Published on *The National Law Review* https://natlawreview.com

Why is Norton Anti-Virus Becoming a Crypto Mining Botnet?

Article By:

Theodore F. Claypoole

In the before-times – the heady days of 2017 when the prices of both Bitcoin and Ethereum skyrocketed and seemed immune to gravity – several well-known companies boosted their value by claiming to build new products on the blockchain or to create a solid trustworthy crypto-coin. The trend has continued through the pandemic.

We often note a whiff of desperation in old-economy businesses trying to re-invent themselves as blockchain or crypto companies. For example, according to Krebs On Security, RadioShack relaunched in 2020 as an online brand and "now says it plans to chart a future as a cryptocurrency exchange" by helping old-school customers feel comfortable with crypto speculation. We know that a few years ago photo giant Kodak, whose primary product was replaced by ubiquitous digital cameras on smartphones, announced moves into cryptocurrency called KodakCoin and Kodak KashMiner which quickly and temporarily boosted Kodak's stock price 60%. The New York Times stated at the time, "Almost immediately, critics pounced on the company's plans, characterizing them as a desperate money grab." Kodak soon abandoned the coin and digital mining effort and Kodak now claims to be a drug company. Who is next, Blockbuster as NFT-factory?

No, the newest surprising news is Norton LifeLock as a crypto miner. Not that Norton LifeLock is an old-economy company, but it is a relatively stogy security firm offering a two-decade-old product that seems less relevant now than it used to be. In the internet age, software firms from the 1990s may count as "old-economy."

Norton LifeLock has started offering the "Norton Crypto" tool as part of its famous yellow-branded Norton 360 software for home and business computers. Norton Crypto allows paying customers to mine cryptocurrencies while their computers are otherwise inactive. When the tool is turned on, Norton brings together all of its customers' mining capacity into a pool of computing power that mines Ethereum then breaks the value of the mined currency into pieces and deposits a small percentage into a Norton digital wallet held in the cloud for each participating customer. Norton skims 15% vigorish as a service fee before any of the value is allocated to customers. Norton claims to be offering this tool as a way to help customers improve security by providing trusted mining tools and avoiding "Unvetted code on their machines that could be skimming from the earnings or even planting ransomware."

Despite some public accusations to the contrary, Norton does not automatically turn on Norton Crypto when you subscribe to Norton 360 security software. You would need to turn the tool on if you

wanted to use it. Turning it off seems relatively simple as well. The company states, “If users have turned on Norton Crypto but no longer wish to use the feature, it can be deleted through Norton 360 by temporarily shutting off "tamper protection" (which allows users to modify the Norton installation) and deleting NCrypt.exe from your computer.”

Writers for The Verge debunked the worst scare-myths about Norton’s move into using its customers’ computer and electricity bills for crypto-mining, but were concerned about the high fees charged by Norton. They wrote that Norton’s 15% fees were much higher than most crypto-mining pool aggregators, observing that “Pool operators do often take a cut or fee for bringing everyone together. However, the fees are usually closer to 1 or 2 percent, which is obviously significantly lower. And, of course, there’s the elephant in the room: anyone using Norton’s software to mine has already paid the company a subscription fee for its security software…. In real numbers, a night of mining on an RTX 3060 Ti netted $0.66 cents worth of Ethereum and cost $0.66 in off-peak electricity. Norton took all the profit.” Before you can use the cryptocurrency that you just mined, you will need to transfer it from your Norton wallet to a Coinbase account, incurring a gas fee charged by the Ethereum network.

Fees are likely to eat your profits and possibly more. Is this the kind of boldness that Matt Damon goads us to embrace in his pro-crypto-investment television commercials? No, but bringing more people into Ethereum mining increases the pool for those already invested, so the result is positive for the crypto-hype people (like the ones paying Damon to hype for them). Not so much for others. The Winklevoss brothers win; we lose.

Why would this strategy make sense to Norton, a security software company? Despite dubiously claiming that Norton Crypto is a security-focused product, Norton may simply be offering this product to open new revenue streams for the company. Norton has undoubtedly been noticing troubling trends with its traditional product line, all companies in the antivirus software industry may be hurting soon if they aren’t already. After a 20-year ascent, the independent anti-virus software industry could be obsolete within a few years. As with many important tools, antivirus shields are being built into our machine operating systems now, so Apple, Google and Microsoft will be providing acceptable anti-virus protection to most personal computer purchases.

As succinctly stated in Vice three years ago, “with the rise of security minded operating systems such as iOS and even Windows 10, there’s a growing chorus of experts who think that, perhaps, the best days of antivirus software are behind us. People might not need it so much anymore, and in some edge cases, it could pose some risks for users.” Norton may be reacting to the late life cycle position of its flagship product by forcing crypto-mining on a shrinking customer base while the base is still huge, pliant and receptive. Maybe this is a sensible play for a formerly ascendant company desperate for a second act.

Norton is now in the Ethereum mining business and it wants your computer to participate in this voluntary crypto-mining botnet. Can viral NFT trading cards from MacAfee or Kaspersky be far behind?

National Law Review, Volume XII, Number 18