KASPERSKY lab

Kaspersky Security Bulletin 2015

EVOLUTION DES MENACES CONTRE LA SÉCURITÉ INFORMATIQUE DANS LES ENTREPRISES

GREAT

#KLReport

SOMMAIRE

A la fin de l'année 2014, nous avions publié nos prévisions sur les types d'événements qui marqueraient 2015 sur le front des menaces et de la sécurité cybernétiques. Sur les neuf prévisions que nous avions formulées, quatre concernaient des menaces pour les entreprises. Il s'avère que nos prévisions étaient sérieuses car 75 % d'entre elles se sont déjà confirmées :

- Les cybercriminels vont assimiler les attaques ciblées de catégorie APT : confirmé.
- Les attaques des groupes APT vont se fragmenter et se diversifier : confirmé.
- Les attaques contre les distributeurs automatiques de billets et les terminaux de point de vente vont se renforcer : confirmé.
- Les systèmes de paiement virtuels vont être attaqués : non confirmé.

Revenons un instant sur les incidents les plus marquants de 2015 et sur les nouvelles tendances liées à la sécurité de l'information que nous avons observées dans les milieux professionnels.

CHIFFRES DE L'ANNÉE

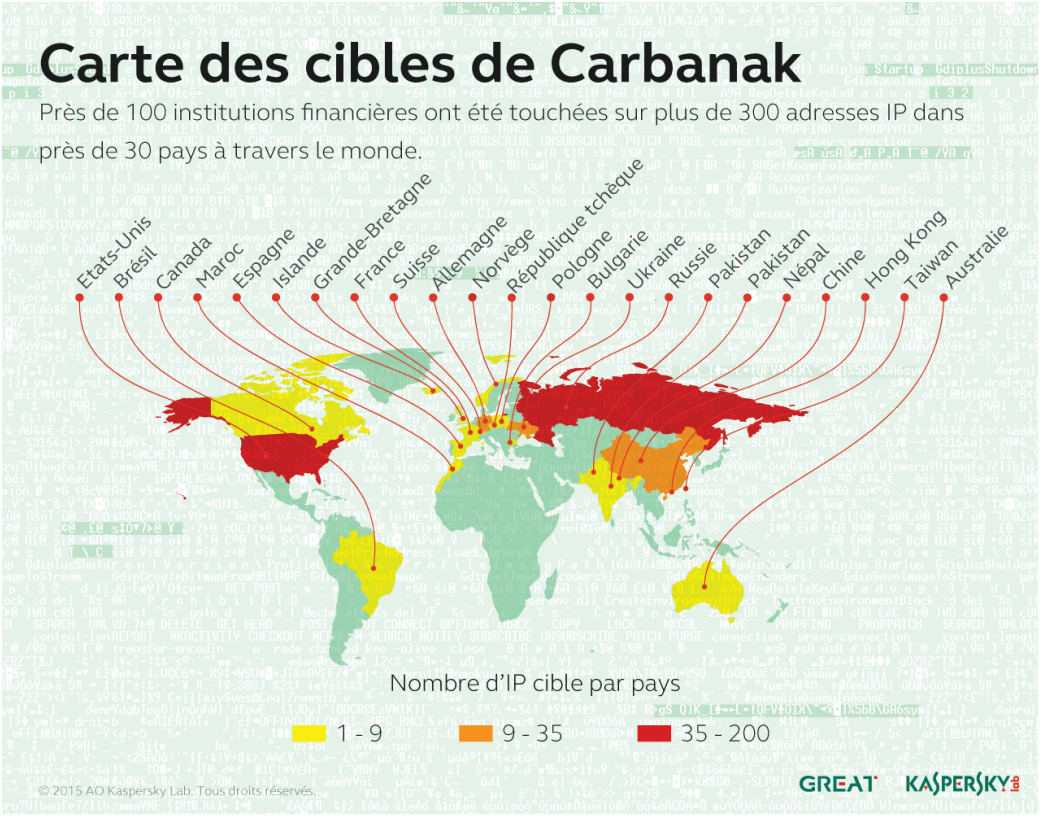
- En 2015, au moins une attaque de malware a été déjouée sur 58 % des ordinateurs d'entreprise, soit une progression de 3 points de pourcentage par rapport à l'année antérieure.
- 29 % des ordinateurs, soit près d'un ordinateur sur trois dans les entreprises, ont été exposés au moins à une attaque organisée via Internet.
- Lors des attaques contre les entreprises, les codes d'exploitation de vulnérabilités présentes dans des applications de bureautique sont utilisés 3 fois plus souvent que dans les attaques contre des particuliers.
- L'Antivirus Fichiers s'est déclenché sur 41 % des ordinateurs d'employés d'entreprises (détection d'objets sur des ordinateurs ou des périphériques amovibles tels que des clés USB, des cartes mémoire, des téléphones, des disques durs externes, des disques réseaux, etc.).

ATTAQUES CIBLÉES CONTRE LES ENTREPRISES : APT ET CRIMINALITÉ

2015 aura été marqué par plusieurs attaques de type APT menées contre des entreprises. L'arsenal et les méthodes adoptés par les individus malintentionné ressemblaient beaucoup à ce que nous avions découvert lors de nos analyses d'attaques APT, la différence étant que ces attaques n'étaient pas organisées par des Etats, mais par des structures cybercriminelles. Même si la démarche adoptée par les cybercriminels n'était pas classique pour des cybercriminels, les objectifs poursuivis étaient identiques : retirer des avantages financiers.

L'opération Carbanak illustre parfaitement le transfert de l'attention des attaques ciblées de type APT sur les organisations financières. Cette opération fut un véritable braquage numérique : les individus malintentionnés s'étaient introduit dans le réseau de la banque victime et s'étaient lancé à la recherche du système critique qui allait permettre de soustraire de l'argent à l'organisation financière. Après avoir volé une somme importante (entre 2,5 et 10 millions de dollars), les criminels recherchaient la prochaine victime.

