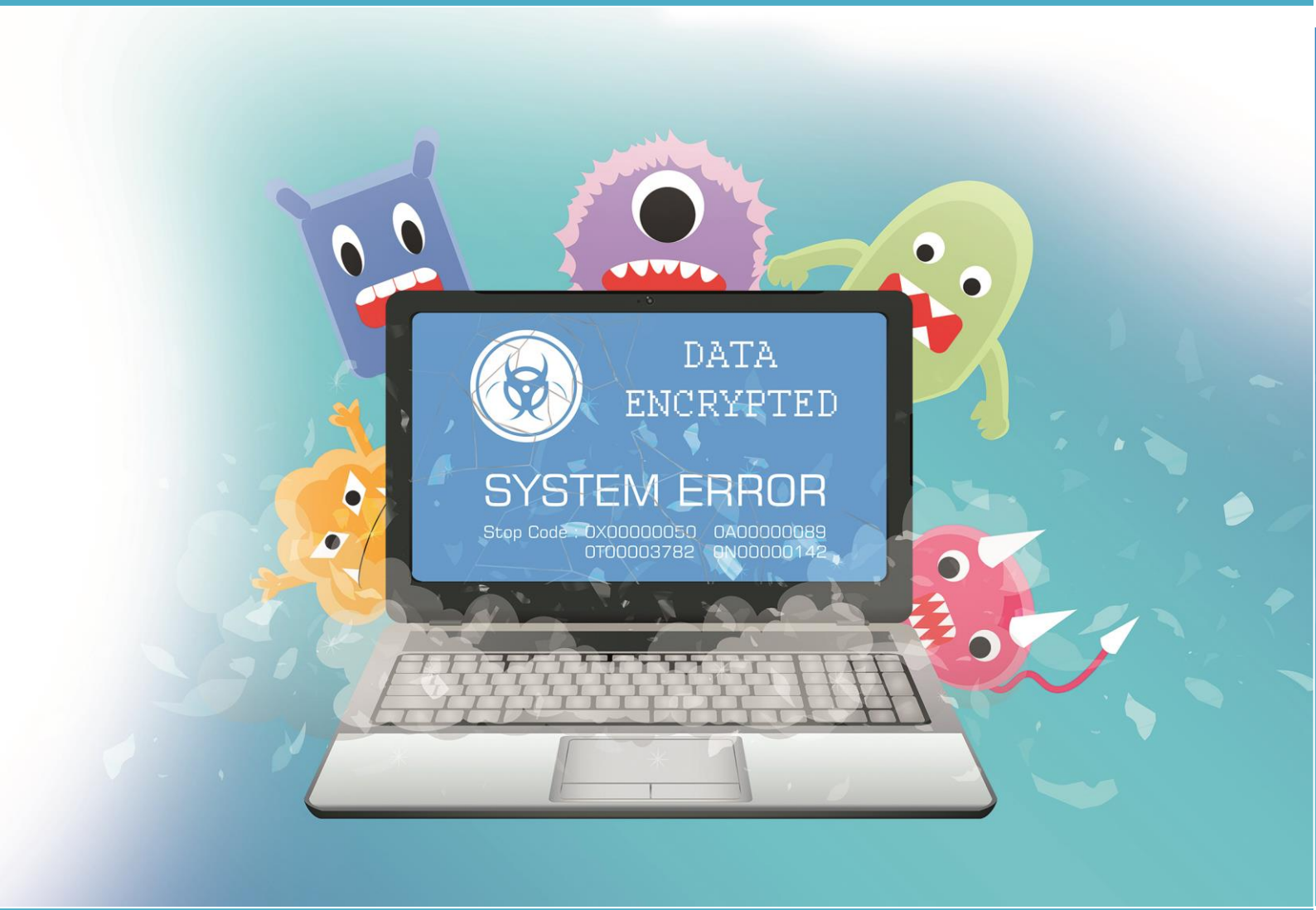
CONTRER LES RANSOMWARES

LIVRE BLANC

MIEL



En partenariat avec

paloalto NETWORKS

RES

DataCore SOFTWARE

EVault

CONTENU

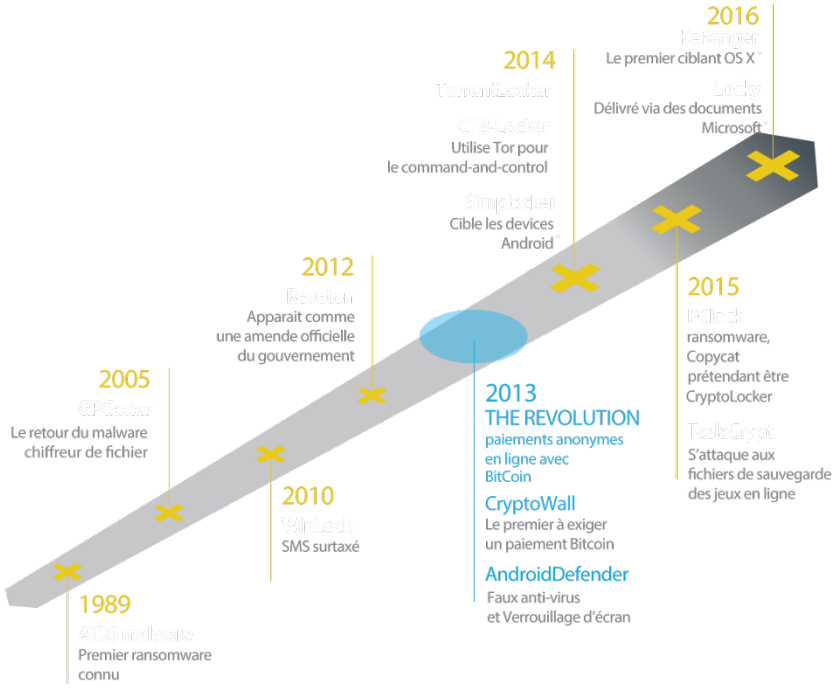
Les spécialistes de Miel rencontrent des responsables informatiques au quotidien qui, pour certains, ont déjà subi des attaques par ransomware (ou rançongiciel), quelle que soit la taille de leur entreprise ou leur secteur. C'est pourquoi nous avons choisi dans ce document de vous décrire cette menace à travers son historique et ses principes pour bien comprendre à quoi l'on fait face et penser la protection contre ces nuisances qui peuvent causer beaucoup de dégâts. Nous présenterons ensuite les trois domaines à couvrir pour élaborer cette protection aujourd'hui indispensable : la préparation, la prévention et la réaction. Et ce sera sous l'angle de quatre de nos partenaires technologiques que nous évoquerons concrètement les mesures et systèmes à votre disposition pour éviter toute perte de données et tout blocage de votre activité.

Le ransomware n'est pas quelque chose de nouveau. Il y a 30 ans déjà, en 1989, le principe était apparu : prendre en otage les données d'un poste ou d'un serveur en les chiffrant, et proposer leur « libération » en fournissant la clé de déchiffrement en échange d'une rançon. Ce type d'attaque est cependant resté longtemps assez peu fréquent, mais le phénomène connaît une très forte recrudescence depuis 2015, qui s'accélère encore en 2016[1].

