KASPERSKY lab

Kaspersky Security Bulletin 2015

PRINCIPALES STATISTIQUES POUR 2015

GREAT

#KLReport

SOMMAIRE

CHIFFRES DE L'ANNÉE

- En 2015, les solutions de Kaspersky Lab ont déjoué des tentatives d'exécution de malwares conçus pour voler l'argent via les systèmes de banques électroniques sur les ordinateurs de **1 966 324** utilisateurs.
- Des ransomwares ont été détectés sur **753 684** ordinateurs d'utilisateurs uniques, tandis que les malwares de chiffrement ont attaqué **179 209** ordinateurs.
- Sur l'année, notre antivirus Internet a détecté **121 262 075** objets malveillants uniques (scripts, codes d'exploitation, fichiers exécutables, etc.).
- Les solutions de Kaspersky Lab ont déjoué **798 113 087** attaques organisées depuis diverses ressources Internet réparties à travers le monde.
- Au cours de l'année, **34,2%** des ordinateurs des internautes ont été exposés au moins une fois à une attaque Internet.
- Afin d'organiser ces attaques via Internet, les individus malintentionnés ont utilisé **6 563 145** hôtes uniques.
- **24%** des attaques Internet bloquées par nos produits ont été organisées depuis des ressources malveillantes situées aux États-Unis.
- Notre antivirus fichiers a détecté **4 000 000** de malwares et autres programmes potentiellement indésirables sur les ordinateurs des utilisateurs.

APPLICATIONS VULNÉRABLES UTILISÉES PAR LES INDIVIDUS MALINTENTIONNÉS

En 2015, nous avons observé l'utilisation de nouvelles techniques de dissimulation de codes d'exploitation, de shellcodes et de charges utiles dont le but était de rendre la détection de l'infection et l'analyse du code malveillant plus difficiles. Et plus particulièrement, les individus malintentionnés :

- Utilisé le protocole de chiffrement Diffie-Hellman
- Dissimulé un exploit kit dans un objet Flash

Un des événements les plus marquants de l'année aura été la découverte de deux familles de vulnérabilités critiques sous Android. L'exploitation de la vulnérabilité Stagefright permettait à l'attaquant, qui avait envoyé un MMS spécial au numéro de la victime, d'exécuter un code arbitraire sur le périphérique. L'exploitation Stagefright 2 poursuivait le même objectif, mais cette fois-ci à l'aide d'un fichier média spécialement préparé.

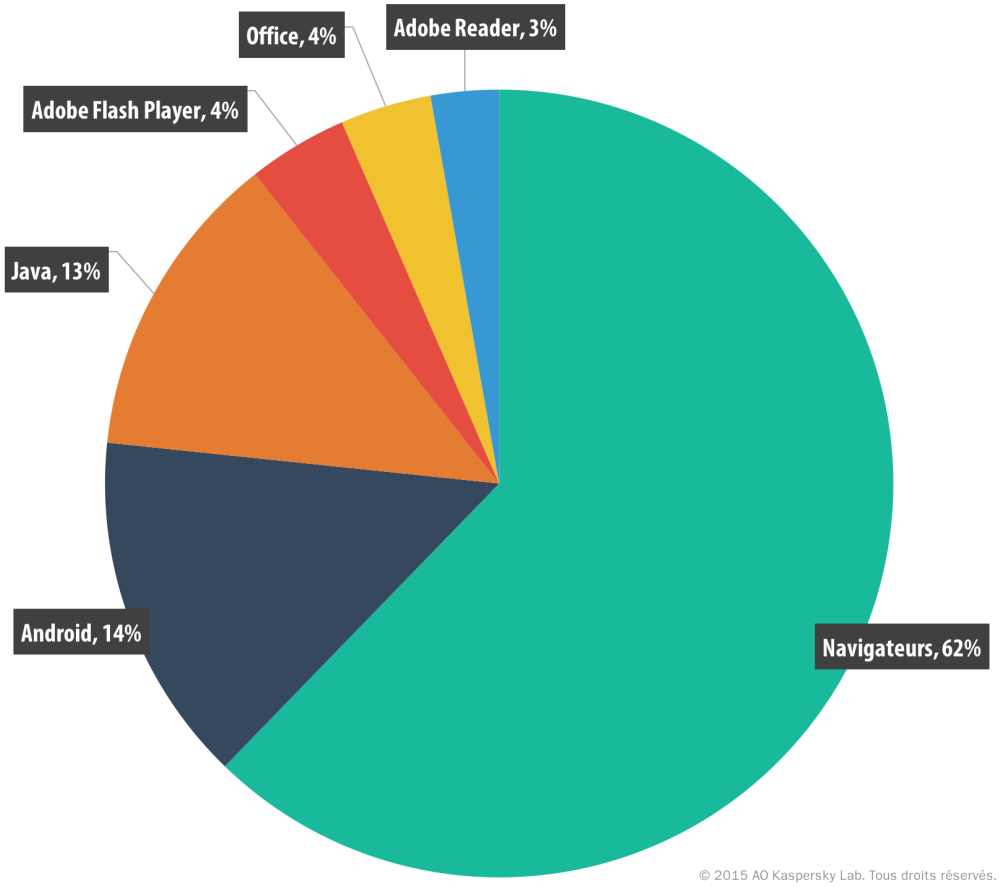
Les codes d'exploitation pour Adobe Flash Player ont été très prisés par les auteurs de virus en 2015. Cela s'explique par le nombre important de vulnérabilités détectées dans ce produit tout au long de l'année. De plus, suite à la fuite de données dont Hacking Team fut victime, des informations relatives à des vulnérabilités inconnues dans Flash Player ont été dévoilées au public et les individus malintentionnés en ont profité.

Les développeurs de différents exploit kits ont réagi efficacement à la découverte de nouvelles vulnérabilités dans Adobe Flash Player et ont enrichi leurs produits de nouveaux codes d'exploitation. Voici les vulnérabilités dans Adobe Flash Player exploitées par les individus malintentionnés et ajoutées aux exploit kits diffusés :

1. CVE-2015-0310
2. CVE-2015-0311
3. CVE-2015-0313
4. CVE-2015-0336
5. CVE-2015-0359
6. CVE-2015-3090
7. CVE-2015-3104
8. CVE-2015-3105
9. CVE-2015-3113
10. CVE-2015-5119

11. CVE-2015-5122
12. CVE-2015-5560
13. CVE-2015-7645

Comme d'habitude, certains exploit kits connus contenaient un code d'exploitation pour une vulnérabilité dans Internet Explorer (CVE-2015-2419). On aura observé également en 2015 l'infection d'utilisateurs à l'aide d'une vulnérabilité dans Microsoft Silverlight (CVE-2015-1671). Mais ce code d'exploitation ne fait pas l'objet d'une très forte demande parmi les principaux "acteurs" du marché des codes d'exploitation.



Répartition, par type d'application ciblée, des codes d'exploitation utilisés par les individus malveillants dans les attaques, 2015

Le classement des applications vulnérables repose sur les données relatives aux codes d'exploitation bloqués par nos produits et utilisés par des individus malintentionnés dans le cadre d'attaques via Internet ou lors de l'infection d'applications locales, y compris sur les appareils mobiles des utilisateurs.

Bien que la part de codes d'exploitation pour Adobe Flash Player n'atteint que 4 % dans notre classement, ils sont bien plus fréquent dans la nature. Au moment d'examiner ces statistiques, il ne faut pas oublier que les technologies de Kaspersky Lab détectent les codes d'exploitation à

différentes étapes. Par conséquent, la catégorie "Navigateurs" (62 %) reprend également les détections des landing pages qui diffusent les codes d'exploitation. Et d'après nos observations, ces pages chargent le plus souvent des codes d'exploitation pour Adobe Flash Player.

Au cours de l'année, nous avons observé une réduction du nombre de cas d'utilisation de codes d'exploitation pour Java. Alors qu'à la fin de l'année 2014, ils représentaient 45 % de l'ensemble des codes d'exploitation bloqués, ils ont perdu progressivement 32 points de pourcentage cette année pour atteindre 13%. De plus, à l'heure actuelle, les codes d'exploitation Java ne figurent dans aucun des exploit kits les plus connus.

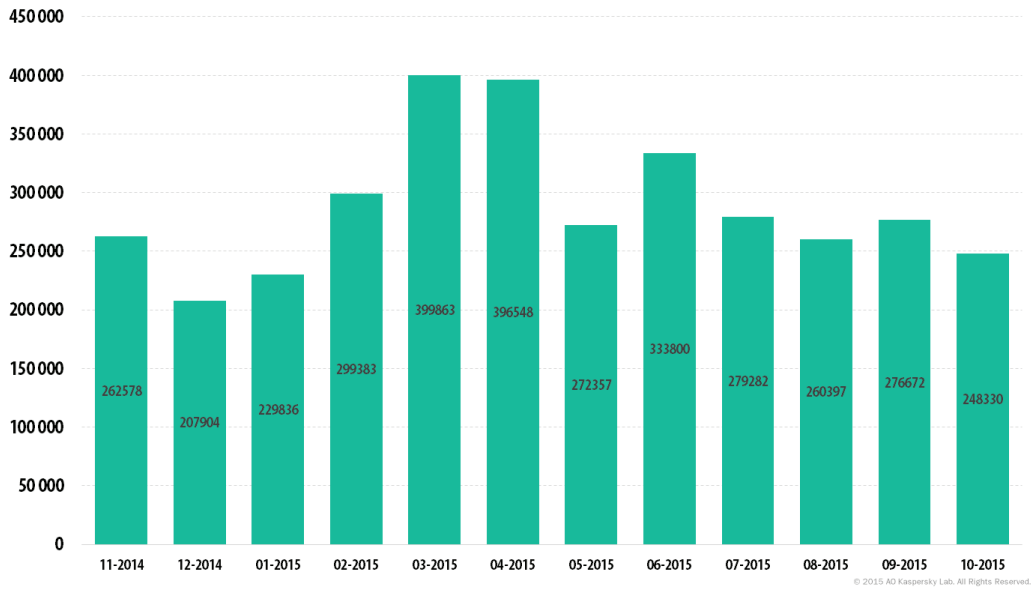
Nous avons par contre observé une augmentation de l'utilisation des codes d'exploitation pour Microsoft Office qui passe de 1 à 4 %. D'après nos observations, ces codes d'exploitation ont été propagés en 2015 dans le cadre de campagnes de spam massives.

