Quel avenir pour les antivirus nouvelle génération ?

Les cyberattaques sont en augmentation constante, tandis que la prolifération des terminaux multiplie les points d'entrée potentiels vers vos données. Or, beaucoup trop d'entreprises s'en remettent encore à des antivirus basés sur les signatures pour protéger leurs terminaux. Malheureusement, ces logiciels historiques, tout comme leurs successeurs de nouvelle génération, exposent les entreprises à tout un arsenal de techniques d'attaque sans fichier et sans signature, auquel viennent s'ajouter des rafales constantes de nouveaux malwares particulièrement virulents – dont la plupart sont déployés moins de 24 heures après leur création. Ce document livre aux équipes de sécurité quelques clés pour faire évoluer leur protection des terminaux afin de renforcer leur défense contre ces menaces.

Les entreprises veulent disposer d'outils capables de détecter les attaques avancées et de retracer le fil des évènements, d'identifier les causes racines et de corriger les terminaux touchés. Les acteurs de la cybersécurité se sont donc penchés sur la question et ont répondu de trois manières : « antivirus nouvelle génération » (NGAV), « plateformes de protection des terminaux » (EPP) ou « détection et réponse sur les terminaux » (EDR). Soit trois outils dont les fonctionnalités se recoupent souvent à plusieurs niveaux. Dans ces conditions, difficile de faire le bon choix, d'autant qu'aucune de ces solutions n'a prouvé sa capacité à répondre aux besoins de sécurité réels des entreprises. Selon une étude du Ponemon Institute, près de 67 % des entreprises disent ne pas disposer de suffisamment de temps et de ressources pour corriger toutes les vulnérabilités sur leurs terminaux et éviter toute compromission.[1] Par ailleurs, des tests menés par le SANS Institute ont révélé que les produits EDR ne détectent généralement que 26 % des vecteurs d'attaque initiaux.[2] Entre les plateformes EPP qui ne fournissent aucune prévention et les produits EDR qui ne détectent pas les attaques, ni l'un ni l'autre n'apporte de véritable solution.

Ce livre blanc revient sur les fonctionnalités spécifiques dont les entreprises ont besoin pour protéger leurs terminaux contre les menaces actuelles. Nous examinerons également diverses stratégies de déploiement pour optimiser les workflows SecOps et renforcer la sécurité, aujourd'hui comme demain.

La prévention reste la règle d'or de la sécurité

Les cybercriminels sont de plus en plus habiles, tandis que le volume et la variété des terminaux potentiellement vulnérables continuent de croître. Il est donc difficile, voire impossible de stopper 100 % des menaces, du moins pas sans bloquer également les activités bénignes ni perturber considérablement les opérations métiers.

Ceci dit, il est important de comprendre qu'une détection et une réponse efficaces passent d'abord par une prévention cohérente et coordonnée. Le problème des produits EDR même les plus performants, c'est qu'ils ne détectent les attaques que lorsque le mal est déjà fait. Or, détecter une attaque à ce stade place le SecOps sur la défensive et l'oblige dans un premier temps à prendre connaissance de la situation, puis à investir les ressources opérationnelles nécessaires pour évaluer l'ampleur des dommages, avant d'essayer de limiter les dégâts tant bien que mal. Un produit EDR fonctionne un peu comme l'airbag d'un véhicule. Certes les airbags sauvent des vies, mais l'idéal est d'éviter les accidents en premier lieu. Adopter une approche préventive de la sécurité, c'est un peu comme équiper sa voiture d'un système anticollision. Et la première étape vers une prévention efficace consiste à revoir la manière dont les organisations gèrent les menaces.

Protection des terminaux : trois exigences majeures

Vol de données ou installation d'un ransomware : quel que soit l'objectif visé, les attaquants doivent procéder en plusieurs étapes qui forment le « cycle d'attaque ». Dans presque tous les cas, ce cycle passe par la compromission d'un terminal. Or, bien que la plupart des entreprises aient déployé des solutions de protection de leurs terminaux, les infections sont toujours monnaie courante.

Aujourd'hui, beaucoup d'attaquants combinent deux grandes méthodes : l'une consiste à cibler les vulnérabilités des applications et l'autre à déployer des fichiers malveillants. Si ces méthodes peuvent être utilisées séparément ou dans des combinaisons diverses, elles sont complètement différentes par nature :

- **Un exploit** se sert de différentes techniques pour s'infiltrer dans les failles et accéder à un système d'exploitation ou un code applicatif.
- **Un malware** est un fichier ou un code permettant à un cybercriminel d'atteindre un but précis au sein d'un système (infecter, explorer, voler, etc.).
- **Un ransomware** est un type de malware permettant à un cybercriminel de chiffrer des données ou fichiers importants, qu'il ne déchiffrera qu'en échange d'une rançon.

