Livre blanc

Bitdefender®

Chiffrer les données des entreprises : une activité rentable pour les cybercriminels

Résumé

Le ransomware, cybermenace la plus prolifique du moment, se propage au sein des entreprises via les réseaux de partage de fichiers, les pièces jointes, les liens malveillants ou encore les sites Internet compromis autorisant les téléchargements directs. Le premier trimestre 2016 a enregistré une croissance de 3 500% du nombre de domaines utilisés pour la diffusion de ransomwares, établissant au passage un nouveau record.

Selon une étude réalisée par Bitdefender aux États-Unis en 2015, les ransomwares occupent la seconde place des principales préoccupations des DSI en matière de sécurité dans les moyennes et grandes entreprises. D'après les conclusions de cette étude, 13,7% des entreprises interrogées perçoivent le ransomware comme une menace difficile à contrer. L'étude montre également que les ransomwares et les rootkits sont perçus comme des questions particulièrement complexes à aborder par les entreprises ayant une expérience limitée des attaques de malwares.

Le ransomware était déjà considéré comme une menace majeure dans la liste des principales prévisions en matière de cybersécurité pour 2016, établie par Bogdan Dumitru, Directeur de la Technologie chez Bitdefender. En mars 2016, les chercheurs de Palo Alto Networks ont révélé que les utilisateurs de macOS avaient pour la première fois été la cible d'un ransomware, KeRanger, confirmant ainsi les prédictions de Bitdefender sur l'expansion des ransomwares vers de nouveaux systèmes d'exploitation en 2016.

En décembre 2015, Bogdan Dumitru affirmait : « Nous connaissons déjà les ransomwares pour Linux, Windows et Android. Ce n'est qu'une question de temps avant que macOS ne soit touché à son tour. Les ransomwares ciblent à la fois les particuliers et les entreprises, et les versions de 2016 ne se contenteront pas de chiffrer les fichiers et de demander une rançon, mais diffuseront également tous les documents sur Internet si la rançon n'est pas payée. Comble de l'ironie, la victime sera en mesure de récupérer ses fichiers chiffrés… une fois qu'ils auront été rendus accessibles à tout le monde sur Internet, souvent dans le but d'humilier la victime. »

« Les ransomwares constituent probablement la menace la plus insoluble pour les internautes depuis 2014 et il restera l'un des moteurs les plus importants de la cybercriminalité dans les prochains mois », indiquait Bitdefender. « Alors que certains cybercriminels préféreront se concentrer sur le chiffrement des fichiers, certains groupes plus innovants développeront des « extortionwares » (des malwares qui bloquent les comptes sur différents services en ligne ou qui rendent publiques les données stockées localement). Courant 2016, les ransomwares de chiffrement de fichiers vont très probablement s'étendre également à macOS. »

L'année dernière, les rapports ont révélé que des millions d'utilisateurs avaient été victimes de la version 3.0 de Cryptowall (et encore, beaucoup de cas n'ont pas été déclarés), ce qui a permis de détourner plus de 350 millions de dollars vers les comptes bancaires des cybercriminels.

Principaux pays touchés par des ransomwares, sous Windows

Les menaces visant les PC et les appareils mobiles ont augmenté, à la fois en nombre et en complexité au cours des deux dernières années. Toutefois, certaines variantes de malwares ont été plus prolifiques que d'autres, principalement parce que les cybercriminels les ont utilisées pour générer des revenus importants en soutirant de l'argent aux victimes infectées.

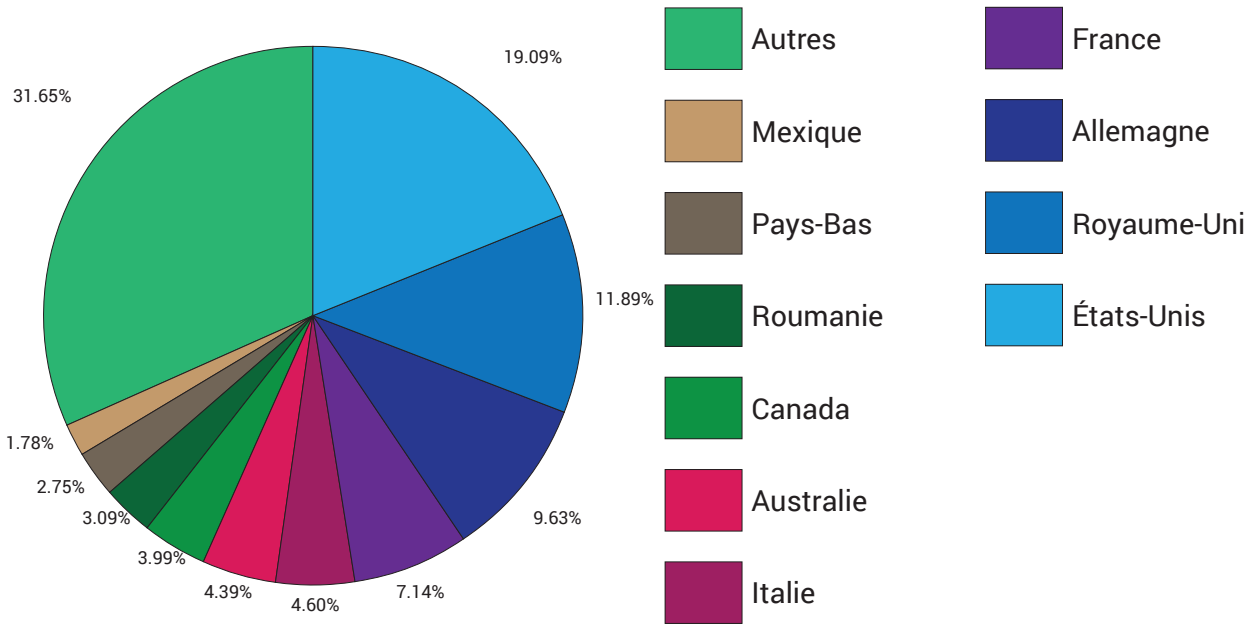
Le malware de type chiffrement de fichiers – connu donc sous le nom de ransomware – est un malware qui a généré plusieurs centaines de millions de dollars de gains au moyen d'actes d'extorsion, le FBI estimant même qu'il pourrait conduire à des pertes financières dépassant globalement le milliard de dollars en 2016.

Le ransomware est non seulement devenu une menace croissante pour les utilisateurs de PC, mais également pour les appareils fonctionnant sous Android. Au cours du premier semestre 2016, c'est aux États-Unis que le plus grand nombre d'attaques de ransomwares ont été recensées, avec 19,09% de l'ensemble des attaques de ransomwares déclarées dans le monde.

Le Royaume-Uni est arrivé en deuxième position, avec 11,89%, soit seulement 2,26 points de plus que l'Allemagne (9,63%), laquelle figurait à la troisième place de notre classement des pays les plus touchés par des attaques de ransomwares.

