SANS
Security Operations
Summit & Training
New Orleans
SUMMIT: June 24-25 | TRAINING: June 26 - July 1
sans.org/SecOps

How to Disrupt an Advanced Cyber Adversary

Manny Castillo, FBI

Advanced Persistent Threat - NIST 800-39

An adversary that possesses **sophisticated levels of expertise** and significant **resources** which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) **pursues** its objectives **repeatedly over an extended period of time**; (ii) **adapts** to defenders' efforts to resist it; and (iii) **is determined** to maintain the level of interaction needed to execute its objectives.

Advanced Cyber Adversary

- Nation-State
- Organized Cyber Criminal Groups
- Cyber Mercenaries

NSA Chief Hacker

“If you really want to protect your network, you really have to know your network. You have to know the devices, the security technologies, and the things inside it. So why are we successful? We put the time in to know that network. We put the time in to know it better than the people who designed it and the people who are securing it. And that’s the bottom line”

“So another key point inside this, you know the technologies you intended to use in that network. We know the technologies that are actually in use in that network. Subtle difference.”

Rob Joyce
Chief of Tailored Access Operations (TAO)
National Security Agency
@ USENIX Enigma 2016

What Do We Need?

- Cyber Operational Awareness
- Network Visibility
- Special Procedures
- Defensive Mindset

CYBER OPERATIONAL AWARENESS

Cyber Operational Awareness could be defined as the perception of operational elements and events with respect to the cyber domain, the comprehension of their meaning, and the projection of their status after some variable has changed, or some other variable, such as a predetermined event.

CYBER OPERATIONAL AWARENESS

- Know and Understand your Network
- Cyber Hygiene
- Device Configuration

Know and Understand your Network

- Critical Security Controls
- Baseline
- Layer 7 Awareness

Cyber Hygiene

- Patching & Updates

Device Configuration

- Misconfiguration

NETWORK VISIBILITY

What does it mean for the cyber security team to have sufficient visibility into the enterprise to properly manage risk?

NETWORK VISIBILITY

Achieving this level of visibility requires leveraging the countless and different sources of data currently being tracked in their own networks and systems. All of this information must be meaningful, relevant and analyzed in real time.

NETWORK VISIBILITY

- Collection, Storage and Analysis
- Collect for Analysis
- Dynamic Sensor Placement

Collection, Storage and Analysis

- Log Retention Policy
- Data Sources
- Analysis of Data

Collect for Analysis

- Avoid Over Collecting Data
- Relevant and Meaningful Data

Dynamic Sensor Placement

- Dynamic relocation of sensor assets in order to collect in difficult places or enhance network visibility of critical assets.

SPECIAL PROCEDURES

- Everything in Cyber is a double-edge sword.
- Special Procedures are your operational TTPs in special conditions.

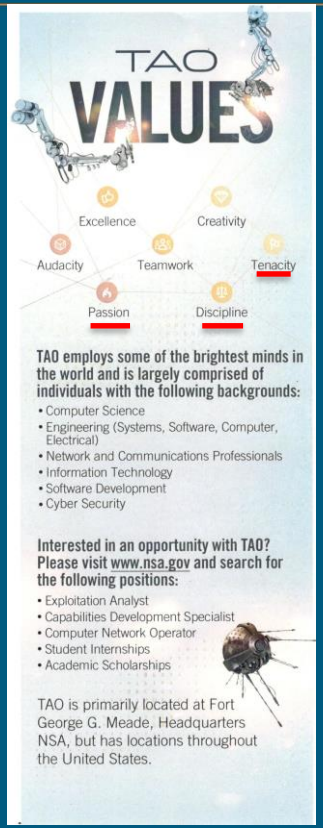
SPECIAL PROCEDURES

- Plan B Scenario
- Deception

DEFENSIVE MINDSET

- Mindset: Set of beliefs that adjusts our reactions and tendencies.
- Defensive Mindset: Takes proactive offensive and defensive measures with energetic focus to create and implement defensive measures due to the perceived awareness of danger.

OFFENSIVE MINDSET



DEFENSIVE MINDSET

- Holistic Mindset
- Resilient Mindset
- Warrior Mindset

HOLISTIC MINDSET

Dialectical reasoning and involves understanding a system by sensing its large-scale patterns and reacting to them.

RESILIENT MINDSET

Psychological resilience is the ability to cope with a crisis or to return to pre-crisis status quickly. Resilience exists when the person uses "mental processes and behaviors in promoting personal assets and protecting self from the potential negative effects of stressors"

WARRIOR MINDSET

“ *Warrior Mindset* is more than aggressiveness and determination, it is about over coming challenge and adversity. It’s about possessing, understanding, and being able to utilize a set of psychological and physical skills that allow someone to be effective, adaptive, and persistent. It also allows someone to use optimal decision-making, psychological techniques, physical and tactical skills learned in training and by experience”.

Harvok Journal

WARRIOR MINDSET

Being able to overcome challenging and adverse defensive situations in the cyber domain with determination. It's about possessing, understanding, and being able to utilize a combination of cyber skills that would allow you to be effective, adaptive, and persistent. Allows the mind to use optimal decision-making under stress using techniques learned in training and by experience.

CONCLUSION

- Cyber Operational Awareness
- Network Visibility
- Special Procedures
- Defensive Mindset

Questions?