STORMSHIELD

VISION : MULTILAYER COLLABORATIVE SECURITY*

COORDONNER LES SYSTÈMES DE PROTECTION POUR ÉLEVER LE NIVEAU DE SÉCURITÉ GLOBALE ET RÉPONDRE AUX ATTAQUES LES PLUS ÉVOLUÉES

* La sécurité collaborative multi-couches

Livre blanc

NETWORK SECURITY I ENDPOINT SECURITY I DATA SECURITY

Difficilement détectables, **les dernières attaques avancées requièrent une protection multi-couches**. Les solutions de sécurité de l'entreprise doivent être soigneusement intégrées et coordonnées.

Les attaques en réseau, toujours plus élaborées, deviennent de plus en plus difficiles à détecter. Très discrètes, ces nombreuses menaces combinent plusieurs vecteurs d'attaques pour atteindre leur objectif.

Une fois la victime identifiée, ce type d'attaque démarre souvent par l'utilisation d'un premier vecteur d'intrusion considéré comme anodin. A ce stade, la victime ne se rend pas compte qu'elle subit une attaque qui est passée totalement inaperçue pour les systèmes de protection en place. L'attaque va ensuite s'étendre au sein de l'entreprise cible au moyen de plusieurs techniques distinctes et successives afin d'aboutir à l'objectif fixé (corruption de serveur, exfiltration de données, …). Le délai entre le démarrage de l'attaque et l'atteinte de l'objectif forme une des caractéristiques des **attaques avancées persistantes ou APT (Advanced Persistent Threat).**

DES PROTECTIONS À COORDONNER

Ces attaques avancées sont conçues pour contourner les systèmes de protection traditionnels et la combinaison de différentes solutions de sécurité sous forme de silo n'est d'ailleurs pas suffisamment efficace. Cependant, ces attaques laissent un certain nombre de traces que l'on peut qualifier de signaux faibles comme par exemple l'accès à un site web non catégorisé.

En associant ces signaux faibles entre eux et en les corrélant avec une cartographie des vulnérabilités, on peut identifier la menace qui révèle ainsi son véritable caractère critique. Il est **donc possible de combattre ces attaques multi niveaux en associant et faisant inter-agir plusieurs couches de protection.**

En pratique, on peut y parvenir de deux façons distinctes. La première consiste à corréler les événements au travers de solutions de type SIEM. Les événements et incidents de sécurité sont collectés puis analysés afin d'identifier un comportement anormal. Cependant, la corrélation d'événements ne peut se faire qu'une fois que l'attaque a eu lieu. On ne peut agir sur la politique de sécurité que de manière réactive.

La seconde façon, avec une approche basée sur l'intégration des moteurs de sécurité et une véritable interaction entre les différentes solutions de défense, les différents moyens de protection collaborent entre eux en échangeant des données et analysent un comportement en fonction des autres événements détectés. **La corrélation s'effectue en temps réel et les différents signaux faibles sont pris en compte dans leur globalité.** Le niveau de protection se trouve ainsi renforcé et la politique de sécurité peut s'adapter de façon dynamique. Les comportements anormaux peuvent alors être bloqués plus rapidement voire même de façon proactive.

Cette approche constitue le fondement de la vision de Stormshield pour répondre aux nouvelles menaces.

SOMMAIRE

Comprendre les attaques avancées

- Un environnement ouvert aux plateformes vulnérables
- Une menace bien organisée
- Personne n'est à l'abri
- Une mine de renseignements en ligne
- Les trois phases de l'APT

Choisir une protection multi-couches

- Les limites de la protection en silos
- La corrélation d'événements
- L'approche multi-couches
- La protection collaborative
- La protection contextuelle
- La protection globale

L'approche Stormshield

Comprendre les attaques avancées

Soigneusement préparée, une attaque avancée profite des vulnérabilités pour s'immiscer dans le réseau interne, repérer de nouvelles cibles puis **désactiver des services cruciaux ou voler des données sensibles**.

UN ENVIRONNEMENT OUVERT AUX PLATEFORMES VULNÉRABLES

En trois décennies, le paysage numérique s'est transformé: l'informatique devient un bien de consommation courante, le PC, le smartphone puis la tablette tactile transformant, tour à tour, les usages privés et professionnels. Le Web et les réseaux sociaux bouleversent également nos habitudes de communication et de collaboration. La création et la diffusion d'informations sont simplifiées; tout le monde peut partager ses contenus et interagir avec son environnement.

Cet environnement ouvert et connecté en permanence est une véritable opportunité pour la malveillance informatique. Le niveau de sensibilisation des utilisateurs ayant augmenté, les hackers doivent trouver des techniques plus élaborées pour parvenir à leurs fins. Ils exploitent des vulnérabilités présentes sur des sites légitimes ou dans des pièces jointes d'e-mail pour infecter les postes de travail des utilisateurs qui les consultent. Les codes malicieux utilisés par les hackers exploitent fréquemment des vulnérabilités de type Zero-day, et plus particulièrement celles présentes dans les applications les plus utilisées pour consulter des documents ou des contenus Web.

