CYBERARK®

EBOOK

Comment garder une longueur d'avance sur les rançongiciels :

UNE ÉTUDE DE LA COMBINAISON EDR ET EPM

UNE DÉFENSE EN PROFONDEUR AVEC LES SYSTÈMES DE DÉTECTION ET DE RÉPONSE SUR LES TERMINAUX (EDR) ET ENDPOINT PRIVILEGE MANAGER (EPM) DE CYBERARK

L'ÉTAT PRÉSENT DE LA PROTECTION DES TERMINAUX ET DES RANÇONGICIELS

Selon les estimations, à l'échelle mondiale, le coût des dommages liés aux rançongiciels atteindra 20 milliards USD en 2021 – soit un coût 57 fois plus élevé qu'en 2015. Cela fait des rançongiciels le type de cybercriminalité qui connaît la croissance la plus rapide.[1]

Les terminaux connectés à Internet sont de très loin le point d'entrée principal des rançongiciels. La surface d'attaque s'est considérablement élargie, en parallèle à la prolifération des types d'appareils connectés, à l'augmentation de la main-d'œuvre à distance et à l'expansion des écosystèmes tiers. Les cybercriminels en ont profité pour multiplier la fréquence des attaques et faire usage de rançongiciels plus sophistiqués.

Les entreprises sont donc confrontées au défi de réduire les risques liés à la sécurité de leurs terminaux. Les dommages perpétrés peuvent prendre la forme d'une perturbation des opérations commerciales et/ou d'extorsion. Et comme de nombreuses victimes en attestent, les rançongiciels ne s'arrêtent pas aux terminaux, mais cherchent à se propager au sein des organisations pour soutirer des données plus précieuses.

Cet eBook examine en quoi une stratégie approfondie de défense des terminaux contre les rançongiciels requiert de combiner des systèmes de contrôle d'identité et des technologies de sécurité des terminaux. Nous mettrons l'accent sur la manière dont les systèmes Endpoint Privilege Manager (EPM) et Endpoint Detection and Response (EDR) de CyberArk peuvent fonctionner conjointement pour vous aider à garder une longueur d'avance face aux attaques par rançongiciel.

Les rançongiciels en hausse

- En 2020, la transition de masse au travail à domicile a donné lieu à une augmentation de 800 % du nombre de signalements d'attaques par rançongiciel.[2]
- En mars 2020, TechRepublic a fait état d'une hausse de 667 % du nombre d'attaques par harponnage. En avril, le FBI avait observé une hausse de 400 % du nombre de cyber-attaques.[3]
- Selon une estimation du Ponemon Institute, les nouveaux risques et défis posés par le travail à distance accroîtront le coût moyen mondial des fuites de données comptabilisé en 2020 de 137 000 USD, pour un total d'environ 4 millions USD par incident.[4]

[1] Steve Morgan, Cybercrime Magazine, Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021, 21 octobre 2019.
[2] Danielle Waugh, CBS12 News, Coronavirus crisis brings increase in cyber attacks, 22 mars 2020.
[3] Esther Shein, TechRepublic, 667% spike in email phishing attacks due to coronavirus fears, 26 mars 2020.
[4] Ponemon Institute, Cost of a Data Breach Report, 2020.

Les rançongiciels reviennent à la charge !

« Nous avons entendu parler d'une entreprise qui a payé une rançon (un peu moins de 6,5 millions de livres sterling aux taux de change actuels) et récupéré ses fichiers (en utilisant le déchiffreur fourni par les attaquants), mais n'a ensuite fait aucun effort pour identifier la cause profonde de l'attaque et sécuriser son réseau. Moins de deux semaines plus tard, le même pirate attaquait à nouveau le réseau de la victime, en utilisant le même mécanisme qu'auparavant et en redéployant son rançongiciel. La victime a senti qu'elle n'avait pas d'autre choix que de payer à nouveau la rançon. »[6]

