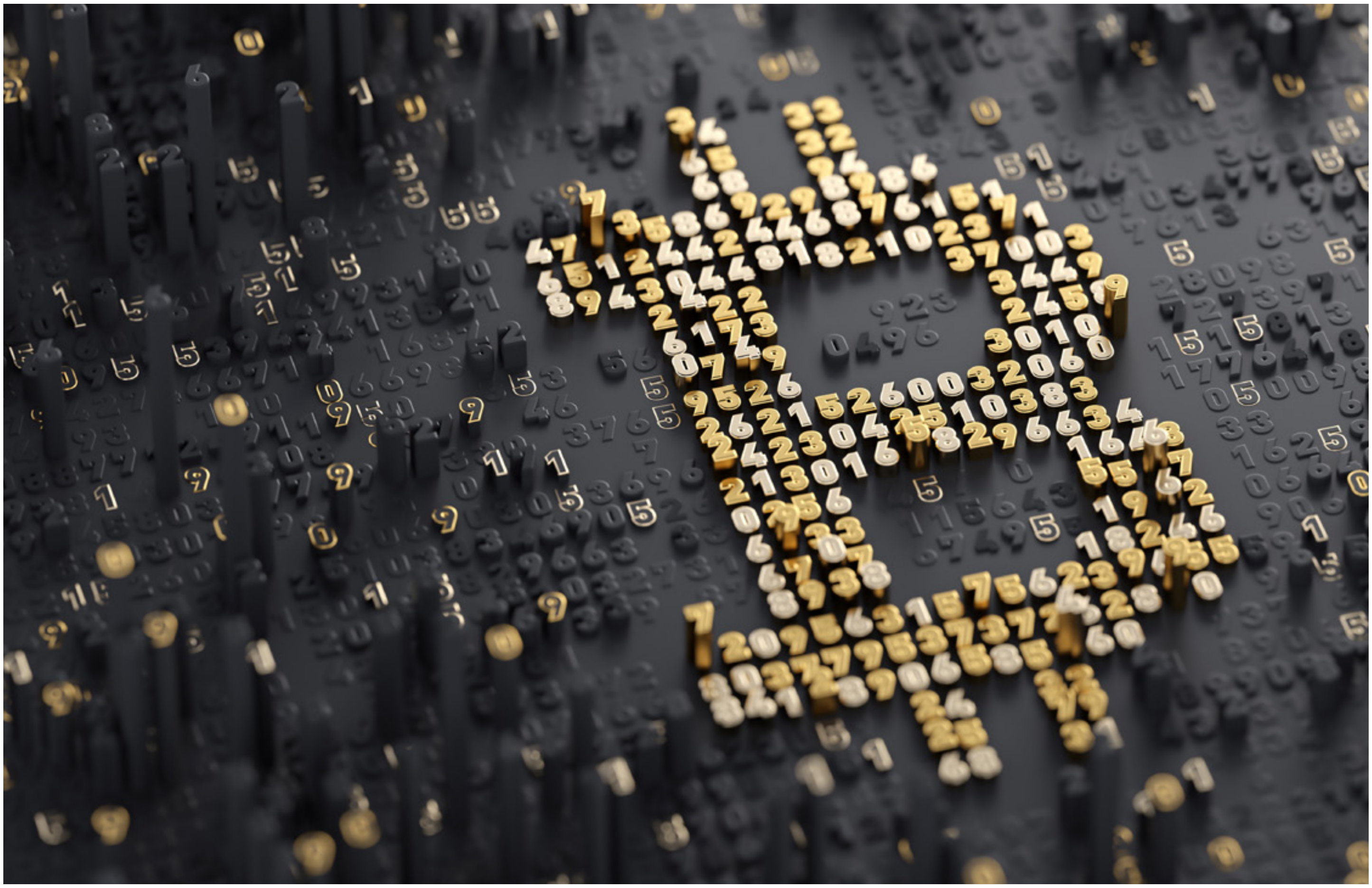
Intelligent Security. Everywhere.

Solution Brief



Countering Cryptojacking with Intel vPro and BlackBerry

Quickly Detect Cryptomining Activity at the Hardware Level

Problem

Crypotojacking, or the use of unauthorized or stolen computing resources for cryptomining, is a subtle but serious threat to organizations worldwide. In 2018, infecting machines with cryptomining malware surpassed ransomware as a top cyber threat[1]. Recently in Europe, multiple supercomputers in the U.K., Germany, Spain, and Switzerland were infected with cryptomining malware and forced to shut down[2]. While supercomputers and large processing centers make appealing targets for cryptojackers, many attackers prefer infecting business desktops, laptops, and mobile devices. Businesses who prefer cloud computing will find no refuge, as cryptojackers have refined methods for creating cloud compute instances to run cryptomining code[3].

What Is Cryptomining?

At the most basic level, cryptomining is receiving digital currency for using processors to solve complex mathematical puzzles.

