新聞

【災情持續擴大，全球每天新增300個挖礦網站】黑色產業覬覦瀏覽器挖礦，5億訪客不知電腦變礦工

海盜灣偷藏挖礦程式曝光後，反而掀起了全球挖礦綁架的跟風，才3周，就有220個網站暗藏挖礦程式碼，5億名訪客的電腦成了挖礦肉雞，趨勢科技估計，全球每天會新增300個挖礦網站，挖礦綁架成了資安威脅清單一定要列上的新名詞

文/ iThome | 2017-11-06 發表

資料來源：AdGuard，2017年10月12日，iThome整理製圖

「天啊！上線8天，用量從每秒10萬次，暴增到每秒1,350萬次。」足足是135倍的爆量成長。瀏覽器挖礦服務Coinhive團隊在官網第一周營運報告中，毫不隱瞞自己的驚訝，也向數百封抱怨伺服器滿載的使用者投訴信，統一致歉。

9月14日，Coinhive剛推出了一項新型態的虛擬貨幣採礦平臺Coinhive，這是一個可在瀏覽器環境，用JavaScript執行球門羅幣（Monero，代號XMR）挖礦計算的服務。上線第一天，每秒只有10萬次挖礦雜奏運算（Hash）的API呼叫，但是，到了第8天，Coinhive平臺累計的挖礦雜奏運算呼叫次數，就爆衝到每秒1,350萬次呼叫，占了門羅幣這個全球第六大虛擬貨幣整體區塊Hash值計算量的5%，同時連上Coinhive的WebSocket連線數，多達220萬個，若以預設值每臺電腦用3個WebSocket連線數估算，相當有73萬臺電腦成了挖礦機。

原本Coinhive平臺所有系統，都部署在單一臺伺服器上，Coinhive也緊急在幾天內擴充到38臺主機規模的分散式叢集（28臺WebSocket代理伺服器、6臺Web伺服器、2臺資料庫伺服器和2臺維運用VPS），才撐住百倍爆量的需求。

但，Coinhive團隊的驚喜，旋即成了全球網民的痛苦。因為許多挖礦電腦的擁有者，並不知道自己的筆電、PC，或是手機，都成了暗中幫陌生人賺錢的挖礦機，CPU運算滿載，系統效能遲緩，甚至連打開文書處理軟體要寫份報告，都要等上好久。

9月15日，全球最大BT種子網站的使用者最先傳出災情，發現每次瀏覽海盜灣首頁，CPU使用率都會突然衝破80%，直到關閉網頁才停止。分析網頁程式碼後發現，海盜灣暗中執行Coinhive程式來挖礦，但沒有坦白告知而引用戶不滿，甚至鬧上媒體。

海盜灣事件讓Coinhive這個瀏覽器挖礦程式聲名大噪，廣大引起的關注，甚至引來了黑色產業的覬覦。趨勢科技研發部資深工程師王博榮指出，看上挖礦程式可以無風險地賺取虛擬貨幣利益，開始有黑色產業濫用Coinhive挖礦程式，將Coinhive挖礦程式惡意植入他人網頁。像趨勢科技就在9月19日時首次發現，惡名昭彰的惡意廣告組織ElTest，展開了植入Coinhive程式偷挖礦的活動，追查之下，早在9月14日，趨勢全球用戶已有人連上了暗藏Coinhive挖礦程式的網頁，最高峰是9月20日，一天內高達7萬次連線。

王博榮表示，觀測到9月底，嵌入Coinhive挖礦程式的網站，45%是英文語系，又以盜版影片網站和部落格為大宗，在臺灣也有幾個部落格上榜，不過多數網站都會首頁告知，一旦連上該網頁，就會用使用者的CPU來挖擴，若不願意提供CPU資源也可關閉，讓使用者選擇。

不過，依照趨勢科技的統計，全球每天至少增加300個藏有Coinhive挖礦程式的網站，甚至，95%以上的網站都未經用戶同意或告知，就開始偷偷挖礦。

依照趨勢的監控，黑色產業最初利用Coinhive的事件是發生在9月19日，EITest利用技術詐騙網頁的方式，讓用戶在不知情的情況下，淪為礦工，王博榮指出，這類的攻擊手法，是透過網站伺服器上執行的軟體系統，辨識造訪網頁用戶的電腦軟體漏洞，並藉機植入惡意程式。

