Architecture & Technologie

Comment Cyber Crucible fonctionne en coulisses - IA génétique, fonctionnement au niveau du noyau, Rogue Process Prevention, indépendance vis-à-vis du système d'exploitation, et pourquoi les décisions sont prises au niveau du poste (endpoint).

Pourquoi votre réponse consiste-t-elle à suspendre les programmes ?

Les criminels ont appris qu'en opérant uniquement en mémoire, à l'aide de techniques telles que l'injection de processus, ils bénéficient de divers avantages :

1. Prise de contrôle de l'identité d'un utilisateur pour ce programme.
2. Évasion des contrôles de gestion des identités.
3. Évasion des règles de pare-feu basées sur les applications et des listes blanches.
4. Évasion des outils de prévention des pertes de données sur les serveurs.
5. Suppression de presque toutes les preuves en mémoire lorsque le processus est arrêté.
6. Suppression de presque toutes les preuves en mémoire une fois l'ordinateur redémarré.

En suspendant les programmes sous le contrôle de l'attaquant, les preuves sont figées dans le temps.

L'attaquant est également figé.

Les preuves sont disponibles pour les outils d'investigation numérique dans le cadre d'un processus d'enquête.

Si l'organisation n'est pas équipée pour effectuer une investigation numérique à ce moment-là, un simple redémarrage par l'attaquant ramènera le système à un état sain. Forcer l'arrêt du programme suspendu, puis le redémarrer, a généralement également l'effet souhaité.

Cyber Crucible bloque-t-il toute injection de processus ?

Non !

Il existe une variété d'activités qui se produisent sur les systèmes et qui constituent de l'injection de processus, mais qui ne sont pas nécessairement malveillantes.

Cyber Crucible rend visibles toutes ces activités d'injection de processus à des fins de threat hunting et d'analyse des causes profondes, mais n'arrête pas l'activité à moins que les activités d'extorsion de données, à savoir le vol de données ou le chiffrement par ransomware, ne commencent.

Vous trouverez ci-dessous un exemple d'injection de processus effectuée par le logiciel de sécurité des terminaux PC Matic, appelé PCPitStop. Il s'agit probablement d'un comportement qu'ils adoptent pour inspecter les processus en cours d'exécution.

5373968.png?width=680
Grâce à l'analyse comportementale au niveau du noyau de Cyber Crucible, vous disposez d'une visibilité complète sur toutes les activités, quel que soit le niveau de permission du logiciel (y compris les logiciels Microsoft ou des éditeurs d'antivirus hautement privilégiés).

Si une réponse automatisée est effectuée, cette page ainsi que la page Process Creations peuvent être consultées pour fournir des résultats d'investigation rapides.

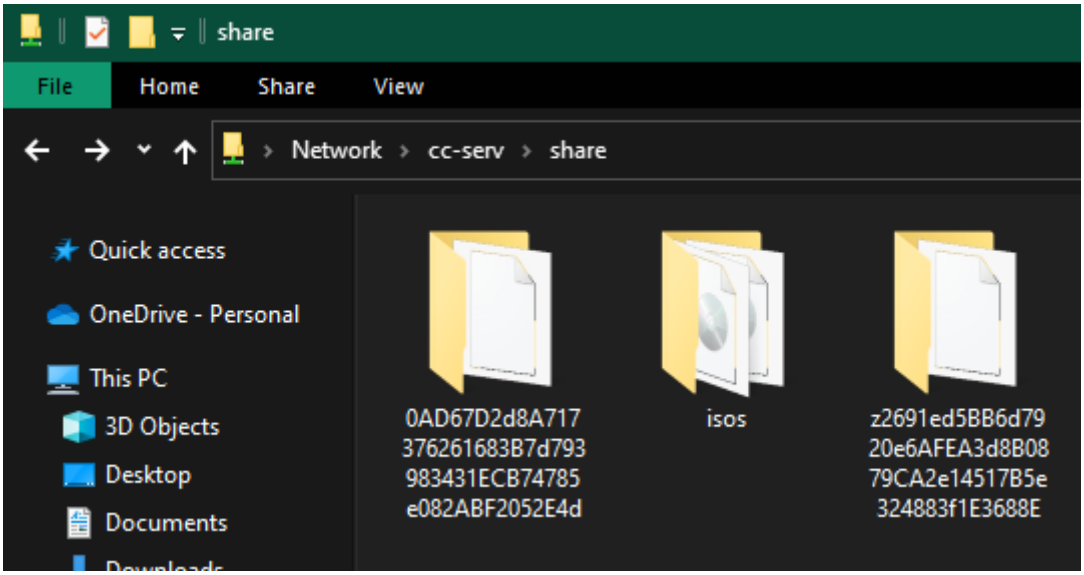
De plus, l'API REST peut être exploitée par les équipes de threat hunting pour rechercher des indicateurs de tactiques malveillantes potentielles en mémoire.

