CERIAS
The Center for Education and Research in Information Assurance and Security

Using Link Analysis to Improve Advanced Persistent Threat Intelligence and Detection

Capt. Corey T. Holzer, USA

MOTIVATION, PROBLEM STATEMENT, & INTENDED GOAL

Over the past decade, the Advanced Persistent Threat (APT) has risen to forefront of cybersecurity threats. APTs are a major contributor to the billions of dollars lost by corporations around the world annually. The threat is significant enough that the *Navy Cyber Power 2020* plan identified them as a “must mitigate” threat in order to ensure the security of its warfighting network. However, the manner in which these threats operate makes them difficult to detect.

The goal of the current research is to use open source intelligence pertaining to known APTs to establish an APT ontology and then employ the ontology and link analysis with the goal of increasing the amount of intelligence about individual APTs as aggregated from the whole knowledge base.

WHAT IS AN APT?

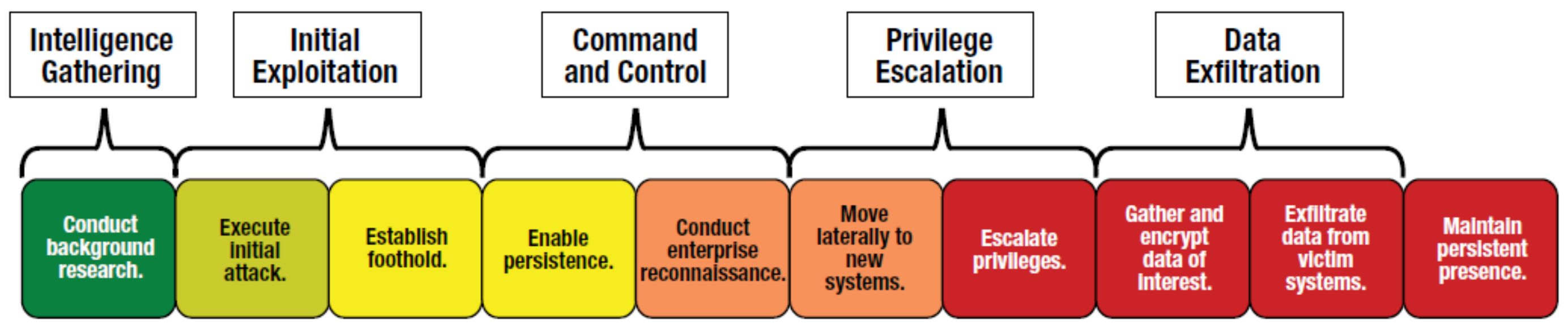
The term originated in 2006 when the United States Air Force coined the phrase as an unclassified moniker (Ask et al., 2013).

APTs are well organized groups with the ability to systematically bypass “best practice” defense-in-depth cyber security measures (Cole, 2013; Dambella, 2010).

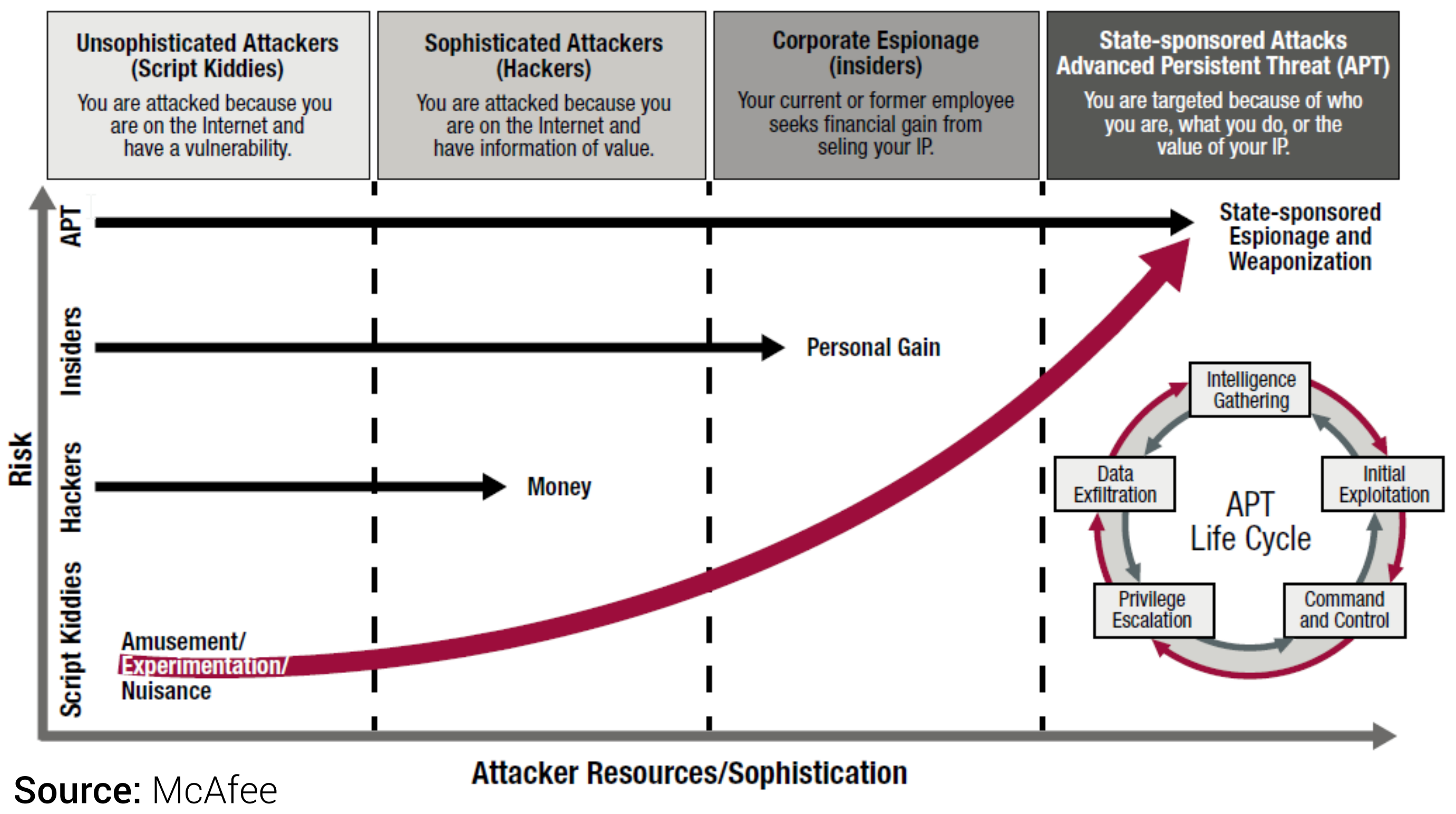
They can infiltrate a network and remain hidden while monitoring it for a specific target or data to exfiltrate (Bodeau D., Graubart, Heinbockel, & Laderman, 2014).

