



VERSION INTÉGRALE

# WSTR

RAPPORT 2016  
SUR LES MENACES DE  
SÉCURITÉ DES SITES WEB

# Sommaire

<b>Symantec™ Global Intelligence Network</b>	03	Diversification des botnets	37
<b>Introduction du WSTR</b>		Publicités malveillantes (malvertising)	38
Vulnérabilité des sites web aux malwares et violations de données	04	Côté client	39
Sécurité complète des sites web	04	Smartphones et terminaux mobiles	39
Événements marquants de 2015	05	• Un téléphone par personne	39
À retenir	05	• Menaces trans-terminaux	39
Renforcement des modes d'authentification	06	• Furtivité des nouvelles attaques Android	42
Raisons d'espérer	07	• Les utilisateurs Android sous le feu du phishing et des rançongiciels	42
		• Le ver est dans la pomme pour les utilisateurs d'Apple iOS	42
<b>L'année 2015 en chiffres</b>		Protection des terminaux mobiles	42
État des lieux	08	Perspectives	43
Vulnérabilités : la porte ouverte aux attaques	09	Menaces sur les e-mails et les communications	43
Menaces internes	10	• Courrier indésirable et frauduleux	43
L'odeur de l'argent	10	• Spam	44
Marché noir vs. représentants de la loi	14	• Phishing	44
• Cyberéconomie de l'ombre	14	• E-mails infectés	44
• Un business en plein boom	14	• Cryptage d'e-mails	46
• Coups de filet	14	• Attaques par contournement du cryptage	46
• Réduction des risques	15	• Conseils pour la sécurité de vos e-mails	46
		Perspectives	46
<b>Au-delà du terminal et du réseau, l'utilisateur est en ligne de mire</b>		Ordinateurs, cloud computing et infrastructure informatique	47
La méfiance est de mise	16	• Cloud et systèmes virtuels	48
Sexe, mensonges et vidéo	17	• Vulnérabilités du cloud	48
Fausse identité	18	• Protection de l'infrastructure informatique	48
Avènement de l'e-économie	18	Protégez toutes vos informations, où qu'elles se trouvent	49
Baisse de confiance des internautes	19	<b>Les acteurs de la sécurité organisent la riposte</b>	
• La bourse ou la vie	19	Évolution du cryptage	50
• Mais pourquoi les rançongiciels ont-ils à ce point les faveurs des cybercriminels ?	19	L'union fait la force	50
• Dyre : fléau de la banque en ligne	20	Équilibre des pouvoirs	51
• Hackers sans frontières	20	Transition accélérée vers Always-On SSL	51
Lois sur la confidentialité des données	21	Renforcement de la confiance	52
Prévention d'une cyber-apocalypse	22	<b>Perspectives</b>	
		À suivre	53
<b>Au-delà du terminal et du réseau, l'entreprise est en ligne de mire</b>		• Multiplication des attaques de phishing	53
Menaces APT	23	• Généralisation des pages HTTPS	53
Diversité des failles zero-day	24	• Menaces hybrides : attaques mobiles	53
Groupes d'attaques actifs en 2015	24	• Besoin croissant de compétences en sécurité	53
Terreur mondiale, attaques locales	25	Sujets d'actualité	
Délit d'initié et effet papillon	25	• Gros plan sur l'authentification	54
Cybersécurité, cybersabotage et théorie du cygne noir	27	• Internet des objets non sécurisés	54
L'obscurité n'est pas un gage de sécurité	27	• Hacktivisme, terrorisme, responsabilité des États et respect de la vie privée	54
<b>Vecteurs d'attaques</b>		TLS 1.3 – par Ivan Ristic	55
Kits, attaques web et exploitation des vulnérabilités en ligne	28	<b>Recommandations et bonnes pratiques</b>	
Linux en ligne de mire	28	Conformité aux standards du secteur	56
Problèmes de plugins	29	Usage correct du protocole SSL/TLS	56
• Flash : la fin est proche	29	Solution complète de sécurité des sites web	56
• Exploitation des plugins pour serveurs web	29	Sensibilisation de vos salariés	57
Infection par injection	29	Protection des terminaux mobiles	57
Kits d'attaques web	30	Travail d'équipe	57
Nuclear : le support technique au service des rançongiciels	31		
Déni de service distribué (DDoS)	32		
• Le DDoS en quelques mots	32		
• Simple mais efficace	34		
• Les applications web connectées de plus en plus dans la tourmente	36		

## Symantec™ Global Intelligence Network

Symantec dispose du système de cyberveille le plus exhaustif de la planète. Son nom : Symantec™ Global Intelligence Network. Doté de plus de 63,8 millions de détecteurs d'attaques, cet observatoire enregistre des milliers d'événements à la seconde.

Pour surveiller l'activité sur le front des menaces dans plus de 157 pays et territoires, le Global Intelligence Network exploite toutes les synergies des produits et services Symantec. Parmi eux :

- Symantec DeepSight™ Intelligence
- Symantec™ Managed Security Services
- Produits Norton™ grand public
- Symantec Website Security

Il recourt également à des sources de données externes. Symantec gère par ailleurs l'une des bases de données de vulnérabilités les plus complètes au monde, avec à ce jour plus de 74 180 vulnérabilités répertoriées (pendant plus de 20 ans) sur plus de 71 470 produits développés par plus de 23 980 constructeurs informatiques et éditeurs de logiciels.

### Nos statistiques sur les spams, le hameçonnage (phishing) et les malwares proviennent de diverses sources :

- Symantec Probe Network, un système de plus de 5 millions de comptes leurrés
- Symantec.cloud
- Symantec Website Security
- Plusieurs autres technologies de sécurité signées Symantec

Skeptic™, la technologie heuristique développée par Symantec.cloud, est capable de détecter de nouvelles menaces ciblées et ultra perfectionnées en amont, avant qu'elles ne frappent les réseaux des clients. Plus de 9 milliards de messages électroniques sont ainsi traités chaque mois, tandis que plus de 1,8 milliard de requêtes web sont filtrées chaque jour dans 13 data centers. Symantec assure également une veille des activités de phishing à travers un vaste écosystème d'entreprises, d'éditeurs de solutions de sécurité et plus de 50 millions de consommateurs.

Sans interruption de service depuis 2004, Symantec Website Security protège plus d'un million de serveurs web dans le monde. L'infrastructure de validation traite au quotidien plus de 6 milliards de recherches OCSP (Online Certificate Status Protocol), utilisées pour vérifier l'éventuelle révocation de certificats numériques X.509 à travers le monde.



Chaque jour, le sceau Norton™ Secured apparaît près d'un milliard de fois sur les sites web de 170 pays, mais aussi dans certains moteurs de recherche sur les navigateurs compatibles.

Forts de ces ressources exclusives d'une richesse incomparable, les analystes Symantec ont pu identifier, analyser et commenter les dernières tendances en matière d'attaques, de propagation de codes malveillants, de phishing et de spam. Le tout a ensuite été compilé dans le rapport annuel Symantec sur les menaces de sécurité par Internet (Internet Security Threat Report) qui synthétise les informations indispensables à une sécurisation efficace des systèmes de particuliers et d'entreprises de toutes tailles – aujourd'hui comme demain.

## Introduction duWSTR

---

Shopping, impôts, travail... toute notre existence tourne désormais autour des services en ligne et de la confiance que nous y accordons. La bonne nouvelle, c'est que de nouveaux modes d'utilisation et de sécurisation d'Internet sont appelés à renforcer cette confiance dans la confidentialité des données et la sécurité des transactions en ligne. La sécurité des sites web ne se limite pas au simple transfert d'informations entre vos serveurs et les terminaux des internautes. C'est pourquoi les entreprises doivent reconsidérer leur site web comme partie intégrante d'un vaste écosystème qui requiert une attention de tous les instants. Il en va de la confiance même des internautes.

Au vu de la généralisation de l'e-commerce dans le quotidien de tout un chacun, l'enjeu est de taille. Des courses de la semaine à la réservation de nos prochaines vacances d'été, nous effectuons de plus en plus de transactions en ligne. Concrètement, d'après l'organisme européen [Ecommerce Europe](#), en 2014, le chiffre d'affaires mondial de l'e-commerce B2C a augmenté de 24 % pour atteindre 1 943 milliards de dollars (1 766 milliards d'euros). Quant aux transactions B2B en ligne, elles devraient peser 6 700 milliards de dollars (6090 milliards d'euros) d'ici à 2020. Dans ce contexte, jamais la sécurité des sites web n'a revêtu une telle importance.

Un site mal protégé ne représente pas seulement un coût pour l'entreprise qui l'exploite, il contribue à éroder la confiance du public et à pénaliser l'économie dans son ensemble.

### Vulnérabilité des sites web aux malwares et violations de données

Les sites web représentent un point de passage presque obligé dans les attaques d'envergure, sorte de porte d'entrée vers votre réseau, vos données et vos clients et partenaires.

Ainsi, l'émergence de malwares ciblant les serveurs web Linux – notamment chez les hébergeurs de sites web – est la preuve criante qu'aux yeux des cybercriminels, l'infrastructure sous-jacente s'avère aussi, voire plus précieuse que les informations cryptées par des certificats SSL/TLS.

Une maintenance régulière des serveurs suffirait pourtant à bloquer bon nombre d'attaques, mais les chiffres indiquent que les propriétaires de sites web peinent à tenir le rythme.

Ainsi, en 2015, les trois quarts des sites web analysés par Symantec comportaient des vulnérabilités, un chiffre

désespérément stable depuis des années. Au lieu de ne penser que protection, les responsables de sites doivent également envisager leur sécurité sous l'angle de la détection et de l'intervention. Ils doivent pour cela utiliser des outils automatisés qui surveillent leurs sites en permanence pour détecter d'éventuelles vulnérabilités, repérer les menaces, neutraliser les attaques, créer des rapports, et enfin mettre à jour et corriger les systèmes en conséquence.

### Sécurité complète des sites web

En 2015, les cybercriminels ont encore trouvé des failles dans l'infrastructure des sites web. À commencer par FREAK, une méthode qui permet aux pirates d'intervenir au moment de l'ouverture d'une connexion sécurisée afin de forcer l'utilisation d'un protocole plus faible, et donc plus facile à décrypter.

Certes, les bibliothèques de protocoles SSL/TLS comme OpenSSL publient régulièrement des mises à jour pour combler de telles failles. Mais encore faut-il les installer. Dans une même logique, la migration des certificats SHA-1 vers les certificats SHA-2 s'accélère. Toutefois, là encore, les entreprises doivent déployer les nouveaux certificats correctement afin de garantir leur efficacité.

En 2015, les attaques par déni de service distribué (DDoS) ont continué d'exercer leur pouvoir de nuisance sur les entreprises. Bien que seules les attaques de grande ampleur, comme celle qui a touché la BBC à la fin de l'année 2015, tendent à faire les gros titres, la menace touche des entreprises de toutes tailles. De fait, lorsqu'un hébergeur doit déconnecter plusieurs serveurs pour protéger un client victime d'une attaque, les autres sites présents sur ces serveurs feront fatalement partie des victimes collatérales.

[www.ecommerce-europe.eu/news/2015/global-e-commerce-turnover-grew-by-24.0-to-reach-1943bn-in-2014](http://www.ecommerce-europe.eu/news/2015/global-e-commerce-turnover-grew-by-24.0-to-reach-1943bn-in-2014)  
[www.frost.com/sublib/display-report.do?id=MA4E-01-00-00-00](http://www.frost.com/sublib/display-report.do?id=MA4E-01-00-00-00)  
[www.bbc.co.uk/news/technology-35204915](http://www.bbc.co.uk/news/technology-35204915)

Le message est clair : les entreprises doivent se montrer plus proactives dans leur implémentation du protocole SSL/TLS. Puisqu'il ne s'agit pas d'une tâche ponctuelle mais d'un travail de longue haleine, il est essentiel de recourir à des outils qui automatisent et rationalisent le processus.

### Événements marquants de 2015

- Le prix des données volées (adresses e-mail, numéros de cartes bancaires, etc.) a chuté, signe d'une offre de plus en plus abondante.
- La Chine a été à l'origine de 46 % de l'activité des bots malveillants (contre 16 % en 2014), tandis les États-Unis tombaient à 8 %, contre 16 % l'année précédente.
- Les déclarations de cybersinistres sont devenues plus courantes, avec pour effet la hausse du montant des primes et du coût total des violations de données. L'étude annuelle [NetDiligence](#) a recensé des déclarations pouvant atteindre 15 millions de dollars (13,6 millions d'euros), tandis que la plupart se situaient dans une fourchette comprise entre 30 000 \$ et 263 000 \$ (27 000 € et 240 000 €).
- Le nombre médian d'identités exposées par violation a diminué d'environ 33 % pour s'établir à 4885. Toutefois, on note une augmentation de 85 % du nombre de cas pour lesquels la quantité d'identités exposées reste inconnue.
- Parmi les victimes figure Hacking Team, une entreprise italienne qui travaille pour divers États au développement de logiciels de surveillance et d'espionnage. Dans la foulée, un certain nombre de ses exploits se sont retrouvés sur le Net, avant d'être intégrés dans des kits d'attaques web.
- Tout comme les attaques contre les serveurs d'hébergement Linux, les publicités malveillantes (malvertising) continuent de faire des ravages, comme en témoigne l'augmentation du nombre de sites infectés cette année.
- Les attaques à l'encontre des acteurs de la santé et des assurances se sont multipliées, avec notamment près de 80 millions de dossiers de patients exposés lors d'une seule attaque chez le prestataire de soins Anthem. En 2015, la santé est arrivée en tête des secteurs les plus touchés.
- Si des attaques sophistiquées, perpétrées par des organisations suspectées d'agir pour le compte d'États, ne sont pas nouvelles, 2015 a en revanche vu l'apparition de Butterfly, un groupe de hackers aux motivations purement commerciales.

- Des attaques contre des voitures, des appareils domestiques et médicaux connectés, mais aussi des systèmes de contrôle industriels, ont mis en lumière les problèmes de sécurité posés par l'Internet des objets.
- L'explosion des vulnérabilités sur les terminaux mobiles et la hausse de nombre d'applis malveillantes sur Android ont exposé les téléphones à un flux ininterrompu d'attaques. Pour la première fois, ces menaces plus discrètes et plus sophistiquées ont même compromis des terminaux Apple iOS non débridés.
- Si l'année 2015 a enregistré une baisse du nombre de rançongiciels génériques, les attaques par crypto-rançongiciels sont en revanche à la hausse. Ces dernières ont même ciblé des serveurs Linux d'hébergement de sites web et des smartphones. Enfin, on sait maintenant que les [smart TV](#) et les montres connectées ne sont pas à l'abri.
- Ensemble, la hausse des cas de sextorsion en Asie et l'onde de choc de la violation de sécurité du site de rencontres extra-conjugales Ashley Madison ont donné une toute nouvelle dimension à l'exploitation des informations personnelles volées à des fins financières.

Des méthodes et des outils anti-DDoS existent. Mais au final, la sécurité d'un site web dépend de l'assiduité avec laquelle ils sont mis en œuvre.

### À retenir

En 2015, les vulnérabilités zero-day ont atteint des niveaux sans précédent. Outre leurs cibles habituelles (plugins web, systèmes d'exploitation, etc.), les pirates ont eu recours aux zero-day sur de nouveaux fronts comme les logiciels open source. Pire encore, de graves vulnérabilités zero-day touchant les systèmes de contrôle industriels ont été découvertes.

L'année dernière, les travaux de reconnaissance ont encore joué un rôle déterminant dans les attaques ciblées. Ces repérages permettent aux pirates de collecter discrètement des informations sur les systèmes ciblés avant de lancer des attaques d'envergure. De grandes opérations de cybersabotage comme celles basées sur les chevaux de Troie Trojan. Laziok et BlackEnergy, respectivement à l'encontre du secteur de l'énergie du Moyen-Orient et des centrales électriques ukrainiennes, doivent beaucoup à ces attaques.

Quant aux violations de données, presque tous les chiffres sont unanimes : l'année 2015 a enregistré un nombre record d'attaques, d'identités volées et de méga-intrusions. Du côté des violations de sécurité à haut risque, des secteurs d'activité comme l'hôtellerie et les assurances bénéficient d'une attractivité dont ils se passeraient bien. Ciblées pour les informations privées (numéros de cartes bancaires, dossiers médicaux, etc.) qu'elles stockent, ces industries sont davantage sous le feu des pirates que d'autres.

### Renforcement des modes d'authentification

Tout dans ce tableau n'est pas si sombre. En 2015, les certificats SSL/TLS ont continué de gagner du terrain, tant en termes d'efficacité que d'adoption. En parallèle, les Autorités de Certification (AC) ont œuvré pour plus de transparence dans l'émission de certificats.

Mieux encore, d'après [une étude de Sandvine](#), aux États-Unis, près de 40 % de tout le trafic Internet aval est désormais crypté, tandis que les prévisionnistes tablent sur plus de 70 % d'ici la fin de l'année prochaine.

Toutefois, comme le souligne Robert Hoblit, Vice-président des produits émergents chez Symantec : « dans un monde où tout est crypté, les consommateurs pensent à tort que, chaque fois qu'ils voient le préfixe HTTPS, ils sont en sécurité, sur un site hébergé par une entreprise légitime et authentifiée ».

En réalité, la grande majorité des fraudes se produit sur [des sites dotés de certificats de validation de domaine \(DV\)](#), qui ne garantissent en rien l'identité de l'exploitant du site. Pour M. Hoblit, « les contraintes de mise en conformité aux directives PCI vont pousser les entreprises à resserrer leurs exigences en matière d'authentification ».

Dans le cas d'un certificat DV, l'AC confirme la demande de certificat auprès d'un contact chez l'exploitant du domaine en question, généralement par téléphone ou par e-mail, et souvent de façon automatisée. C'est pourquoi ces certificats sont pour la plupart moins chers que les certificats SSL Extended Validation (EV), qui impliquent un processus de vérification et de validation plus poussé et rigoureux.

Bien que la procédure d'émission de certificats DV demande le consentement du propriétaire du domaine concerné, elle ne prévoit en revanche aucune authentification de ce dernier, ce qui en fait un outil idéal pour les attaques de phishing et d'interception (Man-In-The-Middle, MITM). Toutefois, Symantec prédit une réaction des entreprises, en particulier celles soumises aux directives PCI, en faveur d'un renforcement de leurs modes d'authentification et de l'adoption de certificats SSL EV pour des niveaux de garantie supérieurs.

Avec le passage de SHA-1 à SHA-2, le cryptage SSL/TLS gagnera aussi en puissance. Historiquement, les certificats SHA-1 ont toujours intégré une fonction de hachage unidirectionnelle, qui génère une valeur de hachage unique à partir de chaque source. En d'autres termes, deux sources différentes ne devraient jamais générer la même valeur. Toutefois, dès 2005, les premières failles sont apparues dans cet algorithme. Depuis, les choses se sont détériorées jusqu'à [l'annonce par Google](#) en 2014 de la fin du support des sites utilisant SHA-1, avec en corollaire des messages de mise en garde des internautes tentant d'accéder à des pages protégées par des certificats SHA-1 encore valides après le 1<sup>er</sup> janvier 2017. Plusieurs autres éditeurs de navigateurs lui ont emboîté le pas, signant ainsi l'arrêt de mort de SHA-1.

En somme, l'industrie de la sécurité a entrepris un réel travail de fond qui laisse entrevoir une baisse considérable du taux de réussite des attaques à l'encontre des sites web. Mais encore faut-il que les propriétaires de sites jouent vraiment le jeu.

### Raisons d'espérer

En dépit du pessimisme ambiant et hormis les cas d'attaques ultrasophistiquées, les entreprises bien gérées et les utilisateurs attentifs ont les moyens de se prémunir contre toutes les menaces. Et ce n'est pas tout ! Par exemple, aux États-Unis, près de 40 % de tout le trafic Internet aval est désormais crypté, un chiffre qui grossira encore d'ici la fin de l'année. Les derniers standards web et les versions récentes des navigateurs mettent l'accent sur le cryptage et la sécurité.

Dans cette même veine, les développeurs de téléphones, de logiciels et de technologies IoT ont élevé leur niveau de jeu en matière de sécurité (quoique certains partent de loin). Enfin, bien entendu, des entreprises comme Symantec jettent toutes leurs forces dans la bataille contre les espions, cybercriminels et autres escrocs sur Net.



**DANS UN MONDE OÙ TOUT EST  
CRYPTÉ, LES CONSOMMATEURS  
PENSENT À TORT QUE LE PRÉFIXE  
HTTPS LEUR PROCURE LA  
SÉCURITÉ D'UN SITE LÉGITIME  
ET AUTHENTIFIÉ.**



Robert Hoblit, Vice-président des produits émergents chez Symantec

## L'année 2015 en chiffres

Menaces internes ou cybercriminels, sites web ou terminaux de points de vente : les violations de données se sont accélérées en 2015, avec une facture plus lourde que jamais pour leurs victimes.

### État des lieux

Selon l'étude 2015 sur le coût des violations de données, ces deux dernières années, le coût total moyen de ce type d'incident a connu une hausse de 23 % pour atteindre 3,79 millions de dollars (3,45 millions d'euros). Vu que, dans le même temps, le nombre total d'intrusions a légèrement baissé et que le nombre médian d'identités exposées par violation a chuté d'environ 33 % pour s'établir à 4 885, on peut en déduire que les données exfiltrées ont une valeur ou un niveau de sensibilité tels que le préjudice est plus grave pour les entreprises victimes.

#### NOMBRE TOTAL DE VIOLATIONS

Source : Symantec | CCI



2015	Évolution	2014	Évolution	2013
305	-2 %	312	+23 %	253

#### NOMBRE TOTAL D'IDENTITÉS EXPOSÉES

Source : Symantec | CCI



2015	Évolution	2014	Évolution	2013
429 millions	+23 %	348 millions	-37 %	552 millions

Résultat : les déclarations de cybersinistres sont devenues plus courantes. Ainsi, une étude NetDiligence de cette année a recensé des déclarations pouvant atteindre 15 millions de dollars (13,6 millions d'euros), tandis que la plupart se situent dans une fourchette comprise entre 30 000 \$ et 263 000 \$ (27 000 € et 240 000 €). Qui dit plus de sinistres dit aussi hausse des primes de cyber-assurance, et donc du coût global des violations de données.

Dans le secteur de la grande distribution, cette augmentation des primes a même atteint 32 % au premier semestre 2015, tandis que le secteur de la santé a vu certaines primes tripler. Reuters fait également état d'une augmentation des franchises, et même d'un plafonnement des polices à 100 millions de dollars sur des clients à risques dans certaines grandes compagnies d'assurance.

## Vulnérabilités : la porte ouverte aux attaques

En 2015, en dépit du renforcement du cryptage, de nombreuses attaques à l'encontre du protocole SSL/TLS se sont concentrées sur les failles de l'écosystème SSL/TLS au sens large.

« L'année dernière, l'attention s'est davantage tournée vers les bibliothèques de code sur lesquelles reposent les implémentations SSL/TLS », explique Michael Klieman, Directeur général de la gestion produits chez Symantec. « En conséquence, nous avons observé un flux relativement régulier de mises à jour et correctifs. »

Certes, c'est une bonne nouvelle. Mais au vu des vulnérabilités les plus couramment constatées sur les serveurs web l'an passé, les propriétaires de sites ne parviennent pas à appliquer les correctifs au rythme de leur publication.

Pourtant, il est vital pour eux de maintenir l'intégrité de leurs implémentations SSL/TLS. Une fois un certificat installé, leur travail ne fait que commencer.

Bien qu'aucune vulnérabilité aussi nocive que la faille Heartbleed de 2014 ne soit apparue, OpenSSL a publié plusieurs mises à jour et correctifs tout au long de l'année 2015. Présente sur deux tiers des sites web de la planète, OpenSSL est l'une des implémentations les plus répandues des protocoles cryptographiques SSL et TLS. Les mises à jour publiées sont venues combler des failles allant de minimales à sévères pour prévenir des attaques par interception (Man In The Middle), l'espionnage de communications sécurisées, ou encore des attaques par déni de service (DoS).

