Anatomie des cyberattaques dans l'éducation : menaces réelles et méthodes de défense

Introduction

Dans le monde de l'éducation, les professionnels de l'informatique et de la cybersécurité sont constamment confrontés à des acteurs malveillants. En effet, il leur suffit d'une vulnérabilité ou d'un identifiant compromis pour prendre pied dans un réseau scolaire – alors que vous, en défense, devez réussir à chaque fois.

Dans le monde connecté d'aujourd'hui, la moindre erreur peut exposer les établissements à des problèmes de conformité ou à des attaques de phishing ouvrant la porte à une violation de données, et c'est l'ensemble de l'infrastructure qui peut en subir les conséquences.

> ***« Le savoir, c'est le pouvoir ».***
> – Thomas Jefferson

La citation ci-dessus vaut autant pour les gentils que pour les méchants. Les pirates doivent connaître les failles des défenses des établissements pour identifier et cibler les points faibles. Inversement, les gentils ont tout intérêt à comprendre la nature des cyberattaques qui les visent pour anticiper les plans d'attaque de leurs adversaires.

Dans ce document, nous allons :

- Décomposer la cyber kill chain
- Présenter une attaque réussie contre un établissement scolaire
- Opposer des protections stratégiques aux enchaînements de l'attaque
- Rappeler l'importance de combler les failles de sécurité

En observant à la loupe chaque phase de la cyber kill chain et en examinant attentivement l'anatomie d'une attaque, les équipes d'assistance du secteur de l'éducation peuvent réduire les risques et renforcer leurs protections grâce à des boucles de rétroaction. **Avant d'aborder la cyber kill chain, rappelons pourquoi les acteurs malveillants ciblent le secteur de l'éducation.**

Pourquoi les écoles sont-elles une cible aussi attractive ?

Leurs ressources limitées, leur infrastructure obsolète et leurs données précieuses font des établissements d'enseignement des cibles de plus en plus attrayantes pour les cybercriminels. *Les écoles du monde entier éprouvent des difficultés à maintenir une posture de sécurité solide* tout en répondant à des besoins essentiels tels que le recrutement personnel, les services aux élèves et les salaires. Les contraintes financières, l'ancienneté du matériel et des logiciels et la détention d'un grand volume de données sur les étudiants et les enseignants se combinent pour créer une situation de grande vulnérabilité qui dépasse les capacités et les ressources du service informatique. Ces facteurs créent un effet domino qui fait des institutions scolaires des cibles de choix pour les acteurs malveillants.

Des ressources limitées

Faire plus avec moins : bien plus qu'un dicton, c'est un véritable mode de vie pour tous les acteurs du monde de l'éducation, des étudiants aux enseignants en passant par l'administration. Bien que ce document s'intéresse à la prévention des menaces plutôt qu'aux limites budgétaires, il n'en reste pas moins que les celles-ci nuisent aux efforts de cybersécurité des administrations scolaires du monde entier. Bien d'autres aspects essentiels se disputent les fonds qui pourraient servir à la sécurité : recrutement du personnel, qualité des repas des étudiants, compétitivité des salaires, etc.

Les établissements font souvent de leur mieux pour affecter des fonds à des cas d'utilisation spécifiques, mais le manque de ressources financières oblige souvent les administrateurs à privilégier certaines fonctions au détriment d'autres qui sont tout aussi vitales. Les acteurs malveillants l'ont bien compris, ce qui explique en grande partie le succès de leurs attaques contre les écoles. Plusieurs facteurs contribuent à la réussite des attaques :

Ordinateurs obsolètes

On considère généralement que la durée de vie utile d'un ordinateur est de 3 à 5 ans. L'absence de prise en charge des nouvelles fonctionnalités de sécurité, les baisses de performance et les problèmes de compatibilité nuisent à la convivialité des machines, pour les étudiants comme pour les enseignants.

Logiciels dépassés

Tout comme le matériel, les logiciels doivent être tenus à jour pour réduire au minimum les vulnérabilités de sécurité. Bien que l'accès aux dernières versions du code soit moins problématique avec les applications sur abonnement, leur coût à long terme peut dépasser celui d'une licence perpétuelle, et il peut devenir difficile de tenir le rythme des mises à niveau.

