Proposé par

Se défendre contre les ransomwares

for dummies
A Wiley Brand

Une édition spéciale de Cisco

- Identifiez les caractéristiques des ransomwares
- Prévenez les attaques de ransomwares
- Créez une nouvelle architecture de sécurité sophistiquée

Lawrence Miller, CISSP

À propos de Cisco

Cisco conçoit et vend des gammes de produits complètes, fournit des services et propose des solutions intégrées visant à développer et à connecter des réseaux dans le monde entier.

En tant que leader mondial de notre industrie, nous aidons nos clients à se connecter, à se digitaliser et à se développer. Ensemble, nous changeons la façon dont le monde travaille, vit, joue et apprend.

Depuis plus de 30 ans, nous aidons nos clients à bâtir des réseaux, et à automatiser, orchestrer, intégrer et numériser des produits et services informatiques.

Dans un monde de plus en plus connecté, Cisco ouvre la voie en transformant les entreprises, les gouvernements et les villes du monde entier en adoptant une approche innovatrice et différentiée.

La défense contre les ransomwares de Cisco
http://www.cisco.com/go/ranswomware

La solution de défense contre les ransomwares de Cisco exploite l'architecture de sécurité de Cisco pour protéger les réseaux des entreprises, de la couche DNS à la messagerie et aux terminaux. C'est la defense ultime contre les ransomwares qui est simple, automatique et efficace.

 https://twitter.com/CiscoSecurity

 https://www.facebook.com/CiscoSecurity

 https://www.linkedin.com/company/Cisco-Security

 https://www.youtube.com/Cisco

Se défendre contre les ransomwares

Une édition spéciale de Cisco

par Lawrence Miller, CISSP

for dummies®
A Wiley Brand

Se défendre contre les ransomwares pour les nuls®, une édition spéciale de Cisco

Publié par
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-37961-4 (pbk); ISBN 978-1-119-37952-2 (ebk)

Imprimé aux États-Unis d'Amérique

10 9 8 7 6 5 4 3 2 1

Pour obtenir des informations générales sur les autres produits et services, ou sur la publication d'un livre *Pour les Nuls* adapté à votre entreprise ou organisation, veuillez contacter notre service de développement commercial aux États-Unis par téléphone 877-409-4177, par courriel info@dummies.biz, ou par le biais du site www.wiley.com/go/custompub. Pour obtenir des informations sur la licence de la marque *Pour les Nuls* pour des produits ou services, veuillez contacter BrandedRights&Licenses@Wiley.com.

Remerciements de l'éditeur

Cet ouvrage a été réalisé avec la participation de certaines personnes dont les suivantes :

Éditeur du développement : Elizabeth Kuball

Rédacteur de copie : Elizabeth Kuball

Rédacteur chargé des acquisitions : Amy Fandrei

Rédacteur en chef : Rev Mengle

Représentant du développement commercial : Karen Hattan

Éditeur de la production : Siddique Shaik

Assistance spéciale : Rachel Ackerly, Mary Briggs, Dan Gould, Aivy Iniguez, Kate MacLean, Ben Munroe, Mark Murtagh

Table des matières

Introduction

Au cours des dernières années, le problème que représente les ransomwares a pris de l'ampleur en devenant une activité criminelle très lucrative. Les organisations victimes considèrent souvent le paiement de la rançon comme la méthode la plus économique pour récupérer leurs données. Malheureusement, si cela peut paraître vrai, il ne faut pas se leurrer : non seulement il n'y a aucune garantie de récupération des fichiers mais encore moins d'effacement du ransomware. De plus, chaque entreprise qui paye pour récupérer ses fichiers finance directement le développement de la prochaine génération de ransomwares. Par conséquent, le ransomware évolue à un rythme effrayant, avec de nouvelles variantes plus sophistiquées.

Il faut empêcher, si possible, l'intrusion des ransomwares, les détecter dès qu'ils tentent de s'infiltrer sur un réseau et les contenir pour limiter les dommages potentiels d'une infection des systèmes et des terminaux. La solution de défense contre les ransomwares exige une nouvelle approche architecturale sophistiquée qui couvre l'ensemble de l'organisation, depuis la couche DNS jusqu'au Data Center en passant par les terminaux, quel que soit l'endroit où ils sont utilisés.

À propos de cet ouvrage

Se défendre contre les ransomwares pour les nuls est composé de cinq chapitres courts qui examinent le fonctionnement du ransomware et ses caractéristiques fondamentales (chapitre 1), les bonnes pratiques pour réduire les risques liés aux ransomwares (chapitre 2), une nouvelle architecture de sécurité (chapitre 3), la solution de défense de Cisco contre les ransomwares (chapitre 4) et les conseils importants à retenir sur la défense contre les ransomwares (chapitre 5).

Hypothèses de départ

Partons de quelques hypothèses…

Supposons que vous possédez quelques connaissances sur la sécurité informatique. Vous êtes peut-être un cadre supérieur informatique, un directeur IT, un architecte réseau, un analyste ou un responsable, ou encore un administrateur de la sécurité, d'un réseau ou d'un système. Ce livre a été écrit principalement pour les techniciens qui ont une

certaine connaissance des réseaux, des infrastructures et des systèmes IT des entreprises.

Si l'une de ces hypothèses vous correspond, alors ce livre est pour vous ! Si aucune de ces hypothèses ne vous décrit, poursuivez quand même votre lecture. C'est un excellent livre. Lorsque vous l'aurez terminé, vous en saurez suffisamment sur la défense contre les ransomwares pour être dangereux (pour les méchants) !

Icônes employées dans cet ouvrage

J'utilise des icônes particulières tout au long de ce livre pour attirer l'attention du lecteur sur des informations importantes. Voici à quoi vous attendre :

RAPPEL

Cette icône signale des informations à inscrire obligatoirement dans votre mémoire non volatile, votre matière grise ou votre crâne, à côté des dates d'anniversaire !

TECHNIQUE

Vous n'allez pas trouver une carte du génome humain ici, mais si vous cherchez à atteindre le septième niveau du nirvana des nerds, vous allez être servi ! Cette icône explique le jargon qui se trouve derrière le jargon ; la véritable substance des légendes (ou des nerds en fait) !

ASTUCE

Merci de lire ce livre. J'espère que vous allez l'apprécier. Soyez gentil avec vos auteurs ! Sérieusement, cette icône signale des suggestions et des informations utiles.

AVERTISSEMENT

Cette icône attire votre attention sur ce contre quoi votre mère vous avait mis en garde. Ou peut-être pas. Mais vous devez quand même en tenir compte ; vous pourriez gagner du temps et vous éviter bien des frustrations !

Au-delà de cet ouvrage

Ce sujet est tellement vaste qu'il est impossible de tout couvrir en 48 pages. Donc, si à la fin du livre vous pensez : « Oh, ce livre était génial. Où pourrais-je en savoir plus ? », allez simplement sur `http://www.cisco.com/go/ransomware`.

DANS CE CHAPITRE

- Identifier le ransomware et ses caractéristiques fondamentales
- Rechercher les tendances dans le domaine des ransomwares
- Comprendre le fonctionnement du ransomware

Chapitre 1
Qu'est-ce qu'un ransomware ?

Aujourd'hui, le ransomware est le type de programme maveillant qui connaît la plus forte croissance ; il a déjà atteint le stade de l'épidémie. Selon un rapport interinstitutions du gouvernement des États-Unis, il y a eu plus de 4 000 attaques de ransomwares en moyenne par jour depuis janvier 2016. Dans ce chapitre, vous apprendrez ce qu'est un ransomware, quelle est son évolution en tant que menace et comment il fonctionne.

Définition du ransomware

Un *ransomware* (ou logiciel de rançon) est un programme malveillant utilisé lors d'une cyberattaque pour crypter les données de la victime à l'aide d'une clé cryptographique que seul l'attaquant connaît. Les données deviennent donc inutilisables jusqu'au paiement d'une rançon (en général, en *crypto-monnaie* comme le Bitcoin) par la victime.

TECHNIQUE

Une crypto-monnaie est une monnaie numérique alternative qui utilise un système de cryptage pour réguler « l'émission » des unités de monnaie (comme les bitcoins) et pour vérifier le transfert de fonds entre des parties, sans aucun intermédiaire ou banque centrale.

En général, les montants des rançons sont élevés, mais pas exorbitants. Pour les particuliers, les demandes vont souvent de 300 $ à 600 $, mais en général les entreprises doivent payer des montants plus importants. En 2016, un district scolaire de Caroline du Sud aux États-Unis a payé une rançon estimée à 10 000 $ et un hôpital californien a versé environ

17 000 $ à des cybercriminels. Ces montants s'ajoutent rapidement et ont dépassé, selon le FBI, la somme de 200 millions de dollars pour les trois premiers mois de l'année 2016. Cette caractéristique du ransomware est intentionnelle : pousser la victime à simplement payer la rançon au plus vite, au lieu de contacter la police et d'avoir éventuellement à supporter des coûts directs et indirects bien plus élevés en raison de la perte de leurs données et de la publicité négative.

AVERTISSEMENT

Par ailleurs, plus la victime attend, plus le montant de la rançon risque d'augmenter. C'est là encore intentionnel, afin de limiter les choix de la victime et de l'amener à payer la rançon le plus vite possible.

Identifier le ransomware dans le paysage moderne des menaces

Le ransomware n'est pas une menace nouvelle (voir la Figure 1-1). Le plus ancien ransomware a été lancé en 1989 sous le nom de PC Cyborg. Les ransomwares ont beaucoup évolué depuis cette date et sont bien plus sophistiqués qu'auparavant. Ils sont également plus généralisés et lucratifs, notamment en raison des développements suivants :

- **Le lancement du téléphone Android :** Android est devenu un vecteur d'attaque populaire (macOS est également ciblé aujourd'hui, et il ne fait aucun doute qu'Apple iOS deviendra une cible).
- **La progression du bitcoin :** grâce au bitcoin, il est facile de verser une rançon à des cybercriminels de façon pratiquement impossible à tracer.
- **L'émergence du ransomware en tant que service (RaaS) :** un *RaaS* (ransomware qui peut être acheté à bas prix et/ou en échange d'un pourcentage de la rançon) permet à presque tout le monde d'utiliser un ransomware.

En dépit des gros titres sur des vols massifs de données dans des organisations et des entreprises telles que l'Office of Personnel Management (OPM) des États-Unis, Anthem Blue Cross Blue Shield, Target et Home Depot, dans le but d'effectuer des usurpations d'identité et des fraudes à la carte de crédit, le ransomware, de par sa progression, est devenu l'une des menaces les plus généralisées pour les organisations et les entreprises (ainsi que les particuliers) au cours de l'année passée.

