RAPPORT 2016 SUR LES MENACES

Avancez sans crainte

Présenté par

FORCEPOINT Security Labs™

FORCEPOINT
POWERED BY Raytheon

SOMMAIRE

SYNTHÈSE **02**

RAPPORT PRINCIPAL **06**

MENACES INTERNES 06

MENACES AVANCÉES :
ÉTUDES DE CAS DE LA CELLULE SI
(« SPECIAL INVESTIGATIONS ») 10

WEB ET MESSAGERIE ÉLECTRONIQUE :
UNE DOUBLE MENACE 20

L'ADOPTION DU CLOUD 22

AVIS D'EXPERTS RSSI 25

CONCLUSION **29**

SYNTHÈSE

En l'espace d'un an, la nature des cyberattaques a profondément change. Alors que les logiciels malveillants s'efforcent toujours à subtiliser furivement des données, c'est l'autonomie de l'employé moderne qui pourrait bien représenter la plus grande menace en matière de vol d'informations. Les ransomware font l'affaire d'une nouvelle génération qui délaisse la furtivité pour mieux clamer qu'un pirate a crypté vos données et vous les échangera contre une rançon Le profit est immédiat. Face aux innovations anti-malware, les pirates recyclent de vieilles méthodes : ils s'appuient sur des fichiers Microsoft® Office chargés de macros, lesquels atterrissent sur votre poste de travail. La migration croissante vers le cloud est accompagné de nouveaux défis en matière de sécurité. En parallèle, de nouveaux botnets mettent à l'épreuve la capacité du secteur de la sécurité à détecter et à intercepter les objectifs tactiques et stratégiques de ses adversaires.

Ainsi, il est essentiel d'informer au plus vite les décisionnaires du contexte délicat qui entoure ces attaques, qu'elles aient lieu dans le monde ou au sein-même de leurs réseaux, pour qu'une majorité du temps et des ressources soit affectée à la lutte contre les menaces les plus graves. Fidèles à leur slogan « Avancez sans crainte », les équipes de Forcepoint Security Labs, Special Investigations (SI) et Experts RSSI trient et analysent la multitude d'informations générées par les attaques du monde entier, et identifient les menaces et les innovations les plus importantes dans le but de mieux vous guider.

Le **rapport Forcepoint 2016 sur les menaces** constitue une analyse complète des menaces informatiques modernes présentant des risques significatifs pour les aspects techniques, opérationnels et financiers des entreprises touchées. À la fin de chaque section de ce rapport les conseils prodigués par l'équipe de Forcepoint Security Labs vous aideront à mieux combattre les menaces évoquées. Le contenu des chapitres :

1. MENACES INTERNES : PAR MALVEILLANCE OU PAR INADVERTENCE

Des recherches réalisées par Forcepoint ainsi que par des tiers (page 5) indiquent que la surveillance des activités internes et la justification des accès privilégiés sont les problèmes de sécurité que les entreprises sont le moins préparées à affronter. En effet, 30 % des capacités de sécurité restent affectées à la défense du périmètre[1], tandis que moins de 40 % des entreprises interrogées disposent d'un budget dédié à la défense contre les menaces internes[2]. Pourtant, de nombreux employés sont habilités à se connecter à distance et accèdent par intermittence aux serveurs contenant vos données les plus sensibles.

2. MENACES AVANCÉES ET ÉTUDES DE CAS MENÉES PAR LA CELLULE SI : PRÉSENTATION DE JAKU ET ANALYSE DES RANSOMWARE

L'équipe Special Investigations de Forcepoint nous offre un regard sur les menaces avancées. Ce groupe d'élite composé de chercheurs et d'experts affectés aux recherches sur les cyber-menaces et à la réaction en cas d'incident se spécialise dans les menaces s'appuyant sur des outils, tactiques et processus uniques. L'an dernier, SI a notamment découvert un nouveau réseau zombie surnommé JAKU et a craqué une souche persistante de ransomware connue sous le nom de Locky.

3. WEB ET MESSAGERIE ÉLECTRONIQUE : UNE DOUBLE MENACE

Même dans les entreprises les plus à cheval sur la sécurité, la productivité des employés dépend bien souvent d'Internet et de la messagerie électronique, qui sont donc une porte ouverte aux contenus malveillants, envoyés sous forme de pièces jointes ou de liens redirigeant vers des sites Internet qui contiennent des logiciels malveillants. Environ 92 % des courriels non sollicités (par ex. spam, courriel malveillant) contiennent une URL. En outre, la présence de macros malveillantes dans les courriels est en augmentation de 44,7 % (page 20).

4. LES PRÉOCCUPATIONS CONCERNANT LA SÉCURITÉ RESTENT UN OBSTACLE À L'ADOPTION DU CLOUD

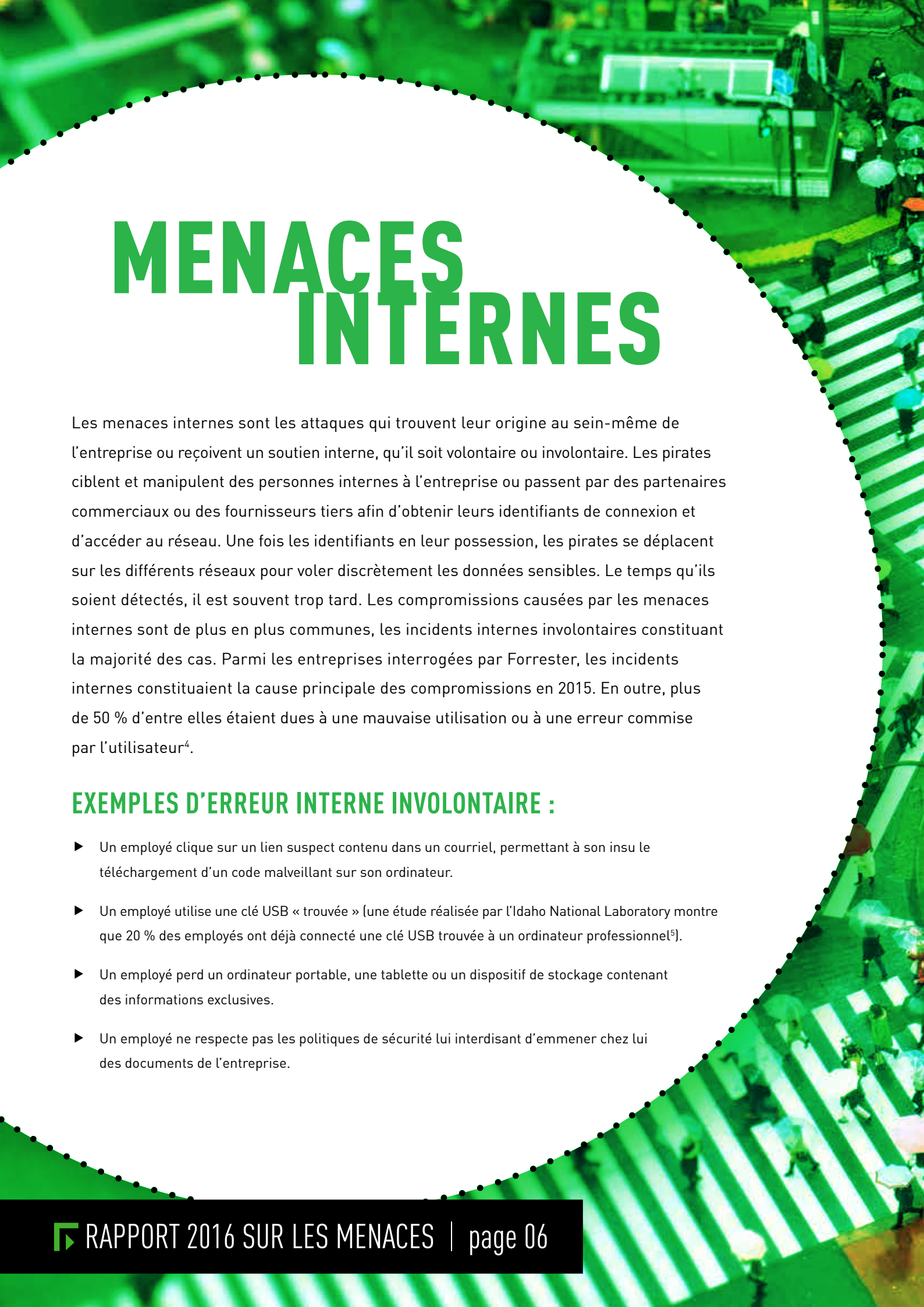
Pour de nombreuses entreprises, le coût, l'accessibilité et la capacité de changement d'échelle offerts par le cloud contrebalancent les risques de sécurité. Ces risques sont néanmoins une source de préoccupations pour bien des prospects, qui redoutent l'effet de l'incompatibilité des contrôles de sécurité réalisés par les fournisseurs avec leur propre environnement Paradoxalement, les DSI et les RSSI les plus réticents à adopter le cloud doivent corriger les conséquences des incidents causés par des employés qui décident d'utiliser des applications cloud de leur propre chef. Si elles peuvent leur apporter un gain de productivité ou de commodité, elles présentent également un risque important. Ainsi, plus de 80 % des décisionnaires interrogés pensent que le Shadow IT a des conséquences graves[3].

