Distinguishing

Incident Response from Computer Network Defense

Michael Cloppert
Intelligence Fusion Lead
Lockheed Martin CIRT

Curriculum Vitae

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

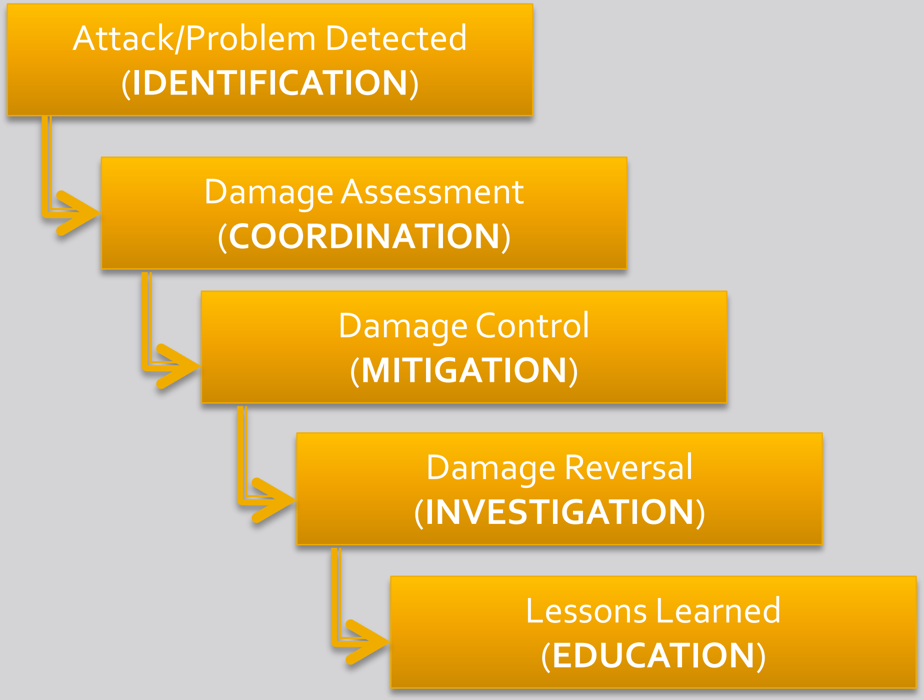
Reaction to Incident

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**)

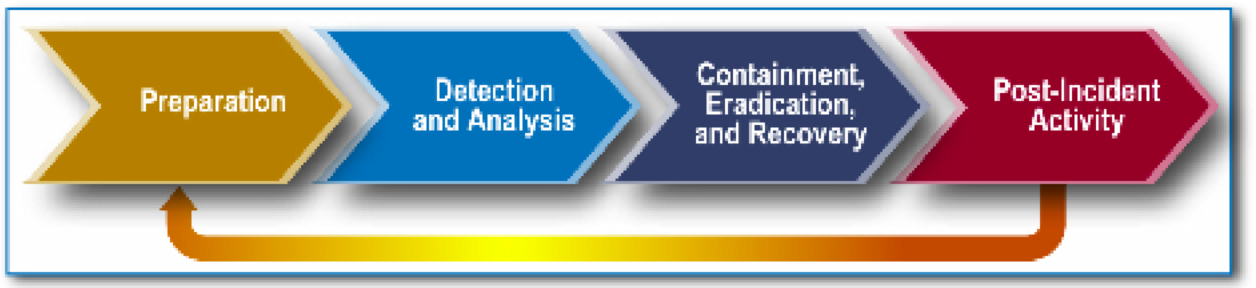
Lessons Learned (**EDUCATION**)

[adapted from van Wyk & Forno, 2001]

<u>GCIH Paraphrase</u>

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

[GIAC, 2011]



[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”

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

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

Detection Strategies

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.

Seeing the Whole Problem

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]

