At a glance
Cisco public

Threat of the Month: Social Media & Black Markets

What is the threat?

While many people think cybercrime is something that’s cast to the far corners of the Internet, hidden in the shadows where only those technically inclined and malicious in intent will find them.

Unfortunately, that doesn’t appear to be the case. Some of this activity takes place in very public places, such as social media platforms.

What sorts of activities?

Our researchers in Cisco Talos uncovered 74 Facebook groups run as marketplaces and communities for malicious actors looking to buy and sell stolen information or cybercrime tools to launch phishing campaigns.

A total of 385,000 members belonged to these groups, sharing information that was suspicious at best and illegal at worst. That’s the equivalent of the population of a city like Tampa, Florida.

Is there a direct danger?

The silver lining here is that users are not being targeted directly through this social media activity. The data being discussed, bought, and sold had likely previously been stolen through data breaches, point of sale compromises, phishing scams, or by keyloggers on compromised devices or web sites.

However, this activity had grown to the extent that Talos was able to establish that some of the tools being shared via the Facebook groups can be connected to malicious activity carried out in past campaigns that Talos has monitored.

Further reading

- 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

Has the activity been contained?

After identifying the malicious groups, Talos worked with Facebook to get them removed from the platform. However, it's highly likely that new groups will appear. This is only the latest instance of malicious actors leveraging Facebook groups, where a similar set was identified and shut down about a year ago.

Not only that, but this type of activity isn't just limited to Facebook. Malicious actors have been seen leveraging other social media platforms for similar purposes.

What should I do?

Facebook, and other social media platforms, do work to remove the such groups. Users should work to be as informed and skeptical as possible. As a user, the best thing to do is report such activity when spotted on a platform. The more often it's called out, the more attention can be drawn to it.

Beyond that, security teams and vendors must work together to actively share information, act, and inform customers. Businesses need to be diligent about their protection and cyber hygiene efforts.

How does Cisco protect you?

Cisco Email Security	Includes advanced threat defense and phishing capabilities that detect, block, and remediate threats in incoming email faster.
Cisco Umbrella	Can be used to identify and block domains involved in malicious activity.
Threat Grid	Helps identify malicious file behavior and automatically informs all Cisco Security products.
AMP for Endpoints	Offers continuous monitoring and retrospective security capabilities that provide a last line of defense for the endpoint.
Cisco Threat Response	Can be leveraged to determine if threats identified as being distributed by malicious actors are present in your network.