Bitdefender Global Leader In Cybersecurity

L'économie parallèle derrière les RANSOMWARES

Table des matières

Bitdefender Global Leader In Cybersecurity

Introduction

La cybercriminalité, à l'instar d'une entreprise, évolue et affine ses opérations pour gagner en efficacité et en rentabilité. En démocratisant l'accès aux ransomwares, les RaaS (ransomwares en tant que service) font partie des grandes évolutions récentes. Tout comme Uber a révolutionné les transports en permettant à toute personne possédant une voiture de devenir chauffeur, la démocratisation des RaaS permet aux individus, indépendamment de leur expertise technique, de lancer des attaques de ransomware sophistiquées, inscrivant de fait les cyberactivités illicites dans une économie à la demande.

Les RaaS ont augmenté la fréquence et la sophistication des attaques de ransomwares, faisant des ransomwares l'une des principales menaces de sécurité, augmentant le nombre d'alertes générées par les différents outils et entraînant des inefficacités dans la gestion des opérations de cybersécurité. Ces attaques ciblent tous les secteurs et peuvent causer des dommages économiques et opérationnels colossaux, qui se chiffrent souvent en millions de dollars en raison des temps d'arrêt, des pertes de données et des atteintes réputationnelles qui en découlent.

Une fois intégrés, les affiliés ont accès à des outils de ransomware personnalisés adaptés à leurs activités. Cette relation repose sur un modèle de partage des bénéfices, sur la base duquel les affiliés reçoivent une part significative des rançons, ce qui les incite à maximiser l'impact des attaques. Cette motivation entraîne une augmentation des attaques ciblant les entreprises dont la posture de sécurité ou la maturité sécuritaire est la plus faible, d'où la nécessité d'une meilleure allocation des ressources pour prévenir les attaques en dépit de contraintes budgétaires.

Si le modèle de partage des bénéfices attire les cybercriminels, il implique également des risques importants. Les conséquences juridiques peuvent être graves, ce qui ajoute une couche de danger à leurs activités. La confiance demeure une question délicate ; avec de tels enjeux, le risque de trahison peut rendre vulnérables les affiliés, soit en leur faisant perdre des bénéfices, soit en les exposant à des poursuites judiciaires si les opérateurs choisissent de rompre les liens ou de divulguer des informations aux autorités.

Opérateurs et affiliés

Les opérateurs et affiliés entretiennent une relation symbiotique cruciale pour la réussite des opérations. Jouant le rôle d'architectes, les opérateurs développent et optimisent les ransomwares, en veillant à ce qu'ils demeurent indétectables, et gèrent l'infrastructure nécessaire à ces attaques, de la maintenance des serveurs aux plateformes de collecte des rançons. Les affiliés, ou « agents de terrain », déploient ces ransomwares, sélectionnent les cibles et exécutent les attaques, qui aboutissent à des négociations de rançons. Ce partenariat commence par un processus de sélection rigoureux sur des forums du Dark Web et des canaux chiffrés, processus qui permet aux opérateurs d'évaluer les affiliés potentiels en fonction de leurs compétences et de leur capacité à échapper à la détection.

Rôles et responsabilités spécifiques au sein du modèle RaaS

L'efficacité du modèle RaaS favorise la spécialisation, au-delà des opérateurs et des affiliés. En se spécialisant, chaque individu apporte son expertise et son expérience, augmentant ainsi les chances de réussite des attaques.

- Les opérateurs jouent un rôle déterminant dans la gestion du développement des ransomwares et dans la supervision de leur déploiement et de l'infrastructure de collecte des rançons. Ils gèrent des processus financiers complexes et fournissent une assistance technique et des mises à jour logicielles afin de soutenir l'ossature des opérations.

- Les développeurs de logiciels se concentrent sur le développement et la maintenance des outils techniques nécessaires aux opérations, en veillant à ce que les ransomwares et leurs mécanismes de développement soient constamment mis à jour et, ainsi, plus susceptibles de contourner les protocoles de sécurité.

