PANORAMA DES CYBER-MENACES

Guide pratique

David Emm
Senior Regional Researcher, équipe Global Research & Analysis, Kaspersky Lab

KASPERSKY lab

À PROPOS DE L'AUTEUR

David Emm
Senior Regional Researcher
Équipe Global Research & Analysis (GReAT)

David fait partie de Kaspersky Lab depuis 2004. En sa qualité de Senior Technology Consultant, David a présenté des informations sur les programmes malveillants et d'autres menaces informatiques lors de salons et de manifestations, et s'est exprimé auprès de la presse écrite, radio et télévisée. Senior Regional Researcher de l'équipe Global Research & Analysis depuis 2008, David s'intéresse particulièrement à l'écosystème des programmes malveillants, le vol d'identité et les technologies Kaspersky Lab. Il a conçu et développé l'atelier de l'entreprise sur la protection contre les programmes malveillants (Malware Defence Workshop).

David travaille depuis 1990 dans l'industrie anti-virus, où il a occupé diverses fonctions. Avant de rejoindre Kaspersky Lab, David a travaillé comme Systems Engineer, Product Manager et Product Marketing Manager chez McAfee, après avoir occupé les postes de Technical Support Manager et Senior Technology Consultant chez Dr Solomon's Software.

SOMMAIRE

CHAPITRE 1

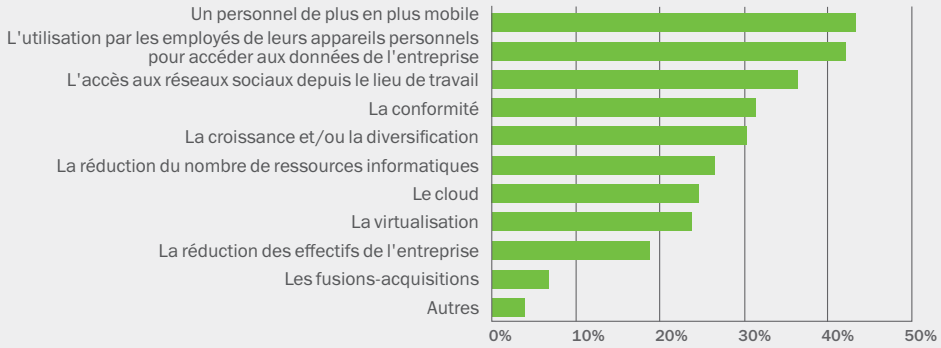
L'ÉVOLUTION DES PROGRAMMES MALVEILLANTS

CONTEXTE

Les premiers virus informatiques sont apparus il y a plus de 25 ans. Au fil du temps, la nature des menaces a profondément évolué. Les menaces que les entreprises rencontrent actuellement n'ont jamais été aussi complexes.

Selon l'enquête 2013 de Kaspersky sur les risques informatiques mondiaux, ce sont les nouvelles technologies, sources de nouvelles méthodes de travail, qui constituent la principale source de préoccupation des responsables informatiques : la mobilité, l'utilisation des appareils personnels au travail (BYOD) et les médias sociaux sur le lieu de travail arrivent en tête du classement.

Quels défis constituent le principal casse-tête de sécurité pour votre entreprise ?



Ce résultat est révélateur du bouleversement qui affecte l'environnement technologique. Voici les principales tendances ayant des répercussions sur les entreprises au niveau de la sécurité :

- **Mobilité/BYOD :** la généralisation de la mobilité et la consumérisation croissante de l'environnement professionnel a créé une communauté d'utilisateurs finaux mobile.
- **Cloud :** le cloud, qui permet d'accéder aux données de l'entreprise avec des appareils de plus en plus divers, représente une pression supplémentaire en termes de sécurité informatique.
- **Virtualisation :** l'utilisation croissante d'environnements virtualisés visant à réduire les coûts et à renforcer la flexibilité crée des domaines spécifiques complexes en termes de sécurité informatique.
- **Médias sociaux :** l'utilisation des réseaux sociaux par les employés constitue rarement un problème en soi, mais les cyber-criminels exploitent de plus en plus le comportement « ouvert » des utilisateurs sur ces sites pour accéder à des données sensibles.

DES ATTAQUES À L'ENVERGURE ET À LA GRAVITÉ CROISSANTES

La connectivité apportée par Internet permet aux auteurs de programmes malveillants et aux organisations criminelles qui les commanditent de lancer des attaques sur les ordinateurs des victimes de manière aussi large ou ciblée qu'ils le souhaitent.