[1] http://www.distributique.com/actualites/lire-les-pme-sont-victimes-d-un-ransomware-toutes-les-40-secondes-25623.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter, 12 déc. 2016 ; http://www.lesechos.fr/tech-medias/hightech/0211566598845-les-ransomwares-logiciels-extorqueurs-ont-explose-en-2016-2049004.php, 8 déc. 2016

UN MODELE CRIMINEL DEVENU LUCRATIF

Si on se réfère aux résultats des investigations menées et notamment à celles du laboratoire Unit42 de Palo Alto Networks qui travaille sur les cyber menaces[2], la révolution est apparue en 2013 avec l'apparition d'un malware nommé CryptoWall et son dérivé CryptoLocker. C'est la première fois qu'on passait à un véritable modèle économique criminel. Ce modèle a pu en fait s'établir, il y a trois ou quatre ans, parce que les systèmes de chiffrement et surtout de déchiffrement sont devenus beaucoup plus fiables. Auparavant, la victime n'était pas encline à payer car rien ne lui garantissait le rétablissement de ses données une fois la rançon payée.



Paradoxalement, c'est donc les avancées technologiques en termes de chiffrement qui facilitent le travail des malfaiteurs, qui peuvent de surcroît s'appuyer sur les nouveaux systèmes fiables de paiement anonyme en-ligne, non traçables, comme la monnaie BitCoin. Les auteurs peuvent chiffrer des données, les déchiffrer puis recevoir un paiement sans être tracés. Cette pratique criminelle devient donc une source lucrative de revenu avec des investissements simples et légers puisqu'on a même vu

[2] http://researchcenter.paloaltonetworks.com/2016/05/unit-42-ransomware-trends/, 10 mai 2016

apparaître des plates-formes Ransomware-as-a-Service à la disposition de tous. A tel point qu'en 2016, Unit42 a détecté pour la première fois des attaques contre des systèmes MacOS, en quelque sorte une consécration pour ce genre de malwares.

Aujourd'hui, on compte plus de 30 familles de ransomware actives observées dans le monde, chiffre en constante augmentation, capables d'infecter tout type de systèmes et pas seulement Windows, et toujours plus de victimes potentielles.

Les exemples se multiplient dans la presse, comme celui des transports publics de San Francisco qui a abouti à la gratuité des trajets pendant toute la journée du 26 novembre 2016 avec le manque à gagner qu'on peut imaginer. Les pirates exigeaient une rançon de 78000 dollars[3].

[3] http://www.lemondeinformatique.fr/actualites/lire-les-transports-de-san-francisco-attaques-par-un-ransomware-66632.html, 28 nov. 2016

LA MENACE EST UNIVERSELLE ET AVEUGLE

Vous avez peut-être malheureusement déjà vu un des écrans suivants. Voici à quoi ressemble une demande de rançon par ransomware. On a ici les plus connus, TeslaCrypt (https://youtu.be/7EcJlJX9sxc), CryptoLocker, ou encore Locky auquel tellement de monde a été confronté. Si vous voyez un de ces pop-ups apparaître, il est déjà trop tard : il ne reste plus qu'à payer pour récupérer ses données ou consentir à les abandonner en comptant sur une sauvegarde !

Toutefois les attaques par ransomware ne sont pas aussi perfectionnées qu'on pourrait l'imaginer. D'une manière générale, les cyber criminels utilisent ce qui fonctionne, ce qui a déjà marché. En l'occurrence, les

technologies initiées par CryptoWall et CryptoLocker. 90% des ransomwares aujourd'hui en sont des variantes. Les malfaiteurs vont reprendre ces sources, vont les modifier légèrement pour créer des variantes qui échapperont à la détection, ou même les utiliser tels quels. Le plus gros du travail a déjà été fait, et les attaquants minimisent ainsi leurs coûts de production.

Ils peuvent concentrer leurs investissements sur les vecteurs d'attaque. C'est là qu'est le point crucial : la macro, l'exploit kit (qui contient tous les bouts de code pour exploiter les vulnérabilités et livrer le malware) qui introduit le ver dans le fruit. Ils vont bénéficier des réseaux qui leur garantissent l'anonymat (TOR, I2P…) et les maintiennent sous les radars. Les criminels vont également s'attacher maintenant à adapter les messages à leurs victimes, dans leur langue, se faisant parfois passer pour des autorités officielles avec tout l'habillage que cela implique.

Une caractéristique propre au ransomware est sa portée universelle. L'attaque n'a pas besoin d'être vraiment adaptée à la victime. Du particulier à la très grande entreprise, en passant par les PME, quel que soit le secteur d'activité, la zone géographique, le système d'exploitation (y compris Android et MacOS), tout le monde peut être touché : le malfaiteur ira là où il trouve une porte ouverte. Et l'activité peut être très lucrative en multipliant les petites sommes. Pour décider la victime à payer, il suffit d'exiger un montant « raisonnable » qui rendra plus rentable de payer que d'essayer de déchiffrer ou récupérer ses données au regard du manque à gagner induit par le blocage des données pendant ce temps. Le modèle économique est devenu si juteux que des plateformes de Ransomware-as-a-Service proposent, moyennant finances de lancer des attaques pour des tiers !

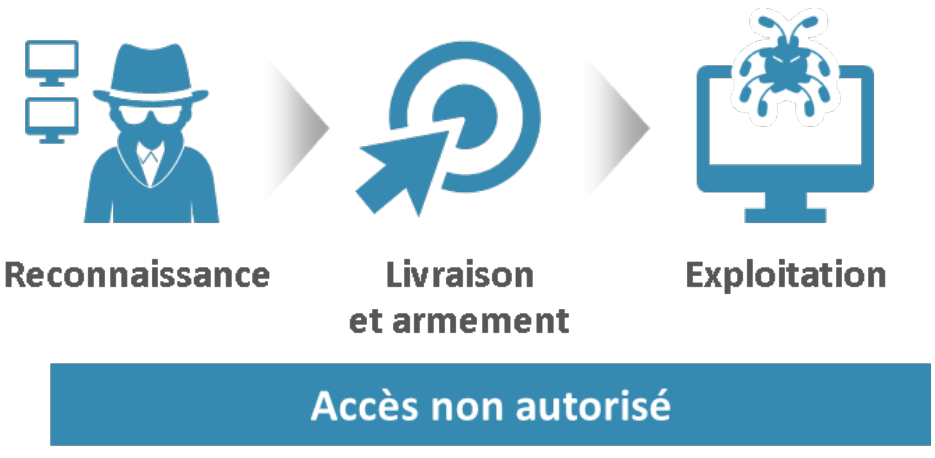
COMPRENDRE LA CHAINE DE FRAPPE DU RANSOMWARE

Pour encore mieux connaître cette menace, étudions comment elle fonctionne. Comment un ransomware va pénétrer dans le réseau et agir. Comme pour tout malware, on peut décrire le processus de l'attaque au moyen d'un schéma de chaine de frappe tel que peuvent l'utiliser les militaires (cf. le concept de « Kill Chain » énoncé par Lockheed Martin).

Pénétration du périmètre

D'abord il faut faire le tour du propriétaire pour trouver comment pénétrer le réseau. Cela consiste à faire de la surveillance, de l'ingénierie sociale pour arriver à ouvrir une porte qui permettra d'introduire le vecteur d'attaque. On utilise pour ce faire des techniques d'hameçonnage ou *spear fishing* : l'ingénierie sociale va identifier un utilisateur à cibler et les failles qu'il présente pour ensuite l'inciter à une action, via une pièce attachée corrompue d'un e-mail, une bannière trafiquée sur un site web légitime ou une adresse URL conduisant à un site frauduleux. En termes militaires, il s'agirait de la reconnaissance et de l'armement.

Un exemple d'ingénierie sociale : sur les réseaux sociaux, j'ai repéré deux personnes qui discutent d'un sujet qui leur est commun. Je me fais passer pour un des deux individus et j'envoie un e-mail à l'autre personne sur le sujet de leur discussion avec un fichier joint, une photo illustrant le sujet. Le destinataire n'a pas de raison de se méfier. Il clique et arme ainsi l'attaque.