Que sont ces fichiers étranges à l'aspect aléatoire que je vois ?

Notre logiciel Data Extortion Prevention reçoit des indicateurs comportementaux de plusieurs moteurs avant de prendre une décision en une fraction de seconde quant à une éventuelle attaque en cours. L'un de ces moteurs, le moteur de surveillance des fichiers, utilise des fichiers spéciaux à plusieurs emplacements.

Ces fichiers que vous voyez parfois, et parfois non, sont placés là par Cyber Crucible. Selon la manière dont une application peut lister les fichiers, il se peut que vous les voyiez. Par exemple, un programme qui utilise l'Explorateur de fichiers pour lister les fichiers à enregistrer ou à ouvrir vous les affichera désormais.

Nous appelons ces fichiers des « canaris », comme dans l'expression « le canari dans la mine de charbon » (wiki).



Qu'est-ce qui est particulier au sujet des fichiers canaris de Cyber Crucible ?

Les fichiers canaris contiennent des données spéciales dissimulées, au cas où ils seraient un jour dérobés par un attaquant. Cyber Crucible peut retracer le fichier jusqu'à son propriétaire d'origine.

Les noms de fichiers sont en grande partie aléatoires (on parle de pseudo-aléatoire) de manière à ce que les attaquants ne puissent pas les identifier et les éviter. Les noms sont créés à l'aide d'une formule mathématique spéciale de Cyber Crucible, qui permet à notre logiciel de reconnaître un fichier comme étant un canari, même si les noms diffèrent d'une machine à l'autre ou d'un fichier à l'autre.

La capacité du logiciel Cyber Crucible à reconnaître ces fichiers signifie également qu'il suffit d'un seul fichier canari par serveur, même si des milliers de postes de travail utilisent ce serveur.

Où se trouvent les fichiers canaris ?

Les canaris se trouvent à divers endroits de votre système de fichiers.

Chaque fois qu'une nouvelle source de fichiers apparaît sur votre système, provenant de n'importe quel utilisateur possible, Cyber Crucible vérifie automatiquement si des canaris ont déjà été placés. Cela inclut les lecteurs amovibles tels que les clés USB, les sources de fichiers réseau et le stockage de fichiers basé sur le cloud.

Comment Cyber Crucible utilise-t-il l'analyse de la mémoire ?

Les analyses du noyau de Cyber Crucible suivent l'état de la mémoire d'un programme pendant tout son cycle de vie, du démarrage du programme jusqu'à sa fin. Elles suivent également l'état des interactions en mémoire avec d'autres programmes.

La surveillance comportementale recherche des états dangereux dans la mémoire du programme. Cela peut correspondre à une exploitation, à un bogue logiciel, ou à des attaques connues en mémoire (dites « sans fichier », ou « file-less ») en cours.

Cette surveillance est effectuée en temps réel sur les programmes de manière hautement efficace, afin de garantir que les opérations du système et du client ne soient pas affectées par l'analyse de Cyber Crucible.

Au moment d'un comportement potentiellement malveillant visant le vol d'identité, le vol de données ou l'extorsion, ce suivi et cette analyse comportementale de la mémoire sont intégrés aux autres données de télémétrie collectées, afin de déterminer si un programme doit être suspendu.

En quoi l'analyse comportementale de la mémoire de CC diffère-t-elle de l'analyse de la mémoire ?

Qu'est-ce que l'analyse de la mémoire ?