Des codes malveillants peuvent être intégrés aux e-mails, introduits dans de faux packs logiciels ou placés dans la zone grise de pages Web pour qu'un cheval de Troie installé sur un ordinateur infecté les télécharge.

L'ampleur du problème, rien qu'en termes de chiffres, est aussi croissante.
Le nombre d'échantillons de programmes malveillants uniques analysé au quotidien atteint plusieurs centaines de milliers.

19 % des personnes interrogées ont placé les cyber-menaces en tête des risques actuels pour les entreprises

DU CYBER-VANDALISME À LA CYBER-CRIMINALITÉ

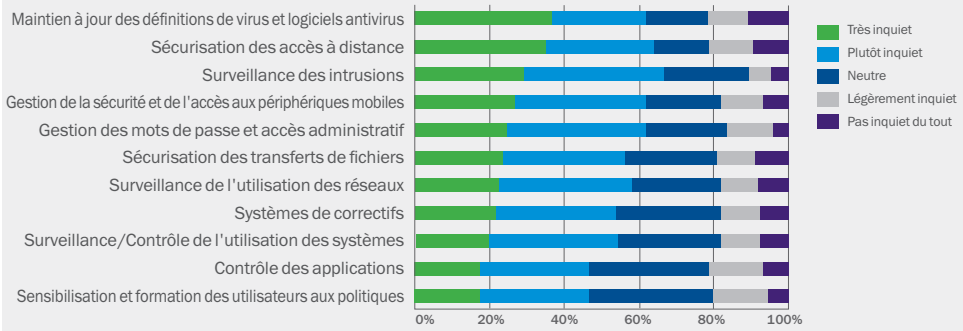
Jusqu'aux alentours de 2003, les virus et autres types de programmes malveillants représentaient surtout des actes isolés de vandalisme informatique, un moyen d'exprimer des idées anti-sociales à l'aide de la technologie. La plupart des virus se contentaient d'infecter d'autres disques ou programmes.

Le panorama des menaces a changé après 2003. La plupart des programmes malveillants actuels sont spécialement conçus pour détourner des ordinateurs et gagner de l'argent illégalement.

Aussi, les menaces qui pèsent sur les entreprises sont devenues bien plus complexes. Les administrateurs informatiques sont confrontés à beaucoup plus de problèmes : les types de menaces contre lesquelles ils doivent protéger l'entreprise sont bien plus nombreux et provoquent des préjudices qui ne se limitent plus à un simple temps d'arrêt informatique, mais sont souvent financiers.

Tout cela explique pourquoi l'ampleur et la complexité des préoccupations en matière de sécurité informatique qui ressortent de notre enquête 2013 sur les risques informatiques mondiaux atteignent un tel niveau et pourquoi les administrateurs n'ont plus un seul gros problème, mais plusieurs problèmes divers à gérer.

Dans quelle mesure les problèmes de sécurité informatique suivants au sein de votre entreprise vous inquiètent-ils ?



NOUVEAUX MOTIFS, NOUVELLES TACTIQUES

Le changement de motif a également entraîné un changement de tactique. On a observé une baisse du nombre d'épidémies mondiales, conçues pour propager les programmes malveillants le plus rapidement et le plus largement possible. Les attaques sont devenues plus ciblées.

La principale cause de ce changement est que les attaques ont désormais une fin criminelle et visent à dérober des données confidentielles, qui doivent ensuite être traitées et utilisées. Lorsque des millions de machines sont affectées, il est plus facile de détecter le programme malveillant, ce qui entraîne une vaste opération logistique. C'est pourquoi les auteurs de code malveillant préfèrent désormais cibler leurs attaques.

L'EXPLOSION DES CHEVAUX DE TROIE

Les chevaux de Troie sont utilisés pour récupérer des informations confidentielles (nom d'utilisateur, mot de passe, code PIN, etc.) à des fins de fraude informatique. Ils peuvent être utilisés dans les attaques DDoS (Distributed Denial of Service, déni de service distribué) contre des entreprises. Ces attaques peuvent permettre d'extorquer de l'argent aux entreprises : la « démonstration » d'une attaque DDoS donne à la victime un avant-goût de ce qui se passera si elle ne paie pas.

On observe également une croissance continue du nombre de chevaux de Troie de type « ransomware », utilisés pour extorquer de l'argent à des utilisateurs individuels. Ces programmes cryptent les données des victimes et affichent un message (sous forme d'un fichier « readme » ou d'une fenêtre contextuelle) demandant à la victime de transférer de l'argent à l'auteur du programme en utilisant l'un des nombreux services de paiement en ligne disponibles.