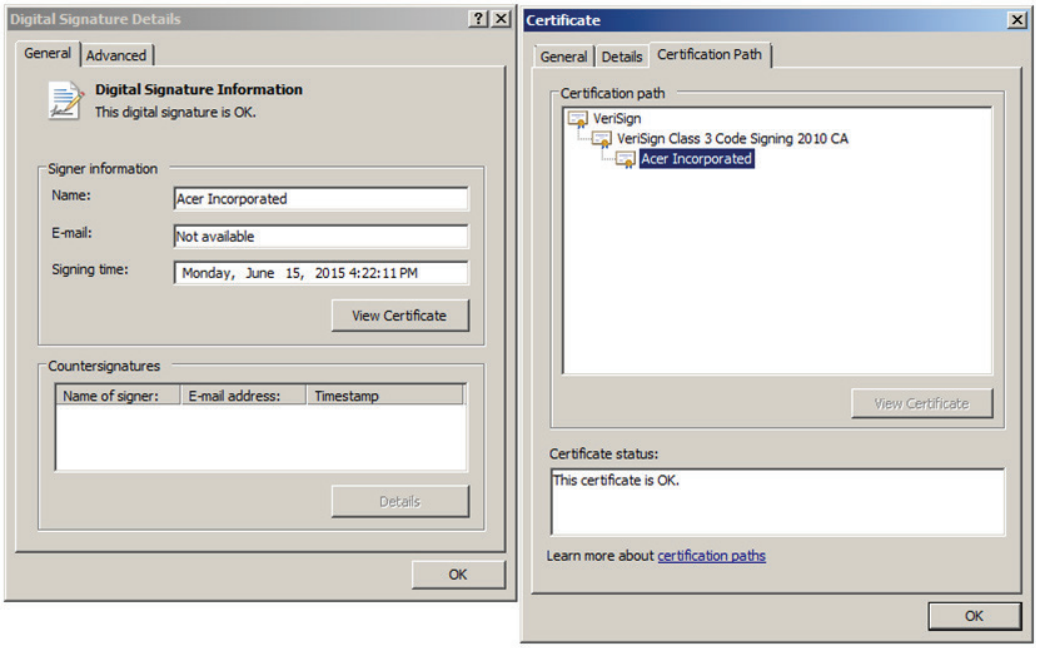
La majorité des victimes de cette campagne malveillante se trouvait en Europe de l'Est. Mais cela n'a pas empêché la campagne Carbanak de viser des organisations aux Etats-Unis, en Allemagne et en Chine également. Cette attaque a touché plus de 100 victimes à travers le monde et les pertes subies par les organisations ciblées (des banques principalement) pourraient atteindre 1 milliard de dollars.



Il ne faut pas oublier non plus que les informations peuvent également valoir beaucoup d'argent, surtout lorsqu'elles permettent de conclure des contrats ou de jouer en bourse, que se soit sur des titres ou des devises, y compris des cryptodevises. L'attaque Wild Neutron (connue également sous le nom Jripbot ou Morpho) est un exemple d'attaque ciblée qui visait peut-être l'obtention de telles informations. Cette campagne de cyberespionnage a beaucoup fait parler d'elle pour la première fois en 2013. A l'époque, elle avait touché directement des sociétés connues dont Apple, Facebook, Twitter et Microsoft. Après la divulgation de ces incidents, les organisateurs de cette opération de cyberespionnage ont suspendu leur activité. Toutefois, environ un an plus tard, Kaspersky Lab a enregistré une reprise de l'activité de Wild Neutron.

Notre enquête a établi que la campagne de cyberespionnage avait infecté des ordinateurs de 11 pays ou territoire, dont la Russie, la France, la Suisse, l'Allemagne, l'Autriche, la Slovénie, la Palestine, les Emirats arabes unis, le Kazakhstan, l'Algérie et les Etats-Unis. Parmi les victimes, il y avait des bureaux de juristes, des sociétés d'investissement, des organisations qui utilisaient les bitcoins, des groupes de sociétés et de compagnies impliqués dans des fusions et acquisitions, des sociétés de technologie de l'information, des établissements de soin, des agences immobilières ainsi que des particuliers.

Signalons que dans le cadre de la campagne Wild Neutron, le certificat utilisé était un certificat de signature de code volé chez Acer.

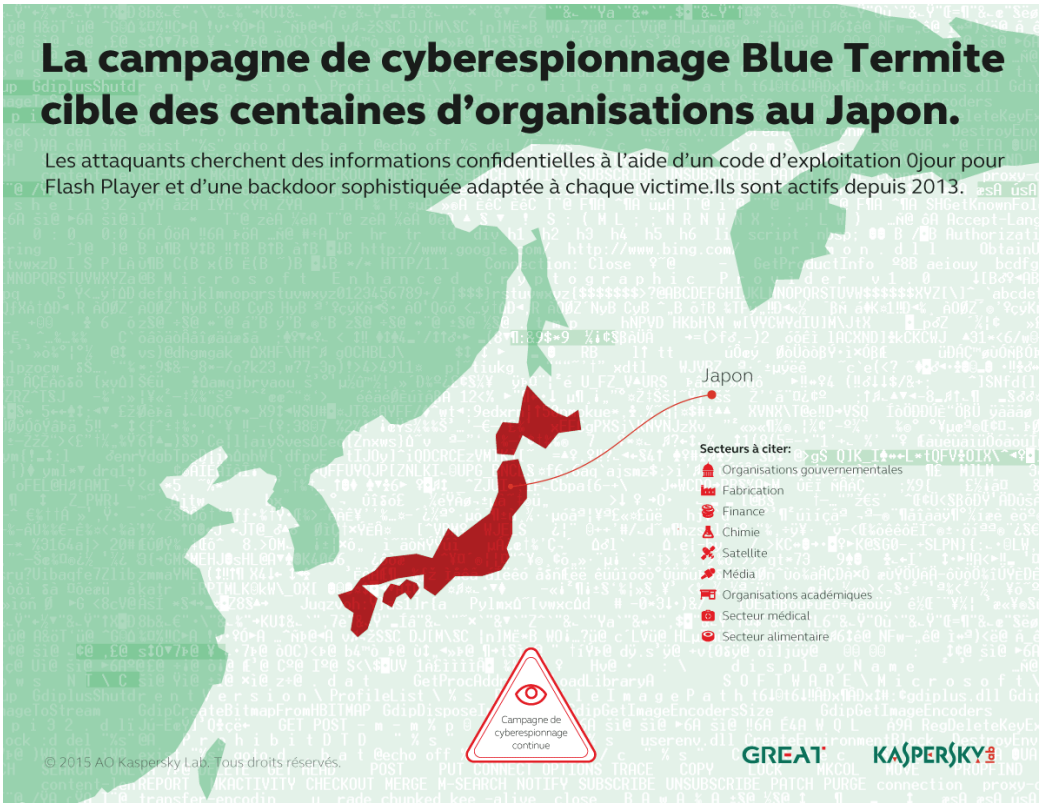


Signature de la société Acer dans le programme d'installation de Wild Neutron

Le changement de cible des attaques du groupe Winnti illustre bien la tendance à la diversification des attaques APT. Pendant longtemps, on a cru que le groupe cybercriminel chinois Winnti visait uniquement les sociétés actives dans le secteur des jeux électroniques. Toutefois, à partir du printemps 2015, nous avons commencé à recevoir des informations qui démontraient que les individus malintentionnés, après avoir testé leurs outils et méthodes, tentaient d'obtenir des revenues en s'en prenant à d'autres cibles. Leurs intérêts ne se limitent plus uniquement au secteur des divertissements : le groupe a commencé à cibler des sociétés pharmaceutiques et de télécommunications. L'analyse de la nouvelle vague d'attaques de Winnti, à l'instar de Wild Neutron, a permis de découvrir que le rootkit de Winnti est signé à l'aide d'un certificat volé dans une division d'un grand conglomérat japonais.