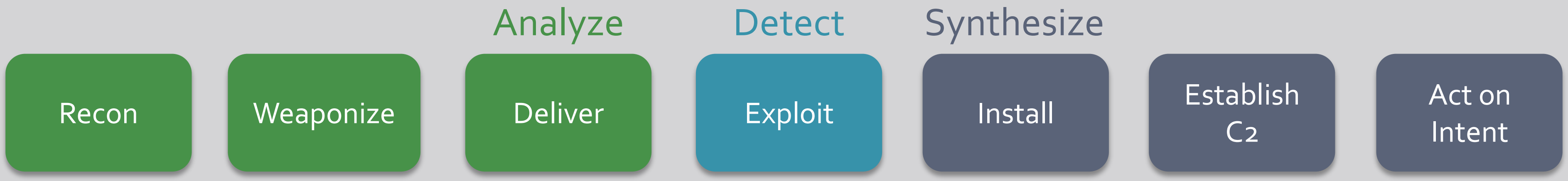
Scope & Limitations

- 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



Analyze

Detect

Synthesize

Recon

Weaponize

Deliver

Exploit

Install

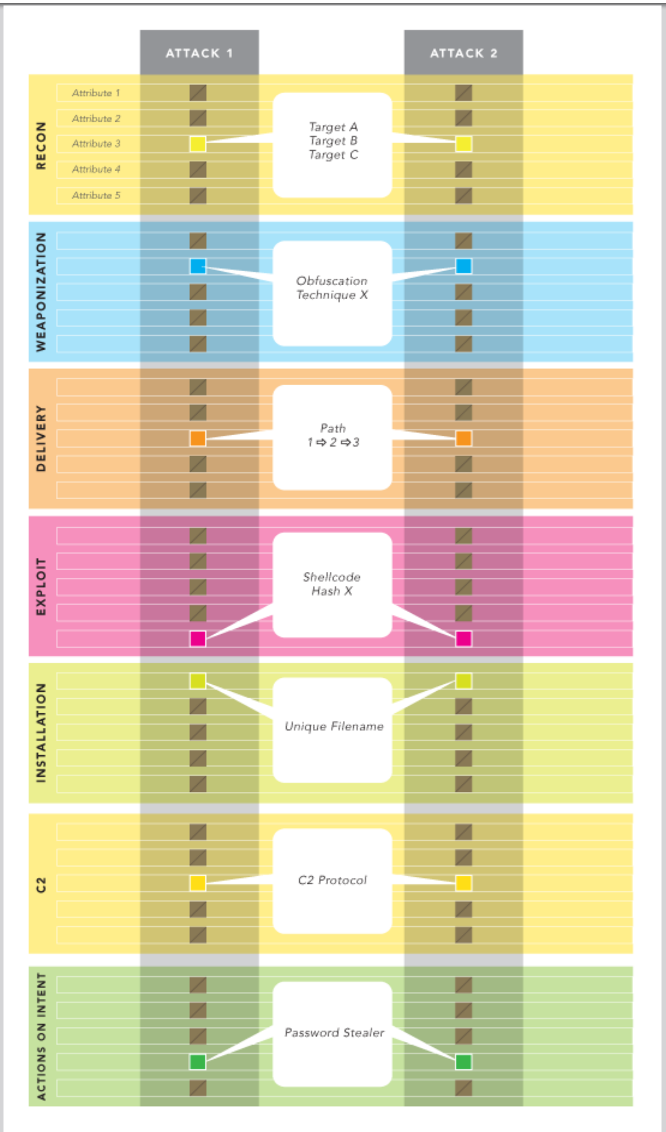
Establish C2

Act on Intent

- Intel sourced from
  - forensics: Act on Intent/Install
  - log analysis: C2/Deliver/Recon
  - malware RE: Weaponize/Exploit/Install/C2