En général, les ordinateurs infectés constituent des réseaux. Les activités de ces réseaux de bots, ou botnets, sont contrôlées à l'aide de sites Web ou de comptes Twitter. Si le botnet dispose d'un seul serveur de contrôle et de commande (C2), il est possible de le mettre hors service une fois son emplacement 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. Le cheval de Troie « Storm Worm », découvert début 2007, a été le premier à employer cette méthode et a été intégré à de nombreux botnets depuis (notamment Conficker, Kelihos et Red October).

Il y a encore quelques années, la plupart des épidémies avaient recours à des vers informatiques qui détournaient le système de messagerie pour se propager de manière proactive, récupérant ainsi des contacts supplémentaires des machines infectées au fur et à mesure de leur propagation.

Aujourd'hui, un nombre croissant de programmes malveillants sont délibérément envoyés sur les machines des victimes sous forme de spams, ce qui permet à leur(s) auteur(s) de contrôler la diffusion de leur code sur une population de PC cible, plutôt que de le laisser se propager à son gré.

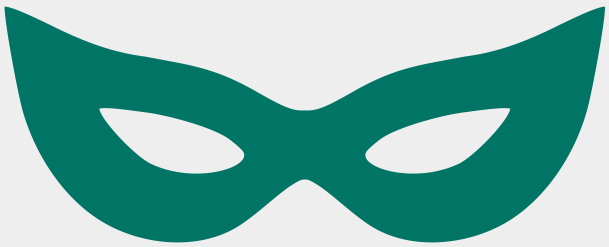
LE PHISHING – SE FAIRE PASSER POUR QUELQU'UN D'AUTRE

L'utilisation de code malveillant n'est pas la seule méthode à laquelle les cyber-criminels ont recours pour recueillir des données personnelles qu'ils peuvent utiliser pour gagner de l'argent illégalement. Le phishing consiste à piéger des individus pour les amener à divulguer des informations personnelles (nom d'utilisateur, mot de passe, code PIN ou autres informations d'accès), puis à utiliser ces données pour obtenir de l'argent sous un faux prétexte.

Les spécialistes du phishing créent par exemple une réplique presque parfaite du site Web d'un établissement financier. Ils envoient ensuite massivement un e-mail qui imite une correspondance authentique de l'établissement financier réel.

Les spécialistes du phishing utilisent généralement de vrais logos, un style commercial convaincant et citent parfois les dirigeants de l'établissement financier par leur nom. Ils imitent également l'en-tête de l'e-mail pour qu'il ressemble à celui de la vraie banque.

Les faux e-mails distribués par les spécialistes du phishing ont une chose en commun : ce sont des appâts utilisés pour inciter le client à cliquer sur un lien fourni dans le message. Si le client mord à l'hameçon, le lien dirige directement l'utilisateur vers un site imitant celui de la banque, qui contient un formulaire que la victime doit compléter. Cette dernière fournit alors à son insu toutes les informations dont le cyber-criminel 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. Le terme rootkit a été emprunté à l'environnement Unix, où il était utilisé pour décrire des outils servant à maintenir l'accès « racine » (root en anglais) tout en restant invisible aux yeux de l'administrateur système. Mais, dans le contexte des attaques visant Windows, il s'agit d'une technique de dissimulation utilisée par les auteurs de programmes malveillants pour masquer les modifications qu'ils ont apportées à la machine de la victime.

En général, l'auteur de programme malveillant accède au système en usurpant un mot de passe ou en exploitant la vulnérabilité d'une application, puis en l'utilisant pour obtenir d'autres informations système jusqu'à obtenir l'accès administrateur à la machine. Les rootkits sont souvent utilisés pour masquer la présence d'un cheval de Troie en dissimulant les modifications des registres, les processus de cheval de Troie 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 appelé Mebroot). L'objectif 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 MBR (Master Boot Record) 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 les instructions dans le BIOS). Depuis, les bootkits n'ont cessé de se développer, notamment dans des versions 64 bits.

LE TERME EST EMPRUNTÉ À L'ENVIRONNEMENT UNIX, OÙ IL ÉTAIT UTILISÉ POUR DÉCRIRE DES OUTILS SERVANT A MAINTENIR L'ACCÈS « RACINE » (ROOT EN ANGLAIS) TOUT EN RESTANT INVISIBLE AUX YEUX DE L'ADMINISTRATEUR SYSTÈME.

