ENDPOINT SECURITY (HTTPS://BLOGS.VMWARE.COM/SECURITY/ENDPOINT-SECUITY)

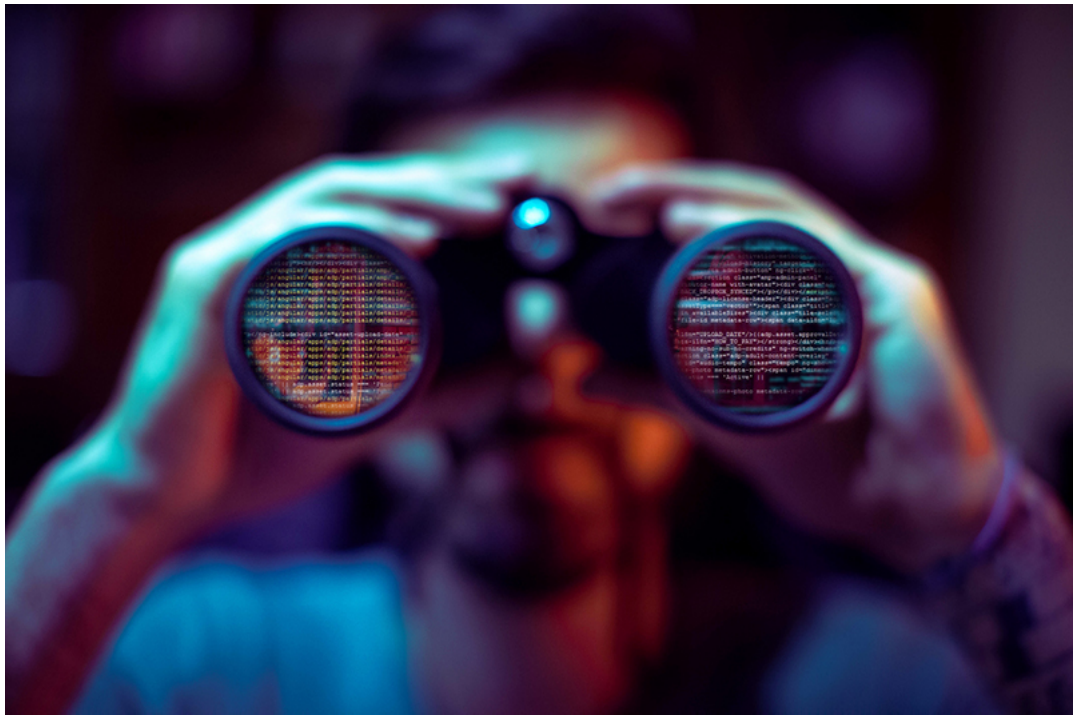
# 5 Crypto Crime Concerns: Your Top Cryptocurrency Mining Questions Answered

Posted April 5, 2018

0 Comments

[vc_row][vc_column][vc_column_text]By the end of 2017, cryptojacking, or the secret use of computing resources for mining cryptocurrency, had already gained noticeable momentum. It's a smart strategy if you're a cyber criminal. Why try and ransom someone's system and wait for them to pay you when you can essentially print money?

Recently, two members of the Carbon Black Threat Analysis Unit (https://www.carbonblack.com/why-cb/threat-analysis-unit/), Adam Nadrowski and Brian Sturk, gave us a quick overview and live demonstration of what cryptocurrencies are, why cyber criminals use them, and how you can use CB Response to hunt for indicators of malicious mining applications.



(https://secure.carbonblack.com/operationalizing-your-threat-hunt.html?utm_source=carbon-black&utm_medium=blog&utm_campaign=operationalizing-your-threat-hunt&utm_term=none&utm_content=none)
April 12, 2018 2:00PM EST

Live Webinar: Operationalizing Your Threat Hunt

Join Carbon Black and Red Canary for a live threat hunting demo.