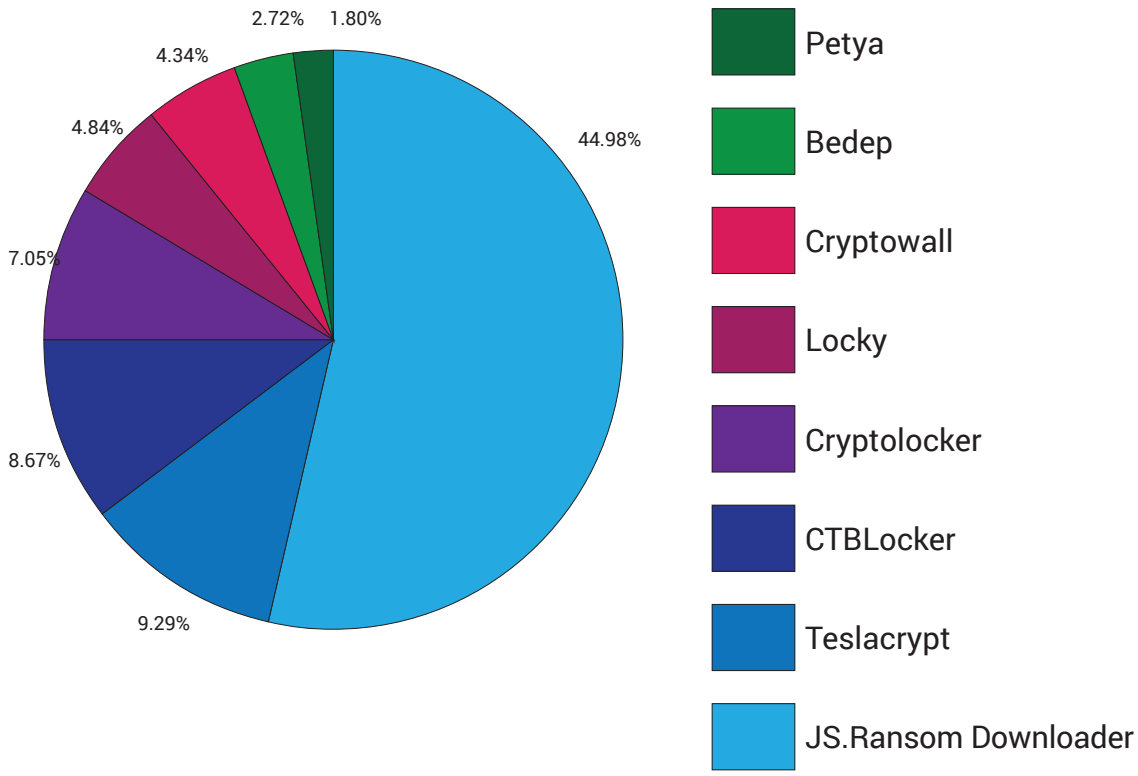
Néanmoins, en ce qui concerne les familles de ransomwares les plus prolifiques, il est intéressant de noter que la part la plus importante d'incidents liés aux ransomwares, semble le biais de fichiers JavaScript. Que les ransomwares soient intégrés à des pièces jointes ou diffusés via des sites Web malveillants, il semblerait qu'il s'agisse de la méthode la plus utilisée par les cybercriminels lorsqu'ils infectent leurs victimes. 44,98% de l'ensemble des attaques de ransomwares déclarées, rendent compte de l'utilisation de fichiers JavaScript pour infecter clandestinement les PC de leurs victimes.

L'une des raisons pour lesquelles nous avons vu les fichiers JavaScript se classer si haut dans notre rapport pourrait être liée au fait que les cybercriminels cherchent à éviter que leurs injecteurs soient identifiés par les solutions de sécurité et à masquer les noms de domaines depuis lesquels est téléchargé le downloader de ransomwares.



Principaux pays touchés par des ransomwares sous Windows, 1er semestre 2016*

En deuxième position avec 9,29% de l'ensemble des attaques de ransomwares recensées, la famille de ransomwares Teslacrypt semble avoir été une « arme de choix » très prisée en matière d'activités cybercriminelles. CTBLocker et Cryptowall figurent eux aussi parmi les cinq principales familles de ransomwares les plus répandues, enregistrant respectivement 8,67% et 7,05% du nombre total d'attaques de malwares déclarées dans le monde. CryptoWall et Bedep atteignent respectivement 4,34% et 2,72%, tandis que Petya – que Bitdefender Labs avait analysé courant 2016 – représentait 1,80% du nombre total d'attaques de malwares.

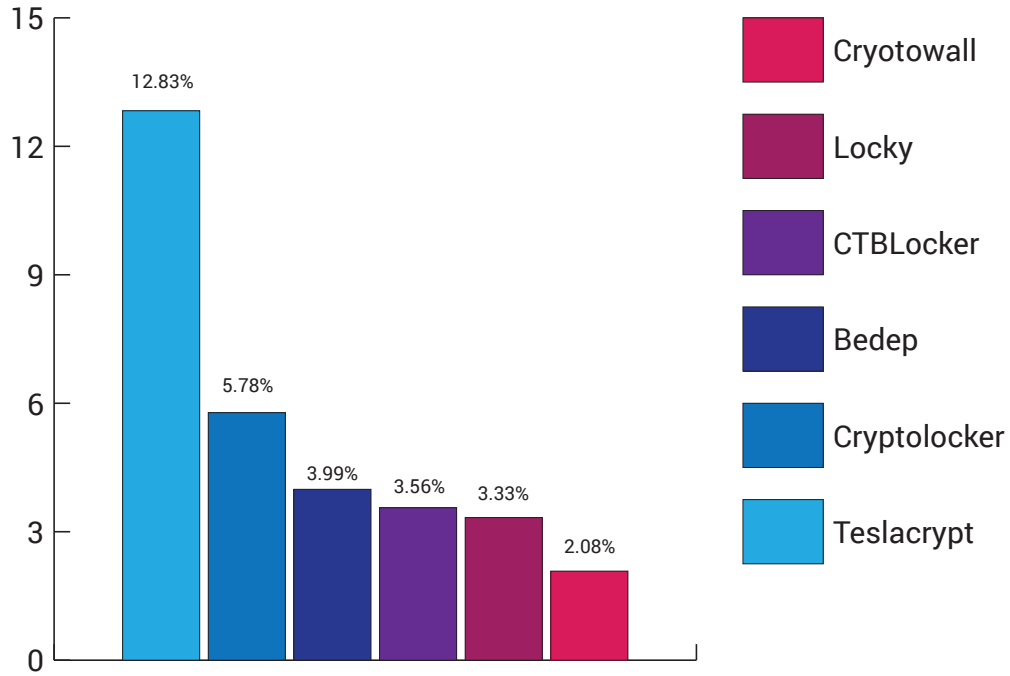


Principales familles de ransomwares sous Windows*

Quand il s'agit de désigner quelques-unes des familles de ransomwares les plus populaires ayant ciblé des pays spécifiques, Teslacrypt, CTBLocker et Bedep ressortent clairement comme étant les attaques préférées des cybercriminels.

