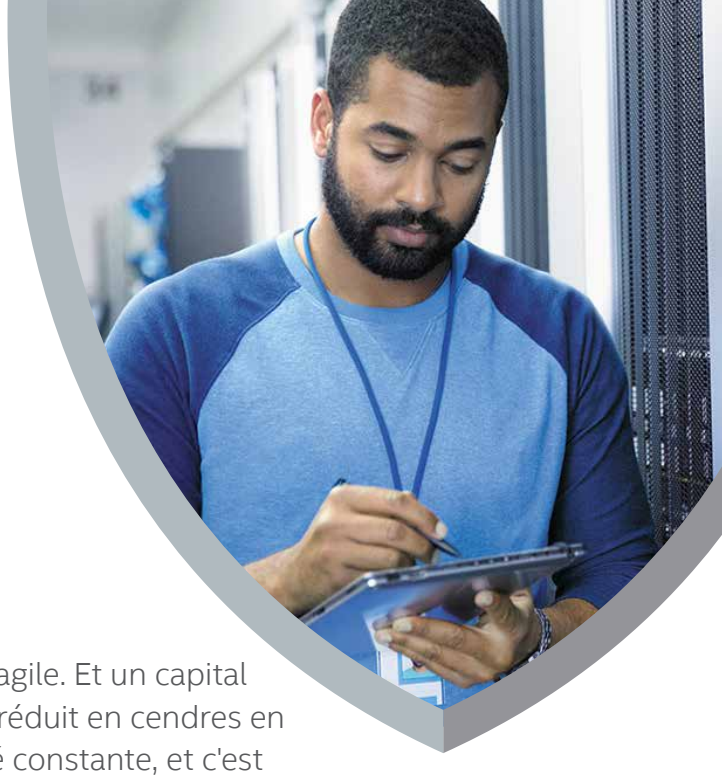
Présentation de solution



Abus de confiance

La confiance brisée des utilisateurs

La confiance dans les relations est aussi précieuse que fragile. Et un capital confiance qui a mis des années à se construire peut être réduit en cendres en quelques secondes. La notion de confiance n'a jamais été constante, et c'est d'autant plus vrai au regard de la dépendance croissante de la population vis-à-vis d'Internet, partout dans le monde.

Que recouvre ici la notion d'« abus de confiance » ?

L'exploitation de la confiance des utilisateurs est abordée en détail dans le **Rapport de McAfee sur le paysage des menaces de novembre 2014**. Dans le cybermonde, nous partons du principe que ce que nous voyons est digne de confiance, qu'il s'agisse d'une application téléchargée sur un terminal mobile, d'une publicité en apparence inoffensive sur un site web populaire, ou d'un e-mail émanant d'une entreprise avec laquelle nous entretenons des relations d'affaires. Les cyberpirates exploitent cette confiance de nombreuses façons, dans le but principal de leurrer de malheureuses victimes. Voici quelques types d'attaques abordés dans le rapport :

- **Publicités malveillantes —** Lorsque les publicités apparaissant sur le site Internet d'une entreprise sont à l'origine d'une attaque dirigée contre des consommateurs qui ne se doutent de rien, ces derniers sont en droit de se demander si leur confiance est mal placée. **Les réseaux publicitaires malveillants tels que « Kyle and Stan »** transmettent du malware par le truchement de publicités malveillantes sur des sites web tels que amazon.com, youtube.com et de **grands réseaux publicitaires tels que Double-Click et Zedo**.
- **Logiciels malveillants signés —** Une tactique de plus en plus courante chez les auteurs de logiciels malveillants consiste à acquérir des certificats auprès d'une autorité de certification pour ensuite les utiliser pour exploiter indûment la confiance accordée à des enseignes connues ou pour usurper l'identité d'une entreprise légitime. Les cybercriminels abusent de la confiance que nous accordons aux autorités de certification. Récemment, une campagne publicitaire malveillante a distribué des variantes signées de CryptoWall par l'intermédiaire du réseau publicitaire Zedo ; celles-auraient **pris pour cible des utilisateurs de sites web en tête du classement de popularité Alexa**. La signature numérique utilisée était délivrée à « Trend », un nom probablement destiné à évoquer dans l'esprit de l'internaute l'éditeur de solutions de sécurité Trend Micro. C'est là un parfait exemple de cas où les utilisateurs accordent leur confiance « par association ».
- **Applications falsifiées —** Les marques ne ménagent ni leur temps ni leurs efforts pour protéger leurs clients contre les contrefaçons qui exploitent la confiance établie entre elles et les consommateurs. Dans la mesure où les applications proposent des fonctions dont la portée va bien au-delà du monde numérique, il n'est pas surprenant que des pirates entreprenants aient recours à des copies frauduleuses de programmes légitimes et populaires.

