KASPERSKY lab

Mythe ou réalité : quelles sont vraiment les menaces actuelles

www.kaspersky.fr

#truecybersecurity

Mythe ou réalité : quelles sont vraiment les menaces actuelles

Y a-t-il un sens à parler d'une nouvelle génération de menaces ?

La guerre sans fin entre pirates et fournisseurs de solutions de cybersécurité illustre à merveille le principe de « survie du plus apte ». Les principaux développeurs de solutions défensives ne ménagent pas leurs efforts quand il s'agit d'enrayer les attaques. Et, jusqu'à récemment du moins, la réussite était globalement de leur côté. Mais cette pression a également poussé les pirates à élaborer de nouvelles astuces, de nouvelles techniques, voire de nouveaux modèles économiques pour ne pas se laisser distancer.

Ce saut qualitatif darwinien en matière d'évolution a donné naissance à une progression intéressante, dans deux directions opposées : d'un côté vers la simplicité, de l'autre vers une sophistication ciblée. Dans les faits, ces deux progressions se traduisent par une complexification croissante du paysage des menaces. Pour y faire face, il faut faire preuve d'inventivité, posséder des ressources et offrir une expérience dont seuls peuvent se prévaloir quelques acteurs du marché, dignes de l'appellation de « fournisseurs de solutions de sécurité nouvelle génération ».

Faut-il comprendre que les fameuses menaces de nouvelle génération sont déjà là, guettant les entreprises comme les particuliers ?

Oui et non.

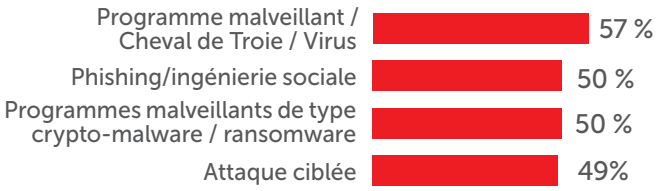
Pour les professionnels de la sécurité informatique, naturellement, la réponse est **négative**.

Personne n'a encore constaté la moindre progression catastrophique dans les techniques de piratage, qui confère aux attaquants des pouvoirs sans précédent face aux systèmes de sécurité actuels. Parmi les « nouvelles » techniques, certaines ont déjà été testées il y a plusieurs années. Leur succès marginal s'expliquait à l'époque par la présence de contraintes technologiques dans les environnements informatiques. Ces techniques d'attaque ressurgissent aujourd'hui, à la faveur des dernières évolutions et donnent aux attaquants un avantage indéniable face à de nombreuses solutions existantes.

Certains systèmes de défense s'en tirent mieux que d'autres. Leurs éditeurs, sans cesse à l'affût des dernières astuces de l'adversaire, déploient des arsenaux entiers de mesures tout à fait nouvelles, sans que leurs clients n'en sachent quoi que ce soit. Pour les clients, tout semble naturel. De fait, aucun fournisseur ne voudra s'exposer aux complications et aux coûts qu'impliquerait l'introduction d'une nouvelle technologie qui forcerait les clients à changer leurs habitudes, dès lors que la même technologie peut être mise en œuvre discrètement, en toute transparence, et assurer, au final, un résultat tout aussi performant pour le client.

Mais il y a un mais...

Car pour l'utilisateur final, cet environnement informatique en pleine évolution, où le risque de perte est de plus en plus important et la pression des attaquants de plus en plus forte, peut être perçu comme une espèce de dragon menaçant de se déchaîner à tout moment. Après tant d'années d'insouciance, à peine ponctuées çà et là d'une infection par un programme malveillant, les entreprises deviennent tout d'un coup les vaches à lait de cybercriminels particulièrement entreprenants et qui n'ont aucune intention de les laisser tranquilles. Pour ceux-là, les « menaces de nouvelles génération » sont bien réelles.



Les 4 préoccupations principales en matière de sécurité informatique pour les entreprises du monde entier portent sur les menaces directes[1].

Ainsi, lorsque quelqu'un demande : « faut-il vraiment s'inquiéter des fameuses menaces de nouvelle génération ? », la réponse n'est jamais simple. Les attaques en question ne sont pas forcément nouvelles, mais elles sont puissantes et difficiles à enrayer. À ce titre, elles exigent donc souvent de la part des fournisseurs de solutions de protection un niveau élevé de compétence, d'expérience et d'implication. L'envergure et l'ampleur des informations sous-jacentes sur les menaces, combinées aux technologies déployées auprès des utilisateurs et des fournisseurs, sont d'une importance capitale, dans ce contexte.

