Les logiciels malveillants dans l'enseignement primaire et secondaire

une introduction

Bienvenue dans notre série sur la cybersécurité dans les établissements primaires et secondaires ! Nous partons à la découverte de quelques-unes des menaces les plus courantes auxquelles les écoles sont confrontées - des menaces qui nuisent à la sécurité de l'environnement d'apprentissage et qui peuvent avoir des conséquences pour les élèves, même après leur départ de l'école. Nous verrons **ce qu'ils sont, comment ils affectent les écoles et comment les prévenir**.

L'étape du jour : **les logiciels malveillants**.

jamf

DANS CET E-BOOK, NOUS ALLONS NOUS PLONGER DANS LES LOGICIELS MALVEILLANTS QUI CIBLENT LE DOMAINE DE L'ÉDUCATION EN ABORDANT SPÉCIFIQUEMENT :

Qu’est-ce qu’un logiciel malveillant ?

Les logiciels et micrologiciels malveillants constituent une menace importante pour les établissements primaires et secondaires. Ils présentent de nombreuses formes et emploient de nombreux moyens, et c’est pourquoi il est aussi difficile de s’en défendre. En général, les logiciels malveillants visent à compromettre la confidentialité, l’intégrité et/ou la disponibilité des données ou des applications d’un système.

Le groupe de pirates informatiques Vice Society, par exemple, a mené **43 attaques par ransomware contre des écoles entre juin 2022 et mai >2023**. L’agence américaine de cybersécurité et de sécurité des infrastructures (CISA) **explique la méthode employée par Vice Society** :

1. Exploiter des applications accessibles par Internet pour recueillir des identifiants compromis et obtenir un accès initial.
2. Explorer le réseau et trouver des moyens d’étendre l’accès aux données.
3. Échapper à la détection en déguisant les logiciels malveillants en fichiers légitimes.
4 Exfiltrer des données.
5 Déployer un ransomware, en menaçant de publier les données sensibles si la rançon n’est pas payée.

Cette situation est effectivement très inquiétante. Mais les écoles ont le pouvoir de réduire le risque de succomber à ces attaques.

Apprendre la sécurité en classe

Les logiciels malveillants sont une catégorie spécifique de logiciels, spécialement conçus pour être néfastes. Ils peuvent avoir de nombreuses fonctions différentes : espionner des individus, voler des informations, prendre le contrôle d’un ordinateur ou inciter les gens à verser de l’argent.

Idées de cours :

1. Demandez aux élèves de créer un sketchnote qui illustre ce que sont les logiciels malveillants.

2. Créer un rap sur le thème de la sécurité face aux logiciels malveillants.

Les différents types de logiciels malveillants

RANÇONGICIELS

Les ransomwares, ou rançongiciels, sont des logiciels malveillants qui permettent à des pirates d'accéder aux fichiers d'un utilisateur, de les chiffrer et de les rendre inaccessibles. Pour récupérer l'accès à ses fichiers, l'utilisateur doit verser une rançon. Les pirates peuvent exiger un paiement pour déchiffrer les données et confirmer qu'ils ont bien supprimé les données de leurs propres systèmes.

CHEVAUX DE TROIE

Les chevaux de Troie prennent l'apparence de programmes légitimes, mais ils contiennent en réalité du code malveillant. Ce code peut être associé à des fichiers téléchargés sur Internet, comme des versions piratées ou compromises de logiciels connus.

Les chevaux de Troie créent des portes dérobées qui permettent ensuite à des acteurs malveillants d'entrer et de sortir d'un réseau, d'exploiter les vulnérabilités des applications, de déposer des ransomwares et bien d'autres choses encore. Contrairement aux virus et aux vers, les chevaux de Troie ne se reproduisent pas d'eux-mêmes et ne se propagent pas à d'autres systèmes. Ils peuvent toutefois contenir des logiciels malveillants qui, eux, sont capables de se reproduire et de se répandre.

