VECTRA
SECURITY THAT THINKS

EBOOK

Lutte contre les ransomwares : la réalité du terrain

Introduction

Si aucune entreprise ne souhaite découvrir que son environnement est la cible d'une attaque de ransomware, l'identifier au plus tôt vous offrira de meilleures chances de la neutraliser. Mais comment procéder ? Voilà la question que nous allons étudier ici, au travers d'exemples concrets présentant la manière dont nos principaux clients collaborent avec l'équipe Vectra Sidekick pour intervenir au stade précoce des attaques de ransomOps et éviter les répercussions désastreuses qu'induirait le déploiement d'un ransomware.

Cet eBook vous explique tout, de l'importance de la détection des activités des attaquants et des ransomOps aux diverses procédures de sécurité adoptées par les professionnels pour contrer efficacement les tactiques des cybercriminels. Nous vous expliquons également comment les services Vectra Sidekick aident nos clients à détecter presque immédiatement les attaques en cours, et nous détaillons les principaux enjeux, observations et recommandations dont toute entreprise devrait avoir conscience.

Une chose est sûre, en matière de lutte contre les ransomwares, la réactivité et la rapidité d'intervention sont fondamentales.

Service MDR Vectra Sidekick

La solution MDR Vectra Sidekick est un service de cyberveille fonctionnant en continu, qui analyse de manière proactive les activités malveillantes signalées par Vectra Detect.

La solution MDR Vectra SideKick agit comme un démultiplicateur de votre équipe de sécurité en déployant des analystes expérimentés pour vous aider à tirer pleinement profit de l'intelligence artificielle Vectra afin d'anticiper les menaces et de mettre fin aux compromissions. Associée à la plate-forme Vectra, la solution MDR Sidekick vous offre les avantages suivants :

- Renforcement de votre équipe de sécurité par le soutien d'analystes de sécurité expérimentés pour contrer et expulser les adversaires et les acteurs de ransomware les plus sophistiqués.
- Expertise, contexte et précisions concernant les premiers indices relevés par Vectra Detect au sujet d'une éventuelle attaque, menace ou présence de ransomware et aide proactive favorisant une intervention rapide.
- Surveillance proactive 24 heures sur 24, 7 jours sur 7 et 365 jours par an permettant d'identifier les menaces prioritaires et les détections de ransomware qui nécessitent une intervention immédiate.
- Personnalisation du déploiement de votre solution Vectra en fonction de votre propre environnement, de vos objectifs métier et des risques propres à votre secteur. Cela comprend la personnalisation des contrôles, le partage de recommandations d'experts, de tendances et d'indicateurs en relation avec votre environnement, ainsi que le soutien aux investigations.

Le phénomène des ransomwares : un business avant tout

En dehors de toute considération éthique, les gangs de ransomware et leurs associés exercent essentiellement une activité économique, dont l'objectif est de générer du profit. Motivés par l'appât du gain, ils tirent parti de leurs compétences pour s'infiltrer dans les systèmes, y voler des données aussi rapidement que possible et exiger une forte rançon pour les restituer.

Cette mentalité trouve un écho dans bon nombre des observations relevées dans cet eBook, tandis que la compréhension des motivations qui animent les attaquants est essentielle pour élaborer une stratégie de sécurité efficace. Si vous connaissez ces motivations et que vous pouvez identifier clairement les systèmes et données de votre environnement dont la compromission est susceptible d'engendrer des perturbations, votre entreprise sera capable de mettre des bâtons dans les roues des cyberpirates.

Voyons le rôle que les exercices de simulation ont à jouer dans cette approche, et découvrons comment les tests d'intrusion peuvent participer à l'élaboration d'un rapport objectif sur votre état de préparation.

Ne pas négliger les mesures de base

Dans un monde idéal, les gangs de ransomware seraient maintenus en permanence à l'écart de votre environnement. Mais, la prévention n'étant jamais infaillible, leur souci de la rentabilité pourrait finalement tourner à votre avantage. En réalité, réduire considérablement les risques d'attaque est possible, en adoptant de bonnes pratiques fondamentales en matière d'authentification et d'application de correctifs.

En effet, pour s'introduire dans les systèmes, les attaquants privilégient généralement les vulnérabilités non corrigées ou exposées de la DMZ, les comptes dépourvus d'authentification multifacteur (MFA) ou d'autres cibles faciles d'atteinte. Fondamentalement, face aux entreprises qui négligent certaines mesures de prévention de base, les cyberpirates n'ont pas besoin de recourir à des tactiques chronophages et sophistiquées.