AVERTISSEMENT

Selon un rapport de l'ICIT (Institute for Critical Infrastructure Technology), 2018 sera l'année où le ransomware « fera des ravages au sein de la communauté des infrastructures critiques aux Etats-Unis. »

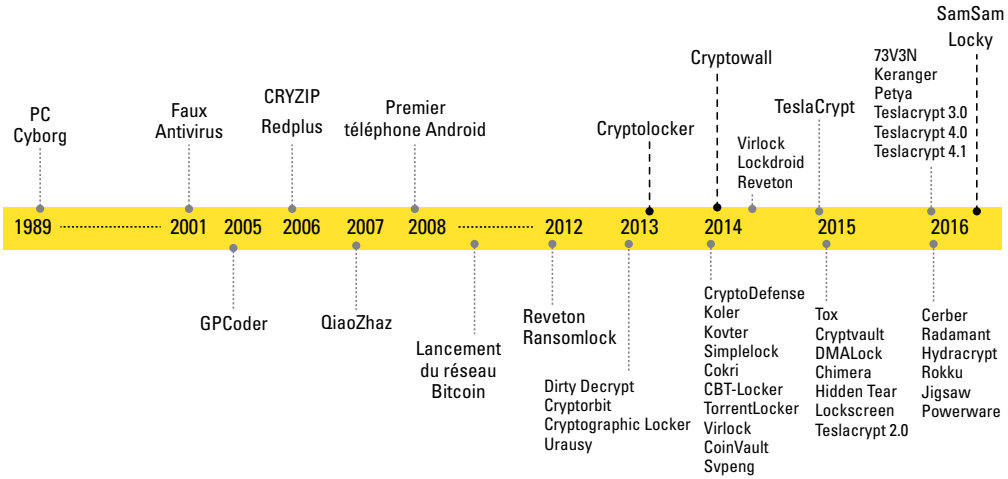


FIGURE 1-1: L'évolution du ransomware.

Ainsi, Locky est une variante agressive de ransomware qui attaque jusqu'à 90 000 victimes par jour. La rançon moyenne pour Locky tourne autour de 0,5 à 1 bitcoin. D'après les statistiques du groupe de renseignements de sécurité et de recherche Cisco Talos, en moyenne 2,9 % des victimes attaquées par un ransomware payent la rançon. Par conséquent, comme Locky pourrait potentiellement infecter 33 millions de victimes en 12 mois, cela correspond à un paiement total de rançons de 287 à 574 millions de dollars (voir le Tableau 1-1).

TABLEAU 1-1 Estimation du montant total des rançons payées pour Locky

Prix de la rançon	1 bitcoin	0,5 bitcoin
Victimes/jour	90 000	90 000
Nombre de paiements/jour	2 610	2 610
Valeur actuelle du bitcoin (au 2 octobre 2016)	610,82 $ = 1 bitcoin	610,82 $ = 1 bitcoin
Bénéfices en 1 jour	1 594 240 $	797 120 $
Bénéfices en 1 mois	47 826 206 $	23 913 603 $
Bénéfices en 12 mois	573 926 472 $	286 963 236 $

Bien qu'une estimation conservatrice de 287 millions de dollars puisse sembler insignifiante par rapport à une seule fuite de données (comme dans le cas de Target, dont le coût estimé est supérieur à 300 millions de dollars), il ne faut surtout pas oublier que les estimations de pertes de données reposent sur les coûts supportés par l'organisation ciblée, et non par les victimes individuelles dont les identités et/ou informations de carte de crédit sont volées. Les coûts supportés par l'organisation comprennent :

- **Les amendes et sanctions réglementaires** imposées par différents organismes, comme Payment Card Industry (PCI)
- **Les frais juridiques** associés au règlement du litige qui découle de la faille
- **Les pertes d'activités** en raison des interruptions d'exploitation, de l'atteinte à la réputation de la marque et de la perte de clients
- **Les remises en état** avec la résolution de l'incident et la reprise des activités, les relations publiques, la notification de faille et les services de contrôle du crédit pour les particuliers affectés

ASTUCE

Selon le Ponemon Institute, le coût moyen d'une faille atteint environ 6,5 millions de dollars pour les organisations ciblées.

En général, les cybercriminels vendent les informations volées sur les cartes de crédit et les identités sur le *dark web* (un contenu Internet anonyme couvrant notamment des services tels que la vente de médicaments sur le marché noir, la pornographie infantile, le cybercrime ou d'autres activités visant à éviter la surveillance ou la censure, et qui exige un logiciel d'accès spécial, une configuration et/ou une autorisation d'accès particulière) pour quelques centimes ou quelques dollars par enregistrement. Selon l'étude 2015 sur le coût du cybercrime du Ponemon Institute, le prix de vente moyen des données provenant d'une carte de crédit volée aux États-Unis se situe entre 0,25 et 60 $. En comparaison, un cybercriminel peut gagner plusieurs centaines à plusieurs dizaines de milliers de dollars en rançons, qui lui sont payées directement par les particuliers et les organisations.

Selon le rapport *2016 Identity Fraud Study* de Javelin Strategy and Research, le coût réel pour les victimes d'usurpation d'identité et de fraude à la carte de crédit a été estimé à 15 milliards de dollars en 2015. D'après cette étude, bien que le nombre d'Américains ayant été victimes d'une usurpation d'identité ou d'une fraude à la carte de crédit soit resté relativement stable depuis 2012, avec une moyenne d'environ 12,8 millions de particuliers touchés, les pertes provoquées par ces escroqueries ont chuté d'environ 25 pour cent ; par conséquent, les bénéfices récoltés par les cybercriminels, bien que toujours élevés, baissent également.

Par opposition à cette tendance à la baisse de l'usurpation d'identité et de la fraude à la carte de crédit, le FBI a signalé que, par rapport à l'année précédente, les crimes par ransomware ont déjà décuplé au cours des seuls trois premiers mois de l'année 2017. Le coût pour les organisations et entreprises américaines atteint une estimation conservatrice de plus de 200 millions de dollars. Le total des rançons payées aurait donc dépassé le milliard de dollars en 2016 et suivrait une croissance exponentielle en 2017.

Comprendre le fonctionnement du ransomware

Le ransomware est souvent livré dans un Exploit Kit, dans des *attaques dites de point d'eau ou oasis* (pendant lesquelles un ou plusieurs sites web visités fréquemment par une organisation sont infectés par un programme), dans une publicité malveillante ou lors de campagnes de phishing par mail (voir la Figure 1-2).

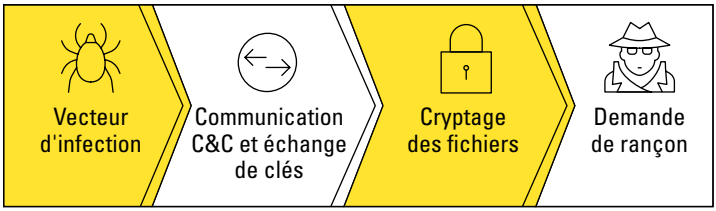


FIGURE 1-2: Comment un ransomware infecte un terminal.

ASTUCE

Allez sur `https://youtu.be/4gR562GW7TI` pour visionner l'anatomie d'une attaque par ransomware.

Une fois livré, le ransomware identifie en général les fichiers et données utilisateurs à crypter par le biais d'une liste d'extensions de fichier qui lui est intégrée.. Il est également programmé pour éviter d'interagir avec certains répertoires systèmes (comme le répertoire système WINDOWS, ou certains répertoires de fichiers programmes) afin d'assurer un système suffisamment stable pour le paiement de la rançon lorsqu'il aura terminé son exécution. Les fichiers situés dans des emplacements spécifiques qui correspondent à l'une des extensions de fichiers listées sont alors cryptés. Dans le cas contraire, le ou les fichiers sont ignorés. Une fois les fichiers cryptés, le ransomware laisse en général une notification à l'utilisateur, avec des instructions pour le paiement de la rançon (voir la Figure 1-3).

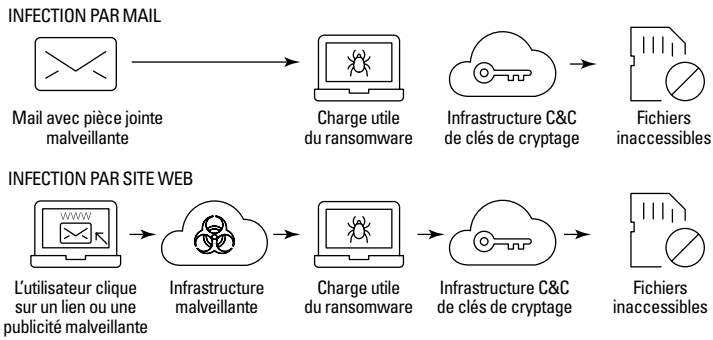


FIGURE 1-3: Le fonctionnement du ransomware

AVERTISSEMENT

Les voleurs ne tiennent pas leur parole. Bien qu'en général, le criminel vous fournisse la clé de décryptage de vos fichiers si vous payez la rançon, il n'est pas garanti qu'il n'a pas déjà installé un autre programme malveillant ou kit d'exploit sur votre terminal ou d'autres systèmes en réseau, qu'il ne volera pas vos données à d'autres fins criminelles ou qu'il ne vous extorquera pas plus d'argent à l'avenir.

DANS CE CHAPITRE

- Être proactif en matière de défense contre les ransomwares
- Automatiser les solutions de défense contre les ransomwares pour une réaction rapide
- Se regrouper après une attaque

Chapitre 2
Bonnes pratiques pour réduire les risques

Dans ce chapitre, j'analyse les bonnes pratiques en matière de sécurité et les stratégies de réduction des risques qui, si elles sont appliquées correctement et entièrement, permettront à votre organisation de se défendre efficacement contre les ransomwares et autres menaces.

Avant une attaque : recherche, renforcement, durcissement

Il existe évidemment un certain nombre de bonnes pratiques que les organisations peuvent mettre en œuvre de manière proactive avant même d'être ciblées par un attaquant. S'il est difficile pour l'attaquant de s'immiscer dans votre organisation (de mettre un pied dans la porte pour ainsi dire), il va certainement s'intéresser à une victime plus facile, sauf si votre organisation fait l'objet d'une attaque ciblée.

Les attaques par ransomware peuvent être opportunistes : l'attaquant est souvent motivé par l'argent, avec le moins de risque et d'effort possible. La méthode la plus efficace pour briser l'enchainement des phases de l'attaque « kill chain » et prévenir en tout premier lieu le succès d'une attaque par ransomware consiste à empêcher un attaquant de pénétrer sur votre réseau à l'aide d'une approche architecturale.

RAPPEL

Le modèle de la « kill chain » de Lockheed Martin comprend sept phases d'attaque : reconnaissance, intrusion, livraison, exploitation, installation, commande & contrôle (C&C) et exécution des objectifs. Les cinq premières étapes ont toutes pour objectif d'accéder au réseau et aux systèmes de la cible.

En général, les attaquants obtiennent un accès initial à la cible en utilisant l'une des deux méthodes suivantes :

- Ingénierie sociale/phishing afin d'installer un programme malveillant ou d'inciter un utilisateur peu méfiant à révéler ses informations d'identification de réseau
- Exploitation d'une vulnérabilité dans une application ou un service ouvert aux utilisateurs (Internet)

AVERTISSEMENT

Concernant le phishing et la sensibilisation à la sécurité, le rapport d'enquête 2016 de Verizon sur les compromissions de données (DBIR) déplore que « la communication entre le criminel et la victime soit apparemment bien plus efficace que la communication entre les employés et le personnel de sécurité. »

ASTUCE

Les bonnes pratiques qui suivent, doivent être mises en place pour empêcher les attaquants d'avoir accès au réseau et aux systèmes de votre organisation :

- **Sensibiliser les utilisateurs finaux à la sécurité par le biais d'une formation continue.** Cette formation doit être convaincante et présenter les toutes dernières informations sur les menaces et les tactiques. Veillez à :
  - Renforcer les politiques de l'entreprise concernant l'interdiction de partager ou de révéler les identifiants utilisateur (même avec le personnel informatique et/ou de sécurité), l'obligation d'utiliser des mots de passe robustes et le rôle de l'authentification dans la sécurité (y compris le concept de *non-répudiation,* qui donne aux utilisateurs la possibilité de rétorquer : « Ce n'était pas moi ! »).
  - Encourager l'utilisation des applications SaaS (logiciel en tant que service), comme les programmes de partage de fichiers, pour échanger des documents avec des collègues, au lieu d'utiliser les pièces jointes à un mail, dans le but d'atténuer (ou d'éliminer complètement) les attaques par phishing qui contiennent des pièces jointes malveillantes.

