「政治真相」网站遭植入转址编程，用户被迫参与挖虚拟货币。《华盛顿邮报》图

绍祈编译

近期知名的政治爆料网站「政治真相」(PolitiFact)，疑似遭到重新导向网址的绑架，让意图拜访该网站的用户，都被导向另一个虚拟货币的网站。电脑专家透露，此类”转址绑架”的模式是网路常见的恶意软体，尽量减少点击网站或安装网路免费软体，是防止电脑遭骇的基本防护之道。

根据《华盛顿邮报》报道，网络安全研究员Troy Mursch在10月13日发现，自己的电脑在点击了「政治真相」网站後，电脑的运算核心(CPU)瞬间成了全速运转。原来拜访「政治真相」的用户都被转址导入了另一个网站，一旦用户进入这个类似比特币名为Monero币的网站，电脑便将该站的编程导入，让电脑变成自动采矿来开采Monero币。在这种情况下，用户的电脑将处於全面停摆，专注於编程挖虚拟币的状态。

另一网络安全记者Brian Krebs随後也证实了此一现象。坦帕湾时报(Tampa Bay Time)业主暨「政治真相」的执行长Aaron Sharockman回应，这应与一个第三方广告供应商有关，该网站正在升级广告与IT程式，将於稍後回复用户。

网路的虚拟货币在生成时，通常需要一个人来操控一台或多台计算机，透过数学运算来来产生虚拟货币。这类透过电脑运算产生虚拟币的情况，通常被俗称为挖矿。若在挖扩过程中投入更多的计算机来运算，将有助於加速虚拟货币的生成速度。

而「政治真相」网站用户所遭到的情况，就是典型的网路绑架，骇客透过恶意软体把用户绑架去参与挖扩。这类网路绑架是常见的网路恶性软体，有时透过关闭Java Script或使用广告拦截器，能帮助网路用户被绑架，但由於恶性软体防不慎防且常会更新版本，所以很难能避免这类网路的陷阱。

这已非第一次高流量网站遭虚拟货币的挖矿编程植入转址程式，知名的网路电视台Showtime和Pirate Bay等都曾改善网站避免被骇。而「政治真相」网站被植入的恶性转址编程码，也已在同日下午近4时左右完成清除。

「政治真相」网站公告已经清除了转址编程。《华盛顿邮报》图