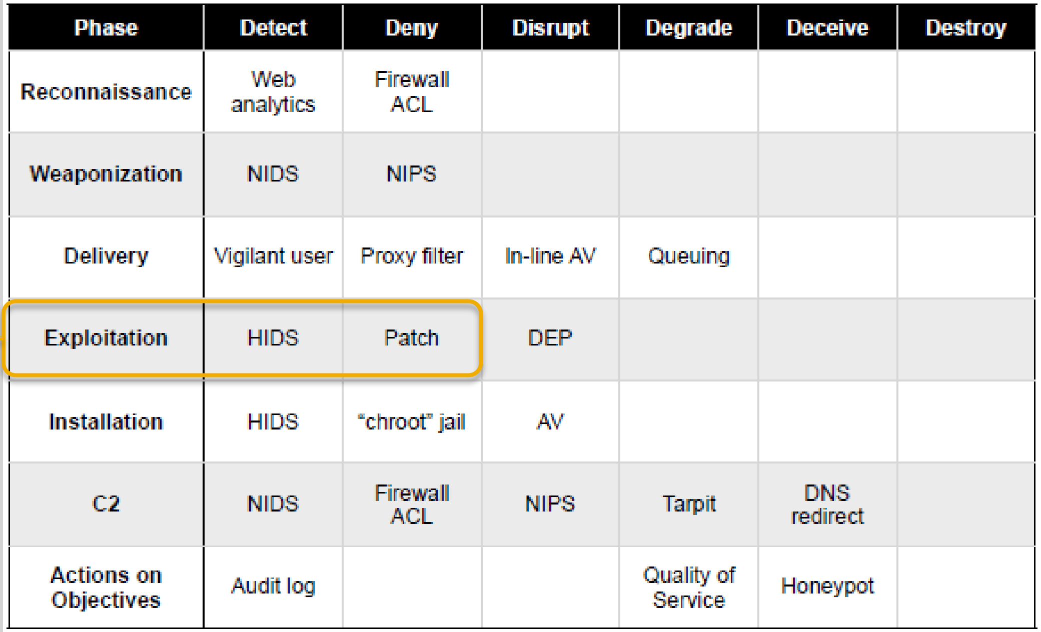
Guiding Intel Collection

- Missing/overlooked intel prevents campaign correlation
- New behaviors in one campaign suggest analytical opportunities in others
- Disciplines similar to “guiding response” per phase



Guiding Investment

- 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



Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

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

Guiding Tool Development

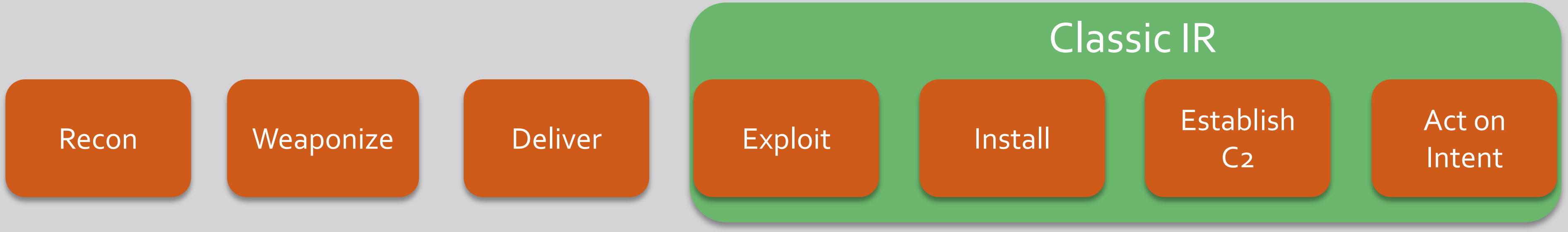
- Requirements from Courses of Action
- Tool development may
  - cover FOSS, COTS missing requirements
  - automate repeatable analytical tasks
  - implement a new analytical method
- Examples include
  - Forensics (Enscripts)
  - Malware RE (binary executable extraction)
  - IDS/Log analysis (automated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

Intel-driven CND Examples

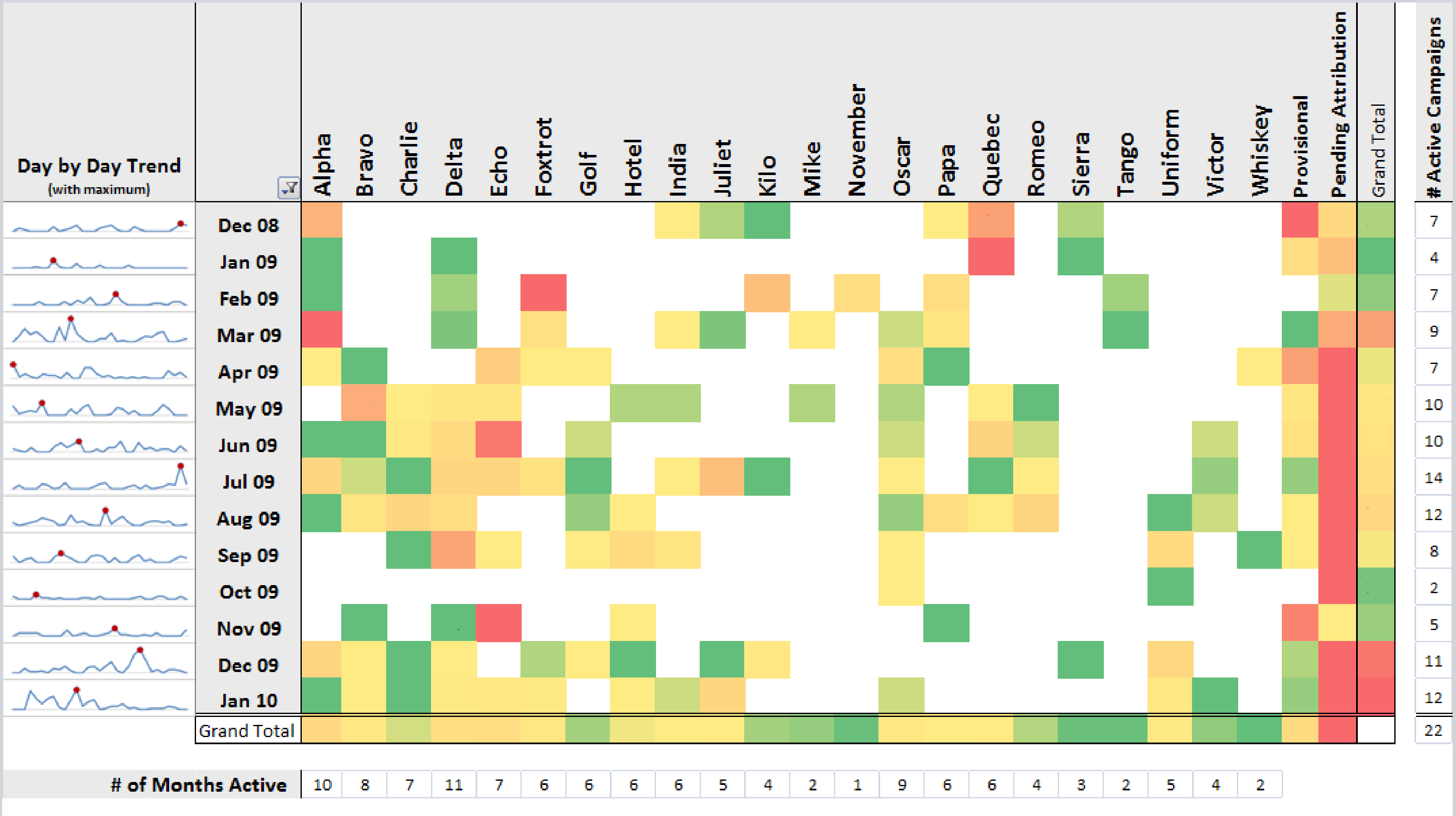
Various elements of the model can be used for SA, tasking, and prioritization. Herein are examples from LM-CIRT.