- Les courtiers en accès initial sont des experts en pénétration, qui se spécialisent dans la recherche de vulnérabilités et la sécurisation des points d'accès permettant de pénétrer dans les systèmes cibles, préparant ainsi le terrain des attaques.

- Les affiliés exécutent les attaques en tirant parti des accès pour déployer les ransomwares, en naviguant à travers les défenses des réseaux et en gérant la propagation dans les infrastructures des victimes.

- Les négociateurs professionnels mènent les négociations relatives aux rançons, en particulier dans les cas de grande valeur, afin d'optimiser le résultat en prenant le contrôle des données des victimes.

Chaque spécialiste se concentre sur le perfectionnement de ses compétences dans son domaine, permettant ainsi le développement de méthodes d'infiltration et d'exécution d'attaques plus avancées et plus furtives. Chaque rôle occupe une position unique dans le cycle d'attaque des ransomwares, contribuant ainsi à garantir que chaque attaque porte atteinte à la sécurité tout en s'alignant stratégiquement sur les objectifs globaux de ces entreprises illicites.

Collaboration entre cybercriminels

La collaboration sur le Dark Web et sur les canaux de communication chiffrés intensifie les attaques, apportant son lot d'outils, de techniques et d'informations critiques sur les vulnérabilités potentielles et les stratégies fructueuses. Les criminels favorisent une communauté d'apprentissage et de développement, qui encourage l'innovation dans la création de malwares plus furtifs et de campagnes de phishing plus ciblées.

Ces efforts accélèrent l'évolution des tactiques de ransomware, et les professionnels de la cybersécurité ont de plus en plus de mal à suivre le rythme. La nature collaborative de ces groupes exacerbe les failles de sécurité et accroît la nécessité de stratégies avancées d'atténuation des risques. Les défenseurs doivent adapter et peaufiner en permanence leurs stratégies et leurs technologies, ce qui pousse les forces de l'ordre et les agences de cybersécurité à développer des approches intégrées sophistiquées capables de rivaliser avec la coordination et la spécialisation des criminels.

La nature collaborative de ces groupes exacerbe les failles de sécurité et accroît la nécessité de stratégies avancées d'atténuation des risques.

Forces économiques motrices **de la cybercriminalité**

La cybercriminalité repose sur les mêmes principes économiques que ceux qui régissent les marchés légitimes (offre et demande, barrières à l'entrée, concurrence), mais il possède une dynamique propre. La demande en accès illégaux, en données et en exploits logiciels alimente l'offre en méthodes de cyberattaques de plus en plus sophistiquées. Avec l'essor d'outils tels que les RaaS, les barrières à l'entrée sont plus faibles que jamais, créant de fait une environnement hautement concurrentiel qui oblige les cybercriminels à innover constamment pour conserver leur avantage compétitif.

La cybercriminalité est principalement motivée par des raisons financières, car elle offre des marges de profit élevées et implique moins de risques que la criminalité traditionnelle. Les cybercriminels ont la possibilité d'agir de pratiquement n'importe où, ce qui réduit significativement pour eux le risque d'être appréhendés. Tout cela a conduit à la transformation de la cybercriminalité en opérations hautement organisées, basées sur des considérations économiques, dont la structure reflète celle des entreprises traditionnelles, mais qui se concentrent sur la maximisation des profits et la minimisation des risques.

L'impact économique considérable de la cybercriminalité coûte des milliards à l'économie mondiale et influence les politiques et réglementations internationales en matière de cybersécurité, ce qui nécessite des investissements substantiels dans les technologies défensives pour rester en conformité. Cette dimension internationale de la cybercriminalité présente également des défis complexes pour les systèmes juridiques, dans la mesure où une coopération internationale est essentielle pour répondre à ces menaces numériques en constante évolution.

Comparaison avec les marchés classiques

Le marché de la cybercriminalité reprend les structures des marchés légitimes. Il opère avec des hiérarchies et des spécialisations distinctes, mais sous couvert d'anonymat et en dehors du cadre de toute réglementation officielle. Ces milieux numériques intègrent des rôles semblables à ceux des entreprises traditionnelles : les opérateurs sont les DG, les affiliés sont les commerciaux ou agents de terrain, les codeurs et les testeurs sont les employés des départements de R&D. Contrairement aux marchés conventionnels, soumis à la transparence et à la supervision réglementaire, la cybercriminalité s'appuie sur le secret (facilité par des technologies telles que Tor et par les canaux de communication chiffrés) pour préserver l'anonymat.

Sur ces marchés clandestins, la confiance et l'anonymat sont cruciaux. Les cybercriminels utilisent les réseaux Tor et les cryptomonnaies pour effectuer leurs transactions sans révéler leur identité. Pour établir et maintenir la confiance au sein de ces environnements anonymes, ils recourent à des mécanismes similaires à ceux du e-commerce, tels que l'évaluation des fournisseurs, les retours clients et les services de séquestre qui conservent les fonds jusqu'à la finalisation des transactions. En dépit de l'absence de supervision officielle, cet environnement pseudo-réglementaire permet aux transactions de se dérouler avec un semblant de fiabilité.

Toutefois, cet anonymat pose d'importants problèmes aux forces de l'ordre et aux professionnels de la cybersécurité, en compliquant les efforts mis en œuvre pour retracer les activités illégales et perturber les opérations criminelles. Pour relever ces défis, il est nécessaire de bien comprendre la dynamique du marché et les outils spécialisés conçus pour percer l'anonymat qui protège ces réseaux criminels.

Avec l'essor d'outils tels que les RaaS, les barrières à l'entrée sont plus faibles que jamais, créant de fait une environnement hautement concurrentiel qui oblige les cybercriminels à innover constamment pour conserver leur avantage compétitif.

Modèles de partage des bénéfices et analogie de l'économie à la demande

Les RaaS recourent à un modèle de partage des bénéfices similaire à celui utilisé dans l'économie à la demande, où les revenus sont basés sur des tâches ponctuelles : les opérateurs et les affiliés partagent les recettes de chaque attaque. Cet arrangement incite les affiliés à lancer le plus grand nombre d'attaques possible, ce qui augmente leurs revenus et profitent aux opérateurs, qui reçoivent une partie de chaque rançon. Ce modèle reflète la flexibilité et l'évolutivité de l'économie à la demande, en permettant aux réseaux cybercriminels d'ajuster rapidement leurs stratégies et d'étendre leurs opérations sans investissements initiaux ni infrastructures fixes.

L'adoption d'un tel cadre d'économie à la demande dans le domaine de la cybercriminalité a changé la composition de la main-d'œuvre cybernétique. Cela a abaissé les barrières à l'entrée, permettant à toute personne, moyennant un investissement initial minimal, de participer à des activités cybercriminelles. Ces nouveaux venus peuvent progressivement endosser des rôles plus complexes, en commençant par des tâches simples, à mesure qu'ils acquièrent de l'expérience et gagnent la confiance du réseau. Ce modèle permet non seulement de diversifier le vivier de talents de ces entreprises illicites, mais il offre également la souplesse du télétravail, attirant un éventail plus large de participants et élargissant la portée et les capacités des réseaux cybercriminels.

Défis et **menaces**

Les professionnels de la sécurité n'ont pas la tâche facile quand il s'agit de faire face à la sophistication croissante des attaques. Les avancées techniques telles que l'intelligence artificielle (IA) et le Machine Learning créent une course à l'armement entre les cybercriminels d'une part, qui tirent parti de ces technologies à des fins malveillantes, et les défenseurs de la cybersécurité d'autre part, qui les utilisent pour renforcer les mesures de protection.

