Cryptojacking in K12 for Beginners

Welcome back to our cybersecurity in K-12 series! You're reading the third book in the series; if you want to start at the beginning, read our Malware in K-12 for Beginners or Phishing in K-12 for Beginners e-books.

Our next stop in this journey is **cryptojacking**.

jamf

IN THIS E-BOOK, WE'LL TALK ABOUT :

What is cryptojacking?

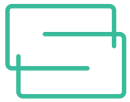
Cryptojacking is a combination of two words: **cryptocurrency** and **hijacking**. In cryptojacking, attackers take over a computer using malware or phishing techniques and use it to mine for cryptocurrency like Bitcoin. To understand cryptomining, let's use the U.S. 100 dollar bill as an example.

Money is more than a piece of paper. Printing a legitimate $100 bill requires:

A unique serial number

Color-changing and magnetic ink

Tiny printed images that can't be seen by the naked eye or be printed by a standard printer



A three-dimensional ribbon that changes patterns as it you move it

A specific cotton/linen blend paper with red and blue fibers woven throughout it

If any one part of these complex features is off, your money isn't worth anything. **Authentic cryptocurrency has similar complexities.**

Creating cryptocurrency is complicated, even though it lives only in the virtual world. There's no central cryptocurrency bank that creates cryptocurrency or keeps track of transactions. Cryptominers act like bankers to keep a ledger of other people's cryptocurrency transactions to make sure people aren't spending the same currency twice. As a reward, they are able to create cryptocurrency to keep or sell. But like when a 100 dollar bill is printed, you have to prove that it's real.

The cryptocurrency community decided that the way for miners to prove they've validated a transaction is to solve a complex puzzle — in this case a cryptographic hash — which is essentially a very complicated math problem.

This isn't something your average calculator can solve; it requires a computer to spend a lot of time and processing power to crack the code.

Because this mining is so complicated, it uses a lot of a device's processing power, which can slow down a device until it's not useful. That's one of cryptojacking's dangers to you: **attackers make money (literally) while your computer runs itself into the ground.** This is also why attackers take over other people's devices. They don't have to purchase any devices specifically for cryptomining, nor do they have to dedicate any devices they do own to mining. Instead, they can try to attack as many devices as possible to increase their profits and minimize their cost.

What does cryptojacking look like?

There are multiple ways cryptojacking malware could find its way onto your computer. It could be a **download from a third-party website**, an **email attachment, clicking on a malicious link** and so on. Let's look at one possible scenario:

1. **You like to play classic games.**
2. **On a popular gaming forum, you see a link to download Super Mario.**
3. **Mario Forever. You've heard a lot about this game, so you download it.**
4. **This download does include the game, but it also includes cryptojacking malware. Once you run the installer, the game and the malware are active in your system.**
5. **The malware collects information about your hardware and connects to a mining server to start mining.**
6. **Hiding from detection by using real process names, the mining continues without your knowledge. The malware also installs an information stealer to steal your private data.**

This is hardly hypothetical, as reported by Bleeping Computer. It's not difficult to imagine an unsuspecting student finding themselves in this situation either. They may not even notice unless their computer starts slowing down or acting up in other ways.

Cryptojacking in K-12 schools

Ok, so why is this relevant for schools?

Cryptojacking is a rising threat. According to the 2024 SonicWall Cyber Threat Report, cryptojacking **increased 659%** in 2023 compared to 2022. In fact, November and December 2023 each saw more cryptojacking attacks than in all of 2022!

Although these are numbers across all industries, K-12 school are no exception. While analyzing cybersecurity for the 2022-2023 school year, the Center for Internet Security found that CoinMiner, malware designed for cryptojacking, made up **20% of malware attacks against schools.** This made CoinMiner the second-most common malware affecting K-12.

Cryptojacking hurts schools in a few ways:

- If a student's device starts slowing down or stops working, they may have difficultly keeping up with classes or doing their work until the issue is solved.
- Infected devices take up unnecessary network bandwidth that should be left for educational purposes.
- Depending on how the malware is built, cryptojacking malware may leave devices vulnerable to other attacks.
- Cryptojacking forces devices to use a lot of energy, likely costing schools money.

In other words, the rising threat of cryptojacking threatens to disrupt learning and teaching. Let's learn how to prevent it.

Preventing cryptojacking

Device management

If you've read the other e-books in this series, you've heard this before: **you can't have security without device management, because you can't secure what you can't see.** Once a device is added to a mobile device management (MDM) solution, IT admins can:

- See what resources the device is connecting to
- Check if the device is meeting security standards
- Set security policies like a required passcode
- Install apps onto a device
- Block access to inappropriate or malicious websites
- Keep devices and software up to date

Keeping devices up to date with the latest security patches is crucial for protecting against various types of malware, including cryptojacking. MDM solutions offer patch management capabilities to ensure that devices and apps are promptly updated with security patches and fixes.

Network monitoring

Cryptojacking can be hard to spot, as it generally runs in the background, but it still leaves traces! Monitoring your network helps identify possible attacks. For example, you might see:

- Frequent communication with an unknown server
- Requests at all times of day, even when devices are unattended
- An overall increase in network usage

Spotting this behavior requires understanding your baseline behavior, so it's necessary to start monitoring before an attack is suspected. Using monitoring tools with artificial intelligence (AI) and machine learning (ML) makes it easier to spot unusual behavior. After all, AI/ML don't need to take breaks or leave the school building; they work 24/7 to find anomalies.

Preventing cryptojacking

Content filtering

Content filtering can go a long way in preventing threats like cryptojacking by blocking access to websites that might be distributing malware. Intelligent filtering that uses AI and ML goes beyond manual block/allow lists that may miss dangerous sites. Students can still have the freedom to explore the web without coming across websites containing inappropriate content or trying to steal their data.

User education

Attackers have all kinds of tricks to try to get users to download malware. Educating users about the signs to look for can stop them in their tracks. Users should know:

- Not to download email attachments or other files without making sure they're legitimate
- Common signs of phishing
- What to do if they download, click on or receive something potentially malicious
- To avoid downloads from third-party websites
- Signs their device is infected, like a reduction in performance or sudden worse battery life

IMPLEMENTATION:

JAMF SCHOOL AND JAMF SAFE INTERNET

When it comes to cybersecurity in schools, we have MDM and security solutions designed with schools in mind.

Jamf School

Jamf School is MDM built to help IT admins, teachers, parents and students foster a great education. Jamf School features:

- Transparency into managed devices, users and apps
- Simple software deployment and upgrades
- The ability to configure device security settings, including passcode policies and content filtering
- Robust and secure app deployment and updating with apps pre-approved by IT
- Classroom management tools to keep learners focused

Security and management go hand in hand. Jamf School gives admins the insights they need to keep devices and their users safe.

Jamf Safe Internet

Jamf Safe Internet offers education-focused content filtering and network threat protection. It protects students, devices and organizational data from bad actors and malicious content. Jamf Safe Internet includes:

- Simple deployment with fully customizable policies
- Safe browsing with enforced Google SafeSearch and YouTube Restricted Mode
- On-device content filtering for known and unknown threats, powered by artificial intelligence and advanced machine learning
- In-network protection to block zero-day threats like phishing sites and malicious domains
- Data capping and alerts when data usage thresholds are reached

Jamf Safe Internet works whether devices live in a cart, are deployed 1:1 or are owned by students — even if the device isn't on the school network. And unlike cryptojacking malware, Jamf solutions don't slow your devices down or invade your privacy.

jamf

See how Jamf can help be a part of your technology, security, and content filtering solution

Get Started

www.jamf.com