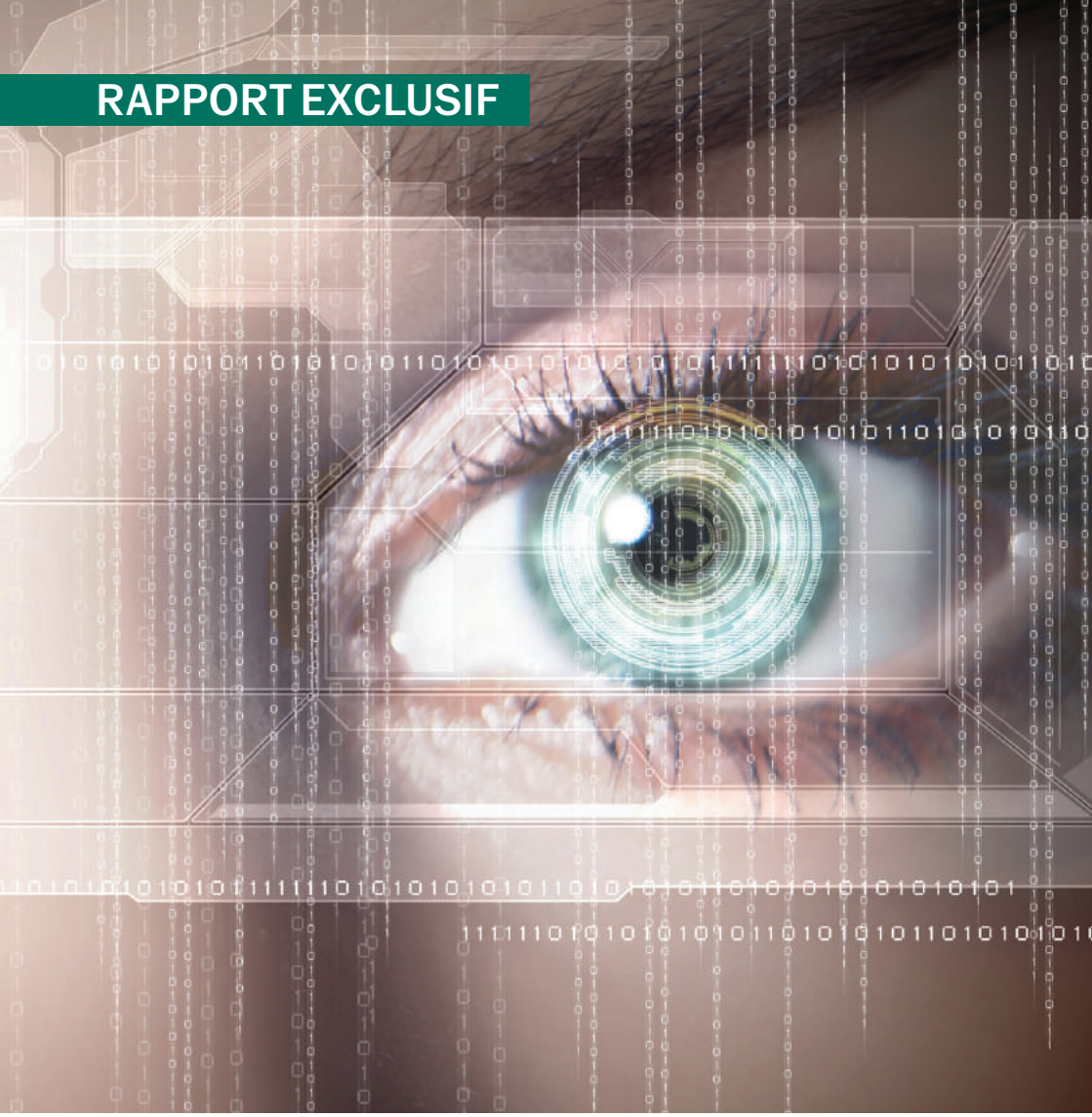
RAPPORT EXCLUSIF



QUI VOUS ESPIONNE ?

Aucune entreprise n'est à l'abri du cyber-espionnage

« Les attaques ciblées de haut niveau sur les entreprises sont de plus en plus répandues. Des milliers d'entreprises ont déjà fait l'objet d'actes de piratage et de vols de leurs données sensibles ayant entraîné des pertes financières s'élevant à plusieurs milliards de dollars. Le cyber-espionnage est désormais une menace mondiale, tangible et en pleine expansion. La lutte contre ce phénomène fait partie de nos priorités. »

EUGENE KASPERSKY
PDG, KASPERSKY LAB

SOMMAIRE

Cyber-espionnage :

Pourquoi votre entreprise doit-elle s'en préoccuper ? 4
L'espionnage n'a rien de nouveau 5
Quelle est la finalité recherchée du cyber-espionnage ? 7
Certaines entreprises sont-elles à l'abri ? 8

Méthodes de propagation des programmes malveillants de cyber-espionnage 14
Au-delà du cyber-espionnage 16
Comment pouvez-vous protéger votre entreprise ? 17
Comment les technologies de sécurité de Kaspersky Lab peuvent vous aider 22

Annexe :

Aperçu de quelques cyber-menaces importantes 28
Cyber-glossaire 30
À propos de Kaspersky 34

« Il est possible de limiter de nombreuses cyber-attaques en mettant en place des mesures relativement simples. Malheureusement, certaines personnes ignorent les précautions de base : utiliser des mots de passe difficiles à craquer, appliquer les correctifs de sécurité, utiliser une solution de sécurité, etc. Il est souvent plus facile de pénétrer dans un réseau d'entreprise qu'il n'y paraît. »

COSTIN RAIU
DIRECTEUR, ÉQUIPE GLOBAL RESEARCH & ANALYSIS
KASPERSKY LAB

POURQUOI VOTRE ENTREPRISE DOIT-ELLE SE PRÉOCCUPER DU CYBER-ESPIONNAGE ?

RÉSUMÉ ANALYTIQUE

Quand on parle de cyber-espionnage, on a tendance à croire que cela n'existe que dans les films. Et pourtant, pratiquement toutes les entreprises peuvent un jour ou l'autre en être la cible ou être victimes de dommages collatéraux.

Peu importe que votre entreprise soit directement visée ou pas. Dans les deux cas, les conséquences peuvent être dramatiques.

Dans ce rapport, les experts en cyber-sécurité de Kaspersky Lab vous montrent :

- En quoi les entreprises peuvent être affectées par les attaques directes et indirectes de cyber-espionnage
- Ce que vous pouvez faire pour protéger votre entreprise et sa réputation
- Comment certaines technologies peuvent vous aider à défendre votre réseau et vos données d'entreprise contre les menaces sophistiquées

Les risques sont bien réels et même de plus en plus nombreux et sophistiqués. Heureusement, Kaspersky Lab est là pour vous proposer des conseils avisés et des technologies de protection innovantes.

L'ESPIONNAGE N'A RIEN DE NOUVEAU

L'espionnage existe sous une forme ou une autre depuis que des organisations ou des individus ont un intérêt à dérober les informations confidentielles de tiers. Nous avons tous déjà entendu parler de tentatives de vol perpétrées par des États pour s'approprier les secrets d'autres pays. De même, l'espionnage industriel fait partie de la vie des entreprises depuis longtemps. Néanmoins, le niveau et la nature des menaces d'espionnage, qui pèsent aujourd'hui sur les entreprises de toutes tailles, ont considérablement évolué ces dernières années.

La simplicité de mise en œuvre des opérations d'espionnage incite désormais un plus grand nombre d'entreprises à s'adonner à cette pratique alors qu'elles n'auraient jamais envisagé de mettre à exécution des actes d'espionnage industriel classique.

QU'EST-CE QUI A DONC CHANGÉ ?

Avec l'amélioration des communications mobiles et du débit des connexions d'Internet, les entreprises ont rapidement compris l'utilité d'offrir à leurs employés, clients et fournisseurs un accès à tout moment et en tout lieu à leurs systèmes et données. Les avantages en termes d'efficacité et de productivité ont été considérables, voire révolutionnaires pour de nombreuses sociétés, Internet les aidant à créer de nouveaux débouchés et à générer des revenus supplémentaires.

Cependant, cette connectivité permanente aux informations de l'entreprise et à d'autres données sensibles a également fait le jeu des cyber-criminels. Maintenant que les entreprises stockent leurs ressources de propriété intellectuelle et leurs informations confidentielles dans des systèmes en réseau, les opérations d'espionnage sont bien plus faciles à mettre en œuvre et peuvent être bien plus rentables pour leurs auteurs.

SIMPLIFICATION DE L'ESPIONNAGE ET ACCÉLÉRATION DES RÉSULTATS

Il est loin le temps où il fallait pénétrer par effraction dans les bureaux d'une entreprise ou attendre patiemment que des « infiltrés » recueillent des informations et dévoilent des secrets. Fouiller dans les corbeilles à papier des entreprises ou rémunérer des employés en échange d'informations est non seulement peu efficace, mais cela demande du temps et les risques sont élevés. Aujourd'hui, ce genre de pratiques n'a tout simplement plus lieu d'être. Avec les compétences informatiques adéquates, des individus et des organisations peuvent espionner des entreprises et obtenir de précieuses informations via un simple ordinateur.

Ils profitent pour cela du manque de sécurité des sites Web de ces entreprises, des failles des logiciels professionnels qu'elles utilisent ou du manque de discernement de leurs employés, qui cliquent sur des liens ou des pièces jointes d'e-mails infectés par du code malveillant.

LES CYBER-ATTAQUES ONT DE SÉRIEUSES RÉPERCUSSIONS SUR LES BÉNÉFICES D'UNE ENTREPRISE.

PERTES MOYENNES EN CAS DE CYBER-ATTAQUE CIBLÉE :

2 400 000 $

Source : enquête 2013 sur les risques liés à la sécurité informatique pour les entreprises mondiales, B2B International

LORSQUE DES ENTREPRISES PERDENT DES DONNÉES, ELLES PERDENT SOUVENT BIEN PLUS QUE CELA.

COÛT MOYEN D'UNE PERTE DE DONNÉES POUR UNE GRANDE ENTREPRISE :

649 000 $

Source : enquête 2013 sur les risques liés à la sécurité informatique pour les entreprises mondiales, B2B International

QUELLE EST LA FINALITÉ RECHERCHÉE DU CYBER-ESPIONNAGE ?

IL EXISTE DIFFÉRENTS TYPES D'ASSAILLANTS QUI POURSUIVENT CHACUN DES OBJECTIFS DIFFÉRENTS :

- Les cyber-criminels mesurent parfaitement la valeur des informations d'entreprise. Ils peuvent gagner de l'argent en ayant recours à l'extorsion et en demandant des rançons, mais aussi en revendant des données volées sur le marché noir.
- Les hacktivistes (contraction de hacker, - pirate -, et d'activiste) ont pour but de perturber et de nuire à la réputation d'organisations auxquelles ils sont opposés. Ils savent que les fuites d'informations confidentielles, qu'elles concernent leurs clients, leurs fournisseurs ou leurs employés, peuvent sérieusement les compromettre et leur valoir de graves sanctions pénales.
- Les cyber-mercenaires proposent leurs services aux entités (gouvernements, groupes de protestation ou entreprises) prêtes à les payer pour obtenir des informations.
- Les États (agences gouvernementales) ou leurs sous-traitants cherchent à recueillir des informations stratégiques ou à perturber le fonctionnement d'installations industrielles de pays hostiles.

« Les informations étant synonymes de pouvoir, quand un cyber-criminel vole des informations, il neutralise les avantages dont bénéficie le propriétaire légitime de ces données.

Cela vaut également si la cible est un État (qui détient des secrets militaires) ou une entreprise dont la propriété intellectuelle et les secrets commerciaux lui confèrent un avantage concurrentiel. »

SERGEY LOZHKIN
CHERCHEUR EN SÉCURITÉ
ÉQUIPE GLOBAL RESEARCH & ANALYSIS
KASPERSKY LAB

« Les entreprise de toutes tailles traitent et stockent des données précieuses pour elles-mêmes, pour leurs clients et pour leurs concurrents.

Même une simple base de données contenant les coordonnées de clients a de la valeur. »

PETER BEARDMORE
DIRECTEUR SENIOR MARKETING PRODUIT
KASPERSKY LAB

EXISTE-T-IL DES ENTREPRISES QUI SOIENT À L'ABRI DU CYBER-ESPIONNAGE ?

La réponse est non. Même les toutes petites entreprises peuvent être directement ciblées en raison des informations sensibles ou précieuses qu'elles détiennent, qu'il s'agisse de coordonnées bancaires de clients, d'informations sur les fournisseurs ou même de données pouvant servir à lancer une attaque contre une plus grande entreprise.

Par exemple, les « attaques contre la chaîne d'approvisionnement » telles qu'IceFog (voir annexe I) recueillent des informations auprès de tiers/fournisseurs, puis utilisent ces données pour développer et lancer des attaques ciblées contre des entreprises ou des organisations en particulier.

« Lorsque vous évaluez les risques pour votre entreprise, ne sous-estimez jamais le rôle du facteur humain dans votre système de défense. Si des employés tombent dans le piège d'opérations de phishing ciblé ou cliquent sur le lien infecté d'un e-mail, votre sécurité peut être mise en danger. »

SERGEY LOZHKIN
CHERCHEUR EN SÉCURITÉ
ÉQUIPE GLOBAL RESEARCH & ANALYSIS
KASPERSKY LAB

« Qu'il s'agisse d'une entreprise du classement Fortune 500 ou de la start-up de deux ados travaillant dans le garage de leurs parents, chacune a quelque chose à perdre. »

CHARLES KOLODGY
VICE-PRÉSIDENT, RECHERCHE, PRODUITS DE SÉCURITÉ
IDC

VOTRE ENTREPRISE EST-ELLE UNE CIBLE DE CHOIX ?

On comprend facilement pourquoi les organismes gouvernementaux et les agences militaires font l'objet d'attaques de cyber-espionnage. Si certaines initiatives sont commanditées par des États, des groupes de protestation indépendants tentent également de perturber le fonctionnement d'activités gouvernementales ou de voler des informations sensibles. Les cyber-mercenaires ciblent eux-aussi les organismes gouvernementaux pour satisfaire les objectifs de leur employeur, à savoir le vol d'argent et de données.

De même, au vu de la grande quantité d'informations de valeur et de la réputation durement acquise qu'elles doivent protéger, les grandes entreprises et les multinationales sont elles aussi la cible évidente de cyber-attaques en tous genres, parmi lesquels des actes de cyber-espionnage.

