AN INTERVIEW WITH JEFF SPENCER
CEO, HYAS

CYBER ATTRIBUTION INTELLIGENCE

DETERMINING the source of a cyber-attack is recognized by most in our industry as one of the most challenging tasks for an enterprise security team. The simplicity of spoofing and the relative anonymity of the Dark Web contribute to this challenge, but the primary root challenge is the complexity of infrastructure. Weaving an attack from one compromised host to another, and another, is an easy way to hide the source of a threat.

HYAS provides a world-class capability to enterprise security teams who choose to address this attribution challenge. As one might expect, security analytics as one might find in a SOC are greatly assisted, perhaps even enabled, with the context of accurate attribution. We recently caught up with Jeff Spencer, CEO of HYAS, to learn more about how the company enables enterprises to solve many of the challenges of cyber attribution.

EA Why is determination of accurate cyber attribution such a difficult activity?

JS As you know, Ed – threat actors range from cybercriminals vandalizing systems for profit to nation-state actors targeting critical infrastructure. In the vast majority of cases, the actor would like to hide their identity. This might be to avoid law enforcement, hack backs, or other forms of retribution. As a result, threat actors have developed a host of strategies to obfuscate the infrastructure they use to carry out their attacks. Some common examples are; working from a compromised host, using non-attributable services like dynamic DNS and privacy protected domains, spoofing source IP addresses, and many others. The net result is that it's quite challenging to attribute infrastructure back to an actor and determine their intent using traditional security tools and threat intelligence. Because of this, most organizations have not focused on attribution because it was just too difficult. Recently however, we find that law enforcement, enterprise security and fraud teams, and other groups are increasingly wanting to identify the specific threats and threat actors targeting their organization, and focusing on the infrastructure threat actors use is one of the best ways to do that.

EA How does your solution offering address this challenge?

JS We provide cyber attribution intelligence by collecting and deriving information from a variety of traditional and non-traditional DNS sources, and help weave the intelligence into a clear picture for the organization of where a given attack likely originated. Obviously, we cannot do the types of things a nation-state might do with planted spies, signals intelligence, and other advanced means for collecting information. But in the context of legal, reasonable intelligence gathering, our Comox platform is the best resource in the world.

EA How do customers make use of this intelligence?

JS Customers use the Hyas Attribution and

Response Platform through subscription access to the web portal and also via API. Threat intelligence and Fraud teams are using the platform to bring attribution into their investigations where it wasn't possible or realistically feasible before. The feedback we've gotten is that this type of attribution is not available anywhere else, so we are confident that we are on the right track. Attribution has several layers of meaning to our customers: 1) Differentiating the attack by two kids out of a suburban UK home vs Class A office space in St Petersburg Russia, 2) Understanding which attacks are attacking the entire Internet vs the ones targeting just the customer and maybe their suppliers, 3) Preemptively blocking threat actors' infrastructure before it's used in an attack, and 4) Gathering the evidence to taking the actor off the street.

EA What's been your approach to supporting law enforcement?

JS I'm glad you mention this, because law enforcers have a different goal, obviously. Where an enterprise team might be providing information for their board, or might be using the data to enhance the accuracy of some SOC-based threat hunting, law enforcers are trying to bring offenders to justice. This is certainly complementary to what we enable for enterprises, but the motivation is different. We're honored to help law enforcers with this important task.

EA Any near- or long-term predictions about cyber attribution?

JS We'd like to think that our solution will help make attribution intelligence a standard tool for every analyst. We fully understand that the ease with which threat actors can hide will always make attribution a challenge, but that's why it's essential for analysts, CISOs, enterprise security staff, and law enforcers to take a close look at the Hyas platform. We believe we can provide substantive help to any organization's security program with the addition of attribution intelligence.