Les complexités juridiques et géopolitiques, exacerbées par des divergences juridictionnelles qui permettent aux cybercriminels d'exploiter des zones sûres, nuisent à la coopération internationale en matière de lutte contre la cybercriminalité. Les disparités en termes de ressources compliquent encore la situation, en rendant les petites organisations particulièrement vulnérables aux attaques de ransomwares, car elles manquent souvent de moyens pour se défendre convenablement.

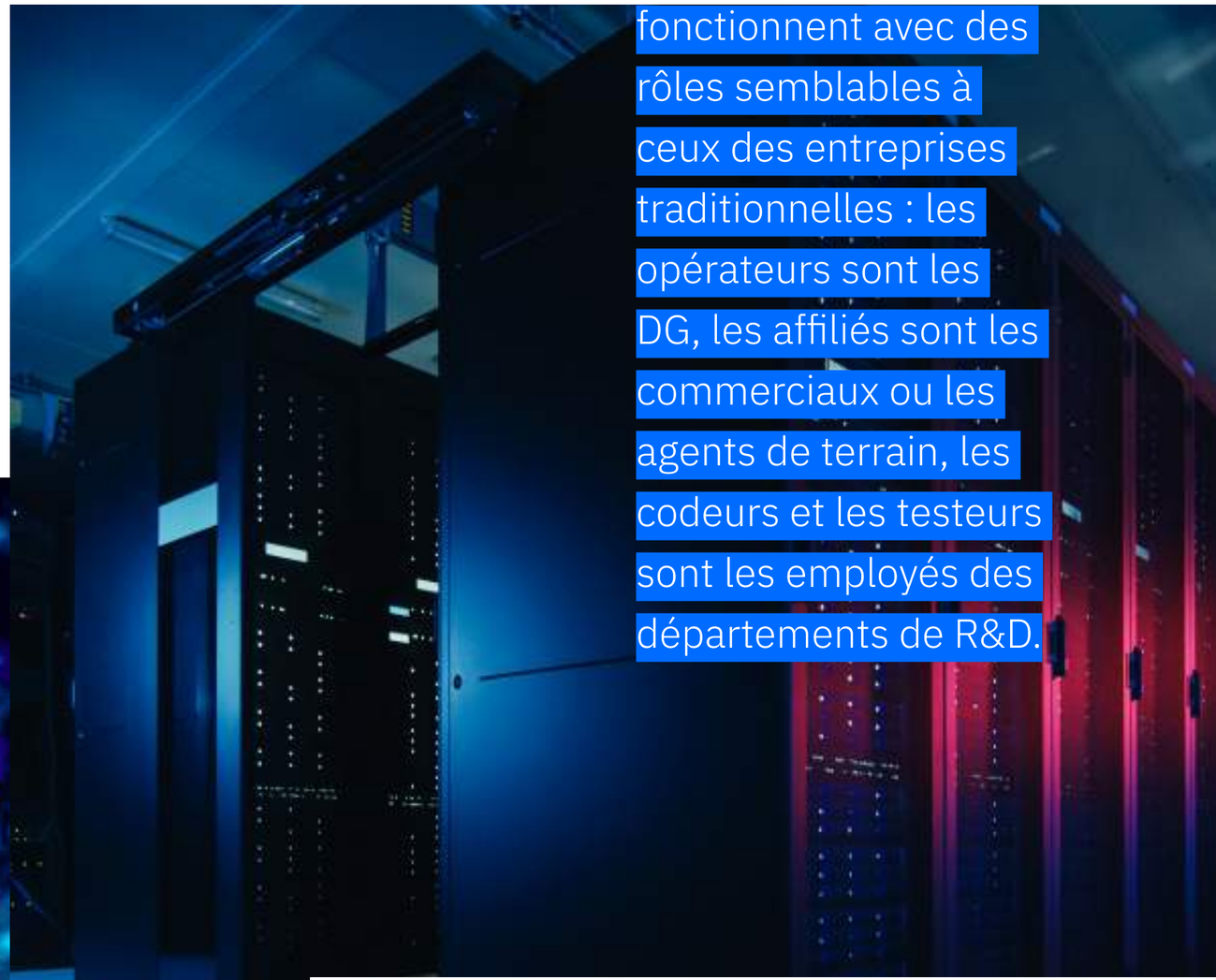
Sophistication et évolutivité croissantes des attaques