5. AVIS DES RSSI DE FORCEPOINT

En 2015, l'équipe RSSI de Forcepoint a identifié les fusions et acquisitions comme étant l'un des vecteurs de risque les plus importants en matière de cybersécurité, tous secteurs confondus. Les RSSI puisent ainsi dans l'expertise de ses spécialistes en cybersécurité et en protection de données pour résumer la façon dont des contrôles de sécurité exhaustifs ont été effectués pendant la fusion-acquisition qui a donné naissance à Forcepoint. Celle-ci consiste en l'intégration de Websense® et Raytheon Cyber Products (RCP), ainsi que de Stonesoft® NGFW (pare-feux de nouvelle génération).

LA FORMATION DE FORCEPOINT

Forcepoint, une jeune entreprise qui adopte une approche neuve de la cybersécurité, a été présentée le 14 janvier 2016. Cette joint venture de Raytheon Company et Vista Equity Partners associe trois entreprises performantes : Websense, Raytheon Cyber Products et Stonesoft, chacune d'entre elles dotée d'une riche histoire d'innovation. Grâce à son accès constant aux ressources, à la propriété intellectuelle et à l'expertise de Raytheon, Forcepoint dispose d'un véritable atout pour assurer la sécurité des clients, même face aux problèmes les plus compliqués. Au fil de ce rapport, nous mettrons en évidence les avantages que Forcepoint tire du soutien apporté par Raytheon, permettant à nos clients de jouir d'une supériorité cruciale et inégalée dans le monde exigeant de l'informatique moderne.



MENACES INTERNES

Les menaces internes sont les attaques qui trouvent leur origine au sein-même de l'entreprise ou reçoivent un soutien interne, qu'il soit volontaire ou involontaire. Les pirates ciblent et manipulent des personnes internes à l'entreprise ou passent par des partenaires commerciaux ou des fournisseurs tiers afin d'obtenir leurs identifiants de connexion et d'accéder au réseau. Une fois les identifiants en leur possession, les pirates se déplacent sur les différents réseaux pour voler discrètement les données sensibles. Le temps qu'ils soient détectés, il est souvent trop tard. Les compromissions causées par les menaces internes sont de plus en plus communes, les incidents internes involontaires constituant la majorité des cas. Parmi les entreprises interrogées par Forrester, les incidents internes constituaient la cause principale des compromissions en 2015. En outre, plus de 50 % d'entre elles étaient dues à une mauvaise utilisation ou à une erreur commise par l'utilisateur[4].

EXEMPLES D'ERREUR INTERNE INVOLONTAIRE :

- Un employé clique sur un lien suspect contenu dans un courriel, permettant à son insu le téléchargement d'un code malveillant sur son ordinateur.
- Un employé utilise une clé USB « trouvée » (une étude réalisée par l'Idaho National Laboratory montre que 20 % des employés ont déjà connecté une clé USB trouvée à un ordinateur professionnel[5]).
- Un employé perd un ordinateur portable, une tablette ou un dispositif de stockage contenant des informations exclusives.
- Un employé ne respecte pas les politiques de sécurité lui interdisant d'emmener chez lui des documents de l'entreprise.

DES MÉTHODES DE TEST UNIQUES AU MONDE

Chez Raytheon, l'équipe de chercheurs dédiée à la sécurité s'appuie sur les technologies les plus récentes pour évaluer les vulnérabilités, réduire l'exposition aux risques et maximiser l'efficacité de la sécurité. Celles-ci comprennent notamment des centaines de millions de tests effectués chaque semaine, une analyse logicielle statique et dynamique, des engagements coopératifs et non coopératifs, ainsi que l'émulation réseau de plus de 100 000 terminaux et processus. C'est ainsi que nous pouvons transformer les indicateurs de menace en mesures défensives.

D'après des recherches initiées par Forcepoint auprès du Ponemon Institute[6], les employés représentent la plus grave menace pour la sécurité d'une entreprise, principalement de par la difficulté de détection des abus en interne. Par exemple, les identifiants volés liés à des comptes valides sont souvent utilisés pour atteindre des données sensibles auxquelles l'utilisateur légitime a normalement accès, ce qui évite d'éveiller tout soupçon. Cet état de fait a connu un écho dans une enquête[7] réalisée en mars 2016, qui a conclu que la détection d'activité malveillante en interne ou le piratage d'un compte doté de privilèges constituaient les événements pour lesquels les banques se considéraient le moins bien préparées. La popularité croissante des appareils personnels utilisés comme outils professionnels (concept du BYOD) ajoute à la complexité des menaces internes et crée de nombreux points d'entrée pour les pirates, qui peuvent alors s'introduire dans le réseau sans être repérés par l'équipe de sécurité. Par conséquent, les entreprises doivent trouver un équilibre entre l'accessibilité des données et le risque de les voir perdues ou utilisées à mauvais escient.

Bien souvent, le maillon menant à la perte accidentelle de données essentielles est l'utilisateur, qui en fait mauvais usage à cause de sa méconnaissance ou de sa négligence vis-à-vis des pratiques de sécurité.

Les erreurs et la négligence des employés comptent ainsi pour près de 15 % des compromissions de données survenues en 2015[8]

La raison en est évidente : à peine plus de la moitié du personnel connaît la politique de sécurité de l'entreprise[9].

Malgré l'ampleur des dégâts (notamment la perte d'identifiants de connexion, de propriété intellectuelle, de données financières d'entreprise et d'informations personnelles identifiables), les entreprises continuent à utiliser des méthodes de formation inefficaces et les employés ne savent toujours pas comment appliquer les bonnes pratiques de sécurité au travail[10]. Puisque les menaces internes constituent un danger si manifeste, pourquoi la défense du périmètre demeure-t-elle la priorité ?

Une étude récemment réalisée par Ponemon[11] nous apporte quelques éléments de réponse. Bien que le problème soit reconnu, moins de 40 % des entreprises interrogées disposent d'un budget dédié à un programme de lutte contre les menaces internes. Ces entreprises invoquent le manque d'informations contextuelles et de visibilité ainsi qu'une pléthore de faux positifs pour justifier leur utilisation d'outils inadaptés à la résolution du problème. Des technologies plus sophistiquées sont désormais capables de déterminer si une menace vient véritablement de l'intérieur ou si elle est le fait d'un pirate utilisant des identifiants volés. Ces technologies associent prévention contre la perte de données (DLP) et analyse du comportement des utilisateurs, qu'elles corrèlent avec d'autres activités informatiques et des systèmes commerciaux (par ex. journaux d'accès RFID et d'enregistrements IP).

Les menaces internes ne sont toutefois pas qu'un problème informatique. Elles concernent en effet tout le personnel. Un programme efficace de gestion des menaces internes est doté de contrôles technologiques assortis de plans de gestion des risques, ainsi que d'une formation enseignant les bonnes pratiques aux employés. Parmi les composantes clés d'un tel programme on retrouve les éléments suivants :

- **Politiques :** Communiquer les politiques détaillant les méthodes d'utilisation des technologies au sein de l'organisation, des appareils adaptés à la manipulation des données, en passant par l'utilisation d'Internet.
- **Processus :** Séparer correctement les tâches et les points de contrôle au sein des processus.
- **Contrôles technologiques :** Limiter l'accès selon le principe du moindre privilège, en fonction du rôle assigné à chaque personne.
- **Gestion des risques :** Mettre au point un plan de gestion des risques pour donner une priorité absolue aux domaines présentant le plus de risques.
- **Audit et surveillance :** Vérifier que tous les composants clés sont efficaces et répondent aux besoins de l'entreprise.

ÉTUDE DE CAS SUR LES MENACES INTERNES : LES DONNÉES FACE AUX SUPPRESSIONS DE POSTES

Selon une enquête sur la sécurité réalisée par Forrester[13], 39 % des compromissions survenues au cours des 12 derniers mois sont le résultat d'un incident interne. Vingt-six pour cent de ces compromissions sont dues à des abus délibérés ou à des opérations malveillantes, tandis que 56 % d'entre elles sont dues à un mauvais usage accidentel des données (18 % des compromissions relèvent des deux catégories).