Livraison du malware

En cliquant sur une pièce jointe ou un lien, on exécute sans le savoir un bout de code, léger, qui va exploiter une vulnérabilité d'une application ou d'un système d'exploitation, vulnérabilité qui va ouvrir la voie à une exploitation par un code un peu plus important. La brèche est ouverte. On peut livrer le malware.

Mouvement latéral

Lorsque le malware est livré, il va faire deux choses. D'abord l'installation et la dissimulation : prendre les privilèges du système hôte, observer s'il peut se répliquer, se disséminer ou exploiter d'autres vulnérabilités pour éventuellement télécharger d'autres malwares. L'objectif est de se rendre le plus persistant possible et d'atteindre sa cible réelle finale au sein du data center.

Chiffrement des données

Puis il va tenter d'ouvrir un canal de communication vers l'extérieur, vers le serveur source qui le contrôle pour établir un trafic de « command & control ». Dans le cas précis du ransomware, ce trafic va inclure le protocole d'échange de clés pour chiffrer les données sous son contrôle.

Pendant longtemps, le but des cyber attaques était de voler ces données, de les extraire aux fins d'espionnage ou pour les proposer au plus offrant.

Aujourd'hui, on se contente de chiffrer ces données et d'en proposer le déchiffrement contre le paiement d'une rançon. La rançon va payer la clé de déchiffrement.

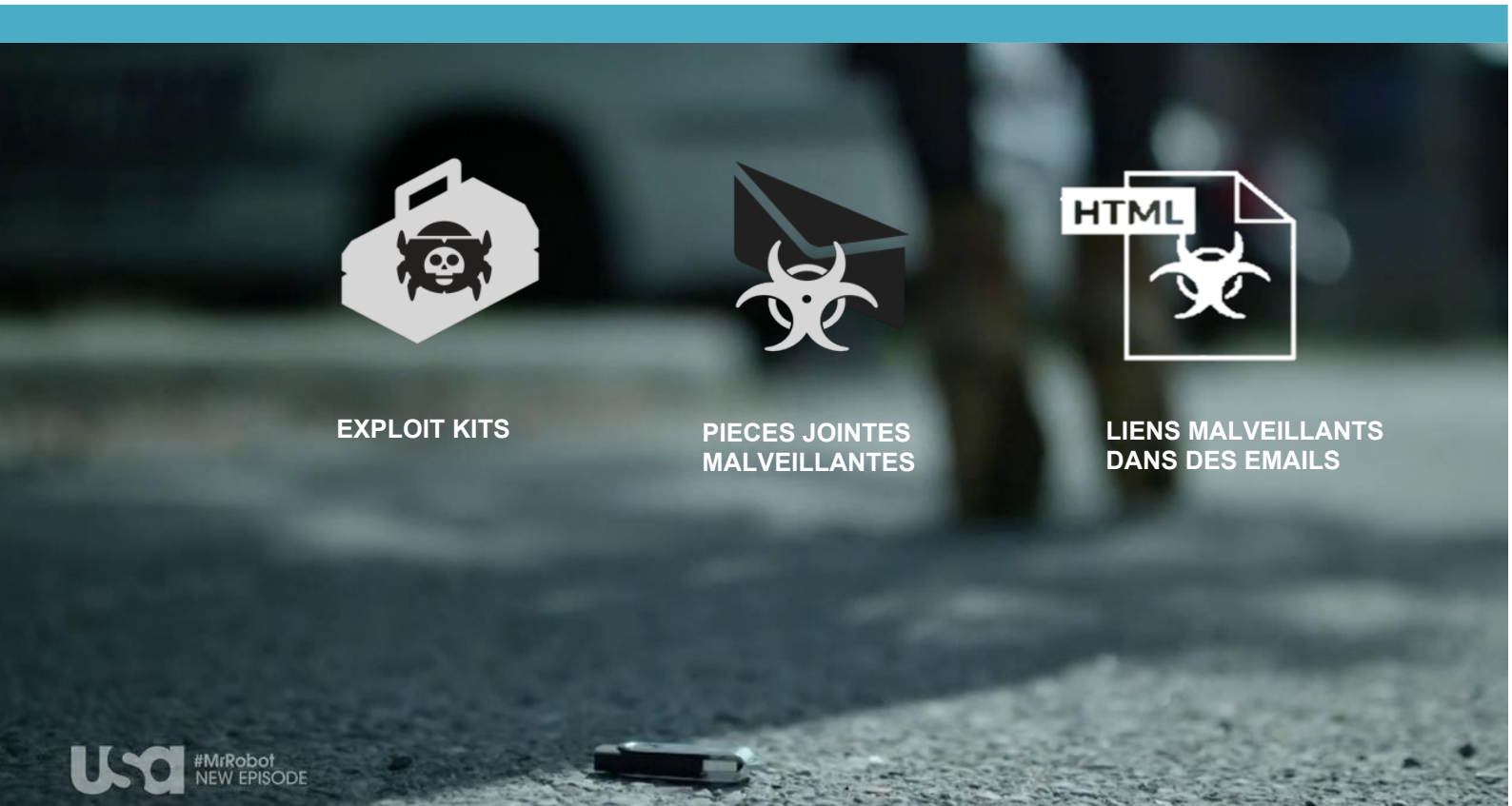
La bonne nouvelle, c'est qu'il suffit d'intervenir au niveau d'une seule de ces phases pour stopper net l'attaque.

AVEZ-VOUS VU MR. ROBOT ? (DISSEMINATION)

Pour pénétrer le système, le moyen le plus couramment utilisé par les ransomwares est l'e-mail (pièces jointes malveillantes ou lien vers des pages web corrompues). On trouve également des exploit kits : dès qu'une telle boite est ouverte, une suite d'utilitaires va s'exécuter de manière automatisée pour lancer l'infection initiale jusqu'à la livraison du malware en passant par l'exploitation des vulnérabilités.

Et bien que les utilisateurs soient aujourd'hui plutôt bien éduqués vis-à-vis de ces e-mails malveillants, on s'aperçoit vite qu'on ne peut pas se reposer sur cette bonne information. On risque en effet, d'une part, de supprimer des e-mails ou des pièces jointes valides et d'autre part, certains ransomwares se déclenchent par le simple affichage d'un message e-mail dans le panneau d'aperçu ! Et comment un utilisateur pourrait-il deviner qu'un malware peut lui être transmis par le simple affichage d'une publicité légitime sur un site grand public ?

Comme on le voit, une cyber attaque de ransomware peut utiliser plusieurs méthodes et on peut être sûr que si un des chemins est négligé par l'entreprise, c'est ce chemin qu'empruntera le malfaiteur.



La première de ces routes est bien évidemment le réseau (web et e-mail). On pense souvent que c'est la seule, mais il faut maintenant prendre en compte l'accès aux applications SaaS et en particulier le partage de fichiers en-ligne. L'équipe Unit42 de Palo Alto Networks a clairement identifié ces systèmes dans leurs études comme une source qui augmente en flèche pour la livraison de ransomwares. Et il y aura toujours des moyens de livraison directe du malware sur le terminal utilisateur (« endpoint »), soit par une attaque ultra ciblée, soit par une infection hors site (clé USB corrompue consultée par curiosité ou poste infecté dans un cyber-café avant le retour au bureau…). Il faut prendre conscience que le endpoint est la cible ultime. Le dernier champ de bataille dans un monde de brèches généralisées.