ATTAQUE CONTRE GOOGLE, ADOBE ET D'AUTRES ENTREPRISES

Décrite comme un tournant dans l'histoire de la cyber-sécurité, l'attaque Opération Aurora a affecté Google, Adobe et plus de 30 autres entreprises d'envergure en 2009.

En dépit des efforts déployés pour résoudre les vulnérabilités logicielles exploitées par les auteurs de cette attaque, on a appris en 2012 que celle-ci continuait de cibler des entreprises du secteur de la défense et les chaînes d'approvisionnement de société tierces.

Les auteurs de ces attaques cherchent à prendre le contrôle de systèmes d'entreprise et à accéder aux données confidentielles. Les sites Web non sécurisés et les stratégies d'e-mails de phishing sont au cœur de ce qui est largement considéré comme une attaque de cyber-espionnage commanditée par un État.

ATTAQUES CONTRE AMERICAN EXPRESS ET JP MORGAN CHASE

En 2013, American Express et JP Morgan Chase ont été victimes de cyber-attaques revendiquées par un groupe religieux. Néanmoins, les services de renseignements américains et les experts en sécurité pensent que c'est l'Iran qui était à l'origine de ces attaques, qui ont conduit à l'indisponibilité des services en ligne des deux entreprises pendant plusieurs heures.

Pendant une période de six semaines début 2013, quinze des plus grandes banques américaines ont été victimes d'une interruption de leurs services en ligne pendant un total de 249 heures à la suite de cyber-attaques.

TOUTE ENTREPRISE PEUT UN JOUR OU L'AUTRE ÊTRE VISÉE.

Les petites et moyennes entreprises doivent être conscientes qu'elles sont elles aussi en danger. Les PME ont tendance à ignorer les menaces potentielles de cyber-espionnage et de cyber-terrorisme et à penser que seuls les États et les grandes multinationales sont exposés. Ce faux sentiment de sécurité peut les amener à adopter un comportement laxiste en matière de protection des systèmes et des données, facilitant ainsi le travail des cyber-espions.

En outre, les cyber-criminels considèrent souvent les PME comme un moyen d'atteindre de plus grandes entreprises. De nombreuses petites sociétés figurent parmi les partenaires de confiance de grandes entreprises, une relation que les criminels ont de plus en plus tendance à exploiter.

VOTRE ENTREPRISE PEUT-ELLE SERVIR DE PASSERELLE À DES ATTAQUES VISANT D'AUTRES ORGANISATIONS ?

Agences gouvernementales, ministères de la Défense, propriétaires d'infrastructures stratégiques (producteurs d'énergie, fournisseurs de gaz, réseaux de distribution d'énergie, fournisseurs d'eau, etc.) et grandes entreprises de pratiquement tous les secteurs de marché : tous sont conscients qu'ils peuvent être des cibles de choix. Ces organisations ont probablement toutes investi dans des mesures de cyber-sécurité efficaces.

Un grand nombre d'entreprises travaillant avec ces organisations, que ce soit en tant que fournisseurs ou sous-traitants, ne sont en revanche peut-être pas suffisamment conscientes des menaces qui pèsent sur elles ni des mesures à prendre pour se prémunir contre les cyber-attaques. Cette situation permet évidemment aux cyber-criminels d'accéder à leur cible première en exploitant les failles de sécurité des systèmes de fournisseurs ou de sous-traitants de plus petite taille.

Toutes les entreprises, y compris :

- les prestataires de services
- les fournisseurs de matériel
- les entreprises de services externalisés
- les petits cabinets de conseil
- les intervenants externes/employés intérimaires

peuvent servir de passerelle à une attaque contre une multinationale ou un organisme public.

« Depuis peu, les auteurs d'attaques ont de plus en plus de mal à pénétrer dans les réseaux de grandes entreprises. C'est pourquoi ils préfèrent se concentrer sur la chaîne d'approvisionnement. En pénétrant dans les réseaux de PME, les pirates exploitent les connaissances et les identités de petites sociétés pour s'introduire dans des entreprises de plus grande taille. »

COSTIN RAIU
DIRECTEUR, ÉQUIPE GLOBAL RESEARCH & ANALYSIS
KASPERSKY LAB

DES ATTAQUES CONTRE DES FOURNISSEURS AIDENT À LANCER UNE ATTAQUE CIBLÉE CONTRE UN GRAND FABRICANT AMÉRICAIN.

En 2011, une entreprise américaine du secteur de la défense, Lockheed Martin, a fait l'objet d'une cyber-attaque notoire.

L'auteur de cette attaque s'en était d'abord pris à deux fournisseurs de Lockheed Martin, dont RSA, une société de sécurité. On pense que les informations recueillies auprès de ces entreprises ont facilité l'attaque contre Lockheed Martin.

Lockheed Martin a rapidement détecté la menace et protégé ses systèmes et données. Toutefois, cet exemple montre comment des entreprises tierces peuvent servir de passerelle pour compromettre la sécurité de plus grandes entreprises.

PERTE RÉPUTATIONNELLE

Bien entendu, si votre entreprise sert simplement de vecteur d'attaque contre une autre organisation, vous ne subirez peut-être pas de dommages directs. Mais les dommages indirects potentiels sont considérables. Il est utile de prendre en considération les conséquences dont pourrait souffrir votre entreprise si sa vulnérabilité était exploitée dans le cadre d'une attaque de cyber-espionnage contre un de vos clients ou partenaires :

- Dans quelle mesure votre relation avec votre client/partenaire en serait-elle affectée ?
- Votre entreprise risquerait-elle d'être exposée à des conséquences juridiques ?
- À quel point une mauvaise publicité nuirait-elle à votre réputation sur le marché ?
- Pourriez-vous prouver que vous avez pris toutes les précautions possibles pour prévenir cette attaque ?

Il est évidemment recommandé de faire tout ce qui est en possible pour éviter d'avoir à gérer une situation embarrassante et la perte de réputation que pourrait provoquer une attaque indirecte.

« Pour se forger une réputation solide, une entreprise doit faire preuve de persévérance et de cohérence sur une période prolongée. Une réputation forgée au prix de maintes années d'efforts peut s'effondrer du jour au lendemain. »

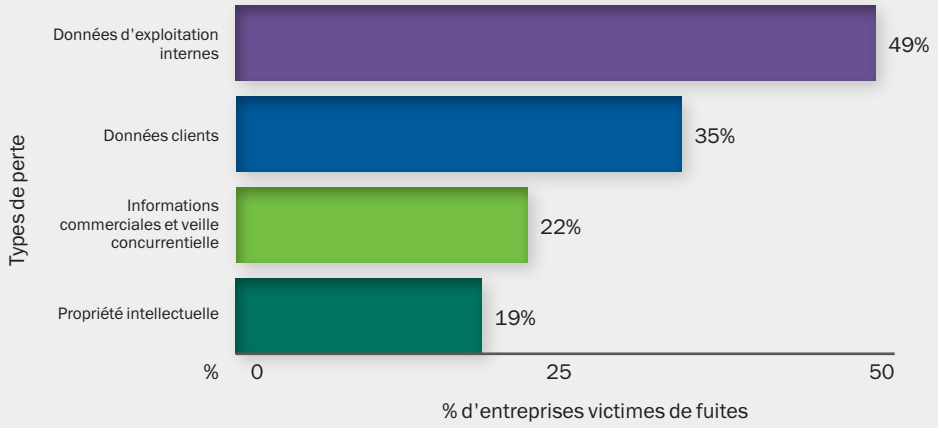
DAVID EMM
CHERCHEUR SENIOR
ÉQUIPE GLOBAL RESEARCH & ANALYSIS
KASPERSKY LAB

PERTE DIRECTE D'INFORMATIONS PRÉCIEUSES

Il est également utile d'évaluer le type d'informations qui pourraient être exposées à des risques si votre entreprise devenait la cible principale d'une attaque de cyber-espionnage. Dans quelle mesure votre entreprise serait-elle affectée si les données suivantes étaient dérobées :

- Informations commerciales, y compris informations « internes » sur vos points forts, vos points faibles et votre compétitivité
- Designs de produits, détails sur des processus innovants, savoir-faire et autres ressources de propriété intellectuelle
- Informations personnelles sur vos employés
- Bases de données et informations confidentielles sur vos clients
- Informations (sensibles ou non) sur vos partenaires

Une récente étude a révélé que les entreprises ayant été victimes de fuites de données avaient subi les pertes suivantes :



Source : enquête 2013 sur les risques liés à la sécurité informatique pour les entreprises mondiales, B2B International

MÉTHODES DE PROPAGATION DES PROGRAMMES MALVEILLANTS DE CYBER-ESPIONNAGE

Pour propager des programmes de cyber-espionnage, les cyber-criminels ont recours à plusieurs méthodes identiques à celles qu'ils utilisent pour diffuser d'autres formes de programmes malveillants :

- Exploitation des vulnérabilités de systèmes d'exploitation ou d'applications, notamment des produits logiciels les plus courants tels que :
    - o Java
    - o Adobe Reader
    - o Microsoft Office
    - o Internet Explorer
    - o Adobe Flash… entre autres
- Techniques de piratage informatique, comme les attaques de phishing ciblé
- Téléchargements intempestifs par le biais desquels la simple consultation d'un site Web infecté peut contaminer la machine d'un utilisateur

L'EFFET BOOMERANG

Dès lors qu'un nouveau programme de cyber-espionnage a été détecté et identifié, on aurait tendance à croire que la sécurité est rétablie. Malheureusement, ce n'est pas le cas ! Les risques peuvent augmenter, et les effets négatifs de l'attaque peuvent même se retourner contre les auteurs de la menace.

Des cyber-criminels copient parfois les méthodes d'attaque et lancent de nouvelles attaques contre l'auteur d'origine.

« Notre compréhension des cyber-attaques a évolué ces dernières années. Des attaques qui semblaient constituer des incidents isolés, Stuxnet et Duqu par exemple, ne représentaient en fait que la surface émergée de l'iceberg. En réalité, il existe des centaines, voire des milliers d'attaques simultanées à un instant T… même si quelques-unes seulement sont identifiées. »

COSTIN RAIU
DIRECTEUR, ÉQUIPE GLOBAL RESEARCH & ANALYSIS
KASPERSKY LAB

AU-DELÀ DU CYBER-ESPIONNAGE… LES CYBER-GUERRES ET LES RISQUES DE DOMMAGES COLLATÉRAUX

Les actes de cyber-guerre (qui consistent pour un État à lancer des cyber-attaques contre un autre pays) se multiplient et peuvent également avoir des conséquences pour les entreprises.

Dans les guerres traditionnelles, le terme « dommages collatéraux » est un euphémisme utilisé pour désigner les infrastructures et les civils non ciblés victimes d'opérations militaires. Dans le monde de la cyber-guerre, des entreprises et des individus innocents peuvent constituer des dommages collatéraux victimes d'une attaque contre une autre cible.

Une fois qu'une attaque de cyber-guerre contre un État a été lancée sur Internet, elle peut avoir de nombreuses conséquences incontrôlables ou indésirables qui s'étendent bien au-delà de la cible initialement visée. Les États, les forces militaires, votre entreprise utilisent tous Internet. Une attaque de cyber-guerre peut toucher des entreprises innocentes et infecter leurs réseaux informatiques.
En matière de dommages collatéraux, tout système connecté à Internet est vulnérable. C'est aussi simple que cela.

En outre, en cas d'attaque contre l'infrastructure stratégique d'un État, même si vos systèmes d'entreprise ne sont pas directement affectés, vous pouvez tout de même subir les conséquences suivantes :

- Perte d'accès aux services et au stockage de données sur le cloud
- Impossibilité d'effectuer des transactions financières en ligne (notamment de payer des fournisseurs et des employés ou de permettre à des clients de passer des commandes)
- Problèmes de chaîne d'approvisionnement, y compris retards d'expédition et de traitement des importations/exportations
- Mise hors service de systèmes de télécommunications, y compris communications via des lignes VoIP ou LAN
- Mise hors service d'autres éléments d'une infrastructure stratégique d'un pays, notamment production/distribution d'énergie
- Perte de données nécessaires aux activités de mise en conformité

COMMENT DÉFENDRE VOTRE ENTREPRISE CONTRE LE CYBER-ESPIONNAGE ?

Bien que certaines attaques aient l'air de sortir tout droit d'un roman de science-fiction, celles-ci sont bien réelles. Elles font partie du monde d'aujourd'hui, et vous devez vous en protéger.

« Les cyber-criminels sont curieux des nouvelles techniques qui peuvent rendre leurs attaques plus efficaces. Ils déploient des efforts considérables pour procéder à la rétroconception d'attaques les plus sophistiquées, y compris celles développées par les États.

Une fois le « génie sorti de la bouteille » et de nouveaux programmes malveillants « lâchés dans la nature », votre seul espoir, c'est que votre fournisseur de solutions de sécurité soit au sommet de son art. »

SERGEY LOZHKIN
CHERCHEUR EN SÉCURITÉ
ÉQUIPE GLOBAL RESEARCH & ANALYSIS
KASPERSKY LAB

ÉVALUEZ LES RISQUES… ET METTEZ EN PLACE UNE POLITIQUE DE SÉCURITÉ

Il est important que toutes les entreprises évaluent les risques qui pourraient les affecter et établissent leur propre politique de sécurité.

De nombreuses entreprises font l'erreur de baser leur stratégie de sécurité sur une perception obsolète des risques qui existaient il y a une dizaine d'années. Veillez à ce que votre politique soit adaptée aux risques d'aujourd'hui et repose sur une solide compréhension du panorama de menaces actuel. Votre politique doit :

- Définir des procédures de sécurité quotidiennes
- Établir un plan de réponse aux attaques
- Inclure un mécanisme de mise à jour des procédures pour que ces dernières suivent l'évolution des menaces
- Faire un audit régulier de vos infrastructure de sécurité informatique

PRÉVOIR LA FORMATION DE VOTRE PERSONNEL À LA GESTION DES RISQUES

Il s'agit d'un préalable indispensable. De nombreuses attaques de cyber-espionnage et autres attaques cyber-criminelles misent sur l'erreur humaine ou la naïveté des utilisateurs pour créer les conditions permettant à leurs auteurs d'accéder aux systèmes et aux données des entreprises. En matière de protection contre les attaques, « un homme averti en vaut deux ». Veillez donc à sensibiliser vos collègues sur :

- Les risques de sécurité et les méthodes utilisées par les cyber-criminels pour tenter de dérober des informations et des mots de passe
- Les coûts potentiels pour l'entreprise si elle est attaquée
- Les précautions simples que les employés peuvent prendre pour améliorer la sécurité
- La politique de sécurité de votre entreprise et ce que les employés doivent faire pour satisfaire à ses exigences