Au vu des différences intrinsèques entre exploits et malwares, il est impératif d'opter pour une prévention qui vous protège contre les deux et intègre les fonctionnalités ci-après.

1. Analyses des malwares

Face au volume, à la diversité et à la complexité des menaces qui planent sur les environnements d'entreprise, la mise en place d'une prévention réellement efficace tient souvent de la gageure. S'ajoute à cela la difficulté à détecter les malwares et exploits inconnus, en plus de ceux déjà connus.

Pour lutter efficacement contre ces menaces sophistiquées, ciblées et furtives, la protection des terminaux doit être associée à une Cyber Threat Intelligence (CTI) mutualisée qui permet d'actualiser les défenses en permanence. Selon une étude IDC Research, 39 % des professionnels de la sécurité considèrent le partage d'informations CTI comme une priorité élevée, voire absolue, pour renforcer la sécurité.[3] En ce sens, l'intégration d'une Threat Intelligence en mode cloud aux systèmes de protection des terminaux permet d'approfondir les analyses pour détecter rapidement les menaces potentiellement inconnues. Dans le cas de malwares encore plus furtifs, des fonctionnalités de machine learning installées sur le terminal doivent permettre d'évaluer rapidement un fichier. Objectif : identifier les signes suspects, effectuer des analyses dynamiques plus approfondies et, si besoin, placer le fichier dans une sandbox.

2. Prévention contre les ransomwares

Bien que les ransomwares ne datent pas d'hier, des attaques majeures comme WannaCry, Petya/NotPetya et TrickBot ont démontré l'incapacité des méthodes de prévention traditionnelles. Incapacité d'autant plus criante que les attaquants utilisent désormais des malwares encore plus sophistiqués, automatisés, ciblés et hautement furtifs.

Prévenir les ransomwares exige la présence de fonctionnalités de « défense en profondeur » (DiD) sur le terminal pour détecter et stopper ces menaces à différentes étapes du cycle d'attaque. Dans le cas de WannaCry, cela consiste d'abord à détecter toute tentative d'élévation des privilèges d'accès au noyau côté utilisateur, puis à bloquer l'attaque. En cas d'échec, le système de protection contre les processus enfants doit détecter le processus parent et l'empêcher d'engendrer un processus enfant. Si ces mesures ne suffisent pas pour détecter les menaces, l'agent installé sur le terminal doit pouvoir se servir d'analyses locales et du machine learning pour identifier les caractéristiques connues de WannaCry.

1. « Challenging State of Vulnerability Management Today: Gaps in Resources, Risk and Visibility Weaken Cybersecurity Posture », Balbix, Inc. et le Ponemon Institute, juillet 2018, https://www.balbix.com/app/uploads/Ponemon-Survey-Vuln-Management-.pdf.
2. « Endpoint Protection and Response: A SANS Survey », SANS Institute, 12 juin 2018, https://www.sans.org/reading-room/whitepapers/analyst/membership/38460.
3. Konstantin Rychkov et Duncan Brown, « Bridging Security Gaps with Network-to-Endpoint Integration », IDC Research, octobre 2018, https://www.paloaltonetworks.com/resources/whitepapers/bridging-security-gaps-with-network-to-endpoint-integration.

WastedLocker : à la croisée des malwares et des exploits

Déjà coupable d'extorsions à hauteur de plusieurs millions de dollars, le ransomware WastedLocker s'exécute par un savant mélange de malwares et d'exploits, sans compter ses fonctionnalités innovantes de contournement des systèmes de protection des terminaux. WastedLocker incite ses victimes à télécharger du code malveillant sur de faux sites Internet de mises à jour logicielles. Un chargeur Cobalt Strike personnalisé est alors installé sur le système visé pour déclencher le ransomware. WastedLocker se propage ensuite latéralement sur le réseau de la victime, exploite un ou plusieurs utilitaires de gestion de système pour garantir sa bonne exécution, puis libère enfin sa charge active.