intel Security

Au cours du dernier trimestre, McAfee a observé des escrocs tentant de distribuer une application qui semblait être à première vue Adobe FlashPlayer 11. D'après le nombre de téléchargements sur Google Play et les données télémétriques de détection de McAfee Mobile Security, ces escrocs ont rencontré un certain succès puisqu'un grand nombre d'internautes ont téléchargé cette version frelatée.

- **Chargement latéral de fichiers DLL —** Les cybercriminels savent que s'ils parviennent à intégrer leur code malveillant dans une application approuvée, ils auront plus de chances de parvenir à leurs fins. Les logiciels malveillants ont profité de cette situation pendant des années, en adoptant une technique d'attaque appelée chargement latéral de fichiers DLL (*DLL side loading*). Cette technique consiste à exécuter une application légitime qui exécute elle-même le code d'une DLL externe. Les cybercriminels conçoivent leur charge active pour qu'elle endosse le rôle du fichier DLL externe, poussant ainsi l'application légitime à exécuter le code malveillant.

  Au cours du troisième trimestre, McAfee Labs a observé des attaques à l'encontre de l'application Google Updater. La nouvelle variante de la famille de malware PlugX endosse le rôle du module goopdate.dll importé, mais va encore plus loin pour dissimuler ses méfaits. Le module goopdate.dll n'est rien de plus qu'un intercepteur qui lit le contenu d'un fichier de données chiffré (goopdate.dll.map), le déchiffre dans sa mémoire, puis envoie une commande d'exécution au code malveillant.

- **Systèmes d'exploitation et logiciels réseau —** Il existe de nombreux exemples d'attaques qui exploitent abusivement les relations de confiance entre les systèmes d'exploitation et les logiciels réseau, et au sein même de ceux-ci. Certaines attaques utilisent les logiciels qui établissent des connexions sécurisées sur Internet. Les applications font confiance aux connexions qui leur sont transmises par le système d'exploitation, qui fait lui-même confiance au logiciel réseau qui a établi des connexions censées être sécurisées. D'autres attaques tirent profit des vulnérabilités au sein des systèmes d'exploitation et des logiciels réseau. Souvent, elles exploitent des logiciels à code source libre (*open source*) intégrés dans le système d'exploitation ou la pile logicielle réseau.

  BERserk est une vulnérabilité **révélée récemment** qui falsifie les signatures et, ce faisant, abuse de la confiance des systèmes d'exploitation et des logiciels réseau. BERserk permet à des pirates d'exécuter des attaques de type « intercepteur » (*man-in-the-middle*), dans le cadre desquelles ils falsifient les signatures RSA et contournent ainsi le mécanisme d'authentification des sites web utilisant les protocoles SSL/TLS.

Solutions McAfee

La technologie de sécurité McAfee peut vous aider à vous protéger contre les attaques qui exploitent abusivement la confiance que votre entreprise place dans ses opérations quotidiennes. Voici quelques produits McAfee visant à garantir que les processus informatiques de l'entreprise basés sur la confiance ne sont pas abusés par des cyberpirates.

