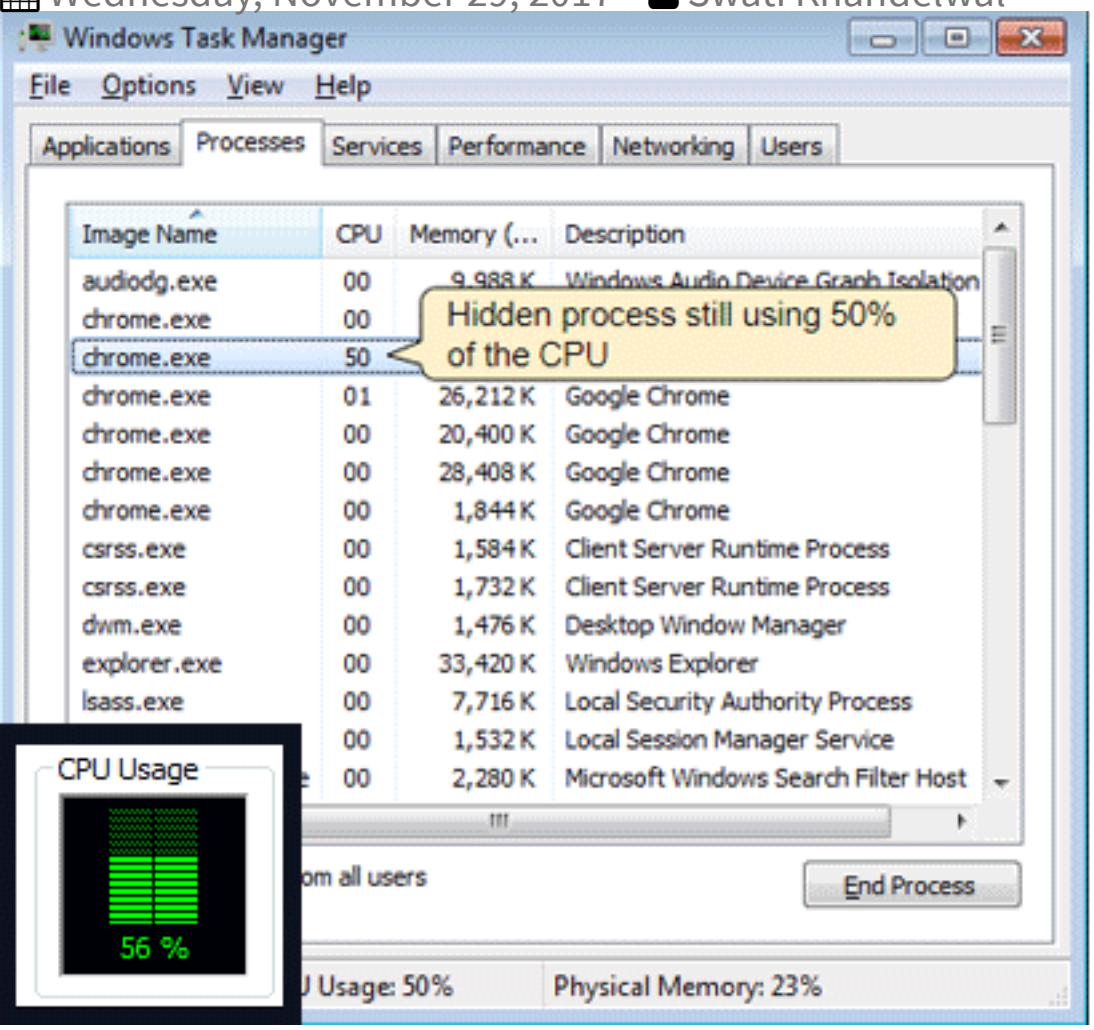
The Hacker News™
Security in a serious way

+1,698,300 421,550 2,070,880

Cryptocurrency Mining Scripts Now Run Even After You Close Your Browser

Wednesday, November 29, 2017 Swati Khandelwal



Some websites have found using a simple yet effective technique to keep their cryptocurrency mining javascript secretly running in the background even when you close your web browser.

