Phishing et ransomwares : Prolifération accélérée
Sécurité
Posté par : JPilo
Publiée le : 7/11/2017 13:30:00

Les attaques de phishing et de ransomwares et leurs variantes (telles que le harponnage (spear phishing) et l'arnaque au président (Business Email Compromise) sont de plus en plus courantes et ont des effets dévastateurs sur les entreprises de toutes tailles.

L'impact financier réel de la cybercriminalité en général, et du phishing et des ransomwares en particulier, est difficile à évaluer, mais le FBI aux Etats Unis estime que les ransomwares ont coûtés à eux seuls aux organisations 209 millions de $ au cours des trois premiers mois de 2016.

La situation ne s'est pas améliorée depuis, bien au contraire. Le phishing et les crypto-ransomwares augmentent aujourd'hui au rythme de plusieurs centaines de pour cent par trimestre, et cette tendance, d'après le cabinet d'études Osterman Research, devrait se poursuivre pendant au moins les 18 à 24 prochains mois.

En mai 2017 par exemple, l'attaque du ransomware Wannacry a infecté plus de 300.000 ordinateurs dans 150 pays, y compris le système de santé national (NHS) au Royaume Uni.

Mais qu'est ce qui rend le phishing et les ransomwares aussi efficaces ?

Le succès des tentatives d'hameçonnage et d'infiltration par des ransomwares dépend d'un certain nombre de facteurs, notamment :

** la naïveté ou le manque de méfiance des victimes lorsqu'elles reçoivent des e-mails où font face à d'autres pièges tendus par des cybercriminels,

** la quantité et la qualité de la formation qu'elles ont suivie, la qualité de l'infrastructure de sécurité de leur organisation et la quantité d'informations qu'elles peuvent rassembler pour lutter contre les attaques potentielles.

Cependant, certains facteurs font que le phishing et les ransomwares sont aujourd'hui particulièrement efficaces :

De nombreuses attaques utilisent les e-mails, et les liens et pièces jointes qu'ils contiennent, comme principale méthode d'infiltration. Beaucoup d'utilisateurs sont en « surdose d'informations » en ce qui concerne leurs e-mails, ce qui fait qu'ils sont moins susceptibles de vérifier prudemment les tentatives d'hameçonnage, d'arnaque au président ou arnaque BEC ou toute autre tentative.

Une enquête d'Osterman Research réalisée en juillet 2016 à l'initiative de Barracuda Networks auprès d'utilisateurs finaux en entreprise a révélé que 94 % des utilisateurs éprouvent un certain niveau d'overdose d'informations par e-mail, et 32 % indiquent qu'ils en souffrent « considérablement. »

Les cybercriminels créent du contenu de plus en plus pertinent afin de tromper les utilisateurs et de contourner les technologies de détection. L'utilisation de logos, le ton professionnel des messages ainsi que la personnalisation du contenu rendent les tentatives d'hameçonnage plus convaincantes. Ainsi, les victimes potentielles sont plus susceptibles de cliquer sur les liens et les pièces jointes contenus dans les e-mails.

L'amélioration des méthodes des cybercriminels s'explique notamment par le fait qu'ils ont tendance à travailler pour des organisations criminelles très bien financées, qui disposent des ressources financières et techniques nécessaires pour améliorer leurs techniques.

Les cybercriminels mettent au point de nouvelles formes de ransomwares plus efficaces, ainsi que des méthodes améliorées de communication avec les systèmes infectés. En partant des ransomwares plus classiques de verrouillage de données qui constituaient la norme il y a quelques années, des variantes basées sur le chiffrement ont émergé, comme CryptoWall (2014), CTB-Locker (2014), TeslaCrypt (2015), Samas (2016), Locky (2016) et Zepto (2016). De plus, le ransomware as a service devient plus courant ; par exemple, le service Cerber a infecté 150 000 terminaux en juillet 2016 et engrangé des bénéfices de près de 200 000 $ par mois.

De nombreux utilisateurs partagent trop d'informations sur les réseaux sociaux, et donnent ainsi des renseignements que les cybercriminels peuvent utiliser pour créer des emails personnalisés et plus crédibles, donc plus difficiles à détecter.