McAfee Application Control

Il est crucial de protéger votre entreprise et ses applications légitimes contre du code malveillant tel que BERserk. **McAfee Application Control** permet à votre entreprise de contrôler les applications autorisées à s'exécuter dans votre environnement par le truchement de listes blanches dynamiques et de stratégies de mise en œuvre, qui s'appliquent tant aux terminaux connectés qu'à ceux hors connexion.

- **Listes blanches dynamiques —** Cette fonction permet à l'entreprise de gérer efficacement les applications sur liste blanche en développant automatiquement cette dernière à mesure que les systèmes sont corrigés et mis à jour. McAfee Application Control réduit votre exposition à BERserk en bloquant l'exécution d'applications appelant le code de vérification de signatures RSA vulnérable.

- **Réputation des fichiers —** L'intégration à McAfee Global Threat Intelligence permet à McAfee Application Control d'interroger les flux d'informations en temps réel définissant les types de fichiers dont la réputation est bonne, mauvaise ou inconnue, de façon à aider l'entreprise à identifier les nouvelles vulnérabilités telles que BERserk.
- **Protection des équipements, qu'ils soient connectés ou hors connexion —** Les contrôles sont mis en œuvre sur les serveurs, les machines virtuelles, les terminaux et les équipements fixes tels que les terminaux de point de vente, qu'ils soient connectés ou non.

McAfee Email Gateway
L'innocuité du courrier dans les boîtes de réception des employés constitue une préoccupation importante des entreprises. Les pirates utilisent par exemple des e-mails de *spear phishing* (harponnage) pour amener des utilisateurs trop confiants à provoquer eux-mêmes une compromission, par l'intermédiaire de logiciels malveillants incorporés ou d'URL malveillantes. **McAfee Email Gateway** offre une protection contre ces types d'attaques au moyen de différentes fonctionnalités :

- **ClickProtect —** Élimine les menaces transmises par des URL incorporées dans les e-mails en les analysant au moment où l'utilisateur clique dessus. L'inspection comprend un contrôle de la réputation des URL et une émulation proactive assurée par McAfee Gateway Anti-Malware Engine.
- **Intégration avec McAfee Advanced Threat Defense —** Détecte les logiciels malveillants sophistiqués et difficiles à identifier grâce à l'analyse statique approfondie du code et à l'analyse dynamique appliquées aux fichiers suspects joints aux e-mails. Cette méthode permet de bloquer les fichiers malveillants avant qu'ils ne puissent atteindre la boîte de réception.
- **Intégration à McAfee Global Threat Intelligence —** La combinaison des informations réseau locales et des données sur la réputation fournies par McAfee Global Threat Intelligence permet d'offrir la protection la plus complète contre les menaces entrantes, le spam et les logiciels malveillants.

McAfee Global Threat Intelligence
McAfee Global Threat Intelligence (GTI) est un service complet de renseignements sur les menaces, délivré en temps réel et basé dans le cloud, qui permet aux produits McAfee de bloquer les cybermenaces sur tous les vecteurs : fichiers, Web, messagerie électronique et réseau. Il assure une protection proactive contre l'abus de confiance grâce aux fonctionnalités suivantes :

- **Réputation des certificats —** Le système interroge les flux de données en temps réel qui renseignent les certificats dont la bonne ou mauvaise réputation est connue, dans le but de protéger votre entreprise contre des menaces telles que les logiciels malveillants signés qui peuvent être transmis par le truchement de réseaux publicitaires malveillants.
- **Réputation des fichiers —** L'entreprise est protégée contre les applications falsifiées sur les postes de travail, en plus d'être informée des applications susceptibles d'être vulnérables à des attaques telles que BERserk. Les flux de données interrogés signalent les fichiers légitimes, malveillants ou inconnus en temps réel pour assurer une protection efficace.
- **Renseignements par corrélation des vecteurs —** Le système collecte et corrèle les données provenant de tous les principaux vecteurs de menaces (fichiers, Web, messagerie électronique et réseau) afin de détecter les menaces combinées, telles que la distribution de logiciels malveillants signés par des réseaux publicitaires, des e-mails de spear phishing émanant de sources en apparence fiables, ou encore les téléchargements à l'insu de l'utilisateur sur des sites malveillants ou des sites web censés être légitimes et pourtant compromis.
- **Security Connected —** McAfee GTI est intégré aux produits de sécurité McAfee pour fournir les informations les plus détaillées sur les menaces, la corrélation des données la plus précise et l'intégration aux produits la plus complète de façon à assurer une protection optimale contre les menaces pratiquant l'abus de confiance.