- Envisager le rendu de documents non natifs pour les fichiers PDF et Microsoft Office dans le cloud. Les applications de bureau telles qu'Adobe Acrobat Reader et Microsoft Word contiennent souvent des vulnérabilités non corrigées qui peuvent être exploitées.
- Informer les utilisateurs qui n'utilisent pas régulièrement des macros de ne jamais activer les macros dans des documents Microsoft Office. On a récemment observé un retour des programmes malveillants à base de macros, qui utilisent des techniques sophistiquées pour échapper à la détection.
- Expliquer les procédures de notification des incidents et s'assurer que les utilisateurs n'ont aucun problème à signaler les incidents, en ayant recours à des messages comme « vous êtes la victime, pas l'instigateur » et « camoufler un incident est pire (en termes de dommages) que l'incident proprement dit ».
- Ne pas oublier de parler de la sécurité physique. Bien que moins courantes que les autres formes d'ingénierie sociale, les tactiques et politiques d'escorte des visiteurs, comme la fouille des poubelles, le vol des identifiants en regardant par-dessus l'épaule de la victime, et le passage à deux personnes (ou talonnage), qui menacent potentiellement leur sécurité personnelle, ainsi que la sécurité des informations, doivent être rappelées aux utilisateurs.

» **Effectuer des évaluations continues des risques pour identifier toutes les vulnérabilités et faiblesses sécuritaires au sein de l'organisation et corriger toutes les expositions aux menaces pour réduire le risque.**
Veillez à :

- Réaliser régulièrement des analyses des ports ouverts et des vulnérabilités.
- Assurer une gestion robuste et rapide de la mise en en place des correctifs.
- Désactiver tous les services inutiles et vulnérables, et respecter les conseils de renforcement du système.
- Si possible, faire appliquer les exigences de mots de passe robustes et mettre en œuvre l'authentification à deux facteurs.
- Centraliser les journaux de sécurité sur un collecteur central ou une plateforme de gestion des incidents et failles de

sécurité (SIEM), mais aussi vérifier et analyser fréquemment les informations des journaux.

Malheureusement, en dépit de tous les efforts mis en œuvre, les gens sont ce qu'ils sont et il existera toujours des menaces « zero-day » qui exploitent des vulnérabilités inconnues jusqu'ici (et donc sans correctif). Si un attaquant parvient à accéder à votre réseau, il cherche ensuite à établir des communications C&C pour

- Assurer la persistance de son accès
- Élever ses privilèges
- Se déplacer latéralement sur le réseau, le data center et l'environnement utilisateur final

En vue d'atténuer les effets d'une intrusion réussie, appliquez les bonnes pratiques suivantes :

- Déployez une protection au niveau de la couche DNS (Domain Name System) capable d'identifier les adresses IP, les infrastructures Internet et les domaines malveillants afin de vous aider à atténuer les risques d'attaque.
- Activez systématiquement un pare-feu, une protection avancée contre les programmes malveillants, un cryptage des données et une prévention contre la perte de données sur tous les terminaux, y compris les appareils mobiles personnels (si une politique d'utilisation d'appareils personnels (BYOD) est autorisée) et les supports amovibles (comme les clés USB), qui sont tous transparents pour l'utilisateur et n'exigent aucune action de celui-ci. Les utilisateurs à distance et itinérants sont ainsi protégés qu'ils soient sur le réseau ou non, même lorsqu'ils ne respectent pas à la lettre les bonnes pratiques et politiques établies.
- Activez les fonctions de sécurité sur les passerelles de messagerie, y compris le blocage ou la suppression des fichiers exécutables et autres documents jointes potentiellement malveillantes. Vérifiez le SPF (système de vérification de l'identité du nom de domaine de l'expéditeur d'un courrier électronique) pour atténuer l'usurpation d'adresses de courrier électroniques et la limitation des mails (ou « greylisting ») pour limiter le taux des mails potentiellement indésirables.
- Activez les produits et services de sécurité qui analysent le trafic Internet, les mails et les fichiers pour éviter les infections et l'exfiltration de données (sujets abordés plus en détail dans les

chapitres 3 et 4), et exploitez les services fournissant du renseignement sur les menaces (threat intelligence) afin d'analyser plus précisément le contexte et permettre une investigation plus rapide.

- Concevez et déployez une architecture de sécurité robuste et intrinsèquement sécurisée, qui utilise la segmentation pour limiter le déplacement latéral d'un attaquant dans votre environnement.
- Faites appliquer le principe du moindre privilège et éliminez « l'obtention graduelle de privilèges d'accès » pour limiter l'escalade de privilèges d'un attaquant.
- Sauvegardez régulièrement les systèmes et données critiques et testez périodiquement les sauvegardes pour vous assurer qu'elles sont correctes et peuvent être restaurées. Cryptez également vos sauvegardes et conservez-les hors ligne ou sur un réseau de sauvegarde distinct.
- Évaluez et vérifiez vos capacités de réaction aux incidents, et surveillez et mesurez constamment et continuellement l'efficacité globale de votre stratégie de sécurité.

ASTUCE

La plupart des ransomwares s'appuient sur une infrastructure de communications C&C robuste pour transmettre, par exemple, des clés de cryptage et des messages de paiement. En empêchant un attaquant de se connecter à un ransomware qui a infecté son réseau, une organisation peut empêcher une attaque par ransomware d'aboutir complètement. Si l'attaquant ne parvient pas à envoyer des clés de cryptage à un terminal infecté ou à informer une victime de la méthode à utiliser pour envoyer la rançon, l'attaque est un échec. Comme le montre le tableau 2-1, les variantes de ransomwares les plus courantes aujourd'hui reposent fortement sur le DNS pour assurer les communications C&C. Dans certains cas, un navigateur Tor (« le routeur oignon ») est également utilisé pour les communications C&C.

TABLEAU 2-1 Communications C&C dans un ransomware.

Nom	Clé de cryptage	Message de paiement
Locky	DNS	DNS
TeslaCrypt	DNS	DNS
CryptoWall	DNS	DNS
TorrentLocker	DNS	DNS
PadCrypt	DNS	DNS, Tor
CTB-Locker	DNS, Tor	DNS
FAKBEN	DNS	DNS, Tor
PayCrypt	DNS	DNS
KeyRanger	DNS, Tor	DNS

**Principales variantes en mars 2016*

Pendant une attaque : détection, blocage et défense

Si votre organisation est attaquée, une réaction rapide et efficace aux incidents est nécessaire pour limiter les dommages potentiels. Les efforts de correction et les étapes spécifiques à entreprendre sont fonction de chaque situation. Toutefois, il ne faut pas attendre d'être attaqué pour évaluer l'ampleur et l'étendue des capacités de réaction aux incidents de votre organisation ! Vos processus de réponse aux incidents doivent être bien compris et coordonnés (mesures à prendre avant une attaque), bien documentés et répétables. Ainsi, vous pourrez reconstruire un incident après une attaque et identifier les leçons à en tirer et les domaines potentiels d'amélioration.

Un élément clé souvent ignoré pour assurer une réponse efficace aux incidents est le partage d'information, avec notamment :

- **Une communication opportune et précise des informations à toutes les parties prenantes :** des informations pertinentes doivent être communiquées aux cadres dirigeants pour s'assurer que les ressources dédiées à la réaction et à la correction sont adéquates, que des décisions professionnelles critiques et étayées peuvent être prises, et que des informations appropriées sont, en retour, communiquées aux

employés, aux autorités d'application de la loi, aux clients, aux actionnaires et au grand public.

- **Un partage automatique des nouveaux renseignements de sécurité à travers toute l'architecture :** le regroupement des données critiques issues de systèmes disparates, notamment ceux des systèmes de gestion des incidents et failles de sécurité (SIEM), des renseignements sur les menaces et des outils de sandboxing, permet à l'équipe de réponse aux incidents d'intervenir rapidement et de trier efficacement les incidents de sécurité les plus graves. Par exemple, si la charge utile d'un nouveau programme malveillant est détectée sur un terminal, elle doit être envoyée automatiquement vers une plateforme de type cloud de renseignements sur les menaces pour être analysée en vue d'en trouver et en extraire les indicateurs de compromission (IoC). Puis, les nouvelles contremesures associées doivent automatiquement être déployés et mise en oeuvre.

Après une attaque : étendue, contenu et correction

Les actions importantes à mettre en œuvre lorsqu'une attaque est terminée comprennent :

- La reprise des activités professionnelles normales, incluant la restauration à partir des sauvegardes et la réinstallation des systèmes, si nécessaire
- Collecte et préservation des preuves à l'intention des organismes d'application des lois et d'audit
- Analyse des données techniques pour prévoir et prévenir de futures attaques, par exemple, en identifiant les domaines et programmes malveillants en lien avec les adresses IP, les signatures numériques des fichiers et les domaines associés à l'attaque
- Réalisation d'une analyse des causes fondamentales, identification des leçons apprises et redéploiement des ressources de sécurité si besoin

ASTUCE

Les renseignements prédictifs sur les menaces permettent de mettre en œuvre une stratégie de sécurité proactive, permettant à votre organisation de voir l'infrastructure C&C utilisée par les attaquants pour leurs attaques actuelles et futures, et de garder ainsi un coup d'avance sur la menace.

DANS CE CHAPITRE

- Choisir entre un système sophistiqué et tout-en-un
- Obtenir le meilleur des deux mondes avec un portefeuille de sécurité intégré

Chapitre 3
Création d'une nouvelle architecture de sécurité sophistiquée

Dans ce chapitre, vous apprendrez quels sont les différents défis associés aux approches actuelles de l'architecture de la sécurité et quelle est la meilleure architecture pour mieux répondre aux menaces modernes, y compris le ransomware.

Reconnaître les limites des conceptions actuelles de la sécurité

Par le passé, la plupart des entreprises pensaient avoir fait un choix en matière de sécurité :

- Elles pouvaient utiliser des produits qui s'avéraient efficaces contre des types spécifiques de menaces émergentes, sans pour autant s'intégrer entièrement dans une approche architecturale pour intégrer les solutions de défense.
- Elles pouvaient adopter une approche systémique qui assimilait dans une architecture système intelligente des produits de sécurité autonomes (ou ponctuels) « suffisamment bons ».

Aujourd'hui, la plupart des organisations ont déployé une architecture de réseau hiérarchique composée d'une couche d'accès, d'une couche

de distribution et d'une couche principale avec de multiples produits de sécurité autonomes, déployés dans une Zone Demilitarisée ou de services locaux, comme un pare-feu et/ou un serveur proxy web. Malheureusement, cela n'a rien à voir avec une véritable « défense en profondeur » (voir la Figure 3-1).