L'étude de cas suivante, réalisée par Forcepoint et partagée pour la première fois, présente un scénario typique de menace interne. À la suite d'une fusion-acquisition, un client décide de réduire l'effectif du service d'ingénierie logicielle. Les employés sont avertis de l'imminence des licenciements. Certains ont lieu immédiatement, d'autres sont prévus après la finalisation des projets actuels. La propriété intellectuelle et les actifs de l'entreprise doivent être protégés en échange d'une indemnité de licenciement généreuse (comprenant une année de salaire). Malgré cela, de nombreux ingénieurs retournent à leur bureau pour tenter de voler des données confidentielles. S'étant préparée pour ce cas de figure, l'entreprise utilise SureView® Insider Threat de Forcepoint pour observer les comportements à risque des employés (lesquels sont comparés à un historique sur 30 jours de leurs comportements habituels). En conséquence, les opérations inhabituelles (par ex. tenter de copier et d'enregistrer des fichiers sur un périphérique de stockage USB ou d'envoyer des fichiers ou du code source par courriel ou vers le cloud via Internet) sont signalées immédiatement par la technologie de Forcepoint. SureView Insider Threat peut ainsi arrêter les compromissions et, plus important encore, l'entreprise est capable de protéger les éléments les plus précieux de sa propriété intellectuelle en identifiant les employés qui enfreignent l'accord de licenciement. Bien que cette étude de cas illustre une situation où la fuite d'informations est le fait d'un acte malveillant, un employé pourrait aussi bien déclencher les mêmes alarmes par inadvertance, par exemple en se faisant voler ses identifiants ou pirater son ordinateur, ce qui entraînerait des mouvements sur le réseau, des connexions après les heures de travail ou des transferts de données inhabituels.

CONSEILS FORCEPOINT

1. Identifiez les risques spécifiques à votre activité ainsi que leur cause. Mettez en place sans attendre une norme de référence pour le comportement des utilisateurs. Comprendre la façon dont les utilisateurs se comportent habituellement est nécessaire à la détection d'anomalies pouvant indiquer une menace interne.

2. Autonomisez les utilisateurs en abordant les risques de façon proactive grâce à des programmes de formation et de sensibilisation.

3. Élaborez un plan de réaction aux incidents internes doté de processus formels destinés à l'identification, la communication et la remontée hiérarchique des incidents internes.

4. Envisagez d'investir dans des solutions proposant une analyse comportementale sophistiquée et un suivi sur la durée afin d'identifier rapidement les comportements pouvant indiquer ou causer une faille de sécurité. En identifiant les utilisateurs à risque le plus tôt possible, il est possible d'arrêter les compromissions rapidement, voire avant même qu'elles ne se produisent.

MENACES AVANCÉES

ÉTUDES DE CAS

Étant donné l'augmentation spectaculaire de l'ampleur et de la complexité de l'informatique, la vision actuelle de ce qu'est une « menace avancée » sera bientôt obsolète. Les entreprises font désormais face à des « menaces collectives » aux capacités étendues du fait de la dissolution des périmètres traditionnels et de la dissémination des données sur divers terminaux, réseaux, appareils mobiles, ainsi que dans le cloud. Cette nouvelle complexité exige d'adopter des approches novatrices et souligne l'avantage que présentent les solutions intégrées capables de partager les renseignements sur les menaces et de réduire la durée de compromission[14].

La durée de compromission commence lorsqu'un pirate pénètre dans le réseau et continue jusqu'à ce qu'il en parte ou en soit délogé. Face à une durée de compromission minimale, le pirate n'a pas loisir d'effectuer son parcours latéral pour dérober des données critiques.

C'est sur ce nouveau genre d'attaque avancée que l'équipe Special Investigations (SI) de Forcepoint se concentre. Elle intervient lorsqu'un exploit comporte des outils, tactiques et processus anormaux. L'équipe SI dispose de compétences et de connaissances en rétro-ingénierie, en analyse d'attaque avancée et en neutralisation des logiciels malveillants évasifs, dont elle fait bénéficier les autorités.

Elle définit également des points de référence dans les données des attaques connues, puis approfondit son enquête pour mieux comprendre et affronter les techniques mises en œuvre par les nouveaux outils, tactiques et processus. Cette méthode a permis d'analyser JAKU, une attaque globale via réseau zombie récemment identifiée et décrite ici pour la première fois.

PRÉSENTATION DE JAKU

JAKU est une attaque globale via réseau zombie toujours en cours. Elle illustre la réutilisation de l'infrastructure et des outils, tactiques et processus, et présente une sorte de dédoublement de la personnalité. JAKU infecte des victimes en masse, puis mène des attaques ciblées sur des victimes sélectionnés grâce à la mise en œuvre parallèle de campagnes opérationnelles. S'ensuit une fuite d'informations machine, le profilage des utilisateurs finaux et leur incorporation dans d'autres bases de données d'attaques.

Au terme d'une enquête longue de six mois, Forcepoint Security Labs a pu localiser précisément les serveurs de commande ainsi que les victimes, dans le monde entier. À l'aide d'une analyse statique et comportementale, l'équipe Forcepoint Security Labs a réussi à comprendre la composition de l'attaque et le mécanisme de suivi utilisé par ce réseau zombie. Au cours de ses recherches et de l'enquête, elle a établi une coordination avec les autorités policières et est aujourd'hui en mesure de rendre publiques ses conclusions. Les clients de Forcepoint étaient protégés des menaces présentées par JAKU avant même l'ouverture de l'enquête, en octobre 2015.

« La grande originalité de JAKU tient à l'exécution parallèle de plusieurs opérations au sein d'une même campagne, qui utilise des outils, tactiques et processus quasi-identiques pour infecter des milliers d'ordinateurs, le tout dans le cadre d'une opération ciblée. »

– Dr. Richard Ford, Expert scientifique en chef chez Forcepoint, à propos de JAKU

TOP CINQ DES VICTIMES DE JAKU PAR PAYS

DURÉE DE COMPROMISSION MOYENNE : 93 JOURS

DURÉE DE COMPROMISSION MAXIMUM : 348 JOURS

JAKU

LES FAITS ET LES CHIFFRES

DURÉE DE L'ENQUÊTE À CE JOUR

6 MOIS

LOCALISATION DES VICTIMES :

MONDE ENTIER

(FORTE CONCENTRATION AU JAPON, EN CORÉE DU SUD ET EN CHINE)

CONTENU MALVEILLANT LIVRÉ PAR :

EXPOSITION À DES SITES BITTORRENT COMPROMIS, UTILISATION DE LOGICIELS SANS LICENCE ET TÉLÉCHARGEMENT DE LOGICIELS WAREZ

LOCALISATION DES SERVEURS DE COMMANDE ET CONTRÔLE :

MALAISIE, THAÏLANDE ET SINGAPOUR

TECHNIQUES D'ÉVASION UTILISÉES :

CRYPTOGRAPHIE, STÉGANOGRAPHIE, FAUX TYPES DE FICHIERS, INJECTION SILENCIEUSE, DÉTECTION DE MOTEUR ANTIVIRUS (ET AUTRES)

NOMBRE DE VICTIMES UNIQUES :

19 000

TYPE DE LOGICIEL MALVEILLANT :

SUIVI MULTI-ÉTAPES ET EXFILTRATION DE DONNÉES

NOMBRE DE PAYS AFFECTÉS PAR JAKU

134

FAQ SUR JAKU

Quand l'analyse technique complète de JAKU sera-t-elle rendue publique ?

Un rapport technique complet reprenant tous les indicateurs de compromission sera rendu public sur le blog Security Labs le 4 mai 2016.

Quels autres acteurs de la sécurité étaient impliqués dans la recherche ?

Forcepoint tient à reconnaître les travaux exhaustifs fournis par Kaspersky dans l'analyse de la campagne Dark Hotel, ainsi que la UK National Crime Agency (NCA), CERT-UK, Europol et Interpol, pour leur aide dans cette enquête. Pour qu'Internet devienne plus sûr, à la fois comme lieu de vie moderne et d'affaires, il est indispensable d'adopter une approche collaborative de la collecte et de l'analyse des informations.

CONSEILS FORCEPOINT

1. Mettez au point des processus pour réduire la durée de compromission potentielle[15].
2. Évitez d'entrer en contact avec les sites de torrents et les logiciels illégaux.
3. Surveillez les activités inhabituelles, comme le trafic envoyé depuis des serveurs de commande, reconnu par les dispositifs de renseignement sur les menaces.

UNE **FORCE** DONT IL FAUT TENIR COMPTE

« DeepRed » est une équipe composée d'ingénieurs de Raytheon et de spécialistes informatiques de Forcepoint. Dans le cadre du Cyber Grand Challenge organisé par la DARPA (Defense Advanced Research Projects Agency), elle s'attelle à créer un programme capable de détecter les failles de sécurité d'un logiciel et de les réparer quasi-instantanément. En août 2016, DeepRed participera à la célèbre convention du piratage informatique DEF CON organisée à Las Vegas, qui récompensera le gagnant par un prix de deux millions de dollars.