> Dans un monde idéal, les gangs de ransomware seraient maintenus en permanence à l'écart de votre environnement.

La bonne nouvelle est qu'en activant l'authentification multifacteur au niveau de votre VPN, de votre fournisseur d'identité et de vos autres points d'entrée, vous compliquez la vie des attaquants à tel point qu'ils pourraient simplement vous préférer une autre victime. Le même principe s'applique à la gestion des correctifs : veiller à appliquer les bonnes pratiques de correction des problèmes sur l'ensemble de votre DMZ contribue à repousser les attaques. Et si aucune stratégie de prévention n'est infaillible, des investissements judicieux en la matière compliqueront la tâche des cyberpirates.

Se tenir prêt à intervenir rapidement... de jour comme de nuit

Adopter des mesures de sécurité de base réduit le risque, mais ne l'élimine pas totalement. Les raisons à cela sont nombreuses, mais le fait est qu'il ne suffit que d'une petite erreur dans la configuration d'un compte, de l'oubli d'un seul correctif, d'un simple clic sur un lien malveillant... ou d'une nouvelle menace jour zéro dans votre VPN principal (financée par l'argent qui afflue en masse vers l'écosystème des ransomwares) pour créer une brèche dans votre système. Ce ne sont pas les options qui manquent.

Dès lors qu'un acteur malveillant accède à votre environnement, attendez-vous à ce qu'il se déplace VITE. Si nous avons déjà eu affaire à des attaques dont la progression lente s'étalait sur plusieurs jours, il n'est cependant pas rare que le gros d'une attaque se concentre sur une seule soirée, à des heures tardives. Souvenez-vous que pour un cybercriminel motivé par le profit, le temps c'est de l'argent. Soit parce qu'ils ne souhaitent pas laisser aux équipes de sécurité le temps de réagir, soit parce qu'ils visent avant tout une grande quantité de cibles, nous observons généralement peu de cas où les attaquants essaient de rester discrets. En réalité, la durée globale d'implantation des attaques de ransomware a fortement baissé ces dernières années.

La bonne nouvelle pour les équipes de sécurité est qu'à condition de disposer de la bonne technologie, cette rapidité de déploiement rend aussi ces attaques plus facilement détectables. Chez Vectra, nous avons par exemple déjà identifié des attaques au niveau de systèmes critiques dans les deux minutes suivant l'intrusion initiale. Cette vitesse de progression implique toutefois d'être prêt à intervenir rapidement et de manière décisive afin de stopper la menace avant que le ransomware ne soit déployé.

Malheureusement, cette capacité à réagir vite ne répond pas à la logique des horaires de bureau. Les mesures de reconnaissance précoce et les déplacements latéraux s'observent à toute heure, vraisemblablement à chaque fois que les acteurs malveillants disposent d'un peu de temps. Ils agissent ainsi en pleine journée, durant la nuit, le week-end ou même les jours fériés. Toutefois, nous avons observé que l'assaut final pour l'exfiltration et le chiffrement des données tendait à se produire en pleine nuit, le week-end ou les jours fériés — bref, au moment où les capacités de résolution des incidents sont à leur plus bas niveau.

Concrètement, cela rend la surveillance 7 jours sur 7 et 24 heures sur 24 indispensable.

Disposer d'une stratégie d'intervention sur incidents

La première étape pour contrer une menace de ransomware consiste à détecter l'adversaire dans votre environnement. Par ailleurs, disposer de plans d'action qui tiennent compte de divers scénarios est tout aussi essentiel. Mais jusqu'où êtes-vous prêt à aller ? Confrontée à un attaquant qui avait obtenu un accès administrateur à son contrôleur de domaine, l'équipe de sécurité de l'un de nos clients s'est vue contrainte de prendre sur-le-champ la décision de déconnecter complètement ses systèmes d'Internet pour se donner le temps d'intervenir. Heureusement pour ce client, cette stratégie a fonctionné.

Si cette équipe a frôlé de très près le déploiement du ransomware, ce type de scénario n'est pas si rare. Et vous, que feriez-vous si votre entreprise se retrouvait dans la même situation ? Un tel niveau de perturbation des activités serait-il acceptable dans votre cas ? Seriez-vous capable d'intervenir efficacement en privant de connectivité votre personnel de sécurité agissant à distance ? Pourriez-vous envisager d'autres options d'intervention ?

