Le cryptojacking dans l'enseignement primaire et secondaire

une introduction

Bienvenue dans notre série sur la cybersécurité dans les établissements primaires et secondaires ! Vous lisez le troisième e-book de la série. Si vous voulez commencer par le début, lisez Introduction aux logiciels malveillants dans l'enseignement primaire et secondaire ou Introduction au phishing dans l'enseignement primaire et secondaire.

Ce nouvel épisode est consacré au **cryptojacking**.

jamf

DANS CET E-BOOK, NOUS ABORDONS :

Qu’est-ce que le cryptojacking ?

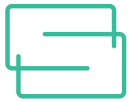
Le cryptojacking combine deux mots : **cryptomonnaie** et **hijacking**, ou détournement. Le cryptojacking consiste à prendre le contrôle d’un ordinateur à l’aide de logiciels malveillants ou de techniques de phishing et à l’utiliser pour miner des cryptomonnaies, des Bitcoins par exemple. Pour comprendre ce qu’est le minage de cryptomonnaie, prenons l’exemple du billet de 100 dollars américains.

C’est plus qu’un simple morceau de papier. Pour imprimer un billet de 100 dollars authentique, il faut :

Un numéro de série unique

De l’encre magnétique et polychrome

De minuscules images imprimées invisibles à l’œil nu et impossibles à imprimer avec une imprimante standard



Un ruban tridimensionnel qui change de motif quand vous changez l’éclairage

Un papier spécifique en mélange de coton et de lin avec des fibres rouges et bleues tissées

S’il manque la moindre de ces caractéristiques sophistiquées, votre billet ne vaut rien. **Les cryptomonnaies authentiques présentent des complexités similaires.**

La cryptomonnaie est le fruit d’un processus complexe, même si elle n’a cours que dans le monde virtuel. Aucune banque centrale n’assure l’émission des cryptomonnaies ni le suivi des transactions. Les cryptomineurs assument le rôle de banquiers et tiennent un registre des transactions en cryptomonnaies effectuées par d’autres personnes pour veiller à ce qu’elles ne dépensent pas deux fois la même somme. En échange de quoi, ils sont autorisés à créer des cryptomonnaies qu’ils peuvent conserver ou à vendre. Mais comme pour notre billet de 100 dollars, il faut prouver l’authenticité de la cryptomonnaie.

Selon les règles de la communauté des cryptomonnaies, le mineur qui veut prouver qu’il a validé une transaction doit résoudre un problème mathématique hautement complexe, et plus précisément un hachage cryptographique. Ce calcul est hors de portée d’une calculatrice ordinaire ; il faut beaucoup de temps et de puissance de calcul pour déchiffrer le code.

Du fait de sa complexité, cette activité mobilise une grande partie de la puissance de traitement d’un appareil, qui peut ralentir au point de devenir inutilisable. C’est là que réside l’un des dangers du cryptojacking : **les pirates gagnent littéralement de l’argent pendant que votre ordinateur se noie sous les calculs**. C’est d’ailleurs pour cela qu’ils cherchent à prendre le contrôle des appareils de leurs victimes. Cela leur évite d’acheter des appareils spécifiquement destinés au minage de cryptomonnaies ou de dédier leurs machines à ces calculs. Ils préfèrent attaquer le plus grand nombre d’appareils possible pour augmenter leurs profits sans accroître leurs coûts.

Comment se manifeste le cryptojacking ?

Les logiciels malveillants de cryptojacking peuvent s'introduire dans votre ordinateur de différentes manières. Ils peuvent provenir d'un téléchargement **sur un site web tiers**, d'une **pièce jointe à un e-mail, d'un clic sur un lien malveillant**, etc. Examinons un scénario classique :

1

Vous êtes amateur de rétrogaming.

2

Sur un forum de jeux populaire, vous voyez un lien pour télécharger Super Mario.

3

Mario Forever. Vous avez beaucoup entendu parler de ce jeu, alors vous le téléchargez.

4

Ce téléchargement inclut le jeu, mais aussi un logiciel malveillant de cryptojacking. Une fois le programme d'installation exécuté, le jeu et le logiciel malveillant sont tous les deux actifs dans votre système.

