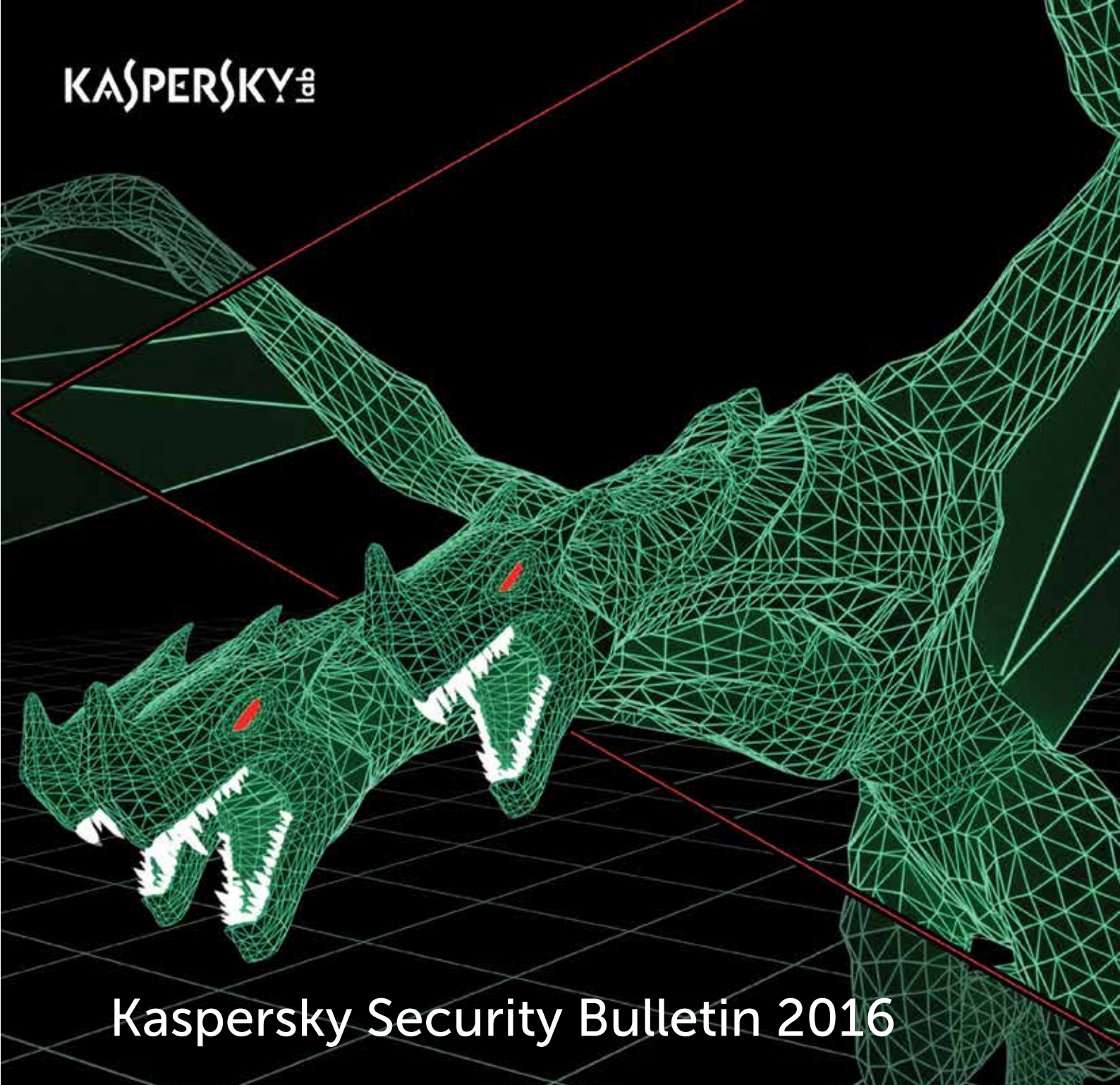
KASPERSKY lab



Kaspersky Security Bulletin 2016

LA RÉVOLUTION DU RANSOMWARE : HISTOIRE DE L'ANNÉE

GREAT

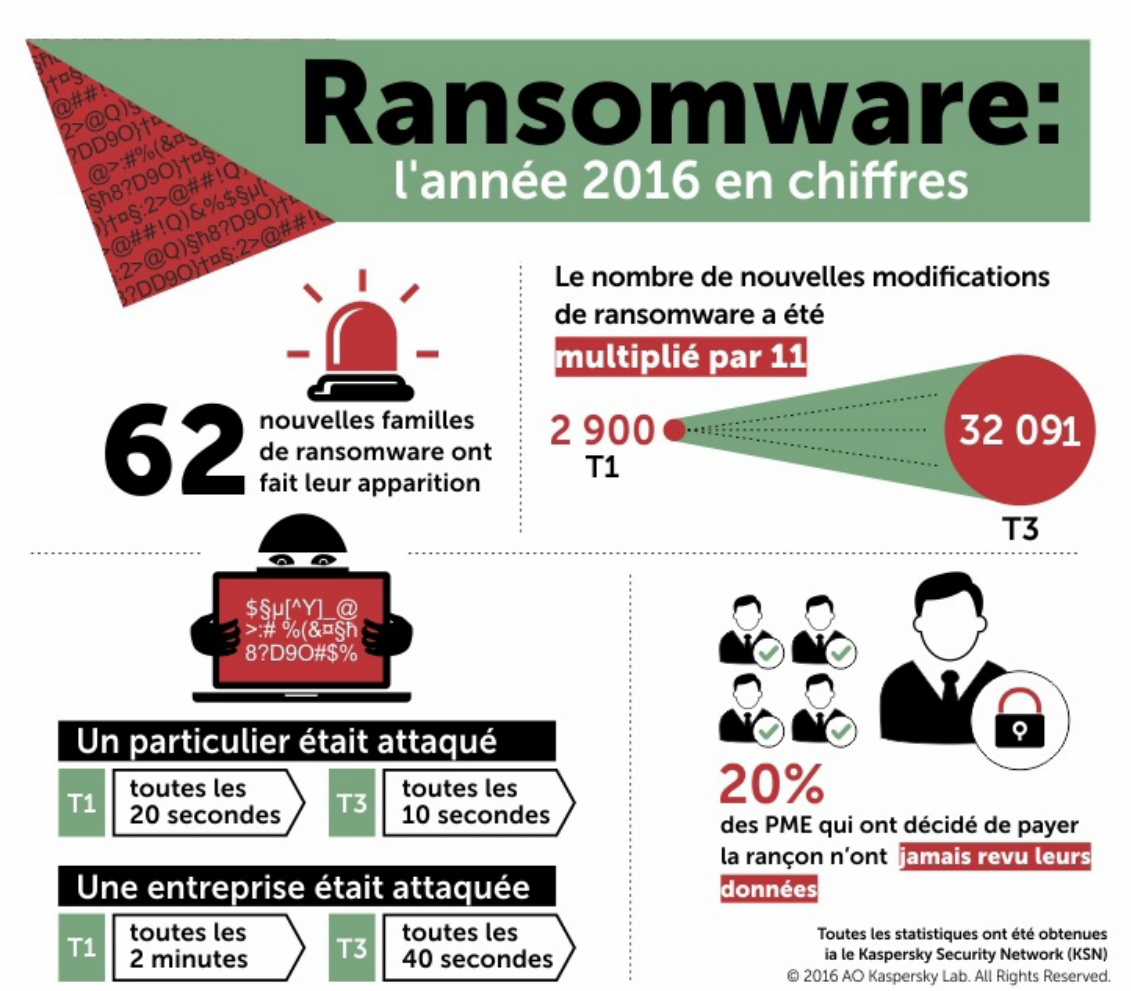
SOMMAIRE

INTRODUCTION

Au cours de l'année 2016, les ransomwares ont continué à semer la panique à travers le monde. Ils ont resserré l'étau sur les données et les appareils, ainsi que sur les particuliers et les entreprises.

Les chiffres parlent d'eux-mêmes :

- 62 nouvelles familles de ransomware ont vu le jour.
- Le nombre de modifications de ransomware a été multiplié par 11 : nous sommes passés de 2 900 nouvelles modifications en janvier/mars à 32 091 en juillet/septembre.
- Les attaques contre les entreprises ont triplé entre janvier et la fin du mois de septembre : la fréquence est passée d'une attaque toutes les deux minutes à une attaque toutes les 40 secondes.
- Pour les particuliers, la fréquence est passée d'une attaque toutes les 20 secondes à une attaque toutes les 10 secondes.
- 20 % des petites et moyennes entreprises qui ont décidé de payer la rançon n'ont jamais revu leurs données.