Certaines solutions anti-hameçonnage et anti-ransomwares ne s'appuient pas sur des ressources d'intelligence en temps réel suffisantes sur les attaques par email, et ne peuvent donc pas détecter les dernières techniques utilisées par les spécialistes du phishing et des ransomwares.

De nombreux utilisateurs ne sont pas suffisamment formés sur le phishing et les ransomwares, ainsi que sur les meilleures pratiques de gestion des menaces non connues. En fait, beaucoup d'entre eux ne font pas preuve de suffisamment de vigilance lorsqu'ils reçoivent des messages les incitant à effectuer des actions telles que virer des fonds, ouvrir des pièces jointes ou transmettre des informations sensibles.

Des exploit kits, comme ceux utilisés pour infecter des victimes avec des ransomwares, ne nécessitent que des connaissances limitées de la part des cybercriminels. Ces kits, qui exploitent les vulnérabilités d'une large gamme de logiciels disponibles sur le marché, intègrent des logiciels

malveillants clés en mains, disponibles soit à la vente soit en location. S'il peut être coûteux d'acheter directement ces exploit kits, ils peuvent être loués pour seulement 500 $ par mois.

En outre, les techniques employées par les ransomwares se sont considérablement sophistiquées au fil du temps, et les victimes n'ont généralement qu'un court laps de temps pour les déjouer.

Il faut ajouter à cela le fait que les spécialistes en hameçonnage et en ransomwares ne cessent de se perfectionner dans le vol de données financières ou autres. Par exemple :

Certaines menaces peuvent rester inactives sur une période prolongée et sont moins susceptibles d'être détectées par de nombreuses solutions habituelles anti-hameçonnage et anti-ransomwares.

Certains types de logiciels malveillants peuvent détecter s'ils ont été placés dans un 'sandbox' (bac à sable) et ils ne s'exécuteront qu'une fois qu'ils n'y seront plus.

Certains cybercriminels coordonnent leurs attaques sur plusieurs lieux de diffusion notamment les emails, les réseaux sociaux, les navigateurs Web, les fichiers, etc.

Un logiciel malveillant peut en diriger un autre qui semble inoffensif.

Certains logiciels malveillants nécessitent une interaction avec l'utilisateur (par exemple, cliquer sur un bouton d'une boîte de dialogue) avant de s'activer et détectera si l'utilisateur clique sur le bouton dans un 'sandbox'.

Quelles sont les tendances à venir ?

Comme l'avait prévu l'étude d'Osterman Research en 2016, les attaques d'hameçonnage et de ransomwares ont continué d'augmenter en 2017, et continueront de le faire en 2018, de même que le nombre de familles et variantes de ransomwares diffusées.

Une part toujours croissante des tentatives d'hameçonnage visera à installer des ransomwares sur les ordinateurs infectés. Déjà en 2016, un spécialiste de la sécurité avait déterminé que 93 % des e-mails d'hameçonnage visaient à diffuser des ransomwares.

Si le problème général des courriers indésirables est en déclin depuis plusieurs années, les courriers indésirables constitueront toujours un moyen efficace de diffuser de logiciels malveillants, dont des ransomwares, au moins en tant que canal secondaire.

Étant donné la facilité avec laquelle les cybercriminels non-initiés peuvent pénétrer le marché, l'écosystème des ransomwares va progressivement se scinder en deux segments distincts. D'un côté les ransomwares d'entrée de gamme, qui demandent une rançon de quelques centaines de dollars et sont envoyés par des amateurs et d'autres criminels de faible envergure en utilisant des techniques classiques d'hameçonnage.

Et de l'autre, les ransomwares « haut de gamme, » envoyés par des cybercriminels plus sophistiqués et qui visent des cibles à fort potentiel dans des secteurs tels que la santé, les services financiers ou les assurances, capables de payer des sommes importantes pour récupérer leurs données chiffrées.

Le phishing et plus particulièrement les ransomwares ne cibleront plus à terme que les entreprises, délaissant les particuliers, moins rémunérateurs.

Eric Heddeland - Regional Sales Director, EMEA Southern Region