Décryptage des Cyber-Attaques

Partie I. Le modèle Cyber-Kill Chain.

Adaptive Defense

pandasecurity.com/intelligence-platform/

Sommaire.

1. Introduction.

L'évolution de la réalité et de la fréquence des menaces, ainsi que la sophistication et la nature ciblée des adversaires imposent une évolution des pratiques opérationnelles de sécurité, afin de combiner les volets prévention, détection et réponse concernant les cyber-attaques.

La majorité des organisations sont en mesure de détecter les menaces connues, même si peu d'entre elles sont encore susceptibles de se produire. Une difficulté historique est la capacité d'arrêter les attaques inconnues, lesquelles sont conçues sur mesure pour contourner les toutes dernières protections en changeant de signature et de modèle comportemental.

De nombreuses organisations ont réalisé des investissements considérables afin de mettre sur pied leur propre équipe de lutte contre les menaces et/ou de déléguer à des prestataires de services administrés la tâche inévitable et critique consistant à faire constamment évoluer les techniques de défense, ainsi que la recherche de meilleurs outils et approches pour préserver la sécurité de la propriété intellectuelle et des actifs numériques.

La compréhension du fonctionnement de ces adversaires et la cartographie de la stratégie de défense des organisations face à leur cycle de vie montrent comment celles-ci peuvent détecter, arrêter et interrompre une attaque, comment elles peuvent se remettre d'une telle attaque et sur quels points elles doivent renforcer leurs opérations de sécurité.

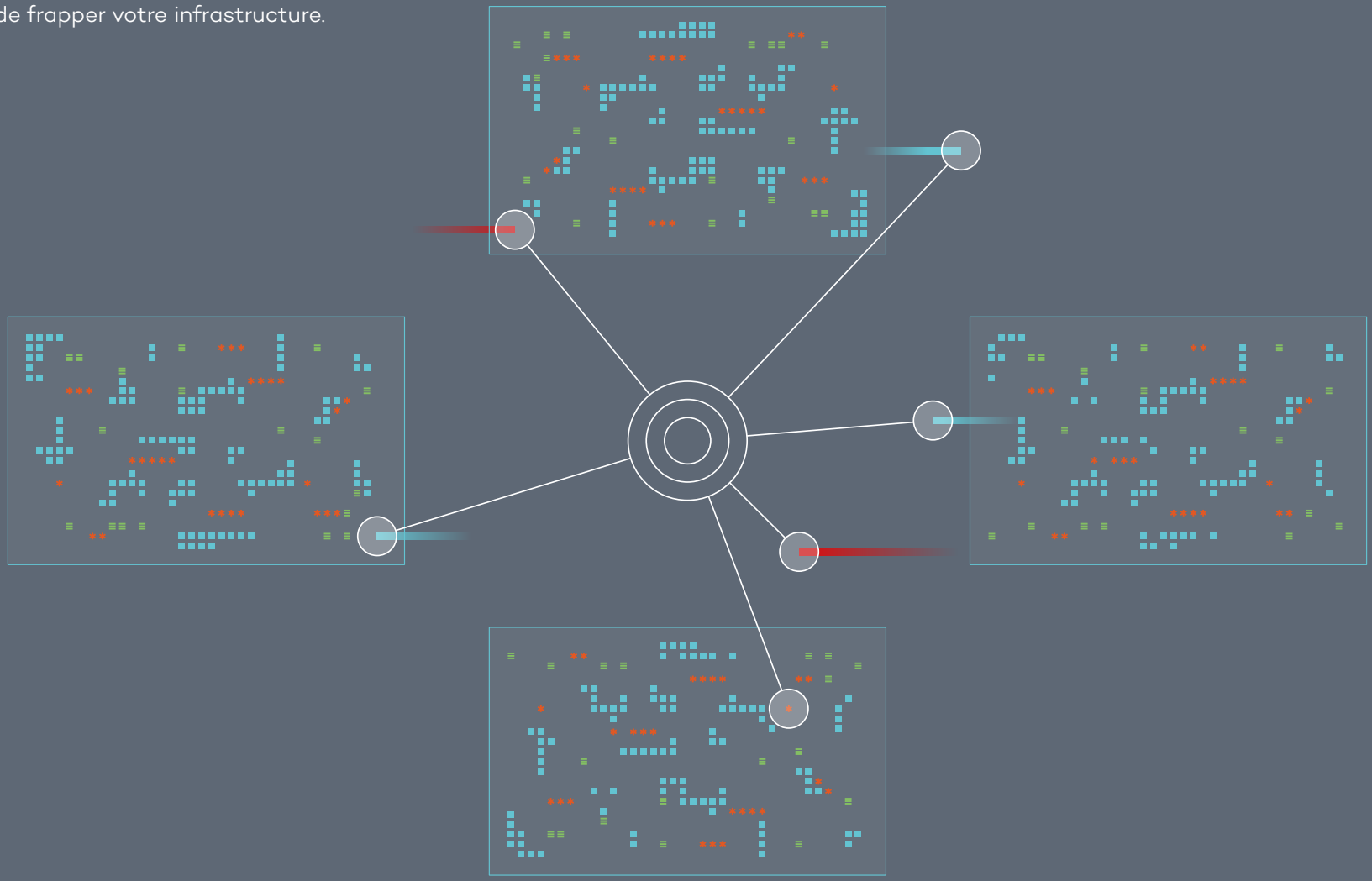
Ce rapport aide les équipes de sécurité à comprendre le modèle bien connu de cycle de vie des cyber-attaques, appelé modèle Cyber-Kill Chain (CKC), et son extension à l'ensemble du réseau. Il explique aussi comment le service Panda Adaptive Defense couvre l'intégralité du cycle de vie au niveau des postes clients.