Principales familles de ransomwares sous Windows aux États-Unis, 1er semestre 2016

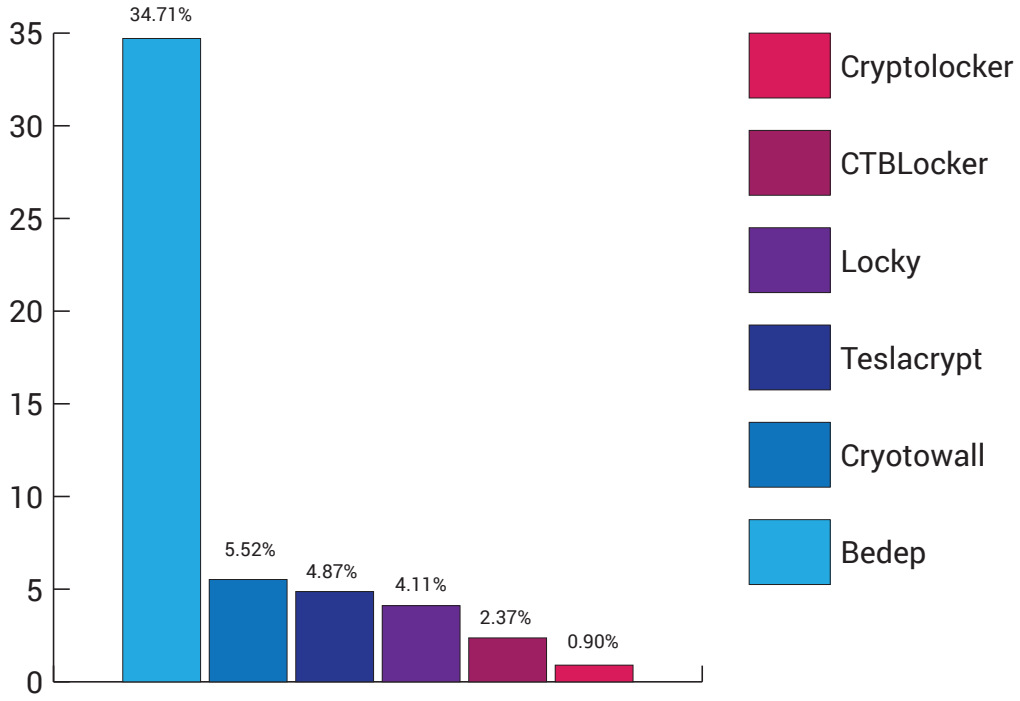
12,83% du nombre total d'attaques de ransomwares déclarées aux États-Unis sont relatives à Teslacrypt, faisant de celui-ci – et de loin – la menace la plus significative. Avec 5,78% des rapports le concernant, Cryptolocker n'atteint pas la moitié du nombre d'attaques enregistrées relatives à Teslacrypt. Bedep suit de près, avec 3,99% des attaques de ransomwares relevées aux États-Unis – les trois principales familles de ransomwares représentant ensemble près de 23% du nombre total d'attaques de ransomwares.



Principales familles de ransomwares sous Windows aux États-Unis, 1er semestre 2016*

Principales familles de ransomwares sous Windows au Royaume-Uni, 1er semestre 2016

Contrairement aux États-Unis où Teslacrypt arrive en première position, au Royaume-Uni, Bedep est de très loin l'une des armes de prédilection des cybercriminels. Avec 34,71% du nombre total d'attaques de ransomwares déclarées, les incidents liés à Bedep représentent un tiers de l'ensemble des incidents liés aux ransomwares. Les attaques liées à Cryptowall arrivent en deuxième position, avec 5,52% du nombre total d'attaques de ransomwares au Royaume-Uni, suivies de près par celles de Teslacrypt, qui atteignent 4,87%.

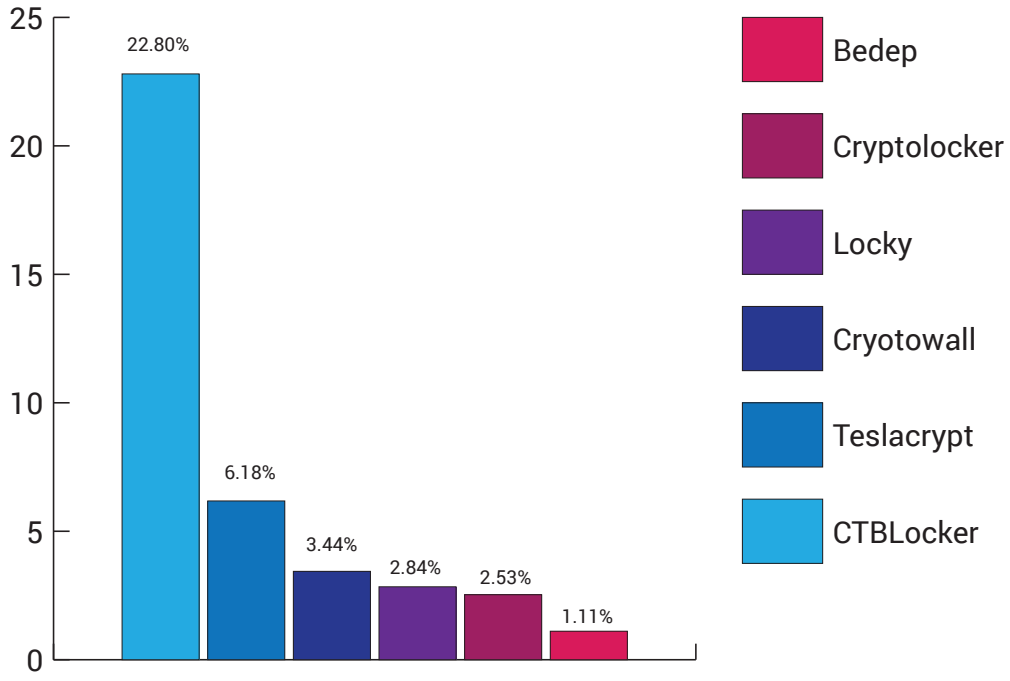


Principales familles de ransomwares sous Windows au Royaume-Uni, 1er semestre 2016*

L'information clé à retenir parmi ces conclusions, est que les cybercriminels semblent avoir ciblé les Britanniques avec le ransomware Bedep, ce qui est intéressant dans la mesure où les chercheurs en sécurité ont constaté qu'il était généralement diffusé par le biais du kit d'exploit Angler. Par conséquent, les attaques de types « drive-by » représentent généralement la méthode par laquelle, Bedep s'exécute sur les machines des victimes. Que ce soit via des sites Web légitimes ayant été utilisés pendant le processus de diffusion ou par le biais de sites Web malveillants, les Britanniques semblent davantage sujets aux attaques liées à l'Internet lui-même qu'aux attaques liées à des pièces jointes infectées – qui sont pourtant en règle générale le principal vecteur de diffusion de ransomwares.

Principales familles de ransomwares sous Windows en Allemagne, 1er semestre 2016

A l'instar du Royaume-Uni, la première des familles de ransomwares les plus prolifiques, devance de loin la seconde. Ainsi, CTBLocker représente 22,80% du nombre total d'attaques de ransomwares relevées en Allemagne, là où Teslacrypt, avec un score de 6,18% seulement, se hissait à la deuxième place. La famille de ransomwares Cryptowall s'est quant à elle classée troisième, avec seulement 3,44% du nombre d'attaques de ransomwares.

