GUIDE DU RANSOMWARE 2018

Qu'est-ce qu'une attaque par ransomware ?

Ransomware a grandi pour être l'un des plus gros problèmes sur le web. C'est une forme de logiciel malveillant qui crypte des documents sur un PC ou même sur un réseau. Les victimes ne peuvent retrouver l'accès à leurs fichiers et PC cryptés qu'en payant une rançon aux hackers derrière le ransomware.

Le web est devenu le principal vecteur de propagation des attaques de ransomwares via les sites frauduleux qui exploitent les failles de sécurité des machines vulnérables non protégées.

Une infection ransomware peut commencer aussi par quelqu'un qui clique sur ce qui ressemble à une pièce jointe innocente, et cela peut être un casse-tête pour les entreprises de toutes tailles si les fichiers et documents vitaux (pensez feuilles de calcul et factures) sont soudainement cryptés et inaccessibles.

Les cybercriminels n'avaient pas l'habitude d'être si évidents. Si les pirates infiltraient votre réseau d'entreprise, ils feraient tout leur possible pour éviter la détection. Il était dans leur intérêt de ne pas alerter une victime qu'elle avait été victime d'un cybercriminel.

Mais maintenant, si vous êtes attaqué avec un ransomware de chiffrement de fichiers, les criminels vont annoncer effrontément qu'ils tiennent vos données d'entreprise en otage jusqu'à ce que vous payiez une rançon pour le récupérer.

Cela peut sembler trop simple, mais cela fonctionne: les cybercriminels ont empoché plus d'un milliard de dollars d'attaques de rançongiciels au cours de la seule année 2016 et un rapport d'Europol le décrit comme ayant «éclipsé» la plupart des autres menaces cybercriminelles mondiales en 2017 et en 2018.

Quelle est l'histoire de ransomware?

Alors que les ransomwares ont explosé l'an dernier , augmentant d'environ 748%, ce n'est pas un phénomène nouveau: le premier exemple de ce que nous appelons maintenant ransomware est apparu en 1989.

Connu sous le nom de SIDA ou PC Cyborg Trojan, le virus a été envoyé aux victimes - principalement dans l'industrie des soins de santé - sur une disquette. Le rançongiciel comptait le nombre de fois que le PC était démarré: une fois qu'il atteignait 90, il chiffrait la machine et les fichiers et demandait à l'utilisateur de 'renouveler sa licence' avec 'PC Cyborg Corporation' en envoyant 189 $ ou 378 $ à un bureau de poste boîte au Panama.

Comment le ransomware a-t-il évolué?

Ce rançongiciel précoce était une construction relativement simple, utilisant une cryptographie de base qui, pour la plupart, changeait juste le nom des fichiers, le rendant relativement facile à surmonter.

Mais cela a déclenché une nouvelle branche de la criminalité informatique, qui a lentement mais sûrement pris de l'ampleur - et a vraiment décollé à l'ère d'Internet. Avant de commencer à

utiliser la cryptographie avancée pour cibler les réseaux d'entreprise , les pirates ciblaient les utilisateurs d'Internet généraux avec des rançongiciels de base.

L'une des variantes les plus réussies était le «rançongiciel policier», qui tentait d'extorquer des victimes en prétendant être associé à l'application de la loi. Il a verrouillé l'écran avec une note de rançon avertissant l'utilisateur qu'ils avaient commis une activité illégale en ligne, ce qui pourrait les faire envoyer en prison.

Cependant, si la victime payait une amende, la «police» laisserait glisser l'infraction et rétablir l'accès à l'ordinateur en remettant la clé de déchiffrement. Bien sûr, cela n'avait rien à voir avec l'application de la loi - c'était des criminels qui exploitaient des innocents.

Un exemple de «police ransomware» menaçant un utilisateur britannique.

Image: Sophos

Malgré un certain succès, ces formes de rançongiciel ont souvent simplement superposé leur message d'avertissement sur l'affichage de l'utilisateur - et le redémarrage de la machine a permis de résoudre le problème et de restaurer l'accès aux fichiers qui n'ont jamais été cryptés.

