Déploiement dans un environnement déjà infecté

Contexte

Les déploiements chez les clients de Cyber Crucible aboutissent régulièrement à la découverte d'infections jusque-là inconnues. Les réseaux ne sont normalement pas exempts d'infections, même si les outils de défense en cybersécurité existants ont donné le feu vert.

Une attaque par rançongiciel constitue un point de démarcation, ou point pivot, hautement visible, permettant à une entreprise de mesurer à quelle fréquence les pirates réussissent à réattaquer, et avec quel succès.

- Les rapports en source ouverte et le renseignement sur les menaces révèlent un taux de réattaque d'environ 80 % chez les non-clients de Cyber Crucible.
- Cyber Crucible a observé qu'environ 10 % des terminaux subissent au moins une tentative d'usurpation d'identité, telle que le vol de mots de passe, de clés ou de jetons, par période de 90 jours.
- Cyber Crucible observe des attaquants tentant de reprendre pied dans un environnement environ une fois par mois.

Du point de vue de la réponse à incident ou de l'analyse judiciaire (forensique), Cyber Crucible est un excellent outil pour reprendre le contrôle du réseau. En particulier pour les victimes d'attaques, nous soupçonnons que les attaquants conservent une visibilité sur l'état de rétablissement et la santé financière des victimes, afin de mieux choisir le moment de frapper à nouveau.

Ce qui se passe immédiatement après l'installation

Cyber Crucible commence automatiquement à suspendre les programmes en cours d'exécution observés comme ayant un comportement malveillant.

Le déploiement du produit Cyber Crucible peut entraîner la suspension de plusieurs programmes sur plusieurs machines à mesure que l'environnement est nettoyé.

Parfois, un déploiement partiel de Cyber Crucible peut amener le pirate à tenter de reprendre le contrôle via les machines qui ne bénéficient pas de la protection Cyber Crucible.

Par exemple, Cyber Crucible avait été installé sur seulement une partie des postes de travail lors d'une récente violation de données subie par une victime. Les pirates ont tenté de désinstaller Cyber Crucible en se connectant depuis les machines non protégées, puis ont fini par éteindre les machines protégées.

Que se passe-t-il pour les logiciels malveillants dormants, en attente d'une future activation ?

Un logiciel malveillant qui n'agit pas pour le compte des attaquants est déclenché dès qu'il commence à accéder aux données.

Voyons un scénario :

Deux machines contiennent des logiciels malveillants. Appelons-les Machine A et Machine B.

Les deux échantillons de logiciels malveillants sont actuellement indétectables par vos outils de sécurité préférés.

Le logiciel malveillant de la Machine A ne fait rien, mais attend des instructions. Cyber Crucible ne détecte pas le logiciel malveillant. Ce dernier n'est pas non plus encore détectable par d'autres outils de sécurité.

Le logiciel malveillant de la Machine B tente d'accéder à des données ou à des données d'identité. Immédiatement après une attaque réussie, le comportement le plus courant que nous observons, lorsque les attaquants pilotent leur logiciel malveillant, consiste à s'assurer qu'ils disposent de données d'identité fraîches, telles que des mots de passe ou des jetons, et à recenser de nouvelles données. Il s'agit donc en partie de « récupérer les nouveaux mots de passe après que les administrateurs les ont réinitialisés », et en partie de « surveiller l'apparition de nouvelles données ».

Sur la Machine B, Cyber Crucible suspend immédiatement l'application.

Après une période allant d'un mois à un an, le logiciel malveillant de la Machine A finit par être repéré une fois qu'un nombre suffisant de victimes a signalé ce logiciel malveillant aux bases de données des éditeurs de sécurité. Plus les attaquants font preuve de discipline dans la distribution de cet échantillon, plus ce logiciel malveillant particulier échappera longtemps à la détection.

Le logiciel malveillant de la Machine B a été neutralisé, figé sur place.

Le logiciel malveillant de la Machine A est piégé. Dès la seconde (en fait, les 100 millisecondes) où il tente d'accéder à des données ou à des informations d'identité, le logiciel malveillant de la Machine A est suspendu. Le client est protégé, même si le logiciel malveillant existe pendant des jours, voire des années, sans être détecté par d'autres outils.

Détails supplémentaires - Les redémarrages peuvent être utiles

Certaines de nos analyses sont les plus précises lorsque le cycle de vie d'un processus peut être suivi depuis le démarrage de l'application jusqu'à l'état actuel.

Redémarrer une machine après l'installation peut être avantageux.

Les programmes déjà en cours d'exécution avant l'installation ne bénéficieront pas d'une inspection analytique complète de la part de Cyber Crucible. Le redémarrage force ces programmes à se relancer, fournissant ainsi une inspection complète pour tous les programmes.

Revision #1
Created 2026-07-24 06:38:10 UTC by Dennis Underwood
Updated 2026-07-24 06:38:10 UTC by Dennis Underwood