MANDIANT
NOW PART OF Google Cloud

Guide pratique des équipes de sécurité (numéro 3)

Fruit des observations faites par Mandiant sur le terrain, notre Guide pratique des équipes de sécurité vous éclaire sur des questions de cyberdéfense toujours plus capitales.
Au sommaire de ce nouveau numéro :

Transition vers l'authentification sans mot de passe

Auparavant, l'authentification défi/réponse basée sur un seul mot de passe constituait le principal moyen employé par les entreprises pour confirmer l'identité d'un utilisateur. Toutefois, cette transaction unique sans autre vérification pouvait entraîner des risques non négligeables pour ces organisations.

À mesure que les attaquants ont peaufiné leurs tactiques de compromission des identités, de nouveaux contrôles et de nouvelles méthodes ont permis de réduire ces risques. Ainsi, de nombreuses entreprises ont adopté l'authentification multifacteur (MFA), qui consiste à allier deux méthodes distinctes, voire plus, pour vérifier une identité.

Si les méthodes MFA traditionnelles se sont généralisées, les attaquants ne cessent de leur côté de perfectionner leurs techniques de compromission des identités, comme en témoignent les observations faites par Mandiant dans le cadre de multiples investigations de réponse aux incidents :

Contournement de l'authentification multifacteur

Détournement des méthodes MFA plus faibles (p. ex., SMS, notifications push, appels téléphoniques)

Enregistrement d'appareils contrôlés par les attaquants pour un accès via MFA

Cette intensification de la menace a favorisé l'adoption de nouveaux outils employant des méthodes MFA plus fortes comme les codes à usage unique (OTP), les notifications télémétriques contextuelles et les mots de passe à usage unique basés sur le temps (TOTP). En outre, afin de renforcer encore davantage les méthodes MFA, fournisseurs et entreprises ont recours aux clés/jetons FIDO2 (Fast Identity Online 2), aux jetons logiciels/matériels OATH (Open Authentication) ou aux certificats d'authentification.

Authentificateurs

Pour améliorer toujours plus la sécurité, les entreprises ont intégré un nouveau concept à leurs pratiques de gestion des identités et des accès : celui des « authentificateurs ». À mille lieues du contexte unique des mots de passe, ces authentificateurs s'appuient sur plusieurs éléments pour confirmer une identité. Par exemple, ils pourront associer le tandem nom d'utilisateur/mot de passe à des méthodes MFA fortes, des certificats, des données sur l'état de l'appareil, un calcul de risque, ou encore des méthodes sans mot de passe.

Ainsi, ce concept permet de réduire considérablement le risque de compromission de mot de passe, car ce dernier ne constitue plus la seule ligne de défense du processus d'authentification.

Qu'est-ce que l'authentification sans mot de passe ?

Dans la droite ligne des méthodes MFA fortes, l'authentification sans mot de passe s'impose peu à peu dans de nombreuses entreprises. Il s'agit essentiellement de vérifier une identité sans exiger un secret connu de l'utilisateur. À la place, cette méthode repose sur quelque chose que l'utilisateur possède (appareil) ou l'une de ses caractéristiques propres (biométrie), éliminant du processus d'authentification le recours à une information connue (mot de passe).

Il existe plusieurs méthodes pratiques et évolutives pour implémenter l'authentification sans mot de passe :

- **Applications mobiles d'authentification** – Elles peuvent soit générer un code à usage unique (OTP) (basé sur un algorithme synchrone), soit servir à approuver ou faire correspondre une suite de chiffres visible pour l'utilisateur.
- **Clés et jetons matériels FIDO2** – Ils peuvent interagir avec un appareil via une connexion physique, par Bluetooth ou par NFC (communications en champ proche). Dans le cas de la méthode FIDO2 WebAuthn, le jeton matériel associé à l'appareil peut servir à authentifier l'utilisateur auprès d'une application cible à l'aide d'une paire unique de clés cryptographiques (stockée dans l'authentificateur itinérant) et de la cryptographie à clés publiques. FIDO2 WebAuthn permet d'utiliser efficacement l'authentification sans mot de passe pour lutter contre le phishing, l'usurpation d'identité et les attaques par interception.
- **Clés d'accès** – Comme avec le jeton FIDO2, une paire de clés cryptographiques, générée et stockée sur un appareil mobile, s'échange à l'aide de la cryptographie à clés publiques afin d'authentifier un utilisateur auprès d'une application (qui détient la clé publique). Pour accéder à une clé d'accès configurée, cet utilisateur devra passer par une identification biométrique, taper un code PIN ou tracer un schéma de déverrouillage (fréquent sur les appareils mobiles courants).
- **Certificats numériques** – Basés sur une paire de clés, l'une publique et l'autre privée, ils permettent de générer une signature numérique valable en réponse à une demande d'authentification. Sur les appareils d'aujourd'hui, le module de plateforme de confiance (TPM) peut faire office d'authentificateur interne pour le stockage de la clé cryptographique privée qui sert à signer un certificat dont la validation dépendra de la clé publique correspondante.

- **Biométrie** – Il s'agit là d'utiliser les caractéristiques physiques uniques d'un utilisateur humain pour confirmer son identité. Le plus souvent, l'authentification biométrique repose sur les empreintes digitales (Touch ID, Fingerprint Unlock, etc.) et sur la reconnaissance faciale (Face ID, Face Unlock, etc.) – des méthodes intégrées à de nombreux smartphones, appareils mobiles et ordinateurs portables récents.

Planifier l'adoption de l'authentification sans mot de passe

Les applications et infrastructures traditionnelles, incompatibles avec les méthodes d'authentification plus fortes, peuvent freiner les entreprises désireuses d'intégrer les authentificateurs. Ainsi, plutôt que de vouloir à tout prix appliquer ce concept à chaque application, ces organisations utilisent généralement une solution tierce d'authentification unique (SSO) en front-end, qui délègue ensuite le contrôle des accès à d'autres applications en back-end.

L'adoption des méthodes sans mot de passe comme authentificateur ne se fait pas en un jour. Vous devez d'abord :

Identifier…

- Les technologies et plateformes existantes qui font office de plateformes et de magasins d'identités de référence.
- Les magasins d'identité existants qui prennent en charge l'authentification sans mot de passe en natif – ou qui nécessiteront une intégration et des intermédiaires tiers.
- Les identités existantes au sein de l'entreprise, y compris les types d'identités qui pourraient servir à tester et valider l'expérience sans mot de passe.
- Les mécanismes de compensation et de détection améliorée des types d'identités qui s'avèrent incompatibles avec les méthodes d'authentification forte ou sans mot de passe (p. ex., comptes de service/programme).
- L'impact pour les utilisateurs tiers/invités potentiellement incompatibles avec l'intégration des méthodes sans mot de passe.
- Les appareils auxquels les utilisateurs ont recours pour l'authentification et les accès (afin de déterminer s'ils prennent en charge l'authentification sans mot de passe).
- Les applications directement compatibles avec les méthodes sans mot de passe et celles qui prennent en charge l'intégration de la SSO à une plateforme tierce elle-même compatible avec ces méthodes.