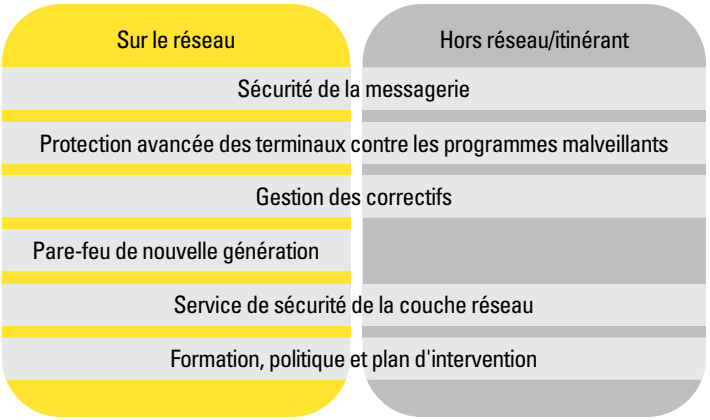


FIGURE 3-1: La sécurité consiste à gérer les risques à travers les couches.

Parmi les limites associées aux approches actuelles, on peut citer :

- **L'absence d'intégration ou de corrélation.** Des produits de les équipes réduites d'analystes sécurité avec des informations détaillées non coordonnées qu'il est difficile de tirer, ce qui les oblige à chercher la fameuse « aiguille dans la botte de foin ».
- **Une sécurité basée sur la défense du périmètre ne suffit pas pour établir une architecture efficace.** Les pare-feux, passerelles web sécurisées et technologies de sandboxing déployés en périphérie du réseau ne voient passer que le trafic de et à destination l'Internet. Le trafic au sein du Data Center (trafic entre les applications et les utilisateurs finaux qui ne passe pas via l'Internet) peut représenter jusqu'à 80% du trafic total du réseau. Il est donc nécessaire d'avoir une visibilité complète sur l'ensemble du réseau.
- **Les employés ont quitté les bureaux.** Non seulement les cybercriminels ont modifié leur façon de travailler (leurs tactiques et techniques), mais la méthode de travail et d'interaction numérique de nos utilisateurs a également évolué. En raison du nombre grandissant d'utilisateurs distants et itinérants qui travaillent avec différents appareils directement

via le cloud, les technologies de sécurité basées sur la défense du périmètre et les réseaux privés virtuels (VPN) ne sont plus capables de protéger parfaitement les appareils et les données de l'entreprise. La plupart des services de type cloud (comme Salesforce.com et Office 365) proposent un accès pratique sans connexion VPN, mais n'assurent qu'une protection basique pour ces applications et données, comme une protection contre les programmes malveillants. Selon Gartner, d'ici 2018, 25% du trafic de données d'entreprise contournera la sécurité périmètrique et passera directement des appareils mobiles au cloud. Les solutions de sécurité modernes doivent permettre à votre entreprise d'adopter le cloud et de travailler depuis n'importe quel appareil, n'importe où, et n'importe quand, en étendant la protection existante bien au-delà du périmètre traditionnel du réseau.

- **Un manque de visibilité.** Les traditionnels pare-feux basés sur les ports sont aveugles à la plupart des menaces qui utilisent des techniques d'évasions, comme l'utilisation de ports non standard, le *port-hopping* (saut de ports) et le cryptage.
- **La segmentation est insuffisante et la segmentation traditionnelle peut être complexe.** Les réseaux sont couramment segmentés en zones « fiables » et « non fiables » de façon statique par des VLANs définis sur des commutateurs, qui peuvent être difficiles à configurer et à maintenir. Cette structure arbitraire ne correspond pas aux nouvelles architectures des data center modernes : des machines virtuelles qui se déplacent dynamiquement à travers les data centers et dans le cloud. A la place, une segmentation granulaire multiple (y compris une micro-segmentation) doit être définie sur l'ensemble des appareils réseaux du data center à l'aide d'une segmentation dynamique définie par logiciel.
- **Les mises à jour statiques ne constituent que le point de départ.** Le téléchargement et l'installation de fichiers de signature anti-programmes malveillants ne sont que le point de départ pour lutter efficacement contre les menaces « zero day » d'aujourd'hui qui évoluent rapidement. Les fichiers de signature statiques ont besoin d'être soutenus par des renseignements sur les menaces provenant en temps réel du cloud.

Définition de la nouvelle architecture de sécurité sophistiquée

Pour protéger les entreprises contre les ransomwares et autres menaces modernes, une nouvelle architecture de sécurité sophistiquée s'appuie sur un portefeuille de solutions intégrées qui sont à la fois simples, ouvert et automatisé, par opposition aux traditionnels produits ponctuels. Cette nouvelle architecture :

- Partage automatiquement des renseignements sur les menaces et fournit un contexte agrégé et corrélé avec d'autres produits et services de sécurité, à la fois en local et dans le cloud
- Réduit la complexité et apporte une visibilité complète dans l'ensemble de l'environnement
- Permet une meilleure intégration avec les solutions de sécurité quelles soient nouvelles ou existantes à l'aide de normes et de technologies ouvertes et évolutives
- Utilise l'intégration pour réagir de manière automatisée. Ainsi, la sécurité gagne en efficacité et réduit la charge de travail des autres équipes informatiques

Cette nouvelle version d'une architecture « best of breed » de sécurité est composée des éléments suivants (voir la Figure 3-2) :

- Pare-feux de nouvelle génération (NGFW) et systèmes de prévention des intrusions de nouvelle génération (NGIPS) qui ont visibilité sur les personnes qui accèdent au réseau et sur ce qu'elles font, surveillent l'application des politiques, analysent le trafic et analysent les trajectoires des fichiers/ressources
- Renseignements provenant du cloud sur les menaces
- Sécurité au niveau de la couche DNS (Domain Name System) pour étendre la protection au-delà des pare-feux de l'organisation
- Segmentation très granulaire du réseau définie par logiciel, avec une application des politiques en fonction des rôles, quel que soit le lieu, l'appareil ou l'adresse IP
- Sécurité de la messagerie et d'Internet (et pas seulement du trafic web)
- Protection avancée contre les programmes malveillants que ce soit au niveau du réseau comme du poste de travail, avec des capacités de sandboxing

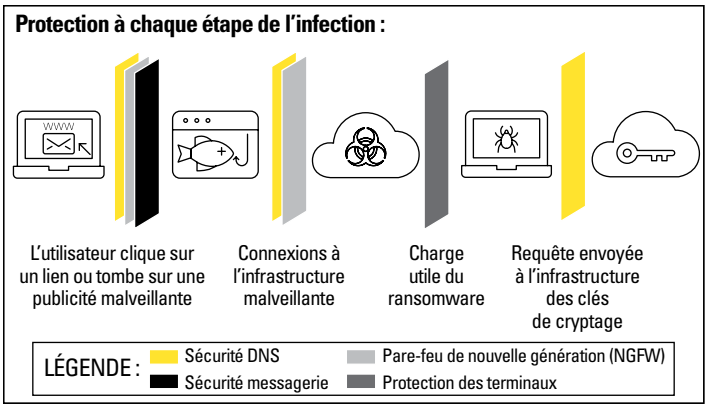


FIGURE 3-2: La nouvelle architecture de sécurité sophistiquée couvre la plus grande surface d'attaques possibles avec une défense en profondeur.

CAMUTO GROUP DÉFEND SES PROPRIETES INTELLECTUELLES SANS COMPROMETTRE SA PRODUCTIVITÉ

Le défi : les entreprises de création doivent équilibrer la facilité d'accès et la protection du patrimoine intellectuelle

Camuto Group, un fabricant reconnu de chaussures et de vêtements possédant des magasins aux États-Unis et en Europe et des centres de fabrication au Brésil, en Italie et en Chine, prospère grâce à ses créations uniques. La créativité est l'arme la plus puissante de l'entreprise, mais pour les professionnels de la sécurité informatique de l'entreprise, c'est une arme à double tranchant. Parmi les 500 employés de Camuto, 100 travaillent sur des ordinateurs distants et 250 depuis des ordinateurs portables itinérants, qui doivent être protégés contre le vol de données ; cependant, les créatifs et les commerciaux doivent pouvoir accéder librement à de nombreux sites web avant-gardistes, que bon nombre de solutions de filtrage Internet bloquent à mauvais escient.

Selon Tom Olejniczak, le responsable de l'ingénierie du réseau de Camuto Group, « la protection des produits de Camuto Group par le biais de la sécurité est l'un de nos principaux objectifs. Nos produits et

(à suivre)

(suite)

créations sont l'essence même de l'entreprise ; la protection de ce patrimoine est primordiale pour participer au succès de notre activité. »

Au cours de ses précédentes expériences, M. Olejniczak a découvert que l'approche traditionnelle de la sécurité Internet (les serveurs proxy) créait des obstacles qui devaient être surmontés manuellement. Selon M. Olejniczak, « De nombreux sites web inoffensifs sont mal cryptés ou s'appuient sur des contrôles obsolètes du contenu, comme ActiveX. ». « Chaque fois qu'une personne devait aller sur un tel site web, elle avait besoin de l'intervention du service informatique. »

Chez Camuto, en raison du nombre d'employés nomades, ce type d'intervention manuelle était simplement impossible. Avec la progression des programmes malveillants et la baisse de productivité due aux réseaux sociaux, Camuto Group devait trouver une solution de sécurité réseau qui protégeait les appareils sur et en dehors du réseau sans ajouter de latence ni gêner les activités professionnelles.

La solution : Cisco Umbrella s'avère la première ligne de défense la plus efficace

M. Olejniczak affirme avoir « suivi Umbrella depuis le début, » avant même que cette solution ne soit sélectionnée. Pour trouver la solution la mieux adaptée à Camuto, le service informatique a testé deux alternatives : Zscaler et Websense.

Dans le mois où M. Olejniczak a abandonné Umbrella pour tester Zscaler, « le nombre de programmes malveillants a augmenté de 30%. Nous luttions contre trois infections par jour, et passions à chaque fois, de une à trois heures pour nettoyer et d'avantage si une réinstallation s'avérait nécessaire. » M. Olejniczak a découvert que les filtres Internet de type proxy qu'il utilisait par le passé fonctionnaient mal avec les sites exigeant des certificats. « Il fallait beaucoup d'interventions manuelles », précise-t-il.