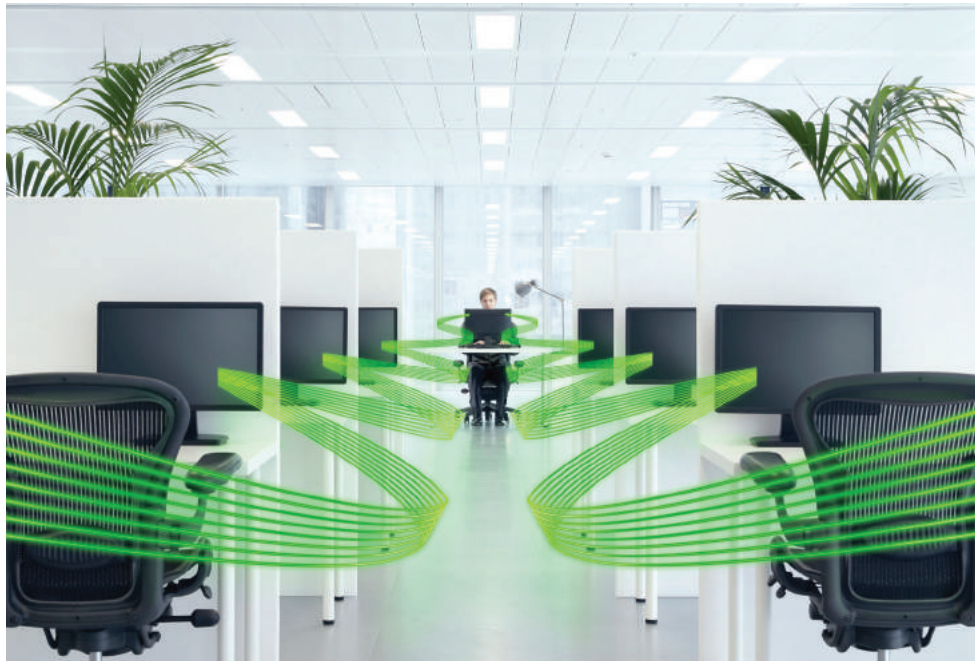
RÉFLÉCHISSEZ À VOTRE STRATÉGIE EN MATIÈRE DE SYSTÈME D'EXPLOITATION.

Gardez à l'esprit que les systèmes d'exploitation récents tels que Windows 7, Windows 8 ou Mac OS X sont généralement plus sûrs que leurs prédécesseurs. C'est donc un élément à prendre en compte au moment de concevoir votre stratégie de mise à niveau informatique.

De même, les versions 64 bits de la plupart des systèmes d'exploitation sont en principe plus résistantes aux cyber-attaques.

« Nous avons récemment assisté à l'apparition d'une nouvelle tendance : l'émergence des programmes malveillants destructeurs. Shamoon, qui a été utilisé pour attaquer Saudi Aramco et Rasgas en 2012, en est un exemple. Les programmes malveillants destructeurs cherchent à endommager le réseau des victimes pour interrompre temporairement leurs activités ou causer des dégâts irréparables. Cette approche est totalement différente de celle qui sous-tend les attaques motivées par l'appât du gain (les chevaux de Troie visant le secteur bancaire, par exemple), et elles sont peut-être encore plus dangereuses. »

SERGEY LOZHKIN
CHERCHEUR EN SÉCURITÉ
ÉQUIPE GLOBAL RESEARCH & ANALYSIS
KASPERSKY LAB



DÉPLOYEZ UNE SOLUTION DE SÉCURITÉ INFORMATIQUE COMPLÈTE

Le recours à une protection contre les programmes malveillants est primordial, mais il ne suffit pas. Choisissez une solution de sécurité qui intègre également les technologies de sécurité suivantes :

- Évaluation des vulnérabilités
- Gestion des correctifs
- Contrôle des applications, qui incorpore également des fonctionnalités de liste blanche et de blocage par défaut
- Contrôle des périphériques, qui vous aide à gérer les périphériques autorisés à être connectés à vos systèmes/votre réseau
- Contrôle du Web, qui facilite la gestion, la restriction et l'audit de l'accès aux ressources Web
- Défenses zero-day
- Chiffrement des données
- Sécurité mobile et gestion des appareils mobiles (MDM)

L'IMPORTANCE DE LA SÉCURITÉ MOBILE

Les smartphones actuels sont bien plus que des téléphones. Ce sont des ordinateurs puissants qui peuvent stocker de nombreuses informations (et mots de passe) pouvant avoir une valeur particulièrement élevée pour les cyber-espions. Il est donc important de protéger les appareils mobiles, tablettes et smartphones compris, de manière aussi rigoureuse que vous protégez vos systèmes informatiques.

Face à l'augmentation du risque de vol ou de perte, on comprend bien que les appareils mobiles nécessitent effectivement des niveaux de protection plus élevés pour protéger les données présentes sur les appareils perdus ou volés.

Si votre entreprise a mis en place une stratégie BYOD, cela peut constituer une source de préoccupation supplémentaire en matière de sécurité mobile. La diversité des plates-formes et modèles à protéger est un élément à prendre en compte dans votre politique de sécurité.

Même si vous n'avez pas adopté de politique BYOD officielle, vous devez être conscient que vos employés sont susceptibles d'apporter leur smartphone personnel sur leur lieu de travail.

CONTRÔLE DES APPLICATIONS AVEC BLOCAGE PAR DÉFAUT

Le blocage par défaut est une méthode simple permettant de gérer les applications autorisées à être exécutées sur vos systèmes.

Seuls les logiciels figurant sur votre liste blanche d'applications sécurisées pourront être lancés et tous les autres logiciels seront automatiquement bloqués.

SÉCURISEZ VOS ENVIRONNEMENTS VIRTUELS.

Certaines entreprises sont convaincues que les environnements informatiques virtualisés sont bien plus sûrs, ce qui est faux. Les machines virtuelles étant exécutées sur des serveurs physiques, ces derniers restent exposés aux attaques malveillantes.

Autrement dit, les machines virtuelles doivent être protégées. Toutefois, dans un souci d'amélioration de votre retour sur investissement, il peut être utile de privilégier des solutions de sécurité qui intègrent des dispositions spéciales pour les environnements virtuels. Par exemple, en choisissant une solution de sécurité sans agent plutôt qu'une solution de sécurité classique basée sur des agents, vous devriez pouvoir renforcer les ratios de consolidation de vos serveurs.

COMBINEZ SÉCURITÉ ET GESTION DE SYSTÈMES POUR PLUS DE VISIBILITÉ ET DE SIMPLICITÉ.

Privilégiez une solution qui associe sécurité et diverses fonctions de gestion des systèmes informatiques. Vous gagnerez ainsi en visibilité sur votre réseau, ce qui vous permettra d'appliquer plus facilement les mesures de sécurité appropriées.

« L'objectif de la virtualisation est d'optimiser votre infrastructure informatique. Si vous utilisez des logiciels traditionnels de protection contre les programmes malveillants sur vos serveurs virtualisés, vous risquez de perdre une grande partie de la puissance de traitement et de capacité de stockage de votre serveur, ce qui pourrait aller à l'encontre de votre programme de virtualisation et réduire considérablement votre retour sur investissement. »

DAVID EMM
CHERCHEUR SENIOR
ÉQUIPE GLOBAL RESEARCH & ANALYSIS
KASPERSKY LAB

COMMENT LES TECHNOLOGIES DE SÉCURITÉ DE KASPERSKY LAB PEUVENT VOUS AIDER À PROTÉGER VOTRE ENTREPRISE

Les cyber-criminels utilisant des méthodes de plus en plus sophistiquées pour lancer des cyber-attaques, il est fondamental que les entreprises choisissent une solution de sécurité capable de faire face aux menaces les plus récentes.

