HUNT

root9B

"As the organization that first introduced proactive HUNT operations to the commercial space in 2013, root9B has developed and refined its proprietary capabilities and methodologies to create the necessary shift from the current dependence on automated passive technologies."

May 25, 2016 root9B: The Threat Defiance Report

HUNT SECURING THE COMMERCIAL SECTOR SINCE 2013

Authored By: Eric Hipkins, John Harbaugh, Michael Morris & David Aucsmith

The current approach of cybersecurity is not working. This has been made abundantly clear by the media reports of a multitude of recent events and breaches (and others incidents not publicly reported). The damage caused by these events has affected every business sector: energy, retail, manufacturing, finance, medical, insurance, private and public.

These victims have adhered to the regulatory requirements and implemented industry accepted standard practices. These efforts have had little to no impact on the adversary's ability to successfully breach their network.[1] In many cases, the adversary continues to maintain access to the victim enterprise in excess of 140 days.

The current landscape of cyber victims is not negligent or unsophisticated. In most cases victims adhere to all compliance, regulatory, and industry standard practices. While these defensive measures are important, they are inadequate, especially when pitted against a patient, well-resourced Advanced Persistent Threat (APT) whose sophisticated techniques far outpace standard automated solutions. The issue is less about the organization's cyber investment, capability, or security infrastructure than it is about the current defensive practice used for cyber defense. Today's network defenders rely on traditional passive defense and automation. That said, adversaries are applying advanced techniques, orchestrating attacks, and actively targeting victims.

Adversaries find and exploit the gaps in defenses that rely solely on automated tools. Firewalls, security sensors, telemetry tools, and post-incident response protocols are no match for them. The only effective counter is another human being who stands in opposition to the APT's malicious activities. This trained and equipped defender must serve as the centerpiece of the organization's cyber defense strategy. 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 requires a significant shift in current cybersecurity protocol: bringing the human defender back to the center of cyber defense while leveraging advanced technology to meet and defeat the human adversary.

root9B, a root9B Technologies company (OTCQB: RTNB), has developed a new cyber defense approach focused on Active Adversary Pursuit (HUNT).

Their HUNT technique has been honed through cyber operations and training both within the Department of Defense and commercial community. These operations, and related training, include Network Defense Operations, HUNT missions[2], and the implementation of state-of-the-art defensive network designs. As the organization that first introduced proactive HUNT operations to the commercial space in 2013, root9B has developed and refined its proprietary capabilities and methodologies to create the necessary shift from the current focus and dependence on automated passive technologies. This new active defense, Manned Information Security, is currently being adopted across the Department of Defense, finance, retail and industrial control markets. The model is focused on identifying the adversary and its tactics, implementing pragmatic, cost-effective mitigation strategies, and understanding the client's business context (understanding what is most important to them) to pre-emptively defend against cyber-attacks. This is an operationally focused, human enabled model distinctly different from the often exploited, technology-driven passive defense protocols employed within most enterprise networks.

The current cybersecurity play-book is an inherently passive model. It is passive in that it relies on static hardening of the organizations' infrastructure and deployment of monitoring sensors around its network boundary to detect malicious code or intent. The defensive cyber sensors are configured to identify known artifacts or other predefined adversary indicators. Guidance on how to implement this cyber defensive structure abounds. Current cybersecurity best practices guide how cybersecurity professionals should harden their infrastructure and what their passive technologies should monitor. A broad assortment of organizations[3], industry forums[4], and even security vendors[5] publish supplemental cybersecurity standards and best practices. However, all of the best practices contain essentially the same three elements: reducing the organization's attack surface, identification and neutralization of malicious code, and the detection of anomalous behavior.

- Reducing the organization's attack surface - Best practices recommend technology and processes to isolate the organization, to the extent feasible, from the world at large and the steps that should be taken to reduce the possible points of attack. These recommendations are based on well-established and sound security principles such as least privilege, separation of privilege, audit, minimal number of open ports, services etc.

- Identification and neutralization of malicious code - standard practices tend to focus on technology and processes for identifying malicious code and intrusion techniques. This includes malware signature identification of attack tools (e.g., antivirus technology) and rapidly remediating any vulnerability targeted by malicious code (e.g., patching). It requires the collection of network traffic and the identification of indicators of malicious activity.