MALWARES FINANCIERS

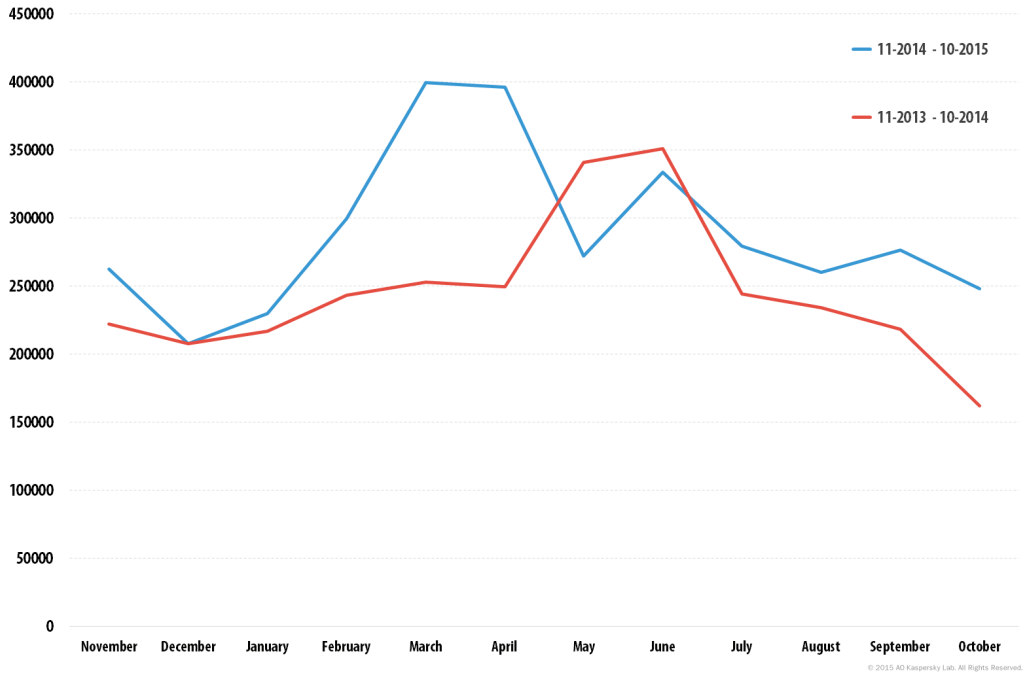
Les statistiques réelles reposent sur les verdicts détectés par les produits de Kaspersky Lab qui ont été transmis par les utilisateurs des produits de Kaspersky Lab qui avaient accepté de transmettre des statistiques.

Les statistiques annuelles pour 2015 reposent sur les données récoltées au cours de la période suivante : novembre 2014 à octobre 2015.

En 2015, les solutions de Kaspersky Lab ont déjoué des tentatives d'exécution de malwares conçus pour voler l'argent via les systèmes de banques électroniques sur les ordinateurs de **1 966 324** utilisateurs. Ce chiffre enregistre une augmentation de 2,8% par rapport à 2014 (1 910 520).



Nombre d'utilisateurs attaqués par des malwares financiers, novembre 2014 à octobre 2015

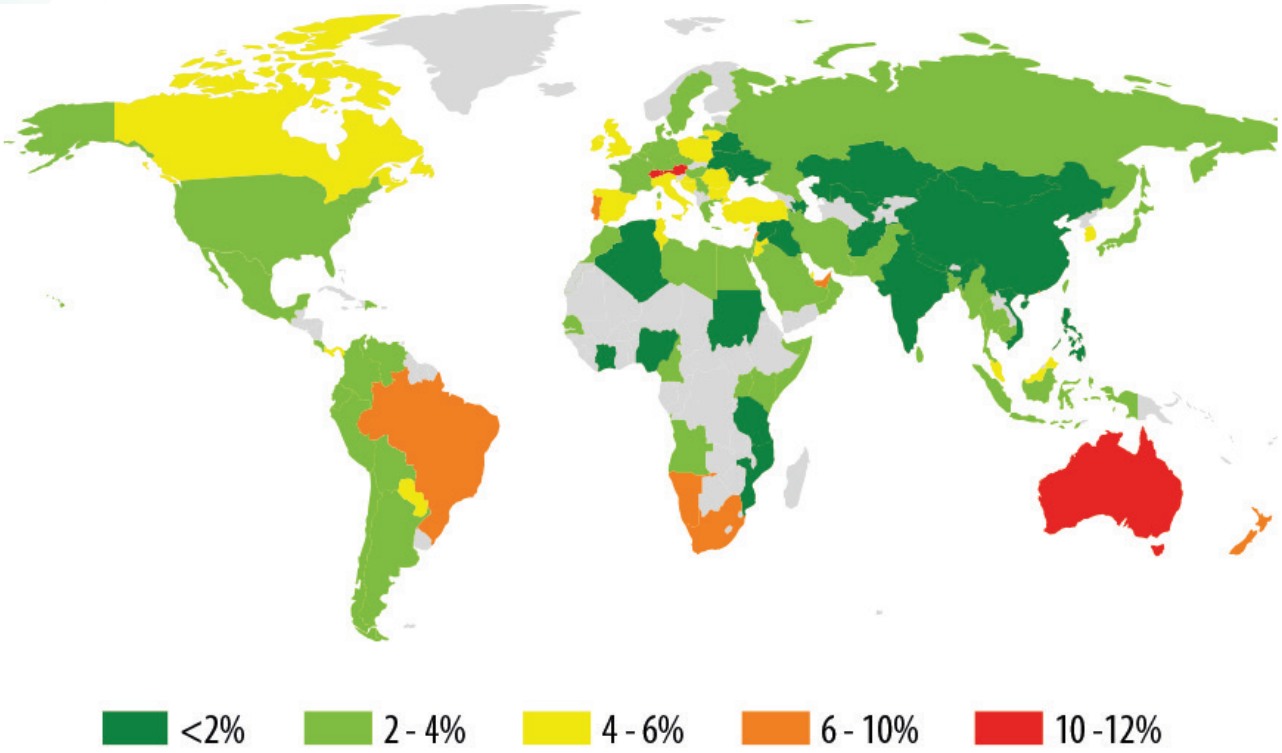


Nombre d'utilisateurs attaqués par des malwares financiers, en 2014 et 2015

En 2015, l'activité des malwares financiers a augmenté de février à avril et le pic a été enregistré en mars-avril. Une autre poussée a été enregistrée en juin. En 2014, c'est en mai-juin que le plus grand nombre d'utilisateurs avait été attaqué par des malwares financiers. De juin à octobre, en 2014 et 2015, le nombre d'utilisateurs attaqués a progressivement diminué.

Répartition géographique des attaques

Pour évaluer la popularité d'un malware financier auprès des individus malintentionnés et le risque qu'il représentait, nous avons calculé pour chaque pays le pourcentage d'utilisateurs des produits de Kaspersky Lab qui avaient été confrontés à cette menace au cours de la période couverte par le rapport sur l'ensemble des utilisateurs uniques de nos produits attaqués dans le pays.



Répartition géographique des attaques de malwares bancaires en 2015 (pourcentage d'utilisateurs attaqués par des Trojans bancaires sur l'ensemble des utilisateurs attaqués par des malwares)

Top 10 des pays en fonction du pourcentage d'utilisateurs attaqués en 2015

	Pays*	% d'utilisateurs attaqués**
1	Singapore	11.6
2	Autriche	10.6
3	Suisse	10.6
4	Australie	10.1
5	Nouvelle-Zélande	10.0
6	Brésil	9.8
7	Namibie	9.3
8	Hong Kong	9.0
9	Afrique du Sud	8.2
10	Liban	6.6

** Pour les calculs, nous avons exclu les pays où le nombre d'utilisateurs de produits de Kaspersky Lab est relativement faible (inférieur à 10 000).*
*** Pourcentage d'utilisateurs uniques de Kaspersky Lab, victimes d'attaques de malwares financiers, sur l'ensemble des utilisateurs uniques des produits de Kaspersky Lab attaqués dans le pays.*

Singapour domine ce classement. Dans ce pays, sur l'ensemble des utilisateurs de produits de Kaspersky Lab attaqués par des malwares au cours de l'année, 11,6 % ont été confrontés à des Trojans bancaires. Ce point illustre la popularité des menaces financières par rapport à toutes les autres menaces dans ce pays.

En Espagne, 5,4 % des utilisateurs attaqués ont été confrontés au moins une fois au cours de l'année à des Trojans bancaires. Ce chiffre est de 5 % pour l'Italie, 5,1 % pour la Grande-Bretagne, 3,8 % pour l'Allemagne, 2,9 % en France, 3,2 % aux États-Unis et 2,5 % au Japon.

En Russie, 2 % des utilisateurs attaqués ont été confrontés à des Trojans bancaires.

Top 10 des familles de malwares bancaires

Top 10 des familles de malwares utilisés dans le cadre d'attaques contre les utilisateurs de services de banque électronique en 2015 (part d'utilisateurs attaqués) :

	Nom*	% d'utilisateurs attaqués**
1	Trojan-Downloader.Win32.Upatre	42.36
2	Trojan-Spy.Win32.Zbot	26.38
3	Trojan-Banker.Win32.ChePro	9.22
4	Trojan-Banker.Win32.Shiotob	5.10
5	Trojan-Banker.Win32.Banbra	3.51
6	Trojan-Banker.Win32.Caphaw	3,14
7	Trojan-Banker.AndroidOS.Faketoken	2.76
8	Trojan-Banker.AndroidOS.Marcher	2.41
9	Trojan-Banker.Win32.Tinba	2.05
10	Trojan-Banker.JS.Agent	1.88

** Verdicts détectés par les produits de Kaspersky Lab. Les informations ont été fournies par les utilisateurs des produits de Kaspersky Lab qui ont accepté de transférer des statistiques.*
*** Pourcentage d'utilisateurs uniques attaqués par ce malware sur l'ensemble des utilisateurs attaqués par des malwares financiers.*

L'écrasante majorité des familles de malwares du Top 10 utilise la technique d'injection d'un code HTML arbitraire dans la page affichée par le navigateur (un classique pour les Trojans bancaires) et d'interception ultérieure des données de paiement saisies par les utilisateurs dans les formulaires en ligne originaux et ajoutés par le Trojan.

