Information Security as Counterintelligence

Nick Levay
nick@nicklevay.net
@rattle1337

About Nick

- Past Roles
  - Chief Security Officer, Bit9+CarbonBlack (Boston)
  - Director, Information Security and Operations, Center for American Progress (DC)
  - Director, Global Systems and Tools Engineering, iAsiaWorks (SF/HKG)
  - . . . lots of consulting (NJ, NYC, TN, ATL, SF, LA, et cetera..)
- Practicing professionally since 1997
- Certified Information Systems Security Professional
- Educational background in Communications (Not CS/LEO! Weird right?)
- Areas of Focus
  - Information Warfare
  - Cyber Counterintelligence
  - Security Operations

Agenda

- BLUF: A (quick and informal) case study of battling nation-state actors
- Information Security program maturity levels
- Things you should study
- A bit about espionage threat actors
- Examples of attacks
- Q&A (if possible, wouldn't that be cool..)

Information Security Program Maturity

- **Immature**
  - No formal Information Security program
  - Security as a function of Information Technology
- **Progressive**
  - Information Security as an independent function with FTEs
  - Operational SOC (Security Operations Center)
  - Pentesting and Red Team engagements
- **Adaptive**
  - Open-ended bounty based Red Teaming
  - Active Defense (Constant hunting and trap laying)
  - Intelligence Driven Defense
  - Counterintelligence Pratice

Study Topics

- Conti/Raymond/Cross “Library of Sparta” talk/paper
- Operation SMN Axiom report
- Lockheed Cyber Kill Chain™
- OODA Loop
- Intelligence Loss/Gain Analysis
- Deception Tactics
- Transactional Analysis
- Foreign and Public Policy related to your business

(Just Google for links!)

The Advanced Persistent Threat

- The APT is NOT:
  - A “what” = type of threat
  - A botnet
  - Directly financially motivated
- The APT is:
  - A “who” = A Threat Group
    - Term coined by Air Force in 2006(?)
  - Foreign Espionage!
  - Extremely Organized
    - Multiple groups
    - Division of labor by function

Advanced

- Works full spectrum of computer intrusion
- Uses pedestrian publicly available exploits
  - … but can elevate to use 0day
- Adjusts tactics based on target's posture

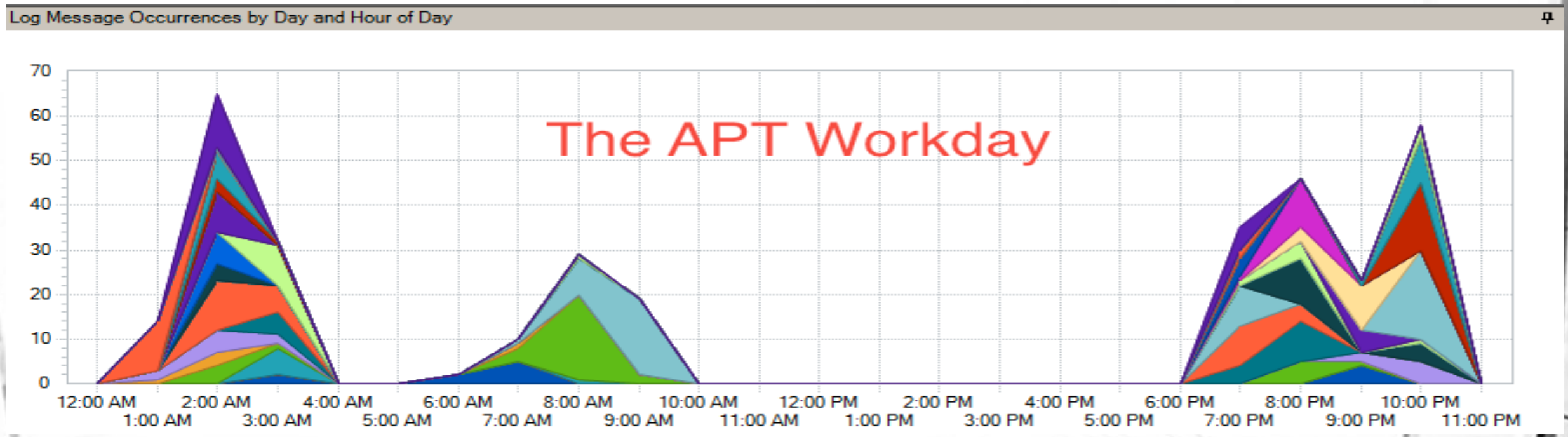
They do what's necessary to get the job done.