Les criminels ont appris de cela et maintenant la majorité des systèmes de ransomware utilisent la cryptographie avancée pour verrouiller un PC infecté et les fichiers qui s'y trouvent.

Quels sont les principaux types de ransomware?

Ransomware est en constante évolution, avec de nouvelles variantes apparaissant continuellement dans la nature et de nouvelles menaces pour les entreprises. Cependant, il existe certains types de rançongiciels qui ont eu beaucoup plus de succès que d'autres.

Peut-être la forme la plus notoire de ransomware est Locky , qui a terrorisé les organisations à travers le monde tout au long de 2016. Il infâme fait les manchettes en infectant un hôpital d'Hollywood . L'hôpital a donné suite aux demandes des cybercriminels et versé une rançon de 17 000 $ pour la restauration de ses réseaux.

Locky est resté réussi parce que ceux qui sont derrière le mettre à jour régulièrement le code pour éviter la détection. Ils le mettent même à jour avec de nouvelles fonctionnalités, y compris la possibilité de faire des demandes de rançon dans 30 langues, afin que les criminels puissent plus facilement cibler les victimes partout dans le monde. Locky est devenu un tel succès, il est devenu la forme la plus répandue de logiciels malveillants à part entière .

Bien qu'il ne soit pas aussi prolifique que par le passé, Locky reste l'une des formes les plus dangereuses de rançongiciels, se taisant régulièrement avant de réapparaître avec de nouvelles techniques d'attaque .

Cryptowall est une autre forme de ransomware qui a connu un grand succès pendant une période prolongée. Commençant la vie en tant que doppelganger de Cryptolocker, il est devenu l'un des types de ransomware les plus réussis.

Comme Locky, Cryptowall a été régulièrement mis à jour afin d'assurer son succès continu et même brouiller les noms de fichiers pour rendre plus difficile pour les victimes de savoir quel fichier est, ce qui met la pression supplémentaire sur la victime à payer.

Alors que certains développeurs de ransomware - comme ceux derrière Locky ou Cryptowall - gardent leur produit de près, le gardant uniquement pour leur propre usage, d'autres distribuent joyeusement ransomware à n'importe quel hacker désireux de profiter de la cyber-extorsion - et il est prouvé une méthode très réussie pour une large diffusion.

L'une des formes les plus communes de rançongiciels distribués de cette manière est Cerber, qui a infecté des centaines de milliers d'utilisateurs en un seul mois. Les créateurs originaux de Cerber le vendent sur le Dark Web , permettant à d'autres criminels d'utiliser le code en échange de 40% de chaque rançon payée.

Cerber ransomware a connu un tel succès qu'il a dépassé Locky - qui semblait disparaître mystérieusement à Noël, mais réapparu en avril avec de nouvelles techniques d'attaque - pour devenir la forme la plus dominante de ransomware sur le web, représentant 90% des attaques ransomware sur Windows. à la mi-avril 2017 .

Cette famille de rançongiciels est en constante évolution, avec ses développeurs ajoutant régulièrement de nouvelles fonctionnalités pour assurer son succès continu. En effet, la cryptographie derrière Cerber est si avancée qu'il n'y a actuellement aucun outil de décryptage disponible pour aider les personnes infectées par les dernières versions.

Mais ne se contente pas de gagner de l'argent illicitement grâce aux paiements de rançon, Cerber a maintenant la possibilité de voler pour voler des informations sur le portefeuille et le mot de passe Bitcoin , en plus de crypter des fichiers.

En échange d'abandonner une partie des bénéfices pour l'utilisation de Cerber, les cyber-fraudeurs potentiels reçoivent tout ce dont ils ont besoin pour gagner de l'argent grâce à l'extorsion de victimes.

En effet, certains groupes criminels offrent maintenant ce type de système de ransomware-as-a-service aux utilisateurs potentiels sans frais au point d'entrée. Au lieu de facturer des frais pour le code ransomware, ils veulent une réduction de 50 pour cent des paiements de rançon.

Une autre forme de ransomware réussie est SamSam , qui est connu pour charger une rançon de dizaines de milliers de dollars pour la clé de décryptage.