« Le produit Websense était simplement trop lent ; on avait l'impression d'avoir un logiciel supplémentaire sur le PC », déclare-t-il. « Il augmentait la latence de 40 à 50%. » Finalement, Camutao a arrêté son choix sur Umbrella et a déployé le client itinérant sur les ordinateurs portables pour étendre les capacités de sécurité et de filtrage d'Umbrella. « Nous utilisons Umbrella comme première ligne de défense », précise M. Olejniczak, « en l'associant à notre protection antivirus et d'autres protections réseau proactives contre les menaces. »

L'impact : Camuto Group bloque 400 programmes malveillants par jour tout en accélérant les performances Internet

« Il s'agit d'une solution cloud qui remplace le travail de filtrage web que nous faisions en interne par le passé ; c'est bien ce qui me plaît dans Umbrella », explique M. Olejniczak. Afin de protéger les employés sur site, Camuto a déployé les appliances virtuelles d'Umbrella, ce qui leur donne la capacité d'identifier les réseaux internes ou les utilisateurs Active Directory infectés ou ciblés par des attaques, sans avoir à modifier les appareils ou à procéder à une nouvelle authentification des utilisateurs. Les employés travaillant en dehors du réseau de l'entreprise sont protégés par le biais du client itinérant d'Umbrella, dont l'installation « est aussi facile que d'ajouter une personne à un groupe dans de Microsoft Active Directory. »

Camuto Group a immédiatement constaté des effets mesurables sur la sécurité. « Lorsque je vais sur le tableau de bord d'Umbrella le matin », indique M. Olejniczak, « je vois en général que 400 programmes malveillants ont été redirigés ; cela revient à des milliers par semaine. » Cependant, les utilisateurs ne perçoivent pas la présence d'Umbrella. « En fait, cette solution a amélioré légèrement la vitesse d'Internet », indique M. Olejniczak. « Nous constatons une amélioration de peut-être 5 à 10% environ, ce qui représente près de 30 pour cent de performances de plus que les autres produits. »

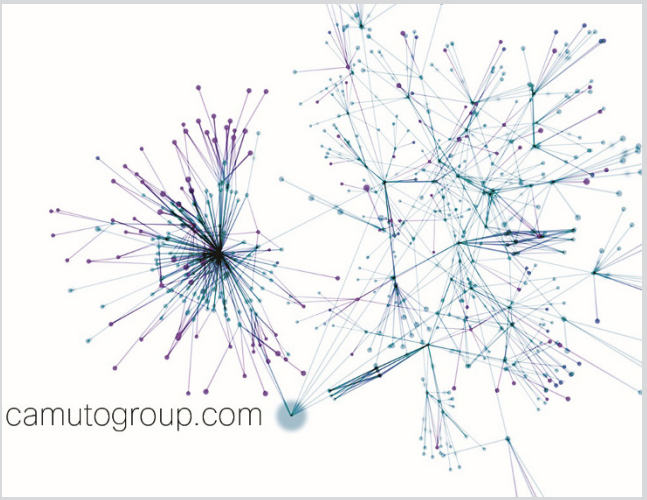
Dans une entreprise qui dépend de l'accès de ses créatifs à des sites de mode sophistiqués, la capacité de gérer des listes blanches et noires devient rapidement critique. « Nous pouvons choisir des catégories sûres et acceptables par les ressources humaines pour filtrer rapidement le contenu », précise M. Olejniczak. Lorsque les rapports présentent des sites auparavant inconnus et inappropriés ou risqués (ou quand les employés demandent un accès à des sites légitimes qui ont été bloqués), il est facile de mettre les listes à jour. « Cette solution est extrêmement efficace : je peux me connecter, apporter des modifications et me déconnecter en moins de trois minutes. »

M. Olejniczak remarque que la valeur d'Umbrella augmente avec le temps. « Plus vous utilisez le produit », selon lui, « mieux vous vous portez. Parmi les produits que j'ai utilisés dans ma carrière, peu d'entre eux font vraiment ce qu'ils prétendent faire, mais Umbrella est l'un d'entre eux. » Ce graphe de données (voir la figure ci-dessous) représente une vue générale, qui explique comment Cisco Umbrella voit l'infrastructure du domaine camutogroup.com et comment une partie des utilisateurs

(à suivre)

(suite)

d'Umbrella (plus de 65 millions) interagissent avec ce domaine et son infrastructure associée.



ASTUCE

Le chapitre 4 vous décrira l'approche Cisco pour appréhender cette nouvelle architecture de sécurité sophistiquée grâce à la solution de défense contre les ransomwares. La Figure 3-3 présente les solutions Cisco qui permettent de prévenir, détecter et répondre aux attaques par ransomware.

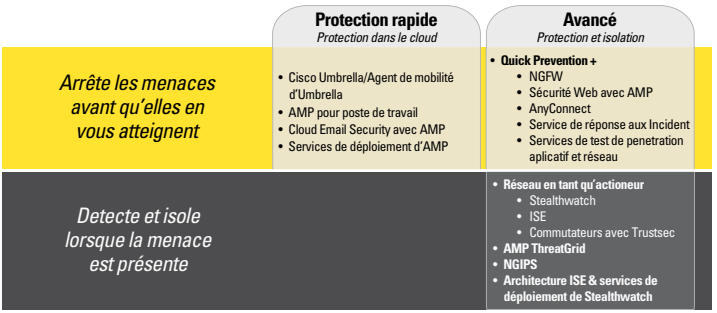


FIGURE 3-2: Groupes de solutions Cisco de défense contre les ransomwares disponnibles

DANS CE CHAPITRE

- Transférer la défense contre les ransomwares dans le cloud
- Fermer les vecteurs d'attaque des ransomwares sur les terminaux et dans la messagerie
- Faire appliquer les politiques de sécurité avec une segmentation et des pare-feux de nouvelle génération
- Faire appel aux services de conseil en sécurité de Cisco

Chapitre 4
Déploiement de la solution de défense Cisco contre les ransomwares

La solution de defense contre les ransomwares de Cisco permet d'utiliser l'architecture de sécurité de Cisco pour protéger les entreprises. Cette solution offre une approche architecturale pour lutter contre les ransomwares partout où ils tentent d'infiltrer un réseau. Par conséquent, vous profitez d'une protection en couches complémentaires, allant du DNS à la messagerie, au réseau et au terminal. Ce chapitre vous présente cette proposition d'architecture de défense complète.

Le DNS comme première ligne de défense dans le cloud

L'attaque d'un ransomware comprend de nombreuses étapes. Avant d'attaquer, le pirate informatique doit mettre en place l'infrastructure Internet qui soutiendra les étapes d'infection et de contrôle & commande (C&C). Cisco Umbrella est la première ligne de défense qui arrête les attaques des ransomwares (et autres cyberattaques) dès le début de l'enchainement des étapes d'attaque, en bloquant les connexions Internet vers les sites malveillants qui diffusent les ransomwares. Basé sur

les fondements d'Internet, Umbrella applique la sécurité au niveau de la couche DNS (Domain Name System) et des protocoles Internet (IP) (voir la Figure 4-1).

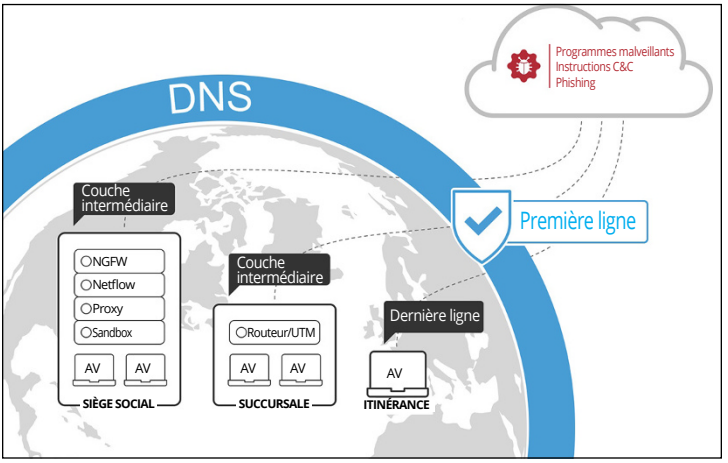


FIGURE 4-1: La couche DNS est la première ligne de défense bloque les attaques des ransomwares.

Umbrella assure une visibilité complète de l'activité Internet en tout lieu, sur tout appareil et pour tout utilisateur, et bloque les menaces sur tous les ports ou protocoles avant même qu'elles n'atteignent votre réseau ou vos terminaux. En analysant et en apprenant de l'activité Internet, Umbrella découvre automatiquement l'infrastructure mise en place par l'attaquant pour les menaces en cours et émergentes, et bloque dynamiquement les requêtes vers les destinations malveillantes avant même d'établir une connexion ou de télécharger un fichier malveillant. Umbrella peut également bloquer les connexions de type contrôle & commande (C&C) vers les serveurs des pirates et empêcher les systèmes compromis d'exfiltrer des données. Avec Umbrella, vous pouvez interrompre plus tôt le phishing et les infections de malwares, identifier plus rapidement les appareils déjà infectés et empêcher l'exfiltration des données.

ASTUCE

Contrairement aux appliances, le service cloud protège les terminaux qui sont sur et en dehors du réseau d'entreprise. Contrairement aux agents, la protection au niveau de la couche DNS s'étend à chaque appareil connecté au réseau, et même à l'Internet des objets (IoT). Déployable en seulement 30 minutes, il s'agit de la méthode la plus rapide et la plus facile pour protéger tous vos utilisateurs. Téléchargez le livre blanc : « Why a DNS Layer Matters: 30 Minutes to a More Secure Enterprise » (L'importance de la couche DNS : 30 minutes pour une entreprise plus sûre) sur `http://cs.co/30-mins-to-a-more-secure-enterprise` pour en savoir plus.

LES SERVICES INFORMATIQUES DE CISCO METTENT EN ŒUVRE UMBRELLA COMME MOYEN DE DÉFENSE CONTRE LES RANSOMWARES ET AUTRES MENACES

En décembre 2016, Cisco a adopté Umbrella pour protéger ses services informatiques interne ciblant deux objectifs essentiels :

- Renforcer la protection contre les programmes malveillants, les botnets et les failles : en tant que service de résolution DNS mondial, Umbrella voit 5 % des requêtes Internet de la planète. Il découvre rapidement les menaces émergentes et les bloque avant qu'elles ne fassent des dégâts.
- Apprendre à connaître les comportements à risque des utilisateurs : Umbrella génère un journal sur toutes les activités se déroulant sur Internet, quels que soient le port et le protocole. Ces journaux augmentent les capacités de visibilité et d'audit des équipes informatiques et de sécurité de Cisco.

La transition vers Umbrella a été extrêmement simple. « Nous avons ajouté de nouveaux services de contrôle puissants sans déployer de nouveaux matériels, sans reconfigurer le réseau, ni mener de vastes essais d'interopérabilité ou modifier d'autres systèmes », précise Rich West, l'architecte de la sécurité des systèmes d'information (InfoSec) de Cisco.

Cisco a réuni une équipe de huit personnes issues des services informatiques et InfoSec afin de planifier et de mettre en œuvre Umbrella. Les aspects techniques de la transition ont été réglés très rapidement. Les membres de l'équipe ont passé la majeure partie de leur temps à expliquer les avantages de cette transition aux responsables des applications et aux équipes de gestion du réseau et à répondre à toutes leurs questions concernant les répercussions potentielles sur les performances des applications et des réseaux.

Ce processus de conversion peut se faire tout simplement en ajoutant quatre lignes au fichier de configuration DNS des serveurs DNS internes de Cisco, pour qu'ils renvoient des requêtes à Umbrella. Aujourd'hui, les serveurs DNS des services informatiques de Cisco envoient à Umbrella les requêtes DNS récursives au lieu d'interroger leurs voisins en amont. Grâce à la transparence de cette conversion, les utilisateurs internes n'ont même pas remarqué le changement.

UN FABRICANT MONDIAL DE MATÉRIEL MÉDICAL CONTRE UN RANSOMWARE

Le défi : lutter contre des menaces de sécurité illimitées avec des ressources limitées

Au cours des décennies qui ont suivi sa création en 1983, l'entreprise Octapharma est devenue peu à peu l'un des plus grands fabricants mondiaux de protéines humaines. Forte d'une initiative lancée pour doubler ses capacités de production et accroître son efficacité globale d'ici 2019, l'entreprise connaît actuellement une expansion sans précédent.

Cette poussée de croissance a clairement des répercussions dans toute l'entreprise, même au niveau du réseau. « En augmentant le nombre d'employés et de bureaux, nous avons augmenté le nombre d'appareils mobiles et de services cloud, mais nous avons aussi ajouté de nouvelles vulnérabilités en termes de sécurité du réseau », déclare Jason Hancock, l'ingénieur réseau en chef global d'Octapharma. « Nous avons assisté à une explosion des activités malveillantes en tous genres, y compris les ransomwares.

