Understanding and Responding to the Advancing Cyber Threat

Greg Rattray

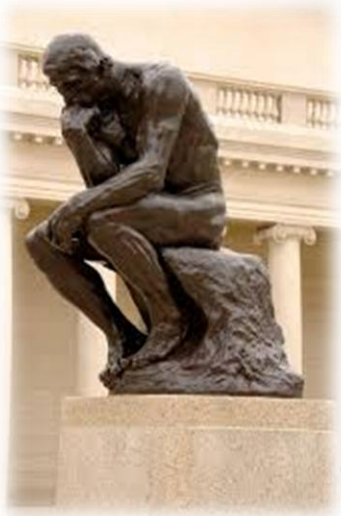
CEO, Delta Risk LLC

28 June 2013

Today's Talk

Walk though History

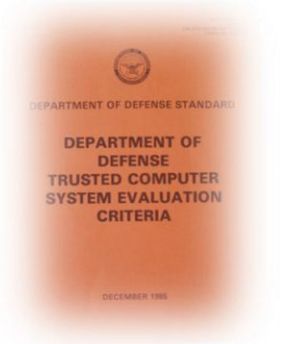
Understanding the Advanced Threat



What Does it Mean for Cyber Defense?

Before the Internet

Orange Book



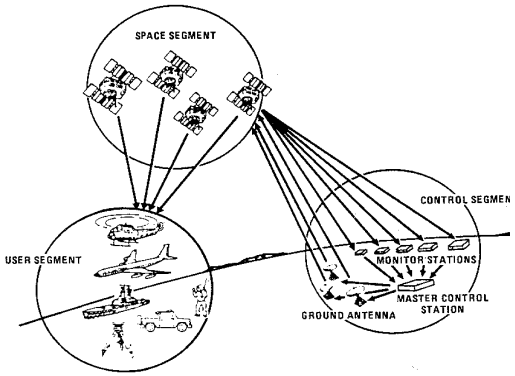
Espionage as a Constant

Cold War

Intercept

Technology

Public Switched Telephone Network



Phreaking

Cyber Threat Intelligence

- Know Adversaries Signals Intelligence Capabilities
- Little in Private Sector

DELTARISK
Cyber Security | Business Resiliency | Risk Management

Entering the Internet Age – late '80s-'90s

First Gulf War

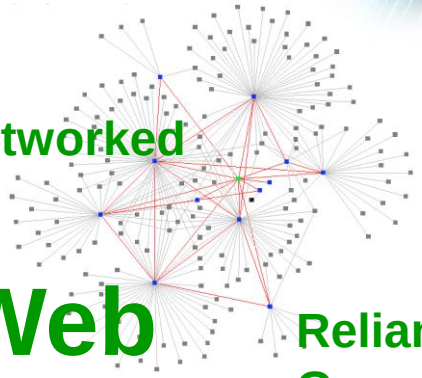
Morris Worm

Computers at Risk

Cyber Threat Intelligence

- Hunting Hackers
- Worry about National Security Impact

Info War



Networked

Web

Reliance Growing

Clinton Presidential Commission

DELTARISK
Cyber Security | Business Resiliency | Risk Management

Wake Up Calls – Early 2000's

Slammer

Nimda

Code Red

Solar Sunrise

Moonlight Maze

2000 E-Commerce Attacks

amazon

ebay

Cyber Threat Intelligence

Dedicated Intelligence Organizations

Attribution Difficult

Rise of CERTs

Patriotic Hacking

Rise of E-commerce

A Dark Age - 2001-2007

9/11

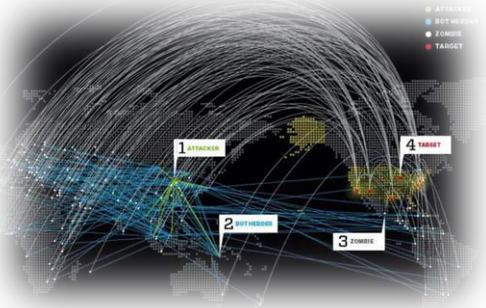
Iraq

Afghanistan

GWOT

Byzantine Hades

Botnets



Internet Underground

Global Crossing

Internet Bubble Bursts

Reliance Still Grows

Cyber Threat Intelligence

Supply Chain Risks

Little on Adversary Capabilities

Exposures of Espionage

Renewed Attention - 2007-2011

Advanced Persistent Threats

Estonia

Georgia

Korea

Ghost Net

RBN

Technology

Control Systems on Internet

Night Dragon

Cyber Threat Intelligence

Start Real Focus

Attribution Progress

Rise of Private Teams – Providers and Collaboratives

Rising Fear – Present Day

STUXNET

Flame

Cyber Threat Intelligence

Shamoon

Dire Estimates; Need Method

Info Sharing

APT 1

Technology

Mobility

Social Media

Cloud

DDoS vs. Banks

DELTARISK
