資安

挖礦：您扮演的角色是羊還是狼？


Ben Nahorney
2018 年 12 月 11 日 0 則留言

對威脅發動者而言，金錢就算不是最具吸引力的誘因，也是一項極具吸引力的誘因。無論是殭屍網路的擁有者將其服務出租供他人發動 DDoS 攻擊，或者技術支援騙子用亂槍打鳥的方式聯絡使用者，意圖說服他們相信自己的電腦發生問題了，還是銷售點木馬程式側錄信用卡卡號，賺錢正是今日我們所見到之威脅相關活動的根本動機所在。

截至目前為止，惡意挖礦已經登上 2018 年最賺錢的威脅伎倆的寶座。這是目前思科 Talos 威脅情報團隊已經研究了一段時間的主題。對攻擊者而言，這幾乎就是完美的犯罪活動了：不但可以隱身幕後，與受害目標的互動少得幾乎可以忽略不計，而且還獲利豐厚。

不過，在我們深入了解威脅層面之前，我們要先退一步想想，了解加密貨幣與挖礦的相關資訊。

什麼是加密貨幣？

從根本來說，加密貨幣是一種數位貨幣，它與世界各國家或經濟區所經營之集中管理的銀行體系沒有關聯。加密貨幣大約在十年前首次問世（正是比特幣），如今的加密貨幣市場則出現了數以千計的數位貨幣。

使加密貨幣如此風行的一項特色就是「區塊鏈」，那是一種公共數位總帳，可用於驗證貨幣與交易。區塊鏈技術的主要優勢就在於它難以修改或竄改，而且由於加密技術與其分散的特性，更有助於確保使用加密貨幣交易的安全性。

什麼是挖礦？

無論是稱為貨幣挖礦，加密貨幣挖礦或者簡稱為挖礦，這就是指產生或賺取新貨幣的程序。盡管各種貨幣之間或許稍有不同，大致上，挖礦是指在區塊鏈上驗證交易的程序，執行此程序所付出的努力會因此獲得支付的費用做為報酬。事實上，您可以藉由協助驗證區塊鏈及其中的交易總帳而賺取貨幣。

在某些加密貨幣中（如比特幣），新貨幣可以在新的交易區塊加入區塊鏈時產生。這個範例，正是在驗證區塊鏈上的交易時，以「挖礦」方式獲得新貨幣的本質。

那有什麼壞處嗎？

其實，可以說是沒有。無論是加密貨或挖礦都與惡意手段毫無關係。如今有很多好人正在使用加密貨幣，並參與挖礦活動。區別您日常進行的挖礦與惡意挖礦的一個主要層面，就在於：同意。

使用者自行安裝的挖礦軟體與惡意人士安裝的挖礦軟體之間的區別，往往十分微小。事實上，在許多情況下，兩者都是完全相同。其中的差別在於，惡意挖礦軟體是在擁有者不知情的情況下執行。然而，在裝置上執行的任何軟體，只要擁有者不知情，都會產生隱憂。

惡意挖礦是如何崛起的？

在惡意挖礦之前，勒索軟體也曾經成為以不正當的惡意方式賺錢者的寵兒。不過，由於使用者對於鎖定電腦的惡意軟體的伎倆日益熟悉，而企業也能以更完善的方式防範勒索軟體威脅要製造的災難，惡意人士開始把目光轉向他處。

惡意挖礦也具有一些先前的賺錢技倆所無具備的獨特優勢。使用勒索軟體，並不確保裝置使用者絕對會付錢。使用者手邊可能就有定期備份，因此他們並不在乎遭到入侵裝置上所發生的事情。在上述兩種案例中，只要使用檔案復原裝置，就能解決問題。

更危險的是，世界各地的執法單位都開始打擊勒索軟體攻擊者。由於針對勒索軟體的逮捕行動已經展開，越來越多的不肖之徒，開始轉向風險較低的叫賣惡意挖礦軟體。

過去幾年直到 2018 年上半年，加密貨幣的價值大幅攀升。惡意人士會留意任何與軟體相關、而且具有價值的事物，尤其是在勒索軟體的效力江河日下之時。

惡意挖礦具有的獨特優勢，使其得以蓬勃發展。挖礦另一項吸引人的因素，就在於在威脅方面，它正好位於灰色地帶。由於合法挖礦與惡意挖礦之間的差異甚微，因此許多使用者淪為後者的獵物時，其憂慮程度並不如他們發現自己的系統中存在其他威脅。如果他只是在背景中默默地挖礦賺取貨幣，也沒有做其他的壞事，那又何必憂慮？在這種情況下，就會對攻擊者形成顯著的吸引力，因為他們可以攫取種種利益，而且還不會打擾到他們作案的對象。

