Understanding Looming Threats and the Need to Hunt With Anonymity: A Security Week Article

Organizations are starting to adopt proactive cyber threat hunting to supplement traditional threat management practices. These existing practices were more focused on detection during and action after an incident has occurred. In contrast, the threat hunting approach involves actively searching your internal network for vulnerabilities, like un-patched systems and poor configurations that could potentially allow an attacker to get through. The next development for threat hunting is to go outside your network perimeter to understand the attackers themselves. The methodology emphasizes an enhanced awareness of your online surroundings as a key component to successfully identifying and anticipating threats.

In my Security Week Article, "Understanding Looming Threats and the Need to Hunt With Anonymity," I discuss the importance of situational awareness when engaging online – especially when hunting for threats outside the organization's firewalls. This kind of threat hunting is much less common because it requires special skills and introduces a whole new realm of risks and unknowns. However, hunting in the "wild" can produce unique and critical threat intelligence for your organization.

When hunting for threats, you don't want to draw attention to yourself or your mission.

In the article, I draw an analogy to the use of plain-clothed police officers in unmarked patrol cars. If a target realizes you are watching them, they can block your access, hide, feed you false information, or even attack your computer. So, blending into your surroundings with a form of digital camouflage is imperative. The problem with this is that remaining anonymous online is becoming more difficult. The minute you step out on the public internet, your target will be able to recognize you. Your IP address reveals your organization, and various trackers and metadata in your browser give away information about you and your online activities.

In the same way that the police department utilizes unmarked patrol cars, you can successfully remain anonymous on the internet if you have the right technology and avoid the tricks and pitfalls.

"Incognito mode" will not make you anonymous.

A common misconception is that turning on "incognito mode" in your browser will make you anonymous. But in reality, this only ensures that your browsing session's history and cookies are not saved. It does not mask critical identifiers such as your IP address, advanced trackers, or browser fingerprint.

NTREPID®

The first step to "getting out of uniform" while threat hunting is to use an IP address that is not associated with you, your organization, or even your general location. Next is to make sure that trackers can't make it easy for websites to recognize you when you visit. Tracking techniques are always evolving, which makes it difficult to completely remove them. The best approach is to operate within a virtual machine (VM). Virtual machines allow you to begin every session with a clean image, which you can restore to a clean saved version when you are done. This eliminates all trackers and destroys any malware that was picked up along the way, even if they have not been detected.

Finally, you need to make sure your browser's fingerprint can't reveal your identity. Completely hiding your browser fingerprint is impossible, but using one that is shared by many other people can help hide your identity. If you use a VM, it will always appear as if you're browsing on a newly installed operating system, which is the most common browser fingerprint.

If you can manage these identifiers, you will successfully blend-in to your online surroundings while monitoring activity and proactively searching for threats. To read my full Security Week Article, click here. For a more detailed explanation of hunting for advanced threats, tune in to my recent BrightTALK webinar, Wear Camouflage While Hunting Threats in the Wild.

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®