CYBERSECURITY

2015 NTX-ISSA Cyber Security Conference (Spring)

Advanced Persistent Threat (APT) Life Cycle Management

Raytheon

Customer Success Is Our Mission

APT Life Cycle

Advanced Persistent Threat(s)

1 APT compromises supplier website / sends email attachment to an internal user.

2 User visits compromised website and/or opens infected attachment.

3
- Software downloaded to User's machine
- Regular successful connections to camouflaged C2 domain
- FTP connections over non-standard port

SOC Tier I

4
Collected by Network Probe:
- DNS Requests
- HTTP Request
- Netflow Log Entries

From devices within Network:
- User/Machine/IP (AD Log Entry)
- Proxy Log Entries
- Browsing History

Automated Data Analysis Reveals Behaviours:

5
- Beaconing
- Camouflaged C2 Domain
- DNS Requests contain keywords
- Invalid Port/Protocol Combination
- Unknown Software Downloaded

6 **ALERT**
Correlated Events

7 SOC Analyst investigates alert & raises Security Incident.

8 actions and closes incident.

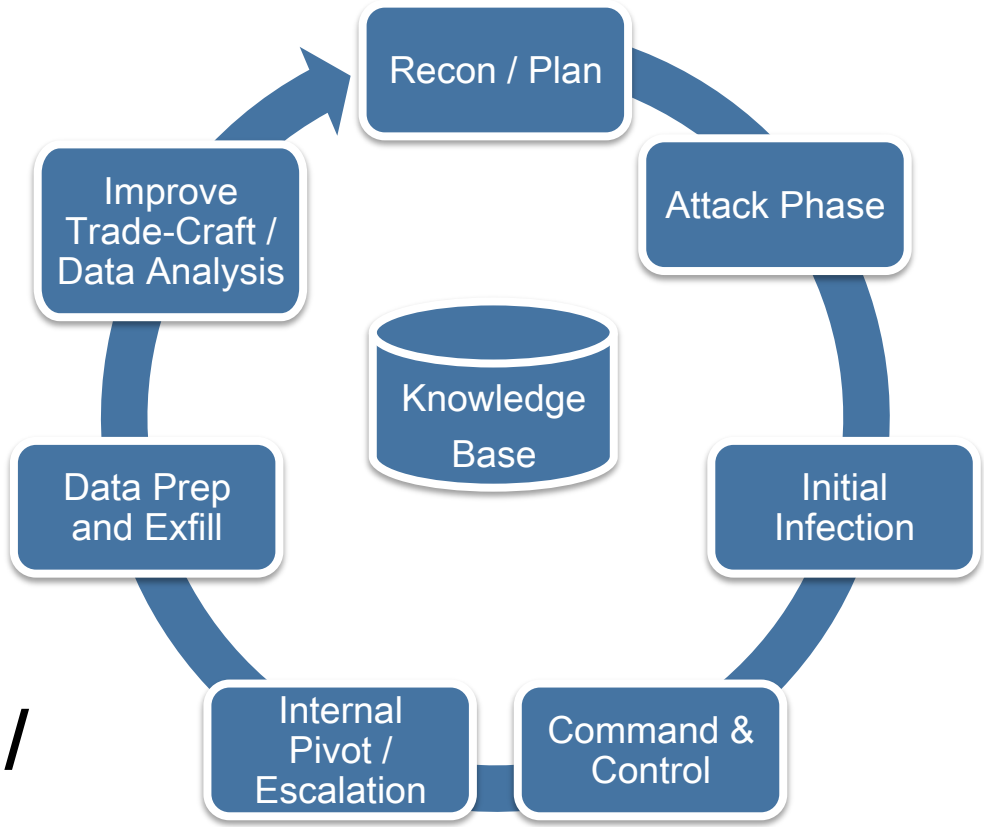
9 User's machine passed to the Forensics Lab for analysis. Malware Lab generates new IOCs.

SOC Tier II+

10 Threat Fusion Teams conducts attribution analysis on Attack Group; tasks probes with new signature and behaviours; and informs external partners (depending on policy).