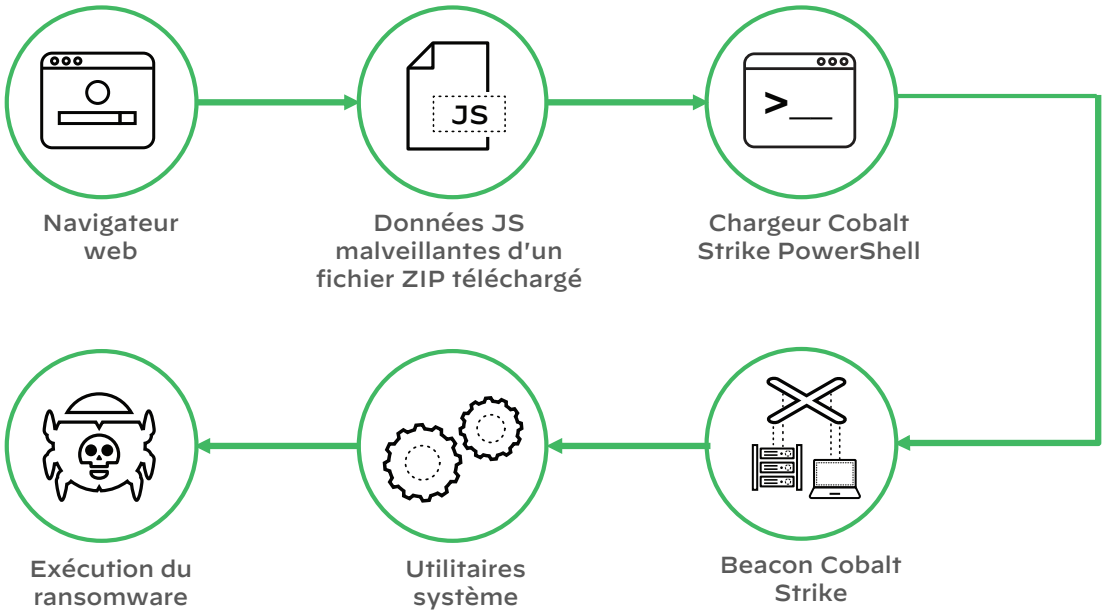

Figure 1 : Séquence simplifiée d'une attaque WastedLocker

3. Prévention contre les exploits

Des milliers d'exploits et de failles logicielles sont découverts chaque année, ce qui oblige les éditeurs à distribuer continuellement de nouveaux correctifs, en complément de ceux déjà gérés par les administrateurs système et sécurité de chaque organisation. Les correctifs ont donc pour mission d'empêcher l'exploitation des vulnérabilités.

Comprendre les techniques d'exploit

Beaucoup de menaces avancées reposent sur l'infiltration de code malveillant dans des fichiers data a priori inoffensifs. Lorsque l'un de ces fichiers est ouvert, le code malveillant exploite des vulnérabilités non corrigées de l'application en question, puis s'exécute en toute liberté. Étant donné qu'il s'agit d'une application autorisée par les politiques de sécurité, ce type d'attaque n'a aucun mal à contourner les contrôles d'autorisation d'applications.

