The Guardian

Cryptojacking attack hits Australian government websites

Hackers used plug-in to force computers to secretly mine cryptocurrency

Australian government websites were infected with the malware on Sunday. Photograph: Dave Hunt/AAP

Naaman Zhou

Mon 12 Feb 2018 12.48 AEDT

A series of Australian government websites, including the Victorian parliament's, have been compromised by malware that forces visitors' computers to secretly mine cryptocurrency, as part of a worldwide security breach.

The process, known as cryptojacking, forces a user's computer to mine cryptocurrency without their permission, generating profits for the hacker.

Government websites were infected with the malware on Sunday after a browser plug-in made by a third-party was compromised. Thousands of sites, including the UK's National Health Service, and the UK's own data protection watchdog, were affected.

In Australia the cryptojacking attack hit the official website of the Victorian parliament, the Queensland Civil and Administrative Tribunal, the Queensland ombudsman, the Queensland Community Legal Centre homepage, and the Queensland legislation website, which lists all of the state's acts and bills.

Hackers exploited a vulnerability in the popular browser plug-in Browsealoud, a program that converts website text to audio for visually impaired users.

The makers of Browsealoud, Texthelp, confirmed that hackers inserted a script known as Coinhive into their software. Coinhive hijacks the processing power of a user's computer to mine the cryptocurrency Monero.

On Monday morning, Texthelp took the Browsealoud plugin offline, which meant that new visitors to the affected sites would no longer load the cryptojacking script.

At the time of publication on Monday, the Queensland legislation website had taken the further step of removing the Browsealoud script entirely, but it remained on the sites of the Victorian parliament, QCAT and the Queensland ombudsman. On Monday afternoon QCAT contacted the Guardian to say it had removed the script from its website.

Scott Helme, a UK-based security researcher who discovered the malware, said government websites could have done more to prevent the attack.

"When you load software like this from a third party, that third party can change it and make it do whatever they want," he said. "There are easy ways to make sure they don't do that.

"We don't know how Texthelp were compromised yet, so it is hard to say whether they were really unlucky or there was some kind of inherent problem with what they were doing.

"But there were ways the government sites could have protected themselves from this. It may have been difficult for a small website, but I would have thought on a government website we should have expected these defence mechanisms to be in place."

Helme documented the attack on his website, while Texthelp said an investigation was under way.

"The company has examined the affected file thoroughly and can confirm that it did not redirect any data, it simply used the computers' CPUs to attempt to generate cryptocurrency," it said.

"The exploit was active for a period of four hours on Sunday. The Browsealoud service has been temporarily taken offline and the security breach has already been addressed, however Browsealoud will remain offline until Tuesday 12.00 GMT."

Other government sites affected include Victoria's City of Casey council, Western Australia's City of Bayswater council, South Australia's City of Unley council, and the office of the Queensland Public Guardian, which protects the rights of young children in care.

In December the Guardian reported that nearly 1 billion visitors to the video sites Openload, Streamango, Rapidvideo and OnlineVideoConverter were also being cryptojacked.

The office of the Queensland Parliamentary Council, which operates the Queensland legislation website, and the Victorian parliament have been contacted for comment.

Topics
Cybercrime