RIPOSTE CONTRE LES RANSOMWARE :
GROS PLAN SUR LOCKY

On parle de « ransomware » lorsque les logiciels malveillants cryptent vos fichiers puis vous proposent d'en acheter la clé de déchiffrement pour les récupérer. Si le propriétaire légitime des fichiers ne peut pas se permettre de les récupérer, ceux-ci sont tout simplement détruits.

L'année dernière, les ransomware sont malheureusement devenus monnaie courante. Depuis plusieurs années, Forcepoint Security Labs suit le développement des techniques utilisées par les pirates, qui envoient souvent les ransomware dans des pièces jointes ou via des publicités malveillantes.

Après avoir appris qu'un hôpital[16] a payé une rançon pour éviter le blocage complet du service, l'équipe SI a enquêté pour découvrir comment empêcher le cryptage des fichiers et comment partager ses découvertes avec le reste de la communauté.

FORCEPOINT DÉVERROUILLE LOCKY :
RÉTRO-INGÉNIERIE DE L'ALGORITHME DE GÉNÉRATION DE DOMAINE

Forcepoint a proposé à ses clients de les protéger contre l'appât servant à diffuser le contenu malveillant de Locky (un courriel contenant un fichier Microsoft Office doté d'une macro malveillante). Forcepoint Security Labs s'est également rendu compte qu'il était possible de désactiver le processus de cryptage des fichiers.

Locky utilise un cryptage AES 128 bits capable de crypter des bases de données SQL, du code source, des portefeuilles BitCoin, etc. L'analyse du contenu malveillant dans notre module Threat Protection Cloud (sandboxing comportemental des fichiers) a identifié un contact manifeste avec des serveurs de commande déjà connus.

Malheureusement, Locky s'appuie sur un algorithme de génération de domaines qui génère une série d'URL différentes sur la base d'un horodateur et d'une valeur initiale. Sans enquête approfondie, il est impossible de s'assurer que toutes les URL sont connues. La première analyse effectuée par Security Labs a mis en évidence le fait que Locky contactait jusqu'à six URL par jour.

Au moyen de techniques de rétro-ingénierie, Forcepoint Security Labs a reconstitué l'algorithme de génération de domaines de Locky et l'a rendu public, ce qui a donné l'occasion de riposter et de bloquer l'accès aux domaines contactés par le ransomware[17]. En empêchant le ransomware d'accéder aux URL connues et d'obtenir les clés de chiffrement requises un jour donné, les fichiers demeuraient intacts.

Cinq jours plus tard, les créateurs de Locky ont modifié leur algorithme et mis à jour les valeurs initiales. Le ransomware était alors capable de contacter 14 domaines par jour. Forcepoint a une fois de plus révélé l'algorithme et a fourni la liste des domaines à contacter au cours des 30 jours suivants[18]. Grâce à ce suivi constant, Forcepoint a découvert que les créateurs de Locky avaient une fois de plus modifié leur tactique 23 jours plus tard[19].

Bien que cela ne garantisse pas la récupération des fichiers, certaines entreprises se sont résignées à payer la rançon demandée, qui dépassait souvent plusieurs milliers de dollars[20].

Certains d'entre eux, comme CTB-Locker, n'ont pas besoin de contacter de serveur de commande pour accéder aux clés nécessaires au cryptage des fichiers, ce qui complique la tâche des personnes tentant d'interrompre le processus. C'est la raison pour laquelle Forcepoint concentre ses efforts sur l'interception du logiciel malveillant lors des étapes initiales de la menace, notamment au moment où « l'appât » est mis en place (les cybercriminels créent un courriel d'aspect inoffensif ou tout autre appât destiné à inciter l'utilisateur à cliquer sur un lien menant à un site compromis[22]).

Les ransomware savent désormais s'adapter à la langue du pays ciblé[23] ou, à l'inverse, éviter d'infecter les utilisateurs se trouvant dans un territoire donné[24]. Les créateurs de logiciels malveillants emploient ces méthodes pour éviter d'attirer l'attention des autorités locales ou pour cibler des pays et des marchés où le paiement d'une forte rançon est probable.

FAQ SUR LES RANSOMWARE

Une fois l'ordinateur infecté, à quelle vitesse le ransomware crypte-t-il les fichiers ?

Instantanément (dès sa connexion au serveur de commande).

Un ransomware commence le cryptage dès qu'il a dénombré tous les disques et recherché les types de fichiers ciblés (par extension).

Certains ransomware n'ont toutefois pas besoin de se connecter au serveur de commande pour commencer le cryptage. Ils peuvent en effet générer les clés de façon autonome puis, une fois le processus de cryptage terminé, renvoyer les informations relatives à la clé au serveur de commande. CTB-Locker est un bon exemple de logiciel n'ayant pas besoin d'établir de connexion.

Quelle est la probabilité de récupérer ses fichiers après avoir payé la rançon ?

Les créateurs de logiciels malveillants ont tout intérêt à restituer les fichiers afin d'encourager les futures victimes à payer. Toutefois, si le serveur de commande où se situent les informations de cryptage est supprimé, les fichiers ne pourront pas être décryptés, même si la rançon a été payée.

Quels sont les algorithmes de cryptage utilisés par les ransomware ?

Certains types de ransomware utilisent des algorithmes symétriques comme AES-256 (Teslacrypt). D'autres utilisent des algorithmes à clé publique RSA-2048 (CryptoLocker, CryptoWall). Certains rares ransomware utilisent un algorithme de cryptage personnalisé.

CONSEILS FORCEPOINT

1. Sauvegardez vos données sur un disque dur ou service externe. Vous n'aurez pas besoin de payer une rançon si vous pouvez récupérer vos documents depuis ces supports.
2. Informez les utilisateurs des dangers liés à l'ouverture de pièces jointes inattendues ou inconnues, ou à celle de liens hypertextes inconnus.
3. Identifiez les faiblesses de votre infrastructure et de vos processus pouvant être exploitées par les ransomware.
4. Posez-vous la question : le coût d'une rançon payée pour récupérer vos données ne serait-il pas mieux investi dans des mesures vous protégeant efficacement contre ce type d'incident ? Parmi ces mesures, l'on peut notamment retenir la sensibilisation des utilisateurs et le sandboxing des URL et pièces jointes.

DÉMASQUER LES ÉVASIONS

Les pare-feux de nouvelle génération servent à contrôler les utilisateurs et les applications tout en identifiant et en contrecarrant les attaques très efficacement. Contrairement aux pare-feux traditionnels, ils sont compatibles avec les applications et sont capables de suivre de façon granulaire l'état du trafic réseau. Les pare-feux de nouvelle génération sont également très utiles pour améliorer la visibilité du réseau.

Pour contourner les contrôles de sécurité, les pirates utilisent des techniques d'évasion qu'ils combinent parfois pour rendre leur intrusion d'autant plus difficile à détecter. Ces tactiques sont la réponse directe des créateurs des logiciels malveillants à la visibilité octroyée à l'administrateur sécurité par les meilleures solutions de sécurité moderne (dont les pare-feux de nouvelle génération).

Forcepoint Security Labs regroupe en trois catégories les cas de figure dans lesquels l'évasion est employée : le canal entrant (l'évasion sert à éviter les défenses du réseau), le canal sortant (contenu malveillant utilisant l'évasion pour contacter l'auteur des faits), et l'évasion comme moyen d'accéder aux ressources interdites (par exemple à l'aide de TOR). Ces techniques d'évasion avancées constituent une menace importante pour la sécurité des données d'entreprise.

ÉVASION DANS LA NATURE

Les techniques d'évasion avancées combinent plusieurs méthodes pour en créer de nouvelles, qui seront inédites et plus efficaces. Les créateurs de logiciels malveillants et d'exploits utilisent parfois un répertoire de méthodes d'évasion pour manipuler le flux au niveau du protocole et contourner la détection.

- **Fragmentation IP**

  La fragmentation IP est le processus visant à décomposer un datagramme IP en plusieurs paquets de taille réduite. Ce processus est détaillé dans la norme RFC 791[25].

  Les exploits de fragmentation IP utilisent le protocole de fragmentation au sein de l'IP comme vecteur d'attaque, en disséminant le contenu malveillant dans plusieurs trames.

- **Segmentation TCP et désordre**

Le protocole TCP (Transmission Control Protocol) est défini dans la norme RFC 793[26]. Les numéros des séquences servent à ordonner les segments reçus dans le désordre.