Typical APT Primary Mission Flows

- Recon / Plan
- Attack Phase
- Initial Infection
- Command & Control
- Internal Pivot / Escalation
- Data Prep and Exfill
- Improve Trade-Craft / Data Analysis
  - Update Knowledge Base



Recon / Plan

- **Attackers**
  - Open Source Collection and Target Identification
  - Attack and Command & Control (C2) Domain Setup / Registration
  - C2 Framework Development (Usually Custom)
    - Persistence and Stealth
    - Reverse Shell Access (On Beacon) Primary Goal
- **Defenders**
  - Open Source Foot Printing - Understand How Attackers See You
  - Information Sharing and Open Source Intel Collection on Attackers / Tools / Underground Sites
  - Prepare Defensive Controls
    - Training for all, more for High-Value / High-Exposure Users
    - Canaries / Miss-Information – to Detect / Mislead Attackers
    - Update Defensive Controls… w/ Intel from Above

Attack Phase

- **Attackers**
  - Gain initial foothold once attack code is executed
  - Prepare and package 0-Day or N-Day Exploits
  - Embed customized exploit and payload (no previous signatures)
  - Make sure attack is not detected by conventional detection tools
  - Utilize Previous Research to Attack Likely Targets via Spear-Phishing and/or Water-Hole Attack
  - Gain initial foothold once attack code is executed
- **Defenders**
  - Hopefully have pre-deployed defenses against these attacks
  - Advanced Anti-Malware for Email / Web (behavioral analysis)
  - Sensors Configured To Alert / Log to SIEM
  - Updated AV, Patching, Limited Admin, and Other Controls
  - Disrupting or Limiting Egress Traffic
  - Good Intel to Pre-Blacklist / Pre Gray-Listing C2 domains is effective

Initial Infection / Command & Control (C2)

- Attackers
  - Ride the “Initial Infection” (reverse shell) into the enterprise
    - Usually done near real-time (the initial attack is not usually persistent)
  - Escalation of initial foothold via installation of one or more Command and Control (C2) binaries that beacon out and wait for instructions / reverse shell
  - Get additional login credentials and beacon hosts
  - “A Team” and “B Team” hand-off
- Defenders
  - Defenders quickly to triage this initial access and prevent C2 client installations
  - Disruption of this C2 (and Initial Infection) is highly valuable when achievable
  - Good credential management, limiting admin rights, and multi-factor auth help greatly (as does restricting or not enabling RDP)
  - Heuristically looking for unusual login times, unusual RDP use, or “beacon tells”
  - White-Listing of known executables does wonders to prevent this stage
  - Don’t let servers connect to the internet unless to a White-List site
  - Backdoors and side-doors into your network need to be defended

Internal Pivot / Escalation

- **Attackers**
  - At this point the “B Team” (collection specialists) are usually in control of the operation
    - Attackers use RDP over the Web C2 as it beacons out
    - Will often use previously compromised credentials to move between hosts and look for data (traffic will fan out from these C2 client hosts)
  - Escalate credentials and look for pivot points between networks
  - Sometimes the “B Team” asks the “A Team” to further enable their access…
  - Attackers will identify data and systems for exfill
- **Defenders**
  - Good credential management, limiting admin rights, and multi-factor auth help greatly (as does restricting or not enabling RDP)
  - Heuristically looking for unusual login times / “beacon tells” / unusual uses of RDP / unusual data movements (volumes, types of data)

