Explication des menaces

Explications en langage clair des techniques d'attaque que Cyber Crucible est conçu pour arrêter - logiciels malveillants sans fichier, attaques en mémoire, automatisation par des pirates, infostealers et vol de jetons de session.

Cyber Crucible peut-il arrêter le mouvement latéral d'un attaquant ?

Le moteur comportemental du produit et les méthodologies Zero Trust permettent de recueillir efficacement des preuves de mouvement latéral.

Il peut s'agir de preuves de mouvement latéral de processus à processus sur la machine elle-même, ou de la découverte du point d'entrée d'un attaquant dans le système à partir d'un système distant, lors de la réalisation d'une analyse des causes profondes (Root Cause Analysis).

Les programmes et leurs arguments associés aux méthodes d'injection de processus et aux processus « living off the land » ouvrant d'autres processus sont capturés et envoyés à Cyber Crucible.

Grâce à l'analyse comportementale des processus au niveau du noyau, aucun processus n'est trop privilégié pour être observé et signalé par Cyber Crucible (y compris d'autres pilotes de noyau, voire d'autres outils de sécurité des postes de travail).

Des réponses automatisées de contre-extorsion se déclenchent dès que des actions d'extorsion de données ou de chiffrement par rançongiciel sont amorcées.

Par exemple, voici une vidéo démontrant un mouvement latéral à travers une machine, utilisant des techniques en mémoire, et l'exploit Log4J. Veuillez noter que la suspension automatisée du ou des processus concernés est intervenue après le début des comportements de vol de données et de rançongiciel.

rr-log4j-procinj-3mins.mp4

Un autre exemple de cette dynamique démontre l'utilisation par un attaquant pour ouvrir un shell Windows. L'observation a permis de capturer toutes les preuves, mais l'activité a été suspendue dès que le shell Windows a commencé à tenter des activités d'extorsion de données (dans ce cas, un vol de données).

rr-com-dll.mp4

Enfin, la migration depuis un navigateur exploité est également observée, et dans ce cas, l'attaquant n'a jamais réussi à se déplacer depuis le navigateur Chrome exploité, grâce à la surveillance de l'état de la mémoire du navigateur :

rr-untrusted-chrome.mp4

L'application whitelisting fonctionne-t-elle ?

Qu'est-ce que l'Application Whitelisting ?

L'application whitelisting est un concept dans lequel vous disposez d'une liste de programmes autorisés à fonctionner, et tout le reste n'est pas autorisé à fonctionner.

Les technologies de liste blanche d'applications les plus avancées combineront un certain type de logique de source et de destination. Par exemple, une liste blanche d'applications peut indiquer : « Le Bloc-notes Windows est autorisé à accéder au dossier Taxes de mon bureau, mais pas Microsoft Word. »

Nous approfondirons ce point, mais de manière générale, les stratégies défensives de liste blanche d'applications reposent fortement sur ces deux variables :

1. Les attaquants acceptent de suivre les règles que vous avez établies pour eux concernant votre outil de cybersécurité de liste blanche d'applications.
2. Votre environnement est très petit, avec peu d'applications qui restent assez stables, et sans exploits.

Inconvénients des technologies de liste blanche d'applications

Complexité

Les réseaux informatiques sont comme des organismes complexes

Même les petits réseaux informatiques sont des entités en constante évolution, avec une myriade de comportements. Les applications sont constamment ajoutées et supprimées par les utilisateurs. Les modules à l'intérieur des applications sont constamment ajoutés et supprimés par les créateurs de programmes, en particulier lors des mises à jour. Enfin, les comportements des applications, en plus des changements de code entraînant des modifications de comportement, sont utilisés de différentes manières par différents utilisateurs à différents moments. Imaginez maintenant l'équipe qui devrait assurer le suivi constant de tout cela, ainsi que les tickets d'assistance informatique qui devraient constamment être ouverts.

En réalité, le seul environnement informatique stable est celui piloté par des kiosques, dans lesquels les programmes sont installés sans possibilité de mise à niveau, d'ajout ou de suppression, et où les utilisateurs sont strictement autorisés à effectuer une ou deux fonctions seulement. Peut-être un kiosque d'impression de photos ou quelque chose de similaire. Dans ce cas, la liste blanche d'applications ne devrait être mise à jour qu'à chaque mise à niveau du terminal du kiosque, disons deux fois par an.

