RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: SPO-W08B

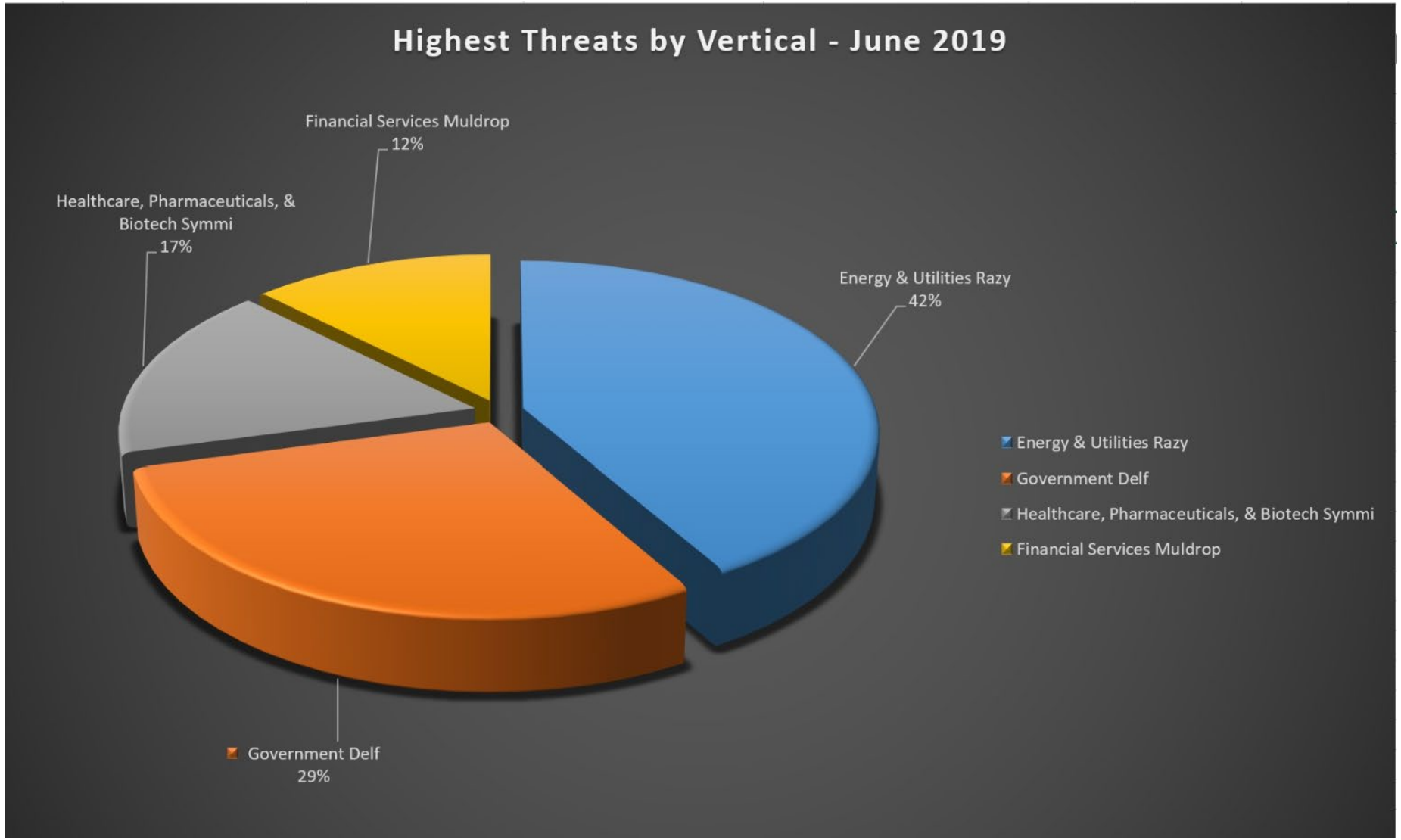
The Year of Digital Guerrilla Warfare