VIRUS

À l'instar des virus qui nous rendent malades et se répandent dans la population, les virus logiciels sont capables de se multiplier et de se propager à d'autres appareils grâce aux interactions des utilisateurs. Comme ils restent dormants jusqu'à ce qu'une action de l'utilisateur les active, il est souvent difficile d'en identifier la source.

Les virus remplissent de nombreuses fonctions pour les pirates : ils peuvent désactiver ou lancer des applications, afficher des fenêtres contextuelles ou envoyer des e-mails en masse à l'insu de l'utilisateur. Ils se propagent grâce à des liens contenus dans des e-mails, des pièces jointes ou des téléchargements en ligne. Ils perturbent les systèmes, provoquent des problèmes opérationnels majeurs et entraînent des pertes et des fuites de données.

Apprendre la sécurité en classe

Idée de cours :

1. Demandez aux élèves de créer une courte vidéo sur un autre type de logiciel malveillant.

2. Imaginez un jeu ! Créez un jeu d'association et demandez aux élèves de relier le nom des différents logiciels malveillants à leur description.

VERS

Comme les virus, les vers sont capables de se reproduire en toute autonomie. Mais contrairement à eux, ils se propagent d'eux-mêmes en se frayant un chemin d'un appareil à l'autre. Les vers sont utilisés pour créer des portes dérobées, déployer d'autres logiciels malveillants, collecter des données, surcharger les réseaux, etc. Pour se propager, ils utilisent notamment le phishing et divers moyens de communication ou de partage de fichiers, en exploitant les vulnérabilités des logiciels et des réseaux.

CRYPTOJACKING

Le cryptojacking, qui consiste à prendre le contrôle d'un ordinateur pour lui faire miner des cryptomonnaies, est une menace croissante pour les institutions. Selon Sonicwall, les cas de cryptojacking se sont multipliés par 320 au cours du premier semestre de 2023. Le cryptojacking, contrairement au ransomware, ne manifeste pas bruyamment sa présence sur un appareil. Bien au contraire, il exploite la puissance de calcul de votre appareil, au point de réduire la vitesse de votre système jusqu'à 70 %.

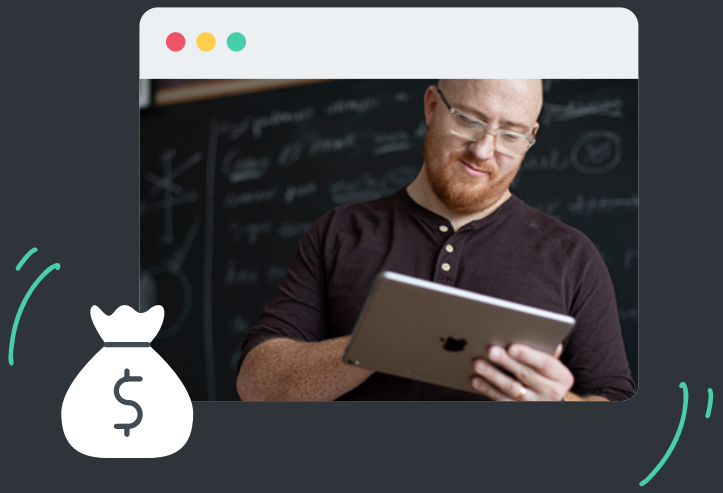
Restez à l'écoute : dans un prochain épisode de cette série d'e-books, nous nous pencherons sur cette problématique en hausse dans les établissements scolaires.

LOGICIELS ESPIONS

Les logiciels espions suivent discrètement l'activité d'un appareil. Ils peuvent, par exemple, enregistrer les mouvements de la souris, les clics et tout autre type d'action de l'utilisateur. Ils servent notamment à recueillir des identifiants ou des informations personnelles.

