Approaching Intelligent Analysis For Attribution And Tracking The Lifecycle Of Threats

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Timur Snoke

1/15/2015

Scope

Goal of the Net Defender is to address threats that impact the network.

This requires the Net Defender to understand their network, characterize the threat and respond accordingly.

To accomplish this end they must:

- Harden the Network
- Identify Breaches
- Mitigate Attacks

Why is this hard?

What can we do about it?

Problem

Network defense is a craft.

Network defense coverage is best effort.

Network defense responses are alert driven.

Attribution is hard and sometimes problematic.

Reporting is often light on context.

Goal

Improve Net Defense by providing repeatable methodology to place threat within a richer context.

Leverage existing models to extend our understanding of the threats we are defending against.

- Lockheed Martin Cyber Kill Chain®
- The Diamond Model

Expand our response beyond the incident to the campaign.

Method

- Identify reporting of interest
- Evaluate situational awareness to identify events
- Capture network touch points associated with the event
- Expand touch points into larger context
- Aggregate events into campaigns
- Mitigate, Remediate, Rinse, Repeat.

Elements to Synthesize

Incident Management Processes

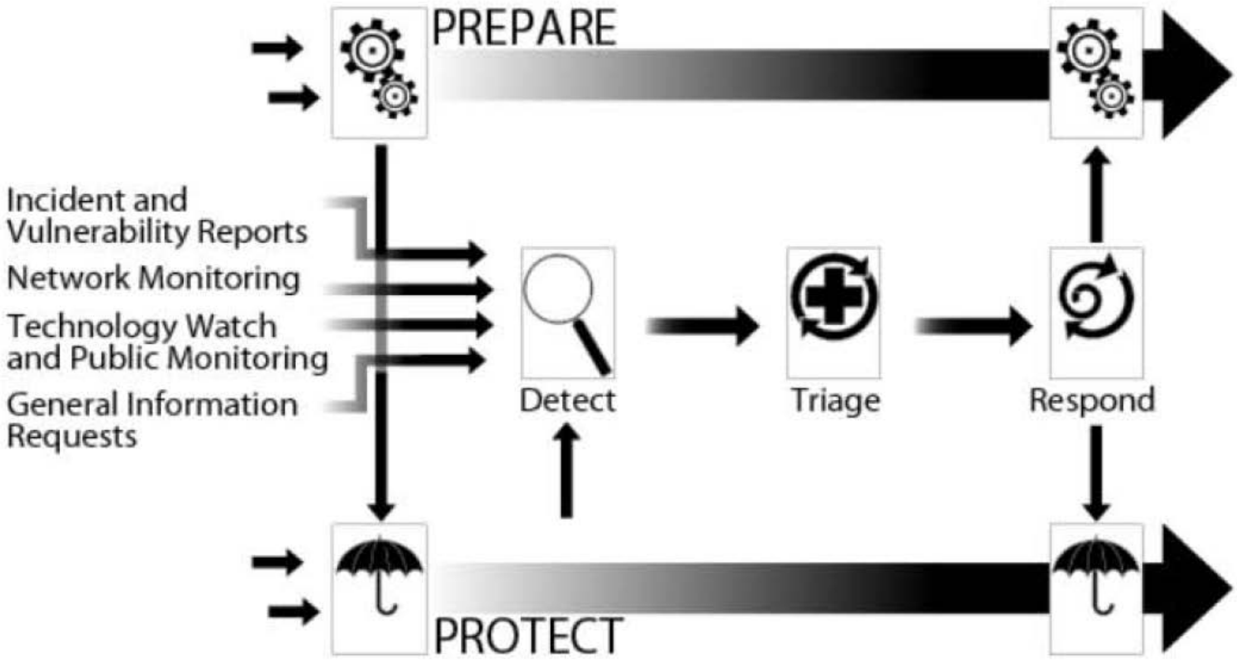
Intelligence Analysis

Intrusion Kill Chain event modeling

Diamond Model of intrusion analysis

Understood properly, these elements combine for powerful results.