Conseil de l'équipe GReAT : développez une stratégie de sécurité

Votre stratégie de sécurité doit être adaptée à votre entreprise au lieu de reposer sur des « meilleures pratiques » génériques et des estimations approximatives. Une évaluation approfondie des risques permet de déterminer les risques auxquels votre entreprise est exposée. Vous aurez besoin d'un mécanisme pour mesurer l'efficacité de vos outils de sécurité et d'un processus permettant de mettre à jour une stratégie visant à répondre aux nouvelles menaces.

CHAPITRE 2

ÊTES-VOUS PARTICULIÈREMENT VISÉ ?

UNE NOUVELLE ÈRE D'ATTAQUES CIBLÉES

ATTAQUES CIBLÉES

Le panorama des menaces continue d'être dominé par des attaques spéculatives et aléatoires conçues pour voler des informations personnelles à toute personne suffisamment malchanceuse pour être victime d'une attaque. Mais il est clair que le nombre d'attaques ciblées augmente et que ce type de menace est devenu un élément bien ancré dans le panorama des menaces.

Les attaques ciblées cherchent à pénétrer une entreprise cible, à dérober les données d'une société ou à nuire à la réputation d'une entreprise. Nous sommes entrés dans une ère où un code malveillant peut devenir une cyber-arme et, même si une entreprise n'est pas la cible directe de ce genre d'attaque, elle peut être victime de « dommages collatéraux » si elle n'est pas correctement 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 devenir victime. Toutes les entreprises détiennent des données qui peuvent être utiles aux cyber-criminels. De plus, elles sont toutes susceptibles de servir de « tremplins » permettant d'atteindre d'autres entreprises.

Conseil de l'équipe 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.

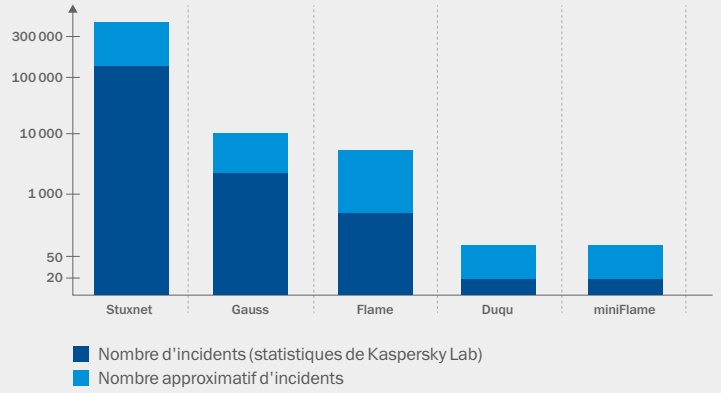
CYBER-ARMES

Stuxnet a été le premier programme malveillant hautement sophistiqué utilisé pour réaliser des attaques ciblées contre des sites de production stratégiques. L'apparition d'autres attaques commanditées par un État (Duqu, Flame et Gauss) a clairement démontré que ce type de menace ne constituait pas un incident isolé.

Nous vivons désormais dans une ère de « cyber-guerre froide » où les nations ont la possibilité de se 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. Les cibles de ce genre d'attaques pourraient notamment être 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.

Nombre de victimes



CHAPITRE 3

DES PROGRAMMES MALVEILLANTS AUSSI MOBILES QUE VOUS

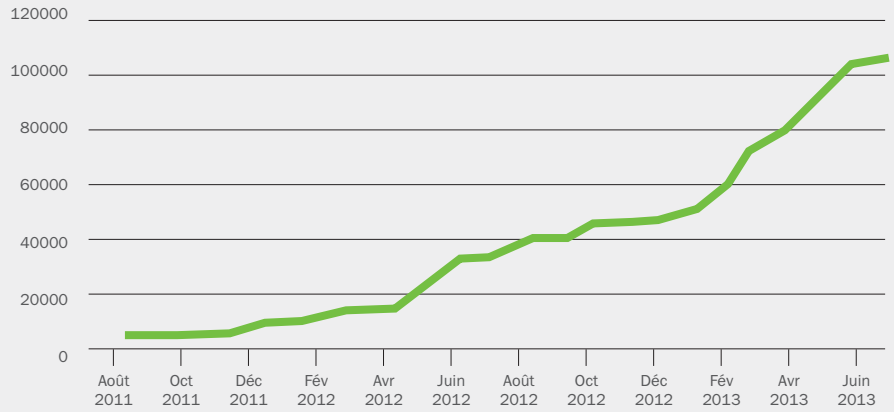
LA CROISSANCE DES PROGRAMMES MALVEILLANTS CONTRE LES APPAREILS MOBILES

Les cyber-criminels se concentrent de plus en plus 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. Le tournant a eu lieu en 2011. Le même nombre de menaces a été détecté en 2011 autant que sur l'ensemble de la période 2004-2010.