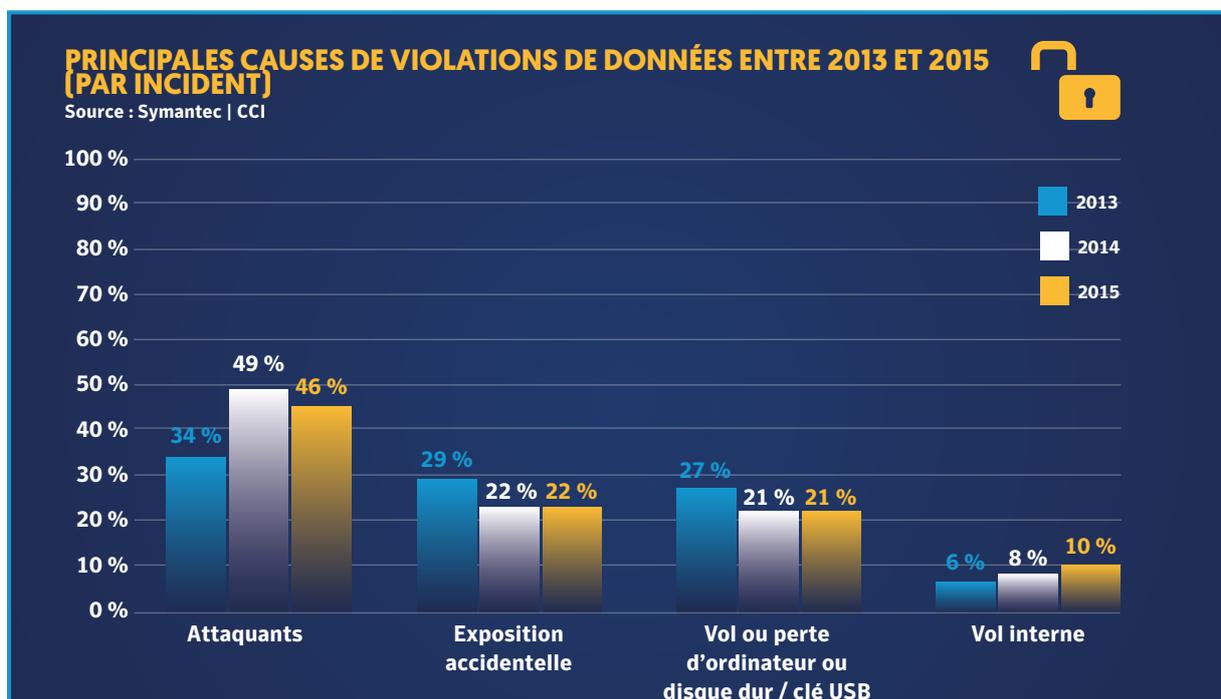
## TOP 10 DES VULNÉRABILITÉS NON CORRIGÉES DÉTECTÉES SUR LES SERVEURS WEB DIAGNOSTIQUÉS

Source : Symantec | Services de confiance



Classement	Nom
1	Vulnérabilité Poodle SSL/TLS
2	En-tête X-Content-Type-Options manquant
3	En-tête X-Frame-Options manquant
4	Certificat SSL signé à l'aide d'un algorithme de hachage faible
5	Vulnérabilité cross-site scripting (XSS)
6	En-tête Strict-Transport-Security manquant
7	Détection de la prise en charge du SSL v2
8	Attributs de sécurité manquants dans un cookie de session cryptée (SSL)
9	Prise en charge de suites de cryptage SSL faibles
10	Vulnérabilité de renégociation des protocoles SSL et TLS

<http://www.symantec.com/connect/blogs/critical-openssl-vulnerability-could-allow-attackers-intercept-secure-communications>  
<http://www.symantec.com/connect/blogs/new-openssl-vulnerability-could-facilitate-dos-attacks>



#### Menaces internes

Bien que les vols en interne n'ont représenté que 10 % des violations de données en 2015, l'étude [NetDiligence](#) a recensé des complicités en interne dans 32 % des cybercriministes déclarés sur la même année. D'après son PDG, [un col-laborateur mécontent](#) serait même à l'origine de la violation de données la plus retentissante de l'année, celle du site Ashley Madison. Si ces allégations venaient à se confirmer, l'incident illustrerait alors parfaitement les dégâts qu'un salarié malveillant peut infliger à sa propre entreprise.

Si la menace interne a toujours beaucoup fait parler d'elle, en 2015, les pouvoirs publics ne se sont pas seulement contentés d'étudier la question, ils ont aussi agi.

- Ainsi, plus des trois quarts des agences gouvernementales US interrogées pour le [rapport MeriTalk sur les menaces fédérales internes](#) affirment qu'elles prêtent davantage d'attention aux menaces internes aujourd'hui qu'il y a un an.
- En 2015, le Centre for Defence Enterprise britannique a soutenu plusieurs projets destinés à surveiller le [comportement numérique des salariés](#) afin de prédire et [identifier les menaces internes](#) en temps réel, mais aussi à créer [des simulateurs](#) pour la formation à la détection des risques.

[http://netdiligence.com/downloads/NetDiligence\\_2015\\_Cyber\\_Claims\\_Study\\_093015.pdf](http://netdiligence.com/downloads/NetDiligence_2015_Cyber_Claims_Study_093015.pdf)  
<http://uk.businessinsider.com/ashley-madison-ceo-says-hack-was-an-inside-job-2015-7>  
[http://cdn2.hubspot.net/hubfs/407136/PDFs/Symantec/MeriTalk\\_-\\_Symantec\\_-\\_Inside\\_Job\\_Report\\_-\\_FINAL.pdf?t=1445970735623](http://cdn2.hubspot.net/hubfs/407136/PDFs/Symantec/MeriTalk_-_Symantec_-_Inside_Job_Report_-_FINAL.pdf?t=1445970735623)  
<https://www.gov.uk/government/news/protecting-information-from-an-insider-threat>  
<https://www.gov.uk/government/news/identifying-cyber-insider-threats-in-real-time>  
<https://www.gov.uk/government/news/securing-against-the-insider-threat>

#### L'odeur de l'argent

En matière de violations de données, l'argent reste la motivation première : plus un pirate accumule d'informations sur une victime, plus il lui sera facile d'usurper son identité. C'est pourquoi les cybercriminels s'en prennent plus particulièrement aux assurances, administrations et structures de santé.

En 2015, les types d'informations exposées aux hackers n'ont pas changé, mis à part quelques mouvements mineurs dans leur classement. Ainsi, les noms réels restent le type d'informations le plus couramment exposées, puisque présents dans plus de 78 % des cas de violations de données. Comme en 2014, les adresses postales, les dates de naissance, les numéros d'identification auprès d'organismes publics (par ex., sécurité sociale), les dossiers médicaux et les informations financières figurent tous dans 30 % à 50 % des cas d'intrusions. Toutefois, leur classement diffère légèrement. En queue du Top 10, les adresses e-mail, les numéros de téléphone, les informations d'assurance et les noms d'utilisateur/mots de passe sont encore une fois présents dans 10 % à 30 % des cas.

Non pas que les données de cartes bancaires n'ont plus la cote. Certes, au marché noir, la valeur unitaire de ces données n'est pas très élevée, leur durée de vie étant réduite par la capacité des émetteurs de cartes à vite repérer les comportements d'achat anormaux (tout comme les détenteurs). Toutefois, l'activité reste soutenue sur ce front.

## TOP 10 DES SECTEURS LES PLUS TOUCHÉS PAR DES VIOLATIONS DE DONNÉES (PAR NOMBRE ET POURCENTAGE D'IDENTITÉS EXPOSÉES)

Source : Symantec | CCI



Classement	Secteur	Nombre d'identités exposées	Pourcentage d'identités exposées
1	Services sociaux	191 035 533	44,5 %
2	Compagnies d'assurance	100 436 696	23,4 %
3	Services aux personnes	40 500 000	9,4 %
4	Gestion des ressources humaines	21 501 622	5,0 %
5	Agents, courtiers et services en assurance	19 600 000	4,6 %
6	Services aux entreprises	18 519 941	4,3 %
7	Commerce de gros - Biens durables	11 787 795	2,7 %
8	Exécutif, législatif et général	6 017 518	1,4 %
9	Éducation et formation	5 012 300	1,2 %
10	Services de santé	4 154 226	1,0 %

## TOP 10 DES TYPES D'INFORMATIONS EXPOSÉES

Source : Symantec | CCI



Classement	Type en 2015	% en 2015	Type en 2014	% en 2014
1	Noms réels	78,3 %	Noms réels	68,9 %
2	Adresses postales	43,7 %	Numéros d'identification auprès d'organismes publics (par ex., sécurité sociale)	44,9 %
3	Dates de naissance	41,2 %	Adresses postales	42,9 %
4	Numéros d'identification auprès d'organismes publics (par ex., sécurité sociale)	38,4 %	Informations financières	35,5 %
5	Dossiers médicaux	36,2 %	Dates de naissance	34,9 %
6	Informations financières	33,3 %	Dossiers médicaux	33,7 %
7	Adresses e-mail	20,8 %	Numéros de téléphone	21,2 %
8	Numéros de téléphone	18,6 %	Adresses e-mail	19,6 %
9	Assurance	13,2 %	Noms d'utilisateurs et mots de passe	12,8 %
10	Noms d'utilisateurs et mots de passe	11,0 %	Assurance	11,2 %

Un examen des branches d'activité au sens large permet de constater que le secteur des services a subi le plus de violations de sécurité, tant en nombre d'incidents qu'en quantité d'identités exposées. Toutefois, pour chaque sous-catégorie de ces grandes branches, les raisons diffèrent.

Les services de santé enregistrent ainsi le plus grand nombre d'intrusions, avec 39 % de toutes les violations recensées en 2015. Rien d'étonnant au regard des règles strictes de signalement des incidents auxquelles sont soumis les acteurs de la santé. Cependant, le nombre d'identités exposées s'y avère relativement bas. Si les pirates se donnent la peine, c'est donc que ces données valent de l'or.

Au rang du plus grand nombre d'identités exposées, on trouve les services sociaux. Ce chiffre s'explique toutefois largement par le vol de 191 millions d'identités lors d'une seule et même violation de données record. Si l'on fait abstraction de cette intrusion, ce sous-secteur chute en bas de classement, place qu'il occupe déjà dans la liste des secteurs ayant subi le plus de violations de sécurité.

La grande distribution reste un secteur lucratif pour les cybercriminels, même si, avec l'introduction du standard EMV, c'est-à-dire des cartes à puce avec code PIN pour remplacer la signature aux États-Unis, les informations que les pirates pourront exfiltrer des terminaux de points de vente perdront de leur valeur.

Dans certains pays, le format des cartes à puces est utilisé depuis les années 90 ou le début des années 2000. Appelé EMV, ce standard international sert à authentifier les transactions de ces cartes avec code PIN. À la suite des nombreuses violations de données massives de ces dernières années et de la multiplication des fraudes à la carte bancaire, les émetteurs de cartes aux États-Unis ont décidé de migrer vers cette technologie afin de réduire l'impact de telles arnaques.

Auparavant, les cybercriminels pouvaient accéder aux données de la piste ISO-2, soit celles stockées sur la piste magnétique de la carte. Ainsi, ils pouvaient cloner les cartes bancaires plus facilement et les utiliser en magasin, voire même aux distributeurs de billets s'ils avaient le code PIN.

La piste ISO-1 contient plus d'informations que la piste ISO-2, y compris le nom du titulaire de la carte, son numéro de compte et d'autres données facultatives. Il arrive que les compagnies aériennes l'utilisent pour garantir les réservations par carte bancaire.

La valeur de ces données se reflète dans leur prix de vente sur le Dark Net, où des données de piste ISO-2 peuvent coûter jusqu'à 100 \$, soit 91 € par carte. Au mois d'octobre 2015, 40 % des consommateurs américains possédaient des cartes conformes au standard EMV, mais seuls 25 % des commerçants étaient équipés de terminaux de paiement compatibles.

Toutefois, le passage au standard EMV complique grandement le clonage des cartes. Bien que cette transition risque de prendre quelques années, si l'on prend aussi en compte le renforcement de la sécurité sur les points de vente, les vols de grande ampleur de données de ce type devraient se compliquer et perdre de leur rentabilité pour les cybercriminels.

Reste à savoir le risque que représentent vraiment les violations de données. Lorsqu'un secteur d'activité subit un grand nombre de violations de sécurité ou expose de nombreuses identités, ces données sont-elles toujours exploitées à des fins malveillantes ?

On sait par exemple que dans 48 % des cas, les données sont exposées par accident. Erreur dans le destinataire de certaines informations, mauvaise configuration d'un site web entraînant l'affichage de données privées par inadvertance... ces incidents ont effectivement exposé des données personnelles. La question est de savoir si ces dernières se sont retrouvées dans les mains de personnes mal intentionnées. Dans beaucoup de cas, la réponse est non. Lorsqu'une grand-mère retraitée reçoit accidentellement le dossier médical d'un autre patient par e-mail, il est peu probable qu'elle usurpe l'identité de ce dernier. Non pas que cela ne se produise jamais, mais la grande majorité des expositions de ce type représentent un risque minime.

Vos données courent un danger bien plus grand lorsque des hackers ou un collaborateur malveillant sont à l'origine de la violation de sécurité. Dans ces cas de figure, l'intention est presque toujours de faire main basse sur les données.

<http://www.symantec.com/connect/blogs/demystifying-point-sale-malware-and-attacks>  
<http://www.usatoday.com/story/money/personalfinance/2015/09/30/chip-credit-card-deadline/73043464/>  
<http://arstechnica.com/business/2015/10/today-all-stores-in-the-us-should-accept-chip-and-pin-cards-yeah-right/>

## Une attaque bien peu ordinaire

En 2015, l'attaque lancée contre Hacking Team s'est distinguée des autres dans la mesure où ses auteurs ne couraient ni après de l'argent ou des identités, mais du cyberarmement. On parle donc ici d'un cas unique de piratage entre pirates.

L'entreprise italienne Hacking Team se spécialise en effet dans le développement de logiciels de surveillance et d'espionnage qu'elle revend ensuite à des États.

L'attaque a exposé des exploits zero-day encore inconnus que les pirates se sont empressés de rendre publics.

Au bout de quelques jours seulement, des informations circulaient sur des exploits zero-day « armés » et de nombreux chevaux de Troie utilisés par le groupe. Quelques heures plus tard, des auteurs de kits les avaient déjà intégrés à leur arsenal.



## Marché noir vs. représentants de la loi

Où qu'ils se trouvent, les cybercriminels sont maintenant de plus en plus rattrapés par la justice. De fait, malgré un marché noir florissant et une prolifération de la cybercriminalité, l'année 2015 a été le théâtre d'un nombre croissant d'arrestations et d'opérations de démantèlement de grande envergure. Côté rançongiciel, si les attaques ont diminué, c'est aussi pour mieux se diversifier. Parmi leurs nouvelles cibles : les serveurs web Linux.

### Cyberéconomie de l'ombre

Les cybercriminels se professionnalisent et font preuve de plus d'audace, non seulement dans le choix de leurs cibles, mais aussi dans les montants qu'ils convoitent. Ces entreprises criminelles qui se voient comme les acteurs d'un secteur pleinement opérationnel couvrent une multitude de domaines, chacun avec ses propres spécialités. Tout comme les entreprises légitimes, elles ont des partenaires, des associés, des revendeurs, des fournisseurs, etc.

### Un business en plein boom

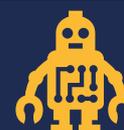
Tandis que le [prix des adresses e-mails](#) sur le marché noir a chuté ces dernières années, celui des cartes bancaires

reste relativement bas mais stable. Toutefois, associées à des données « de luxe » – confirmation que les comptes du vendeur sont encore actifs ou que la carte n'a pas encore été bloquée – elles valent désormais de l'or.

Côté « outillage », un kit d'attaque drive-by se loue entre 100 et 700 dollars la semaine (entre 91 et 637 euros), mises à jour et assistance 24h/7j incluses. Les attaques DDoS, elles, se monnaient entre 10 et 1000 dollars par jour (entre 9 et 910 euros). Dans le haut de gamme, le prix d'une vulnérabilité zero-day peut atteindre des centaines de milliers de dollars. On note par ailleurs que ces chiffres ont peu changé depuis 2014.

## TOP 10 DES ACTIVITÉS MALVEILLANTES PAR SOURCE : BOTS, 2014 – 2015

Source : Symantec | GIN



Classement	Pays/Région en 2015	Pourcentage de bots en 2015	Classement	Pays/Région en 2014	Pourcentage de bots en 2014
1	Chine	46,1 %	1	Chine	16,5 %
2	États-Unis	8,0 %	2	États-Unis	16,1 %
3	Taiïwan	5,8 %	3	Taiïwan	8,5 %
4	Turquie	4,5 %	4	Italie	5,5 %
5	Italie	2,4 %	5	Hongrie	4,9 %
6	Hongrie	2,2 %	6	Brésil	4,3 %
7	Allemagne	2,0 %	7	Japon	3,4 %
8	Brésil	2,0 %	8	Allemagne	3,1 %
9	France	1,7 %	9	Canada	3,0 %
10	Espagne	1,7 %	10	Pologne	2,8 %

### Coups de file

« L'année dernière, les autorités ont gagné en efficacité dans leur lutte contre ces groupes », affirme Dick O'Brien, Développeur informatique senior chez Symantec. « Ce combat nécessite une action internationale coordonnée car les membres des groupes d'attaques se situent rarement tous dans un même pays. Toutefois, les coups de filets font mal aux pirates et augmentent les risques et les coûts potentiels de leurs méfaits. »

<http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>

#### Au tableau de chasse des autorités en 2015 :

- **Démantèlement de Dridex.** En octobre, le botnet Dridex spécialisé dans le vol d'informations bancaires a été la cible d'une opération de police internationale qui a conduit à l'inculpation d'un homme. Au final, les autorités ont pu siphonner des milliers d'ordinateurs compromis pour les libérer du contrôle du botnet.
- **Fermeture de Simda.** En avril, l'infrastructure des auteurs du botnet Simda, y compris un certain nombre de serveurs de commande et contrôle (CnC), a été saisie par les autorités.
- **Saisie de Ramnit.** En février, une opération de police conduite par Europol, avec notamment le concours de Symantec et Microsoft, a permis la saisie de serveurs et autres éléments d'infrastructure détenus par le groupe de cybercriminels derrière le botnet Ramnit.
- **Inculpation des responsables présumés du piratage de JP Morgan Chase.** Les autorités fédérales américaines ont inculpé au moins quatre hommes en lien avec des incidents de piratage ayant conduit au vol de plus de 100 millions de dossiers clients. Ces quatre hommes sont accusés du piratage de plusieurs établissements financiers, ainsi que de fraude boursière.

#### Réduction des risques

Il n'en reste pas moins qu'un grand nombre de violations de données pourraient être évité par la simple application de quelques règles de bon sens :

- Correction des vulnérabilités
- Maintenance logicielle à jour
- Déploiement de filtres efficaces sur les messageries
- Utilisation de logiciels de prévention et de détection des intrusions
- Restrictions d'accès aux données de l'entreprise par des tiers
- Protection de données par cryptage le cas échéant
- Mise en place de technologies DLP (prévention de la perte de données)

Bien entendu, il s'agit là exclusivement de mesures de prévention des attaques externes. Pour ce qui est des risques internes d'exfiltration accidentelle ou intentionnelle, les entreprises doivent se concentrer sur la sensibilisation de leurs collaborateurs et les mesures de prévention des pertes de données.

Elles devront ainsi inculquer quelques règles « d'hygiène sécuritaire » de base à leurs salariés, dans la même veine que les actions de santé publique qui nous incitent à nous couvrir la bouche lorsque nous toussons ou à désinfecter nos mains dans les hôpitaux. Les entreprises devront également recourir aux outils de prévention des pertes de données pour localiser, suivre et protéger leurs données – où qu'elles se trouvent dans l'entreprise. L'objectif est ici de savoir en temps réel qui fait quoi et avec quelles données.

En somme, la sécurité devrait faire partie intégrante de l'action et du comportement des salariés, et non se limiter à une simple option ou une case à cocher dans les audits. Les violations de données ne risquent pas de disparaître de sitôt. Mais leur ampleur et leur impact pourraient certainement diminuer si les entreprises prenaient conscience du fait que la sécurité informatique n'est pas de la seule responsabilité des DSI ou responsables IT, mais qu'elle dépend de tout un chacun.

## Au-delà du terminal et du réseau, l'utilisateur est en ligne de mire

L'année dernière, la sophistication et la brutalité de certaines attaques et tactiques ont prouvé à quel point les internautes sont vulnérables, avec pour conséquence une perte de confiance du public vis-à-vis du Net.

En 2015, les violations de données, la surveillance des États et les bonnes vieilles arnaques en ligne ont toutes contribué à menacer un peu plus la vie privée des internautes. Photos personnelles, identifiants de compte ou dossiers médicaux, toutes vos données sont exposées.

### La méfiance est de mise

L'année 2015 aura été le théâtre de nombreuses arnaques et autres attaques par malware classiques dont le seul but est de collecter des informations personnelles. On citera notamment les cas de socionauts auxquels des escrocs font miroiter un flot gratuit de followers sur Instagram pour les inciter à révéler leur mot de passe. D'autres pirates se sont fait passer pour le Trésor public australien pour pousser les contribuables à télécharger des pièces jointes malveillantes.

Dans leur forme la plus simple, de nombreuses arnaques s'appuient encore sur les mauvais réflexes du grand public en matière de sécurité. Toutefois, la sécurisation insuffisante des sites web peut elle aussi exposer des données des clients. Dans ce dernier cas, si un site web comporte des vulnérabilités favorisant les violations de données, aucun mot de passe ne sera assez fort pour stopper les pirates.

Plus inquiétant peut-être, certaines attaques recensées en 2015 ont reposé sur des méthodes d'ingénierie sociale sophistiquées qui ont permis aux hackers de contourner les systèmes d'authentification à deux facteurs conçus pour protéger les utilisateurs.

Dans un autre registre, une arnaque consistait à déclencher un processus de réinitialisation de mot de passe légitime et à se faire passer pour Google via SMS, permettant ainsi d'abuser la confiance du public dans les figures d'autorité afin d'accéder aux comptes de messagerie des victimes sans éveiller leurs soupçons. (Pour plus d'infos, reportez-vous à l'encadré.)

<http://www.symantec.com/connect/blogs/free-instagram-followers-compromised-accounts-phishing-sites-and-survey-scams>  
<http://www.symantec.com/connect/blogs/australians-beware-scammers-are-impersonating-australian-taxation-office>  
<http://www.symantec.com/connect/blogs/password-recovery-scam-tricks-users-handing-over-email-account-access>

### Fonctionnement de l'arnaque Gmail

1. Un pirate trouve l'adresse e-mail et le numéro de téléphone d'une victime – des informations généralement accessibles au public.
2. Il se fait passer pour la victime et demande la réinitialisation de son mot de passe à Google.
3. Ensuite, le pirate envoie à la victime un SMS contenant un message du type « Google a détecté une activité inhabituelle sur votre compte. Merci de nous envoyer le code reçu sur votre mobile pour stopper toute activité non autorisée. »
4. La victime transmet au pirate le code de vérification envoyé par Google pour la réinitialisation de son mot de passe.
5. L'escroc peut alors réinitialiser le mot de passe. Une fois qu'il a obtenu ce qu'il voulait ou qu'il a activé un transfert d'e-mails, il informe la victime – là encore en se faisant passer pour Google – de son nouveau mot de passe temporaire, afin de la duper.

## Sexe, mensonges et vidéo

En plus des arnaques traditionnelles, l'année 2015 a vu l'apparition de scams plus vicieux et de nouvelles atteintes à la vie privée.

La sextorsion, par exemple, s'avère particulièrement répandue en Asie. Le principe : des groupes criminels ciblent des internautes à l'aide de pseudonymes aguicheurs pour inciter leurs victimes à envoyer des vidéos à caractère sexuel.

Les cybercriminels demandent ensuite à leur victime de télécharger une application pour « prolonger la discussion ». Il s'agit en fait d'un malware qui collecte les coordonnées de la victime et de ses contacts.

Enfin, le gang la menace d'envoyer son contenu à caractère sexuel à toute sa liste de contacts si elle ne paie pas un certain montant. À cause de la nature même de la menace, les victimes n'osent souvent pas faire appel aux autorités et préfèrent payer une rançon de centaines, voire des milliers d'euros aux pirates.

Dans la même veine, l'attaque contre Ashley Madison a entraîné un pic d'e-mails de spam autour du thème de l'adultère : « Comment vérifier si le piratage d'Ashley Madison vous a démasqué », « Piratage d'Ashley Madison : votre partenaire vous trompe-t-il ? », etc. L'attaque elle-même sortait d'ailleurs des sentiers battus, ses ramifications allant bien au-delà de l'aspect financier pour nuire aux relations personnelles et à la réputation des personnes concernées.



<http://www.symantec.com/connect/blogs/online-criminal-group-uses-android-app-sextortion>  
[http://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html?\\_r=0](http://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html?_r=0)  
<http://www.symantec.com/connect/blogs/scammers-quick-capitalize-ashley-madison-breach>

## Fausse identité

En 2015, les arnaques dites « sociales » ont prospéré, profitant de la confiance des socionauts dans leurs propres cercles d'amis pour propager des arnaques, des liens frauduleux et des attaques de phishing.

Pour parvenir à duper leurs victimes, les auteurs doivent faire preuve d'habileté pour donner à leurs tactiques d'ingénierie sociale une apparence convaincante.

Une escroquerie en particulier est allée jusqu'à créer une arborescence entière de centaines de milliers de faux comptes Twitter, chacun renforçant la crédibilité de l'autre, afin d'obtenir de vrais followers et des retweets de véritables utilisateurs. Au sommet de cette arborescence se trouvaient des comptes frauduleux de sites de news et de célébrités, qui contenaient même de vrais tweets des comptes légitimes pour augmenter leur crédibilité.

Avant d'accorder votre confiance à qui que ce soit sur les médias sociaux, suivez ces quelques conseils :

- **Cherchez le badge bleu de vérification.**



Les utilisateurs de Twitter devraient toujours s'assurer que le compte d'une marque ou d'une célébrité a été vérifié avant de le suivre. Le badge bleu montre que Twitter a vérifié l'identité du détenteur du compte.

- **Méfiez-vous des nouveaux followers.** Si un inconnu décide de vous suivre, ne devenez pas automatiquement son follower. Examinez ses tweets. Partage-t-il du contenu qui ressemble à du spam ? Si oui, cet inconnu est très certainement un bot.
- **Les chiffres mentent.** Même si ces inconnus affichent des dizaines de milliers de followers, il est facile de fabriquer ces chiffres de toutes pièces. Par conséquent, ne décidez pas de les suivre en retour uniquement sur la base de leur nombre de followers.

## Avènement de l'e-économie

Aux États-Unis, c'est au cours du week-end de Thanksgiving 2015 que le balancier est finalement passé du côté de l'e-commerce. D'après la National Retail Foundation, le nombre de shoppers en ligne a en effet excédé les affluences de consommateurs en magasins.

L'e-commerce représente un business colossal : selon Ecommerce Europe, en 2014, le chiffre d'affaires du commerce B2C en ligne mondial a augmenté de 24 % pour atteindre 1 943 milliards de dollars (1 766 milliards d'euros). Toutefois, ce chiffre peut sembler bien bas comparé aux 6 700 milliards de dollars (6 090 milliards d'euros) que devrait peser le marché de l'e-commerce B2B d'ici à 2020, d'après Frost & Sullivan. À noter que les prévisions du cabinet de conseil incluent toutes formes de commerce électronique, y compris Internet et les systèmes d'échange de données informatisé (EDI).