Planifier…

- L'achat et l'intégration sécurisée des appareils qui prendront en charge l'authentification sans mot de passe.
- La formation des utilisateurs à l'expérience sans mot de passe.
- Les modifications de configuration des appareils et des magasins d'identités nécessaires pour intégrer les méthodes sans mot de passe.
- Les tests et la validation de cette intégration à l'aide d'utilisateurs pilotes et d'une sélection d'applications.
- Le premier déploiement et l'intégration initiale, ainsi que la généralisation des méthodes sans mot de passe dans toute l'entreprise.

Il est également important d'adapter les étapes de récupération en cas de perte ou de vol d'une clé ou d'un appareil puisque ces derniers s'avèrent indispensables pour authentifier une identité à l'aide de ces méthodes. Pour élaborer un processus de récupération sécurisé, vous devez évaluer non seulement les risques pour l'entreprise, mais aussi les avantages et les inconvénients de l'enregistrement des utilisateurs et de leur expérience en self-service.

Si les authentificateurs internes (les appareils avec un TPM intégré, par exemple) permettent d'exporter (stocker) ou de synchroniser les clés privées entre différents équipements, ils peuvent également représenter un risque en cas de mauvaise sécurisation ou de stockage inadapté des clés. Lorsque vous utilisez des fournisseurs d'identités (IdP) tiers, vous pouvez également reconstituer une identité sans mot de passe sur un nouvel appareil à l'aide d'expressions et de clés de récupération. Dans le cas d'authentificateurs itinérants, il est possible de récupérer une identité par le biais de messages de validation envoyés à un appareil mobile ou une adresse e-mail.

Abandonner les mots de passe uniques au profit d'une méthode d'authentification sans mot de passe n'est pas une mince affaire. Pour de nombreuses entreprises qui ont adopté le concept des authentificateurs, l'implémentation de ces méthodes passe impérativement par la MFA forte. Planification, exécution et validation… une telle transition ne s'improvise pas. Mais elle s'accompagne d'une réduction des risques et d'une protection renforcée. Il s'agit là de deux avantages inestimables à l'heure où l'hybridation des modèles opérationnels propulse les identités au rang de nouveau périmètre de sécurité.

Réduction des risques pour souscrire un contrat de cyberassurance

Aux États-Unis, les banques ont identifié 1,2 milliard $ de transactions liées aux ransomwares sur un total de 1 489 rapports remis aux régulateurs en 2021. C'est beaucoup plus que les 416 millions $ des 487 signalements de l'année précédente[4].

Entre 2020 et 2021, le montant des rançons versées par les victimes de ransomware a plus que doublé[1]. Les cyberassureurs ont alors essuyé des pertes plus importantes, avec pour conséquence la volatilité de leur marché qui commence tout juste à se stabiliser. Certes, à la fin de l'année 2022, la hausse des primes de cyberassurance affichait un ralentissement de 80 %, de bon augure pour 2023[2]. Mais la plupart des compagnies du secteur tablent encore et toujours sur des cyber-risques accrus puisque les ransomwares continuent de dominer le champ des menaces[3]. Ainsi, lors de la souscription d'un contrat de cyberassurance, les entreprises peuvent s'attendre à une vérification toujours plus minutieuse de leurs contrôles de sécurité et de leurs processus et procédures internes. En outre, certaines exclusions de garantie préoccupantes subsistent, à savoir celles qui concernent des menaces répandues (comme Log4j) et des incidents associés à la guerre en Ukraine ou attribuables à des groupes d'attaque à la solde d'États. De fait, les compagnies de cyberassurance continuent de réduire voire de supprimer de leurs polices les attaques par ransomware lorsqu'elles jugent que les entreprises assurées n'ont pas déployé des moyens adaptés pour gérer ce type de risque.

Ces 12 derniers mois, Mandiant a constaté que les cyberassureurs s'impliquaient davantage lors de ses missions de réponse aux incidents. Bien que les RSSI n'aient pas toujours leur mot à dire en la matière, nous leur recommandons de collaborer avec le directeur juridique et le responsable risque de leur entreprise afin de veiller à la rigueur du processus de souscription, et d'examiner les polices de cyberassurance pour éviter les mauvaises surprises en cas de compromission.

Les bases de la cyberassurance

Au milieu des années 2000, les compagnies d'assurance ont élargi leur offre pour indemniser les entreprises victimes de cyberattaques à hauteur des coûts encourus[5]. Depuis, cette couverture étendue permet aux responsables des risques financiers et de la cybersécurité de réduire les risques et de compenser les coûts des compromissions et autres incidents de sécurité. En règle générale, les polices de cyberassurance couvrent les risques pour l'entreprise (risques internes) et ceux qui planent sur des tiers (responsabilité civile). Auparavant, le processus de souscription se concentrait sur les coûts associés aux compromissions de données. Ainsi, les entreprises devaient fournir des renseignements sur les types d'enregistrement, les données clients et les données règlementées qu'elles traitaient, mais aussi certifier leur conformité règlementaire (RGPD, HIPAA, PCI DSS, etc.). Seulement voilà, les ransomwares et la double extorsion génèrent des risques supplémentaires d'interruption de service, potentiellement coûteux et néfastes pour l'activité.

1. Wall Street Journal, Reported Ransomware Incidents, Cost Soared in 2021, Treasury Says, 4 novembre 2022
2. Marsh, US Cyber Insurance Market Update Signs of improvement in third quarter of 2022, 7 octobre 2022
3. Woodruf Sawyer, 2023 Property & Casualty Looking Ahead Guide, 10 janvier 2023
4. Wall Street Journal, Reported Ransomware Incidents, Cost Soared in 2021, Treasury Says, 4 novembre 2022
5. Banque de la réserve fédérale de Chicago, Chicago Fed Letter, No. 426, The Growth and Challenges of Cyber Insurance, 2019

TABLEAU 1. Couverture des cyber-risques courants

Risques internes	Responsabilité civile
Coûts de la réponse aux incidents et de l'analyse forensique	Sécurité et confidentialité des données des tiers
Notification, suivi des usurpations d'identité et fraudes bancaires	Responsabilité pour les communications médias/ multimédias
Récupération des données	Assistance juridique et sanctions règlementaires
Interruption de service	Infraction PCI DSS
Cyberextorsion et cybercriminalité	Assistance juridique en cas de violation des lois sur le télémarketing
Atteinte à la réputation	

*Source : Honigman LLP Attorneys and Counselors, Cyber Insurance 101, 19 mai 2021

C'est pourquoi les compagnies de cyberassurance accordent désormais une plus grande attention aux contrôles techniques d'une entreprise et aux moyens qu'elle met en œuvre pour réduire le risque d'interruption et de pertes financières. Ainsi, elles suivent un processus de souscription plus rigoureux afin de déterminer les risques en présence et le montant de la prime d'assurance. Aujourd'hui, les entreprises assurées doivent répondre à des questions supplémentaires, passer des entretiens et se soumettre à une analyse externe de leur environnement.