Cette croissance explosive continue de se développer.

Nombre d'échantillons uniques



LE DÉVELOPPEMENT DES PROGRAMMES MALVEILLANTS CONTRE LES APPAREILS MOBILES

Les premières attaques contre les appareils mobiles ont ciblé Symbian et, dans une moindre mesure, WinCE. Toutefois, les auteurs de programmes malveillants ont rapidement développé des menaces utilisant Java Mobile Edition (J2ME), poussés par le besoin de créer des programmes malveillants sur plusieurs plates-formes à une époque où le marché des smartphones était fragmenté.

Fin 2009, environ 35 % des attaques reposaient sur Java. L'année suivante, le nombre des menaces basées sur Java représentait environ 57 % des attaques sur les appareils mobiles, Symbian perdant sa place de cible principale des auteurs de programmes malveillants.

En 2012, près de 94 % des attaques visaient Android

En 2011, on a observé une hausse massive du nombre de menaces visant Android (64 %). En 2012, près de 94 % des attaques ciblaient Android.

Cette évolution est principalement due au fait qu'Android fournit un environnement ouvert aux développeurs d'applications, ce qui a abouti à la création d'une sélection d'applications large et diverse. 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. Le risque en termes de sécurité est donc moindre : pour propager un code, les auteurs de programmes malveillants doivent trouver un moyen de l'introduire dans l'App Store.

Il est donc probable qu'Android reste la principale cible des cyber-criminels, pour un certain temps tout du moins.

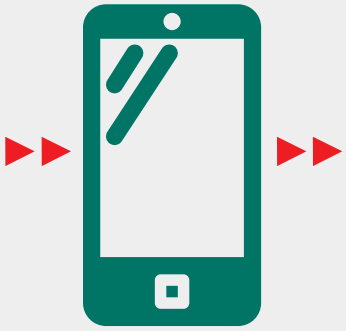
BANQUE MOBILE – LA PROCHAINE PROIE DES CYBER-CRIMINELS ?

L'utilisation des smartphones pour les opérations bancaires en ligne n'étant pas encore très répandue, les cyber-criminels ne vont pas se concentrer pleinement sur ce sujet dans l'immédiat. Néanmoins, il est 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 envoyant 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).

Connues sous le nom d'attaques « Man-in-the-Mobile », trois menaces spécifiques ont été développées à cet effet : ZeuS-in-the-Mobile (ou ZitMo), SpyEye-in-the-Mobile (ou SpitMo) et Carberb-in-the-Mobile (ou CitMo).

Les cyber-criminels étudient en permanence différents moyens de gagner de l'argent, notamment avec les smartphones. Ainsi, le botnet SpamSold, apparu fin 2012, envoie des SMS indésirables à partir d'appareils infectés.

À ce jour, la plupart des programmes malveillants ont été conçus pour obtenir un accès racine à l'appareil. À l'avenir, il est probable que les cyber-criminels utilisent les vulnérabilités qui ciblent le système d'exploitation pour développer des « téléchargements intempestifs ».



Conseil de l'équipe GReAT : mettez en place une politique de sécurité de type « follow me »

Vérifiez 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

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 la principale méthode actuellement utilisée 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. L'ordinateur de la victime est infecté si une application non sécurisée et non corrigée y est installée.

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 grand pays, qui constitue une réserve de victimes potentielles toute prête. Les cyber-criminels utilisent les réseaux sociaux de différentes manières.

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

Les cyber-criminels profitent du fait que les utilisateurs de réseaux sociaux sont prédisposés à partager trop d'informations et à faire confiance aux personnes qu'ils connaissent.

MESSAGERIES ÉLECTRONIQUES ET INSTANTANÉES

Près de 3 % des e-mails contiennent des programmes malveillants sous forme de pièces jointes ou de liens. Les attaques ciblées ont également recours aux e-mails pour pénétrer dans la ou les entreprise(s) cible(s). Le cyber-criminel envoie un e-mail à une personne spécifique de l'entreprise, dans l'espoir que cette dernière lira la pièce jointe ou cliquera sur le lien et lancera le processus lui permettant d'accéder au système. Cette méthode porte le nom de « phishing ciblé ».

Pour optimiser leurs chances de réussite, les cyber-criminels envoient la plupart du temps leur e-mail à des employés en contact avec le public qui n'appartiennent généralement pas aux services techniques (des responsables commerciaux et marketing, par exemple). 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'entreprise pour paraître authentique.