Examples: Incident Report Template

IR report TOC

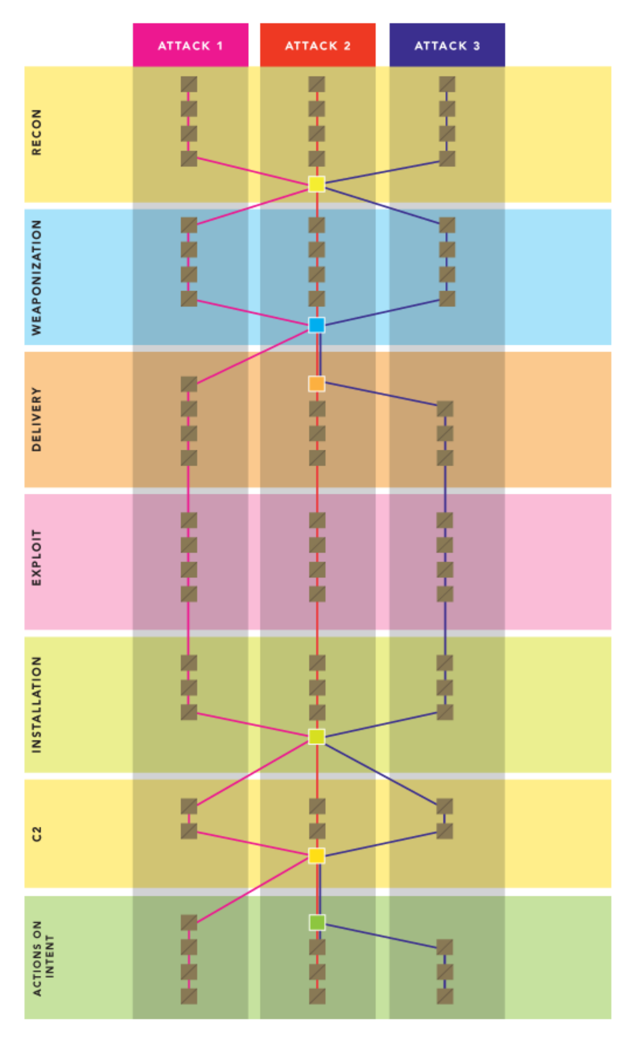
1. Executive Summary 1
2. Incident Analysis 2
2.1 Introduction & Overview 2
2.2 Incident Scope 7
2.2.1 Evidence of Compromise8
2.2.2 Intelligence-based Searching for Other Actors 9
2.3 Timeline 9
2.4 Adversary 11
2.4.1 Campaign Overview 11
2.4.2 Incident Indicator Summary 12
2.5 Campaign "Kill Chain" 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	# Active Campaigns
	Dec 08	🟧								🟨	🟩	🟩				🟨	🟧		🟩					🟥	🟨	🟩	7
	Jan 09	🟩			🟩												🟥		🟩					🟨	🟧	🟩	4
	Feb 09	🟩			🟩		🟥					🟧		🟨		🟨				🟩					🟩	🟩	7
	Mar 09	🟥			🟩		🟨			🟨	🟩		🟨		🟩	🟨				🟩				🟩	🟧	🟧	9
	Apr 09	🟨	🟩			🟧	🟨	🟨							🟨	🟩							🟨	🟧	🟥	🟨	7
	May 09		🟧	🟨	🟨	🟨			🟩	🟩			🟩		🟩		🟨	🟩						🟨	🟥	🟨	10
	Jun 09	🟩	🟩	🟨	🟨	🟥		🟩							🟩		🟧	🟩				🟩		🟨	🟥	🟨	10
	Jul 09	🟨	🟩	🟩	🟨	🟨	🟨	🟩		🟨	🟧	🟩			🟨		🟩	🟨				🟩		🟩	🟥	🟨	14
	Aug 09	🟩	🟨	🟨	🟨			🟩	🟨						🟩	🟨	🟨	🟨			🟩	🟩		🟨	🟥	🟨	12
	Sep 09			🟩	🟧	🟨		🟨	🟨	🟨					🟨						🟨		🟩	🟨	🟥	🟨	8
	Oct 09														🟨						🟩				🟥	🟩	2
	Nov 09		🟩		🟩	🟥			🟨							🟩								🟥	🟨	🟩	5
	Dec 09	🟨	🟨	🟩	🟨		🟩	🟨	🟩		🟩	🟨							🟩		🟨			🟩	🟥	🟥	11
	Jan 10	🟩	🟨	🟩	🟨	🟨	🟨		🟨	🟩	🟨				🟩						🟨	🟩		🟩	🟥	🟥	12
	Grand Total	🟨	🟨	🟩	🟨	🟨	🟨	🟩	🟨	🟨	🟨	🟩	🟩	🟩	🟨	🟨	🟨	🟩	🟩	🟩	🟨	🟩	🟩	🟨	🟥		22
	# of Months Active	10	8	7	11	7	6	6	6	6	5	4	2	1	9	6	6	4	3	2	5	4	2				