La sophistication et l'évolutivité des attaques de ransomwares ont considérablement évolué, mettant à mal les défenses cybersécuritaires. Ces attaques se déroulent généralement en plusieurs phases : infiltration initiale du réseau via du phishing ou de l'exploitation de vulnérabilités, puis mouvements latéraux pour explorer les systèmes et exploiter d'autres de leurs points faibles. Cette progression aboutit souvent au verrouillage ou à l'exfiltration des données, chaque phase étant méticuleusement conçue pour maximiser l'impact et échapper à la détection.

L'automatisation du déploiement des ransomwares à l'aide de scripts sophistiqués permet aux cybercriminels de cibler simultanément de multiples organisations, ce qui élargit considérablement le paysage et diminue grandement l'efficacité des mesures de sécurité. L'évolutivité des ransomwares complique les défis auxquels sont confrontées les petites entreprises qui essaient de maintenir une robuste posture de sécurité en dépit de ressources limitées et d'une pénurie de compétences. Ces opérations sont d'autant plus délétères qu'elles s'intègrent à d'autres cybercrimes tels que le vol de données et les attaques par déni de service distribué (DDoS), compliquant là aussi les stratégies de défense et amplifiant les dommages potentiels ; la nécessité de disposer de capacités avancées en matière de détection et de réponse se fait donc ressentir.

Dynamique de la confiance au sein des réseaux cybercriminels

La confiance est le principal obstacle auquel sont confrontés les cybercriminels en raison de la nature illicite de leurs activités. Les cybercriminels ont coopté des mécanismes de confiance issus de pratiques commerciales légitimes pour créer un sentiment de fiabilité au sein de leurs réseaux. La réputation joue un rôle crucial dans l'établissement de cette confiance. À l'instar des systèmes de commentaires sur les plateformes d'e-commerce légitimes, les marchés et les forums du darknet utilisent les scores de réputation pour évaluer les membres et garantir l'imputabilité, réduisant ainsi les risques de fraudes. De plus, les cybercriminels recourent à des services de séquestre dans le cadre des transactions, pour résoudre les problèmes de confiance entre parties qui ne se connaissent pas, en conservant les fonds ou les biens numériques de manière sécurisée jusqu'à ce que les conditions des transactions soient validées.



Ces milieux numériques fonctionnent avec des rôles semblables à ceux des entreprises traditionnelles : les opérateurs sont les DG, les affiliés sont les commerciaux ou les agents de terrain, les codeurs et les testeurs sont les employés des départements de R&D.

Malgré ces systèmes, les relations au sein des réseaux cybercriminels demeurent intrinsèquement instables, en raison des enjeux élevés et du contexte illégal. Au fil du temps, les cybercriminels peuvent former des alliances qui stabilisent les opérations et favorisent la loyauté, ce qui est essentiel à la coordination d'opérations complexes impliquant de nombreux spécialistes. Toutefois, le potentiel de trahison est élevé, avec des conflits internes, des trahisons et un risque d'exposition aux forces de l'ordre qui menacent l'intégrité de ces partenariats. Ces trahisons perturbent les opérations et peuvent conduire à l'arrestation et à la poursuite des parties impliquées.