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

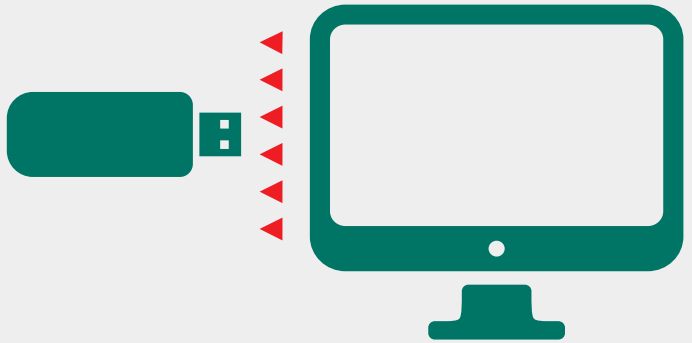
POUR OPTIMISER LEURS CHANCES DE REUSSITE, LES CYBER-CRIMINELS ENVOIENT LA PLUPART DU TEMPS LEUR E-MAIL A DES EMPLOYÉS EN CONTACT AVEC LE PUBLIC, QUI N'APPARTIENNENT GÉNÉRALEMENT PAS AUX SERVICES TECHNIQUES (DES RESPONSABLES COMMERCIAUX ET MARKETING, PAR EXEMPLE).

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.

Ils s'en servent également pour aider les programmes malveillants à passer d'un ordinateur non fiable connecté à Internet à un réseau fiable (une méthode utilisée par Stuxnet, par exemple).

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



VULNÉRABILITÉS ET FAILLES D'EXPLOITATION

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 par leurs applications.

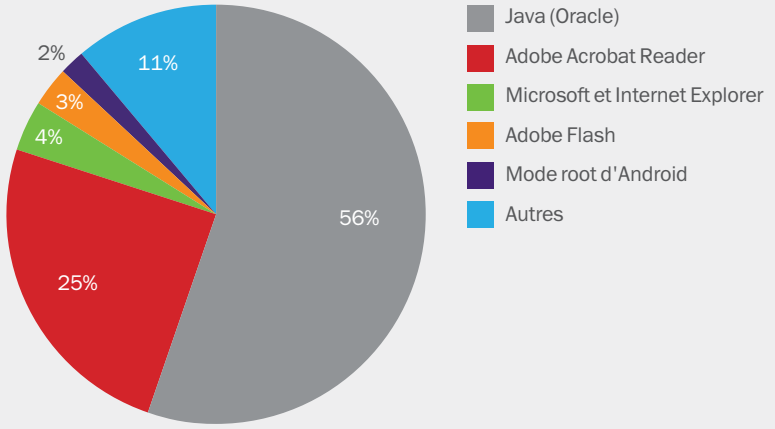
Ces vulnérabilités, également appelées bugs, peuvent être présentes dans le système d'exploitation. Les cyber-criminels se concentrent généralement sur les applications les plus courantes susceptibles de ne pas être corrigées pendant le plus longtemps possible, ce qui leur donne une marge suffisante pour atteindre leurs objectifs.

FAILLES D'EXPLOITATION ZERO-DAY

Mais ils ne se contentent pas de compter sur le fait que les utilisateurs ne corrigent pas leurs applications : ils sont parfois capables d'identifier des vulnérabilités avant même le fournisseur de l'application.

Ces vulnérabilités, appelées vulnérabilités « zero-day », permettent aux cyber-criminels de propager leurs programmes malveillants sur n'importe quel ordinateur hébergeant l'application vulnérable, que la correction la plus récente ait été installée ou non.

Applications les plus ciblées



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, les cyber-criminels réussissent non seulement à émettre de faux certificats pour leurs programmes malveillants en utilisant des certificats « auto-signés », mais ils sont également capables de violer le système d'autorités de certification et d'utiliser les 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.