Data Prep and Exfill

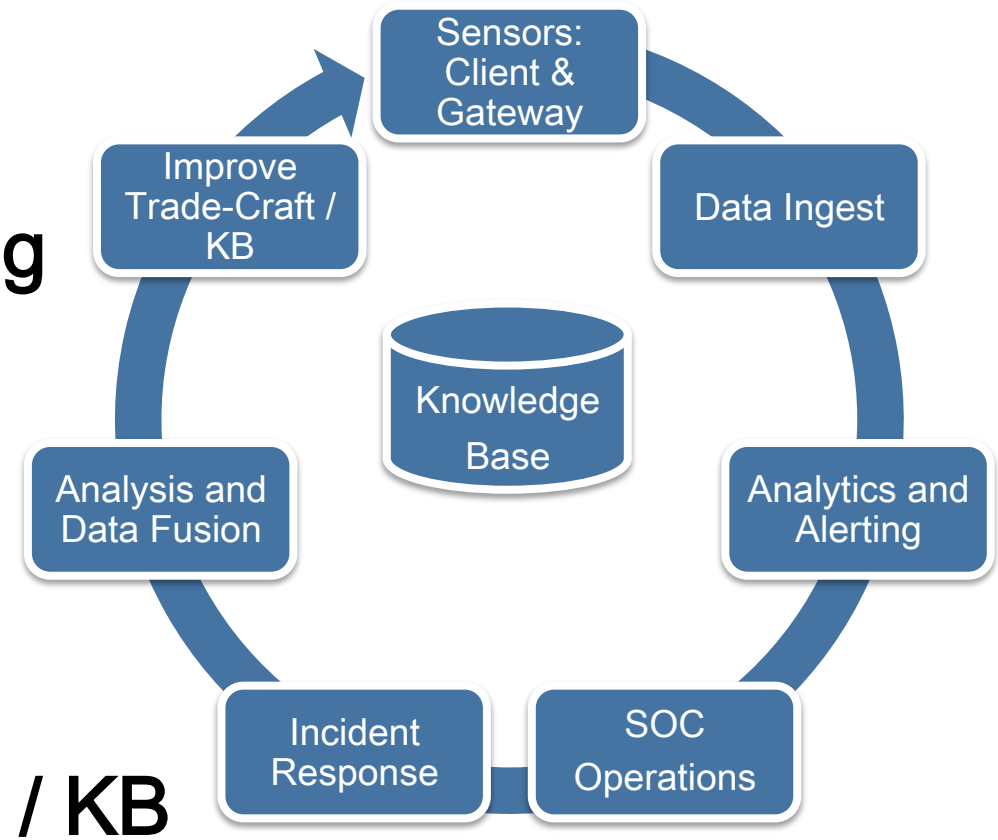
- **Attackers**
  - Attackers will collect data and move it to a host for exfill
    - Of note these hosts are usually not the originally compromised host nor one of the C2 client hosts or first-hops off that host
  - Data will be in encrypted archive (often RAR, sometimes ZIP)
  - When enough data has been collected it will be sent back to the attacker via FTP, Email, HTTP/HTTPS (including web email) are their favorite protocols
  - Often the remote endpoint is not a previously used domain
  - Any intermediary files / tools will be securely deleted from host
- **Defenders**
  - Watch for uncharacteristic file types (RAR, ACE, GZIP, etc.)
  - Heuristic watch for unusual data collection points / transfers (internal hosts)
  - Watch for large bundled data transfers out of your network

Improve Trade-Craft / Data Analysis (APT)

- **Attackers**
  - Receives data (new external host) and sends to home base for analysis
  - Attackers extract the archive(s) and analyze the data
  - Data analysis yields collection requirements to be executed
  - Attackers will track and monitor C2 beacon hosts and come back in and re-infect if your IT staff gets too good at finding their C2 hosts
    - If they lose access they will restart the recon / attack phase
  - Attackers use their previous Intel of network info, download personnel lists / email addresses, identified admin and admin hosts, dumped AD / SAM files, documented / identified key information flows / information brokers to facilitate and plan future attacks
- **Defenders**
  - Defenders have limited options in this phase
  - Innovation, unpredictable / evolving defenses help

Typical CND Primary Mission Flows

- Collect Sensor Data
- Data Ingest
- Analytics and Alerting
- SOC Operations
- Incident Response
- Analysis and Data Fusion
- Improve Trade-Craft / KB
  - Update Sensors / Active Defense
  - Update Knowledge Base / Manage Threat & Risk



Collect Sensor Data / Data Ingest

- **Attackers**
  - Improving Trade-Craft to evade sensors
  - Attackers will look for side door / back door not being watched
  - Attackers test packages against your AVs / IDSes to avoid detection
- **Defenders**
  - Sensors will block some of the attacks on your network (good Intel helps)
  - Network choke points used to watch the traffic crossing them
  - Watch ingress / egress traffic (egress may be of higher value)
  - Lock and watch any side doors / back doors to your network
  - Log / ingest as much as possible / practical to analytics / SIEMs
  - Perform as much full packet / netflow capture as possible
  - Collect at the perimeter of the network and at “crown jewels” of your network

