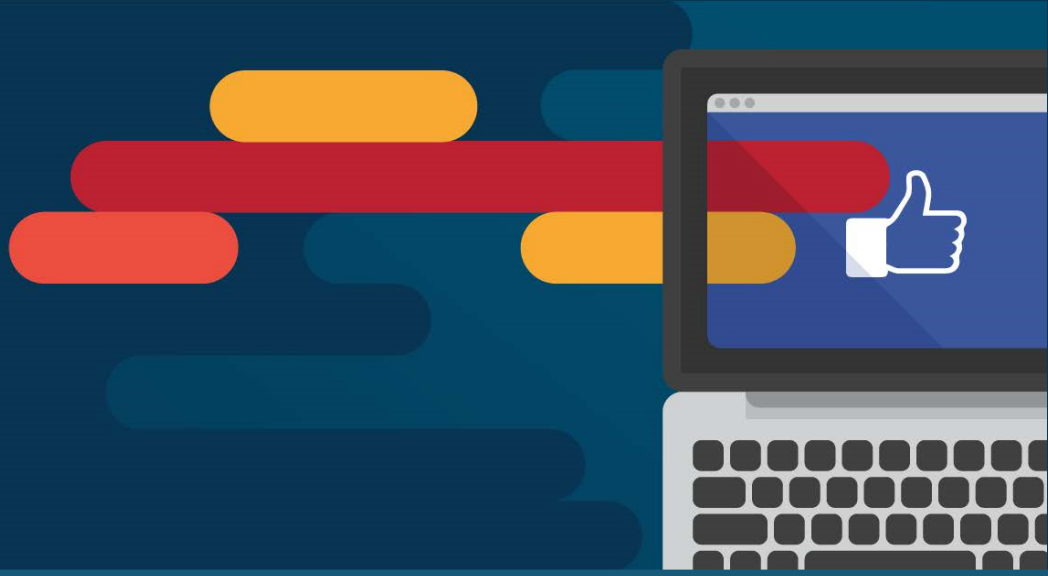

本月威脅：社交媒體與黑市

有什麼威脅？

許多人認為，網路犯罪只會發生在網際網路的邊緣地帶，而且躲藏在陰暗處，只有那些技術傾向和抱有惡意意圖的人才會找到它們。

不幸的是，情況似乎並非如此。其中一些活動在非常公開的場合進行，例如社交媒體平台。

什麼類型的活動？

Cisco Talos 的研究人員發現有 74 個 Facebook 群組作為市場和社群營運，目的是讓尋求購買和銷售被盜資訊或網路犯罪工具的攻擊者，發起網路釣魚活動。

共有 385,000 萬名成員屬於這些群組，群組成員會共用可疑的資訊，而最糟糕的情況下，這些共用的資訊是非法的。這等於佛羅里達州坦帕市的人口數。

是否有直接的危險？

往好處想的話，這項社交媒體活動目前尚未直接鎖定使用者們作為目標。被討論、購買和銷售的資料可能之前是透過資料外洩、銷售點入侵、網路釣魚詐騙，或遭入侵的裝置或網站上的鍵盤側錄程式竊取的。

但是，這項活動已發展到一定規模，讓 Talos 能夠確定，透過 Facebook 群組共用的部分工具，與受 Talos 監控的過往攻擊活動中所執行的惡意活動有關。

深入閱讀

- https://blog.talosintelligence.com/2019/04/hiding-in-plain-sight.html
- https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/
- https://blogs.cisco.com/security/social-media-and-black-markets

CXX-XXXXXX-00 0/19

該活動是否已遭遏制？

找出惡意群組之後，Talos 已與 Facebook 攜手合作，將這些群組從平台中移除。但是，很有可能會出現新的惡意群組。這只是惡意攻擊者利用 Facebook 群組的最新實例，我們在一年前發現過類似的狀況，並已將其關閉。

不僅如此，這種類型的活動不僅限於 Facebook。有人發現，惡意攻擊者曾利用其他社交媒體平台作類似用途。

我該怎麼做？

Facebook 和其他社交媒體平台致力於移除這類的群組。使用者應盡可能瞭解情況，並對類似情形有所警覺。身為使用者，最好的做法是在平台上發現這類活動時加以回報。回報的頻率越高，就越能吸引更多的注意力。

除此之外，資安團隊和廠商必須攜手合作，積極共用資訊、採取行動並告知客戶。各大企業必須致力於推動其防護和網路衛生工作。

思科如何保護您？

思科電子郵件安全	包含進階威脅防禦和網路釣魚防護功能，可更迅速地偵測、封鎖並修復傳入電子郵件中的威脅。
思科資安防護傘	可用於識別和封鎖涉及惡意活動的網域。
Threat Grid	協助識別惡意檔案行為，並自動通知所有思科資安產品。
AMP 終端版	提供持續監控和可追溯的安全功能，為終端提供最後一道防線。
思科威脅回應	可用來確認您的網路中是否存在被識別為惡意攻擊者所散佈的威脅。