Incident Management Basics


PREPARE
Incident and Vulnerability Reports
Network Monitoring
Technology Watch and Public Monitoring
General Information Requests
Detect
Triage
Respond
PROTECT

Alberts, Christopher; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. Defining Incident Management Processes for CSIRTs: A Work in Progress (CMU/SEI-2004-TR-015). Software Engineering Institute, Carnegie Mellon University, 2004. *http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=7153*

Intelligence Analysis

“**Intelligence analysis** is the process of taking known information about situations and entities of strategic, operational, or tactical importance, characterizing the known, and, with appropriate statements of probability, the future actions in those situations and by those entities.”

Intelligence analysis - Wikipedia, the free encyclopedia. Accessed October 1, 2014.

http://en.wikipedia.org/wiki/Intelligence_analysis

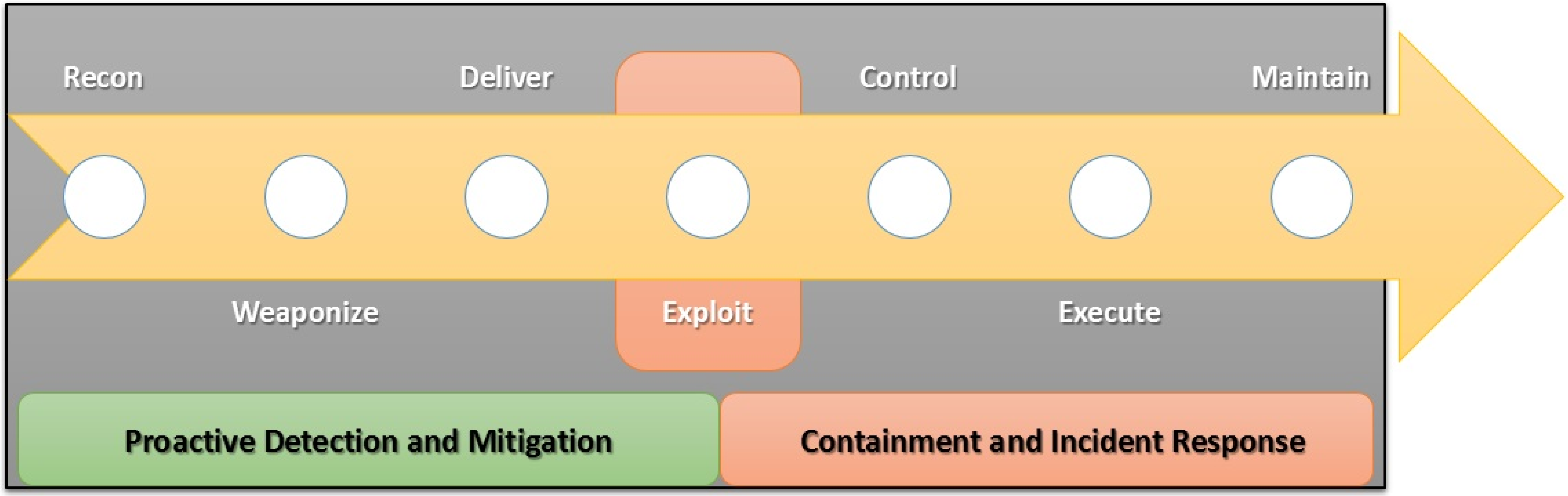
Lockheed Martin - Cyber Kill Chain®

“…an intelligence-driven defense process, **Cyber Kill Chain®**, which allows information security professionals to proactively remediate and mitigate advanced threats in the future.”

Lockheed Martin - Cyber Kill Chain®. Accessed October 1, 2014.

http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html

Lockheed Martin - Cyber Kill Chain® (MITRE Variant)


Recon
Deliver
Control
Maintain
Weaponize
Exploit
Execute
Proactive Detection and Mitigation
Containment and Incident Response

Lockheed Martin - Cyber Kill Chain® (MITRE Variant). Accessed October 1, 2014.