Le visionnage de la récente série télévisée américaine Mr Robot est très instructif en la matière. La série a été jugée très réaliste par des experts[4] et on peut y voir en application toutes les méthodes et vecteurs de diffusion de malware et de cyber attaques : de l'ingénierie sociale à la clé USB abandonnée sur un parking et qui finit irrémédiablement insérée dans un ordinateur de l'entité ciblée.

Pour se défendre contre les ransomwares, il faudrait aujourd'hui tout prévoir. La première chose à laquelle on pense est de bloquer en amont toute attaque : réduire la surface d'attaque, détecter qu'un fichier est un malware, et bloquer tout programme malveillant. Malgré toutes les précautions en la matière, on sait qu'on n'est jamais intégralement à l'abri d'un ransomware. Il faut donc envisager l'éventualité de devoir payer, mais surtout d'avoir à récupérer des données exploitables pour reprendre le service le plus vite possible.

[4] https://blog.avast.com/fr/les-piratages-mis-en-scène-dans-la-série-mr.-robot-sont-ils-réalistes, 20 sept. 2016 ; http://tvmag.lefigaro.fr/programme-tv/mr-robot-un-realisme-impressionnant_4ac6ac68-872e-11e6-b864-d8ad46b42f96/, 3 oct. 2016

3 ETAPES POUR SE DEFENDRE CONTRE LES RANSOMWARES

Si on remet cela dans l'ordre, si l'on veut se défendre de manière pertinente et efficace contre les ransomwares, il faut envisager trois étapes : la préparation, la prévention et la réponse.

1.

La préparation

Il s'agit là d'être prêt à une attaque qui aurait réussi. C'est-à-dire pouvoir disposer de données qui seraient non chiffrées, disponibles, donc sauvegardées efficacement et facilement récupérables, avec beaucoup de granularité. Et se préparer, c'est aussi assurer le plus de contrôle possible sur l'environnement utilisateur, sur ce qu'il peut faire, et ainsi réduire drastiquement la surface d'attaque exposée aux menaces.

2.

La prévention

Se prémunir des ransomwares, c'est faire en sorte que le malware ne puisse pas pénétrer dans le réseau à travers une cyber attaque et l'empêcher de s'exécuter lorsqu'il a atteint sa cible sur le endpoint. Il s'agit donc du contrôle réseau des attaques, donc des e-mails et des exécutables la plupart du temps et du contrôle du endpoint. On emploie ici les solutions traditionnelles de sécurité réseau et endpoint : firewall nouvelle génération (identifier et bloquer le trafic dangereux), système de détection des menaces inconnues (« zero-day ») (car les solutions basées sur des signatures ont prouvé leur inefficacité), et, comme les systèmes de sécurité réseau ne voit pas certains vecteurs, il faut pouvoir contrôler l'installation et l'exécution de malware au niveau du endpoint.

3.

La réponse (ou réaction)

En cas d'attaque réussie, il faut intervenir à quatre niveaux : d'abord comprendre l'attaque, d'où elle provient, ce qu'elle a touché ; abandonner les données chiffrées et pouvoir restaurer vite ces données dans une version suffisamment récente pour reprendre le travail, ce qui implique que la phase préparation a été bien conduite au préalable ; il faut aussi

penser à l'éventualité de céder au chantage en payant, en réduisant autant que faire se peut les délais pour récupérer les données rapidement et minimiser l'interruption de service et le manque à gagner ; prévoir possiblement de forcer le déchiffrement des données, mais on ne connaît pas de solution fiable pour l'instant sur le marché.

Miel est importateur de technologies dernier cri pour l'informatique des entreprises depuis 1985. Et c'est dans ce cadre que nous sommes en mesure de conseiller aujourd'hui notamment les solutions de quatre de nos partenaires technologiques pour préparer votre défense contre les ransomwares :

DataCore et **EVault** pour préparer vos données à cette éventualité et RES pour contrôler très finement l'environnement de travail numérique de vos utilisateurs.

Palo Alto Networks et **RES** pour réduire encore la surface d'attaque et disséminer tout au long de la chaine de frappe les mesures indispensables de cyber sécurité.

DataCore et **EVault** nous aideront également dans la phase restauration de l'accès à des données saines pour une reprise d'activité dans les meilleurs délais. Et **Palo Alto Networks** propose une solution nommée AutoFocus™ très performante pour comprendre les attaques.

LA PREPARATION

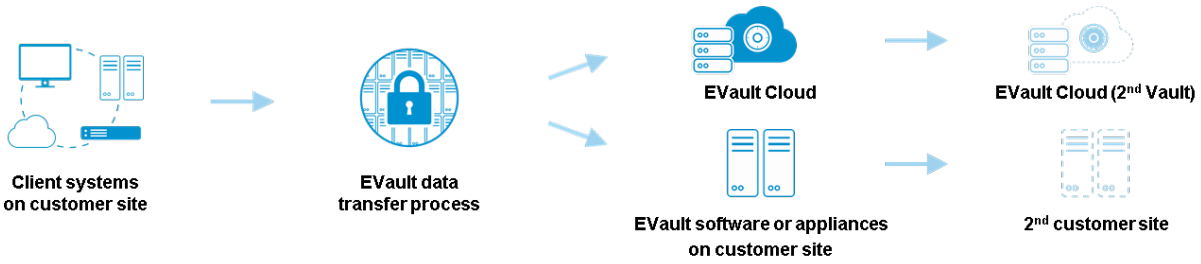
Préparer ses données

On a vu que la première mesure à prendre contre les ransomwares est de se doter d'un système de sauvegarde et restauration performant. Si on est capable de récupérer nos données dans une version précédant le chiffrement, l'activité peut être relancée avec un impact mineur sur l'organisation.

Bien-sûr, il faut que les sauvegardes se trouvent dans un emplacement non- ou difficilement accessible par les malwares. Les attaquants ciblent également les sauvegardes pour être sûrs d'arriver à leurs fins. Le système de sauvegarde choisi devra être dûment testé pour établir les procédures de restauration (*recovery process*) rapides et efficaces.

Miel promeut depuis plusieurs années la solution logicielle EVault de sauvegarde et restauration de disque à disque (www.evault.com). EVault propose une technologie brevetée sophistiquée pour protéger un réseau vraiment hétérogène : n'importe quel type de poste, n'importe quel type de serveur ; avec plusieurs options de déploiement, sur site, dans un site de réplication, ou chez un tiers *Cloud provider*. Des agents sont installés sur les serveurs et/ou les *endpoints*, qui vont initier les sauvegardes vers des serveurs dédiés EVault via des flux qui sont particulièrement optimisés. La fonction DeltaPro d'EVault va dédupliquer, compresser et chiffrer les données de bout-en-bout. La déduplication permet de réduire considérablement les échanges et de produire des fenêtres de sauvegarde

beaucoup plus courtes et réduire le besoin en stockage de deux à dix fois selon le type de données, par rapport aux solutions traditionnelles. L'aspect chiffrement des éléments transférés apporte une parfaite confidentialité des informations.



Les sauvegardes se font plus rapidement et les restaurations également en cas d'attaque réussie. A cela, EVault ajoute la fonction de réplication. Pour qu'une donnée soit en sécurité, il faut absolument qu'elle soit écrite au moins à deux endroits. Le serveur principal de sauvegarde et les données sont répliqués vers un second serveur EVault sur un autre site ou vers un Cloud de confiance. Le tout est administré à partir d'une console web très intuitive qui permet une gestion centralisée, une délégation hiérarchique des tâches, la programmation des jobs de sauvegardes, la définition des politiques de rétention, la gestion des agents et le paramétrage des points de restauration rapide, ce dernier étant crucial dans la procédure de récupération des données non corrompues le cas échéant.