L'expansion géographique, tant au niveau des attaques que des attaquants, est une autre caractéristiques de l'année 2015. Ainsi, dans le cadre de l'analyse d'un incident survenu au Proche-Orient, les experts de Kaspersky Lab ont mis à jour l'activité d'une structure inconnue jusque là qui organisait des attaques ciblées. Ce groupe, baptisé Faucons du désert (Desert Falcons), est la première structure arabe à organiser des opérations de cyberespionnage à part entière. Au moment de sa découverte, ce groupe avait déjà fait environ 300 victimes, dont des organisations financières.

Un groupe dénommé Blue Termite a quant à lui attaqué des organisations et des sociétés au Japon :



Les rapports suivants publiés par Kaspersky Lab fournissent des informations complémentaires sur les attaques ciblant le monde des affaires : Carbanak, Wild Neutron, Winnti, DarkHotel 2015, Desert Falcons, Blue Termit, Grabit. Les résultats plus détaillés des enquêtes sont accessibles aux abonnés du Kaspersky Intelligence Service (intelreports@kaspersky.com).

L'analyse de ces incidents permet de dégager plusieurs tendances au niveau du développement des attaques qui ciblent les entreprises :

- Les individus malintentionnés ont attaqués des organisations qui conservent de l'argent : des banques, des fonds d'investissement et des sociétés liées aux opérations boursières, y compris sur des cryptodevises.
- Les attaques font l'objet d'une préparation minutieuse, les individus malintentionnés étudient les centres d'intérêt des victimes potentielles (les employés des sociétés ciblées) et identifient les sites qu'ils fréquentent le plus souvent. Ils étudient également les contacts des victimes, ainsi que les sous-traitants qui fournissent du matériel et des services à la société.
- Ces données récoltées durant la phase de préparation sont activement exploitées. Les attaquants compromettent les sites légitimes identifiés, les comptes de certains contacts des employés de la société attaquée. Ces comptes et ces sites sont utilisés pendant quelques heures seulement, le temps de propager le code malveillant. Lorsque cette

étape est terminée, l'infection de ces ressources est désactivée. Cette méthode permet aux individus malintentionnés d'utiliser à nouveau la ressource compromise après quelques mois.

- La collecte d'informations dans le réseau attaqué s'opère à l'aide de fichiers signé et d'applications légitimes.
- Les attaques sont diversifiées et peuvent toucher des PME.
- Les attaques qui visent les entreprises sont distribuées du point de vue géographique : l'attaque la plus importante a touché le Japon et il y a des groupes APT dans le monde arabe.

Bien que le nombre d'attaques de type APT organisées par le milieu cybercriminel est relativement faible, les tendances dans leur développement vont sans aucun doute influencer les stratégies et les méthodes utilisées par les cybercriminels "classiques" contre les sociétés.

STATISTIQUES

Nous tenons d'abord à signaler que les statistiques relatives aux utilisateurs professionnels (répartition géographique des attaques, classement des objets détectés) coïncident généralement avec les statistiques pour les utilisateurs particuliers. Cela n'a rien de surprenant car les utilisateurs professionnels ne vivent pas dans une bulle. Leurs ordinateurs sont victimes d'attaques organisées par des individus malintentionnés qui propagent leurs malwares sans tenir compte de victimes en particulier. Ces attaques/malwares constituent la majorité et les données relatives aux attaques qui visent précisément des utilisateurs professionnels n'ont que très peu d'influence sur les statistiques générales.

En 2015, au moins une attaque d'un malware a été déjouée sur **58 %** des ordinateurs en entreprise, soit une progression de 3 points de pourcentage par rapport à l'année dernière.

Menaces sur Internet (attaques via Internet)

En 2015, 29 % des ordinateurs, soit pratiquement un ordinateur sur trois dans les entreprises, ont été exposés au moins à une attaque organisée via Internet.

TOP 10 des malwares, attaques via Internet

Pour rappel, ce classement ne reprend que les malwares. Nous avons exclu les logiciels publicitaires qui agissent contre la volonté de l'utilisateur et l'embêtent, mais qui ne nuisent pas à l'ordinateur.

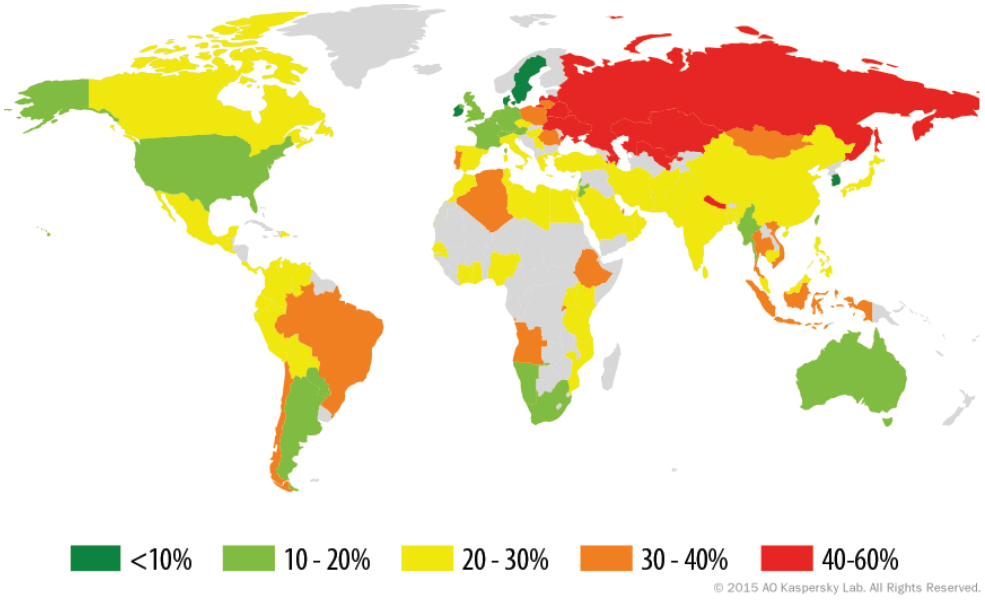
	Nom*	% d'utilisateurs attaqués**
1	Malicious URL	57%
2	Trojan.Script.Generic	24.7%
3	Trojan.Script.Iframer	16.0%
4	Exploit.Script.Blocker	4.1%
5	Trojan-Downloader.Win32.Generic	2.5%
6	Trojan.Win32.Generic	2.3%
7	Trojan-Downloader.JS.Iframe.diq	2.0%
8	Exploit.Script.Generic	1.2%
9	Packed.Multi.MultiPacked.gen	1.0%
10	Trojan-Downloader.Script.Generic	0.9%

** 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 d'utilisateurs attaqués par ce malware sur l'ensemble des utilisateurs attaqués.*

Presque la totalité du Top 10 est composée de verdicts attribués à des objets utilisés dans le cadre d'attaques de type drive-by. Il s'agit de divers trojan-downloaders et de codes d'exploitation.