Chaque jour, de nouveaux sites Web sont pris pour cible dans le but d'injecter et d'héberger des codes malveillants. Ces codes détournent les nombreuses vulnérabilités des navigateurs Web et de leurs composants associés, tels Flash ou Java, pour compromettre les postes des internautes.

L'amélioration des techniques d'attaque répond également à l'évolution des moyens de protection. Le principe actuel consiste soit à utiliser des codes malveillants totalement inconnus soit à combiner plusieurs techniques qui présentent un niveau de gravité suffisamment faible pour passer au travers des filtrages mis en place.

UNE MENACE BIEN ORGANISÉE

La cybercriminalité est devenue une véritable économie souterraine avec ses organisations, ses sources de financement dédiées et ses propres monnaies. Les objectifs de la cybercriminalité sont variés :

- La cyber guerre, la déstabilisation politique, le cyber espionnage au profit d'organisations étatiques,

- L'activisme politique ou idéologique (Anonymous ou Lultsec),
- Le gain financier (rançons, chantage, vol et revente de données, « services » de piratage ou d'attaques),

Cette cybercriminalité est souvent très bien préparée pour réaliser des attaques efficaces et ciblées. Pour réussir une campagne malveillante, l'objectif et la cible sont conjointement et soigneusement sélectionnés.

Le tableau 1 révèle que les attaques APT frappent indifféremment des ministères, des journaux, des sociétés de l'industrie informatique, des loisirs et de l'énergie.

Attaque	Année	Vecteur	Objectifs	Cible(s)	Sources suspectées
Stuxnet	2008	Clé USB et ver attaquant un système de contrôle industriel Siemens	Sabotage industriel par le biais des centrifugeuses	Industrie Nucléaire en Iran	USA et Israel
Opération Aurora	2009	Vulnérabilités Zero-day et porte dérobée	Vol de codes sources de multinationales innovantes	Bases de codes d'Adobe, Google, Juniper, Rackspace, etc.	Chine
Bercy (Ministère de l'Economie, des Finances et de l'Industrie)	2010	Pièce jointe PDF avec cheval de Troie	Collecte d'informations sur le G20	150 systèmes infectés	Asie
RSA	2011	Logiciel malveillant Htran	Vol d'informations au sujet des token SecurID	Réseau de la filiale sécurité du groupe EMC	Chine
New York Times	2013	Attaque 'spear-phishing' : email avec liens malicieux	Vol de mots de passe et de fichiers des journalistes	Bureaux du quotidien	Chine
Sony Pictures	2014	Spear-phishing probable avec cheval de Troie et rançongiciel	Destruction de fichiers, vol de données privées et de films inédits	Serveurs de production des studios	Corée du Nord

Tableau 1
Quelques attaques APT médiatisées depuis 2008

PERSONNE N'EST À L'ABRI

La cybercriminalité sous toutes ses formes tire profit de l'interconnexion des systèmes d'informations d'entreprises de toutes tailles, regroupées au sein d'écosystèmes informatiques. Par conséquent, aucun fournisseur, ni aucun partenaire commercial ou technologique n'est à l'abri.

Pour contourner la vigilance de l'entreprise ciblée, le hacker s'appuie sur les réseaux informatiques tissés entre les TPE et PME coopérant en toute confiance. En compromettant une machine d'un partenaire ou d'un sous-traitant, c'est l'écosystème complet qu'il met en péril.

Face à la diversité des objectifs de la cybercriminalité, la plupart des plus petites structures sont également concernées. En effet, les données financières des clients d'un cabinet comptable, les informations des patients d'un centre médical ou encore les secrets de fabrication d'un bureau d'étude sont autant de données à protéger. De plus, un incident de sécurité sur le système d'information d'une petite structure peut très vite conduire à l'arrêt de son activité, tant cette dernière est devenue dépendante de l'outil informatique.

UNE MINE DE RENSEIGNEMENTS EN LIGNE

L'explosion des réseaux sociaux facilite la collecte d'informations sur la victime et augmente les chances de réussite de l'attaque. Une fois que l'entreprise cible a été choisie et les objectifs définis, l'attaquant cherche à identifier la victime de la primo attaque, généralement une personne de l'entreprise active sur les réseaux sociaux. Le but est d'identifier la façon de tromper la vigilance du collaborateur ciblé.

Cette phase d'ingénierie sociale permet d'identifier le vecteur de l'attaque, par exemple, un e-mail au contenu ciblé ou une clé USB laissée intentionnellement sur un lieu fréquenté par la victime.

LES TROIS PHASES DE L'APT

Les menaces les plus élaborées sont relayées par une APT ou attaque avancée persistante (Advanced Persistent Threat). Très ciblée, l'APT combine plusieurs vecteurs d'attaque et opère en trois temps pour se rendre indétectable.