Des listes blanches d'applications plus avancées signifient plus de complexité

Les listes blanches d'applications les plus simples se limitent à des listes de programmes autorisés à exister sur le système d'un utilisateur.

Cela peut déjà être difficile à gérer en soi, mais cela conduit à une variété d'améliorations potentielles.

Par exemple, ce n'est pas parce que le service de paie dispose d'une application pour interagir avec le système de paie de l'entreprise qu'il ne devrait pas y avoir un ensemble de règles distinct pour l'équipe de l'entrepôt, qui utilise des applications différentes (non liées à la paie) ?

Ainsi, des améliorations concernant les divisions ou les utilisateurs pouvant exécuter quelles applications constituent une amélioration évidente. Une amélioration qui a désormais créé une complexité supplémentaire, en plus du simple suivi du nombre, du type et des versions des programmes présents sur votre réseau.

Maintenant, supposons que nous ayons besoin d'un autre ensemble d'améliorations : nous devons décider quel utilisateur a accès à quelle application, pour quel ensemble de données.

Cela aussi a parfaitement du sens, n'est-ce pas ? Vous ne voulez pas que votre équipe de l'entrepôt ait accès aux dossiers RH, et l'équipe RH n'a probablement pas besoin d'accéder aux données opérationnelles de l'équipe de livraison de l'entrepôt.

Il s'agit d'un ensemble de combinaisons ridiculement complexe à suivre, maintenant que l'emplacement des données a été ajouté comme variable.

Ainsi, avec chaque amélioration nécessaire pour rendre les technologies de liste blanche d'applications efficaces, la gestion, la configuration et le support continu (sans doute sans fin, toujours croissant) nécessaire pour la maintenir fonctionnelle rend la technologie inutilisable. Le résultat est généralement que de grands groupes d'utilisateurs se voient accorder l'accès à de grands groupes d'applications, et probablement à la quasi-totalité des données. Il en résulte donc une configuration de la technologie presque inutile, car aucune entreprise ne dispose des ressources nécessaires pour la gérer correctement.

Les applications interagissent entre elles

Il est courant dans les systèmes d'exploitation modernes que les applications interagissent avec d'autres applications. Parfois, cette interaction est due à une intégration entre deux applications, qui améliore l'expérience utilisateur, comme un document Word ouvrant Microsoft Photos. À d'autres moments (cela est très courant), il existe des appels entre programmes qui sont effectués d'une manière généralement invisible pour l'utilisateur final.

Qu'est-ce que la mise en liste blanche des applications ?

Introduction

La mise en liste blanche des applications, dans le contexte de Cyber Crucible, consiste à accorder à une application l'autorisation d'effectuer une action qui, autrement, pourrait être considérée comme suspecte ou malveillante.

La technologie de mise en liste blanche des applications se retrouve généralement dans les techniques défensives d'analyse comportementale, bien que certains attaquants l'utilisent également (non traité ici) dans leurs opérations.

Pensez-y comme à l'école, où les élèves n'étaient normalement pas autorisés à circuler dans les couloirs pendant les cours. Cependant, s'ils recevaient un « laissez-passer » sous une forme ou une autre d'une figure d'autorité, les élèves n'étaient pas renvoyés dans leur classe ni conduits au bureau du principal.

Types de mise en liste blanche des applications - une

description non technique

Si nous poursuivons avec l'analogie du « laissez-passer », il peut exister différentes techniques que les responsables de l'administration scolaire ont apprises, qui ont contribué à formaliser les comportements que certains élèves (certainement pas notre PDG Dennis) auraient pu tenter d'adopter. Toutes ces techniques ont une corrélation directe avec les opérations de sécurité.

Le laissez-passer évident et encombrant (une bonne chose)

21987331.jpg?width=278
Vous souvenez-vous d'avoir eu un laissez-passer, ou une clé pour une salle quelconque, qui était incroyablement grande et voyante ?

