Deloitte.

Advanced Persistent Marketing

Demystifying Advanced Persistent Threats and Cyber Espionage


Official Professional Services Sponsor

About the presenter

Lance James

Head of Cyber Intelligence, Deloitte & Touche LLP

- Author of "Phishing Exposed" and co-author of "Emerging Threat Analysis"
- Advisory board member of the Digital PhishNet
- Centre for Strategic Cyberspace + Security Science (CSCSS.org), creator of InvisibleNet (IIP/I2P)
- Co-Founder of Secure Science Corporation
- Loves Karaoke
- Very Hyper (but quiet in the evenings)

Life-Like Drawing

Lance has more than a decade of experience in programming, network security, digital forensics, malware research, cryptography design & cryptanalysis, attacking protocols, and deep experience in information security, and has provided consultation to small start-ups, national and international governments, and Fortune 500 companies, including top American financial institutions.

Digital 007

- Are we really surprised?
  - The game has never changed just the environment
  - Dossiers of yesterday are your databases today
- Fourth Generation Warfare Theory (asymmetric)
  - Terrorism, insurgencies
  - Decentralized
  - Opportunistic
  - Psychological and guerilla tactics
  - Survival and influence - typical goal
    - Affects the cost of warfare
    - Belief vs. duty

Adversaries

- Nation-State
  - Drivers such as economic, political, war, belief, revenge
- Corporate
  - Intellectual property theft
    - Is it that common?
    - Mostly insider threats
    - Risk of Incarceration (ROI)
- Insurgencies
  - Non-state sponsored
  - Pro-state or rebels
  - Cyber paramilitary factions
    - Electronic armies

Wild Wild Web

- Increasingly hostile Internet
  - Conflicts are no longer physically separated
  - Distributed Denial of Service (DDoS), swatting, phishing/malware, turf wars, espionage
  - Global unrest means Internet unrest
- Problems solved
  - Phishing?
  - Malware?
  - Espionage?
  - DDoS?
- And now add anonymity
  - Tor, I2P, Bitcoin, Virtual Private Network (VPN) proxies
  - Silk Road, CryptoLocker, TorLocker, Dyre, CryptoWall

Rethinking information security

- InfoSec castle defense methodology
  - Armor up and await attacks
  - Shiny boxes with blinking lights
    - Is this a technology problem?
    - Is this a cost problem?

- Security monitoring
  - One team to monitor all
    - Cognitive overload
    - Total Cost of Ownership is not lowered
  - Threat feed correlations
    - Many organizations are not ready for threat intelligence
    - Threat feeds ≠ threat intelligence

Awareness exercises

- Example
  - Intelligence comes out on the wire
    - An electronic army group hacks a celebrity social media account
- What is your first question? Usually –
  - Who did it? Why?
  - What tools, tactics, procedures (TTPs)?
  - What is the impact?
- What about this question?
  - What was the target's timeline?
  - What provoked the attacker?
- What do we learn?
  - Adversaries habits
    - Media, motives and maneuvers