Les malwares de la famille Trojan-Downloader.Win32.Upatre ont mené ce classement tout au long de l'année. La taille de ces Trojans ne dépasse pas 3,5 Ko et leur fonction se limite au téléchargement d'une "charge utile" sur l'ordinateur infecté. Le plus souvent, il s'agit de Trojans bancaires de la famille Dyre/Dyzap/Dyreza. La tâche principale des Trojans bancaires de cette famille est le vol des données de paiement de l'utilisateur. Pour ce faire, Dyre intercepte les données de la session bancaire entre le navigateur de la victime et l'application Internet de banque électronique. En d'autres termes, il utilise la technique dite de l'homme au milieu (MITB). Signalons que ce malware se propage beaucoup à l'aide de messages électroniques spécialement créés pour l'occasion qui contiennent en pièce jointe un document avec le downloader. De plus, à l'été 2015,

l'outil Trojan-Downloader.Win32.Upatre a été remarqué sur des routeurs domestiques compromis, ce qui témoigne des nombreuses utilisations de ce Trojan pour les individus malintentionnés.

Trojan-Spy.Win32.Zbot (2e position) est un autre habitué de ce classement qui maintient sa position. Sa présence continue dans le haut du classement n'a rien d'étonnant. Les Trojans de la famille Zbot figurent parmi les premiers à avoir utilisé les injections Internet pour compromettre les données de paiement des utilisateurs de systèmes de banque électronique et modifié le contenu des pages Internet de la banque. Ils ont utilisé plusieurs niveaux de chiffrement pour leurs fichiers de configuration et le fichier de configuration déchiffré n'est pas conservé en entier dans la mémoire, mais bien chargé en plusieurs morceaux.

Les représentants de la famille de Trojans Trojan-Banker.Win32.ChePro ont été détectés pour la première fois en octobre 2012. À l'époque, ils attaquaient principalement des utilisateurs au Brésil, au Portugal et en Russie. À l'heure actuelle, ils sont utilisés dans le cadre d'attaques contre des utilisateurs de nombreux pays. La majorité des exemplaires de ChePro sont des downloaders indispensables à d'autres fichiers pour garantir la réussite d'une infection. En règle générale, ces malwares sont capables de prendre des captures d'écran, d'enregistrer les frappes au clavier, de lire le contenu du presse-papiers, etc. Autrement dit, ils possèdent des fonctions qui permettent d'utiliser ce malware dans le cadre d'attaques contre pratiquement n'importe quel système de banque électronique.

Signalons que ce classement compte la présence de deux familles de Trojans bancaires pour appareils mobiles : Faketoken et Marcher. Les malwares de cette famille volent les données de paiement depuis les appareils mobiles Android.

Les représentants de la famille Trojan-Banker.AndroidOS.Faketoken travaillent en coopération avec les Trojans bancaires pour ordinateurs. Les cybercriminels ont recours à l'ingénierie sociale pour le diffuser : Lorsqu'un client accède à la page du système de banque électronique via son ordinateur infecté, le Trojan modifie la page en question et propose de télécharger une application Android censée protéger la transaction. Le lien mène en réalité au malware Faketoken. Une fois que le malware est arrivé sur le smartphone de la victime, les criminels utilisent l'ordinateur infecté par le Trojan bancaire pour accéder au compte en banque. Le périphérique mobile infecté leur permet, quant à lui, d'intercepter le mot de passe à usage unique de l'authentification à deux facteurs (mTAN).

La deuxième famille de Trojans bancaires pour appareil mobile est Trojan-Banker.AndroidOS.Marcher. Une fois qu'ils ont infecté un appareil mobile, ces malwares sont à l'affût du lancement de deux applications seulement : le client du système bancaire mobile d'une banque européenne et Google

Play. Si l'utilisateur lance Google Play, Marcher affiche une fausse fenêtre de Google Play pour la saisie des données de la carte de crédit qui arrivent ainsi directement aux individus malintentionnés. Le Trojan adopte une technique similaire lorsque l'utilisateur ouvre l'application bancaire.

La 10e position du classement appartient à la famille Trojan-Banker. JS.Agent, un code JS malveillant qui est le résultat d'une procédure d'injection dans une page de banque électronique. Ce code vise à intercepter les données de paiement que l'utilisateur saisit dans le formulaire sur la page du système de banque électronique.

2015, UNE ANNÉE INTÉRESSANTE POUR LES RANSOMWARES

La catégorie Trojan-Ransom regroupe les malwares développés dans le but d'introduire des modifications non autorisées dans les données d'un utilisateur au point de rendre l'ordinateur inutilisable (par exemple, des malwares de chiffrement) ou de bloquer le fonctionnement normal de celui-ci. En règle générale, les propriétaires du malware exigent le versement d'une rançon pour déchiffrer les fichiers et débloquer l'ordinateur.

La catégorie Ransomware a parcouru un long chemin depuis ses débuts avec CryptoLocker en 2013. Ainsi, c'est en 2014 que nous détections la première version d'un ransomware pour Android. À peine un an plus tard, 17 % des infections que nous avons observées touchaient des périphériques Android.

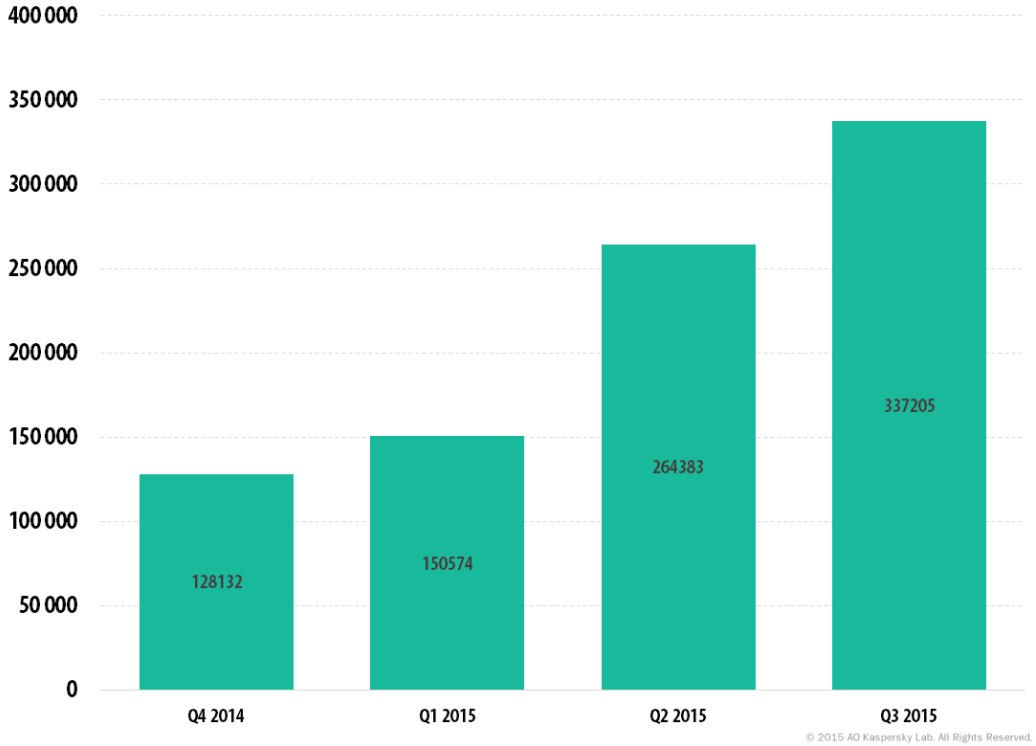
2015 aura également été l'année du premier ransomware pour Linux, dans la catégorie Trojan-Ransom.Linux. L'élément positif était que les auteurs du malware avaient commis une petite erreur de mise en œuvre qui permettait de déchiffrer les fichiers sans devoir payer la rançon.

Malheureusement, ce genre d'erreur devient de plus en plus rare. C'est ce qui avait motivé la déclaration suivante du FBI : "Les ransomware sont vraiment très forts... Pour être franc, nous conseillons souvent aux victimes de simplement payer la rançon". Comme nous avons pu le voir cette année, ce n'est pas toujours une bonne idée : après l'arrestation par la police des Pays-Bas de deux suspects liés au malware CoinVault, nous avons reçu les 14 000 clés de chiffrement que nous avons ajoutées à un nouvel outil de déchiffrement. Toutes les victimes de CoinVault ont alors pu récupérer leurs fichiers sans verser un centime.

L'année 2015 aura également été l'année de la naissance de TeslaCrypt. TeslaCrypt est connu pour utiliser les interfaces utilisateur graphiques d'autres familles de ransomwares. Au début, il avait utilisé celle CryptoLocker, puis il était passé à celle de CryptoWall. Cette fois-là, les auteurs de TeslaCrypt avait recopié complètement la page HTML de CryptoWall 3.0 et s'étaient contentés de remplacer les adresses Internet.

Nombre d'utilisateurs attaqués

Le diagramme suivant illustre l'augmentation du nombre d'utilisateurs chez qui un Trojan-Ransom a été détecté au cours de l'année dernière :



Nombre d'utilisateurs attaqués par un malware de la catégorie Trojan-Ransom (T4 2014 - T3 2015)

Sur l'ensemble de l'année 2015, des représentants de la catégorie Trojan-Ransom ont été détectés sur 753 684 ordinateurs. Les ransomwares posent donc de plus en plus de problèmes.