CYBER SECURITY | BUSINESS RESILIENCY | RISK MANAGEMENT

Rise of the Advanced Persistent Threat

- Top tier national security issue
  - **US President declared a national security and economic challenge**
  - **Major part of relations with China**
  - US DOD assumes it is **unstoppable** – goal is to manage risk/mitigate
  - Working to collaborate with private sector

- Corporate risk varies widely
  - Intellectual property and competitive information gathering
  - Groups target sectors and look for weakest actors
  - Sophisticated responses exist but rare

What is an Advanced Persistent Threat?

- Adversaries employ advanced tools and techniques, integrated into sophisticated campaigns
- Often combine multiple methods, tools and techniques in order to reach and compromise a target and to maintain access

- Adversaries are focused on long-term, and aim to establish and maintain a foothold in the organization
- Invest in data and intelligence gathering
- Build infrastructure for long term use
- 'Low and slow' approach

Advanced Persistent Threat

APT adversaries have both capability and intent, are skilled, organized and well funded. Attacks are executed by coordinated human action, with specific objectives

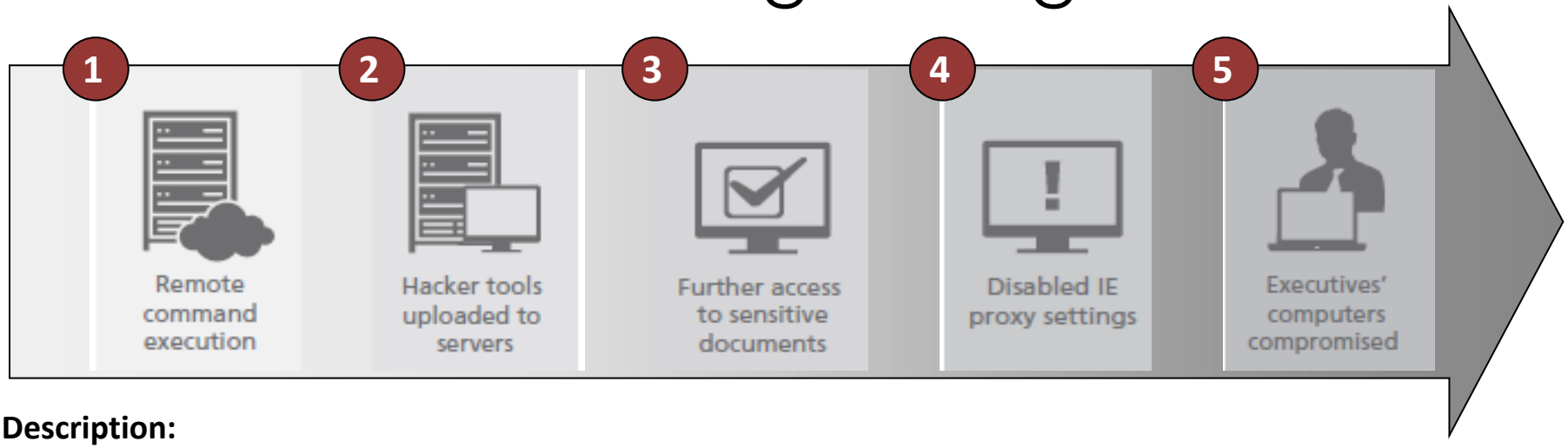
Risks	Typical adversaries
Loss of reputation	Competitors, Hacktivists
Loss of competitive advantage — Theft of ID — Compromise negotiations	State sponsored and commercial espionage
Profit from insider information	Organized crime
Degrade ability to operate	Competitors, State sponsored entities

Night Dragon Attacks - Overview

- In 2010, McAfee uncovered a series of coordinated, covert attacks targeting oil, energy and petrochemical companies
  - These attacks targeted financial documents related to oil and gas field exploration and bid negotiations, as well as operational details
  - Touched companies, individuals and executives in Kazakhstan, Taiwan, Greece and the United States
- Dubbed Night Dragon, the attacks demonstrate how an APT may operate, and highlight specific considerations in defending against them