舉例來說，駭客會發送偽裝成微軟技術解決的提醒視窗，提醒用戶的電腦系統，已經被惡意軟體侵害，但是用戶卻無法關閉該視窗，接著，該網頁就就會從Coinhive的伺服器上，下載JavaScript的挖礦腳本，並偷偷將用戶的電腦，變成一個礦工。

黑色產業開始覬覦，3周災情就蔓延全球

黑色產業覬覦瀏覽器挖礦，災情越演越烈。知名廣告過濾服務AdGuard展開了一項全球性的網站清查，緊急在10月12日公布了結果。AdGuard發現，海盜灣網站不是特例，Alexa排名前10萬的網站，有220個網站，暗藏了挖礦程式，其中最大者是在法國排名70大的檔案分享平臺Uptobox，每月訪客數多達6,000萬人次，臺灣也有4個網站上榜。這批網站每月平均訪客，累計多達5億人次，若不考慮一人造訪多個網站的重複情況，可以說，全球這5億名訪客的電腦，都成了挖礦機，在瀏覽這批網站時，偷偷地暗中挖礦。

這些網站大多沒有告知使用者，就像是偷用使用者的瀏覽器來挖礦，像Uptobox技術長緊急出面解釋，暗中執行挖礦程式而未告知，是為了測試新的營收模式，事件曝光後，也承諾會改回原來的網路廣告模式。

綁架10萬臺PC的瀏覽器挖礦，能獲利多少？

根據Check Point估計，目前每天約可以挖出720個門羅幣區塊，獎勵金合計有4,464個門羅幣。而一般PC的算力，啟用4個瀏覽器執行緒時，每秒可以計算出45個Hash值，相較於全球門羅幣的算力是每秒2億6,612.2萬個Hash，按算力比例，一臺PC執行一天可以賺到0.000754個門羅幣。以10月底門羅幣每顆約88.46美元的幣值，挖礦網站若能綁架10萬臺PC，連續執行1天挖礦程式，就可以不勞而獲，賺到相當於臺幣20萬元的收入。

暗中測試這種靠用戶挖礦獲利的網站，不只Uptobox，AdGuard後來還發現，美國知名CBS媒體集團旗下，有百萬用戶的影音串流服務Showtime.com網站也藏了Coinhive程式，直到事件曝光後就移除了，但Showtime拒絕說明這是主動測試還是網站遭駭。

挖礦綁架植入手法開始多元化

這種綁架使用者瀏覽器暗中挖礦的行為，開始出現一個專有名詞「挖礦綁架」（Cryptojacking）來形容，成了專家資安威脅清單上最新一項威脅，趨勢科技、Fortinet、Check Point等資安業者相繼投入研究，甚至開始攔截，或列入要阻擋的惡意威脅清單。

如廣告過濾軟體如AdGuard開始提供阻擋機制，而防毒軟體Avast則是當用戶瀏覽這類網站時，直接阻擋挖礦程式碼。Check Point也將這類挖礦綁架的網頁視為重大威脅，在自家安全閘道器產品中列入封鎖名單。更有電信業者，如中華電信開始將Coinhive網址列入企業資安黑名單，禁止用戶瀏覽。CDN業者Cloudflare也開始封鎖那些擅自利用使用者電腦資源採礦的帳號與服務。Coinhive官方更因產品遭濫用而出面道歉，並推出了會強制跳出告知說明的新版JavaScript挖礦程式，但，舊版本仍持續服務。

不過，瀏覽器挖礦技術還在持續變化，而挖礦綁架手法也開始進化，一來開始出現更多種類的挖礦程式，除了Coinhive，還有JSEcoin、CryptoLoot、MineMyTraffic，以及10月底出現的Papoto，有意用瀏覽器挖礦者開始有更多選擇，而資安黑名單要封鎖的挖礦程式網址，也越來越多，甚至防不勝防。

挖礦腳本程式植入手法越來越多元，先前大多是藏在網頁頁尾程式碼中，但最近，網站安全公司Sucuri就發現了好幾種新手法，一來是將Coinhive程式碼加密，降低被發現的機率，另一種是直接植入知名部落格平臺WordPress核心網頁，如管理模組標頭網頁admin-header.php，或通用範本檔general-template.php中，第三種Sucuri發現的新手法則更難偵測，挖礦腳本程式直接寫入了開源電商平臺Magento的資料庫，當你打開購物車程式，從資料庫取出的不是訂單資訊，而是要來綁架瀏覽器的挖礦程式。而資安公司Check Point則發現，有影音網站跳出的Flash Video Player安裝提醒視窗中，也會暗中執行挖礦程式。甚至，WordPress已有一項挖礦免費擴充套件，直接安裝就可以啟用瀏覽器挖礦功能，來偷用用戶的CPU資源。王博榮表示，這款套件預設是不開啟使用者告知機制。趨勢科技甚至發現了多款含有採礦能力的行動App，利用內建Webview動態載入JavaScript與原生程式碼注入來閃避偵測，其中有兩款App用的就是Coinhive的挖礦程式。

