Kryptojacking in Schulen

für Einsteiger*innen

Willkommen zurück zu unserer Serie über Cybersicherheit in Schulen! Dies ist das dritte Buch der Reihe; wenn Sie ganz am Anfang beginnen möchten, lesen Sie unsere E-Books Malware in Schulen für Einsteiger*innen oder Phishing in Schulen für Einsteiger*innen.

Unser nächstes Thema in dieser Reise ist **Kryptojacking**.

jamf

IN DIESEM E-BOOK GEHT ES UM:

Was ist Kryptojacking?

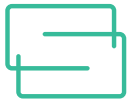
Kryptojacking ist eine Kombination aus zwei Wörtern: **Kryptowährung** und **Hijacking**. Beim Kryptojacking übernehmen Cyberkriminelle mithilfe von Malware oder Phishing-Techniken einen Computer und nutzen ihn zum Schürfen von Kryptowährung wie Bitcoin. Um Kryptomining zu verstehen, nehmen wir den 100-Dollar-Schein der USA als Beispiel.

Geld ist mehr als nur ein Stück Papier. Um einen echten 100-Dollar-Schein zu drucken, braucht man:

Eine eindeutige Seriennummer

Farbwechselnde und magnetische Tinte

Winzige Druckbilder, die weder mit bloßem Auge noch mit einem Standarddrucker zu erkennen sind



Ein dreidimensionales Band, das seine Muster verändert, wenn man es bewegt

Ein spezielles Baumwoll-/ Leinenmischpapier mit roten und blauen Fasern, die in das Papier eingewoben sind

Wenn auch nur eines dieser Dinge fehlt, ist Ihr Geld nichts mehr wert. **Authentische Kryptowährung ist ähnlich komplex.**

Die Schaffung einer Kryptowährung ist kompliziert, auch wenn sie nur in der virtuellen Welt existiert. Es gibt keine zentrale Bank für Kryptowährungen, die Kryptowährungen erstellt oder Transaktionen verfolgt. Kryptominer agieren wie Bänker, die ein Buch über die Transaktionen anderer Leute mit Kryptowährung führen, um sicherzustellen, dass die Leute nicht zweimal dieselbe Währung ausgeben. Als Belohnung können sie Kryptowährung erzstellen, die sie behalten oder verkaufen können. Wenn ein 100-Dollar-Schein gedruckt wird, muss man beweisen, dass er echt ist. Das Gleiche gilt auch für Kryptowährung.

Die Kryptowährung-Community hat beschlossen, dass die Miner den Nachweis erbringen müssen, dass sie eine Transaktion validiert haben, indem sie ein komplexes Puzzle lösen - in diesem Fall einen kryptografischen Hash - der im Wesentlichen ein sehr kompliziertes mathematisches Problem darstellt. Solch eine Aufgabe kann nicht mit einem normalen Taschenrechner gelöst werden; sie erfordert einen Computer, der viel Zeit und Rechenleistung aufwenden muss, um den Code zu knacken.

Da dieses Verfahren so kompliziert ist, beansprucht es einen Großteil der Rechenleistung eines Geräts, was dazu führen kann, dass ein Gerät immer langsamer wird, bis es unbrauchbar ist. Das ist eine der Gefahren von Kryptojacking: **Angreifer*innen machen Geld (im wahrsten Sinne des Wortes), während Ihr Computer den Geist aufgibt.** Das ist auch der Grund, warum die Cyberkriminellen die Geräte anderer Leute übernehmen. Sie müssen weder spezielle Geräte für das Kryptomining kaufen, noch müssen sie die Geräte, die sie besitzen, für das Mining verwenden. Stattdessen können sie versuchen, so viele Geräte wie möglich anzugreifen, um ihre Gewinne zu steigern und ihre Kosten zu minimieren.

Wie sieht Kryptojacking aus?

Es gibt mehrere Möglichkeiten, wie Kryptojacking-Malware auf Ihren Computer gelangen kann. Dabei kann es sich um einen **Download von der Website eines Drittanbieters**, einen **E-Mail-Anhang, das Klicken auf einen bösartigen Link** usw. handeln. Schauen wir uns ein mögliches Szenario an:

1

Sie spielen gerne klassische Spiele.

2

In einem beliebten Spieleforum sehen Sie einen Link zum Download von Super Mario.

3

Mario Forever. Sieh haben schon viel über dieses Spiel gehört, also laden Sie es herunter.

4

Dieser Download enthält zwar das Spiel, aber auch Kryptojacking-Malware. Sobald Sie den Installer ausführen, werden sowohl das Spiel als auch die Malware auf Ihrem System aktiviert.