http://nigesecurityguy.wordpress.com/2013/06/04/defensible-security-posture/

The Diamond Model

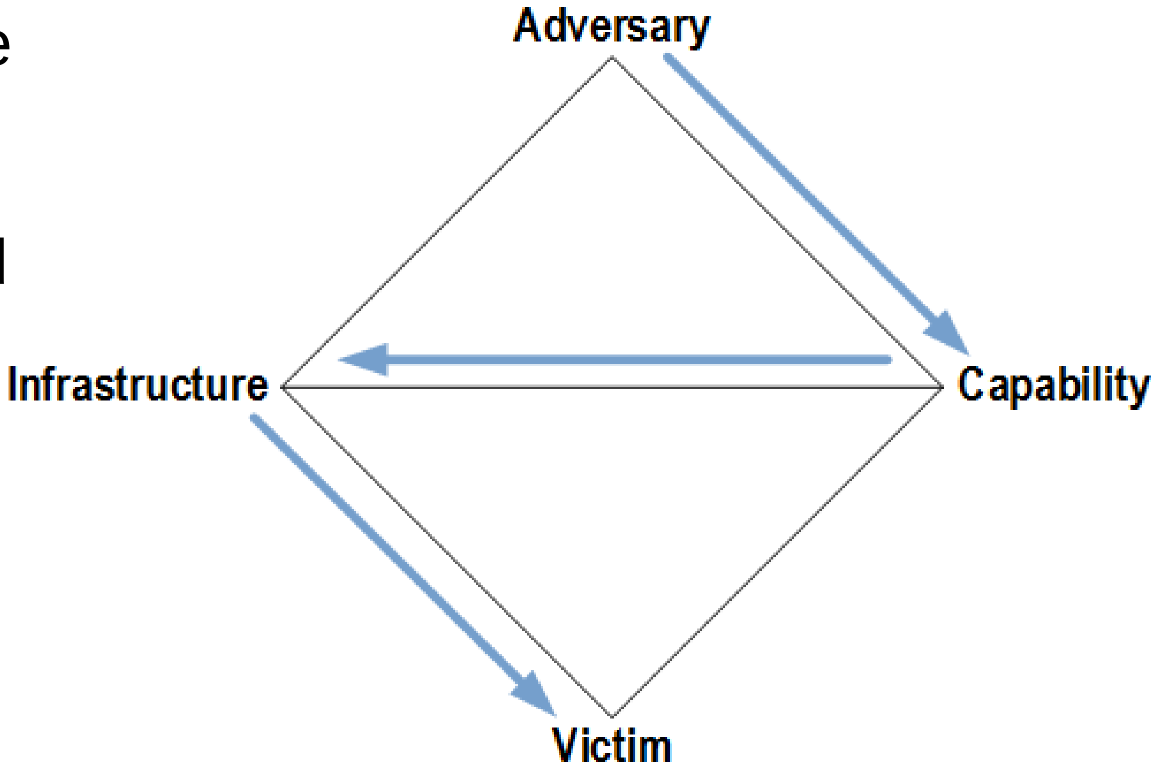
“**…**a formal method applying scientific principles to intrusion analysis particularly those of measurement, testability, and repeatability providing a comprehensive method of activity documentation, synthesis, and correlation…”

The Diamond Model of Intrusion Analysis. Accessed October 1, 2014.

http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

The Diamond Event

Axiom 1 For every intrusion event there exists an adversary taking a step towards an intended goal by using a capability over infrastructure against a victim to produce a result.



The Diamond Model of Intrusion Analysis. Accessed October 1, 2014.

http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

The Diamond Model – Event Defined

$$\left.\begin{array}{l}
\{\{\text{Adversary}, \text{Confidence}_{\text{adversary}}\}, \\
\{\text{Capability}, \text{Confidence}_{\text{capability}}\}, \\
\{\text{Infrastructure}, \text{Confidence}_{\text{infrastructure}}\}, \\
\{\text{Victim}, \text{Confidence}_{\text{victim}}\},
\end{array}\right\}\ \textbf{Core Features}$$

$$\left.\begin{array}{l}
\{\text{Timestamp}_{\text{start}}, \text{Confidence}_{\text{timestamp}_{\text{start}}}\}, \\
\{\text{Timestamp}_{\text{end}}, \text{Confidence}_{\text{timestamp}_{\text{end}}}\}, \\
\{\text{Phase}, \text{Confidence}_{\text{phase}}\}, \\
\{\text{Result}, \text{Confidence}_{\text{result}}\}, \\
\{\text{Direction}, \text{Confidence}_{\text{direction}}\}, \\
\{\text{Methodology}, \text{Confidence}_{\text{methodology}}\}, \\
\{\text{Resources}, \text{Confidence}_{\text{resources}}\}\}
\end{array}\right\}\ \textbf{Meta Features}$$