如何避免自家電腦淪為礦工？

一般用戶可以開啟系統監控CPU使用率的工具，是否連上特定網頁時，CPU使用率突然飆高，關掉網頁後卻又恢復正常，就可能藏有挖礦程式。或使用Chrome瀏覽器時，按下F12打開開發者工具，查看Network功能分頁，若開啟的網頁藏有挖礦程式，會出現異常網路流量，或有不尋常的wasm檔案。

而在企業端，王博榮建議，因挖礦網站須連回Coinhive伺服器才能進行挖礦作業，因此，企業只要封鎖Coinhive網址的連線行為，就能阻止。目前也有廣告過濾程式如AdBlock Plus和AdGuard可以直接阻擋Coinhive的JavaScript程式，Chrome瀏覽器也出現了幾款專門封鎖挖礦行為的外掛，如AntiMiner、No Coin、MinerBlock等。

而對網站開發人員而言，王博榮提醒，需注意所用的第三方套件，最好用程式碼掃描工具，過濾挖礦程式的API，或是避免出現挖礦程式函式庫的連結，也要避用剛推出而未有大量使用者的套件，尤其是整合多功能的複雜套件，應更謹慎。文⊙王宏仁、何維涓

更多 iThome相關內容

- 鼎新電腦貼公告，提醒BPM用戶注意挖礦程式偷算力
- 採礦程式商Coinhive的DNS遭駭，開採的Monero加密貨幣全進了駭客口袋
- 【軟體供應鏈上游出包，開發老手都難防】挖礦綁架臺灣曝光第一例，遭害苦主保哥現身說法
- 資安與情報專家接掌資策會CEO，未來將切入臺灣資安市場與創業輔導需求
- Sony用區塊鏈技術強化多因素認證安全
- 久等了! 蘋果釋出iOS 11.1修補KRACK漏洞，新增逾70款表情符號

讚 4.5 萬

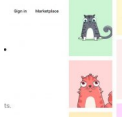
熱門新聞

圖靈耗費2年心力，但雲端加AI只用15分鐘，就破解了納粹Enigma密碼機

2017-12-04

蘋果緊急釋出iOS 11.2，修補iPhone當機問題

2017-12-04



以太幣遊戲《CryptoKitties》上線不到一周，交易額突破190萬美元

2017-12-04

Autodesk營運表現不佳，準備大砍13%人力、裁逾1000個職位

2017-11-30

macOS High Sierra最新修補沒效？用戶抱怨更新後根漏洞還在！蘋果緊急呼籲：更新完得重開機才有用

2017-12-04

Linux重大漏洞Dirty COW修補不完全，再補一次!

2017-12-04

NSA雇員坦承將機密資料帶回家，傳駭客利用卡巴斯基竊取資料

2017-12-04

卡巴斯基又面臨政府抵制!? 英國網安單位呼籲不要使用俄國籍防毒軟體

2017-12-04

Google在印度發表專為低階手機打造的Go版Android Oreo

2017-12-05

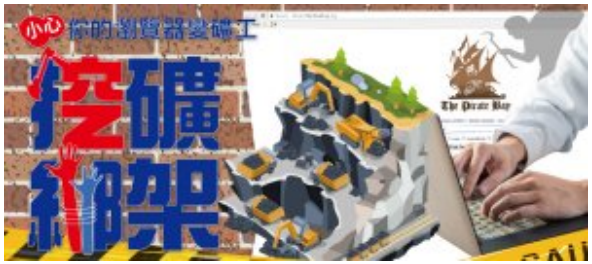
總統府將首度舉辦府會資安周，展示過去一年資安即國安的成果

2017-12-05

專題報導

臺灣人工智慧的困局，真的無解嗎？

新容器調度時代：Kubernetes稱王



挖礦綁架，小心你的瀏覽器變礦工

2017全快閃儲存陣列採購大特輯【市場總覽篇】

網頁安全閘道設備採購大特輯