MANDIANT

PRÉSENTATION DE SOLUTION

COMBATTRE LES RANSOMWARES

Double extorsion : déjouez les plans des attaquants

Qui dit double extorsion dit double peine pour les entreprises qui, en plus d'un ransomware destructeur, doivent subir le préjudice d'une compromission de données. Réputation écornée, amendes pour infraction à la réglementation, recours collectifs en justice, coup d'arrêt aux projets de transformation digitale… les conséquences d'une compromission de données sont aujourd'hui bien plus graves qu'en 2019, année pivot où le ransomware a basculé dans la double extorsion.[1]

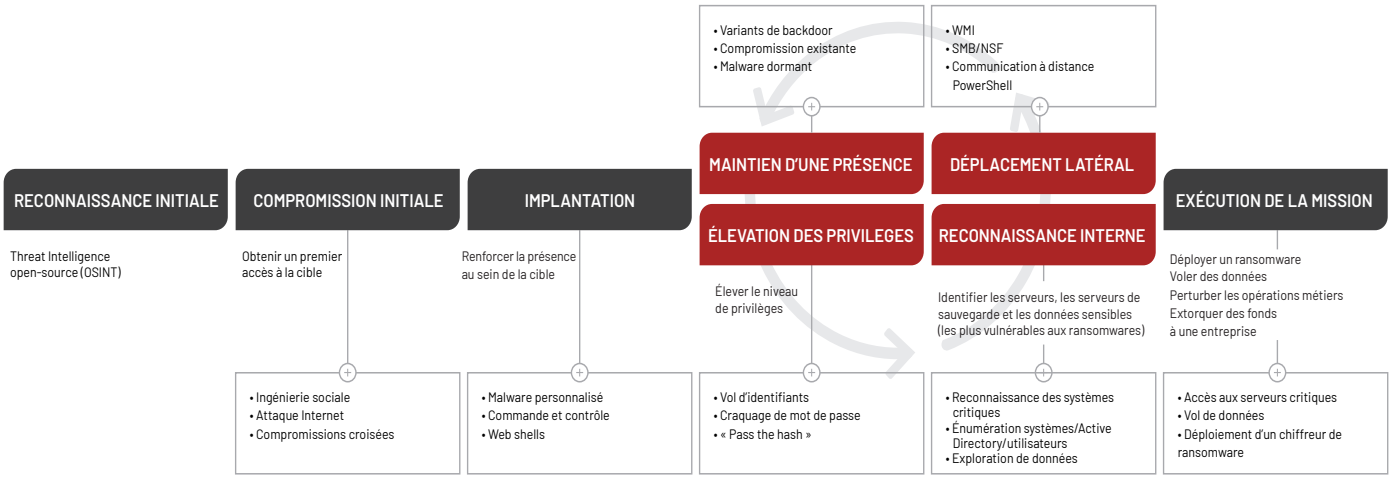
Pour les entreprises de toutes tailles et de tous horizons, le ransomware et les attaques par double extorsion représentent les plus grandes menaces cyber auxquelles elles sont confrontées. Paralysie d'infrastructures critiques, mise en danger de la santé et de la sécurité publiques, détournement de ressources publiques d'importance vitale, perturbation des établissements d'enseignement, compromission de la confidentialité des données… les auteurs d'attaques par ransomware ne reculent devant rien. Le temps moyen d'interruption après une attaque par ransomware est de 21 jours.[2]

De plus en plus agressifs, les acteurs du ransomware transforment ces attaques relativement simples autrefois en opérations d'extorsion multifacette plus sophistiquées – et plus lucratives. Vol de données, chiffrement par ransomware, humiliation publique (name-and-shame)… la double extorsion se caractérise par de multiples points d'attaques qui présentent des risques bien plus sérieux pour les entreprises.

En mars 2021, l'une des plus grandes compagnies d'assurance des États-Unis déclarait avoir versé une rançon de 40 millions $,[3] soit la somme la plus élevée à ce jour.

1 FireEye (2021). M-Trends 2021.
2 Coveware (1er février 2021). « Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands. »
3 Business Insider (22 mai 2021). « One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack. »

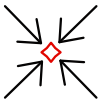
Anatomie d'une attaque ciblée par ransomware



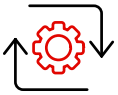
Défense anti-ransomware : les objectifs

Lorsqu'un ransomware parvient à se propager, les entreprises subissent des dommages techniques et autres qui paralysent leurs opérations. Elles se heurtent bien souvent à deux problématiques : le manque de visibilité sur l'efficacité des contrôles et des systèmes de détection d'une part, et la sophistication des outils et modes opératoires des cybercriminels d'autre part. D'où l'importance d'une stratégie complète de réduction des risques qui s'étend du CA jusqu'aux équipes de sécurité.