L'année **2016 aura également été l'année de la diversification et de la sophistication des ransomwares**. Voici quelques exemples de ces tendances : changement d'objectif en cas de détection d'un logiciel financier, programmation en langages de script, exploitation de nouvelles voies d'infection, ciblage accru des victimes et offre de solutions de ransomware en tant que services « clé en main » à des individus moins doués ou ne disposant pas du temps ou des ressources nécessaires pour créer leur propre ransomware, le tout dans un écosystème clandestin en pleine croissance et de plus en plus efficace.

Parallèlement à cela, nous avons observé en 2016 les premiers efforts de coopération dans la lutte contre ce fléau :

Le projet No More Ransom, qui unit la police des Pays-Bas, Europol, Intel Security et Kaspersky Lab, a été lancé au mois de juillet. 13 organisations ont rejoint l'initiative en octobre. Parmi les réalisations du projet, une des plus remarquables est la création de plusieurs outils de déchiffrement gratuits en ligne qui ont aidé à ce jour des milliers de victimes des ransomwares à récupérer leurs données.

Mais ceci n'est qu'un avant-goût des nombreuses choses qu'il reste encore à réaliser. Ensemble, nous pouvons obtenir bien plus de résultats que chacun séparément.

Qu'est-ce qu'un ransomware ?