Contrôler l'espace de travail numérique de l'utilisateur

La plupart des attaques vont se dérouler parce qu'un utilisateur aura malencontreusement (en général) exécuté un mauvais fichier. Il est dès lors intéressant de se doter d'une technologie qui va nous permettre de contrôler au maximum le type de fichier ou le type de *process* qui peuvent être lancés par l'utilisateur. Le leader mondial dans le domaine est RES (http://www.res.com), dont l'objectif est de proposer une mise à disposition des ressources (applications, environnement) automatisée et adaptée au contexte, qu'il s'agisse d'une espace physique ou virtuel.

Plus de GPO, plus de scripting fastidieux et mal organisé, et plus de « trous dans la raquette » en termes d'accès et de sécurisation. Ainsi chacun a toujours accès à ce dont il a besoin pour faire son travail et surtout, il n'a pas accès à ce qui ne lui est pas autorisé. On peut donc :

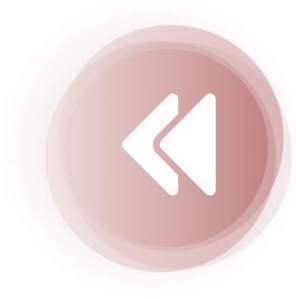
1. Personnaliser l'espace de travail en fonction du contexte de manière automatisée
2. Imposer des listes blanches et listes noires pour n'autoriser que ce qui est nécessaire à la productivité de l'utilisateur
3. Adapter automatiquement les autorisations en fonction de l'identité, du lieu, du moment, sur des environnements locaux, centralisés ou virtuels.

La technologie RES n'est pas perçue comme une solution de sécurité, mais, de fait, elle participe grandement au contrôle de l'activité de l'utilisateur. Et en la matière, les préconisations de cet éditeur sont très pertinentes. L'éducation des utilisateurs est certes fondamentale, pour limiter les comportements dangereux comme les clics intempestifs sur des éléments malicieux, et pour expliquer pourquoi l'on réduit le champ d'utilisation au strict nécessaire à l'employé. RES propose même d'envoyer de faux e-mails malveillants aux utilisateurs et d'aller à la rencontre de ceux qui auront eu le mauvais réflexe.

Et, grâce à RES, on va réduire la surface d'attaque exposée aux ransomwares via les fonctions suivantes :

1. Whitelisting / blacklisting
2. Généralisation du « *Read Only* »
3. Protection des disques USB
4. Protection site web et réseau

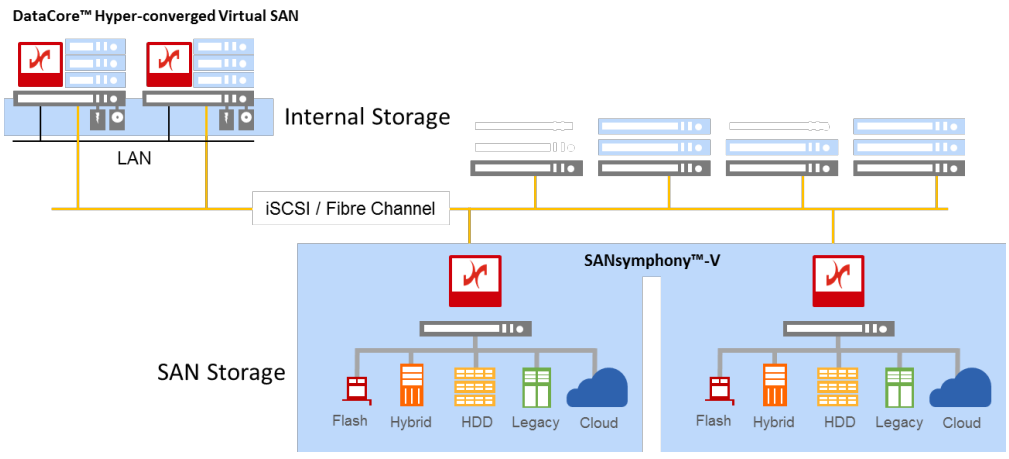
Mais à ce stade, on entre dans la phase préventive de notre défense contre les ransomwares, que nous détaillerons plus loin.



Prévoir un bouton « marche arrière » pour retrouver ses données

Dans notre phase de préparation, nous nous intéressons toujours aux données à mettre à l'abri. Et qui dit données, dit stockage. C'est pourquoi nous mettons en avant également à ce stade la solution de gestion du stockage de DataCore qui plait à un public d'entreprises toujours plus nombreuses. Cette solution de Software-Defined Storage (SDS) est une couche logicielle qui repose au-dessus de l'ensemble du stockage et agit comme un hyperviseur de virtualisation des matériels de stockage. L'objectif de DataCore est de supprimer les silos de stockage, de sorte que la capacité de stockage soit regroupée en un pool unique global, quels que soient les supports de stockage à disposition, y compris hétérogènes. Et de présenter cette capacité de stockage simplement aux applications qui en ont besoin, avec des fonctionnalités constantes gérées de manière globale. Parmi les plus pertinentes, on peut citer la réplication, la réplication synchrone, l'allocation granulaire, des techniques d'écritures qui vont multiplier les performances de manière stupéfiante, mais tel n'est pas le sujet de notre présent document.

Cependant, certaines de ces fonctions indépendantes du matériel vont nous servir dans le cadre de la défense contre les ransomwares. Deux choses principalement : les *snapshots* et le CDP (*Continuous Data Protection*).



Le *snapshot* est bien connu au sein des systèmes d'exploitation, pour prendre la photo des données à un instant t, mais dans le cas de DataCore, on va le capturer au niveau SAN et cela va offrir de nombreux avantages : on ne dépend pas du logiciel sur l'hôte qui gère les fichiers, on ne consomme pas les ressources du système hôte, on n'a pas besoin d'avoir une baie de disques compatible, c'est également plus économique car on peut faire un *snapshot* du contenu d'une baie tier-1 et le placer dans un matériel tier-2 ou tier-3. Enfin, grâce à cette virtualisation, on consomme moins pour les *snapshots* parce qu'on va les paramétrer pour ne capturer que les changements par rapport à la source originale. Cela apporte une granularité importante pour, plus tard, récupérer les données suite à une éventuelle attaque par ransomware.

Et pour notre défense contre cette menace, la fonction CDP du logiciel DataCore SANsymphony-V va nous être d'une grande utilité également. On la regardera en détail plus loin au chapitre de la réponse au ransomware. Mais l'essentiel à ce stade est de mettre en place cette fonction pour pouvoir récupérer les données. C'est une fonction puissante, sans coût ni ressource additionnels, sans prendre de sauvegarde explicite, grâce à un enregistrement des I/O et un horodatage de ces I/O qui permet de revenir jusqu'à 14 jours en arrière, directement, à la seconde près dans les données de production.

Une bonne préparation repose donc sur une bonne gestion du stockage, un système de sauvegarde fiable et efficace et à un environnement utilisateur maîtrisé.

Réduire la surface d'attaque

Avec RES, on réduit la surface d'attaque par le contrôle de l'espace de travail numérique de l'utilisateur et on met en place toute une série de mesures pour prévenir la pénétration ou le lancement d'une chaine de frappe. Les utilisateurs ne doivent pouvoir utiliser que les bonnes applications au moment où ils en ont besoin, et seulement celle-là.

Cela va se traduire par l'imposition d'une **liste blanche** et de **listes noires**, empêchant toute exécution de programmes non explicitement autorisés.

Par défaut, nous pouvons généraliser le mode « ***Read Only*** » pour restreindre les possibilités de lancement de tâches malicieuses.

Il est crucial de protéger ou restreindre l'accès aux **disques amovibles** qui, on l'a vu, est un vecteur de menace des plus courant.