Bien qu'il ne s'agisse pas techniquement d'un logiciel espion, certaines écoles choisissent de surveiller les ordinateurs qu'elles mettent à disposition des élèves, pour préserver leur concentration et assurer leur sécurité. Mais cette approche offre-t-elle réellement un gain de sécurité ? Ce type de logiciel **soulève des inquiétudes quant au respect de la vie privée** et au bien-être des élèves, sans pour autant sécuriser l'environnement.

LOGICIELS MALVEILLANTS DANS L'ENSEIGNEMENT PRIMAIRE ET SECONDAIRE



80 %

des participants de l'enseignement primaire ont été touchés par un ransomware, soit une augmentation de 24 % par rapport à 2022. Sans payer la rançon, le coût de récupération des données s'élevait en moyenne à **1,59 million de dollars.**

Les **logiciels malveillants peuvent entrer dans un système par l'intermédiaire d'un enseignant, d'un élève ou d'un administrateur**, compromettant potentiellement les données de chacun de ces groupes. En **2020, le système scolaire public de Toledo a été victime d'une violation de données**. Des pirates ont tenté d'utiliser les informations des enfants scolarisés pour ouvrir des comptes de carte de crédit, contracter des prêts automobiles et commettre d'autres escroqueries du même type. En 2020, une attaque contre un district scolaire américain a permis aux pirates d'accéder aux informations personnelles identifiables (PII) de plus de 500 000 élèves et à des renseignements sur plus de 56 000 employés. Les élèves, souvent bien trop jeunes pour avoir une carte de crédit, sont particulièrement en danger lorsque leurs données sont exposées.

Les ransomwares représentent un enjeu de cybersécurité majeur dans l'éducation. Cette menace pittoresque est malheureusement bien réelle et très fréquente, en particulier dans les écoles. Les **établissements du primaire et du secondaire sont même la cible privilégiée** des ransomwares. Dans le rapport intitulé **L'État des ransomwares dans l'éducation 2023** et publié par Sophos, **80 % des participants issus de l'enseignement primaire disaient avoir été touchés par un ransomware, soit une augmentation de 24 % par rapport à 2022. Sans payer la rançon, le coût de récupération des données s'élevait en moyenne à 1,59 million de dollars.**

Pourquoi les écoles sont-elles une cible privilégiée des ransomwares ?

Les établissements scolaires n'ont pas toujours la même préparation ni les mêmes ressources que les entreprises. Cela peut s'expliquer par un manque de sensibilisation, de budget ou de solutions logicielles adaptées. De ce fait, les **écoles victimes d'attaques informatiques subissent généralement** :

3 à **21** jours d'apprentissage **perdus**

Un rétablissement **pouvant durer** plusieurs mois

Le paiement d'une rançon de près de **900 000 $**

(quand elles choisissent de payer)

L'exposition possible de **données sensibles**

Heureusement, **la plupart des établissements récupèrent leurs données**.

73 % ont utilisé des sauvegardes

47 % ont payé la rançon

2 % ont utilisé d'autres moyens

Mais attention : cela ne signifie pas nécessairement que la fuite de données a été endiguée. Les pirates peuvent avoir vendu ou diffusé les données d'une façon quelconque.

PROTECTION CONTRE LES LOGICIELS MALVEILLANTS

Selon le rapport Sophos sur l'état de l'éducation, les attaques par ransomware exploitent principalement :

- Des vulnérabilités
- Des identifiants compromis
- Des e-mails malveillants
- Le phishing

La stratégie consiste en partie à arrêter les logiciels malveillants avant qu'ils ne s'installent dans votre système. Et comme aucune défense n'est sans faille, il faut également avoir les moyens de se rétablir en minimisant l'impact sur l'apprentissage, les coûts et les temps d'arrêt. La question n'est pas de savoir si une école va être attaquée, mais *quand*. Voyons comment réduire l'impact des logiciels malveillants sur votre système de plusieurs manières.

