Keeping Up with the Adversary: Creating a Threat-Based Cyber Team

Anthony Talamantes
Manager, Defensive Cyber Operations
Johns Hopkins Applied Physics Laboratory

Todd Kight
Lead Analyst, Defensive Cyber Operations
Johns Hopkins Applied Physics Laboratory
Where We Were

- **Ground Up Approach**
  - Continuous Monitoring
    - Anti-Virus
    - IPS/IDS
    - Blackhole/Sinkhole
    - Sandboxes
    - Application Whitelisting
  - Triaging
    - Alerts
    - Tickets
    - Initial IR
  - Mitigation
    - Internal
    - USG

Cyber Operations

- Monitoring
- Triage
- Mitigation

Threat Intel
Behavioral
Hunting
APL Targeted by Nation State – Case Study

- Malware evolution
  - Persistence in Registry
  - Enumerate running processes
  - Anti-Analysis Techniques
  - TASKKILL on malicious process

- Actor Consistencies
  - Office themed emails
  - Time stomping
  - Used SSL for C2
  - Active development
Peer Collaboration - Nation State Compromise

- Never Let a Good Incident Go to Waste
  - Extensive use of cloud and SSL
    - C2
    - Exfiltration
    - Distributing malware
  - PowerShell
    - Reflective injection
    - Lateral movement
  - Persistence
    - WMI
    - Scheduled tasks
    - RunOnce
  - Actor’s actions on network – more agile than incident responders
How Would Our Defenses Perform?

**Ground Up Approach**

- Continuous Monitoring
  - Anti-Virus
  - IPS/IDS
  - Blackhole/Sinkhole
  - Sandboxes
  - Application Whitelisting

- Triaging
  - Alerts
  - Tickets
  - Initial IR

- Mitigation
  - Internal
  - OSInt
  - USG

Cyber Operations

- Monitoring
- Triage
- Mitigation

No Alerts!
No Triage!
No Mitigation!
Philosophy Change

- Red Queen Hypothesis proposes that organisms must constantly adapt, evolve, and proliferate not merely to gain reproductive advantage, but also simply to survive while pitted against ever-evolving opposing organisms in an ever-changing environment.
New Philosophy

- Top Down Approach
  - Threat identification
  - Target advanced tactics, techniques and procedures of adversary
  - Operationalize Malware analysis

- Enlightenment
  - Silver Bullet or Single Event
  - Assumptions
Cyber Threat Team Construct

- Blue sky threats
- Research threat actors
- Threat Intelligence
- Tradecraft research
- Profiling and Patterns

- Purple Team collaboration
- Hybrid Threat Emulation
- Proof of concept testing
- External Adaptive RT

- Hunting
- Continuous monitoring
- Gap analysis
- Fidelity identification
- Comparative analysis

- Scripting
- Content Creation
- Compound Correlation
- Enrichment
- Orchestration

Research
Adaptive
Red Team
Analytics
Development
Defensive Cyber ConOps

Cyber Threat Team
- Research
- Adaptive Red Team
- DevOps
- Analytics

Fidelity

Cyber Hunt Team
- Ad-hoc hunting
- Behaviors of compromise
- Artifacts of compromise
- Pivoting on artifacts
- Procedural
- Closing steps

Analysis & Response

• Analysis & Response to alerts
Putting it All Together

Building the Team
Overview

- Adopt a framework for addressing threats
- Gap Analysis
- Automate low hanging fruit
- Shift our focus
- Build content
Framework – Threats / Countermeasures

**Predict**
- Fully understand the threat and viability
- Identify gaps and understand capabilities and competencies

**Prevent**
- Mitigations against known indicators
- Rules to prevent known behaviors

**Detect**
- Mitigation is not feasible
- Build context rich use cases with assigned confidence/severity

**Respond**
- Identify – Contain – Recover
Gap Analysis and Actions

- **Staff**
  - Repurposed talent and expanded roles (DevOps, Purple Team)

- **Visibility**
  - Email headers, embedded email links, command lines, process trees, registry modifications...

- **Technology**
  - Support additional analytics – YARA custom signatures
  - Support processing IOCs in a timely fashion
  - SIEM – getting to data fast
Automation / Orchestration

- Ingest
  - Reports contain context for use case development (TTPs, strings for YARA, etc.)
  - IOCs are low hanging fruit

- Enrich
  - Use OSINT to your advantage
  - Determine prevalence in your environment
  - Consider your source

- Act
  - Mitigate where feasible (API)
  - Provide enriched ‘exception’ reports for review
Focus Shift – Passive to Active Defense

Events
- Passive: Appliance Generated Alerts
- Active: **Context Rich Use Cases**

IOCs
- Passive: Static IOCs and Signatures
- Active: **Behaviors and Patterns**

Data
- Passive: Benign or Malicious
- Active: **Objective, Uniqueness, Pivoting**