Autre vecteur, les **macros**, vont être désactivées par défaut à chaque démarrage de Microsoft Office pour éviter des activités masquées et responsabiliser l'utilisateur vis-à-vis de leur lancement. Ce qui rejoint l'action complémentaire de la technologie Traps™ de Palo Alto Networks sur le *endpoint* que nous étudierons plus loin.

La maîtrise des **privilèges d'administration** d'un poste virtuel ou physique peut être assurée avec RES, pour qu'un malware qui s'en empare n'ai pas les droits pour se disséminer. On peut les limiter par défaut, les étendre selon le contexte ou sur demande, de manière temporaire.

Côté réseau, il est possible de ne laisser les applications communiquer que sur les **ports** et serveurs nécessaires.

Et il est facile de **tracer** qui a eu accès à quels systèmes et à quel moment à partir des logs sur les processus utilisateur.

Le nouveau vecteur que représentent les applications Cloud peut également être mieux contrôler grâce à l'automatisation des tâches d'enrôlement (*on-boarding*) et de retrait (***off-boarding***) des utilisateurs du

système d'information de l'entreprise. Afin d'éviter qu'un employé parti puisse garder trop longtemps ses accès aux applications SaaS hors domaine par exemple.

Beaucoup d'entreprises ont mis en place les fonctions de RES historiquement pour maitriser notamment des sessions Windows centralisées (ou non) avec Microsoft ou Citrix et elles s'aperçoivent aujourd'hui que cela leur apporte de fait une protection efficace sur ces environnements qui sont sous contrôle.

Maintenant, il faut pouvoir étendre la vision de la sécurité informatique à tout ce qu'on ne contrôle pas directement. La révolution numérique actuelle a ouvert les réseaux d'entreprise à tous les vents, en imposant de nouvelles pratiques comme les réseaux sociaux, les applications Cloud, les politiques BYOD ou CYOD (Bring Your Own Device/Choose Your Own Device), la mobilité, le shadow IT (informatique fantôme).

Repenser sa cyber sécurité

Palo Alto Networks est un des tout premiers champions de la cyber sécurité aujourd'hui (www.paloaltonetworks.com). C'est la société qui a introduit le concept de Firewall nouvelle génération (NGFW) pour prendre en compte les nouvelles réalités auxquelles doivent faire face les entreprises. Elle propose l'autorisation, la validation des applications en toute sécurité, la visibilité du trafic, le contrôle du endpoint et le blocage des menaces inconnues.

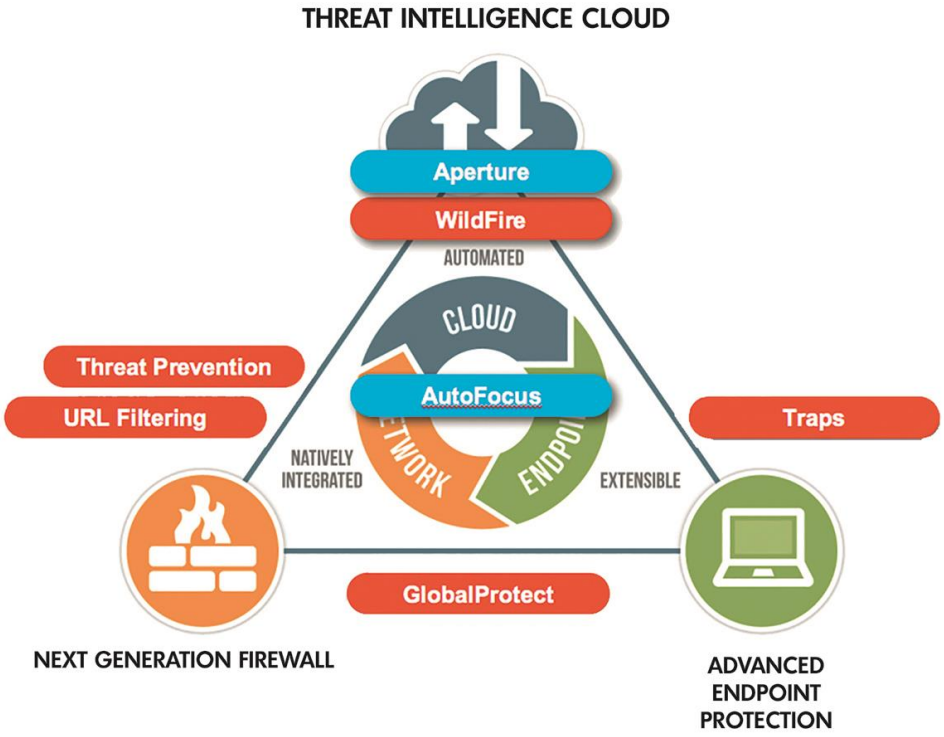
Concernant ce dernier point des cyber attaques et en particulier des ransomwares pour ce qui nous occupe, Palo Alto Networks définit trois conditions que toute bonne solution de sécurité se doit de respecter pour prévenir complètement et efficacement les menaces modernes :

1. Réduire la surface d'attaque en limitant au maximum les chemins potentiels : les applications, les utilisateurs, avec des règles précises
2. Des éléments dangereux passeront malgré tout et il faut déjà supprimer toutes les menaces connues, référencées (malwares, virus, URLs, etc.) en se basant sur les signatures partagées
3. Mais on constate que seul 30% des menaces sont connues. Les pirates innovent constamment, générant sans cesse de nouvelles variantes, cherchant à exploiter les milliers de nouvelles

vulnérabilités créées chaque mois. Il faut démasquer une nouvelle menace inconnue au moment où elle se présente et dès lors nourrir avec cette identification les étapes précédentes, règles réseau et bases de connaissance des cyber menaces.

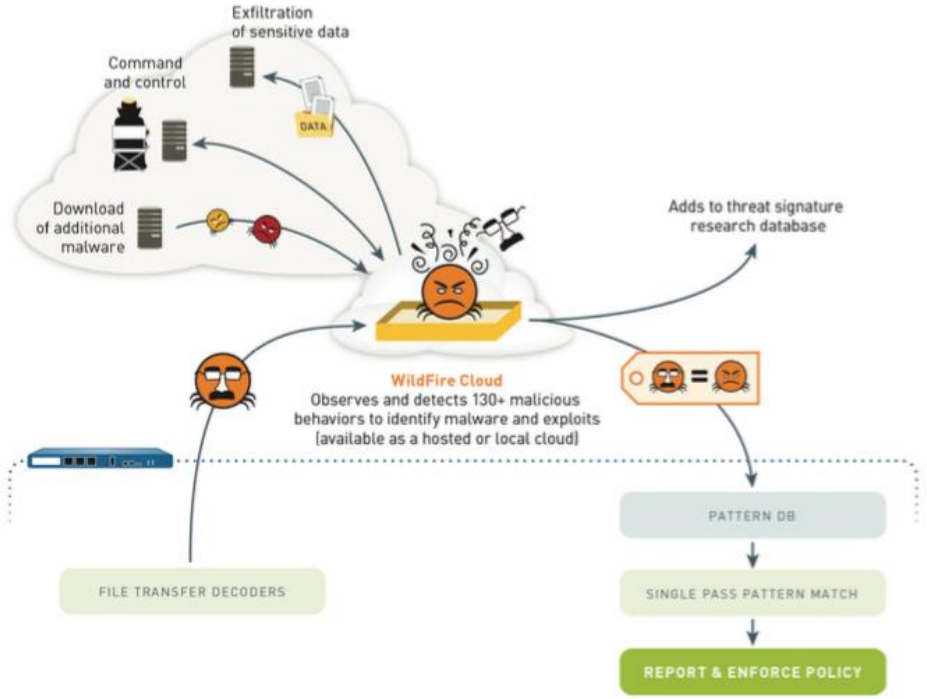
Palo Alto Networks propose bien-sûr l'infrastructure qui défend tous les points et auto-alimente ses bases de connaissance. On contrôle, l'usage, les applications, les utilisateurs, et le système est reprogrammé à la volée quand apparaissent de nouveaux dangers qu'il a identifiés. La sécurité informatique de l'entreprise est ainsi repensée, avec trois composants essentiels et complémentaires :

Le firewall nouvelle génération qui valide, à la vitesse du fil, les applications, les utilisateurs qui échangent sur le réseau physique, à l'intérieur du data center virtualisé ou même à travers le Cloud. Il va appliquer les règles définies et se référer aux bases de signatures auxquelles l'entreprise a souscrit pour bloquer les malwares, exploit kits, flux de Command & Control, URLs connus.