Le modèle CKC et son extension à l'ensemble du réseau constituent un excellent outil pour comprendre comment les organisations peuvent renforcer significativement les défenses de leur environnement en interceptant et en arrêtant les menaces à chaque phase du cycle de vie des attaques. Un des enseignements du modèle est le suivant : pour réussir, les adversaires doivent passer par toutes les phases, alors que pour nous, l'interruption de la chaîne à n'importe quelle étape suffit pour casser l'attaque.

Il faut avoir à l'esprit que les actifs les plus précieux, et parfois non contrôlés, d'une organisation résident sur les postes clients et les serveurs. Tous les attaquants ciblent les postes clients pour accéder aux actifs critiques des organisations. En stoppant les adversaires à ce niveau, vous réduisez automatiquement la probabilité de réussite d'un cyber-attaquant, vous simplifiez le travail d'interruption de la chaîne et vous augmentez significativement l'efficacité et les performances des opérations de sécurité.

Le service Panda Adaptive Defense a pour objectif d'aider les équipes internes ou les prestataires en charge de la sécurité à améliorer leur capacité à **prévenir, détecter et remedier aux dernières cyber-menaces en les appréhendant à travers la totalité de leur cycle opératoire**, et ce, quelque soit le moment ou elles décident de frapper votre infrastructure.

En outre ses **services administrés** fournissent des renseignements et diagnostics à valeur ajoutée sur les menaces afin de les aider à mieux identifier les actions malveillantes et à mettre en oeuvre les strategies défensives adaptées.



2. Compréhension du modèle Cyber-Kill Chain.

L'approche Cyber Kill-Chain a été, à l'origine, publiée par Lockheed Martin dans le cadre du modèle Intelligence Driven Defense1 pour l'identification et la prévention des activités de cyber-intrusions.

Le modèle identifie les étapes que les adversaires doivent accomplir pour atteindre leur objectif, à savoir cibler le réseau, exfiltrer des données et assurer leur persistance dans l'organisation.

Grâce à ce modèle, nous avons appris qu'il suffit de stopper les adversaires à n'importe quel stade pour casser la chaîne de l'attaque. Les adversaires doivent passer par l'ensemble des phases pour réussir. En tant que défenseurs, il nous suffit de les bloquer à n'importe quel stade pour réussir.

Nous allons voir dans la section suivante que le poste client est un point incontournable pour toutes les attaques et, par conséquent, que leur interruption à ce niveau augmente considérablement la chance de stopper n'importe quelle cyber-attaque. Le taux de réussite sera supérieur si l'adversaire est stoppé le plus tôt possible dans la chaîne.

Par ailleurs, toute intrusion et les traces qu'elle laisse au niveau du poste client constituent une opportunité de comprendre davantage nos adversaires et d'exploiter leur persistance à notre avantage. Une meilleure connaissance des adversaires et de leurs traces permet d'organiser plus efficacement les défenses.

Selon le modèle Cyber-Kill Chain, les adversaires doivent toujours exécuter six étapes de base pour accomplir leurs méfaits :

Reconnaissance externe

Cette étape constitue la phase de sélection de la cible et d'identification des détails de l'organisation, des exigences législatives verticales du secteur, des informations sur les choix technologiques, de l'activité sur les réseaux sociaux ou des listes de publipostage.

L'adversaire cherche essentiellement à répondre aux questions suivantes : "Quelles méthodes d'attaque offriront le plus haut degré de réussite ?" et "Lesquelles sont les plus faciles à exécuter en termes d'investissement ?"