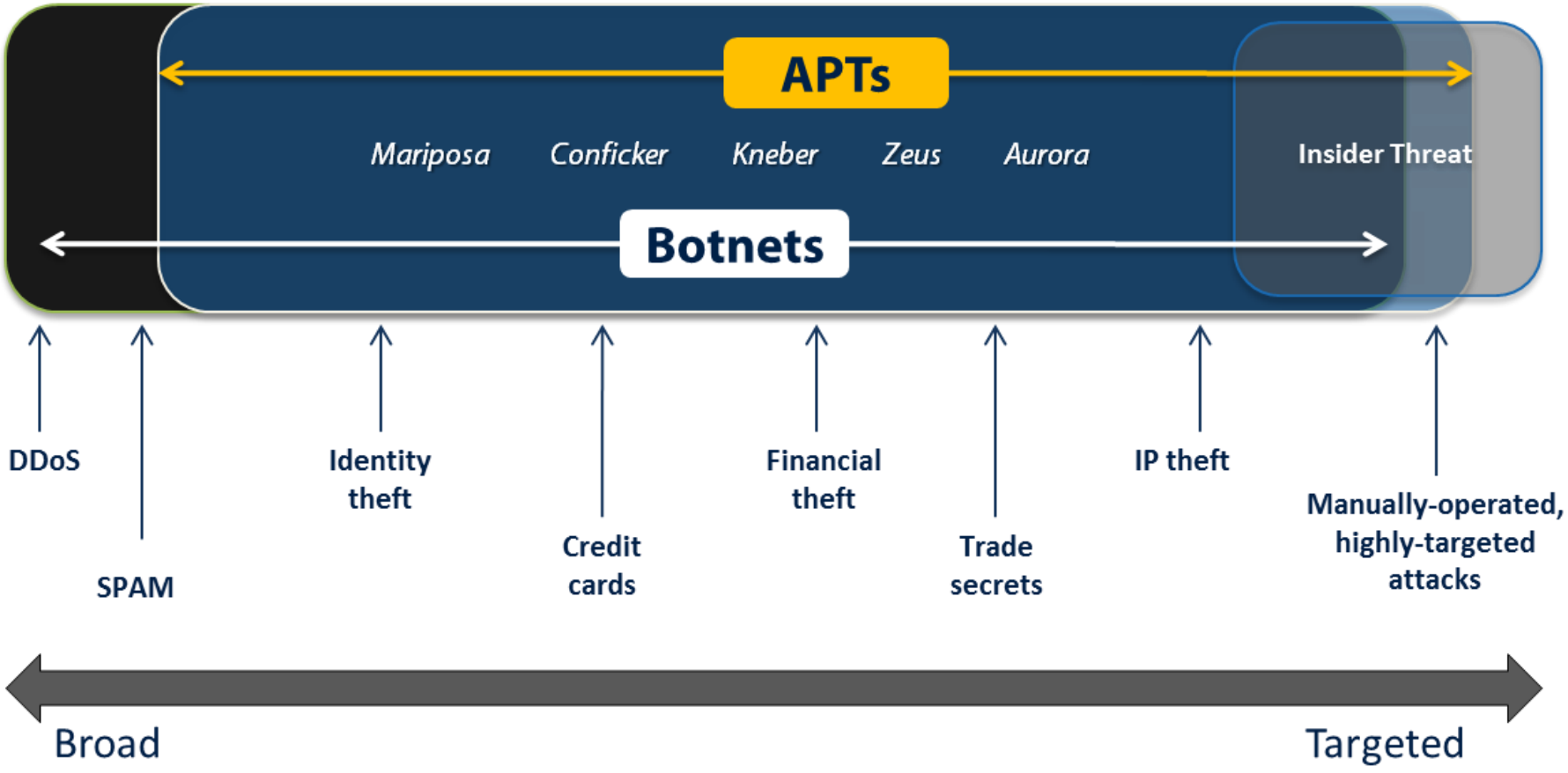
Counterintelligence

- Spy vs. spy
  - Espionage countermeasure is counterintelligence
  - Insurgency countermeasure is counterinsurgency
  - Terrorism countermeasure is counterterrorism
- Counterintelligence (CI) serves as subset of security
  - One without the other does not work
  - CI introduces toolset empowering agile strategy
  - Perception and deception management
  - Behavior analysis, psychology, information security, investigations, human intelligence (HUMINT)
  - Self- and situational awareness
    - Complements threat modeling
    - Attacks are reactive and possibly controllable

Advanced or organized?