The Diamond Model of Intrusion Analysis. Accessed October 1, 2014.

http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

The Diamond Model – Adversary / Victim

Axiom 2 There exists a set of adversaries (insiders, outsiders, individuals, groups, and organizations) which seek to compromise computer systems or networks to further their intent and satisfy their needs.

Axiom 3 Every system, and by extension every victim asset, has vulnerabilities and exposures.

The Diamond Model of Intrusion Analysis. Accessed October 1, 2014.

http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

The Diamond Model – Phase / Resources

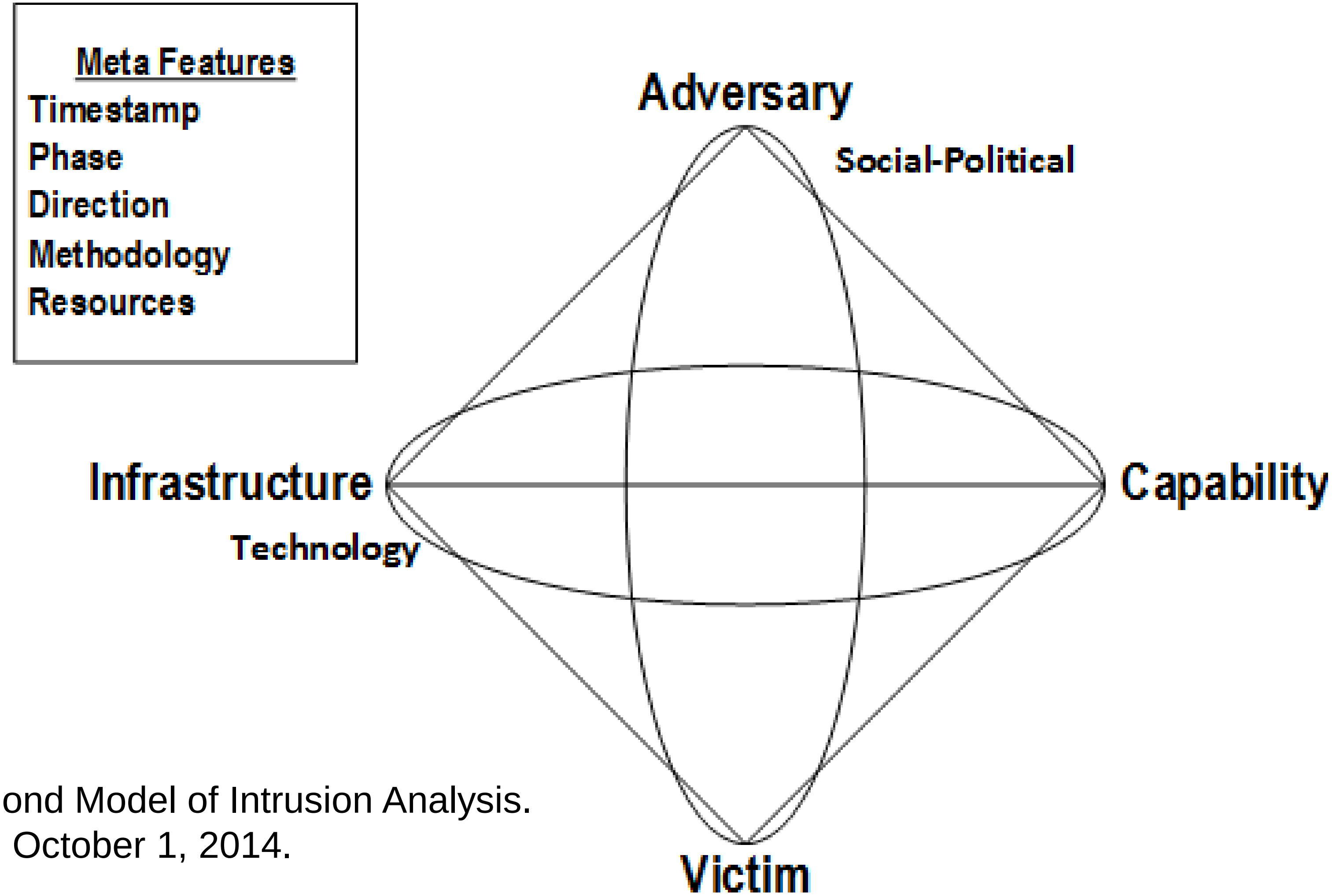
Axiom 4 Every malicious activity contains two or more phases which must be successfully executed in succession to achieve the desired result.