Tom Kellermann, CISM

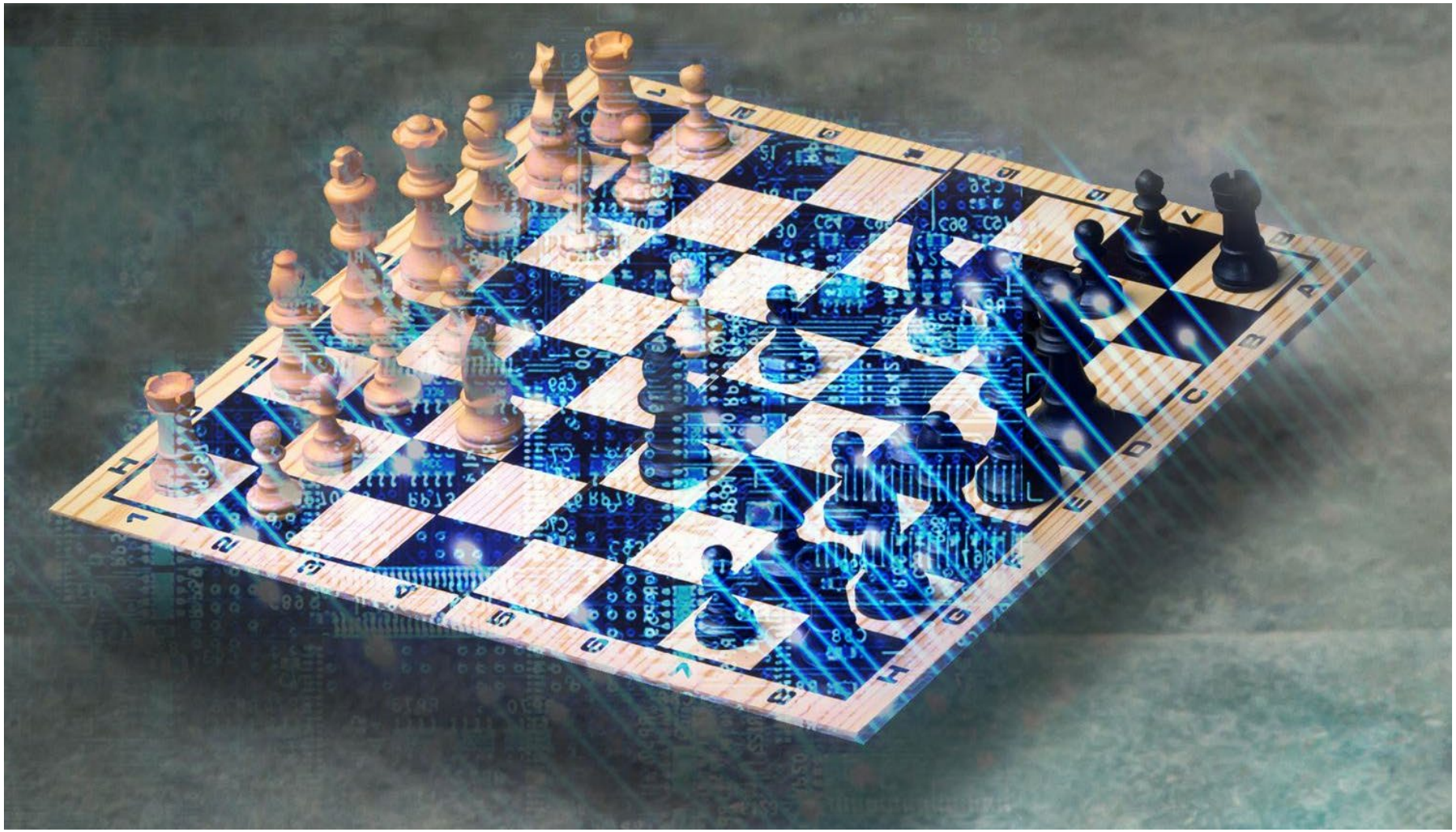
Chief Cybersecurity Officer
Carbon Black
@takellermann

Multiplicity of Threat Actors Creates a Free-fire Zone

Most Prevalent Threats Per Vertical



The Incident Response Threat Report: Offense Informs Defense



Island Hopping Occurs 51% of the Time

Hackers Move Laterally 70% of the Time

Secondary C2 on a Sleep Cycle is Employed 40% of the Time

Living Off the Land

Steganography is Flourishing

56% Observed Counter-Incident Response

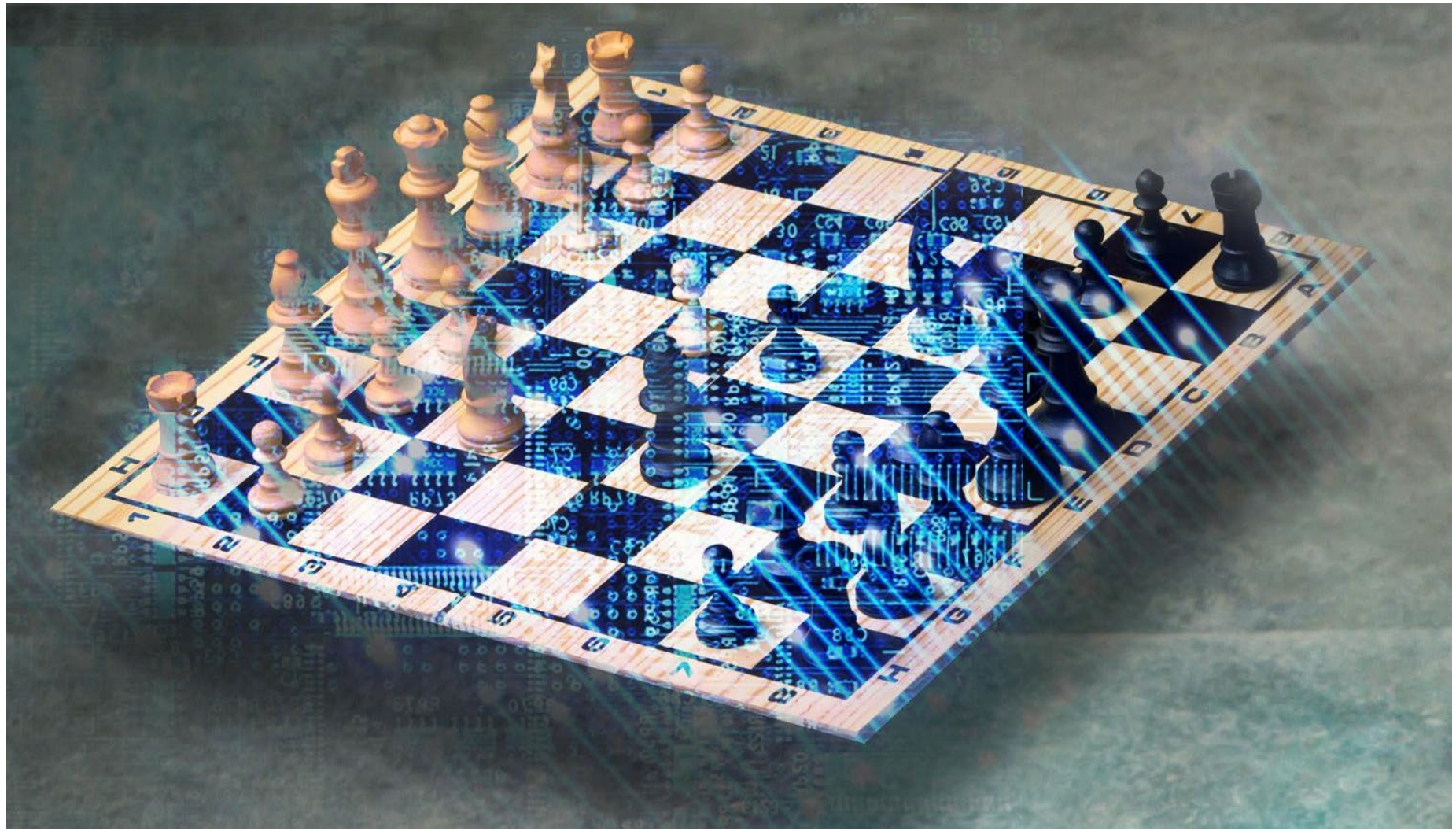
28% of the Time IoT Used as an Attack Vector