Conseil de l'équipe 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 5

LE FACTEUR HUMAIN EN MATIÈRE DE SÉCURITÉ

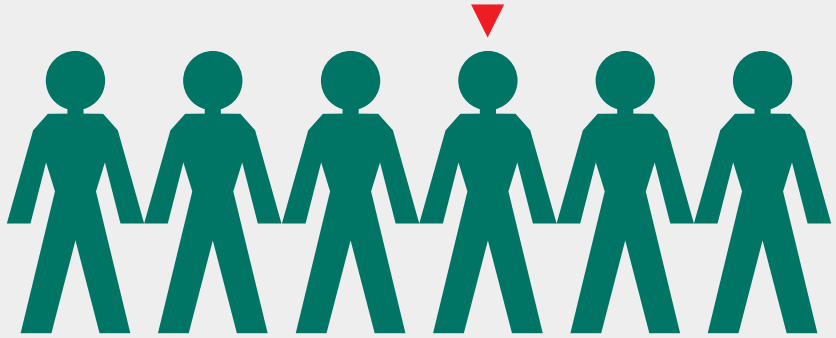
LE FACTEUR HUMAIN

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 informées des ruses utilisées par les cyber-criminels
- Elles ne connaissent pas les signes auxquels elles doivent prêter attention
- De plus, les escroqueries successives ne sont jamais vraiment identiques, ce qui rend difficile de savoir ce qui est sûr et ce qui ne l'est pas

Parfois, les utilisateurs prennent des raccourcis pour se simplifier la vie et ne sont pas conscients des conséquences que leur comportement peut avoir en termes de sécurité. Cela vaut notamment pour les mots de passe. De nombreux utilisateurs utilisent le même mot de passe pour tout, en général un mot facile à mémoriser. Ou bien, ils choisissent simplement « motdepasse » !

Cette attitude renforce la probabilité qu'un cyber-criminel devine leur mot de passe. Et si un compte est infecté, cela facilite l'accès à d'autres comptes. Même lorsqu'on les informe du danger potentiel, la plupart des individus ne voient pas d'alternative réalisable, car ils ne sont pas en mesure de mémoriser un grand nombre de mots de passe différents.



PIRATAGE INFORMATIQUE

Le piratage informatique repose sur la manipulation de la psychologie humaine : faire en sorte que quelqu'un fasse ce qu'on attend de lui. Dans le contexte de la sécurité informatique, cela consiste à piéger une personne pour qu'elle fasse quelque chose qui compromet sa sécurité ou la sécurité de l'entreprise dans laquelle elle travaille.

Les e-mails de phishing offrent un bon exemple de piratage informatique. Ils prennent souvent la forme de courriers indésirables envoyés à une grande quantité de personnes et imitent les vrais e-mails d'une entreprise réelle. Ils imitent 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 croiront 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 toutes 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.

Conseil de l'équipe GReAT : sensibilisez

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 d'autres conseils sur la manière de diffuser le message à vos collègues, consultez les 10 conseils utiles figurant à la fin de ce guide.

CHAPITRE 6

TECHNOLOGIE DE PROTECTION CONTRE LES PROGRAMMES MALVEILLANTS

LES TECHNOLOGIES DE PROTECTION CONTRE LES PROGRAMMES MALVEILLANTS UTILISÉS AUJOURD'HUI

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 principales technologies de protection contre les programmes malveillants utilisées aujourd'hui sont présentées ci-dessous.

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 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'examiner comment le code se comportera lorsqu'il sera exécuté sur l'ordinateur réel.

Analyse comportementale

Cette démarche consiste à surveiller le système en temps réel pour voir comment un code agit avec l'ordinateur. Les dispositifs d'observation de système les plus sophistiqués n'examinent pas uniquement le code de manière isolée : ils suivent également leurs activités sur différentes sessions et observent comment le code interagit avec d'autres processus sur l'ordinateur.

Liste blanche

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 procèdent de manière inverse en bloquant les codes qui ne figurent pas sur la liste des programmes acceptables.

Pour en savoir plus sur les listes blanches, rendez-vous à l'adresse suivante :
http://whitelist.kaspersky.com/
Pour obtenir des informations détaillées, téléchargez le pdf ci-dessous :
http://media.kaspersky.com/en/business-security/application-security-control-tools%20best-practices.pdf

Recherche des vulnérabilités

Étant donné que les cyber-criminels utilisent très souvent les vulnérabilités des applications, il est utile de pouvoir identifier sur un système les applications qui sont vulnérables aux attaques, afin de permettre aux entreprises ou aux individus de mettre en place des actions correctives. Certaines solutions sont également dotées d'une fonction d'analyse en temps réel des ordinateurs pour bloquer l'utilisation des vulnérabilités zero-day.

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 fournisseur, 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.

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 panorama de 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.

Pour en savoir plus sur les plates-formes intégrées, téléchargez le pdf ci-dessous :
http://media.kaspersky.com/en/business-security/10-Kaspersky-Integrated-Security-Solution-Benefits.pdf

Conseil de l'équipe GReAT : utilisez une technologie proactive

Déployez des solutions de protection contre les programmes malveillants rassemblant différentes technologies pour bloquer les nouvelles menaces inconnues 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 et Analysis Team (GReAT) de Kaspersky Lab.

