ACNO Skill 12: Malware Analysis & Reverse Engineering

Knowledge of:

- Relevant Operating Systems.
- Current trends in attack vectors & targeted applications / protocols / services.
- Malware bootstraping, persistance, communication protocols and propagation techniques.
- Exploitation techniques (stack & heap overflows, XSS, SQL Injection, etc).
- Personal Security Products (Anti-Virus, HIDS, etc).
- Public and 5-eyes malware analysis tools.
- File formats and content verification tools.
- Anti-SRE, anti-debugging & anti-emulation techniques.

Ability to:

- Identify malicious code.
- Analyse and understand captured malware.
- Identify and construct signatures & heuristics for detection.
- Reverse engineer malware.
- Use IDA Pro to statically uncover and annotate functionality.
- Determine sophistication level of malware.
- Apply malware discovery tools and techniques.
- Develop malware discovery & analysis tools.
- Provide mitigation advice.

Level 0
Understands basic concept of malware identification and analysis but does not yet have the breadth of knowledge needed to apply this skill in an operational context. Has basic understanding of attack vectors and impact of an infection.

Level 1
Has knowledge of open-source and commercial SRE tools and techniques. Can determine basic functionality of malware using these tools, but requires technical guidance to go further.

Level 2
Has detailed knowledge of internal and 5-eyes analysis tools, and how they operate. Works unsupervised to high-level task definitions. Develops discovery and analysis tools to enhance capability. Can determine main functionality of malware through static analysis (i.e. SRE).

Level 3
Provides technical direction and guidance to colleagues. Considered a known point of reference in the field. Contributes to key architectural design decisions when developing new capability. Displays advanced SRE skills, and uses experience to provide accurate sophistication & impact assessments.

Level 4
Considered an expert in the field of malware analysis, and a point of reference throughout the intelligence community and possibly industry. Consistently delivers, and leads the development of groundbreaking capability. Speaks at conferences and

delivers specialised training in the field. Has a wealth of experience relating to malware trends & evolving techniques.