Their goal is stealthy or low and slow execution instead of the kind of attack that draws attention to the person or persons committing the crime.

Dr. Eric Cole compared APTs to sophisticated shoplifters who can enter a store and are indistinguishable from legitimate shoppers; thus, they are harder to detect and harder to prevent (Cole, 2013).


Intelligence Gathering
Initial Exploitation
Command and Control
Privilege Escalation
Data Exfiltration
Conduct background research.
Execute initial attack.
Establish foothold.
Enable persistence.
Conduct enterprise reconnaissance.
Move laterally to new systems.
Escalate privileges.
Gather and encrypt data of interest.
Exfiltrate data from victim systems.
Maintain persistent presence.

Source: Intel Security


Unsophisticated Attackers (Script Kiddies)
You are attacked because you are on the Internet and have a vulnerability.
Sophisticated Attackers (Hackers)
You are attacked because you are on the Internet and have information of value.
Corporate Espionage (insiders)
Your current or former employee seeks financial gain from seling your IP.
State-sponsored Attacks Advanced Persistent Threat (APT)
You are targeted because of who you are, what you do, or the value of your IP.
Risk
APT
Insiders
Hackers
Script Kiddies
State-sponsored Espionage and Weaponization
Personal Gain
Money
Amusement/ Experimentation/ Nuisance
Intelligence Gathering
Initial Exploitation
Command and Control
Privilege Escalation
Data Exfiltration
APT Life Cycle
Attacker Resources/Sophistication

Source: McAfee

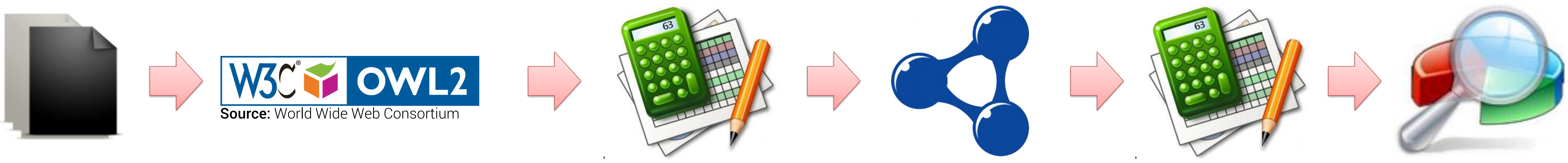
HYPOTHESES

Null Hypothesis (H_0): Link analysis will provide the same amount of intelligence about APTs as what is currently available.

Alternate Hypothesis (H_a): Link analysis will improve the intelligence about APTs as what is currently available.

METHODOLOGY

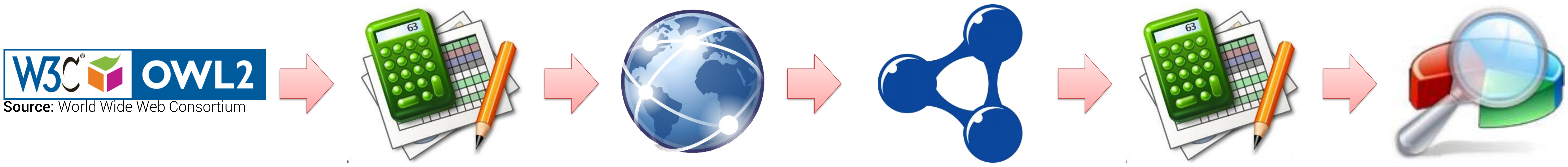
FIRST ITERATION



Source: World Wide Web Consortium

Collect Open Source Intelligence (OSINT) → **Build an Ontology using W3C’s OWL** → **Establish a Scorecard and Calculate Baselines for each APT** → **Perform Link Analysis On Baseline Data** → **Recalculate Scores for each APT** → **Analyze and Report**

SECOND ITERATION



Source: World Wide Web Consortium

Update Ontology (if applicable) → **Recalculate Scores for each APT (if applicable)** → **Use Ontology to search WWW** → **Perform Link Analysis On Data** → **Recalculate Scores for each APT** → **Analyze and Report**

CERIAS
PURDUE UNIVERSITY