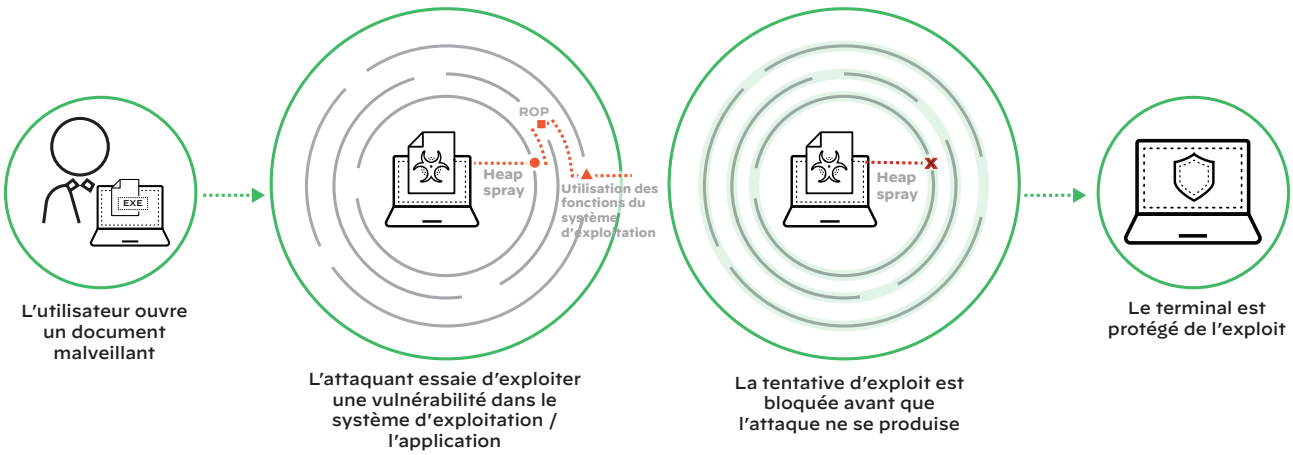

Figure 2 : Ciblez les techniques employées plutôt que les exploits en eux-mêmes

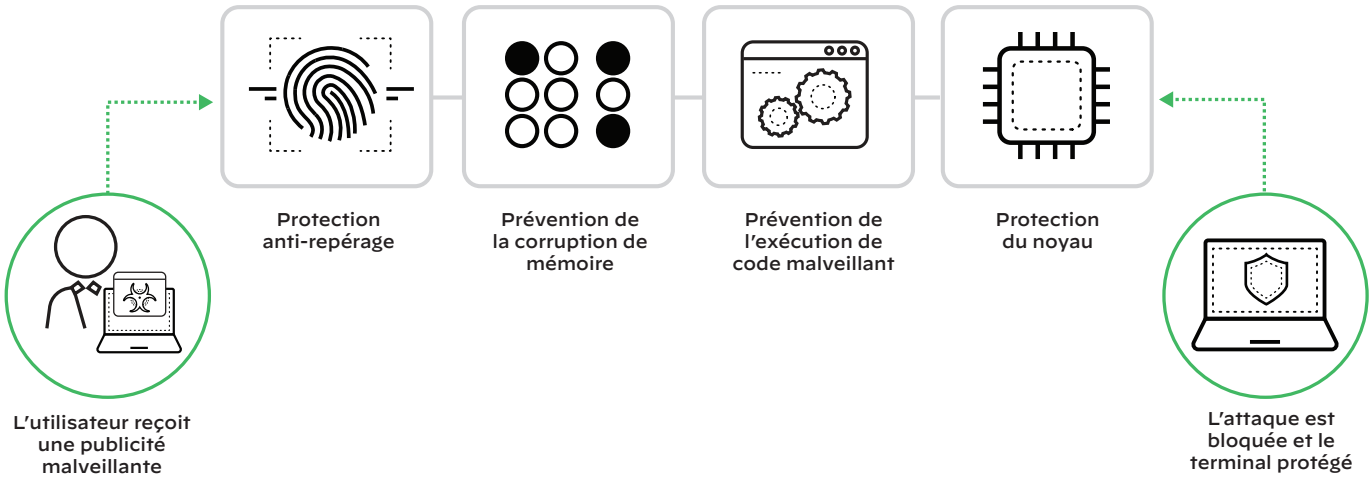

Figure 3 : Multiples méthodes de prévention des exploits

Malgré l'existence de milliers d'exploits, les cybercriminels s'appuient généralement sur un noyau dur de techniques qui évoluent rarement. Indépendamment de l'exploit et de sa complexité, le succès d'une attaque passe par la capacité de son auteur à exécuter ces techniques dans un certain ordre, comme pour trouver la sortie d'un labyrinthe.

La prévention des exploits consiste donc à neutraliser ces techniques de base, de manière à rendre totalement inexploitables les vulnérabilités des applications, qu'elles soient corrigées ou non. Cette approche est particulièrement importante lorsqu'il s'agit de protéger des environnements hétérogènes (ceux comportant des workloads cloud, par exemple) où les contrôles physiques des terminaux peuvent engendrer des complications imprévues dans les environnements virtuels.

Stratégie pérenne de sécurité des terminaux

Si toute sécurité qui se respecte commence par une bonne prévention, cela ne suffit pas à assurer une protection efficace contre les attaques avancées. En effet, même si votre solution de protection des terminaux parvient à bloquer 98 % des tentatives de compromission, 2 % d'entre elles restent encore à découvrir et à neutraliser. Or, cela demande des fonctionnalités de détection et de réponse.

Ces fonctionnalités doivent s'étendre au-delà du terminal concerné. Après tout, les attaquants ne s'arrêtent pas à vos terminaux, alors pourquoi vos outils de sécurité le devraient-ils ? Et c'est précisément là que l'EDR atteint ses limites, car il conduit souvent des équipes de sécurité déjà surchargées à remonter la piste d'une activité malveillante pendant des heures, avec le peu d'indices dont ils disposent, pour finalement constater qu'elle a été bloquée par un pare-feu ou un autre point de contrôle. L'idéal ici est d'intégrer des fonctionnalités de protection et de détection à une plateforme étendue de détection et de réponse (XDR) qui applique le machine learning à un flux de données centralisé. Objectif : offrir une visibilité complète des attaques sur l'ensemble des sources de données et coordonner la prévention sur tous les points de contrôle. Le XDR pousse les capacités de prévention plus loin que n'importe quel NGAV ou EDR. Il offre la visibilité totale et les analyses puissantes dont les équipes de sécurité ont besoin pour lutter contre les attaques sophistiquées actuelles et futures.