Top 10 des familles Trojan-Ransom

Voici le Top 10 des familles de ransomwares les plus présentes. La liste contient des familles de programme de blocage ou d'extorsion via navigateur et quelques malwares de chiffrement bien connus. Les programmes de blocage de Windows qui limitent l'accès à un système (par exemple, la famille Trojan-Ransom.Win32.Blocker) et exigent le versement d'une rançon étaient très populaires il y a quelques années. Partis de Russie, ils s'étaient propagés vers l'Ouest. De nos jours, ils ne sont plus aussi répandus et ne figurent même pas dans le Top 10.

	Nom*	Pourcentage d'utilisateurs**
1	Trojan-Ransom.HTML.Agent	38.0
2	Trojan-Ransom.JS.Blocker	20.7
3	Trojan-Ransom.JS.InstallExtension	8.0
4	Trojan-Ransom.NSIS.Onion	5.8

	Nom*	Pourcentage d'utilisateurs**
5	Trojan-Ransom.Win32.Cryakl	4.3
6	Trojan-Ransom.Win32.Cryptodef	3.1
7	Trojan-Ransom.Win32.Snocry	3.0
8	Trojan-Ransom.BAT.Scatter	3.0
9	Trojan-Ransom.Win32.Crypmod	1.8
10	Trojan-Ransom.Win32.Shade	1.8

**Ces statistiques reposent sur les verdicts de détection renvoyés par les produits de Kaspersky Lab, envoyés par les utilisateurs de produits de Kaspersky Lab qui ont accepté de fournir leurs statistiques.*
*** Pourcentage d'utilisateurs attaqués par un membre de la famille Trojan-Ransom par rapport à l'ensemble des utilisateurs attaqués par un malware Trojan-Ransom.*

Trojan-Ransom.HTML.Agent (38 %) occupe la 1re position, suivi de Trojan-Ransom.JS.Blocker (20,7 %). Ces familles représentent des pages Internet qui bloquent les navigateurs à l'aide de contenu indésirable et qui affichent en général un message d'extorsion (par exemple un "avertissement" de la police) ou qui contient un code JavaScript qui bloque le navigateur avec un message.

La 3e position revient à Trojan-Ransom.JS.InstallExtension (8 %), une page Internet de blocage de navigateur qui impose l'installation d'une extension Chrome à l'utilisateur. Souvent, si l'utilisateur tente de fermer la page, il entend un fichier vocal mp3 qui dit : «Pour fermer cette page, cliquez sur le bouton 'Ajouter'». Les extensions impliquées ne provoquent pas de dégâts, mais l'offre est très envahissante et l'utilisateur peut difficilement la rejeter. Ce type de propagation d'extension est utilisé par les programmes de partenariat. Ces trois familles sont surtout présentes en Russie, mais également dans certains pays de l'ex-URSS.

Lorsque nous analysons les zones où les ransomwares sont les plus présents (pas seulement les trois familles citées ci-dessus), nous voyons un trio de tête composé du Kazakhstan, de la Russie et de l'Ukraine.

Cryakl a été particulièrement actif en 2015. Nous avons observé des pics pouvant atteindre 2 300 tentatives d'infection par jour. Cryakl se distingue également par son modèle de chiffrement. Au lieu de chiffrer tout le fichier, Cryakl chiffre les 29 premiers octets plus trois autres blocs choisis aléatoirement dans le fichier. Ceci permet d'éviter la détection basée sur le comportement et le chiffrement des 29 premiers octets détruit l'en-tête.

Cryptodef est le tristement célèbre ransomware Cryptowall. À la différence des autres familles évoquées ici, Cryptowall se retrouve souvent aux États-Unis. En fait, on dénombre trois fois plus d'infections aux États-Unis qu'en Russie. Cryptowall se propage via des messages de spam qui contiennent un JavaScript comprimé. Une fois exécuté, le JavaScript télécharge Cryptowall et celui lance le chiffrement des fichiers.

On observe également une modification dans le message de la rançon : les victimes sont félicitées par les auteurs du malware pour «avoir rejoint la grande communauté Cryptowall».

Les programmes de chiffrement peuvent être mis en œuvre non seulement comme des fichiers exécutables, mais également à l'aide de langage de programmation de scripts simples, comme c'est le cas pour la famille Trojan-Ransom.BAT.Scatter. La famille Scatter a fait son apparition en 2014 et elle s'est développée très vite, notamment en se dotant d'une fonction Email-Worm et Trojan-PSW. Le chiffrement utilise deux paires de clés asymétriques, ce qui permet de chiffrer les fichiers de l'utilisateur sans dévoiler la clé privée. Les fichiers sont chiffrés à l'aide d'utilitaires légitimes renommés.

Le malware de chiffrement Trojan-Ransom.Win32.Shade, très présent également en Russie, est capable de solliciter au serveur de commande une liste qui contient les adresses Internet d'un autre malware. Ensuite, il télécharge ce malware et l'installe dans le système. L'ensemble de ses serveurs de commande se trouvent dans le réseau Tor. Shade serait également propagé via un programme de partenariat.

Top 10 des pays attaqués par des malwares de la catégorie Ransomware

	Pays*	% d'utilisateurs attaqués par Trojan-Ransom**
1	Kazakhstan	5,47
2	Ukraine	3,75
3	Fédération de Russie	3,72
4	Pays-Bas	1,26
5	Belgique	1,08
6	Biélorussie	0,94
7	Kirghizie	0,76
8	Ouzbékistan	0,69
9	Tajikistan	0,69
10	Italie	0,57

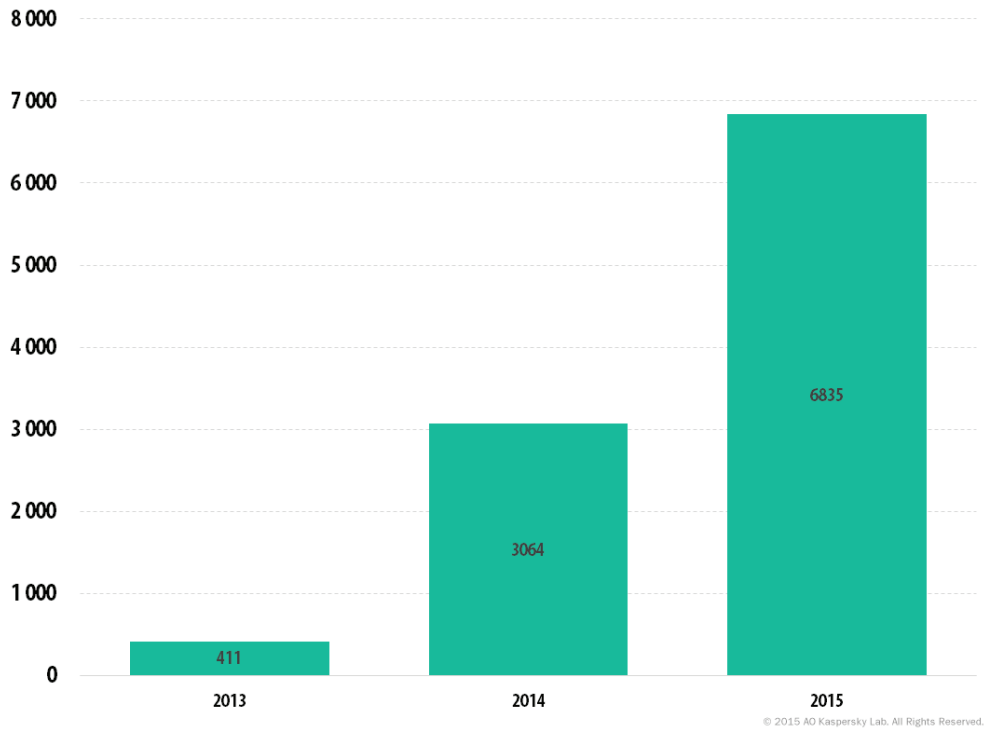
**Nous avons exclu les pays où le nombre d'utilisateurs de logiciels de Kaspersky Lab est relativement faible (moins de 10 000).*
***Utilisateurs uniques dont les ordinateurs ont été ciblés par Trojan-Ransom en tant que pourcentage de tous les utilisateurs uniques des produits de Kaspersky Lab dans le pays.*

Malware de chiffrement

Même si de nos jours, les malwares de chiffrement ne jouissent pas d'une popularité aussi grande que celle des malwares de blocage parmi les cybercriminels, ils provoquent plus de dégâts pour les utilisateurs. Il est donc important de les analyser à part.

Nombre de nouveaux malwares de chiffrement de la famille Trojan-Ransom

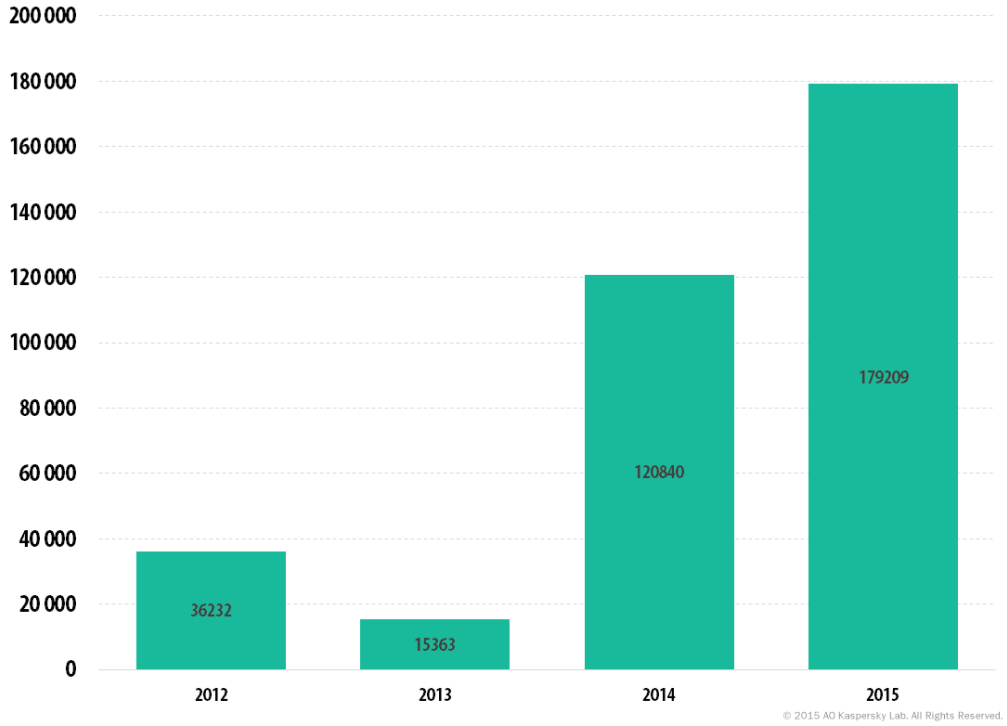
Le diagramme suivant illustre l'augmentation du nombre de nouvelles modifications de malwares de chiffrement par année.