À la tête du pôle cybersécurité et confidentialité des données du cabinet d'avocats Woods Rogers, Beth Burgin Waller consacre beaucoup de temps à l'examen et à la négociation des polices de cyberassurance de ses clients, quand elle ne leur prodigue pas des conseils juridiques pour la réponse aux incidents. À ce titre, elle leur recommande de préparer le processus de souscription en collaboration avec le département juridique et l'équipe de gestion des risques.

Souvent, les questionnaires des cyberassureurs s'appliquent mal aux infrastructures complexes, multiréseaux et multiclouds d'aujourd'hui. Par exemple, en plus de demander si vous utilisez l'authentification multifacteur (MFA) dans toute votre entreprise, la compagnie pourra exiger des preuves de cette implémentation, des sauvegardes aux applications cloud, en passant par les VPN. À cet égard, votre département juridique et votre équipe de gestion des risques pourront vous mettre en garde en cas de déclarations trop catégoriques et vous aider à compléter vos réponses pour fournir des informations claires sur les contrôles en place et les projets d'amélioration.

Cerner les nuances des couvertures IR

Beth Burgin Waller recommande vivement d'étudier le spécimen (modèle) de contrat. « À l'heure où le marché se stabilise, la terminologie de la cyberassurance se standardise, comme celle des autres polices d'assurance », explique-t-elle. Ce modèle limite peut-être la couverture des interruptions de service. Pire encore, si vous ne l'examinez pas, vous passerez peut-être à côté d'exclusions concernant les logiciels d'ancienne génération, les menaces répandues comme Log4j, ou encore les actes de guerre – qui, ajoutés tout récemment, écartent les incidents attribués aux groupes d'attaque à la solde des États. L'avocate suggère également de se pencher sur les plafonds fixés dans la police de cyberassurance. Certains contrats de base prévoient un plafond pour les incidents liés au phishing et requièrent des entreprises qu'elles souscrivent une couverture supplémentaire pour les cas de ransomwares. « En lisant attentivement le spécimen de votre police en amont, vous pouvez cerner l'étendue de votre couverture avant qu'un incident survienne et ainsi vous épargner un véritable un casse-tête », insiste Beth Burgin Waller.

Mais qu'en est-il de la couverture des prestataires de réponse aux incidents et des coûts associés ? Dans ce domaine, l'équipe IR de Mandiant distingue trois scénarios courants :

1) Le prestataire IR est un fournisseur approuvé avec des tarifs négociés à l'avance, ce qui facilite le lancement de la mission et simplifie la déclaration de sinistre pour le client.

2) Le prestataire IR n'est pas préapprouvé et l'assureur limite la prise en charge à un montant horaire bien précis. Si le tarif du prestataire est supérieur à cette prise en charge, le client devra alors payer la différence.

3) Le prestataire IR n'est pas préapprouvé et l'assureur ne couvrira pas le coût de sa mission. Ce scénario reste le plus problématique en cas de compromission.

En somme, il est important d'étudier le modèle de police de cyberassurance pour veiller à une couverture complète du processus de réponse aux incidents. Certains contrats ne prennent en charge que l'investigation et excluent le paiement des rançons, les frais d'assistance juridique, ou encore les coûts associés à la reprise d'activité et aux efforts de remédiation sur le long terme. En outre, certaines compagnies d'assurance refusent de couvrir une investigation complète, nécessaire pour identifier le point d'entrée des attaquants et pour vérifier l'absence de backdoors qui exposeraient le client à une réinfection. Il revient alors à l'entreprise d'opter ou non pour cette investigation approfondie afin de réduire les risques à l'avenir.

Une nouvelle approche

Globalement, le marché de la cyberassurance gagne en maturité. De fait, les compagnies travaillent main dans la main avec leurs clients pour renforcer leur cyberrésilience. Le secteur de l'assurance s'appuie sur des programmes de modélisation des risques ultrasophistiqués afin d'améliorer la sécurité des entreprises.

De nombreux assureurs élaborent également des listes de fournisseurs et de solutions approuvés par leurs équipes. L'objectif : aider leurs clients à s'y retrouver sur le marché de la cybersécurité et à réduire les risques grâce à des technologies à l'efficacité éprouvée.

Les compagnies d'assurance ont même identifié des contrôles de sécurité bénéfiques pour le niveau de risque des entreprises et les coûts de cyberassurance associés[6]. De son côté, Mandiant intègre les recommandations de ce secteur et distingue les cinq pratiques suivantes qui, implémentées correctement, peuvent prévenir les attaques courantes ou au moins en réduire l'impact :

1. **Authentification multifacteur :** la MFA, ou l'authentification à deux facteurs, allie au moins deux informations d'identification différentes (mot de passe, jeton de sécurité, empreintes digitales, reconnaissance faciale, etc.) pour authentifier un utilisateur et lui octroyer l'accès. Or, si les méthodes MFA traditionnelles se sont généralisées, les attaquants ne cessent de leur côté de perfectionner leurs techniques de compromission des identités, comme en témoignent les observations faites par Mandiant dans le cadre de multiples investigations de réponse aux incidents. L'implémentation d'outils et de méthodes d'authentification multifacteur forte (codes à usage unique, notifications télémétriques contextuelles, mots de passe à usage unique basés sur le temps, etc.) sur tous les portails de connexion externe et toutes les applications internes sensibles peut réduire les risques liés aux vecteurs courants d'accès initial.
2. **Gestion des identités et comptes privilégiés :** à l'heure de l'hybridation des modèles opérationnels, les identités constituent le nouveau périmètre de sécurité. À cet égard, Mandiant identifie souvent des compromissions de systèmes de gestion des annuaires et des accès lors de ses missions de réponse aux incidents. C'est parce que les attaquants utilisent régulièrement ces systèmes pour élever leurs privilèges. Pour les en empêcher, les entreprises doivent veiller à octroyer des droits d'accès adaptés en fonction des utilisateurs et des systèmes, mais aussi configurer correctement les systèmes de gestion des annuaires et des accès.
3. **Sauvegardes sécurisées, chiffrées et testées :** Mandiant recommande aux entreprises d'élaborer un plan solide de chiffrement et de sécurisation des sauvegardes afin de faciliter la restauration des systèmes et des données en cas de cyberattaque. Les solutions de sauvegarde et de stockage externe peuvent réduire les risques de perte de propriété intellectuelle et d'autres données de valeur. Ainsi, de plus en plus d'entreprises utilisent des solutions de service cloud pour garder une copie de leurs réseaux cloud ou hybrides et minimiser ainsi les interruptions en cas d'incident.