Une APT se prépare en choisissant l'entreprise cible et sa victime. Une étude d'ingénierie sociale détermine le vecteur idéal de la primo attaque, afin d'augmenter ses chances de réussite. Puis, l'attaque démarre par une primo infection qui profite des vulnérabilités des applications du poste de travail de la victime. Le vecteur de l'at-

taque, un e-mail ou une clé USB, contient soit un document attaché et spécifiquement forgé soit un lien vers un site Web malveillant.

Une fois le poste de travail de la victime infecté, la phase d'expansion vise à atteindre la machine ou bien les données ciblées. La première charge virale peut être modifiée pour établir un canal de commande et contrôle et chercher à compromettre d'autres machines connectées au réseau. Enfin l'attaque persistante avancée entre dans sa troisième phase afin de mettre en œuvre l'action définie. A ce stade, l'attaque devient active pour mettre un serveur hors service ou encore extirper des données confidentielles. Si un serveur mis hors service révèle rapidement l'attaque, en revanche, la fuite de données peut être progressive; l'attaque persiste alors et reste indétectable.

Prenons l'exemple d'un salarié chargé des expéditions. L'ingénierie sociale permet d'identifier le poste de travail de cette victime et le nom d'un transporteur logistique habituel. Pour faire croire à l'employé qu'il lit un message officiel, l'e-mail malveillant usurpe l'identité du transporteur et renferme une pièce jointe plausible, un bon de livraison par exemple.

PHASE 1 :
LA PRIMO INFECTION

Les codes malicieux s'appuient sur les vulnérabilités d'applications courantes telles que les navigateurs web et les outils de bureautiques (Office, PDF). Les failles des navigateurs Web et de leurs compléments logiciels constituent une cible toute particulière puisqu'une attaque Web sur trois exploite ainsi les vulnérabilités de plugins Java.

Les codes malicieux peuvent également être véhiculés par des documents joints aux e-mails. La victime ouvrira un document attaché ou naviguera sur un site Web corrompu, installant à son insu le code malveillant. Cette installation étant silencieuse, la victime ne se rend compte de rien.

En reprenant notre exemple, le chargé des expéditions croit ouvrir un bon de livraison ordinaire. L'ouverture du document exploite une faille système pour installer discrètement un code malveillant.

PHASE 2 :
L'EXPANSION

La primo infection constitue le point d'entrée de l'attaque persistante avancée qui va chercher ensuite à s'étendre au sein de l'entreprise ciblée. L'APT combine plusieurs vecteurs pour trouver différents points d'ancrage et atteindre l'objectif fixé. Ces points d'ancrage sont généralement initiés par l'établissement d'un canal de commande et contrôle entre l'attaquant et les machines compromises. Ce canal va permettre de modifier à distance le comportement de la charge malveillante. La machine infectée établit ainsi une connexion légitime vers un serveur inconnu de commande et contrôle.

La phase d'expansion s'effectue sur deux axes simultanés :

- La charge malicieuse est transformée au travers du canal de commande et contrôle. Il peut mettre à jour le malware pour ajouter des fonctionnalités afin de pénétrer plus efficacement l'entreprise cible. Il peut aussi tenter d'élever des privilèges ou lancer une exécution arbitraire de code pour établir des connexions réseaux sur d'autres machines voire rejouer une phase d'authentification.
- Le nombre de machines infectées augmente : le code malveillant ou le canal de commande et contrôle inconnu sert de relai pour la recherche de nouvelles machines vulnérables. Cette phase combine différents vecteurs d'attaques et cherche à compromettre des machines potentiellement moins protégées.

La propagation de l'attaque a pour but d'atteindre la cible fixée par avance, un serveur de transactions financières ou une base de données. Cette cible une fois localisée, l'APT entre dans sa dernière phase. L'attaque devient réellement active et, dans certains cas seulement, détectable.