VECTEURS ET IDENTITÉ DES RANÇONGICIELS

Les attaques par rançongiciel commencent par l'installation d'un logiciel malveillant en exploitant les failles de configuration et les vulnérabilités des accès. Les quatre principaux vecteurs d'accès des rançongiciels aux terminaux sont les suivants :

- Téléchargements de logiciels malveillants via un navigateur
- E-mails d'ingénierie sociale – hameçonnage
- Vol ou compromission d'identifiants
- Exploitation de vulnérabilités connues (CVE)[5]

Les privilèges élevés associés aux comptes administrateur en font les cibles les plus attrayantes. La visibilité des privilèges d'administrateur dynamiques sur les terminaux (par exemple, les comptes administrateur Microsoft Windows ou MacOS) a toujours représenté un point sensible. Il est notoirement difficile de gérer ces privilèges de manière sécurisée sans affecter la productivité.

[5] CyberArk, The CISO View 2021 Survey: Zero Trust and Privileged Access, 2021.

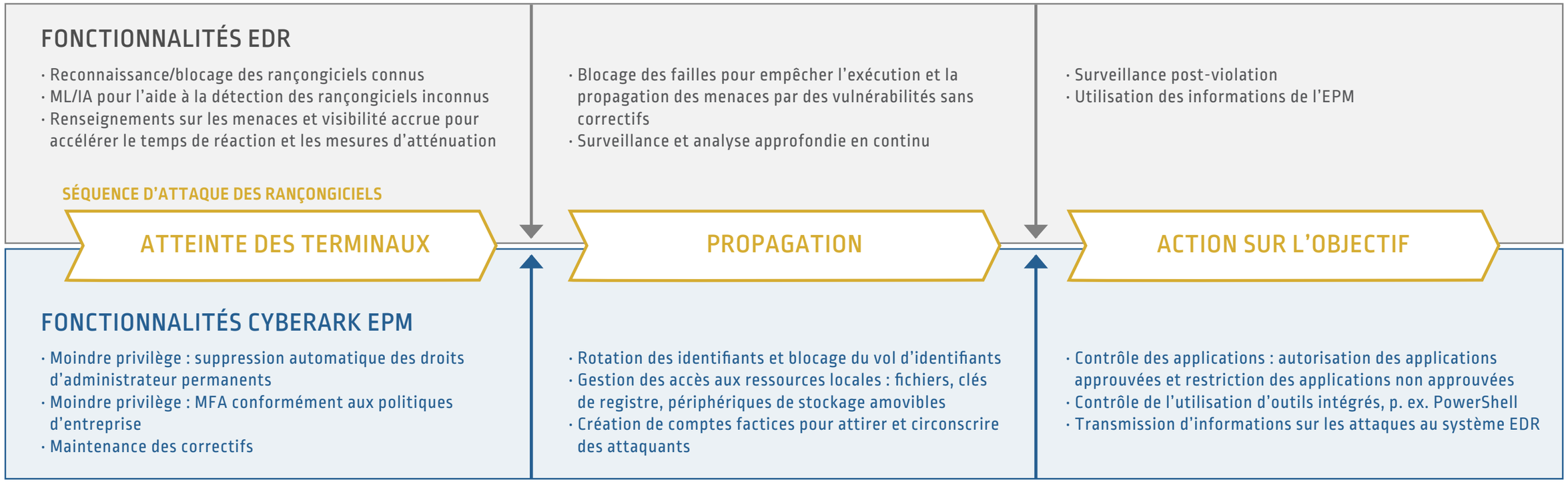
[6] Danny Palmer, ZDNet, Ransomware: A company paid millions to get their data back, but forgot to do one thing. So the hackers came back again, 5 avril 2021.

Une fois installés, les rançongiciels passent en mode furtif en désactivant la sécurité des terminaux et les systèmes de surveillance dans la mesure du possible. Leur objectif suivant consiste à collecter des identifiants pour accéder à des niveaux de privilèges encore plus élevés et à se propager de façon latérale, en quête d'autres systèmes et de données plus précieuses pour mener à bien leur mission d'extorsion. Ce faisant, ils corrompent les sauvegardes, effacent les copies masquées et déverrouillent des fichiers dans le but de maximiser l'impact de l'attaque. Certains rançongiciels plus sophistiqués sont même capables de laisser des portes dérobées ou des identifiants cachés en vue d'attaques futures.

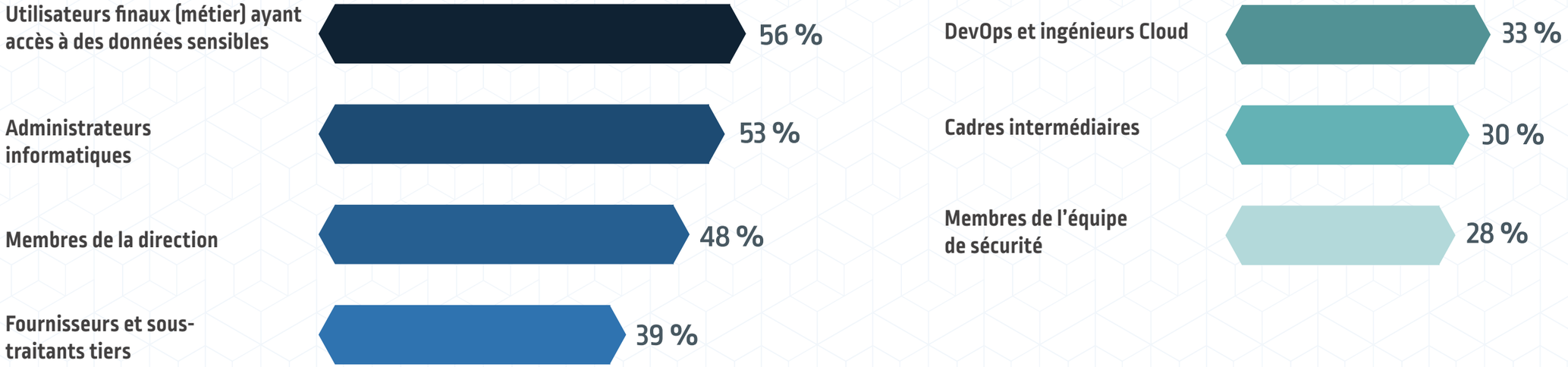
Pour finir, le rançongiciel s'exécute et passe à l'action sur les fichiers cibles, généralement en exploitant les autorisations de lecture et d'écriture pour chiffrer les fichiers et les prendre en otage.

L'objectif des contrôles d'identité et des technologies de sécurité des terminaux est non seulement de détecter et de bloquer les rançongiciels, mais aussi de veiller à ce que les privilèges d'administrateur ne puissent être exploités à aucun moment au cours d'une attaque.

EPM et EDR, la meilleure combinaison contre les attaques par rançongiciel



56 % signalent un ciblage accru des utilisateurs finaux ayant accès à des données sensibles[7]



Ce que disent les RSSI[7]

97% des répondants ont déclaré que les attaquants de plus en plus de voler un ou plusieurs types d'identifiants.

56% du harponnage des utilisateurs finaux, tels que les utilisateurs métier ayant accès à des données sensibles.

53% ont signalé une augmentation du harponnage des administrateurs informatiques.

[7] CyberArk, Enquête CISO View 2021 : Zero Trust et accès à privilèges, 2021.

L'ÉVOLUTION ET L'EXTENSION DES SYSTÈMES EDR

Distincts à l'origine des solutions antivirus visant à empêcher la pénétration par des logiciels malveillants, les systèmes EDR étaient axés sur la détection et l'analyse des activités suspectes au niveau des terminaux. Ces systèmes étaient proposés en tant que couche de sécurité supplémentaire, en plus d'un antivirus et/ou d'un logiciel de protection des e-mails et d'autres outils d'atténuation des menaces.

