NSIGHT SERIES

October 2019 — Issue 2

Not Too Big to Fail

Managed attribution, VPNs, and a dark web market

"They obviously let their guard down after a surge in popularity."

This was the consensus on Reddit—"the front page of the internet"—after authorities seized the dark web marketplace Wall Street Market in April 2019. Observers attributed the market's seizure and the arrest of its three administrators to "a lack of basic OpSec [sic] from the hidden service operators."

But poor operational security (OPSEC) wasn't the sole contributor to Wall Street Market's demise; the administrators facilitated their own arrests by attempting to operate anonymously online using commercial virtual private networks (VPNs). As one Redditor commented, "In the end, you can't be 100% anonymous…and the poorer OPSEC you have, the easier it gets to identify you."

Wall Street Market's fate illustrates that VPNs are not an effective solution for managing your online attribution. Managed attribution (MA) is the process of controlling both the technical and behavioral indicators associated with your online identity or attribution. It is the foundation for successful online operations and combines technical solutions with operational best practices. By comparison, VPNs only encrypt your internet traffic and route it through a proxy; they do not protect user identities, particularly across multiple online sessions.

The Wall Street Market Admins

Three factors contributed to the arrest of the Wall Street Market administrators, Tibo Lousee, Jonathan Kalla, and Klaus-Martin Frost. First, was a result of VPN connection failures. Second, a lack of tools to help the administrators isolate their illicit activity from their private system. Third, the administrators' inability to manage their behavioral artifacts online. In short—the troublesome trio of administrators did not employ proper MA solutions.

Mr. Lousee was first identified after his VPN connection failed, causing his system to automatically connect to dark web infrastructure using an open, unencrypted connection that exposed his IP address and device information. Authorities confirmed his identity by assessing his online behavior, particularly his use of similar usernames across different sites. These usernames often included "420" references—references that also appeared on his vehicle's license plate and his bedroom wall. Thus, Mr. Lousee's failed VPN connection not only disclosed identifying information,

his VPN was also unable to provide him with any tools to compartmentalize his illicit online activity from his real life.

With Mr. Kalla, authorities first identified his true IP address and captured the dates and times that he accessed his commercial VPN from his personal computer. They then correlated this data with the dates and times that the commercial VPN's IP address (which was also known to authorities) accessed administration-only elements in the Wall Street Market's server infrastructure. The VPN failed to provide Mr. Kalla with an environment that would separate his illicit activities from his personal system. As a result, Mr. Kalla was able to be identified by third parties.

Finally, Mr. Frost's error was not technical, but rather behavioral. He cross-contaminated his cryptographic and cryptocurrency accounts by using the same PGP public key for two accounts on two separate markets. He also attached a bitcoin wallet with buyer information—including part of his legal name and a personal email address—to the second account. As opposed to Mr. Lousee, Mr. Frost's VPN did not fail; however, the VPN was completely unable to protect him from his own behavior.

Who Am I?

What can we gather from the Wall Street Market case? While VPNs attempt to mask your identity, true anonymity online is impossible. Every time you're online, you communicate information about yourself to other websites, users, and cyber entities. Leaving those identifiers blank or incoherent can attract unwanted attention. While VPNs offer a more private and secure means of trafficking data, they are not a complete managed attribution solution because they do not allow users to develop a curated web identity.

Moreover, VPNs are known and recognizable entities. This means that some websites will block or alter content for VPN users. Netflix and Pandora, for example, prevent VPN users from consuming most—if not all—of their content. Even if you can access a site's content, VPNs do not inhibit those sites from collecting technical and behavioral information about your browsing session. Social media platforms additionally use sophisticated mechanisms to track and compile users' data across the web. VPNs do not manage this information (e.g., cookies, DNS records, etc.), which can be correlated together to reveal your actual identity to the platforms with which you engage. In contrast, a more fulsome managed attribution solution can give you control over all of the information you are communicating.

Managed attribution solutions, by comparison, enable you to create and maintain a misattributed identity. This misattributed identity not only conceals your true affiliation

©2020 Ntrepid LLC. All rights reserved.
Ntrepid LLC Proprietary Information. 1-20-002

and information, it may also appeal to other users or grant you access to closed groups or sites. Thus, the Wall Street Market administrators fell short, in part, because they were using half-methods to obscure their identity and did not employ any methods to craft a replacement one. They were focused on not appearing as themselves, instead of developing a misattributed identity.

The Illusion of Security

VPNs are a satisfactory option for specific uses cases: ones that are low risk with short-term goals for users who want to partially obfuscate their identity from unsophisticated adversaries like internet service providers. They are insufficient for medium- to long-term operations with specific target audiences, and they do not include any tools to help users manage the behavioral artifacts that are associated with their online presence and present a risk to the discovery of their true identity. By using commercially available VPNs for their illicit activities, the Wall Street Market administrators left identifiable digital breadcrumbs online and exposed their true identities.

Ultimately, the greatest risk of using a VPN is that you believe that your identity is sufficiently hidden when it is not. At the time of its seizure Wall Street Market was the second largest dark web market in operation. Regardless of the scale of its shady success, however, because the admins relied on VPNs as their only MA solution, Wall Street Market was not too big to fail.

About Ntrepid

Ntrepid's suite of managed attribution products enable organizations to safely conduct their online activities. We are dedicated to understanding the challenges our customers face in order to build environments to facilitate secure operations in the most hostile network environments and against the most sophisticated opponents. We are proud to support Fortune 500 companies in the financial and healthcare sectors and customers across the national security community.

Contact us to learn more about the full spectrum of Ntrepid solutions.

www.ntrepidcorp.com
1.800.921.2414
solutions@ntrepidcorp.com

Ntrepid's Nsight Series analyzes emerging trends, challenges, and technologies that impact your online operations—all from the perspective of better managing your online attribution.

NTREPID®

©2020 Ntrepid LLC. All rights reserved.
Ntrepid LLC Proprietary Information. 1-20-002