31% Experienced Destructive Attacks

Future Attack Trends

1. Destructive Attacks
2. Island Hopping via Cloud
3. OT Attacks
4. Vapor Worms
5. Increase of Watering Hole Attacks

Cognitions of a Cybercriminal

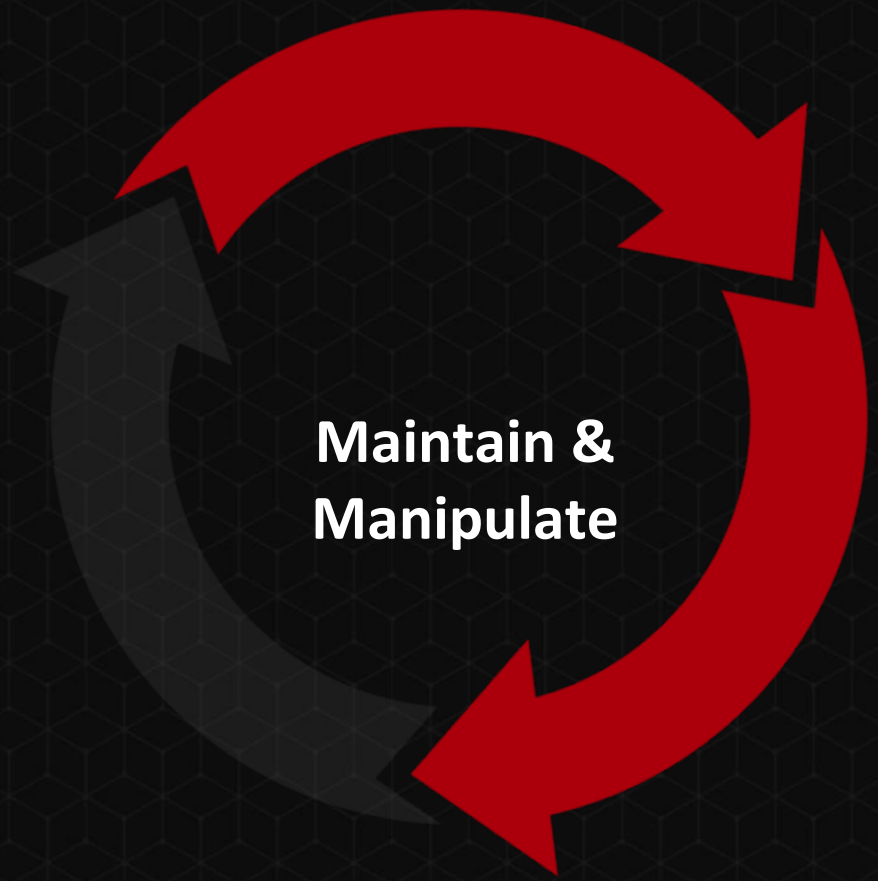


Cognitive Attack Loop

Carbon Black.

- Gather Intel
- Exploitation
- Social Engineering
- Delivery

Carbon Black.



- Execution
- Privilege
- Persistence
- Evasion
- Communication

Carbon Black.

- Capture
- Exfiltration
- Destruction
- Disinformation

Carbon Black.

Intrusion Suppression: A Proactive Cybersecurity Architecture

CB LiveOps

CB Response / CB Threat Hunter

CB Defense

CB Protection

RSAConference2019
Asia Pacific & Japan

The Year of Digital Guerrilla Warfare

Tom Kellermann, Chief Cybersecurity Officer, Carbon Black