SPRING 2018 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss leading cryptocurrency fundamentals, blockchain infrastructure basics and the regulatory, security and legal impact.

Cryptojacking: A Confluence of Opportunity and Intention

Confluence began as a geography term meaning the place where multiple streams or rivers meet. Like many words, the definition has expanded to encompass more modern ideas, including the meeting of multiple elements or ideas into a third. Hence, with the rapidly increasing processing requirements of cryptocurrency mining, meeting the near ubiquitous desire to monetize internet sites, and the ability of developers to adapt code, a confluence called "cryptojacking" is an increasing concern. Cryptojacking is the surreptitious introduction of cryptomining code onto a host device for the purpose of harnessing processing power and electrical resources to mine cryptocurrency without the device owner's permission or knowledge. Cryptojacking is another of those terms that follows the "what you see is what you get" philosophy of technology nomenclature: hijacking a CPU to work on cryptocurrency processing.

Good Intentions: The Road to Bad Places

The majority of sources trace the introduction of cryptojacking to Coinhive, a self-described "group of developers" who promoted their code as an alternative to intrusive advertising on websites. The idea was this: website owners would download the Coinhive mining code and provide site visitors with a choice to either allow the site to harness a fraction of CPU power from the visitor's device while visiting the site to mine (primarily the cryptocurrency Monero, the preferred cryptocurrency of Coinhive), and in exchange, the site would not pester you with intrusive advertising, such as those self-starting video ads. Coinhive would process the mining proceeds and pay the website owners, minus Coinhive's fees, the proceeds. Digital media outlet Salon.com has exactly this arrangement running on its site in a transparent manner: viewers can read about the process and choose whether or not to participate by allowing or blocking cryptomining via their device. In this way, website owners can continue to monetize their content and generate funds necessary to maintain services or just create a profit, and visitors have a choice about how they wish to "pay the piper."

As with many well intentioned, reasonable solutions, cryptojacking is the nefarious evolution of Coinhive's original proposal. Coinhive proposed a transparent, voluntary arrangement between

website and visitor. Cryptojacking is involuntary, and while not yet deemed illegal, appears to function like theft, as well as potentially causing physical harm. Cryptojacking code can be embedded directly into the Java script of a website (without the website owner's permission or knowledge) or can be spread by a click-through to a masked site purporting to be something other than a cryptojacking download. Currently, approximately 33,000 websites have some variation of cryptomining coded embedded in their script, and it's impossible to determine which sites have embedded the code intentionally, and which are victims of cryptojackers, as not all website owners announce their intention to conduct in-browser mining despite having added the code.

A Skilled Pickpocket

Cryptojacking occurs beneath the surface in several ways. First, there's no announcement on the host site letting visitors know that the code is lurking within the website's script. There's no option to opt-in or opt-out; the code self-installs and executes. Second, whereas the original Coinhive design was that once a user terminated their connection to the site, the cryptomining activitity would stop, with cryptojacking, in many cases, the code has been altered to continue harnessing CPU power and electricity as long as there remains a functional internet connection. Third, cryptojacking coders are utilizing pop-unders to place mining code on the task bar in Windows environments and continue mining without users being able to terminate the program by just closing the browser app. As an aside, cryptojacking can happen on mobile devices, although the processing power just isn't as great as desktop devices, so the occurrence is much less frequent.

The natural question that emerges from cryptojacking is: if there's a voluntary option that allows site visitors and cryptominers to agree to an above-board exchange, why would anyone engage in cryptojacking? Because the voluntary program allows users to opt-out thus denying CPU access, and, because the voluntary arrangement generally reallocates a small amount of CPU processing power from the device. Cryptojackers are inclined to harvest as much of the CPU power available as they can, a potentially damaging practice for device owners. CPU processing creates heat, and heat may damage the processing unit and by extension the device. Consuming CPU processing power can also slow down device speed, increasing the time required to execute tasks. Increased CPU processing also requires additional electrical power, and cryptojacking requires internet bandwidth, leaving the device owner with bigger electrical bills and slower internet. If you're an employer with a large network of internet connected devices, cryptojacking can become expensive in terms of device wear and tear, utility consumption, and lost employee time. Finally, there's evidence that cryptojacking code can open doors to ransomware and other cyberattacks, a clear and present danger to all.

Ghostbusting Cryptojackers

The good news is that there are ways to detect and prevent cryptojacking.

Detection – watch for these symptoms of cryptojacking:

1. Device fan runs more frequently and/or longer than usual. This could indicate that your CPU is heating up as a result of cryptojacking.
2. Device speed drops, or you notice lags in response time from apps or tasks. Your CPU may be busy with cryptomining, leaving little processing power for you.
3. Open your Task Manager (Windows) or Activity Monitor (Apple) and check the CPU usage. If it's running high, especially for internet browsing apps, it may indicate cryptojacking. High CPU usage is a relative term, and unless you're familiar with

your device's normal usage rate, you may wish to review this with experienced IT professionals such as Digital Mountain.

4. Expand the Taskbar (Windows) or Dock (Apple) and check for pop-unders hiding in the lower right corner near the date and time. Irrespective of the source, you want to ensure that anything lurking behind trusted function/app icons isn't a bad actor.
5. Monitor network traffic from a device not tied to a user's actions. Traffic that can't be connected to the specific tasks engaged in by a user may be an indication of cryptojacking. Again, you may wish to consult professionals such as Digital Mountain to analyze network traffic.

Prevention – basic steps to help prevent cryptojacking:

1. Keep security software updated. Many companies famous for their virus blocking software are now including cryptojacking protection. Check with your provider to see if they are.
2. Install a browser extension designed to block in-browser mining. Chrome's Coin-Hive Blocker is a script that prevents cryptomining scripts from running or downloading via Chrome. Simple to install and free, Coin-Hive Blocker can be accessed from Chrome's webstore. Apple's Opera browser for desktop devices has some cryptojacking protection as part of its ad-blocking software code. Windows Defender for Microsoft Edge claims to have cryptojacking prevention built-in. Firefox Tracking Protection claims the same.
3. Don't wait to respond to potential cryptojacking symptoms. While it may not be cryptojacking causing your device's fan to run overtime, it's still a sign that your device is heating up and may need attention.
4. Consult with IT professionals, such as Digital Mountain, who are knowledgeable and staying abreast of cryptojacking developments.
5. Include in your corporate IT policy language prohibiting the unauthorized mining of cryptocurrency by employees on company devices.

We're well past the point where we need to point out that the fast-flowing current of technology innovations has both advantages and risks. Cryptocurrency is an attractive product that many are looking to acquire, but not all police themselves witth integrity. Cryptojacking will undoubtedly continue to grow, as will defenses against it. At some point, we can be sure that a cryptojacking case will be heard by the courts, but until that time, our best defense is our vigilance. By creating our own confluence of education, prevention, and detection, we can help keep cryptojacking from churning up peaceful waters.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

ENFUSE 2018
Las Vegas, NV: May 21-24, 2018

MASTERS CONFERENCE
Chicago, IL: May 22, 2018

2018 EDRM WORKSHOP
Durham, NC: May 23-25, 2018

CYBERSECURITY LAW INSTITUTE
Washington, DC: May 23-24, 2018

NINETEENTH ANNUAL INSTITUTE ON PRIVACY AND DATA SECURITY LAW
New York, NY: May 29-30, 2018

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.

4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: