Cyber Hunt Team Operations and Counterintelligence

By SpearTip

June 10, 2015

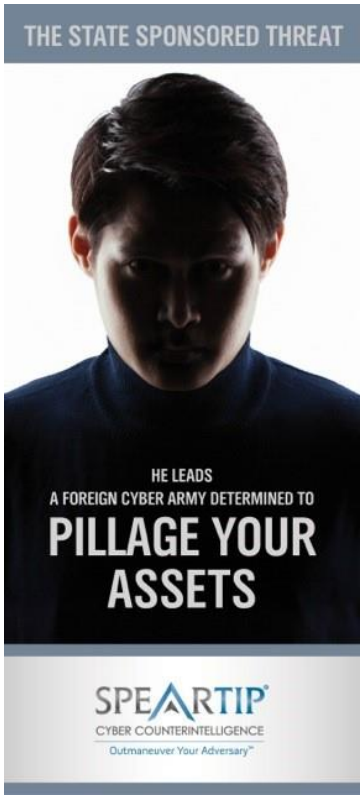
Q: What is a Cyber Hunt Team?

A: *A Cyber Hunt Team blends traditional counterintelligence techniques with new age, proprietary technical collection mediums to identify and exploit the adversary.*

The term "cyber counterintelligence" is often misused by cyber security organizations to dazzle audiences and clients, in hopes of legitimizing the marketing of overpriced rudimentary practices in human intelligence (HUMINT) collection on the Internet. Effective counterintelligence operations include the placement of defensive and offensive mechanisms to deter, detect, and counter an adversary. This collection occurs through various technical and non-technical means, and relies heavily on trained counterintelligence and HUMINT professionals for management.

Cyber counterintelligence activities seek to counter adversaries operating in cyberspace and cause those entities to act in observable or exploitable ways. A trained counterintelligence agent is generally not interested in neutralizing a target, initially. Proper counterintelligence collection is conducted in a cycle. A superior cyber hunt team will not only seek to identify the threat actor, but will also continually assess for tactics, techniques and procedures (TTP) of their clients' adversaries to more effectively wipe out the threat. Unlike some in this industry, an effective cyber hunt team, when identifying

an adversary TTP, would not reveal their findings to that adversary. Holding true to counterintelligence roots, the cyber hunt team should expend considerable effort into maintaining signatures for easy identification in future engagements, and to enable industry and government partners to enhance their operational capabilities.



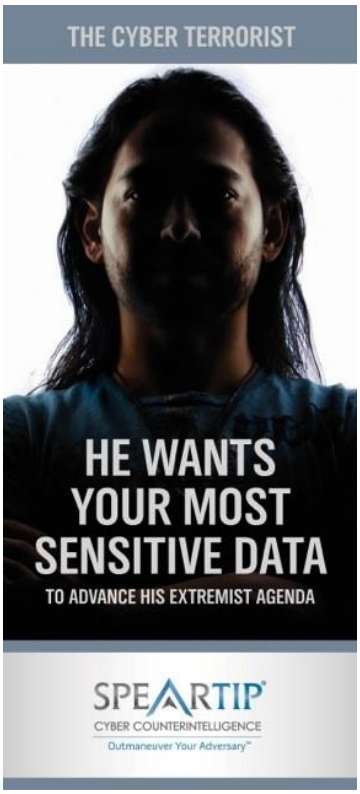
Counterintelligence operations are designed to be efficient in nature. Relying heavily on HUMINT collection techniques, validation can occur machine to human, or human to human. Experienced IT security professionals know the importance of human validation, understanding that machine to machine validation of network defense information has proved time and time again to cross-pollinate false positive and negative results. Focusing purely on the traditional layered security approach and passive security measures such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) is much costlier than a well-adapted counterintelligence capability.

Adapting to the various threats encountered in cyberspace is extremely difficult when dealing with very persistent and agile adversaries. Utilizing trained professionals to manage technology and adapt to the threat is a force multiplier and a proven cost-saving tool for organizations of all sizes.

Cyber Hunt Team Operations and Offensive Counterintelligence (OFCO)

The cyber landscape has experienced measurable change throughout the last decade. The adversary has evolved to the point where cyber-attacks five years ago would be considered rudimentary or script kiddie by today's hacking standards. Terminology has also evolved, and although the term "Cyber Hunt" has been around for years within government channels, the term is becoming more mainstream as yet another shiny marketing device in the cyber security practitioner's toolkit.

Cyber Hunt Team Operations should be viewed as a form of Offensive Counterintelligence (OFCO). Organizations and governments have managed OFCO for decades, using disinformation, double-agent operations, counterespionage, and technical countermeasures. Stopping short of hack-back operations to avoid violating any legal parameters, an experienced cyber hunt team should use OFCO methods for discovery and validation in proactive and reactive scenarios on behalf of their clients to ensure optimal results.



Cyber Hunt Team Operations should blend traditional counterintelligence techniques with new age, proprietary technical collection mediums to identify and exploit the adversary. In the age of bulk data flows and sophisticated DDoS, brute force, and advanced malware attacks, it is essential to maintain efficiency and the ability to root out a particular threat in any given scenario. Expert cyber hunt teams do not produce single-source reporting, or pull information from a silo. Instead, they utilize a mix of trained counterintelligence agents and some of the most cutting edge technology available, to ensure that their cyber hunt techniques are un-paralleled.

If you are in need of a cyber hunt team, make sure you choose a leader in identifying advanced, zero-day malware, and one that has helped countless clients recover assets, intellectual property, to win favorable judgements, and eradicate persistent threats.

About the Author: Josh Vander Veen, Director of Incident Response at SpearTip, is a former Special Agent, U.S. Army Counterintelligence, with over a dozen years of counterintelligence investigative and human intelligence (HUMINT) operations and collections experience. Specialized in counter-espionage activities, counterintelligence investigations, threat vulnerability assessments, and multi-discipline counterintelligence analysis. Additionally, Josh was selected to be a senior instructor at the U.S. Army's Joint Center of Excellence, where he instructed intelligence professionals in advanced source operations.