Plutôt que d'être distribués via des courriels d'hameçonnage, les pirates recherchent des systèmes Internet non sécurisés, puis les exploitent pour aider à propager SamSam latéralement à travers les réseaux .

Qu'est-ce que WannaCry ransomware?

WannaCry - également connu sous le nom de WannaCrypt et Wcry - a causé le chaos à travers le monde lors d'une attaque qui a débuté le vendredi 12 mai 2017.

WannaCrypt ransomware demande 300 $ en bitcoin pour débloquer des fichiers cryptés - un prix qui double après trois jours. Les utilisateurs sont également menacés, via une note de rançon sur l'écran, d'avoir tous leurs fichiers définitivement supprimés si la rançon n'est pas payée dans une semaine.

WannaCry ransomware a infecté les systèmes Windows XP à travers le monde.

Image: Cisco Talos
Plus de 300 000 victimes dans plus de 150 pays ont été victimes des rançongiciels au cours d'une fin de semaine, les entreprises, les gouvernements et les particuliers du monde entier étant tous touchés.

Les organisations de soins de santé à travers le Royaume-Uni ont eu des systèmes déconnectés par l'attaque ransomware, forçant les rendez-vous des patients à être annulés et les hôpitaux à éviter les services d'urgence et d'urgence sauf si c'était nécessaire.

De tous les pays touchés par l'attentat, la Russie a été la plus durement touchée, selon les chercheurs en sécurité, avec le malware WannaCry qui écrase les banques russes, les opérateurs téléphoniques et même les systèmes informatiques supportant l'infrastructure de transport. La Chine a également été durement touchée par l'attaque, 29 000 organisations ayant été victimes de cette forme de rançongiciel particulièrement vicieuse.

Parmi les autres objectifs importants, citons le constructeur automobile Renault qui a été contraint de stopper les lignes de production dans plusieurs endroits alors que le ransomware faisait des ravages dans les systèmes.

Ce que toutes les cibles avaient en commun, c'est qu'elles exécutaient des versions non prises en charge de Microsoft Windows, y compris Windows XP, Windows 8 et Windows Server 2003.

Le ver ransomware est si puissant car il exploite une vulnérabilité logicielle connue appelée EternalBlue. La faille de Windows est l'un des nombreux jours-zéro qui étaient apparemment connus par la NSA - avant d'être divulgué par le collectif de hackers Shadow Brokers . Microsoft a publié un correctif pour la vulnérabilité plus tôt cette année - mais seulement pour les systèmes d'exploitation les plus récents.

En réponse à l'attaque, Microsoft a pris l'initiative sans précédent d'émettre des correctifs pour les systèmes d'exploitation non pris en charge afin de se protéger contre les logiciels malveillants.

Les services de sécurité aux Etats-Unis et au Royaume-Uni ont depuis lors désigné la Corée du Nord comme étant l'auteur de l'attaque ransomware WannaCry , la Maison Blanche déclarant officiellement Pyongyang comme la source de l'épidémie dans un rapport publié en décembre .

Cependant, la Corée du Nord a qualifié les accusations selon lesquelles elle était «absurde» derrière WannaCry .

Peu importe qui était finalement derrière WannaCry, si l'objectif du plan était de faire de grandes quantités d'argent, il a échoué - seulement environ 100 000 $ a été payé.

Il a fallu près de trois mois avant que les attaquants de WannaCry retirent finalement les fonds des portefeuilles bitcoin WannaCry - ils ont fait un total de 140 000 $ grâce aux fluctuations de la valeur de bitcoin.

Mais malgré la mise à disposition de correctifs critiques pour protéger les systèmes contre WannaCry et d'autres attaques exploitant la vulnérabilité SMB, un grand nombre d'organisations ont apparemment choisi de ne pas appliquer les mises à jour. On pense que c'est la raison pour laquelle LG a subi une infection WannaCry en août - trois mois après l'éclosion initiale. La société a depuis lors déclaré avoir appliqué les correctifs appropriés.