Répartition géographique des attaques Internet



Répartition géographique des attaques via des ressources Internet, 2015 (pourcentage d'utilisateurs professionnels attaqués dans le pays)

Menaces locales

L'Antivirus Fichiers s'est déclenché sur **41 %** des ordinateurs d'employés d'entreprises (détection d'objets sur des ordinateurs ou des périphériques amovibles tels que des clés USB, des cartes mémoire, des téléphones, des disques durs externes, des disques réseaux, etc.).

TOP 10 des malwares, menaces locales

Ce classement ne reprend lui aussi que les malwares. Nous avons exclu les logiciels publicitaires qui agissent contre la volonté de l'utilisateur et l'embêtent, mais qui ne nuisent pas à l'ordinateur.

	Nom*	% d'utilisateurs attaqués**
1	DangerousObject.Multi.Generic	23.1%
2	Trojan.Win32.Generic	18.8%
3	Trojan.WinLNK.StartPage.gena	7.2%
4	Trojan.Win32.AutoRun.gen	4.8%
5	Worm.VBS.Dinihou.r	4.6%
6	Net-Worm.Win32.Kido.ih	4.0%
7	Virus.Win32.Sality.gen	4.0%
8	Trojan.Script.Generic	2.9%
9	DangerousPattern.Multi.Generic	2.7%
10	Worm.Win32.Debris.a	2.6%

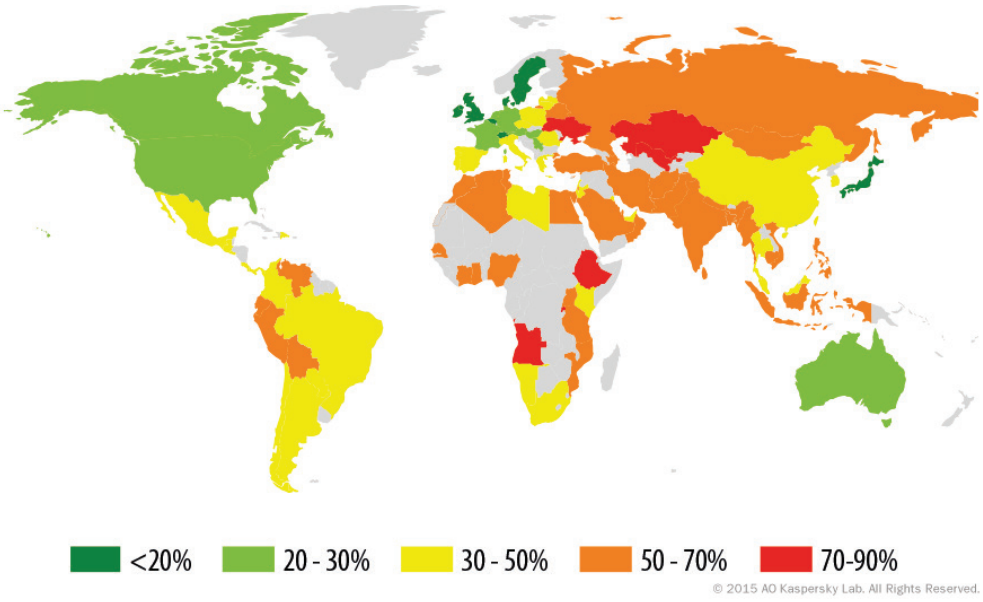
** Verdicts détectés par les modules OAS et OAD de l'antivirus et transmis par les utilisateurs des produits de Kaspersky Lab qui ont accepté de partager les données statistiques.*

*** Pourcentage d'utilisateurs attaqués par ce malware sur l'ensemble des utilisateurs attaqués.*

La première place du classement revient à divers malwares détectés à l'aide de technologies dans le nuage sous le nom DangerousObject. Multi.Generic. Ces technologies interviennent lorsque les bases antivirus ne contiennent pas encore les définitions et qu'il n'est pas possible de détecter le malware à l'aide de l'analyse heuristique, mais l'éditeur de logiciels antivirus a accès dans le " nuage " aux informations relatives à l'objet. Dans le cas des sociétés qui ne sont pas autorisées à envoyer des statistiques dans le cloud, il est possible d'utiliser Kaspersky Private Security Network au lieu de désactiver les technologies dans le cloud. Ainsi, les ordinateurs du réseau peuvent être protégés par le cloud.

Les autres membres du classement sont principalement des malwares qui se propagent eux-mêmes et leurs composants..

Géographie des menaces locales



Répartition géographique des menaces locales, 2015
(pourcentage d'utilisateurs professionnels attaqués dans le pays))

PARTICULARITÉS DES ATTAQUES CONTRE LES ENTREPRISES

Les statistiques générales relatives aux utilisateurs dans les entreprises ne nous apprennent rien sur les spécificités des attaques menées contre les entreprises. Elles nous renseignent sur la probabilité de l'infection d'un ordinateur dans un pays ou sur la popularité de tel ou tel malware chez les individus malintentionnés.

Toutefois, l'analyse plus poussée permet de dégager les particularité des attaques contre les entreprises :