Theory
- Passive: White Papers, Blog Posts, Vendor Reports
- Active: **Countermeasures and Threat Emulation**
Use Case Development Areas

**Delivery**
- Spoofed email
- Email sender
- X-headers
- Email infra mismatch
- Multiple sender infra

**Exploit**
- YARA alert
- Bypass techniques
- Second stage acquisition
- Code execution
  - **Persistence**

**Internal Access/C2**
- Privilege escalation
- Beacons to C2 infra
- Living off the land
- Lateral movement
- Data gathering
Use Case: Windows Persistence (WMI)

- **Permanent WMI**
  - WMI service polls for WMI queries
  - WMI executes code (Consumer) when query (Filter) is satisfied

- **Pros & Cons**
  - Very difficult to detect
  - Specific knowledge is needed to remove payload
  - Requires elevation

- **Artifacts**
  - `Get-WMIObject -Namespace root\Subscription -Class __EventFilter`
  - `Get-WMIObject -Namespace root\Subscription -Class __EventConsumer`
  - `Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding`
Use Case: Windows Persistence (WMI)

- Execution of ActiveScriptEventConsumer
  - Use Case: VBScript being called (as defined in Consumer) when an action occurs (as defined in Filter)
- What to look for:
  - process_name: scrcons.exe
  - parent_name: svchost.exe
  - username: SYSTEM
  - cmdline: "c:\windows\system32\wbem\scrcons.exe –embedding"
Use Case: Windows Persistence (WMI)

- Execution of CommandLineEventConsumer
  - Use Case: Powershell being called (as defined in Consumer) when an action occurs (as defined in Filter)

- What to look for
  - process_name:powershell.exe
  - parent_name:wmiprvse.exe
  - username:SYSTEM
### WMI Event Subscription – Artifacts

<table>
<thead>
<tr>
<th><strong>CLASS</strong></th>
<th><strong>RELPATH</strong></th>
<th><strong>EventFilter</strong></th>
<th><strong>EventFilter</strong>.Name=&quot;DoBadOnScheduleFilter&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>DoBadOnScheduleFilter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Query</td>
<td>SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32_LocalTime' AND (TargetInstance.Minute = 45 OR TargetInstance.Minute = 55) GROUP WITHIN 60</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CLASS</strong></th>
<th><strong>RELPATH</strong></th>
<th>CommandLineEventConsumer</th>
<th>CommandLineEventConsumer.Name=&quot;DoBadOnScheduleConsumer&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>CommandLineTemplate</td>
<td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe –E</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ZwB3AG0AaQAgAHcAaQBuADMAAgBFAGMAAbwBtAHAAdQB0AGUAaQAgAHwAlAbvAHUAAdAAttAGIAaQBsAGUAIAAttAGYAwBByAGMAZQAaQEMAgBcAAAcBvAGcAegBhAG0ARABhAHQAYQBcAFQAaAbhAG4AawBzAEYAbwByAEEAdAB0AGUAaBkAGkAbgBnAFIAUwBBAC4AdAB4AHQA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>CLASS</strong></th>
<th><strong>RELPATH</strong></th>
<th><strong>FilterToConsumerBinding</strong></th>
<th><strong>FilterToConsumerBinding</strong>.Consumer=&quot;CommandLineEventConsumer.Name=&quot;/&quot;DoBadOnScheduleConsumer&quot;&quot; ,Filter=&quot;/&quot;<strong>EventFilter</strong>.Name=&quot;/&quot;DoBadOnScheduleFilter&quot;&quot;</th>
</tr>
</thead>
</table>
Success Stories

- Heartbleed
  - Legacy NT sysadmin tool usage
- Poweliks
  - Mshta spawning processes
- DMZ Incident
  - SQL injection
  - Stacking the deck
- Peer Collaboration
  - Validated Use Cases
Challenges
Management Challenges

- Where are we getting these new teams?
  - Leverage existing talent in Cyber Operations & IT
  - Create Internal Cyber Programs
  - Identify champions

- Drinking the Kool-Aid
  - Senior Leadership support
    - Success stories
    - Communication
  - Team support
Philosophical Challenges

- What is behavioral monitoring anyways?
- Mitigation and Detection
- Threat Intelligence
- False positive acceptance
- An imperfect start is better than a perfect unimplemented plan

*Progress is impossible without change and those who cannot change their minds cannot change anything.*

-George Bernard Shaw
Technical Challenges

- We didn’t have the visibility we needed
  - Host, Network, Process
- Managing larger data sets
- Skill development & agility
- Display new content
- Tracking Hunt activities
Summary

- Adversary is evolving & we must mature and evolve

- **The Analysts**

- **The Process**
  - Define threat and targeting
  - Identify gaps in Cyber Operations
  - Create visibility to identify threat
  - Create and apply appropriate Use Cases
  - Repeat...