Nombre de modifications de malwares de chiffrement de la catégorie Trojan-Ransom dans la collection de virus de Kaspersky Lab (2013 – 2015)

Le total de modifications de malwares de chiffrement dans notre collection de virus à ce jour est d'au moins **11 000**. Dix nouvelles familles de malwares de chiffrement ont vu le jour en 2015.

Nombre d'utilisateurs attaqués par des malwares de chiffrement



Nombre d'utilisateurs attaqués par un malware de chiffrement de la catégorie Trojan-Ransom (2012 - 2015)

En 2015, **179 209** utilisateurs uniques ont été attaqués par des malwares de chiffrement. Environ 20 % de ces victimes appartenaient au milieu professionnel.

Il ne faut pas oublier que le nombre réel d'incident est plusieurs fois supérieur : les statistiques ne représentent que les résultats des détections à l'aide des signatures et des méthodes heuristiques alors que dans la majorité des cas, les produits de Kaspersky Lab détectent les Trojans de chiffrement à l'aide de modèles de reconnaissance du comportement.

Top 10 des pays attaqués par des malwares de chiffrement

	Pays*	% d'utilisateurs attaqués par des malwares de chiffrement
1	Pays-Bas	1.06
2	Belgique	1.00
3	Fédération de Russie	0.65
4	Brésil	0.44
5	Kazakhstan	0.42
6	Italie	0.36
7	Lettonie	0.34
8	Turquie	0.31
9	Ukraine	0.31
10	Autriche	0.30

**Nous avons exclu les pays où le nombre d'utilisateurs de logiciels de Kaspersky Lab est relativement faible (moins de 10 000).*
***Utilisateurs uniques dont les ordinateurs ont été ciblés par un malware de chiffrement de la catégorie Trojan-Ransom en tant que pourcentage de tous les utilisateurs uniques des produits de Kaspersky Lab dans le pays.*

Les Pays-Bas occupent la 1re position. La famille de malware de chiffrement la plus répandue est CTB-Locker (Trojan-Ransom.Win32/NSIS.Onion). En 2015, un programme d'affiliés construit sur CTB-Locker a été lancé et de nouvelles langues ont été ajoutées, dont le néerlandais. Les utilisateurs sont principalement infectés par des messages électroniques avec des pièces jointes malveillantes. Il semblerait qu'un néerlandophone soit impliqué dans cette campagne d'infection car le texte des messages est rédigé dans un néerlandais presque parfait.

Une situation identique existe en Belgique : CTB-Locker est le malware de chiffrement le plus répandu dans ce pays également.

En Russie, Trojan-Ransom.Win32.Cryakl domine la liste des malwares de chiffrement qui ciblent les utilisateurs.

MALWARES SUR INTERNET (ATTAQUES VIA DES RESSOURCES INTERNET)

Les données statistiques présentées dans ce chapitre ont été obtenues via l'antivirus Internet qui protège les utilisateurs au moment de télécharger des objets malveillants depuis une page infectée. Les sites malveillants sont des sites créés spécialement par des individus malintentionnés ; les sites infectés peuvent être des sites dont le contenu est fourni par les internautes (par exemple, des forums) ou des ressources légitimes qui ont été compromises.

Top 20 des objets malveillants sur Internet

Sur l'ensemble de l'année, notre antivirus Internet a détecté **121 262 075** objets malveillants uniques (scripts, codes d'exploitation, fichiers exécutables, etc.).

Nous avons mis en avant les 20 menaces les plus souvent rencontrées sur Internet en 2015. À l'instar de l'année dernière, les logiciels publicitaires et leurs composants occupent 12 positions dans ce Top 20. Tout au long de l'année, les logiciels publicitaires et leurs composants ont été enregistrés sur 26,1 % de l'ensemble des ordinateurs des utilisateurs où notre antivirus s'est déclenché. L'augmentation du nombre de logiciels publicitaires, les méthodes agressives utilisées pour les diffuser et leur résistance à la détection par les logiciels antivirus sont des tendances qui avaient déjà été observées en 2014.

S'il est vrai que la publicité agressive peut embêter les utilisateurs, les logiciels publicitaires ne nuisent pas aux ordinateurs. Pour cette raison, nous avons créé un autre classement qui ne reprend que les objets malveillants (les programmes des catégories Adware et Riskware n'y figurent pas). Ces objets malveillants ont été responsable de 96,6 % des attaques de malwares.

	Nom*	% de l'ensemble des attaques**
1	Malicious URL	75.76
2	Trojan.Script.Generic	8.19
3	Trojan.Script.Iframer	8.08
4	Trojan.Win32.Generic	1.01
5	Expoit.Script.Blocker	0.79
6	Trojan-Downloader.Win32.Generic	0.69
7	Trojan-Downloader.Script.Generic	0.36
8	Trojan.JS.Redirector.ads	0.31

	Nom*	% de l'ensemble des attaques**
9	Trojan-Ransom.JS.Blocker.a	0.19
10	Trojan-Clicker.JS.Agent.pq	0.14
11	Trojan-Downloader.JS.Iframe.diq	0..13
12	Trojan.JS.Iframe.ajh	0.12
13	Exploit.Script.Generic	0.10
14	Packed.Multi.MultiPacked.gen	0.09
15	Exploit.Script.Blocker.u	0.09
16	Trojan.Script.Iframer.a	0.09
17	Trojan-Clicker.HTML.Iframe.ev	0.09
18	Hoax.HTML.ExtInstall.a	0.06
19	Trojan-Downloader.JS.Agent.hbs	0.06
20	Trojan-Downloader.Win32.Genome.qhcr	0.05

** Verdicts détectés du module Antivirus Internet. Les informations ont été fournies par les utilisateurs des produits de Kaspersky Lab qui ont accepté de transférer des statistiques.*
*** Pourcentage de l'ensemble des attaques via Internet de la malware enregistrées sur les ordinateurs d'utilisateurs uniques.*

Le Top 20 reprend une majorité de verdicts attribués à des objets utilisés en général dans le cadre d'attaque de type drive-by. Il sont détectés par les méthodes heuristiques sous les noms Trojan.Script.Generic, Expoit.Script.Blocker, Trojan-Downloader.Script.Generic ou autres. Les objets de cette catégorie occupent 7 positions dans notre classement.

Malicious URL est un verdict attribué aux liens de notre liste noire (liens vers des pages qui redirigent les internautes vers des codes d'exploitation, des sites hébergeant des codes d'exploitation ou d'autres malwares, vers des centres d'administration de réseaux de zombies, des sites d'arnaque, etc.)

Le verdict Trojan.JS.Redirector.ads (8e position) est attribué au script que les individus malintentionnés placent sur des ressources Internet infectées. Ce script est chargé de rediriger les utilisateurs vers d'autres sites Internet, par exemple, vers des sites de casino en ligne. L'entrée de ce verdict dans le classement doit rappeler aux administrateurs de ressources Internet à quel point il est simple d'infecter leurs sites même avec les programmes les plus élémentaires.

Le verdict Trojan-Ransom.JS.Blocker.a (9e position) est un script qui, à l'aide de la mise à jour cyclique d'une page, tente de bloquer le navigateur et affiche un message qui annonce la nécessité de payer une «amende» pour avoir consulté du contenu déplacé. L'utilisateur doit envoyé l'argent à un porte-monnaie électronique qui lui sera indiqué. Ce script figure principalement sur des sites pornographiques et il est actif en Russie et dans les pays de la CEI.

Le script qui a reçu le verdict Trojan-Downloader.JS.Iframe.diq (11e position) se retrouve également sur des sites infectés et administrés à l'aide de WordPress, Joomla et Drupal. La campagne d'infection massive de sites à l'aide de ce script a débuté en août 2015. Il commence par envoyer au serveur des individus malintentionnés des informations sur l'en-tête de la page infectée, le domaine actuel et l'adresse de la page via laquelle l'utilisateur est arrivé sur la page infectée par le script. Ensuite, un iframe permet de télécharger un autre script dans le navigateur de l'utilisateur. Ce script récolte des informations sur le système de l'ordinateur de l'utilisateur, le fuseau horaire et la présence ou non d'Adobe Flash Player. Après plusieurs redirections, l'utilisateur arrive sur un site qui propose soit d'installer une prétendue mise à jour d'Adobe Flash Player qui est en réalité un logiciel publicitaire, soit d'installer un plug-in pour le navigateur.