DES TECHNOLOGIES INNOVANTES QUI VOUS OFFRENT UNE PROTECTION MULTI-NIVEAUX

Outre ses fonctions de protection contre les programmes malveillants maintes fois primées, Kaspersky Lab continue de développer des technologies innovantes qui offrent de nouveaux niveaux de protection aux entreprises :

Analyse automatique des vulnérabilités et gestion des correctifs

Un grand nombre des solutions de sécurité de Kaspersky Lab sont capables d'analyser automatiquement votre réseau d'entreprise pour détecter la présence de vulnérabilités non corrigées dans vos systèmes d'exploitation ou applications.

Dotées de la base de données Microsoft WSUS, de la base de données Secunia et de sa propre base de données de vulnérabilités (fournie par le réseau Kaspersky Security Network dans le cloud), les solutions Kaspersky Lab synchronisent régulièrement les mises à jour et correctifs Microsoft, avant de les distribuer automatiquement sur votre réseau. En outre, pour les applications autres que Microsoft, des informations sur les correctifs peuvent être téléchargées directement des serveurs Kaspersky Lab.

Prévention automatique des failles d'exploitation (AEP)

La technologie de prévention automatique des failles d'exploitation de Kaspersky Lab vous protège contre les infections de programmes malveillants pouvant être provoquées par des vulnérabilités non corrigées présentes dans les systèmes d'exploitation ou les applications utilisées sur vos ordinateurs.

Kaspersky Security Network

Des millions de membres de la communauté mondiale Kaspersky Lab se sont portés volontaires pour transmettre à Kaspersky Security Network (KSN) des informations sur les activités suspectes et les tentatives d'infection par des programmes malveillants présents sur leurs ordinateurs. Même si vous décidez de ne pas fournir de données au KSN, votre entreprise bénéficiera de ce flux de données relatives aux menaces recueillies en temps réel sur le terrain.

Le réseau KSN vous aide à apporter une réponse bien plus rapide aux nouvelles menaces. En outre, il vous permet de réduire l'incidence des faux positifs et d'aider ainsi votre entreprise à optimiser sa productivité.

Contrôle des applications

Les capacités de contrôle des applications de Kaspersky Lab vous aident à gérer le mode d'exécution de vos applications sur votre réseau d'entreprise. Vous pouvez facilement configurer une politique d'autorisation par défaut (qui bloque le lancement d'applications figurant sur votre liste noire tout en autorisant les autres logiciels à se lancer) ou appliquer une politique de blocage par défaut qui permet aux seules applications figurant sur votre liste blanche de se lancer.

Whitelisting Lab

Kaspersky Lab est le seul fournisseur de solutions de sécurité ayant investi dans la création d'un laboratoire dédié à la gestion des listes blanches (Whitelisting Lab). Ce laboratoire est chargé d'évaluer la sécurité des applications les plus courantes et propose en permanence des mises à jour de la base de données d'applications sûres figurant sur la liste blanche de Kaspersky Lab.

Les mises à jour de la liste blanche sont fournies par le réseau Kaspersky Security Network sur le cloud pour permettre aux clients de Kaspersky Lab de bénéficier des données les plus récentes.

ZetaShield

La technologie ZetaShield (Zero-Day Exploit and Targeted Attack Shield) de Kaspersky Lab offre une protection contre les programmes malveillants et les failles d'exploitation inconnus pour vous protéger contre les attaques zero-day et zero-hour, et contre les menaces persistantes avancées. La combinaison du puissant moteur antivirus de Kaspersky et de la technologie ZetaShield améliore considérablement le taux de détection des programmes malveillants pour un niveau de protection encore supérieur.

Sécurité mobile et gestion des appareils mobiles

Les technologies de sécurité mobile de Kaspersky Lab offrent une protection multi-niveaux pour les appareils mobiles et intègrent des fonctions spéciales de protection des données présentes sur les appareils perdus ou volés. En outre, Kaspersky Lab offre une vaste gamme de fonctionnalités de gestion des appareils mobiles (MDM) qui aident les entreprises à réduire le temps consacré à la gestion des terminaux mobiles.

Sécurité des environnements virtualisés

Kaspersky Lab propose une protection spécialement développée pour répondre aux exigences uniques des environnements informatiques virtualisés, notamment les serveurs, postes de travail et centres de données virtualisés.

En fournissant une solution de protection sans agent contre les programmes malveillants, Kaspersky Lab offre une méthode de protection plus efficace des infrastructures virtualisées afin de préserver les performances, de limiter l'impact sur la densité de virtualisation et d'augmenter le retour sur investissement global.

Des capacités de gestion des systèmes de premier ordre

En automatisant de nombreuses tâches d'administration récurrentes, Kaspersky Systems Management offre aux entreprises une visibilité et un contrôle accrus de leurs ressources informatiques tout en soulageant les administrateurs informatiques qui peuvent se consacrer à d'autres tâches.

UNE AUTORITÉ MONDIALE EN MATIÈRE DE CYBER-SÉCURITÉ

En sa qualité d'entreprise privée, Kaspersky Lab est entièrement indépendante. Bien qu'elle conseille de nombreuses agences gouvernementales, elle n'entretient de lien politique avec aucun gouvernement. Les experts de Kaspersky Lab travaillent en étroite collaboration avec la communauté mondiale de la sécurité informatique, notamment avec les organismes Computer Emergency Response Teams (CERT) du monde entier, et réalise des enquêtes conjointes portant sur les menaces de cyber-espionnage, de cyber-sabotage et de cyber-guerre.

Faites appel à l'équipe GReAT

L'équipe Global Research & Analysis (GReAT) est l'un des atouts technologiques majeurs de Kaspersky Lab. Grâce à ses chercheurs de premier plan disséminés aux quatre coins du monde, l'équipe GReAT analyse en permanence de nouvelles cyber-menaces et développe des solutions de protection.

« Créée en 2008, l'équipe Global Research & Analysis (GReAT) de Kaspersky Lab apporte son leadership en matière de recherche et d'innovation sur la protection contre les programmes malveillants et sur le cyber-espionnage, en interne comme en externe. Basés aux quatre coins du globe, les analystes de sécurité de l'équipe apportent chacun un ensemble unique de compétences et d'expertise à la recherche et à la conception de solutions visant à lutter contre des codes malveillants de plus en plus complexes.

L'équipe GReAT intervient en cas d'incidents liés à des programmes malveillants. Elle a pour principales responsabilités d'assurer un leadership éclairé en matière de renseignement sur les menaces, d'encourager et d'exécuter des initiatives relatives à l'amélioration de l'efficacité et de détection des programmes malveillants, mais aussi d'apporter une assistance avant-ventes et après-ventes aux grands comptes concernant les programmes malveillants.

Ces dernières années, l'alliance d'expertise, de passion et de curiosité de l'équipe GReAT a conduit à la découverte de plusieurs attaques de cyberespionnage, notamment Flame, Gauss, Red October, NetTraveler et Icefog. »

COSTIN RAIU
DIRECTOR, ÉQUIPE GLOBAL RESEARCH & ANALYSIS
KASPERSKY LAB

« Avec l'émergence des menaces persistantes avancées, le panorama mondial des cyber-menaces s'est transformé, mettant en péril les infrastructures stratégiques, le secteur des finances et des télécommunications, les instituts de recherche, les entrepreneurs militaires et les infrastructures réseau des gouvernements.