Dépendance à l'égard d'une plateforme unique

Les solutions adaptées à une plateforme spécifique sont connues pour offrir une prise en charge complète de l'OS pour lequel elles ont été conçues. À l'inverse, les solutions généralistes compensent souvent un coût de service inférieur par une prise en charge lacunaire. Le résultat : des appareils mal gérés et mal protégés.

Personnel informatique surchargé

En règle générale, on compte en moyenne 1 informaticien pour 100 employés. Mais **dans le secteur de l'éducation, c'est trois fois moins** : il y en a 1 pour 300 personnes, voire plus. Le manque de personnel et l'épuisement des équipes sont de puissants facteurs d'affaiblissement de la posture de sécurité et de dégradation de la conformité dans les secteurs réglementés tels que l'éducation.

Manque de compétitivité des salaires

La fourchette de salaire moyenne des techniciens informatiques (aux États-Unis) est de 45 000 à 71 000 $ par an avec 1 à 3 ans d'expérience. Dans le secteur de l'enseignement, un technicien aux qualifications équivalentes touchera 42 000 à 63 000 $ par an. Si l'on ajoute à cela les problèmes de sous-effectif, **ce salaire inférieur de 9 % à la valeur du marché** ne permet pas d'attirer et de retenir les meilleurs talents, et la sécurité des réseaux scolaires s'en ressent négativement.

Manque de formation continue

Les techniciens informatiques veulent acquérir de nouvelles compétences et élargir leur base de connaissances : la formation structurée figure en effet parmi les **trois principales demandes formulées par les équipes informatiques** à leurs supérieurs. Henry Ford a résumé l'enjeu du coût dans une formule simple : *« La seule chose qui soit pire que de former vos employés pour les voir partir, c'est de ne pas les former et qu'ils restent. »*

Des données précieuses

Sensibles et exploitables à long terme, les données des établissements primaires et secondaires constituent une cible de choix pour les cybercriminels, d'autant que les ressources pour les protéger sont limitées. Les données personnellement identifiables (IPI) des élèves peuvent être exploitées à des fins de fraude financière, d'usurpation d'identité et d'ingénierie sociale, et leur circulation passe souvent inaperçue pendant des années. Les conséquences juridiques et financières d'une violation peuvent être très lourdes, tout comme les dommages qu'elle peut causer à la réputation d'un établissement. De leur côté, les pirates considèrent les institutions scolaires comme des coffres-forts où sont entreposés de véritables trésors numériques, mais sans les puissantes mesures de sécurité des banques pour les protéger.

Demandes de rançon

L'une des principales motivations du vol de données réside dans la valeur qu'elles représentent pour les établissements et les personnes concernées. Les acteurs malveillants en sont parfaitement conscients : leur but est d'extorquer de l'argent en échange de la promesse que les données sensibles ne seront pas diffusées. Le montant varie selon les incidents, mais le **coût moyen d'une violation de données par ransomware** se situe entre 4,38 et 5,37 millions de dollars. REMARQUE : *La fourchette correspond au coût de confinement de l'incident et n'inclut pas le paiement de la rançon.*

Réputation

Lorsqu'une attaque est rendue publique, les ennuis ne font que commencer. Les incidents provoquent souvent des enquêtes qui nuisent à l'image publique de l'établissement ou de l'administration scolaire. Les pirates le savent et l'utilisent à leur avantage en renouvelant leurs tentatives d'extorsion. Cette récidive contribue d'ailleurs sans aucun doute à la **hausse de 69 % des attaques mondiales de ransomware ciblant le secteur de l'éducation** au premier trimestre 2025.