Il y avait plusieurs bonnes raisons à cela :

1. Pour qu'il ne se perde pas.
2. Pour réduire le temps et l'énergie qu'une figure d'autorité devait investir pour vérifier rapidement les activités approuvées de l'élève.

Un bon logiciel ne « perdra » pas une liste blanche, mais un logiciel de mise en liste blanche des applications devrait permettre une validation rapide et économe en ressources du fait que l'application a été inspectée.

Le laissez-passer générique (probablement pas une bonne chose)

C'est probablement le moins utile pour la surveillance des applications comme pour les écoles, mais il nécessite le moins de gestion ou d'expertise.

Dans ce cas, l'élève est autorisé à effectuer sa course dans le couloir. L'enseignant peut être au courant, par exemple, mais il n'y a aucune validation par les surveillants de couloir quant à ce que fait l'élève. De plus, en cas de tentative de validation, il existe deux niveaux d'investissement considérable en ressources :

1. le niveau d'effort pour approcher l'élève et l'interroger sur ses comportements et ses intentions
2. le niveau d'effort pour s'assurer que l'élève est honnête, afin de valider son explication

Pour les applications, cela se produit le plus souvent lorsqu'un programme est ajouté à une liste blanche, sans qu'aucune validation supplémentaire des comportements ou des activités autorisées ne soit effectuée. Malheureusement, la capacité d'obtenir du contexte sur les comportements d'une application n'est généralement pas disponible à l'acquisition, si elle n'est pas suivie en externe par un autre cadre.

Le laissez-passer génériquement spécifique

À ne pas confondre avec : « vas-y Application, fais ce que tu veux ! »

Revenons au laissez-passer pour les toilettes, car il est particulièrement approprié ici. Étant donné la visibilité du laissez-passer, il est relativement facile d'évaluer ce que l'élève devrait faire. Les comportements flagrants en dehors des comportements « aller aux toilettes » peuvent être évalués sans grande difficulté.

La mise en liste blanche des applications avec des limites génériques d'activités est la plus courante, bien que dans de nombreux cas, ces limites équivalent à autoriser un élève muni d'un laissez-passer pour les toilettes à jouer dans la cour de récréation.

Le laissez-passer spécifique-spécifique

À ne pas confondre avec le laissez-passer « génériquement spécifique » !

22642689.jpg?width=340
Alors qu'avec le laissez-passer génériquement spécifique, nous savons que l'élève utilise les toilettes - dans une grande école, nous ne savons pas :
1. Qui a donné la permission à l'élève

2. D'où il venait juste avant.

3. Quelles toilettes la figure d'autorité avait en tête lorsqu'elle a donné son approbation.

4. Depuis combien de temps l'élève est « dehors et en déplacement ».

Cela a nécessité davantage de travail sur le cadre d'autorité de l'école.

Pour revenir à la mise en liste blanche des applications, l'analyse comportementale est plus précise lorsque davantage de variables sont ajoutées à toute capacité de prise de décision.

De plus, lors de l'examen d'un laissez-passer délivré, il n'est normalement pas nécessaire de remonter une chaîne de 5 enseignants pour retrouver la source. Vous pouvez également presque toujours faire confiance au fait que l'enseignant n'était pas un « mauvais enseignant » incitant les élèves à mal se comporter. La mise en liste blanche des applications, dans un exemple de liste blanche spécifique-spécifique, nécessite de remonter le fil, pour examiner chaque application parente ou ancêtre ayant ouvert l'application suivante. Par exemple, un logiciel malveillant peut avoir ouvert un utilitaire Windows légitime.

Les questions suivantes sont à peu près équivalentes au « laissez-passer d'élève » évoqué ci-dessus :

1. Pour quoi l'application a-t-elle été lancée, ou que lui a-t-on demandé de faire ? Nous devons connaître le comportement prévu.
2. Qui a lancé l'application ? Il s'agit généralement d'un autre programme.
3. Quels programmes « parents » ou « ancêtres » ont conduit à l'ouverture de ce programme ? Que faisait, ou avait l'intention de faire, chacun d'entre eux ?