Même les États deviennent de plus en plus dépendants des services digitaux pour maintenir leur équilibre budgétaire. Ainsi, le gouvernement britannique a récemment révélé que la transformation numérique et technologique lui avait permis d'économiser 1,7 milliard de livres Sterling, soit 2,15 milliards d'euros, en 2014.

Si les certificats SSL/TLS, les marques de confiance et la protection des sites web constituent des piliers de l'e-économie, tout l'édifice pourrait bien s'effondrer en cas de défiance vis-à-vis des fondements mêmes de la sécurité en ligne.

### Baisse de confiance des internautes

En 2015, d'autres formes d'attaques ont également montré jusqu'où les cybercriminels sont prêts à aller d'un point de vue technique et moral pour s'enrichir.

#### La bourse ou la vie

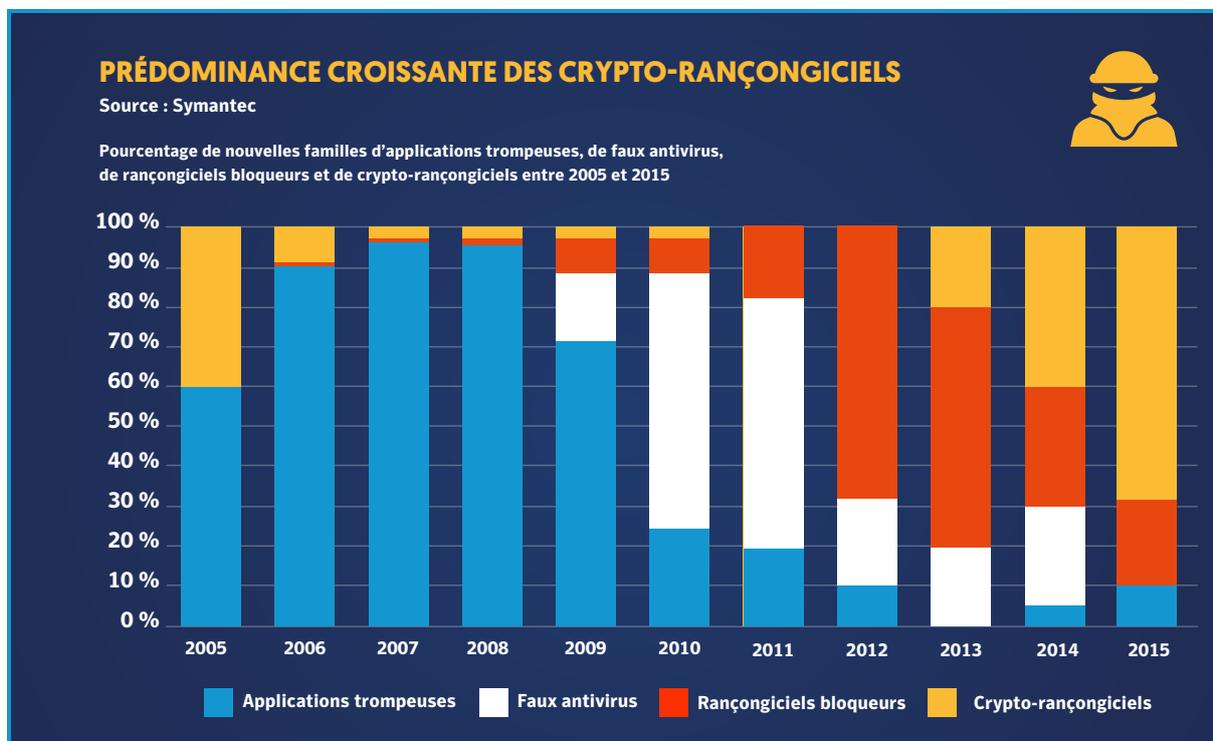
En 2015, beaucoup s'attendaient à voir les rançongiciels poursuivre sur leur lancée de ces dernières années. Pourtant, au fil de leur diversification, ces attaques ont diminué en nombre. Désormais, elles ciblent les terminaux mobiles pour crypter les fichiers et tout autre bien pour lequel la victime est prête à payer le prix. Un expert Symantec a démontré que le "ransomware" pouvait même s'attaquer aux smart TV.

Désormais, certains rançongiciels menacent également de publier vos fichiers sur Internet si vous ne payez pas – un vilain tour qui risque de faire des émules puisqu'il rend totalement désuète la parade qui consiste à faire des sauvegardes régulières.

« Dans toute l'histoire de l'humanité, jamais le monde n'avait connu un phénomène d'extorsion de l'ampleur que l'on connaît aujourd'hui. »

#### Mais pourquoi les rançongiciels ont-ils à ce point les faveurs des cybercriminels ?

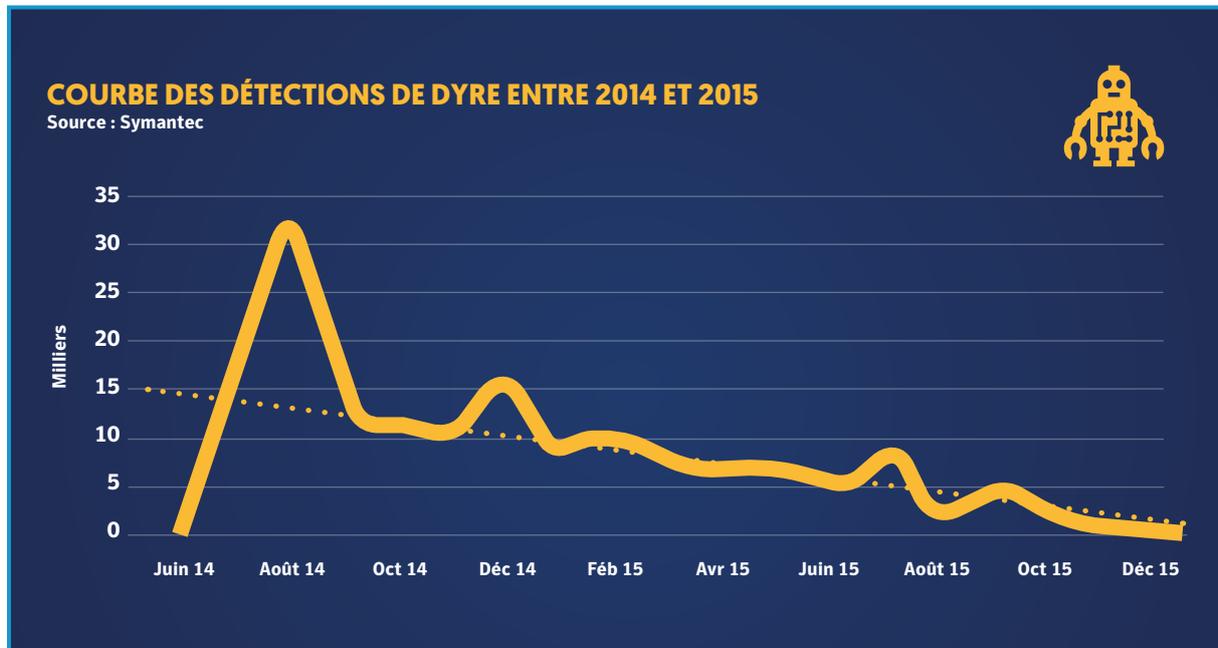
- La surabondance d'informations volées sur le marché noir et l'introduction du standard EMV pour des paiements par carte plus sûrs aux États-Unis ont réduit le potentiel économique des données de cartes bancaires volées.
- Les fraudes à la carte bancaire nécessitent l'intervention de plusieurs protagonistes et les lois de protection des consommateurs minimisent désormais les pertes financières des victimes. Par contre, un pirate peut facilement se procurer un kit de rançongiciel sur le marché noir, puis piéger ses victimes de manière à ne leur donner d'autre choix que de payer. Le cybercriminel n'a aucun intermédiaire à rémunérer, et aucun dispositif n'a été mis en place pour réduire les pertes de sa victime. Le jeu en vaut donc la chandelle.



<http://www.symantec.com/connect/blogs/how-my-tv-got-infected-ransomware-and-what-you-can-learn-it>  
<http://www.computerworld.com/article/3002120/security/new-ransomware-program-threatens-to-publish-user-files.html>  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/the-evolution-of-ransomware.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf)

## Dyre : fléau de la banque en ligne

Dyre est le nom du malware bancaire qui avait pris la place laissée vacante par plusieurs botnets financiers majeurs démantelés par les forces de police.



Non seulement Dyre était capable de détourner les navigateurs web et d'intercepter les sessions de banque en ligne pour voler des informations, mais il pouvait également télécharger d'autres malwares sur l'ordinateur de sa victime, souvent pour l'ajouter au réseau « zombie » de l'auteur de l'attaque.

Configuré pour escroquer les clients de plus de 1 000 banques et autres entreprises dans le monde entier, Dyre est tout d'abord apparu comme l'une des opérations de fraude financière les plus dangereuses au monde.

Toutefois, en novembre, le groupe de cybercriminels contrôlant le cheval de Troie a subi un énorme revers à la suite d'une opération des forces de police russes. Comme l'explique le blog de [Symantec Security Response](#), la télémétrie Symantec a confirmé l'arrêt quasi-total des activités du gang. Détecté par Symantec en tant que [Infostealer.Dyre](#), Dyre se propageait via des campagnes d'e-mails. Or, aucune campagne de ce type n'a été recensée depuis le 18 novembre 2015. Rapidement après cette date, les détections du

cheval de Troie Dyre et des malwares associés ont considérablement chuté. Au début de l'année 2015, d'après nos estimations, on dépassait les 9 000 infections par mois. En novembre, ce chiffre était passé sous la barre des 600.

### Hackers sans frontières

En 2015, d'autres formes d'attaques ont également montré jusqu'où les cybercriminels sont prêts à aller pour s'enrichir, tant d'un point de vue technique que moral. Où que vous viviez et quelle que soit votre langue, vous pourriez vous retrouver dans leur ligne de mire. Prenez l'exemple de Boleto. Ce système de paiement utilisé uniquement au Brésil évolue de fait sur un marché niche. Il ne devrait donc a priori pas intéresser les pirates. Pourtant, l'année 2015 a vu l'apparition de [trois familles de malwares](#) spécialement conçues pour le cibler.

À travers le monde, la multiplication des attaques localisées de ce type prouve que les cybercriminels se donnent beaucoup de mal pour manipuler leurs victimes, quels que soient leur pays et leur langue.

<http://www.symantec.com/connect/blogs/dyre-emerges-main-financial-trojan-threat>  
<http://www.symantec.com/connect/blogs/dyre-operations-bank-fraud-group-grind-halt-following-takedown>  
[http://www.symantec.com/security\\_response/writeup.jsp?docid=2014-061713-0826-99](http://www.symantec.com/security_response/writeup.jsp?docid=2014-061713-0826-99)  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/boleto-malware.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/boleto-malware.pdf)



Le tableau montre le rôle crucial joué par les médias sociaux dans les attaques par ingénierie sociale. Toutefois, ces dernières années, ces sites ont pris des mesures fermes contre de tels abus afin de compliquer la tâche des pirates.

Les kits de phishing permettent d'adapter extrêmement facilement des arnaques à une cible spécifique dans un pays donné. Pour changer ces paramètres, les pirates peuvent rapidement modifier les modèles fournis. Souvent, ces mêmes modèles sont localisés via un logiciel de traduction automatique, ce qui suffit souvent à duper des victimes dont ce n'est pas la langue maternelle.

### Lois sur la confidentialité des données

« Les gens s'intéressent non seulement aux pirates, mais aussi aux fuites en puissance », explique Shankar Somasundaram, Directeur senior chargé de la gestion produits et de l'ingénierie chez Symantec.

En mai 2014, la décision en faveur du « droit à l'oubli » de la Cour européenne de justice s'est propagée dans la communauté de collecte des données, si bien qu'à la fin de l'année 2015, Google avait reçu 348 085 demandes de suppression de résultats de recherche spécifiques.

Si beaucoup voyaient dans ce jugement un moyen d'éviter des scandales et des accusations, d'après la FAQ de Google,

parmi les cas de demandes de suppression les plus courants figurent des sites contenant des coordonnées personnelles ou « des informations uniquement relatives à la santé, l'orientation sexuelle, l'ethnie, la religion, l'affiliation politique et syndicale d'une personne ».

Cette année encore, la Cour européenne de justice a de nouveau attiré l'attention sur les problématiques de respect de la vie privée en invalidant l'accord « Safe Harbor » de 2000. Comme l'explique Monique Goyens, Directrice générale de l'association européenne des consommateurs, la décision confirme qu'un « accord qui permet aux entreprises américaines de simplement déclarer qu'elles adhèrent aux règles européennes de protection des données, sans même qu'une autorité quelconque vérifie cette affirmation, n'a strictement aucune valeur ».

Le quotidien The Guardian avait alors écrit que l'invalidation de l'accord pourrait « empêcher le gouvernement américain d'accéder à des données utilisateurs provenant de l'UE » et « ouvrir la voie vers d'autres enquêtes, plaintes et procès d'individus et organismes de réglementation des données ».

[http://www.cio.com/article/3008661/google-receives-steady-stream-of-right-to-be-forgotten-requests.html#tk.rss\\_all](http://www.cio.com/article/3008661/google-receives-steady-stream-of-right-to-be-forgotten-requests.html#tk.rss_all)  
[http://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=en#common\\_delisting\\_scenarios](http://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=en#common_delisting_scenarios)  
[http://www.beuc.eu/publications/beuc-pr-2015-020\\_historic\\_victory\\_for\\_europeans\\_personal\\_data\\_rights.pdf](http://www.beuc.eu/publications/beuc-pr-2015-020_historic_victory_for_europeans_personal_data_rights.pdf)  
<http://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection>

Dans un contexte de prolifération des violations de données et d'internetisation de nos existences, les régulateurs et pouvoirs judiciaires devraient encore resserrer l'état juridique autour de la protection de la vie privée en 2016.

Du côté des entreprises, il est temps d'envisager la sécurité sous l'angle de la pédagogie et de l'épidémiologie. Le maintien de l'intégrité digitale d'une entreprise est l'affaire de tous ses collaborateurs. De même, les DSI et les responsables informatiques doivent prendre conscience

des nombreux risques en présence et rechercher activement d'éventuels symptômes. L'objectif : diagnostiquer les « maladies digitales » avant qu'elles ne mettent les données et la confiance des clients en péril.

Enfin, Symantec croit fermement au respect de la vie privée et le défend ardemment à travers le monde. Nous n'acceptons pas cette fatalité qui voudrait que ce concept soit mort, mais pensons au contraire qu'il faut le préserver avec soin.

### Prévention d'une cyber-apocalypse

D'après BofA Merrill Lynch Global Research, chaque année, la cybercriminalité coûte jusqu'à 575 milliards de dollars (523 milliards d'euros) à l'économie mondiale. Selon leur rapport, si une « cyber-apocalypse » venait à se produire en 2020, les cybercriminels pourraient s'approprier jusqu'à un cinquième de la valeur créée sur Internet.

Chacun d'entre nous a donc un rôle à jouer dans la prévention d'un tel scénario.

Du côté des consommateurs, il est temps de bannir les mauvais réflexes. Beaucoup connaissent les règles de base d'une bonne sécurité informatique. Pourtant, aux États-Unis, plus d'un tiers des personnes qui disent partager leurs mots de passe ont déjà transmis à d'autres les identifiants d'accès à leur compte bancaire en ligne. Chacun doit donc prendre ses propres responsabilités pour cesser ce type d'imprudence et mieux se protéger en ligne.

**L'IMPACT ÉCONOMIQUE DE LA  
CYBERCRIMINALITÉ S'ÉLÈVE À  
575 MILLIARDS DE \$ CHAQUE  
ANNÉE**

**575  
MILLIARDS DE \$**

[http://us.norton.com/cyber-security-insights?id=us\\_hho\\_nortoncom\\_clp\\_norton-hp-ribbon-award\\_nrpt](http://us.norton.com/cyber-security-insights?id=us_hho_nortoncom_clp_norton-hp-ribbon-award_nrpt)

# Au-delà du terminal et du réseau, l'entreprise est en ligne de mire

Les attaques persistantes et sophistiquées qui ciblent les entreprises de toutes tailles menacent la sécurité des États et de l'économie. Dans un contexte d'augmentation du nombre des vulnérabilités zero-day, leur exploitation dans des attaques en tous genres est désormais avérée. Pour gagner en efficacité, les campagnes de spear-phishing se sont faites plus discrètes en ciblant moins de personnes et d'entreprises à la fois.

## Menaces APT

Une violation de sécurité majeure chez Anthem, deuxième plus grand prestataire de soins de santé des États-Unis, a exposé 78 millions de dossiers patients. L'attaque a été révélée en février 2015. Lors de son enquête, Symantec est remonté jusqu'à Black Vine, un groupe de hackers bénéficiant de gros moyens et qui serait lié à une entreprise de sécurité informatique chinoise appelée Topsec. Black Vine et ses malwares personnalisés avancés sont à l'origine de nombreuses campagnes de cyberespionnage perpétrées contre plusieurs secteurs d'activité, y compris l'énergie et l'aérospatiale.

En 2015, parmi les cibles du cyberespionnage figuraient également la Maison Blanche, le Pentagone, le Bundestag allemand et le Bureau du personnel de la fonction publique aux États-Unis qui a perdu 21,5 millions de dossiers d'employés, y compris des informations sensibles (situation financière, antécédents médicaux, casiers judiciaires, et même empreintes digitales).

Ces attaques s'inscrivent dans le cadre d'un nouveau genre de cyberespionnage sophistiqué, persistant et richement doté, qui touchent le monde entier. Elles ciblent des secrets d'État, le capital intellectuel des entreprises (modèles, brevets, plans, etc.), mais aussi – comme le montrent les dernières violations de données – des informations personnelles.

Les vulnérabilités zero-day s'avèrent inestimables pour les pirates. L'une d'entre-elles a notamment servi à l'attaque d'un organisme gouvernemental à l'aide d'un e-mail contenant un document Word infecté. Leur valeur est d'ailleurs telle que les hackers font tout leur possible pour en

préserver le secret et garder ainsi l'avantage. Ils peuvent par exemple concevoir un malware qui s'activera uniquement à une certaine heure ou en certains lieux pour échapper à la détection des experts en sécurité qui exécutent leur logiciel de détection à une autre heure ou sur un autre site.

Parce que les vulnérabilités zero-day représentent de toute évidence un atout rare, les pirates couvriront leurs traces pour éviter de se faire repérer et l'exploiter le plus longtemps possible.

Ainsi, les attaques sophistiquées dites du « point d'eau », qui utilisent des sites web compromis, se déclencheront uniquement lorsqu'un visiteur provient d'une adresse IP bien particulière. De cette façon, les pirates réduisent les dommages collatéraux, ce qui augmente d'autant leurs chances de masquer leurs exploits. Cette approche complique également la tâche des spécialistes en sécurité qui visiteraient le site web depuis une autre adresse IP. Souvent, une fois l'exploit rendu public par le fournisseur informatique concerné, les attaquants implantés sur ces sites « point d'eau » passeront à un autre exploit inconnu basé sur une autre faille zero-day.

Quant à l'enquête menée par Symantec sur le cheval de Troie Regin, elle nous donne un aperçu des moyens techniques des pirates soutenus par des États. Ce travail de longue haleine a révélé 49 nouveaux modules correspondant chacun à une nouvelle fonctionnalité (enregistrement des saisies claviers, accès aux e-mails, etc.) ainsi qu'une infrastructure étendue de commande et contrôle (CnC). Pour nos analystes, le niveau de sophistication et de complexité de Regin laisse supposer que son développement aurait pu prendre des mois, voire des années, à des équipes de développeurs aux ressources importantes.

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/the-black-vine-cyberespionage-group.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf)  
<http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/>  
<http://www.wsj.com/articles/nsa-chief-says-cyberattack-at-pentagon-was-sophisticated-persistent-1441761541>  
<http://ca.reuters.com/article/technologyNews/idCAKBN002GA20150610>  
<http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/>  
<http://www.symantec.com/connect/blogs/regin-further-unravelling-mysteries-cyberespionage-threat>  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/regin-analysis.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf)

Actuellement, le spear-phishing et les « points d'eau » qui exploitent des sites web compromis constituent les techniques privilégiées pour les attaques ciblées. Toutefois, à mesure que le parc technologique des entreprises s'élargit, leur surface d'attaque s'étend en conséquence. Le passage aux technologies cloud et la prolifération des appareils connectés laissent présager une exploitation des vulnérabilités de ces systèmes dans les attaques ciblées d'ici un ou deux ans. De par leur vulnérabilité aux exploits de type injection SQL, il est fort probable que les services cloud soient les premiers touchés. Quant aux campagnes de spear-phishing qui exploiteront les erreurs de configuration et les faibles niveaux de protection des utilisateurs, elles se chargeront des cibles plus faciles que des fournisseurs de services cloud intrinsèquement mieux protégés.

Pour prévenir leur détection, les campagnes de spear-phishing se concentrent sur un nombre restreint d'individus pour se faire plus discrètes. Cela ne les empêche pourtant pas de se multiplier. Bientôt, ces attaques ne devraient plus viser qu'une seule cible, ou un petit groupe d'individus dans la même entreprise. En outre, les plus grandes campagnes recourront certainement toutes aux attaques web du point d'eau en exploitant des vulnérabilités zero-day pour compromettre des sites web.

### VULNÉRABILITÉS ZERO-DAY

Source : Symantec | SDAP, Wiki

2015	Évolution	2014	Évolution	2013
54	+125%	24	+4%	23

### Diversité des failles zero-day

En 2015, 54 vulnérabilités zero-day ont été découvertes. Ce chiffre record représente plus du double de celles recensées en 2014. La découverte de vulnérabilités inconnues et leur exploitation sont clairement devenues la technique de prédilection des attaquants dits « avancés » – une tendance qui n'est pas prête de s'infléchir.

**Les vulnérabilités zero-day se vendent à prix d'or sur le marché noir. Pour cette raison, et par leur nature même, nous pensons que le nombre de vulnérabilités zero-day recensées se situe bien en-deçà de leur quantité réelle.**

En 2015, la plupart de ces failles zero-day ciblaient des technologies anciennes et « éprouvées », déjà visées depuis des années. Ainsi, tout au long de l'année, les pirates ont découvert et exploité 10 vulnérabilités zero-day différentes contre Adobe Flash Player. Microsoft n'était pas en reste, même si les 10 nouvelles failles découvertes sur ses logiciels se répartissaient entre plusieurs produits : Microsoft Windows (6 failles), Internet Explorer (2 failles), et Microsoft Office (2 failles). En 2015, quatre vulnérabilités zero-day ont également ciblé le système d'exploitation Android.

### Groupes d'attaques actifs en 2015

Parmi les groupes d'attaques ciblées les plus actifs en 2015, on trouve :

- Black Vine – groupe d'attaques chinois ciblant principalement les secteurs de l'aérospatiale et de la santé à la recherche de données personnelles et de propriété intellectuelle. À son tableau de chasse cette année : Anthem et le Bureau du personnel de la fonction publique (deux cibles américaines),
- Rocket Kitten – groupe de cyberespionnage à la solde de l'État iranien, qui cible les journalistes, les défenseurs des droits de l'Homme et les scientifiques
- Cadelle et Chafer – groupe basé en Iran et spécialisé dans l'attaque de compagnies aériennes, de fournisseurs d'énergie et d'opérateurs télécoms du Moyen-Orient, à l'exception d'une entreprise victime aux États-Unis
- Duke et Seaduke – groupe d'attaques apparu en 2010 et dont les principales cibles sont les administrations européennes, des personnalités et des organismes de recherche privés et de politique internationale
- Emissary Panda – groupe d'attaque chinois spécialisé dans le vol de données de propriété intellectuelle dans de nombreux secteurs : finance, aérospatiale, renseignement, télécommunications, énergie et ingénierie nucléaire. Connu pour avoir exploité CV-2015-5119, une vulnérabilité zero-day révélée lors de l'incident Hacking Team
- Waterbug et Turla – groupe de cyberespionnage basé en Russie et spécialisé dans les attaques de spear-phishing et du point d'eau à l'encontre d'ambassades et d'institutions gouvernementales. Actif depuis 2005
- Butterfly – groupe d'attaques ciblant les géants de la pharmaceutique, des matières premières et de l'informatique, y compris Facebook et Apple, à des fins de délits d'initié

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/the-black-vine-cyberespionage-group.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf)  
<http://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets>  
<http://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory>  
[https://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/waterbug-attack-group.pdf](https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf)  
<http://www.symantec.com/connect/blogs/butterfly-profiting-high-level-corporate-attacks>  
<http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats>

## Terreur mondiale, attaques locales

« Les cybercriminels se professionnalisent et font preuve de plus d'audace dans le choix de leurs cibles et les montants convoités », affirme Stephen Doherty, Analyste cyberveille senior chez Symantec.

À l'approche des élections présidentielles aux États-Unis, des e-mails de spam infectés surfent sur la vague des primaires pour appâter leurs victimes. Leurs auteurs savent jouer sur la corde sensible des internautes autour de thèmes brûlants comme la crise des réfugiés au Moyen-Orient, l'immigration, les questions de politique étrangère, l'économie, et même le terrorisme.

Dans une récente campagne de spam, des pirates se sont ainsi faits passer pour des forces de police locales au Moyen-Orient et au Canada, afin d'inciter leurs victimes à télécharger un malware déguisé en soi-disant conseils de sécurité. Tous les noms d'officiels utilisés par les cybercriminels étaient en poste au moment des faits. En outre, dans la plupart des cas, l'objet du message citait en référence le nom d'un collaborateur de l'entreprise ciblée.