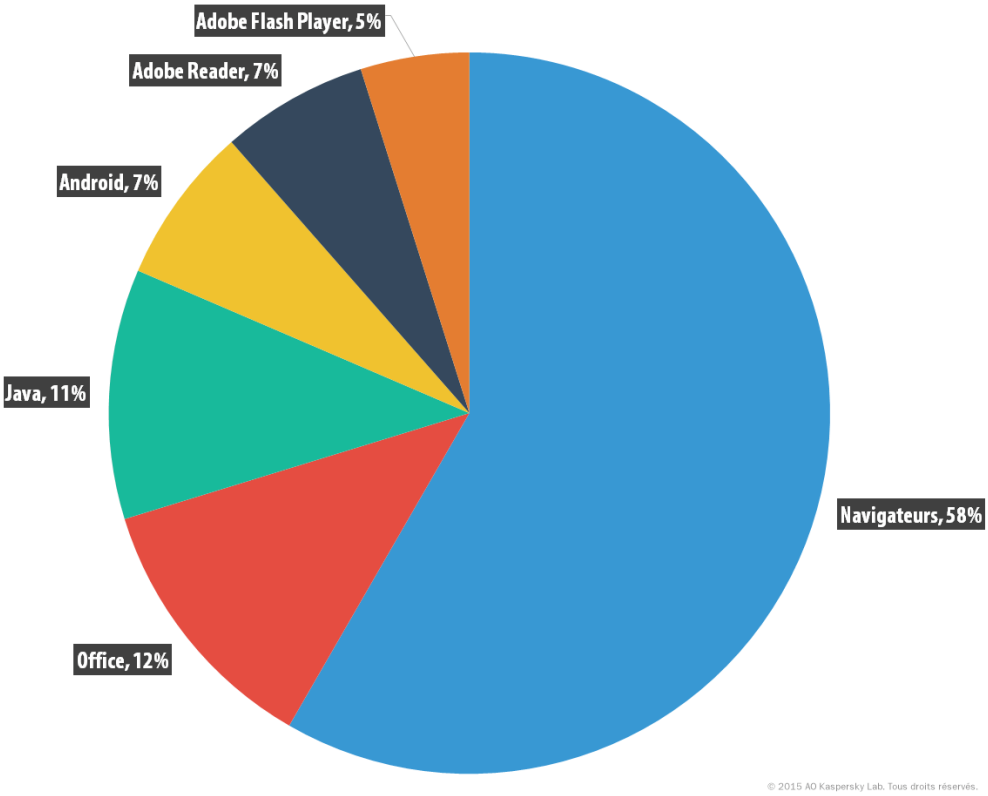
- Les codes d'exploitation de vulnérabilités dans des applications de bureautique sont 3 fois plus souvent utilisés que dans les attaques contre des particuliers.
- Les attaques utilisent des fichiers malveillants signés par des certificats numériques valides.
- Les attaques reposent sur l'utilisation d'applications légitimes accessibles qui permettent aux attaquants de passer inaperçus pendant plus longtemps.

De plus, nous avons remarqué une augmentation active du nombre d'ordinateurs d'employés infectés par des ransomwares.

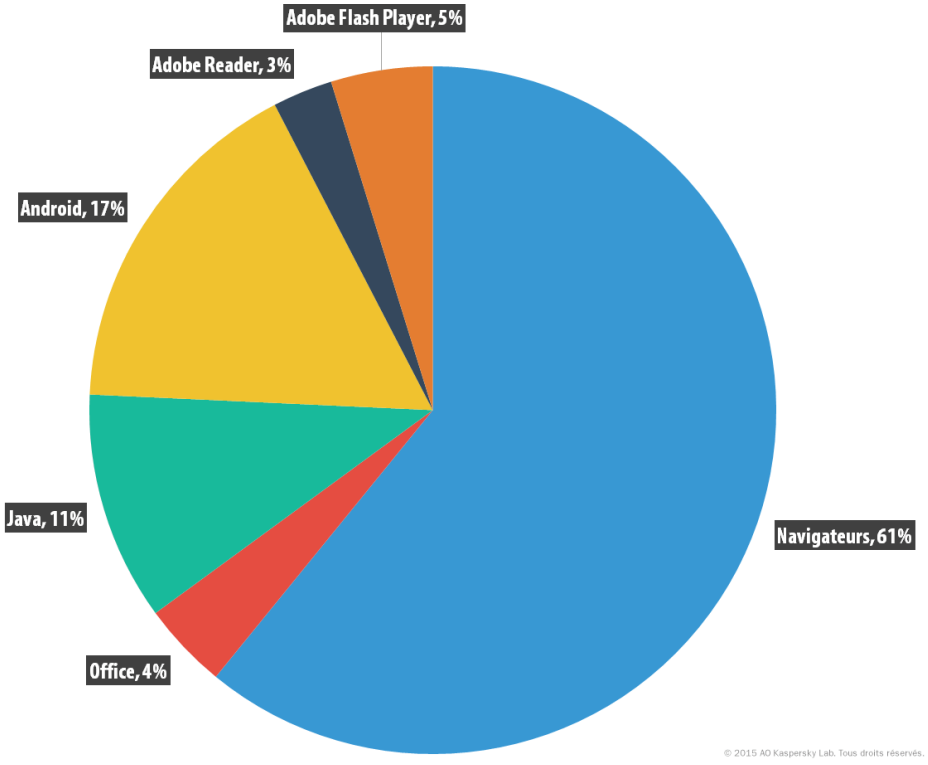
Dans ce cas, il ne s'agit pas toujours d'attaques de type APT : les individus malintentionnés "traditionnels" ciblent les employés en général, parfois au sein d'une entreprise en particulier.

Codes d'exploitation utilisés dans les attaques contre les entreprises

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 courrier électronique ou lors de l'infection d'applications locales, y compris sur les appareils nomades des utilisateurs.



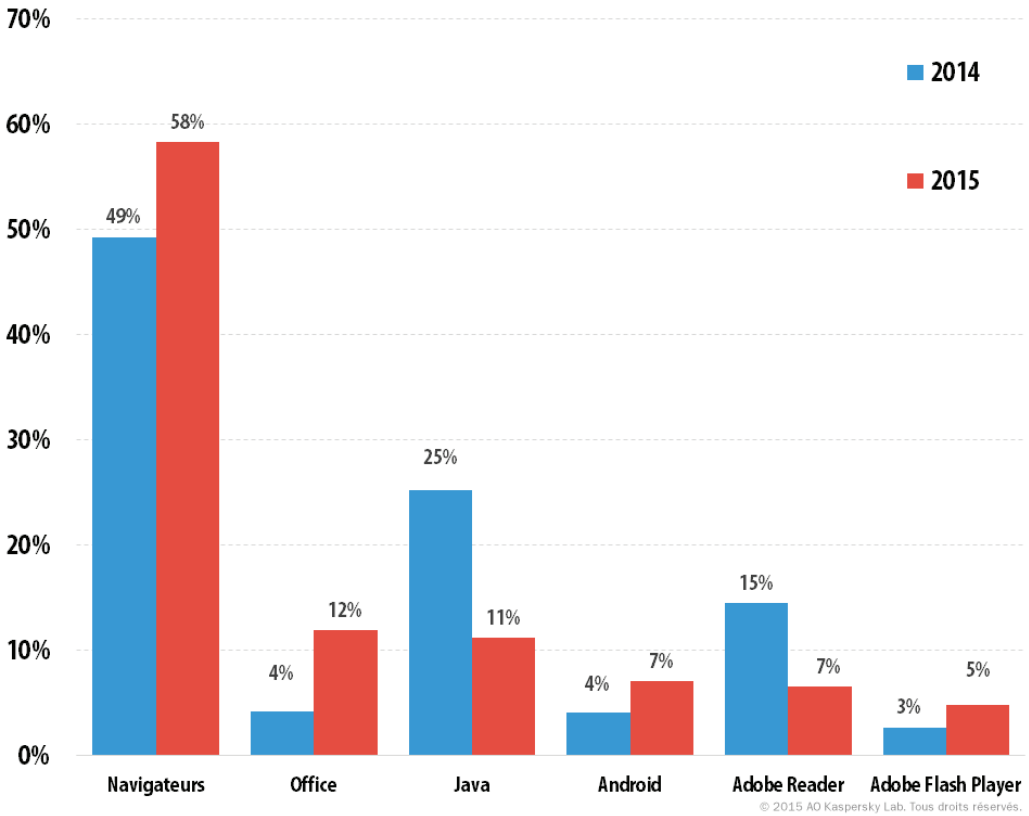
Répartition, par type d'application ciblée, des codes d'exploitation utilisés par les individus malveillants dans les attaques (utilisateurs professionnels, 2015)