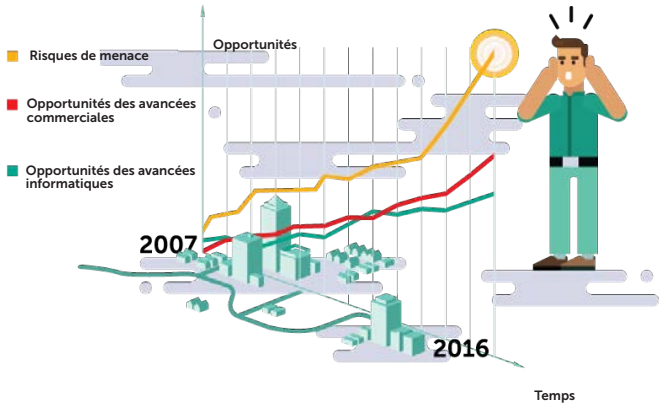
Mais ne suffirait-il pas d'installer des antivirus nouvelle génération pour faire face à l'assaut qui se profile ? C'est hélas une conclusion bien trop hâtive. D'une part parce que, face à la diversité de ces menaces de nouvelle génération, les mesures de protection doivent afficher un degré de diversité comparable. Il faut entendre par là une cybersécurité réellement multi - niveaux, capable d'assurer une protection contre TOUTES les menaces, d'où qu'elles viennent, et pas uniquement contre celles qui semblent avoir les faveurs du moment auprès des attaquants les plus actifs.

Malheureusement, la nécessité d'une protection fiable face à l'éventail de menaces le plus large est trop souvent négligée par les fournisseurs de « nouvelle génération » au profit d'une simplicité maximale et d'un impact minimal sur les performances. Cela a été amplement démontré par des tests indépendants.

À l'inverse, les leaders du marché comme Kaspersky Lab sont tout à fait conscients de la diversité et de la sophistication de ces menaces et offrent donc

1 Source : enquête 2016 sur les risques informatiques mondiaux pour les grandes entreprises, B2B International et Kaspersky Lab

de *multiples* techniques pour en protéger leurs clients. Nous ne négligeons pas non plus l'importance des tests approfondis selon les scénarios les plus proches de la réalité possible. Notre participation régulière à tous les tests indépendants nous aide à perfectionner nos diverses couches protectrices, ainsi qu'à démontrer la validité de ce que nous affirmons.



Ce qui nous amène à l'aspect réellement « nouveau » des menaces actuelles.

La progression bidirectionnelle des menaces

Tendance à la simplification

Cette tendance à la simplification, qui repose avant tout sur un calcul de rentabilité, se confirme dans les efforts de développement comme dans les attaques elles-mêmes. Les développeurs, qui se contentent de reprendre des programmes malveillants déjà prêts, moyennant quelques modifications mineures, misent sur l'insuffisance de mesures de sécurité appropriées de leurs victimes. Et le taux de réussite de cette approche est loin d'être négligeable. Pourquoi prendre la peine de développer entièrement un programme malveillant quand d'anciens font très bien l'affaire ? C'est aussi simple que cela !

Autre domaine concerné par la simplification : le marketing des programmes malveillants, qui offre des modèles économiques convenant parfaitement aux cybercriminels à la fois peu doués et peu patients. La vente de services plutôt que de programmes malveillants proprement dit, ou le conditionnement de programmes existants sous la forme d'interfaces plus conviviales, de FAQ détaillées et d'une assistance technique en prime, a entraîné un développement considérable d'un « marché aux pirates » et attiré en grand nombre de jeunes apprentis pirates. Naturellement, cette nouvelle vague est venue augmenter la quantité totale des cyberattaques et renforcer la pression subie par les entreprises.

Tendance à la sophistication

Cette simplification des modèles économiques n'empêche pas la sophistication technologique des outils et des techniques utilisés par les cyberattaquants d'aujourd'hui, bien au contraire. Même les « apprentis » peuvent désormais accéder à des programmes malveillants beaucoup plus avancés aujourd'hui que par le passé. Exploitées par de vrais spécialistes (et la communauté pirate n'en manque pas), les dernières avancées peuvent devenir redoutables.