SOURCE: McAfee

Breakdown of a Night Dragon Attack



Description:

1	2	3	4	5
▪ **Extranet web servers compromised** ▪ Set up remote command and control	▪ Basic **hacker tools uploaded to servers** ▪ Gained access to sensitive internal servers	▪ **Password cracking attacks** ▪ Accessed additional usernames and passwords	▪ Enabled direct communication from infected Machine to internet	▪ Exfiltrated sensitive documents and emails

Vulnerabilities:

1	2	3	4	5
▪ Vulnerable exterior applications and users	▪ Unverified trust relationships with extranet servers	▪ Vulnerable users and no policy enforcement	▪ Systems not monitored for alterations	▪ No data loss prevention capabilities

SOURCE: McAfee

Could the impact of these attacks been limited?

Intelligence and information sharing

- Nothing new here: Gh0st, modified hacker tools, SQL injection, spear phishing, etc.
- Know the indicators of the adversary tactics, techniques and procedures

Use your own network to find adversary

- Lots of data had the signs buried within: host files/registry keys, AV alerts, network data, etc.

Focus on defense of key assets

- Executive systems and the data contained therein was the target
- Password complexity audits for executives and users

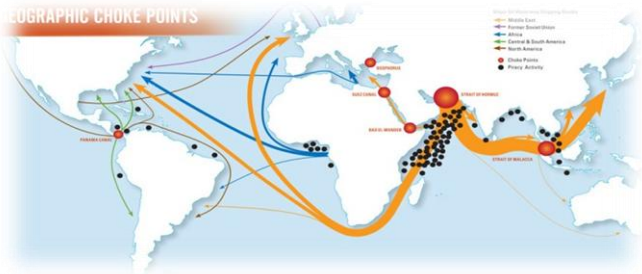
Advanced Cyber Defense

Castle Walls Eroded
Enemy Inside Gates

Know Your Attacker > Must Manage Risk

"If you know the enemy and know yourself you need not fear the results of a hundred battles"