L'application compromise

Vous souvenez-vous, dans divers récits ou films de science-fiction ou d'horreur, lorsqu'un imposteur a en quelque sorte pris

22413315.jpg?width=226
le contrôle du comportement d'un personnage ? Dans les écoles, il y a peu de chances qu'un enseignant soit pris de contrôle par des extraterrestres.

La prise de contrôle d'une application est une technique privilégiée par les attaquants car, comme dans les films, la plupart des observateurs ne remarquent rien d'anormal jusqu'à ce qu'il soit trop tard.

Dans ce cas, un attaquant s'empare d'un programme en cours d'exécution, actuellement chargé en mémoire. Ainsi, le programme intact présent dans le système de fichiers est ignoré. Le programme en mémoire est modifié pour y ajouter le code de l'attaquant. Un peu comme un extraterrestre à l'intérieur du corps d'un humain. L'attaquant accomplit ses actes criminels, et lorsque le programme termine son exécution, la plupart des preuves ont disparu. Lorsque le programme légitime s'exécute à nouveau, si l'attaquant ne modifie pas le code une nouvelle fois, il fonctionne exactement comme les concepteurs légitimes l'avaient prévu à l'origine. Peut-être qu'une meilleure analogie, dans ce cas, serait celle d'un loup-garou ?

Une liste blanche d'applications doit donc nécessiter un travail supplémentaire pour s'assurer que le programme, ainsi que tous ses ancêtres ou programmes parents, sont intacts, sans qu'un pirate n'ait modifié les programmes pendant leur exécution.

En résumé - Questions à poser lors de l'examen d'une fonctionnalité de liste blanche d'applications

Assurez-vous de bien comprendre les limites de ce qu'autorise une liste blanche, lorsque vous discutez de la mise en liste blanche des applications avec votre équipe technique ou votre fournisseur.

1. Cette fonctionnalité examine-t-elle et suit-elle ce qu'un programme est censé faire, et compare-t-elle les comportements attendus aux comportements observés ?
2. Quel niveau de détail la fonctionnalité de liste blanche capture-t-elle dans sa prise de décision ? Plus, ou moins, qu'un laissez-passer d'élève détaillé ?
3. La fonctionnalité de liste blanche suit-elle et examine-t-elle les programmes parents et ancêtres à la recherche d'une éventuelle malveillance ? (Le programme A ouvre B, qui ouvre C, qui ouvre D - très courant)
4. La fonctionnalité de liste blanche valide-t-elle que le programme en cours d'exécution n'a pas été altéré ?

Lecture approfondie du National Institute of Standards & Technology (NIST)

Une publication faisant autorité, qui ne se prête pas à une lecture occasionnelle, mais qui est très détaillée.

Bien qu'elle ne couvre pas tous les scénarios, et que les spécificités ne soient pas mises à jour assez fréquemment pour suivre chaque scénario, les descriptions sont suffisamment stratégiques pour être utiles dans la plupart des circonstances.

L'équipe de Cyber Crucible accorde toujours une grande valeur aux enseignements tirés des publications du NIST, et y consacre du temps en conséquence.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf

Comment puis-je savoir ce qui aurait été suspendu sans le comportement personnalisé ?

Les utilisateurs peuvent voir quelles réponses à l'extorsion auraient été suspendues si un comportement personnalisé n'existait pas, en accédant d'abord à la page Réponses à l'extorsion, disponible sous l'onglet Opérations dans la barre latérale.

La colonne Exclu indique si une réponse à l'extorsion a été exclue ou non, et le filtre de colonne par défaut affiche les réponses non exclues et non silencieuses.

ExcludedColumn.png
Pour afficher les réponses exclues, ouvrez le filtre de la colonne Exclu et sélectionnez uniquement Exclu.

ExcludedFilter.png
Après avoir cliqué sur Appliquer, la grille affichera les réponses à l'extorsion exclues qui auraient été suspendues si le comportement personnalisé n'existait pas.

Pour voir quel comportement personnalisé a été appliqué à une réponse, cliquez d'abord sur la flèche dans la colonne Nombre d'incidents de la ligne concernée. Dans la grille interne qui apparaît après avoir cliqué sur la flèche, la colonne Règle de masquage affichera le nom du comportement personnalisé qui a été appliqué à la réponse.