Les attaques s'appuyant sur la segmentation TCP et le désordre cherchent à dissimuler leurs actions en utilisant cette fonctionnalité du protocole TCP.

- **Pointeur TCP URG**

Le champ de pointeur urgent (URG) TCP est également défini dans la norme RFC 793. Ce pointeur indique la présence de données urgentes ou hors-bande qui, si elles sont incluses lors de l'analyse du contenu malveillant, peuvent permettre à un code malveillant ou exploit d'échapper à la détection.

LES CINQ PRINCIPALES UTILISATIONS ATTENDUES DE L'ÉVASION EN 2016

1. CONTOURNEMENT DES CONTRÔLES D'ACCÈS
pour accéder à un réseau interdit

2. POINTS D'ENTREE DES ATTAQUES
communiquer avec un point d'entrée de façon intraçable ne déclenche pas les alertes et réactions habituelles de l'équipe de sécurité du réseau

3. DISPONIBILITÉ DU RÉSEAU ZOMBIE
dissimuler le trafic entrant/sortant du serveur de commande augmente la résilience et assure la disponibilité du réseau zombie

4. EXPLOITS (LIVRAISON ET EXÉCUTION)
l'exécution du code peut être obtenue en introduisant des exploits normalement facilement détectables

5. EXFILTRATION DE DONNÉES
le trafic indétectable par le pare-feu peut servir à cacher le transfert des données volées

CONSEILS FORCEPOINT

1. Assurez-vous que les technologies que vous avez déployées sont adaptées pour identifier et réduire le risque d'évasion.
2. Assurez-vous que les techniques d'évasion soient bien comprises dans toute la chaîne de destruction. Le principe du maillon faible s'applique si à n'importe quel moment du cycle, la visibilité est réduite ou insuffisante.

WEB ET MESSAGERIE ÉLECTRONIQUE
UNE DOUBLE MENACE

De nos jours, le Web et la messagerie électronique sont les canaux de communication les plus utilisés, et ils demeurent ainsi les vecteurs d'attaque principaux des cybercriminels. En 2015, il ne fait aucun doute que la messagerie électronique a ainsi servi de point d'entrée initial dans les entreprises pour y mener des attaques ciblées à l'aide de contenu malveillant, dissimulé dans des documents Office et des fichiers compressés. Forcepoint Security Labs a découvert que par rapport à 2014, le nombre de courriels contenant des logiciels malveillants a augmenté de 250 %. Dridex[27] (une souche de logiciel bancaire malveillant) ainsi que diverses campagnes ransomware[28] étaient en grande partie responsable de cette augmentation. Les logiciels et les liens malveillants contenus dans un courriel peuvent s'appuyer sur les vulnérabilités d'un ordinateur pour l'infecter via Internet, puis toucher le réseau tout entier. En tant que vecteurs d'attaque, la messagerie électronique et le Web faisaient l'objet d'une convergence importante en 2015. En effet, 9 courriels indésirables sur 10 contenaient une URL. D'après le rapport intitulé Data Breach publié en 2015 par l'Identity Theft Resource Center[29], l'exposition accidentelle par Internet et messagerie électronique constituait en 2015 la troisième cause de compromission des données, ce qui souligne l'importance de l'analyse des menaces sur ces deux vecteurs d'attaque.

- **91,7 %** des courriels indésirables contiennent une URL.
- **2,34%** des courriels indésirables contiennent une pièce jointe.
- Augmentation de **44,7 %** des macros malveillantes dans les pièces jointes – les macros servent à télécharger du contenu malveillant hébergé sur le Web.
- **68,4 %** des courriels sont des spams (par rapport à 88,5 % en 2014).

Les données de Forcepoint indiquent que les macros malveillantes contenues dans des fichiers de type Microsoft Office ont constitué un moyen d'attaque de premier plan en 2015. Le rapport sur les menaces publié l'an dernier[30] a constaté l'observation de trois millions de macros malveillantes sur une période de trente jours, à la fin de l'année 2014. Sur un échantillon temporel équivalent, à la fin de l'année 2015, Forcepoint a détecté plus de quatre millions de macros, soit une augmentation de 44,7 % par rapport à 2014.

LES CINQ PRINCIPAUX TYPES DE FICHIERS MALVEILLANTS ENVOYES EN PIECE JOINTE

1. ARCHIVE ZIP
2. PROGRAMME SDOS/WINDOWS
3. FICHIERS TEXTE
4. MICROSOFT WORD 97
5. FORMAT MHT

LES DIX PRINCIPAUX PAYS HEBERGEANT DU CONTENU MALVEILLANT

1. ÉTATS-UNIS
2. ITALIE
3. ALLEMAGNE
4. RUSSIE
5. TURQUIE
6. IRLANDE
7. ROYAUME-UNI
8. FRANCE
9. PAYS-BAS
10. INDONÉSIE

LES HUIT PRINCIPAUX PAYS HEBERGEANT DES SITES DE HAMEÇONNAGE

1. ÉTATS-UNIS*
2. BELIZE
3. HONG KONG
4. BELGIQUE
5. ROYAUME-UNI
6. CHILI
7. ALLEMAGNE
8. SUÈDE

*Les États-Unis hébergeaient plus de sites de hameçonnage que tous les autres pays du top 8 réunis

CONSEILS FORCEPOINT

1. Recherchez les solutions de sécurité développées à partir d'analyse d'attaques réalisées via le Web et la messagerie électronique. Ces analyses vous garantiront une meilleure efficacité pour chaque produit.
2. Mettez en œuvre un programme de formation/sensibilisation rappelant régulièrement aux utilisateurs les techniques classiques permettant d'identifier un courriel malveillant contenant des pièces jointes ou des URL susceptibles de se connecter à Internet pour y récupérer davantage de contenu malveillant.
3. Envisagez de vous doter d'une technologie de sandboxing des URL et des pièces jointes afin d'empêcher les utilisateurs de prendre de mauvaises décisions ou de laisser passer un courriel malveillant.

L'ADOPTION DU CLOUD

De plus en plus d'entreprises adoptent les technologies basées sur le cloud afin de faire des économies et de collaborer plus efficacement. Bien que le marché de l'informatique dématérialisée soit toujours en développement, ses avantages, notamment la réduction des besoins en matériel et en support, la flexibilité pour les employés et la rapidité d'exécution de tâches complexes, motivent son adoption progressive. Dans une enquête internationale réalisée par Harvard Business Review Analytic Services[31], 85 % des personnes interrogées ont signalé que leur entreprise allait utiliser des outils cloud modérément ou intensivement au cours des trois prochaines années.

Malgré les nombreux avantages qu'il présente pour l'exécution des tâches d'entreprise, le cloud a connu une adoption assez lente, gênée dans certaines entreprises par la peur que les applications dématérialisées soit mal protégées ou se trouvent en conflit avec les règles de conformité. Plus de 60 % des entreprises citent les « préoccupations concernant la sécurité » comme leur raison principale de reporter l'adoption du cloud[32]. D'après Ponemon[33], les préoccupations se concentrent autour de la difficulté à faire respecter des méthodes de sécurité efficaces lors de l'utilisation d'applications et de produits dématérialisés, ainsi que l'incertitude qui entoure l'attribution des responsabilités entre les utilisateurs finaux et les fournisseurs de services cloud en ce qui concerne la sécurité des données.

Toutefois, résister à l'adoption du cloud ne retarde pas nécessairement son utilisation. Certains employés, groupes, voire divisions toutes entières migrent vers le cloud sans l'aval de leur entreprise. Lorsque des solutions externes répondent mieux à leurs besoins en matière de productivité, ils se passent ainsi de toute approbation ou effort d'intégration. Cet état de fait crée la possibilité pour des technologies n'ayant reçu aucune approbation formelle de compromettre la sécurité et la conformité d'une entreprise, ce qui l'expose à des risques indésirables et imprévus.

INFORMATIQUE FANTÔME

CE NE SONT PAS CES NUAGES-LÀ QUE VOUS RECHERCHEZ

- **SEULES 8 %** des entreprises connaissent l'étendue de l'informatique fantôme (« shadow IT ») dans leur organisation

- **71 %** des entreprises trouvent l'informatique fantôme assez préoccupante ou très préoccupante*

*« RAPPORT SUR LES PRATIQUES D'ADOPTION DU CLOUD ET ENQUÊTE SUR LES PRIORITÉS », janvier 2015, Cloud Security Alliance

Plus de 80 % des décisionnaires informatiques pensent que le l'informatique fantôme présente un risque en matière de sécurité informatique. Un tiers d'entre eux considère ce risque comme étant extrêmement grave et 16 % d'entre eux le considèrent comme le risque le plus grave[34]. En revanche, seuls 34 % des utilisateurs de l'informatique fantôme pensent que cette pratique présente un risque de sécurité, plus de la moitié d'entre eux arguant du fait qu'elle améliore la productivité des services commerciaux[35]. Malheureusement, un service informatique ne peut pas protéger correctement les données dont il n'a pas conscience, ce qui crée un environnement propice à leur vol ou à leur perte.