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

La comparaison des codes d'exploitation utilisés par les individus malintentionnés dans le cadre d'attaques contre des utilisateurs particuliers et des utilisateurs professionnels met clairement en évidence l'utilisation supérieure de codes d'exploitation pour applications bureautiques chez les utilisateurs professionnels. Alors que ces codes d'exploitation de vulnérabilités dans des applications de bureautique n'interviennent que dans 4 % des attaques contre les utilisateurs particuliers, ils représentent 12 % de l'ensemble des codes d'exploitation découverts au cour de l'année dans les attaques contre les utilisateurs professionnels.

Les navigateurs conservent leur première position dans le classement des applications ciblées par les codes d'exploitation, aussi bien dans les attaques contre les utilisateurs particuliers que dans les attaques contre les utilisateurs professionnels. 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. La catégorie "navigateurs" contient également les détections des pages d'atterrissage qui "diffusent" les codes d'exploitation. D'après nos observations, il s'agit le plus souvent de codes d'exploitation pour Adobe Flash Player.



Répartition, par type d'application ciblée, des codes d'exploitation utilisés par les individus malveillants dans les attaques, 2014-2015

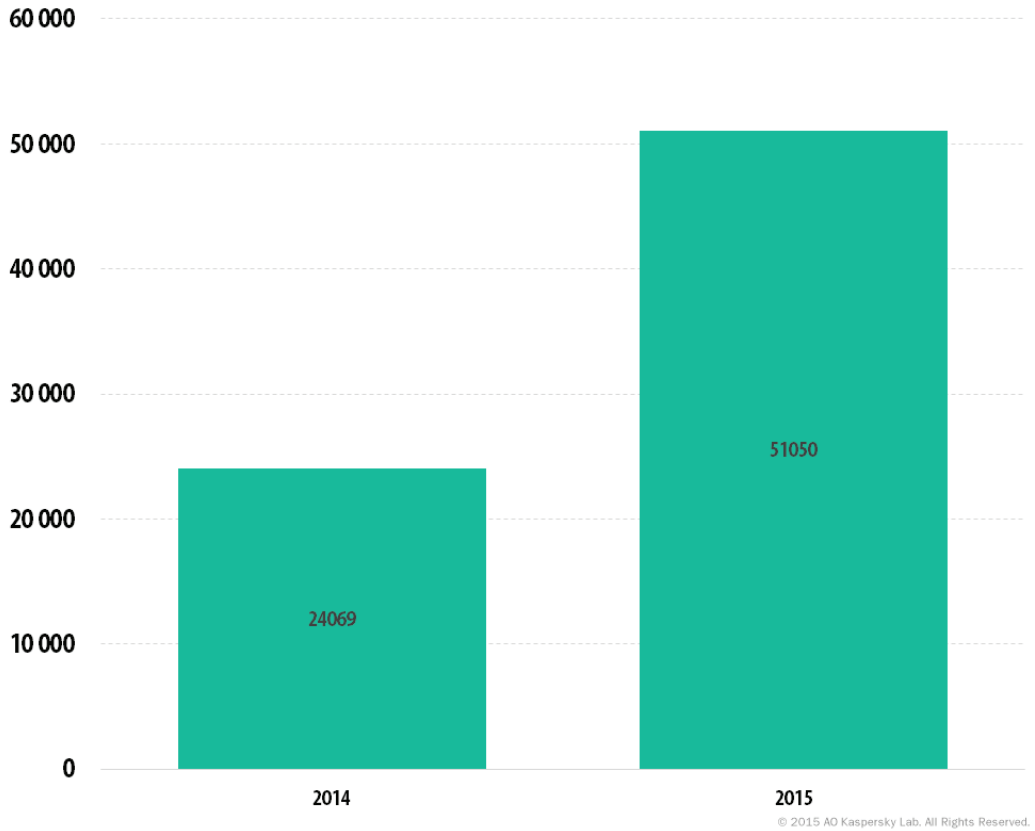
Par rapport à 2014, les parts des codes d'exploitation pour Java et PDF a sensiblement diminué. Elles enregistrent un recul de 4 et de 8 points de pourcentage respectivement. Les codes d'exploitation pour Java sont devenus moins populaires malgré la découverte de plusieurs vulnérabilités de type 0jour au cours de l'année. Par contre, la part d'attaques qui exploitent des vulnérabilités dans les applications bureautiques (+ 8 points de pourcentage), les navigateurs (+ 9 points de pourcentage), Adobe Flash Player (+ 9 points de pourcentage) et Android (+ 3 points de pourcentage) a augmenté.

Comme l'indique la pratique de l'analyse des incidents de sécurité, même dans le cas des attaques ciblées contre des entreprises, les individus malintentionnés utilisent souvent des codes d'exploitation pour des vulnérabilités déjà connues, ce qui se justifie par la lenteur de l'application des correctifs dans les entreprises. La progression jusqu'à 7 % de la part des codes d'exploitation pour applications Android vulnérables témoigne de l'appétit croissant des individus malintentionnés pour les données professionnelles stockées sur les appareils mobiles des employés.

Ransomwares

Pendant longtemps, les Trojans de type ransomware ont été considérés comme une menace qui ne concernait que les particuliers. D'après les données dont nous disposons, les individus malintentionnés qui gagnent leur vie grâce aux ransomwares s'intéressent de plus en plus souvent aux entreprises.

Nos solutions de protection ont détecté en 2015 des ransomwares sur plus de **50 000 postes de travail** dans des réseau d'entreprise, soit **deux fois plus que l'année antérieure**. Il faut toutefois bien se dire que la quantité réelle d'incidents est bien plus élevée : ces statistiques ne tiennent compte que des résultats des analyses heuristique et à l'aide de signatures tandis que les produits de Kaspersky Lab détectent les trojans de type ransomware à l'aide d'une analyse du comportement dans la majorité des cas.