6. Marsh, Cyber Insurance Market Overview: Fourth Quarter 2021, 7 décembre 2021

4. **Planification et test de la réponse aux incidents :** pour Mandiant, cette pratique s'avère indispensable. Elle consiste à passer en revue les contrôles techniques existants, les architectures réseau et les capacités de réponse initiale. Mandiant recommande notamment de planifier la réponse aux scénarios courants et de réévaluer continuellement les fonctionnalités de cyberdéfense pour endiguer rapidement la menace en cas d'incident.
5. **Assistance juridique et équipe IR toujours disponibles :** la planification de la réponse aux incidents peut nécessiter de faire appel à des intervenants externes afin de se prémunir contre les risques juridiques et de bénéficier d'une expertise IR. Les juristes – en particulier ceux spécialisés en cybersécurité – doivent pouvoir collaborer efficacement avec les analystes forensiques en cas d'attaque, pour évaluer les risques et la responsabilité juridique de l'entreprise. Quant aux équipes IR externes, elles réduisent considérablement les délais de réponse, et donc l'impact d'une compromission. Un contrat d'astreinte pour la réponse aux incidents (IRR) permet aux entreprises de fixer les conditions des services d'intervention avant même qu'un incident de sécurité se produise.

Les cyberassureurs offrent également des services de conseil en sécurité pour accompagner les organisations dans le processus de souscription. De nombreux courtiers et compagnies d'assurance se démarquent en proposant même des évaluations, des services d'hygiène cyber et d'autres procédures destinées à mettre en place des moyens de défense efficaces.

Et pour vous y retrouver sur le marché de la cyberassurance, vous pouvez compter sur les partenaires Mandiant, nos podcasts, nos webinaires et les offres Google Cyber Risk.

Étude de cas : détection et élimination d'une compromission de supply chain logicielle par nos analystes

Activation des fonctions de détection et de réponse : mode d'emploi

L'année dernière, Mandiant a fait état d'une véritable explosion des compromissions de supply chain. En 2021, les chaînes d'approvisionnement étaient en effet à l'origine de 17 % des intrusions, contre moins de 1 % en 2020[7]. Il faut dire que 86 % des compromissions traquées par Mandiant étaient liées à l'attaque SolarWinds et à SUNBURST[8]. Toutefois, cette hausse s'explique également par le fait que les entreprises entretiennent des relations avec 244 fournisseurs de technologies en moyenne[9].

Les attaques contre la supply chain logicielle ne datent pas d'hier. En 2017, NotPetya a fait des ravages dans le monde entier. Le code malveillant, maquillé en ransomware, reposait sur l'exploit EternalBlue, développé par la NSA et divulgué par des hackers, pour infiltrer des réseaux, puis détruire des données de manière systématique. Les attaquants derrière NotPetya ont ainsi compromis une entreprise de développement de logiciels de comptabilité, fournisseur de l'administration ukrainienne.

La même année, l'utilitaire CCleaner[10] a lui aussi été compromis. Les hackers ont ainsi pu remplacer la version légitime du logiciel par une version malveillante, avec pour conséquence la compromission de plus de 2 millions d'hôtes.

En 2020, c'est un composant SolarWinds qui a permis une attaque de grande ampleur. D'après les analyses, le choix des cibles du groupe responsable, APT29 (anciennement UNC2452), servait les intérêts stratégiques de la Russie[11]. Parmi les victimes d'APT29 figuraient des administrations et des entreprises du Fortune 500. Là encore, les attaquants s'en prenaient à la supply chain logicielle en injectant un backdoor dans Orion pour pouvoir accéder aux environnements internes des victimes et ainsi déployer le malware SUNBURST après la diffusion du code mis à jour via un processus légitime.

En somme, les attaquants ont trouvé le moyen de compromettre l'une des pierres angulaires de nos entreprises numériques. En ciblant et en compromettant un package plébiscité par les développeurs de logiciels, ils peuvent aisément diffuser leur code malveillant à grande échelle et atteindre directement leurs victimes. Cette approche a de quoi désarçonner les équipes de sécurité. Dans le monde entier, les entreprises font tout pour maintenir la visibilité sur leur surface d'attaque et veiller à l'efficacité de leurs fonctions de détection et de réponse. Trop souvent, elles ignorent si elles pourront détecter et bloquer rapidement les cyberattaques exploitant leur supply chain logicielle, notamment parce qu'elles ne disposent pas d'équipes de sécurité suffisamment formées et qu'elles les mobilisent trop rarement pour mettre à jour leur formation et leurs connaissances.

7. Mandiant, rapport M-Trends 2022
8. Mandiant, rapport M-Trends 2022
9. Mandiant, Guide pratique des équipes de sécurité (numéro 2), 2022
10. Mandiant Threat Intelligence, CCleaner Supply-Chain Compromise Possibly Linked to Chinese Cyber Espionage Operators, septembre 2017
11. Mandiant, Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, décembre 2020

Parfois difficiles à détecter, les compromissions de supply chain logicielle exploitent la confiance des entreprises dans leurs fournisseurs pour accéder indirectement à l'environnement de leur victime. Au final, la capacité des entreprises à identifier et à bloquer les attaques avancées dépend beaucoup de l'expertise et du processus d'investigation de ses analystes sécurité.

Dans le cas des attaques contre la supply chain, la relation de confiance préexistante complique grandement la détection directe du code malveillant injecté. Des capacités de détection et de réponse actives et efficaces s'avèrent d'autant plus indispensables qu'un évènement suspect détecté à un stade plus avancé du même cycle d'attaque permet aux analystes de détecter l'injection indirectement, en reconstituant les actions des attaquants lors d'une investigation.

– Steve Ledzian, Vice-président, CTO de la région APAC, Mandiant

Détection et investigation d'une compromission de supply chain logicielle par nos analystes

À la mi-octobre 2021, des analystes sécurité du service managé de détection et de réponse de Mandiant ont identifié de multiples évènements correspondant à une contamination de référentiels open source. L'étude de cas ci-dessous présente leur processus de détection et d'investigation – ainsi que les questions qu'ils se sont posées – en lien avec des packages hébergés sur Node Package Manager (NPM), un gestionnaire de packages de la plateforme JavaScript Node.js.