D'après une enquête réalisée par IDG Enterprise[36], les DSI pensent que 2016 sera la première année où les services seront davantage situés sur le cloud que dans l'entreprise. Pour assurer la conformité avec la réglementation, il est indispensable de mettre en œuvre des solutions de sécurité et de confidentialité centrées sur les données et recouvrant l'ensemble des plateformes et systèmes informatiques. En plus de la mise en place de défenses sensibles aux données, les évaluations indépendantes (telles que CSA STAR Certification[37]) peuvent vous aider à évaluer la sécurité des fournisseurs de services cloud.

CONSEILS FORCEPOINT

1. Les solutions de prévention contre la perte de données et les pare-feux de nouvelle génération peuvent aider les entreprises à prendre la pleine mesure de leur informatique fantôme.
2. Une fois que les services et les entités informatiques auxquels se connectent les utilisateurs sont connus, les entreprises peuvent, selon leurs politiques internes, faire respecter les directives relatives aux données et à leur utilisation, former les utilisateurs ou désactiver certaines fonctions.
3. Bien souvent, les employés se servent de l'informatique fantôme pour s'extraire du conformisme professionnel et faire preuve d'originalité. Un contrôle trop rigoureux peut entraîner la frustration des utilisateurs et les pousser à contourner les restrictions. N'hésitez pas à travailler main dans la main avec les employés pour les aider à améliorer leur productivité plutôt que de les décourager à innover.

BESOIN DE CYBER-TALENTS

Les données continuant à s'éloigner des périmètres de défense, il est essentiel de disposer d'une force de cybersécurité capable de protéger vos informations des menaces qui les guettent. L'étude annuelle de Raytheon, « Securing Our Future : Closing the Cyber Talent Gap[38] », menée en collaboration avec la National Cyber Security Alliance, cherche à identifier les causes premières du manque de professionnels formés à la cybersécurité dans le cadre d'un engagement à établir une réserve de talents stable sur le long terme.

AVIS DE CSO

Les fusions et acquisitions de nouvelles entreprises sont en plein essor, mais elles complexifient toutefois la protection des données sensibles de l'entreprise. Étant donné que 84 % de la valeur du S&P 500 repose désormais sur la propriété intellectuelle (PI) et d'autres actifs immatériels[39], il est indispensable de rendre les données accessibles aux parties intéressées tout en prévenant leur perte, leur vol ou leur utilisation à mauvais escient. La technologie et les processus commerciaux nécessaires à la protection des données sensibles et au maintien d'un avantage concurrentiel font partie intégrante des fusions, acquisitions et autres propositions commerciales de cet ordre. Une perte de PI ou d'autres données a un effet immédiat sur la réputation de l'entreprise, mais peut également entraîner des recours juridiques ou réglementaires et nuire au positionnement concurrentiel, au prix de l'action et à la valeur pour l'actionnaire. La création d'un schéma directeur destiné à la consolidation et à la gestion des données sensibles est indispensable à la réussite de l'intégration des entreprises prenant part à la fusion.

LA FORMATION DE FORCEPOINT : LES CLÉS DE L'INTÉGRATION RÉUSSIE D'UNE ENTREPRISE DE CYBER-SÉCURITÉ

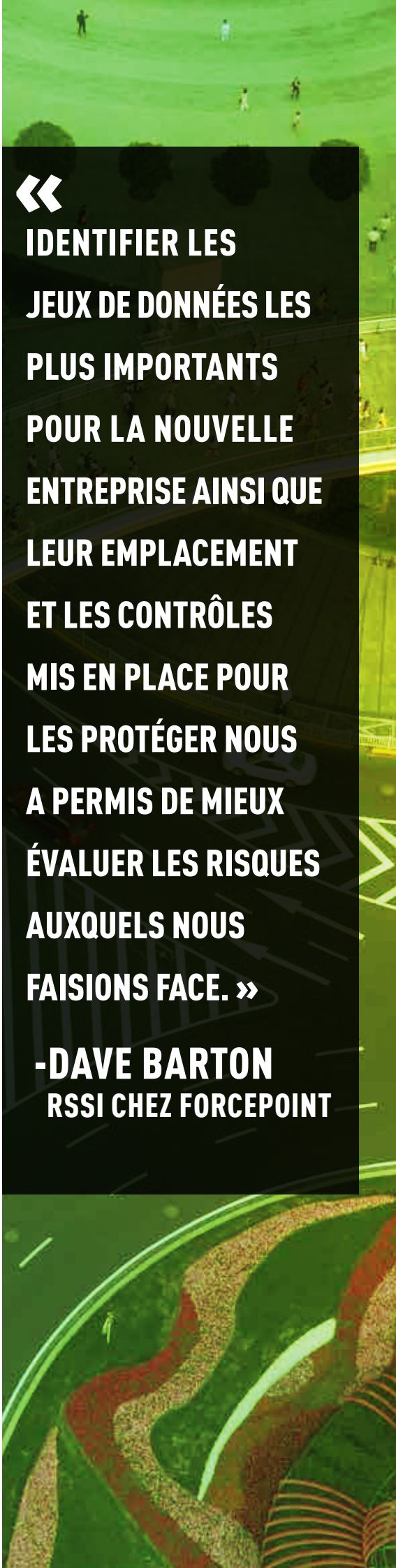
Le 14 janvier 2016, une nouvelle joint venture fondée sur l'intégration de Websense, Raytheon Cyber Products et les solutions NGFW de Stonesoft a été annoncée. Nommée Forcepoint, cette nouvelle entreprise est le fruit d'une année d'intégration des systèmes commerciaux.

ÉVALUATION

Avant que l'intégration des données, systèmes ou processus puisse commencer, il était nécessaire de réaliser une évaluation des pratiques que chacune des entreprises adoptait vis-à-vis de la sécurité, en interne et en externe. Une société tierce a effectué des tests de pénétration et s'est plongée dans le Web profond pour repérer d'éventuelles discussions concernant les vulnérabilités ou les piratages en cours étant passés inaperçus. Les membres de l'équipe de sécurité ont détaillé leur programmes : sensibilisation des utilisateurs, gestion des vulnérabilités, classification et flux des données, et administration des contrôles d'accès. Cet audit a confirmé que les politiques internes étaient effectivement mises en œuvre et a mis en lumière les différences entre les entreprises, par exemple lorsque l'une d'entre elles justifiait des exigences de sécurité plus strictes devant servir de référence pour les autres entreprises.

ÉVALUATION

À la suite de notre propre évaluation de la sécurité, une évaluation des menaces sur les réseaux des entités à fusionner a commencé. Un outil spécialement conçu a ainsi été utilisé pour détecter et signaler toute activité suspecte et pour évaluer la santé du réseau afin de produire des recommandations. Celles-ci étaient souvent d'une grande simplicité : par exemple, appliquer un correctif sur un serveur ou mettre à jour des certificats.



« IDENTIFIER LES JEUX DE DONNÉES LES PLUS IMPORTANTS POUR LA NOUVELLE ENTREPRISE AINSI QUE LEUR EMPLACEMENT ET LES CONTRÔLES MIS EN PLACE POUR LES PROTÉGER NOUS A PERMIS DE MIEUX ÉVALUER LES RISQUES AUXQUELS NOUS FAISIONS FACE. »

-DAVE BARTON
RSSI CHEZ FORCEPOINT

Dans le même temps, les données les plus précieuses de RCP et Websense (PI, données financières, etc.) ont été identifiées, et une communication adaptée a été mise en place pour affronter les menaces ciblées et les activités malveillantes (par ex. spam et hameçonnage), qui ont souvent lieu lors de la fusion de plusieurs entreprises. Forcepoint a reçu ce qui semblait être des courriels émanant de Raytheon, lesquels demandaient l'envoi de données sensibles et d'informations financières. Grâce aux mesures proactives déjà mises en place, ces tentatives d'intrusions malveillantes ont échoué.

ACTION

Avant le jour de l'annonce, un essai statique et dynamique a été effectué sur l'intégralité du code source de l'entreprise nouvellement formée. Cet essai visait à identifier les vulnérabilités du code qui n'avaient pas encore été décelées.