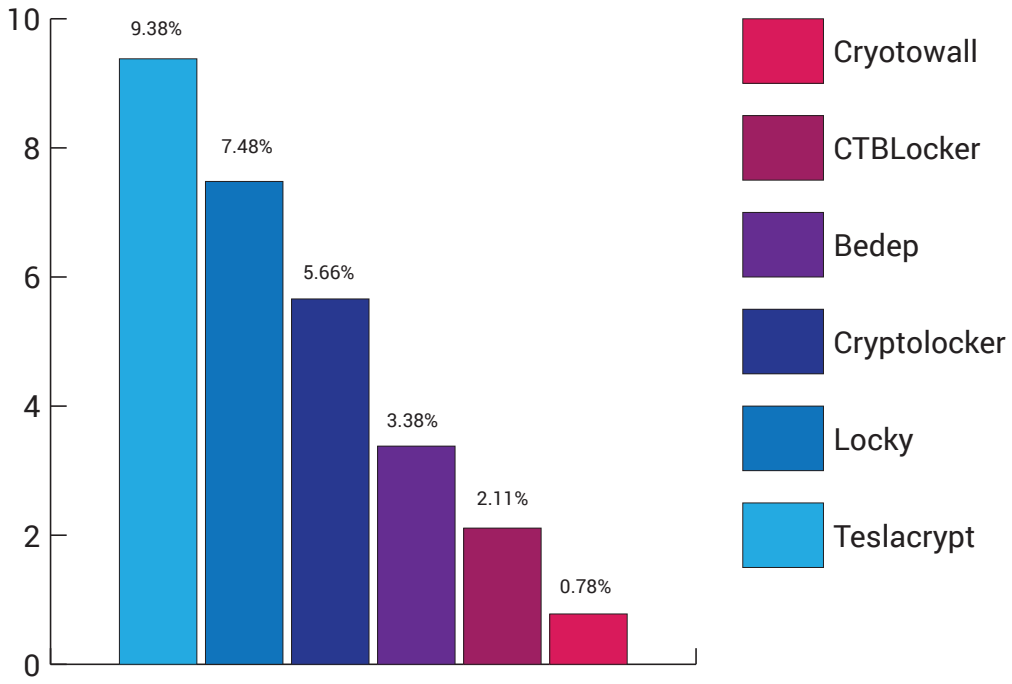


Principales familles de ransomwares sous Windows en Allemagne, 1er semestre 2016*

Contrairement à ce qui se passe au Royaume-Uni, où la plupart des infections de ransomwares sont diffusées via des téléchargements de type « drive-by », en Allemagne, les principaux vecteurs d'infection de CTBLocker sont généralement des pièces jointes infectées et de faux téléchargements. Le chiffrement des fichiers et la modification de leurs noms, au moyen de l'extension de fichier .ctbl, est souvent un bon indicateur d'une infection liée à CTBLocker – du moins, quand cela n'a pas été clairement spécifié dans les instructions de paiement.

Principales familles de ransomwares sous Windows en France, 1er semestre 2016

La situation de la France se distingue par rapport à celles des pays précédemment analysés, les trois principales menaces représentant globalement 22,52% du nombre total d'infections de ransomwares. Teslacrypt arrive en tête avec 9,38% de l'ensemble des attaques de ransomwares déclarées, Locky se classe en seconde position avec 7,48% et Cryptolocker se hisse à la troisième place, avec 5,66%.

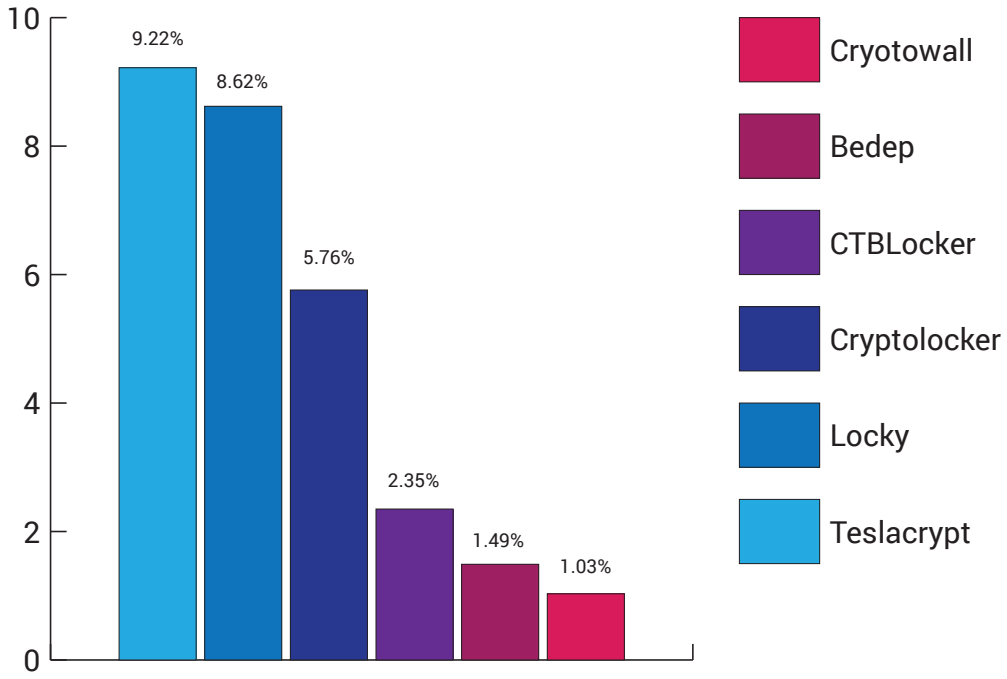


Principales familles de ransomwares sous Windows en France, 1er semestre 2016*

Les écarts minimes qui séparent le trio de tête, semblent indiquer que les cybercriminels ont utilisé une large palette de techniques pour infecter leurs victimes. Si d'autres pays ont été plus particulièrement visés par des infections de ransomwares spécifiques, il semblerait qu'en France, les cybercriminels aient recouru à tout l'arsenal de techniques possibles pour diffuser des ransomwares.

Principales familles de ransomwares sous Windows en Australie, 1er semestre 2016

Comme en France, les trois principales menaces de ransomwares en Australie sont au coude à coude, Teslacrypt arrivant en première position avec 9,22% de l'ensemble des attaques de ransomwares déclarées dans le pays. Locky suit de près avec 8,62% et Cryptolocker se classe à la troisième place avec 5,76%.

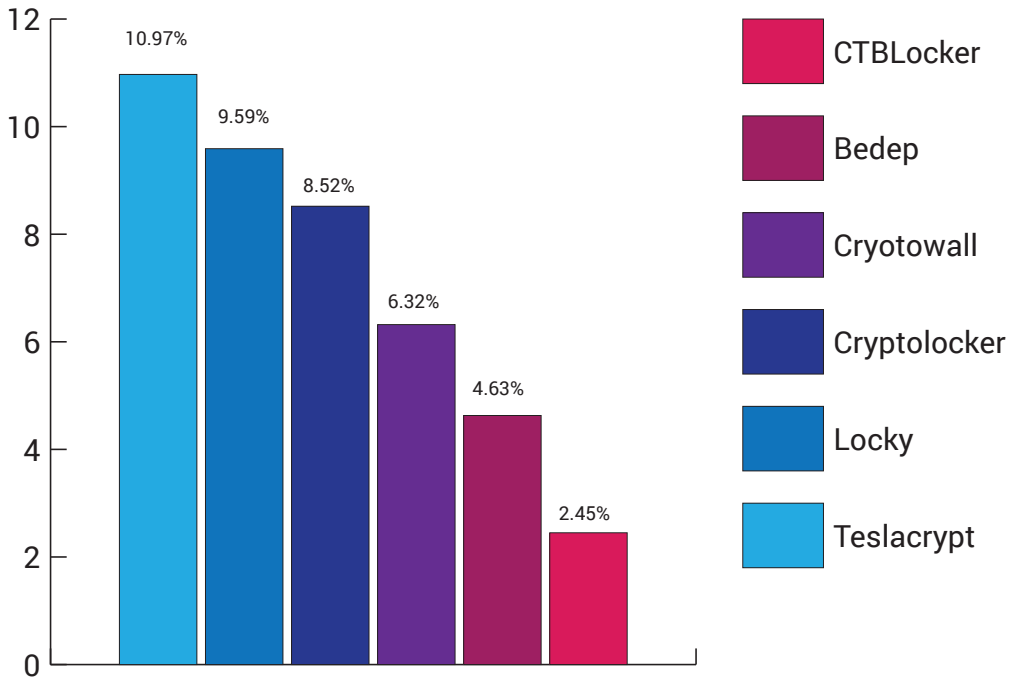


Principales familles de ransomwares sous Windows en Australie, 1er semestre 2016*