Armement et conditionnement

Cette phase peut revêtir de nombreuses formes : Exploitation d'application Web, logiciel malveillant standard ou personnalisé (téléchargé pour réutilisation ou acheté), vulnérabilités de documents composites (fournis au format PDF, Microsoft Office ou dans d'autres formats) ou d 'attaques de type watering hole[2].

Les préparatifs de cette phase s'appuient généralement sur des activités opportunistes ou très spécifiques de collecte d'informations sur une cible donnée.

Livraison

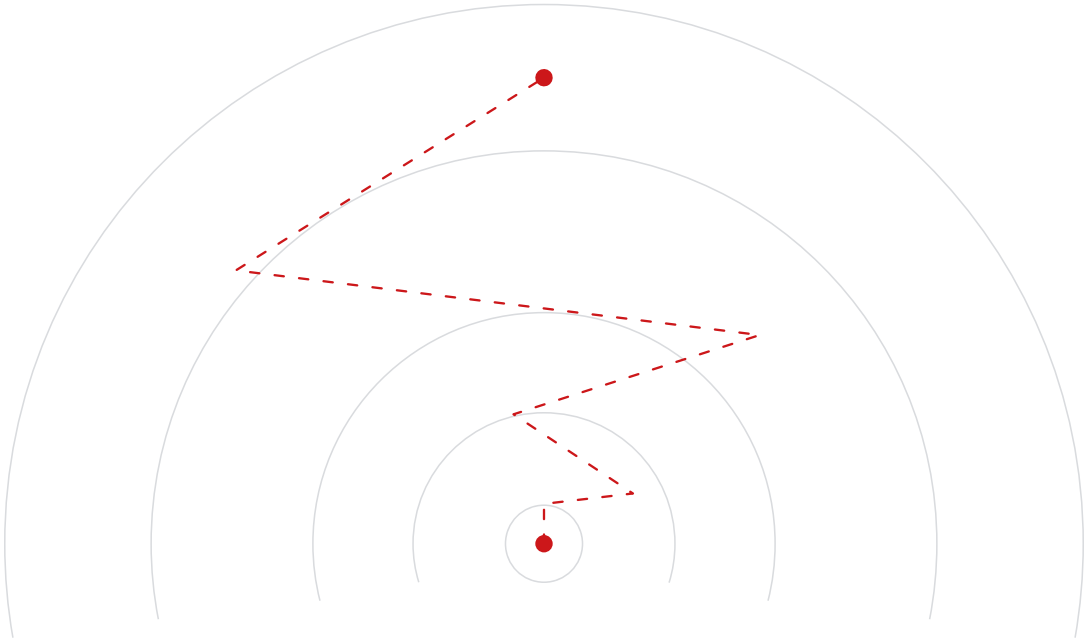
La transmission de la charge malveillante est déclenchée par la cible (par exemple, un utilisateur navigue vers une page Web malveillante, déclenchant un exploit livrant le logiciel malveillant, ou il ouvre un fichier PDF infecté) ou par l'attaquant (injection SQL ou compromission de services réseau).

Exploitation

Une fois remise à l'utilisateur, à l'ordinateur ou à l'appareil, la charge malveillante compromet l'actif et prend donc pied dans l'environnement cible.

Une méthode fréquente consiste à exploiter une vulnérabilité connue pour laquelle un correctif a été fourni antérieurement.

Même si, selon la victime, des exploitations zero-day sont employées, il n'est, dans la majorité des cas, pas nécessaire d'en arriver jusque-là.



Installation

L'installation prend souvent la forme d'un élément communiquant activement avec des tiers extérieurs. Le fonctionnement du logiciel malveillant est généralement furtif et il demeure persistant sur les postes clients sur lesquels il s'est implanté. L'adversaire peut ensuite contrôler cette application sans alerter l'organisation.

Commande et contrôle

Pendant cette phase, les adversaires contrôlent les actifs de l'organisation cible à travers des méthodes de contrôle (souvent à distance), telles que DNS, ICMP, des sites Web et des réseaux sociaux. L'adversaire utilise ce biais pour indiquer à l'actif contrôlé ce qu'il doit faire ensuite et quelles informations il doit collecter.

Les méthodes employées pour collecter des données sur commande incluent les captures d'écran, la surveillance des saisies au clavier, le déchiffrage de mots de passe, la surveillance du réseau pour récupérer les identifiants, ou encore la collecte de contenus et documents sensibles. Bien souvent un hôte intermédiaire est identifié pour y copier toutes les données internes. Celles-ci sont alors compressées et/ou cryptées et préparées pour leur exfiltration.