Une petite équipe d'analystes sécurité de Mandiant a d'abord pris connaissance de plusieurs alertes indiquant qu'un utilitaire Windows natif **CERTUTIL.EXE** servait à télécharger des payloads depuis une seule et même URL **(hxxps://citationsherbe[.]at/sdd.dll)**. Puisque d'autres analystes du centre opérationnel de sécurité (SOC) commençaient eux aussi à recevoir des alertes similaires, l'équipe s'est mise à coordonner ses efforts pour trouver des réponses à ses questions.

De quoi s'agit-il ? Comment s'est-il retrouvé sur le système ?

Les deux premières questions à se poser lors d'une investigation sont les suivantes : « De quel malware s'agit-il et comment fonctionne-t-il ? » et « Comment s'est-il retrouvé sur le système ? ». Les analystes se sont procuré le payload à partir des hôtes initiaux pour comprendre le fonctionnement du fichier binaire suspect. L'analyse de tri a permis de déterminer qu'il s'agissait d'un variant de DANABOT, un malware qui cible les identifiants pour le vol de données via des communications CnC avec un serveur sous le contrôle des attaquants. À l'aide de l'adresse CnC du malware, les analystes ont identifié d'autres systèmes communiquant avec l'infrastructure des attaquants dans l'environnement. Ainsi, ils ont pu vérifier si le même malware ou des malwares similaires avaient été déployés sur d'autres systèmes sans déclencher une alerte. Une fois la menace confirmée, l'équipe d'analystes a confiné les hôtes compromis à distance ou en mobilisant l'équipe de réponse aux incidents.

DANABOT est une backdoor codée en Delphi qui communique à l'aide d'un protocole binaire personnalisé via TCP. Elle implémente un framework de plug-ins qui lui permet d'ajouter des capacités via des plug-ins téléchargés. DANABOT peut notamment prendre totalement le contrôle d'un système avec un plug-in VNC ou RDP, collecter des vidéos et des captures d'écran, enregistrer les saisies clavier, exécuter des commandes shell arbitraires et transférer des fichiers. Le plug-in de proxy de DANABOT lui permet de rediriger ou de manipuler le trafic réseau associé à des sites web ciblés. Il s'en sert souvent pour subtiliser des identifiants ou des données de moyens de paiement. DANABOT peut également extraire des identifiants stockés, associés aux navigateurs web et clients FTP.

"ua-parser-js" est un package léger à faible impact, déployé dans une application web ou côté serveur pour extraire et filtrer les données nécessaires à l'analyse d'une chaîne de caractères User-Agent (navigateur, moteur, OS, CPU et appareil).

Comment est-il arrivé là ?

Pour comprendre le processus de déploiement d'un malware, les analystes s'appuient généralement sur les données collectées par les technologies de détection et de réponse sur les terminaux (EDR). Grâce à ces données télémétriques, ils ont identifié des commandes légitimes exécutées par des utilisateurs pour mettre à jour les packages NPM.

Puisque le répertoire **UA-PARSER-JS PACKAGE** de chacun des hôtes concernés contenait un fichier similaire, les analystes en ont déduit que ce répertoire était compromis et diffusait le malware. La modification malveillante du répertoire JS Package ajoutait une étape préalable au processus d'installation du package, qui déclenchait le téléchargement du malware. En examinant le script compromis, les analystes ont découvert qu'il téléchargeait et déployait également des coinminers (aussi appelés mineurs de cryptomonnaies) sur l'hôte. En consultant les problèmes liés au package dans le référentiel GitHub, ils ont aussi trouvé le message d'un utilisateur qui demandait si le package avait été récemment compromis. Un problème soulevé sur GitHub le 22 octobre 2021 vers 12h15 (UTC) a permis de confirmer que le package NPM « **ua-parser-js** », une bibliothèque Node.js téléchargée plus de 7 millions de fois par semaine, avait été compromis et diffusait des malwares. Les attaquants étaient parvenus à publier trois versions malveillantes du package en détournant le compte NPM de l'auteur. D'après le journal Git du référentiel, le 22 octobre entre 16h14 et 16h25 (UTC), l'auteur du package a ajouté une version non infectée des packages malveillants afin d'empêcher d'autres compromissions.

Quelles autres opérations ces attaquants ont-ils menées ?

Une fois les hôtes confinés, les analystes ont poursuivi leurs recherches pour identifier la cause racine de l'attaque. En étudiant le journal Git du référentiel du package, ils ont trouvé des horodatages correspondant aux modifications des hackers et à la correction survenue quelques heures plus tard. Une analyse approfondie des modes opératoires des acteurs malveillants a permis à l'équipe de faire le lien avec d'autres packages NPM compromis par les mêmes attaquants et de cerner l'étendue de leurs activités. Les analystes ont ainsi pu, avec une quasi-certitude, attribuer ces activités à UNC3379. Ils ont analysé le malware, documenté le comportement des attaquants et mis au point de nouvelles techniques de détection pour bloquer ce type d'activités à l'avenir.

Pour en savoir plus sur cette compromission de supply chain logicielle, lisez l'article de blog intitulé « Compromissions de la supply chain par package Node.js : les mineurs doivent être accompagnés ».

Misez sur l'instinct, l'expérience et l'esprit critique de vos analystes

Quelle que soit l'ampleur de l'investigation, chaque minute compte. Pour les investigations et la réponse aux incidents, Mandiant s'appuie sur les connaissances, l'expérience et l'esprit critique de ses analystes. Véritables cyberdétectives, ils exploitent les indices, les preuves et les artefacts forensiques pour faire toute la lumière sur les incidents. Les investigations ont pour but de répondre à des questions clés sur les attaques :

- Portée de l'intrusion
- Menace active ou non
- Première date de compromission et cause de l'intrusion
- Type et quantité de données exposées
- Identité et motivations des attaquants

Les réponses à ces questions détermineront la marche à suivre pour endiguer l'attaque, éliminer la menace et rétablir l'activité. Mandiant vous recommande de miser sur l'expérience de terrain, des simulations et des formations pour donner les moyens à vos analystes de mener des investigations et de prendre des décisions importantes afin de confiner rapidement les systèmes compromis et d'éradiquer efficacement la menace. « Il n'est pas rare que les entreprises mènent leur propre investigation et répondent elles-mêmes à un incident pour déclencher prématurément la remédiation », explique Eric Sales, Vice-président de Mandiant. « Or, mieux vous comprenez une attaque, plus vous avez de chances de la neutraliser et de vous en remettre. »

Dans le cas de l'investigation présentée plus haut, les analystes des services MDR de Mandiant ont développé des indicateurs clés ultraprécis en lien avec les activités. Ils ont également procédé au tri des malwares déployés pour déterminer les bonnes mesures de remédiation. Enfin, à l'aide de nos connaissances et recherches approfondies sur le groupe d'attaque, ils ont pu analyser les environnements de nos clients pour identifier d'autres activités malveillantes liées à cette campagne non détectée par leurs produits EDR.