Les trois principales menaces étant à l'origine de 23,6% de l'ensemble des attaques de ransomwares déclarées en Australie, il est probable qu'un quart environ des infections de ransomwares aient été provoquées par l'une des familles de ransomwares citées précédemment.

Principales familles de ransomwares sous Windows en Roumanie, 1er semestre 2016

La Roumanie présente probablement l'un des profils les plus atypiques en termes d'attaques de ransomwares, dans la mesure où les pourcentages qui séparent les trois principales familles de ransomwares en tête du classement, sont encore plus resserrés. Bien que Teslacrypt arrive en tête avec 10,97% de l'ensemble des attaques de ransomwares déclarées dans le pays, Locky le talonne avec 9,59% et Cryptolocker arrive en troisième position avec 8,52%.



Principales familles de ransomwares sous Windows en Roumanie, 1er semestre 2016*

Ces rapports suggèrent probablement que les cybercriminels ont, là encore, déployé autant de versions de ransomwares que possible en utilisant divers vecteurs d'attaque, afin de s'assurer qu'ils infectent un grand nombre de victimes ayant différents comportements en ligne. Même si certaines personnes ont pu être infectées par le biais de téléchargements de type « drive-by », des pièces jointes et de faux programmes d'installation semblent également avoir été diffusés.

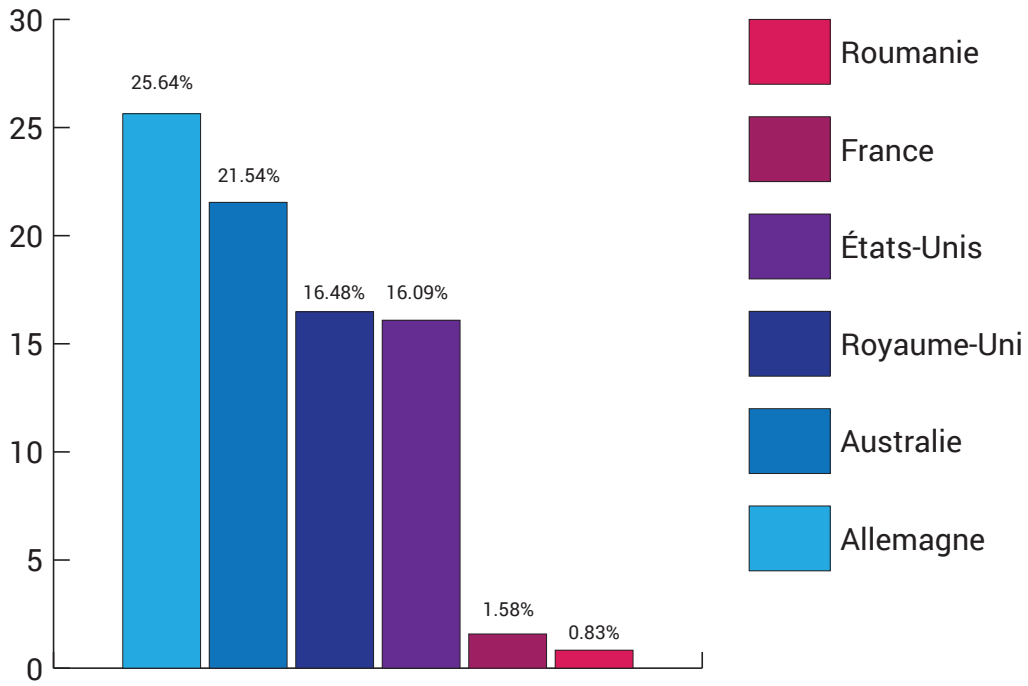
Ransomwares sous Android

Android étant le système d'exploitation archi-dominant dans le secteur des téléphones mobiles avec une part de marché culminant à 87,6%, selon IDC, les développeurs de malwares se sont logiquement focalisés sur le développement de menaces mobiles ciblant spécifiquement ce système d'exploitation. Dans la mesure où les ransomwares visant les PC se sont avérés être une excellente source de revenus, ce n'était qu'une question de temps jusqu'à leur transposition sous Android.

Même si nous avons vu des ransomwares pour Android apparaître dans de précédents rapports sur le paysage des menaces touchant les mobiles, au cours du premier semestre 2016, cette menace particulière a pris beaucoup d'ampleur, à la fois en termes d'occurrences et de complexité. Parmi les pays les plus touchés au sein desquels des attaques perpétrées par la famille de ransomwares Android SLocker ont été rapportées, figurent l'Allemagne, l'Australie, le Royaume-Uni et les États-Unis.

Principaux pays ayant déclaré le plus d'attaques de ransomwares

Même si des problèmes de ransomwares visant Android ont été signalés dans le monde entier, touchant tous les pays indépendamment de leur niveau de développement économique, il semblerait que l'Allemagne ait été la plus touchée, avec 25,64% de l'ensemble des attaques de malwares sous Android, déclarées au niveau mondial, dont plus d'une sur quatre était un ransomware.



Pays touchés par le ransomware Android.Trojan.Slocker*

Même si l'Allemagne semble détenir le record en matière de ransomwares sous Android, l'Australie se classe deuxième du classement, les ransomwares sous Android totalisant 21,54% du nombre total d'attaques de malwares déclarées dans le pays. Bien que les deux pays se trouvent aux antipodes l'un de l'autre, les cybercriminels se sont probablement concentrés sur eux, en raison de la forte pénétration du système d'exploitation Android sur ces marchés et aussi parce que les utilisateurs respectifs de ces deux pays sont particulièrement enclins à payer pour récupérer leurs données, plutôt que prendre le risque de les perdre.

Le Royaume-Uni et les États-Unis sont au coude à coude, avec le Royaume-Uni enregistrant 16,54% des attaques et les États-Unis 16,48%. Toutefois, bien que les pourcentages puissent sembler très proches, il y a probablement une grande différence entre les deux pays quant au nombre réel d'infections. Cela est vraisemblablement dû au fait que les rapports proviennent de deux bases d'utilisateurs complètement différentes.