5

Le logiciel malveillant collecte des informations sur votre matériel et se connecte à un serveur de minage pour commencer l'extraction.

6

Dissimulé derrière des noms de processus bien réels, le minage se poursuit à votre insu. Le logiciel malveillant installe également un outil qui vole vos données privées.

Ce scénario n'a rien d'hypothétique, comme l'explique Bleeping Computer. Et on imagine très bien qu'un étudiant peu méfiant se retrouve dans cette situation. Il est même probable qu'il ne s'en rende pas compte avant que son ordinateur ne commence à ralentir ou à se comporter bizarrement.

Le cryptojacking dans les établissements d'enseignement primaire et secondaire

Très bien, mais en quoi cela concerne-t-il les écoles ?

Le cryptojacking est une menace croissante. Selon le Rapport sur les cybermenaces 2024 de SonicWall, le cryptojacking **a augmenté de 659 %** en 2023 par rapport à 2022. On a d'ailleurs enregistré davantage d'attaques de cryptojacking pendant les mois de novembre et décembre 2023 que durant toute l'année 2022 !

Ces chiffres concernent tous les secteurs, mais les établissements d'enseignement primaire et secondaire ne font pas exception. Dans une analyse de cybersécurité sur l'année scolaire 2022-2023, le Center for Internet Security a constaté que CoinMiner, un outil de cryptojacking, représentait **20 % des attaques de logiciels malveillants ayant visé les écoles**. CoinMiner est ainsi devenu le deuxième logiciel malveillant le plus répandu dans l'enseignement primaire et secondaire.

Le cryptojacking nuit aux écoles à plusieurs titres :

- Quand l'appareil d'un élève ralentit ou cesse de fonctionner, il est gêné pour suivre en classe et faire ses travaux tant que le problème n'est pas résolu.
- Les appareils infectés consomment inutilement la bande passante du réseau qui devrait être réservé à des fins éducatives.
- Selon la manière dont ils sont conçus, les logiciels malveillants de cryptojacking peuvent exposer les appareils à d'autres attaques.
- Le cryptojacking pousse les appareils à consommer beaucoup d'énergie, ce qui représente un coût supplémentaire pour les écoles.

En d'autres termes, la présence croissante du cryptojacking est une véritable menace pour l'apprentissage et l'enseignement. Apprenons à l'éviter.

Prévenir le cryptojacking

Gestion des appareils

Si vous avez lu les autres e-books de cette série, vous le savez déjà : **il n'y a pas de sécurité sans gestion des appareils, parce qu'on ne peut sécuriser ce que l'on ne voit pas.** Quand un appareil est ajouté à une solution de gestion des appareils mobiles (MDM), les administrateurs informatiques peuvent :

- Voir à quelles ressources l'appareil se connecte
- Vérifier si l'appareil répond aux normes de sécurité
- Définir des règles de sécurité, par exemple pour imposer l'utilisation d'un code secret
- Installer des applications sur l'appareil
- Bloquer l'accès aux sites web inappropriés ou malveillants
- Maintenir les appareils et les logiciels à jour

Il est essentiel que les appareils restent à jour et reçoivent les derniers correctifs de sécurité pour se protéger contre de nombreux logiciels malveillants et en particulier le cryptojacking. Les solutions MDM offrent des capacités de gestion des correctifs qui veillent à ce que les appareils et les applications soient rapidement mis à jour lors de la publication de nouveaux correctifs.

Surveillance des réseaux

Parce qu'il s'exécute le plus souvent en arrière-plan, le cryptojacking peut être difficile à repérer. Mais il laisse tout de même des traces ! La surveillance du réseau permet d'identifier d'éventuelles attaques. Par exemple, vous observerez peut-être :

- Des communications fréquentes avec un serveur inconnu
- Des requêtes à tout moment de la journée, même lorsque personne n'utilise les appareils
- Une augmentation globale de l'utilisation du réseau

Pour repérer ces anomalies, il faut d'abord établir le comportement de référence, et donc entamer la surveillance avant la survenue d'une attaque. Les outils de surveillance dotés d'intelligence artificielle (IA) et de machine learning (ML) repèrent plus facilement les comportements inhabituels. C'est une réalité, l'IA et le ML n'ont pas besoin de faire des pauses et ne quittent jamais l'enceinte de l'école ; ils travaillent 24 heures sur 24, 7 jours sur 7 pour repérer les anomalies.