Nous avons vu des actions rapides et décisives réalisées sous pression se transformer en éléments clés de la réussite d'une intervention. Connaître et éprouver votre plan d'action avant d'en avoir véritablement besoin peut faire toute la différence.

Bloquer les ransomwares en amont

Les attaques modernes de ransomware (les ransomOps pour être exact) ne déploient leur fichier binaire qu'à la toute fin du processus. Ce qui signifie que si vous détectez un ransomware, c'est probablement que vous arrivez trop tard.

Contrairement aux idées reçues, pour parvenir à stopper ce type d'attaque en cours, il faut détecter et contrer les étapes qui viennent AVANT le déploiement du ransomware. Il est d'ailleurs fort probable que vous deviez intervenir sans connaître véritablement votre adversaire ou son objectif final. Dans la plupart des cas, vous assisterez à une progression rapide de l'attaque et détecterez certains indices clés en analysant les outils ou l'infrastructure C&C (Command & Control), qui vous permettront d'établir une hypothèse éclairée sur ce qui se passe.

À cette étape, vos plans d'intervention sur incidents devront adopter une approche plus globale de la progression des attaques et des intrusions, et tenir compte du fait que la motivation de l'attaque n'est qu'une simple probabilité et non une certitude.

Comptes et outils d'administration : des éléments stratégiques clés

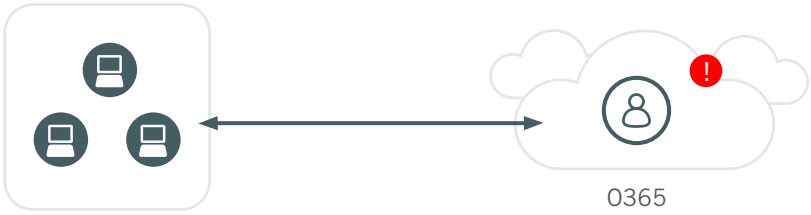
Il arrive que les attaquants utilisent des exploits pour obtenir un accès initial à votre système et parfois pour y réaliser leurs déplacements latéraux. Mais les identifiants des comptes d'administration et de service restent malgré tout au centre des attaques modernes. Parallèlement aux protocoles administrateur, ils correspondent à la technique d'approche préférée de la grande majorité des acteurs de ransomware.

Leur objectif est généralement d'obtenir un accès administrateur au contrôleur de domaine, de façon à pouvoir lancer la phase finale de leur attaque. Cette position avantageuse leur permet d'accéder facilement aux données les plus précieuses. Les outils d'administration, dont les objets Stratégie de groupe (GPO), constituent un autre moyen extrêmement rapide de déployer des ransomwares.

En raison de l'intérêt porté aux identifiants, il est absolument essentiel de surveiller attentivement l'utilisation des comptes à privilèges qui, d'après notre constat, constitue l'un des plus précieux indices dans la détection des attaques.

Constats communs

Les analystes Vectra ont compilé ci-dessous les enjeux liés aux utilisateurs, aux processus et à la sécurité les plus couramment recensés auprès de nos clients.



Accès initial

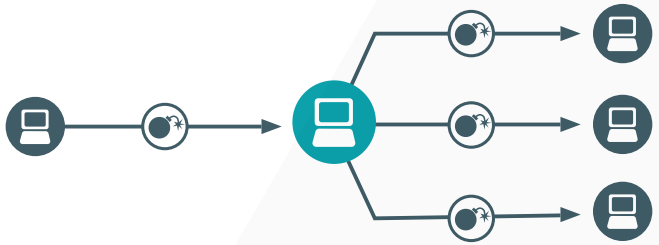
- Les attaquants recherchent les vulnérabilités sur les systèmes et services accessibles au public et connectés à Internet.
- Les serveurs exécutant le protocole RDP, FTP ou associés à un VPN sont des cibles prisées, qui fournissent un accès initial aux systèmes et aux clouds des entreprises.
- L'absence d'authentification multifacteur (MFA) est une faille souvent exploitée.
- La progression des attaques à compter de l'intrusion initiale peut prendre quelques heures, quelques jours, voire plusieurs semaines. Cela laisse suffisamment de temps aux équipes de sécurité pour détecter et résoudre les incidents, à condition d'être vigilantes 24 heures sur 24 et 7 jours sur 7.