Axiom 5 Every intrusion event requires one or more external resources to be satisfied prior to success.

The Diamond Model of Intrusion Analysis. Accessed October 1, 2014.

http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

The Extended Diamond Model



The Diamond Model of Intrusion Analysis. Accessed October 1, 2014.

http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

The Diamond Model – Social-Political / Persistence

Axiom 6 A relationship always exists between the Adversary and their Victim(s) even if distant, fleeting, or indirect.

Axiom 7 There exists a sub-set of the set of adversaries which have the motivation, resources, and capabilities to sustain malicious effects for a significant length of time against one or more victims while resisting mitigation efforts. Adversary-Victim relationships in this sub-set are called persistent adversary relationships.

- **Corollary 1** There exists varying degrees of adversary persistence predicated on the fundamentals of the Adversary-Victim relationship.

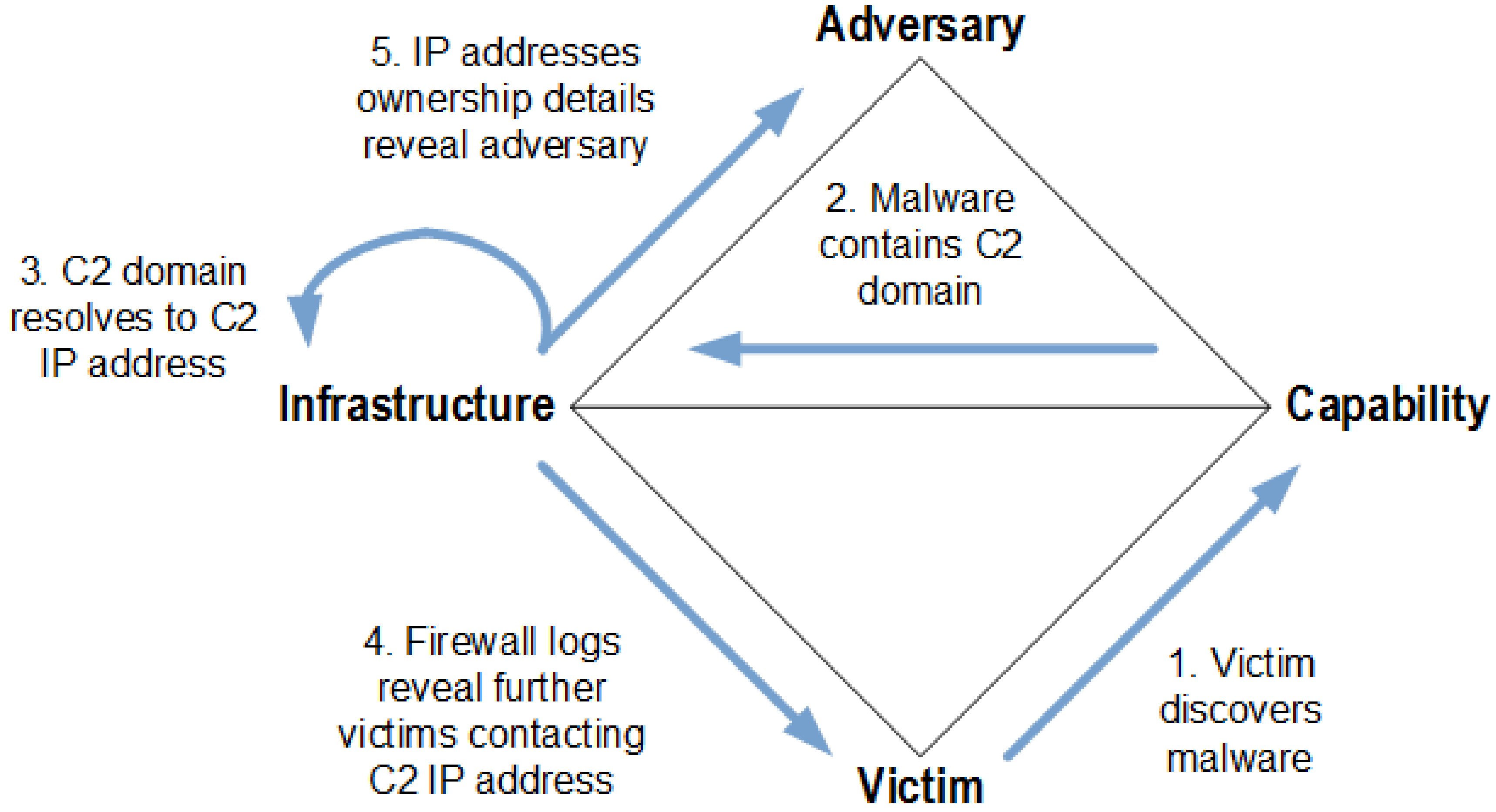
The Diamond Model of Intrusion Analysis. Accessed October 1, 2014. *http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf*

