ivanti

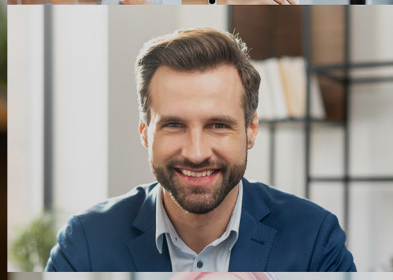
Toolkit de cyberstratégie 2023 pour susciter l'adhésion interne

Apprenez à défendre votre budget et à convaincre les parties prenantes (hors InfoSec) de l'importance de votre stratégie de cybersécurité

En collaboration avec

CSW Cyber SecurityWorks

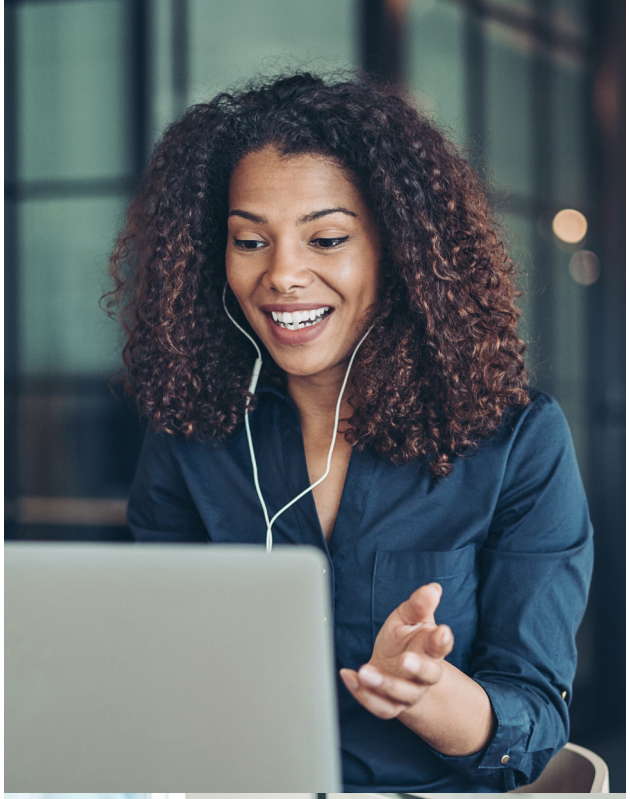


Avant-propos

Bienvenue !

Cet eBook a pour objectif de vous aider à justifier votre stratégie de cyberdéfense pour l'année à venir. Vous serez en mesure de présenter une stratégie qui suscitera l'adhésion interne. En étant facilement compréhensible, votre stratégie recevra un meilleur accueil des parties prenantes qui seront ainsi plus enclines à la financer et à la suivre.



Á la fin de cet eBook :

1. **Les équipes hors InfoSec disposeront d'un panorama contextualisé** des acteurs malveillants et de leurs schémas d'attaques en 2022. Les « Unes » alarmantes des médias seront ainsi mises en parallèle avec vos recommandations stratégiques de sécurité.

2. **Vous serez en mesure de démontrer** comment les mesures de sécurité proactives que vous avez voulu implémenter auraient pu bloquer des attaques dévastatrices.

3. **Vous serez capable de responsabiliser les parties prenantes et les utilisateurs finaux** afin qu'ils soient conscients d'avoir empêché des failles et des attaques majeures, simplement en mettant en œuvre et en respectant ce que vous leur demandez de faire depuis des années.

Notre objectif est de vous aider à préserver la sécurité de votre entreprise en 2023. Pour cela, vous allez devoir rompre avec l'approche réactive qui consiste à « appliquer essentiellement les correctifs qui font la Une des journaux ».

D'autant que cette approche est épuisante pour votre équipe.

Et elle l'est aussi pour votre entreprise !

Appuyez-vous sur ce toolkit pour expliquer votre stratégie d'une façon facilement compréhensible par les personnes extérieures au département InfoSec : plutôt que de présenter uniquement le « quoi », présentez aussi le « pourquoi ».

Plutôt que de présenter uniquement le « quoi », présentez aussi le « pourquoi ».

Vous pourrez ainsi obtenir les investissements nécessaires pour arrêter les cyberattaques avant qu'elles ne se produisent.

Nous vous souhaitons bonne chance. Nous espérons que ce guide aidera votre équipe à obtenir les ressources, les effectifs et le temps nécessaires pour faire ce qu'elle fait le mieux : garantir la sécurité de votre entreprise tout au long de l'année à venir… et au-delà.

Faites parler les statistiques : nous avons rassemblé ici des histoires vraies, celle d'entreprises comme la vôtre, attaquées par différents cybercriminels avec des motivations et des styles d'intrusion uniques.

Allez au-delà de l'analyse MITRE et de la criticité des CVE pour montrer aux parties prenantes comment un investissement minimal en « extras de sécurité » aurait pu contrer des attaques dévastatrices qui se sont produites sur le terrain et ce, dans un langage et avec un format que les personnes non-InfoSec comprendront.

Démontrez qu'en accordant un peu plus de temps et des ressources supplémentaires à votre équipe, cette dernière pourra tester et déployer des correctifs et des solutions de remédiation dans tous les départements, sans interrompre les opérations habituelles de l'entreprise, avant que les cybercriminels ne ciblent vos systèmes.

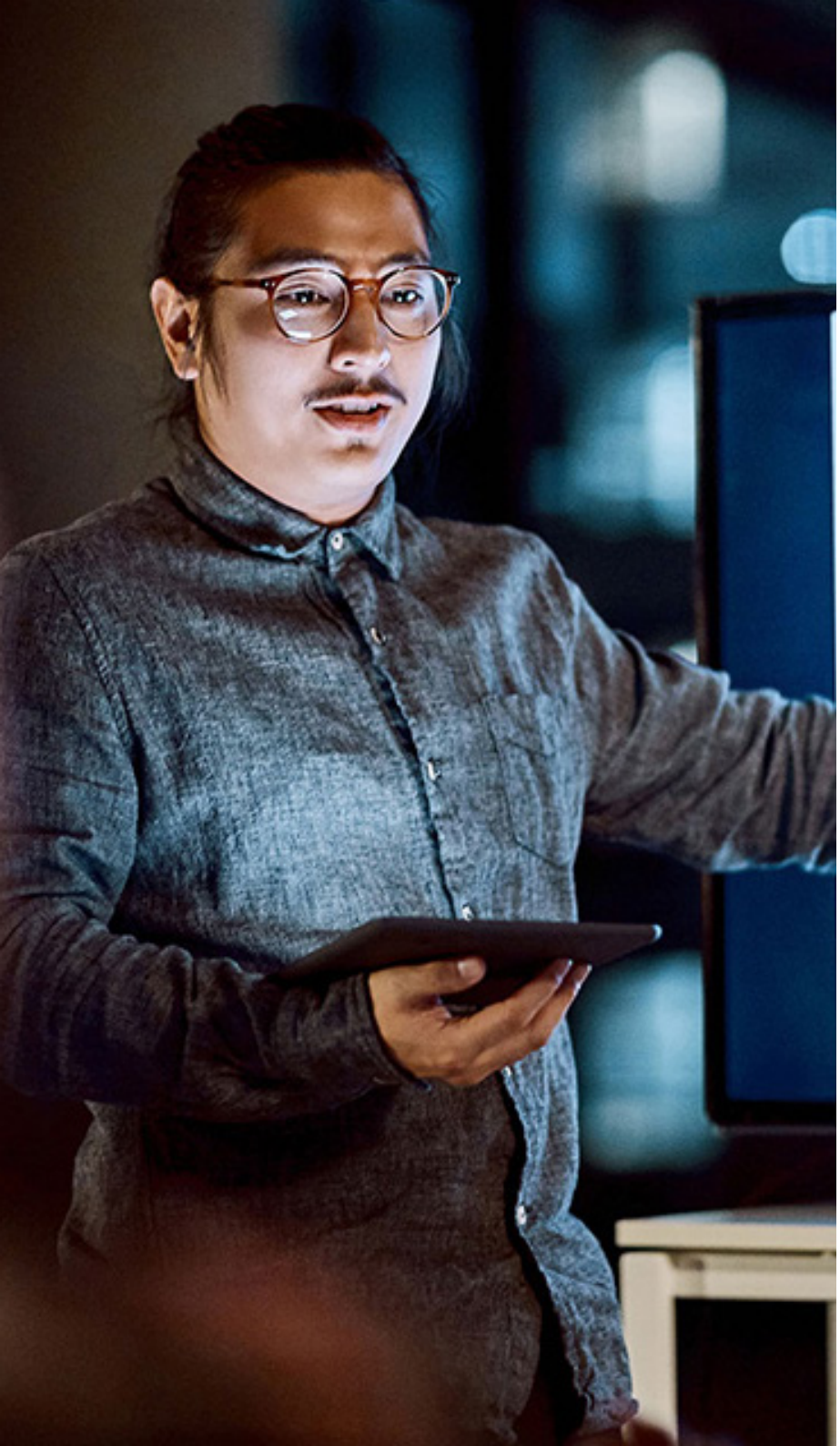


Table des matières

La boîte à outils en cybersécurité :

16 outils pour armer vos employés contre les menaces

ivanti CSW Cyber SecurityWorks

Avant de nous intéresser aux menaces que vous allez chasser pour les douze mois à venir, nous allons voir comment vous préparer en interne. Vous découvrirez quels sont les outils et les mesures de sécurité à implémenter pour éviter qu'une faille majeure ne se produise.

En fait, chacune des solutions présentées peut vous protéger, d'une façon ou d'une autre, contre pratiquement tous les acteurs malveillants mentionnés dans ce toolkit.

Une fois que les différents mécanismes de défense auront été assimilés au sein de votre entreprise (à condition d'avoir le temps et les ressources nécessaires ainsi que l'adhésion des dirigeants), nous évoquerons où et comment ces techniques auraient pu bloquer certaines des cyberattaques les plus importantes et les plus dommageables survenues en 2022.

Chaque tactique de cyberdéfense inclut :

- Son délai d'efficacité et son coût d'achat.
- Une description simplifiée de l'outil.
- Les raisons qui font que la tactique fonctionne pour repousser certains types de cyberattaques.
- Un aide-mémoire « Armez vos collaborateurs ! » pour répondre aux objections courantes des parties prenantes internes et faire en sorte que la conversation sorte du « Pourquoi est-ce nécessaire ? » pour plutôt parler de « Comment pouvons-nous contribuer au financement et à l'implémentation de cet outil ? ».

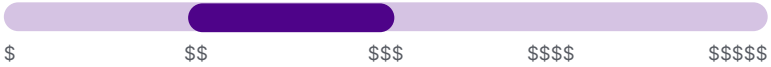
La boîte à outils en cybersécurité :
16 outils pour armer vos employés contre les menaces

Dans cette section

Anti-hameçonnage

Délai d'efficacité

Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)



Description

Le terme « anti-hameçonnage » ou « anti-phishing» désigne souvent une série d'outils conçus pour empêcher les pirates de tromper les utilisateurs en les incitant à cliquer sur des liens infectés ou à télécharger des fichiers malveillants, et ce pour plusieurs plateformes, périphériques, navigateurs, applications et messages texte.

Comment la protection fonctionne

Les humains ne sont pas parfaits ! Si un pirate réussit à tromper quelqu'un pour qu'il clique sur un lien ou lance un téléchargement de fichier, ces outils empêchent les activités malveillantes de réellement se produire.

Armez vos collaborateurs et avancez vos arguments

N'a-t-on pas déjà un filtre contre les messages de spam ? Pourquoi nous faudrait-il autre chose ?

Oui, certains navigateurs et logiciels d'e-mail comportent des outils gratuits. Cependant, ils ne sont pas disponibles pour toutes les plateformes et les incidents se multiplient parce que les collaborateurs utilisent de plus en plus des périphériques personnels dans un but professionnel.

Pourquoi l'anti-hameçonnage est-il si long à implémenter après l'achat ?

Répertoriez tous les OS, types de périphérique, systèmes réseau, navigateurs et autres postes client que votre solution anti-hameçonnage doit couvrir. Normalement, cela suffit à montrer pourquoi l'opération n'est pas instantanée !

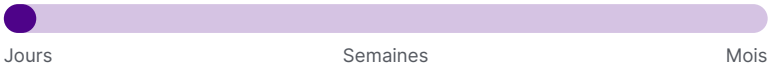
Pourquoi payer plus pour ces outils, alors qu'il existe des versions gratuites ?

Le coût plus élevé des outils anti-hameçonnage plus robustes vient généralement du fait qu'ils couvrent plusieurs plateformes et périphériques. Le craquage des informations d'authentification par hameçonnage est une tactique commune à presque tous les acteurs malveillants, quelle que soit leur motivation ultime.

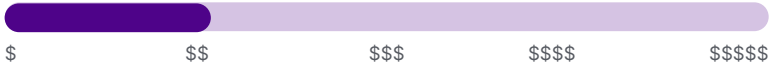
Ainsi, les outils anti-hameçonnage constituent sans doute la méthode la plus simple et la plus économique pour éviter de coûteuses failles de cybersécurité !

Antivirus / Antimalware

Délai d'efficacité



Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)



Description

C'est la solution de cybersécurité la plus basique. Elle offre une large protection et dissuade généralement les tentatives d'intrusion élémentaires.

Comment la protection fonctionne

En deux mots, l'antivirus et l'antimalware sont les protections minimales que toutes les entreprises doivent implémenter… juste pour bloquer et dissuader les menaces les plus élémentaires ou les plus opportunistes.

Armez vos collaborateurs et avancez vos arguments

Pourquoi dépenser plus pour cet outil, quand il existe des offres « gratuites » intégrées chez nos fournisseurs ?

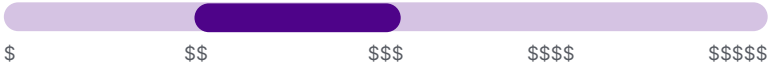
Vous pouvez peut-être justifier le passage à une solution antivirus ou antimalware améliorée si la version gratuite ralentit les ordinateurs ou provoque plus généralement des problèmes de fonctionnement.

Si l'impact opérationnel est suffisamment important, vous pouvez même affirmer que le logiciel gratuit ne vaut pas l'économie réalisée. Vos parties prenantes vous féliciteront probablement d'avoir trouvé de nouveaux outils antivirus ou antimalware.

Contrôle des applications

Délai d'efficacité

Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)



Description

Les outils de contrôle des applications autorisent uniquement certaines applications dans l'environnement qu'ils protègent. Le plus souvent, on utilise ce type de contrôle dans les environnements ou entreprises strictement réglementés.

Comment la protection fonctionne

En autorisant uniquement les applications ou les logiciels figurant sur une « liste blanche » de fournisseurs déjà vérifiée, le contrôle des applications empêche le téléchargement accidentel par un collaborateur de charges malveillantes cachant des malwares ou des chevaux de Troie, surtout sans certificat.