5

Die Malware sammelt Informationen über Ihre Hardware und stellt eine Verbindung zu einem Mining-Server her, um mit dem Schürfen zu beginnen.

6

Es werden echter Prozessnamen verwendet, damit sie nicht entdeckt werden. So wird das Schürfen ohne Ihr Wissen fortgesetzt.
Die Malware installiert auch ein Programm, das Ihre privaten Daten stiehlt.

Laut Bleeping Computer ist dies ein realistisches Szenario. Es ist nicht schwer, sich vorzustellen, dass dies den ahnungslosen Schüler*innen ganz leicht passieren kann. Sie bemerken es vielleicht nicht einmal, bis ihr Computer langsamer wird oder auf andere Weise Probleme macht.

Kryptojacking in Schulen

Warum ist dies also für Schulen relevant?

Kryptojacking stellt eine zunehmende Bedrohung dar. Laut dem SonicWall Cyber Threat Report 2024 **stieg die Anzahl der Kryptojacking-Angriffe 2023 um 659 %** im Vergleich zu 2022. Tatsächlich gab es im November und Dezember 2023 jeweils mehr Angriffe durch Kryptojacking als im gesamten Jahr 2022!

Obwohl diese Zahlen für alle Branchen gelten, bilden die Schulen dabei keine Ausnahme. Bei der Analyse der Cybersicherheit für das Schuljahr 2022-2023 stellte das Zentrum für Internetsicherheit fest, dass CoinMiner, eine für Kryptojacking konzipierte Malware, **20 % der Malware-Angriffe auf Schulen ausmacht.** Damit war CoinMiner die zweithäufigste Malware, von denen Schulen betroffen waren.

Kryptojacking schadet Schulen in mehrfacher Hinsicht:

- Wenn das Gerät eines Schülers langsamer wird oder nicht mehr funktioniert, kann es für ihn schwierig werden, dem Unterricht zu folgen oder seine Arbeit zu erledigen, bis das Problem gelöst ist.
- Infizierte Geräte beanspruchen unnötige Netzwerk-Bandbreite, die für Bildungszwecke genutzt werden sollte.
- Je nachdem, wie die Malware aufgebaut ist, kann Kryptojacking-Malware die Geräte für andere Angriffe anfällig machen.
- Kryptojacking zwingt die Geräte dazu, viel Energie zu verbrauchen, was die Schulen viel Geld kostet.

Mit anderen Worten: Die wachsende Bedrohung durch Kryptojacking droht das Lernen und Lehren zu stören. Schauen wir uns einmal an, wie man das verhindern kann.

Verhinderung von Kryptojacking

Geräteverwaltung

Wenn Sie die anderen E-Books dieser Reihe gelesen haben, kennen Sie diese Aussage bereits: **Ohne Geräteverwaltung gibt es keine Sicherheit, denn was man nicht sieht, kann man auch nicht schützen.** Sobald ein Gerät zu einer Mobile Device Management (MDM)-Lösung hinzugefügt wurde, können IT Admins es verwalten:

- Man kann sehen, mit welchen Ressourcen das Gerät verbunden ist
- Man kann überprüfen, ob das Gerät die Sicherheitsstandards erfüllt
- Man kann Sicherheitsrichtlinien, wie ein Passwort, festlegen
- Man kann Apps auf dem Gerät installieren
- Man kann den Zugang zu unangemessenen oder bösartigen Websites blockieren
- Die Geräte und Software können auf dem neuesten Stand gehalten werden

Um sich vor verschiedenen Arten von Malware, einschließlich Kryptojacking, zu schützen, ist es wichtig, die Geräte mit den neuesten Sicherheitspatches auf dem aktuellsten Stand zu halten. MDM-Lösungen bieten Patch-Verwaltungsfunktionen, um sicherzustellen, dass Geräte und Apps umgehend mit den neuesten Sicherheitspatches und -updates aktualisiert werden.

Überwachung von Netzwerken

Kryptojacking kann schwer zu erkennen sein, da es im Allgemeinen im Hintergrund läuft, aber es hinterlässt Spuren! Die Überwachung Ihres Netzwerks hilft, mögliche Angriffe zu erkennen. Bei diesen Dingen sollten Sie wachsam werden:

- Häufige Kommunikation mit einem unbekannten Server
- Anfragen zu jeder Tageszeit, auch wenn die Geräte nicht genutzt werden
- Eine allgemeine Zunahme der Nutzung des Netzwerks

Um dieses Verhalten zu erkennen, muss man das Grundverhalten kennen. Deshalb muss man mit der Überwachung beginnen, bevor es zu einem Angriff kommt. Der Einsatz von Überwachungstools mit künstlicher Intelligenz (KI) und Maschinellem Lernen (ML) macht es einfacher, ungewöhnliches Verhalten zu erkennen. Schließlich brauchen KI/ML keine Pausen zu machen oder das Schulgebäude zu verlassen; sie arbeiten rund um die Uhr, um Anomalien zu finden.