Principales tendances **des** ransomwares

Alors que les ransomwares évoluent, plusieurs tendances se dégagent. Les attaques s'améliorent, exploitant de nouvelles technologies et plateformes pour trouver et exploiter des vulnérabilités. Les ransomwares ont ainsi été portés à la connaissance du grand public, conduisant à l'adoption de lois plus strictes en matière de protection des données et contraint les organisations à trouver un équilibre entre l'amélioration de leur cybersécurité et l'adhésion à des exigences de conformité en évolution, ajoutant ainsi une nouvelle couche de complexité à leurs opérations. Malgré cette prise de conscience, de nombreux utilisateurs sont encore très mal formés à la défense contre les malwares, ce qui augmente le risque de propagation involontaire du problème.

Exfiltration de données

Les cybercriminels recourent de plus en plus souvent à des techniques d'exfiltration de données pour copier et transférer des données sensibles avant leur chiffrement, ce qui renforce considérablement leur avantage sur les victimes et complique leurs processus de prise de décisions. Cette approche forme la base de la tactique de la double extorsion, au moyen de laquelle les attaquants demandent une rançon en échange du déchiffrement des données et menacent de rendre publiques les données volées si leurs demandes ne sont pas satisfaites. Cette tactique affecte particulièrement certains secteurs, tels que ceux de la santé et des services financiers, qui s'exposent à de grands risques juridiques et réputationnels en cas de compromission de données personnelles et/ou financières.

Les organisations mettent en œuvre des mesures de défense complètes pour contrer ces attaques, y compris des systèmes de détection avancés pour surveiller les mouvements de données inhabituels, une meilleure segmentation des données et de robustes programmes de formation des employés pour identifier et atténuer les menaces. La mise en place de plans de réponse immédiate aux incidents est essentielle, afin de garantir une récupération rapide et un minimum de dommages suite à de telles attaques.

La nature collaborative de ces groupes cybercriminels exacerbe les failles de sécurité et accroît la nécessité de stratégies avancées d'atténuation des risques.

Opérations manuelles de piratage

L'adoption croissante des techniques de piratage manuel renforce l'efficacité de ces cyber-assauts et aide les cybercriminels à contourner les défenses automatisées. Ces techniques sophistiquées permettent aux attaquants de naviguer dans des environnements réseau complexes, en choisissant soigneusement des points d'entrée et des chemins d'accès qui minimisent la détection et maximisent l'impact. Ces opérations requièrent de grandes compétences et une grande adaptabilité, ce qui place les opérateurs humains en première ligne pour orchestrer ces attaques tout en leur permettant d'échapper aux mesures de défense et d'exploiter les nouvelles vulnérabilités à mesure qu'elles sont découvertes au sein du réseau.

Ces opérations manuelles reprennent souvent les codes des activités réseau légitimes, ce qui les rend particulièrement difficiles à détecter. Les systèmes de sécurité automatisés traditionnels échouent parfois à identifier ces activités comme étant malveillantes, en raison de leur nature subtile et discrète, qui leur permet de se fondre dans les tâches ordinaires effectuées par les utilisateurs légitimes. Faute de personnel informatique spécialisé, ces attaques passeront inaperçues jusqu'à ce qu'il soit trop tard. Les plans de réponse proactive aux incidents, qui peuvent être déployés facilement, augmentent la résilience mais ne font qu'atténuer les dommages.

Vulnérabilités des dispositifs de réseaux périphériques

Les dispositifs de réseaux périphériques, en particulier ceux qui fonctionnent dans les zones démilitarisées (DMZ) tels que les appliances VPN, les logiciels d'accès à distance et les services de transfert de fichiers, élargissent considérablement la surface d'attaque accessible aux cybercriminels. Ces dispositifs, essentiels pour faciliter l'accès externe aux réseaux d'entreprise, posent des problèmes de sécurité considérables. Les vulnérabilités nouvellement découvertes dans ces dispositifs sont rapidement exploitées, ce qui permet de les cibler comme points d'accès initiaux pour les attaques de ransomwares, en raison de leur exposition à Internet et de l'accès critique qu'ils fournissent.