McAfee Vulnerability Manager
Les attaques telles que BERserk sont une illustration parfaite du paysage des menaces en perpétuelle évolution qui affecte le modèle des relations de confiance. Cela dit, déterminer si vous courez effectivement un risque et évaluer votre degré de vulnérabilité à ces nouvelles attaques peuvent apparaître comme des épreuves insurmontables. Voici, à titre d'exemple, comment **McAfee Vulnerability Manager** et **McAfee Asset Manager** peuvent aider votre entreprise à comprendre les vulnérabilités telles que BERserk et à prendre les mesures nécessaires pour combler efficacement les failles éventuelles :

- **Analyse complète des vulnérabilités —** McAfee Vulnerability Manager est un produit autonome hautement évolutif pour la découverte des hôtes, la gestion des actifs, l'évaluation des vulnérabilités et la génération de rapports sur tous les équipements réseau. Il peut évaluer le risque de succomber à BERserk en recherchant les systèmes qui exécutent des versions vulnérables de Firefox, de Chrome et d'autres produits qui appellent le code de vérification de signatures RSA vulnérable.
- **Personnalisation des analyses en fonction des nouvelles menaces —** L'outil FSL (Foundstone Scripting Language) Editor peut optimiser les contrôles prédéfinis et les mises à jour pour améliorer la détection des menaces et des vulnérabilités « jour zéro » telles que BERserk, grâce à la création de scripts et de contrôles personnalisés destinés à évaluer votre environnement. McAfee Vulnerability Manager peut désormais détecter les systèmes vulnérables à BERserk au moyen de ses contrôles prédéfinis, et ce depuis le 24 septembre 2014.
- **Rapports et corrections flexibles —** McAfee Vulnerability Manager et McAfee Asset Manager fonctionnent de concert pour assurer une gestion et une surveillance automatisées de l'analyse, de la correction, de la mise en œuvre et de la génération de rapports. Vous évitez ainsi les exercices d'alerte et les processus ponctuels fastidieux, vous éliminez les erreurs et vous protégez plus de systèmes avec efficacité.
- **Connaissance de votre niveau de risque —** McAfee Asset Manager indique à l'entreprise les systèmes vulnérables à BERserk en mettant en corrélation des analyses de vulnérabilités avec des analyses de découverte des hôtes. L'identification en temps réel des systèmes précis qui exécutent des versions vulnérables de certaines applications permet de perdre moins de temps en spéculations et d'en consacrer davantage aux mesures correctives.

McAfee Web Gateway
Les publicités malveillantes, les téléchargements à l'insu de l'utilisateur et les URL malveillantes incorporées à des URL légitimes ne sont que quelques-unes des attaques utilisées pour abuser de la confiance. **McAfee Web Gateway** optimise la protection de votre entreprise contre ce type de menaces.