Implications légales

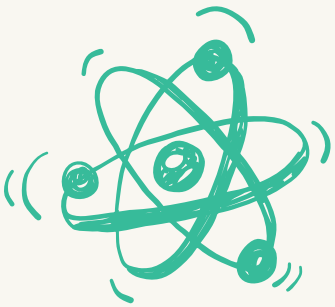
L'éducation étant un secteur réglementé et fortement dépendant des financements gouvernementaux, toute violation de données doit être signalée et faire l'objet d'une enquête. Les établissements sont tenus de protéger les données sensibles des élèves et du personnel. L'exposition non autorisée de données peut donc entraîner de lourdes amendes et faire perdre l'accès aux financements nationaux, fédéraux ou régionaux, en cas d'infraction avérée aux réglementations. En outre, les **violations peuvent entraîner des poursuites civiles et/ou pénales** vis-à-vis des personnes qui n'auraient pas pris les mesures requises.

Vol d'identité

Les données des élèves servent de matériau de base aux pirates pour créer des profils de synthèse qui serviront à diverses activités criminelles. Si les motivations sont le plus souvent financières, comme nous le verrons dans la prochaine section, les pirates ciblent également des individus pour les harceler ou les pister, puis obtenir des informations supplémentaires **au moyen de techniques d'ingénierie sociale.**

Conséquences financières

Les mineurs n'ont souvent aucun antécédent en matière de crédit ou de finances, ce qui rend leurs données particulièrement attractives pour **les acteurs malveillants qui utilisent ces IPI pour effectuer des transactions financières non autorisées** *« pendant de très nombreuses années avant que les victimes ne l'apprennent ».* De plus, du fait de l'absence d'historique financier, les enfants d'âge scolaire ne disposent généralement d'aucun service de surveillance capable de détecter les comptes bancaires, les applications de prêts ou les cartes de crédit ouverts en leur nom, et ne s'en aperçoivent qu'à l'âge adulte.



Qu’est-ce que la cyber kill chain ?

Les attaques varient parce que les pirates choisissent leurs techniques en fonction des cibles sélectionnées et des vulnérabilités qu’elles présentent. Si les attaques ont souvent des caractéristiques communes, leurs spécificités et les nombreuses variables qui influent sur la sécurité des terminaux font de la cybersécurité un art autant qu’une science.

Mais en dépit de cette variété, une certitude demeure : une attaque présente une succession d’étapes articulées en cyber kill chain. Composée de sept phases, de la préparation initiale à l’exécution, chaque étape de la kill chain offre aux équipes de cybersécurité la possibilité d’identifier les points faibles que des pirates pourraient exploiter.

« Voilà mes projets, et voilà mes plans » – Tears for Fears

Avant d’apprendre à lire la feuille de route d’un pirate, voyons les sept phases de la cyber kill chain :

1. **RECONNAISSANCE :** recherche et identification de cibles en ligne et hors ligne.

2. **ARMEMENT :** les résultats de la recherche servent à mettre au point et/ou à acquérir les outils qui seront utilisés.

3. **LIVRAISON :** des outils malveillants sont activement utilisés contre les cibles pour obtenir un accès.

4. **EXPLOITATION :** une fois l’accès obtenu, les pirates cherchent à l’étendre en exploitant les vulnérabilités et les failles de sécurité.

5. **INSTALLATION :** le déploiement de code malveillant jette les bases de la réussite de la campagne.

6. **COMMANDEMENT ET CONTRÔLE :** un moyen de communication avec les dispositifs compromis est établi avant la phase finale de l’attaque.

7. **PASSAGE À L’ACTION :** une fois les préparatifs terminés, les pirates mettent en œuvre les outils pour atteindre leurs objectifs : collecte d’informations confidentielles, exfiltration de données, exécution d’un ransomware, etc.

Modèle d'une attaque de ransomware ciblant un établissement scolaire

Dans cette section, nous étudions **l'attaque par ransomware qui a récemment ciblé l'administration des Écoles publiques de la ville de Baltimore (BCPS)**. Soulignons que cette attaque fait toujours l'objet d'une enquête du FBI à l'heure où nous écrivons ces lignes. Pour cette raison, les détails se limitent à ce qui a été divulgué et cet exemple ne présente qu'une possibilité de déroulement d'une attaque de ce type en conditions réelles.

1.