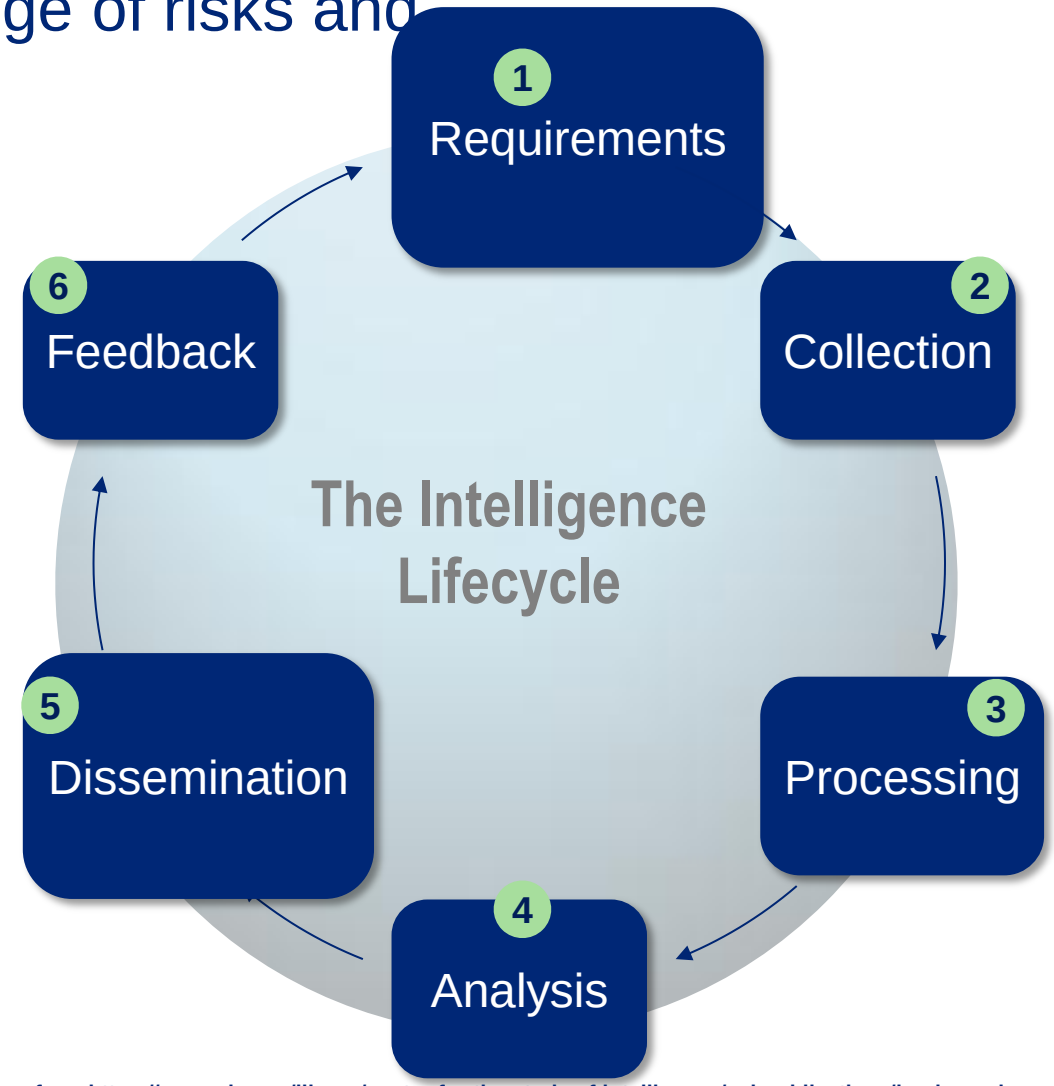
- Today's Advanced Persistent Threat (APT)
  - We called the technique "hacking" in the 90's
  - Tools and tactics are the same as they have always been
  - Cyber crime is opportunistic, i.e., grab all, get out
  - Cyber espionage is strategic in nature
- Organized Persistent Threat (OPT)
  - Planned for persistence
  - Move laterally through the network
  - Malware typically used for entry
  - Human-driven, manually operated
  - Motive is the biggest differentiator

Common factor



Where do we begin?