Examples: Indicator Convergence



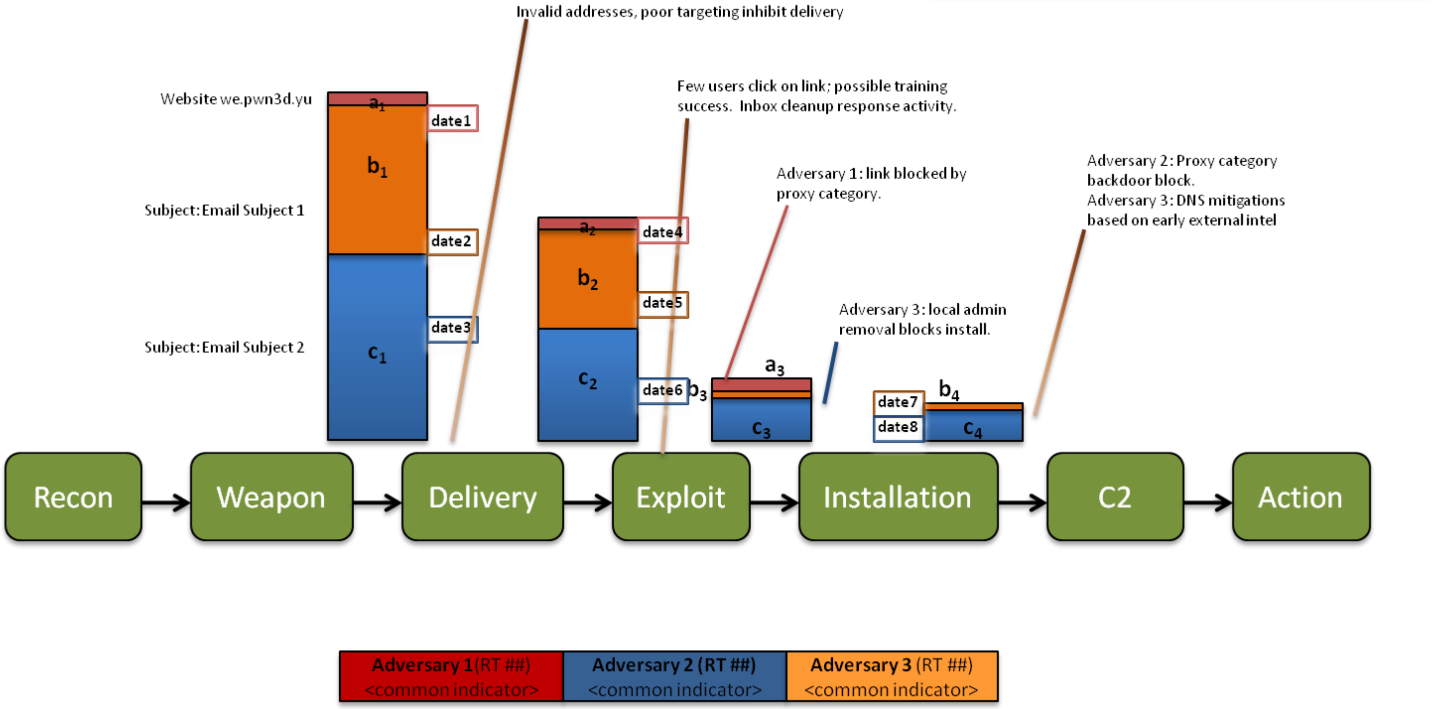
Examples: Incident One-Slider

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



Invalid addresses, poor targeting inhibit delivery

Website we.pwn3d.yu

Subject: Email Subject 1

Subject: Email Subject 2

Few users click on link; possible training success. Inbox cleanup response activity.

Adversary 1: link blocked by proxy category.

Adversary 3: local admin removal blocks install.

Adversary 2: Proxy category backdoor block.
Adversary 3: DNS mitigations based on early external intel