Reconnaissance

Au cours de la phase de collecte de renseignements, les pirates recueillent des informations détaillées sur l'infrastructure et l'environnement réseau de l'établissement. Leur but est d'identifier les fournisseurs, les prestataires de services et le personnel clé en faisant des recherches dans des sources publiques et en utilisant des techniques d'ingénierie sociale. La reconnaissance peut être passive ou active. Dans le second cas, elle peut déclencher des alertes en raison d'activités suspectes, comme une augmentation inhabituelle du trafic réseau lors de l'exploration du réseau de la cible. L'objectif : dresser le profil de la cible, identifier les vulnérabilités et améliorer les chances de réussite de l'attaque. Une bonne compréhension de ces tactiques peut aider les responsables informatiques à détecter les signes avant-coureurs d'une attaque et à renforcer les mesures de défense.

2.

Armement

Après la reconnaissance, les pirates utilisent les renseignements qu'ils ont recueillis pour adapter leurs outils en vue de l'étape suivante de l'attaque. Ils vont généralement personnaliser ou acquérir des logiciels malveillants, dont les cadres et l'infrastructure nécessaires au fonctionnement du ransomware. De nombreux pirates s'appuient désormais sur des fournisseurs de Ransomware-as-a-Service (RaaS) : ce modèle commercial clé en main fait baisser le coût et le niveau de difficulté technique des attaques. Des acteurs malveillants de tout niveau de compétence peuvent ainsi cibler des établissements dotés de compétences avancées en échange d'une commission sur le montant extorqué. Les équipes informatiques ont tout intérêt à comprendre ce modèle pour anticiper l'évolution des menaces et s'y préparer.

3.

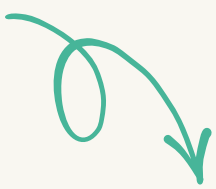
Livraison

Au cours de la phase de diffusion, les pirates s'appuient souvent sur des tactiques d'ingénierie sociale, phishing en tête, pour distribuer du code malveillant sur le maximum de terminaux avec un minimum d'effort. La multiplication des canaux (e-mail, SMS et réseaux sociaux) augmente leurs chances de succès, en particulier lorsqu'ils ciblent des utilisateurs individuels. Des solutions comme Jamf for K-12 permettent de se défendre contre ces menaces en bloquant les URL de phishing, en surveillant l'intégrité des appareils et en imposant la séparation des données grâce à des profils d'inscription sécurisés. En cas de violation, les équipes informatiques peuvent automatiser l'assainissement des données pour protéger les données sensibles de l'école. Ces outils sont indispensables pour mener une stratégie de défense proactive dans le secteur de l'éducation.

4.

Exploitation

Au cours de la phase d'exploitation, les pirates utilisent du code malveillant pour exploiter les vulnérabilités du système, élever leurs privilèges ou utiliser des identifiants obtenus par phishing pour accéder au réseau, selon les résultats de la phase précédente de reconnaissance. Des variantes sophistiquées de logiciels malveillants sont conçues pour échapper à toute détection en chiffrant leurs processus pour les dissimuler. Les solutions de Jamf permettent d'atténuer ces attaques en surveillant la santé des appareils, en déclenchant des workflows de correction en temps réel et en désactivant les comptes compromis. En outre, l'intégration parfaite de la gestion, des identités et de la sécurité permet de sécuriser l'utilisation des identifiants grâce à l'authentification multifacteur (AMF), et de veiller à ce que les appareils restent à jour et reçoivent tous les correctifs. Cette défense à plusieurs niveaux permet aux équipes informatiques de réduire les risques et de réagir rapidement aux incidents dans l'ensemble de l'environnement.



5.

Installation

Lors de la phase d'installation, le ransomware est déployé sur les appareils compromis afin de préparer le terrain à l'attaque proprement dite, consistant à extraire les données des élèves et des enseignants et à perturber les divers systèmes informatiques de l'administration. Pour se défendre à ce stade, les équipes informatiques doivent miser sur la visibilité et la conformité en détectant, en prévenant et en corrigeant les menaces. Jamf y contribue en bloquant les logiciels malveillants connus, en isolant le code nuisible et en surveillant la santé des appareils pour détecter le moindre changement dans la posture de sécurité. Dans le cas de menaces inconnues, les journaux des appareils peuvent être transmis à un SIEM pour approfondir la recherche des menaces et répondre plus rapidement aux incidents survenant dans les environnements scolaires.