Il y a deux types de ransomware. Le genre de ransomware le plus commun est le chiffreur. Ces programmes chiffrent les données sur l'appareil de la victime, puis promettent de les restaurer en échange du paiement d'une rançon. L'autre catégorie quant à elle, celle des bloqueurs, ne touche pas aux données stockées sur l'appareil. Ils se contentent de priver la victime de l'accès à son appareil. La demande de rançon affichée se présente souvent sous la forme d'un avis de la police qui signale à la victime qu'elle a consulté un site Internet au contenu illégal et qu'elle doit payer une amende forfaitaire. Vous trouverez ici une présentation générale des deux types de ransomware.

RANSOMWARE : TENDANCES ET DÉCOUVERTES PRINCIPALES DE 2016

"La majeure partie des ransomwares se nourrit d'une relation de confiance improbable entre la victime et l'agresseur, à savoir que les fichiers pris en otage seront restitués une fois que la rançon aura été payée. Les cybercriminels ont fait preuve d'un surprenant semblant de professionnalisme dans le respect de cette promesse."

GReAT, Prévisions sur les menaces pour 2017

Nouveautés et disparitions

En 2016, le monde a fait la connaissance de Cerber, Locky et CryptXXX, ainsi que de 44 287 nouvelles modifications de ransomwares.

A ce jour, Locky est présent dans

114

pays

Cerber et Locky sont apparus au début du printemps. Il s'agit de deux souches dangereuses et virulentes de ransomwares qui ont été largement diffusées, principalement via des pièces jointes dans le spam et des kits d'exploitation. Ils se sont très vite imposés en tant qu'acteurs majeurs qui ciblaient à la fois des particuliers et des entreprises. CryptXXX suivait de près. Ces trois familles poursuivent leur évolution et menacent toujours le monde, aux côtés de menaces déjà bien implantées comme CTB-Locker, CryptoWall et Shade.

Voici le Top 10 d'octobre 2016 des familles de ransomwares détectées par les produits de Kaspersky Lab :

	Nom	Verdicts*	Pourcentage d'utilisateurs**
1	CTB-Locker	Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion	25,32
2	Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7,07
3	TeslaCrypt (actif jusqu'en mai 2016)	Trojan-Ransom.Win32.Bitman	6,54
4	Scatter	Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan-Dropper.JS.Scatter	2,85
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2,79
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2,36
7	Shade	Trojan-Ransom.Win32.Shade	1,73
8	(generic verdict)	Trojan-Ransom.Win32.Snocry	1,26
9	Crysis	Trojan-Ransom.Win32.Crusis	1,15
10	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0,90

*Ces statistiques reposent sur les verdicts de détection renvoyés par les produits de Kaspersky Lab, chez les utilisateurs de nos produits qui ont accepté de fournir leurs statistiques.

** Pourcentage d'utilisateurs ciblés par un membre d'une famille de crypto-ransomware par rapport à l'ensemble des utilisateurs ciblés par des crypto-ransomwares.

Disparition de Teslacrypt, Chimera et Wildfire, ou du moins c'est ce que l'on croyait...