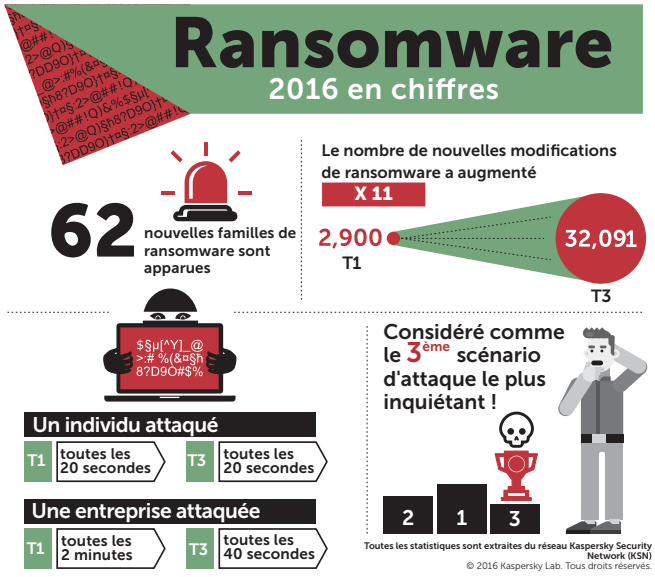
Par ailleurs, certaines techniques réservées jusque-là à des attaquants spécifiques sont de plus en plus adoptées pour des campagnes d'infection de masse (qui peuvent à tout moment se transformer en offensives plus ciblées).

Le voile de l'anonymat

C'est peut-être l'un des changements les plus marquants dans le cadre des récentes transformations du paysage des menaces : le développement de l'anonymat. L'émergence de la technologie Bitcoin et des autres cryptodevises a permis les paiements intraçables, tandis que les réseaux maillés d'anonymisation tels que Tor offrent aux pirates de nouveaux espaces où échanger idées, informations et technologies, pratiquement sans risquer de s'exposer. Si les cybercriminels les plus chevronnés continuent de former des communautés très fermées que l'on ne peut rejoindre que par cooptation, ils ne rechignent pas devant les avantages offerts par ces nouvelles techniques. De fait, certains modèles économiques de cybercriminalité, comme le ransomware (classé troisième dans la liste des préoccupations de sécurité informatique au niveau mondial[2]), ont grimpé en flèche.

Ransomware

Sans qu'il soit attribuable à une technologie en particulier, ce phénomène est l'un des plus emblématiques de la nouvelle génération des menaces. À bien y réfléchir, le ransomware est le modèle économique cybercriminel par excellence. Du point de vue technologique, il s'appuie non seulement sur un vaste éventail d'outils et de techniques d'attaque, mais également sur diverses mesures



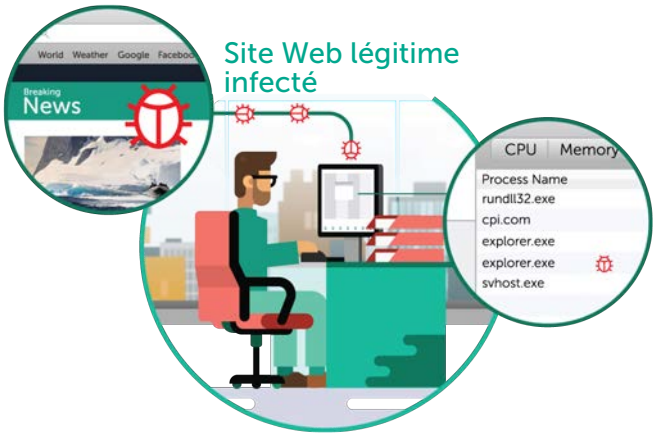
2 B2B International, mai 2016

d'anonymisation. L'émergence des cryptodevises et des réseaux maillés (Tor, I2P, etc.) permet aux criminels de recevoir des paiements incognito, ce qui a entraîné la vague actuelle de ransomwares, la plus grande à ce jour. Faute de mesures adéquates, le ransomware peut vous porter un préjudice direct et dévastateur, et la probabilité d'en atténuer les effets est très faible. En outre, si l'on en croit les statistiques, une victime sur cinq versant la rançon échoue malgré tout à déchiffrer ses fichiers. Sans oublier que le financement des coupables ne fait qu'encourager la prochaine vague de ransomwares.

