Malicious ads dig virtual money right on the browser

The author of the malicious code uses JavaScript code transmitted via malvertising and digs a lot of digital currency on the user's browser without them knowing.

The author of the malicious code uses JavaScript code transmitted via malvertising and digs a lot of digital currency on the user's browser without them knowing.

This technique is currently being exploited on Russian and Ukrainian websites but bad guys are also planning to expand to other areas.

Ads malicious on game and streaming sites

Bad guys take advantage of online advertising companies that allow advertising to be exploited with custom JavaScript code. It is a modified version of MineCrunch (also known as Web Miner), a script launched in 2014 that can dig virtual money with JavaScript code running inside the browser.

Virtual money digging is very expensive and will slow down the user's computer. To avoid suspicion, the bad guys spread the malicious ads mainly on the video or game streaming sites in the browser.

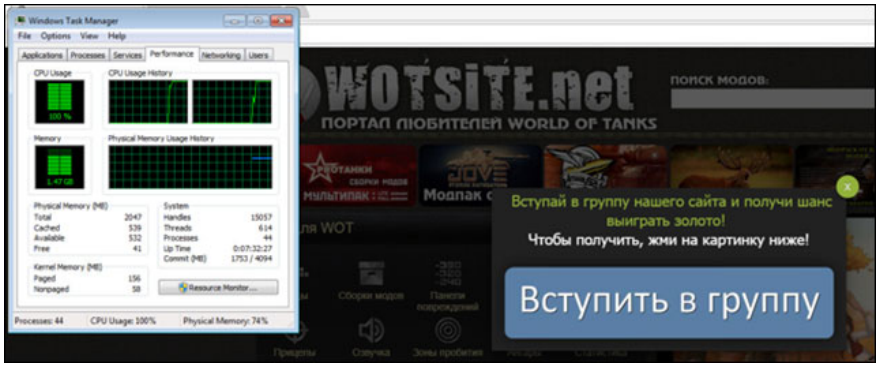
Both types of sites use a lot of resources and users will not be suspicious when their computer is a bit slow. Moreover, users also tend to stay longer on games or video stream sites, allowing digging and making profits for bad guys.

Monero, Zcash money digging tools and many other virtual currencies

ESET, the security company that discovered the malicious ad, said that JavaScript digging scripts can dig Monero, Feathercoin and Litecoin.

The bad guys seem to only have to use the Monero digging feature, the configuration for the Litecoin digging tool is left blank while Feathercoin is set by default, using the same Feathercoin address as on the demo page on GitHub. https://kukunin.github.io/webminer/

In addition, the researchers also found another campaign to conduct Zcash digging, apparently by another group. They do not use malicious ads but host JavaScript digging code right on the page. It is unclear whether this page is hacked or if the admin of the site knows the Zcash digging tool is hosted on its domain.



Digging virtual money when accessing net wotsite [.] Page

Based on DNS Lookup numbers for domains associated with the Monero digging campaign, ESET believes that the malicious ad domain receives a lot of DNS Lookup traffic like GitHub's Gist service.

Ad blocking tools can prevent JavaScript digging

The good news is that users can protect themselves from the JavaScript-based digging tools hidden in the code with ad blocking tools. The mining will stop when the user leaves the site and does not need any other cleaning tools to remove the malware from the computer.

1. How to block ads when surfing the web
2. 9 effective ad blocking tools for faster browsing

The ad blocking tool will not help if the code digs with JavaScript loaded from outside the selected domain or ad slot - the case of the website host and download the script from their own domain.

This is not the first time

The mining tool on the browser is nothing new. Services like Bitp.it have tested it since 2011 but eventually collapsed. In 2015, the company called Tidbit provided website owners with a way to dig virtual money on visitors' machines. Authorities think that this is illegal, no different from hacking because Tidbit or website owner does not ask the user to perform that action.

Digging virtual money is an attractive business for malware owners. According to a recent report, at least 1.65 million computers are infected with malware digging virtual money this year.