un e-mail de phishing et, par conséquent, éviter d'informer les bonnes personnes.

10
Consultez l'équipe marketing
Lorsqu'il s'agit de communications internes au sein de votre organisation, ce sont les experts. Demandez-leur donc de l'aide pour trouver le meilleur moyen de retenir l'attention de vos collaborateurs.

PRENEZ DES MESURES SANS PLUS ATTENDRE : ESSAI GRATUIT DE 30 JOURS

Découvrez comment nos solutions de sécurité peuvent protéger votre entreprise des programmes malveillants et de la cyber-criminalité en les essayant gratuitement pendant un mois.

Rendez-vous dès aujourd'hui sur http://www.kaspersky.fr/downloads/trials/business-trials pour télécharger des versions complètes de nos produits et évaluer leur capacité à protéger parfaitement votre infrastructure informatique, vos terminaux et les données confidentielles de votre entreprise.

EFFECTUEZ UN ESSAI GRATUIT DÈS MAINTENANT

RETROUVEZ-NOUS SUR LES RÉSEAUX SOCIAUX

#SecureBiz

Visionnez nos vidéos sur YouTube

Rejoignez nos fans sur Facebook

Suivez-nous sur Twitter

Retrouvez-nous sur LinkedIn

Découvrez nos présentations sur Slideshare

Découvrez notre blog https://business.kaspersky.com

Rejoignez-nous sur Threatpost

Retrouvez-nous sur Securelist

À PROPOS DE KASPERSKY LAB

Kaspersky Lab est une des entreprises de cyber-sécurité du monde connaissant la croissance la plus rapide. C'est aussi la plus grande société privée du secteur. Elle fait partie des quatre principaux éditeurs mondiaux de solutions de sécurité informatique (IDC, 2014). Depuis 1997, Kaspersky Lab a été pionnière en matière de cyber-sécurité. Elle offre des solutions de sécurité numériques efficaces et une surveillance des menaces pour les grandes entreprises, les PME et le grand public. Kaspersky Lab est une société internationale et est actuellement présente dans près de 200 pays et territoires à travers le monde, où elle apporte une protection à plus de 400 millions d'utilisateurs.

kaspersky.fr/business
kaspersky.fr/entreprise-securite-it
#SecureBiz