Ces menaces étant bien plus complexes et discrètes que les programmes malveillants classiques, nous continuons d'investir dans l'équipe GReAT, groupe d'élite d'experts en cyber-sécurité. »

EUGENE KASPERSKY
PDG KASPERSKY LAB

COSTIN RAIU
DIRECTEUR, ÉQUIPE GLOBAL RESEARCH & ANALYSIS
KASPERSKY LAB

Costin Raiu a rejoint Kaspersky Lab en 2000 et dirige l'équipe GReAT depuis 2010. Il s'est spécialisé dans l'analyse des menaces persistantes avancées et dans les attaques malveillantes de haut niveau. M. Raiu travaille notamment sur l'analyse des sites Web malveillants, les failles d'exploitation et les programmes malveillants ciblant les banques en ligne.

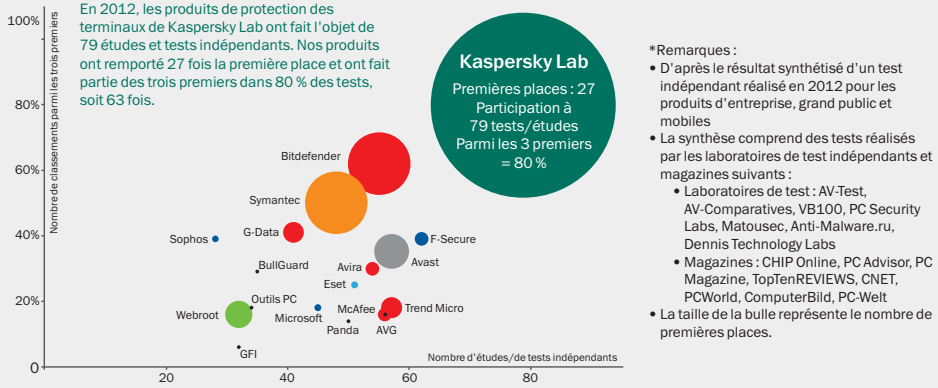
Fort de plus de 19 ans d'expérience en matière de technologies antivirus et de recherche sur la sécurité, Costin Raiu est membre du comité consultatif technique de Virus Bulletin, membre de la Computer Antivirus Researchers' Organization (CARO) et reporter pour WildList Organization International. Avant de rejoindre Kaspersky Lab, Costin a travaillé pour GeCad en tant que Chief Researcher et Data Security Expert avec le groupe de développeurs de l'antivirus RAV.

LES RÉCOMPENSES ET RÉUSSITES INDÉPENDANTES

Kaspersky Lab est naturellement fier du nombre de récompenses et distinctions remportées par ses technologies :

- « Fournisseur de solutions de sécurité des informations de l'année » – SC Magazine Awards Europe 2013
- « Équipé dédiée à la sécurité des informations de l'année » – SC Magazine Awards Europe 2013
- Lauréat du Prix d'excellence – SC Magazine Awards 2013
- Kaspersky Endpoint Security for Windows a reçu le premier prix dans le cadre du test de protection antivirus pour les entreprises d'avril à juin 2013 réalisé par Dennis Technology Labs
- Le plus grand nombre de récompenses Or et Platine décernées par le projet indépendant Anti-Malware Test Lab (toutes catégories de tests confondues) depuis 2004
- Plus de 50 tests rigoureux VB100 réussis depuis 2000
- Prix Checkmark Platinum Product décerné par West Coast Labs
- Produit de l'année – AV Comparatives 2011

KASPERSKY LAB FOURNIT LA MEILLEURE PROTECTION DU SECTEUR* :



*Remarques :
- D'après le résultat synthétisé d'un test indépendant réalisé en 2012 pour les produits d'entreprise, grand public et mobiles
- La synthèse comprend des tests réalisés par les laboratoires de test indépendants et magazines suivants :
  - Laboratoires de test : AV-Test, AV-Comparatives, VB100, PC Security Labs, Matousec, Anti-Malware.ru, Dennis Technology Labs
  - Magazines : CHIP Online, PC Advisor, PC Magazine, TopTenREVIEWS, CNET, PCWorld, ComputerBild, PC-Welt
- La taille de la bulle représente le nombre de premières places.

« En 2012, les produits Kaspersky Lab ont fait l'objet de 79 tests et études indépendants. Nos produits ont reçu 27 premiers prix et ont figuré 63 fois parmi les trois premiers. »

APPENDIX 1

APERÇU DE QUELQUES CYBER-MENACES IMPORTANTES

LES MENACES DE CYBER-ESPIONNAGE

Icefog

Cette menace persistante avancée lancée en 2011 a ciblé des entreprises industrielles ainsi que des institutions gouvernementales et des entrepreneurs militaires. La plupart de ses cibles se trouvent au Japon ou en Corée du Sud, mais ses attaques provoquent des problèmes de chaîne d'approvisionnement pour les entreprises mondiales. Les auteurs de ces attaques semblent viser les opérateurs de télécommunications, les exploitants de satellites, les médias et les services de télévision, ainsi que les opérations militaires, les activités de construction navale/maritimes, le développement d'ordinateurs et de logiciels et les entreprises de recherche.

En général, les e-mails de phishing ciblé servent à propager des programmes malveillants qui exploitent les vulnérabilités d'applications courantes telles que Java et Microsoft Office. Bien que ces vulnérabilités soient connues et que des correctifs soient facilement accessibles, les cyber-criminels profitent du fait que de nombreuses victimes mettent du temps à distribuer les correctifs dans l'ensemble de leur infrastructure informatique. On pense que leurs auteurs sont des cyber-mercenaires payés pour lancer ces attaques.

Kimsuky

Un groupe de pirates nord-coréens est soupçonné d'avoir lancé l'attaque de cyber-espionnage Kimsuky dans le but de voler des données relatives à la défense et à la sécurité de cibles sud-coréennes. Les chercheurs de Kaspersky Lab ont découvert cette attaque qui a recours à des techniques de phishing ciblé pour dérober des mots de passe et d'autres informations utilisateur. Ces pirates prennent également le contrôle d'ordinateurs infectés.

Red October

Détectée dès 2007, l'opération Red October continuait d'être active en 2013. Cette attaque de cyber-espionnage avancé cible les institutions diplomatiques et gouvernementales aux quatre coins du globe. Elle a également visé des institutions de recherche, des compagnies pétrolières et gazières, ainsi que d'autres organisations commerciales. Red October dérobe des données présentes sur des systèmes informatiques, des téléphones portables et des réseaux d'entreprise. Ses attaques exploitent notamment les failles de sécurité de Microsoft Office et de Microsoft Excel.

NetTraveler

Il s'agit d'une campagne de cyber-espionnage ayant fait plus de 350 victimes, parmi des notables de 40 pays. Le principal outil utilisé par les cyber-criminels dans le cadre de ces attaques est NetTraveler, un programme malveillant de surveillance informatique conçu pour dérober des données sensibles, enregistrer l'activité du clavier et récupérer des listes de système de fichiers ainsi que divers documents Office ou PDF.