Les technologies d'attaque et les méthodes d'infection varient selon les « souches » de ransomwares. Il est donc essentiel de mettre en œuvre des solutions multiniveaux équipées de technologies spécialisées contre le ransomware pour protéger l'ensemble de votre système. Par exemple, notre produit Kaspersky Endpoint Security for Business fournit un système d'annulation des chiffrements illicites, capable de bloquer le programme malveillant (crypteur) et, pour les fichiers que l'attaquant serait parvenu à chiffrer, d'en rétablir l'état antérieur. Kaspersky Security for File Servers et Kaspersky Security for Storage intègrent un autre moteur anti-crypteur, complémentaire du précédent, qui bloque les processus de chiffrement lancés par un autre hôte sur le réseau. Et si vous utilisez les solutions d'autres fournisseurs, notre utilitaire autonome (et gratuit) Kaspersky Anti-Ransomware Tool peut vous assurer une protection élémentaire. La technologie sur laquelle s'appuie cet utilitaire gratuit est d'ailleurs la même que celle que l'on retrouve dans Kaspersky Endpoint Security, à la différence près que dans notre solution complète, elle est renforcée par de nombreuses autres couches de protection absentes de la version gratuite.

Programmes malveillants de type « mémoire uniquement »

Le fait que la plupart des programmes malveillants se présentent sous la forme de fichiers classiques justifie l'importance accordée à la détection basée sur les fichiers. C'est à ce niveau qu'a lieu la plus grande partie de la détection. Évidemment, il ne s'agit pas seulement de simples signatures : tout un arsenal heuristique, dont l'analyse structurelle et l'analyse par code, permet la détection de programmes malveillants précédemment inconnus. Mais il suffit que le programme malveillant agisse en dehors du système de fichiers pour que tout cet arsenal devienne soudainement moins utile. Les artefacts de fichiers peuvent aussi fournir au cyberdiagnostic une mine d'informations. C'est pourquoi les attaquants se tournent de plus en plus vers les approches de type « mémoire uniquement », notamment pour les attaques ciblées. Ils peuvent pour cela passer par des techniques d'infection dites « attaques de point d'eau » ou par l'ouverture d'un fichier en pièce jointe, suffisamment bien dissimulé pour éviter toute détection précoce. Le résultat est le même dans un cas comme dans l'autre : un élément est injecté dans un processus déjà en cours d'exécution, ce qui permet au programme malveillant de fonctionner sans jamais toucher le système de fichiers, y compris charger et lancer des modules auxiliaires et commencer à se déplacer horizontalement dans l'infrastructure infectée.



Pour détecter les types de programmes malveillants avancés les plus variés, y compris ceux qui résident en mémoire vive, Kaspersky Endpoint Security intègre une fonctionnalité de surveillance du système. Cette technologie, basée sur la détection des comportements d'application suspects, surveille toute l'activité au sein d'un système donné. Avec cette approche, peu importe qu'un « corps » de fichier se cache ou non derrière le processus surveillé : tout activité malveillante sera bloquée. Les principes de détection de la surveillance du système s'appuient sur des processus de machine learning qui s'exécutent en permanence. Ces processus exploitent les informations sur les menaces recueillies par Kaspersky Security Network grâce à son traitement scientifique des statistiques obtenues dans le monde entier.

PowerShell : interprète légitime, activités illicites

Les fichiers de script shell ont longtemps été perçus comme inoffensifs. Avec un peu de créativité et d'intentions malveillantes, toutefois, ils peuvent néanmoins se transformer en véritable arme. Mais les scripts PowerShell tombent dans une catégorie à part. Leur puissance offre en effet aux attaquants un immense champ de possibilités. Télécharger des modules auxiliaires depuis Internet, exécuter des programmes malveillants sans « corps », exécuter à distance n'importe quel code sur d'autres machines du réseau, le tout sous couvert d'un utilitaire intrinsèquement inoffensif, l'interpréteur PowerShell, fourni en standard avec Windows depuis Windows 7. Parmi les adeptes les plus notoires de cette technique citons notamment les cyberbraqueurs de banque du célèbre groupe criminel Carbanak.

Kaspersky Lab n'ignore rien de cette vague d'attaques via PowerShell, ni de l'utilisation de scripts shell standard à des fins malveillantes. Les chaînes transmises à nos moteurs sont analysées attentivement et toute détection positive entraîne le blocage de l'exécution.