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. L'équipe GReAT a été à l'avant-garde de la détection et de l'élimination de plusieurs des programmes malveillants majeurs apparus ces dernières années, y compris Stuxnet, Duqu, Flame et NetTraveler. En 2013, elle a remporté le titre d'« Équipe dédiée à la sécurité des informations de l'année » aux SC Awards.

Ce rapport est émaillé de conseils de l'équipe GReAT conçus pour vous aider à tirer le meilleur de votre logiciel de sécurité.

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 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.

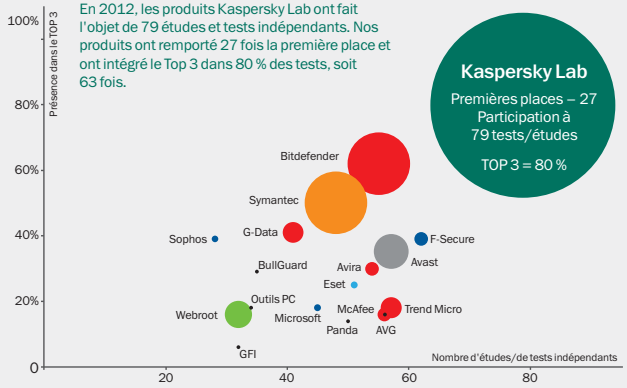
En 2012, les produits Kaspersky Lab ont fait l'objet de 79 tests et études indépendants. Nos produits ont reçu 27 premiers prix et ont intégré 63 fois le Top 3.

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 qui surgissent.

Pour en savoir plus, rendez-vous à l'adresse suivante :
www.kaspersky.com/fr/business-security

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

10 CONSEILS UTILES POUR SENSIBILISER SUR LA SÉCURITÉ DANS VOTRE ENTREPRISE

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

1 DÉSIGNEZ CORRECTEMENT VOTRE PUBLIC

Évitez d'employer le mot « utilisateur » pour désigner vos interlocuteurs, il est impersonnel et peut donner à votre public l'impression de ne pas être vraiment concerné par votre message. Utilisez plutôt les mots « employé », « collaborateur », « collègue » ou « personne ».

2 UTILISEZ UN TON APPROPRIÉ

Si vous utilisez un ton accessible et amical, vous pourrez communiquer plus efficacement avec vos collègues et les informer de ce qu'ils peuvent faire pour protéger l'entreprise.

3 FAITES APPEL AUX ÉQUIPES RH ET JURIDIQUE

Si nécessaire, elles peuvent mettre en place des politiques réelles et apporter leur soutien en cas d'atteinte à la sécurité informatique.

4 TENEZ VOS COLLÈGUES INFORMÉS

Réfléchissez à la fréquence et au moment adéquats pour communiquer vos informations en matière de sécurité informatique. Veillez à ce qu'elles soient régulières et marquantes.

5 FAITES APPEL À VOTRE IMAGINATION

Il y a de nombreux moyens de rendre des informations plus accrocheuses. Plus votre message est créatif et intéressant, plus il a de chances d'être lu. Faites appel à des bandes dessinées, des affiches et des questionnaires.

6 FAITES LE POINT SUR VOS ACTIONS

Vos informations ont-elles été bien comprises ?
Testez vos collègues et voyez ce qu'ils ont retenu et ce qu'ils ont oublié. Vous pouvez par exemple commencer par leur soumettre un questionnaire sur les 5 problèmes majeurs de sécurité informatique.

7 APPORTEZ UNE TOUCHE PERSONNELLE

Si vous faites appel aux intérêts personnels de vos collègues, vous les aiderez à mieux comprendre l'importance et le contexte de la sécurité informatique. Par exemple, parlez-leur des failles de sécurité qui pourraient affecter leurs appareils mobiles.

8 ÉVITEZ D'UTILISER DU JARGON

La plupart de vos collègues n'ont pas le même niveau de connaissance que vous.
Pensez donc à tout expliquer d'une manière qui soit facilement compréhensible.

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. Certaines personnes ont peur d'être sanctionnées si on apprend qu'elles ont cliqué sur le lien d'un e-mail de phishing, c'est pourquoi elles évitent d'avertir les personnes qui doivent en être informées.

10 CONSULTEZ L'ÉQUIPE MARKETING

En matière de communication interne au sein de votre entreprise, ce sont eux les experts.
Demandez-leur de vous aider à trouver comment impliquer au mieux vos collègues.

KASPERSKY lab