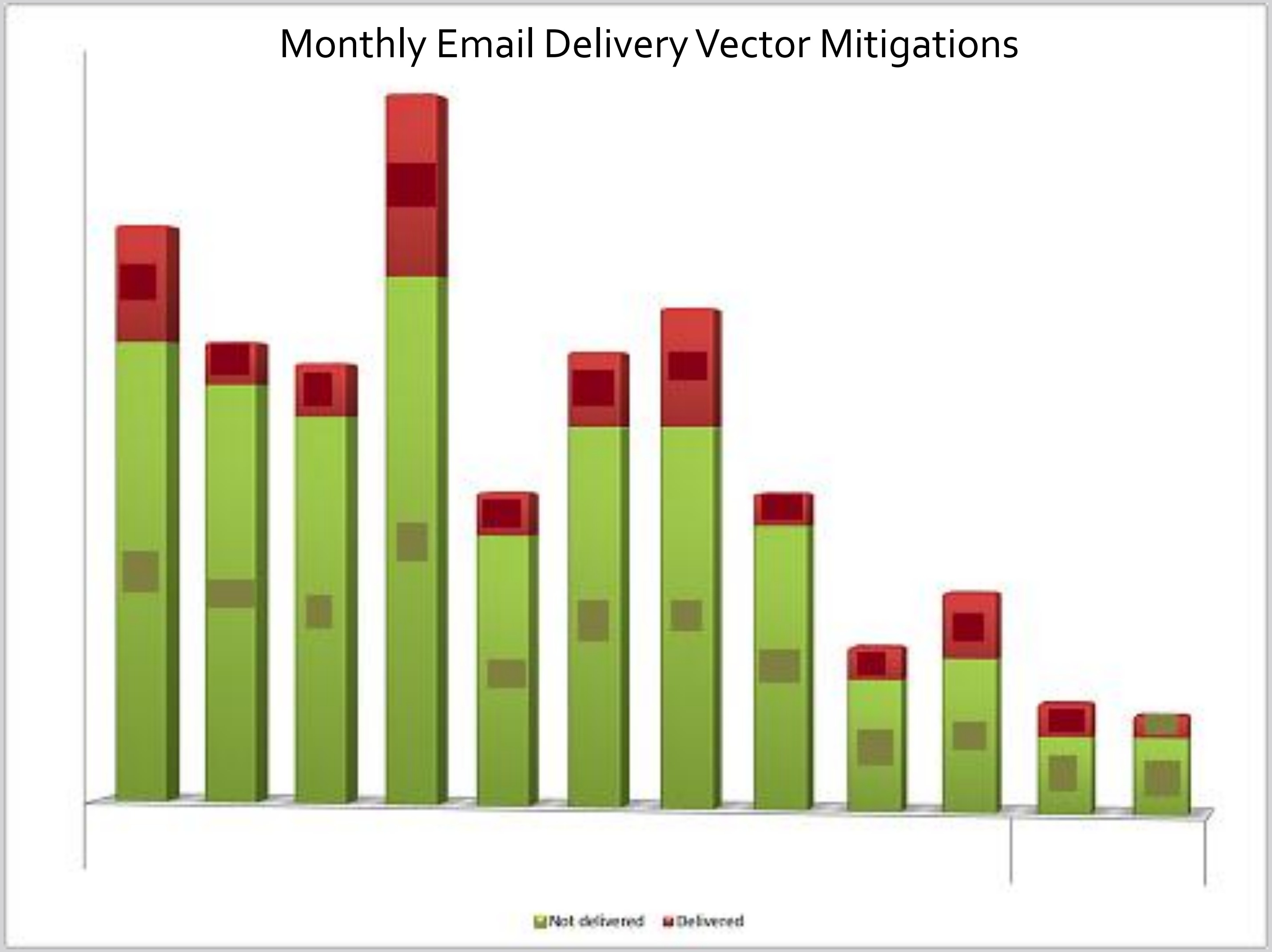
Examples: Mitigation Effectiveness

			Present capabilities																					***Future***		
			Early		**Inbound Protect** *Delivery*				**Detect** *All Phases*						**Outbound Protect** *Exploit, Installation, C2*									**Proposed**		
Incident	**Vector**	**Exploit**	IDS/SIM Recon	Vendor Notification	Firewall	Intel-based email blocks	Email AV	HTTP Proxy	Sourcefire IDS	Custom Detections	SIM	FPC	Shared Intel	Employee Report	Manual Inbox Cleanup	Desired user action	AV/HIPS	Architecture (Proxy, etc)	Intel-based Proxy blocks	Proxy Category Blocks	