6.

Commandement et contrôle

Dans la phase de commande et contrôle, les appareils compromis commencent à communiquer avec le serveur du pirate pour récupérer les fichiers cibles et les clés de chiffrement nécessaires au vol de données et à l'extorsion. Les appareils compromis sont scannés pour localiser les fichiers de grande valeur (Word, Excel, PDF et bases de données). Les pirates téléchargent parfois des outils supplémentaires pour atteindre leurs objectifs. Leur but : maximiser l'accès aux réseaux scolaires. Il est indispensable de bloquer ce type de communication. Les outils intégrés de sécurité et d'identité peuvent désactiver les identifiants compromis, bloquer l'accès aux serveurs malveillants et déclencher des processus de remédiation automatisés lorsque les appareils cessent d'être conformes. Ils aident ainsi les équipes informatiques à défendre l'environnement scolaire et à freiner les pirates dans leur entreprise.

7.

Passage à l'action

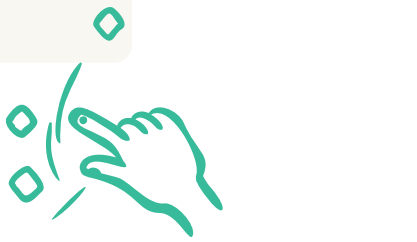
Dans la phase finale de la cyber kill chain, les pirates concrétisent leur objectif : exfiltration de données, extorsion, déplacement latéral, attaques DDoS, etc. Le plus souvent, les ransomwares chiffrent les fichiers, suppriment les originaux et laissent derrière eux une demande de rançon. Les cas les plus graves s'accompagnent de menaces de divulgation ou d'exploitation des données volées. Chaque attaque est adaptée aux objectifs de ses auteurs, d'où le caractère imprévisible et potentiellement dévastateur de ces événements pour les établissements. L'intégration étroite des outils de gestion des appareils, de gestion des identités et de sécurité permet d'arrêter le trafic malveillant, d'empêcher l'exfiltration de données et de désactiver les identifiants compromis. Grâce aux workflows de correction automatisés et à la télémétrie en temps réel, seuls les appareils conformes ont accès aux réseaux scolaires, une pratique décisive pour une stratégie de défense en profondeur.

Comblez les failles de votre armure

Des protections inadéquates, essentiellement pensées pour les systèmes d'exploitation de bureau, présentent des lacunes de sécurité néfastes pour les appareils mobiles, qui sont souvent exploités par les acteurs malveillants pour compromettre les réseaux.

Bien que les appareils mobiles ne soient pas les seuls risques à l'origine des violations de données, ils restent des cibles privilégiées en raison de leur omniprésence sur le lieu de travail et du fait qu'ils sont de plus en plus utilisés pour accéder aux données. Une **étude de Jamf Threat Labs** a chiffré ce risque : *« 40 % des utilisateurs mobiles utilisent un appareil qui présente des vulnérabilités connues. »* Grâce aux failles non corrigées des appareils vulnérables, les acteurs malveillants peuvent :

- **Exécuter du code malveillant sur les appareils**
- **Espionner les utilisateurs à leur insu**
- **Contourner les protections de sécurité internes**
- **Pivoter à partir de l'appareil infecté pour compromettre les réseaux**
- **Accéder à des données d'entreprises sans autorisation**
- **Exfiltrer des données personnelles et professionnelles, ainsi que des informations confidentielles**
- **Obtenir des données personnelles sans autorisation**



Apple est connu pour allier forme et fonction, pour marier style et pertinence. Cette philosophie s'applique à une caractéristique cruciale de la conception : la sécurité et la protection de la vie privée. Les systèmes d'exploitation macOS et iOS intègrent nativement plusieurs protections qui protègent les appareils, les utilisateurs et leurs données contre une myriade de menaces, tant au niveau matériel que logiciel.