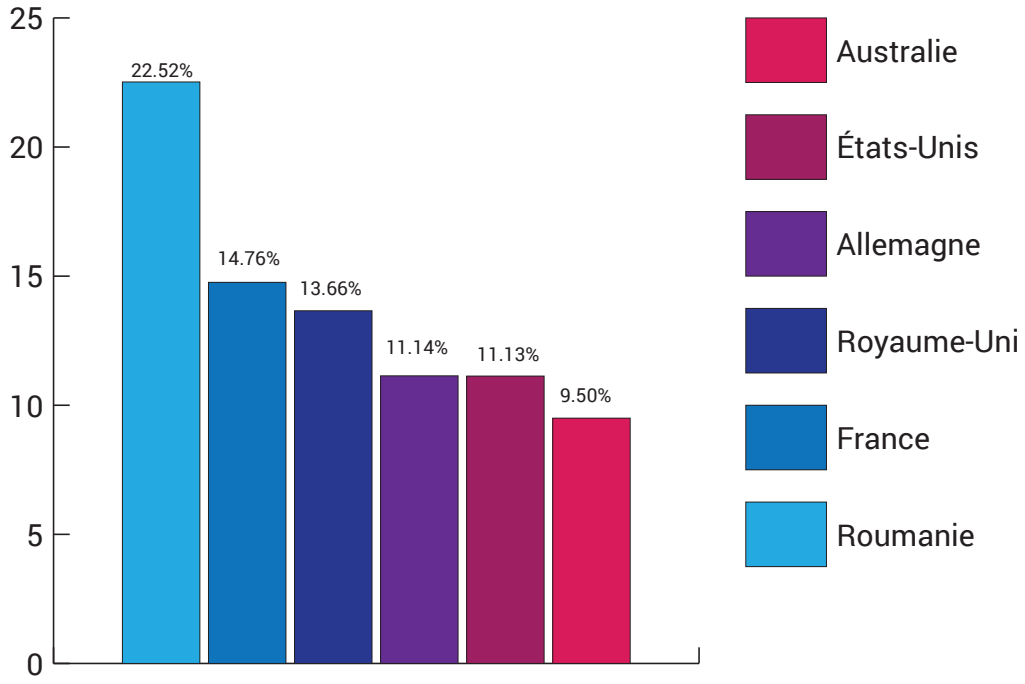
La France et la Roumanie représentent respectivement 1,58% et 0,83% des attaques, ce qui semble positif et peut signifier à la fois que les

utilisateurs sont bien plus conscients de la nécessité de sécuriser leurs appareils mobiles dans ces régions, ou qu'ils ne constituent pas une cible particulièrement lucrative aux yeux des cybercriminels.

Les adwares, les faux installeurs et les applications cachées toujours en tête des menaces dans le monde

Comme nous l'avons vu dans quelques-uns de nos précédents rapports, les malwares sous Android, les faux programmes d'installation et les applications de type adware demeurent une menace permanente pour les utilisateurs. Si les cybercriminels ont diffusé les ransomwares, prioritairement dans les pays les plus développés du point de vue économique, il semblerait que les adwares et les faux installeurs aient, quant à eux, été principalement diffusés dans les pays où les déclarations d'attaques de ransomwares ont été les plus rares.

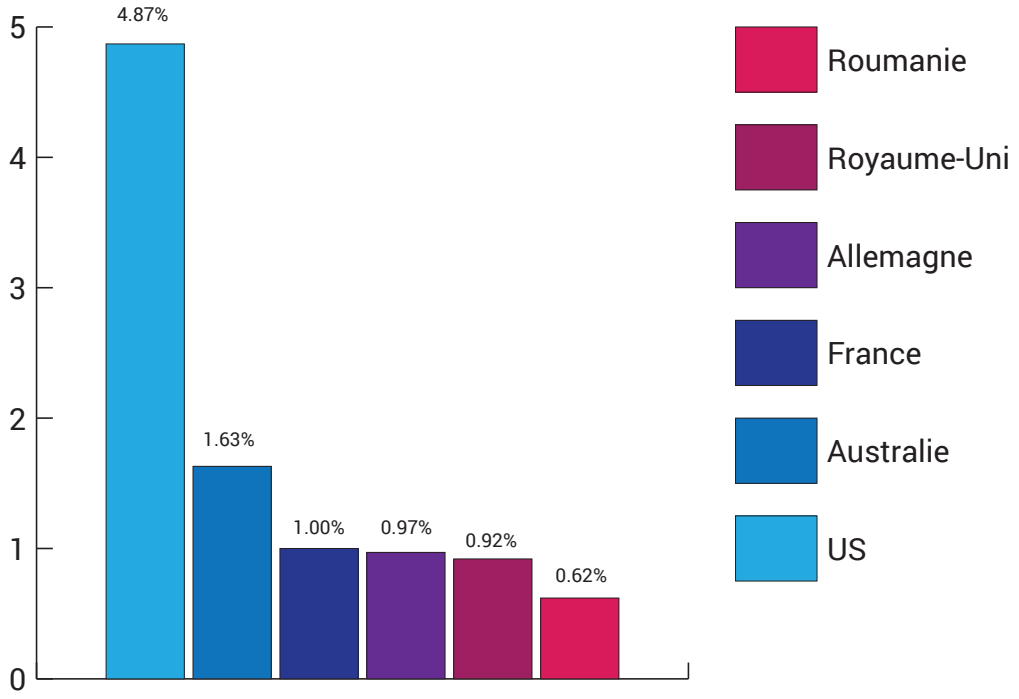
Par exemple, la Roumanie semble détenir le plus grand nombre d'adwares, la famille Android.Trojan.HiddenAds étant à l'origine du plus grand nombre de déclarations relatives à des malwares dans le pays, avec 22,52%. À titre comparatif, la même famille de malwares a été à l'origine de moins de 15% (14,76%) de l'ensemble des malwares en France, de 13,66% au Royaume-Uni, de 11,14% en Allemagne, de 11,13% aux États-Unis et de 9,50% en Australie. Même si les développeurs de malwares ciblent dans une moindre proportion la Roumanie et la France avec des ransomwares, il semblerait qu'ils génèrent des revenus conséquents via des applications dans lesquelles ont été injectées des publicités agressives.



Pays touchés par la famille de malware Android.Trojan.HiddenAds*

L'une des conséquences de l'installation d'applications, qui sont truffées d'adwares, est que les utilisateurs sont constamment sollicités par des fenêtres pop-up, redirigés par leur navigateur Web, et souvent à court de batterie en raison de cette activité incessante. Même si ces adwares ne sont pas malveillants en soi, ils ont tendance à gêner les utilisateurs et à gâcher l'utilisation de leurs appareils Android.