- **McAfee Gateway Anti-Malware Engine —** L'analyse des intentions sans signatures filtre, en temps réel, le contenu malveillant du trafic web. L'émulation et l'analyse comportementale protègent de manière proactive contre les attaques ciblées et de type « jour zéro ». McAfee Gateway Anti-Malware Engine inspecte les fichiers et empêche leur téléchargement s'ils sont malveillants. McAfee Web Gateway est le produit leader du marché pour sa capacité à bloquer les téléchargements de malware, grâce à la fonctionnalité d'inspection unique de ce moteur.
- **Intégration avec McAfee GTI —** Les flux de données en temps réel de McAfee GTI sur la réputation des fichiers, la réputation web et la catégorisation web offrent une protection contre les dernières menaces, car McAfee Web Gateway bloque les tentatives de connexion à des sites malveillants connus ou à des sites web utilisant des réseaux publicitaires malveillants.

McAfee SiteAdvisor® Enterprise
Ne pas se laisser distancer par le paysage des menaces en évolution perpétuelle constitue un défi de taille. En particulier lorsqu'il s'agit de protéger les utilisateurs en ligne contre des menaces telles que des abus de confiance, sans pour autant imposer des stratégies trop restrictives qui gâchent l'expérience utilisateur.

- **Identification aisée de menaces telles que des sites web malveillants se présentant comme légitimes —** Fondé sur un système de classification intuitif avec codes de couleur, **McAfee SiteAdvisor Enterprise** offre une couche de protection supplémentaire au niveau du poste de travail. McAfee SiteAdvisor Enterprise bloque les connexions vers les sites malveillants connus et informe les utilisateurs du danger.
- **Sécurité optimisée par McAfee GTI —** McAfee GTI procure des renseignements sur les menaces en temps réel à McAfee SiteAdvisor Enterprise, pour que ce dernier évalue les sites web en s'appuyant sur les informations les plus récentes.

McAfee Threat Intelligence Exchange
L'abus de confiance peut prendre de multiples formes. Dès lors, une plate-forme de renseignements capable de s'adapter aux besoins de votre environnement au fil du temps constitue un outil vital. **McAfee Threat Intelligence Exchange (TIE)** réduit considérablement l'exposition aux attaques grâce à sa visibilité sur les menaces telles que les certificats malveillants détectés dans votre environnement.

- **Réputation des certificats —** L'intégration à McAfee GTI permet à votre entreprise de se protéger en temps réel contre les attaques qui exploitent le code malveillant signé, en interrogeant les flux d'informations en temps réel sur la bonne ou mauvaise réputation des certificats. McAfee TIE peut protéger vos terminaux contre les certificats malveillants au travers de stratégies gérées de manière centralisée, qui peuvent être déployées pour protéger à la fois les terminaux connectés et déconnectés.
- **Blocages des attaques telles que les chargements latéraux de DLL, les applications falsifiées, etc. —** Une technologie de protection des terminaux de pointe prend les décisions en matière d'exécution de fichiers grâce à une logique basée sur des règles en rapport avec le contexte du terminal (attributs des fichiers, des processus et de l'environnement) et aux renseignements collectifs sur les menaces.
- **Indicateurs de compromission —** Il est possible d'importer dans McAfee TIE des informations sur les hachages de fichiers dangereux et les certificats malveillants connus, dans le but d'immuniser l'environnement contre ces fichiers dommageables grâce à la mise en œuvre de stratégies adéquates. Si l'un des indicateurs de compromission (IoC) déclenche une alerte dans l'environnement, McAfee TIE peut bloquer tous les processus et applications associés à cet IoC.

McAfee VirusScan® Mobile Security

- **Blocage des applications falsifiées —** Soutenu par McAfee GTI, **McAfee VirusScan Mobile Security** peut bloquer les applications frauduleuses transmettant du malware pratiquement en temps réel. La solution peut détecter des logiciels malveillants en moins de 200 millisecondes sans interrompre la connectivité ou les opérations sans fil.

Protéger votre entreprise contre des adversaires qui tentent d'exploiter le modèle de relations de confiance dynamique n'est pas une sinécure. La technologie de sécurité McAfee peut permettre à votre entreprise de se protéger de manière proactive contre les attaques qui se fondent sur l'abus de confiance.

McAfee. Part of Intel Security.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com