Les pirates font évoluer leurs techniques. Ils imaginent de nouvelles menaces et créent des variantes de logiciels malveillants émergents, comme la famille des Infostealers. Les protections de sécurité qui reposent uniquement sur la détection de signatures statiques ne permettent plus de se défendre contre les menaces sophistiquées. Certaines attaques, comme le ransomware qui a touché BCPS, montrent des signes de **collaboration entre plusieurs groupes malveillants pour l'obtention de l'accès initial** en amont du lancement de la campagne. Dynamique par nature, les menaces sophistiquées échappent souvent aux protections intégrées des systèmes d'exploitation (quelle que soit la plateforme), ce qui expose les appareils, les acteurs et les données à un risque de violation, comme les **25 000 personnes touchées par l'attaque de BCPS**.

Avec un plan de sécurité basé sur un **cadre de défense en profondeur** mature, les organisations ont toutes les cartes en main pour réduire les risques sur l'appareil, **se protéger des menaces basées sur le web**, prévenir les attaques connues et répondre rapidement aux incidents. Les workflows de correction automatisés rétablissent la conformité des terminaux.

En intégrant et en superposant les solutions, les entreprises opposent aux menaces sophistiquées des protections complètes et multicouches qui capturent et atténuent les risques. Ces couches de protection s'appliquent à l'ensemble de l'entreprise et constituent une base de défense pour tous les types d'appareils et de systèmes d'exploitation qui ont besoin d'accéder aux ressources et aux données de l'entreprise.

Selon un récent rapport **Frost Radar : Sécurité des terminaux 2023**, le cabinet Frost & Sullivan a mis en évidence que Jamf était un leader de la sécurité des terminaux en raison des capacités de défense en profondeur de nos solutions :

- **Détection en temps réel des applications et des scripts malveillants, et recommandation d'actions aux utilisateurs**
- **Un cadre de configuration et d'audit élargi pour aider les clients à remplir leurs obligations de conformité**
- **Gestion cohérente des vulnérabilités, prévention des menaces et contrôle des règles**
- **Des données télémétriques riches sur les terminaux, exportables dans des outils tiers de collecte et d'analyse des journaux.**
- **Rapports de sécurité sur toutes les plateformes Mac et mobiles, dont macOS, iOS/iPadOS et Android ; la protection contre les menaces web couvre aussi Windows et les Chromebooks**
- **Une application cohérente des règles sur les appareils d'entreprise autant que les appareils personnels.**

Conclusion

La cyber kill chain fournit aux équipes informatiques un cadre structuré permettant d'anticiper le déroulement des attaques de ransomware, de la reconnaissance à l'extorsion en passant par l'exfiltration des données.

Comme l'illustre l'incident subi par les Écoles publiques de la ville de Baltimore, chaque phase met en évidence les lacunes et les vulnérabilités qui seront exploitées si elles ne sont pas corrigées. Avec leurs budgets limités, leur infrastructure vieillissante et leurs équipes informatiques surchargées, les établissements scolaires doivent surmonter des obstacles considérables pour se défendre contre les menaces sophistiquées.

Jamf for K-12 facilite la mise en place d'une stratégie de défense en profondeur en intégrant la gestion des appareils, des identités et des accès, ainsi que la sécurité des terminaux, pour une protection complète de ce que les établissements ont de plus précieux : les élèves, les enseignants et les données. Notre approche donne aux équipes de support les moyens de détecter, prévenir et corriger les menaces dans tous les environnements Apple et multiplateformes, de façon homogène et uniforme. Grâce à la télémétrie en temps réel, aux workflows automatisés et aux contrôles d'accès sécurisés, les administrations scolaires peuvent combler les lacunes de sécurité critiques et renforcer leur conformité. Face au paysage actuel des menaces, les protections multicouches ne sont plus un luxe : elles sont une nécessité pour préserver l'avenir de l'éducation.

Vous voulez savoir ce que donnerait la défense en profondeur dans votre environnement ?

jamf

Essayez Jamf