For example, Bitcoin, the most popular cryptocurrency, was built upon the concept of creating a decentralized financial network. This distributed model, known as **blockchain**, does not use a trusted centralized ledger, but shares the financial record across multiple nodes. When a bitcoin miner solves a puzzle, it broadcasts its answer to the validating network of Bitcoin nodes. If 51% of the nodes confirm the answer, the miner is rewarded with bitcoins and the resulting transaction is added to the blockchain[4].

Bitcoins are designed to be successfully mined at an average pace of ten minutes apart. This rate is achieved by increasing the complexity of the puzzles to reflect the computing power currently committed to mining. As more computing power is harnessed to mine bitcoins, the complexity of the puzzles increases. Miners have reacted to this increasing complexity by searching for better processors to increase their chances of solving the puzzle first. They upgraded from using CPUs, to high-end GPUs, and ultimately on to specialized mining hardware called application-specific integrated circuits (ASICs).

As more miners joined the hunt for bitcoins using high-end ASICs farms, the electrical power required for mining increased dramatically. By 2019, Iceland was using more electricity to mine bitcoin than to power its citizens' homes[5]. Innovative coin miners also turned to cloud computing and browser-based coin mining to increase their chances of success. Each new group of miners and advance in computing power increased the difficulty of successfully mining bitcoins.

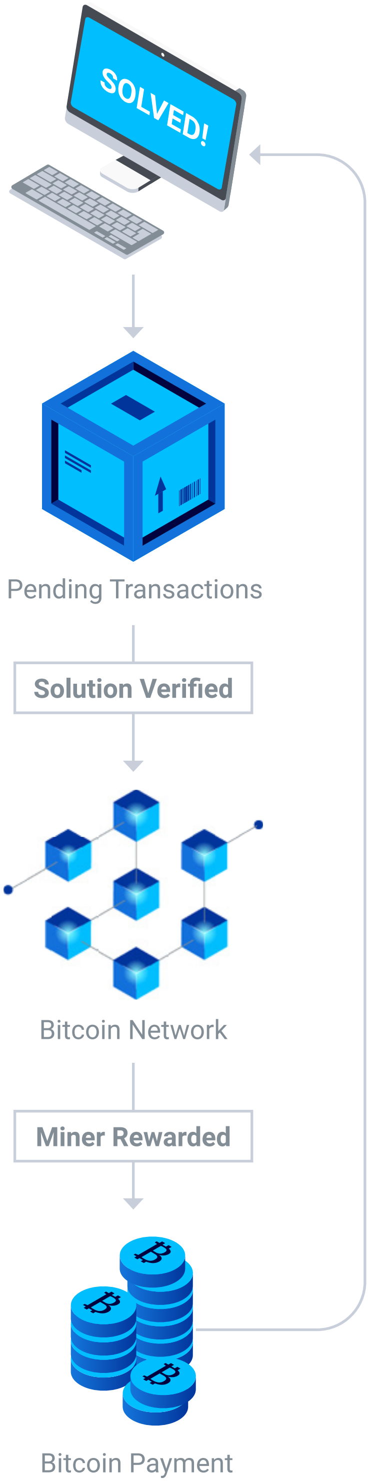


Figure 1. A simplified example of bitcoin mining.

[1] https://www.forbes.com/sites/jasonbloomberg/2018/07/29/cryptojacking-displaces-ransomware-as-most-popular-cyberthreat/#48e81d9a86e9

[2] https://www.zdnet.com/article/supercomputers-hacked-across-europe-to-mine-cryptocurrency/

[3] https://www.wwt.com/article/malicious-cryptomining-shifts-malware-focus-from-data-theft-to-compute-power-in-the-cloud

[4] https://threatvector.cylance.com/en_us/home/threat-research-report-the-state-of-cryptomining.html

[5] https://www.wired.com/story/iceland-bitcoin-mining-gallery/

The normal laws of economics would dictate that cryptocurrency mining should taper off as the costs begin to outweigh the profits. However, cryptojackers have found a way to keep mining extremely profitable – by stealing electricity and computing power from others.

Cryptojacking is considerably less obtrusive than aggressive cyber threats like ransomware. It silently siphons resources and productivity from an organization and may operate undetected for long periods of time.

Symptoms and Effects of Cryptojacking

Cryptojacking is considerably less obtrusive than aggressive cyber threats like ransomware. It silently siphons resources and productivity from an organization and may operate undetected for long periods of time. Threat actors have devised multiple ways to deliver crypotojacking malware to a wide variety of devices, which complicates detection and remediation efforts. Since cryptominers rely heavily upon processing power, the following symptoms may indicate a cryptojacking infection:

- Unusually sluggish machine performance
- Faster than usual battery depletion
- High CPU or GPU utilization, especially during off hours
- Inexplicable overheating
- Outbound network traffic to cryptomining-related sites

Cryptojackers have a variety of negative impacts on an organization. They reduce the operational capacity of technology by stealing processing cycles to mine currency. The wear and tear inflicted on devices used for mining is likely to reduce their functional lifespan. Continuously running CPUs and GPUs at full power will cause hardware to overheat and likely result in permanent damage to the system[6]. The additional power consumed by cryptomining activities will increase an organization's utility costs.