Persistent

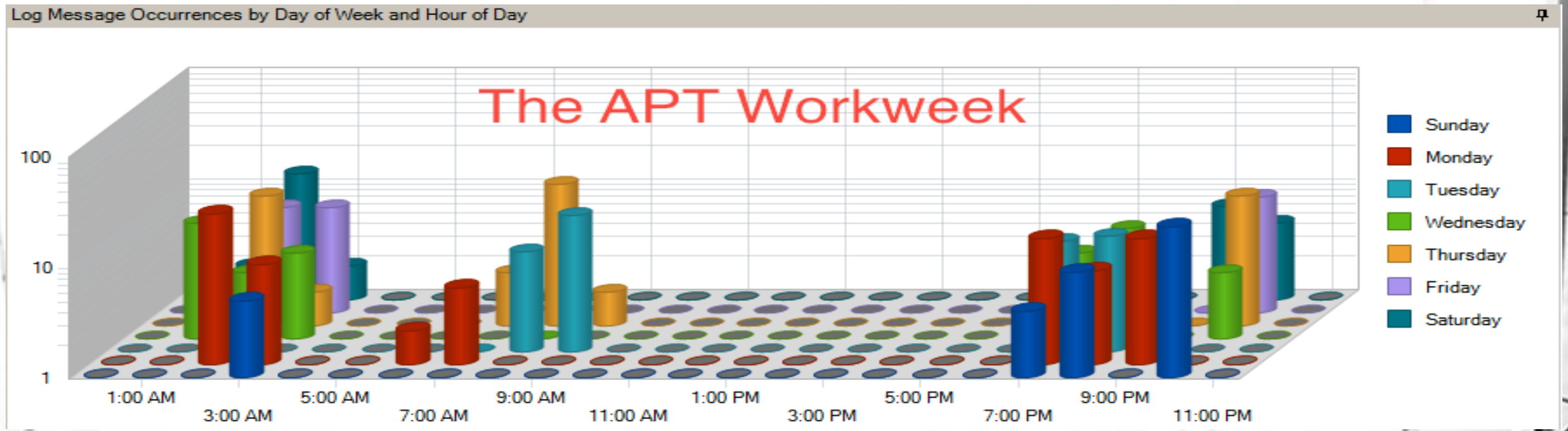
- Formally tasked to accomplish a mission
  - … not opportunistic intruders
- Works like an intelligence unit
  - … receives directives, delivers intelligence product
- Does not mean constant activity in target network
  - … maintains level of activity necessary for objectives

They don’t give up.

APT Exfiltration Team Activity



APT Exfiltration Team Activity



Threat

- Adversary is not a mindless piece of code
- Adversary is organized, funded, and motivated
- Consists of multiple “groups” with dedicated “crews”

“As an intelligence professional, I stand back in absolute awe and wonderment at the Chinese espionage effort against the United States of America. It is magnificent in its breath, its depth and its efficiency.”

- Gen. Michael Hayden

Spearphishing Examples

Circa 2010

(Chatham House Rule please..)

EXAMPLES [REDACTED]

(sorry)

Nick Levay
nick@nicklevay.net
@rattle1337

Questions?

Nick Levay
nick@nicklevay.net
@rattle1337

Thank You!