La décharge publique de l'exploit EternalBlue derrière WannaCry a conduit à divers groupes de piratage tentant de tirer parti de cela pour stimuler leur propre malware .

Les chercheurs ont même documenté comment une campagne ciblant les hôtels européens par l'APT28 - un groupe de piratage russe lié à l' ingérence dans l'élection présidentielle américaine - utilise maintenant la faille de la NSA.

Qu'est-ce que Petya / NotPetya / GoldenEye?

Un peu plus d'un mois après l'épidémie de ransomware WannaCry, le monde a été frappé par une autre attaque ransomware mondiale .

Cette cyberattaque a d'abord touché des cibles en Ukraine, notamment sa banque centrale, son principal aéroport international et même l'installation nucléaire de Tchernobyl, avant de s'étendre rapidement dans le monde entier, infectant des organisations européennes, russes, américaines et australiennes .

Après une première confusion quant à la nature de ce malware - certains ont dit que c'était Petya, d'autres ont dit qu'il s'agissait d'autre chose - les chercheurs de Bitdefender ont conclu que l'épidémie était une version modifiée de Petya ransomware, combinant des éléments de

GoldenEye - un parent particulièrement vicieux de Petya - et WannaCry ransomware en malware extrêmement puissant.

Cette deuxième forme de rançongiciel exploite également le même exploit Windows EternalBlue qui a fourni à WannaCry les fonctionnalités de type ver pour se propager sur les réseaux (pas simplement par le biais d'une pièce jointe comme souvent) et atteindre 300 000 ordinateurs dans le monde.

Cependant, Petya / NotPetya / GoldenEye est une attaque beaucoup plus vicieuse. Non seulement l'attaque crypte les fichiers des victimes, mais elle crypte également les disques durs entiers en écrasant l'enregistrement de redémarrage principal , empêchant l'ordinateur de charger le système d'exploitation ou de faire quoi que ce soit.

Les pirates demandent une rançon bitcoin de 300 $ à envoyer à une adresse e-mail spécifique - qui a maintenant été fermée par l'hôte du service de messagerie. Cependant, la façon dont ce ransomware très sophistiqué était apparemment équipé de fonctions non-automatisées très basiques pour accepter des rançons a conduit certains à suggérer que l'argent n'est pas l'objectif.

Certains ont même spéculé que la note de ransomware était juste une couverture pour le but réel du virus - pour causer le chaos par effacement irrémédiable des données des machines infectées.

Quel que soit le but de l'attaque, cela a eu un impact important sur les finances des organisations qui ont été infectées. L'entreprise britannique de biens de consommation Reckitt Benckiser a déclaré avoir perdu 100 millions de livres de recettes à la suite de sa disparition de Petya .

Mais c'est une perte relativement modeste par rapport aux autres victimes de l'attaque: l' opérateur de navires de transport et de livraison Maersk et la compagnie de livraison de marchandises FedEx ont tous les deux estimé des pertes de 300 millions de dollars en raison de l'impact de Petya.