L'analyse de la mémoire est la pratique consistant à prendre un bloc de mémoire, généralement en le copiant vers un autre emplacement du système à des fins d'analyse, puis à l'analyser.

Photographie versus action en direct

Il ne s'agit pas d'une analyse en direct du programme pendant son fonctionnement, mais d'un instantané du programme à un moment donné. Pensez-y comme à une photographie, par opposition à une diffusion en direct. L'état du programme peut varier considérablement d'un instant à l'autre, ce qui la rend surtout utile comme exercice d'analyse forensique dans un environnement contrôlé. Elle est moins utile dans un environnement non contrôlé, comme celui d'un client. Plus une machine est occupée, ou plus un programme effectue d'opérations, plus il est difficile d'obtenir une image précise de l'état actuel d'un programme.

Cyber Crucible a débuté avec un usage intensif de l'analyse de la mémoire, en essayant de prendre de nombreuses « photographies » des états mémoire des programmes. À mesure que nous gagnions en rapidité, nous avons rencontré plusieurs goulots d'étranglement liés à la vitesse à laquelle les instantanés mémoire pouvaient être pris, et ce, sur plusieurs programmes à la fois.

Préoccupations liées à la consommation de ressources CPU ou

GPU

Cette analyse de la mémoire peut être extrêmement gourmande en ressources et peut prendre un certain temps pour les programmes volumineux. Lorsque Cyber Crucible utilisait l'analyse de la mémoire, plutôt que la surveillance comportementale intelligente de la mémoire, un cœur de CPU entier était dédié à cette analyse.

Intel propose une technologie innovante appelée Intel TDT AMS, disponible sur des architectures spécifiques basées sur Intel dotées d'un GPU Intel intégré.

Elle analyse la mémoire d'un programme dès son démarrage, en utilisant le GPU pour éviter de surcharger le CPU. De plus, le GPU offre de meilleures performances pour le type d'analyse effectuée (nous y reviendrons plus loin).

Méthodologie d'analyse

L'analyse de la mémoire est effectuée pour rechercher des codes ou des « chaînes » spécifiques. Il s'agit souvent des mêmes éléments de données que les outils antivirus/EDR recherchent dans les fichiers potentiellement malveillants.

L'analyse de la mémoire, en particulier, est plus limitée que certaines des recherches complexes pouvant être effectuées sur un fichier.

Par conséquent, l'analyse recherche par défaut des éléments déjà connus, comme des logiciels malveillants plus anciens, mais sa capacité à le faire est limitée.

Cyber Crucible analysait auparavant les segments de mémoire à la recherche de matériel cryptographique, mais cette méthode s'est révélée trop limitée pour les environnements modernes, et nous avons inventé une méthode différente pour observer les comportements, en utilisant une logique basée sur le noyau.

Méthodologies basées sur le comportement versus l'analyse

Cyber Crucible est passé d'une méthodologie basée sur l'analyse à une méthodologie basée sur le comportement pour plusieurs raisons.

Inconvénients de l'analyse

La première raison est qu'une image en direct devait être utilisée pour l'ensemble des programmes. Les instantanés rendaient très difficile l'achèvement, même d'une analyse limitée, avant qu'un nouvel instantané ne soit nécessaire. Trop d'activité des programmes passait inaperçue, un peu comme une caméra vidéo fonctionnant à un taux d'images par seconde trop faible. Ce problème était aggravé par la nécessité de surveiller tous les programmes simultanément. Les serveurs ou les postes de travail très sollicités, sans doute les ordinateurs nécessitant le plus de surveillance et étant les plus importants, se retrouvaient avec le pourcentage de surveillance le plus faible. Quelle que soit l'entreprise ou le produit, les limites technologiques étaient évidentes et intenables.

La seconde raison est que, au-delà de la consommation de ressources, l'analyse nécessite, par défaut, la recherche de **quelque chose de connu**. Ainsi, l'analyse de la mémoire doit être basée sur des signatures. De plus, cette analyse par signature doit se limiter à un sous-ensemble des fonctionnalités plus complètes de l'analyse par signature que l'on trouve dans l'analyse antivirus basée sur les fichiers. Les attaquants échappent déjà depuis des années aux défenses basées sur les signatures de fichiers ; il y a donc très peu de chances qu'ils soient détectés par un système basé sur des signatures moins performant.