Le firewall coopère avec **un système Cloud d'analyse et d'identification** des éléments douteux, nommés WildFire et PANDB (URL Filtering). Il les leur communique pour vérification, et si une nouvelle menace est révélée,

l'information est partagée avec les 35000 firewalls nouvelle génération connectés au service dans les cinq minutes qui suivent.



Cette intelligence collective va également bénéficier aux appareils endpoints équipés du logiciel Traps de Palo Alto Networks. Traps est capable d'actions qui sont aujourd'hui les plus avancées en termes de **protection du poste client**. Avec deux modules : la protection contre l'exploitation des vulnérabilités et l'anti-malware. Au lieu d'essayer de détecter et combler les centaines de vulnérabilités possibles sur le *endpoint*, on va plutôt se concentrer sur les méthodes d'exploitation de ces failles car elles sont finalement très peu nombreuses et il n'en apparaît de nouvelles que très rarement. Cette technique a l'avantage de bloquer les attaques *zero-day* puisque, même si leur signature est encore inconnue, on va tout-de-même immédiatement repérer leur mode opératoire et intervenir tout-de-suite. On partage alors avec WildFire le contexte de la vulnérabilité qu'il a cherché à exploiter.

Le fonctionnement de Traps opère sur tout type de malware bien entendu. Elle est certes valable contre les ransomwares mais on peut admettre que si désagréables qu'elles soient, les attaques par ransomwares ne sont pas fatales si on peut récupérer ses données, en payant ou en les restaurant. En revanche, Traps, en nous signalant l'infection par ransomware, doit

alerter l'entreprise sur le fait qu'il a pu entrer et que des malwares beaucoup plus violents, beaucoup plus néfastes pourraient se disséminer !

L'agent Traps ne fait pas de scan, ne reçoit pas de mise à jour de signatures, pèse à peu près 35 Mo et prend environ 0,1% de CPU, pour une couverture de protection bien supérieure à celles des anti-virus. Tout programme qui tente de se lancer va passer au crible de Traps.

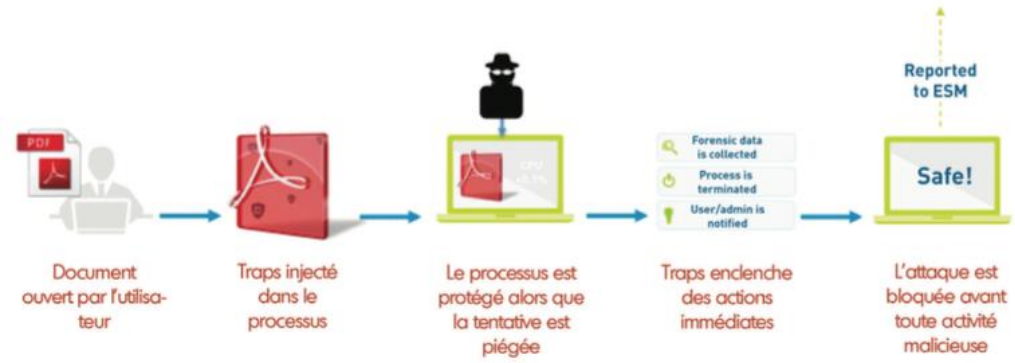
On peut limiter l'exécution depuis un support USB, ou interdire la création de processus secondaires dans des macros, par exemple.

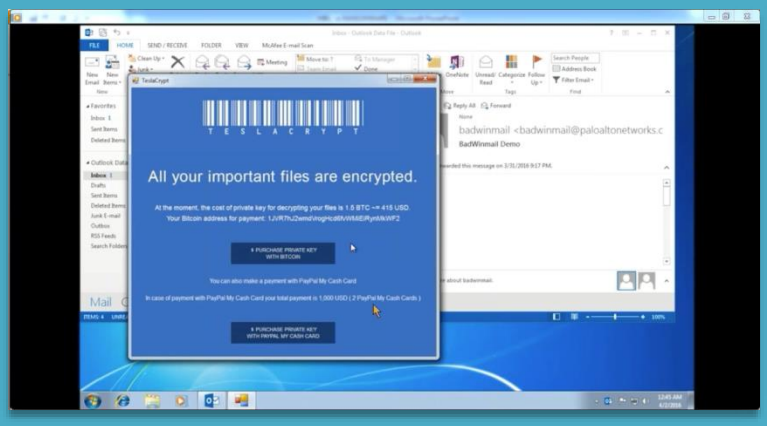
On peut établir des listes d'éditeurs de confiance ou interdire l'exécution de fichiers non signés par les éditeurs

Si on est connecté à WildFire, on peut envoyer un hash identifiant le fichier au service pour savoir s'il le connaît et le juge bénin ou malicieux

Se référer aux modèles génériques (patterns) de menace fournis par WildFire pour une analyse statique

Et finalement l'envoyer à WildFire pour analyse et partager le résultat avec tous les systèmes connectés.





Visionnez notre démo sur la chaine YouTube de Miel https://youtu.be/7EcJlJX9sxc

LA REPONSE (OU REACTION)

Comme évoqué, on peut essayer de forcer le déchiffrement des données chiffrées par le ransomware. Mais à ce jour, aucune technologie n'a prouvé son efficacité et cela risque de ne se traduire qu'en une perte de temps précieux.

Payer ?

On peut encore choisir de payer la rançon demandée, souvent volontairement modeste. D'ailleurs, aux tout débuts du phénomène, le FBI américain suggérait aux victimes de payer. Encore faut-il être prêt, avec son service financier, à effectuer ce règlement dans les monnaies Internet et dans un délai rapide. N'oublions pas, tout-de-même, que nous avons affaire à des malfaiteurs et ne pouvons donc compter sur aucune garantie de recevoir en échange la clé de déchiffrement. Cela pourrait même encourager ces criminels à récidiver : s'ils ont réussi une fois à pénétrer votre réseau, il devrait pouvoir le faire une seconde fois. C'est pourquoi le FBI conseille désormais de se prémunir contre cette menace en sauvegardant ses données et en renforçant la cyber sécurité.