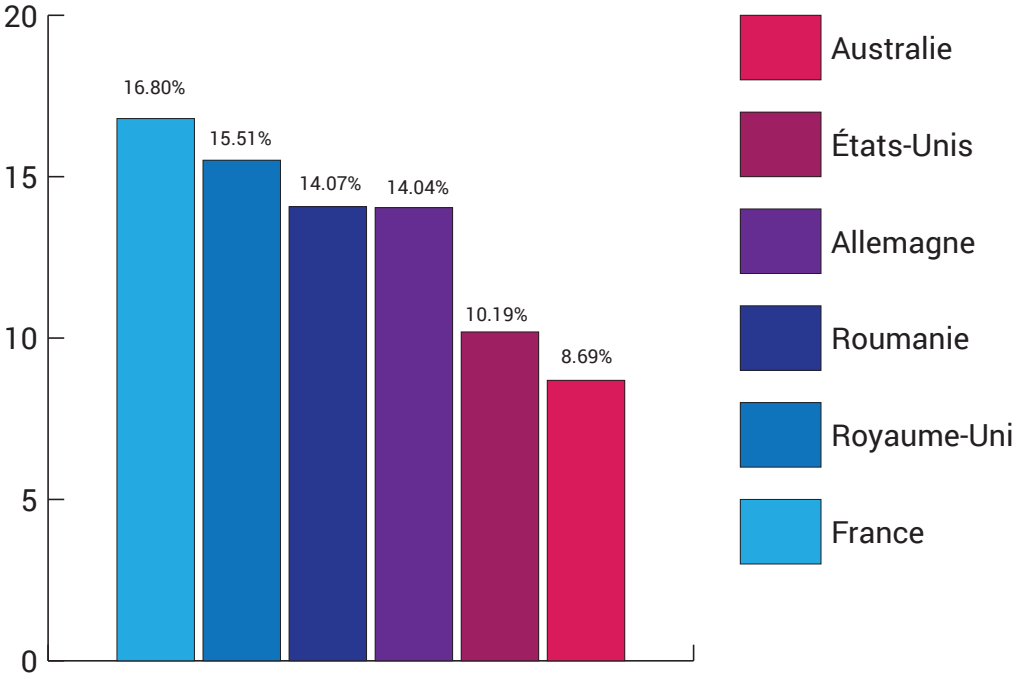
Dans la catégorie des fausses applications se faisant passer pour des applications populaires pour inciter les utilisateurs à les installer, la famille de malwares Android.FakeInst a fait l'objet du plus grand nombre de signalements aux États-Unis, avec 4,87% de l'ensemble des déclarations d'attaques de malwares sur Android, dans le pays.



Pays touchés par la famille de malware Android.Trojan.FakeInst*

Bien souvent, les familles de malwares de ce type se font passer pour des logiciels de sécurité pour mobile, afin d'inciter les utilisateurs peu méfiants à les télécharger. Après avoir réalisé une fausse analyse du système, les malwares tentent d'affoler leurs victimes et les poussent à payer diverses sommes d'argent pour pouvoir débloquer « l'ensemble des fonctionnalités » des applications, qui leur permettront, soi-disant, de débarrasser leur appareil de tous les (faux) malwares. Évidemment, les options de paiement incluent rarement des services permettant un suivi des transactions, tels que PayPal, et impliquent fréquemment l'utilisation de « MoneyPack » ou autres options de paiement similaires.

Une autre famille de malwares touchant Android, connue sous le nom d'Android.HiddenApp, a deux objectifs : inciter les utilisateurs à installer les malwares et dissimuler leur présence – en modifiant leur nom en quelque chose se rapprochant d' « Administrateur système » – une fois installés sur l'appareil. À partir de là, les malwares commencent à solliciter les utilisateurs pour qu'ils installent d'autres applications comprenant des publicités agressives ou encore abonnent leurs victimes à des numéros surtaxés.



Pays touchés par la famille de malware Android.Trojan.HiddenApp*

Même si la plupart de ces applications sont généralement téléchargées et installées par le biais de marketplaces non officielles, il y a eu des cas où elles ont été trouvées sur Google Play, la boutique officielle de Google.

La famille Android.HiddenApp a été principalement signalée en France (16,80%), puis au Royaume-Uni (15,51%), en Roumanie (14,07%) et en Allemagne (14,04%), qui sont les pays principalement touchés par cette famille de malware. Ce n'est probablement pas une coïncidence de considérer que la famille de malwares Android.HiddenApp semble être présente dans les mêmes pays.

Technologie de Machine Learning, brevetée pour la détection des ransomwares

Avec déjà plus de sept brevets publiés pour l'utilisation des algorithmes de Machine Learning pour la détection des malwares et autres menaces en ligne, l'utilisation de techniques d'apprentissage automatique et de détection basée sur les anomalies, joue un rôle crucial dans la lutte proactive contre les menaces nouvelles et inconnues.

Les ransomwares sont non seulement devenus un fléau pour Windows, mais ils ciblent également Android depuis quelques années. Les pertes financières, évaluées à plusieurs centaines de millions de dollars – certaines estimations indiquant qu'elles pourraient atteindre un milliard de dollars en 2016 – montrent que les mécanismes et les technologies de sécurité traditionnels n'ont pas réussi à assurer une protection complète contre ce type de malware.

Chez Bitdefender, nous travaillons sur les algorithmes de Machine Learning depuis 2009, en les développant et en les entraînant sans cesse à identifier de nouvelles menaces inconnues. L'intelligence artificielle et les algorithmes de Machine Learning sont essentiels pour lutter contre un ensemble de menaces toujours plus vaste et plus sophistiqué que jamais. Contrairement aux autres éditeurs de solutions de sécurité, Bitdefender cumule de nombreuses années d'expérience dans la mise au point de ces technologies, et nos solutions obtiennent clairement de meilleurs taux de détection, avec moins de faux positifs que la concurrence lors des tests des organismes indépendants.

Les algorithmes d'apprentissage automatique améliorent considérablement le temps de détection des menaces de ransomwares, dans la mesure où ils sont capables d'analyser de grandes quantités de données beaucoup plus rapidement que ne le ferait n'importe quel être humain. S'ils sont entraînés à détecter précisément différents types de comportements de malwares, les algorithmes de Machine Learning peuvent obtenir un taux de détection élevé, même lorsqu'il s'agit d'échantillons nouveaux ou inconnus.

L'alliance de l'ingéniosité humaine et de l'apprentissage automatique, fort de sa rapidité et de la constance de son analyse des données, accélère nettement les réactions contre les nouveaux échantillons de ransomwares, offrant même une protection contre des échantillons jusque-là inconnus. Toutefois, la détection ne repose pas toujours sur un algorithme d'apprentissage automatique unique. Par exemple, la détection des ransomwares nécessite le croisement de plusieurs algorithmes, chacun étant spécialisé dans la détection de familles spécifiques ayant des comportements individuels. Cela augmente significativement les chances de détecter des échantillons de ransomwares similaires tout en réduisant le nombre de faux positifs.

Lorsque l'on entraîne les algorithmes d'apprentissage automatique sur de grands ensembles d'échantillons de ransomwares, ils sont capables d'identifier rapidement les indicateurs de compromission et d'aider la solution de sécurité à empêcher le chiffrement de fichiers par les échantillons de ransomwares nouveaux ou inconnus.

Des défenses multiples contre les ransomwares avec Bitdefender GravityZone

Grâce à l'utilisation de technologies avancées d'analyse comportementale, Bitdefender a détecté 99,99% des menaces inconnues lors des tests indépendants réalisés par l'organisme AV-Comparatives.

Bitdefender Advanced Threat Control (ATC) surveille en continu les processus en cours d'exécution à la recherche de comportements malveillants. Cette technologie innovante lancée en 2008 sous le nom d'AVC (Active Virus Control) est constamment améliorée afin de permettre à Bitdefender de garder une longueur d'avance sur les menaces émergentes.

Bitdefender possède également deux couches de défense anti-ransomware supplémentaires – une liste noire de plus de 2,8 millions d'échantillons qui ne cesse d'augmenter, ainsi qu'un vaccin capable d'immuniser les appareils contre le processus de chiffrement.