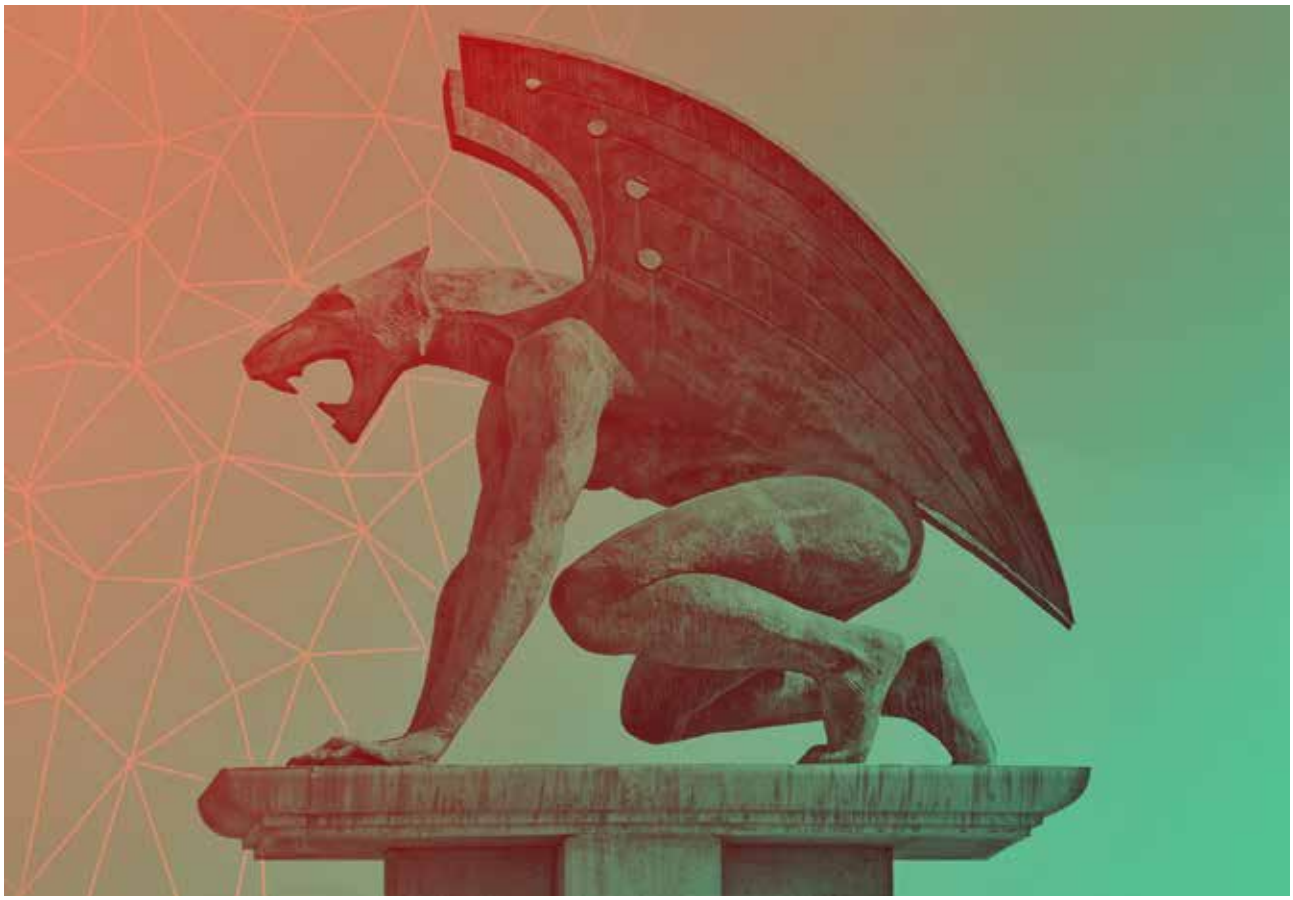
La plus grande surprise de 2016 aura probablement été l'arrêt des activités de TeslaCrypt, suivi par la divulgation de la clé principale, vraisemblablement par les auteurs du malware eux-mêmes.

TeslaCrypt s'est « suicidé » tandis que la police a démantelé les activités du ransomware en tant que service (RaaS) Encryptor et Wildfire. #KLReport

Encryptor RaaS, un des premiers trojans à proposer le modèle du ransomware en tant que service aux autres criminels, a fermé boutique après le démantèlement de son réseau de zombies par la police.

Ensuite, au mois de juillet, près de 3 500 clés du ransomware Chimera ont été divulguées par une personne qui affirme être à l'origine du ransomware Petya/Mischa. Toutefois, dans la mesure où Petya utilisait une partie du code source de Chimera pour son propre ransomware, il pourrait en fait s'agir du même groupe qui actualise tout simplement sa gamme de produits et provoque des problèmes.

De la même manière, Wildfire, dont les serveurs avaient été saisis et pour lequel une clé de déchiffrement avait été créée suite aux efforts conjoints de Kaspersky Lab, d'Intel Security et de la police néerlandaise, semble avoir refait surface sous le nom d'Hades.



Abus d'un ransomware « pédagogique »

Des chercheurs animés de bonnes intentions avaient développé un ransomware « pédagogique » dans le but d'offrir aux administrateurs système un outil pour simuler une attaque de ransomware et tester les mesures de protection. Les criminels n'ont pas perdu de temps pour détourner ces produits pour leurs propres fins malveillantes.

Un ransomware développé dans un contexte « pédagogique » a entraîné la naissance, entre autres, de Ded Cryptor et Fantom. #KLReport

Le développeur du ransomware pédagogique Hidden Tear & EDA2 eut la bonne idée de publier la source sur GitHub. Il n'est dès lors pas étonnant que de nombreux trojans malveillants inspirés de ce code soient apparus en 2016. Citons parmi ceux-ci Ded_Cryptor qui remplaçait le fond d'écran de l'ordinateur de la victime par l'image d'un méchant Père Noël et exigeait le versement d'une rançon importante de 2 Bitcoins (environ 1 300 dollars américains). Ou encore Fantom qui reproduisait un écran semblable à un écran de mise à jour Windows véritable.

Méthodes atypiques

Les attaquants visent désormais les sauvegardes et les disques durs et ils obtiennent les mots de passe par force brute #KLReport

- Pourquoi se contenter d'un fichier quand tout le disque est à portée de main ?

  De nouveaux concepts d'attaque de ransomware ont été utilisés pour la première fois en 2016. Nous pensons notamment au chiffrement de disque : les attaquants bloquent l'accès à tous les fichiers d'un coup ou chiffrent l'ensemble de ceux-ci. Petya appartient à cette catégorie : il brouille l'index principal du disque dur d'un utilisateur et rend le redémarrage impossible. Dcryptor, un autre trojan connu également sous le nom de Mamba, va encore plus loin en verrouillant l'ensemble du disque dur. Ce ransomware est particulièrement désagréable dans la mesure où il brouille chaque secteur du disque, dont le système d'exploitation, les applications, les fichiers partagés et toutes les données personnelles, à l'aide d'une copie du logiciel open-source DiskCryptor.