Due to the recent surge in cryptocurrency prices, hackers and even legitimate website administrators are increasingly using JavaScript-based cryptocurrency miners to monetize by levying the CPU power of their visitor's PC to mine Bitcoin or other cryptocurrencies.

After the world's most popular torrent download website, **The Pirate Bay**, caught secretly using **Coinhive**, a browser-based cryptocurrency miner service, on its site last month, thousands of other websites also started using the service as an alternative monetization model to banner ads.

However, websites using such crypto-miner services can mine cryptocurrencies as long as you're on their site. Once you close the browser window, they lost access to your processor and associated resources, which eventually stops mining.

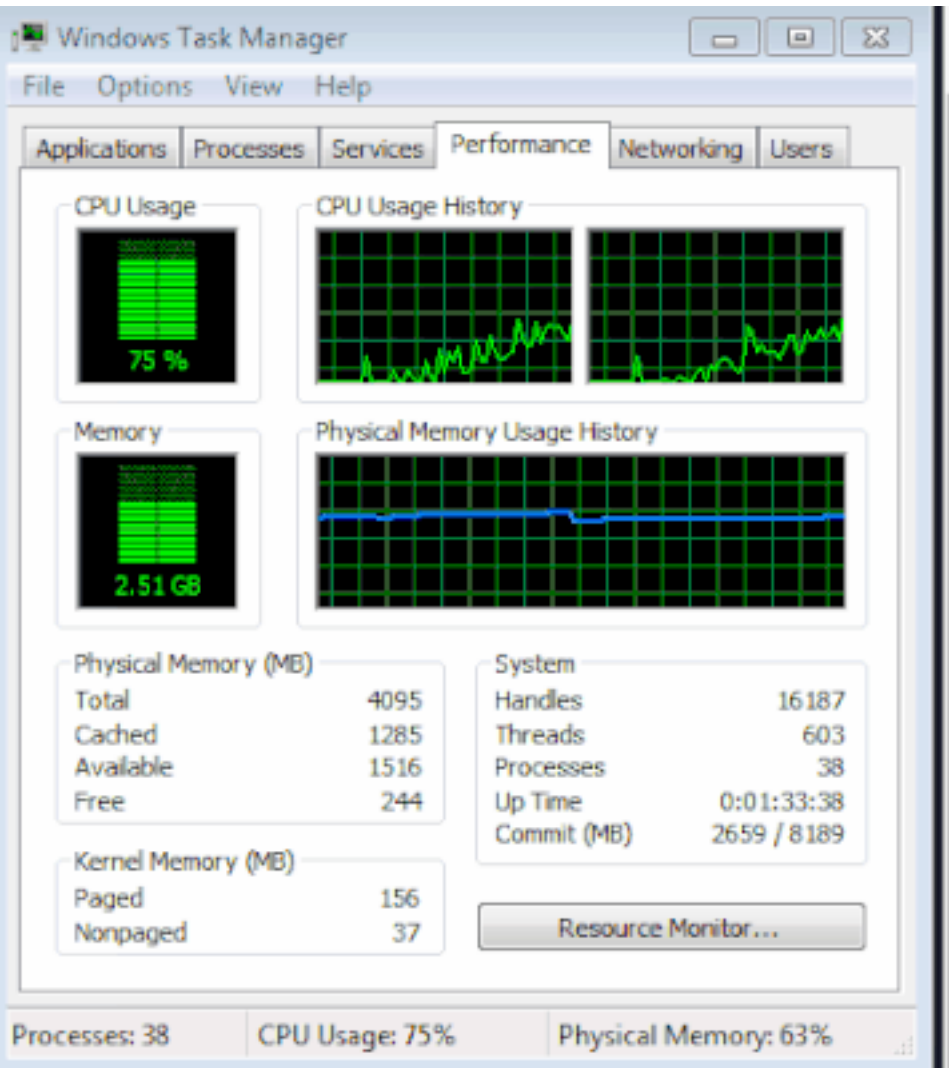
Unfortunately, this is not the case anymore.