Articulation de la cyberdéfense autour des objectifs multisectoriels de performance de la CISA

Les groupes d'attaque étatiques continuent de cibler les technologies d'infrastructure critique. L'année dernière, Mandiant alertait sur l'existence d'outils personnalisés qui permettent aux attaquants de rechercher, de compromettre et de se retrouver aux manettes de certains systèmes de contrôle industriel (ICS) ou de contrôle et d'acquisition de données (SCADA), une fois infiltrés sur un réseau de technologies opérationnelles (OT)[12]. Les infrastructures industrielles et les OIV étant de plus en plus connectés, la neutralisation de ces menaces sophistiquées passe par de nouvelles pratiques de cybersécurité. C'est pourquoi, aux États-Unis, en collaboration avec d'autres organismes, la CISA (Cybersecurity and Infrastructure Security Agency) et le NIST (National Institute of Standards and Technology) ont élaboré des objectifs de cybersécurité communs à tous les secteurs incluant des infrastructures critiques.

En octobre 2022, la CISA a ainsi publié les objectifs multisectoriels de performance en cybersécurité (CPG)[13] afin d'aider les entreprises à identifier et à prioriser les pratiques clés en la matière. Les objectifs CPG de la CISA doivent servir de référentiel pour répondre aux problématiques courantes dans ce domaine, le but pour tous étant de réduire les cyber-risques, en vue de mieux protéger les infrastructures critiques des pays : hôpitaux, fournisseurs d'énergie, transports publics, grands groupes industriels, etc.

De son côté, Mandiant intègre pleinement les directives CPG de la CISA comme point de départ d'une stratégie de réduction des risques. Ces CPG offrent également une première série d'objectifs au mémorandum américain sur la sécurité nationale (NSM-5) pour le renforcement de la cybersécurité des systèmes de contrôle des infrastructures critiques. S'ils ne constituent en aucun cas un programme de sécurité complet, ces objectifs représentent une étape clé vers l'amélioration des pratiques cyber.

12. Mandiant, INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems, 13 avril 2022
13. Cybersecurity and Infrastructure Security Agency, CPG Cross-Sector Cybersecurity Performance Goals 2022

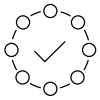
Pour vous permettre de bâtir votre plan de réduction des cyber-risques sur des bases solides, les CPG intègrent un certain nombre d'éléments clés :

Sous-ensemble mappé de pratiques de cybersécurité

Conseils spécifiques aux technologies IT et OT

Pratiques de réduction des risques classées par ordre de priorité

Prise en compte des menaces observées par la CISA et les secteurs et administrations partenaires



Objectifs applicables à tous les secteurs incluant des infrastructures critiques

Les CPG mettent l'accent sur des actions et des éléments bien particuliers, liés aux technologies opérationnelles et aux ICS, afin d'aider les entreprises à mieux protéger leur infrastructure critique.

Quelle que soit sa taille, une entreprise ne peut protéger son infrastructure critique sans un tableau complet des menaces en présence, un protocole de tests rigoureux et des capacités de détection et de réponse couvrant l'intégralité de sa structure. Les CPG l'aident à investir d'abord dans les solutions les mieux à même de renforcer sa sécurité, tout en tenant compte de son budget, de ses effectifs et de son expertise. Ces investissements dans des pratiques en phase avec les CPG permettront « d'éliminer de graves risques pour la sécurité, la santé et les moyens de subsistance des États-Uniens »[14].

14. Cybersecurity and Infrastructure Security Agency, CPG Cross-Sector Cybersecurity Performance Goals 2022

Tableau complet des cybermenaces en présence

Les CPG aident les entreprises à garder un œil sur les menaces en présence et à analyser les modes opératoires des acteurs malveillants pour détecter les attaques en cours. Cet inventaire des risques existants fait partie intégrante de l'approche de la sécurité OT de Mandiant. En effet, nous permettons à nos clients de dresser un état des lieux complet pour améliorer leurs fonctionnalités de détection des menaces sur les réseaux IT et OT[15]. Les équipes de sécurité et de réponse aux incidents ont grand intérêt à se concentrer sur les modes opératoires tout au long du cycle d'attaque, surtout détectables sur les « systèmes intermédiaires » – essentiellement des systèmes à la croisée des périmètres IT et OT ou des serveurs et postes de travail du réseau OT dont les protocoles et les systèmes d'exploitation ressemblent beaucoup (ou sont identiques) à ceux du réseau IT. Si cette approche s'avère efficace, c'est parce que la majorité des attaques avancées contre les technologies OT exploitent ces systèmes intermédiaires pour atteindre leur cible.