Vos appareils et les règles de votre école sont configurés pour empêcher les logiciels malveillants de s'installer, mais chacun peut agir !

Voici ce que vous pouvez faire :

1. Ne communiquez jamais vos identifiants à qui que ce soit.

2. Ne téléchargez pas de fichiers ou de logiciels sur Internet. Vérifiez qu'ils proviennent d'une source fiable et posez la question si vous n'êtes pas sûr.

3. Faites attention à la destination des liens avant de cliquer. Le nom et l'apparence du site web sont-ils parfaitemnt conformes ? S'il vous semble suspect, ne saisissez pas vos informations. Il est souvent préférable de retaper l'adresse du site web pour être sûr que vous êtes sur la bonne page.

4 Mettez à jour vos appareils en installant les versions les plus récentes des logiciels.

DISTRIBUTION ET MISE À JOUR DES LOGICIELS

La mise à jour des applications et des systèmes d'exploitation permet de réduire le risque d'exploitation des vulnérabilités. Les pirates peuvent créer des logiciels malveillants qui ciblent les vulnérabilités présentes dans des applications courantes. Ils cherchent généralement à acquérir des privilèges de niveau supérieur ou à diffuser d'autres logiciels nuisibles.

Les téléchargements en ligne, qu'ils proviennent de sources fiables ou non, - peuvent être porteurs de logiciels malveillants. On peut donc éviter une partie du problème en interdisant le téléchargement de logiciels. Selon la façon dont les appareils sont gérés, plusieurs options permettent de déployer des applications approuvées auprès des utilisateurs :

- Portail Jamf Self Service
- App Store
- Apple School Manager
- **Via votre solution MDM**

L'AUTHENTIFICATION MULTIFACTEUR

L'authentification multifacteur (AMF) est la première ligne de défense face au risque de compromission d'identifiants. L'AMF exige au moins deux facteurs d'authentification avant d'autoriser la connexion à un compte.
Ces facteurs sont de plusieurs types :

- Une information que vous **connaissez**, comme un mot de passe ou un code PIN
- Un objet que vous **avez**, comme une application d'authentification ou un badge.
- Un élément de votre **identité**, comme une empreinte digitale, un scan de la rétine ou du visage

Les appareils offrant un mode d'authentification biométrique, comme l'iPad, peuvent être plus simples pour les jeunes élèves qui n'ont pas forcément accès à un autre outil d'authentification. Les écoles et les administrations scolaires peuvent ajouter une deuxième ligne en associant l'authentification unique (SSO) à la MFA pour éviter aux élèves de devoir retenir d'innombrables mots de passe.

SAUVEGARDES

Comme le laissent entendre les paragraphes précédents, les sauvegardes peuvent faire toute la différence lors d'une attaque de ransomware. Effectuées régulièrement, elles peuvent également servir de point de restauration si vos systèmes sont compromis par un autre type de logiciel malveillant. Ces deux avantages justifient à eux seuls l'importance stratégique des sauvegardes pour maintenir l'intégrité et la sécurité de vos données.

Apprendre la sécurité en classe

Idée de cours :

1. Demandez aux élèves de créer une présentation sur une autre méthode de prévention différent et d'expliquer pourquoi elle contribue à la sécurité de tous.

GESTION DES APPAREILS

La gestion des appareils mobiles (MDM) sert de base pour préserver la santé des appareils. Une solution MDM permet aux administrateurs de :

- Tenir un inventaire des appareils connectés aux ressources de l'école.
- Déterminer la conformité des appareils aux critères de sécurité et intervenir si nécessaire
- Mettre à jour les appareils et leurs applications en installant les dernières versions des logiciels
- Exiger certaines règles de sécurité pour réduire le risque de violation des données
- Empêcher l'accès à certaines applications et/ou sites web

FILTRAGE DE CONTENU

Malgré une bonne sensibilisation, les gens commettent des erreurs, en particulier sur les appareils mobiles où il est difficile de prévisualiser les liens. En bloquant les liens malveillants, les **outils de filtrage de contenu** s'avèrent très utiles pour prévenir les attaques. Par exemple, si un étudiant reçoit un e-mail de phishing bien fait et clique sur un lien destiné à recueillir ses identifiants, le filtrage de contenu peut bloquer son accès au site malveillant.