Mobilité

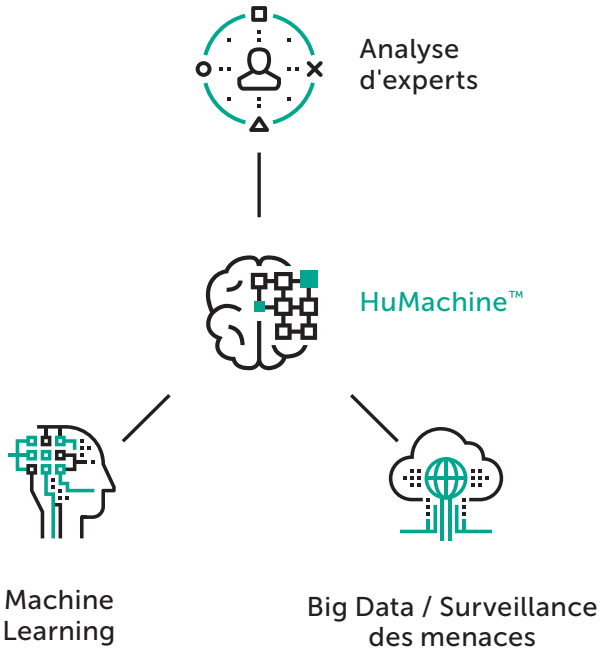
Smartphones et tablettes sont d'ores et déjà les moyens les plus utilisés pour accéder à Internet. D'ici la fin 2017, le nombre de smartphones utilisés dans le monde aura atteint les 2,1 milliards. Quelle aubaine pour les pirates ! Les appareils mobiles sont déjà très intégrés aux processus et aux flux de données des entreprises, mais pas toujours, hélas, à leurs infrastructures de cybersécurité. Des facteurs très différents (tensions géopolitiques croissantes, utilisation de plus en plus fréquente des appareils mobiles pour la gestion financière, quantité vertigineuse de données sensibles actuellement conservées sur ces appareils, entre autres) font craindre une explosion des attaques contre les mobiles. L'exploitation des failles de type « zero-day » sur les appareils mobiles à des fins de cyberespionnage est déjà une réalité. Il n'en reste pas moins que des moyens moins sophistiqués peuvent également se révéler très efficaces, surtout lorsque la victime ne s'y attend pas. En guise d'exemple, il suffit de repenser à la terrible attaque par « malvertizing » lors de laquelle un cheval de Troie bancaire a été automatiquement téléchargé lors de la consultation par l'utilisateur de certains sites liés à un grand réseau publicitaire et infectés par un programme JavaScript malveillant. L'immense majorité des smartphones Android pouvant être « rootés » sans beaucoup d'efforts (y compris par des applications factices/malveillantes), sans parler des appareils sur lesquels un programme malveillant a été directement préinstallé, les programmes malveillants système cachés sous la couche du système d'exploitation accessible à l'utilisateur sont monnaie courante.

Kaspersky Mobile Security for Business présente plusieurs couches de détection, comparables à celles des solutions pour ordinateurs de bureau. Certaines de ces couches reposent sur le machine learning et exploitent toute la puissance de notre intelligence « HuMachine ». Cette solution intègre également de puissantes couches de sécurité supplémentaires, telles que le contrôle des applications. La sécurité mobile doit s'intégrer dans un tout dont la gestion des appareils mobiles et la gestion des applications mobile. Seule une telle approche peut permettre aux entreprises d'élaborer une stratégie solide et résolument sécurisée pour leur flotte mobile.

Conclusion

Les techniques mentionnées ici, dont la liste est loin d'être exhaustive, montrent un niveau d'ingéniosité que seuls peuvent atteindre des professionnels humains chevronnés. Mais sans doute convient-il, après avoir suscité chez le lecteur tant de crainte, de doute et d'incertitude, de rappeler plusieurs points importants.

D'abord, répétons-le : **ces nouvelles techniques ne sont pas si nouvelles que cela**. L'avancée la plus digne de l'appellation « nouvelle génération » tient aux moyens de paiement et de communication intraçables, tels que la technologie Bitcoin et les réseaux de type Tor. Mais même ces technologies ont déjà une certaine ancienneté et ne sont pas intrinsèquement mauvaises. Les cybercriminels en exploitent seulement le potentiel de nuisance, comme ils le font avec tant d'autres outils légitimes.
Ces technologies sont donc connues et comprises, et les moyens de s'en prémunir existent d'ores et déjà, auprès de fournisseurs comme Kaspersky Lab. Notre approche « HuMachine », une fusion efficace entre l'acquisition des statistiques de menace, l'exploitation de la science des données reposant sur des processus d'apprentissage machine et une équipe d'experts de renommée mondiale, assure aux clients le meilleur résultat possible. Quel que soit l'aspect que prendront demain les menaces de « nouvelle génération », nous parviendrons toujours à les dévoiler et à les contrer efficacement par des techniques de protection, elles aussi de nouvelle génération. C'est là un aspect important de notre vision d'une cybersécurité sans faille.



Kaspersky Lab, **www.kaspersky.fr**
Tout savoir sur la sécurité sur Internet : **www.securelist.fr**
Rechercher un partenaire près de chez vous :
www.kaspersky.fr/partners

www.kaspersky.fr