披著羊皮的狼，仍然是頭惡狼

經過深刻反思，會發現我們有充足的理由要擔心惡意挖礦。

如同安裝在電腦上的任何軟體一般，挖礦都需要資源。只要有軟體耗用太多資源，就會對整體的系統效能產生不良影響。非僅如此，使用額外的資源也需要額外的電力才能進行。單一系統的耗電量增加或許不多，不過，在乘上組織中的端點數量後，您就會發現電費出現驚人的攀升。

此外，挖礦者在賺取來自企業網路的營收時，可能會牽涉到法規遵循的問題。這對於金融機構而言，尤其適用；因為利用企業資源來產生營收的作法（無論負責人是否知悉該作法），可能會受到嚴格的規範。

不過，最值得憂慮的或許是網路營運負責人對於惡意挖礦感染情況的渾然不覺，可能會導致網路組態或整體資安政策出現資安漏洞。攻擊者可以輕易的將這類漏洞用於其他用途。基本上，如果在網路中發現挖礦感染，還有什麼能夠阻止其他惡意威脅利用相同的漏洞進行惡意活動？

惡意挖礦是如何感染一台裝置的？

方法有很多，儘管鮮少有新穎的方法。傳遞惡意挖礦軟體所使用的手法，與傳遞其他惡意威脅的方法並無二致：

- 利用端點和伺服器應用程式中的漏洞
- 利用殭屍網路將挖礦軟體散播至先前就遭到入侵的裝置
- 傳送包括惡意附件的電子郵件
- 利用允許在網頁瀏覽器中進行挖礦的 JavaScript
- 利用會安裝瀏覽器外掛程式的廣告軟體威脅的手法，可以用來執行挖礦

這些都是惡意採礦感染裝置越來越普遍惡意的方式。很自然地，就威脅來說，只要有辦法感染系統，攻擊者就會嘗試利用。

我要如何防止惡意挖礦？

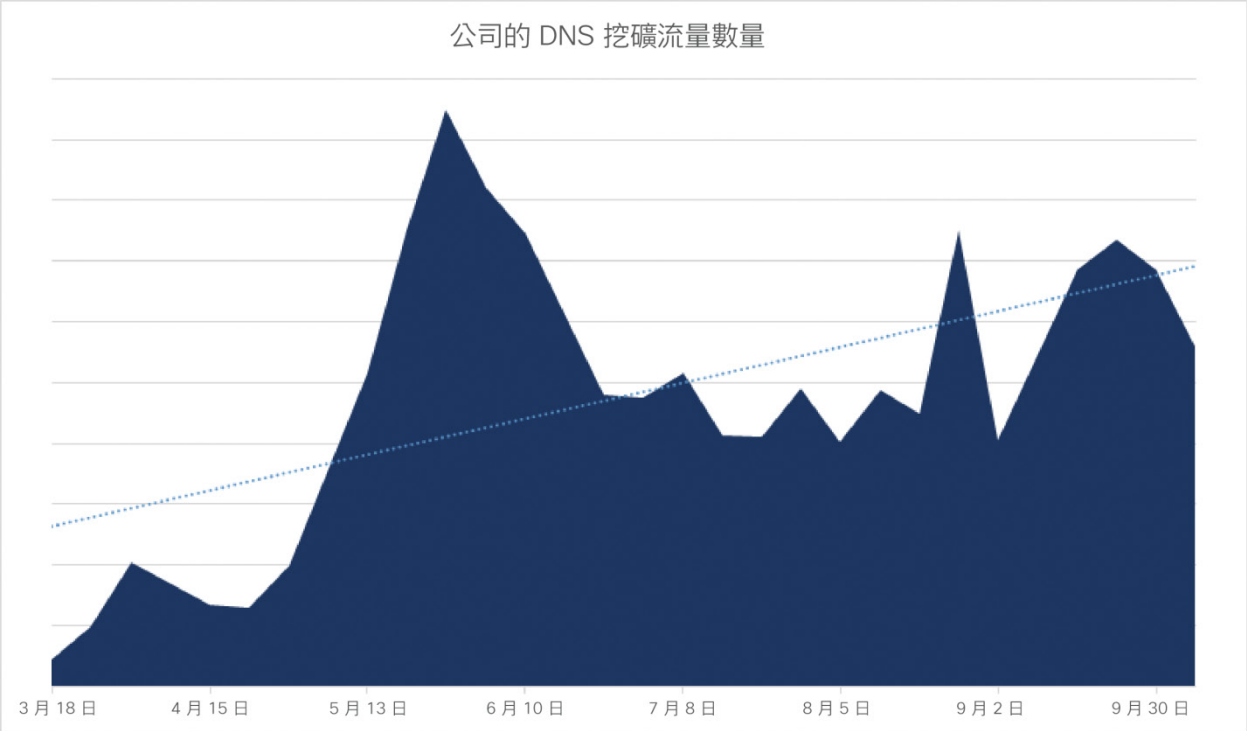
對於任何與威脅相關的事物而言，能夠將惡意挖礦拒之門外的良好資安防護，還有一條漫長的路途要走。