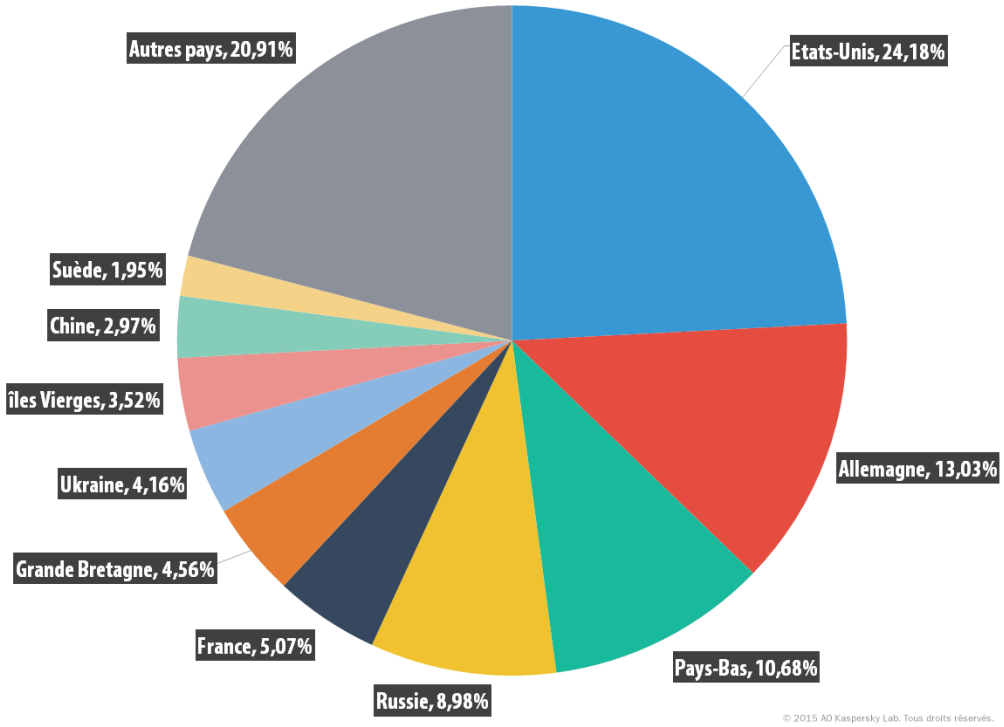
Pays source des attaques Internet : Top 10

Ces statistiques montrent la répartition par pays des sources des attaques Internet bloquées par l'Antivirus Internet sur les ordinateurs des utilisateurs (pages Internet avec redirection vers des codes d'exploitation, sites avec des codes d'exploitation et autres programmes malveillants, centres d'administration de réseaux de zombies). Signalons que chaque hôte unique peut être la source d'une ou de plusieurs attaques via Internet. Ces statistiques ne tiennent pas compte des sources de diffusion des logiciels publicitaires et des hôtes associés à l'activité de logiciels publicitaires.

Pour définir la source géographique des attaques Internet, nous avons utilisé une technique de comparaison du nom de domaine et de l'adresse IP authentique sur laquelle se trouve ce domaine et la définition de l'emplacement géographique de cette adresse IP (GEOIP).

Pour organiser les **798 113 087** attaques via Internet bloquées en 2015, les individus malintentionnés ont utilisés **6 563 145** hôtes uniques, soit un recul de 16 % par rapport à 2014.

80% des notifications relatives aux attaques Internet bloquées ont été obtenues lors du blocage d'attaques lancées depuis des ressources Internet réparties dans dix pays.



Répartition par pays des sources d'attaques Internet, 2015

Les 4 premières positions n'ont pas changé par rapport à l'année dernière. La France progresse de la 7e à la 5e position (5,07 %) et l'Ukraine recule de la 5e à la 7e position (4,16 %). Le Canada et le Viêt Nam ne figurent plus dans le classement. Ils sont remplacés par la Chine et la Suède, en 9e et 10e position respectivement.

Ce classement démontre que les cybercriminels préfèrent mener leurs activités et utiliser les services d'hébergement dans les pays développés où le marché des services d'hébergement est dynamique.

Pays dont les internautes ont été le plus exposés au risque d'infection via Internet

Pour évaluer le risque d'infection via Internet auquel sont exposés les ordinateurs des utilisateurs dans différents pays, nous avons calculé sur un an la fréquence de déclenchement de l'Antivirus Internet chez les utilisateurs des logiciels de Kaspersky Lab dans chacun des pays au cours du trimestre. Les données obtenues indiquent le degré d'agressivité de l'environnement dans lequel les ordinateurs fonctionnent dans les divers pays.

Classement des 20 pays où le risque d'infection des ordinateurs via Internet est le plus élevé

	Country*	% of unique users**
1	Russie	48.90
2	Kazakhstan	46.27
3	Azerbaïdjan	43.23
4	Ukraine	40.40
5	Viêt Nam	39.55
6	Mongolie	38.27
7	Biélorussie	37.91
8	Armenie	36.63
9	Algerie	35.64
10	Qatar	35.55
11	Lettonie	34.20
12	Népal	33.94
13	Brésil	33.66
14	Kirghizstan	33.37
15	Moldovie	33.28
16	Chine	33.12
17	Thaïlande	32.92
18	Lituanie	32.80
19	Emirats arabes unis	32.58
20	Portugal	32.31

Ces statistiques reposent sur les verdicts détectés par l'Antivirus Internet et transmis par les utilisateurs des produits de Kaspersky Lab qui ont accepté de partager les données statistiques.

** Pour les calculs, nous avons exclu les pays où le nombre d'utilisateurs de produits de Kaspersky Lab est relativement faible (inférieur à 10 000).*

***Pourcentage d'utilisateurs uniques exposés à des attaques sur Internet, sur l'ensemble des utilisateurs uniques des produits de Kaspersky Lab dans le pays.*

Le trio de tête de ce classement pour 2015 n'a pratiquement pas changé par rapport à 2014. La Russie conserve la tête du classement, mais le pourcentage d'utilisateurs uniques y a diminué de 4,9 points de pourcentage.

L'Allemagne, le Tadjikistan, la Géorgie, l'Arabie saoudite, l'Autriche, le Sri Lanka et la Turquie ne figurent plus dans le classement. Parmi les nouvelles entrées, citons la Lettonie, le Népal, le Brésil, la Chine, la Taïlande, les Emirats arabes unis et le Portugal.

Les pays peuvent être répartis en trois catégories en fonction du risque d'infection pendant la navigation sur Internet.

1. **Groupe à risque élevé**

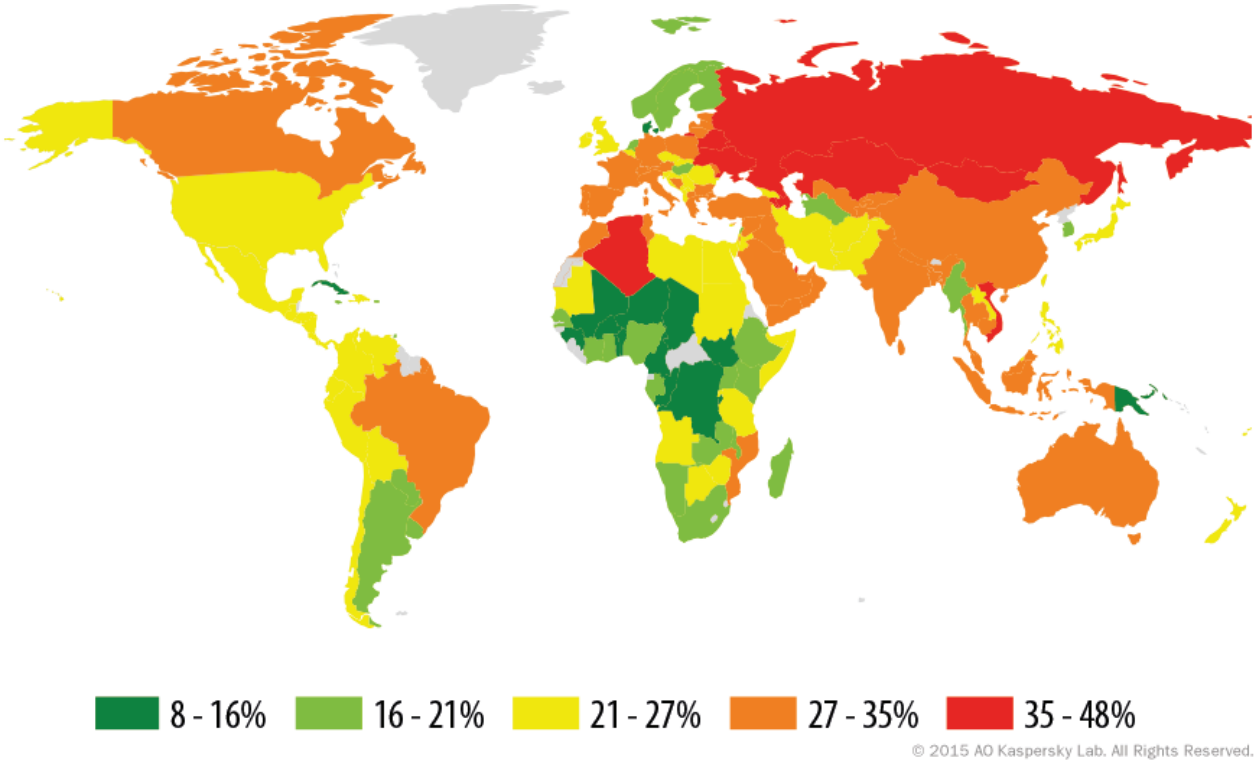
   Ce groupe réunit les pays où la probabilité d'infection est supérieure à 41 %. On y trouve les 3 premiers pays du Top 20, à savoir la Russie, le Kazakhstan et l'Azerbaïdjan. Il a diminué puisqu'en 2014, 9 pays appartenaient à ce groupe.

2. **Groupe à risque**

   Ce groupe, qui réunit les pays où la probabilité d'infection est comprise entre 21 et 40,9 %, compte 109 pays, dont : la France (32,1 %), l'Allemagne (32,0 %), l'Inde (31,6 %), l'Espagne (31,4 %), la Turquie (31,0 %), la Grèce (30,3 %), le Canada (30,2 %), l'Italie (29,4 %), la Suisse (28,6 %), l'Australie (28,0 %), la Bulgarie (27,0 %), les États-Unis (26,4 %), la Géorgie (26,2 %), Israël (25,8 %), le Mexique (24,3 %), l'Egypte (23,9 %), la Roumanie (23,4 %), la Grande-Bretagne (22,4 %), la République tchèque (22,0 %), l'Irlande (21,6 %) et le Japon (21,1 %).