PHASE 3 : LA COMPROMISSION OU LA FUITE DE DONNÉES

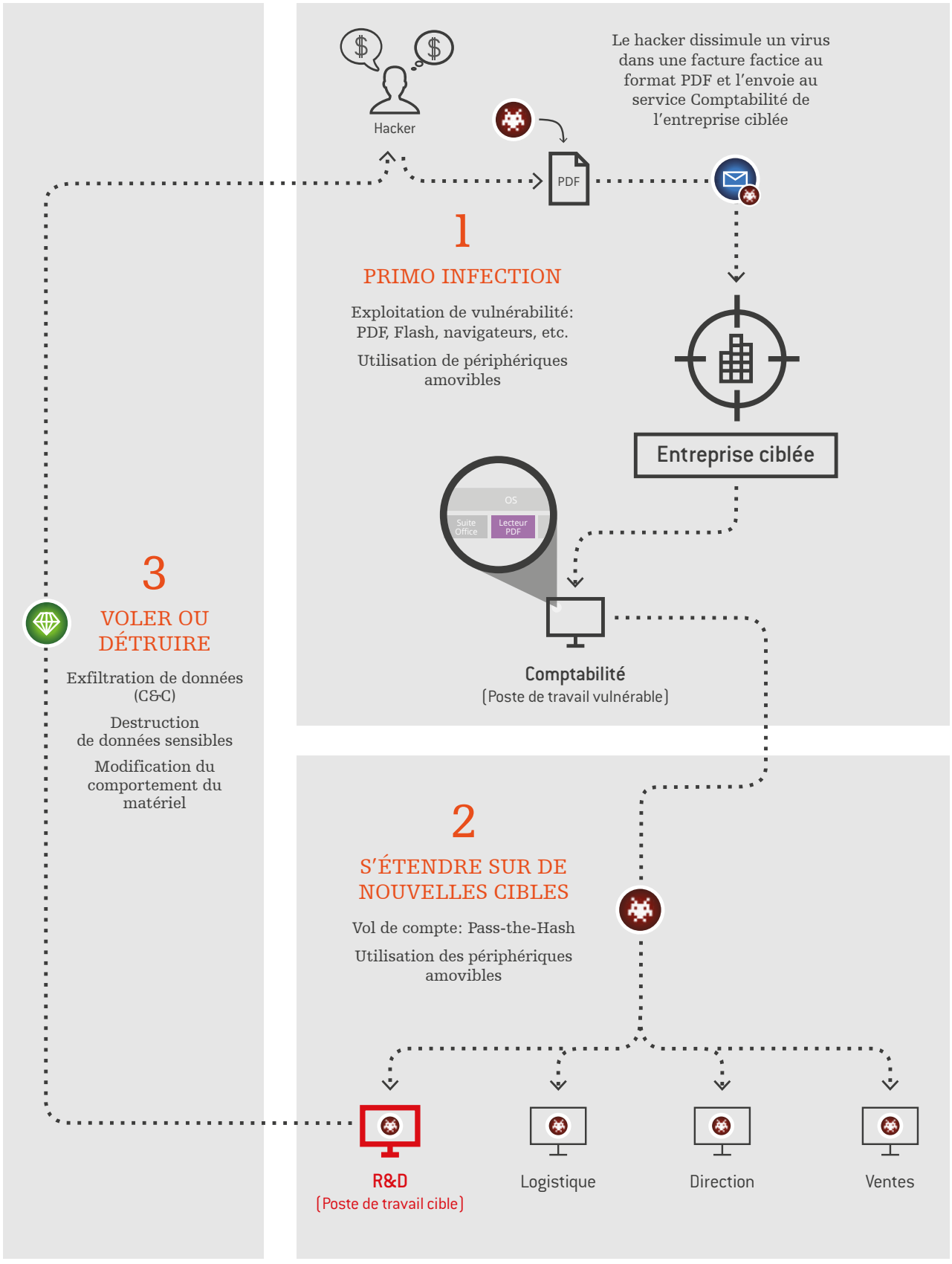
Cette phase de l'attaque persistante avancée frappe la plate-forme choisie dans un objectif précis. Il peut s'agir d'un PC de la Direction des Ressources Humaines éditant les bulletins de paie, d'un ordinateur de la chaîne de services d'approvisionnement, d'un serveur de commerce électronique ou de transactions financières. L'attaquant a préparé, par exemple, son attaque pour bloquer un service en ligne puis réclamer une rançon pour le rétablir, ou bien pour extraire des données confidentielles dans le but de les revendre. Pour illustration, en juin 2014 la société Domino's Pizza s'est vue réclamer la somme de 30 000 € suite au vol d'informations personnelles de 600 000 clients.

Dans le cas d'un serveur compromis, la mise en œuvre de l'attaque signale la présence d'un code malveillant auprès de l'entreprise ciblée. Pour autant, son éradication ne suit pas instantanément cette découverte. Le serveur peut être rétabli jusqu'à ce que l'attaquant décide d'exploiter à nouveau le code néfaste, de réclamer une nouvelle rançon ou de détruire des fichiers à distance.

Dans le cas d'une fuite de données suffisamment discrète, l'attaque APT n'est pas forcément détectée. L'attaquant peut donc continuer à récupérer des informations confidentielles pendant de nombreux mois ou années.

Explication d'une attaque sophistiquée

Fonctionnement des Attaques Avancées Persistantes (APT)



Choisir une protection multi-couches

Les protections en place dans l'entreprise doivent **échanger des informations sur les comportements observés, entre elles et à l'échelle mondiale**, pour être en mesure d'anticiper les prochaines attaques.

LES LIMITES DE LA PROTECTION EN SILOS

Face aux menaces de plus en plus élaborées, les protections traditionnelles (anti-virus, IPS, HIPS filtrage URL…) réduisent certes la surface d'attaque mais elles montrent aussi leurs limites. La combinaison de plusieurs vecteurs et charges unitaires de l'APT augmentent les risques. Et la primo infection de l'APT n'active pas directement le code malveillant ; elle utilise une faille système ou applicative pour repérer puis contrôler à distance l'ordinateur ciblé.