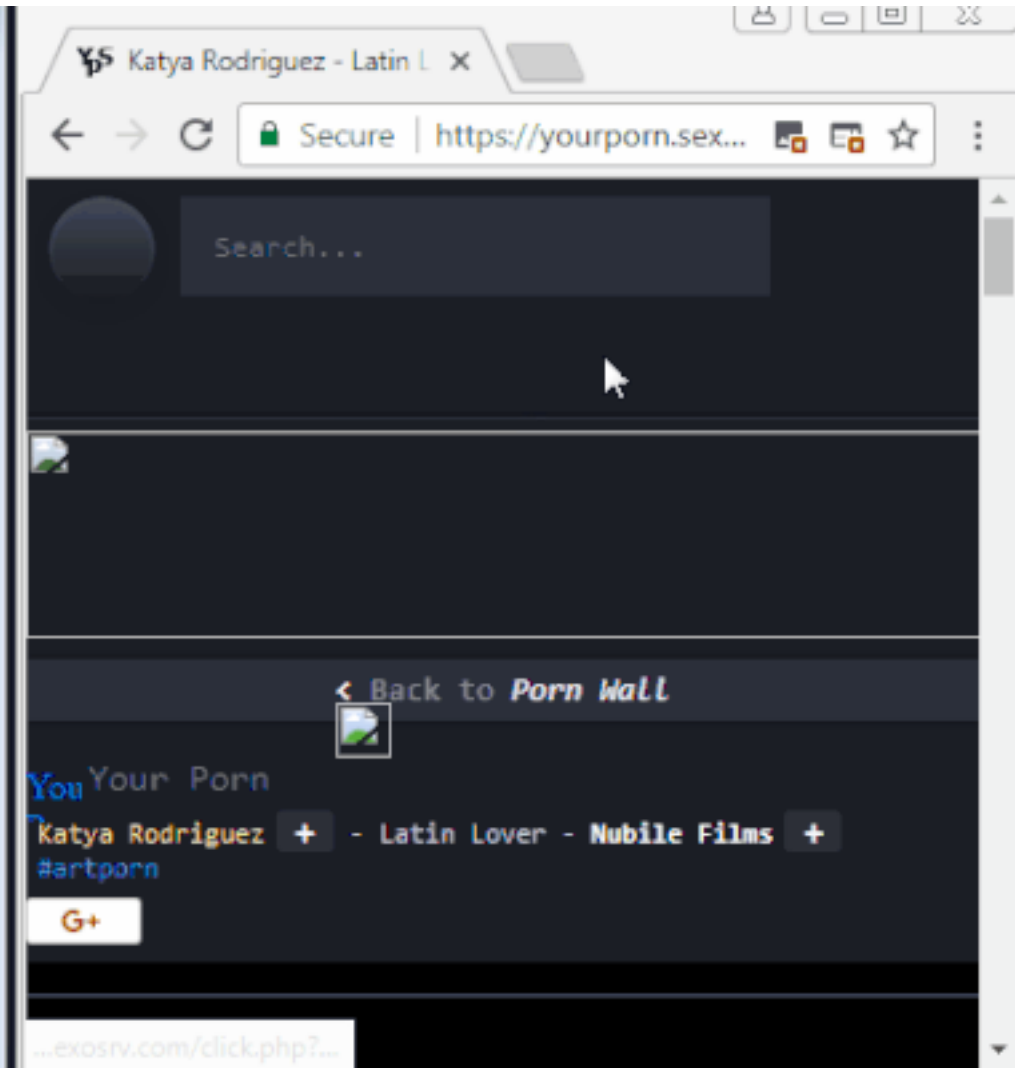
Security researchers from anti-malware provider Malwarebytes have found that some websites have discovered a clever trick to keep their cryptocurrency mining software running in the background even when you have closed the offending browser window.