3. **Groupe des pays les plus sûrs en terme de navigation sur Internet**

   Ce groupe comprend 52 pays. On y retrouve entre autres : le Kenya (20,8 %), la Hongrie (20,7 %), Malte (19,4 %), les Pays-Bas (18,7 %), la Norvège (18,3 %), l'Argentine (18,3 %), Singapour (18,2 %), la Suède (18 %), la Corée du Sud (17,2 %), la Finlande (16,5 %) et le Danemark (15, 2 %).



En 2015, **34,2%** des ordinateurs des internautes ont été exposés au moins une fois à des attaques via Internet pendant la navigation.

Sur l'ensemble de l'année, le niveau de danger d'Internet a diminué en moyenne de 4,1 points de pourcentage. Cette tendance à la baisse s'est amorcée en 2014 et se maintient pour la deuxième année consécutive. Elle peut s'expliquer par plusieurs facteurs :

- Tout d'abord, les développeurs des navigateurs et des moteurs de recherche, qui se soucient de la sécurité de leurs utilisateurs, ont contribué à la lutte contre les sites malveillants.
- Deuxièmement, les utilisateurs naviguent de plus en plus souvent à l'aide de leur appareil mobile ou de leur tablette.
- Troisièmement, de nombreux exploit kits ont commencé à vérifier si nos produits étaient installés sur les ordinateurs des victimes potentielles. Si c'est le cas, les codes d'exploitation évitent d'attaquer l'ordinateur.

MENACES LOCALES

Les statistiques relatives aux infections locales des utilisateurs sont un indicateur important. Elles reprennent les objets qui sont parvenus sur un ordinateur via l'infection de fichiers ou de disques amovibles, ou les objets qui sont arrivés sur l'ordinateur de manière dissimulée (par exemple, des programmes au sein de programmes d'installation complexes, des fichiers chiffrés, etc.) En outre, ces statistiques tiennent compte également des objets détectés sur les ordinateurs des utilisateurs après la première analyse du système par l'antivirus fichiers de notre solution.

Ce chapitre est consacré à l'analyse des données statistiques obtenues sur la base du fonctionnement de l'antivirus qui analyse les fichiers sur le disque dur lors de leur création ou lorsqu'ils sont sollicités ainsi que les données tirées de l'analyse de divers disques amovibles.

Sur l'ensemble de l'année 2015, 4 millions de malwares et programmes potentiellement indésirables ont été recensés. Soit le double de l'année dernière.

Top 20 des objets malveillants découverts sur les ordinateurs des utilisateurs

Nous avons mis en avant les 20 menaces les plus souvent rencontrées sur les ordinateurs des utilisateurs en 2015. Ce classement ne reprend pas les programmes des catégories Adware et Riskware.

	Nom*	% d'utilisateurs uniques attaqués**
1	DangerousObject.Multi.Generic	39.70
2	Trojan.Win32.Generic	27.30
3	Trojan.WinLNK.StartPage.gena	17.19
4	Trojan.Win32.AutoRun.gen	6.29
5	Virus.Win32.Sality.gen	5.53
6	Worm.VBS.Dinihou.r	5.40
7	Trojan.Script.Generic	5.01
8	DangerousPattern.Multi.Generic	4.93
9	Trojan-Downloader.Win32.Generic	4.36
10	Trojan.WinLNK.Agent.ew	3.42
11	Worm.Win32.Debris.a	3.24
12	Trojan.VBS.Agent.ue	2.79
13	Trojan.Win32.Autoit.cfo	2.61

	Nom*	% d'utilisateurs uniques attaqués**
14	Virus.Win32.Nimnul.a	2.37
15	Worm.Script.Generic	2.23
16	Trojan.Win32.Starter.lgb	2.04
17	Worm.Win32.Autoit.aiy	1.97
18	Worm.Win32.Generic	1.94
19	HiddenObject.Multi.Generic	1.66
20	Trojan-Dropper.VBS.Agent.bp	1.55

Ces statistiques sont les verdicts détectés par les modules OAS et ODS de l'Antivirus transmis par les utilisateurs de logiciels de Kaspersky Lab qui ont accepté de transmettre des statistiques.

** Verdicts détectés par les modules OAS et OAD de l'antivirus et transmis par les utilisateurs des produits de Kaspersky Lab qui ont accepté de partager les données statistiques.*

*** Pourcentage d'utilisateurs uniques sur les ordinateurs desquels l'Antivirus Fichiers a détecté l'objet, par rapport à l'ensemble des utilisateurs uniques des produits de Kaspersky Lab chez qui l'Antivirus s'est déclenché suite à la détection d'un programme de la malware.*

Le verdict DangerousObject.Multi.Generic occupe la 1re position (39,70%). Il est attribué aux malwares détectés à l'aide des technologies Cloud. Ces technologies interviennent lorsque les bases antivirus ne contiennent pas encore les définitions et qu'il n'est pas possible de détecter le programme malveillant à l'aide de l'analyse heuristique, mais l'éditeur de logiciels antivirus dispose déjà dans le « nuage » d'informations relatives à l'objet. En général, c'est ainsi que sont détectés les programmes malveillants les plus récents.

La part des virus continue de chuter : par exemple, Virus.Win32.Sality.gen avait été détecté l'année dernière chez 6,69% des utilisateurs. Ce chiffre n'est que de 5,53% en 2015. En 2014, Virus.Win32.Nimnul.a avait atteint 2,8 %. Il passe à 2,37 % en 2015. Le verdict rojan-Dropper.VBS.Agent.bp qui occupe la 20e position du classement est un script VBS qui extrait et installe Virus.Win32.Nimnul sur le disque.

En plus des verdicts heuristiques et des virus, le Top 20 contient également des verdicts pour les vers, qui se propagent via les disques amovibles, et leurs composants. Le présence dans le Top 20 s'explique par leur diffusion et la création de plusieurs copies. Le ver peut continuer à se propager pendant de longues périodes, même si ses serveurs d'administration ne fonctionnent plus.

Pays où les ordinateurs des utilisateurs ont été le plus exposés au risque d'infection locale

Pour chaque pays, nous avons calculé le nombre de fois où les utilisateurs ont été exposés à des déclenchements de l'Antivirus Fichiers. Nous avons tenu compte des objets détectables trouvés directement sur les ordinateurs des utilisateurs ou sur les disques amovibles connectés (carte mémoire d'appareil photo, de téléphone, disques durs externes). Ces statistiques indiquent le degré d'infection des ordinateurs dans différents pays.

Top 20 des pays en fonction du degré d'infection des ordinateurs

	Pays*	% d'utilisateurs uniques**
1	Viêt Nam	70.83
2	Bangladesh	69.55
3	Russie	68.81
4	Mongolie	66.30
5	Arménie	65.61
6	Somalie	65.22
7	Géorgie	65.20
8	Népal	65.10
9	Yémen	64.65
10	Kazakhstan	63.71
11	Irak	63.37
12	Iran	63.14
13	Laos	62.75
14	Algérié	62.68
15	Cambodge	61.66
16	Rwanda	61.37
17	Pakistan	61.36
18	Syrie	61.00
19	Palestine	60.95
20	Ukraine	60.78

Les statistiques réelles reposent sur les verdicts détectés de l'Antivirus Fichiers qui ont été signalés aux utilisateurs des produits de Kaspersky Lab qui avaient accepté de transmettre des statistiques.

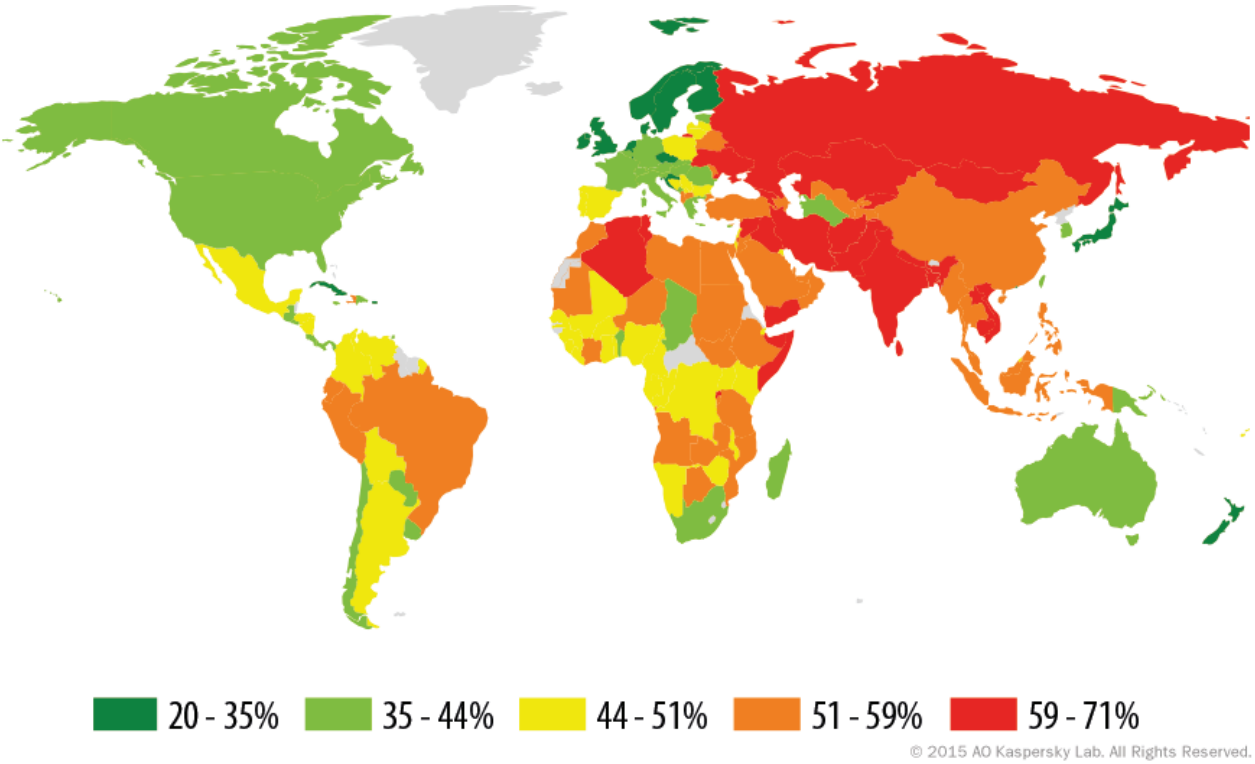
** Pour les calculs, nous avons exclu les pays où le nombre d'utilisateurs de produits de Kaspersky Lab est relativement faible (inférieur à 10 000).*

***Pourcentage d'utilisateurs uniques sur les ordinateur desquels des menaces locales ont été bloquées, par rapport à l'ensemble des utilisateurs uniques de produits de Kaspersky Lab dans le pays.*

Pour la troisième année consécutive, le Viêt Nam occupe la tête de ce classement. La Mongolie et le Bangladesh ont échangé leurs positions : la Mongolie passe de la 2e à la 4e position, tandis que le Bangladesh progresse de la 4e à la 2e place. La Russie, absente du Top de l'année dernière, fait son entrée directement en 3e position.