Avantages de l'analyse comportementale

La surveillance de la mémoire basée sur le comportement de Cyber Crucible ne nécessite pas de signatures et exploite l'accès à la mémoire du noyau pour suivre les comportements de tous les programmes simultanément. Décomposons cela.

Premièrement, la surveillance comportementale signifie que les nouveaux logiciels malveillants, ou ceux modifiés par des attaquants pour paraître nouveaux, peuvent être facilement détectés en temps réel. L'analyse basée sur les signatures, qu'il s'agisse de la mémoire ou des fichiers, repose sur le fait d'avoir déjà rencontré ce logiciel malveillant spécifique auparavant. Les attaquants échappent aux défenses basées sur les signatures depuis des années, malgré une suite complète de techniques d'analyse appliquées aux fichiers. Les techniques d'analyse disponibles pour la mémoire ne constituent qu'un sous-ensemble de celles-ci, et sont encore moins efficaces.

Deuxièmement, la nouvelle surveillance comportementale de la mémoire de Cyber Crucible est capable de rester en temps réel sur l'ensemble des programmes simultanément, pendant toute la durée de leur exécution. L'analyse de la mémoire souffre de graves goulots d'étranglement de ressources qui s'aggravent à mesure que davantage de programmes s'exécutent. Les attaquants exécutent généralement des dizaines d'échantillons de logiciels malveillants à la fois, ce qui engorge l'analyse de la mémoire en raison de la vitesse et du nombre de programmes à examiner simultanément, qu'il s'agisse d'une menace de type zero-day ou d'un logiciel malveillant plus

ancien.

Que se passe-t-il lorsque CC détecte des attaques en mémoire

Tout d'abord, il est très important de noter que les altérations de mémoire se produisent pour plusieurs raisons différentes :

1. Attaques en mémoire
2. Interaction entre programmes
3. Bugs logiciels
4. Exploits

Ainsi, une injection de processus ou une technique d'altération de mémoire utilisée, même entre programmes, n'est pas nécessairement une action malveillante.

Si un programme ayant subi un événement mémoire probablement malveillant (donc, #1 ou #4 ci-dessus) est impliqué dans une réponse automatisée de Cyber Crucible, une activité de collecte automatisée se produit.

La portion de mémoire qui a été altérée dans un programme, ainsi que l'état « avant », est enregistrée dans un format structuré Cyber Crucible appelé .ccdiff

Cette portion de mémoire injectée ou altérée est enregistrée et disponible en téléchargement dans le portail web Cyber Crucible.

Pourquoi cela n'est-il pas automatiquement soumis à Virustotal (etc.) pour analyse ?

Dans certaines circonstances, le code malveillant utilisé dans une attaque contient des variables qui sont propres à une attaque, spécifiquement à une victime.

Soumettre ce code malveillant à un moteur d'analyse public tel que Virustotal représenterait une divulgation d'informations identifiant la victime, non souhaitée, à la communauté de la sécurité.

Pourquoi la soumission de ces données binaires à Virustotal (etc.) serait-elle utile ?

Les outils antivirus et EDR basés sur des signatures recherchent des chaînes ou des octets de code observés lors d’attaques précédentes. Même si ce logiciel malveillant n’a jamais été observé auparavant, il pourrait, après un certain temps, être connu de la communauté de la sécurité. Ces outils d’analyse n’ont généralement pas besoin que le code soit dans un binaire correctement formaté pour signaler une association avec un logiciel malveillant connu.

Qu'est-ce que la Genetic AI, et en quoi diffère-t-elle d'un LLM ?

Réponse courte : Genetic AI est l'IA de sécurité conçue sur mesure par Cyber Crucible. Elle modélise le comportement des programmes — en mémoire, à travers les processus, et vis-à-vis des fichiers — et détecte les déviations malveillantes en temps réel. Ce n'est pas un grand modèle de langage (LLM) ; les LLM analysent des schémas textuels, ce qui constitue un problème entièrement différent.