Example Intrusion Indicators

Phase	Indicators
Reconnaissance	[Recipient List] Benign File: tcnom.pdf
Weaponization	Trivial encryption algorithm: Key 1
Delivery	dn...etto@yahoo.com Downstream IP: 60.abc.xyz.215 Subject: AIAA Technical Committees [Email body]
Exploitation	CVE-2009-0658 [shellcode]
Installation	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp
C2	202.abc.xyz.7 [HTTP request]
Actions on Objectives	N/A

Intelligence-Driven Computer Network Defense. Accessed October 1, 2014. *http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf*

The Diamond Model – Analytic Pivoting


Adversary
5. IP addresses ownership details reveal adversary
2. Malware contains C2 domain
3. C2 domain resolves to C2 IP address
Infrastructure
Capability
4. Firewall logs reveal further victims contacting C2 IP address
Victim
1. Victim discovers malware

The Diamond Model of Intrusion Analysis. Accessed October 1, 2014. http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

Putting it all together

Cyber Kill Chain

- progression to track a compromise event

The Diamond Model

- mechanism to provide attribution for threats
- aggregation of activities into a campaign

How?

- Enriched context around attacks
- Multiple sources for enrichment
- Groups common characteristics consistently
- Utilize Indicator Expansion

A Notation for Describing the Steps in Indicator Expansion. Accessed November 7, 2014.

http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=73560

Why Do We Care?

We can more intelligently defend our networks against the threats with our greater understanding.

Questions?

Resources

Alberts, Christopher; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. Defining Incident Management Processes for CSIRTs: A Work in Progress (CMU/SEI-2004-TR-015). Software Engineering Institute, Carnegie Mellon University, 2004. *http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=7153*

J. M. Spring, "A Notation for Describing the Steps in Indicator Expansion," in IEEE eCrime Researchers Summit. Anti-Phishing Working Group, Sep 17, 2013. *http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=73560*

Intelligence analysis - Wikipedia, the free encyclopedia. Accessed October 1, 2014. *http://en.wikipedia.org/wiki/Intelligence_analysis*

Intelligence-Driven Computer Network Defense. Accessed October 1, 2014. *http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf*

Lockheed Martin - Cyber Kill Chain®. Accessed October 1, 2014. *http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html*

Lockheed Martin - Cyber Kill Chain® (MITRE Variant) . Accessed October 1, 2014.

http://nigesecurityguy.wordpress.com/2013/06/04/defensible-security-posture/

The Diamond Model of Intrusion Analysis. Accessed October 1, 2014. http://*www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf*

Contact Information

Timur Snoke
Member of Technical Staff
CERT/CC
Telephone: +1 412-268-5800
Email: netsa-contact@cert.org

U.S. Mail
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

Web
www.cert.org
www.cert.org/contact/