C&C

- Cobalt Strike est l'outil qui semble avoir la cote actuellement.
- Des outils d'accès à distance populaires, qu'ils soient ou non autorisés, sont également utilisés pour contrôler les systèmes. Dans un cas particulier, il a été fait usage du logiciel Cisco AnyConnect pour permettre à une personne externe de contrôler les machines à l'intérieur de l'environnement ciblé.

Reconnaissance et déplacement latéral

- Dans la plupart des cas, la recherche de failles est agressive et inclut le mappage du réseau, les requêtes rDNS et l'énumération des partages. Cette analyse rapide rend généralement les attaques visibles dans les minutes qui suivent l'accès initial.
- L'usage de la reconnaissance, notamment des requêtes LDAP et des appels RPC, pour mapper l'emplacement des identifiants est également courant.
- Les déplacements latéraux observés au cours des phases initiales des attaques s'appuient sur des exploits communs. Les phases ultérieures reposent quant à elles principalement sur les identifiants et les protocoles d'administration.



Exfiltration

- Les sites gratuits de partage de fichiers sont couramment utilisés pour importer les informations de reconnaissance à analyser. On retrouve parmi eux Mega Upload (mega.com) et temp.sh.

Recommandations

Chaque jour, nous apportons notre aide aux équipes de sécurité dans leur gestion des alertes critiques générées par les solutions Vectra de détection et aide à la résolution des incidents appuyées par l'intelligence artificielle. Lorsque nous intervenons auprès des clients, nous ne savons pas forcément si la menace détectée est un ransomware. Tandis qu'elle s'aggrave, l'alerte nous permet de gagner en précision et en contexte, et d'en confirmer la nature. Grâce à cette approche, nous avons pu recenser toute une gamme d'outils et pratiques de sécurité qui permettent de mener la vie dure aux campagnes de ransomware, mais aussi de contrer efficacement les adversaires. En voici quelques exemples :

Prévention

- Évaluez régulièrement votre stratégie de sécurité externe et appliquez les correctifs de haute priorité. Concentrez-vous surtout sur l'infrastructure d'accès à distance et sur les services connus pour être vulnérables comme les protocoles RDP et FTP, qui se sont avérés des cibles populaires.
- Activez l'authentification multifacteur (MFA) au niveau de tous les fournisseurs d'identité ou de toute infrastructure d'accès à distance, dès que cela est possible.
- Des règles, des stratégies et des contrôles préventifs solides rendent l'élévation des privilèges plus complexe et ce, même si l'intrusion initiale a déjà eu lieu, ce qui offre davantage de temps pour intervenir.
- Une attention particulière doit être portée aux comptes à privilèges. Bien que cela reste complexe d'un point de vue opérationnel, l'emploi de serveurs intermédiaires (jump servers) et de systèmes de gestion des comptes à privilèges rendra toute procédure d'élévation plus difficile.

Détection

- L'attaque peut être stoppée dès l'intrusion dans le système et avant que les données ne soient exfiltrées ou que le ransomware ne soit déployé.
- Investissez dans des solutions de détection et d'aide à la résolution des incidents pour votre réseau, votre infrastructure d'identités, votre cloud et vos terminaux pour augmenter vos chances de détection rapide.

Investigation et intervention sur incidents

- Les attaques de ransomware peuvent progresser rapidement, à n'importe quelle heure du jour ou de la nuit. Veiller à la surveillance des alertes critiques 24 heures sur 24, 7 jours sur 7 et 365 jours par an est essentiel. Pour ce faire, vous pouvez choisir de recruter du personnel supplémentaire ou de mettre à profit des solutions managées de détection et d'aide à la résolution des incidents (MDR) ou de fournisseurs de services de sécurité managés (MSSP).
- L'intégration de la télémétrie aux journaux relatifs au réseau, aux terminaux et au cloud aide à contextualiser les événements, à gagner en précision et à investiguer plus efficacement les menaces afin d'en déterminer précisément la cause fondamentale.
- La recherche d'une activité d'analyse accrue au niveau de votre DMZ et d'outils d'OSINT préalable aux intrusions peut vous fournir de manière anticipée de précieuses informations sur les acteurs de menace présumés, qui vous seront utiles dans votre stratégie d'intervention.

Pour plus d'informations, contactez-nous à l'adresse info_france@vectra.ai.

E-mail : info_france@vectra.ai vectra.fr