Actions sur les cibles

Cette phase finale englobe la partie exfiltration des données et/ou endommagement des actifs informatiques, ainsi que la persistance concomitante dans l' organisation visée. Ensuite, des mesures sont mises en place pour identifier plus de cibles, étendre l'empreinte au sein de l'organisation et -point le plus critique- exfiltrer des données.

Le processus CKC se répète alors. En fait, un aspect critique du processus CKC est son modus operandi circulaire et non linéaire. Dès qu'un adversaire pénètre sur le réseau, il y relance le processus CKC, en élargissant l'action de reconnaissance et en effectuant des mouvements latéraux à l'intérieur du réseau.

Par ailleurs, il est à noter que, même si la méthodologie est la même, les méthodes employées par les adversaires pour les étapes du processus CKC interne une fois dans la place différeront de celles employées à l'extérieur de l'environnement cible.

En fait, une fois que l'attaquant est dans la place, il devient un initié, autrement dit un utilisateur disposant de privilèges et d'une persistance. Les équipes de sécurité de l'organisation ne peuvent alors pas suspecter l'attaque et elles ne réalisent pas qu'elles en sont déjà aux phases avancées du modèle Cyber-Kill Chain étendu.

.

Figure 1. Schéma des étapes du processus Cyber-Kill Chain du périmètre jusqu'au poste client. Modèle Cyber-Kill Chain externe.

3. Version étendue du modèle Cyber-Kill Chain.

Le processus Cyber-Kill Chain étant circulaire et non linéaire, l'attaquant effectue des mouvements latéraux à l'intérieur du réseau. Les étapes employées sont identiques à celles utilisées pour accéder au réseau, mais les techniques et tactiques diffèrent.

La combinaison des processus Cyber-Kill Chain externe et interne est appelée dans le métier processus Cyber-Kill Chain étendu. Cela consiste à ajouter plus d'étapes, qui correspondent en fait au même ensemble, et à y accoler le terme «interne». Ainsi le modèle Cyber-Kill Chain devient le modèle Cyber-Kill Chain interne avec ses propres étapes, sa reconnaissance interne, son armement interne, etc.

Une fois à l'intérieur du réseau de la victime, chaque phase de l'attaque peut durer de quelques minutes à plusieurs mois, y compris le temps d'attente final, lorsqu'une attaque est en place et prête à être déclenchée.

Il convient de noter que l'attaquant attendra le meilleur moment pour obtenir un impact maximum.

Les phases de reconnaissance et d'armement peuvent durer plusieurs mois. Il est difficile de les interrompre car elles sont réalisées sans connexion avec l'attaquant. C'est la raison pour laquelle il est vital que les mesures de sécurité sur les postes clients puissent analyser et superviser tous les systèmes et applications qui s'exécutent sur ces appareils. Cela gênera considérablement le travail des attaquants et l'attaque ne leur procurera aucun bénéfice.