Pour rendre ce type d'attaques convaincant, les pirates doivent effectuer un travail de recherche important, comme c'est manifestement le cas dans cet exemple de phishing. Fautes d'informations sur les salariés, les pirates allaient même jusqu'à contacter d'autres personnes qui pouvaient leur servir de points d'entrée, comme les services client ou les RH.

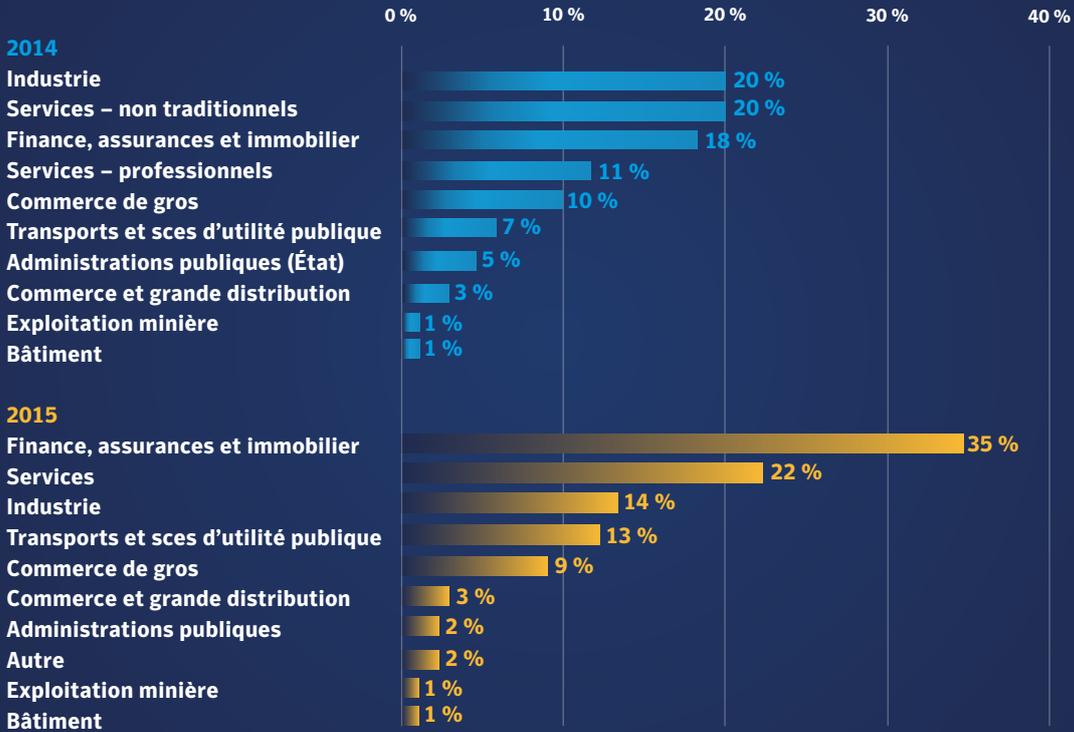
Ce niveau de recherche et de localisation, qui peut mobiliser jusqu'à plusieurs centaines de personnes, se généralise dans les arnaques aux botnets. De fait, le Dark Net n'est pas qu'un simple marché de revente de biens volés : il s'agit d'une industrie à part entière, composée des structures et des talents que l'on retrouve dans n'importe quel secteur d'activité légitime. Le parallèle va même jusqu'à la prédominance de puissances émergentes telles que la Chine, comme dans la vraie économie.

## Délit d'initié et effet papillon

Groupe de hackers ultracompetents et ultra-organisés, Butterfly (« papillon » en français) soutire des informations aux entreprises pour en tirer un avantage en Bourse, soit en revendant ces données, soit en commettant eux-mêmes des délits d'initié. Ces premières attaques remontent à 2013, lorsque le groupe a accroché quelques entreprises célèbres comme Apple, Microsoft et Facebook à son tableau de chasse. Difficile pourtant de les repérer, car ils utilisent des moyens sophistiqués pour couvrir leurs traces, y compris des serveurs de commande et contrôle (CnC) virtuels cryptés. Leur appétence aux zero-day révèle en outre un niveau de sophistication encore jamais vu dans des attaques à but lucratif.

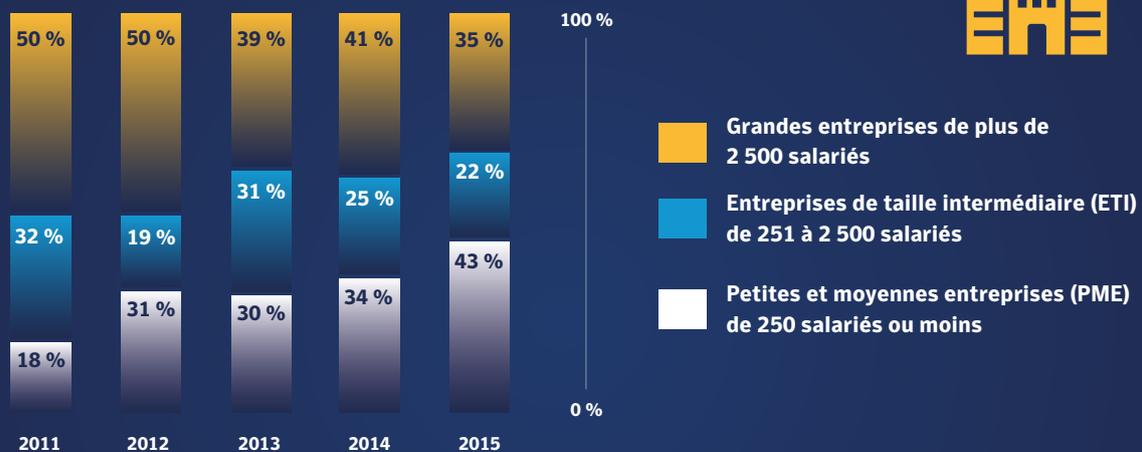
### LES DIX SECTEURS D'ACTIVITÉS LES PLUS CIBLÉS PAR LE SPEAR-PHISHING ENTRE 2014 ET 2015

Source : Symantec I cloud



### TAILLE DES ENTREPRISES VICTIMES DU SPEAR-PHISHING ENTRE 2011 ET 2015

Source : Symantec I cloud



## Cybersécurité, cybersabotage et théorie du cygne noir

Si le cyberespionnage est monnaie courante, les cas de cybersabotage se font étonnamment rares. Pourtant, ce ne sont pas les ressources qui manquent pour infliger des dommages physiques, ni même la surface d'attaque avec la prolifération des terminaux connectés à Internet, systèmes de contrôle industriels en tête.

L'édition 2015 de la [revue de sécurité et de défense](#) du gouvernement britannique résume parfaitement les enjeux :

« L'éventail de cyberacteurs menaçant le Royaume-Uni s'est élargi. La menace s'avère de plus en plus asymétrique et mondiale. En règle générale, une cyberdéfense fiable et cohérente requiert des compétences avancées et des investissements substantiels. Mais un nombre croissant d'États haussent encore leur niveau de jeu avec des ressources et des capacités potentiellement déployables en situation de conflit, notamment contre des infrastructures nationales critiques et des institutions gouvernementales. Quant aux acteurs privés, y compris les terroristes et les cybercriminels, ils trouveront facilement sur Internet les outils et les technologies nécessaires pour commettre leurs activités destructrices. »

La cyberattaque [Stuxnet](#) contre le programme nucléaire iranien constitue l'exemple le plus connu d'une attaque d'infrastructures physiques perpétrée via Internet. Peut-être d'autres attaques ont-elles atteint leurs cibles sans que nous n'en sachions rien, ni que les malwares n'aient encore été activés. Dans tous les cas, il n'existe aucun danger contre lequel l'infrastructure critique mondiale ne soit totalement immunisée. L'attaque perpétrée à la fin 2014 contre une [usine sidérurgique allemande](#) laisse présager des incidents potentiellement plus graves.

## L'obscurité n'est pas un gage de sécurité

La meilleure forme de protection contre le cyberespionnage consiste à rester constamment sur ses gardes. Toutes les entreprises sont des victimes en puissance d'attaques ciblées comme [le point d'eau](#) et le [spear-phishing](#). Une petite taille et un relatif anonymat ne protègent personne.

En 2015, la plus grande proportion des attaques de spear-phishing (43 %) a ciblé les petites entreprises, même si dans l'absolu, la probabilité d'une attaque a diminué. De fait, si les PME ont enregistré le plus fort volume d'attaques, ces actions se sont focalisées sur un nombre restreint d'entreprises (3 %).

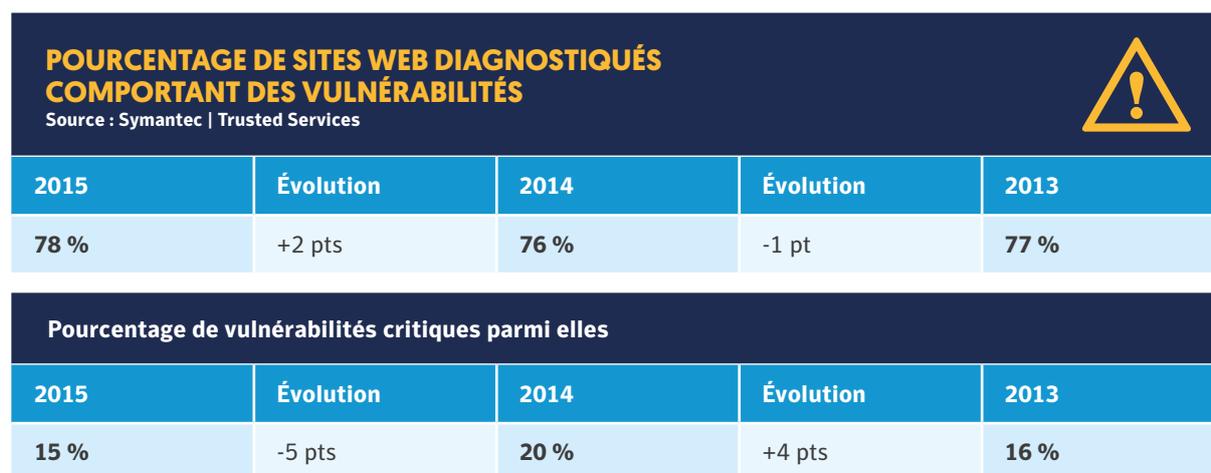
Ces chiffres contrastent avec ceux des grandes entreprises, qui ont enregistré 35 % des attaques de spear-phishing en valeur absolue, mais dont surtout 38 % ont été ciblées au moins une fois. Ce qui est le signe de campagnes de plus grande ampleur et d'une approche tous azimuts.

Une fois les risques reconnus, les entreprises peuvent prendre des mesures pour s'en prémunir : bilans réguliers des plans de sécurité et d'intervention, demande de conseils et d'assistance le cas échéant, mise à jour des dispositifs techniques de défenses, pédagogie et formation des utilisateurs, et traitement continu des dernières informations.

## Vecteurs d'attaques

Kits, attaques web et exploitation des vulnérabilités en ligne

Si les serveurs web sont vulnérables, les sites qu'ils hébergent et les internautes qui les visitent le sont tout autant. Qu'on se le dise : les pirates sont prêts à s'engouffrer dans toutes les failles possibles pour compromettre les sites et prendre le contrôle de leurs serveurs hôtes.



Une vulnérabilité est considérée comme critique lorsque son exploitation permet l'exécution de code malveillant, sans interaction utilisateur, avec pour conséquence possible une violation de données et la compromission des visiteurs du site web infecté.

Comme toujours, ces chiffres montrent que les exploitants de sites web ne corrigent, ni ne mettent à jour leurs sites et leurs serveurs aussi souvent qu'ils le devraient.

### Linux en ligne de mire

L'année 2015 a connu une forte hausse des malwares dirigés contre Linux, le système d'exploitation n°1 sur les serveurs web, entre autres services Internet essentiels.

Souvent, les attaquants contaminent les serveurs web à l'aide d'un code qui renvoie vers des kits d'exploits. L'envoi d'e-mails de spam et le vol des noms d'utilisateurs et mots de passe sont également monnaie courante. De même, les serveurs web compromis servent souvent de rampe de lancement à toutes sortes d'attaques, y compris les fameux DDoS au pouvoir destructeur. Pour leurs auteurs, la compromission des serveurs d'un hébergeur est d'autant plus intéressante que sa bande passante est autrement plus puissante que la connexion haut débit d'un particulier.

La prolifération des kits d'attaques spécialisés et automatisés rend les attaques contre les systèmes Linux à la portée d'une majorité de cybercriminels. Pour faciliter le repérage de serveurs potentiellement vulnérables, ces kits recherchent des systèmes de gestion de contenus non sécurisés et d'autres applications web exposées.

### Quelques conseils pour protéger votre serveur

- Appliquez tous les correctifs et mises à jour sur votre serveur.
- Déployez plusieurs rideaux de protection de façon à limiter le nombre de zones touchées en cas de compromission.
- Déployez un système de prévention et de détection des intrusions sur votre réseau, tout en surveillant de près votre système de messagerie électronique sur votre serveur.
- Équipez-vous d'un bon pare-feu et analysez régulièrement les logs d'accès pour détecter les activités potentiellement suspectes.
- Utilisez un logiciel antivirus pour la détection et le blocage des malwares.
- Faites des sauvegardes hors site.

<http://www.symantec.com/connect/tr/blogs/phishing-economy-how-phishing-kits-make-scams-easier-operate>

En 2015, un rançongiciel dirigé contre les systèmes Linux a également été découvert : il concentrait son action sur des fichiers bien particuliers, avec des extensions associées aux applications web. Le code malveillant cryptait également les archives et les répertoires qui contenaient le mot « backup », ce qui ne faisait qu'empirer la situation en cas de sauvegarde sur site.

## Problèmes de plugins

Le système d'exploitation n'est pas le seul talon d'Achille des serveurs web. Bien que la plupart des grands éditeurs de systèmes de gestion de contenus ont amélioré leur sécurité et déployé des mises à jour automatiques ces dernières années, la sécurité de leurs plugins pose encore un énorme problème.

### Flash : la fin est proche

En 2015, le nombre de vulnérabilités dans les plugins Adobe a augmenté, signe que les pirates cherchent à exploiter des plugins qui sont non seulement multiplateformes, mais aussi universels. La plupart des failles Adobe se trouvent dans Adobe Flash Player (aussi appelé Shockwave Flash).

Cela fait des années que les hackers exploitent ce plugin. Ainsi, rien que l'année dernière, 10 vulnérabilités zero-day y ont été découvertes (17 %), contre 12 en 2014 (50 %) et 5 en 2013 (22 %). Avec de telles pépites, rien d'étonnant à ce que Flash reste une cible incontournable des pirates. De leur côté, Apple, Google et Mozilla ont tous fait part de leurs inquiétudes quant au plugin Flash. Récemment, Google et Mozilla ont même annoncé l'arrêt du support Flash en natif dans Chrome et Firefox.

D'un point de vue sécuritaire, Adobe Flash devrait progressivement tomber en désuétude dans les années à venir.

### Exploitation des plugins pour serveurs web

Mais les attaquants ne limitent pas leur action aux plugins des navigateurs. Prenez l'exemple de la plateforme WordPress, sur laquelle repose aujourd'hui un quart des sites web du monde entier.

Tout le monde peut créer un plugin WordPress – et c'est bien là le souci. Malgré l'utilité de certains, d'autres s'avèrent totalement loufoques, comme la Logout Roulette :

### Conseils pour limiter les risques sur les plugins

- Mettez régulièrement vos plugins à jour.
- Consultez régulièrement les alertes de sécurité sur les listings spécialisés et dans les médias.
- Pour réduire votre surface d'attaque, montrez-vous très sélectif dans votre utilisation des plugins.

« à chaque chargement de page admin, vous avez une chance sur 10 d'être déconnecté ».

Le problème réside dans le fait que certains plugins sont affreusement dangereux. Windows attire de nombreux exploits du fait de sa large base d'utilisateurs. Il en va de même pour les plugins WordPress. En somme, les plugins vulnérables des sites sous WordPress peuvent et seront exploités.

### Infection par injection

L'année 2015 a également marqué le retour du Team GhostShell qui revendique le piratage d'un grand nombre de sites web. Plus tôt dans l'année, l'équipe Symantec Security Response réagissait :

« Depuis les premières apparitions, la liste récemment publiée de sites web piratés semble aléatoire et n'indique aucun ciblage d'un pays ou d'un secteur particulier. Le groupe choisit très certainement ses cibles en fonction de leur vulnérabilité. À en juger par son *modus operandi* passé, il est probable que le gang ait compromis des bases de données par l'intermédiaire d'injections SQL et de scripts PHP mal configurés. »

Encore une fois, il s'agit d'attaques qu'une meilleure gestion des serveurs et des sites web aurait sans aucun doute permis d'éviter. Les injections SQL constituent une méthode d'attaque bien connue. Pourtant, la recette continue de fonctionner du fait de faiblesses inutiles dans les paramètres de recherche définis par les administrateurs.

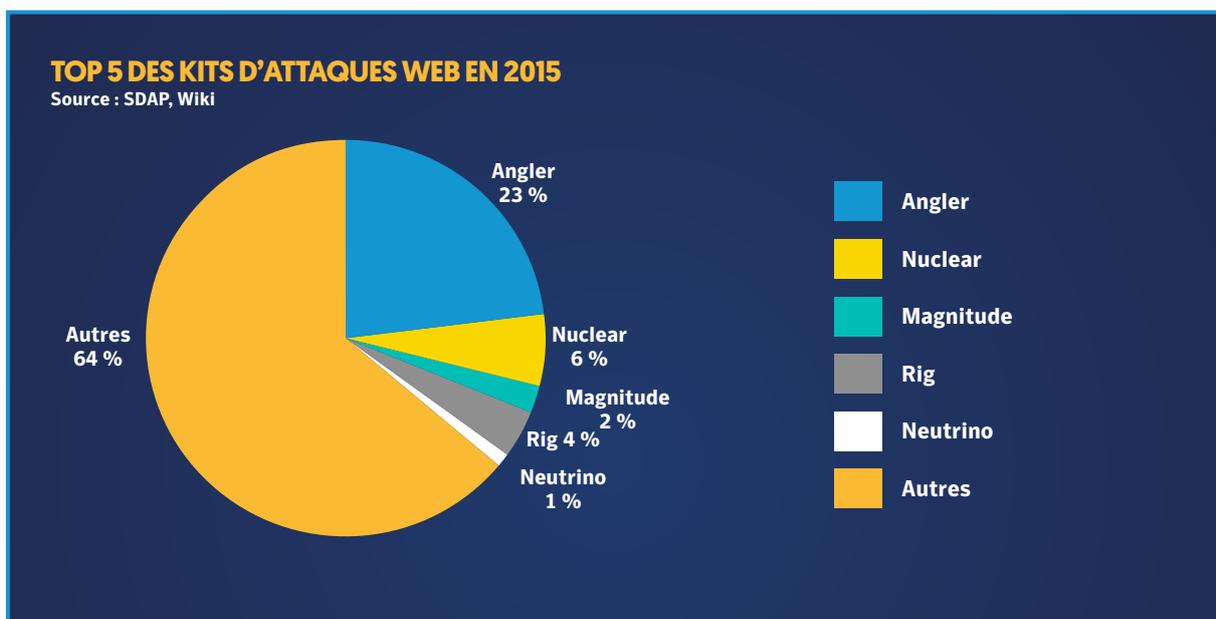
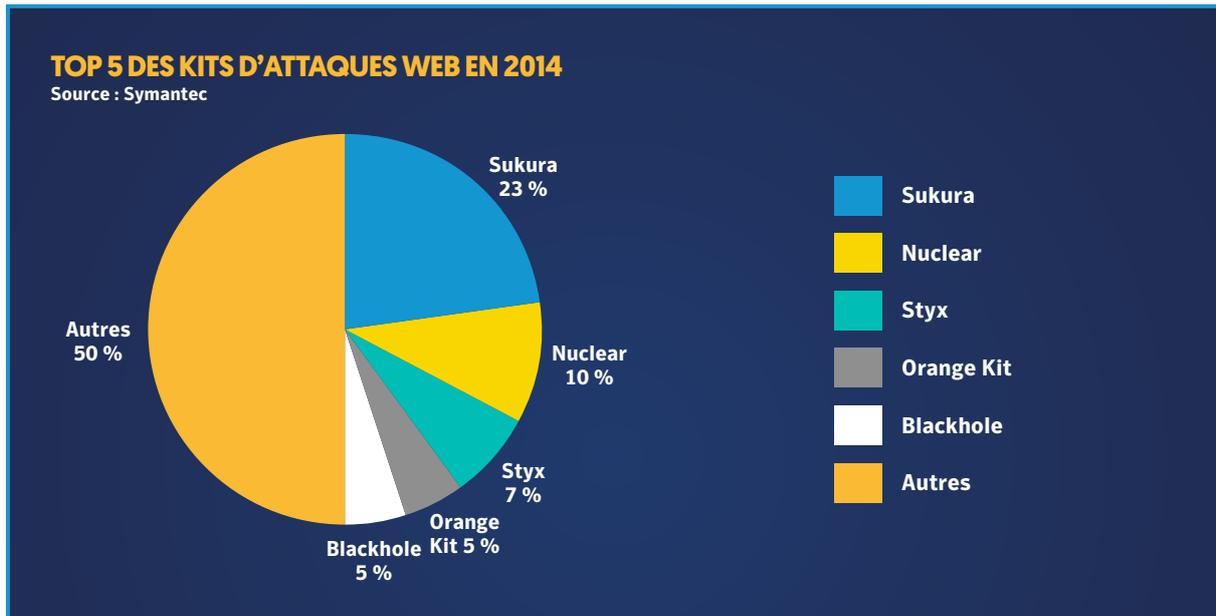
Tant sur les navigateurs que sur les serveurs, les plugins doivent être mis à jour régulièrement. Dans la mesure du possible, évitez d'utiliser des versions obsolètes.

[https://www.symantec.com/security\\_response/writeup.jsp?docid=2015-110911-5027-99](https://www.symantec.com/security_response/writeup.jsp?docid=2015-110911-5027-99)  
<http://w3techs.com/blog/entry/wordpress-powers-25-percent-of-all-websites>  
<https://wordpress.org/plugins/logout-roulette/>  
<http://www.symantec.com/connect/blogs/team-ghostshell-hacking-group-back-bang>

### Kits d'attaques web

Par définition, il est difficile de se défendre contre une vulnérabilité que l'on ne connaît pas. C'est le cas des zero-day pour lesquels il n'existe aucun correctif, d'autant plus que les attaquants font tout ce qu'ils peuvent pour les exploiter avant que les éditeurs de logiciels aient le temps de réagir.

La violation des systèmes de Hacking Team, une entreprise basée en Italie, a conduit à la publication par ses auteurs d'exploits zero-day encore inconnus. Au bout de quelques heures seulement, ces exploits avaient déjà été intégrés à des kits d'attaques.



<http://www.symantec.com/connect/blogs/hacking-team-woes-adds-dangers-faced-internet-using-public>

Parmi eux, on notera la suractivité d'Angler en 2015, dont Symantec a dû bloquer des centaines de milliers d'attaques. Au total, nous en avons recensé plus de 19,5 millions. Angler privilégiait les publicités malveillantes comme mécanisme de frappe, avec un fort penchant pour les failles d'Adobe Flash. En 2015, Windows fut la cible n°1 d'Angler, notamment Windows 7 (64 % des attaques contre 24 % pour Windows 8.1). De son côté, Mac OS X est resté relativement épargné par Angler. Mais les choses pourraient bien changer à mesure que les cybercriminels se penchent sur le cas de l'écosystème Apple.

### Nuclear : le support technique au service des rançongiciels

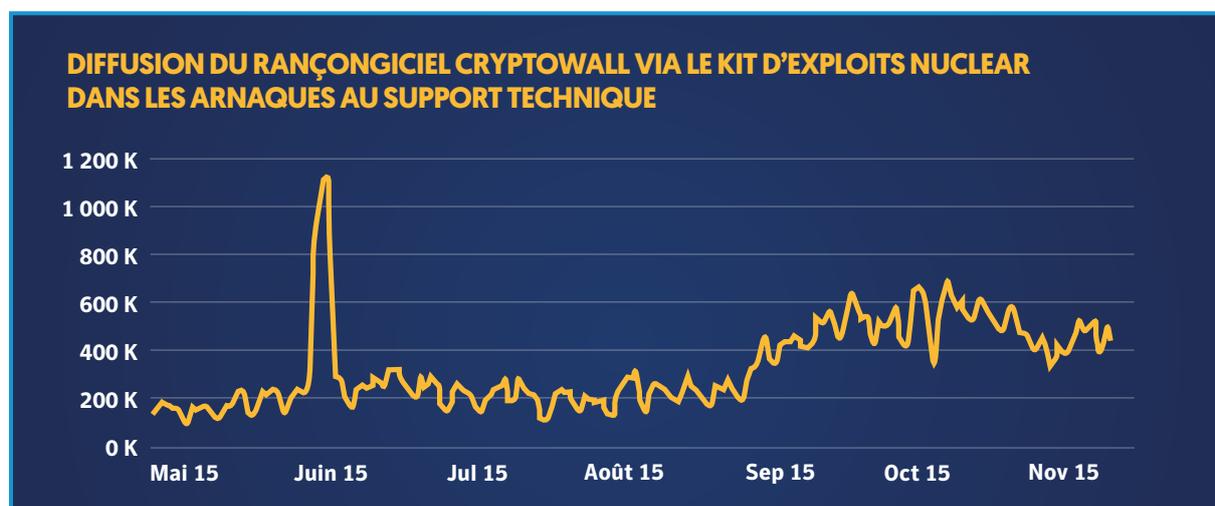
En 2015, Symantec a constaté une hausse de 200 % des arnaques au support technique par rapport à l'année précédente.