Mais l'EDR a parcouru un long chemin depuis. Aujourd'hui, un système EDR peut essentiellement fonctionner comme un agent unique en « quasi-temps réel », conçu pour :

- capturer l'activité des terminaux grâce à une surveillance continue afin que les clients sachent à tout moment ce qui se passe ;
- assurer une visibilité et une analyse approfondies pour permettre la détection automatique des activités suspectes, l'interception des attaques furtives et l'interruption des violations ;
- accélérer les opérations de sécurité, en permettant aux utilisateurs de minimiser l'effort consacré au traitement des alertes pour analyser les attaques et réagir rapidement.

Les nouvelles fonctions étendues de détection et de réponse (XDR) au niveau des terminaux peuvent inclure ou être vendues avec d'autres solutions de sécurité, telles que des solutions antivirus de nouvelle génération (NGAV) et des suites d'analyse de données et de réseau, de chasse aux menaces et de réponse aux incidents.

Exemple de MFA sensible aux risques

De nombreuses violations de données notoires ont commencé par la compromission d'identifiants VPN par les attaquants, permettant à ces derniers d'accéder aux systèmes internes d'une entreprise.

L'application de la MFA aux accès VPN permet aux entreprises de fournir à leurs employés et partenaires un accès à distance sécurisé à leur réseau, aux applications sur site et aux ressources.

Pour adopter une approche de défense en profondeur, effectuez également une inspection du système d'exploitation et une autorisation de certification de groupe.

Ces systèmes peuvent exploiter un certain nombre de technologies modernes dans la lutte contre les rançongiciels, notamment l'intelligence artificielle, la détection comportementale et les algorithmes d'apprentissage machine. Ils permettent aux entreprises :

- de détecter et bloquer les rançongiciels connus ;
- d'identifier et bloquer d'autres rançongiciels inconnus à l'aide d'indicateurs d'attaques (IOA) ;
- de bloquer des failles pour empêcher l'exécution et la propagation des rançongiciels par des vulnérabilités sans correctifs ;
- de se protéger contre les nouvelles variantes de rançongiciels qui n'utilisent pas les fichiers pour chiffrer les systèmes victimes ;
- de contrôler et atténuer les risques liés aux périphériques USB en définissant les périphériques autorisés et le niveau d'accès ;
- de gérer les pare-feux en créant et appliquant des politiques avec une approche centralisée simple pour se protéger contre les menaces réseau.

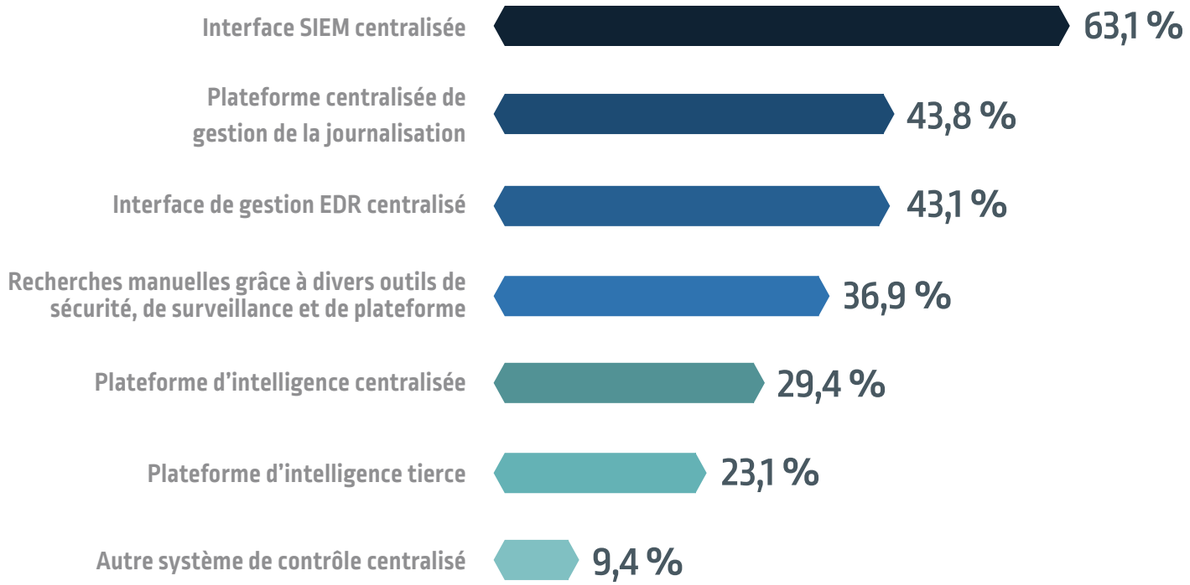
Selon une récente enquête de SANS, les systèmes EDR évoluent pour devenir les plateformes privilégiées de gestion des terminaux. (La même enquête indique que la majorité (51,6 %) des violations de sécurité ont été détectées par des solutions EDR.)[8]