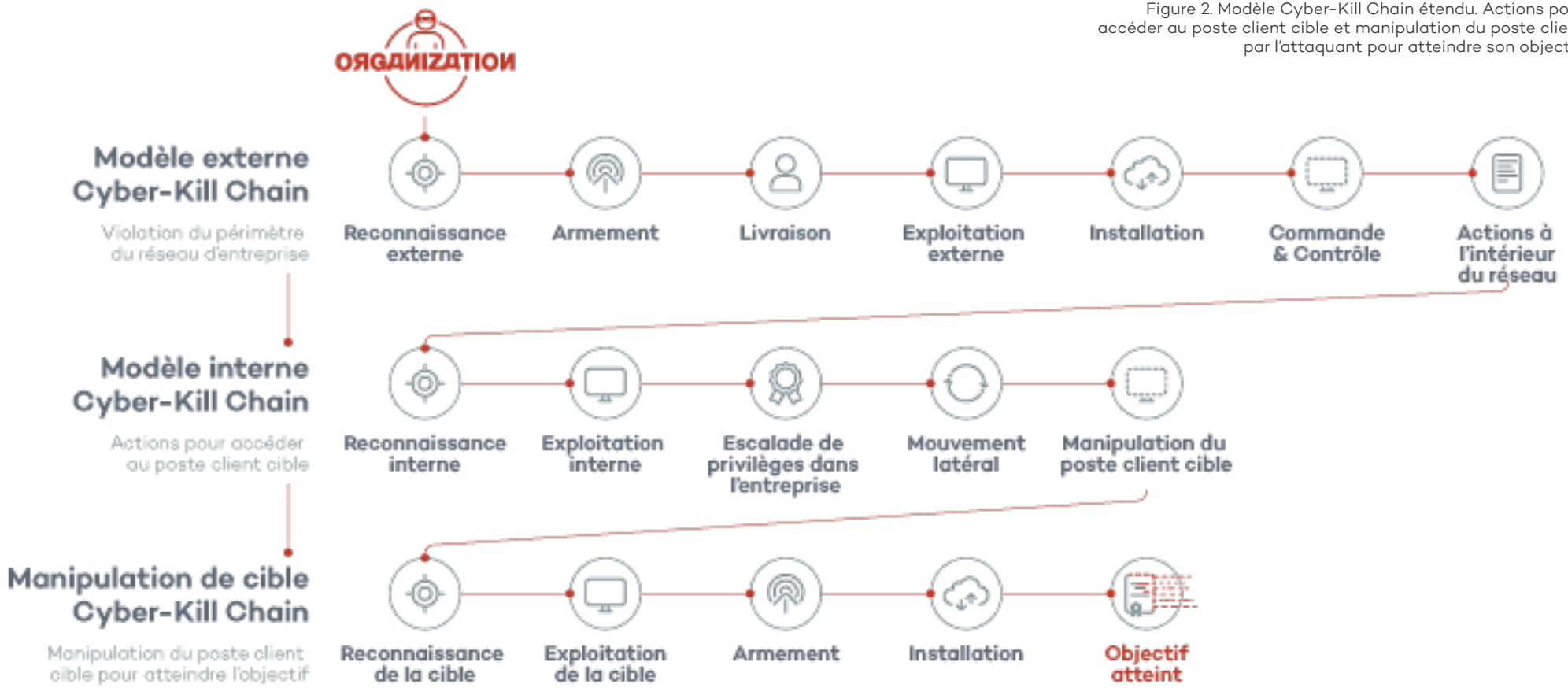
Reconnaissance interne

Lors de cette étape, les adversaires ont accès au poste de travail d'un seul utilisateur et l'explorent afin de déterminer quels sont ses fichiers locaux, ses partages réseau, son historique de navigation et son accès à des sites wiki et à SharePoint. L'objectif est de trouver comment la machine pourrait aider à cartographier le réseau et permettre d'atteindre des actifs plus intéressants.

Exploitation interne

Elle consiste, pour les attaquants, à profiter de correctifs manquants, de vulnérabilités d'applications Web, de protocoles de diffusion, d'usurpations d'identité, voire d'un élément aussi simple que des identifiants par défaut, pour passer de postes de travail à des serveurs au moyen d'une **escalade de privilèges, de mouvements latéraux sur le réseau et de la manipulation de machines individuelles ciblées**.

Figure 2. Modèle Cyber-Kill Chain étendu. Actions pour accéder au poste client cible et manipulation du poste client par l'attaquant pour atteindre son objectif.



4. Panda Adaptive Defense et le modèle Cyber-Kill Chain.

Les attaquants ont des objectifs et sont prêts à leur consacrer une certaine quantité de ressources pour les atteindre. Si les mécanismes de sécurité du poste client peuvent décupler les coûts – d'ordre financier, en personnel ou en temps – afin qu'ils soient largement supérieurs au bénéfice escompté par les attaquants, la réussite de ces derniers sera moins fréquente, quitte à les dissuader d'attaquer l'organisation.

La mission de Panda Security est de faire en sorte que ce soit toujours le cas pour nos clients et, au vu des résultats, c'est précisément ce que réalise la protection Panda Adaptive Defense.

Toutes les organisations doivent être prêtes à s'interroger sur ce qu'elles feraient si l'adversaire avait accès au réseau interne, aux noms d'utilisateurs et mots de passe, ainsi qu'à toutes les documentations et spécifications des appareils du réseau, systèmes, sauvegardes et applications, et elles doivent être prêtes à réagir immédiatement.

L' objectif plus large de la stratégie de sécurité des postes clients et actifs de l'entreprise doit être de mettre en place une entreprise plus résiliente. Cela ne préviendra pas toutes les attaques, mais en arrêtera plus, et plus tôt. Un des objectifs est d'avoir les mécanismes de défense efficaces du modèle Cyber-Kill Chain étendu, afin de ralentir les attaquants, de rendre la poursuite de leur attaque toujours plus onéreuse et de compliquer autant que possible leur passage à l'étape suivante.

Si les adversaires ne peuvent pas atteindre leur objectif de façon rentable, ils changeront d'objectif ou poursuivront des objectifs similaires en ciblant une autre organisation.

La stratégie de sécurité des organisations doit prendre en considération le mode opératoire d'une attaque, tant à partir de l'extérieur que de l'intérieur, car une fois dans la place, les attaquants deviennent des initiés qui accèdent aux postes clients et à leurs actifs.