Chaque jour, ces arnaques, qui n'ont pourtant rien de nouveau, touchent des centaines de milliers de personnes dans le monde entier. Au tout début, un téléopérateur contactait

les utilisateurs par téléphone pour essayer de leur vendre une formule de support technique censée résoudre des problèmes évidemment inexistantes sur les ordinateurs des victimes.

Avec le temps, ces arnaques ont évolué. Plus récemment, on a notamment observé l'apparition d'une multitude de faux messages d'avertissement incitant à appeler un numéro vert pour obtenir de l'aide. Lorsqu'elles composent ce numéro, les victimes tombent sur un téléopérateur très professionnel en apparence, qui tentera de les convaincre d'installer un programme qui réglerait tous leurs problèmes, alors qu'il s'agit en fait d'un malware ou d'une application indésirable de ce genre.

Aux dernières nouvelles, ces faux techniciens support utilisaient même le kit d'exploits Nuclear pour installer des rançongiciels sur les ordinateurs de leurs victimes. Ils font généralement diversion pendant que le rançongiciel crypte les fichiers, car plus le nombre de fichiers est élevé, plus la rançon monte.



<http://www.symantec.com/connect/blogs/what-symantec-s-intrusion-prevention-system-did-you-2015>

Même si le rançongiciel n'a rien de nouveau dans ce type d'arnaque au support technique, les dernières variantes passaient par une balise HTML iframe malveillante qui redirigeait les visiteurs du site factice vers un serveur hébergeant le kit Nuclear. Ce kit d'attaques exploite notamment la dernière vulnérabilité Adobe Flash Player permettant l'exécution de code arbitraire à distance (CVE-2015-7645), le but de la manœuvre étant d'installer soit Trojan.Cryptowall (un rançongiciel), soit Trojan.Miuref.B (un cheval de Troie destiné au vol d'informations).

Pour Symantec, il s'agissait des premiers cas d'utilisation du kit d'exploits Nuclear pour l'installation de rançongiciels dans les arnaques au support technique. Si la combinaison s'avère gagnante, nul doute que les cas devraient se multiplier. Bien que l'on puisse imaginer une collaboration entre les escrocs du support technique et les spécialistes du kit Nuclear, il est également fort probable que les serveurs web des escrocs aient été compromis par un groupe adepte de Nuclear. Au total, l'année dernière, Symantec a bloqué plus de 100 millions d'arnaques au support technique. Les pays les plus touchés étaient les États-Unis, le Royaume-Uni, la France, l'Australie et l'Allemagne.

### Déni de service distribué (DDoS)

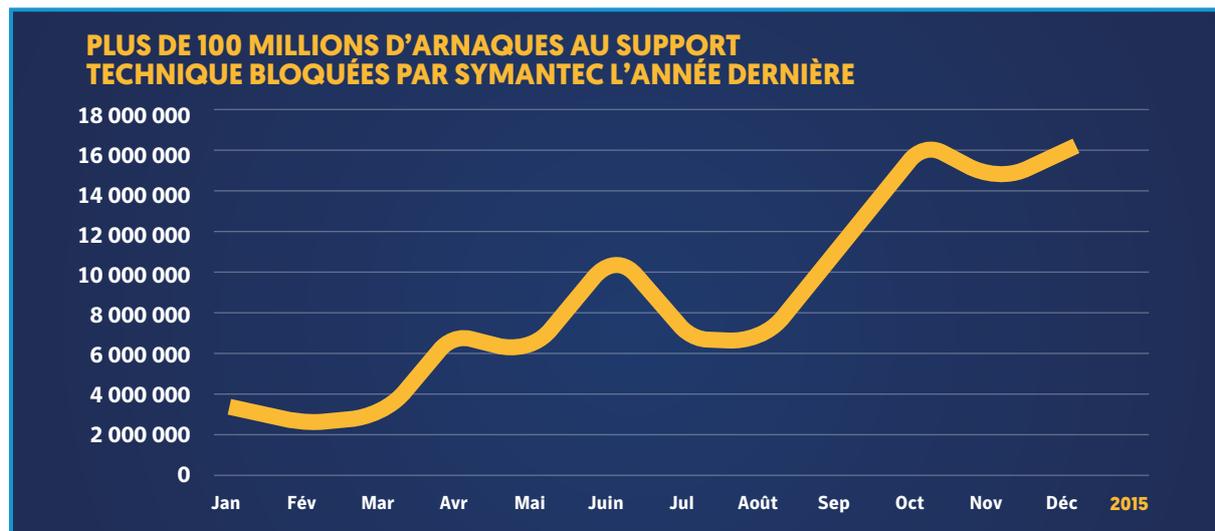
Alors que le marché du « botnet locatif » a le vent en poupe et que l'Internet des objets (IoT) apporte un surplus de munitions aux armées de bots, les attaques par déni de service distribué (DDoS) gagnent en ampleur et en durée.

### Le DDoS en quelques mots

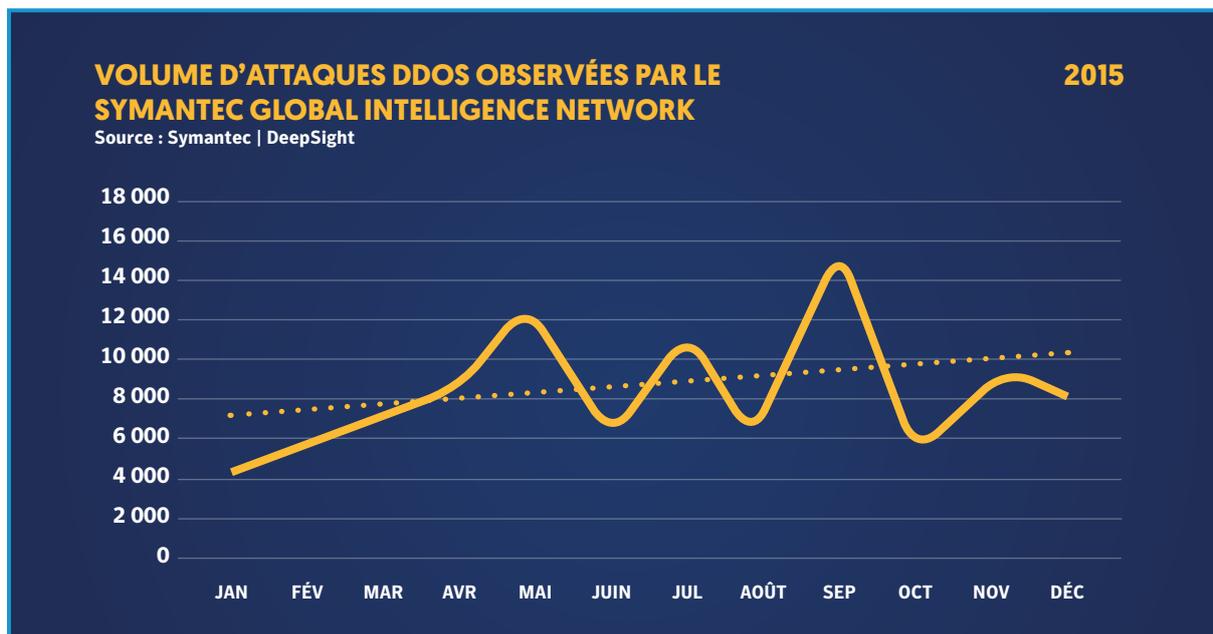
Certaines attaques DDoS rapportent encore des sommes conséquentes à leurs auteurs par voie d'extorsion et de chantage. Quant à l'entreprise dont le site web est fortement perturbé, elle n'a parfois pas d'autre choix que de payer la rançon. Toutefois, l'opération n'est pas sans risque pour les cybercriminels car l'argent laisse des traces. De même, les technologies de neutralisation des attaques DDoS augmentent les besoins des pirates en bande passante pour que leur attaque ait une chance d'aboutir. Ainsi, plus récemment, certaines des pires attaques ont été l'apanage de groupes d'hacktivistes, et parfois des services d'un État.

Prenons l'exemple du récent piratage de la BBC, qui a conduit à l'indisponibilité de son site web et de services comme iPlayer pendant plusieurs heures le jour de la Saint-Sylvestre. Elle serait la plus grande attaque de ce type jamais perpétrée, du moins selon New World Hacking, qui l'a revendiquée. Le groupe de hackers anti-État islamique affirmait alors que la taille de l'infrastructure de la BBC lui avait donné l'occasion de tester ses capacités. Toujours selon lui, l'attaque a atteint un pic de 602 Gbits/s.

Cela dit, les attaques DDoS présentent encore un certain potentiel économique, le vecteur le plus courant restant le chantage : une somme d'argent contre la fin de la menace. Par le passé, le DDoS a également servi d'opération de « diversion » en marge de certaines des attaques ciblées perpétrées en 2015. Le principe : les pirates inondent de requêtes le site web de l'entreprise victime, mobilisant ses équipes informatiques dans l'attente d'une demande de rançon, alors qu'en même temps, les attaquants mènent une autre attaque à couvert.



<http://www.symantec.com/connect/blogs/when-tech-support-scams-meet-ransomlock>  
<http://www.symantec.com/connect/blogs/tech-support-scams-redirect-nuclear-ek-spread-ransomware>  
[https://www.symantec.com/security\\_response/vulnerability.jsp?bid=77081](https://www.symantec.com/security_response/vulnerability.jsp?bid=77081)  
[https://www.symantec.com/security\\_response/writeup.jsp?docid=2014-061923-2824-99](https://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99)  
[https://www.symantec.com/security\\_response/writeup.jsp?docid=2015-032402-2413-99](https://www.symantec.com/security_response/writeup.jsp?docid=2015-032402-2413-99)  
<http://www.bbc.co.uk/news/technology-35204915>  
<http://www.techradar.com/news/internet/attack-against-bbc-website-was-the-biggest-volley-of-ddos-fire-ever-seen--1312864>  
<http://www.americanbanker.com/news/bank-technology/banks-lose-up-to-100khour-to-shorter-more-intense-ddos-attacks-1073966-1.html?pg=1>  
[https://www.symantec.com/security\\_response/writeup.jsp?docid=2014-061923-2824-99](https://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99)



Cette courbe montre l'augmentation du nombre d'attaques DDoS au deuxième semestre, avant sa chute en novembre et décembre. En 2015, on a enregistré davantage de pics d'activité dans la mesure où les attaques se veulent désormais plus courtes et plus discrètes.

### TOP 5 DU TRAFIC D'ATTAQUES DDOS OBSERVÉES PAR LE SYMANTEC GLOBAL INTELLIGENCE NETWORK

Source : Symantec | DeepSight

Classement	Attaques en 2015	Taux d'attaques en 2015	Attaques en 2014	Taux d'attaques en 2014
1	Attaque par inondation de paquets ICMP standards	85,7 %	Attaque par amplification DNS	29,44 %
2	Attaque DoS par inondation de paquets TCP SYN standards	6,4 %	Attaque par inondation de paquets ICMP standards	17,20 %
3	Attaque DoS « Smurf » par inondation de paquets Ping standards	2,1 %	Attaque DoS « Smurf » par inondation de paquets Ping standards	16,78 %
4	Attaque DoS Teardrop/Land standard	2,0 %	Attaque DoS Teardrop/Land standard	7,17 %
5	Attaque DoS via l'exploit RFProwl	0,6 %	Attaque DoS par messages ICMP standards du type « Host Unreachable »	5,71 %

La majorité des DDoS correspondaient à des attaques par inondation de paquets ICMP, dans lesquelles un grand volume de requêtes (généralement) Ping finit par saturer la cible au point qu'elle ne peut plus accueillir ses visiteurs légitimes.

[https://en.wikipedia.org/wiki/Internet\\_Control\\_Message\\_Protocol](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol)

### Simple mais efficace

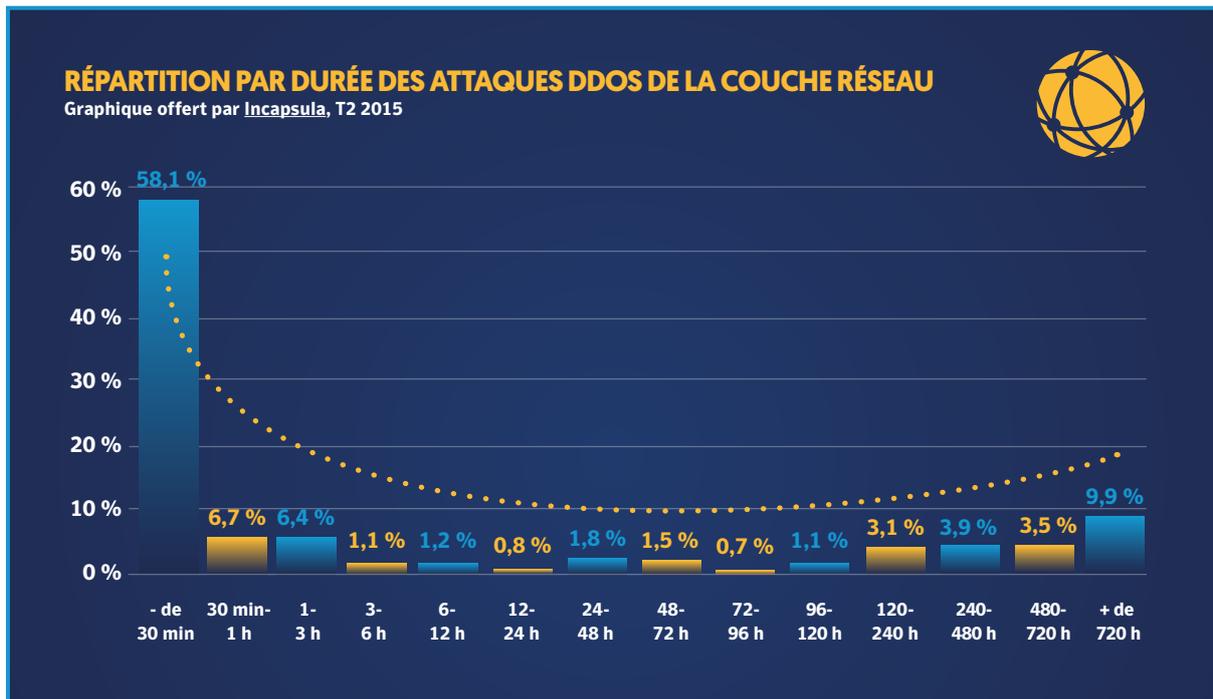
Mais pourquoi les attaques DDoS ont-elles tant le vent en poupe ? Depuis notre [premier article sur le sujet en 2002](#), les raisons n'ont pas changé : elles sont simples à mettre en place, difficiles à stopper et redoutablement destructrices. Et l'émergence des « botnets localifs » ne fait que confirmer cet état de fait.

Selon [Incapsula](#), un partenaire Symantec, au deuxième trimestre 2015, les botnets loués étaient à l'origine d'environ 40 % de toutes les attaques DDoS sur la couche réseau. Certes, les cybercriminels peuvent toujours se donner la peine d'infecter de multiples terminaux vulnérables afin de créer leur propre botnet pour leurs attaques DDoS. Mais il est souvent bien plus simple de louer des botnets préfabriqués pour une durée déterminée.

En 2015, les prix sur le marché noir sont restés assez stables. Pour les attaques DDoS, il fallait compter entre 10 \$ et 1 000 \$ par jour.

Côté entreprises, la facture s'avèrera bien plus élevée, parfois jusqu'à 1 000 fois ces chiffres, en fonction de la nature de son activité et de l'importance de son site web. Par conséquent, le retour sur investissement est potentiellement énorme pour l'attaquant.

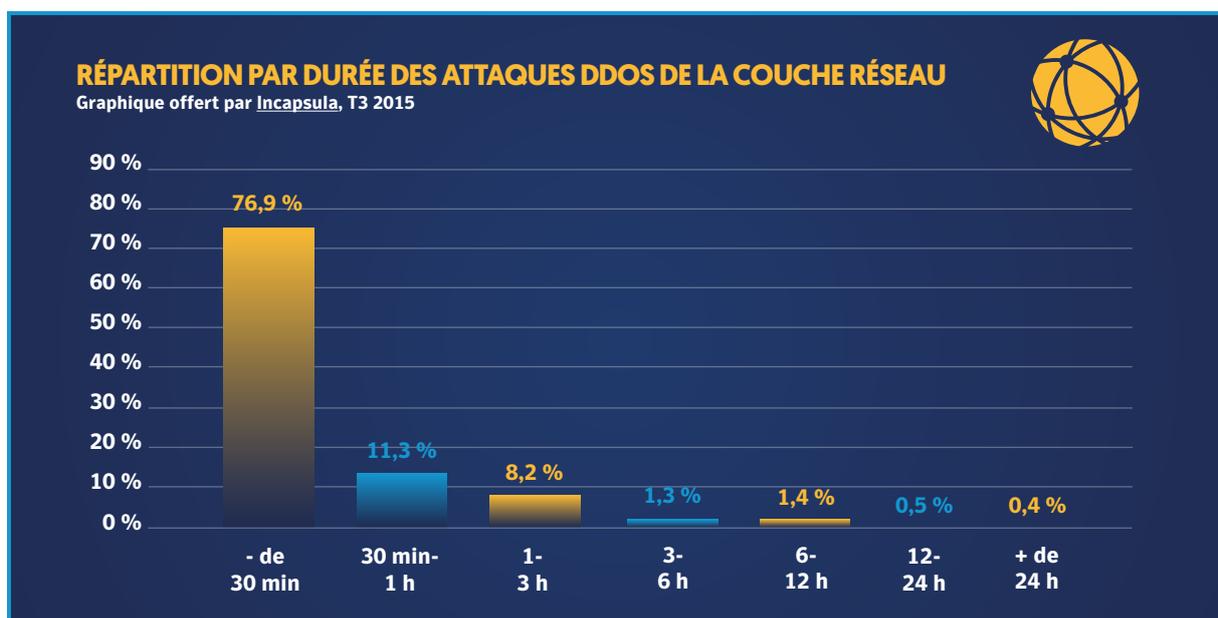
Ces attaques éclairs sont également le signe d'une plus grande utilisation des offres d'attaques DDoS sous forme de service. Le principe : un abonné se voit allouer un accès limité à l'ensemble des ressources d'un botnet en colocation avec d'autres attaquants. En règle générale, ces ressources suffisent juste pour mener quelques actions courtes et de puissance moyenne. Ces attaques peuvent également permettre aux pirates de tester l'efficacité des solutions de neutralisation de l'infrastructure cible, afin d'évaluer les moyens à déployer. Par ailleurs, Incapsula fait état d'une généralisation des attaques de plus de 100 Gbits/s, à raison d'une tous les deux jours.



Cette courbe montre comment, à la fin du deuxième trimestre 2015, une grande partie des attaques DDoS pouvaient encore durer plusieurs heures, jours, semaines, voire plusieurs mois.

<http://www.symantec.com/connect/articles/barbarians-gate-introduction-distributed-denial-service-attacks>  
<https://www.incapsula.com/blog/ddos-global-threat-landscape-report-q2-2015.html>  
<http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>

Comme le montre le graphique ci-dessous, la popularité grandissante des attaques DDoS sous forme de service fait écho à l'énorme chute de la durée des attaques de la couche réseau entre le deuxième et le troisième trimestre 2015. Certains de ces services DDoS en location se sont eux-mêmes rebaptisés « stresser » pour une simple raison : du fait du caractère illégal des attaques DDoS, les fournisseurs se cachent derrière le faux prétexte de proposer des stress-tests pour évaluer la résilience des serveurs.



Cette figure montre qu'à la fin du troisième trimestre, le nombre de DDoS de plus de 24 heures était quasi-nul, ne représentant qu'à peine 0,5 % de toutes les attaques recensées.

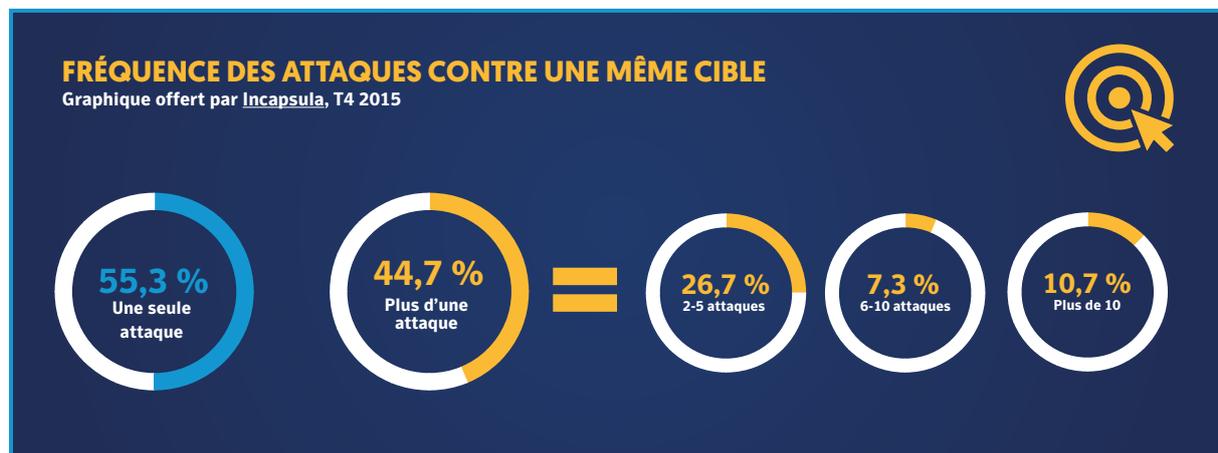
À mesure que les assaillants se sont reconvertis dans des actions éclaircies, le nombre même de ces attaques s'est envolé. Ainsi, Incapsula a signalé une hausse de 133,8 % de la fréquence des attaques réseau au second semestre 2015.

### Les applications web connectées de plus en plus dans la tourmente

Dans un schéma semblable aux attaques de la couche réseau, les incidents au niveau des applications se sont eux aussi raccourcis, sans pour autant perdre en ténacité. Au quatrième trimestre 2015, la plus grande attaque contrée sur une couche applicative s'est avérée aussi courte qu'intense, avec un pic à 161 300 requêtes à la seconde.

D'une part, cet événement nous rappelle que le problème des dénis de service distribués touche tout l'écosystème Internet. D'autre part, il montre combien il est facile de conduire une attaque sur des applications à l'aide de quelques terminaux compromis seulement. Il n'en faut généralement pas davantage pour mettre hors service un site web de taille moyenne, et prolonger son indisponibilité pour très longtemps.

Ainsi, le quatrième trimestre 2015 a lui aussi été marqué par une forte fréquence des attaques applicatives répétées, avec 44,7 % des cibles touchées plus d'une fois et 18 % d'entre elles visées plus de cinq fois.



<https://www.incapsula.com/blog/ddos-report-q4-2015.html>

### Diversification des botnets

Qu'ils soient loués ou créés par les attaquants eux-mêmes, les botnets constituent un élément essentiel des DDoS. Plus le botnet est puissant, plus il pourra envoyer de requêtes simultanées, et plus les perturbations seront importantes.

Mais une armée de bots ne se compose pas uniquement de PC infectés. En octobre, nous avons vu des malwares cibler des serveurs MySQL, qui offrent une bande passante bien supérieure aux publics d'internautes traditionnellement visés. Cette méthode n'est pas nouvelle, mais elle prouve que les cybercriminels continuent de créer des botnets toujours plus puissants et toujours plus performants.

En outre, en 2015, les appareils IoT connectés sont venus grossir les rangs de leurs armées de bots. Les caméras de surveillance ont été particulièrement ciblées, probablement

parce qu'elles constituent le gros des appareils IoT actuellement connectés. En 2014, on comptait 245 millions de caméras de vidéosurveillance actives et installées par des professionnels dans le monde entier.

À l'avenir, on peut redouter une exploitation croissante des vulnérabilités de certains appareils IoT dans le cadre d'attaques DDoS de masse. Bien qu'il existe des solutions anti-DDoS, les entreprises devront également adapter les moyens de protection à ces nouveaux types de terminaux connectés si elles ne veulent pas faire elles-mêmes partie du problème.

Sans une bonne solution de sécurité en place, vous aurez toutes les peines du monde à savoir si votre imprimante, votre réfrigérateur, votre thermostat ou votre grille-pain font partie d'un dangereux botnet mondial.

**SANS UNE BONNE SOLUTION DE SÉCURITÉ EN PLACE, VOUS AUREZ TOUTES LES PEINES DU MONDE À SAVOIR SI VOTRE IMPRIMANTE, VOTRE RÉFRIGÉRATEUR, VOTRE THERMOSTAT OU VOTRE GRILLE-PAIN FONT PARTIE D'UN DANGEREUX BOTNET MONDIAL.**

### Publicités malveillantes (malvertising)

Au milieu de l'année 2015, les cas de malvertising ont proliféré dans presque toutes les branches d'Internet financées par la publicité. Une explication possible : les publicités malveillantes représentent tout simplement un moyen plus facile d'infecter les internautes que les e-mails de spam renvoyant vers des sites compromis. Pour un pirate, il est bien plus simple d'essayer de compromettre ou d'héberger des publicités malveillantes sur des sites web ultrafréquentés car cette tactique le dispense de maîtriser toutes les nuances de l'ingénierie sociale. Autant dire que cela lui enlève une bonne épine du pied.

Souvent, les régies publicitaires demandent assez peu d'informations aux personnes qui leur soumettent des contenus. Les cybercriminels peuvent alors se faire passer pour des entreprises légitimes et charger des publicités

malveillantes qui pourront s'afficher sur n'importe quel site. Grâce aux cookies, les auteurs de malwares peuvent également personnaliser leur code ou leur adresse de renvoi pour cibler les utilisateurs par géographie, heure de la journée, entreprise, centre d'intérêt ou activité Internet récente.