Ce qui la distingue

- **Conçue sur mesure pour la sécurité**, et non adaptée d'un modèle de texte généraliste.
- **Comportementale, et non basée sur des signatures** — pas de signatures, pas de flux de renseignement sur les menaces, pas d'attente qu'un tiers découvre l'attaque en premier.
- **Entièrement autonome** — les outils traditionnels reposent sur une collaboration homme-machine ; Genetic AI décide et agit d'elle-même.
- **Avant exécution** — elle bloque le comportement malveillant avant qu'il ne s'exécute, plutôt que de le décrire après coup.

IA verticale

Genetic AI est un exemple d'IA verticale : une intelligence artificielle adaptée aux défis spécifiques d'un secteur donné plutôt qu'un raisonnement à usage général. Dans le domaine de la sécurité, cette spécialisation est ce qui permet une décision sur l'intention en moins de 200 millisecondes.

Les résultats sont mesurables — Cyber Crucible a stoppé plusieurs attaques zero-day sur des réseaux clients jusqu'à 90 jours avant que tout autre éditeur ne les signale ou n'y réponde.

Comment Cyber Crucible prend-il une décision en moins de 200 millisecondes ?

Réponse courte : Il exécute une boucle en trois étapes — Detect-Decide-Respond — entièrement sur le point de terminaison au niveau du noyau, à l'aide d'un moteur d'analyse informatique en périphérie (edge computing) breveté. Comme rien n'a besoin de transiter par un service cloud pour revenir ensuite, et qu'aucun humain n'intervient dans la boucle, l'ensemble du cycle se termine en moins de 200 millisecondes.

La boucle

1. **Detect** — des capteurs novateurs au niveau du noyau identifient les schémas comportementaux malveillants dans la mémoire, l'activité des processus et l'accès aux fichiers.
2. **Decide** — le modèle comportemental renforcé par l'IA évalue instantanément l'intention de l'accès aux données du programme.
3. **Respond** — si l'intention est malveillante, le programme est intercepté et suspendu.

Pourquoi le traitement local n'est pas négociable

Envoyer la télémétrie à un serveur cloud, attendre l'analyse, puis recevoir une réponse en retour ajoute des millisecondes que l'attaquant utilisera avec plaisir. Pour donner une idée de l'échelle en jeu : cette décision se produit plus rapidement qu'un influx nerveux ne voyage de l'œil au cerveau. Toute architecture comportant un aller-retour réseau dans le chemin critique a déjà perdu cette course.

La télémétrie brute est tout de même copiée sur des serveurs par la suite à des fins de preuve et d'enrichissement — mais la décision de protection n'attend jamais ce processus.

Qu'est-ce que la Rogue Process Prevention (RPP) ?

Réponse courte : Rogue Process Prevention est l'approche brevetée de Cyber Crucible consistant à intervenir contre un processus malveillant plutôt qu'à se contenter de l'observer. Qu'il s'agisse d'un ransomware commençant à chiffrer des données ou d'un infostealer cherchant à récupérer un jeton de session, le processus est stoppé avant que les données ne quittent l'appareil.

Observer contre intervenir

La majorité du marché des solutions de sécurité des postes de travail est conçue pour observer. RPP est conçue pour intervenir. La distinction est la même qu'entre une caméra de sécurité qui enregistre un cambriolage pour un visionnage ultérieur et un garde qui arrête le voleur avant qu'il n'atteigne le coffre.

Contre quoi cela protège-t-il

RPP traite les trois menaces fondamentales ensemble, car les attaques modernes sont généralement menées sur plusieurs fronts à la fois :

- **Vol d'identité** — accès aux clés, jetons et mots de passe, souvent sans aucune interaction de l'employé.
- **Vol d'informations** — exfiltration massive de données à la vitesse de la machine.
- **Ransomware** — analyse comportementale associée à une technologie de tromperie des pirates (hacker deception) empêchant le chiffrement, même d'un seul fichier.

Une défense se concentrant uniquement sur le ransomware manquerait les deux premières étapes, là où le véritable dommage commence généralement.

Quel rôle jouent les analyses de mémoire dans l'ensemble de la plateforme ?

Réponse courte : Les analyses de mémoire constituent le socle sur lequel tout le reste est construit. Elles sont la source de détection et d'analyse alimentant toute la modélisation comportementale — protection des données, protection des identités et FortressAI. Chaque décision prise par ces capacités repose sur la connaissance de ce que fait réellement la mémoire d'un programme.