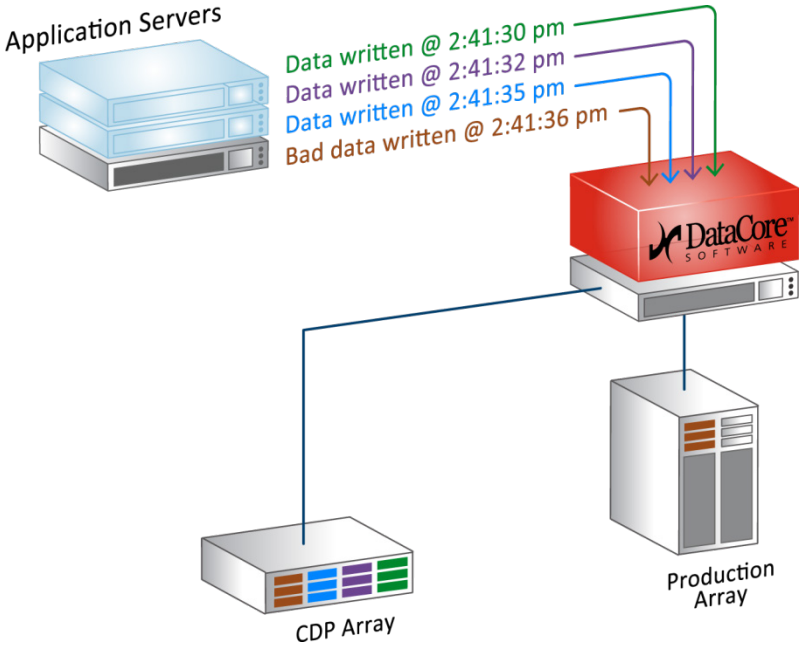
Restaurer des données saines

Répondre à une attaque par ransomware réussie, c'est donc avant tout pouvoir compter sur une solution de sauvegarde fiable qui nous permet de restaurer les données les plus récentes possible et dans le délai le plus court. Il faut bien-sûr avoir détecté l'heure de l'attaque, avoir coupé la sauvegarde ou, le cas échéant, le lien vers la sauvegarde secondaire.

Ainsi EVault apporte la granularité, la capacité de rétention et la facilité de récupération nécessaire. On va pouvoir restaurer la dernière sauvegarde fiable à partir des serveurs Evault primaires ou secondaires.

Si on a mis en place la solution de virtualisation du stockage de DataCore, on peut utiliser la fonction CDP (Continuous Data Protection) pour être capable de

récupérer directement la donnée de production. La sauvegarde est indispensable comme on l'a vu, mais sa restauration implique de ramener les données d'ailleurs, de réhydrater ces données (elles ont été compressées). L'idée de CDP est d'enregistrer en temps réel chaque I/O avec l'horodatage correspondant dans un volume protégé. On obtient ainsi un vrai volume de roll-back, nous permettant de faire un retour rapide, comme sur la barre de défilement d'un film, et de reprendre le fil avant l'événement. L'événement étant ici le chiffrement des données par le ransomware. DataCore permet de revenir jusqu'à 14 jours en arrière et de reprendre l'activité de manière quasi-instantanée à partir de ce point avec des données non chiffrées.



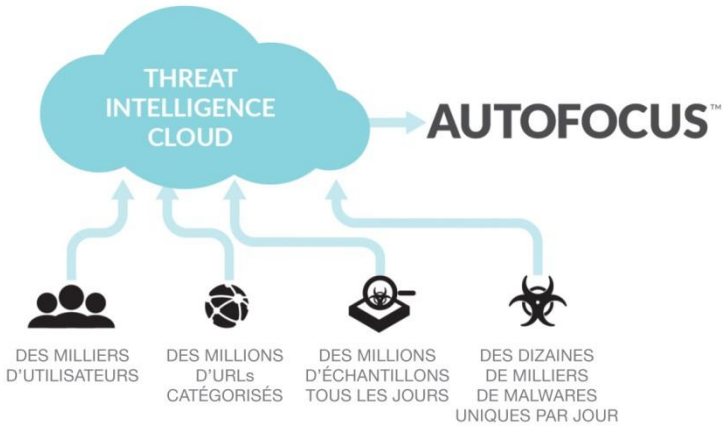
Pour les entreprises déjà équipées de DataCore, il s'agit d'un surcoût mineur en regard des du service rendu, et pour les autres, c'est un argument supplémentaire pour envisager de s'équiper d'un tel système de stockage piloté par logiciel (Software-Defined Storage), l'argument numéro un étant la simplification de la gestion et de l'évolution du stockage et le numéro deux le gain en performances.

Analyser l'attaque

Côté prévention, le risque zéro n'existe pas et il restera toujours une chance pour qu'une cyber attaque réussisse. Et dans ce cas, il faut pouvoir

réagir en analysant la menace, en déterminant quel a été le point d'entrée, quel a été le point faible, s'il s'agit d'une attaque classique dont on pourrait encore être la cible, et à quelle famille de malware, de ransomware dans notre cas, on a eu affaire. C'est pourquoi Palo Alto Networks propose le système AutoFocus™ dont l'objectif est avant tout d'accélérer très fortement la vitesse d'analyse de la menace et la vitesse du workflow de la réponse. AutoFocus va s'appuyer pour cela sur l'ensemble des informations collectées sur les menaces par le Cloud WildFire, sur le travail du laboratoire Unit42 de Palo Alto Networks et d'autres services similaires d'analyse des cyber menaces de par le monde pour lancer des analyses de type big data.

On peut alors alerter l'entreprise. Non pas pour signaler qu'il y a un malware, mais plus précisément pour annoncer que TeslaCrypt est dans son réseau, qu'il faut y prêter attention et même en faire une priorité. C'est une analyse synthétique de la menace dont on fait l'objet, et une comparaison avec les phénomènes similaires touchant les autres clients. Une fois reçue cette notification, on est en mesure d'avoir tous les détails sur cette famille de ransomware : quelles sont les clés de registre, d'où l'attaque a été lancée, quels sont les indicateurs de compromission, est-ce que cela fait partie d'une campagne globale contre une catégorie de cible ; autant d'informations d'une grande valeur pour décider des mesures à



prendre. Enfin, les renseignements sont corrélés avec les autres attaques similaires et un rapport est fourni automatiquement pour permettre aux intervenants, équipes sécurité, équipe SOC, partenaires de redéfinir la politique de prévention des menaces de l'entreprise.

AutoFocus va nous dispenser d'une analyse alerte après alerte, de milliers d'informations et de logs qui prendrait des heures en interrogeant de multiples sources, des outils opensource, des données publiques, de scripts, etc. La solution de Palo Alto Networks s'enclenche automatiquement et fournit l'analyse en quelques minutes.

CONCLUSION : TENEZ-VOUS PRET

La protection contre les infections par ransomware nécessite une mobilisation de tous les instants des équipes informatiques et de toutes les parties du système.

Préparez vos données : assurez une sauvegarde et une restauration des données rapide, granulaire, simple et sécurisée.

Prévenez l'infection en repensant votre architecture de sécurité pour réduire la surface d'attaque, éliminer les menaces connues et inconnues, du réseau au *endpoint.*

Réagissez vite en cas d'attaque réussie : minimisez les temps de rupture de service, et analysez très vite les failles pour empêcher la prochaine attaque.

Comprenez les avancées proposées par nos partenaires technologiques DataCore, EVault, Palo Alto Networks et RES en vous rendant sur leurs sites :

www.datacore.com

www.evault.com

www.paloaltonetworks.com

www.res.com

A PROPOS DE MIEL

Créée en 1985, Miel découvre et introduit sur le marché français les nouvelles technologies à l'attention des services informatiques des entreprises, dans les domaines de la sécurité, des réseaux, de la virtualisation et du stockage. Souvent originaires des Etats-Unis, les fournisseurs choisis proposent des avancées spectaculaires dans la manière d'assurer la productivité de l'informatique vis-à-vis des directions générales.

http://info.miel.fr/blog

retrouvez la version électronique de ce document

https://goo.gl/tNSxyp

appelez 01 60 19 34 52

MIEL – PARC BUROSPACE 5 – 91571 BIEVRES CEDEX – WWW.MIEL.FR