- La technique d'infection « manuelle »

  L'infection de Dcryptor se déroule manuellement : les attaquants obtiennent les mots de passe par force brute en vue d'accéder à distance à l'ordinateur de la victime. Cette méthode n'est pas neuve, mais elle a été employée à de nombreuses reprises en 2016, souvent pour attaquer des serveurs et accéder au réseau d'une entreprise.

  Si l'attaque réussit, le trojan s'installe, puis chiffre les fichiers sur le serveur, voire sur l'ensemble des dossiers partagés accessibles depuis le serveur en question. Nous avons découvert TeamXRat qui adopte également cette méthode pour diffuser son ransomware sur des serveurs brésiliens.

Shade téléchargeait un spyware quand il trouvait des logiciels financiers #KLReport

- Deux infections en une

  Nous avons repéré au mois d'août un échantillon de Shade doté d'une fonction inattendue : s'il s'avérait que l'ordinateur infecté appartenait à des services financiers, le malware oubliait sa fonction principale et téléchargeait, puis installait un spyware, probablement dans le but à long terme de voler de l'argent.

Ransomware en langages de script

L'augmentation du nombre de chiffreurs programmés en langages de script est une autre tendance qui a attiré notre attention en 2016. Rien qu'au cours du 3e trimestre, nous avons découvert plusieurs nouvelles familles programmées en Python, dont HolyCrypt et CryPy, ainsi que Stampado, créé dans le langage d'automatisation AutoIt.

Une ribambelle d'amateurs et de copieurs

Un ransomware de qualité médiocre augmente la probabilité de perdre les données à tout jamais #KLReport

Parmi tous les nouveaux trojans ransomwares détectés en 2016, un grand nombre s'est avéré être de qualité médiocre, d'un niveau primaire avec des erreurs de programmations et des fautes grossières dans les demandes de rançon.

Nous avons également enregistré un augmentation des ransomwares copieurs. En effet, nous avons remarqué les éléments suivants :

- Bart copie la demande de rançon et le style de la page de paiement de Locky.
- Une copie Autoit de Locky (baptisée AutoLocky) utilise la même extension « .locky ».
- Crusis (connu également sous le nom de Crysis) copie l'extension « .xtbl » utilisée à l'origine par Shade.
- Xorist adopte la nomenclature de Crusis pour les fichiers chiffrés.

Mais la copie la plus flagrante que nous avons découverte cette année a été Polyglot (connu également sous le nom MarsJoke). Il imite parfaitement l'aspect et la méthode de traitement des fichiers de CTB-Locker.

Toutes ces tendances vont se renforcer en 2017.

"Alors que la popularité de ce type d'attaque continue d'augmenter et que des criminels de bas étage entrent en scène, il faut s'attendre à voir de plus en plus de ransomwares dépourvus de l'assurance qualité ou des capacités de codage générales pour respecter cette promesse. Il faudra compter sur l'émergence de ransomwares de « script kiddies » qui bloquent l'accès aux fichiers ou au système ou qui suppriment simplement les fichiers, amènent la victime à payer la rançon et ne rendent rien en retour."

GReAT, Threat Predictions for 2017

L'ÉCONOMIE FLORISSANTE DU RANSOMWARE

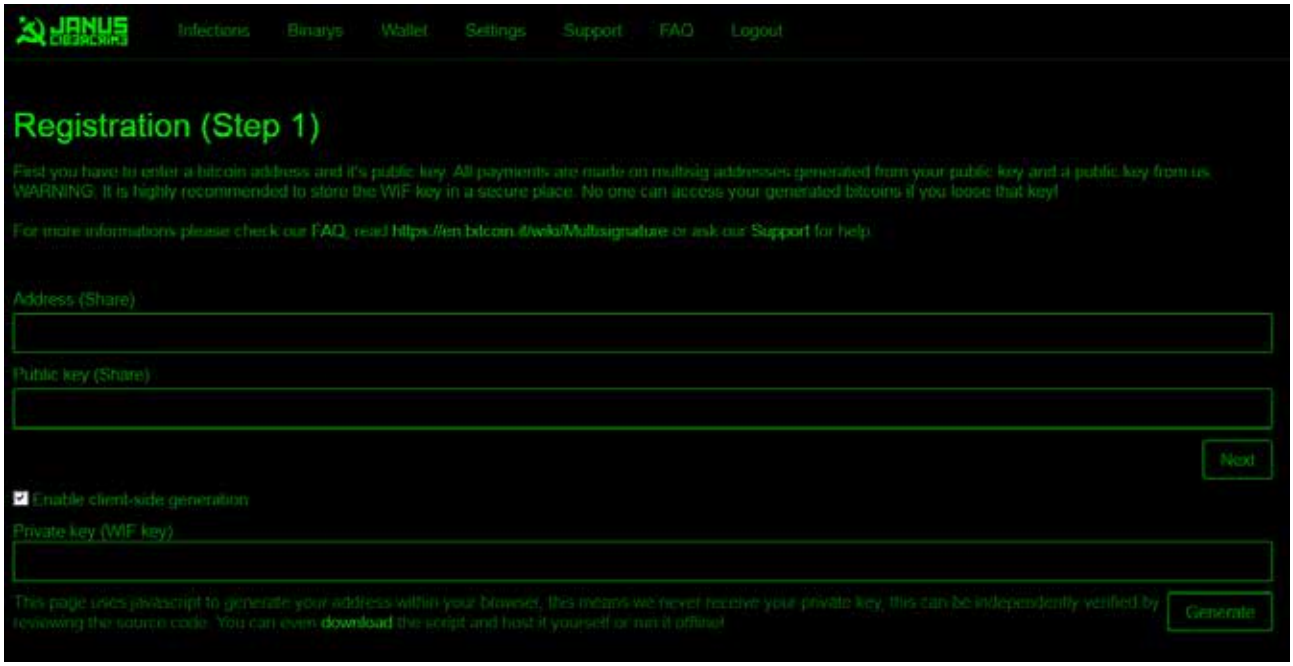
Le ransomware est de plus en plus souvent disponible à la demande dans les milieux clandestins criminels #KLReport