Au lieu de surveiller tous les accès en embauchant des professionnels de sécurité qualifiés déjà difficiles à trouver, nous avons choisi d'identifier de nouvelles solutions pour résoudre ces vulnérabilités et de les aligner avec les objectifs d'efficacité de l'organisation », ajoute-t-il.

« En gardant cette priorité à l'esprit », précise Hancock, « nous devions tout d'abord éviter les pannes de réseau toutes les 15 minutes et améliorer leur efficacité, à la fois pour notre équipe et pour les utilisateurs. Lorsque je suis venu travailler dans cette entreprise en 2014, je souhaitais en premier lieu stabiliser la situation afin de pouvoir me concentrer sur la prévention des programmes malveillants de plus en plus agressifs, comme Cryptolocker dont nous avons été victimes. »

La solution : une fonctionnalité adaptée

« Avant mon arrivée à Octapharma, l'équipe avait travaillé pendant quelque temps sur une migration des appliances de sécurité web vers le service cloud d'un fournisseur que mon prédécesseur avait sélectionné. À l'origine, j'avais pour mission de terminer ce déploiement », se souvient M. Hancock. « Après avoir analysé la situation, j'ai compris que nos besoins ne seraient pas satisfaits.

Nous avons rencontré des difficultés majeures remettant en cause la viabilité de la solution dans notre environnement, en commençant par la fonctionnalité Internet. » Selon M. Hancock, « notre équipe a reçu de nombreux commentaires des utilisateurs insatisfaits du service Internet, ce qui a été attribué à la fois au service cloud et au navigateur installé sur les machines des utilisateurs.

En outre », poursuit-il, « le jeu de fonctionnalités n'était pas aligné sur nos besoins, et toute l'équipe éprouvait des difficultés en matière d'administration. Par conséquent, nous avons dû organiser une formation poussée pour permettre une gestion détaillée et non intuitive des politiques et autres composants.

Après un déploiement nord-américain pour le moins compliqué, notre réseau tombait régulièrement en panne. Le manque de fiabilité associé à la disparition du service Internet pendant plusieurs heures d'affilée a jeté une ombre sur notre équipe. De plus, ce problème ne pouvait pas être résolu par les services d'assistance du produit », explique M. Hancock. « Finalement, [le fournisseur] nous a proposé d'abandonner la migration vers le cloud en faveur des appliances virtuelles, ce qui nécessitait une redirection du trafic provenant de quelque 50 emplacements dans le monde ; une solution peu souhaitable et dans certains cas impossible.

C'est là que je suis intervenu : « Cisco Umbrella est la seule façon de résoudre ce problème et je peux faire déployer ce service pour qu'il protège notre réseau mondial en six semaines. » Après avoir tant investi dans une solution qui ne nous convenait pas, nous étions prêts à adopter une solution que je savais adaptée grâce à mon expérience passée : Umbrella. »

Le résultat : réduction draconienne des ransomwares

Après un déploiement aisé, Octopharma a constaté immédiatement les résultats. « Depuis la mise en place d'Umbrella, nous n'avons eu aucune faille de sécurité », précise M. Hancock.

« Nous avons très fortement réduit notre exposition aux ransomwares, et depuis le déploiement d'Umbrella, nous n'avons été victimes d'aucun ransomware suite à un clic sur un lien malveillant. Nous constatons en fait des dizaines de milliers de blocages par semaine en raison de la politique de sécurité ; sans compter les blocages reposant sur les politiques de filtrage de contenu basées sur des catégories, » ajoute-t-il. « Nous avons couvert un risque majeur dans le vecteur d'at-

(à suivre)

(suite)

taque web des ransomwares et nous avons considérablement amélioré notre expérience utilisateur par rapport à la connectivité Internet.

Nous avons même identifié quelques courriels de phishing et les avons testés en tentant de cliquer sur leurs liens ; grâce à Umbrella, les sites étaient inaccessibles. »

Un autre avantage inattendu ? Selon l'ingénieur réseau, « en mettant en corrélation les précieuses données issues du tableau de bord d'Umbrella et les données de nos systèmes internes, nous avons découvert des machines infectées qui n'avaient pas été détectées par le passé. »

Sa pile de sécurité étant désormais en mesure de bloquer les menaces au niveau de la couche DNS, l'entreprise continue à chercher des moyens de renforcer son réseau avec une gestion proactive de la sécurité. « Alors que le service de sécurité Umbrella est tout à fait capable de bloquer des sites en appliquant des politiques de catégories, il est plus efficace comme outil de sécurité. En gardant cette idée à l'esprit lors de notre déploiement, il devient un composant critique de notre stratégie de défense en profondeur. J'examine actuellement d'autres outils appartenant au portefeuille de sécurité de Cisco pour renforcer davantage cette stratégie », déclare l'ingénieur réseau. « J'envisage une amélioration des pare-feux, une protection des terminaux contre les programmes malveillants et une plus grande coordination entre les produits de notre trousse à outils de sécurité. »

Pour Jason Hancock, il faut le voir pour le croire. « J'utilise Umbrella chez moi depuis des années », indique-t-il. « Après avoir également constaté son succès au sein de deux organisations différentes, mes collègues sont très satisfaits de l'approche unique et très efficace de Cisco en matière de sécurité. »

Sécurisation des terminaux et de la messagerie

Aujourd'hui, les menaces que représentent les programmes malveillants sont plus sophistiquées que jamais. Des programmes malveillants avancés, y compris des ransomwares, évoluent rapidement et peuvent échapper à la détection après avoir infecté un système de différentes manières, en utilisant notamment les méthodes suivantes :

- Techniques de mise en veille
- Polymorphisme et métamorphisme
- Cryptage et obscurité (du code)
- Utilisation de protocoles inconnus

En même temps, un programme malveillant avancé représente une rampe de lancement pour un attaquant persistant qui se déplace latéralement sur le réseau infecté d'une organisation.

Les campagnes de phishing par mail sont particulièrement prisées par les cybercriminels comme vecteur d'attaque (étonnamment efficace). Les récentes variantes de ransomwares comme Locky et Chimera utilisent toutes des techniques de phishing pour infecter leurs victimes.

Les solutions de défense contre les ransomwares de Cisco qui sécurisent les terminaux et protègent la messagerie comprennent Cisco AMP (Advanced Malware Protection) for Endpoints et Cisco Cloud Email Security avec AMP.

Cisco AMP for Endpoints

Les logiciels anti-malware traditionnels qui n'utilisent que des techniques de détection ponctuelles ne seront jamais totalement efficaces. Et il suffit qu'une seule menace échappe à la détection pour infecter l'ensemble de votre environnement. En utilisant des programmes malveillants sensibles au contexte, les pirates possèdent les ressources, l'expertise et la ténacité pour déjouer les solutions de défense ponctuelles. En outre, la détection ponctuelle ignore complètement l'étendue et la profondeur d'une faille exploitée. Les organisations sont donc dans l'incapacité d'empêcher l'infection de se répandre ou de prévenir une attaque similaire dans l'avenir.

ASTUCE

Bien qu'il n'existe aucune solution capable de supprimer les ransomwares ou de décrypter des fichiers une fois le terminal infecté, Cisco permet aux organisations de détecter les ransomwares de manière proactive et de les bloquer avant même qu'ils n'atteignent le réseau.

Grâce à cette compréhension des programmes malveillants, Cisco a créé AMP for Endpoints afin de proposer une structure complète de capacités de détection et d'analyse Big Data pour maintenir une analyse continue des fichiers et du trafic, et ainsi identifier et bloquer les menaces avancées. Des techniques sophistiquées d'apprentissage automatique évaluent plus de 400 caractéristiques associées à chaque fichier. *La sécurité rétrospective* (la capacité de revenir en arrière pour tracer les processus, les activités des fichiers et les communications afin de

comprendre l'étendue complète d'une infection, d'en définir les causes fondamentales et de lancer des mesures correctives) permet de détecter des fichiers qui deviennent malveillants après la décision initiale et bien évidemment vous alerter. Cette association d'une analyse continue et d'une sécurité rétrospective représente une protection avancée contre les programmes malveillants, qui va bien au-delà de la détection ponctuelle traditionnelle (voir la Figure 4-2).

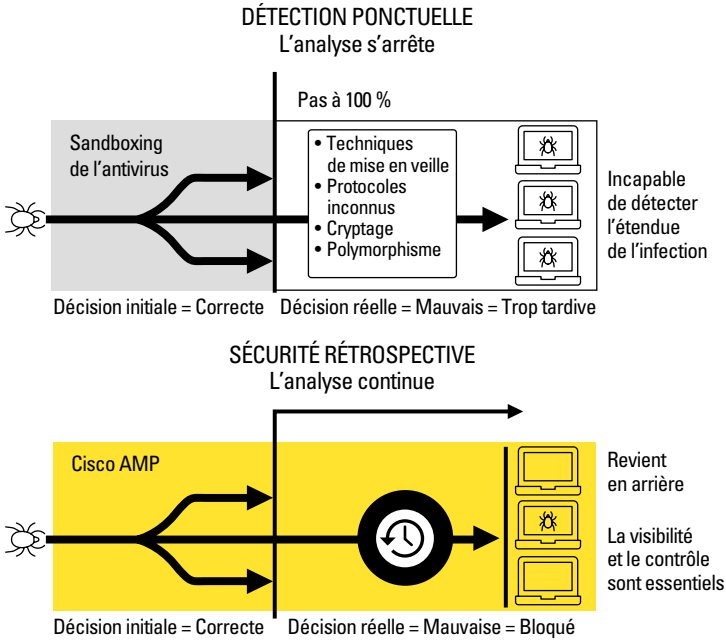


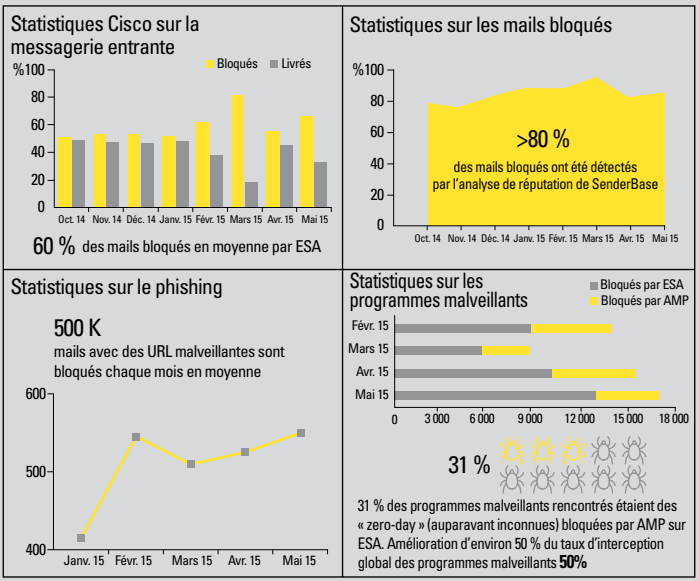
FIGURE 4-2: Comparaison entre la détection ponctuelle et la sécurité rétrospective/l'analyse continue.

Cisco Email Security avec AMP

La messagerie est un outil de communication professionnel primordial, mais elle peut exposer les entreprises à un large éventail de menaces sophistiquées. Cisco Email Security avec AMP bloque les spams, les mails de phishing, les pièces jointes et les URL malveillantes, qui constituent un vecteur d'attaque important pour les ransomwares. La technologie AMP est la même que celle appliquée sur le terminal, mais elle est déployée au niveau de la passerelle de messagerie.