Armez vos collaborateurs et avancez vos arguments

**Pourquoi acheter un outil de contrôle des applis ?
On a déjà d'autres outils de contrôle des utilisateurs !**

Bien entendu, tous les outils de contrôle fonctionnent ensemble et se superposent pour constituer la meilleure cyberdéfense possible.

Cependant, pour obtenir un budget spécifique pour le contrôle des applications, vous pouvez dire aux parties prenantes non-InfoSec que le contrôle des applications fait faire des économies à l'entreprise, en surveillant l'utilisation des applications et en éliminant les logiciels non utilisés.

Avec ce genre de solution, je ne pourrai plus exécuter l'appli XYZ dont j'ai besoin pour travailler !

Encore une situation où une communication proactive avec toutes les parties prenantes de vos départements non-InfoSec est essentielle.

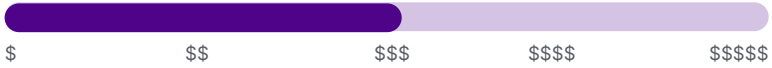
Procurez-vous la liste complète des applications actuellement utilisées par tous les départements… et repérez si possible celles qu'ils paient personnellement en tant qu'applis « Shadow IT ». Ensuite, lors de la création de la liste blanche, vérifiez que chaque appli de la liste ne présente aucune menace pour la sécurité, afin que les opérations métier puissent se poursuivre sans trop d'interruption.

Ensuite, faites en sorte que les demandes d'ajout de nouvelles applis puissent se faire aussi facilement et rapidement que possible, tout en garantissant qu'au moins une personne contrôle chaque demande. Si vous automatisez entièrement le processus, des pirates pourraient en tirer avantage et octroyer secrètement des permissions à leurs propres activités.

Gestion des configurations

Délai d'efficacité

Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)



Description

Paramètres, ports, protocoles… autant d'éléments à prendre en compte pour la gestion des configurations, afin de garantir que le système entier possède une baseline sécurisée. La gestion des configurations vérifie également que tous les actifs que vous achetez sont bien installés sur les bons périphériques et sont bien utilisés !

Comment la protection fonctionne

Il est fréquent que les configurations et les ports ouverts soient connus des acteurs malveillants. La conservation des valeurs par défaut ou de versions qui ne sont plus prises en charge étend votre surface d'attaque.

La gestion des configurations soutient également la pile de sécurité globale, car elle garantit que les autres programmes de sécurité ne sont pas oubliés, et sont correctement installés sur vos périphériques et dans vos environnements.

Armez vos collaborateurs et avancez vos arguments

Pourquoi acheter un outil de gestion des configurations ?

Les petites entreprises, qui ont peu d'obstacles réglementaires à surmonter, peuvent trouver que la comparaison coûts/avantages penche trop du côté coûts pour que les outils de gestion des configurations leur paraissent vraiment intéressants. Cela peut également représenter des coûts élevés de traitement manuel, alors veillez à bien montrer que l'outil que vous voulez ne va pas devenir un fardeau administratif pour votre équipe.

Cependant, si elle est réalisée correctement, la gestion des configurations aide votre entreprise à faire des économies, car elle vérifie que les technologies dans lesquelles tous vos départements ont investi sont bel et bien installées.

Hygiène et gestion des périphériques

y compris découverte et rapprochement des périphériques

Description

Pour le propos de ce toolkit, nous vous proposons de définir une solution d'hygiène et de gestion des périphériques comme suit : outil ou suite d'outils nécessaire pour trouver, répertorier, surveiller et traiter en continu les menaces sur tous les postes client, et actifs matériels et logiciels de votre environnement. Pour des raisons de sécurité, ces solutions doivent aussi intégrer ou faciliter les opérations de remédiation ou les actions requises dans l'éventualité où un intrus serait identifié.

Comment la protection fonctionne

Vous ne pouvez pas protéger ce que vous ne connaissez pas. Une solution de cybersécurité exige une prise en compte robuste, dynamique et automatique de tous les postes client du réseau protégé, car les audits traditionnels des périphériques ne sont exacts qu'au moment où la découverte est finalisée. Les fonctions de découverte des actifs soutiennent les programmes d'hygiène et de gestion, car elles repèrent les périphériques non pris en compte pour la protection et, potentiellement, les intrus prétendant n'être qu'« un ordinateur portable de plus » sur le réseau.

Armez vos collaborateurs et avancez vos arguments

Nous avons déjà l'ITAM. Pourquoi nous faut-il plus ?

En général, un outil ITAM standard fait uniquement le suivi des périphériques et des actifs qu'il s'attend à trouver, à partir des entrées des journaux d'achats et des annuaires Active Directory. Rappelez à cette partie prenante que c'est ce que vous ne voyez pas ou n'avez pas encore trouvé qui présente le plus grand danger pour les opérations quotidiennes de l'entreprise.

Il devient alors difficile de rapprocher l'annuaire Active Directory, le système de gestion des achats, la gestion des terminaux et les systèmes de protection du poste client. Sachez que 20-30 % des actifs devant être protégés passent au travers des mailles du filet. Sans parler des périphériques que des pirates ou autres acteurs malveillants pourraient introduire, ou des malwares véhiculés par des programmes BYOD non pris en compte.

Pourquoi payer pour une mise à niveau ?

Lorsqu'une entreprise se développe, le nombre des périphériques atteint rapidement un niveau qui dépasse les capacités des solutions bon marché. Et les rapprochements se compliquent.

De plus, n'oubliez pas que la plupart des outils gratuits inclus dans des suites logicielles sont dépourvus de fonctions de découverte dynamique des actifs, qui détectent les périphériques inconnus ou non pris en compte dès qu'ils arrivent dans l'environnement ou le quittent.

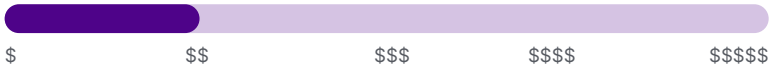
Du point de vue de la sécurité et lorsqu'il s'agit de gérer la surface d'attaque, la découverte des actifs est une pièce pivot du puzzle, et n'a pas un caractère accessoire.

Détection et réponse des terminaux (Endpoint Device & Response - EDR)

y compris système de détection des intrusions (IDS) et système de prévention des intrusions (IPS)

Délai d'efficacité

Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)



Description

Les solutions EDR sont capables d'identifier et même de bloquer tout accès non autorisé avant qu'il ne réussisse. Elles sont souvent combinées à d'autres solutions de contrôle d'accès, comme les pare-feux ou les protections antivirus/antimalware. Ces outils peuvent aussi se trouver dans un pare-feu, par exemple pour détecter les adresses IP dont l'origine n'est pas autorisée. Les solutions EDR peuvent être automatisées pour détecter les schémas d'accès et tendances de trafic qui diffèrent de la référence de base, afin de vous avertir des attaques possibles.

Comment cela vous protège

Vous ne pouvez réagir qu'aux incidents que vous connaissez. Plus vous créez d'alarmes et de pièges pour les pirates, plus vous êtes averti des attaques... et pouvez les stopper.

Armez vos collaborateurs et avancez vos arguments

Pourquoi payer une solution EDR alors qu'on a un pare-feu gratuit ?

Expliquez aux utilisateurs non-InfoSec que la différence est similaire à celle qui existe entre un simple mur et un mur protégé par des sentinelles. Le mur est un bon dissuasif, mais il ne recherche pas proactivement les menaces et ne tente pas de les bloquer.

Les solutions EDR appliquent de nombreuses mesures de sécurité automatiques pour un investissement relativement faible, autant financièrement qu'en personnel.

Pourquoi est-ce si long ?

Rappelez à vos parties prenantes que de nombreux éléments doivent être réglés dans les coulisses. Votre équipe se charge de tout régler pour que les autres équipes n'en aient pas conscience une fois l'implémentation terminée.

Votre équipe doit aussi surveiller l'installation initiale sur une longue période pour s'assurer que les résultats générés par la solution EDR sont fiables. Les ajustements qui sont apportés sont susceptibles de provoquer des problèmes même après l'implémentation.

Détection et isolement du chiffrement malveillant

Délai d'efficacité

Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)

Description

Lorsqu'un acteur malveillant commence à chiffrer ou à exfiltrer des fichiers ou des données pour les voler ou demander une rançon, ce type de logiciel est capable de détecter automatiquement les fichiers attaqués, et d'isoler des portions du réseau ou du serveur pour empêcher tout chiffrement supplémentaire.

Comment la protection fonctionne

Si tout le reste échoue, la détection et l'isolement du chiffrement malveillant vous aident à repérer les cybercriminels avant qu'ils ne volent ou ne verrouillent assez de données pour causer des dommages.

Armez vos collaborateurs et avancez vos arguments

Pourquoi devrions-nous payer pour cela ?

Rappelez à vos parties prenantes non-InfoSec le dicton « Attendez-vous au meilleur, mais préparez-vous au pire ».

Même si les cyberattaques seront en amont bloquées par vos autres outils de sécurité, ce logiciel peut servir de frein d'urgence s'il détecte le chiffrement ou l'exfiltration de données sensibles.

Et comment les employés vont-ils réagir s'ils apprennent que vous ne prenez pas toutes les mesures réalistes possibles pour protéger leurs informations ? Ou vos actionnaires, si vous ne protégez pas leur investissement des vols de propriété intellectuelle ?

On a une cyberassurance, pourquoi s'embêter à faire plus ?

La cyberassurance peut vous aider à payer le contrôle et le nettoyage des dommages. Toutefois, soyez conscient qu'il est plus facile et moins coûteux de faire une déclaration de presse sur une intrusion bloquée, que de devoir réparer les dégâts d'une fuite importante.

Vos primes d'assurance augmenteraient en flèche, et vous devriez probablement mettre en place des garde-fous supplémentaires (et peut-être encore plus onéreux), juste pour pouvoir être assuré.

Segmentation réseau

Délai d'efficacité

Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)

Description

La segmentation réseau consiste à diviser les réseaux Internet et intranet d'une entreprise, afin que seuls certains périphériques aient accès à des sections d'application ou de serveur spécifiques. Cela peut être très simple, comme donner aux périphériques IoT (Internet of Things) leur propre segment réseau, ou très complexe si vous octroyez à chaque département et serveur ses propres environnement et réseau.

Comment la protection fonctionne

La segmentation réseau empêche les pirates d'avoir accès aux autres zones de votre réseau, non accessibles avec les informations d'authentification ou le point d'accès initialement infecté. Si un pirate s'introduit dans une portion minime de votre environnement (comme un four compatible IoT, par exemple), son accès reste limité à cette portion.

Armez vos collaborateurs et avancez vos arguments

Pourquoi faut-il payer autant pour un outil de segmentation réseau ?

Les outils de segmentation réseau permettent à l'équipe Sécurité de gagner du temps et des ressources, car ils identifient les intrus sur le réseau et rendent plus intuitif le trafic autorisé entre les différents environnements.

Ainsi, rappelez à vos parties prenantes hors InfoSec qu'en passant moins de temps à gérer ou à surveiller les réseaux, vous aurez plus de temps pour traiter les demandes que les autres équipes adressent à votre équipe.

Par ailleurs, plus l'outil est sophistiqué, plus il sera facile à ces équipes de passer d'un segment réseau à un autre.

Pourquoi est-ce maintenant si difficile d'obtenir les documents dont j'ai besoin dans cet environnement ?

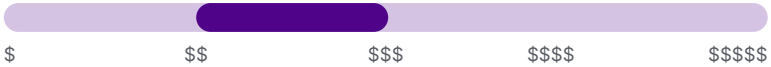
Pour vos parties prenantes hors InfoSec, essayez de simplifier le processus de soumission des demandes de changement et de le rendre aussi intuitif que possible.

Rappelez à votre équipe d'être aussi patiente que possible face aux plaintes… surtout au début ! Pour minimiser la plupart de ces plaintes, vous pouvez proactivement impliquer des responsables de tous les départements dans le processus d'implémentation, en tant que consultants sur le projet, pour qu'ils vous disent qui a besoin d'accéder à tel ou tel segment, et vous expliquent leurs workflows généraux.

Authentification multifacteur (MFA) sans mot de passe

Délai d'efficacité

Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)



Description

Les outils MFA sans mot de passe sont des outils de connexion qui exigent une authentification double (par texto/SMS, e-mail, appli d'authentification ou même données biométriques) pour l'accès aux applications ou l'octroi de permissions. Contrairement aux outils MFA à deux facteurs traditionnels, les connexions MFA sans mot de passe ne nécessitent aucun mot de passe.

Comment la protection fonctionne

Généralement, les collaborateurs hors InfoSec évitent de créer des mots de passe complexes ou uniques. Si vous éliminez les mots de passe, les pirates ne peuvent pas accéder à vos systèmes en craquant les informations d'authentification, en obtenant les mots de passe par force brute ou parce qu'un collaborateur laisse son mot de passe aux yeux de tous sur un post-it.

En outre, les programmes MFA sans mot de passe renforcent la mise en conformité avec les programmes de sécurité, car cela fait un code de moins que les collaborateurs doivent mémoriser !

Armez vos collaborateurs et avancez vos arguments

Pourquoi le MFA sans mot de passe coûte-t-il tellement plus cher que les autres alternatives ?

Il existe toute une gamme d'outils MFA sans mot de passe. En général, plus le prix par utilisateur est élevé, plus les niveaux de chiffrement et les contrôles personnalisés disponibles sont nombreux.

Un meilleur chiffrement permet d'empêcher les pirates de pénétrer dans votre système grâce à leur pure puissance informatique.

De plus, les contrôles personnalisés réduisent les coûts de main-d'œuvre tout en rendant le système plus convivial pour tous les utilisateurs.

Les expirations de sessions sont tellement pénibles ! Pouvez-vous les supprimer ?

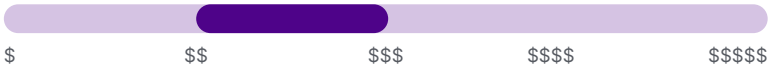
D'abord, si votre relation avec la partie prenante est suffisamment amicale, vous pouvez en plaisanter et lui dire : « Si vous trouvez ça pénible, imaginez à quel point ça l'est pour un pirate ! Au moins, vous, vous pouvez revenir. »

Ensuite, plus sérieusement, vous pouvez montrer à vos parties prenantes non-InfoSec que l'accès au réseau n'est que la première étape d'une cyberattaque en vous appuyant sur les arguments présentés plus loin dans cet eBook. Plus l'entreprise fait en sorte qu'il soit difficile pour un pirate de rester infiltré, plus il est facile pour votre équipe de détecter l'invasion et de chasser le pirate pour de bon.

Gestion des privilèges

Délai d'efficacité

Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)



Description

La gestion des privilèges contrôle les profils des collaborateurs ayant besoin de permissions spécifiques sur leurs machines connectées au réseau ou personnelles. Par exemple, un employé de bureau aura besoin du statut de superadministrateur sur sa machine personnelle, mais n'a généralement pas besoin de permission d'installation de PowerShell.

Comment la protection fonctionne

Comme pour le contrôle des accès, si un pirate parvient à accéder à l'ordinateur de bureau d'un collaborateur (où ce dernier est connecté en tant que superadministrateur), il ne peut cependant pas déployer de nombreux outils de piratage ni obtenir un accès réseau plus large, en raison des permissions limitées.