Pourtant, les systèmes EDR ou XDR ne sont pas conçus pour analyser et gérer de façon spécifique et sécurisée les identités et les privilèges, dont la compromission est à la base de nombreuses attaques de rançongiciel.

[8] SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey Results.

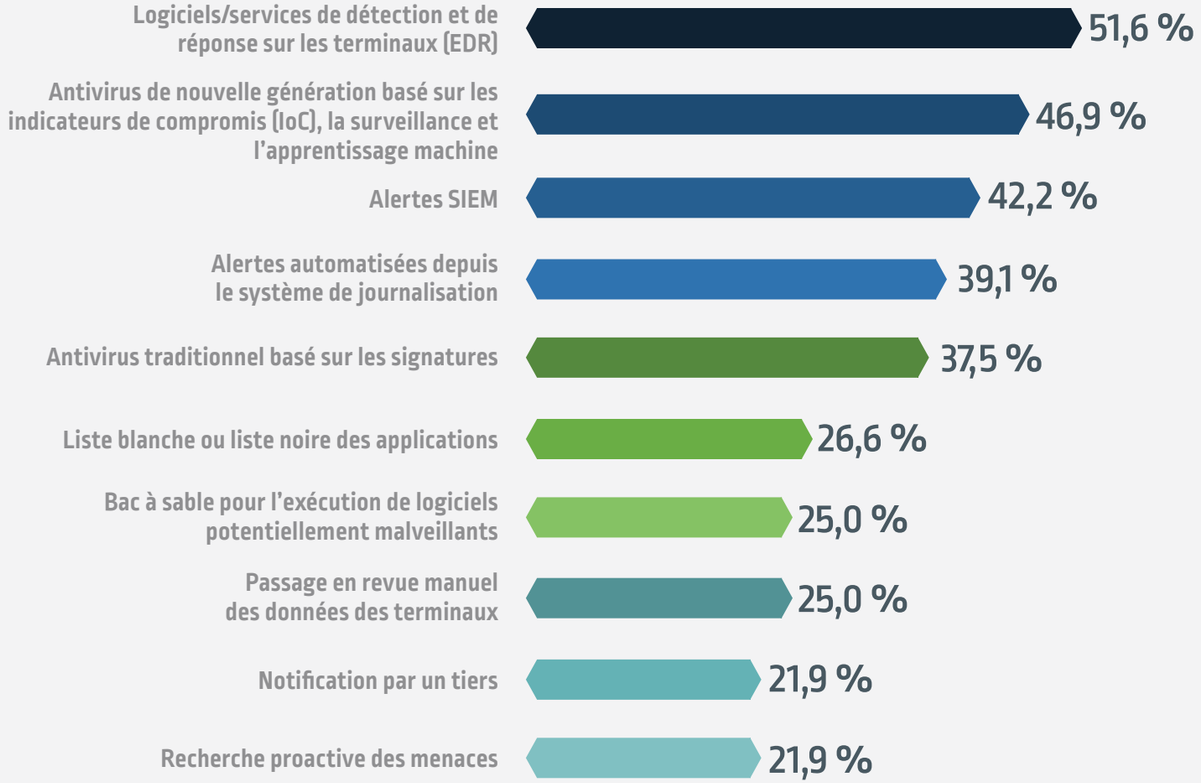
Collecte de données des terminaux[9]

