Q&A WITH FOUNDER, CHAIRMAN AND CEO OF CYBER DEFENSE FIRM ROOT9B

CYBERSECURITY VENTURES
OCTOBER 2016

Q&A WITH FOUNDER, CHAIRMAN AND CEO OF CYBER DEFENSE FIRM ROOT9B

The editors at Cybersecurity Ventures recently caught up with Eric Hipkins, Founder, Chairman and Chief Executive Officer at root9B, a rapidly expanding, publicly-traded cyber defense firm focused on advanced adversary pursuit — a.k.a. HUNT. Hipkins has served as CEO since May 2011. He has built a team of more than 50 tier-I Cyber Network Operators and Security Specialists, some of the top cyber-fighters in the world.

IN A NUTSHELL FOR PEOPLE WHO ARE NOT FAMILIAR, WHAT EXACTLY DOES IT MEAN TO HUNT?

Hunt is a defensive strategy that incorporates an active cyber defender (human) to proactively maneuver through the organization's proprietary network in order to identify indicators of an attack and preemptively counter these threats. In this approach, the human defender is armed with network telemetry and intelligence coupled with advanced detection and proactive response technologies. Essentially, the approach pits an active, thinking defender against an active, thinking attacker.

IS HUNTING DEFENSIVE OR OFFENSIVE?

Active Adversary Pursuit, or Hunt, in its purest form is Defensive; but is based on the model of thinking offensively in nature; "think like the attacker" to conduct defensive operations.

This man-against-man defensive concept is a familiar and proven approach in the physical landscape. The use of manned guards has become all too familiar in sensitive areas of both commercial and government organizations. The defender in the physical space leverages technology (fences, alarms, cameras, locks, etc.) to augment or supplement his or her ability to rapidly engage an adversary attempting to breach the perimeter or operating within the protected space. Should the guard identify a breach, he or she is equipped with appropriate defenses to actively secure the physical space and take action. These human defenders, are actively patrolling and investigating, cued by technology where there are indications of a breach in their space.

The concept of HUNT for Cyber operations is really no different. It is bringing the human defender back to the center of cyber defense while leveraging advanced technology to meet and defeat the human adversary. This defender must occupy the center of cyber defense while leveraging advanced technology to meet and defeat the human adversary residing in the uncontested network space. This implies a dedicated intelligence capability that studies the adversary and develops specific tools, techniques, and procedures to counter the adversary.

TO EFFECTIVELY HUNT, WHAT TYPE OF SKILL SET IS REQUIRED?

There are a number of fantastic security engineers in the cyber defense space with skill-sets that facilitate HUNT. These include backgrounds in security assessments, forensics, malware analysis, reverse engineering, incident response, etc.

That said, regardless of the specific skill-set, the defender must understand the adversary's mindset, motives, tactics, tendencies, and exploitation techniques. They must be well-trained, intimately familiar with both their adversaries, as well as the tactics and techniques employed by these threat actors.

They must understand not only their adversary, but also the vulnerabilities and potential targets within the organization they are defending. All of this must be backed by business context driven, specific, and actionable threat intelligence.

CAN CORPORATIONS TRAIN THEIR OWN IT SECURITY PEOPLE TO HUNT?

Absolutely.

Unfortunately, in order to conduct HUNT operations you really have to focus your training on understanding the mentality of the attacker and where they would focus their efforts. Rather than "reacting" to network attacks, HUNT Operators have to be focused on proactive surveillance of their networks. True security requires defenders to constantly evaluate their networks in order to deter attacks, create mitigation techniques, provide attribution, detection, and an appropriate response. They have to be prepared to adapt to their threat and tailor an appropriate solution.

DOES ROOT9B HAVE PRODUCTS THAT SUPPORT HUNT OPERATIONS?

root9B has developed several products that directly support Adversary Pursuit Operations or HUNT. These products enable cybersecurity professionals to actively maneuver and engage adversaries in their proprietary network. Examples include ORION, which features an agentless remote interrogation capability that provides full chain-of-custody, data analytics and live memory analysis. ORION delivers the expected level of back-end data analytics and easy network implementation for the client to realize immediate benefits from HUNT operations. ORKOS, provides interactive credential risk assessment and remediation by identifying the credential risks that lead to network breaches and adversary lateral movement within an enterprise.

"root9B brings vast military cyber experience to private sector firms and commercial enterprises" says Steve Morgan, founder and CEO at Cybersecurity Ventures. "Offering people with HUNT backgrounds to CIOs, CISOs, and IT security teams who are struggling with cyber operations and threat defense in the face of a severe cybersecurity workforce shortage is what really sets root9B apart from the rest of the field" adds Morgan.