Armez vos collaborateurs et avancez vos arguments

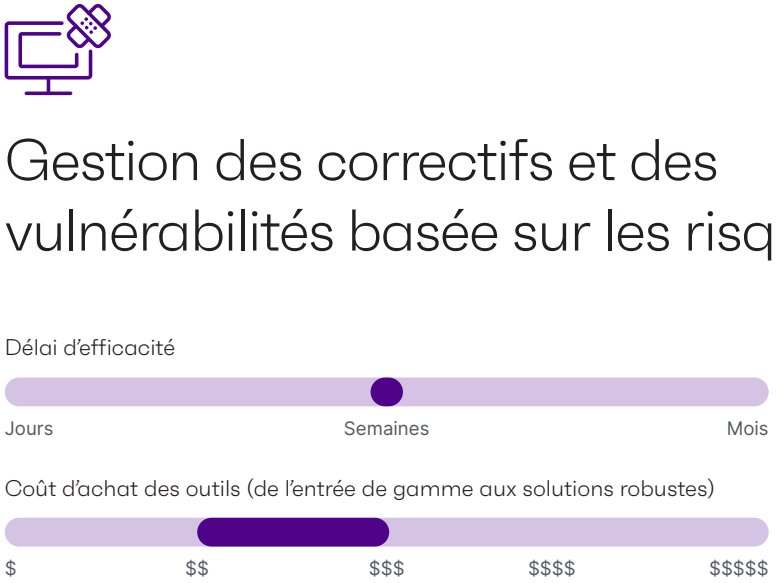
Pourquoi acheter aussi cet outil ?
Il va falloir plus de main-d'œuvre pour le déployer et le gérer !

Oui, en général, l'implémentation et la maintenance de programmes performants de gestion des privilèges demandent plus de travail, parce qu'ils nécessitent une supervision constante et des mises à jour au niveau de l'utilisateur. Ce besoin accru de maintenance est la raison pour laquelle ces outils sont généralement utilisés par les grandes entreprises ou celles des secteurs fortement réglementés.

Donc, si le coût ou le support interne de ce programme pose un problème à d'autres parties prenantes non-InfoSec, envisagez d'abandonner la discussion pour cette année. Ensuite, prêtez plus d'attention aux permissions initiales lors de l'onboarding, et évitez par principe d'accorder aux utilisateurs des permissions d'accès Administrateur.

Si plus de demandes (justifiées) d'exceptions à vos règles commencent à s'accumuler, rassemblez-les en vue de justifier le choix d'une solution de gestion des privilèges plus technique. À un certain stade, il devient économiquement judicieux d'investir dans un outil capable d'automatiser au moins une partie du processus.

Gestion des correctifs et des vulnérabilités basée sur les risques



Description

Ces outils identifient, priorisent et déploient les correctifs en fonction de l'environnement et des besoins de l'entreprise au lieu de les appliquer en fonction des scores externes de criticité des vulnérabilités ou des conseils de sécurité du fournisseur.

Comment cela vous protège

Les outils RBPM et RBVM aident les entreprises à traiter en priorité les correctifs et failles de sécurité les plus importants pour leurs périphériques et leur cas d'usage. Cela implique de mettre l'accent sur les faiblesses et vulnérabilités que les cybercriminels utilisent à ce moment précis !

Armez vos collaborateurs et avancez vos arguments

**On applique déjà des correctifs, non ?
En quoi est-ce différent cette fois-ci ?**

D'abord, confirmez que, oui, votre équipe applique déjà des correctifs. Et rappelez aux parties prenantes l'intérêt des exercices d'incendie. Souhaitez-vous continuer à fonctionner de façon réactive dans l'urgence à chaque fois qu'une menace fait la Une des journaux ? Le RBPM et le RBVM peuvent, respectivement, identifier proactivement les menaces importantes et leur appliquer des correctifs, avant que les pirates ne s'intéressent à vous.

Ensuite, mentionnez explicitement le schéma d'attaque des pirates qui ont ciblé des entreprises comme la vôtre, afin de préciser point par point comment l'application de correctifs pour les vulnérabilités exploitées ou plus anciennes aurait bloqué ces attaques bien plus tôt.

Enfin, soulignez qu'il est impossible de réaliser une telle application de correctifs manuellement. Seuls les outils RBPM et RBVM sont capables de déterminer automatiquement les exploitations les plus importantes pour votre environnement de menaces spécifiques et de vérifier si vos périphériques et données sont protégés !

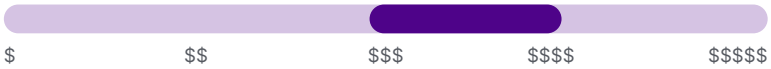
Pourquoi payer pour ces outils alors qu'il existe des logiciels gratuits d'application automatique des correctifs ?

Précisez que les outils de gestion des vulnérabilités basée sur les risques peuvent agir sur les points de contact qui intéressent les acteurs malveillants mentionnés dans cet eBook. L'investissement dans des outils RBPM et RBVM peut donc prévenir plusieurs cyberattaques, même si vous ne savez pas qu'un pirate s'est introduit dans le système.

Audits des programmes de sécurité

Délai d'efficacité

Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)



Description

L'audit des programmes de sécurité couvre un large éventail de services. Cependant, on peut le résumer ainsi : des consultants ou analystes tiers s'assurent que vos solutions et programmes de cybersécurité fonctionnent bien, vérifient que vos environnements et rôles ne présentent aucun problème, et déterminent si des ajustements sont nécessaires. Cela peut notamment inclure des tests d'intrusion et la formation des collaborateurs à l'hameçonnage.

Comment la protection fonctionne

En toute franchise, les personnes impliquées dans un programme ou projet ont rarement conscience de ses faiblesses et défauts. Très souvent, un audit de sécurité externe mené par un fournisseur de confiance est votre seul moyen de savoir si votre programme de sécurité fonctionne réellement comme prévu.

Un audit en profondeur peut aussi révéler des anomalies, ou des intrusions dormantes dues à des menaces internes ou externes. Un audit permet également de régler les points en suspens et les détails aléatoires qui n'ont pas été rapprochés ou réalignés sur leur rôle actuel.

Armez vos collaborateurs et avancez vos arguments

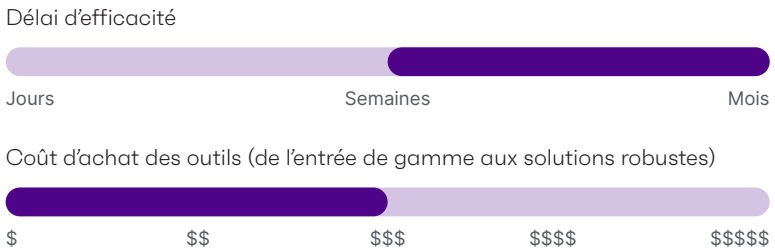
**Est-ce qu'on ne vient pas de faire un audit ?
Pourquoi payer pour un autre ?**

La fréquence des audits est plus élevée pour les environnements, les partenaires et les fournisseurs à haut risque. Plus un environnement comporte de connexions à des systèmes vitaux ou à des cibles connues des acteurs malveillants (organismes publics ou sous-traitants militaires par exemple), plus les pirates sont susceptibles de tenter d'accéder à cet environnement.

Des audits fréquents permettent par ailleurs de repérer un hacker à l'affût, qui collecte des informations avant de lancer l'attaque proprement dite. L'identification précoce des acteurs malveillants les plus experts peut permettre à votre entreprise d'économiser des millions de dollars en perte de données ou de réputation, et en frais juridiques.

Automatisation stratégique

et plus précisément, alertes et demandes de permission



Description

Dans le présent contexte, nous parlons d'alertes automatisées pour les activités non souhaitées ou inattendues, comme les demandes de permission bizarres ou inhabituelles. L'automatisation facilite également les activités quotidiennes des programmes de sécurité généraux.

Comment la protection fonctionne

Une entrée de journal d'événements peut passer inaperçue, même pour un professionnel de la sécurité obsédé du détail. Cependant, ce même événement peut déclencher un seuil d'alerte afin de prévenir l'équipe de remédiation appropriée, et lancer automatiquement un processus transparent d'analyse et de remédiation.

Comme les menaces deviennent plus complexes et que les responsabilités de l'équipe InfoSec s'étendent, l'automatisation aide vos équipes de sécurité débordées et en sous-effectif à accomplir leur mission en assurant la protection de l'entreprise.

Armez vos collaborateurs et avancez vos arguments

Pourquoi payer pour des outils d'automatisation ?

Souvent, l'achat de solutions plus automatisées s'avère moins coûteux et plus efficace que l'embauche de spécialistes en cybersécurité. Encore faut-il trouver des candidats qualifiés pour le poste.

Souvent, l'automatisation est une fonction essentielle d'un autre outil. Cette valeur ajoutée peut justifier le choix d'une solution ou d'un outil plutôt qu'un autre.

On a déjà fait une tentative d'automatisation, et ça a tout cassé.

Soulignez pour les parties prenantes inquiètes que l'automatisation ne remplace pas le jugement humain, et qu'elle ne sera jamais déployée sans réflexion, sans test ou sans souci de perturber les processus métiers.

Dans cet objectif, lorsque vous émettez votre demande, répertoriez exactement ce que l'automatisation va faire et ne pas faire, pour clarifier les attentes et apaiser tout le monde.

Pourquoi est-ce qu'on soumet encore des tickets pour les demandes d'accès ? (« Peut-on automatiser tel service ? »)

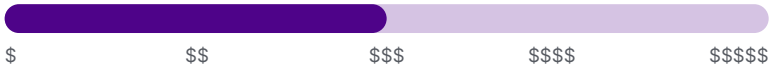
Même si l'automatisation allège en partie le travail administratif, les pirates peuvent (et vont) tirer parti des systèmes entièrement automatisés.

Par exemple, ils peuvent tromper un processus de demandes d'accès entièrement automatisé afin d'obtenir des permissions d'accès plus élevées et d'atteindre une plus grande portion du réseau. L'œil humain permet de repérer et de stopper cette escalade.

Contrôle des accès utilisateur

Délai d'efficacité

Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)



Description

Les outils de contrôle des accès utilisateur gèrent proactivement la liste des collaborateurs et des intitulés de poste qui ont besoin d'accéder à telle ou telle portion du réseau et à des applications pour leur travail. Ces outils permettent aussi de supprimer les anciennes permissions d'accès au fur et à mesure que les responsabilités et les rôles évoluent.

Comment la protection fonctionne

Même si un pirate obtient les références d'authentification d'un collaborateur, les contrôles d'accès des utilisateurs autorisent uniquement ce pirate à accéder à ce qui est accessible pour le collaborateur en question, et pas à tous les fichiers ou serveurs de données possibles. Le contrôle des accès utilisateur peut aussi vous avertir des demandes d'accès inhabituelles ou des tentatives d'intrusion, en vous prévenant très tôt des mouvements latéraux de pirates jusqu'alors invisibles.

Armez vos collaborateurs et avancez vos arguments

Pourquoi le contrôle des accès utilisateur coûte-t-il si cher ?

En général, les outils de contrôle des accès utilisateur fonctionnent selon le modèle de « paiement par tête ». Ainsi, plus votre entreprise est grande, plus le coût global augmente. Et vous devrez aussi prévoir une évolution du budget alloué chaque année, selon que votre entreprise prévoit ou non de s'agrandir ou de mutualiser ses opérations.

Essayez de reformuler la question en termes d'assurance par individu. Quelle somme par personne la partie prenante serait-elle prête à payer pour éviter le risque de voir sa propriété intellectuelle mise à nue et ses dossiers clients publiquement exposés par simple faute d'un collaborateur qui aurait accidentellement divulgué ses authentifiants ?

Je n'ai plus accès à ce dont j'ai besoin !

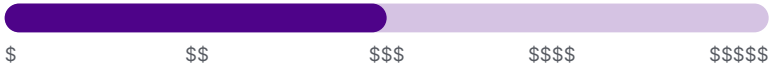
Pour vos parties prenantes non-InfoSec, essayez de simplifier le processus de soumission d'une demande de changement de permissions et rendez-le aussi intuitif que possible.

Rappelez à votre équipe d'être aussi patiente que possible face aux plaintes… surtout au début ! Pour minimiser la plupart de ces plaintes, vous pouvez proactivement impliquer des responsables de tous les départements dans le processus d'implémentation, en tant que consultants sur le projet, pour qu'ils vous disent qui a besoin d'accéder à telle ou telle application, et vous expliquent leurs workflows généraux.

Formation et sensibilisation des utilisateurs

Délai d'efficacité

Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)



Description

Il existe plusieurs façons de former et sensibiliser les collaborateurs non-InfoSec. Cela va des modules de formation de base aux exercices sur table et aux simulations immersives.

Comment la protection fonctionne

L'homme est le maillon faible de toute chaîne de sécurité. Aucune technologie au monde ne peut empêcher les accidents de sécurité déclenchés par des personnes, même les mieux intentionnées. C'est grâce à la formation que les employés pourront assurer et renforcer leur propre cybersécurité par une meilleure compréhension de l'environnement de sécurité de l'organisation dans son ensemble.

Armez vos collaborateurs et avancez vos arguments

Comment mettre en oeuvre efficacement la formation ?

Incitez les collaborateurs non-InfoSec à tirer profit de leur formation, informez-les des attaques qu'ils ont personnellement aidé à prévenir, comme lorsqu'ils signalent une attaque par hameçonnage.

Vous pouvez aussi appliquer des protocoles de sécurité sains en finançant des gestionnaires de mots de passe.

En règle générale, évitez de sanctionner les collaborateurs qui ne respectent pas les règles de conformité. Il vaut mieux délibérément souligner et féliciter les comportements conformes, pour que la sécurité devienne une responsabilité collective.

Pourquoi former des utilisateurs à la sécurité coûte-t-il si cher ?

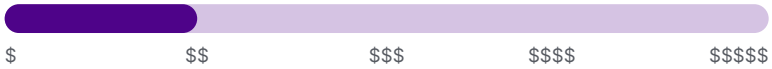
Pour être efficace, une formation à la cybersécurité doit être interactive, s'appuyer sur des contenus de haute qualité allant jusqu'aux scripts personnalisés. Ces modules de formation sont difficiles à concevoir et peuvent donc être assez onéreux.

Cependant, plus l'utilisateur considère que sa formation est interactive et pertinente, plus il s'investit personnellement et mémorise son contenu. Il pourra donc mettre en pratique ses connaissances en cybersécurité au moment où cela sera nécessaire.

Restrictions de contenu Web

Délai d'efficacité

Coût d'achat des outils (de l'entrée de gamme aux solutions robustes)



Description

Ces outils limitent les éléments que les utilisateurs peuvent consulter ou auxquels ils peuvent accéder en ligne lorsqu'ils travaillent sur un périphérique protégé.

