Distinguishing Incident Response from Computer Network Defense

Michael Cloppert
Intelligence Fusion Lead
Lockheed Martin CIRT
Relatively standard human sensory system
Fairly poor memory
Marginal analytical abilities
Ability & propensity to think critically
Strong grasp on causality
Distrust of convention

Security isn’t hard, sometimes we just need to think about it differently
Challenges for Existing Models

Something is rotten in the state of CIRT...
Why are we here?

Information Security is Risk Management

NOT Risk Prevention

Effective Security Elements [Schneier, 2000]

1. Prevention
2. Detection
3. Reaction (we say "response")

Conventional strategies treat each separately
A computer security incident is a *violation* or *imminent threat of violation* of computer security policies, acceptable use policies, or standard security practices. [NIST, 2008]

Two key phrases we’ll come back to:
- Violation
- Imminent threat of violation
Canonical Incident Response

- **Attack/Problem Detected** (IDENTIFICATION)
- **Damage Assessment** (COORDINATION)
- **Damage Control** (MITIGATION)
- **Damage Reversal** (INVESTIGATION)
- **Lessons Learned** (EDUCATION)

GCIH Paraphrase
1. Detect
2. Contain
3. Eradicate
4. Recover
5. Lessons Learned

[adapted from van Wyk & Forno, 2001]

[NIST, 2008]
Modern Intrusion “Violation”

Intrusion perpetrators
- Maintain high Situational Awareness (SA)
- Adapt based on environment
- Large set of supporting tools, infrastructure

Organic SA, intel not suited to pipeline response process

“CIRT Superposition”

<table>
<thead>
<tr>
<th>IR Phase</th>
<th>Challenges to Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect</td>
<td>Knowledge mgmt, tool flexibility, separating concurrent intrusions</td>
</tr>
<tr>
<td>Contain</td>
<td>Unidentified/idle comps used to establish different access</td>
</tr>
<tr>
<td>Eradicate</td>
<td>What is “eradication” for systems accessed using stolen credentials?</td>
</tr>
<tr>
<td>Recover</td>
<td>Rebuilt systems re-compromised via containment failure</td>
</tr>
<tr>
<td>Lessons</td>
<td>Campaign-style intrusions ongoing, never reach lessons learned</td>
</tr>
</tbody>
</table>
Imminent Threat of Intrusion

Let’s think about this for a second…
1. Detect imminent threat (not yet happened)
2. Con... tain... ?
3. ?
4. ?
5. ? Profit ?
If mitigation successful, what is response?

Chewbacca is a Wookiee, from the planet Kashyyk. But Chewbacca lives on the planet Endor. Now think about it; that does not make sense!
In other words...

The conventional IR model *presumes compromise* for response actions to begin.

Because post-mortem is never truly reached, *the feedback loop is broken.*
Brief aside: What is Risk?

- Risk (arbitrary definition selected)
  - Impact
  - Vulnerability
  - Threat
    - Intent
    - Opportunity
    - Capability
Mantra: Write to vulnerability, not exploit. Vuln-based detections “better.”

- Observed as recently as 2010 preso on US-CERT site

Tools bias capabilities toward vulnerabilities
- Signatures provided by vendor often for vulns
- Capabilities focus on executable code

Weaker capabilities, less focus on threat element of risk
- Limited detection of non-executable code
- Weak/no decoding of metadata for signatures
- Detection & management of large set of indicators difficult/unsupported
IR Problems, In Summary...

(for modern sophisticated adversaries)

- Phases don’t represent incident states
- Pipeline process poor reflection of action order
- Process presumes compromise
- Feedback loop never completes
- Tools & analysts focused on vulnerabilities
Computer Network Defense

A change in approach and adjustment to tools can enable holistic defense.
Seek one model encapsulating all elements...

1. Prevention
2. Detection
3. Reaction

...that also more accurately represents IR.

Adjust tool requirements to support this model.

Understand how, where this supplants classic IR
Our Solution: Intel-driven CND

Interdependent tools inform all elements

- Indicator Lifecycle
- Kill Chain
- Courses of Action
- Campaign Analysis

[Cloppert, Hutchins, 2011]
Scope & Limitations

- Designed for use against certain threats
  - Manual interaction ("hands-on-keyboard")
  - Corp/nat’l espionage objectives
  - Others, YMMV

- Designed to manage “threat” risk element
  - Fully models security elements in that context
  - No direct utility for Vulnerability element
Guiding Response

- Kill chain highlights success of intrusion, informs response steps
  - Intel sourced from
    - forensics: Act on Intent/Install
    - log analysis: C2/Deliver/Recon
    - malware RE: Weaponize/Exploit/Install/C2
Guiding Intel Collection

- Missing/overlooked intel prevents campaign correlation
- New behaviors in one campaign suggest analytical opportunities in others
- Disciplines similar to “guiding response” per phase
Courses of Action completeness identifies capability gaps
- Investments made to fill key gaps
- Many disciplines leveraged to understand tech capabilities, limitations
  - Non-security devices may be used to fill security requirements

Heavy vulnerability focus means more mature FOSS/COTS capabilities at exploit phase
Guiding Tool Development

- Requirements from Courses of Action
- Tool development may
  - cover FOSS, COTS missing requirements
  - automate repeatable analytical tasks
  - implement a new analytical method
- Examples include
  - Forensics (Enscripts)
  - Malware RE (binary executable extraction)
  - IDS/Log analysis (automated pattern detection)
  - Packet analysis (protocol decoders)
Guiding Research

- Lack of usable indicators at given phase for a campaign, intrusion
- Response efficiency
- Formalization of methods
- Disciplines heavily leveraged
  - Computer Science & Engineering
  - Log / IDS analysis
  - Packet analysis
Where is classic IR?