Pour ne rien arranger, les publicités malveillantes sont particulièrement difficiles à traquer, d'autant plus que les cybercriminels suppriment le code malveillant de leurs annonces au bout d'une heure ou deux, ce qui les rend presque invisibles. Au vu de leur redoutable efficacité et de la difficulté à les repérer, on peut s'attendre à une nouvelle recrudescence de publicités malveillantes à l'avenir. Toutefois, une hausse de la demande de bloqueurs de publicités (plugins, applis, etc.) pourrait bien à son tour réduire la capacité de nuisance du malvertising.

### CLASSEMENT DES SITES WEB LES PLUS FRÉQUEMMENT EXPLOITÉS, 2014 – 2015

Source : Symantec | SDAP, Safe Web, Rulespace

Classement	2015 – Top 10 des catégories de sites les plus attaquées	Pourcentage 2015 du nombre total de sites web infectés	Top 10 en 2014	Pourcentage 2014
1	High-tech	23,2 %	High-tech	21,5 %
2	Business	8,1 %	Hébergement	7,3 %
3	Recherche	7,5 %	Bloggging	7,1 %
4	Blogs	7,0 %	Business	6,0 %
5	Contenus dynamiques	6,4 %	Sites d'anonymisation	5,0 %
6	Éducation	4,0 %	Divertissement	2,6 %
7	Domaines parqués	3,2 %	Sites marchands	2,5 %
8	Divertissement	2,6 %	Sites illégaux	2,4 %
9	Sites marchands	2,4 %	Domaines parqués	2,2 %
10	Sites illégaux	2,1 %	Communautés virtuelles	1,8 %

En 2015, les sites à caractère high-tech et business ont été les plus touchés par les contenus malveillants et le malvertising.

<http://www.symantec.com/connect/blogs/malvertising-campaign-targets-brazilian-users>

## Côté client

### Smartphones et terminaux mobiles

Les smartphones constituent une cible de plus en plus attractive pour les cybercriminels. C'est pourquoi ils n'hésitent pas à investir dans de nouvelles techniques d'attaques sophistiquées pour extorquer de l'argent ou voler des données personnelles. Si les utilisateurs Android sont particulièrement dans la tourmente, l'année 2015 a également vu la compromission de terminaux Apple non débridés.

### Un téléphone par personne

Selon le Worldwide Quarterly Mobile Phone Tracker d'IDC (27 janvier 2016), en 2015, plus de 1,4 milliard de smartphones se sont vendus dans le monde, soit une hausse de 10 % par rapport aux 1,3 milliard d'appareils vendus en 2014. Cinq de ces nouveaux téléphones sur six fonctionnaient sous Android, tandis qu'un combiné sur sept était équipé de l'iOS d'Apple (IDC, Parts de marché des différents systèmes d'exploitation pour smartphones, T2 2015). D'après le fabricant de téléphones mobiles Ericsson, d'ici fin 2020, le monde pourrait compter jusqu'à 6,4 milliards d'abonnements pour smartphones, soit presque un appareil par personne.

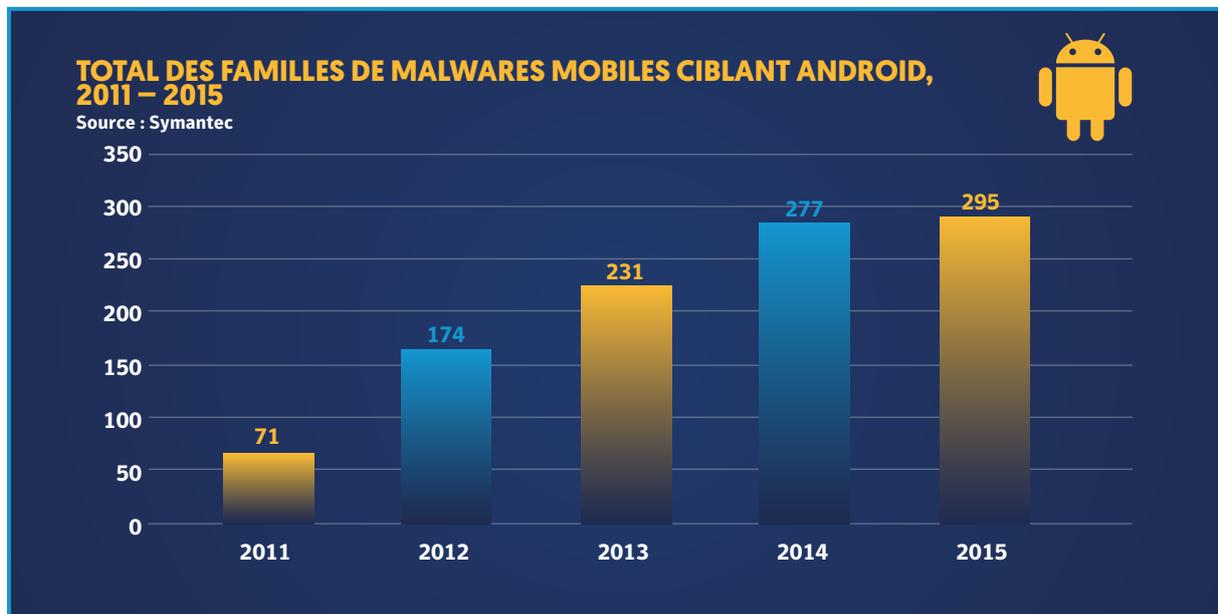
Outre la puissance des processeurs sur les téléphones et tablettes haut de gamme, la 4G leur offre désormais une connexion mobile à haut débit. Sans compter qu'ils contiennent désormais des informations personnelles précieuses, à l'image du lancement d'Apple Pay en 2015 et d'autres systèmes de paiement mobile dans son sillage. Rien d'étonnant, donc, à ce que les cybercriminels jettent leur dévolu sur les smartphones.

### Menaces trans-terminaux

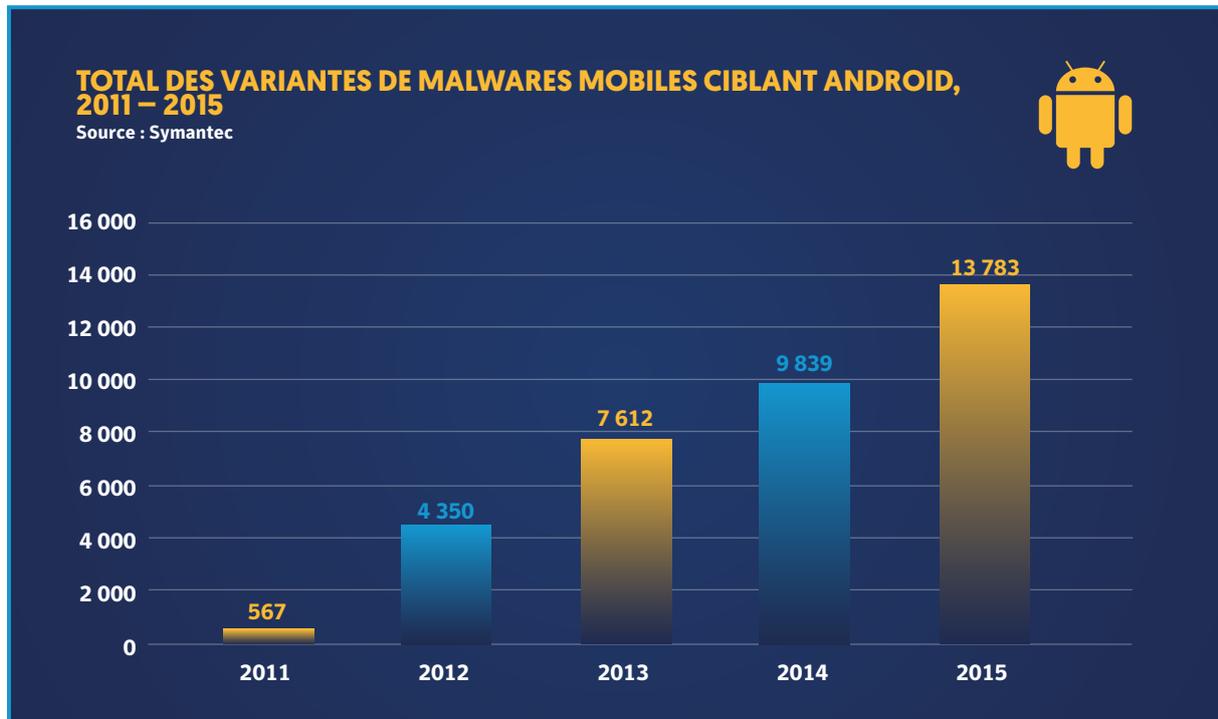
De nombreux « app stores » permettent aux utilisateurs de rechercher, acheter et installer à distance des applications depuis leur ordinateur, ouvrant ainsi de formidables possibilités de transversalité pour les attaquants. Par exemple, avec Google Play, les clients peuvent parcourir le Play Store depuis leur ordinateur à l'aide d'un navigateur web normal, puis installer des applications directement sur leur téléphone. Des malwares Windows récents ont ainsi exploité cette possibilité en subtilisant les cookies de navigation des sessions Google Play d'un ordinateur infecté. Grâce aux identifiants de connexion ainsi récupérés, ils ont pu usurper l'identité des victimes et installer à leur insu des applications sur leurs téléphones et tablettes.

ANALYSE D'APPLICATIONS PAR SYMANTEC NORTON MOBILE INSIGHT			
Source : Symantec   SDAP			
	2015	2014	2013
<b>Total des applis analysées</b>	10,8 millions	6,3 millions	6,1 millions
<b>Total des applis classées comme malware</b>	3,3 millions	1 million	0,7 million
<b>Total des applis classées comme grayware</b>	3 millions	2,3 millions	2,2 millions
<b>Total des graywares reclassés en madware</b>	2,3 millions	1,3 million	1,2 million
<b>Définition d'un malware</b>	Programmes et fichiers créés dans le but de nuire. Ils regroupent notamment les virus, les vers et les chevaux de Troie.		
<b>Définition d'un grayware</b>	Programmes qui ne contiennent pas de virus et n'apparaissent pas a priori comme malveillants, mais qui peuvent présenter une certaine capacité de nuisance pour l'utilisateur (par exemple, outils de piratage, accessware, spyware, adware, composeurs et canulars).		
<b>Définition d'un madware</b>	Techniques agressives de placement de publicités dans les albums photos, les entrées de calendrier ou la barre de notification de votre mobile. Les madwares peuvent même remplacer une sonnerie par une publicité.		

<http://www.idc.com/getdoc.jsp?containerId=prUS40980416>  
<http://www.idc.com/prodserv/smartphone-os-market-share.jsp>  
<http://www.ericsson.com/mobility-report>  
<https://www.census.gov/population/international/data/idb/worldpopgraph.php>



En 2015, le nombre de nouvelles familles de malwares ciblant Android a augmenté de 6 % seulement, contre 20 % en 2014.

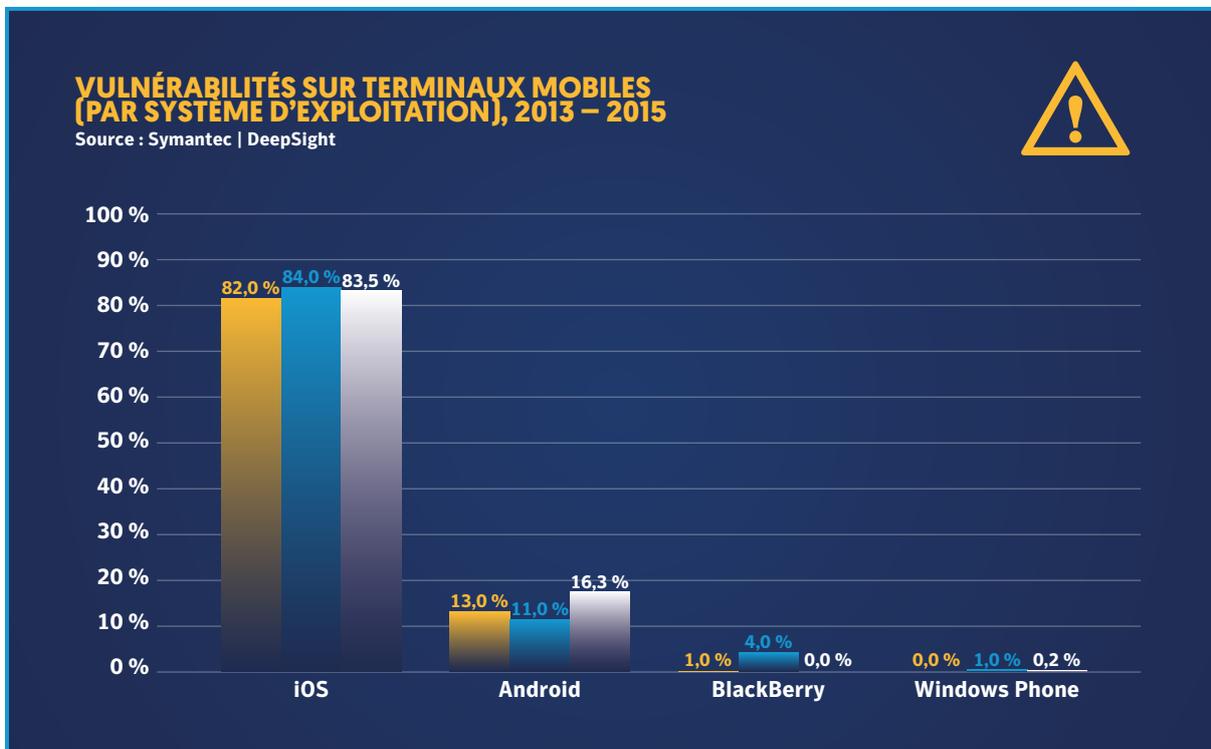


Toutefois, le volume de variantes sous ce même OS a lui enregistré une hausse de 40 %, contre 29 % en 2014.

Le nombre de vulnérabilités sur les terminaux mobiles a augmenté sur chacune des trois dernières années. Contrairement à Android, les vulnérabilités iOS ont joué un rôle critique dans l'accès des pirates aux terminaux Apple, en particulier pour le débridage. Le débridage permet à un utilisateur d'installer des applications non autorisées sur l'App Store, contournant par là même la sécurité intégrale d'iOS. Il est bien plus difficile de compromettre un appareil non débridé, puisque cela nécessite généralement l'installation d'une appli téléchargée depuis l'App Store. Or, Apple est bien connu pour la rigueur de ses processus de vérification qui ont jusqu'à présent permis de limiter le nombre d'applis malveillantes sur iOS par rapport à Android.

En 2012, IOS.Finfish représentait le tout premier exemple d'application malveillante sous iOS dans l'App Store. Finfish permettait le vol d'informations d'un appareil compromis. L'année 2014 a ensuite vu l'apparition d'OSX.Wirelurker, qui utilisait des connexions USB à un Mac ou un PC pour installer des applis sur des terminaux iOS non débridés.

Toutefois, 2015 a marqué un nouveau tournant avec XcodeGhost et YiSpecter, deux malwares qui sont parvenus à compromettre des appareils iOS sans l'exploitation de vulnérabilités, ni le débridage de ces derniers.



Sur ces dernières années, iOS reste néanmoins le système d'exploitation n°1 en nombre de vulnérabilités. Pour les pirates, la motivation première reste le débridage des terminaux et un accès non autorisé pour l'installation de malwares.

[http://www.symantec.com/security\\_response/writeup.jsp?docid=2012-083015-4511-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2012-083015-4511-99&tabid=2)  
[https://www.symantec.com/security\\_response/writeup.jsp?docid=2014-110618-0523-99](https://www.symantec.com/security_response/writeup.jsp?docid=2014-110618-0523-99)

### Furtivité des nouvelles attaques Android

Les malwares qui ciblent Android se font plus discrets. Pour contourner les logiciels de sécurité basés sur les signatures, certains auteurs ont commencé à en masquer le code avant de lancer leurs attaques. D'autres malwares sont même capables de vérifier s'ils s'exécutent sur de vrais téléphones ou sur le genre d'émulateurs que les experts en sécurité utilisent.

### Les utilisateurs Android sous le feu du phishing et des rançongiciels

Hormis les arnaques habituelles comme la vente d'applications factices, les pirates ont recours à des techniques plus sophistiquées pour s'enrichir sur le dos de leurs victimes. Entre autres, les chercheurs Symantec ont découvert un nouveau cheval de Troie pour Android qui déclenche l'ouverture d'une page de connexion frauduleuse venant se superposer sur l'appli bancaire légitime. Le but : intercepter la saisie des identifiants et mots de passe des utilisateurs. Dans la même veine, le dernier rançongiciel sous Android prend l'apparence des produits et services Google pour donner plus de poids et d'autorité aux faux avertissements du FBI sur leur écran de verrouillage. En parallèle, certains rançongiciels ne se contentent plus de changer le code PIN des téléphones mais vont jusqu'à en crypter les contenus, notamment les photos.

### Le ver est dans la pomme pour les utilisateurs d'Apple iOS

Grâce à la main de fer d'Apple sur son App Store et son système d'exploitation, les menaces sur les iPhone et iPad sont restées rares et isolées. Du moins jusqu'en 2015 :

- En 2015, nous avons identifié neuf nouvelles familles de menaces contre iOS, contre un total de quatre auparavant.
- La version piratée du logiciel pour développeurs, baptisée XcodeGhost, a infecté jusqu'à 4 000 applications.
- Le malware YiSpecter a contourné l'App Store via le framework de provisionnement des applis de l'entreprise.
- Des chercheurs ont trouvé Youmi dans 256 applications iOS. Ce logiciel affiche des publicités dans les applications, tout en envoyant des informations personnelles vers un site distant à l'insu des utilisateurs.
- Les vulnérabilités présentes dans le système de transfert de fichiers sans fil Apple AirDrop pourraient permettre à un attaquant d'installer des malwares sur les appareils Apple.

### Les rançongiciels s'attaquent aux mobiles



Imaginez le choc pour un mobinaute qui télécharge une appli sympa pour finalement se retrouver avec un téléphone verrouillé et un avertissement du FBI sur son écran de démarrage. Ses options : payer une soi-disant amende et espérer que le pirate débloque son téléphone, ou bien dire adieu aux photos, contacts et souvenirs auxquels il tient.

Au vu des ventes record d'iPad et iPhone, les cybercriminels devraient intensifier leur offensive sur iOS, attirés notamment par le revenu disponible plus élevé (en moyenne) de leurs propriétaires. Privés ou professionnels, les détenteurs de produits Apple doivent se rendre à l'évidence : la marque à la pomme n'est plus synonyme d'immunité.

### Protection des terminaux mobiles

Nous conseillons aux utilisateurs et à leurs employeurs de traiter les appareils mobiles pour ce qu'ils sont, à savoir des mini-ordinateurs puissants qu'il convient de protéger en conséquence. Les mesures à prendre :

- Contrôle des accès, y compris à l'aide de dispositifs biométriques si possible
- Prévention des pertes de données avec, par exemple, un cryptage intégré
- Sauvegardes automatiques
- Outils de recherche et d'effacement à distance, en cas de perte d'un terminal
- Mises à jour régulières. Par exemple, la version 6.0 d'Android, lancée en octobre sous le nom de code « Marshmallow », intègre un certain nombre de fonctionnalités destinées à contrecarrer les attaques. D'après Statista, en octobre 2015, KitKat (version 4.4) était encore l'une des moutures les plus répandues d'Android (38,9 % des terminaux), tandis que Lollipop (version 5.0) représentait 15,6 % des appareils

<http://www.symantec.com/connect/blogs/android-banking-trojan-delivers-customized-phishing-pages-straight-cloud>  
<http://www.symantec.com/connect/blogs/android-ransomware-uses-material-design-scare-users-paying-ransom>  
[http://www.symantec.com/security\\_response/landing/azlisting.jsp?azid=1](http://www.symantec.com/security_response/landing/azlisting.jsp?azid=1)  
<http://www.symantec.com/connect/tr/blogs/new-xcodeghost-malware-variant-discovered>  
<http://www.bbc.co.uk/news/technology-34338362>  
<http://www.symantec.com/connect/blogs/yispecter-threat-shows-ios-now-firmly-attackers-agenda>  
<http://www.symantec.com/connect/blogs/ad-library-behind-pulled-ios-apps-also-used-android-development>  
<http://www.symantec.com/connect/blogs/airdrop-vulnerability-poses-threat-iphone-and-mac-users>  
<http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/>

- Installation d'applications uniquement depuis des sites et sources de confiance. Éviter le débridage des terminaux
- Circonspection à l'égard des permissions demandées par certaines applications
- Mise à jour des applications aussi régulière que possible et suppression des applications suspectes identifiées
- Changement immédiat du mot de passe de votre [ID Apple](#), ou de votre compte [Google Play](#), en cas de compromission possible de votre compte. Sans oublier la protection de vos identifiants et mots de passe sur n'importe quel app store indépendant
- Circonspection face aux e-mails suspects et aux notifications vous demandant vos identifiants ou toute autre information d'identification personnelle
- Jusqu'à l'application d'un correctif, utilisation prudente de votre navigateur mobile pour la prévisualisation de fichiers audio et vidéo non sollicités
- Installation immédiate des mises à jour de sécurité publiées par les opérateurs et fabricants d'appareils Android
- Installation de solutions de sécurité mobile dédiées pour la protection contre les logiciels malveillants. Pour les entreprises, des outils de gestion de la mobilité sont conseillés pour la sécurisation et le contrôle des terminaux mobiles

## Perspectives

Nous prévoyons une nouvelle prolifération des menaces sur les terminaux mobiles en 2016. Peut-être des kits d'exploits pour téléphones, semblables à ceux des PC, apparaîtront-ils bientôt sur le marché noir.

Dans le même temps, Apple et Google travaillent sans relâche à la sécurisation de leurs systèmes d'exploitation et de leurs écosystèmes au sens large. On peut notamment s'attendre à des améliorations dans les processus de validation, de signature et de déploiement des applications. Les détenteurs de smartphones devront donc s'habituer aux mises à jour fréquentes et automatiques de leurs applications et système d'exploitation, ainsi qu'au besoin de logiciels de sécurité sur leur appareil.

Mais peut-être devrions-nous y voir un verre à moitié plein plutôt qu'à moitié vide. Les tendances observées sont en effet le signe que les spécialistes en sécurité, les développeurs de systèmes d'exploitation et les éditeurs d'applications ont haussé leur niveau de jeu sur les questions de sécurité. Bien qu'une augmentation des attaques contre les terminaux mobiles soit à prévoir dans l'année à venir,

on peut espérer que tous ces investissements agissent de concert avec une bonne prévention pour renforcer la protection des utilisateurs.

## Menaces sur les e-mails et les communications

Les systèmes informatiques – ordinateurs et réseaux compris – sont encore la cible de malwares en constante évolution. Les e-mails restent le support de choix des cybercriminels. Leur volume a encore augmenté, tandis que les messages de phishing et de spam ont diminué, les spams représentant encore plus de la moitié du trafic e-mail entrant. En augmentation depuis 2014, les e-mails malveillants restent un vecteur efficace pour les cybercriminels, même si les spams pharmaceutiques ont montré leurs limites.

### Courrier indésirable et frauduleux

Malgré la popularité grandissante des technologies de messagerie instantanée dans les entreprises comme chez les particuliers, les e-mails continuent de dominer les communications digitales. D'après les estimations de Symantec, en 2015, environ 190 milliards de messages électroniques ont circulé chaque jour. D'ici la fin de l'année 2016, ce chiffre devrait encore augmenter de 4 %. En moyenne, chaque jour, chaque utilisateur professionnel a envoyé et reçu 42 e-mails. On note également une augmentation des messages lus sur des terminaux mobiles. En somme, pour les cybercriminels, les e-mails restent le meilleur moyen d'atteindre un maximum de personnes par voie électronique.

Bien évidemment, l'e-mail reste un véhicule important pour le spam, le phishing et les malwares. Toutefois, 2015 a été marquée par le déclin des menaces par e-mail. Les attaques de phishing et malware par e-mail représentaient ainsi environ 1 % de tous les spams. Compte tenu de la nocivité potentielle de ces menaces, Symantec fournit ici une analyse des attaques par phishing et malware pour nous aider à y voir plus clair.

Parce qu'une part importante des e-mails professionnels échangés dans le monde passent par les systèmes de filtrage de Symantec, nous bénéficions d'une perspective unique sur ce mode de communication et les menaces de sécurité qu'il représente. De nombreux messages électroniques ne sortiront jamais de l'entreprise, d'autant plus qu'environ les trois quarts des e-mails professionnels externes sont entrants, dont plus de la moitié sont des spams.

### Spam

Plus de la moitié des e-mails entrants dans les entreprises étaient des spams en 2015. Ce chiffre n'en reste pas moins le plus bas niveau enregistré depuis 2003, qui confirme une tendance à la baisse ces dernières années. Le problème n'est cependant pas près de disparaître. D'autre part, les spammeurs trouvent d'autres façons de parvenir à leurs fins, y compris via les réseaux sociaux et les messageries instantanées, deux types d'applications extrêmement utilisées sur les appareils mobiles. Ces nouveaux vecteurs viennent donc s'ajouter aux e-mails pour compléter leur arsenal.

### Phishing

Au fil des ans, le développement du marché noir a démocratisé l'accès aux campagnes de phishing. Désormais, les pirates coopèrent : certains se spécialisent dans les kits de phishing, tandis que d'autres les vendent à d'autres scammeurs qui mèneront ces campagnes.

Souvent, ces kits se vendent entre 2 \$ et 10 \$ à des utilisateurs qui n'auront besoin d'aucune compétence technique pour les exploiter ou personnaliser leurs pages web. Ces escrocs utiliseront ensuite les données volées pour leur propre compte, ou les revendront à profit sur le marché noir.