Comment cela vous protège

Les pirates et autres acteurs malveillants peuvent router des données et du matériel via une application en ligne. En limitant l'exposition à Internet, vous limitez l'exposition aux autres menaces, y compris les éventuels malwares et intrusions hors réseau qui pourraient « se cacher » dans le trafic Web.

Armez vos collaborateurs et avancez vos arguments

Pourquoi acheter un outil qui limite le contenu Web ?

En général, ce type d'outil est implémenté dans les environnements on-site fortement réglementés, en raison de la complexité de sa mise en œuvre (il faut trouver l'équilibre entre restrictions du contenu en ligne distrayant ou potentiellement dangereux, et besoins en ligne réels liés au travail) et de l'essor du télétravail.

Cela concerne généralement des administrations publiques, des hôpitaux, des centres d'appels et même des banques avec leurs guichets automatiques.

Cependant, si votre entreprise veut intervenir sur des marchés verticaux très réglementés, comme le secteur bancaire, la santé ou les services publics, il peut s'avérer utile d'investir dans des outils plus restrictifs.

Vous pouvez aussi constater que cela booste la productivité… mais faites attention à la façon dont vous présentez cet avantage. La productivité s'améliore uniquement si les collaborateurs conservent l'accès au contenu et aux ressources dont ils ont besoin pour travailler, et que leur accès aux sites distrayants est bloqué pendant les heures ouvrables.

Ces acteurs malveillants qui ont fait la Une en 2022

De nombreux incidents de cybersécurité se sont produits tout au long de l'année 2022, portés par des groupes criminels aux profils et aux motivations variés. Nous avons sélectionné ici quatre menaces identifiées, toutes extrêmement différentes.

Pour chacun de ces groupes, nous fournirons des exemples frappants pour appuyer vos objectifs de cybersécurité stratégique 2023… quel que soit le but que vous recherchez.

ivanti CSW Cyber SecurityWorks

Ces acteurs malveillants qui ont fait la Une en 2022

Dans cette section

ALPHV

Le groupe ALPHV (également appelé « BlackCat » et dernier avatar des gangs de pirates BlackMatter et DarkSide) est l'exemple type d'un groupe cybercriminel qui crée, vend et déploie un modèle de « ransomwares en tant que service » (RaaS).

Qu'est-ce que le RaaS ? Et pourquoi vos parties prenantes doivent-elles s'en inquiéter ?

Dans le modèle RaaS, l'organisation tire une partie de ses revenus de la vente de packages logiciels de piratage directement sur le Dark Web ou par des intermédiaires.

Un peu d'ingénierie sociale stratégique suffit à mettre un pied dans le système ou le réseau IT de la cible en se servant d'informations d'authentification compromises. Le RaaS chiffre alors tous les fichiers critiques : la victime recevra la clé en échange d'une rançon.

ALPHV prélève un pourcentage de « droit d'auteur » sur toutes les rançons sans intervenir directement, ce qui ne l'empêche pas par ailleurs de lancer directement des attaques. Le gang récupère alors toute la rançon.

Le RaaS se différencie des ransomwares ordinaires sur deux aspects :

1. ALPHV et les autres fournisseurs RaaS créent des packages et vendent leurs logiciels de ransomware. En d'autres termes, ils écrivent du code pour le compte d'autres criminels qui ne savent pas (ou ne veulent pas) le faire. Les risques de cyberattaques sur le terrain se multiplient de façon exponentielle.

   Ainsi, si on peut lancer une attaque sans savoir coder, n'importe qui de mal intentionné incarne une cyber menace.

2. Les acteurs étatiques, comme Nobelium, vont utiliser les attaques « prêtes à l'emploi » comme le RaaS de BlackCat pour espionner ou pour cibler d'autres pays. Ce recours au code d'autrui accélère leur force de frappe cyber, dissimule leur implication, et leur permet de réserver les attaques furtives à des cibles plus précieuses.

Certes, l'adoption et l'expansion du « modèle commercial » du RaaS sur le Dark Web démultiplient le nombre d'attaques ciblant toutes sortes d'organisations, d'entreprises et d'organismes publics, mais elles présentent également un avantage pour les équipes rompues à la sécurité.

> **Quel avantage ?** Si de nombreux acteurs malveillants utilisent des exploitations « prêtes à l'emploi » de même provenance ou presque avec des ransomwares identiques ou proches, quelques mesures préventives suffisent alors à bloquer un large éventail d'attaques.

Fiche statistique ALPHV

Alias :

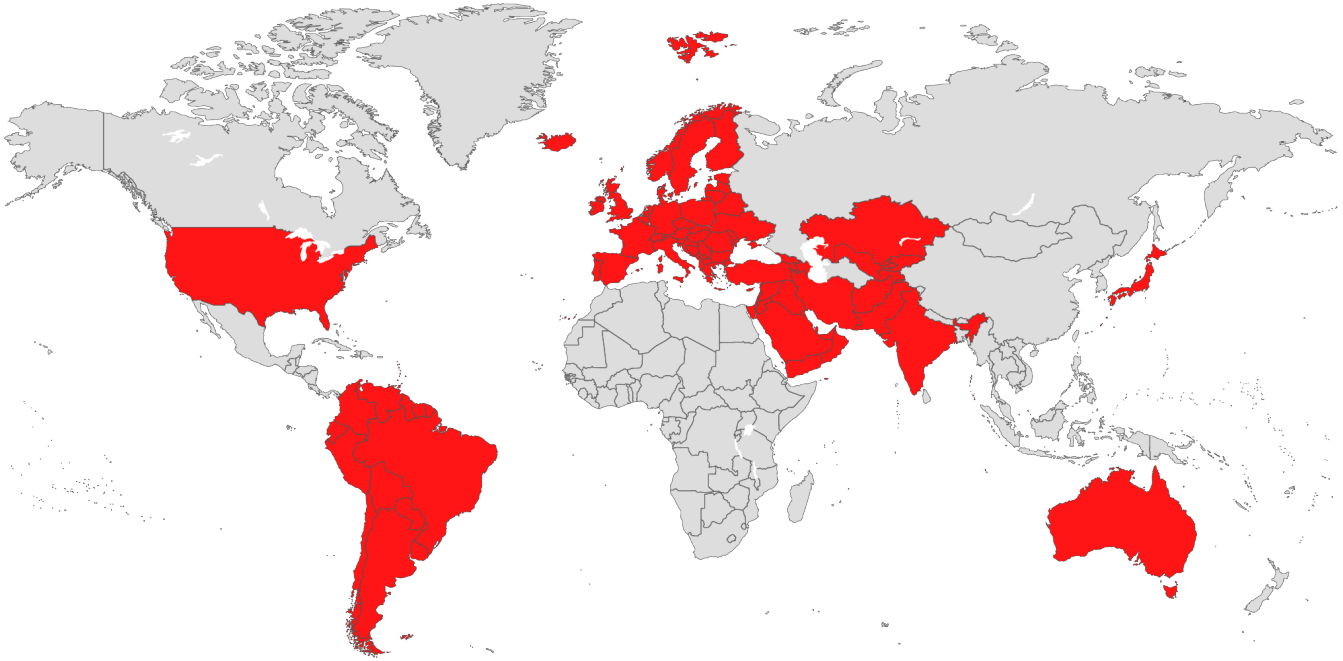
BlackCat
ALPHV
ALPHA
Noburus
AlphaVM

Motivation :

Criminel/Financier

Type de menace :

Gang RaaS (ransomware en tant que service)



Affiliations et associations :

Russie
Ryuk
Revil
DEV-0504
DEV-0237
FIN12
FIN7
Conti
BlackMatter
DarkSide

Exploitations favorites :

CVE-2016-0099
CVE-2019-7481
CVE-2021-31207
CVE-2021-34473
CVE-2021-34523

Zones ciblées connues :

Allemagne
Amérique du Sud
Australie
Autriche
États-Unis
Europe
Inde
Italie
Japon
Moyen-Orient
Suisse

Impact sur l'entreprise d'attaques ALPHV

> La coupure temporaire de nos services IT [...] a impacté les opérations de nos centres logistiques et les activités des services client.

23 décembre 2021 :
Moncler | Mode/Vente au détail | Milan

« Nos terminaux pétroliers fonctionnent en mode dégradé et nous avons déclaré l'état de force majeure [un événement externe, inévitable et imprévisible]. »

« L'incident affecte 233 stations-service dans le nord de l'Allemagne. Il est probablement possible de payer en liquide. »

29 janvier 2022 : Oiltanking + Mabanaft | Logistique | Allemagne

« Notre équipe IT travaille littéralement 24 heures sur 24 pour remédier à cette [attaque]. Je suis vraiment de tout cœur avec mes collègues qui accomplissent un travail herculéen pour remettre nos systèmes en marche et en état. »

7-11 mars 2022 : Université d'État A&T en Caroline du Nord | Éducation | États-Unis

« Nous garantissons que, sur les 3 000 postes de travail IT concernés, les premiers seront de nouveau disponibles quatre jours après l'attaque. [...] Comme l'on dépend des systèmes IT, l'Administration est en mode urgence. »

14 mai 2022 : Carinthie | Administration publique | Autriche

« Lorsqu'on lui a demandé si les données ont été chiffrées ou copiées par ALPHV, un porte-parole a répondu que l'entreprise s'en tiendrait à sa déclaration officielle. »

31 mai 2022 : CMC ELectronics | Militaire/Aéronautique | Canada

« Il est possible que des informations client [...] se soient trouvées sur les serveurs et PC piratés. Nous sommes en train d'identifier [...] les fuites potentielles et l'étendue des dommages, et enquêtons sur leur cause. »

3 juillet 2022 : Bandai Namco | Divertissement | Japon

« Nos systèmes sont restés inaccessibles pendant des jours : nous nous efforçons maintenant de rattraper le retard accumulé. »

22-23 juillet 2022 : Creos | Énergie | Luxembourg

« Nos installations devraient rester fermées lundi, sans date de réouverture prévue. [...]

Nous savons que nous sommes très vulnérables. »

17 août 2022 : Comté de Fremont | Administration publique | États-Unis

Stratégie de cyberdéfense contre ALPHV :

Comment bloquer les attaques ALPHV avant toute demande de rançon

Intrusion à l'aide d'informations d'authentification compromises

Empêcher les attaquants d'entrer sur le réseau est le moyen le plus simple, le plus économique et le plus rapide de protéger toutes les « business units » sans perturber les opérations.

- EDR
- Restriction du contenu Web
- Antivirus/Antimalware
- Anti-hameçonnage sur mobile
- Formation et sensibilisation des utilisateurs
- Authentification multifacteur (MFA) sans mot de passe
- Contrôle des accès utilisateur
- Contrôle des applications
- Hygiène et gestion des périphériques
- Audits des programmes de sécurité
- Automatisation stratégique
- Gestion des configurations

Cartographie des systèmes (informations et réseau)

Si les intrus sont gênés ou bloqués dans leurs déplacements sur le réseau, ils ne trouveront pas les données ou vulnérabilités importantes… ce qui réduit d'autant l'impact sur l'entreprise.

- Gestion des correctifs et des vulnérabilités basée sur les risques
- Segmentation des périphériques et du réseau
- Hygiène et gestion des périphériques
- Rapprochement des actifs
- Protocoles d'accès sécurisé
- Segmentation réseau
- Gestion des privilèges
- Automatisation stratégique
- Gestion des configurations

Ransomwares sur mesure en fonction des failles ou exploitations propres à la victime

Si les cybercriminels ne parviennent pas à lancer leur ransomware, ils ne peuvent pas verrouiller ni voler les données contre rançon.

- Gestion des correctifs et des vulnérabilités basée sur les risques
- Contrôle des applications
- Contrôle des accès utilisateur
- Gestion des privilèges
- Hygiène et gestion des périphériques
- Automatisation stratégique

Arrêt des programmes de sécurité pour les empêcher de bloquer le ransomware ou de supprimer les données.

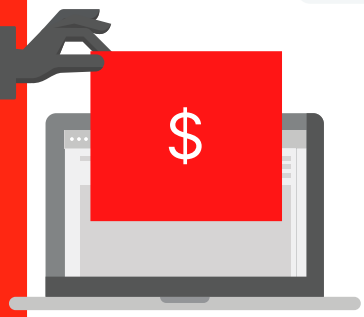
La détection des comportements inhabituels peut signaler les prémices d'une attaque par ransomware avant tout arrêt des activités ou toute demande de rançon.

- Contrôle des applications
- Automatisation stratégique
- Contrôle des accès utilisateur

Chiffrement des fichiers et exfiltration des données (copie voire suppression) pour exercer des pressions sur la victime.

S'ils n'arrivent pas à voler ou verrouiller des données, les escrocs n'auront pas de moyen de coercition pour exiger une rançon.

- Détection et isolement du chiffrement malveillant
- Segmentation des périphériques et du réseau
- Restriction du contenu Web



Trop tard pour la prévention, il faut passer en mode « récupération après sinistre ».

APT29

Les pirates tristement célèbres qui ont fait fuiter les e-mails et documents internes du Comité national démocrate, APT29 (ou « Nobelium »), forment un groupe cyber lié à la branche étranger du service d'espionnage et de renseignement russe.

Acronyme d'« Advanced Persistent Threat » (menace avancée persistante), le terme APT désigne souvent un acteur malveillant sponsorisé par un État, capable de pénétrer dans le réseau d'une entreprise et de s'y dissimuler pendant des mois voire des années avant toute détection ou attaque.

Pourquoi vos parties prenantes devraient-elles s'inquiéter d'APT29 si vous n'êtes pas un organisme public ?

Quand elles découvrent les liens étroits entre les acteurs malveillants à la Une de l'actualité et les services secrets russes, certaines parties prenantes non-InfoSec sont tentées d'ignorer la menace.

« Pourquoi APT29 s'intéresserait-il à nous , disent-elles. Nous ne sommes pas un organisme public ! On ne participe à aucun effort de guerre ! »

Hélas, le monde est petit.

De nombreuses études sur les réseaux sociaux (des thèses de doctorat aux recherches Facebook de Meta, en passant par les jeux de mèmes avec l'acteur Kevin Bacon) examinent les liens d'une personne à l'autre dans des populations de différentes tailles. La « distance » moyenne entre un point de départ quelconque et la « destination » finale semble être d'environ trois à quatre connexions.

Intégrons maintenant ce scénario hypothétique à votre argumentaire en faveur d'une stratégie de cybersécurité proactive.

Même si votre entreprise n'est ni un organisme public ni une ONG militante en désaccord avec la Russie, des acteurs malveillants peuvent la viser en tant qu'intermédiaire (ou relation de relation de relation) vers leur cible finale dans le cadre d'une attaque par la supply chain, en vue de provoquer une crise et de récupérer des informations.

Prenons l'exemple du célèbre incident SolarWinds, une attaque d'APT29 en 2020.

Les pirates APT29 n'ont pas ciblé directement les organismes publics ou les infrastructures critiques. Ils ont choisi d'infecter l'éditeur de logiciel d'un sous-traitant, à savoir une plateforme logicielle de surveillance réseau, pour installer des portes dérobées chez quelques 18 000 clients, dont certains publics, via une mise à jour logicielle de routine.