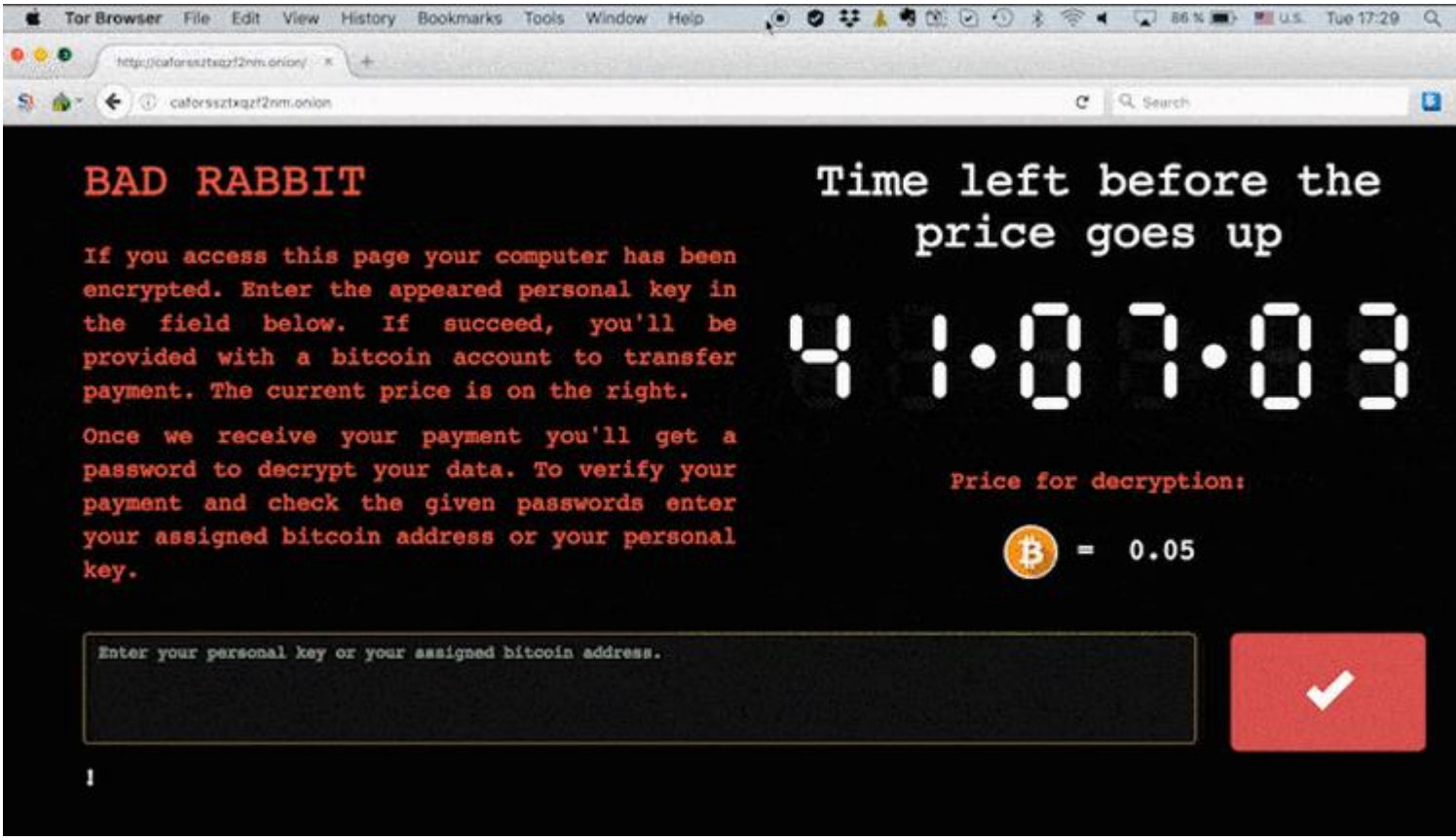
En février 2018, les gouvernements du Royaume-Uni , des États-Unis , d' Australie et d'autres ont officiellement déclaré que le rançongiciel NotPetya avait été l'œuvre de l'armée russe. Le Russe nie toute implication.

Qu'est-ce que Bad Rabbit ransomware?

Octobre 2017 a vu la troisième attaque de ransomware de l'année où des organisations en Russie et en Ukraine ont été victimes d'une nouvelle variante de Petya ransomware.

Surnommé Bad Rabbit , il a infecté au moins trois organisations de médias russes tout en infiltrant les réseaux de plusieurs organisations ukrainiennes, dont le métro de Kiev et l'aéroport international d'Odessa - l'aéroport a alors été victime d'une attaque de hackers.

Le vecteur d'attaque initial utilisé pour distribuer Bad Rabbit consistait à télécharger des fichiers sur des sites Web piratés, dont certains avaient été piratés depuis juin . Aucun exploit n'a été utilisé, plutôt les visiteurs ont été informés qu'ils devaient installer une mise à jour Flash, qui a fait tomber le malware.



Note de rançon Bad Rabbit

Image: Kaspersky Lab
Comme NotPetya auparavant, Bad Rabbit s'est propagé à travers les réseaux à l'aide d'un outil de piratage de la NSA , mais cette fois, c'était via la vulnérabilité EternalRomance SMB, plutôt que l'exploit EternalBlue.