Register Now (https://secure.carbonblack.com/operationalizing-your-threat-hunt.html?utm_source=carbon-black&utm_medium=blog&utm_campaign=operationalizing-your-threat-hunt&utm_term=none&utm_content=none)

---

***There were plenty of additional questions for our threat researchers to answer on the spot after the webinar (https://www.carbonblack.com/resource/crypto-crime-hunting-cryptocurrency-mining-enterprise?utm_source=carbon-black-blog&utm_medium=social&utm_campaign=crypto-threat-hunting-webinar&utm_term=none&utm_content=none), so here's a transcript of what they had to say:***

**Q: So, the first question we have is where else do you see cryptomining being leveraged?**

**A:** In addition to malicious browser mining, which we actually didn't talk about today, but I could imagine someday there being another webinar about that, there's actually been some movement as far as miners with legitimate website monetization. So, rather than showing ads on a webpage, miners run in the background while a user is browsing a site. Salon, Showtime, and if I remember right, the Pirate Bay did this as well. They've tried out some form of mining as an

alternative revenue generator, instead of running ads. I see that actually being a big thing that obviously is going to make it harder to differentiate between malicious and benign. So, there's probably in the future going to be more false positives if this catches on, as far as a revenue generating technique.

**Q: Where does the blockchain fit into this?**

**A:** So, the blockchain—I can't believe I went through the whole presentation without saying the word blockchain. That's pretty funny. The blockchain is like the global ledger that transactions are recorded onto. Miners are validating those transactions, and then they record them to the blockchain. That's kind of where it comes into play. How this all works is way beyond this webinar, this notion of proof of work and proof of stake, and how they get blocks, and who wins. But basically, that's what's going on. The miner is validating transactions and then writing them to the blockchain, which is the global ledger.

**Q: What about GPU miners? How would you adapt to hunt for GPU-focused miners?**

**A:** For XMRig, what I've been seeing in the wild is primarily CPU focused. And I think that is due to the efficiency with CPU mining. I do know that there are some open source XMRig variants that use AMD Nvidia cards. But again, I haven't seen them used in the wild much. And so, within our user community, I do recall one of our [incident response] consultants, Ben Tedesco, provided some insight on GPU mining, and he used a similar strategy to the last one I used, with mod loads and network connections, and digital signatures. But he focused on AMD to Nvidia mod loads, as opposed to sort of the cryptographic functions. So, that is how you could replace or supplement the mod loads that we used during this presentation and add the GPU focused ones.

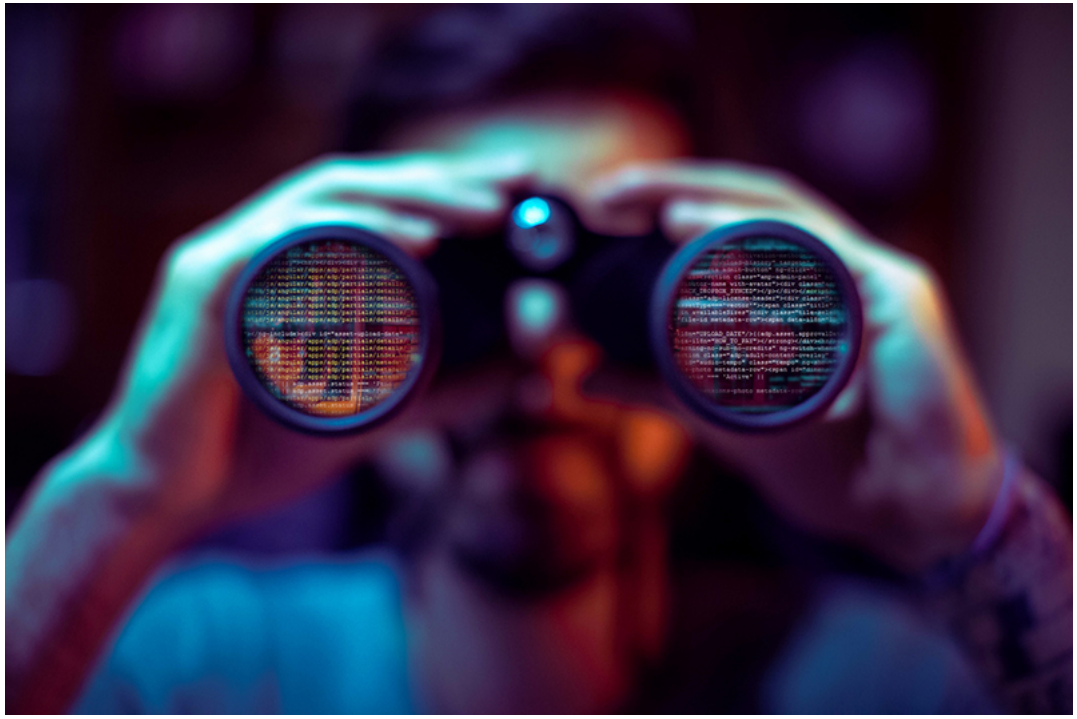
**Q: Next question, how do you create a custom feed in CB Response?**