Channel the Attacks

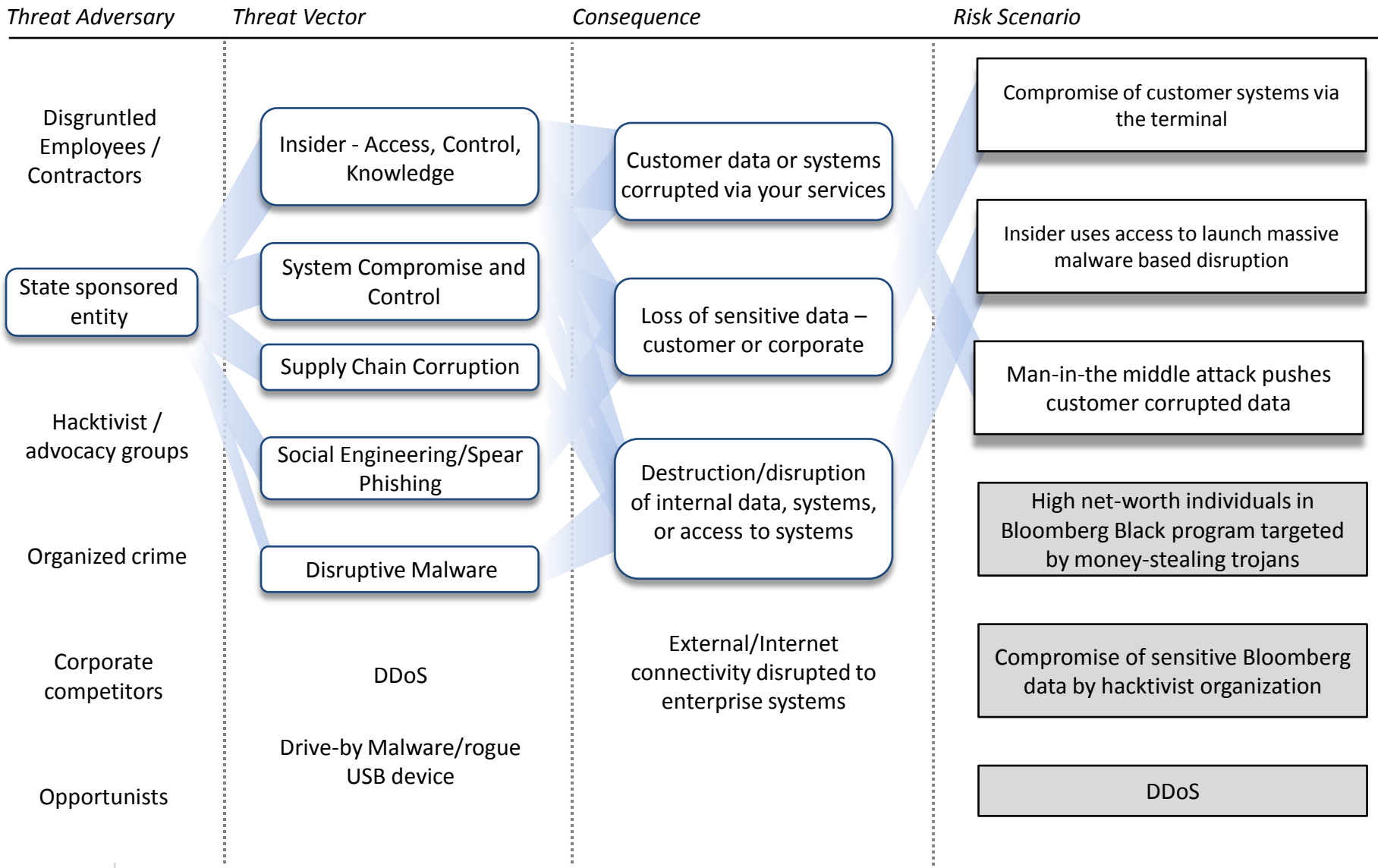


Build Your Team

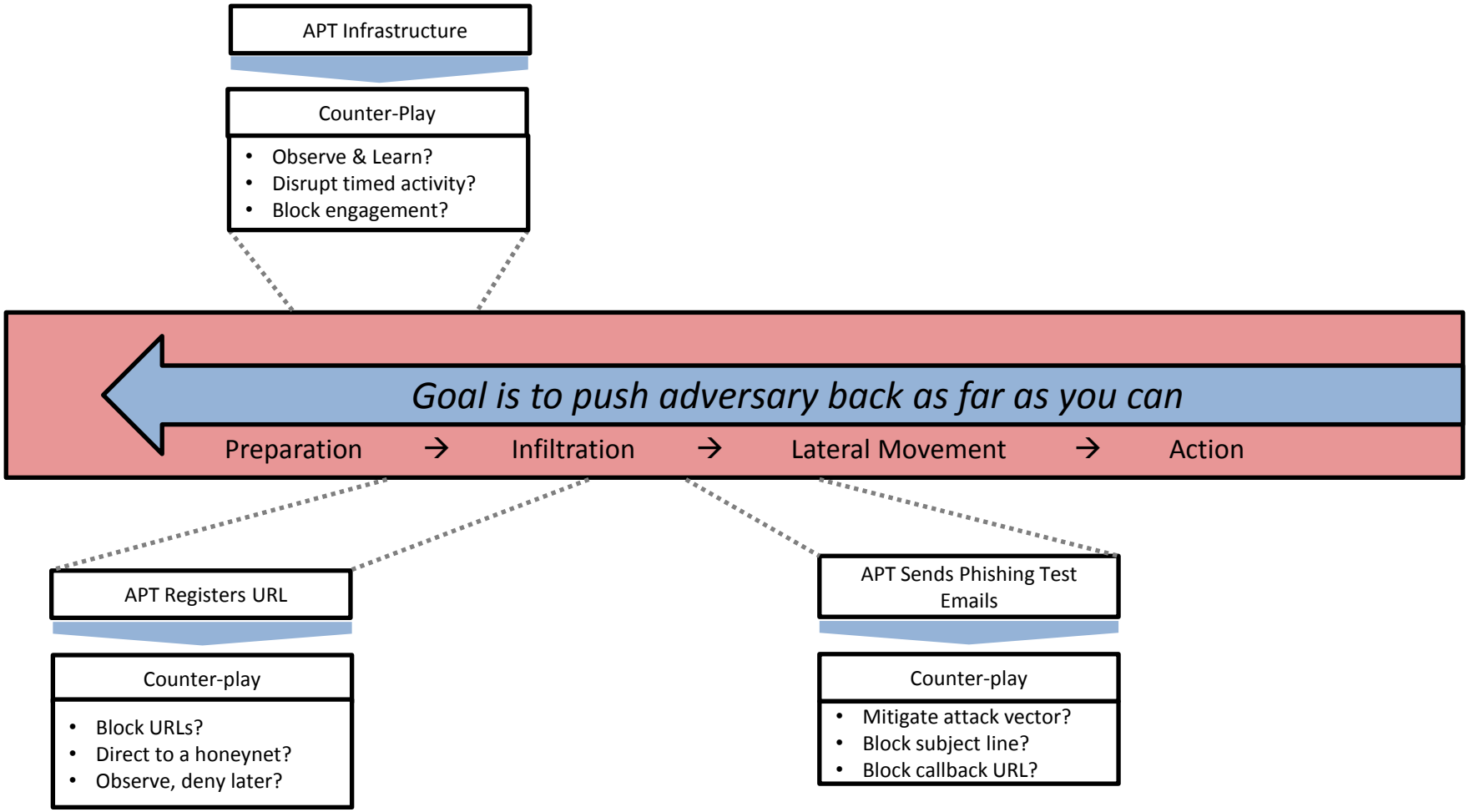
Cyber Threat Spectrum

Risk to Company	Potential adversary	Description & Intent	Example
High	Disgruntled Employees/ Contractor Access	Individuals or smail groups trying to damage the company/make money	2013 Matthew Keys (Thomson Reuters) 2010 Bank of America 2009 Melbourne Harbor sewage dumping
High	State sponsored entity	Well resourced, operational teams with goals to damage competitor interests/impact critical infrastructure operations/track dissidents	On-going oil & gas sector (bids and knowledge in hands of China) On-going banks services degraded by Iranian denial of service
Med.	Hacktivist/ advocacy groups	Decentralized group that targets sectors of interest to disrupt productivity and cause reputational damage or advance specific causes through information gathering	2011 HBGary (60,000 emails posted on line) 2012 DDOS vs NASDAQ, CIA, UFC; 500K cards online
Med.	Organized crime	Independent or collective hackers that collect information that can be sold for a profit or used directly for fraud and extortion; may be for hire for non-state actors	2011 Fidelity Info Service (FIS) $13M loss 2013 Eastern European criminals conduct insider trading
Low	Corporate competitors	Other corporate entities that want to understand inner workings of others or steal intellectual property for internal use	2008 Starwood sues Hilton $75M in damages
Low	Opportunists	Unaffiliated hackers (usually young) looking for bragging rights and hacker community recognitions, and may target information could be of value to sell or use	2000 e-commerce disruptions 2001 hacker access to Worldcom