CISCO GOÛTE À SES PROPRES RECETTES

Les services informatiques de Cisco s'appuient sur Cisco Email Security avec AMP pour sa stratégie de sécurité de la messagerie axée sur les menaces. Comme le montrent les graphiques ci-dessous, les résultats parlent d'eux-mêmes !



Cisco Email Security avec AMP protège la messagerie professionnelle par une protection en couche qui comprend :

- Des renseignements globaux sur les menaces (threat intelligence)
- Un blocage des spams
- Une détection du graymail et un désabonnement sécurisé
- Une protection avancée contre les programmes malveillants
- Des filtres d'épidémie (*outbreak filters*)
- Un suivi des interactions web
- Un contrôle des messages sortants
- Une détection des faux mails
- Une prévention des fuites de données

La protection du réseau par une segmentation et des pare-feux de nouvelle génération

Axés sur les menaces, les pare-feux de nouvelle génération Cisco Firepower (NGFW) assurent une défense intégrée dans tout le continuum de l'attaque (avant, pendant et après l'attaque) avec une visibilité incomparable que les pare-feux traditionnels reposant sur les ports, ne peuvent pas apporter. La technologie Cisco TrustSec assure une segmentation réseau dynamique à base de logiciel. Elle emploie le réseau existant pour faire respecter des politiques de sécurité granulaires basées sur les rôles sur des segments du réseau, quel que soit le lieu ou l'appareil de l'utilisateur. Il en résulte une segmentation plus simple qui aide à prévenir le déplacement latéral des programmes malveillants sur le réseau d'une organisation. En cas d'intrusion, les dommages provoqués peuvent ainsi être limités.

Pare-feu de nouvelle génération Cisco Firepower (NGFW)

Le pare-feu de nouvelle génération Cisco Firepower (NGFW) avec AMP et la technologie de sandboxing Threat Grid bloquent les menaces connues et les connexions de type contrôle & commande (C&C) tout en assurant une analyse dynamique des menaces et programmes malveillants inconnus. Cisco Firepower apporte :

- **Une visibilité et un contrôle précis des applications (AVC) :** identifie et contrôle l'accès des utilisateurs à plus de 4 000 applications commerciales, tout en offrant un support pour les applications personnalisées.
- **L'IPS Cisco de nouvelle génération :** une prévention extrêmement efficace des menaces et une sensibilisation contextuelle totale des utilisateurs, de l'infrastructure, des applications et du contenu vous permettent de détecter les menaces multi-vecteurs et d'automatiser les mesures de défense.
- **Un filtrage des URL selon la réputation et la catégorie :** ce filtrage constitue un vaste système de contrôle et d'alerte sur le trafic web suspect. Il assure le respect des politiques sur des centaines de millions d'URL dans plus de 80 catégories.
- **Une protection avancée contre les programmes malveillants :** une détection efficace des failles avec un faible coût d'acquisition total offre certainement une protection interessante. Une simple

licence logicielle vous permet de détecter, comprendre et arrêter les programmes malveillants et les menaces émergentes.

Utilisation du réseau comme sonde de détection et protection

Cisco utilise le réseau pour appliquer dynamiquement la politique de sécurité avec une segmentation définie par logiciel, conçue pour réduire la surface d'attaque totale, contenir les attaques en empêchant le déplacement latéral su le réseau et minimiser la durée nécessaire à l'isolation des menaces après leur détection.

Les solutions de Cisco permettent au réseau de se comporter comme un capteur et un actionneur. Les solutions Identity Services Engine (ISE) avec TrustSec et Stealthwatch simplifient le provisionnement et la gestion de l'accès réseau sécurisé, confèrent une plus grande visibilité de l'activité réseau anormale, accélèrent les activités de sécurité et assurent le respect constant de la politique sur l'ensemble du réseau. Contrairement aux mécanismes de contrôle d'accès, qui s'appuient sur la topologie du réseau, les contrôles Cisco TrustSec sont définis à l'aide de groupements logiques des politiques. La segmentation des ressources et l'accès sécurisé sont ainsi systématiquement assurés, même si les ressources se déplacent sur des réseaux mobiles et virtualisés. Et quelles sont les conséquences ? L'application des politiques TrustSec peut empêcher la propagation d'une attaque de ransomware à tout votre réseau.

RAPPEL

Les fonctionnalités de Cisco TrustSec sont intégrées dans les produits de commutation, de routage, de LAN sans fil (WLAN) et de pare-feu Cisco pour protéger les actifs et les applications sur les réseaux des entreprises et des centres de données.

Les méthodes traditionnelles de contrôle d'accès segmentent et protègent les actifs en utilisant des réseaux virtuels (VLAN) et des listes de contrôle d'accès (ACL). À la place, Cisco TrustSec utilise des politiques de groupes de sécurité, qui sont rédigées dans une matrice en langage clair et dissociée des adresses IP et des VLANs. Les utilisateurs et les ressources ayant la même classification des rôles sont assignés à un groupe de sécurité.

Les politiques de Cisco TrustSec sont créées au niveau central et automatiquement distribuées vers les réseaux filaires, sans fil et VPN. Ainsi, les utilisateurs et les ressources bénéficient d'une protection et d'un accès cohérents alors qu'ils se déplacent sur les réseaux mobiles et virtuels. La segmentation définie par logiciel permet de réduire le temps consacré aux tâches d'ingénierie du réseau et à la validation de la conformité.

Rationalisation des déploiements et soutien de la réponse aux incidents

Les services Cisco de conseil en sécurité comprennent des services de déploiement pour les solutions Cisco de défense contre les ransomwares, y compris Firepower et AMP, ainsi qu'une solution de réponse aux incidents.

L'équipe de réponse aux incidents des services de sécurité Cisco peut assurer :

- Des services d'aide proactifs de réponse aux incidents pour aider votre organisation à développer et/ou à évaluer ses capacités de réponse aux incidents
- Une intervention réactive dans le cas d'une attaque de ransomware ou d'autres incidents de sécurité

De plus, les services Cisco d'intégration de la sécurité relèvent les défis architecturaux au niveau de la solution. Ils rationalisent le déploiement des solutions telles qu'Advanced Malware Protection (AMP) for Endpoints et les pare-feux de nouvelle génération Cisco Firepower (NGFW).

UN CHEF DE FILE DE LA LOGISTIQUE IMMOBILIÈRE RENFORCE SA SÉCURITÉ ET SES PERFORMANCES AVEC CISCO

Le défi : élaboration d'un système de défense en profondeur

Prologis, Inc., leader mondial en logistique immobilière, loue des installations de distribution modernes à un large éventail d'environ 5 200 clients, selon deux grandes catégories : services aux entreprises (B2B) et commerce de détail/exécution en ligne. Présente dans 20 pays, cette entreprise possède plus de 60 bureaux sur quatre continents. Cotée à la bourse de New York sous le symbole PLD, l'entreprise Prologis est inscrite sur la liste des entreprises les plus admirées du monde et appartient au Top 100 des entreprises les plus durables.

« En tant qu'acteur mondial, nous devons travailler partout, et notre réussite globale nous impose une forte dépendance vis-à-vis du cloud », déclare l'architecte des solutions de sécurité de Prologis, Tyler

(à suivre)

(suite)

Warren. « Étant donné que la majeure partie de l'infrastructure informatique de Prologis est installée dans le cloud, nous ne possédons pas une infrastructure ou un périmètre classique ; la recherche de solutions de sécurité adaptées devient donc difficile. »

En tant qu'entreprise privée d'envergure mondiale orientée cloud, Prologis doit protéger l'intégrité de ses systèmes, et la mission de M. Warren consiste à étoffer la pile de sécurité.

« Avec la multiplication des menaces, nous avons compris que Prologis devait fortifier ses plans de sécurité existants afin de protéger son réseau et ses utilisateurs en ligne et hors-ligne contre les activités malveillantes, comme les connexions de type contrôle & commande, les programmes malveillants et le phishing », poursuit-il. « Un modèle de sécurité en couche nous convenait car aucun élément de sécurité n'est suffisamment solide à lui seul pour tout intercepter. »

La solution : une sécurité renforcée, adaptée à nos besoins et au personnel

« Le développement de notre pile de sécurité a pris du temps. Nous voulions des éléments compatibles et parfaitement intégrables, sans aucune répercussion pour les utilisateurs. Et M. Warren précise : « ils devaient nous protéger là où nous travaillons : partout dans le monde et dans le cloud. »

La petite liste de blocage établie par Prologis sur les types très spécifiques de contenu inadmissible nécessitait un filtrage web, qui était géré à l'origine par un autre fournisseur. Selon M. Warren, « la liste était difficile à gérer, et surtout, elle ne répondait pas à l'objectif de l'entreprise de tout transférer vers le cloud. »

« Nous avions besoin d'une couche de sécurité nous permettant de lutter contre certains problèmes de sécurité liés à l'utilisation d'Internet par les employés, et nous devions également renforcer notre filtrage des sites web », précise-t-il. « Nous avons apprécié le fait qu'Umbrella soit la première couche pour contrer les activités malveillantes. »

Dans sa quête pour répondre à ces besoins, Prologis a exécuté des essais de validation avec trois autres fournisseurs et Cisco. Après avoir éliminé les autres fournisseurs en raison de différents facteurs, notamment les exigences matérielles, la complexité, la configuration complexe et le prix, Prologis a choisi Cisco Umbrella.

« Umbrella répond à tous nos besoins », déclare M. Warren. « Cette solution répond à nos besoins de sécurité spécifiques, s'occupe du filtrage des sites web et couvre nos utilisateurs distants ; tout cela dans une seule solution de type cloud facile à déployer. »

Le résultat : une application des politiques, accompagnée de gains de performance stupéfiants

« Les résultats ne se sont pas fait attendre », précise Warren. « La capacité d'appliquer les politiques partout et systématiquement (y compris sur des appareils hors réseau) est essentielle pour Prologis », ajoute-t-il. « La mise en place du client d'itinérance d'Umbrella a été si transparente que personne n'est conscient de son activation. »

Quant au blocage des activités et sites web malveillants, « au cours des six derniers mois, nous avons eu seulement quatre à cinq faux positifs, et ils provenaient tous de sites non américains. Ce chiffre est incroyable ; moins d'un par mois, c'est vraiment exceptionnel. »

M. Warren souligne également un autre résultat positif avec l'augmentation substantielle des performances. « Après l'installation d'Umbrella, nous avons constaté une amélioration colossale des performances. En Chine et au Japon, les temps de réponse des applications ont diminué de 50 %. Dans notre bureau de Denver, le temps de téléchargement d'un fichier de 10 Mo depuis le cloud est passé de 11,4 secondes avant le déploiement à 4,4 secondes après. Étant donné que la majeure partie des applications utilisées par Prologis sont dans le cloud, les performances sont extrêmement importantes pour nous. 100 % des applications que nous utilisons ont gagné en performance. »

D'autres fonctionnalités d'Umbrella se sont avérées également utiles. « La génération automatique de rapports est inestimable (en particulier, le rapport sur les services du cloud) car je peux partager des données claires et assimilables sur le bon niveau de protection du réseau et le volume d'informatique clandestine (*Shadow IT*) qui se produit dans le cloud, ce qui m'a vraiment ouvert les yeux », précise Warren. « Ces rapports me facilitent la vie en me permettant d'identifier tous les problèmes, et améliorent également la vie de nombreuses personnes en soulignant l'utilité de notre infrastructure de sécurité de défense en profondeur.