Bloquez une attaque avant le déploiement d'un ransomware



Accélérez vos temps de réponse pour **réduire l'impact** d'une attaque



Reprenez vos activités le plus rapidement possible

Dans l'idéal, les entreprises devraient pouvoir bloquer les ransomwares en amont et cerner leurs capacités à en éviter la propagation dans leurs systèmes.

La solution Mandiant

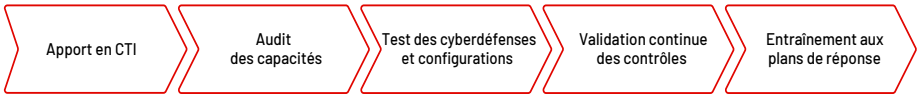
De nombreuses entreprises victimes de ransomware ont fait appel à Mandiant pour les aider dans leur réponse. Fort d'une expérience de terrain sur des centaines d'attaques par ransomware, Mandiant a acquis une expertise et une CTI de pointe qui lui permettent d'identifier les attaquants et de révéler leurs modes opératoires pour mieux les contrer.

Seul Mandiant possède les capacités pour déceler rapidement et à grande échelle les signes avant-coureurs d'un déploiement de ransomware. Grâce à nos solutions automatisées et à nos services complets, votre entreprise peut se préparer, prévenir et répondre aux attaques par ransomware et double extorsion. Les solutions Mandiant renforcent votre degré de préparation et vos cyberdéfenses pour vous aider à neutraliser ces menaces.

Préparation

Threat Intelligence, exercices pratiques, validation des contrôles, évaluation de vos programmes de sécurité… grâce à l'expertise de terrain de Mandiant, vous avez toutes les cartes en main pour renforcer vos systèmes de défense face aux ransomwares et à la double extorsion.

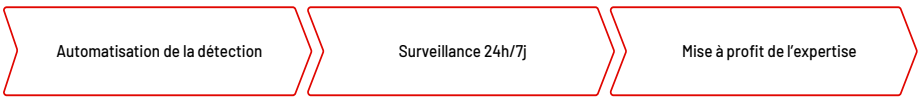
La plateforme et les services Mandiant Advantage vous permettent de préparer votre environnement en accédant directement à une CTI pertinente et actionnable pour accélérer vos prises de décision et réduire les risques. Nos programmes de tests automatisés vous apportent des données concrètes sur l'efficacité de vos contrôles de sécurité. Vous obtenez ainsi une meilleure visibilité sur vos systèmes de défense et sur votre capacité à lutter contre les ransomwares. Pour préparer votre équipe à prévenir ou réduire l'impact d'un ransomware, misez sur la visibilité inégalée, la CTI de pointe et l'expertise innovante de Mandiant.



Prévention

Décelez les signaux faibles d'un déploiement de ransomware et activez les stratégies de prévention appropriées pour contrer l'attaque avant que la situation ne devienne irrémédiable.

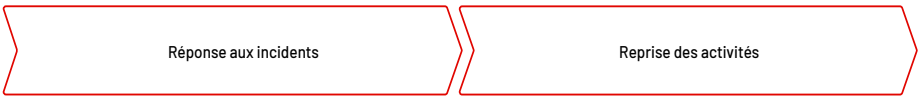
Les outils Mandiant Advantage évaluent vos capacités de défense et vous donnent accès à toute l'expertise de terrain Mandiant. Vos équipes de sécurité peuvent ainsi détecter en un instant les compromissions actives et passives pour mieux prendre les cyberattaquants de vitesse. Premières informées, premières à agir. Vos équipes peuvent compter sur des modules automatisés qui identifient les principaux indicateurs de compromission (IOC) et les aident à prendre l'ascendant sur leurs adversaires. Nos services managés de détection et de réponse (MDR) leur permettent de bénéficier de toute l'expertise Mandiant, y compris de nos recherches approfondies sur les acteurs cyber, afin de repérer plus rapidement les activités malveillantes et de prioriser plus efficacement les mesures de réduction des risques.



Réponse

Agissez vite et de façon décisive afin de limiter l'impact des ransomwares et des attaques par double extorsion sur vos activités.

Pour neutraliser efficacement les attaques par ransomware ou double extorsion, faites appel aux experts de la réponse aux incidents Mandiant. Leur mission ? Décortiquer l'offensive et déclencher des stratégies de gestion de crise sur tout le cycle d'attaque pour vous aider à revenir rapidement à la normale.



