每月热点威胁：社交媒体和黑市

威胁何在？

许多人认为网络犯罪活动已被摒弃于互联网的偏僻角落，只能潜藏于暗网之中，只有从事相关工作的技术人员和蓄意犯罪的恶意攻击者才会发现它。

遗憾的是，事实并非如此。有时候，在社交媒体平台等公共场合也会发生此类活动。

具体活动是什么？

思科 Talos 团队的研究人员发现，有 74 个 Facebook 群组运营市场和社区，恶意攻击者在其间买卖被盗信息或网络犯罪工具，以便发起网络钓鱼活动。

共有 38.5 万名成员加入这些群组分享可疑甚至违法信息，相当于佛罗里达州坦帕一个市的人口。

是否存在直接危险？

令人宽慰的是，这一媒体活动并不会直接将用户选作目标。这些群组讨论、购买和兜售的数据先前很可能是通过窃取数据、入侵销售点、执行网络钓鱼诈骗或利用受感染设备或网站上的键盘记录器窃取的。

但这类活动日益猖獗，以致于 Talos 确定通过 Facebook 群组分享的一些工具可能与过去 Talos 所监控活动中实施的恶意行为有关。

延伸阅读

- 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

该类活动是否遭到遏制？

发现恶意群组后，Talos 会与 Facebook 合作，以将其从平台中清除。但是，很可能会出现新的同类群组。这只是恶意攻击者利用 Facebook群组的最新事例罢了，大约在一年前我们也发现并制止了类似的情况。

不仅如此，这种类型的活动并非局限于 Facebook。有人发现恶意攻击者曾利用其他社交媒体平台以达成类似目的。

应该怎么办？

Facebook 以及其他社交媒体平台会采取行动清除此类群组。用户应尽可能了解情况并保持警惕。对用户而言，最好的做法是举报在平台上发现的此类活动。此类活动的曝光率越高，引起的关注也就更多。

此外，安全团队和供应商必须携手合作以积极分享信息、采取行动并告知客户。企业则需要在防护和网络安全机制方面做足功夫。

思科如何为您提供保护？

思科邮件安全	包括可以更快检测、阻止和修复传入邮件中的威胁的高级威胁防御和钓鱼功能。
思科 Umbrella	可用于识别和阻止恶意活动中涉及的域。
Threat Grid	可以帮助识别恶意文件行为，并自动通知所有思科安全产品。
面向终端的 AMP	提供持续监控和追溯性安全功能，为终端提供最后一道防线。
思科 Threat Response	可用于确定您的网络中是否存在被识别为恶意攻击者所散布的威胁。