Un socle unique, trois capacités

Cyber Crucible suit l'état de la mémoire d'un programme tout au long de son cycle de vie, du début à la fin, y compris ses interactions en mémoire avec d'autres programmes. Ce flux d'analyse unique est ce qui rend le reste possible :

- **Protection des données** — ce processus se comporte-t-il comme quelque chose sur le point de chiffrer ou d'exfiltrer des données ?
- **Protection des identités** — ce processus est-il le propriétaire légitime de l'identifiant qu'il tente d'utiliser, ou a-t-il été détourné ?
- **FortressAI** — cet outil d'IA est-il toujours lui-même, et son accès aux données respecte-t-il la politique en vigueur ?

Il ne s'agit pas de trois moteurs distincts dotés de trois ensembles de capteurs distincts. Ce sont trois politiques exprimées au-dessus du même modèle comportemental de la mémoire.

Pourquoi la mémoire est le bon socle

Les attaques modernes ne laissent de plus en plus aucun fichier à inspecter. Le code est injecté dans des processus de confiance et construit en mémoire, si bien que le seul endroit où l'activité est visible est l'état mémoire d'un programme en cours d'exécution. Une défense incapable d'observer cet espace est aveugle à toute cette catégorie d'attaques.

L'analyse de la mémoire répond également à la question la plus importante avant d'accorder l'accès à toute ressource sensible : **ce programme est-il toujours ce qu'il prétend être ?** Une application de confiance dont le processus ou les bibliothèques ont été altérés n'est plus digne de

confiance, et seule une inspection au niveau de la mémoire permet de le révéler.

Ce n'est pas un balayage de la mémoire

Il s'agit d'un suivi comportemental en temps réel, et non d'un balayage périodique. Le balayage copie un bloc de mémoire et analyse cet instantané — une photographie plutôt qu'un enregistrement en direct. Sur une machine très sollicitée, l'état du programme peut être totalement différent un instant plus tard, ce qui rend les instantanés utiles pour l'analyse forensique contrôlée, mais beaucoup moins efficaces pour une défense en temps réel.

> Voir également les articles existants sur les *Analyses de mémoire* pour le détail technique de la différence avec le balayage de la mémoire, et ce qui se passe lorsqu'une attaque en mémoire est détectée.

Pourquoi Cyber Crucible fonctionne-t-il au niveau du noyau ?

Réponse courte : Le noyau est la couche la plus profonde et la plus privilégiée du système d'exploitation. Y opérer permet à Cyber Crucible de voir et de contrôler l'ensemble de l'activité du système, d'identifier l'intention malveillante d'un processus et de l'arrêter en quelques millisecondes — et cela rend l'outil bien plus difficile à altérer ou à désactiver pour un attaquant.

Ce que l'accès au noyau apporte

- **Une visibilité complète** sur le comportement de la mémoire, le comportement des processus et l'accès aux fichiers, y compris les activités qui ne touchent jamais le disque.
- **La capacité d'agir**, et pas seulement d'observer — les autorisations peuvent être révoquées et les processus suspendus au moment même de l'intention malveillante.
- **Une résilience**, car les attaquants tenteront inévitablement de désactiver l'outil de sécurité lui-même.

À propos des critiques concernant le développement au niveau du noyau

Certains acteurs historiques et analystes déconseillent le développement au niveau du noyau. L'ingénierie du noyau est véritablement complexe et coûteuse, ce qui explique précisément pourquoi une grande partie du marché l'a évitée — et pourquoi les terminaux sont restés dépendants d'une télémétrie en espace utilisateur que les attaques au niveau root peuvent neutraliser.

La qualité et la résistance à l'altération de Cyber Crucible sont validées par le programme de compatibilité matérielle Windows de Microsoft (WHCP).

Que signifie le fait que Cyber Crucible soit indépendant des bibliothèques Windows ?

Réponse courte : Cyber Crucible ne dépend pas des bibliothèques système Windows qu'il protège. Il en a été délibérément découplé, de sorte que lorsque des attaquants compromettent, font planter ou détournent ces bibliothèques, Cyber Crucible continue de fonctionner, continue d'appliquer les règles et continue de signaler.