L'analyse de Bad Rabbit a partagé une grande partie de son code - au moins 67% - avec Peyta et les chercheurs de Cisco Talos ont conclu que cela, combiné avec l'utilisation des exploits SMB, signifie qu'il y a une grande confiance dans un lien entre les deux formes de ransomware. et qu'ils pourraient même partager le même auteur.

Bad Rabbit a été nommé d'après le texte qui apparaissait en haut du site Web de Tor hébergeant la note de rançon. Certains chercheurs en sécurité ont plaisanté sur le fait qu'il aurait dû être nommé d'après les lignes du code référençant les personnages de Game of Thrones.

Combien coûte une attaque de ransomware?

Évidemment, le coût le plus immédiat associé à l'infection par ransomware - si elle est payée - est la demande de rançon, qui peut dépendre du type de ransomware ou de la taille de votre organisation.

Des recherches récentes ont révélé qu'un quart des entreprises qui ont payé une rançon ont payé plus de 5 000 £ pour récupérer leurs données cryptées, tandis qu'un autre quart a payé des hackers entre 3 000 et 5 000 £.

La rançon la plus répandue parmi les petites et moyennes entreprises se situait entre 500 et 1500 livres sterling, ce qui prouve qu'il est encore facile de gagner de l'argent en ciblant des organisations de cette taille .

Il existe également des exemples de cibles de haut niveau payant des frais à cinq chiffres pour retrouver l'accès à leurs réseaux cryptés et à leurs fichiers, en particulier dans les cas où les criminels menacent de supprimer des données s'ils ne sont pas payés.

En fin de compte, quelle que soit la taille de l'entreprise, le temps c'est de l'argent, et plus votre réseau est en panne à cause de logiciels malveillants, plus cela va coûter cher à votre entreprise.

Même si vous récupérez l'accès à vos documents cryptés en payant une rançon, il y aura des coûts supplémentaires en plus. Afin d'éviter de futures attaques - surtout si vous avez été marqué comme une cible facile - soyez prêt à investir dans un logiciel de cybersécurité supplémentaire et à payer pour une formation supplémentaire du personnel.

Il y a aussi le risque que les clients perdent confiance dans votre entreprise en raison de la faible cybersécurité et de la prise de leur coutume ailleurs.

Pourquoi les entreprises devraient-elles s'inquiéter des rançongiciels?

Pour le dire simplement: ransomware pourrait ruiner votre entreprise. Le fait d'être exclu de vos propres fichiers par un logiciel malveillant, même pour une journée, aura un impact sur vos revenus. Mais étant donné que ransomware prend la plupart des victimes hors ligne pendant au moins une semaine , voire des mois, les pertes peuvent être importantes. Les systèmes sont hors ligne depuis longtemps, non seulement parce que le ransomware verrouille le système, mais aussi à cause de tous les efforts requis pour nettoyer et restaurer les réseaux.

Et ce n'est pas seulement le coup financier immédiat de ransomware qui va endommager une entreprise; les consommateurs hésitent à donner leurs données à des organisations qu'ils considèrent comme peu sûres.

Comment ransomware infecte votre PC?

C'est la dépendance de l'entreprise moderne sur Internet qui permet aux rançongiciels de prospérer. Chaque jour, chaque employé reçoit des centaines de courriels et de nombreux rôles exigent que ces employés téléchargent et ouvrent des pièces jointes, c'est donc quelque chose qui est souvent fait sur le pilote automatique. Profiter de la volonté desemployés d'ouvrir des pièces jointes provenant d'expéditeurs inconnus permet aux cybercriminels de mener avec succès des campagnes de ransomware.

Comme d'autres formes de logiciels malveillants, les botnets envoient en masse des ransomwares, avec des millions de courriels d'hameçonnage malveillants envoyés chaque seconde. Les cybercriminels utilisent une variété de leurres pour encourager les cibles à ouvrir un email ransomware, allant des offres de bonus financiers , faux reçus d'achat en ligne , demandes d'emploi d'employés potentiels , et plus encore.