1. Plan, based on knowledge of risks and attack vectors
2. Gather information
3. Normalize data
4. Construct a meaningful picture
5. Distribute to the right audience
6. Improve future intelligence



from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_4_systems_model.htm

Cyber Counterintelligence (CCI)

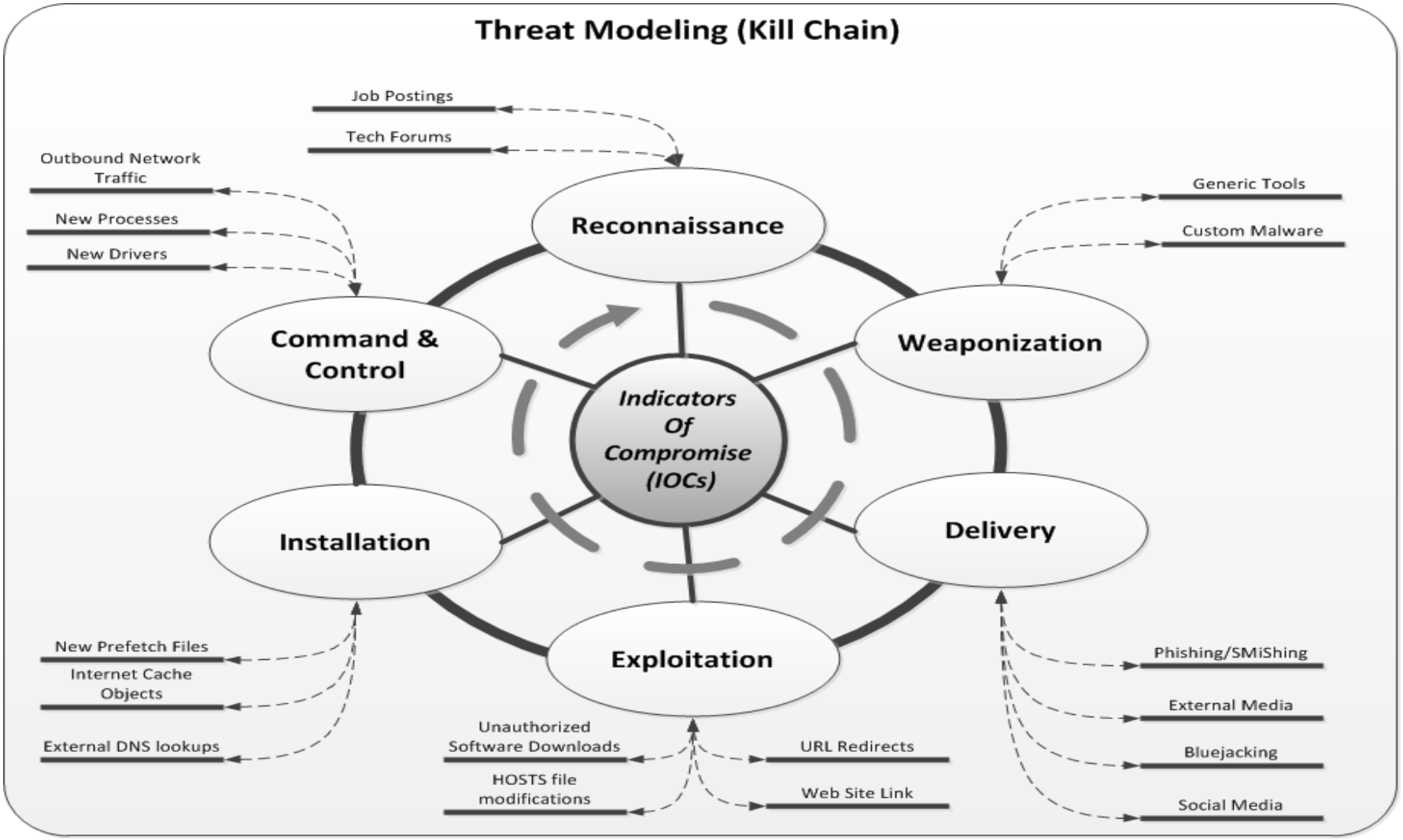
- The efforts made by security teams to prevent hostile or criminal or adversarial organizations from successfully gathering and collecting intelligence against them
- "Actionable" is found in deeply analyzing observable details left by attackers' TTPs
- Traditional defensive counterintelligence
  - Focused on human intelligence and spies
  - Developed during World War II, and has continued to evolve
- Applicable to cyber