DNS Mitigations	Firewall	Vuln Patch/Best Practice	Restricted User Rights	Application Patch	Off-network Restrictions
Word Doc Unattrib	Email+doc	Flash								🟥	🟥				●										🟪	
Actor 1 Web	HTTP	Various									🟥	🟥						🟦					●			
Actor 2 Web	Web driveby	Flash								🟥	🟥	🟥	🟥												🟪	
Military Unattrib	Email+doc	Word								🟥	🟥				●		🟦	🟦			🟦		🟦			
Foreign MitMBX	Email+doc	Word								🟥	🟥				●			🟦			🟦		🟦			

Legend

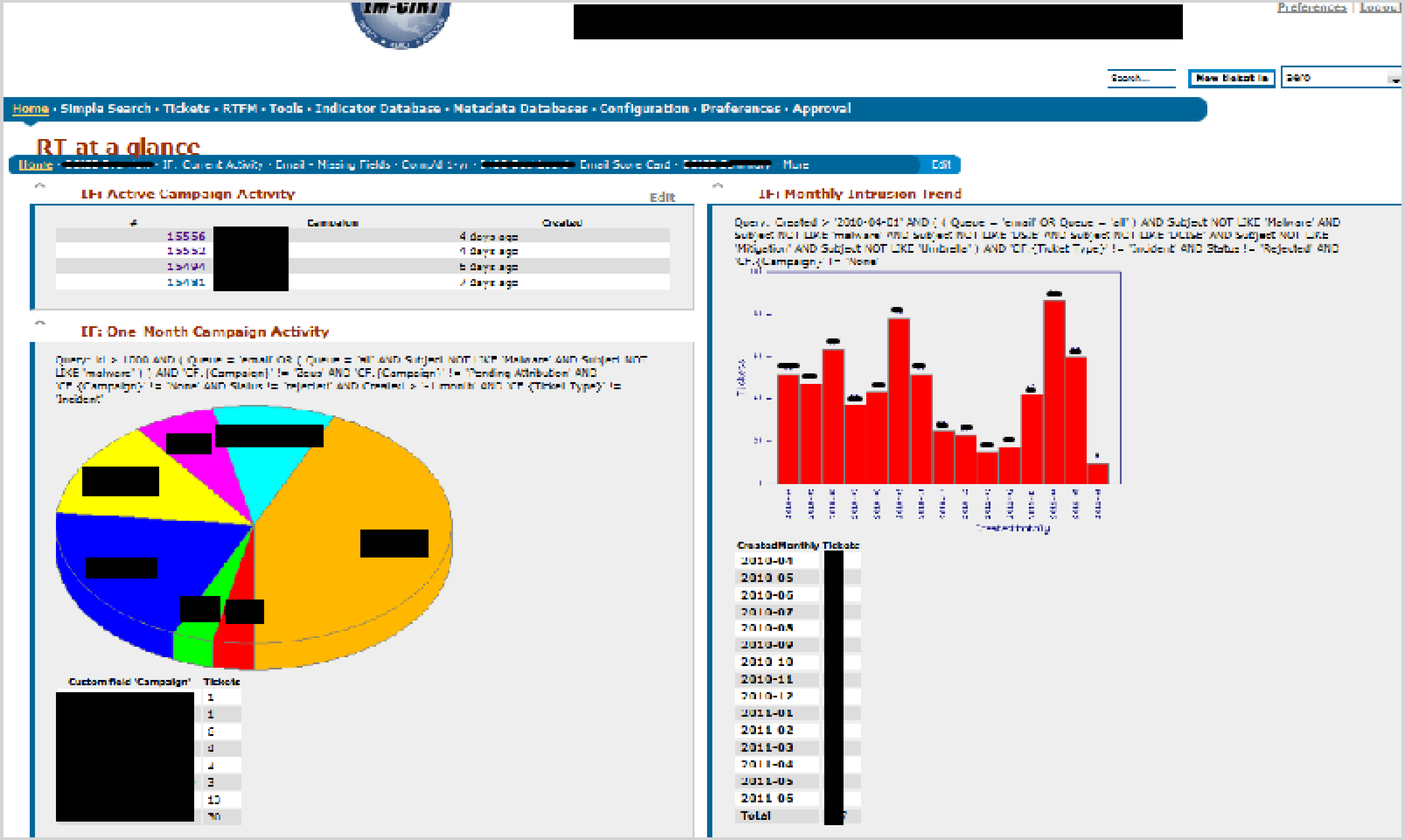
●	🟥 *Applicable*	● *Blocked Activity*	🟪 *Applicable*
🟦	*Inapplicable*	🟦 *Could have blocked*	*n/a*
		Would not block or n/a	