L'avènement du RaaS

Le ransomware en tant que service (RaaS) n'est pas une nouvelle tendance. Elle a poursuivi son développement en 2016 et le nombre d'auteurs de ransomware qui offrent une utilisation « à la demande » de leurs créations ne cesse d'augmenter. Ce concept est particulièrement attrayant pour les criminels qui ne disposent pas des aptitudes, des ressources ou de l'envie nécessaires pour développer leur propre ransomware.

Parmi les exemples les plus marquants de ransomwares apparus en 2016 qui ont adopté ce modèle, nous retrouvons Petya/Mischa et Shark, rebaptisé ultérieurement sous le nom d' Atom.

Ce modèle d'activité est de plus en plus perfectionné :



Le site de partenariat du ransomware Petya

Le partenaire qui choisit cette méthode conclut souvent un accord traditionnel qui repose sur le paiement d'une commission. Par exemple, les tarifs du ransomware Petya nous apprennent qu'un partenaire qui a gagné 125 Bitcoins en une semaine conservera 106,25 Bitcoins après commission.

Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

Tarifs de Petya

N'oublions pas non plus les frais d'utilisation à payer au début. Ainsi, l'individu intéressé par l'idée de travailler avec le ransomware Stompado devra par exemple débourser 39 dollars.

Dans la mesure où d'autres criminels proposent également leurs services pour la diffusion de spam, les demandes de rançons, etc., l'attaquant en herbe peut lancer son activité sans trop de difficultés.

Des réseaux avec commissions jusqu'à l'assistance à la clientèle en passant par le branding

Les criminels proposent un service à la clientèle pour garantir des taux plus élevés de paiement de la rançon #KLReport

Les ataquants les plus « professionnels » proposaient à leurs victimes un service d'assistance pour les accompagner dans la procédure d'achat des Bitcoins nécessaires au paiement de la rançon. Certains d'entre eux acceptaient même de négocier. Chaque étape encourageait un peu plus la victime à payer.

Des experts de Kaspersky Lab qui étudiaient le phénomène ransomware au Brésil ont remarqué que dans de nombreux cas d'attaques, le branding du ransomware revêtait une certaine importance. Les individus malintentionnés qui cherchaient à obtenir l'attention des médias et à faire peur aux clients choisissaient le prestige, une célébrité ou une astuce tandis que ceux qui préféraient la discrétion ignoraient les trompettes de la renommée et se contentaient de présenter aux victimes une adresse email pour les contacts et une adresse Bitcoin pour les paiements.

Tout est une question de Bitcoins

Tout au long de l'année 2016, les Bitcoins ont conservé leur statut de devise préférée des familles de ransomware les plus répandues pour le paiement des rançons. Les exigences de la plupart des ransomwares étaient raisonnables et atteignaient en moyenne 300 dollars américains. Ceci étant dit, certaines victimes ont du payer des sommes bien plus importantes.

Les exploitants d'opérations régionales et plus artisanales préféraient quant à eux une option de paiement local, même si cela signifiait qu'ils ne pouvaient plus profiter de la couverture et se noyer dans le bruit du reste des ransomwares.

LES ENTREPRISES, NOUVELLES VICTIMES DU RANSOMWARE

Une entreprise est victime d'une attaque de ransomware toutes les 40 secondes #KLReport

Au cours du 1er trimestre 2016, 17 % des attaques de ransomware visaient des entreprises. En d'autres termes, une entreprise quelque part dans le monde était victime d'une attaque tous les deux minutes*. A la fin du 3e trimestre, cet indicateur était passé à 23,9 %, soit une attaque toutes les 40 secondes.

D'après des recherches réalisées par Kaspersky Lab , au cours de l'année 2016, une entreprise sur cinq à travers le monde a été victime d'un incident de sécurité de l'information suite à une attaque de ransomware.