Nombre d'utilisateurs professionnels uniques attaqués par des trojans de type ransomware en 2014 et 2015

Ce dynamisme de la croissance de l'intérêt des individus malintentionnés pour les attaques contre les entreprises s'explique par deux facteurs. Tout d'abord, la rançon qui peut être exigée à une entreprise dépasse de loin celle imposée à un particulier. Ensuite, la probabilité qu'une entreprise décide de payer la rançon est plus élevée car une entreprise ne peut tout simplement pas fonctionner si les informations hébergées sur quelques postes de travail ou serveurs critiques ne sont plus accessibles en raison d'un chiffrement.

Un des cas les plus intéressants en la matière survenu en 2015 fut l'apparition du premier ransomware Linux (détecté sous le nom Trojan-Ransom.Linux.Cryptor par les solutions de Kaspersky Lab) qui visaient des sites Internet, dont des sites de magasins en ligne. Grâce à diverses vulnérabilités dans des applications Internet, les individus malintentionnés avaient pu accéder aux sites Internet et charger un malware qui chiffrait les données du serveur. Dans la majorité des cas, le magasin en ligne n'était plus en mesure de fonctionner. La rançon exigée pour déchiffrer les données s'élevait à un bitcoin. Près de 2 000 sites Internet auraient été infectés par ce malware. Vu le nombre de serveur *nix dans les milieux professionnels, il est logique de penser que les attaques de ransomwares contre les plate-formes autres que Windows pourraient se poursuivre en 2016.

Top 10 des familles de trojans de type ransomware

	Famille	% d'utilisateurs attaqués*
1	Scatter	21
2	Onion	16
3	Cryakl	15
4	Snocry	11
5	Cryptodef	8
6	Rakhni	7
7	Crypmod	6
8	Shade	5
9	Mor	3
10	Crypren	2

** Pourcentage d'utilisateurs attaqués par des malwares de cette famille, sur l'ensemble des utilisateurs attaqués.*

Presque toutes les familles de ransomwares de ce classement exigent une rançon en bitcoins.

La première place revient aux trojans de la famille Scatter qui chiffrent les fichiers sur le disque et laissent les fichiers chiffrés avec l'extension .vault. Les malwares de la famille Scatter sont des malwares de script à plusieurs modules et plusieurs fonctions. Cette famille a connu une évolution importante en peu de temps et elle possède, outre les fonctions de chiffrement de fichier, les fonctions des catégories Email-Worm et Trojan-PSW. En deuxième place du classement de la répartition des ransomwares, nous trouvons la famille Onion, connue pour le fait que ces serveurs de commande se trouvent sur le réseau Tor. La famille de ransomwares Cryakl, programmés en Delphi, qui est apparue en avril 2014 occupe la troisième position de ce classement.

Il est parfois possible de déchiffrer les données chiffrées par ces malwares, surtout si l'algorithme contient des fautes. Toutefois, il est impossible à l'heure actuelle, de déchiffrer les données chiffrées par les versions les plus récentes des malwares repris dans ce classement.

Il faut bien comprendre que pour une société, l'infection par un malware de ce genre pourrait provoquer l'arrêt de l'activité si les données chiffrées suite à l'infection possèdent une importance vitale ou si le chiffrement des données provoque le blocage d'un serveur critique. Ce genre d'attaque peut provoquer des pertes considérables, similaires à celle des attaques du malware Wiper qui vise à supprimer les données dans les réseaux informatiques des entreprises.

La lutte contre cette menace passe par l'adoption d'une série de mesures :

- adopter une protection contre les codes d'exploitation ;
- activer sans faute les méthodes de détection sur la base du comportement dans la solution de protection (dans les solutions de Kaspersky Lab, cette tâche revient au module System Watcher) ;
- mettre en place une procédure de sauvegarde des données.

ATTAQUES CONTRE DES TERMINAUX DE POINT DE VENTE

La sécurité des terminaux de point de vente aura été un sujet particulier pour les entreprises en 2015, surtout pour les sociétés actives dans le commerce. De nos jours, n'importe quel ordinateur doté d'une application spéciale auquel est raccordé un périphérique spécial pour lire les cartes peut devenir un terminal de point de vente. Les individus malintentionnés recherchent de tels ordinateurs et les infectent avec des malwares qui permettront de voler les données des cartes utilisées pour réaliser les paiements via ces terminaux.

Les solutions de Kaspersky Lab ont déjoué plus de 11 500 tentatives d'attaques de ce genre à travers le monde. Notre collection compte actuellement 10 familles de programmes développés pour voler les données sur les terminaux de point de vente. Sept d'entre eux sont apparus cette année. Le nombre restreint de tentatives d'attaque ne signifie pas que nous pouvons sous-estimer le danger car une seule attaque qui réussit est capable de compromettre les données de dizaines de milliers de cartes de crédit. Ce volume impressionnant de victimes potentielles s'explique par le fait que les propriétaires et les gérants de magasins ne considèrent pas les terminaux de point de vente comme des éléments à protéger. Par conséquent, il peut s'écouler beaucoup de temps avant la détection de l'infection et pendant toute cette période, le malware enverra à l'individu malintentionné les données des cartes de crédit lues par le terminal.

Ce problème est surtout d'actualité dans les pays qui n'ont pas encore adopté les cartes à puces EMV. La transition aux cartes à puce EMV devrait compliquer considérablement la récupération des données pour le clonage de carte. Mais il s'agit d'un processus à long terme. En attendant, il faut adopter un minimum de mesures pour la protection des terminaux de point de vente et heureusement, il est assez simple de créer pour eux une stratégie de type "interdiction par défaut du lancement d'applications inconnues".

Nous nous attendons à ce que les cybercriminels commencent à attaquer les terminaux de point de vente mobile sous Android.

CONCLUSION

Nos données démontrent que les outils utilisés dans les attaques contre les entreprises diffèrent des outils employés contre les particuliers. Les attaques contre les utilisateurs professionnels reposent beaucoup plus souvent sur l'utilisation de code d'exploitation de vulnérabilités dans des applications de bureautiques. Les fichiers malveillants sont souvent signés par des certificats numériques valides et les individus malintentionnés essaient d'atteindre leurs objectifs à l'aide d'applications légitimes en vue de passer inaperçus plus longtemps. De plus, nous avons remarqué une augmentation active du nombre d'ordinateurs d'employés infectés par des ransomwares. Ceci ne concerne pas uniquement les attaques de type APT : les individus malintentionnés "traditionnels" attaquent délibérément les utilisateurs professionnels, parfois des employés d'une société en particulier.