Comment analysez-vous et protégez-vous les données des terminaux pour prévenir et détecter les menaces ? *Sélectionnez toutes les réponses applicables.*



Détection des violations[10]

Quels outils/services ont détecté la violation ? *Sélectionnez toutes les réponses applicables.*



[9, 10] Matt Bromiley, SANS 2021 Endpoint Monitoring in a Dispersed Workforce Survey, 15 mars 2021.

FERMER LES PORTES AUX ATTAQUANTS AVEC LES COMPTES À PRIVILÈGES

CyberArk EPM se fonde sur la « présomption de violation ». Il s'agit d'adopter l'état d'esprit d'un attaquant pour vous aider à détecter et isoler les attaques par rançongiciel, avant qu'elles ne pénètrent votre réseau et ne se propagent en infligeant de graves dégâts.

CyberArk EPM est conçu pour réduire considérablement la surface d'attaque offerte par les terminaux distribués en combinant le principe du moindre privilège, la protection contre les rançongiciels, le contrôle des applications et d'autres fonctionnalités uniques :

- Amélioration de la prévention des attaques qui partent des terminaux par la suppression des droits d'administrateur local sur les postes de travail Windows, les serveurs et les Mac – peut-être la défense la plus précieuse contre les rançongiciels ;
- Application automatique de contrôles complets du moindre privilège, qui accordent uniquement aux utilisateurs les privilèges requis pour effectuer leur travail ;
- Restriction de l'exécution de rançongiciels qui échappent aux mécanismes de détection ou de blocage par le contrôle des applications, en leur permettant de s'exécuter uniquement dans certaines conditions ou en définissant des stratégies relatives aux capacités de lecture/d'écriture/de modification des applications ;
- Détection et blocage automatiques des tentatives de vol d'identifiants mis en cache par Windows, les navigateurs Web, les gestionnaires de mots de passe, les solutions d'authentification unique (SSO) et d'autres programmes ;
- Application d'un système de sécurité qui ne compromet pas la productivité par l'octroi d'autorisations « juste à temps » ;
- Création de comptes à privilèges factices (« pots de miel ») pour attirer et circonscrire des attaquants au point d'entrée, avant qu'ils ne puissent faire des dégâts ;
- Définitions de politiques prêtes à l'emploi pour la protection contre les rançongiciels, avec des contrôles complets du respect du principe du moindre privilège testés sur des millions d'échantillons de logiciels malveillants ;
- Restriction considérable des mouvements latéraux et de la propagation des rançongiciels, à l'aide d'une MFA automatique basée sur des politiques et d'une protection renforcée des comptes à privilèges.

Conclusions de CyberArk Labs[11]

Des tests continus menés sur 3 millions d'échantillons de grandes familles de rançongiciels ont abouti à une conclusion majeure : quand les droits d'administrateur local étaient supprimés et que des stratégies de contrôle des applications étaient en place, 100 % des échantillons de rançongiciels n'ont pas pu chiffrer les fichiers.

[11] CyberArk Labs, Full Disclosure: Ransomware Exposed, 2021.

DÉFENSE EN PROFONDEUR : COMMENT ASSOCIER EPM ET EDR

CyberArk EPM et EDR réunis permettent aux entreprises de sécuriser leurs systèmes et de réagir aux attaques par rançongiciels, comme le démontre le scénario suivant.