- Detection of anomalous behavior – Best practices recommend the installation of various automated anomaly detection mechanisms. These include network intrusion detection systems (IDS) and computer log scanners. These systems function by matching observed activity with rule sets that correspond to anomalous or known adversarial patterns. Keying on these rule sets allows these systems to identify and stop known bad events.

Unfortunately, these same published standards and practices provide the adversary a play-book of what they can expect from their target network. Through experience, the adversary also has a reasonable expectation that it will not face an active human defender in a cybersecurity landscape filled with automated technologies, published standards, antiquated best practices, and compliance requirements. They know that if they breach the network's boundary, they will most likely have freedom of movement within the victim's uncontested network interior.

The current state of today's cybersecurity programs reflect the learned best practices developed through dealing with the attack tools and techniques used in the past. Those responsible for cybersecurity have developed these best practices to try to deal with the

ever-changing panoply of network worms, viruses, and malicious code. These best practices continue to be necessary to deal with some amount of these types of attack tools and techniques, but are not sufficient when facing an actively engaged adversary targeting a network with motive and purpose.

The failure of the current defensive strategy lies in its static nature. Attack tools and techniques that employ advanced breaching techniques and polymorphic malware have evolved well beyond the capacity of static and passive defenses. The new model for attackers, particularly highly sophisticated or focused APT adversaries, is to execute targeted reconnaissance and intelligence of the victim's network defenses. Attacks are customized, unique, and adapted by a thinking, active, human adversary. If there is any hope of preventing this caliber of sophisticated attack, an active human defender must be involved.

Adversaries carefully develop the intelligence necessary to know what sensors and capabilities the defender has deployed. Adversaries train against those defenses and develop new and unique attack tools, techniques, and procedures that even the best practices of a static defense will not detect. Historically, no static or passive defense will long remain secure against an adversary who has freedom of initiative and movement.

In its simplest form, todays' cyber defense against an active adversary is a human conflict in cyberspace. The man-against-man struggle fits very well within the "OODA loop" (Observe, Orient, Decide, and Act) model of conflict theory developed by Colonel John Boyd between 1977 and 1992.[6] Boyd's theory of conflict is well suited for analyzing conflict in cyberspace, as it is more temporal than physical and spatial.[7] It focuses on the uncertainty created in an adversary who, while being significantly slower at processing situational information, is far more adept and resourceful at bypassing blocking defensive obstacles. William Lind summed up Boyd's theory as:

> *Conflict can be seen as time-competitive observation-orientated decision-action cycles. Each party to a conflict begins by observing. He observes himself, his physical surrounding and his enemy. On the basis of his observation, he orients, that is to say, he makes a mental image or "snapshot" of his situation. On the basis of this orientation, he makes a decision. He puts the decision into effect, i.e., he acts. Then because he assumes his action has changed the situation, he observes again, and starts the process anew . . .With each action, the slower party's action is inappropriate by a larger time margin. Even though he desperately strives to do something that will work, each action is less useful than its predecessor; he falls farther and farther behind. Ultimately, he ceases to be effective.*[8]

Unfortunately, a static defense will always lag behind an active attacker in processing situational information. It is inevitable. As the cyber attacker adapts in real- or near real-time to the tools, techniques, and procedures employed by static defensive measures, the attacker will always prevail. The only effective counter to a skilled, thinking, active attacker is a well-informed, thinking active cyber defender. That is, a defender who can compete with, and surpass, the attacker in Boyd's OODA loop.

The current cybersecurity defense model assumes that the network is secure until an alarm sounds. When this occurs an appropriate team investigates and resolves the issue. This approach is always a forensic or incident "after the fact" response event and is most likely too late to prevent the adversary from achieving its goal. This is a static defense that reacts to an identified threat and then initiates forensic analysis and remediation. The initiative is with the attacker. The current approach provides the adversary the freedom of action and the opportunity to conduct some or all of its offensive operations prior to the activation of the defender's countermeasures. In a best case, this results in a reactive response. In many cases, however, this is a catastrophic loss of network sovereignty for the defender.

A defensive strategy that incorporates an active cyber defender to proactively hunt for, and preemptively engage the adversary within the organization's proprietary network is needed to counter the evolving cyber threat. This new approach – Manned Information Security, or HUNT – pits an active, thinking defender against an active, thinking attacker.

The 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 the sensitive areas of both commercial and government organizations. Guards are present to inspect the current physical security infrastructure and maintain the integrity of their responsible spaces. 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. The key is that guards are not (or should not be) static, but instead present an unpredictable variable to the adversary. These human defenders, are actively patrolling and investigating, cued by technology where there are indications of a breach in their space. Best practices in the physical security space encourage the guards to be neither routine nor predictable; thus the attacker cannot anticipate the defender's actions.