- 若要偵測並封鎖惡意挖礦，需要採用進階的端點保護並將其納入更廣泛的防禦策略中。
- 您可以運用網路資安分析，以找出您的組織中可能會出現挖礦活動的位置。
- 若要一開始就防止安裝挖礦應用程式，請封鎖已知參與挖掘加密貨幣的網站的網路連線。
- DNS 層安全性也可以非常有效地遏止挖礦，防止挖礦交易傳給惡意人士。

整體而言，若您藉由包含新一代防火牆、端點安全分析與 DNS 層在內的一系列有效的防禦措施以分層的方法來實踐資安，在偵測及預防您網路上的挖礦感染情況時，您就會更有把握安全無虞。

目前及長期展望是什麼？

綜觀其歷史，加密貨幣市場呈現相當具巨幅的揮發性。我們觀察發現，加密貨幣價值的暴起暴跌，與挖礦活動是息息相關的。例如，您可以檢視思科在 DNS 層觀察到的與挖礦相關流量的總量。儘管已經成長不少，重點就是挖礦隨著時間發展而更加風行。



有趣的是，許多熱門加密貨幣在相同的時間範圍內已經劇貶，整體趨勢呈現下挫的狀態。以門羅幣這種在惡意挖礦活動中經常使用的加密貨幣為例加以說明。

這些趨勢出現分歧，有幾個可能的原因。這可能只是因為部署容易、被捕的風險又降低，因此惡意人士不斷推出惡意挖礦；而且，如果使用者對於安裝在其裝置是的惡意挖礦軟體渾然不覺或毫不在意，那麼挖礦軟體駐留在裝置上的時間越久，他們獲利就更豐厚。

或者，因為加密貨幣的價值貶值，我們也可能會明確地看到挖礦活動全面地增加。惡意人士由於加密貨幣貶值，及其「憑藉感染所獲得的報酬」下降，為了維持收益金流，勢必進行更多的惡意挖礦活動。

結論

在威脅態勢中，金錢不但現在是，並且很可能向來都是惡意人士的主要誘因。在許多方面，惡意挖礦都是攻擊者視為本小利多地賺錢捷徑，因為相較於其他

威脅，受害者鮮少擔心其裝置上的這種威脅所產生影響。仍是那句老話，間接成本不容忽視，並且無論如何都應該妥善因應。

如需更多資訊，請參閱我們的白皮書了解如何保護您的網路不受挖礦威脅。若您已做好準備要進行下個步驟，請查看我們的 DNS 安全性解決方案的功能，同時索取 14 天免費試用版軟體。一如既往，我們誠摯地歡迎您在下方提供寶貴意見。

您是否喜愛這些類型的文章？訂閱「本月威脅」系列部落格文章，以便在識別出威脅時獲得警示。

更新：我們的 Talos 威脅情報團隊已完成兩篇新部落格文章，內容關於我們讀者可能會有興趣的挖礦狀態。Nick Biasini 的文章說明了 2018 年的挖礦史，包括值得注意的攻擊策略和他對 2019 年的預測。他們也分析了三個值得注意的挖礦團體的活動：Rocke、8220 Mining Group 和 Tor2Mine。

標籤：

- 比特幣
- 加密貨幣
- 挖礦
- 資安
- 資安思維領導
- 威脅情報
- 本月威脅