AVANTAGES

- Accès à la CTI de terrain la plus récente pour cerner l'identité, les cibles, la chronologie, les motifs et les méthodes des acteurs cyber du moment
- Priorisation et focalisation de votre action sur les menaces ciblant spécifiquement votre entreprise et secteur, tests de vos contrôles de sécurité et correction des vulnérabilités
- Réduction des temps de réponse et de l'impact des incidents
- Test sécurisé de l'efficacité de vos cyberdéfenses face à des scénarios de ransomware réels pour détecter les erreurs de configuration existantes et renforcer votre posture de sécurité

Offre

TABLEAU 1. Offre.

Solution	Description	Service
Préparation		
Threat Intelligence Mandiant Advantage	Obtenez des informations sur les dernières menaces observées sur le terrain.	Mandiant Advantage
Ransomware Defense Assessment	Évaluez votre capacité à prévenir, détecter, contenir et neutraliser un ransomware en mesurant l'impact d'une attaque potentielle sur votre réseau interne.	Mandiant Consulting Services
Bilan de sécurité Active Directory	Identifiez les erreurs de configuration, les faiblesses des processus et les failles exploitables d'Active Directory – le service réseau le plus exploité par les attaquants pour élever leurs privilèges lors d'une attaque de ransomware ou de double extorsion.	Mandiant Consulting Services
Red Team for Ransomware	Testez vos capacités à protéger vos ressources les plus précieuses à partir de scénarios d'attaques réalistes. Les experts Mandiant reproduisent les modes opératoires observés lors d'incidents de ransomwares réels pour identifier les points faibles et recommander des améliorations concrètes.	Mandiant Consulting Services
Mandiant Advantage Ransomware Defense Validation	Testez continuellement et sans aucun risque les contrôles de sécurité de votre environnement de production pour évaluer leur efficacité face aux derniers ransomwares. Vous pourrez ainsi déterminer la capacité – ou l'incapacité – de vos contrôles de sécurité à prévenir les tentatives de chiffrement par ransomware de vos machines.	Mandiant Advantage
Exercices de simulation pour les équipes techniques et dirigeantes	Réalisez des exercices de mise en situation pour évaluer votre plan de réponse aux ransomwares. Mandiant identifie les écarts entre les plans documentés d'une part, et les situations du monde réel d'autre part.	Mandiant Consulting Services
Prévention		
Mandiant Advantage Automated Defense	Accédez à l'expertise Mandiant automatisée pour identifier rapidement les indicateurs de compromission (IOC) provenant de ransomwares actifs et ciblés dans votre environnement. Réduisez la durée de présence des cyberattaquants et limitez l'impact d'une attaque grâce à la rapidité, la puissance et la cohérence du machine learning.	Mandiant Advantage
Mandiant Advantage Managed Defense	Faites appel aux experts Managed Defense 24h/7j pour réduire les risques des cybermenaces et protéger votre entreprise contre l'extorsion, les rançons, les interruptions de service et le vol de données.	Mandiant Managed Services
Expertise On Demand	Initiez des missions d'investigation en un seul clic et à tout moment pour jauger les menaces de ransomware. Nos spécialistes vous apportent des explications simples et claires, étayées par une Threat Intelligence collective et l'expertise de Mandiant.	Mandiant Consulting Services
Réponse		
Service de réponse aux incidents	Consultez nos experts de la réponse aux incidents pour décortiquer l'offensive et déclencher des protocoles de gestion de crise sur tout le cycle d'attaque de manière à revenir rapidement à la normale.	Mandiant Consulting Services
Astreinte permanente pour la réponse aux incidents	Pour une réponse aux incidents plus rapide et plus efficace, faites appel aux experts Mandiant dans le cadre d'un contrat d'astreinte avec garantie d'intervention sous deux heures.	Mandiant Consulting Services

Conclusion

Mandiant vous aide à affronter les défis des ransomwares et à limiter voire à réduire drastiquement l'impact global de ce type d'attaque. Une fois que les ressources exposées de votre environnement ont été identifiées, vous pourrez mettre en évidence vos faiblesses techniques et opérationnelles pour engager des mesures de renforcement de vos stratégies et tactiques de défense.

Pour en savoir plus, rendez-vous sur **www.mandiant.fr/solutions/ransomware**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
+1 (703) 935-8012
833.3MANDIANT (362.6342)
info@mandiant.com

À propos de Mandiant

Depuis 2004, Mandiant® s'impose comme le partenaire de confiance des entreprises soucieuses de leur sécurité. Aujourd'hui, l'expertise et la Threat Intelligence leader de Mandiant sous-tendent des solutions dynamiques qui aident les organisations à développer des programmes plus efficaces et à instaurer une plus grande confiance dans leurs cyberdéfenses.

MANDIANT