### E-mails infectés

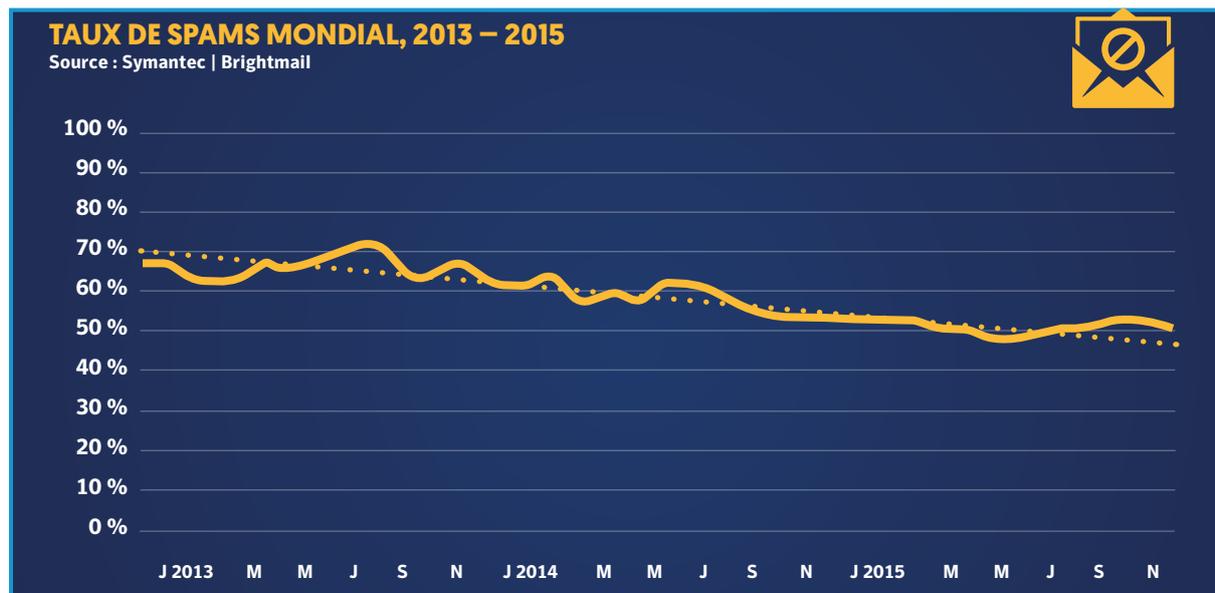
Comme pour le phishing, la diffusion de malwares par e-mail requiert des techniques d'ingénierie sociale assez convaincantes pour inciter la victime à ouvrir la pièce jointe

ou à cliquer sur le lien. Les pièces jointes peuvent être de fausses factures, des documents de bureau ou d'autres fichiers, mais elles nécessitent souvent une vulnérabilité non corrigée dans l'application logicielle associée au type de fichier. De la même façon, les liens malveillants pourront rediriger l'utilisateur vers un site web compromis qui infectera à son tour l'ordinateur du destinataire.

Les auteurs d'attaques comme Dridex utilisent exclusivement des campagnes d'e-mails de spam, avec le nom de vraies entreprises dans l'adresse de l'expéditeur et le corps du message. La grande majorité des spams Dridex se font passer pour des e-mails à caractère comptable, comme des factures, des reçus et des commandes. Ces e-mails contiennent des pièces jointes Word ou Excel malveillantes, dont la charge active libère un malware de captation d'informations de banque en ligne.

Le groupe de cybercriminels derrière cette attaque a utilisé tous les types de spams et de vecteurs de propagation de malwares possibles : des simples pièces jointes malveillantes aux liens de renvoi vers un kit d'exploits dans le corps des messages, en passant par les PDF et les macros de documents infectés.

Les malwares délivrés via e-mail n'ont pas connu le même déclin que le spam en général, sans compter que leur volume relativement bas en comparaison les expose davantage aux fluctuations. Ainsi, des pics d'activité apparaissent en cas de grosse campagne.



Pas étonnant que les cybercriminels exploitent encore largement l'e-mail pour les spams, le phishing et les malwares. Toutefois, ces graphiques révèlent une baisse de ces trois formes d'attaques en 2015.

<http://www.symantec.com/connect/blogs/phishing-economy-how-phishing-kits-make-scams-easier-operate>  
<http://www.symantec.com/connect/blogs/dridex-and-how-overcome-it>  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/dridex-financial-trojan.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf)

### TAUX D'ATTAQUES PAR PHISHING, 2013 – 2015

Source : Symantec | .cloud



### PROPORTION D'E-MAILS COMPORTANT DES VIRUS, 2013 – 2015

Source : Symantec | .cloud



### Cryptage d'e-mails

Le grand avantage du cryptage d'e-mails est de garantir la confidentialité des messages et d'authentifier les expéditeurs. Toutefois, des failles dans ses technologies sous-jacentes (voir ci-dessus) et son adoption encore partielle le rendent vulnérable.

Bien que des systèmes de messagerie web comme Microsoft Outlook.com et Google Mail appliquent un cryptage sur les clients et que presque tous les systèmes de messagerie priviligient les transmissions cryptées, une proportion incroyable d'e-mails est envoyée en clair, via des transferts SMTP non cryptés. Ainsi, selon Google, environ 40 % des messages entrants n'étaient pas chiffrés l'an dernier.

Certes, il existe de bons outils de cryptage des e-mails pour les ordinateurs et les passerelles, à commencer par celui de Symantec. Mais encore faut-il que les entreprises capitalisent pleinement sur les technologies disponibles pour protéger leurs messages en transit et dans leurs boîtes.

### Attaques par contournement du cryptage

Nous avons assisté à une succession d'attaques et de découvertes de vulnérabilités dans le cryptage sous-jacent utilisé pour la sécurisation des transmissions par e-mail. Par exemple, l'attaque baptisée Logjam exploite une faiblesse dans le mécanisme d'échange des clés qui amorce toute communication cryptée.

Pour vérifier l'éventuelle présence de Logjam et d'autres vulnérabilités majeures dans leurs domaines, les clients peuvent utiliser la Symantec SSL Toolbox. Cet outil gratuit leur permet de rechercher des failles critiques comme POODLE et Heartbleed, mais aussi d'éventuelles erreurs dans l'installation de leurs certificats SSL/TLS.

### Conseils pour la sécurité de vos e-mails

Les entreprises et les internautes doivent prendre conscience du fait que, même s'ils ne se voient pas comme une cible évidente pour les cybercriminels, cela ne signifie en rien qu'ils sont à l'abri.

C'est pourquoi une vigilance de tous les instants s'impose. Sur le plan personnel...

- N'ouvrez pas les e-mails d'expéditeurs inconnus.
- Cherchez l'icône du cadenas et vérifiez le certificat SSL/TLS de tous les sites où vous saisissez des données sensibles.
- Évitez les réseaux non sécurisés pour accéder à des données sensibles.

... mais aussi professionnel :

- Déployez des logiciels de prévention et de détection des intrusions.
- Faites l'inventaire de vos données critiques et protégez-les par un système de prévention des pertes de données.
- Surveillez l'emplacement de vos données et l'identité des utilisateurs qui y accèdent.
- Veillez à mettre en place un plan d'intervention efficace en cas d'attaque.

### Perspectives

En déclin depuis trois ans, les attaques de phishing devraient au moins stagner, voire poursuivre leur courbe descendante. Plus ciblées et moins dispersées, nombre de ces attaques s'appuient désormais sur les médias sociaux, ce qui réduit encore davantage le flux d'e-mails de phishing. Là encore, la baisse est plus marquée dans certaines régions du monde que d'autres : de nombreux pays anglophones, l'Amérique du Nord et une partie de l'Europe de l'Ouest ont ainsi enregistré les plus fortes chutes d'e-mails de phishing.

L'internetisation de nos existences et la démocratisation du web et des transactions en ligne dans les pays en développement pourraient conduire à une recrudescence du phishing dans ces régions. Paiement des factures d'eau, de gaz et d'électricité, prise de rendez-vous médicaux, dossiers d'admission aux universités, gestion de comptes "airmiles", souscription d'assurances... les « phisheurs » n'auront que l'embaras du choix.

<http://www.google.com/transparencyreport/saferemail/>  
<http://www.symantec.com/en/uk/desktop-email-encryption/>  
<http://www.symantec.com/en/uk/gateway-email-encryption/>  
<http://www.symantec.com/connect/blogs/logjam-latest-security-flaw-affect-secure-communication-protocols>  
<https://sslttools.websecurity.symantec.com/checker/views/certCheck.jsp>  
<http://www.symantec.com/connect/blogs/when-defenses-fail-case-incident-response>

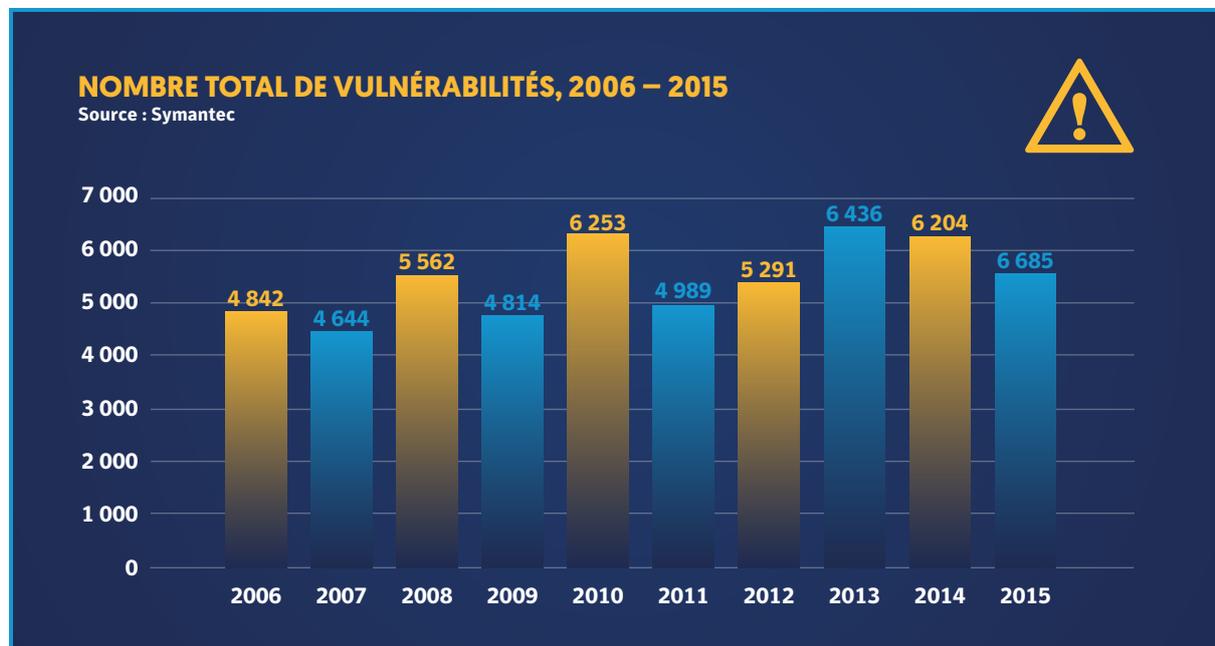
### Ordinateurs, cloud computing et infrastructure informatique

Les systèmes informatiques – ordinateurs et réseaux compris – sont encore la cible de malwares en constante évolution. Aucun système d’exploitation n’est automatiquement immunisé. En témoigne la multiplication des attaques contre Linux et Mac OS X. Même les systèmes virtuels et hébergés dans le cloud sont vulnérables. Les malwares sont capables de rechercher les environnements virtuels et de les infecter.

En somme, la cybersécurité est l’affaire de tous. Les entreprises doivent protéger leurs ordinateurs et leur infrastructure informatique pour stopper les vols, les fraudes et les attaques par malware. Les consommateurs doivent aussi les rejoindre dans leur lutte contre des cyberattaques qui peuvent crypter leurs données et les prendre en otage, mais aussi contre les vols d’identités et les détournements de leurs ordinateurs et leur utilisation comme tremplin pour d’autres attaques.

Essentiellement, la cybersécurité consiste à protéger tous les piliers de l’informatique : ordinateurs, serveurs et réseaux. Le problème est que les malwares sont absolument partout. En 2015, leur surface d’attaque s’est encore élargie, avec les environnements Linux, Mac, les postes virtuels et les systèmes cloud pris directement pour cibles. Gestion de la relation client, services de facturation, réseaux sociaux, messagerie électronique mobile... chaque année, le volume de données gérées dans le cloud s’accroît.

L’un des angles d’attaques consiste à exploiter des vulnérabilités présentes dans la plupart des systèmes. Logées dans les systèmes d’exploitation et les applications qu’ils sous-tendent, celles-ci constituent un aspect essentiel de la cybersécurité. Sans correctif, une vulnérabilité pourra ouvrir la voie à des hackers toujours prêts à l’exploiter à des fins malveillantes. Chaque année, les chercheurs découvrent de nouvelles failles, dont les plus convoitées sont qualifiées de « zero-day », ce qui signifie qu’elles ne font encore l’objet d’aucun correctif.



Ce graphique laisse entrevoir une inflexion à la baisse depuis 2013, qui s’est accentuée nettement en 2015.

### Cloud et systèmes virtuels

Le terme « cloud computing » couvre une grande variété de solutions et environnements techniques : logiciels (SaaS), plateformes (PaaS) ou encore infrastructures (IaaS) sous forme de service. De plus en plus d'entreprises deviennent adaptées du modèle « as-a-Service » pour leurs infrastructures. Or, à mesure que nos données et services migrent vers le cloud, ils attirent de plus en plus l'attention des spécialistes en sécurité, mais aussi des cybercriminels. Comme avec n'importe quel système, chaque fois qu'une nouvelle couche vient s'ajouter à un environnement de services, sa surface d'attaque s'étend. Certes, les environnements cloud pourront comporter des vulnérabilités courantes, comme celles qui permettent les injections SQL. Mais ils sont également exposés à d'autres problèmes. Par exemple, en 2015, [Symantec a découvert](#) que des erreurs de configuration et une mauvaise gestion – par les utilisateurs, et non pas de la part des fournisseurs de services cloud – rendaient certains systèmes hébergés dans le cloud vulnérables aux accès non autorisés. Pire encore, nous avons trouvé 11 000 fichiers accessibles au public, certains contenant des informations personnelles sensibles. Enfin, des identifiants et mots de passe de systèmes cloud volés se retrouvent régulièrement en vente sur le marché noir, généralement pour moins de 10 \$.

### Vulnérabilités du cloud

Les systèmes cloud ne s'avèrent pas toujours intrinsèquement moins sûrs que les services IT traditionnels. Néanmoins, les administrateurs doivent s'assurer de la bonne configuration des services cloud utilisés et de la protection adéquate de toutes les données. L'authentification à deux facteurs est notamment recommandée pour les accès aux systèmes cloud.

Attention également à des vulnérabilités comme [VENOM](#), qui permettent à un pirate de s'extraire d'une machine virtuelle (VM) invitée pour accéder au système d'exploitation hôte natif, ainsi qu'à d'autres VM hébergées sur la même plateforme. Avec le bug VENOM, les attaquants peuvent faire main basse sur les données sensibles de n'importe quelle machine virtuelle du système touché, mais aussi obtenir un accès avancé au réseau local de l'hôte et à ses systèmes. VENOM (CVE-2015-3456) est apparu pour la première fois en 2004 dans l'hyperviseur open source QEMU, souvent installé par défaut sur un certain nombre d'infrastructures utilisant Xen, QEMU et KVM. Il est important de souligner que les hyperviseurs VMware, Microsoft Hyper-V et Bochs ne comportent pas ce bug.

Jusqu'ici, on ne recense aucun cas de son exploitation par les pirates. En outre, les développeurs de QEMU et ceux des autres éditeurs concernés ont depuis créé et diffusé des correctifs pour VENOM.

Aujourd'hui, une variante de malware sur six (16 %) peut détecter la présence d'un environnement virtuel, contre une sur cinq (20 %) en 2014. Ceci permet aux malwares d'échapper à tout repérage, en particulier sur des systèmes de sécurité « sandbox » virtualisés. Plus inquiétant encore, cette sensibilité aux environnements virtuels permet aux attaquants de savoir lorsqu'il est possible d'exploiter et d'infecter d'autres VM sur le même système.

Si la moyenne des malwares capables de détecter un environnement virtuel a tourné autour de 16 % l'an dernier, le quatrième trimestre a cependant enregistré un pic à près de 22 %. C'est pourquoi il est primordial de mettre en place des solutions de sécurité robustes pour vos systèmes virtuels. Les VM et les services cloud doivent faire l'objet du même niveau de protection que vos autres services et terminaux. Vos politiques de sécurité devront donc englober les infrastructures tant virtuelles que physiques, avec l'appui d'outils de sécurité intégrés à travers toutes vos plateformes.

### Protection de l'infrastructure informatique

Face à ces menaces et beaucoup d'autres du même type, ces quelques bons conseils valent pour tous les services d'infrastructure, y compris les serveurs de fichiers, les serveurs web et autres terminaux connectés à Internet :

- Tenez-vous informés des menaces émergentes.
- Appliquez tous les correctifs et mises à jour sur vos systèmes.
- Utilisez des logiciels de sécurité intégrés, y compris pour vos technologies antimalware.
- Dotez-vous d'un pare-feu puissant qui laisse passer uniquement le trafic connu et vérifiez régulièrement les journaux d'accès pour détecter des activités potentiellement suspectes.
- Mettez en place une protection multiniveau, de façon à limiter le nombre de zones touchées en cas de compromission d'une des couches.
- Appliquez de bonnes pratiques et formez vos collaborateurs.
- N'accordez que des droits d'accès strictement nécessaires.
- Déployez un système de prévention et de détection des intrusions sur votre réseau et surveillez les services de messagerie sur votre serveur.
- Conservez toujours des sauvegardes hors site.

Pour vos systèmes cloud, nous conseillons également ces quelques précautions supplémentaires :

- Protégez tous les identifiants et mots de passe utilisés pour accéder aux fonctions d'administration du cloud et limitez l'accès à ces fonctions aux seules personnes qui en ont réellement besoin (principe du « need-to-know »).
- Veillez à bien maîtriser les paramètres de vos ressources cloud pour mieux les configurer.
- Journalisez les événements pour connaître l'identité des utilisateurs qui accèdent à vos données dans le cloud.
- Lisez bien les accords SLA de votre fournisseur cloud pour connaître ses méthodes de sécurisation de vos données.
- Intégrez vos adresses IP dans le cloud à vos processus de gestion des vulnérabilités et effectuez des audits de tous les services fournis via le cloud.

### Protégez toutes vos informations, où qu'elles se trouvent

À l'heure où les entreprises migrent leurs systèmes informatiques vers des environnements virtuels et cloud, elles doivent surmonter de nouveaux défis de sécurité. Comme toujours, la nature humaine constitue elle-même une menace, puisque les collaborateurs s'engouffrent dans la moindre faille des dispositifs pour utiliser leurs propres solutions et systèmes sans l'autorisation de l'entreprise. Baptisé « Shadow IT », ou « informatique de l'ombre », ce phénomène permet aux utilisateurs de sortir totalement du périmètre de contrôle de la DSI. Souvent, le manque de contrôle leur permet de se tourner librement vers des produits externes pour répondre à un besoin immédiat. De leur côté, les responsables informatiques doivent prendre conscience des raisons qui incitent les utilisateurs à court-circuiter le département IT dans ce type de décisions.

Le DSI doit constamment prendre le pouls de l'activité de son entreprise et repérer les besoins émergents en services et applications des différentes équipes. Il pourra ainsi mieux répondre à ces besoins et offrir des services adaptés en toute sécurité. Bref, même lorsque vos informations et données sont hébergées hors site, leur protection passe par la mise en place des bons processus.

## Les acteurs de la sécurité organisent la riposte

Certes, la technologie SSL/TLS demeure au cœur de la confidentialité, de l'authentification et du cryptage en ligne. Mais la technologie n'est rien sans une infrastructure de confiance dont l'efficacité repose sur la maintenance et la vigilance. Quant aux acteurs de la sécurité eux-mêmes, ils doivent sans cesse apprendre et s'adapter.

### Évolution du cryptage

Le 11 août 1994, Daniel Kohn vendait un CD à un ami de Philadelphie. Son ami avait alors utilisé sa carte bancaire pour déboursier 12,48 dollars, plus les frais de port. Ce geste d'apparence anodin fut en fait la toute première transaction protégée par les technologies cryptographiques.

Le lendemain, le New York Times publiait : « Alarmés par le nombre croissant de violations de sécurité signalées sur Internet, de nombreuses entreprises et particuliers hésitent à transmettre des informations sensibles, y compris des numéros de carte bancaire, des informations commerciales, ou encore des messages électroniques privés via le réseau. »

Plus de vingt ans plus tard, les inquiétudes restent les mêmes, bien que les comportements laissent supposer une plus grande appétence au risque chez les internautes, sachant que les banques les dédommageront en cas d'incident. Toutefois, sans une infrastructure SSL/TLS homogène et sécurisée, cette confiance fragile se délitera, signant ainsi la fin du commerce en ligne.

### L'union fait la force

Depuis 1994, la force du cryptage SSL/TLS a beaucoup évolué. Cette année a ainsi marqué le passage de SHA-1 à SHA-2, en réaction à l'extraordinaire augmentation des puissances de calcul qui pouvait laisser craindre un déchiffrement des algorithmes de hachage SHA-1 par simple force brute.

Ainsi, pour de nombreux experts, la vulnérabilité de l'algorithme historique n'est plus qu'une question de temps. C'est pourquoi les principaux éditeurs de navigateurs se sont accordés pour mettre fin à la prise en charge des certificats SHA-1 dans les deux prochaines années. Passé ce délai, les internautes verront s'afficher un message de mise en garde sur les sites équipés de certificats SHA-1.

« Comme Microsoft et Google, nous pensons que les certificats SHA-1 ne devraient plus être émis après le 1<sup>er</sup> janvier 2016, ni garantis au-delà du 1<sup>er</sup> janvier 2017 », déclare Mozilla. Il est même question d'avancer ces dates afin d'accélérer la transition.

Symantec offre un service de mise à niveau gratuit, mais les grandes entreprises doivent veiller à établir un plan de migration complet pour mettre à jour tous les terminaux et applications qui ne reconnaîtraient pas encore SHA-2.

### Il est temps de réagir

Une nouvelle vulnérabilité baptisée FREAK a été découverte au mois de mars (2015). Elle permet aux pirates de s'interposer lors de l'ouverture d'une connexion sécurisée entre un serveur vulnérable et un client pour forcer l'utilisation d'un mode de chiffrement beaucoup plus faible que ceux utilisés aujourd'hui. Compte tenu de la puissance des processeurs actuels, les attaquants peuvent alors aisément décrypter le message transmis.

**LORS DE LA DÉCOUVERTE DE CETTE FAILLE, LES SERVEURS HÉBERGEANT 9,6 % DU MILLION DE DOMAINES DE SITES WEB LES PLUS VISITÉS ÉTAIENT VULNÉRABLES AUX ATTAQUES. NEUF MOIS PLUS TARD, 8,5 % L'ÉTAIENT ENCORE.**

**9,6 %**

<http://www.fastcompany.com/3054025/fast-feed/youll-never-guess-what-the-first-thing-ever-sold-on-the-internet-was?partner=rss>  
<http://www.nytimes.com/1994/08/12/business/attention-shoppers-internet-is-open.html>  
<http://www.infoworld.com/article/2879073/security/all-you-need-to-know-about-the-move-to-sha-2-encryption.html>  
<https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/>  
<http://www.symantec.com/connect/blogs/freak-vulnerability-can-leave-encrypted-communications-open-attack>  
<https://freakattack.com>

## Équilibre des pouvoirs

Pour renforcer l'écosystème SSL/TLS, Symantec n'a eu de cesse de prôner l'adoption généralisée de l'Autorisation de l'Autorité de Certification DNS (CAA). Cette autorisation permet aux entreprises, ou détenteurs de DNS, de préciser le nom de l'autorité de certification (AC) autorisée à leur fournir des certificats SSL/TLS. Ainsi, si une personne mal intentionnée ou un salarié mal informé essaie d'acquérir un certificat d'une AC ne figurant pas sur la liste verte, cette AC peut vérifier le registre CAA et alerter le propriétaire du DNS concerné.

Ce mécanisme réduit le risque d'émission de certificats non autorisés à l'insu d'une entreprise, et par là même la possibilité pour un cybercriminel de créer un site de phishing avec certificat SSL/TLS.

Dans sa lutte permanente contre les certificats non autorisés, Symantec a également répondu présent à la demande de Google d'enregistrer tous les certificats EV émis sur son registre Certificate Transparency. En mars 2016, nous sommes même allés un cran plus loin en y inscrivant tous nos certificats OV et DV. Selon ses auteurs, Certificate Transparency s'inscrit en complément des logiciels de surveillance et d'audit des certificats pour créer « un cadre ouvert permettant à tous d'observer et de vérifier des certificats SSL/TLS nouveaux et existants en quasi-temps réel. »

## Transition accélérée vers Always-On SSL

D'après une étude Sandvine, aux États-Unis, près de 40 % de tout le trafic Internet aval est désormais crypté, tandis que les prévisionnistes tablent sur plus de 70 % d'ici la fin de l'année prochaine. Les ressorts de cette forte hausse :

- **Engagement des grandes entreprises.** Certains des plus grands noms d'Internet ont déjà adopté le protocole HTTPS par défaut, notamment Facebook, Twitter et, plus récemment, Netflix.
- **Classement préférentiel dans les moteurs de recherche.** En 2014, Google a annoncé que l'adoption du protocole HTTPS sur toutes les pages d'un site web le ferait remonter dans ses classements de recherche, ce qui a incité les propriétaires de sites à s'engager sur cette voie.
- **Mise à niveau d'Internet.** L'IETF (Internet Engineering Task Force), organisme normatif d'Internet, a publié une nouvelle version de l'Hypertext Transfer Protocol en 2015. Nommé HTTP/2, il devrait s'imposer comme la nouvelle norme dans un futur proche. Selon l'IETF, HTTP/2 permet une « utilisation plus efficace des ressources réseau », ce qui signifie que le nouveau protocole a été conçu pour augmenter la réactivité et les performances des sites web. En marge de cette annonce, tous les grands éditeurs de navigateurs ont déclaré que leur prise en charge de HTTP/2 se limiterait aux pages protégées par des certificats SSL/TLS. Concrètement, le cryptage sera donc obligatoire pour les sites utilisant ce nouveau standard.