LE JOUR DE L'ANNONCE

Bien que les réseaux n'étaient pas encore été reliés ou ne communiquaient pas encore entre eux, il convenait de prendre des mesures pour s'assurer que, dans les mois suivants, l'intégration se déroulerait sans accroc. Tout d'abord, l'entreprise a présenté à tous les employés les politiques concernant l'accès aux données, en mettant l'accent sur la gestion des données sensibles au cours de la période de transition. De plus, il était interdit de partager les modèles tarifaires exclusifs et autres renseignements concurrentiels avant la conclusion formelle du processus d'acquisition. Cette opération de communication auprès des utilisateurs finaux était indispensable pour protéger les actifs et les informations au cours de ce processus.

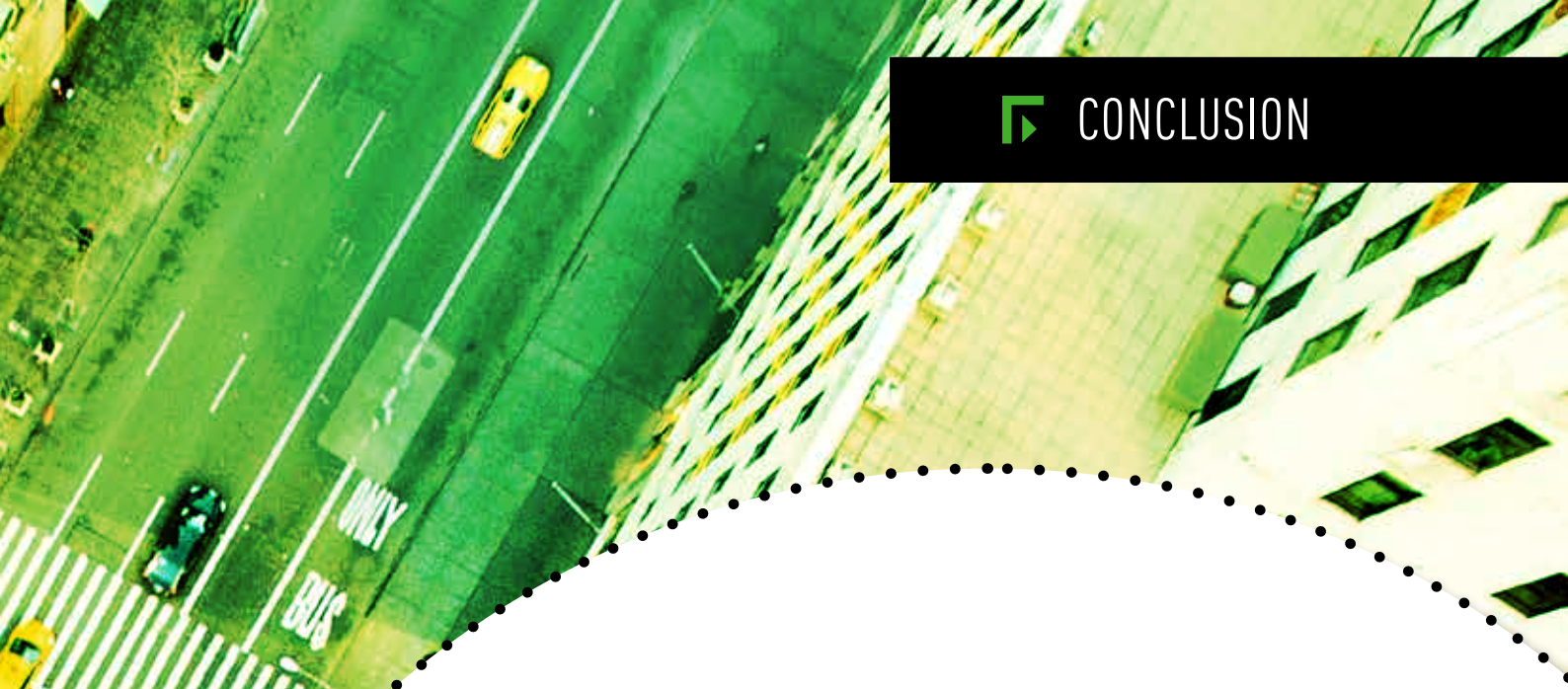
UN NOUVEAU TEST DE RESISTANCE AUX CONTRAINTES

Le centre Cyber Operations, Development and Evaluation (CODE) de Raytheon est une installation informatique de pointe servant à tester la résistance aux cyberattaques des systèmes essentiels actuels ou futurs. Le centre CODE fait partie du réseau mondial de centres Raytheon dédiés à l'innovation informatique et à la démonstration. Ceux-ci aident les clients à trouver rapidement une solution à leurs difficultés les plus complexes en matière de cybersécurité.

Par ailleurs, la surveillance des réseaux de l'entreprise a été renforcée à l'aide d'outils de protection contre le vol de données, en apportant un soin particulier aux comptes d'administrateurs et aux tentatives de transfert de données sensibles via courrier électronique ou Internet. Après avoir reçu les alertes, les équipes informatique, de sécurité et de développement ont commencé à pallier aux menaces et vulnérabilités identifiées. Ainsi, tous les problèmes, lacunes et différences restants en matière de politiques de sécurité ont pu être résolus avant de relier les réseaux.

Si le processus d'intégration n'est jamais simple, celui entrepris par Forcepoint fut particulièrement complexe. En parallèle de ce processus, nous avons procédé à l'acquisition de Stonesoft, pour laquelle nous avons dû répéter une grande partie des étapes ayant mené à la création de la joint venture réunissant Websense et RCP, afin d'assurer une intégration en douceur. De plus, le passage à une nouvelle identité de marque a exigé le transfert des employés, des postes de travail et des données informatiques vers un nouveau domaine, Forcepoint.com. Toutes ces opérations ont eu lieu pendant les journées habituelles de travail, en vue d'éviter la fuite de notre nouveau nom et de notre nouvelle marque avant l'annonce officielle. Pour ce faire, nous avons déployé de nouveaux outils limitant le partage hors réseau des données contenant le nouveau nom et des informations sur la marque. Malgré ces obstacles importants, la planification et le travail préalables ont permis de poursuivre l'intégration à un rythme soutenu, tout en limitant et en résolvant de petites difficultés avant la fin de la fusion.

La sécurité est un aspect essentiel de toute fusion-acquisition. En effet, de nombreux risques potentiels liés à ce processus resteront indécelables sans une forte implication de spécialistes de la sécurité informatique.



CONCLUSION

Le rapport 2016 sur les menaces confirme qu'au cours de l'année dernière, un changement notable s'est opéré dans la nature des attaques. La cybersécurité, qui est bien souvent un domaine où priment débats techniques, alertes et problèmes informatiques, est en voie de devenir une affaire de risques et de conséquences de premier ordre pour les cadres de direction, les élus politiques, les autorités et les dirigeants du monde entier.

Les actions d'une bande organisée derrière un ransomware, d'un employé négligent ou d'une attaque orchestrée avec brio peuvent avoir des conséquences immédiates et catastrophiques. Dans certains cas, elles peuvent aller jusqu'à menacer la stabilité financière d'une entreprise, sa capacité à gérer ses opérations, ou salir une marque reconnue. Malgré tout, toutes les attaques ne constituent pas une menace existentielle. De nos jours, n'importe quel bureau ou objet connecté à Internet peut être attaqué à tout moment.

Nous pensons que pour vaincre rapidement les ennemis les plus déterminés, nos clients doivent adopter une approche holistique neuve, capable de donner à leur entreprise une vision à 360 degrés, d'offrir une analyse en temps réel et d'anticiper les menaces et leurs implications via des alertes pertinentes. Grâce à leur expertise, les équipes de Security Labs, Special Investigations et Office of the CSO continuent à identifier des menaces et des attaques se déroulant dans le monde entier. Ensemble, nous pourrons prendre des décisions avisées pour ***avancer sans crainte.***

RÉFÉRENCES

1. Ponemon Institute LLC. « 2015 Cost of Cyber Crime Study: Global. » Octobre 2015. https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf

2. Ponemon Institute LLC. « Privileged User Abuse & The Insider Threat. » Mai 2014. http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf

3. Anderson, Ed; Nag, Sid, and Gartner, Inc. « Forecast Overview: Public Cloud Services, Worldwide, 2016 Update. » 17 février 2016. https://www.gartner.com/doc/3214717?ref=SiteSearch&sthkw=security%20concerns%20cloud%20adoption&fnl=search&srcId=1-3478922254

4. Shey, Heidi. « Understand The State Of Data Security And Privacy: 2015 To 2016. » Forrester Research, Inc., 8 janvier 2016. https://www.forrester.com/report/Understand+The+State+Of+Data+Security+And+Privacy+2015+To+2016/-/E-RES117447

5. Mearian, Lucas. « Government Tests Show Security's People Problem. » Computerworld. 6 juillet 2011. http://www.computerworld.com/article/2510014/security0/government-tests-show-security-s-people-problem.html