ExcludedResponses.png

Comment gérer les comportements personnalisés

La page des comportements personnalisés se trouve sous l'onglet Opérations dans la barre latérale. Notez que les utilisateurs doivent disposer de l'autorisation « View Tailored Behaviors » pour un groupe afin de pouvoir voir les comportements personnalisés de ce groupe sur cette page

Comment créer un comportement personnalisé

Après avoir accédé à la page des comportements personnalisés, cliquez sur l'icône d'exclusion de processus au-dessus de cette grille.

Cliquer sur cette icône fera apparaître une fenêtre modale permettant de créer le comportement personnalisé.

CreateTailoredBehaviorIcon.png
Create Exclusion.png

Les utilisateurs ont la possibilité de spécifier un programme parent avec l'exception

94732291.png?width=504
Saisissez les restrictions supplémentaires à appliquer

CreateTailoredBehaviorAdditionalRestrictions.png
Les utilisateurs ont désormais la possibilité de limiter l'exception à des déclencheurs d'accès aux fichiers spécifiques ; tous les déclencheurs d'accès aux fichiers sont inclus par défaut. Notez que seuls les agents en version 4.4.6.2 et supérieure disposent de cette capacité de déclencheur d'accès aux fichiers.

Les utilisateurs ont également la possibilité de créer des comportements temporaires, voir plus de détails dans la section suivante

Comment créer et modifier des comportements personnalisés temporaires

Les utilisateurs peuvent créer un comportement personnalisé temporaire en suivant le processus normal de création d'un comportement expliqué ci-dessus, puis en activant le bouton « Make This Tailored Behavior Temporary ». Les utilisateurs peuvent alors saisir le nombre d'heures avant l'expiration du comportement temporaire (jusqu'à une semaine maximum).

Temporary Exclusion.png
La date d'expiration du comportement peut être consultée dans la colonne Expiration Date de la grille.

Pour modifier un comportement temporaire afin de prolonger la date d'expiration, rendre un comportement temporaire permanent, ou rendre un comportement permanent temporaire, cliquez sur l'icône de modification du comportement souhaité dans la colonne Expiration Date.

Edit Temp Behavior Icon.png

Cliquer sur cette icône ouvrira une fenêtre modale où les utilisateurs pourront modifier la date d'expiration du comportement selon leurs besoins

Edit behavior modal.pngScreenshot from 2024-09-09 15-21-58.png

Comment supprimer des comportements personnalisés

Pour supprimer un comportement, ou plusieurs comportements à la fois, sélectionnez d'abord le(s) comportement(s) à supprimer dans la grille et cliquez sur l'icône de la corbeille au-dessus de la grille.

Ensuite, tapez « delete » et cliquez sur le bouton Delete.

RemoveTailoredBehaviorIcon.pngRemoveTailoredBehaviorModal.png

Comment copier des comportements personnalisés vers un autre groupe

Pour copier un comportement (ou plusieurs comportements à la fois) vers un autre groupe, sélectionnez le(s) comportement(s) à copier dans la grille et cliquez sur l'icône de copie au-dessus de la grille.

Cliquer sur cette icône fera apparaître une fenêtre modale dans laquelle vous pouvez sélectionner le groupe vers lequel le(s) comportement(s) doivent être copiés.

Cette fenêtre modale propose également une option permettant de supprimer les comportements existants dans le groupe sélectionné (à l'exception des comportements générés automatiquement), et de ne conserver que les comportements copiés dans le groupe sélectionné après l'envoi de la demande.

CopyTailoredBehaviorIcon.pngCopyTailoredBehaviorModal.png
Après l'envoi de la demande, les comportements copiés apparaîtront désormais pour le groupe sélectionné.

ResultGrid.png

Créer un comportement personnalisé depuis la page des réponses à l'extorsion

Les utilisateurs ont la possibilité de créer des comportements personnalisés depuis la page des réponses à l'extorsion.

Tout d'abord, cliquez sur la flèche de la ligne de réponse à l'extorsion souhaitée dans la colonne Number of Incidents pour afficher la grille interne.