**A:** We do have documentation on the User Exchange (https://community.carbonblack.com/), specifically the user guide on how to do this within the UI. It differs a little bit between response, cloud, and on-prem variants. There's multiple ways of doing it. You could either host it on a web server or save it locally on the CB Response server. It varies. But the instructions are in the user guide. And I would definitely leverage that Python script we saw at the beginning of this presentation because it certainly simplifies things a lot. Like I said, it took me ten minutes.

**Q: Last question we have here is what about browser and JavaScript-based cryptominers?**

**A:** Yeah, we didn't really talk about that today. We focused on the applications. And that's really because it's almost a separate topic. So, these browser-based or crypto-jackers, whatever you want to call them, they run kind of isolated in the browser. They don't really do much else other than make a network connection, so it's a lot more difficult to detect those. You'd have to instrument the browser in some way, be able to either monitor the JavaScript or whatever that's running in there. And obviously, this is going to become a bigger problem going forward as well, since they're served up over ads. They're going to be served up by sites; I mean some legitimate, some maybe not. There's definitely a lot of opportunity there to do that. We may cover, or someone may cover browser-based crypto miners in a different webinar.

We hope this Q&A session answers some of the lingering questions you may have about hunting for cryptocurrency miners in your enterprise environment. If you're looking for more information on Monero, cryptocurrency mining, and how to better defend your environment against this type of malicious activity, we highly recommend checking out a recent blog post by Carbon Black security strategist Rick McElroy (https://www.carbonblack.com/2018/02/28/cryptomining-rules-endpoints-around-get-monero/) that arms security professionals with the right mindset to tackle this emerging threat.



(https://secure.carbonblack.com/operationalizing-your-threat-hunt.html?utm_source=carbon-black&utm_medium=blog&utm_campaign=operationalizing-your-threat-hunt&utm_term=none&utm_content=none)
For more information on strategies, team structure, and processes to help blue teams transform their threat hunting efforts from an ad-hoc tactic into a regular operational effort, join Carbon Black and Red Canary for a live webinar on April 12th.

Register Now (https://secure.carbonblack.com/operationalizing-your-threat-hunt.html?utm_source=carbon-black&utm_medium=blog&utm_campaign=operationalizing-your-threat-hunt&utm_term=none&utm_content=none)

---

[/vc_column_text][/vc_column][/vc_row]

## Comments

0 Comments have been added so far

## VMware Security

VMware Enterprise Security Solutions (http://www.vmware.com/security.html)

VMware Security Response Center (https://www.vmware.com/security/vsrc.html)

VMware Security Certifications (https://www.vmware.com/security/certifications.html)

Security Hardening Guides (https://www.vmware.com/security/hardening-guides.html)

VMware Security Development Lifecycle (https://www.vmware.com/security/sdl.html)

## Company Information

Leadership (http://vmware.com/company/leadership/)

Careers at VMware (http://vmware.com/company/careers/)

Acquisitions (http://vmware.com/company/acquisitions/)

Office Locations (http://vmware.com/company/office_locations/)

Contact VMware (http://vmware.com/company/contact/)

Investor Relations (http://ir.vmware.com/)

VMware Foundation (http://vmware.com/company/foundation.html)

Why Choose VMware? (http://vmware.com/why-choose-vmware/)

## News & Events

Newsroom (http://vmware.com/company/news/)

Articles (http://vmware.com/company/news/articles/)

Events (http://vmware.com/events/)

Awards (http://vmware.com/company/news/media-resources/awards.html)

Media Resource Center (http://vmware.com/company/news/media-resources/)

Media & Contacts (http://vmware.com/company/news/media-contacts.html)

## Community