Mapping Threat/Vector/Consequence to Risk



Actively Countering Advanced Threats

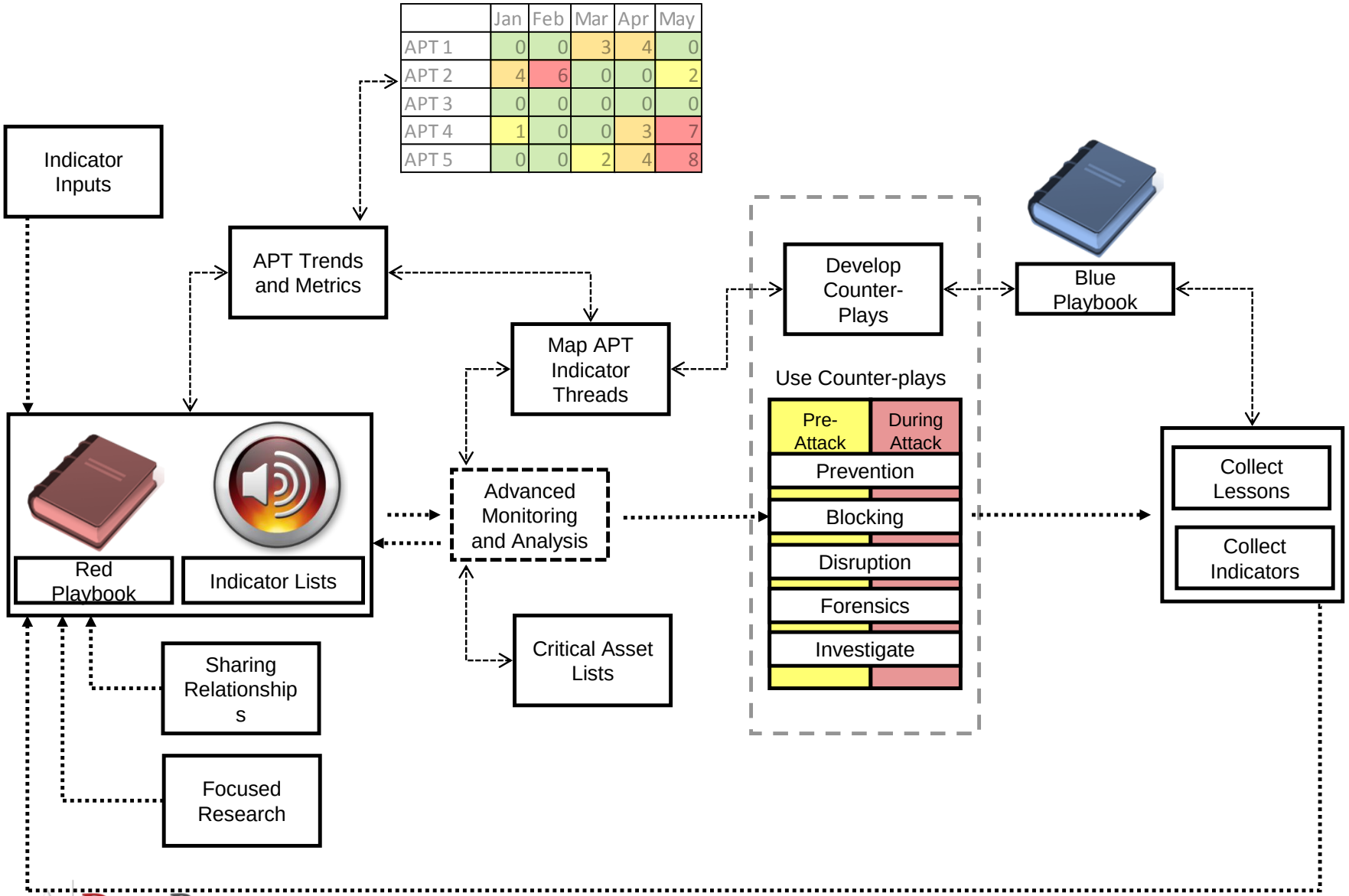


Foundation - Track Your Adversary

- Systems are scattered around world
- Makes attribution difficult
- Might be in legitimate businesses
- Confuses incident responders

Purpose	What is Observable?
Research System • Google searches • Open-source info	• If this system comes from a range of known targeted systems, you might be able to get indicators from your webserver logs
Email System • Gmail account access • Launch phishing	• Email addresses of a certain type • Lists of organization personnel • Info from possible “test runs”
Tool Repository • Use for enumeration • Enable lateral movement	• Possible known IP range • Possible DNS registration
Infection Site • Droppers grab malware stored here	• DNS registration for the site • URL hard-coded in phishing emails
Command/Control • Malware contacts this server for instructions	• DNS registration for the site • Server might be recycled from previous attack on a partner • URL hard-coded in malware
	• DNS registration for the site • Server might be recycled from previous attack on a partner

Approach One – On-Going Action to Disrupt Adversary



Approach Two – Protect Key Corporate Players and Events

Board begins M&A event

Guidance:
- Scope: Tight control
- Timeframe: 4 weeks
- Criticality: High

c-APT Team

Team reviews the playbook

Prepare ACL Member Systems
- AV/Patch Compliance
- Zero-day Mitigation
- System Hardening

Advanced Monitoring of ACL Members
- Spearphish Monitoring
- Bandwidth Anomalies
- Netflow from ACL IP's
- APT Indicators

Critical Document Identification

Intelligence

Monitor Data Leakage

Launch

Campaign Timeframe

DLP Technology Implementation

Access Control Methods

Identify members needing document access | Dev ACL

Successful Adversary Theft | Launch Dynamic Options
- Destroy stolen copies
- Mitigate the loss

Misdirection

Public Announcement

Investing in the Human

- People **to analyze** intelligence -humans are better at pattern recognition
- People **to decide** on how to handle an APT
- People **to test** new indicators and conduct forensics in a lab
- People **to build trust** and participate in sharing forums

People and skills are most sustainable, agile asset

What to do on your own or with help?

Parting Thoughts

- Technology Drives Risks

- Take a Global Perspective

- Collaboration

- Learning