Ensuite, cliquez sur l'icône d'exclusion de réponse dans la colonne Response Name, ce qui fera apparaître une fenêtre modale permettant de créer le comportement personnalisé.

ExcludeResponseIcon.png

Dans cette fenêtre modale, vous pouvez créer des comportements en utilisant les chemins d’exécutables suggérés ou soumettre la réponse pour examen si les chemins suggérés ne correspondent pas à vos besoins.

Exclude Modal.png

Vous pouvez également cliquer sur le bouton Take me to Tailored Behaviors Page, qui vous redirigera vers la page des comportements personnalisés et préremplira automatiquement la fenêtre modale de création de comportement avec le même groupe, chemin et arguments de programme provenant de la réponse.

AutofilledModal.png

Notez que par défaut, l’option Limit Exception to Program + Parent Program est désactivée. Le chemin du programme parent et les arguments de la réponse à l’extorsion seront également remplis automatiquement si vous activez ce paramètre.

PrefilledArgs.png

L’exclusion du comportement personnalisé après avoir cliqué sur Create avec le paramètre Limit Exception to Program + Parent Program activé :

ExlusionResult.png

Qu'est-ce qu'une attaque sans fichier (en mémoire) ?

Réponse courte : Une attaque sans fichier est une attaque qui n'écrit jamais de programme sur le disque. L'attaquant injecte du code malveillant directement dans la mémoire d'un processus légitime et fiable, et y construit sa charge utile. Comme aucun fichier n'est jamais créé, les outils de sécurité qui analysent les fichiers — y compris la plupart des EDR — n'ont rien à détecter.

Pourquoi cela déjoue les outils basés sur les fichiers

La protection traditionnelle des terminaux repose sur une hypothèse simple : un logiciel malveillant est un fichier, il faut donc inspecter les fichiers. Les techniques sans fichier suppriment entièrement le fichier de l'équation.

Dans un déploiement réel, une entreprise de services financiers utilisait trois produits EDR leaders du secteur (Microsoft, CrowdStrike et Sophos) aux côtés d'un SOC géré du Top 50. Les attaquants ont compromis un outil de surveillance à distance fiable, injecté du code dans les processus de gestion de Microsoft SQL Server, et compilé leur ransomware ainsi que leur logiciel malveillant de vol de données directement dans la mémoire du serveur. Comme rien n'a touché le disque dur, les trois EDR, le MDR et le SOC ont été entièrement aveugles. Cyber Crucible a intercepté de manière autonome près de 10 000 processus malveillants — dont 98 % sur la ferme de serveurs SQL — sans la moindre alerte de la part de la suite d'outils historique.

Comment Cyber Crucible perçoit cela

Cyber Crucible surveille le comportement et l'intention au niveau du noyau plutôt que d'analyser les fichiers. Un processus agissant de manière malveillante est arrêté en moins de 200 millisecondes, qu'un fichier ait été écrit ou non.

Qu'est-ce que l'automatisation des pirates informatiques, et pourquoi met-elle en échec les défenses traditionnelles ?

Réponse courte : L'automatisation des pirates informatiques désigne l'utilisation de scripts, d'IA et d'automatisation robotisée des processus pour exécuter chaque étape d'une attaque à la vitesse machine. Une attaque automatisée peut infiltrer une machine, voler des données et supprimer ses propres outils en mémoire en quelques secondes — bien plus rapidement que ce qu'un analyste humain ne pourrait jamais faire.

Ce qui est automatisé

- **Reconnaissance :** des outils scannent Internet à la recherche de systèmes vulnérables et cartographient un réseau cible en quelques secondes, tout en générant des campagnes de phishing convaincantes à grande échelle.
- **Exploitation :** une fois une faiblesse détectée, des frameworks déploient l'exploit immédiatement — une faille zero-day peut être utilisée sur des millions de machines avant qu'un humain ne prenne connaissance de l'alerte.
- **« Braquage éclair » :** les logiciels malveillants modernes n'évaluent pas quels fichiers sont précieux. Ils chiffrent ou exfiltrent tout ce qu'ils peuvent atteindre, aussi vite que possible.