- 42 % des petites et moyennes entreprises ont été victimes du ransomware au cours des 12 derniers mois.
- 32 % d'entre elles ont payé la rançon.
- Une entreprise sur cinq n'a jamais revu ses fichiers, même après avoir payé.
- 67 % des entreprises touchées par un ransomware ont perdu une partie ou la totalité de leurs données d'entreprise et 25 % d'entre elles ont consacré plusieurs semaines au rétablissement de l'accès.

* Ces estimations reposent sur les éléments suivants : 17 % de 372 602 utilisateurs uniques chez qui les produits de Kaspersky Lab ont bloqué des attaques de ransomware au T1 2016 et 23,9 % de 821 865 utilisateurs uniques chez qui les produits de Kaspersky Lab ont bloqué des attaques de ransomware au T3 2016.

Une P.M.E. sur cinq n'a jamais revu ses fichiers, même après avoir payé. #KLReport

Plus aucun secteur n'est épargné désormais #KLReport

L'ingénierie sociale et l'erreur humaine demeurent deux facteurs clé dans la vulnérabilité des entreprises. Un cas sur cinq de pertes significatives de données a été le résultat d'un imprudence ou d'un manque de conscience d'un employé.

S'il est vrai que certains secteurs sont plus touchés que d'autres, nos recherches démontrent que le risque existe pour tous les secteurs.

	Secteur	% victimes d'attaques de ransomware
1	Education	23
2	Informatique/Télécommunications	22
3	Divertissements/Média	21
4	Services financiers	21
5	Construction	19
6	Gouvernement/secteur public/Défense	18
7	Manufacture	18
8	Transports	17
9	Santé	16
10	Vente au détail/Vente en gros/Loisirs	16

"Nous remarquons que le ransomware est plus ciblé. Les groupes criminels sélectionnent soigneusement leurs victimes avant d'organiser une campagne d'harponnage. La sélection s'opère sur la basedesdonnéesquelesvictimespossèdent et/ou sur le fait qu'elles comptent sur la disponibilité de ces données de valeur. "

John Fokker, Coordonnateur de l'équipe numérique de la brigade nationale de lutte contre les délits technologique des Pays-Bas

Attaques de ransomwares qui ont fait la une des journaux

- **Les hôpitaux sont devenus** une cible de prédilection, avec tous les effets dévastateurs que l'on peut imaginer dans la mesure où des interventions chirurgicales sont annulées, des patients sont renvoyés vers d'autres hôpitaux, etc.

  - L'attaque de ransomware qui aura fait le plus parler d'elle s'est produite au mois de mars lorsque des criminels ont verrouillé les ordinateurs du Hollywood Presbyterian Medical Center de Los Angeles, jusqu'à ce que l'hôpital décide de payer un montant de 17 000 dollars américains.
  - Quelques semaines plus tard, des attaques similaires touchaient des hôpitaux en Allemagne.
  - Au Royaume-Uni, 28 entités du National Health Service ont reconnu qu'elles avaient été attaquées en 2016.

- VESK, **le fournisseur de service cloud et de bureau hébergé**, a versé une rançon de près de 23 000 dollars pour récupérer l'accès à un de ses systèmes qu'il avait perdu suite à une attaque organisée en septembre.

- Des **médias de renom**, dont le New York Times, la BBC et AOL ont été touchés en mars 2016 par un malware qui contenait un ransomware.

- **L'Université de Calgary au Canada**, qui est un grand centre de recherches, a admis qu'elle avait payé la somme de 16 000 USD pour récupérer des courriers électroniques qui avaient été chiffrés pendant une semaine.

- Un **petit commissariat de police** au Massachusetts a du payer une rançon de 500 dollars américains (en Bitcoins) afin de récupérer des données essentielles à une enquête en cours après qu'un agent avait ouvert une pièce jointe malveillante.

- **Même le monde des courses automobiles n'a pas été épargné** : une des grandes équipes NASCAR a perdu des données estimées à plusieurs millions de dollars suite à une attaque TeslaCrypt au mois d'avril.losing data worth millions to a TeslaCrypt attack in April

LA RIPOSTE

Par le biais des technologies

Les versions les plus récentes des solutions de Kaspersky Lab destinées aux P.M.E. sont désormais dotées d'une fonction de lutte contre les malwares de chiffrement. De plus, un nouvel outil de lutte contre les ransomwares gratuit a été mis à la disposition de toutes les entreprises, quelle que soit la solution de sécurité qu'elles ont adoptée.

Un nouvel outil de lutte contre les ransomwares, gratuit et indépendant des solutions antivirus utilisées est disponible #KLReport

La solution Anti-Ransomware Tool for Business de Kaspersky Lab est une solution peu encombrante qui fonctionne en parallèle avec n'importe quel logiciel antivirus. Cet outil intègre deux composants indispensables à la détection anticipée des trojans : le Kaspersky Security Network distribué et System Watcher, qui surveille l'activité des applications.