APT26 ne ciblait pas l'ensemble de ces 18 000 clients, mais tous ont été piratés… et tous sont devenus vulnérables parce que pris dans une cyberguerre invisible entre des nations puissantes.

Par conséquent, si l'une de vos parties prenantes non-InfoSec rechigne à se prémunir contre APT29 ou tout autre groupe de menaces avancées persistantes, parce qu'on est neutre ou civil, testez la théorie des 6 degrés de séparation sous forme d'exercice sur table ou d'activité en atelier.

Mais cette fois, faites-le sous l'angle des connexions de votre entreprise avec la Russie.

Statistiquement parlant, votre entreprise risque bien plus d'être la cible d'APT29 (ou de tout autre groupe APT) que vos parties prenantes non-InfoSec ne le pensent.

Fiche statistique APT 29

Alias :

Nobelium	Cozy Bear	UNC-1151
YTTRIUM	CozyDuke	Cloaked Ursa
The Dukes	UAC-0113	

Motivation :

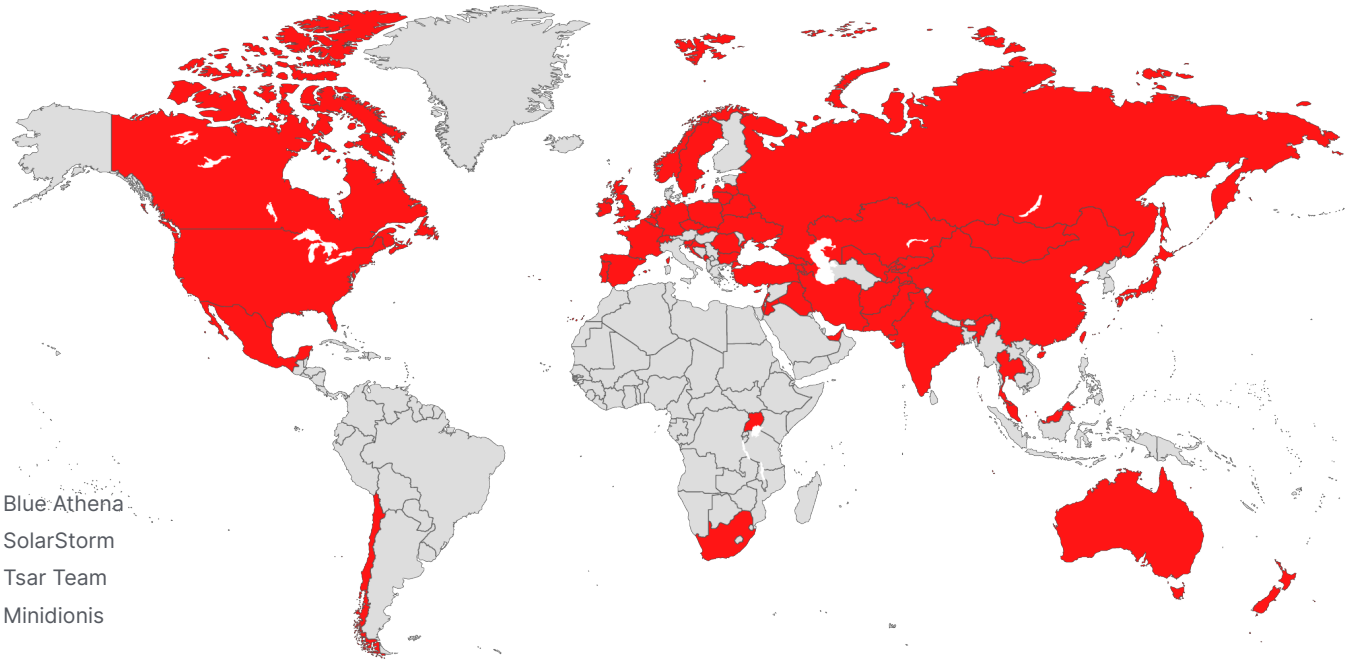
Espionnage/Opérations couvertes

Type de menace :

APT (Advanced Persistent Threat - Menace avancée persistante)

Affiliations et associations :

Russie	APT28	Actinium	Blue Athena
Conti	Strontium	Bromine	SolarStorm
ALPHV	Iridium	Krypton	Tsar Team
Fighting Ursa	DEV-0586	StellarParticle	Minidionis



Exploitations favorites :

CVE-2009-3129	CVE-2019-17026	CVE-2020-14882
CVE-2014-1761	CVE-2019-19781	CVE-2020-4006
CVE-2015-164	CVE-2019-2725	CVE-2020-5902
CVE-2018-13379	CVE-2019-7609	CVE-2021-1879
CVE-2019-11510	CVE-2019-9670	CVE-2021-21972
CVE-2019-1653	CVE-2020-0674	CVE-2021-26855

Secteurs critiques en danger :

Administration	Médias et télécommunications	Éducation supérieure
Armée		Finances
Énergie	ONG et organisations à but non lucratif	Recherche/Groupes de réflexion
IT		
Transports	Santé	

Zones ciblées connues :

Afghanistan	Chili	Hongrie	Liban	Ouzbékistan	Suède
Afrique du Sud	Chine	Inde	Lituanie	Pakistan	Suisse
Allemagne	Chypre	Iran	Luxembourg	Pays-Bas	Tadjikistan
Arménie	Corée du Sud	Iraq	Malaisie	Pologne	Tchétchénie
Australie	Croatie	Irlande	Mexique	Portugal	Thaïlande
Azerbaïdjan	Émirats arabes unis	Israël	Mongolie	République Tchèque	Turquie
Belgique		Japon	Monténégro	Roumanie	Ukraine
Biélorussie	Espagne	Jordanie	Norvège	Royaume-Uni	
Brésil	États-Unis	Kazakhstan	Nouvelle Zélande	Russie	
Bulgarie	France	Kirghizistan		Slovaquie	
Canada	Géorgie	Lettonie	Ouganda	Slovénie	

Impact sur l'entreprise d'attaques APT29

> Les e-mails d'hameçonnage envoyés par APT29 se sont fait passer pour des mémos administratifs liés à différentes ambassades. Ils utilisaient des adresses e-mail légitimes que le groupe s'était appropriées.

Attaque débutée le 17 janvier 2022, dévoilée le 28 avril 2022 : Organes diplomatiques | Europe, Asie, Amérique du Nord

« Ces acteurs malveillants [dont APT29] tirent parti de mots de passe trop simples, de systèmes non corrigés et des collaborateurs peu méfiants pour obtenir l'accès initial. Ils se déplacent ensuite latéralement sur le réseau pour s'y dissimuler durablement et exfiltrer des données. »

Attaque débutée en janvier 2020, dévoilée le 16 février 2022 : Sous-traitants militaires | États-Unis

« Les administrateurs ont trouvé les PC verrouillés affichant une demande de rançon de 10 000 dollars en bitcoins, mais le disque dur de ces machines était irrévocablement endommagé après redémarrage. »

13 janvier 2022 : Administration, Organisations non gouvernementale & IT | Ukraine

« Depuis début mai, Cloaked Ursa [APT29] n'a cessé de faire évoluer ses capacités de diffusion de malwares au travers de services courants de stockage en ligne, y compris Dropbox et Google Drive. »

Attaque débutée en mai 2022, dévoilée le 5 juillet 2022 : Ambassades étrangères | Portugal et Brésil

« Dès mai 2021, des cyberacteurs parrainés par l'État russe ont profité d'un compte mal configuré défini par défaut sur les protocoles MFA dans une organisation non gouvernementale (ONG). Ils ont ainsi pu inscrire un nouveau périphérique pour le MFA et accéder au réseau de la victime. »

Attaque débutée en mai 2021, dévoilée le 15 mars 2022 : Organisation non gouvernementale | États-Unis

« Le risque de cyberattaque augmente, avec de graves conséquences même pour les pays et les entreprises qui ne sont pas ciblés directement [par les campagnes de la Russie]. »

18 février 2022 : « Opérateurs de services essentiels », Nouvelle-Zélande

« Nous constatons l'utilisation notable continue de malwares de base accessibles au plus grand nombre, ce qui montre qu'UAC-0113 [APT29] adapte ses opérations et cherche à diversifier ses outils. »

Annoncé le 19 septembre 2022 : Services publics et secteur privé | « Zones géographiques multiples »

Stratégie de cyberdéfense contre APT29 :

Comment bloquer les attaques APT29 avant toute détection ou suppression

Intrusion dans le réseau par des campagnes d'hameçonnage ou par des prestataires infectés dans votre supply chain.

Empêcher les attaquants d'entrer sur le réseau est le moyen le plus simple, le plus économique et le plus rapide de protéger toutes les « business units » sans perturber les opérations.

- EDR
- Restriction du contenu Web
- Antivirus/Antimalware
- Anti-hameçonnage
- Formation et sensibilisation des utilisateurs
- Authentification multifacteur (MFA) sans mot de passe
- Contrôle des accès utilisateur
- Contrôle des applications
- Hygiène et gestion des périphériques
- Audits des programmes de sécurité
- Automatisation stratégique
- Gestion des configurations

Accès aux profils Admin et/ou interception de paquets d'authentification pour élever les privilèges.

Limiter la capacité des intrus à élever leurs privilèges évite le vol de données et l'extorsion.

- Contrôle des accès utilisateur
- Gestion des privilèges
- Gestion des configurations
- Audits des programmes de sécurité
- Formation et sensibilisation des utilisateurs

Cartographie du réseau pour repérer les informations utiles et les faiblesses.

Si les intrus sont gênés ou bloqués dans leurs déplacements sur le réseau, ils ne trouveront pas les données ou vulnérabilités importantes… ce qui réduit d'autant l'impact sur l'entreprise.

- Gestion des correctifs et des vulnérabilités basée sur les risques
- Périphérique et segmentation
- Hygiène et gestion des périphériques
- Réconciliation des actifs
- Protocoles d'accès sécurisé
- Segmentation réseau
- Gestion des privilèges
- Automatisation stratégique
- Gestion des configurations

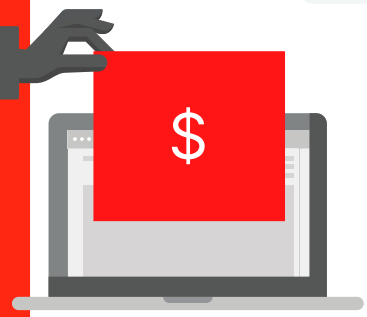
Présence furtive avec exfiltration de données et consolidation de l'ancrage notamment par effacement des journaux pour contrer les systèmes de défense en cas de découverte.

La détection des comportements inhabituels peut signaler les prémices d'une attaque par ransomware avant tout arrêt des activités ou toute demande de rançon.

- Audits des programmes de sécurité
- EDR
- Restriction du contenu Web
- Automatisation stratégique
- Détection et isolement du chiffrement malveillant

Attaque sur commande pour un maximum de confusion et d'impact.

Trop tard pour la prévention, il faut passer en mode « récupération après sinistre ».



Conti

Pour tout professionnel de la cybersécurité qui suit l'actualité des ransomwares, le nom « Conti » est familier. Autre acteur malveillant associé à la Russie voire activement sponsorisé par le pays, ce groupe de ransomware en tant que service (RaaS) a fait la une des journaux en février 2022 pour son « soutien total à la Russie » suite à l'invasion de l'Ukraine.

Mais, depuis que des dissidents ont publié le manuel de formation des affiliés et que des chercheurs en sécurité ont divulgué des documents internes sur Twitter, l'organisation criminelle « Conti » en tant que telle semble complètement dissoute.

En l'absence de gros titres récents pour les pousser à l'action, les parties prenantes non-InfoSec peuvent remettre en question votre stratégie de cybersécurité si vous évoquez la prévention contre les ransomwares Conti… mais vous, vous savez que ce n'est qu'un leurre pour vous détourner de la menace réelle.

Conti n'existe plus, pourquoi chercher à se prémunir contre d'anciennes attaques ?

Pour être honnête, la réputation de Conti a souffert un certain temps… ironiquement, à cause de la médiocrité de sa propre sécurité opérationnelle et du mauvais moral de ses troupes !

Sa dégringolade a commencé par la divulgation des manuels de formation des affiliés Conti. Le dernier clou dans le cercueil, c'est le jour où un spécialiste informatique ukrainien anonyme s'est introduit dans le réseau du gang et a fuité des années de documents internes.

Mais la « mort » de Conti ne signifie pas que ses membres ont pris leur retraite ou que le code malveillant s'est évaporé.

Après tout, Conti était une franchise tentaculaire. Ses affiliés étaient de toute évidence formés à l'utilisation d'un code de ransomware écrit et à des techniques qui restent des menaces pour toute entreprise où des vulnérabilités demeurent.

De plus, ce n'est pas comme si les pirates, les programmeurs et les spécialistes en ingénierie sociale de l'organisation avaient tous été arrêtés ou tués.

En fait, deux mois pleins après la fermeture des serveurs Conti, le Département d'État des États-Unis annonçait dans une nouvelle vidéo une récompense de 10 millions de dollars pour toute information menant à l'arrestation d'un pirate « Conti ».

Récemment, des chercheurs et des analystes en cybersécurité ont reconnu des tactiques de type Conti chez d'autres gangs cybercriminels, notamment :

- BlackByte
- Karakurt
- BlackBasta
- HelloKitty
- AvosLocker
- Hive
- ALPHV – and others!

Les entreprises proactives d'aujourd'hui peuvent tirer les leçons d'anciens incidents Conti pour empêcher une multitude d'attaques apparentées par des acteurs malveillants de moindre envergure qui suivent les mêmes tactiques.