Pourquoi les humains ne peuvent pas gagner cette course

La limite ne vient pas de la qualité de l'équipe ni des effectifs. C'est une question de biologie. Le temps nécessaire à une personne pour voir une alerte, l'analyser et agir est plus long que le temps que met l'attaque à se dérouler entièrement. L'acheminement de la télémétrie vers un serveur cloud pour analyse, puis son retour, ajoute encore un délai supplémentaire.

La seule réponse viable est une défense qui décide et agit de manière autonome, sur le terminal, en quelques millisecondes.

Pourquoi les attaques automatisées ciblent-elles les mêmes emplacements sur chaque ordinateur ?

Réponse courte : Les attaquants ne savent rien de votre environnement spécifique, c'est pourquoi leur automatisation est conçue pour cibler des emplacements qui existent sur pratiquement toutes les machines — les dossiers de profils utilisateurs, les lettres de lecteur et les répertoires de données d'application. Cette prévisibilité constitue une faiblesse que les défenseurs peuvent exploiter.

Les cibles prévisibles

- **Profils utilisateurs et bureaux :** sous Windows, `C:\Users\[Username]` contient de manière fiable des données précieuses. Un script parcourt tous les répertoires utilisateurs sans avoir besoin de comprendre le système.
- **Lettres de lecteur :** les outils automatisés énumèrent `C:\`, `D:\`, et au-delà pour trouver des partages réseau, des lecteurs externes et des partitions montées à chiffrer.
- **Dossiers de données d'application :** chaque système d'exploitation conserve les identifiants, cookies et configurations dans des chemins connus — des cibles de choix pour le vol d'identifiants.

Retourner la prévisibilité contre l'attaquant

Le schéma d'attaque n'est pas réfléchi ; il s'agit d'un balayage brutal des emplacements bien connus. Cyber Crucible surveille précisément ces points d'entrée connus pour le vol d'identité et de données. Tout programme qui accède à des données à ces emplacements — ainsi que ses processus parents et enfants et les bibliothèques associées — voit son intention évaluée en une fraction de seconde, et est intercepté si cette intention est malveillante.

Qu'est-ce qu'un infostealer, et pourquoi le vol de jetons de session est-il si dangereux ?

Réponse courte : Un infostealer est un logiciel malveillant conçu pour dérober des éléments d'identité numérique — mots de passe, jetons de session, clés API et identifiants VPN — et les exfiltrer rapidement. Un jeton de session volé est dangereux car il permet souvent de contourner entièrement les mots de passe et l'authentification multifacteur, laissant un attaquant se connecter en tant qu'utilisateur légitime.

Pourquoi les attaquants volent désormais l'identité au lieu de rester présents

Les attaquants modernes évitent de plus en plus de s'attarder au sein d'un réseau. Rester dans l'environnement augmente les probabilités de détection. Ils préfèrent plutôt s'emparer des éléments d'identité et repartir, ce qui leur procure deux avantages :

1. **Risque réduit** — ils analysent ce qu'ils ont volé depuis un environnement sûr, à leur propre rythme.
2. **Retour facile** — avec un jeton de session, un mot de passe ou une clé VPN valides, ils peuvent revenir quand ils le souhaitent, en apparaissant totalement légitimes aux yeux du système d'authentification.

Pourquoi la rapidité est tout le problème

Ces outils passent de l'infiltration à l'autodestruction en quelques secondes — plus vite qu'une alerte cloud ne peut quitter les locaux. Cyber Crucible détecte l'intention au moment même de l'accès aux données d'identité et suspend le processus en moins de 200 millisecondes, avant que l'exfiltration ne commence.

Que sont les attaques Living-off-the-Land (LotL), et pourquoi la liste blanche d'applications échoue-t-elle contre elles ?

Réponse courte : Les attaques Living-off-the-Land utilisent des logiciels déjà installés et déjà approuvés — utilitaires système, outils d'administration, navigateurs — plutôt que d'introduire de nouveaux fichiers malveillants. La liste blanche d'applications échoue parce que l'attaquant opère à l'intérieur de programmes que la liste blanche autorise explicitement.