Analytics and Alerting

- **Attackers**
  - Use low and slow / fragmented attacks to avoid detection
  - Attempt to overload your sensors with data and/or false positives to make the analysis and alerting more difficult to process
- **Defenders**
  - Collect as much data as you can process and store, but focus on the most critical alerts first
  - The value of your analytics & alerting will be a direct function of:
    - The tools you are using
    - The value added Intel / signatures you generate internally, you buy, or you get from your friends and family network
    - The timeliness and accuracy of your alerts to the SOC
  - Running internally developed tools in addition to commercial tools likely will add additional value
  - A thorough understanding of the “normal baseline” helps for identifying “anomalies”

SOC Operations

- **Attackers**
  - Attackers have limited activities during CND Mission Flow / SOC Operations
  - Will target SOC users to be able to understand / watch your defenses
- **Defenders**
  - Standup of a dedicated SOC is essential to counter sophisticated threats
    - Need solutions that address business and off hours
    - Many of the APTs will not be working your business hours or will target attacks just before normal working hours end
  - SOC staff training is important as the SOC ends up being the first responders and decides how the alerts are processed
    - Escalate alerts, filter out obvious noise, cleanup obvious attacks
  - Reporting and measuring of SOC effectiveness is critical to management support and improvement in operation
  - Improving “cycle time” for all SOC functions is critical

Analysis and Data Fusion

- **Attackers**
  - Attackers have limited activities during Analysis and Data Fusion
  - Many APTs are however improving their Trade-Craft to combat these functions by being more sophisticated in their C2 use
- **Defenders**
  - Analysis and data fusion is critical to an advanced SOC
  - Internal Analysis of malware, indicators, and threats
    - Extraction of C2 resources, analysis, and signature generation
    - Analysis and OSINT on attackers for predictive purposes
    - Tracking of campaigns by threat actors, understanding of who in your org is being targeted and how/why
    - Updating internal defenses from all above
  - External coordination of malware, indicators, and threats
    - Sourcing indicator data from open, commercial, and friends/ family sources
    - Managing how / what you will share with others

Improve Trade-Craft / KB (Defenders)

- **Attackers**
  - Attackers Trade-Craft is improved in their attack lifecycle
- **Defenders**
  - Implement lessons learned and do root cause analysis
  - Migrate defense from reactive to proactive and try get in front of the attackers with strong analysis and information sharing functions
    - Exploit open source, commercial, and industry data feeds
  - Continuously strive to improve efficiencies in defensive operations
    - Drive dwell time to zero (as a goal)
    - Automate the things that can be automated
    - Provide updated training to your defenders and your end users
  - Keep intel on attackers, attacks, threats, and targets current
  - Your network is not static – make sure your defenses are not

Questions?

Presenter Bio

Monty D. McDougal is a Raytheon Intelligence, Information and Services (IIS) Cyber Engineering Fellow. He has worked for Raytheon for the last 16+ years performing tasks ranging from programming to system administration and has an extensive web development / programming background spanning 18+ years. His work has included development/integration / architecture / accreditation work on numerous security projects for multiple government programs, internal and external security / wireless assessments, DCID 6/3 compliant web-based single sign-on solutions, PL-4 Controlled Interfaces (guards), reliable human review processes, audit log reduction tools, mail bannering solutions, and several advanced anti-malware IRADs / products / patents.

Monty holds the following major degrees and certifications: BBA in Computer Science / Management (double major) from Angelo State University, MS in Network Security from Capitol College, CISSP, ISSEP, ISSAP, GCFE, GAWN-C, GSEC, and serves on the SANS Advisory Board. Monty has previously held the GCIH, GCFA, GREM, GCUX, and GCWN certifications. Monty is also the author of the Windows Forensic Toolchest (WFT).

E-mail: Monty_D_McDougal@raytheon.com

Abstract

Advanced Persistent Threat (APT) Life Cycle Management

This presentation will cover the full Advanced Persistent Threat (APT) Life Cycle and Management of the resulting intrusions. It will cover both what the APTs are doing as attackers and what we as defenders should be doing for both the APT Mission Flows and the Computer Network Defense (CND) Mission Flows.

The APT Mission Flows cover:

Recon / Plan, Attack Phase, Initial Infection, Command and Control, Internal Pivot / Escalation, Data Prep and Exfill, Improve Trade-Craft / Data Analysis

The Computer Network Defense (CND) Mission Flows cover:

Collect Sensor Data, Data Ingest, Analytics and Alerting, SOC Operations, Incident Response, Analysis and Data Fusion, Improve Trade-Craft / KB