Prévenir le cryptojacking

Filtrage de contenu

Le filtrage de contenu peut grandement contribuer à la prévention de menaces telles que le cryptojacking en bloquant l'accès aux sites web susceptibles de diffuser des logiciels malveillants. Le filtrage intelligent, qui utilise l'IA et le ML, est plus performant que les listes de blocage et d'autorisation tenues à la main, et qui peuvent passer à côté de sites dangereux. Les élèves peuvent toujours explorer le Web en liberté, mais ils ne risquent pas d'arriver sur des sites inappropriés ou malveillants qui tenteront de leur voler leurs données.

Sensibilisation des utilisateurs

Les pirates ont recours à toutes sortes d'astuces pour inciter les utilisateurs à télécharger des logiciels malveillants. Former les utilisateurs à reconnaître les signes suspects peut être très efficace face à ces tentatives. Les utilisateurs doivent apprendre :

- À ne pas télécharger de pièces jointes et des fichiers sans s'assurer de leur légitimité.
- Les signes courants de phishing
- Quoi faire s'ils téléchargent, cliquent sur ou reçoivent quelque chose de potentiellement malveillant
- À éviter de télécharger des fichiers à partir de sites web tiers
- Les signes d'infection de leur appareil, comme une baisse des performances ou une dégradation soudaine de l'autonomie de la batterie.

MISE EN ŒUVRE : JAMF SCHOOL ET JAMF SAFE INTERNET

Pour améliorer la cybersécurité des écoles, nous proposons des solutions MDM et de sécurité conçues spécialement pour elles.

Jamf School

Jamf School est une solution MDM conçue pour aider les administrateurs informatiques, les enseignants, les parents et les élèves dans leurs efforts pour une éducation de qualité. Jamf School apporte :

- Une visibilité sur les appareils gérés, les utilisateurs et les applications
- Une méthode simple pour le déploiement et la mise à niveau des logiciels
- La possibilité de configurer les réglages de sécurité des appareils, notamment en imposant l'utilisation d'un code secret et en appliquant le filtrage des contenus
- Une méthode robuste et sécurisée de déploiement et de mise à jour des applications approuvées préalablement par l'équipe informatique
- Des outils de gestion de la salle de classe pour maintenir l'attention des élèves

La technologie et la gestion vont de pair. Jamf School donne aux administrateurs toutes les informations dont ils ont besoin pour assurer la sécurité des appareils et de leurs utilisateurs.

Jamf Safe Internet

Jamf Internet Safe applique un filtrage de contenu adapté au contexte scolaire et une protection contre les menaces du réseau. Cet outil protège les étudiants, les appareils et les données de l'établissement contre les pirates et les contenus malveillants. Jamf Safe Internet apporte :

- Un système de déploiement simple avec des règles entièrement personnalisables
- Une navigation sécurisée grâce à Google SafeSearch et au mode limité de YouTube
- Le filtrage des contenus sur l'appareil, qui protège contre les menaces connues et inconnues grâce à l'intelligence artificielle et au machine learning avancé
- Une protection sur le réseau pour bloquer les menaces de type « zero day » telles que les sites de phishing et les domaines malveillants.
- Le plafonnement des données et des alertes lorsque les seuils d'utilisation des données sont atteints.

Jamf Safe Internet fonctionne avec tous les types d'appareils : poste informatique mobile, appareil scolaire individuel et appareils personnels utilisés à l'école, même en dehors du périmètre du réseau de l'établissement. Et contrairement aux logiciels malveillants de cryptojacking, les solutions Jamf ne ralentissent pas vos appareils et respectent votre vie privée.

jamf

Découvrez comment Jamf peut enrichir votre solution de gestion de la technologie, de sécurité et de filtrage de contenu.

Lancez-vous !

www.jamf.com/fr