Fiche statistique Conti

Alias :

N'est plus disponible

Motivation :

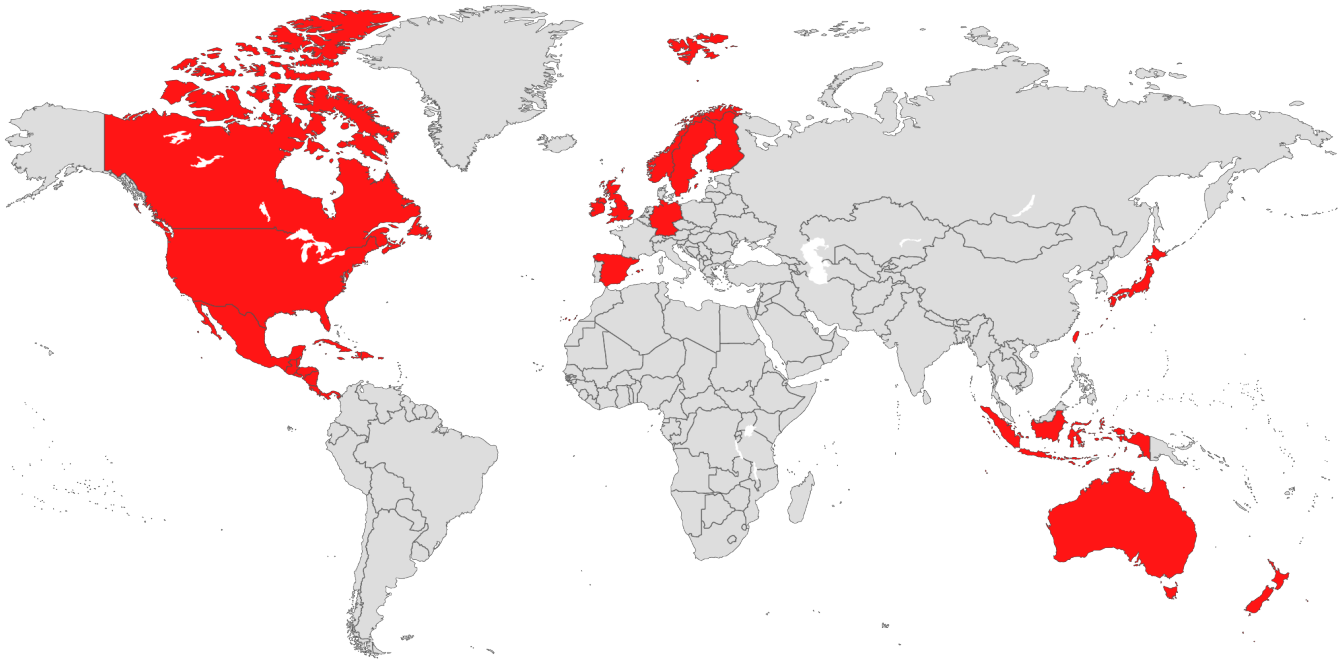
Criminel/Financier

Type de menace :

RaaS (Ransomware en tant que service)

Affiliations et associations :

Russie	BlackBasta	Hive
BlackByte	HelloKitty	AvosLocker
Karakurt	ALPHV	Wizard Spider



Secteurs critiques en danger :

Administration	Hôtellerie	Éducation
Finances	Finances	Alimentation
Énergie	Technologie	Vente et eCommerce
Fabrication	Santé	

Exploitations favorites :

CVE-2017-0143	CVE-2018-13379	CVE-2021-44228	CVE-2019-1069	CVE-2019-1388	CVE-2021-21972
CVE-2017-0144	CVE-2020-0796	CVE-2015-2546	CVE-2019-1129	CVE-2019-1405	CVE-2021-21985
CVE-2017-0145	CVE-2020-1472	CVE-2016-3309	CVE-2019-1130	CVE-2019-1458	CVE-2021-22005
CVE-2017-0146	CVE-2021-1675	CVE-2017-0101	CVE-2019-1215	CVE-2020-0609	CVE-2021-26855
CVE-2017-0147	CVE-2021-31207	CVE-2018-8120	CVE-2019-1253	CVE-2020-0638	
CVE-2017-0148	CVE-2021-34473	CVE-2019-0543	CVE-2019-1315	CVE-2020-0688	
CVE-2018-12808	CVE-2021-34523	CVE-2019-0841	CVE-2019-1322	CVE-2020-0787	
CVE-2018-13374	CVE-2021-34527	CVE-2019-1064	CVE-2019-1385	CVE-2021-1732	

Zones ciblées connues :

Allemagne	Indonésie
Amérique latine	Irlande
Australie	Japon
Canada	Nouvelle-Zélande
Costa Rica	Royaume-Uni
Espagne	Scandinavie
États-Unis	Taïwan

Impact sur l'entreprise d'attaques Conti

Sur les 65 000 ordinateurs du réseau de Delta Electronics, environ 1 500 serveurs et 12 000 ordinateurs ont été chiffrés. […] L'incident s'est produit il y a presque une semaine et le site Web de Delta n'est toujours pas en ligne. Les pertes définitives pourraient dépasser les prévisions.

21 janvier 2022 : Delta Electronics | Fabrication | Taïwan

« […] Conti a chiffré plus de 4 000 périphériques et 120 serveurs VMware ESXi appartenant à Shutterfly. Une page de données privées fuitée montrait également des échantillons des données volées à Shutterfly, dont, nous dit-on, des contrats, des coordonnées bancaires et des informations de comptes de revendeurs, […] et apparemment des informations clients, dont les quatre derniers chiffres des numéros de carte bancaire. »

Attaque du 3 décembre 2021 – Signalée le 26 décembre 2021 : Shutterfly | Vente et eCommerce | États-Unis

« Nous savons que BI a subi une attaque par ransomware le mois dernier. Nous avons été frappés par une cyberattaque. C'est un crime, c'est la réalité, et nous y sommes exposés. »

Attaque de décembre 2021 – Signalée le 20 janvier 2022 : Bank of Indonesia | Finances | Indonésie

« À ce stade, nous ne pouvons pas traiter les commandes ni expédier les marchandises en toute sécurité. Nos équipes travaillent à résoudre le problème, mais sans pouvoir donner de délai. »

28 janvier 2022 : KP Snacks | Alimentation | Royaume-Uni

« Pour protéger les actifs de nos clients, l'accès à distance depuis l'infrastructure IT du groupe Nordex a été désactivée pour les turbines sous contrat. […] L'entreprise continue à réparer ses systèmes IT pour assurer la continuité des opérations et retrouver un fonctionnement normal dès que raisonnablement possible. »

31 mars 2022 : Nordex | Fabrication/Énergie | Allemagne

« Christian Rucavado, directeur général de la Chambre du commerce extérieur du Costa Rica, a déclaré que l'attaque contre l'Agence des douanes avait effondré la logistique d'importation et d'exportation du pays. Il a décrit une course contre la montre pour les denrées périssables bloquées dans des entrepôts frigorifiques et a déclaré qu'il n'y avait pas encore d'estimation des pertes économiques. »

18 avril 2022 : Ministère des finances, du travail et de la sécurité sociale | Costa Rica

GROUPE DÉMANTELÉ EN JUIN 2022

Stratégie de cyberdéfense contre l'héritage de Conti :
Comment bloquer les attaques de type Conti avant toute demande de rançon

Intrusion dans le réseau via des campagnes d'hameçonnage, des pare-feux trop faibles et/ou des serveurs ou périphériques mal configurés connectés à Internet.

Empêcher les attaquants d'entrer sur le réseau est le moyen le plus simple, le plus économique et le plus rapide de protéger toutes les « business units » sans perturber les opérations.

- EDR
- Restriction du contenu Web
- Antivirus/Antimalware
- Anti-hameçonnage sur mobile
- Formation et sensibilisation des utilisateurs
- Authentification multifacteur (MFA) sans mot de passe
- Contrôle des accès utilisateur
- Contrôle des applications
- Hygiène et gestion des périphériques
- Audits des programmes de sécurité
- Automatisation stratégique
- Gestion des configurations

Obtention de privilèges d'administration sur les comptes d'utilisateur de l'attaquant qui fait passer dès le départ ses activités pour des opérations légitimes.

Limiter la capacité des intrus à élever leurs privilèges évite le vol de données et l'extorsion.

- Contrôle des accès utilisateur
- Gestion des privilèges
- Gestion des configurations
- Audits des programmes de sécurité
- Formation et sensibilisation des utilisateurs

Cartographie du réseau pour repérer les informations stratégiques et les faiblesses.

Si les intrus sont gênés ou bloqués dans leurs déplacements sur le réseau, ils ne trouveront pas les données ou vulnérabilités importantes… ce qui réduit d'autant l'impact sur l'entreprise.

- Gestion des correctifs et des vulnérabilités basée sur les risques
- Périphérique et segmentation
- Hygiène et gestion des périphériques
- Réconciliation des actifs
- Protocoles d'accès sécurisé
- Segmentation réseau
- Gestion des privilèges
- Automatisation stratégique
- Gestion des configurations

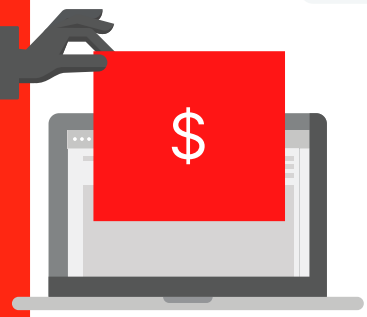
Exfiltration des données à utiliser dans le cadre d'une extorsion.

S'ils n'arrivent pas à voler ou verrouiller des données, les escrocs n'auront pas de moyen de coercition pour exiger une rançon.

- Audits des programmes de sécurité
- EDR
- Restriction du contenu Web
- Automatisation stratégique
- Détection et isolement du chiffrement malveillant

Lancement du ransomware et demande de rançon, éventuellement accompagnée d'une attaque DDoS pour extorquer le paiement.

Trop tard pour la prévention, il faut passer en mode « récupération après sinistre ».



Lapsus$

Comme pour Conti, tout le monde pensait que l'arrestation en mars 2022 à Londres du leader du groupe, un pirate de 16 ans surnommé « White » ou « Breachbase », marquait la fin de Lapsus$.

Mais à peine quelques mois plus tard, de grandes entreprises attribuaient d'anciennes fuites de données au gang que l'on croyait éteint. Et de nouvelles infiltrations au sein de grandes entreprises technologiques ont fait les gros titres !

Comme pour Conti, cette réincarnation venue de nulle part de Lapsus$ peut aider à convaincre vos parties prenantes non-InfoSec que les cybermenaces même « mortes » représentent un danger.

Toutefois, si nous parlons ici de Lapsus$, c'est que ce groupe est particulier par sa motivation et sa méthode d'infiltration.

Effectivement, la principale motivation de Lapsus$ n'est pas l'argent, même si l'on sait qu'il a volé des informations contre rançon et extorqué des millions à des entreprises.

En fait, les attaquants Lapsus$ semblent plutôt mus par la curiosité : « Est-ce que je vais y arriver ? »… et par l'attention que les jeunes cherchent à attirer depuis toujours.

Pourquoi une bande d'adolescents pirates devrait-elle inquiéter vos parties prenantes ?

Pour convaincre vos parties prenantes d'investir dans le blocage des attaques Lapsus$, commencez par leur montrer à quel point leur méthode d'infiltration et d'attaque est différente.

Sans argent et sans relations, ces jeunes pirates, à l'inverse des autres acteurs malveillants adultes cités ici, n'avaient pas de temps à consacrer à une entreprise criminelle, ils n'y travaillaient pas à temps plein pour en tirer leur revenu.

À la place, les pirates Lapsus$ ont exploité un outil à leur portée pour infiltrer les entreprises : les réseaux sociaux.

Sur sa chaîne Telegram publique, le groupe Lapsus$ a annoncé qu'il cherchait des identifiants de connexion et d'autres informations piratables de grandes entreprises ou organisations pour y prendre pied, et éventuellement contre un paiement en cryptomonnaie si l'indicateur le souhaitait.

Et apparemment, des collaborateurs mécontents en ont profité.

Dans les semaines et les mois qui ont suivi la publication Telegram d'origine, plusieurs grandes entreprises ont annoncé des fuites, qu'elles attribuaient au gang Lapsus$.

Une fois obtenu l'accès à une entreprise, les pirates se déplaçaient latéralement dans le système aussi loin que possible… jusqu'à hameçonner en interne des collaborateurs et départements IT à l'aide des informations d'authentification compromises. Ils accédaient ainsi à des lecteurs partagés, espionnaient des réunions à l'arrière-plan et découvraient des documents de mots de passe non chiffrés.

Les attaquants Lapsus$ pouvaient alors exporter ces données, les supprimer et contempler de l'intérieur le chaos qu'ils avaient provoqué. Ils pouvaient envoyer leurs demandes de rançon sur les canaux de communication internes !

Si vos collaborateurs ont le moral en berne et que vos parties prenantes non-InfoSec n'assument pas leur rôle dans la cybersécurité, ils incarnent alors une grave « menace interne » pour la sécurité opérationnelle de votre entreprise (en interne et en externe), comme le montrent les schémas d'attaque de Lapsus$.

Fiche statistique Lapsus$

Alias :

sans objet

Motivation :

Hacktivisme, motif financier

Type de menace :

Pirates généralistes

Affiliations et associations :

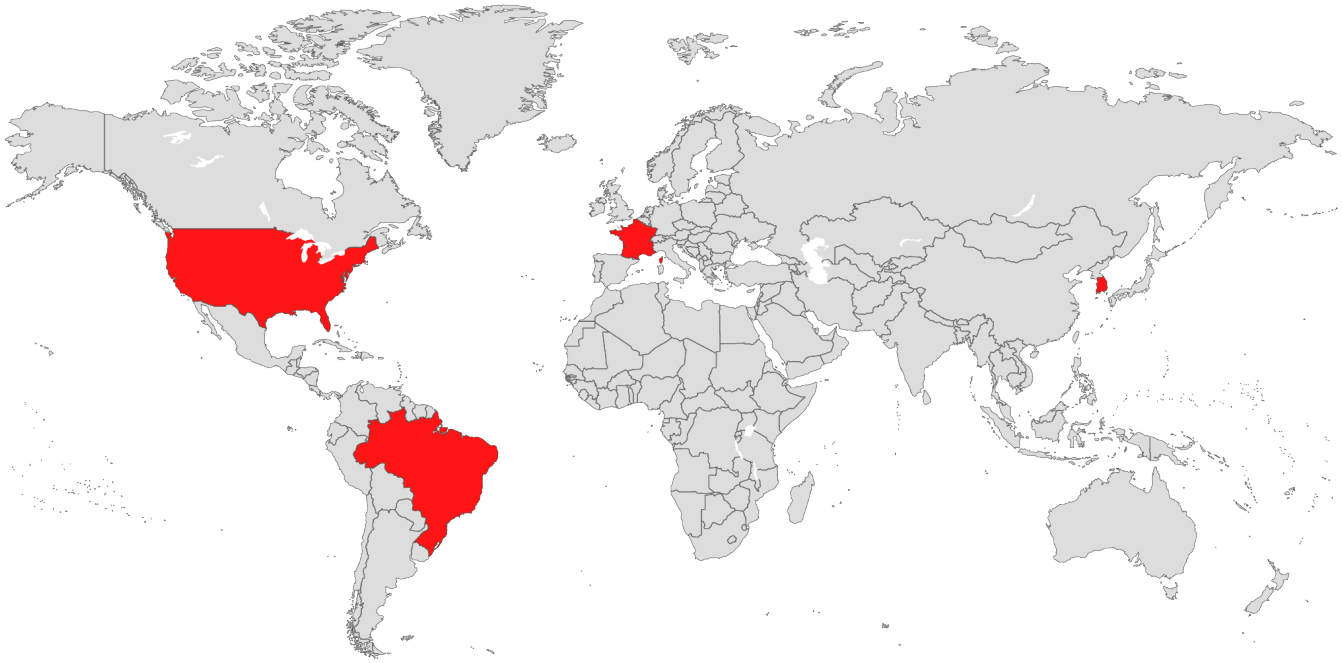
UNC2447

Yanluowangr

Secteurs critiques en danger :

Divertissement

Technologie



Exploitations favorites :

CVE-2021-34484
CVE-2018-13379
CVE-2020-12812
CVE-2020-23852
CVE-2021-26857
CVE-2021-31207
CVE-2021-44864
CVE-2021-44957
CVE-2021-45326
CVE-2021-45328
CVE-2022-0510
CVE-2022-21702
CVE-2022-0139
CVE-2021-45327
CVE-2021-45325
CVE-2021-44956
CVE-2021-34473
CVE-2021-26858
CVE-2021-26855
CVE-2020-23705
CVE-2019-5591
CVE-2021-34484
CVE-2022-21919
CVE-2022-26904
CVE-2021-34484

Zones ciblées connues :

Brésil
Corée du Sud
France
États-Unis

Impact sur l'entreprise d'attaques Lapsus$

"L'attaquant a ensuite tenté à maintes reprises de se connecter au compte Uber du sous-traitant. À chaque fois, le sous-traitant a reçu une demande d'approbation de connexion à deux facteurs, ce qui, au début, a bloqué l'accès. Mais il en a finalement accepté une, et le pirate a réussi à se connecter."