Verhinderung von Kryptojacking

Inhaltsfilter

Die Filterung von Inhalten kann viel dazu beitragen, Bedrohungen wie Kryptojacking zu verhindern, indem der Zugang zu Websites gesperrt wird, die möglicherweise Malware verbreiten. Intelligente Filterung, die KI und ML nutzt, geht über manuelle Sperr-/Zulassungslisten hinaus, bei denen gefährliche Websites übersehen werden können. Schüler*innen können sich im Internet frei bewegen, ohne auf Websites zu stoßen, die unangemessene Inhalte enthalten oder versuchen, ihre Daten zu stehlen.

Benutzerschulung

Angreifer*innen haben alle möglichen Tricks auf Lager, um Benutzer*innen zum Download von Malware zu bewegen. Wenn man die Benutzer*innen schult, auf welche Anzeichen sie achten sollten, kann dies verhindert werden. Das sollten die Benutzer*innen wissen:

- Laden Sie keine E-Mail-Anhänge oder andere Dateien herunter, ohne sich zu vergewissern, dass sie okay sind.
- Häufige Anzeichen für Phishing
- Was zu tun ist, wenn sie etwas herunterladen, anklicken oder erhalten, was potenziell bösartig ist
- Wie sie Downloads von Websites von Drittanbietern vermeiden können
- Anzeichen dafür, dass ihr Gerät infiziert ist, wie z. B. eine verringerte Leistung oder eine plötzlich schlechtere Akkulaufzeit

IMPLEMENTIERUNG:

JAMF SCHOOL UND JAMF SAFE INTERNET

Wenn es um Cybersicherheit in Schulen geht, haben wir MDM- und Sicherheitslösungen, die speziell für Schulen entwickelt wurden.

Jamf School

Jamf School ist ein MDM, das IT-Admins, Lehrkräften, Eltern und Schüler*innen hilft, eine gute Bildung zu fördern. Jamf School – Funktionen:

- Transparenz über verwaltete Geräte, Benutzer*innen und Apps
- Einfache Bereitstellung von Software und Upgrades
- Konfiguration von Sicherheitseinstellungen für jedes Gerät, einschließlich Passwortrichtlinien und Inhaltsfilterung
- Robuste und sichere App-Bereitstellung und -Aktualisierung von Apps, die von der IT genehmigt sind
- Tools für das Unterrichtsmanagement, um die Konzentration der Lernenden aufrechtzuerhalten

Sicherheit und Verwaltung gehen Hand in Hand. Jamf School bietet Admins die nötigen Erkenntnisse, um Geräte und Benutzer*innen zu schützen.

Jamf Safe Internet

Jamf Safe Internet bietet eine auf Bildung ausgerichtete Filterung von Inhalten und Schutz vor Bedrohungen im Netzwerk. Es schützt Schüler*innen, Geräte und Unternehmensdaten vor bösartigen Inhalten und bösartigen Akteuren. Jamf Safe Internet umfasst:

- Einfache Bereitstellung mit vollständig anpassbaren Richtlinien
- Sicheres Surfen mit erzwungenem Google SafeSearch und YouTube (eingeschränkter Modus)
- Inhaltsfilterung auf dem Gerät nach bekannten und unbekannten Bedrohungen, unterstützt durch künstliche Intelligenz und fortschrittliches maschinelles Lernen
- Schutz im Netzwerk, um Zero-Day-Bedrohungen, wie Phishing-Seiten und bösartige Domains, zu blockieren
- Datenbegrenzung und Warnmeldungen bei Erreichen von Schwellenwerten für die Datennutzung

Jamf Safe Internet funktioniert auch, wenn sich die Geräte in einem Cart befinden, 1:1 bereitgestellt werden oder sich im Besitz der Schüler*innen befinden - und selbst wenn das Gerät nicht im Netzwerk der Schule ist. Und im Gegensatz zu Kryptojacking-Malware verlangsamen Jamf-Lösungen Ihre Geräte nicht und verletzen auch nicht Ihren Datenschutz.