In the cyber domain, an active adversary usually gains access to an organization through tailored tools, techniques, and procedures developed through good reconnaissance and intelligence gathering. The adversary exploits gaps in the network defenses using advanced tools or other techniques such as a phishing attack, waterhole attack, or other socially engineered path. Once inside an organization, the adversaries create redundant, stealthy capabilities to maintain their undetected presence and persistence. Eventually, they will attain their objective whether it is access to key corporate information, client/customer data, proprietary material, financial material, or other corporate "critical information." Once the adversary has unfettered access to these items, it will hide the exfiltration within legitimate communications. The theft is rarely observed and the adversary will remove any residual evidence of the operation. At this late stage, traditional passive scanning and detection tools will have an extremely difficult time detecting the adversary's tactics or tools. As a result, many organizations remain compromised in excess of 140 days before recognizing the network breach. This sobering metric is a testament to the challenges passive security defenses and technologies face against the human adversary.

To counter today's advanced cyber threat, the cybersecurity industry must continue to evolve to a Manned Information Security approach that applies a human defender armed with advanced detection and proactive response technology. This approach includes a human-based active adversary pursuit, or HUNT, environment where human defenders actively maneuver through their networks and systems to identify indicators of a network attack and preemptively counter these threats. This new defender needs accurate, relevant, specific intelligence to hunt for the adversary actively targeting their network. The tactics, techniques, and procedures of the adversary – their tradecraft – are constantly evolving. It requires dedicated resources with sophisticated means to remain cognizant of the adversary. It also needs to be comprehensive enough to understand what is important and what is not. This implies a dedicated intelligence capability that studies the adversary and develops specific tools, techniques, and procedures to counter the adversary. The new cyber defender can then localize this intelligence through an array of sensors deployed within an organization in accordance with industry standards and best practices. As noted, the old paradigm is still necessary; it is just no longer sufficient and needs to be supplemented by a Manned Information Security model. The combination of these efforts will create the necessary counter to today's elite human adversary.

The historical, highly published cyber-attacks underscore the weakness in a defensive approach that exclusively focuses on protecting networks with automated sensor systems and signature driven defenses.

The implicit assumption in this new defensive approach is that network defenders will know how to look for and recognize the adversary, deal with them when found, and leverage actionable threat intelligence to prevent the breach in the first place. 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.

This new cyber defense protocol of active, Manned Information Security, informed by relevant and specific threat intelligence, is necessary to halt the adversary's current freedom of maneuver in the defender's networks. This will empower network defense teams to expose and predict network attack vectors that currently go undetected by automated and passive security technologies.

[1] For example, please see AP, "JPMorgan Discloses Data Breach Affected Millions," CBS News, October 2, 2014, accessed March 16, 2016, http://www.cbsnews.com/news/jp-morgan-chase-discloses-massive-data-breach-at-new-york-based-bank/.

[2] "HUNT" is the term used by root9B to denote intelligence driven active manned information security, as in to "hunt" the adversary.

[3] For example, the NIST Cybersecurity Framework, see NIST, "Cybersecurity Framework," NIST, accessed March 17, 2016, http://www.nist.gov/cyberframework/.

[4] For example, the Payment Card Industry Security Standards, see PCI Security Standards Council, "PCI Security Standards," PCI Security Standards Organization, accessed March 4, 2016, https://www.pcisecuritystandards.org/.

[5] For example, Microsoft's Enterprise Security Best Practices, see Microsoft, "Enterprise Security Best Practices," Microsoft, accessed March 4, 2016, https://technet.microsoft.com/en-us/library/dd277328.aspx.

[6] John Boyd, "Patterns of Conflict," Project White Horse, www.projectwhitehorse.com/pdfs/boyd/patterns of conflict.pdf.

[7] Robert B. Polk, "A Critique of the Boyd Theory - Is It Relevant to the Army?" Defense Analysis 16, no. 3 (2000): 258.

[8] William S. Lind, Maneuver Warfare Handbook (Boulder, Colo.: Westview Press, 1985), 5-6.

root9B
102 N. Cascade Ave | Suite 220
Colorado Springs | CO | 80903
info@root9b.com
www.root9b.com

INNOVATION · EXCELLENCE
root9B
AMAT VICTORIA CURAM