L'approche de sécurité traditionnelle doit être étendue avec des méthodes basées sur la compréhension du modèle Cyber-Kill Chain et sur la mise à disposition de technologies capables d'empêcher l'accès des attaquants aux postes clients mais aussi capables de les stopper à n'importe quel stade du modèle Cyber-Kill Chain interne.

La cartographie de la stratégie de défense avec le modèle CKC étendu montre à l'organisation comment avoir une démarche de prévention, de détection, d'interruption et de récupération à toutes les phases de l'attaque, et comment aligner sa sécurité sur les mêmes critères de réussite que ceux des adversaires.

Cette démarche est difficile à mettre en place, du fait d'un certain nombre de facteurs : la complexité et l'interconnexion sans cesse croissantes des applications, leur vulnérabilité liée au fait que la majorité des logiciels ne sont pas développés sur la base de principes de sécurité, et aussi le facteur humain. Les employés et partenaires (clients et fournisseurs) demeurent, par conséquent, un vecteur de risque principal et ouvrent une porte aux attaques basées sur l'ingénierie sociale.

Panda Adaptive Defense et Adaptive Defense 360 englobent les principaux piliers de protection qui, lorsqu'ils sont fournis sous forme de **service administrés, préviennent et détectent les techniques et tactiques d'attaque les plus sophistiquées à chaque stade du modèle Cyber-Kill Chain étendu**. Ils aident les équipes de sécurité des organisations à concevoir une stratégie de sécurité en phase avec le modèle Cyber-Kill Chain étendu.

5. Les principaux piliers d'Adaptive Defense 360.

Prévention des logiciels malveillants connu

La recherche des menaces connues ne protégera pas contre les variantes ou les attaques inconnues, mais en lui adjoignant des couches de sécurité supplémentaires, elle peut arrêter préventivement des menaces connues au niveau du poste client. Panda Adaptive Defense 360 utilise un vaste ensemble de services de réputation pour bloquer de manière proactive les attaquants pendant la phase de livraison au moyen de données du cloud.

Détection avancée des logiciels malveillants

Panda Adaptive Defense et Panda Adaptive Defense 306 détectent et bloquent les logiciels malveillants inconnus et les attaques ciblées, grâce à un modèle de sécurité basé sur trois principes : surveillance continue approfondie de toutes les applications s'exécutant sur les postes clients, classification automatique des processus de postes clients au moyen des techniques d'analyse Big Data et d'apprentissage machine sur une plate-forme cloud, et possibilité pour un expert d'analyser le comportement en profondeur si un processus ne peut pas être classé automatiquement.

Detection d'exploit dynamique[3]

Pendant la phase d'exploitation du modèle Cyber-Kill Chain étendu, les attaquants utilisent des exploits pour cibler des vulnérabilités du code. Ils s'infiltrent ainsi dans des applications et des systèmes, puis installent et exécutent des logiciels malveillants. Les téléchargements à partir d'Internet sont un vecteur courant pour les attaques de type exploit. Panda Adaptive Defense et Panda Adaptive Defense 360 fournissent des fonctions anti-exploit dynamiques, afin d'assurer une protection contre les attaques ciblant les applications et la mémoire.

Panda Adaptive Defense et Panda Adaptive Defense 360 détectent et bloquent, entre autres, les techniques suivantes employées actuellement par les attaquants pendant la phase d'exploitation : heap spray, falsification de pile (stack pivot), attaques ROP et modifications des permissions de mémoire. Par ailleurs, ils détectent de manière dynamique les attaques inconnues en surveillant tous les processus s'exécutant sur les appareils et en corrélant les données à travers des algorithmes d'apprentissage machine dans le cloud, afin d'arrêter toute tentative d'exploitation connue et inconnue. Les technologies anti-exploit d'Adaptive Defense arrêteront l'adversaire au début de l'attaque interne, en identifiant le moment où une application de confiance ou un processus est compromis.

Atténuation

Une protection de poste client de nouvelle génération doit bloquer et détecter les attaquants aux différentes étapes du modèle Cyber-Kill Chain, mais la détection doit être suivie d'une atténuation rapide aux débuts de l'attaque.

Panda Adaptive Defense 360 atténue l'attaque automatiquement et au moment voulu, en plaçant le logiciel malveillant en quarantaine, en arrêtant un processus compromis, voire en arrêtant complètement le système pour limiter au maximum les dommages.

Remediation

Pendant l'exécution, il est fréquent que le logiciel malveillant crée, modifie ou supprime le système de fichiers et les paramètres du Registre, et modifie les paramètres de configuration.

Ces changements ou les traces laissées derrière peuvent rendre le système instable, voire ouvrir la porte à de nouvelles attaques.