Detecting cryptomining can be difficult, especially if only a few machines are infected. Machines mining cryptocurrency are often indistinguishable from those performing normal work operations without extensive analysis. This makes cryptojacking losses nearly invisible until they accrue to a large sum over time. Rather than taking an organization down in one bold stroke, cryptojacking bleeds them slowly, offering death by a thousand cuts.

Solutions

Intel vPro Platform

The Intel vPro® platform is built for business with business-class performance, hardware-enhanced security features, remote manageability, and reliable stability. Intel® Active Management Technology and Intel® Endpoint Management are two key features of the Intel vPro platform. Together, they offer enterprises the ability to "securely manage devices, inside and outside the firewall, over the cloud"[6]. These features greatly benefit organizations based in multiple locations or supporting a

[6] https://www.dignited.com/45408/whats-crypto-mining-and-how-does-it-hurt-your-pc/#:~:text=Overheating,bitcoin%20with%20your%20home%20computer

remote workforce, the very sort of businesses that also appeal to cryptojackers. The Intel vPro platform includes the Intel® Hardware Shield, which offers protection against firmware-based attacks, increased hardware-to-software security visibility[7], hardware-based features that allow systems to boot in a protected state, and offers additional security at runtime. Intel Hardware Shield also includes Intel® Threat Detection Technology (Intel® TDT), a suite of security technologies adept at detecting cryptojacking malware. These technologies rely on hardware-supplied telemetry provided by the Intel vPro platform. By monitoring performance counters, Intel TDT can detect processes that are likely mining cryptocurrencies. BlackBerry calls this process cryptosmacking, as it effectively stops cryptojacking dead in its tracks. The Intel TDT is also capable of scanning system memory for memory-based attacks using only a fraction of the CPU required by other technologies.

Simply put, BlackBerry Cyber Suite uses AI to tackle the tasks where it excels, like threat detection, prevention, and response.

BlackBerry Cyber Suite

BlackBerry® Cyber Suite is a suite of AI-driven threat detection and prevention tools that secures technology ranging from business hardware to mobile devices and embedded systems. It includes:

- **BlackBerry® Protect Endpoint Protection Platform (EPP) —** AI-driven threat prevention, combined with application and script control, memory protection, and device policy enforcement. BlackBerry security AI is trained on millions of safe and unsafe files to identify and block threats before they can cause harm.
- **BlackBerry® Optics Endpoint Detection and Response (EDR) —** Mathematical threat detection models deployed directly on endpoints to monitor for suspicious activity, perform root cause analysis, and smart threat hunting. Advanced capabilities like Focus View and the Context Analysis Engine give security analysts unprecedented insight into the current state of any protected endpoint. Automated playbooks can be configured to perform remediation steps or monitor for specific threat vectors like the MITRE ATT&CK® framework.
- **BlackBerry® Persona Continuous Authentication —** AI-driven continuous authentication that dynamically adapts security policies based on user/entity location, device, and other factors. By establishing and maintaining a trust score over the life of each engagement, BlackBerry Persona delivers a secure Zero Trust, Zero Touch experience[7].
- **BlackBerry® Protect for Mobile —** AI-driven threat prevention, combined with application and script control, memory protection, and device policy enforcement for mobile devices.

Simply put, BlackBerry Cyber Suite uses AI to tackle the tasks where it excels, like threat detection, prevention, and response. As a component of BlackBerry Cyber Suite, the BlackBerry Optics Context Analysis Engine (CAE) is a high-performance analysis and correlation engine that monitors events as they occur on an endpoint in near real time to identify malicious or suspicious activities such as cryptomining and cryptojacking. With the engine deployed on the endpoint, this 24x7 monitoring

[7] https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/infogrfx-bis-from-zero-trust-to-zero-touch.pdf

occurs with zero reliance on, or need for, a cloud connection. Without requiring an active network connection to make intelligent decisions, the CAE's architecture allows you to monitor multiple suspicious behavior paths continuously without posing potential performance impacts.

When the CAE identifies potentially malicious cryptomining and cryptojacking activity, automated response actions against the associated artifacts of interest can begin without any human intervention. These response actions are initiated from the endpoint with no cloud connection required. This frees employees to perform actions where a human touch is critical, like decision-making and coordinating a strategic threat response plan. Consolidating all security tools under a single console allows admins to quickly determine the state of the enterprise and act effectively.

Cooperatively Countering Cryptojackers

BlackBerry and Intel have teamed up to provide a robust defense against cryptojackers. BlackBerry has integrated the Intel TDT suite of technologies and machine-learning algorithms into BlackBerry Optics, our AI-driven EDR tool. This integration offers users a way to quickly detect cryptomining activity at the hardware level, without performing lengthy code analysis. It also provides security analysts the ability to create automated response actions for lightning-fast remediation.

Cryptomining is a subtle and parasitic threat that has been quietly siphoning the resources of organizations for years. Today, BlackBerry and Intel are united in producing an AI-driven solution that will reliably detect this threat and shut it down. For more information on how you can protect your enterprise from cryptojackers, contact us.

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

BlackBerry®
Intelligent Security. Everywhere.

For more information, visit BlackBerry.com and follow @BlackBerry.