L'adoption des méthodes et des malwares du milieu des APT par des groupes de cybercriminels qui attaquent des entreprises fait passer ces attaques à un niveau supérieur et les rend beaucoup plus dangereuses. Tout d'abord, les cybercriminels ont commencé à appliquer ces méthodes pour organiser des attaques contre des banques en vue de voler d'importantes sommes d'argent. Ces mêmes méthodes leur permettent de retirer des banques l'argent des sociétés après avoir obtenu l'accès au réseau de l'entreprise.

Le criminel élabore ses attaques sur la base de vulnérabilités déjà connues, et ce pour profiter de la lenteur de l'application des correctifs pour applications dans les entreprises. De plus, les individus malintentionnés utilisent beaucoup de fichiers malveillants signés et d'applications légitimes afin de mettre en place le canal d'extraction des informations : on retrouve ainsi de célèbres applications d'administration à distance, des clients SSH, des applications de récupération de mot de passe, etc.

De plus en plus souvent, les individus malintentionnés prennent pour cible les serveurs de l'entreprise. Outre le vol de données, il y a déjà eu des cas où les serveurs attaqués ont été utilisés dans des attaques DDoS. Parfois, les données sont simplement chiffrées et les individus malintentionnés exigent une rançon. Les derniers événements ont démontré que cette affirmation concerne aussi bien les serveurs Windows que les serveurs Linux.

De nombreuses sociétés touchées par ces attaques ont été victimes d'un chantage de la part des individus malintentionnés qui exigeaient le paiement d'une somme d'argent pour arrêter une attaque DDoS, déchiffrer des données ou s'abstenir de divulguer les informations volées. Toute société qui se retrouverait dans une situation similaire doit prendre contact avec les autorités policières et judiciaires et des experts de la protection des informations. En effet, rien ne garantit que les criminels tiendront leur parole après avoir reçu l'argent, comme ce fut le cas lors de l'attaque DDoS contre la société qui gère proton-mail : cette attaque s'était poursuivie après le paiement de la rançon.

PRÉVISIONS

Augmentation du nombre d'attaques contre des organisations financières, arnaques financières sur les bourses

Pour l'année prochaine, nous nous attendons à une augmentation du nombre d'attaques contre les organisations financières et ainsi qu'à un changement au niveau de la qualité de ces attaques. Outre le transfert de l'argent vers leur compte suivi du blanchiment, les individus malintentionnés vont adopter de nouvelles techniques, notamment liées à la manipulation de données sur les bourses qui travaillent avec des instruments financiers traditionnels ou avec de nouveaux instruments comme les cryptodevises.

Attaques contre les infrastructures

S'introduire dans une organisation n'est pas toujours facile, mais pratiquement toutes les données de valeurs sont stockées non pas dans l'entreprise, mais sur des serveurs dans des centres de données. L'accès à ces éléments de l'infrastructure sera un des principaux vecteurs d'attaques contre les sociétés en 2016.

Exploitation de vulnérabilités dans l'Internet des objets pour s'introduire dans le réseau de sociétés

Aujourd'hui, presque tous les réseaux d'entreprise comptent des périphériques de l'Internet des objets. Des études menées en 2015 ont démontré qu'il existe plusieurs problèmes au niveau de la sécurité de ces périphériques et il est évident que les individus malintentionnés vont essayer de les utiliser en tant que premier échelon pour l'accès au réseau d'une entreprise.

Normes de sécurité plus strictes, coopération entre les autorités policières et judiciaires

En réaction à l'augmentation du nombre d'incidents informatiques dans le monde des affaires et au changement du paysage des cybermenaces, les organismes de régulation vont développer de nouvelles normes de sécurité ou actualiser les normes existantes. Les entreprises désireuses de conserver leurs avoirs numériques vont coopérer plus avec les autorités judiciaires et policières ou les nouvelles normes citées ci-dessus les y amèneront. Cela pourrait déboucher sur des opérations de capture des cybercriminels plus efficaces et de nouvelles arrestations devraient avoir lieu en 2016.

QUE FAIRE ?

Nous avons vu en 2015 que les cybercriminels ont adopté les méthodes des attaques APT pour s'introduire dans les réseaux des entreprises. Nous voulons parler ici de la reconnaissance en vue d'identifier les maillons faibles de l'infrastructure et d'obtenir des informations sur les employés, de l'organisation d'attaque par harponnage ou méthode du trou d'eau, de l'utilisation active de codes d'exploitation pour exécuter du code et obtenir les autorisations d'administrateur, mais également nous souhaitons évoquer l'utilisation dans les attaques d'applications légitimes pour l'administration à distance, l'analyse de réseau et la récupération de mots de passe en plus des trojans. Tout ceci requiert le développement de méthodes et de technologies de protection des réseaux d'entreprise.

A l'heure d'envisager des recommandations concrètes, il faut avant tout prêter attention au Top 35 des stratégies de neutralisation des attaques contre les entreprises établi par l'Australian Signals Directorate. Après avoir mené une analyse détaillée des attaques et des menaces locales, l'ASD est parvenu à la conclusion qu'au moins 85 % des cyberintrusions ciblées pouvaient être neutralisées à l'aide de quatre stratégies élémentaires. Trois de ces stratégies sont liées à l'utilisation de solutions de protection spéciales (la gamme de produits de Kaspersky Lab propose les solutions technologiques qui recouvrent ces trois stratégies importantes).

Voici les quatre stratégies de base qui réduisent la probabilité de réussite d'une attaque ciblée :

- Mise en place d'une liste blanche d'applications permettant de bloquer l'exécution de malwares ou d'applications non confirmées.
- Installation des correctifs pour les applications Java, les lecteurs de fichiers PDF ou Flash, les navigateurs et les applications Microsoft Office.
- Elimination des vulnérabilités dans le système d'exploitation à l'aide de correctifs.
- Restriction des autorisations d'accès d'administration au système d'exploitation et aux applications sur la base des besoins de chaque utilisateur.

Les détails relatifs aux stratégies préconisées par l'ASD figurent dans un document consacré aux stratégies de neutralisation des menaces publié sur Securelist.

Le deuxième facteur important est l'utilisation de données sur les menaces actuelles, à savoir celles fournies par le service Threat Intelligence (par exemple, Kaspersky Lab propose ce genre de services dans le cadre du

Kaspersky Intelligence Service). La configuration et l'analyse du réseau sur la base de ces informations permettent de se protéger contre les attaques ou d'identifier une attaque à ses débuts.

Les principes fondamentaux de la sécurité dans les réseaux d'entreprise restent inchangés :

- Formation du personnel car la sécurité des informations ne dépend pas seulement du service de sécurité. C'est une obligation de chaque employé.
- Mise en place de processus de sécurité : le système de sécurité doit pouvoir faire face à l'évolution des menaces.
- Utilisation de nouvelles technologies et méthodes : chaque couche de protection complémentaire contribue à la réduction du risque d'intrusion dans le réseau.

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