Panda Adaptive Defense 360 restaure les postes clients à leur état fiable antérieur à l'attaque.

Analyse a posteriori

Avec l'évolution de la réalité et de la fréquence des menaces, mais aussi du fait de la sophistication et de la nature ciblée des adversaires, aucune technologie de sécurité ne peut affirmer qu'elle est efficace à 100 %. Par conséquent, la possibilité de proposer une analyse a posteriori et une visibilité des postes clients en temps réel est indispensable.

Les équipes de cybersécurité d'entreprise doivent avoir un plan pour gérer les violations de reporting, contacter les autorités et faire face à la mauvaise publicité ainsi qu'à d'autres aspects similaires.

Panda Adaptive Defense et Panda Adaptive Defense 360 offrent une visibilité claire et en temps utile des activités malveillantes à l'échelle d'une organisation. Les équipes de sécurité peuvent ainsi évaluer rapidement l'étendue d'une attaque et réagir comme il se doit.

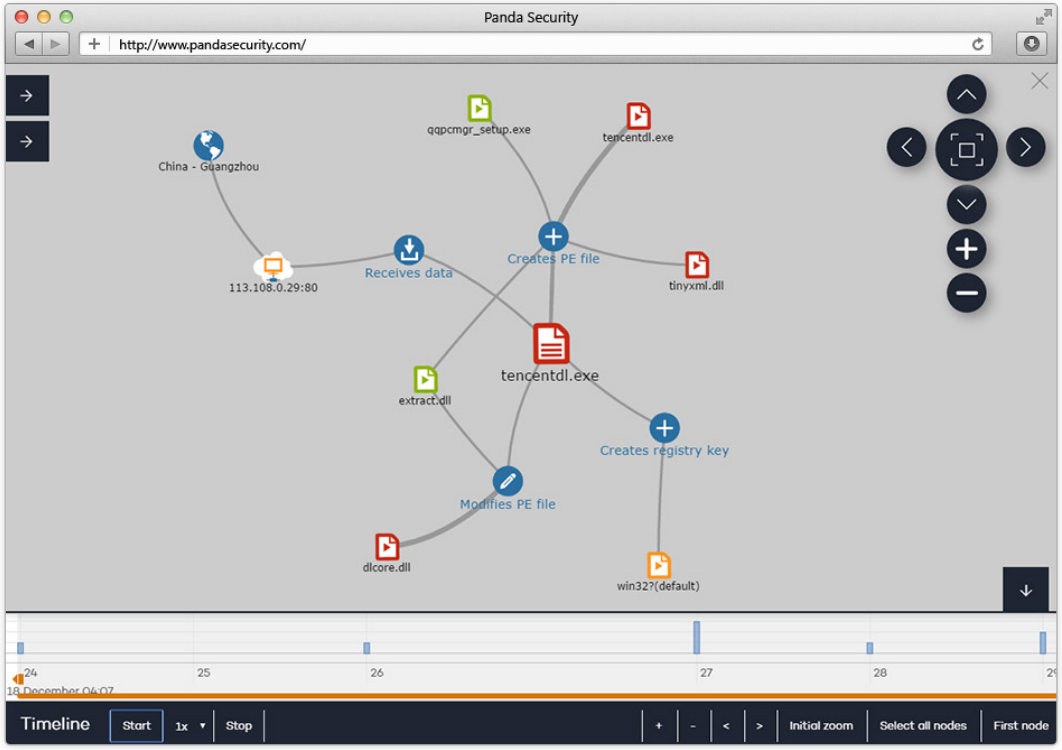


Figure 3. Graphique d'analyse a posteriori du cycle de vie d'une attaque.