Classic IR process captured in *adversary* actions in kill chain

Comprehensive detection, mitigation, response actions & interaction defined within model
Various elements of the model can be used for SA, tasking, and prioritization. Herein are examples from LM-CIRT.
Examples: Incident Report Template

IR report TOC

1. Executive Summary 1
2. Incident Analysis 2
   2.1 Introduction & Overview 2
2.2 Incident Scope 7
   2.2.1 Evidence of Compromise 8
   2.2.2 Intelligence-based Searching for Other Actors 9
2.3 Timeline 9
2.4 Adversary 11
   2.4.1 Campaign Overview 11
   2.4.2 Incident Indicator Summary 12
2.5 Campaign “Kill Chain” 13
   2.5.1 Reconnaissance 13
   2.5.2 Weaponization 14
   2.5.3 Delivery 14
   2.5.4 Exploit 20
   2.5.5 Installation 20
   2.5.8 C2 22
   2.5.9 Actions on Objectives 25
3. Summary and Findings 25
4. Appendix 25
Examples: Campaign Activity

| Day by Day Trend (with maximum) | Alpha | Bravo | Charlie | Delta | Echo | Foxtrot | Golf | Hotel | India | Juliet | Kilo | Mike | November | Oscar | Papa | Quebec | Romeo | Sierra | Tango | Uniform | Victor | Whiskey | Provisional | Pending Attribution | Grand Total |
|---------------------------------|-------|-------|---------|-------|------|---------|------|-------|-------|--------|------|------|----------|-------|------|--------|-------|--------|--------|---------|-------|---------|---------|---------|------------|-------------------|-------------|
| Dec 08                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Jan 09                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Feb 09                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Mar 09                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Apr 09                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| May 09                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Jun 09                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Jul 09                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Aug 09                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Sep 09                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Oct 09                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Nov 09                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Dec 09                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Jan 10                          |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |
| Grand Total                     |       |       |         |       |      |         |      |       |       |        |      |      |          |       |      |        |       |        |        |         |       |         |          |         |            |                   |             |

| # of Months Active | 10  | 8  | 7  | 11  | 7  | 6  | 6  | 6  | 6  | 6  | 5  | 4  | 2  | 1  | 9  | 6  | 5  | 4  | 3  | 2  | 5  | 4  | 2 |
|--------------------|-----|----|----|-----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|

| # of Active Campaigns | 7  | 4  | 4  | 7  | 9  | 7  | 7  | 10 | 10 | 10 | 14 | 12 | 8  | 2  | 5  | 11 | 12 | 22 |    |
Examples: Indicator Convergence
Examples: Incident One-Slider

Some-named Incident
Three adversaries using 0 Day Exploit

**Scope**
- \((b_4 + c_4)\) compromised machines
- No successful C2, exfiltration
- Response, triage and clean-up within 24 hours

---

Recon → Weapon → Delivery → Exploit → Installation → C2 → Action

- **Adversary 1 (RT #1)**<br>**common indicator**
- **Adversary 2 (RT #2)**<br>**common indicator**
- **Adversary 3 (RT #3)**<br>**common indicator**

- Website w/ prom 3d, ya...
- **b_1**
- **c_1**
- **date 1**
- Subject: Email Subject 1

- **b_2**
- **date 2**
- **date 3**

- **b_3**
- **date 4**

- Subject: Email Subject 2
- **c_2**

- **c_3**
- **date 5**

- **a_3**
- **date 6**

- **a_4**

- Few users click on link: possible training success. Inbox cleanup response activity.
- **Adversary 1**: link blocked by proxy category.
- **Adversary 2**: Proxy category backdoor block
- **Adversary 3**: DNS mitigations based on early external intelligence

- Invalide addresses, poor targeting inhibit delivery
## Examples: Mitigation Effectiveness

<table>
<thead>
<tr>
<th>Incident</th>
<th>Vector</th>
<th>Exploit</th>
<th>Early</th>
<th>Inbound Protect</th>
<th>Detect</th>
<th>Outbound Protect</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>IDS/SIM Recon</td>
<td>Vendor Notification</td>
<td>Firewall</td>
<td>Intel-based email blocks</td>
<td>Email AV</td>
</tr>
<tr>
<td>Word Doc Unattrib</td>
<td>Email+doc</td>
<td>Flash</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actor 1 Web</td>
<td>HTTP</td>
<td>Various</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actor 2 Web</td>
<td>Web driveby</td>
<td>Flash</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Military Unattrib</td>
<td>Email+doc</td>
<td>Word</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foreign MitMBX</td>
<td>Email+doc</td>
<td>Word</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend**
- **Applicable**
- **Inapplicable**
- **Blocked Activity**
- **Could have blocked**
- **Would not block or n/a**
- **n/a**
Examples: Hostile Email Residual Risk

Monthly Email Delivery Vector Mitigations
Examples: Ticket Dashboard
Future Directions

- Application of Endsley’s SA model to CND and CNO
- Objective volatility measures for indicators as campaign, indicator properties, automatic correlation, etc.
- Mean Time To Intrusion to compare “softer” (non-binary) mitigations to classic CoA’s