L'ajout d'Umbrella à notre pile de sécurité a été une excellente décision. Tout le monde se réjouit de l'amélioration de la sécurité et des performances suite au déploiement d'Umbrella. »

DANS CE CHAPITRE

- Comprendre les défis de la défense contre les ransomwares
- Construire et déployer un environnement fondamentalement sécurisé
- Choisir la simplicité
- Automatiser les tâches pour garder une longueur d'avance sur les menaces en constante évolution

Chapitre 5
Dix conseils importants à retenir pour se défendre contre les ransomwares

Dans ce chapitre, je couvre certains des points importants qu'il est utile de garder en mémoire pour se défendre efficacement contre les ransomwares !

Le ransomware évolue

Aujourd'hui, le ransomware est le programme malveillant qui connaît la plus forte croissance et l'évolution la plus rapide. CryptoWall, l'une des campagnes de ransomware actuelles les plus lucratives et répandues de l'Internet a été lancée en 2014 et a infecté des milliards de fichiers dans le monde. Depuis cette époque, trois nouvelles variantes de CryptoWall ont été développées, chacune étant plus sophistiquée que la précédente.

Le rythme de l'évolution s'accélère également. Au cours des trois dernières années, le nombre de campagnes originales de ransomwares et de variantes a souvent largement dépassé le nombre total de campagnes et de variantes de ransomwares des 25 années précédentes, depuis la toute première campagne de ransomware (PC Cyborg) en 1989. Le nombre de

variantes de programmes malveillants découvertes au cours du premier trimestre 2016 correspond à la moitié du nombre total de l'année 2015, et il est presque deux fois plus élevé que le nombre total de 2014.

Plusieurs facteurs ont contribué à la croissance et à l'évolution rapides des ransomwares, notamment l'omniprésence des téléphones Android (qui sont devenus un vecteur d'attaque populaire), la progression du bitcoin (qui facilite les paiements presque indétectables des rançons aux cybercriminels) et l'émergence du Raas (le ransomware en tant que service ; voir la section suivante) qui permet à tout un chacun ou presque d'avoir recours au ransomware.

Le ransomware «as a service», une menace émergente

Cette nouvelle menace qu'est le RaaS permet littéralement à toute personne possédant des compétences techniques limitées de devenir un cybercriminel. L'une des premières offres de RaaS connues, Tox, découverte en mai 2015, peut être téléchargée depuis le dark web avec un navigateur Tor et configurée comme suit :

1. Saisissez le montant de la rançon.
2. Créez une demande de rançon.
3. Saisissez un CAPTCHA afin que les créateurs de Tox sachent que vous n'êtes pas un robot.

Le logiciel RaaS peut en général être téléchargé gratuitement ou à un prix réduit. Le véritable profit des créateurs du logiciel RaaS provient de la part qu'ils prélèvent sur les rançons collectées, en général 5 à 30 pour cent.

Le paiement de la rançon ne résout pas les problèmes de sécurité

Pour la plupart des victimes de ransomwares, la méthode de règlement la plus rapide et la plus facile consiste à payer simplement la rançon. Cependant, le paiement de la rançon ne résout pas nécessairement vos problèmes, même si vous pouvez récupérer l'accès à vos fichiers.

Dans la plupart des cas, vos fichiers seront décryptés si vous payez la rançon, mais vous n'avez aucune garantie. Bien qu'il soit dans l'intérêt des cybercriminels de restaurer vos fichiers si vous payez la rançon (si une campagne de ransomware est connue pour ne pas décrypter les

fichiers après le paiement de la rançon, les futures victimes n'auront aucune raison de payer), les voleurs n'ont aucune parole. C'est en particulier vrai avec l'émergence du RaaS (abordé dans la section précédente) car un cybercriminel « débutant » pourrait ne pas apprécier la situation dans son ensemble. Si la clé de cryptage ne fonctionne pas pour une raison ou une autre, vous ne pouvez pas appeler le service clients !

Vous ne pouvez pas non plus être certain que le criminel n'a pas installé un autre programme malveillant ou un exploit kit pour faciliter de futures cyberattaques contre votre organisation. Une copie de vos fichiers peut également avoir été exfiltrée pour d'autres raisons, comme la vente des informations sensibles de votre organisation sur le dark web.

Le paiement de la rançon finance directement et perpétue les futurs cybercrimes. La situation est la même que le paiement d'une rançon à des terroristes ou à des États-nations dits voyous en échange d'otages. Cela encourage, incite et finance de futurs comportements similaires.

Enfin, le paiement d'une rançon n'enlève rien au fait qu'une violation importante de la sécurité a eu lieu au sein de votre organisation. En fonction de la nature, de l'étendue et des circonstances de la faille, ainsi que des règlements sectoriels et des juridictions légales auxquels votre organisation est soumise, l'annonce publique d'une violation peut être obligatoire, et des amendes et sanctions pourraient pleuvoir sur votre organisation ; une sacrée claque après avoir payé une rançon !

ASTUCE

Afin d'atténuer les dommages potentiels d'une attaque par ransomware, les organisations devraient toujours veiller à effectuer des sauvegardes périodiques et validées de tous les fichiers importants et des images actuelles de tous les systèmes critiques.

Bâtir une architecture de sécurité en couche reposant sur des normes ouvertes

Des normes ouvertes et extensibles permettent de créer une nouvelle architecture de pointe qui intègre facilement les technologies de sécurité existantes et nouvelles au sein d'une solution de sécurité complète.

Déployer de meilleures solutions intégrées

L'industrie a depuis longtemps adopté la défense en profondeur comme pratique exemplaire. Malheureusement, jusqu'ici la défense en profondeur a obligé les organisations à déployer des produits de sécurité autonomes (ou ponctuels) qui ne s'intègrent pas facilement avec les autres solutions de sécurité dans l'environnement.

Avec une nouvelle architecture « best of breed » de sécurité, les organisations peuvent déployer un portefeuille de solutions qui s'intègrent les unes aux autres ce qui réduit la complexité au sein de leur environnement de sécurité et améliore leur stratégie de sécurité globale.

La sécurité grâce au réseau

La sécurité doit être inhérente et omniprésente dans l'ensemble de l'environnement informatique de votre organisation, y compris sur le réseau, dans le centre de données, sur les terminaux et dispositifs mobiles, et dans le cloud.

Réduire la complexité de votre sécurité

Les technologies de sécurité doivent être simples à déployer et à utiliser. La complexité introduit un risque en raison de la possibilité d'erreurs et de configurations inadéquates, et peut éventuellement occulter des indicateurs de compromission (IoC) importants et d'autres points de données dans des journaux lourds et détaillés. Pour établir un plan de sécurité intégré et éviter une complexité inutile, n'hésitez pas à vous appuyer sur des services de sécurité tiers et à exploiter leur vaste expérience pour compléter vos propres connaissances et votre compréhension approfondies de l'environnement de votre organisation et de la nature des menaces.

Exploiter des services en temps réel et en Cloud de renseignements sur les menaces

Les ransomwares et autres menaces de cybersécurité évoluent rapidement. Les attaques « zero-day » représentent la plus grande menace pour la plupart des organisations. Les renseignement temps réel sur les menaces basés sur le cloud permettent aux équipes informatiques de déployer le plus rapidement possible les toutes dernières contremesures lorsque de nouvelles menaces émergent, et d'exploiter une expertise en sécurité qui dépasse largement leur organisation.

Automatiser les réactions de sécurité pour raccourcir le temps de réponse

Dès que possible, les réactions de sécurité doivent être automatisées afin de contrer les menaces susceptibles de se répandre en quelques minutes ou secondes sur l'ensemble du réseau d'une entreprise.

Voici quelques exemples de mesures de sécurité qui peuvent être automatisées :

- Distribution et installation de fichiers de signatures d'un système de prévention d'intrusion (IPS) et de solutions anti-programmes malveillants.
- Collecte, corrélation et analyse centralisées de journaux de sécurité et de données sur les menaces
- Protection contre les menaces capables de bloquer les requêtes vers des destinations malveillantes avant même qu'une connexion ne soit établie quelque soit le port utilisé et d'arrêter les menaces avant qu'elles n'atteignent votre réseau ou vos terminaux
- Listes de contrôle d'accès (ACL) dynamiques, listes noires/blanches de domaines et de sites web, et création de règles pour les pare-feux
- Provisionnement/déprovisionnement de compte et gestion des droits d'accès

Si vous voyez quelque chose, dites-le

Le FBI encourage fortement les victimes de ransomwares à signaler les attaques afin de bénéficier d'une vision plus large de l'étendue et de l'impact de ces infections. Selon le FBI, il est difficile de « connaître le nombre réel des victimes de ransomwares car de nombreuses infections ne sont pas signalées. »

Le FBI s'inquiète que les victimes ne portent pas plainte. L'une des principales raisons est que les victimes n'en voient pas l'intérêt, en particulier si elles ont résolu le problème en payant la rançon ou en nettoyant leurs systèmes.

RAPPEL

Le FBI préconise de ne pas payer la rançon. « Le paiement d'une rançon ne garantit pas à la victime qu'elle récupérera un accès à ses données », selon le FBI. « En fait, certaines personnes ou organisations n'obtiennent jamais les clés de décryptage après le paiement d'une rançon. Le paiement de la rançon encourage l'adversaire à cibler d'autres victimes pour gagner de l'argent, et pourrait inciter d'autres criminels à tirer profit d'activités illicites similaires. »

ASTUCE

Pour signaler une infection aux autorités françaises, fournissez les informations suivantes sur le site `https://www.ssi.gouv.fr/en-cas-dincident/`

- Date de l'infection et informations sur l'entreprise victime (comme le type d'industrie et la taille de l'entreprise)
- Variante du ransomware (identifiée sur la page de la rançon ou l'extension du fichier crypté)
- La manière dont l'infection s'est produite (par exemple, un lien dans un courriel, en naviguant sur Internet)
- Rançon demandée et montant payé (le cas échéant)
- Adresse du portefeuille de bitcoins du pirate (peut être affichée sur la page de la rançon)
- Pertes totales associées à l'infection par ransomware (y compris, le montant de la rançon et les répercussions du crime déclarées)

Ne laissez pas un ransomware prendre vos fichiers en otage !

Le ransomware est une menace qui évolue rapidement, qui va pesé plus d'un milliard de dollars en 2016 et pour laquelle on voit une progression annuelle substantielle. Pire encore, les victimes qui payent les rançons (de quelques centaines à plusieurs dizaines de milliers de dollars) financent directement les prochaines générations de ransomwares !

Avec ce livre, apprenez à défendre votre organisation contre les ransomwares et autres menaces.

À l'intérieur…

- Interceptez le ransomware avant qu'il n'atteigne votre réseau
- Installez une protection avancée sur vos terminaux et passerelles de messagerie contre les programmes malveillants
- Bloquez les connexions au serveur de contrôle-commande (C&C) des ransomwares
- Simplifiez les activités de sécurité

Lawrence Miller, CISSP
travaille depuis plus de 25 ans dans le domaine de la sécurité informatique pour différentes industries. Il a co-écrit *CISSP pour les nuls* et plus de 90 autres livres *Pour les nuls* portant sur diverses questions de sécurité et de technologie.

Allez sur Dummies.com®
pour voir des vidéos, des exemples pas à pas, des articles pratiques, ou pour faire des achats !

for dummies®
A Wiley Brand

ISBN: 978-1-119-37961-4

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.