15 septembre 2022 : Uber | Technologie | États-Unis

« Ma plus grande déception vient du long délai entre notre notification à l'entreprise et la publication du rapport d'investigation complet. À la réflexion, dès réception du rapport de synthèse, on aurait dû réagir plus rapidement pour bien comprendre toutes les implications. »

Janvier 2022 : Okta | Technologie | États-Unis

« D'après notre analyse initiale, la fuite de données concerne des codes sources liés au fonctionnement des appareils Galaxy, mais n'inclut pas les informations personnelles de nos clients ou collaborateurs. »

Annoncé le 3 mars 2022 : Samsung | Électronique/Fabrication | Corée du Sud

« Le 11 septembre 2022, les acteurs malveillants qui avaient précédemment publié la liste des noms de fichiers de cet incident de sécurité sur le Dark Web ont publié au même endroit le contenu réel de ces fichiers. »

Attaque du 24 mai 2022 – Signalée le 10 août 2022 : Cisco | Électronique/Fabrication | États-Unis

« Nous savons que le gang de pirates [Lapsus$] a volé des informations d'authentification de collaborateur et certaines informations exclusives Nvidia sur nos systèmes, et a commencé à les faire fuiter en ligne. »

23 février 2022 : Nvidia | Électronique/Fabrication | Corée du Sud

« En publiant ce torrent, Lapsus$ a précisé qu'il contenait 90 % du code source Bing, et environ 45 % du code Bing Maps et Cortana. »

20 mars 2022 : Microsoft | Technologie | États-Unis

« Nous avons récemment subi une intrusion : un tiers non autorisé a obtenu illégalement un accès et a téléchargé des informations confidentielles depuis nos systèmes, notamment les premières images de développement du prochain Grand Theft Auto. »

19 septembre 2022 : Rockstar Games | Divertissement | États-Unis

Votre stratégie de cyberdéfense contre Lapsus$:

Comment bloquer les attaques Lapsus$ avant tout vandalisme ou suppression

Intrusion dans le réseau via des informations d'authentification de source interne, ainsi que via les comptes personnels des collaborateurs, utilisés comme « porte dérobée » pour accéder au réseau de l'employeur.

Empêcher les attaquants d'entrer sur le réseau est le moyen le plus simple, le plus économique et le plus rapide de protéger toutes les « business units » sans perturber les opérations.

- Contrôle des accès utilisateur
- Gestion des privilèges
- Audits des programmes de sécurité
- Contrôle des applications
- Authentification multifacteur (MFA) sans mot de passe
- Segmentation réseau
- Formation et sensibilisation des utilisateurs
- Automatisation stratégique

Recherche des informations d'authentification exposées dans des bases de données partagées ouvertes ou via des attaques par ingénierie sociale depuis l'intérieur.

Limiter la capacité des intrus à élever leurs privilèges évite le vol de données et l'extorsion.

- Contrôle des accès utilisateur
- Gestion des privilèges
- Audits des programmes de sécurité
- Contrôle des applications
- Authentification multifacteur (MFA) sans mot de passe
- Segmentation réseau
- Formation et sensibilisation des utilisateurs
- Automatisation stratégique

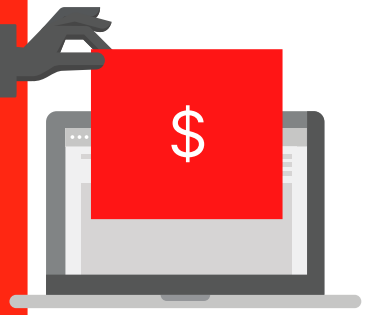
Exfiltration de données soit pour la notoriété (preuve de piratage), soit pour une extorsion future.

S'ils n'arrivent pas à voler de données, les attaquants n'auront pas de moyen de coercition pour exiger une rançon.

- Restriction du contenu Web
- Contrôle des accès utilisateur
- Gestion des privilèges
- Segmentation réseau
- Contrôle des applications
- EDR
- Audits des programmes de sécurité
- Automatisation stratégique
- Hygiène et gestion des périphériques

Lancement de l'extorsion (parfois depuis les canaux internes de la victime !) alors que l'entreprise commence à réagir à l'incident.

Trop tard pour la prévention, il faut passer en mode « récupération après sinistre ».



Index tactique InfoSec

ivanti CSW Cyber SecurityWorks

Index tactique InfoSec

Dans cette section

Carte ALPHV MITRE ATT&CK

1. Reconnaissance

T1595 : Analyse active
T1589 : Collecte des informations d'identité des victimes
  T1589.001 : Informations d'authentification

2. Développement des ressources

sans objet

3. Accès initial

T1078 : Comptes valides
T1190 : Exploitation des applications publiquement exposées

4. Exécution

sans objet

5. Persistance

T1098 : Manipulation des comptes

6. Élévation de privilèges

T1548 : Utilisation abusive du mécanisme de contrôle de l'élévation
  T1548.002 : Contournement du contrôle des comptes d'utilisateur (UAC)

7. Évasion de la défense

T1564 : Dissimulation des artéfacts

8. Artéfacts d'informations d'authentification

T1003 : Collecte mémoire des informations d'authentification d'OS
  T1003.001 : Mémoire de LSASS
  T1003.004 : Secrets LSA

9. Découverte

T1082 : Découverte des informations système
T1135 : Découverte des partages réseau
T1018 : Découverte des systèmes distants
T1087 : Découverte des comptes
  T1087.002 : Compte de domaine
T1487 : Découverte des éléments de confiance du domaine
T1057 : Découverte des processus
T1083 : Découverte des fichiers et répertoires

10. Déplacement latéral

T1563 : Détournement de services à distance
  T1563.002 : Détournement de RDP
T1570 : Transfert d'outil latéral

11. Collecte

T1005 : Données depuis le système local

12. Commande et contrôle

T1090 : Proxy
  T1090.003 : Proxy à plusieurs sauts

13. Exfiltration

T1567 : Exfiltration sur un service Web
  T1567.002 : Exfiltration vers un stockage Cloud

14. Impact

T1486 : Chiffrement des données pour plus d'impact
T1489 : Arrêt des services
T1490 : Inhibition de la récupération système

Carte MITRE ATT&CK APT29

1. Reconnaissance

sans objet

2. Développement des ressources

T1583 : Acquisition de l'infrastructure
- T1583.001 : Domaines
- T1583.006 : Services Web

T1584 : Compromission de l'infrastructure
- T1584.001 : Domaines

T1587 : Développement de capacités
- T1587.001 : Malware
- T1587.003 : Certificats numériques

3. Accès initial

T1078 : Comptes valides
- T1078.002 : Comptes de domaine

T1133 : Services distants externes

T1190 : Exploitation des applications publiquement exposées

T1195 : Compromission de la supply chain
- T1195.002 : Compromission de la supply chain logicielle

T1566 : Hameçonnage
- T1566.001 : Pièce jointe de « spearphishing »
- T1566.002 : Lien de spearphishing

4. Exécution

T1047 : Windows Management Instrumentation

T1204 : Exécution par l'utilisateur
- T1204.001 : Lien malveillant
- T1204.002 : Fichier malveillant

T1053 : Tâche/opération planifiée
- T1053.005 : Tâche planifiée

T1059 : Interpréteur de commandes et de scripts
- T1059.001 : PowerShell
- T1059.003 : Shell de commandes Windows
- T1059.006 : Python

T1203 : Exploitation pour exécution par le client

5. Persistance

T1053 : Tâche/opération planifiée
- T1053.005 : Tâche planifiée

T1078 : Comptes valides
- T1078.002 : Comptes de domaine

T1098 : Manipulation des comptes
- T1098.001 : Informations d'authentification Cloud supplémentaires
- T1098.002 : Permissions de délégation d'e-mail supplémentaires

T1133 : Services distants externes

T1546 : Exécution déclenchée par un événement

T1546.003 : Abonnement aux événements pour Windows Mangement Instrumentation

T1546.008 : Fonctions d'accessibilité

6. Élévation de privilèges

T1053 : Tâche/opération planifiée
- T1053.005 : Tâche planifiée

T1078 : Comptes valides
- T1078.002 : Comptes de domaine

T1484 : Modification de la stratégie de domaine
- T1484.002 : Notification de niveau de confiance de domaines

T1546 : Exécution déclenchée par un événement
- T1546.003 : Description des événements pour Windows Mangement Instrumentation

T1546.008 : Fonctions d'accessibilité

T1547 : Exécution du démarrage auto à l'amorçage ou à la connexion
- T1547.009 : Modification des raccourcis

7. Évasion de la défense

T1027 : Fichiers ou informations obscurcis

T1027.002 : Packages logiciels

T1036 : Camouflage
- T1036.004 : Camouflage comme tâche ou service
- T1036.005 : Usurpation d'un nom ou d'un emplacement légitime

T1070 : Suppression d'indicateurs sur l'hôte
- T1070.004 : Suppression de fichiers
- T1070.006 : Modification d'horodatages

T1078 : Comptes valides
- T1078.002 : Comptes de domaine

T1140 : Désobscurcissement/décodage de fichiers ou d'informations

T1218 : Exécution par l'intermédiaire de fichiers binaires système
- T1218.011 : Rundll32

T1484 : Modification de la stratégie de domaine
- T1484.002 : Notification de niveau de confiance de domaines

T1548 : Utilisation abusive du mécanisme de contrôle de l'élévation
- T1548.002 : Contournement du contrôle des comptes d'utilisateur (UAC)

T1550 : Utilisation de matériel d'authentification alternatif
- T1550.003 : Transmission du ticket
- T1550.004 : Cookie de session Web

T1553 : Subversion des contrôles de confiance
- T1553.002 : Signature de code

T1562 : Affaiblissement des défenses
- T1562.001 : Désactivation ou modification d'outils
- T1562.002 : Désactivation des journaux d'événements Windows
- T1562.004 : Désactivation ou modification du pare-feu système

8. Accès aux informations d'authentification

T1003 : Collecte mémoire des informations d'authentification d'OS
- T1003.006 : DCSync

T1005 : Données depuis le système local

T1552 : Informations d'authentification non sécurisées
- T1552.004 : Clés privées

T1555 : Informations d'authentification dans les emplacements de stockage de mots de passe

T1558 : Vol ou contrefaçon de tickets Kerberos
- T1558.003 : Kerberoasting

T1606 : Contrefaçon d'informations d'authentification Web :
- T1606.001 : Cookies Web
- T1606.002 : Jetons SAML

9. Découverte

T1016 : Découverte de la configuration réseau système
- T1016.001 : Découverte des connexions Internet

T1018 : Découverte des systèmes distants

T1057 : Découverte des processus

T1069 : Découverte des groupes de permissions

T1082 : Découverte des informations système

T1083 : Découverte des fichiers et répertoires

T1087 : Découverte des comptes

T1482 : Découverte des éléments de confiance du domaine

10. Déplacement latéral

T1021 : Services distants
- T1021.006 : Windows Remote Management

T1550 : Utilisation de matériel d'authentification alternatif
- T1550.003 : Transmission du ticket
- T1550.004 : Cookie de session Web

11. Collecte

T1074 : Préparation des données
- T1074.002 : Signature de données à distance

T1114 : Collecte des e-mails
- T1114.002 : Collecte des e-mails à distance

T1560 : Archivage des données collectées
- T1560.001 : Archivage par utilitaire

12. Commande et contrôle

T1001 : Obscurcissement des données
- T1001.02 : Obscurcissement des données : Stéganographie

T1071 : Protocoles de couche d'applications
- T1071.001 : Protocoles Web

T1090 : Proxy
- T1090.001 : Proxy interne
- T1090.003 : Proxy à plusieurs sauts
- T1090.004 : Dissimulation du domaine de destination

T1095 : Protocole hors couche applicative

T1102 : Service Web
- T1102.002 : Communication bidirectionnelle

T1105 : Transfert d'outils externes

T1568 : Résolution dynamique

13. Exfiltration

T1048 : Exfiltration par un protocole alternatif
- T1048.002 : Exfiltration par protocole non-C2 à chiffrement asymétriquel

14. Impact

sans objet

Carte MITRE ATT&CK Conti

1. Reconnaissance

T1595 : Analyse active

2. Développement des ressources

sans objet

3. Accès initial

T11990 : Exploitation des applications publiquement exposées
T1566 : Hameçonnage
- T1566.001 : Pièce jointe de « spearphishing »
- T1566.002 : Lien de spearphishing
- T1566.003 : Spearphishing via un service

4. Exécution

T1072 : Outils de déploiement de logiciels
T1203 : Exploitation pour exécution par le client

5. Persistance

T1037 : Scripts d'initialisation à l'amorçage ou à la connexion
T1542 : Amorçage avant l'OS
T1542.003 : Bootkit
T1543 : Création ou modification de processus système
- T1543.001 : Lancement d'agent
- T1543.002 : Service système
- T1543.003 : Service Windows
- T1543.004 : Lancement de Daemon

T1546 : Exécution déclenchée par un événement
- T1546.001 : Modification des associations de fichiers par défaut
- T1546.004 : Modification de la configuration de Shell Unix
- T1546.008 : Fonctions d'accessibilité

T1547 : Exécution du démarrage auto à l'amorçage ou à la connexion
- T1547.006 : Modules et extensions de noyau (Kernel)
- T1547.009 : Modification des raccourcis

T1574 : Détournement du flux d'exécution
- T1574.008 : Interception de chemins par détournement de l'ordre de recherche
- T1574.009 : Modification des raccourcis
- T1574.010 : Faiblesses des permissions de fichier des services
- T1574.011 : Faiblesses des permissions de registre des services

6. Élévation de privilèges

T1037 : Scripts d'initialisation à l'amorçage ou à la connexion
T1055 : Injection de processus
T1134 : Manipulation des jetons d'accès
T1543 : Création ou modification de processus système
- T1543.001 : Lancement d'agent
- T1543.002 : Service système
- T1543.003 : Service Windows
- T1543.004 : Lancement de Daemon

T1546 : Exécution déclenchée par un événement
- T1546.001 : Modification des associations de fichiers par défaut
- T1546.004 : Modification de la configuration de Shell Unix
- T1546.008 : Fonctions d'accessibilité

T1547 : Exécution du démarrage auto à l'amorçage ou à la connexion
- T1547.006 : Modules et extensions de noyau (Kernel)
- T1547.009 : Modification des raccourcis