Pourquoi cela a été conçu ainsi

Au cours du second semestre 2025, les attaquants se sont tournés vers l'infection des bibliothèques Windows essentielles en mémoire. Étant donné que presque tous les éditeurs de sécurité dépendent de ces mêmes bibliothèques pour fonctionner, cette seule manœuvre a rendu aveugle une grande partie du marché.

Cyber Crucible a consacré environ neuf mois à inventer de nouveaux capteurs, puis cinq mois supplémentaires d'ingénierie pour supprimer entièrement les dépendances aux bibliothèques Windows — y compris l'élimination des dépendances volatiles aux MiniFilters.

À quoi cela ressemble sur le plan architectural

L'architecture fait fonctionner sept sous-systèmes totalement indépendants au sein du noyau, incluant son propre système isolé de chiffrement, de réseau, d'analyse de métadonnées et de suivi des événements. Une phase supplémentaire de ces travaux remplace la bibliothèque réseau standard de Windows (`ws32_2.dll`) par une pile réseau personnalisée au niveau du noyau.

Éprouvé sur le terrain

Avec deux clients, des attaquants bloqués par le moteur de décision opérant uniquement au niveau du noyau ont ensuite tenté d'empêcher que le client soit notifié en attaquant la couche réseau du système d'exploitation. Étant donné que les communications réseau de Cyber Crucible

sont indépendantes du système d'exploitation, la protection a tenu bon et les renseignements sont tout de même parvenus au client.

Cyber Crucible fonctionne-t-il hors ligne ou dans des environnements isolés (air-gapped) ?

Réponse courte : Oui. Toute l'analyse et l'application se font localement sur le poste, si bien que Cyber Crucible assure une protection complète sans connexion internet, sans service cloud et sans aucun signal. Il convient aux réseaux isolés (air-gapped), aux environnements OT et ICS, ainsi qu'aux opérations de terrain déconnectées.

Pourquoi cela fonctionne sans connectivité

Comme la boucle Detect–Decide–Respond s'exécute entièrement dans le noyau sur l'appareil, la connectivité n'est jamais nécessaire pour prendre une décision de protection. La télémétrie se synchronise de manière opportuniste pour la collecte de preuves et le reporting lorsqu'une connexion est disponible, mais la protection n'en dépend pas.

Éprouvé en mer

Dans un déploiement maritime, Cyber Crucible a fonctionné de manière autonome durant des traversées de plusieurs jours sans personnel informatique à bord, s'est adapté à des liaisons satellite à faible bande passante et intermittentes, avec des interruptions dues aux conditions météorologiques, et a conservé des journaux d'investigation numérique riches pendant de longues périodes de déconnexion, en vue d'une analyse post-traversée. Les systèmes protégés allaient des terminaux de loisirs destinés aux passagers aux systèmes de contrôle maritime critiques pour la mission.

C'est également pour cette raison que le même agent convient aux ateliers de production, aux flottes logistiques et à d'autres environnements en périphérie où la connectivité cloud est peu fiable ou délibérément absente.

Pourquoi Cyber Crucible répond-il en suspendant un processus plutôt qu'en arrêtant le système ?

Réponse courte : Suspendre uniquement le processus malveillant — parfois appelé un Selective Freeze — neutralise l'attaque tout en laissant le reste continuer à fonctionner. Il n'y a aucun verrouillage complet du système, aucun redémarrage, et aucune interruption du travail légitime.

Le problème des réponses de type verrouillage

Lorsque de nombreux outils de détection identifient une anomalie, les options de confinement sont brutales : isoler la machine ou la mettre hors ligne. Dans un hôpital, une usine ou une opération de trading, cette réponse peut être presque aussi dommageable que l'attaque elle-même.

Ce que la suspension sélective permet d'accomplir

L'attaque est suspendue en mémoire. Les transactions légitimes ne s'arrêtent jamais. Dans le déploiement de services financiers où près de 10 000 processus malveillants ont été interceptés, les transactions SQL légitimes se sont poursuivies sans interruption tout au long — les opérations n'ont jamais été arrêtées.

C'est ce qui rend la prévention compatible avec la continuité des activités plutôt qu'un compromis à son détriment.