Thousands of websites infected by 'crypto mining' malware

February 12 2018

Researchers report a new kind of malware which operates in stealth mode to "mine" cryptocurrencies has infected at least 4,000 websites including those operated by government agencies

Thousands of websites around the world, including many operated by

governments, have been infected by hackers using the sites' computing power to "mine" cryptocurrencies, security researchers said.

The attack is the first major incident made public in which a new breed of hackers took over a large numbers of websites to effectively create currencies like bitcoin which are generated by using computing power.

The attacks made public over the weekend by British security researcher Scott Helme showed more than 4,000 website were infected in this manner, including those of the British data protection and privacy watchdog and the US federal courts system.

Unlike traditional attacks, these infections do not contain "ransomware" or steal data, but operate in stealth mode to make profits from the shadowy world of cryptocurrencies.

Helme said in a blog post Sunday that the hackers were able to reach large numbers of websites by infecting a commonly used "plug-in," or software which helps a site run better.

In this case, the hackers used the malicious software to create Monero, one of several new cryptocurrencies which are making a splash in financial markets.

"If you want to load a crypto miner on 1,000+ websites you don't attack 1,000+ websites, you attack the 1 website that they all load content from," he said.

The creator of the plug-in, the British software firm TextHelp, said it took the affected software offline after it discovered the "attempt to illegally generate cryptocurrency. "

"This was a criminal act and a thorough investigation is currently

underway," the company said in a statement.

Researchers have been warning in recent weeks about this kind of malware, which can deliver profits without being obvious to users.

Security researchers at Cisco Talos warned last month that this kind of hacking activity "has exponentially increased."

Because of the huge financial gains in cryptocurrencies, Cisco researchers said this has become a prime target for hackers.

"At a high level mining is simply using system resources to solve large mathematical calculations which result in some amount of cryptocurrency being awarded to the solvers," Cisco researchers wrote in a research note.

Security researcher Graham Cluley said the latest attack highlights vulnerabilities in websites which may have weaknesses in third party components.

"Things could have been much worse," Cluley said in a blog post. "Imagine if the plug-in had been tampered with to steal login passwords rather than steal CPU resources from visiting computers."

Citation: Thousands of websites infected by 'crypto mining' malware (2018, February 12) retrieved 4 May 2024 from https://phys.org/news/2018-02-thousands-websites-infected-crypto-malware.html