Si les appareils de l'Internet des objets (IoT), tels que les routeurs, les caméras de sécurité et les capteurs intelligents, sont intégrés aux réseaux d'entreprise pour en améliorer l'efficacité et renforcer leurs capacités de collecte des données, ils sont moins souvent utilisés comme vecteurs d'attaques directs dans le cadre des attaques de ransomwares.

Expansion de la chaîne d'approvisionnement

La complexité des chaînes d'approvisionnement mondiales élargit considérablement la surface d'attaque accessible aux cybercriminels, avec chaque couche de fournisseurs, de fabricants et de prestataires de services offrant des points d'entrée potentiels pour les attaques. Bien que les attaques à fort impact ciblant les chaînes d'approvisionnement en amont, telles que l'incident de SolarWinds, soient rares, elles montrent les conséquences sérieuses que peuvent avoir de telles violations, qui perturbent les opérations et sapent la confiance dans des outils largement utilisés.

Toutefois, une menace plus fréquente et souvent négligée, présente au niveau des chaînes d'approvisionnement, est celle desattaques BEC (compromission des e-mails professionnels) et attaques similaires, dans le cadre desquelles des cybercriminels se font passer pour des dirigeants d'entreprise ou des partenaires de confiance afin d'envoyer des liens malveillants ou des requêtes frauduleuses. Ces attaques quotidiennes peuvent affecter des entreprises de toutes tailles, entraînant d'importantes pertes financières et compromettant les opérations des entreprises.

En réponse à ces diverses menaces, les organisations mettent davantage l'accent sur la sécurité de la chaîne d'approvisionnement, en faisant appel à des tiers pour procéder à des évaluations complètes des risques et en recourant à des protocoles de communication sécurisés pour vérifier et sécuriser les différents composants. Former les employés pour qu'ils reconnaissent les signes de fraudes BEC et autres types de fraudes basées sur les e-mails et y réagissent de manière appropriée permet d'atténuer les risques plus larges associés aux attaques ciblant les chaînes d'approvisionnement.

Chez Bitdefender, nous sommes convaincus qu'une bonne compréhension du comportement des attaquants permet de mettre en place les défenses les plus efficaces possible.

Avec les nombreuses phases et approches qu'ils impliquent, les ransomwares représentent un problème complexe. Malheureusement, il n'existe pas de solution unique.

La seule défense efficace contre les attaques modernes de ransomwares consiste à mettre en œuvre une stratégie de défense multicouche approfondie, avec des contrôles de sécurité efficaces en matière de prévention, de protection, de détection et de réponse. Bitdefender propose aux entreprises de toutes tailles une gamme complète de produits et services permettant de répondre au problème des ransomwares.

Bitdefender® Global Leader In Cybersecurity

Siège en Roumanie
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T : +40 21 4412452
F : +40 21 4412453

Siège aux États-Unis
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com/fr-fr/

Trusted.Always.

Bitdefender est un leader mondial de cybersécurité qui fournit des solutions de pointe en matière de prévention, de détection et de réponse aux menaces. Protégeant des millions d'environnements de particuliers, d'entreprises et de gouvernements, Bitdefender compte parmi les experts les plus fiables de l'industrie pour l'élimination des menaces, la protection de la vie privée et des données, et la cyber résilience. Grâce à des investissements importants dans la recherche et le développement, les Bitdefender Labs découvrent plus de 400 nouvelles menaces chaque minute et répondent à environ 40 milliards de requêtes de menaces par jour. La société a été la première à innover dans le domaine des malwares, de la sécurité de l'IoT, de l'analyse comportementale et de l'intelligence artificielle. Sa technologie est utilisée sous licence par plus de 150 éditeurs parmi les plus reconnus au monde. Fondée en 2001, Bitdefender a des clients dans 170 pays et possède des bureaux dans le monde entier.