6. Ponemon Institute LLC. « Ponemon Study: The Unintentional Insider Risk in United States and German Organizations. » 30 juillet 2015. http://www.raytheoncyber.com/spotlight/ponemon/index.html

7. Bank Director. « Bank Director's 2016 Risk Practices Survey. » 21 mars 2016. http://www.bankdirector.com/download_file/view_inline/4996

8. Identity Theft Resource Center. « 2015 Data Breaches | ITRC Surveys & Studies | ID Theft Blog. » 25 janvier 2016. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

9. Forrester Research, Inc. « Global Business Technographics® Security Survey, 2015. » Juillet 2015. https://www.forrester.com/Global Business Technographics Security Survey 2015/-/E-sus2957

10. Forrester Research, Inc. « Global Business Technographics® Devices And Security Workforce Survey, 2015. » Août 2015. https://www.forrester.com/Global+Business+Technographics+Devices+And+Security+Workforce+Survey+2015/-/E-sus2971

11. Ponemon Institute LLC. « Privileged User Abuse & The Insider Threat. » Mai 2014. http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf

12. Litan, Avivah, and Gartner, Inc. « Best Practices and Success Stories for User Behavior Analytics. » 4 mars 2015. https://www.gartner.com/doc/2998124/best-practices-success-stories-user

13. Forrester Research, Inc. « Global Business Technographics® Security Survey, 2015. » Juillet 2015. https://www.forrester.com/Global Business Technographics Security Survey 2015/-/E-sus2957

14. Forcepoint LLC. « Cyber Dwell Time and Lateral Movement THE NEW CYBERSECURITY BLUEPRINT. » https://www.forcepoint.com/resources/whitepapers/cyber-dwell-time-and-lateral-movement

15. Forcepoint LLC. « Cyber Dwell Time and Lateral Movement THE NEW CYBERSECURITY BLUEPRINT. » https://www.forcepoint.com/resources/whitepapers/cyber-dwell-time-and-lateral-movement

16. Vanian, Jonathan. « Hollywood Hospital Pays Off Hackers To Restore Computer System. » 18 février 2016. http://fortune.com/2016/02/18/hollywood-hospital-hackers-computer-system/

17. Forcepoint Security Labs et Forcepoint LLC. « Locky Ransomware - Encrypts Documents, Databases, Code, BitCoin Wallets and More... » 19 février 2016. https://blogs.forcepoint.com/security-labs/locky-ransomware-encrypts-documents-databases-code-bitcoin-wallets-and-more

18. Forcepoint Security Labs et Forcepoint LLC. « Locky's New DGA - Seeding the New Domains [RUSSIA UPDATE: 26/FEB/16]. » 25 février 2016. https://blogs.forcepoint.com/security-labs/lockys-new-dga-seeding-new-domains

19. pseudo Twitter @Forcepointsec mardi 22 mars 2016. Tweet, https://twitter.com/Forcepointsec/status/712316915687948289

20. Winton, Richard. « Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating. » Los Angeles Times. 18 février 2016. http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

RÉFÉRENCES

21. Vijayan, Jai. « With $325 Million In Extorted Payments CryptoWall 3 Highlights Ransomware Threat. » Dark Reading. 29 octobre 2015. http://www.darkreading.com/endpoint/with-$325-million-in-extorted-payments-cryptowall-3-highlights-ransomware-threat/d/d-id/1322899

22. Forcepoint LLC (anciennement Websense). « The Seven Stages of Advanced Threats. » https://www.websense.com/assets/pdf/understanding-the-cyber-attack-infographic.pdf

23. Forcepoint Security Labs et Forcepoint LLC. « TorrentLocker is Back and Targets Sweden & Italy. » 15 mars 2016. https://blogs.forcepoint.com/security-labs/torrentlocker-back-and-targets-sweden-italy

24. Forcepoint Security Labs et Forcepoint LLC. « Locky's New DGA - Seeding the New Domains [RUSSIA UPDATE: 26/FEB/16]. » 25 février 2016. https://blogs.forcepoint.com/security-labs/lockys-new-dga-seeding-new-domains

25. Information Sciences Institute ; University of Southern California. « DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION. » INTERNET PROTOCOL, Septembre 1981. https://tools.ietf.org/html/rfc791

26. Information Sciences Institute ; University of Southern California. « DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION. » TRANSMISSION CONTROL PROTOCOL, Septembre 1981. https://tools.ietf.org/html/rfc793

27. Forcepoint Security Labs et Forcepoint LLC. « Dridex Down Under. » 5 novembre 2015. https://blogs.forcepoint.com/security-labs/dridex-down-under

28. Forcepoint Security Labs et Forcepoint LLC. « Accounts Payable in the Czech Republic Targeted by Dridex. » 4 août 2015. https://blogs.forcepoint.com/security-labs/accounts-payable-czech-republic-targeted-dridex

29. Identity Theft Resource Center. « 2015 Data Breaches | ITRC Surveys & Studies | ID Theft Blog. » 25 janvier 2016. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

30. Forcepoint LLC. « Rapport Websense 2015 sur les menaces. » 8 avril 2015. https://www.websense.com/content/websense-2015-threat-report.aspx

31. Harvard Business Review. « How the Cloud Looks from the Top: Achieving Competitive Advantage In the Age of Cloud Computing. » 2011. https://hbr.org/resources/pdfs/tools/16700_HBR_Microsoft%20Report_LONG_webview.pdf

32. Anderson, Ed; Nag, Sid, and Gartner, Inc. « Forecast Overview: Public Cloud Services, Worldwide, 2016 Update. » 17 février 2016. https://www.gartner.com/doc/3214717?ref=SiteSearch&sthkw=security%20concerns%20cloud%20adoption&fnl=search&srcId=1-3478922254

33. Ponemon Institute LLC. « The Challenges of Cloud Information Governance: A Global Data Security Study. » Octobre 2014. http://www2.gemalto.com/cloud-security-research/SafeNet-Cloud-Governance.pdf

34. VansonBourne. « Shadow IT ITDMs Data Summary. » p. 34. 11 juillet 2014. http://www.vansonbourne.com/files/1914/1225/3447/VB-Shadow_IT-ITDMs-Data-Summary.pdf

35. VansonBourne. « Shadow IT BDM Data Summary. » p. 24. 22 juillet 2014. http://www.vansonbourne.com/files/7614/1225/3401/VB-Shadow_IT-BDM-Data-Summary.pdf

36. IDG Enterprise. « 2015 IDG enterprise cloud computing survey. » 17 novembre 2015. http://www.idgenterprise.com/resource/research/2015-cloud-computing-study/

37. CAS Cloud Security Alliance. https://cloudsecurityalliance.org/star/certification/

38. Raytheon Company, « Securing Our Future: Closing the Cyber Talent Gap. » 19 octobre 2015. http://raytheon.mediaroom.com/2015-10-26-Many-more-men-than-women-are-drawn-to-cybersecurity-careers-and-the-gap-is-widening-dramatically-new-survey-says

39. Ocean Tomo LLC. « Intangible Asset Market Value Study. » mercredi 4 mars 2015. http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/

QUI EST FORCEPOINT ?

Forcepoint se donne pour mission d'aider les entreprises à avancer. Notre objectif est d'aider nos clients à adopter des technologies commerciales révolutionnaires en toute confiance, dans un monde où les services cloud, les architectures hybrides et la main d'œuvre mobile sont devenues la norme. Le modèle de sécurité basé sur la mise en place d'un périmètre étant désormais obsolète, les entreprises ont besoin de solutions assurant une protection rapprochée des données, où qu'elles aillent : dans différents environnements et appareils, du réseau vers un terminal, et du mobile vers le cloud. Peu importe la région, la clientèle ou la taille de nos clients, les menaces auxquels ils font face gagnent en dangerosité, et les équipes de sécurité disposent bien souvent de moyens trop limités pour les affronter seules. La plateforme Forcepoint permet aux entreprises d'automatiser les activités de sécurité de routine, de simplifier la gamme de produits utilisés et de bénéficier d'informations vitales telles celles incluses dans notre rapport annuel sur les menaces.

THREATSEEKER® INTELLIGENCE CLOUD

Threatseeker Intelligence Cloud a été développé pour offrir à Forcepoint une visibilité sur les menaces les plus récentes. Chaque jour, Threatseeker traite jusqu'à 5 milliards de points de données tirés de nombreuses sources situées dans 155 pays. En travaillant sans interruption en coulisses, Threatseeker nous aide ainsi à protéger nos clients et leurs activités. Les spécialistes de Forcepoint utilisent Threatseeker chaque jour pour collecter les informations et les connaissances précises et en temps réel incluses dans nos rapports annuels sur les menaces et sur les prédictions et nos analyses approfondies de l'industrie.

FORCEPOINT
POWERED BY Raytheon