La charge malicieuse qui exploite une vulnérabilité d'une application bureautique n'a souvent aucune incidence sur le fonctionnement du poste de travail. Elle va, par exemple, initier une connexion http à destination d'un serveur de commande et contrôle pour activer un nouveau code malveillant. N'étant pas détectée comme une réelle menace, elle n'est donc pas bloquée par les protections traditionnelles. Comme cette charge est souvent spécifiquement forgée, elle n'est pas connue par les systèmes à base de signatures.

Ce n'est qu'en associant primo infection et expansion que la menace devient réelle. Dans le cas d'une menace réelle de type Zero-day, le risque augmente à mesure que l'attaque s'étend. L'attaque avancée va cependant laisser quelques traces (connexion à un site web non catégorisé par la solution de filtrage Web, alerte sur détection de connexion interactive ou encore connexion interne suspicieuse) qui sont considérées comme des signaux faibles.

La menace réelle apparaît plus évidente lorsque l'on corrèle entre eux ces différents événements qui sont unitairement considérés comme anodins. Par conséquent, la maitrise du contexte dans lequel interviennent ces signaux faibles est prépondérante dans l'identification ou le blocage des attaques persistantes avancées.

LA CORRÉLATION D'ÉVÉNEMENTS

Une vision globale des événements de sécurité qui surviennent sur le réseau d'entreprise fournit le contexte dans lequel se déroule l'attaque persistante avancée. Plusieurs comportements suspicieux et signaux faibles apparaissent depuis un point central, facilitant la détection d'une menace multi-vecteurs. L'analyse de nombreux événements de sécurité permet d'identifier chacune des menaces unitaires et de suspecter

un comportement anormal global. En revanche, la détection de l'APT requiert une analyse supplémentaire.

L'application de corrélation d'événements facilite ce travail d'analyse. En effet, elle va mettre en lumière un nombre de connexions subitement élevé, à partir d'une machine et sur une plage de temps donnée, des connexions vers des services ou ressources inhabituelles, ...

Ainsi, l'association d'événements unitaires apporte une vue contextuelle pouvant révéler une attaque persistante avancée. Bien que cette approche offre l'avantage de ne pas perturber la production, elle ne détecte l'attaque qu'après coup. Elle nécessite également un effort de suivi permanent des équipes opérationnelles pour analyser les alertes et appliquer les mesures de remédiation qui s'imposent en cas de sinistre.

L'APPROCHE MULTI-COUCHES

L'analyse d'événements corrélés ne permet de répondre aux attaques avancées que de manière réactive. Il est donc nécessaire de mettre en place une approche proactive afin d'élever le niveau de protection et de limiter la surcharge des équipes opérationnelles. Le principe de cette approche est de faire collaborer les différents moyens de protections sur 3 couches distinctes :

- **Couche 1 – Protection collaborative :** les moteurs de protection propres à un système (pare feu multifonctions ou protection de poste) échangent les informations sur les signaux faibles observés afin de détecter et bloquer des comportements malveillants,
- **Couche 2 – Protection contextuelle :** les différentes solutions de sécurité du système d'information collaborent entre elles afin d'échanger leurs signaux faibles, identifier de nouveaux comportements illégitimes et proposer une réaction coordonnée,
- **Couche 3 – Protection globale :** l'ensemble des solutions de protections déployées au sein de multiples organisations remontent des informations permettant d'obtenir une vision globale des menaces et d'observer de nouvelles anomalies. L'exploitation de ces données permet ensuite de mettre en œuvre des contre-mesures ou de nouvelles protections qui seront mises à disposition des solutions de sécurité.

Multi-Layer Collaborative Security

by Stormshield

STORMSHIELD

1 Protection collaborative

Les moteurs de protection propres à un système (pare feu multifonction ou protection de poste) **échangent les informations sur les signaux faibles observés**

2 Protection contextuelle

Les différentes solutions de sécurité du système d'information **collaborent entre elles** afin d'échanger leurs signaux faibles

3 Protection globale

L'exploitation de ces données permet alors de **mettre en œuvre des contre-mesures ou de nouvelles protections** qui seront mises à disposition des solutions de sécurité

LA PROTECTION COLLABORATIVE

La première couche de cette nouvelle approche consiste à intégrer des moteurs de protection d'une solution de sécurité afin qu'ils collaborent. Par exemple les solutions de protection multifonctions et les pares feux de nouvelle génération proposent plusieurs briques de sécurité. Ces produits offrent généralement des fonctions de filtrage de flux, de prévention d'intrusion, d'antivirus, d'antispam, de filtrage d'URL, de prévention de fuite de données ou encore de détection de vulnérabilités.

