OGLE AND YOUTUBE ARE NOW RAPING
ERS CPU'S!

w even YouTube serves ads with CPU-ining cryptocurrency miners

npaign lets attackers profit while unwitting users watch videos.

DAN GOODIN - JAN 26, 2018 7:27 PM UTC

YouTube was recently caught displaying ads that covertly leach off visitors' CPUs and electricity to generate digital currency on behalf of anonymous attackers, it was widely reported.

Word of the abusive ads started no later than Tuesday, as people took to social media sites to complain their antivirus programs were detecting cryptocurrency mining code when they visited YouTube. The warnings came even when people changed the browser they were using, and the warnings seemed to be limited to times when users were on YouTube.

> Great now my browser everytime I watch youtube... my anti virus always blocking coinhive because malware . Idk much about it but this is getting annoying and I need a solution please T n T
>
> — Arung (@ArungLaksmana) January 23, 2018

> Hey @avast_antivirus seems that you are blocking crypto miners (#coinhive) in @YouTube #ads
> Thank you :)https://t.co/p2JjwnQyxz
>
> — Diego Betto (@diegobetto) January 25, 2018

> Por lo visto @YouTube es muy gracioso y no le bastaba con bajarnos la audiencia, ahora van y nos meten el JavaScript de Coinhive para utilizar nuestros dispositivos para minar Monero! De verdad, @Google! Que leeches estáis haciendo con YouTube?? pic.twitter.com/NzMUMlArJs
>
> — ᛗ🦊ᛟErvoᛟ🦊ᛗ (@Mystic_Ervo) January 24, 2018

On Friday, researchers with antivirus provider Trend Micro said the ads helped drive a more than three-fold spike in Web miner detections. They said the attackers behind the ads were abusing Google's DoubleClick ad platform to display them to YouTube visitors in select countries, including Japan, France, Taiwan, Italy, and Spain.

The ads contain JavaScript that mines the digital coin known as Monero. In nine out of 10 cases, the ads will use publicly available JavaScript provided by Coinhive, a cryptocurrency-mining service that's controversial because it allows subscribers to profit by surreptitiously using the computers of other people. The remaining 10 percent of the time, the YouTube ads use private mining JavaScript that saves the attackers the 30 percent cut Coinhive takes. Both scripts are programmed to consume 80 percent of a visitor's CPU, leaving just barely enough resources for it to function.

"YouTube was likely targeted because users are typically on the site for an extended period of time," independent security researcher Troy Mursch told Ars. "This is a prime target for cryptojacking malware, because the longer the users are mining for cryptocurrency the more money is made." Mursch said a campaign from September that used the Showtime website to deliver cryptocurrency-mining ads is another example of attackers targeting a video site.

To add insult to injury, the malicious JavaScript in at least some cases was accompanied by graphics in displayed ads for fake AV programs, which scam people out of money and often install malware when they are run.

The above ad was posted on Tuesday. Like the ads analyzed by Trend Micro and posted on social media, it mined Monero coins on behalf of someone with the Coinhive site key of "h7axC8ytzLJhIxxvIHMeC0Iw0SPoDwCK." It's not possible to know how many coins the user has generated so far. Trend Micro said the campaign started January 18. It's not clear if Google has managed to start blocking the ads yet. Representatives weren't immediately available to comment for this post.

FURTHER READING
Cryptojacking craze that drains yo
now done by 2,500 sites

As the problem of Web-based cryptomining has surged to almost epidemic proportions, a variety of AV programs have started warning of cryptocurrency-mining scripts hosted on websites and giving users the option of blocking the activity. While drive-by cryptocurrency mining is an abuse that drains visitors' electricity and computing resources, there's no indication it installs ransomware or other types of malware, as long as people don't click on malicious downloads.

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Pre
News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001