T1548 : Utilisation abusive du mécanisme de contrôle de l'élévation
T1574 : Détournement du flux d'exécution
- T1574.010 : Faiblesses des permissions de fichier des services
- T1574.011 : Faiblesses des permissions de registre des services

7. Évasion de la défense

T1027 : Fichiers ou informations obscurcis
- T1027.003 : Stéganographie

T1014 : Rootkit
T1036 : Camouflage
- T1036.005 : Usurpation d'un nom ou d'un emplacement légitime

T1055 : Injection de processus
T112 : Modification du registre
T1134 : Manipulation des jetons d'accès
T1218 : Exécution par l'intermédiaire de fichiers binaires signés
- T1218.001 : Fichier HTML compilé

T1542 : Amorçage avant l'OS
- T1542.003 : Bootkit
- T1542.004 : Installation d'un certificat racine

T1548 : Utilisation abusive du mécanisme de contrôle de l'élévation
T1553 : Subversion des contrôles de confiance
T1562 : Affaiblissement des défenses
- T1562.001 : Désactivation ou modification d'outils

T1574 : Détournement du flux d'exécution
- T1574.010 : Faiblesses des permissions de fichier des services
- T1574.011 : Faiblesses des permissions de registre des services

8. Accès aux informations d'authentification

T1005 : Outils de déploiement de logiciels
T1080 : Altération du contenu partagé

9. Collecte

T1005 : Données depuis le système local
T1039 : Données depuis un lecteur réseau partagé
T115 : Données du Presse-papier
T1123 : Capture audio
T1125 : Capture vidéo

10. Commande et contrôle

sans objet

11. Exfiltration

T1020 : Exfiltration automatisée
- T1020.001 : Duplication du trafic

12. Impact

T1498 : Déni de service du réseau
- T1498.001 : Inondation directe du réseau

Carte MITRE ATT&CK Lapsus$

1. Reconnaissance

sans objet

2. Développement des ressources

sans objet

3. Accès initial

T1078 : Comptes valides
T1133 : Services distants externes
T1190 : Exploitation des applications publiquement exposées
T1199 : Relations de confiance

4. Exécution

T1059 : Interpréteur de commandes et de scripts
- T1059.001 : PowerShell
- T1059.003 : Shell de commandes Windows
- T1059.004 : Shell Unix

T1072 : Outils de déploiement de logiciels

5. Élévation de privilèges

T1068 : Exploitation pour l'élévation des privilèges
T1078 : Comptes valides
- T1078.002 : Comptes de domaine

6. Persistance

T1021 : Services
- T1021.001 : Protocole de bureau à distance (RDP)I

T1078 : Comptes valides
- T1078.002 : Comptes de domaine
- T1078.003 : Comptes locaux
- T1078.004 : Comptes Cloud

T114 : Collecte des e-mails
- T114.003 : Règle de transfert des e-mails

T1133 : Services distants externes

7. Évasion de la défense

T1027 : Fichiers ou informations obscurcis
- T1027.002 : Packages logiciels

T1078 : Comptes valides
- T1078.002 : Comptes de domaine
- T1078.003 : Comptes locaux
- T1078.004 : Comptes Cloud

T1553 : Subversion des contrôles de confiance
- T1553.002 : Signature de code

T1562 : Affaiblissement des défenses
- T1562.001 : Désactivation ou modification d'outils

8. Accès aux informations d'authentification

T1003 : Collecte mémoire des informations d'authentification d'OS
- T1003.001 : Mémoire de LSASS

T1111 : Interception de l'authentification à deux facteurs
T1212 : Exploitation pour l'accès aux informations d'authentification
T1528 : Vol de jeton d'accès aux applications
T1552 : Informations d'authentification non sécurisées
- T1552.001 : Informations d'authentification dans des fichiers
- T1552.004 : Clés privées

T1555 : Informations d'authentification dans les emplacements de stockage de mots de passe
- T1555.005 : Gestionnaires de mots de passe

9. Découverte

T1016 : Découverte de la configuration réseau système
- T1016.001 : Découverte des connexions Internet

T1069 : Découverte des groupes
- T1069.002 : Groupes de domaines

T1082 : Découverte des informations système
T1482 : Découverte des éléments de confiance du domaine

10. Déplacement latéral

T1021 : Services
- T1021.001 : Protocole de bureau à distance (RDP)

T1534 : « Spearphishing » interne
T1078 : Comptes valides
- T1078.002 : Comptes de domaine

11. Collecte

T1039 : Données depuis un lecteur réseau partagé
T1114 : Collecte des e-mails
- T1114.003 : Règle de transfert des e-mails

T1213 : Données depuis les référentiels d'informations
- T1213.002 : Sharepoint
- T1213.003 : Référentiels de code

12. Exfiltration

T114 : Collecte des e-mails
- T114.003 : Règle de transfert des e-mails

T1537 : Transfert de données vers un compte Cloud
T1567 : Exfiltration par un service Web

13. Impact

T1485 : Destruction des données
T1529 : Arrêt/redémarrage du système

Références et sources

Outre l'ensemble des analystes, journalistes et organisations cités ici, nous voulons remercier particulièrement les chercheurs et experts internes de Cyber Security Works et Ivanti, qui nous ont donné accès à des insights du secteur et à des informations exclusives sans lesquelles ce toolkit n'aurait pas pu exister.

NIST, « Advanced Persistent Threat » (menace avancée persistante).

« 2022 Global Threat Report. » Crowdstrike.

« Alert (AA22-047A): Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology. » Cybersecurity & Infrastructure Security Agency (CISA).

« APT29. » MITRE ATT&CK.

« Cisco Data Breach Attributed to Lapsus$ Ransomware Group. » Dark Reading. « Cisco Event

Response: Corporate Network Security Incident. » Cisco Security.

« CISCO Talos shares insights related to recent cyber attack on Cisco. » Cisco Talos.

« DEV-0537 criminal actor targeting organizations for data exfiltration and destruction. » Microsoft Security.

« Encevo Cyberattack. » Encevo.

« Experts Call the Conti Ransomware Gang Who Broke BI Dangerous Hackers. » CNN Indonésie.

« General Security Advisory: Understanding and preparing for cyber threats relating to tensions between Russia and Ukraine. » National Cyber Security Centre (NCSC).

« Globant official update. » Globant.

« Hacker attack on the province of Carinthia: “Black Cat” wants five million dollars in Bitcoin. » DerStandard.

« Incident and Agency Updates. » Comté de Fremont, Colorado.

« Lapsus$: An In-Depth Look at Data Extortion Group. » Avertium.

« MITRE Mapping of CISA KEVs and its Challenges. » Cyber Security Works.

« Moncler Press Release - Update on Malware Attack. » Groupe Moncler.

« Nordex Group impacted by cyber security incident. » Nordex Group.

« RE: NOTICE OF DATA BREACH. » Meyer Corporation.

« RESPONSE TO LATEST MEDIA REPORTS ABOUT 27 NOVEMBER CYBER SECURITY INCIDENT. » CS Energy.

« Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and “PrintNightmare” Vulnerability. » Cyber & Infrastructure Security Agency (CISA).

« Russia-Nexus UAC-0113 Emulating Telecommunication Providers in Ukraine. » Insikt Group : Recorded Future.

« Security update. »Actualités Uber.

« STATEMENT ABOUT CYBERSECURITY INCIDENT: DECEMBER 26, 2021. » Shutterfly, Inc.

« Statement from Oiltanking GmbH Group and Mabanaft GmbH & Co. KG Group. » Communications Mabanaft.

« Threat Report: T3 2021. » ESET Security Research.

« Ubisoft Cyber Security Incident Update. » Ubisoft.

« Update on cyber security incident. » Nordex Group.

Abrams, Lawrence. « Lapsus$ hackers leak 37GB of Microsoft’s alleged source code. » Bleeping Computer.

Abrams, Lawrence. « Shutterfly discloses data breach after Conti ransomware attack. » Bleeping Computer.

Amitai Cohen via @AmitaiCo.

Australian Cyber Security Centre (ACSC). « 2021-010: ACSC Ransomware Profile - Conti. »

Batra, Anirudh. « Detailed Analysis of LAPSUS$ Cybercriminal Group that has Compromised Nvidia, Microsoft, Okta, and Globant. » CloudSEK.

Bill Demirkapi via @BillDemirkapi.

Bradbury, David. « Updated Okta Statement on LAPSUS$. » Okta.

Brett Callow via @BrettCallow.

Brown, David - Matthews, Michael - Smallridge, Rob. « LAPSUS$: Recent techniques, tactics and procedures. » nncgroup.

Burgess, Matt. « The Workaday Life of the World’s Most Dangerous Ransomware Gang. » Wired.

Cimpanu, Catalin. « Disgruntled ransomware affiliate leaks the Conti gang’s technical manuals. » The Record.

Clark, Mitchell. « Nvidia says its “proprietary information” is being leaked by hackers. » The Verge.
Responsables Conti via @ContiLeaks.

CÓRDOBA, Javier - Sherman, Christopher. « Cyber attack causes chaos in Costa Rica government systems. » AP News.

Culafi, Alexander. « AdvIntel: Conti rebranding as several new ransomware groups. » SearchSecurity.

Cyberpedia. « What is the MITRE ATT&CK Framework? » Cortex.

DarkFeed via @ido_cohen2.

DarkTracer: DarkWeb Criminal Intelligence via @darktracer_int.

Davis, Griffin. « “GTA 6” Leaker Arrested! Authorities Claim Teenager is Linked to Lapsus$ Hacking Group. » Tech Times.

Digital Security Unit. « Special Report: Ukraine - An overview of Russia’s cyberattack activity in Ukraine. » Microsoft.

DISSENT. « AlphaV claims attack on Florida International University (updated). » DataBreaches.net.

Fadilpašić, Sead. « Conti ransomware group officially shuts down - but probably not for long. » techradar.pro.

Fardkhmanesh, Megan. « The Real Impact of the Grand Theft Auto and Diablo Leaks. » Wired.

Fox, Barbara. « Fremont County government services closed due to a cyber security breach. » KRDO News.

Ganti, Anil. « Samsung says your personal info wasn't leaked in its recent data hack. » SamMobile.

Greenberg, Andy (2019) « Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. »

Greenberg, Andy. « Destructive Hacks Against Ukraine Echo Its Last Cyberwar. » Wired.

Greig, Jonathan. « BlackCat ransomware group claims attack on Florida International University. » The Record.

Greig, Jonathan. « Louisiana authorities investigating ransomware attack on city of Alexandria. » The Record.

Greig, Jonathan. « North Carolina A&T hit with ransomware after ALPHV attack. » The Record.

Gupta, Surojoy. « All About Conti. » Cyber Security Works.

Gurevich, M (1961) « The Social Structure of Acquaintanceship Networks » Cambridge, MA : MIT Press

Harbison, Mike - Renals, Peter. « Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive. » Unit 42, Palo Alto Networks.

Hill, Michael. « Cisco admits hack on IT network, links attacker to LAPSUS$ threat group. » CSO.

Jenkins, Luke - Hawley, Sarah - Najafi, Parnian - Bienstock, Doug. « Suspected Russian Activity Targeting Government and Business Entities Around the Globe. » Mandiant.

Kabelka, Laura. « Austria's Carinthia halts passport issuance over ransomware attack. » Euractiv.

Kan, Michael. « Nvidia Confirms Company Data Was Stolen in Hack. » PC Mag.

Koczwara, Michael. « LAPSUS$ TTPs. ».

Lakshmanan, Ravie. « Uber Blames LAPSUS$ Hacking Group for Recent Security Breach. » The Hacker News.

Lakshmanan, Ravie. « Uber Claims No Sensitive Data Exposed in Latest Breach... But There's More to This. » The Hacker News.

Lyngaas, Sean. « "I can fight with a keyboard": How one Ukrainian IT specialist exposed a notorious Russian ransomware gang. » CNN.

Mari, Angelica. « Brazilian Ministry of Health suffers cyberattack and COVID-19 vaccination data vanishes. » ZDNet.

Meta/Facebook, « Three and a half degrees of separation. »

Minggeng, Liu. « Exclusive / Delta was hacked and extorted 410 million yuan, estimated about 13,500 computers were encrypted. » CTWant News.

Newman, Lily Hay. « The Dire Warnings in the Lapsus$ Hacker Joyride. » Wired.

Panettieri, Joe. « Lapsus$ Cyberattack vs Okta, Sitel: Up to 366 Okta Customers Impacted. » MSSP Alert.

Pearson, James. « UPDATE 4-Shell re-routes oil supplies after cyberattack on German firm. » Reuters.

Peters, Jay. « Ubisoft says it experienced a "cyber security incident", and the purported Nvidia hackers are taking credit. » The Verge.

Pink, Bidara. « Last month Bank Indonesia (BI) was hit by a cyber attack, but it has been resolved. » Kontan Indonésie.

Polityuk, Pavel. « EXCLUSIVE Ukraine suspects group linked to Belarus intelligence over cyberattack. » Reuters.

Ransomware Index Update: Q2-Q3 2022. Cyber Security Works, Ivanti.

Ravindran, Priya. « All about BlackCat (ALPHV). » Cyber Security Works.

Rewards for Justice via @RFJ_USA.

Rockstar Games via @RockstarGames.

Scullion, Chris. « Bandai Namco confirms it's been hacked and says it's investigating damage. » VGC News.

Sharma, Ax. « KP Snacks giant hit by Conti ransomware, deliveries disrupted. »

Soloman, Howard. « Canadian military provider suffered ransom attack, says news report. »

Taipei, Peng Yuwen. « Delta's servers were hacked, and some system recovery operations are estimated to have no major impact. » Yahoo Actualités : Taïwan.

Temple-Raston, Dina. « A "Worst Nightmare" Cyberattack: The Untold Story of the SolarWinds Hack. » NPR.

The Reliants Project, « Six Degrees of Kevin Bacon. »

Tidy, Joe. « Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal. » BBC News.

Todd MicKinnon via @toddmckinnon.

Uchill, Joe. « Globant confirms falling victim to Lapsus$ extortion group. » SC Magazine.

Wadhwani, Sumeet. « Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members. » spiceworks.

Wadhwani, Sumeet. « Ransomware Group Lapsus$ Cries Foul After NVIDIA Allegedly Does a Tit-for-Tat. » spiceworks.

Werkmeister, Luke. « Ripple effects of ransomware attack against Suffolk County continue more than a week later. » The Suffolk Times.

Wolfram, John - Hawley, Sarah - McLellan, Tyler - Simonian, Nick - Veilby, Anders. « Trello From the Other Side: Tracking APT29 Phishing Campaigns. » Mandiant.

Zetter, Kim (2015) « Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. »

Toolkit de cyberstratégie 2023 pour susciter l'adhésion interne

Apprenez à défendre votre budget et à convaincre les parties prenantes (hors InfoSec) de l'importance de votre stratégie de cybersécurité

En collaboration avec

CSW Cyber SecurityWorks

ivanti

ivanti.fr
+33 (0)1 76 40 26 20
contact@ivanti.fr