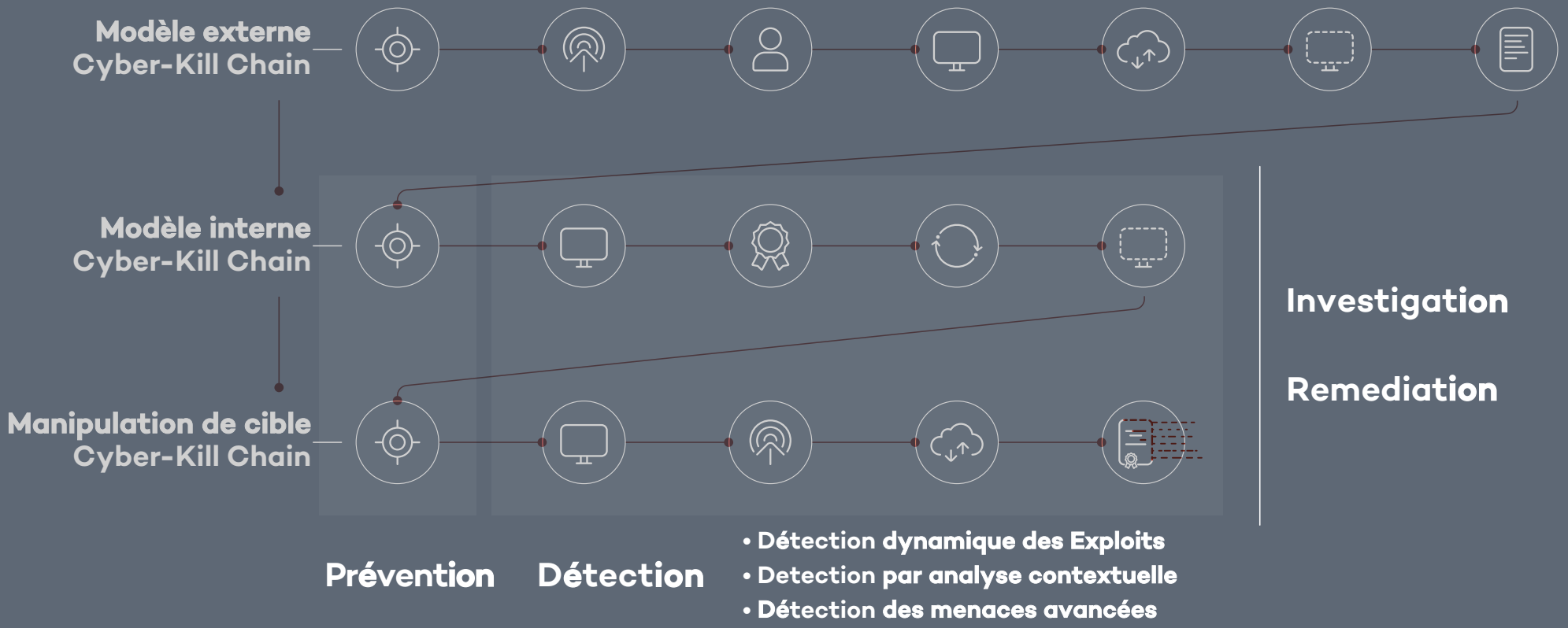


Figure 4. Piliers de la sécurité d'Adaptive Defense 360 pendant le processus Cyber-Kill Chain

References.

- Lockheed Martin's Cyber-Kill Chain: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- Sean T. Mallon, Strategic Cybersecurity Leader & Executive Consultant, at Black Hat 2016: Extended Cyber kill chain
- Mitre's Cybersecurity Threat-Based Defense
- Microsoft's Security Development Life Cycle
- Gartner Research, G00298058, Craig Lawson, 07 April 2016

[1] Eric M. Hutchins,Michael J. Cloppert, and Rohan M.Amín, Ph.D.,Intellígence-Dríven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kili Chains.

[2] **Watering hole attacks**. Un type spécifique d'attaque ciblée, dont les victimes font partie d'un groupe particulier (organisation, secteur d'activité ou région). Dans ce scénario, l'attaquant devine ou observe les sites Web employés fréquemment par le groupe et infecte un ou plusieurs d'entre eux avec des logiciels malveillants. Au final, des membres du groupe ciblé sont infectés.

Le logiciel malveillant employé collecte généralement des informations sur l'utilisateur. Les attaquants à la recherche d'informations spécifiques peuvent uniquement s'en prendre aux utilisateurs ayant une adresse IP spécifique. Cette approche complique aussi la tâche de détection et de recherche des attaquants. Le nom de cette attaque est dérivé des prédateurs du monde réel, lesquels attendent une opportunité pour attaquer leur proie à proximité de points d'eau.

Le fait de s'appuyer sur les sites Web auxquels le groupe fait confiance rend cette stratégie efficace, même avec des groupes qui sont résistants au phishing ciblé ou à d'autres formes de phishing.

[3] **La détection d'exploit dynamique** est la technologie innovante de Panda Security basée sur la surveillance de tous les processus en cours sur le poste client ou le serveur et sur son analyse dans le cloud par des technologies d'apprentissage machine chargées de détecter des tentatives d'exploitation d'applications de confiance.

L'objectif de cette nouvelle technologie est d'arrêter les attaques sur les postes de travail et les serveurs dès les premiers stades du processus Cyber-Kill Chain. En contenant l'attaquant et en l'empêchant d'accéder à l'appareil, cela annule le bénéfice visé par l'attaque, décourage d'autres tentatives et aboutit, par conséquent, à un taux de détection supérieur.

Plus d'informations à l'adresse :

pandasecurity.com/intelligence-platform/