How Does This Browser Technique Work?

According to a blog post published Wednesday morning by Malwarebytes, the new technique works by opening a hidden pop-under browser window that fits behind the taskbar and hides behind the clock on your Microsoft's Windows computer.

From there (hidden from your view), the website runs the crypto-miner code that indefinitely generates cryptocurrency for the person controlling the site while eating up CPU cycles and power from your computer until and unless you notice the window and close it.





Researchers say this technique is a lot harder to identify and able to bypass most ad-blockers because of how cleverly it hides itself. The crypto-miner runs from a crypto-mining engine hosted by Amazon Web Servers.

> "This type of pop-under is designed to bypass adblockers and is a lot harder to identify because of how cleverly it hides itself," Jérôme Segura, Malwarebytes' Lead Malware Intelligence Analyst, says in the post. "Closing the browser using the "X" is no longer sufficient."

To keep itself unidentified, the code running in the hidden browser always takes care of the maximum CPU usage and maintains threshold to a medium level.

You can also have a look at the animated GIF image that shows how this clever trick works.

This technique works on the latest version of Google's Chrome web browser running on the most recent versions of Microsoft's Windows 7 and Windows 10.

How to Block Hidden Cryptocurrency Miners

If you suspect your computer CPU is running a little harder than usual, just look for any browser windows in the taskbar. If you find any browser icon there, your computer is running a crypto-miner. Now simply, kill it.

More technical users can run Task Manager on their computer to ensure there is no remnant running browser processes and terminate them.

Since web browsers themselves currently are not blocking cryptocurrency miners neither does the integrated Windows Defender antivirus software, you can use antivirus programs that automatically block cryptocurrency miners on web pages you visit.

For this, you can contact your antivirus provider to check if they do.

Alternatively, you can make use of web browser extensions, like No Coin, that automatically block in-browser cryptocurrency miners for you, and regularly update themselves with new mining scripts that come out.

Created by developer Rafael Keramidas, No Coin is an open source extension that blocks Coin Hive and other similar cryptocurrency miners and is available for Google Chrome, Mozilla Firefox, and Opera.

No Coin currently does not support Microsoft Edge, Apple Safari, and Internet Explorer. So, those using one of these browsers can use an antimalware program that blocks cryptocurrency miners.

Swati Khandelwal

Technical Writer, Security Blogger and IT Analyst. She is a Technology Enthusiast with a keen eye on the Cyberspace and other tech related developments.

Bitcoin Mining, Browser Hacking, Cryptocurrency, Cryptocurrency Miner, Cryptocurrency Mining, Hacking News, Secure Browser

★ Latest Stories

Best Hacking Courses

💬 Comments

POPULAR STORIES

Pre-Installed Keylogger Found On Over 460 HP Laptop Models

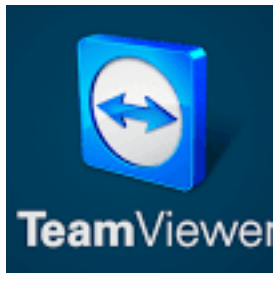
Microsoft Issues Emergency Windows Security Update For A Critical Vulnerability

Largest Crypto-Mining Exchange Hacked; Over $70 Million in Bitcoin Stolen

Learn Ethical Hacking Online: A to Z Training Courses

Collection of 1.4 Billion Plain-Text Leaked Passwords Found Circulating Online

Process Doppelgänging: New Malware Evasion Technique Works On All Windows Versions



New TeamViewer Hack Could Allow Clients to Hijack Viewers' Computer

Security Flaw Left Major Banking Apps Vulnerable to MiTM Attacks Over SSL

Android Flaw Lets Hackers Inject Malware Into Apps Without Altering Signatures

Google Researcher Releases iOS Exploit—Could Enable iOS 11 Jailbreak