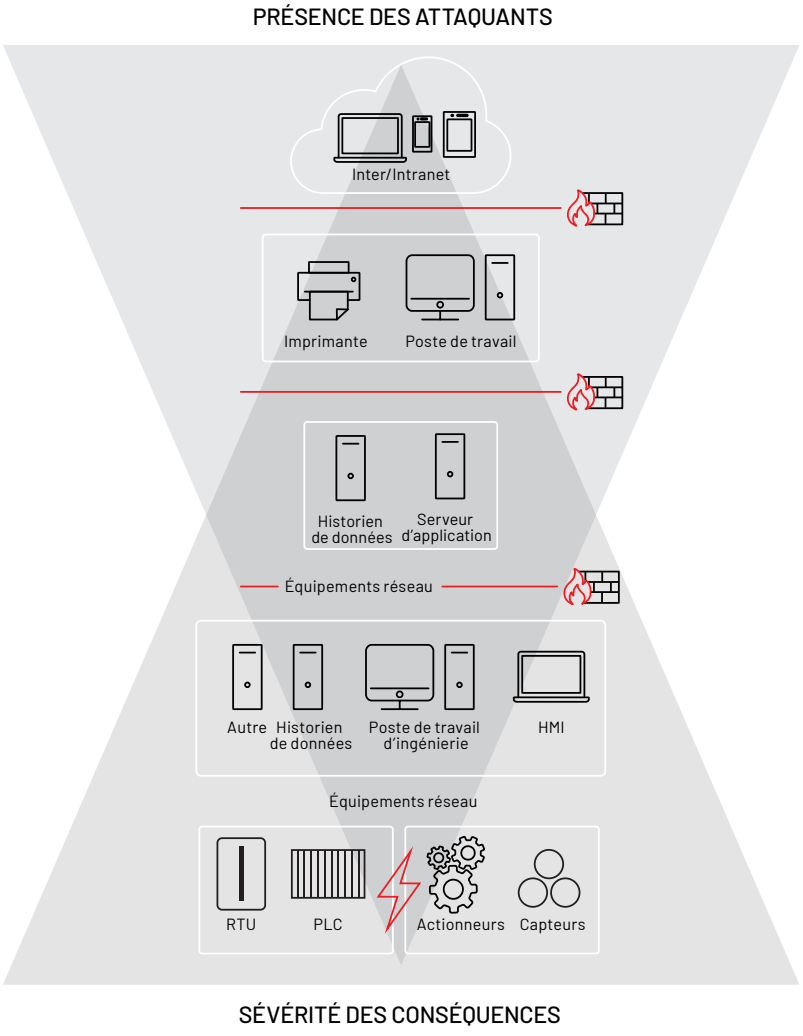


Figure 1. Entonnoir d'opportunités de détection des menaces OT.

15. Mandiant, The Mandiant Approach to Operational Technology Security, décembre 2019

Vous avez de meilleures chances de détecter une attaque ciblant votre réseau OT à l'intersection des deux triangles de la figure 1[16]. C'est là que votre équipe de sécurité bénéficie d'un rapport plus favorable entre le niveau de présence des attaquants et les conséquences opérationnelles d'une intrusion. Cette équipe doit comprendre les modes opératoires des adversaires et utiliser ces connaissances pour traquer et détecter les menaces avancées. Pour une efficacité maximale, mieux vaut traquer les menaces aux abords de la zone démilitarisée (DMZ) du réseau OT et du système de contrôle distribué (DCS), car les éléments détectables d'une intrusion subsistent à ce stade et ses éventuelles conséquences sont graves, mais pas létales.

16. Mandiant, The Mandiant Approach to Operational Technology Security, décembre 2019

2022

En 2022, Mandiant a signalé la divulgation de documents sensibles concernant les réseaux et les technologies OT lors de tentatives d'extorsion par ransomware[17]. Or, ces expositions de données OT confidentielles dans le cadre de ransomwares ou d'autres types de fuites fournissent aux auteurs d'attaques avancées de précieuses informations sur leur cible : l'infrastructure de la victime, ses ressources, ses processus et ses failles de sécurité. Des données de reconnaissance de ce genre permettent d'accroître l'impact et la précision des attaques.

TABLEAU 2. Documents exposés lors de tentatives d'extorsion par ransomware

Victime (anonymisée)	Contenu de la fuite
Constructeur de trains de marchandises et de voyageurs	Identifiant et mot de passe d'administration pour un OEM, exigences de l'architecture de contrôle et des canaux de communication d'un tramway en Europe, sauvegardes des fichiers de projet PLC du portail Siemens TIA, etc.
Deux compagnies pétrolières et gazières	Documents détaillés sur le réseau et les processus, y compris schémas, HMI, tableurs, etc.
Intégrateur de systèmes de contrôle	Documents d'ingénierie des projets clients (certains fichiers étaient protégés par des mots de passe que nous n'avons pas tenté de contourner).
Producteur d'hydroélectricité	Données principalement financières et comptables, mais aussi une liste de noms, d'e-mails, de privilèges utilisateurs, et quelques mots de passe (collaborateurs IT, opérationnels et de maintenance de la centrale).
Fournisseur de services de suivi des véhicules par satellite	Schémas produits, visualisations et code source d'une plateforme propriétaire utilisée pour suivre les flottes de véhicules par GPS.
Producteur d'énergies renouvelables	Contrats entre la victime et ses clients énonçant les conditions de maintenance et de mise à disposition d'une infrastructure d'énergie renouvelable. Ces contrats indiquaient que le fournisseur de services bénéficiait d'un accès total au système SCADA du tiers via des adresses IP publiques.

- Appliquez des politiques strictes pour les collaborateurs et les sous-traitants qui manipulent des données de tous les segments du réseau afin de protéger vos documents internes.
- Évitez de stocker des données opérationnelles ultraconfidentielles sur des réseaux mal sécurisés.
- Sélectionnez des sous-traitants qui implémentent des programmes de sécurité complets pour protéger vos données opérationnelles.
- Évaluez la valeur des données exposées si vous êtes victime d'un ransomware pour identifier les contrôles compensatoires pouvant réduire le risque d'une autre intrusion.
- Modifiez les identifiants et les clés d'API divulgués. Envisagez également de changer les adresses IP exposées des systèmes critiques et des serveurs jump de l'OT.
- Organisez régulièrement des exercices Red Team pour identifier les informations internes exposées et non sécurisées.

17. Mandiant, 1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information, janvier 2022

Protocole de tests rigoureux

Pour renforcer la protection des réseaux OT, il est essentiel de tester de façon sécurisée les contrôles mis en place à chaque couche face aux principales attaques et familles de malware qui ciblent les ressources critiques. À cet égard, les CPG de la CISA recommandent un audit régulier et indépendant de l'efficacité et de la portée des moyens de défense de l'entreprise.

De son côté, Mandiant vous conseille un programme sur mesure, adapté aux besoins d'évaluation de votre organisation. Les meilleurs programmes de tests des réseaux OT sont ceux qui adoptent le point de vue de l'attaquant, qui utilisent des simulations afin de réduire leur impact sur vos opérations en temps réel et qui allient des exercices Red Team et Purple Team à des tests d'intrusion et de sécurité pour éprouver la résistance de vos réseaux et composants. Lorsqu'il est impossible de réaliser des tests proactifs en raison des exigences de disponibilité des environnements OT en production, Mandiant recommande des évaluations techniques qui mesurent l'efficacité de la segmentation réseau, des contrôles d'accès, des systèmes de surveillance, des politiques appliquées aux équipements éphémères et des fonctionnalités de réponse aux incidents. Des tests réguliers permettent non seulement de juger des performances des contrôles de sécurité à un instant *t*, mais aussi d'identifier des problèmes de sécurité complexes sur les réseaux intégrés (IT et OT) avant toute tentative d'exploitation. Un processus de validation permanent peut également préparer l'équipe d'une entreprise à la surveillance, à la détection et à la réponse aux incidents de cybersécurité. Enfin, un bon programme fournit des recommandations tactiques destinées à résoudre les problèmes les plus graves, des conseils stratégiques pour améliorer la sécurité sur le long terme, ainsi qu'une liste des lacunes à corriger en matière de suivi et de réponse aux incidents OT.

Les serveurs Open Platform Communications permettent aux machines, appareils et systèmes de n'importe quel fabricant au sein d'un environnement industriel de s'échanger des données de même nature.

Réponse et reprise post-incident

Dans la section 7 de ses CPG, la CISA invite les entreprises à maintenir, tester et mettre à jour leurs plans de réponse aux incidents liés aux menaces qui les concernent. Parce qu'elle est intervenue sur des incidents OT majeurs comme TRITON et INCONTROLLER, l'équipe de Mandiant comprend mieux que personne la différence de méthodologie IR entre les réseaux IT et OT, et maîtrise les outils et procédures nécessaires pour intervenir en cas d'attaque OT.

Si les objectifs de remédiation et d'endiguement (éliminer la menace et restaurer les systèmes) restent les mêmes dans les environnements IT et OT, les outils varient parfois beaucoup. Les équipes de réponse aux incidents IT utilisent régulièrement des technologies de détection et de réponse pour faciliter les investigations, l'endiguement de la menace et la remédiation ou la reprise d'activité. Or, ces outils sont généralement absents des serveurs et composants des réseaux OT.

Dans les environnements IT, il est relativement simple d'endiguer la menace. En revanche, sur les réseaux OT complexes, cette étape peut avoir des conséquences bien plus critiques. Par exemple, sur un réseau IT, il n'est pas rare d'activer et de désactiver des fonctions spécifiques, voire de supprimer un système entier. Les composants OT supportent beaucoup moins bien ce type d'actions. C'est pourquoi il est primordial de comprendre les processus sous-jacents avant de lancer ou stopper certains d'entre eux ou de mettre un composant hors ligne, sous peine de provoquer des interruptions de service majeures, voire de mettre des vies en danger. Par exemple, la déconnexion de serveurs OPC (Open Platform Communications) peut paralyser toute une chaîne de production pendant des semaines. Ainsi, une planification détaillée (avant tout incident) s'impose, pour permettre aux responsables des systèmes de tenir compte des interruptions potentielles, d'une éventuelle diminution de la production et des risques létaux. La capacité d'une entreprise à identifier les objectifs des attaquants peut également aider ces mêmes responsables à prendre des décisions plus sûres.

Enfin, les réseaux OT se composent de nombreux sous-réseaux exécutés par des fournisseurs, auxquels les entreprises n'ont pas directement accès. À cet égard, Mandiant recommande l'élaboration de playbooks et de plans de réponse qui intègrent ces systèmes tiers, ainsi que des tests en collaboration avec leurs fournisseurs. Il est plus important que jamais de mettre un plan en place et de s'entraîner pour pouvoir répondre rapidement, efficacement et à grande échelle en cas d'incident.

Mandiant offre des solutions de sécurité OT en phase avec les cinq fonctions du framework de cybersécurité du NIST[18], que les CPG de la CISA viennent compléter, afin d'aligner ses services sur le cycle de gestion des cyber-risques d'une entreprise.

18. NIST, Cybersecurity Framework, The Five Functions, mai 2021

		IDENTIFICATION	PROTECTION	DÉTECTION	RÉPONSE	REPRISE
Threat Intelligence	Abonnement Threat Intelligence	■	■	■		
	Analyste CTI attitré	■	■	■		
	Service d'évaluation des vulnérabilités	■	■			
	Analyse personnalisée et audit boîte noire	■				
Conseil	Diagnostic d'intégrité	■	■	■		
	Évaluation du programme de sécurité	■	■			
	Tests d'intrusion	■	■	■		
	Planification de la réponse aux incidents	■			■	■
	Réponse aux incidents				■	■
	Formation en cybersécurité	■	■			
	Conseiller attitré	■	■	■	■	■
Managed Defense pour l'OT	Mise en service	■	■			
	Surveillance continue		■	■	■	
Technologies tierces	Surveillance des protocoles réseau OT	■		■		

Figure 2. Offres Mandiant pour l'OT

Mandiant allie des éclairages cyber collectés sur le terrain à une connaissance approfondie du fonctionnement des systèmes de contrôle industriel, fruit de décennies d'interventions sur les environnements OT et ICS. Les tests de sécurité ultrasophistiqués de nos experts OT permettent aux industriels d'améliorer leurs capacités de détection et de neutralisation des menaces d'un bout à l'autre des réseaux OT. Mandiant aide les entreprises à intégrer les CPG de la CISA à leur stratégie pour un environnement OT plus sûr et une meilleure préparation aux incidents de cybersécurité.

Conclusion

Dans ce numéro de notre Guide pratique des équipes de sécurité, nous recommandons aux entreprises en passe de migrer des mots de passe et des méthodes d'authentification multifacteur (MFA) traditionnelles vers l'authentification sans mot de passe de s'appuyer sur des méthodes MFA fortes et d'envisager des solutions SSO tierces pour déléguer l'authentification sur chaque appareil et application au back-end. Quant à celles et ceux confrontés au marché instable de la cyberassurance, nous leur conseillons 1) de mobiliser la direction juridique et l'équipe de gestion des risques lors de la souscription d'une police, 2) d'étudier soigneusement le modèle de contrat fourni et 3) de former un véritable partenariat avec leur assureur.

Nous mettons également en lumière l'alignement des six grandes fonctions de la cyberdéfense énoncées dans notre guide avec les objectifs multisectoriels de performance en cybersécurité (CPG) récemment publiés par la CISA aux États-Unis. En implémentant ces bonnes pratiques de sécurité, les propriétaires et les opérateurs d'infrastructures critiques peuvent grandement réduire les risques en présence. Enfin, une étude de cas nous permet d'illustrer les tactiques déployées par un SOC optimisé, dans lequel les analystes se coordonnent pour traiter les alertes pertinentes et s'appuient sur leurs connaissances, leur expérience et leur esprit critique pour enquêter sur les compromissions de supply chain.

Dans la lutte contre la cybercriminalité comme ailleurs, savoir c'est pouvoir. C'est pourquoi nous pensons qu'il est essentiel d'apporter aux dirigeants et aux professionnels de la sécurité des informations qui leur permettront de prendre des décisions éclairées. Dans ce contexte, les acteurs de la cybersécurité doivent mettre l'accent sur la collaboration et le partage d'informations pour redonner l'avantage à la défense. C'est là toute la mission de ce guide.

Pour en savoir plus, rendez-vous sur www.mandiant.fr

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190
+1 (703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

À propos de Mandiant

Mandiant est un leader reconnu dans les services de cyberdéfense, Threat Intelligence et réponse aux incidents. Fort de plusieurs décennies d'expérience sur la ligne de front de la cybersécurité, Mandiant aide les entreprises à mieux se préparer et à répondre aux cybermenaces. Mandiant fait désormais partie de Google Cloud.

MANDIANT
NOW PART OF Google Cloud

A-EXT-RT-FR-FR-000483-01-FR