CADRES DE SÉCURITÉ

Les écoles et les administrations scolaires ne disposent pas toutes du personnel, des finances ou des ressources nécessaires pour mettre en œuvre les différents éléments d'un cadre de sécurité, mais ils définissent tout de même des objectifs à atteindre. Les cadres de sécurité suivants orientent les équipes informatiques vers la configuration la plus sûre possible en fonction de leurs ressources :

- **« Cyber Essentials » de l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA)**
- **« Cyber Essentials » britanniques**
- **Bibliothèque d'infrastructure informatique (ITIL)**

jamf

Apprendre la sécurité en classe

Sensibilisation des utilisateurs :

Il n'est jamais trop tôt pour apprendre à faire preuve de vigilance en matière de cybersécurité. Les élèves, les enseignants et le personnel doivent être informés des comportements à risque :

- Cliquer sur des liens sans vérifier leur légitimité
- Partager des identifiants de connexion
- Insérer des clés USB inconnues ou d'autres supports amovibles dans leur ordinateur
- Télécharger des logiciels à partir de sites tiers
- Ne pas mettre à jour leur appareil ou leurs applications.

Les attaques par phishing sont extrêmement courantes : les utilisateurs doivent savoir les reconnaître.

Quelques indices à repérer :

- URL presque identique à l'URL légitime, mais présentant des caractères spéciaux ou un format étrange
- Fautes d'orthographe ou formulations inhabituelles dans un e-mail (mais sachez que les pirates créent des messages de plus en plus crédibles).
- Demande d'action urgente
- Messages inhabituels ou non sollicités, y compris de la part de personnes que vous connaissez

MISE EN ŒUVRE :

JAMF SCHOOL ET JAMF SAFE INTERNET

Très bien, nous avons vu plusieurs moyens de prévenir les logiciels malveillants. Mais comment mettre en œuvre ces stratégies ?