Chacune de ces fonctions prend en compte uniquement le contexte dans lequel elle intervient. La fonction de filtrage et de contrôle des flux réseaux sait bloquer les accès en provenance d'une machine malveillante. La prévention d'intrusions peut alerter en cas de session suspecte ou de nouveau canal de commande et contrôle. Le module antispam remonte des informations sur les principaux destinataires de courriers non sollicités liés aux réseaux sociaux. Enfin, la détection de vulnérabilités peut cartographier le niveau de risques des machines connectées dans l'entreprise.

Bien que chaque brique fonctionne indépendamment, reproduisant les limites de la protection en silos, ces produits pourraient faire collaborer leurs différents moteurs pour accroître le niveau de sécurité. Au moment de traiter un flux ou une donnée, chaque module prendrait en compte les traitements effectués ou les informations fournies par les autres modules. Lorsqu'il évalue un comportement, le module de sécurité agirait ainsi en fonction du contexte dans lequel se déroule une attaque probable.

Prenons l'exemple d'une machine vulnérable utilisée pour naviguer sur un site Web non catégorisé. Elle ne présente pas de risque particulier et le site Web présente seulement un niveau de risque moyen. Par contre, si le module de filtrage d'URL sait que la navigation sur ce site est effectuée depuis une machine vulnérable sur laquelle a été détectée des connexions interactives, il pourra en bloquer l'accès.

Chaque module de sécurité participerait ainsi à une protection globale au niveau du pare feu de nouvelle génération. Au lieu de simplement laisser passer un événement jugé peu risqué, un module particulier pourrait comptabiliser un signal faible et définir le niveau de risque associé.

Quand un autre module analyserait un événement en relation avec le premier, il pourrait relever le niveau de risque ou alors bloquer l'accès. Les divers niveaux de risques auraient leurs propres poids qui s'additionneraient à mesure que les modules de protection se coordonneraient pour détecter les attaques. Chaque module corrèlerait l'événement qu'il traite avec les niveaux de risque définis par les autres modules pour considérer la menace d'un point de vue global.

Le système de protection pourrait alors déclencher une action en fonction du résultat de l'analyse globale. Il bloquerait un flux ou mettrait la machine suspecte en quarantaine ou en zone d'assainissement. La menace serait ainsi bloquée ou atténuée, ce qui rehausserait le niveau de protection.

LA PROTECTION CONTEXTUELLE

La deuxième couche de cette nouvelle approche est plus globale, en considérant qu'une entreprise possède des systèmes de protections déployés à plusieurs endroits de son infrastructure. Un pare feu de nouvelle génération protège les accès réseaux ainsi que les flux transitant au sein de l'entreprise. Un système déployé sur les postes de travail intercepte les menaces Zero-day les plus élaborées et examine les autres vecteurs d'attaque (clé USB, négligences ou malveillances internes).

Selon le même principe de corrélation de signaux faible d'une solution collaborative, la collaboration entre les différentes solutions de sécurité permettrait d'accroitre encore le niveau de protection. On ne prend pas seulement en compte les événements liés au flux réseau ou à la protection de poste mais bien l'ensemble des informations de sécurité disponibles au sein de l'entreprise ; la protection devient contextuelle.

En reprenant notre exemple de machine vulnérable, le mécanisme de détection des failles est amélioré et il offre une information contextuelle plus juste. En effet, l'analyse des vulnérabilités révèle un risque potentiel lié à la présence d'une faille, exploitée ou non, dans une application. Si, suite à ces comportements observés sur le pare feu de nouvelle génération, la solution de protection de poste détecte un accès mémoire illicite ou l'usage d'une clé USB interdite, cette information pertinente corrige la mesure exacte du niveau de risque.

Les systèmes de sécurité gagnent à travailler de concert et à s'échanger des informations pour améliorer le niveau de protection. Le pare feu de nouvelle génération pourrait ainsi limiter les accès réseaux à une zone de quarantaine pour la machine ayant subi un accès mémoire illégitime. Il pourrait également demander au système de protection d'un poste de travail de modifier la politique de sécurité pour isoler la machine ou limiter ses accès au seul serveur de dépollution. De la même manière, le système de protection de poste pourrait communiquer au pare feu des informations sur un contenu illicite afin de contrer la latéralisation d'une attaque ou encore protéger les machines ne disposant pas de systèmes de protection avancée.

LA PROTECTION GLOBALE

La cybercriminalité agissant au niveau mondial, il convient d'apporter une réponse globale. A partir des solutions de protection déployées dans le monde, on peut collecter les informations de sécurité puis les consolider et les corréler à l'échelle mondiale. Cette démarche permet de suivre les toutes dernières techniques d'attaques apparues en tout point du globe et d'apporter une réponse active ou proactive.