La liste blanche devient une liste de cibles

La liste blanche d'applications répond à une seule question : « ce fichier est-il autorisé à s'exécuter ? » Les techniques modernes rendent cette question sans objet. Si les attaquants dissimulent du code malveillant dans la mémoire d'un processus approuvé, la liste blanche a déjà donné son feu vert. En pratique, une liste blanche indique précisément à un attaquant à l'intérieur de quels processus il est le plus sûr de se cacher.

La meilleure question à poser

Une défense efficace doit passer de *« ce fichier est-il autorisé ? »* à *« que fait réellement ce code en ce moment ? »* Cela nécessite d'inspecter le comportement et la mémoire au niveau du noyau, là où l'activité réelle est visible — et non au niveau des fichiers, que l'attaquant a déjà contourné.

Qu'est-ce qu'une attaque en mémoire visant une DLL System32 ?

Réponse brève : Il s'agit d'une attaque qui infecte les bibliothèques de code fondamentales de Windows (les DLL System32) pendant qu'elles sont en cours d'exécution en mémoire. Comme presque toutes les applications et tous les outils de sécurité dépendent de ces bibliothèques pour fonctionner, leur compromission confère à l'attaquant un contrôle quasi total du poste de travail, avec très peu de traces.

Pourquoi il s'agit du summum de l'art offensif sur les postes de travail

Les DLL System32 fournissent les opérations fondamentales sur lesquelles s'appuient Windows et ses applications — allocation mémoire, cryptographie, réseau. Elles ont été conçues pour la rapidité et la fiabilité, jamais pour être corrigées ou instrumentées ("hookées") à la volée en production.

Un attaquant capable de les modifier en mémoire acquiert le pouvoir d'inspecter, de créer, de modifier ou de détruire des données et des programmes sur le système, avec une discrétion quasiment indétectable.

Pourquoi la plupart des outils ne peuvent pas la détecter

Les produits de sécurité qui dépendent des données de capteurs fournies par Microsoft s'appuient, par définition, sur les bibliothèques mêmes qui sont attaquées. Les capteurs nécessaires pour détecter cette catégorie d'attaque n'existent tout simplement pas dans les outils standards — l'outil devient alors muet tout en signalant que tout va bien.

Cyber Crucible a été délibérément conçu pour être indépendant des bibliothèques Windows, de sorte qu'un système d'exploitation compromis ne puisse ni l'aveugler ni le désactiver.

Pourquoi un logiciel malveillant ne s'active-t-il pas toujours dans un laboratoire de test de sécurité ?

Réponse courte : les attaquants conçoivent les logiciels malveillants pour qu'ils restent dormants tant qu'ils ne reçoivent pas un signal de validation provenant d'un serveur de commande et de contrôle (C2) actif qu'ils contrôlent. Au moment où un échantillon parvient à une base de données de logiciels malveillants, l'infrastructure C2 a généralement déjà été déplacée — les chercheurs testent donc souvent un échantillon orphelin qui n'accomplit rien.

Pourquoi les attaquants intègrent une dormance

- **Minimiser le renseignement disponible :** un logiciel malveillant dormant n'effectue aucune action malveillante observable, ce qui laisse moins d'éléments aux analystes pour documenter et moins de matière aux éditeurs pour élaborer des signatures.
- **Empêcher le détournement :** exiger une poignée de main secrète garantit qu'un concurrent ou un chercheur qui s'empare du serveur C2 ne peut pas simplement donner des instructions au logiciel malveillant ni récupérer les données volées.

Ce que cela signifie pour l'évaluation des outils de sécurité

Un test en laboratoire mené sur un échantillon déconnecté ne mesure que très peu de choses. La question pertinente n'est pas de savoir si un outil réagit à un logiciel malveillant dormant et inerte, mais s'il arrête les attaques réelles et rapides au moment où elles se produisent. Cyber Crucible est conçu pour ce second cas de figure : il surveille les points d'entrée liés au vol d'identité et de données que ciblent les attaques réelles, évalue l'intention en moins de 200 millisecondes et arrête le vol avant qu'il n'aboutisse.