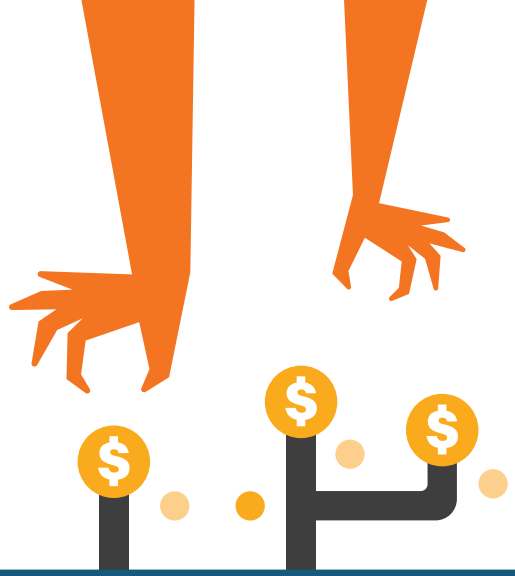
本月威脅：惡意挖礦



這是什麼？

當今我們所見的大多數威脅活動，都是以為惡意人士賺取收益為中心。若是說到勒索軟體，這種情況尤其明顯，攻擊者會鎖住遭到入侵的裝置，使其無法使用，然後向使用者索取贖金。然而，就算受到感染也不能保證對方一定會支付贖金。攻擊者已經了解到挖礦是他們生財之道，而且受害使用者往往對於挖礦一無所知。這種威脅會隱身在幕後為攻擊者賺取收益，而且完全無需綁架系統。這簡直是太完美了：只要使用者未偵測到威脅，駭客就可以坐享其成，看著加密貨幣不斷地滾進荷包。

為何您應該關心？

惡意挖礦盡管不像勒索軟體那樣具有破壞性，但也絕非攻擊者認為的：這是一種共生關係。如同安裝在電腦上的任何軟體一般，它也需要資源。我們都有這種經驗：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，在乘上您的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，挖礦者使用公司資源，可能也會牽涉到法規遵循方面問題。

挖礦是如何進行的？

挖礦就是在數位貨幣中賺取或產生貨幣的程序。賺取貨幣的方法，通常是協助確認支付驗證費的數位交易，或者在該程序中定期產生的新貨幣。挖礦可藉由在電腦上安裝專用應用程式達成，應用程式就會在背景中挖掘貨幣。另一種採礦方法則發生在網頁瀏覽器中。當您向裝載挖礦軟體的 Web 伺服器索取網頁時，伺服器存取網頁時，伺服器就開始挖礦。

為何我們重視這一點？

挖礦應用程式的內容及其本身未必是惡意的。若有人想要在自己的電腦上安裝一個這樣的應用程式，他們絕對有權這麼做。防毒軟體和其他端點技術則未必盡然有能力自行分辨合法挖礦軟體與未經核准的挖礦軟體之間的差異。您必須了解挖礦軟體的來源，以及在安裝後其所進行通訊的對象，而這需要更完善的資安解決方案才能辦到。

深入閱讀

- 使用思科資安產品，杜絕加密貨幣挖礦
- 保護您的網路免於受到挖礦影響
- https://blogs.cisco.com/security/demystifying-cryptocurrency-mining-threats
- https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html

CXX-XXXXXX-00　09/18

瞭解我該怎麼做？

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遏地止挖礦，防止挖礦交易傳給惡意人士。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。

思科如何保護您？

新世代防火牆/新世代入侵防禦系統	偵測並封鎖惡意流量，例如挖礦網站的連線。
進階惡意軟體防護 (AMP) 終端版	封鎖已知的惡意挖礦應用程式安裝。
思科 Stealthwatch®	偵測您網路上任何位置的挖礦活動，即使在加密流量中或隔離區中受到感染的主機也能輕鬆偵測（需使用思科 ISE 才能偵測隔離區）。
思科資安防護傘™	封鎖分類為已知的挖礦網域的流量。