L'Inde, l'Afghanistan, l'Egype, l'Arabie saoudite, le Soudan, le Sri Lanka, le Myanmar et la Turquie ne figurent pas dans le Top 20 de cette année. La Russie, l'Arménie, la Somalie, la Géorgie, l'Iran, le Rwanda, les territoires palestiniens et l'Ukraine figurent parmi les nouvelles entrées.

En moyenne, un objet malveillant a été détecté au moins une fois sur l'ordinateur (disque dur ou disque amovible connecté) chez 67,7 % des utilisateurs de KSN qui nous ont fourni des informations dans les pays de ce Top 20. En 2014, cette valeur avait atteint 58,7 %.



Dans le cas des menaces locales, nous pouvons répartir les pays en plusieurs catégories.

1. **Niveau maximum d'infection (supérieur à 60 %) :** Ce groupe compte 22 pays, dont : la Kirghizie (60,77 %), l'Afghanistan (60,54 %).
2. **Niveau d'infection élevé (41 à 60 %) :** Ce groupe compte 98 pays dont l'Inde (59,7 %), l'Egypte (57,3 %), la Biélorussie (56,7 %), la Turquie (56,2 %), le Brésil (53,9 %), la Chine (53,4 %), les Emirats arabes unis (52,7 %), la Serbie (50,1 %), la Bulgarie (47,7 %), l'Argentine (47,4 %), Israël (47,3 %), la Lettonie (45,9 %), l'Espagne (44,6 %), la Pologne (44,3 %), l'Allemagne (44,0 %), la Grèce (42,8 %), la France (42,6 %), la Corée (41,7 %), l'Autriche (41,7 %).
3. **Niveau d'infection moyen (21 à 40,9 %) :** Ce groupe compte 45 pays, dont la Roumanie (40,0 %), l'Italie (39,3 %), le Canada (39,2 %), l'Australie (38,5 %), la Hongrie (38,2 %), la Suisse (37,2 %), les États-Unis (36,7 %), la Grande-Bretagne (34,7 %), l'Irlande (32,7 %), les Pays-Bas (32,1 %), la

République tchèque (31,5 %), Singapour (31,4 %), la Norvège (30,5 %), la Finlande (27,4 %), la Suède (27,4 %), le Danemark (25,8 %), le Japon (25, 6 %).

Voici le Top 10 des pays les plus sûrs en matière d'infection locale :

	Pays	%*
1	Cuba	20.8
2	Seychelles	25.3
3	Japon	25.6
4	Danemark	25.8
5	Suède	27.4
6	Finlande	27.4
7	Andorre	28.7
8	Norvège	30.5
9	Singapour	31.4
10	République tchèque	31.5

**Pourcentage d'utilisateurs uniques sur les ordinateur desquels des menaces locales ont été bloquées, par rapport à l'ensemble des utilisateurs uniques de produits de Kaspersky Lab dans le pays.*

Par rapport à 2014, cette liste a été modifiée : Andorre fait son entrée, tandis que la Martinique n'y figure plus.

En moyenne, dans les dix pays les plus sûrs, 26,9 % des ordinateurs des utilisateurs ont été attaqués au moins une fois au cours de l'année. Par rapport à l'année dernière, ce résultat a augmenté de 3,9 points de pourcentage.

CONCLUSION

L'analyse des statistiques permet de dégager les grandes tendances au niveau du développement de l'activité des cybercriminels :

- Une partie des personnes impliquées dans des activités cybercriminelles tente de réduire le risque de poursuites judiciaires et abandonne les attaques à l'aide de malwares au profil d'une diffusion agressive de logiciels publicitaires.
- La part des programmes simples utilisés dans des attaques massives augmente. Cette démarche permet aux individus malintentionnés d'actualiser rapidement le malware, ce qui contribue à l'efficacité de l'attaque.
- Les individus malintentionnés ont conquis les plateformes non-Windows comme Android et Linux : presque tous les types de malwares existent pour ces platerformes et ils sont activement utilisés.
- Dans le cadre de leurs opérations, les cybercriminels adoptent les technologies modernes qui contribuent à l'anonymat : Tor pour cacher les serveurs de commande et les bitcoins pour réaliser les transactions.

Une part de plus en plus importante des déclenchements de l'antivirus est imputable aux programmes de la « zone grise » : il s'agit principalement de différents logiciels publicitaires et de leurs modules. Dans notre Top 20 des menaces via Internet pour 2015, les représentants de cette catégorie de programmes occupent 12 places. Tout au long de l'année, les logiciels publicitaires et leur composants ont été enregistrés sur 26,1 % de l'ensemble des ordinateurs des utilisateurs où notre antivirus s'est déclenché. L'augmentation du nombre de logiciels publicitaires, les méthodes agressives utilisées pour les diffuser et leur résistance à la détection par les logiciels antivirus sont des tendances qui avaient déjà été observées en 2014. La diffusion de tels programmes peut rapporter beaucoup d'argent et leurs auteurs, dans la course aux revenus, utilisent parfois des astuces et des techniques propres aux malwares.

La popularité des codes d'exploitation pour Adobe Flash Player parmi les auteurs de virus a augmenté en 2015. Et d'après nos observations, ces pages avec codes d'exploitation chargent le plus souvent des codes d'exploitation pour Adobe Flash Player. Deux raisons peuvent expliquer cela. Tout d'abord, un nombre important de vulnérabilités a été détecté dans ce produit tout au long de l'année. Deuxièmement, suite à la fuite

de données dont Hacking Team fut victime, des informations relatives à des vulnérabilités inconnues dans Flash Player ont été dévoilées au public et les individus malintentionnés en ont profité.

Une modification intéressante est survenue parmi les Trojans bancaires. Les innombrables modifications du Trojan ZeuS qui ont occupé la tête du classement pendant de nombreuses années ont été remplacées par le malware Trojan-Banker.Win32.Dyreza. Au cours de l'année 2015, le classement des malwares développés pour voler de l'argent via les systèmes de banques électroniques a été dominé par Upatre qui téléchargeait sur l'ordinateur des victimes des Trojans bankers de la famille connue sous le nom Dyre/Dyzap/Dyreza. Parmi toutes les menaces bancaires, la part d'utilisateurs attaqués par Dyreza a atteint plus de 40 %. Ce malware bancaire utilise un mode efficace d'injections Web dans le but de voler les données d'accès au système de banque électronique.

Signalons également que deux familles complètes de Trojans bancaires pour appareils mobiles, à savoir Faketoken et Marcher, figurent dans le Top 10 des malwares bancaires pour 2015. Sur la base de ces tendances, nous pouvons supposer que l'année prochaine, les malwares bancaires pour appareils mobiles occuperont un pourcentage plus important de notre classement.

L'année 2015 aura également l'année du changement parmi les Trojans ransomwares :

1. Alors que la popularité des malwares de blocage chute progressivement, le nombre d'utilisateurs attaqués par des malwares de chiffrement a augmenté quant à lui de 48,3 % en un an. Le chiffrement des fichiers au lieu du simple blocage de l'ordinateur est une méthode qui, dans la majorité des cas, ne permet pas à la victime de récupérer facilement l'accès à l'information. Les individus malintentionnés utilisent beaucoup les malwares de chiffrement dans le cadre d'attaques contre des utilisateurs professionnels qui sont plus souvent disposés à payer la rançon que les utilisateurs particuliers. L'apparition en 2015 du premier Trojan de chiffrement pour Linux visant les serveurs Web confirme ce phénomène.
2. Les malwares de chiffrement comptent souvent plusieurs modules et outre la fonction de chiffrement, ils sont également dotés d'une fonction du vol de données sur les ordinateurs.
3. Si Linux vient à peine de tomber dans le collimateur des individus malintentionnés, le premier Trojan ransomware pour Android a été détecté quant à lui en 2014. En 2015, le nombre d'attaques ciblant le système d'exploitation Android a constamment augmenté et à l'issue de l'année, 17 % des attaques de ransomwares ont été bloquées sur des périphériques tournant sous Android.

4. La menace se propage à travers le monde entier : les produits de Kaspersky Lab ont détecté des Trojans de type ransomware dans 200 pays et territoires, autrement dit presque partout.

Nous nous attendons à ce que le développement de malwares de chiffrement axés sur les plates-formes non-Windows se poursuive en 2016 : augmentation de la part d'Android et apparition de malwares de chiffrement pour Mac OS. Quand on sait qu'Android est beaucoup utilisé dans l'électroménager, on peut s'attendre aux premières attaques de malware de chiffrement contre des objets «intelligents».

Viruslist, la ressource pour la recherche technique, les analyses et réflexions des experts Kaspersky Lab.

Suivez-nous

Site Kaspersky Lab

Blog Eugène Kaspersky

Blog Kaspersky Lab B2C

Blog Kaspersky Lab B2B

Service info sécurité Kaspersky Lab

Académie Kaspersky Lab

Twitter.com/
kasperskyfrance

Facebook.com/
kasperskylabfrance

AO Kaspersky Lab, Rueil, France
www.kaspersky.fr

Informations sur la sécurilté online :
www.viruslist.com/fr
www.kaspersky.fr/entreprise-securite-it/

Informations sur les partenaires proches de chez vous :
http://www.kaspersky.fr/partners