Selon une étude Forrester Consulting menée en 2020, seulement 49 % des organisations estiment que leurs outils de sécurité sont bien intégrés. Les entreprises passent trop de temps à rechercher les bonnes données et à les convertir dans des formats adaptés aux analyses. Par ailleurs, ces données doivent parfois être collectées sur de multiples sources pour déterminer quels utilisateurs, appareils, processus ou applications sont associés à des évènements spécifiques. Le XDR automatise ces opérations en corrélant les alertes issues de différentes sources aux incidents de sécurité détectés, ce qui réduit considérablement le volume d'alertes disparates que les analystes doivent gérer au quotidien.

Pour les équipes de sécurité, qui dit moins d'alertes, dit possibilité d'agir plus rapidement. Les solutions XDR de pointe éliminent les angles morts de la sécurité grâce à une intégration parfaite des fonctionnalités de protection, de détection et de réponse sur les terminaux. Outre leur empreinte minime, ils ne dépendent pas de signatures pour la prévention, proposent une interface de gestion en mode cloud et effectuent une collecte étendue des données pour la journalisation des évènements et des alertes. Les équipes de sécurité disposent ainsi de toute la visibilité nécessaire pour adopter une approche opérationnelle préventive sans impacter l'administration des terminaux.

Pour votre prochain investissement NGAV, misez sur le XDR

Les outils cloisonnés et les processus manuels n'ont pas leur place dans les opérations de sécurité de demain. La neutralisation des menaces sophistiquées et de l'arsenal croissant des outils d'attaque nécessitera une utilisation beaucoup plus intelligente et robuste de l'automatisation, du Big Data et du machine learning. Elle passera également par l'intégration plus étroite d'une palette d'outils permettant un déploiement plus rapide et plus complet de nouvelles fonctionnalités. Le choix d'une solution de sécurité des terminaux ne doit plus se baser essentiellement sur la puissance de la protection anti-malware et sur l'empreinte de l'agent installé sur le terminal. Il doit également tenir compte de la capacité de la solution à faciliter les workflows opérationnels indispensables à la sécurité globale d'une organisation.

Tout investissement en sécurité doit prendre en compte un certain nombre d'éléments :

- Contrôles intégrés de protection, de détection et de réponse pilotés par IA et machine learning pour combler automatiquement les failles
- Contrôles unifiés permettant de fluidifier les communications entre le SecOps, les administrateurs des terminaux et du réseau, et les équipes IR
- Alertes de sécurité moins nombreuses mais de meilleure qualité
- Visibilité complète sur toute l'infrastructure (terminaux, réseau et cloud) pour accélérer la détection et la réponse, et réduire la durée d'implantation

Le XDR est la seule solution de sécurité des terminaux capable de répondre à tous ces critères. Pour accélérer les processus de tri des alertes et de réponse à incident, le XDR analyse des données multi-sources (réseau, terminaux et cloud), puis dresse automatiquement un tableau complet de chaque menace et de son origine. Le temps et l'expérience requis à chaque étape SecOps sont ainsi réduits, du tri des alertes jusqu'à la traque de la menace. Une intégration efficace aux points de contrôle permet aux équipes SecOps de répondre rapidement aux menaces et d'utiliser les connaissances acquises pour adapter les défenses, prévenir les futures menaces et ainsi réagir encore plus vite à l'avenir. Enfin, le XDR réduit les niveaux de connaissances et compétences nécessaires aux analystes pour répondre aux attaques, ce qui baisse le coût des opérations de sécurité.

Conclusion

En adoptant une approche préventive de la sécurité autour d'une protection, d'une détection et d'une réponse intégrées, et en tournant l'attention du SecOps du « quoi » vers le « comment », les organisations parviennent à résoudre quatre problèmes qui minent leur efficacité : sécurité insuffisante, surabondance d'alertes, cloisonnement des opérations, et hausse de la durée d'implantation.

Au moment de choisir votre prochaine solution de sécurité des terminaux, intégrez ces exigences à votre cahier des charges : protection intégrée ; élimination du recours systématique aux alertes ; fonctionnalités de détection et de réponse dans un agent léger ; chaînes de causalité avancées permettant de coordonner l'action du SecOps, de l'administration des terminaux et l'IR ; visibilité complète sur toute l'infrastructure (terminaux, réseau et cloud) pour augmenter les taux de détection et de réponse, et réduction de la durée d'implantation.

paloalto NETWORKS

Oval Tower, De Entrée 99 – 197
1101 HE Amsterdam
Pays-Bas
+31 20 888 1883
www.paloaltonetworks.fr