Discipline	Defensive CI
HUMINT	Deception in operations security
SIGINT	Radio OPSEC, use of secure telephones, SIGSEC, deception
COMINT	Deception, OPSEC countermeasures, deception (decoys, camouflage)

CCI process

- Countering espionage
  - Fix the basics via threat modeling
    - Information
    - Secrets
    - Actors
- Self-awareness first
  - Example: single-use Point-of-Sale (POS) breach
    - Why does POS have access to Internet?
  - Lateral movement solved through segmentation
- Situational-awareness
  - Know yourself and control your enemy
  - Perception management

Adversarial awareness



Do you know your network?

- Your network has more intelligence…
  - Than anything you will find on the Internet
  - Than any threat intelligence provider
- Success comes from understanding
  - What is your network doing?
    - Why is Dynamic DNS used on my network?
    - Why have I never seen this domain before?
    - Location, entropy, non-existing domain (NXD), cache, non-DNS
- Known good
  - Do you know what good behavior looks like?
  - Solve the good, minimize the bad

Threat intelligence team

- Pro-active in nature
  - Threat research team
  - Gain adversary understanding
- Threat indicators “indicate” what?

COMPONENT	EXPLANATION
Motivation	***The level of intensity and degree of focus***
Objectives	***Boasting rights, disruption, destruction, learn secrets, make money***
Timeliness	***How quickly they work (years, months, days, hours)***
Resources	***Well funded to unfunded (tools and tactics provide insight)***
Risk Tolerance	***High (don’t care) to low (never want to be caught)***
Skills and Methods	***How sophisticated are the exploits (scripting to hardware lifecycle attacks)***
Actions	***Well rehearsed, ad hoc, random, controlled versus uncontrolled***
Attack Origination Points	***Outside, inside, single point, diverse points***
Numbers Involved in Attack	***Solo, small group, big group***
Knowledge Source	***Chat groups, web, oral, insider knowledge, espionage***

Behavior analysis team

- Behavior profiling
  - Is your company doing this?
    - Skills and abilities
    - Resources
    - Motives/motivations
    - Complexity
- Threat actor attribution and neutralization
  - Requires agile strategic planning
  - Attribution framework
    - Who is attacking you?
  - Operational deception
    - Increase risk, decrease reward

Attribution team

- Does attribution help?
  - Long game, yes
  - Neutralization, exposure, legal action
  - Keeping them out – you know why they reacted
  - If they are known or visible they are compromised
  - Determines their methods

- What to analyze?

TTP ANALYSIS	RESULT
Incident Tracking	***Is this similar to other incidents***
Vulnerability / Exploit	***Tools, and attack methods***
Modus Operandi, Signature, Content, Pattern	***Classification of campaigns and activity***
Tools	***Establish skill set and resources***
Utilization of Access	***Motive, maneuverability, familiarity***
Data Transfer Technique	***Identify, detect, locate, method***
OPSec	***Logging alterations, deletion techniques***

Adversary interaction (i.e., HUMINT)

- Should we?
  - Is it our job?
  - Leave it to the Government?
  - Where's the line when protecting our networks?
  - Should we purchase our own stolen data?
- Skills required
  - Psychology
    - Perception management
    - Transactional analysis
    - Cognitive behavior
    - Game theory
  - Law
    - Entrapment

Cyber espionage

- Basic information security achieved
  - Solve those (one at a time)
  - Save yourself lots of trouble
- People vs. technology
  - Security serves the business
    - Invest in the right people
    - Set the expectations for investing in technology
  - Don’t panic
    - Lots of security “theater” out there
    - Stay strategic
  - They are no more advanced then your enterprise
    - They are persistent about getting in
    - Be persistent about keeping them out

Questions?

Thank you

Lance James

Head of Cyber Intelligence

Deloitte & Touche LLP

lancejames@deloitte.com

Deloitte.

Official Professional Services Sponsor

Professional Services means audit, tax, consulting and financial advisory services.