Cette approche est déjà mise en œuvre par les éditeurs de logiciels anti-virus depuis de nombreuses années. Une fois l'analyse effectuée, les données recueillies remontent les derniers comportements d'attaque ainsi que les derniers vecteurs mis en œuvre. Il est donc possible d'améliorer les mécanismes de protection et d'apporter des réponses aux exploits Zero-day utilisés. La collecte au niveau mondial permet d'apporter une réponse globale à la menace.

Outre les derniers exploits utilisés, l'analyse des données consolidées permet également d'appréhender la façon dont sont coordonnés les vecteurs et les charges virales. Il est ainsi possible d'anticiper les nouvelles techniques d'attaques. En incluant des organismes globaux tels que les CERT, des SOC ou des MSSP, la zone de collecte peut être encore étendue. Elle concernera des solutions de protection d'origines variées et plusieurs centres opérationnels de supervision de la sécurité pour offrir une réponse encore plus large. En complément de l'aspect quantitatif évoqué précédemment, ces organismes sont à même d'apporter une approche qualitative sur les nouveaux comportements.

L'échange de données collaboratif avec l'écosystème de sécurité sur les menaces informatiques aide aussi à préparer des contre-mesures efficaces. On distingue trois types de réponses possibles :

- La définition de signature permet de répondre à une attaque découverte. La signature permet généralement d'identifier la charge virale exploitée.
- La réponse comportementale assure une protection fondée sur l'usage légitime d'une ressource (réseau, mémoire ou registre de données). Elle anticipe l'exploitation d'une faille Zero-day.
- La réponse contextuelle prend en compte l'ensemble des modules de protection. Elle peut modifier le poids des différents signaux faibles en fonction des données récemment collectées.

Ces contre-mesures peuvent être déployées sous la forme de nouvelles signatures, par la mise à jour de logiciels ou la fourniture de recommandations de configuration. Leur utilisation renforce de façon globale la sécurité informatique.

L'approche Stormshield

Pour contrer la compromission de services critiques et la fuite de données sensibles pour l'entreprise, **Stormshield fournit une supervision des menaces à l'échelle mondiale et un système complet de protections coordonnées**.

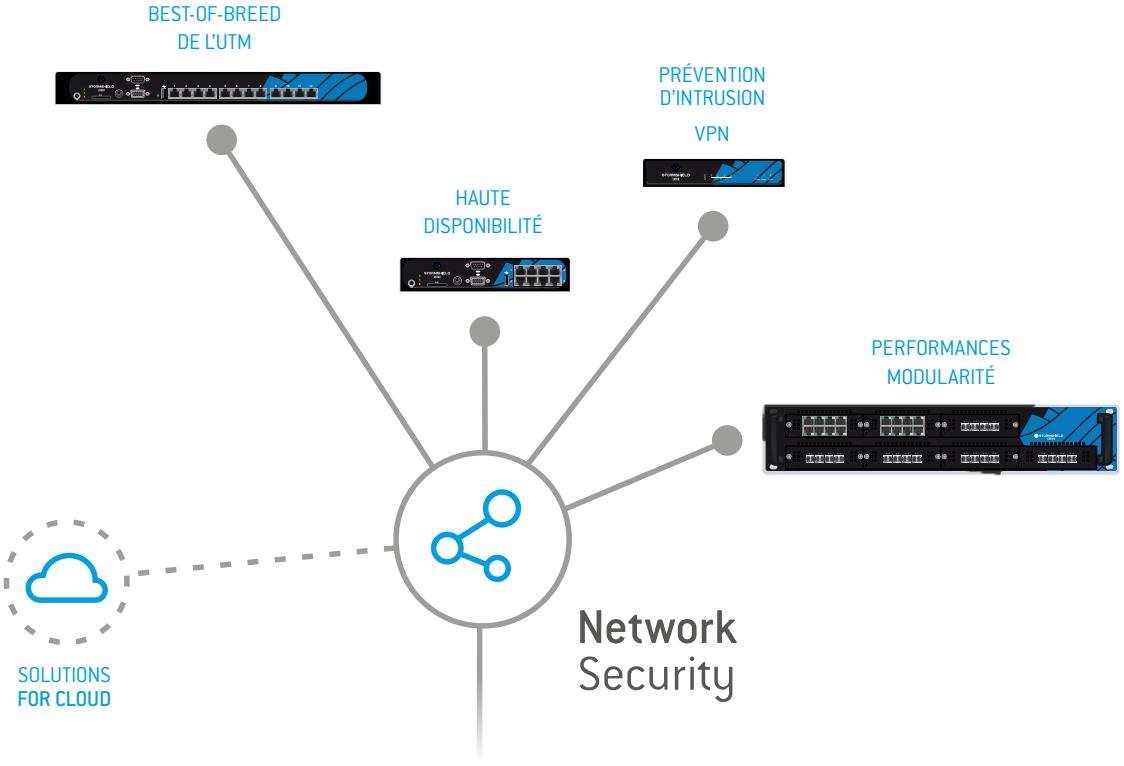
Cette nouvelle approche de **Multi Layer Collaborative Security*** constitue la vision de Stormshield pour améliorer la sécurité. Elle sert de fil conducteur aux développements de ses solutions multifonctions et de son portfolio multi produits.