Examples: Hostile Email Residual Risk



Monthly Email Delivery Vector Mitigations

Examples: Ticket Dashboard


Preferences | Logout
Search...
New ticket in
Home · Simple Search · Tickets · RTFM · Tools · Indicator Database · Metadata Databases · Configuration · Preferences · Approval
Home · [redacted] · IT: Current Activity · Email · Missing Fields · Comp'd Inv · [redacted] · Email Score Card · [redacted] · More
Edit
Tickets
CreatedMonthly

[redacted]

RT at a glance

IT: Active Campaign Activity

#	Campaign	Created
15556	[redacted]	4 days ago
15552	[redacted]	4 days ago
15494	[redacted]	5 days ago
15491	[redacted]	7 days ago

IT: One Month Campaign Activity

Query: id > 1000 AND (Queue = 'email' OR (Queue = 'ir' AND Subject NOT LIKE 'Malware' AND Subject NOT LIKE 'malware')) AND 'CF.{Campaign}' != 'Zeus' AND 'CF.{Campaign}' != 'Pending Attribution' AND 'CF.{Campaign}' != 'None' AND Status != 'rejected' AND Created > '-1 month' AND 'CF.{Ticket Type}' != 'Incident'

Custom field 'Campaign'	Tickets
[redacted]	1
[redacted]	1
[redacted]	6
[redacted]	4
[redacted]	4
[redacted]	3
[redacted]	10
[redacted]	30

IT: Monthly Intrusion Trend

Query: Created > '2010-04-01' AND ((Queue = 'email' OR Queue = 'ir') AND Subject NOT LIKE 'Malware' AND Subject NOT LIKE 'malware' AND Subject NOT LIKE 'Zeus' AND Subject NOT LIKE 'ZEUS' AND Subject NOT LIKE 'Mitigation' AND Subject NOT LIKE 'Umbrella') AND 'CF.{Ticket Type}' != 'Incident' AND Status != 'Rejected' AND 'CF.{Campaign}' != 'None'

CreatedMonthly	Tickets
2010-04	[redacted]
2010-05	[redacted]
2010-06	[redacted]
2010-07	[redacted]
2010-08	[redacted]
2010-09	[redacted]
2010-10	[redacted]
2010-11	[redacted]
2010-12	[redacted]
2011-01	[redacted]
2011-02	[redacted]
2011-03	[redacted]
2011-04	[redacted]
2011-05	[redacted]
2011-06	[redacted]
Total	[redacted]

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

.bib

Cloppert, Hutchins, Amin, *Intelligence-driven CND through Analysis of Adversary Kill Chains and Campaigns*, Proceedings of the 6th Annual Conference on Information Warfare and Security, March, 2011.

GIAC, *Information Security Certification: GIAC Certified Incident Handler (GCIH)*, accessed June 7, 2011.

Scarfone, et. al., *NIST Special Publication 800-61 Computer Security Incident Handling Guide,* March 2008*.*

Schneier, Bruce, *Secrets & Lies: Digital Security in a Networked World,* John Wiley & Sons, Inc., New York, NY, 2000.

Van Wyk, KR and Forno, R, *Incident Response*, O'Reilly & Associates, Seabastopol, CA, 2001.