Plan d'attaque : un pirate prévoit de pénétrer une entreprise cible avec un rançongiciel. Son but à court terme est de prendre en otage des données de la plus haute valeur en les chiffrant et, à moyen terme, de revenir à la charge ultérieurement en installant une porte dérobée.

Pour obtenir l'accès initial, l'hameçonnage d'identifiants mal protégés est une technique courante. D'autres techniques peuvent consister à utiliser des mots de passe volés achetés sur le Dark Web, ou simplement à essayer un grand nombre de mots de passe possibles par des attaques de force brute. Une fois infiltré dans l'infrastructure, l'attaquant s'efforcera de collecter des identifiants – de préférence avec des privilèges d'administrateur – pour exploiter les vulnérabilités et installer et exécuter le code.

Le rôle du système EDR : la surveillance continue et l'analyse approfondie peuvent reconnaître et arrêter les rançongiciels connus et accélérer les opérations de sécurité, en permettant aux utilisateurs de minimiser l'effort consacré au traitement des alertes pour analyser les attaques et réagir rapidement.

Le rôle de CyberArk EPM : même avec un rançongiciel de type « Day 1 » qui échappe à l'EDR, l'attaquant aura du mal à obtenir un accès initial à cause de la suppression automatique des comptes administrateurs sur les terminaux. Les tentatives de vol d'identifiants seront automatiquement détectées et bloquées. Quant à ceux qui parviendraient éventuellement à passer outre, ils ne pourront s'exécuter que dans certaines conditions grâce au contrôle des applications d'EPM, qui applique des stratégies définies au niveau des capacités de lecture/d'écriture/de modification des fichiers. Les mouvements latéraux seront restreints par une MFA automatique basée sur des politiques et la protection renforcée des comptes à privilèges, de manière à limiter encore la propagation et les dommages. Les risques d'installation d'une porte dérobée sont considérablement réduits.

Attaques futures : si vous ne trouvez pas les causes profondes et si vous ne remédiez pas aux vulnérabilités, les attaquants reviendront. Les informations fournies par CyberArk EPM sur la façon dont les attaquants essaient d'abuser des privilèges peuvent être utilisées conjointement avec EDR pour contrer une attaque future. EDR peut également contribuer à la surveillance post-violation (par exemple, pour les rançongiciels inconnus).

COMMENT CYBERARK PEUT VOUS AIDER

CyberArk EPM complète idéalement les capacités de surveillance continue en temps réel et de réponse et d'analyse automatisées des solutions EDR/XDR contre les attaques de rançongiciels.

CyberArk EPM est conçu pour réduire considérablement la surface d'attaque offerte par les terminaux distribués en combinant le principe du moindre privilège, la défense contre les privilèges, la protection contre le vol d'identifiants et les rançongiciels, ainsi que le contrôle des applications. Il en résulte un environnement dans lequel le système EDR et d'autres solutions de sécurité peuvent intervenir plus efficacement.

Sur le plan opérationnel, CyberArk EPM vous permet d'atténuer le risque d'une fuite de données grave d'une manière transparente pour les utilisateurs finaux et sans impact sur la productivité.

En tant que solution SaaS, CyberArk EPM simplifie le déploiement et les opérations et accélère le délai de rentabilisation.

En savoir plus ?

Les rançongiciels exposés : La voie vers des stratégies de chiffrement et d'atténuation

CyberArk Labs analyse des centaines de nouveaux échantillons de rançongiciels chaque jour. Dans ce livre blanc, l'équipe partage son évaluation portant sur plus de 3 millions d'échantillons. Téléchargez ce document dès maintenant.

ACCÉDER AU LIVRE BLANC

Gestion des privilèges des terminaux : Guide de démarrage rapide

Passez directement à l'action avec cette vue d'ensemble pratique du déploiement en 3 phases suggéré par CyberArk de la solution de gestion des privilèges leader sur le marché.

ACCÉDER À LA PRÉSENTATION DE LA SOLUTION