La gamme **Stormshield Network Security** regroupe un ensemble de solutions de protection réseau multifonctions intégrant, entre autres, un module de gestion des vulnérabilités. Les produits **Stormshield Endpoint Security** assurent une protection de poste de travail efficace répondant aux attaques les plus élaborées. Enfin, **Stormshield Data Security** offre une protection des informations les plus sensibles, garantissant une barrière efficace contre la fuite de données.

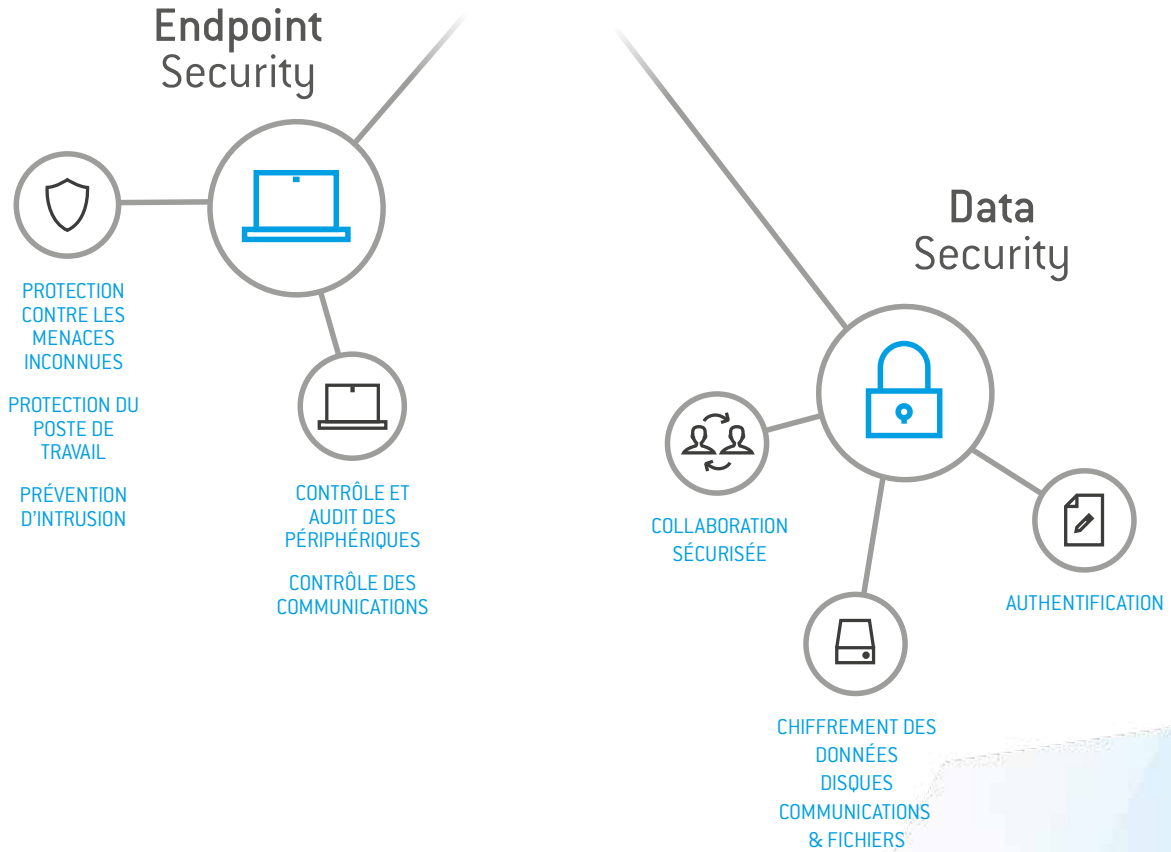
En faisant coopérer ses modules et produits de sécurité entre eux, Stormshield peut apporter une réponse sur les deux premières couches de l'approche collaborative. La remontée d'informations des produits déployés assure une vision globale de la menace à l'échelle de tous ces clients**.

Cette synergie sert la vision de Stormshield qui consiste à répondre aux menaces multi vecteurs par une protection efficace et multi-couches, offrant une collaboration interne, une protection contextuelle et une analyse globale des menaces.

* la sécurité collaborative multi-couches / **Désactivable



MULTI-LAYER COLLABORATIVE SECURITY



STORMSHIELD

N°Cristal 09 69 32 96 29

APPEL NON SURTAXE

WWW.STORMSHIELD.EU

Arkoon Network Security
1 place Verrazzano - CS 30603 69258 - Lyon Cedex 09 - FRANCE

Netasq
Parc Scientifique Haute Borne - Parc Horizon, Bat 6, Avenue de l'Horizon 59650 Villeneuve d'Ascq - FRANCE

Version 1.0 - Copyright Netasq 2015