Kaspersky Security Network vérifie rapidement la réputation des fichiers et des adresses Internet dans le cloud tandis que System Watcher surveille le comportement des applications et offre une protection proactive contre les versions inconnues des trojans. Mais ce qui distingue réellement cet outil, c'est sa capacité à réaliser des copies de sauvegarde des fichiers ouverts par des applications suspectes et à venir à l'état antérieur aux modifications s'il s'avère que ces actions étaient malveillantes.

Par le biais de la coopération : l'initiative No More Ransom

No More Ransom a aidé à ce jour 4 400 personnes à récupérer leurs données et a privé les criminels de plus d'un million et demi de dollars en rançon #KLReport

Le 25 juillet 2016, la police des Pays-Bas, Europol, Intel Security et Kaspersky Lab lançaient le projet No More Ransom, une initiative sans fin commerciale qui réunit des organisations publiques et privées et dont l'objectif est double : informer le public sur les dangers du ransomware et aider les victimes désireuses de récupérer leurs données.

Le portail en ligne propose à l'heure actuelle huit outils de déchiffrement, dont cinq développés par Kaspersky Lab. Ils permettent de récupérer les fichiers chiffrés par plus d'une vingtaine de types de malwares de chiffrement. A ce jour, plus de 4 400 victimes ont pu récupérer leurs données en économisant plus d'un million et demi de dollars de rançon.

Au mois d'octobre, les autorités policières et judiciaires de 13 autres pays ont rejoint le projet : Bosnie-Herzégovine, Bulgarie, Colombie, France, Hongrie, Irlande, Italie, Lettonie, Lituanie, Portugal, Espagne, Suisse et Royaume-Uni.

Eurojust et la Commission européenne soutiennent également les objectifs du projet tandis que l'intégration de nouveaux partenaires issus du secteur privé et des autorités judiciaires et policières devrait être prochainement annoncée.

"L'initiative NMR puisse sa force dans le partenariat entre le secteur public et le secteur privé. La coopération entre les deux est essentielle pour pouvoir lutter efficacement contre ce fléau. Ses capacités et sa portée sont bien supérieures à celles des seules autorités policières et judiciaires."

Steven Wilson, Directeur du service EC3 d'Europol

Faire face au ransomware - Comment se protéger

1. Réalisez des copies de sauvegarde à intervalles réguliers.
2. Adoptez une solution de sécurité fiable et veillez à ne jamais désactiver les fonctions essentielles comme System Watcher.
3. Maintenez le logiciel à jour sur tous vos périphériques.
4. Soyez particulièrement prudents avec les pièces jointes et les messages envoyés par des inconnus. Dans le doute, évitez de les ouvrir.
5. Si vous dirigez une entreprise, pensez à sensibiliser vos employés et votre personnel informatique ; conservez les données sensibles à part ; limitez les accès et réalisez des copies de sauvegarde de tout, tout le temps.
6. Si vous deviez malgré tout être victime d'un malware de chiffrement, ne cédez pas à la panique. Au départ d'un système sain, consultez le site de No More Ransom ; vous y trouverez peut-être l'outil de déchiffrement qui vous aidera à récupérer vos fichiers.
7. Enfin, n'oubliez pas que l'attaque par ransomware est un délit. Signalez-la à la police.

Raisons pour lesquels il ne faut pas payer la rançon – Conseils de la brigade nationale de lutte contre les délits technologique des Pays-Bas

1. Vous devenez une cible encore plus intéressante.
2. Vous ne pouvez pas faire confiance aux criminels. Vous pourriez très bien ne jamais revoir vos données, même si vous payez.
3. Lors de la prochaine attaque, la rançon à payer sera plus importante.
4. Vous encouragez les criminels.

"Nous encourageons les membres du public à signaler les attaques. Chaque victime détient un élément de preuve essentiel qui permet de mieux comprendre le phénomène. De notre côté, nous pouvons les maintenir informés et les protéger de ces offres de déchiffrement « douteuses » formulées par des tiers. Mais nous devons veiller à ce que plus de représentants des autorités judiciaires et policières sachent comment traiter la criminalité numérique".

Ton Maas, Coordonnateur de l'équipe numérique de la brigade nationale de lutte contre les délits technologique des Pays-Bas

PEUT-ON ESPÉRER REMPORTER LA LUTTE CONTRE LE RANSOMWARE ?

Nous pensons que cela est possible, à condition d'unir nos efforts. Le ransomware est une activité criminelle lucrative. Pour y mettre un terme, le monde doit s'unir pour perturber la chaîne d'exécution des criminels et compliquer au maximum l'organisation d'une attaque et l'utilisation des profits engrangés.

Securelist

Retrouvez ici les recherches et analyses de nos experts en sécurité informatique, sur les virus, les hackers, les spams...

Notre site web

Nota Bene – Le blog d'Eugène Kaspersky

Kaspersky Daily — Infos, Trucs et astuces pour les utilisateurs

Kaspersky Business Blog – Des infos pertinentes sur la sécurité informatique

Threatpost – Le site numéro 1 pour des infos exclusives sur la sécurité informatique

Kaspersky Academy