Jamf School

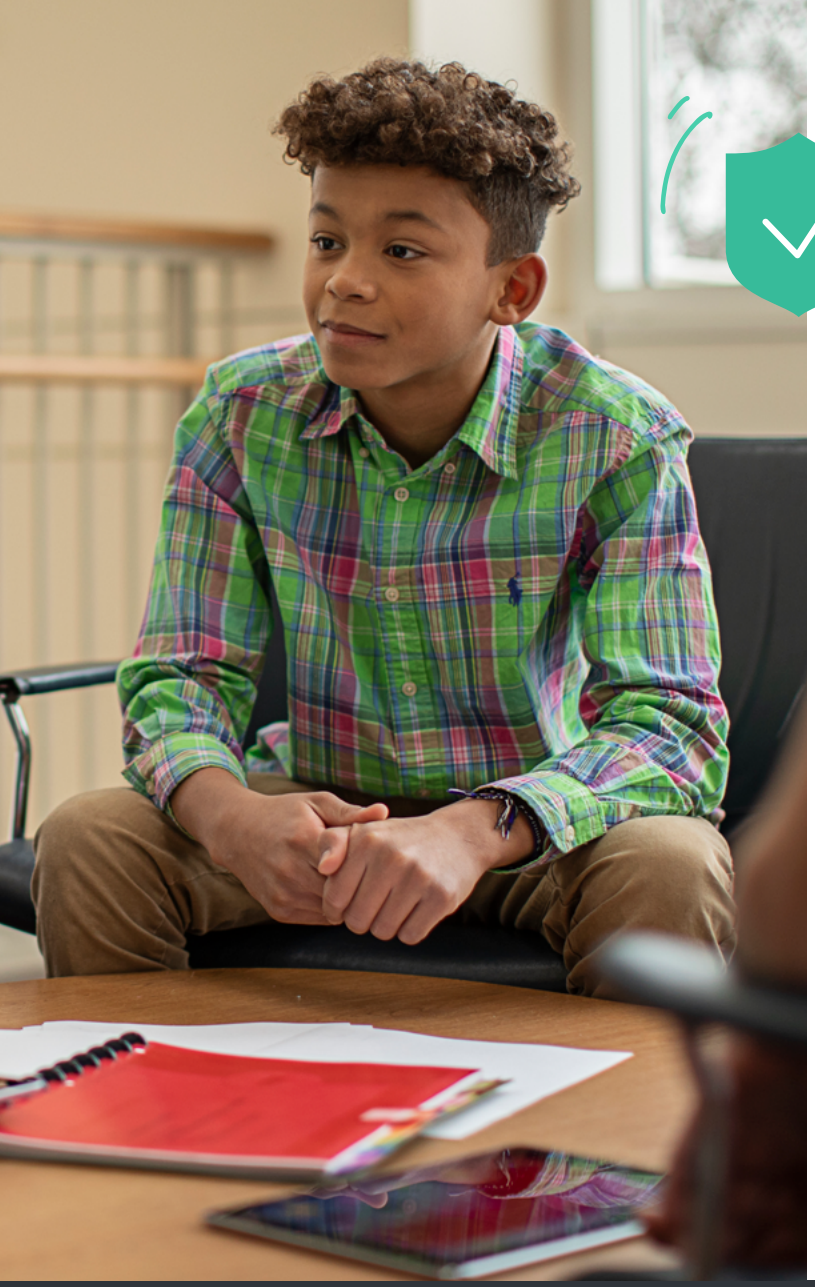
Nous avons dit que la gestion des appareils mobiles est un socle pour la sécurité des appareils sécurisés. Sans être suffisante, elle joue un rôle essentiel en donnant de la visibilité sur les appareils qui interagissent avec les données des élèves et des employés.

D'une certaine manière, **gestion et sécurité sont synonymes.**

Jamf School est une solution MDM axée sur l'éducation. Elle simplifie le déploiement, la gestion et la sécurisation des Mac, des iPad, des iPhone et des Apple TV. Elle offre :

- 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
- Des outils de gestion de la salle de classe pour maintenir l'attention des élèves

La sécurité commence par la gestion. Quand vous connaissez vos appareils et ce qu'ils contiennent, vous pouvez assurer leur sécurité, que ce soit en mettant à jour les logiciels nécessaires ou en déployant des contrôles de sécurité spécifiques.



Jamf Safe Internet

Jamf Safe Internet va au-delà de la gestion pour sécuriser l'environnement d'apprentissage. Cette solution permet aux élèves à naviguer en toute confidentialité, à l'abri des logiciels malveillants et des contenus dangereux. Compatible avec les appareils Apple, ChromeOS et Windows, Jamf Safe Internet :

Est entièrement personnalisable et permet de définir et modifier des règles, puis de les appliquer à différents groupes d'appareils selon leur type, la localisation ou d'autres attributs. Jamf Safe Internet fonctionne avec n'importe quel appareil géré : poste informatique mobile, appareil scolaire ou appareil personnel.

Filtre les contenus web de façon performante en appliquant :

- Google SafeSearch
- Le mode limité de YouTube, qui permet d'afficher uniquement des contenus éducatifs
- Du machine learning avancé pour détecter et prévenir les menaces émergentes
- Une protection en temps réel au sein du réseau pour empêcher l'accès aux sites de phishing et autres domaines malveillants.

Sécurise sans surveiller, en autorisant les élèves à explorer Internet et à développer leur citoyenneté numérique, tout en respectant leur vie privée et en préservant leur bien-être.

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