Au printemps 2016, Bitdefender a été capable de détecter le ransomware Petya et de proposer gratuitement aux victimes potentielles, un outil qui intercepte le processus de chiffrement et fournit la clé de déchiffrement. Il convient de préciser que l'outil doit être installé préalablement à l'infection – et non après – afin d'accomplir correctement ses fonctions.

Auparavant, les chercheurs des Bitdefender Labs avaient publié un nouvel outil de vaccination capable de protéger contre les versions connues et les éventuelles versions futures des familles de ransomwares précédemment citées – CTBLocker, Locky et Teslacrypt – en exploitant les failles dans leurs méthodes de diffusion. D'après les Bitdefender Labs, ces familles de ransomwares font encore partie des plus répandues, à ce jour.

En novembre 2016 est apparu un ransomware très intéressant ciblant les serveurs Web Linux. Heureusement, une faille de programmation a permis aux chercheurs de Bitdefender de découvrir la clé de déchiffrement et de fournir gratuitement aux victimes, un utilitaire de récupération. Deux mois plus tard, le premier ransomware entièrement fonctionnel visant macOS, se basait sur une réécriture du célèbre Linux.Encoder.

Voici quelques actions utiles pour protéger votre entreprise contre les ransomwares :[1]

- Sauvegardez régulièrement vos données et contrôlez l'intégrité de ces sauvegardes. Les sauvegardes sont essentielles en cas d'incidents liés à des ransomwares ; si vous êtes infecté, elles peuvent constituer le meilleur moyen de récupérer vos données critiques.
- Sécurisez vos sauvegardes. Veillez à ce que les sauvegardes ne soient pas connectées aux ordinateurs et aux réseaux qu'elles sauvegardent. Par exemple, réalisez des sauvegardes dans le Cloud ou stockez-les sur un support physique hors ligne. Il convient de noter que certains ransomwares ont la capacité de verrouiller les sauvegardes basées dans le Cloud lorsque les systèmes réalisent en continu des sauvegardes en temps réel, une action également connue sous le nom de « synchronisation continue ».
- Examinez avec attention les liens contenus dans les e-mails et n'ouvrez jamais les documents joints à des e-mails non sollicités.
- Lorsque vous téléchargez des logiciels – en particulier des logiciels gratuits – ne le faites qu'à partir de sites que vous connaissez et en lesquels vous avez confiance. Quand cela est possible, vérifiez l'intégrité du logiciel au moyen d'une signature numérique, avant son exécution.
- Veillez à ce que les correctifs d'applications pour vos systèmes d'exploitation, logiciels et firmwares soient à jour, y compris Adobe Flash, Java, les navigateurs Web, etc.
- Veillez à ce que votre solution antimalware soit paramétrée pour se mettre à jour automatiquement et pour effectuer des analyses régulièrement.
- Désactivez les scripts de macro des fichiers transmis par e-mail. Envisagez d'utiliser le logiciel Office Viewer pour ouvrir les fichiers Microsoft Office transmis par e-mail plutôt que d'utiliser l'ensemble des applications de la suite Office.
- Mettez en place des restrictions logicielles ou d'autres contrôles afin d'empêcher l'exécution de programmes dans des emplacements couramment utilisés par les ransomwares, tels que les dossiers temporaires utilisés par les principaux navigateurs Internet ou les programmes de compression/décompression, y compris ceux qui se trouvent dans le dossier AppData/LocalAppData.

Voici aussi quelques actions supplémentaires que votre entreprise peut mettre en œuvre :

- Misez sur la sensibilisation et la formation. Parce que les utilisateurs finaux sont souvent ciblés, les employés devraient être sensibilisés à la menace que représentent les ransomwares et à la façon dont ils se diffusent, et être formés aux principes et techniques de sécurité de l'information.
- Patchez tous les systèmes d'exploitation des endpoints, les logiciels et les firmwares, à mesure que des vulnérabilités sont découvertes. Cette mesure de précaution peut être facilitée par la mise en place d'un système centralisé de gestion des correctifs.
- Gérez l'utilisation des comptes disposant de privilèges élevés en appliquant le principe de la séparation des privilèges. Aucun utilisateur ne devrait bénéficier d'un accès administrateur, sauf en cas d'absolue nécessité. Les utilisateurs ayant besoin d'un compte administrateur, ne devraient s'en servir que lorsqu'ils en ont besoin ; le reste du temps, ils devraient travailler avec des comptes utilisateurs standards.
- Configurez le contrôle des accès en gardant à l'esprit le principe de la séparation des privilèges. Lorsqu'un utilisateur a uniquement besoin de consulter certains fichiers en lecture, il est inutile de lui accorder un accès en écriture pour ces fichiers, répertoires ou dossiers partagés.
- Utilisez des environnements virtualisés pour exécuter des systèmes d'exploitation ou programmes spécifiques.
- Catégorisez les données sur la base de la valeur organisationnelle et mettez en œuvre la séparation physique/logique des réseaux et des données pour les différentes unités organisationnelles. Par exemple, les recherches critiques ou encore les données de l'entreprise qui ne devraient pas résider sur le même serveur et/ou segment de réseau que l'environnement de messagerie électronique de l'entreprise.

[1]Ransomware victims in the US urged to report infections, FBI " warns », 19 septembre 2016, citant les recommandations du FBI, « Ransomware victims urged to report infections to federal law enforcement », https://www.ic3.gov/media/2016/160915.aspxto report infections to federal law enforcement », https://www.ic3.gov/media/2016/160915.aspx

- Exigez l'interaction obligatoire des utilisateurs lors de l'utilisation d'applications communiquant avec des sites Web non recensés par le proxy réseau ou le pare-feu. Par exemple, exigez la saisie d'informations ou de mots de passe lorsque le système communique avec un site Web non recensé.
- Établissez des listes blanches d'applications. Ne permettez aux systèmes d'exécuter que des programmes connus et autorisés par la politique de sécurité de l'entreprise.

À propos de Bitdefender

Bitdefender est une entreprise mondiale de sécurité qui développe des solutions de cybersécurité de pointe et qui protège plus de 500 millions d'utilisateurs dans plus de 150 pays. Depuis 2001, Bitdefender produit régulièrement des technologies leaders du marché pour les entreprises et les particuliers, et est un fournisseur de choix pour sécuriser les infrastructures hybrides et protéger les endpoints. Grâce aux équipes de R&D, d'alliances et de partenariats, Bitdefender arehaussé les standards de sécurité les plus élevés de l'industrie. Plus d'informations sur www.bitdefender.fr.

***Source :** Bitdefender Labs. **Auteurs :** Liviu Arsene, et Răzvan Mureșan, Spécialistes Sécurité.

Bitdefender propose des technologies de sécurité dans plus de 150 pays via un réseau de partenaires de premier plan, de distributeurs et de revendeurs à valeur ajoutée. Depuis 2001, Bitdefender produit régulièrement des technologies leaders du marché pour les entreprises et les particuliers et est l'un des plus grands fournisseurs de solutions de sécurité pour les technologies de virtualisation et cloud. Grâce aux équipes de R&D, d'alliances et de partenariats, Bitdefender a réhaussé les standards de sécurité les plus élevés de l'industrie en s'appuyant à la fois sur ses technologies classées N°1 et ses alliances stratégiques avec les principaux fournisseurs de technologies de virtualisation et de Cloud dans le monde. Plus d'informations sur www.bitdefender.fr