L'objectif : équiper toutes les pages Internet d'un certificat SSL/TLS d'ici quelques années. Dans cette optique, Symantec collabore déjà avec des hébergeurs de sites pour intégrer le cryptage aux packages qu'ils offrent à leurs clients.

Type de certificat	Domaine validé ?	Cryptage https ?	Validation d'identité ?	Adresse validée ?	Cadenas affiché dans l'interface du navigateur ?	Barre d'adresse verte* ?
DV	Oui	Oui	Aucune	Non	Oui	Non
OV	Oui	Oui	Bonne	Oui	Oui	Non
EV	Oui	Oui	Forte	Oui	Oui	Oui

<https://casecurity.org/2013/09/25/what-is-certification-authority-authorization/>  
<https://knowledge.symantec.com/support/ssl-certificates-support/index?page=content&id=AR2177>  
<https://www.certificate-transparency.org>  
<https://www.sandvine.com/pr/2016/2/11/sandvine-70-of-global-internet-traffic-will-be-encrypted-in-2016.html>  
<http://fortune.com/2015/04/30/netflix-internet-traffic-encrypted/>  
<http://googlewebmastercentral.blogspot.co.uk/2014/08/https-as-ranking-signal.html>  
<http://tools.ietf.org/pdf/draft-ietf-httpbis-http2-17.pdf>  
[https://www.mnot.net/blog/2015/06/15/http2\\_implementation\\_status](https://www.mnot.net/blog/2015/06/15/http2_implementation_status)  
<https://www.hostpoint.ch/en/ssl/freesl.html>

### Renforcement de la confiance

Plusieurs grands éditeurs de navigateurs travaillent également à l'amélioration de leurs indicateurs visuels de sécurité, à savoir les couleurs et symboles utilisés dans la barre d'adresse pour informer les internautes sur la sécurité d'un site. Ils cherchent ainsi à indiquer clairement lorsqu'une page web sécurisée par SSL/TLS contient des éléments non protégés que les pirates peuvent modifier pour conduire une attaque par interception (man-in-the-middle). En d'autres termes, les navigateurs exposeront les manquements et les dangers que représentent des sites qui n'offrent pas de connexion sécurisée

Il ne s'agit que d'un exemple parmi d'autres de la volonté de rassurer encore davantage les internautes et cyberconsommateurs. Dans la même veine, les marques de confiance et les garanties d'achat permettent d'apaiser leurs craintes dans la mesure où ils ne peuvent ni rencontrer le propriétaire du magasin en personne, ni tenir entre leurs mains les articles qu'ils souhaitent acheter.

## NOUVEAUX INDICATEURS DE SÉCURITÉ DE MOZILLA

Extrait du [Blog sécurité de Mozilla](#)

ANCIENNE VERSION	NOUVELLE VERSION
<p><b>Sites avec certificats DV</b></p> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <span style="font-size: 24px;">←</span> <a href="https://blog.mozilla.org/security">https://blog.mozilla.org/security</a> </div>	<div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <span style="font-size: 24px;">←</span> <a href="https://blog.mozilla.org/security">https://blog.mozilla.org/security</a> </div>
<p><b>Sites avec certificats EV</b></p> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <span style="font-size: 24px;">←</span>  Mozilla Foundation (US) <a href="https://mozilla.org/en-U">https://mozilla.org/en-U</a> </div>	<div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <span style="font-size: 24px;">←</span>  Mozilla Foundation (US) <a href="https://mozilla.org/en-U">https://mozilla.org/en-U</a> </div>
<p><b>Sites avec du contenu mixte actif bloqué</b></p> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <span style="font-size: 24px;">←</span>  Mozilla Foundation (US) <a href="https://people.mozilla.org/">https://people.mozilla.org/</a> </div>	<div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <span style="font-size: 24px;">←</span>  Mozilla Foundation (US)   <a href="https://people.mozilla.org/">https://people.mozilla.org/</a> </div>
<p><b>Sites avec du contenu mixte actif autorisé</b></p> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <span style="font-size: 24px;">←</span> <a href="https://people.mozilla.org/domainnametogohere.html">https://people.mozilla.org/domainnametogohere.html</a> </div>	<div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <span style="font-size: 24px;">←</span> <a href="https://people.mozilla.org/domainnametogohere.html">https://people.mozilla.org/domainnametogohere.html</a> </div>
<p><b>Sites avec du contenu mixte passif chargé</b></p> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <span style="font-size: 24px;">←</span> <a href="https://people.mozilla.org/domainnametogohere.html">https://people.mozilla.org/domainnametogohere.html</a> </div>	<div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-bottom: 10px;"> <span style="font-size: 24px;">←</span> <a href="https://people.mozilla.org/domainnametogohere.html">https://people.mozilla.org/domainnametogohere.html</a> </div>

<https://blog.mozilla.org/security/2015/11/03/updated-firefox-security-indicators-2/>  
<https://www.nortonshoppingguarantee.com/>

## Perspectives

---

Cette rubrique vous invite à jeter un regard prospectif sur 2016 et les années à venir. Des tendances émergentes aux nouvelles thématiques, en passant par les débats en cours, nous faisons ici le point sur les développements à suivre et les sujets qui feront l'actualité de la sécurité des sites web. Pour tout savoir sur l'actu de la sécurité, n'oubliez pas de faire un détour par notre [blog Symantec Connect](#).

### À suivre

#### Multiplication des attaques de phishing

Malgré une tendance générale à la baisse ces dernières années, nous prévoyons un rebond des attaques de phishing. Deux raisons à cela : l'augmentation de la consommation de médias en ligne et la généralisation de l'accès Internet et des transactions web dans les pays en développement.

Ajoutez à cela l'internetisation de nos tâches au quotidien (paiement des factures d'eau, de gaz et d'électricité, prise de rendez-vous médicaux, dossiers d'admission aux universités, gestion de comptes "airmiles", souscription d'assurances...) et vous obtiendrez un terreau fertile pour les attaques de phishing.

#### Généralisation des pages HTTPS

On observe un réel élan de démocratisation de l'accès au cryptage, notamment par l'offre de certificats SSL/TLS en option sur certains services cloud ou d'hébergement. L'adoption des certificats SSL/TLS est ainsi montée en flèche, tant au niveau des individus que des entreprises. Cette tendance devrait très certainement s'accroître, en particulier sur le marché des certificats DV (validation de domaine).

Autre question importante : la gestion complexe des certificats SSL/TLS, née d'un flux ininterrompu d'hôtes à authentifier, sécuriser et surveiller (cf. paragraphes sur l'Internet des objets). À cet égard, les outils et services de gestion sont appelés à se multiplier au fil d'une prise de conscience collective des besoins de sécurité. L'importante couverture médiatique de certaines violations de sécurité n'est certainement pas pour rien dans cette tendance.

#### Menaces hybrides : attaques mobiles

Sans surprise, nous prévoyons une nouvelle prolifération des menaces sur les terminaux mobiles en 2016. Peut-être des kits d'exploits pour téléphones, semblables à ceux des PC, apparaîtront-ils bientôt sur le marché noir.

Le nombre de vulnérabilités découvertes sur les terminaux mobiles progresse chaque année depuis trois ans. Mais peut-être devrions-nous y voir un verre à moitié plein plutôt qu'à moitié vide. Les tendances observées sont en effet le signe que les spécialistes en sécurité, les développeurs de systèmes d'exploitation et les éditeurs d'applications ont haussé leur niveau de jeu sur les questions de sécurité. Bien qu'une hausse des attaques contre les terminaux mobiles soit à prévoir dans l'année à venir, on peut espérer que tous ces investissements agissent de concert avec une bonne prévention pour renforcer la protection des utilisateurs.

#### Besoin croissant de compétences en sécurité

Les menaces en ligne évoluent bien plus vite que nos capacités à les appréhender et à organiser la riposte. La faute à la créativité sans bornes des hackers, mais aussi à l'arrivée massive de nouveaux services Internet chaque jour. La plupart du temps, ces services sont créés par des gens dont la priorité est d'offrir quelque chose de neuf, d'utile et d'innovant. La sécurité est toujours reléguée au second plan.

Autre raison que l'on ne peut que déplorer : les compétences nécessaires au développement d'un réseau blindé sont actuellement du côté des malfaiteurs. Essentiellement formés à la création et à la maintenance d'infrastructures réseaux, les informaticiens sont souvent mal préparés aux menaces et vulnérabilités présentes sur les réseaux d'entreprise. Plus grave encore, ces salariés reconnaissent rarement le profil d'un hacker potentiel et ne comprennent pas toujours les motivations des pirates qui attaquent leur entreprise. Ainsi, des serveurs non corrigés et des réseaux mal configurés ne sont pas toujours un signe de négligence. Le plus souvent, ils résultent d'un manque d'information. Faute d'une bonne préparation, il devient bien sûr très difficile pour quiconque de prendre des mesures préventives contre les attaques sur les réseaux. Les seuls à pouvoir le faire... seraient les hackers eux-mêmes.

C'est pourquoi nous prévoyons une nouvelle croissance du marché des hackers « chevaliers blancs » qui travailleront en freelance ou pour des sociétés de conseil en sécurité informatique dans les années à venir. Leurs compétences seront en effet très recherchées dans les nombreuses entreprises qui tenteront de s'attirer les services de spécialistes des tests d'intrusion et de hackers éthiques. Les structures soumises à de strictes obligations de conformité – notamment dans des secteurs qui traitent des données sensibles comme les banques et la santé – alimenteront elles aussi cette demande.

## Sujets d'actualité

### Gros plan sur l'authentification

À mesure que les entreprises développent leur offre de services en ligne, elles doivent rester attentives aux besoins de sécurité et travailler avec leurs clients sur des actions de pédagogie et de mise en confiance. En ce sens, l'authentification à deux facteurs est devenue un impératif. Des solutions alternatives aux connexions par mot de passe commencent même à voir le jour. L'objectif : réduire le risque du phishing et les inévitables coûts associés.

Dans le même temps, Apple et Google travaillent sans relâche à la sécurisation de leurs systèmes d'exploitation et de leurs écosystèmes au sens large. On peut notamment s'attendre à des améliorations dans les processus de validation, de signature et de déploiement des applications. Les détenteurs de smartphones devront donc s'habituer aux mises à jour fréquentes et automatiques de leurs applications et système d'exploitation, ainsi qu'au besoin de logiciels de sécurité sur leur appareil.

### Internet des objets non sécurisés

Bien que le concept d'Internet des objets (IoT) ne soit pas nouveau – [il remonte à 1999](#) – il a eu particulièrement le vent en poupe ces deux dernières années. Par IoT, on entend la connexion de tous les appareils qui font notre quotidien : aujourd'hui, Internet s'imisce partout.

Dans les années à venir, ce sujet occupera sans aucun doute le devant de la scène. Toutefois, l'enthousiasme qu'a tout d'abord suscité la vie dans un monde connecté laisse

désormais place à des inquiétudes croissantes quant à la sécurité de ces appareils et les menaces potentielles qu'ils représentent. En 2015, le piratage de véhicules figurait parmi les problèmes de sécurité les plus débattus de l'IoT. Nul doute que d'autres questions du même genre devraient être évoquées à l'avenir. Une fois encore, l'intérêt croissant des médias pour ces thématiques joue un grand rôle dans la prise de conscience des dangers de l'IoT.

### Hactivisme, terrorisme, responsabilité des États et respect de la vie privée

L'hactivisme et le terrorisme n'ont jamais autant fait parler d'eux. Non seulement la Toile est devenue le vecteur numéro un de propagande et de communication de ces groupes extrémistes, mais elle s'est aussi transformée en un lieu de prédilection pour leurs démonstrations de force. Ainsi, les réseaux anonymes comme TOR ne sont plus réservés aux seuls marchés noirs. On peut aussi s'attendre à une multiplication des attaques spectaculaires à des fins politiques ou idéologiques dans les années à venir. Ce qui devrait très certainement entraîner des dommages collatéraux pour les entreprises et autres entités.

Ces dernières années, la montée en puissance de l'hactivisme a contraint les États à se pencher sur les communications cryptées en ligne. Les révélations d'Edward Snowden en 2013 concernant les programmes de surveillance mis en place par certains gouvernements ont mis au jour des pratiques que beaucoup suspectaient déjà. Pourtant, elles ont tout de même fait l'effet d'une bombe dans l'opinion publique. Depuis, le débat sur la légitimité d'un espionnage actif des citoyens par les États fait rage. La récente invalidation de l'accord Safe Harbor par la Cour européenne de justice l'a d'ailleurs relancé et ne devrait pas s'essouffler pour l'année à venir.

#### Le saviez-vous ?

Symantec a créé des certificats racines spécialement dédiés aux utilisateurs de l'Internet des objets. N'hésitez pas à nous contacter pour en savoir plus sur le déploiement de ces certificats, ou de tout autre certificat racine, sur vos appareils connectés.

## TLS 1.3 – par Ivan Ristic

L'histoire de Transport Layer Security (TLS) débute en 1994, avec la publication de SSL 2.0 – un protocole à la conception médiocre, mais suffisant pour soutenir l'essor de l'e-commerce et du web marchand à l'époque. Au cours des 22 années qui ont suivi, nous avons continué à renforcer la sécurité du protocole au fil des progrès de la cryptographie. Aujourd'hui, TLS 1.2 (publiée en 2008) en représente la dernière version stable. Largement adoptée depuis seulement 2013, cette version offre un bon niveau de protection pour les applications commerciales.

Malgré les nombreuses critiques à l'encontre de TLS ces dernières années, ce protocole a fait ses preuves, comme le montre la croissance phénoménale d'Internet et le peu d'incidents imputables au cryptage. De fait, la plupart de nos problèmes de sécurité dans ce domaine proviennent davantage de notre propre résistance à un cryptage plus généralisé et à l'adoption de protocoles plus récents et plus sécurisés. Sur le web, des progrès sont à noter : la plupart des grands sites renforcent rapidement leur sécurité. Toutefois, dans l'ensemble, le pourcentage de sites web cryptés ne dépasse probablement toujours pas les 10 %. Du côté des e-mails, nous sommes là aussi à la peine. Par exemple, en janvier 2016, si [Gmail envoyait 82 % d'e-mails via des protocoles sécurisés, seul 58 % de son courrier entrant était crypté](#). Par rapport au web, il est comparativement plus facile de crypter efficacement des messages électroniques car un petit nombre de fournisseurs de messagerie gèrent une grande proportion des e-mails mondiaux. D'autre part, la majorité des entreprises préfèrent encore un transfert non sécurisé de leurs e-mails à l'échec pur et simple des envois. Mais le vent a finalement tourné : il est évident que nous progressons vers un Internet au cryptage renforcé.

[Lancés à la fin 2012, les travaux sur la prochaine version de TLS, version 1.3, touchent à leur fin](#). Les développeurs ont récemment invité [un panel plus large de cryptographes à examiner de près les versions préliminaires du protocole](#). L'objectif : chercher les

éventuelles failles du protocole avant son déploiement, d'autant plus qu'il est appelé à sécuriser Internet pour les 20 prochaines années. En dépit du modeste changement dans son numéro de version, TLS 1.3 marque un tournant par rapport à son prédécesseur. Avantage incontournable, hormis sa sécurité renforcée, le nouveau protocole se montre plus rapide (vitesse mesurée principalement en latence réseau, ce qui constitue sa seule limite aujourd'hui).

Dans la pratique, le plus grand impact immédiat de TLS 1.3 sera la suppression du bric-à-brac digital accumulé depuis la première version de SSL, qui subsistait dans les versions 1.2 et antérieures. En fait, aujourd'hui, le principal obstacle pratique à la sécurité réside dans la formation : TLS 1.2 peut être configuré pour une protection maximale, mais pour cela il faut savoir éviter les nombreux pièges cachés. Il existe des ouvrages sur le sujet, mais ces pavés contiennent des centaines de pages. Dans la plupart des cas, les opérateurs de sites web ne possèdent pas les compétences ou n'ont tout simplement pas la motivation pour faire face à ce problème. La solution court-termiste de la communauté : lier étroitement sécurité et amélioration des performances. Par exemple, vous pouvez déployer HTTP/2 uniquement avec TLS 1.2 et à l'aide d'un sous-ensemble de fonctionnalités sécurisées. Sur le long terme, TLS 1.3 sera sécurisé par défaut, quelle que soit la configuration.

Reste à savoir comment se préparer à l'arrivée imminente de cette nouvelle version. Pour cela, commencez à réfléchir à vos besoins en sécurité et à vos solutions. Si vos sites critiques dépendent d'acteurs externes – par exemple, si vous externalisez leur hébergement ou que vous utilisez des matériels spécifiques – il est essentiel de contacter vos fournisseurs dès maintenant. Montrez-leur votre intérêt pour cette question et obtenez d'eux un engagement de prise en charge rapide des nouvelles fonctionnalités de sécurité. Après tout, votre sécurité n'est pas le seul enjeu : les performances de vos sites web sont aussi d'une importance capitale.

## Recommandations et bonnes pratiques

La sécurité des sites web repose sur une implémentation soignée, assortie d'un suivi et d'une maintenance de tous les instants. Bien que des outils existent pour assurer la sécurité de l'écosystème de votre site web, tout part d'une bonne pédagogie. Vous connaissez les risques, découvrons maintenant comment les écarter.

### Conformité aux standards du secteur

- **Implémentez Always-On SSL.** Appliquez le protocole SSL/TLS à toutes les pages de votre site web afin de crypter toutes les interactions entre votre site et vos visiteurs. Un site web entièrement protégé par HTTPS, au moyen de certificats SSL/TLS OV ou EV, prouve non seulement votre crédibilité aux yeux des internautes, elle peut également améliorer votre classement dans les résultats de recherche. De même, Always-On SSL préparera le terrain pour une évolution à terme vers HTTP/2.
- **Migrez vers SHA-2.** Comme nous l'évoquons plus haut dans ce document, les autorités de certification ont cessé toute émission de certificats SHA-1 depuis le 1<sup>er</sup> janvier 2016. À vous désormais de veiller à la migration de vos certificats existants et à la compatibilité de tous vos terminaux et applications avec SHA-2.
- **Envisagez l'ECC.** Symantec offre également l'algorithme de cryptage ECC. Tous les principaux navigateurs, y compris mobiles, prennent en charge les certificats ECC sur toutes les plateformes récentes. L'intérêt de l'ECC se situe au niveau de sa légèreté et de sa sécurité : par rapport à une clé RSA standard de 2 048 bits, les clés ECC de 256 bits s'avèrent 64 000 fois plus complexes à déchiffrer.

### Usage correct du protocole SSL/TLS

La fiabilité du protocole SSL/TLS dépend de son implémentation et de sa maintenance. Nos recommandations :

- **Gardez vos bibliothèques de protocoles à jour.** L'implémentation SSL/TLS requiert une attention de tous les instants. Par exemple, il est vital d'appliquer les correctifs ou mises à jour de vos logiciels le plus tôt possible après leur publication.
- **Ne laissez pas vos certificats expirer.** Effectuez un suivi rigoureux de vos certificats, de l'AC émettrice et

de leurs dates d'expiration. À cet égard, Symantec offre une gamme d'outils de gestion automatisés qui vous permettent de consacrer plus de temps à vos missions de prévention dans le domaine de la sécurité.

- **Affichez des marques de confiance reconnues** (comme le sceau Norton Secured) sur des points stratégiques de votre site web, comme gage de votre sérieux sur les questions de sécurité.
- **Gérez vos clés SSL/TLS avec précaution.** Limitez le nombre de personnes y ayant accès. Nommez des administrateurs différents pour la gestion des mots de passe du serveur de stockage des clés et la gestion des systèmes où les clés sont réellement stockées. Utilisez des systèmes automatisés de gestion des certificats et des clés afin de réduire les interventions humaines.

### Solution complète de sécurité des sites web

- **Procédez à des analyses régulières.** Assurez un suivi sur vos serveurs web afin de détecter tout malware ou vulnérabilité. Des outils d'automatisation peuvent vous y aider.
- **Utilisez un antivirus.** Les logiciels antivirus ne se limitent pas aux PC et smartphones. Sur vos serveurs, ils peuvent prévenir une attaque par malware grave contre toute l'infrastructure de votre site web.
- **Soyez sélectifs dans vos choix de plugins.** Votre logiciel de gestion de votre site web comporte lui aussi des vulnérabilités. Plus vous utilisez de logiciels tiers, plus vous élargissez votre surface d'attaque. Mieux vaut donc déployer uniquement ce dont vous avez réellement besoin.
- **Protégez l'ensemble de votre écosystème.** Vos applications web sont-elles protégées par un pare-feu pour éviter les attaques par injection ? La signature de code pour vos applications web est-elle sécurisée ? Disposez-vous d'outils automatiques de détection et de neutralisation d'attaques DDoS de plus en plus fréquentes ?

Symantec offre une gamme d'outils qui simplifient et optimisent la sécurité complète de vos sites web.

<http://www.symantec.com/connect/blogs/introducing-algorithm-agility-ecc-and-dsa>  
<https://www.symantec.com/en/uk/complete-website-security/>  
<http://www.symantec.com/page.jsp?id=seal-transition>

## Sensibilisation de vos salariés

Comme toujours, la protection de vos sites et serveurs est d'abord une affaire de bon sens et de bons réflexes :

- Veillez à ce que vos salariés n'ouvrent pas les pièces jointes d'expéditeurs inconnus.
- Sensibilisez-les aux risques des réseaux sociaux : offres trop belles pour être vraies, sujets racoleurs utilisés comme appâts, liens vers des pages de connexion frauduleuses, etc.
- Encouragez-les à opter pour une authentification à deux facteurs sur tous les sites web et toutes les applis qui le proposent.
- Assurez-vous qu'ils utilisent différents mots de passe pour chaque compte de messagerie, application et login – en particulier pour les sites et services professionnels.
- Rappelez-leur quelques règles de bon sens – leur anti-virus ne les immunise pas contre les sites web malveillants ou suspects.
- Mettez en place des contrôles d'accès efficaces en limitant leurs droits au strict nécessaire afin de protéger vos serveurs et vos clés privés.

## Protection des terminaux mobiles

Nous conseillons aux utilisateurs et à leurs employeurs de traiter les appareils mobiles pour ce qu'ils sont, à savoir des mini-ordinateurs puissants qu'il convient de protéger en conséquence. Les mesures à prendre :

- Contrôle des accès, y compris à l'aide de dispositifs biométriques si possible
- Prévention des pertes de données avec, par exemple, un cryptage intégré
- Sauvegardes automatiques
- Recherche et effacement à distance
- Mises à jour régulières. Par exemple, la dernière version d'Android, baptisée « Honeycomb », intègre un certain nombre de fonctionnalités destinées à contrecarrer les attaques.
- Pas de débridage des terminaux, ni de téléchargement sur des app stores inconnus
- Formation des utilisateurs, en particulier sur les dangers des permissions demandées par certaines applis
- Solutions de sécurité comme Symantec Mobility ou Norton Mobile Security

<http://www.symantec.com/connect/blogs/how-android-s-evolution-has-impacted-mobile-threat-landscape>  
<http://www.symantec.com/mobility/>  
<https://us.norton.com/norton-mobile-security>

## Travail d'équipe

La confiance des clients se bâtit au fil de multiples interactions, à travers de nombreux sites web opérés par d'innombrables entreprises. Toutefois, il suffit d'une seule mauvaise expérience sur un seul site (vol de données, téléchargement drive-by, etc.) pour ternir la réputation de toute la sphère Internet dans l'esprit du consommateur.

Comme nous le soulignons en ouverture de ce rapport, les responsables de sites web ont une réelle carte à jouer pour réduire le taux de succès des attaques et limiter le facteur risque pour les cyberconsommateurs. Pour cela, ils devront prendre des engagements fermes et enclencher des actions draconiennes.

Opter pour Symantec Website Security, c'est faire de 2016 une année prospère pour la sécurité, et une année « galère » pour la cybercriminalité.

**Opter pour Symantec Website Security, c'est faire de 2016 une année prospère pour la sécurité, et une année « galère » pour la cybercriminalité.**

Retrouvez sur notre site la liste de nos bureaux nationaux et leurs coordonnées téléphoniques.

**Pour plus d'informations sur nos produits, composez le :**

0800 90 43 51 ou +41 (0) 26 429 77 24

**Symantec**

Symantec Website Security

Tour Egée, 17, avenue de l'Arche

France

[www.symantec.fr/ssl](http://www.symantec.fr/ssl)

La reproduction ou la transmission de tout ou partie de ce document technique, sous quelque forme ou par quelque moyen que ce soit, est interdite sans l'accord écrit de son auteur.

© 2016 Symantec Corporation. Tous droits réservés. Symantec, le logo Symantec, le logo en forme de coche et le logo Norton Secured sont des marques commerciales ou des marques déposées de Symantec Corporation ou de ses filiales aux États-Unis et dans d'autres pays. Les autres noms peuvent être des marques commerciales de leurs détenteurs respectifs.