NetTraveler est actif depuis 2004 et a ciblé des activistes tibétains/ouïghours, des compagnies pétrolières, des centres et des instituts de recherche scientifique, des universités, des entreprises privées, des gouvernements et des institutions gouvernementales, des ambassades et des entrepreneurs militaires.

Shamoon

Une fois un ordinateur infecté par Shamoon, ce virus peut exploiter la présence de disques durs partagés pour se propager sur d'autres ordinateurs du réseau de l'organisation ciblée. En plus d'envoyer des données à l'auteur de l'attaque, Shamoon supprime également des fichiers sur les ordinateurs des victimes.

DES DONNÉES SUPPRIMÉES SUR LES ORDINATEURS D'UN PRODUCTEUR MAJEUR DE PÉTROLE

On pense qu'une attaque de Shamoon a détruit des données sur 30 000 ordinateurs de Saudi Aramco.

Que votre entreprise dispose de 10 ou de 10 000 ordinateurs, pourrait-elle se remettre de la perte de données sur toutes ses machines ?

LES MENACES DONT ON PENSE QU'ELLES SONT COMMANDITÉES PAR DES ÉTATS, Y COMPRIS ACTES DE CYBER-GUERRE, DE CYBER-SABOTAGE ET DE CYBER-ESPIONNAGE

Stuxnet (nombre approximatif de victimes : 300 000)

Souvent considéré comme un exemple de cyber-guerre, Stuxnet a été le premier programme malveillant à cibler des systèmes de contrôle industriels. L'objectif de Stuxnet était de perturber et de saboter le fonctionnement d'une installation nucléaire en prenant le contrôle du fonctionnement de centrifugeuses pour l'enrichissement de l'uranium. À ce jour, c'est le seul programme malveillant connu ayant provoqué des dommages physiques sur des systèmes industriels.

Malgré son objectif initial, Stuxnet s'est propagé de manière instable et a entraîné l'infection de centaines de milliers de PC dans des milliers d'entreprises différentes.

Duqu (nombre approximatif de victimes : 50 à 60)

Actif depuis 2007, ce cheval de Troie sophistiqué a été conçu à partir de la même plate-forme d'attaque que Stuxnet. Une fois que Duqu a infecté un ordinateur, il télécharge des composants supplémentaires pour voler des informations sensibles. Il est également capable de détruire toute trace de ses activités.

STUXNET INFECTE LES ORDINATEURS D'UN GÉANT DU PÉTROLE.

En octobre 2012, Chevron, géant mondial de l'industrie pétrolière, a été la première entreprise basée aux États-Unis à signaler avoir été infectée par Stuxnet.

Flame (nombre approximatif de victimes : 5 000 à 6 000)

Flame intercepte les demandes de mise à jour de Microsoft Windows et les remplace par son module malveillant. Ce module intègre un faux certificat Microsoft généré par des cyber-criminels.

Actif depuis 2008, Flame est en mesure d'analyser le trafic réseau de ses victimes, de réaliser des captures d'écran de leurs ordinateurs et d'enregistrer des communications vocales et l'activité du clavier.

Gauss (nombre approximatif de victimes : 10 000)

Mis en œuvre par le même groupe que celui ayant créé la plate-forme Flame, Gauss est un programme de cyber-espionnage actif depuis 2011. Il intègre des modules qui peuvent exécuter divers actes malveillants, notamment:

- Intercepter des fichiers de cookies et des mots de passe dans le navigateur Web de la victime
- Infecter des périphériques de stockage USB pour dérober des données
- Intercepter des données d'accès aux comptes de systèmes de messagerie et de sites Web de réseaux sociaux

Gauss a été utilisé pour accéder à des systèmes bancaires au Moyen-Orient.

CYBER-GLOSSAIRE

Cyber-armes : programmes malveillants développés dans le but de nuire à des tiers. Les cyber-armes sont utilisées pour mettre à exécution des attaques de cyber-espionnage et de cyber-sabotage. Contrairement aux armes traditionnelles, les cyber-armes sont faciles à cloner et à reprogrammer.

Cyber-attaque : attaque réalisée par un pirate ou un criminel contre un ordinateur, un smartphone, une tablette ou un réseau informatique.

Cyber-crime : désigne un large éventail d'activités illégales mises en œuvre par le biais de systèmes informatiques, y compris des appareils mobiles.

Cyber-criminel : individu mettant à exécution des activités criminelles par le biais de systèmes informatiques et d'appareils mobiles. Il peut aussi bien s'agir de criminels individuels et opportunistes que de groupes professionnels hautement qualifiés composés de pirates informatiques. Les cyber-criminels peuvent se spécialiser dans les domaines suivants :

- Développement et vente de programmes malveillants à des tiers qui lancent ensuite eux-mêmes les attaques
- Récupération et vente de données (numéros de carte de crédit, etc.) à d'autres criminels. Les cyber-criminels peuvent également exécuter toutes les étapes d'une attaque, du développement de programmes malveillants jusqu'au vol d'argent à la victime.

Cyber-espace : espace ou environnement virtuel au sein duquel des réseaux informatiques du monde entier communiquent entre eux.

Cyber-espionnage : activité consistant à espionner et à accéder illégalement à des informations en utilisant des systèmes informatiques et/ou Internet.

Cyber-guerre : désigne les attaques lancées par des États contre d'autres États. En général, une cyber-guerre cherche à provoquer des dommages sur des infrastructures publiques ou en dérobant de données sensibles stockées plutôt qu'à voler de l'argent. Les cibles les plus courantes sont notamment les installations militaires et les infrastructures stratégiques, tels que les réseaux de transport, les services de contrôle du trafic aérien, les réseaux de distribution d'énergie, les télécommunications, la chaîne alimentaire, etc.

Cyber-hooligan : individu qui développe des programmes malveillants et lance des attaques pour le plaisir. Alors qu'ils prédominaient pendant les années 1980 et 1990, les cyber-hooligans ne sont plus très nombreux aujourd'hui. Aujourd'hui, les cyber-criminels et les cyber-terroristes constituent des menaces bien plus sérieuses.

Cyber-mercenaire : « pirate à gages ». À l'instar des combattants professionnels qui offrent leurs services au pays le plus offrant pendant une guerre traditionnelle, les cyber-mercenaires sont des cyber-criminels et des pirates qui vendent leurs services à des tiers, y compris des États ou d'autres organisations.

Cyber-sabotage : activités exécutées par des cyber-saboteurs pour perturber des processus ou des entreprises légitimes.

Cyber-sécurité : mesures prises pour protéger des systèmes et périphériques informatiques contre les cyber-attaques.

Cyber-terroriste : individu ou groupe pouvant être recruté par un État ou agir au sein d'une organisation terroriste indépendante pour lancer des cyber-attaques.

Hacktiviste : malgré l'absence du préfixe « cyber » dans leur nom, ces pirates activistes méritent d'être mentionnés dans notre glossaire. Les hacktivistes sont des pirates informatiques qui se sont alignés sur une organisation de protestation ou un groupe d'activistes. Leurs activités sont comparables à celles des cyber-terroristes ou des cyber-saboteurs.

À PROPOS DE KASPERSKY

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. Groupe international présent dans près de 200 pays et territoires à travers le monde, nous fournissons une protection à plus de 300 millions d'utilisateurs et plus de 200 000 entreprises clientes de toutes tailles, des petites et moyennes entreprises aux grandes organisations gouvernementales et commerciales.

Nous proposons des solutions de sécurité intégrées et avancées qui 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.

Pour en savoir plus, rendez-vous sur kaspersky.fr/business