Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Eric M. Hutchins[*], Michael J. Cloppert[†], Rohan M. Amin, Ph.D.[‡]

Lockheed Martin Corporation

Abstract

Conventional network defense tools such as intrusion detection systems and anti-virus focus on the vulnerability component of risk, and traditional incident response methodology presupposes a successful intrusion. An evolution in the goals and sophistication of computer network intrusions has rendered these approaches insufficient for certain actors. A new class of threats, appropriately dubbed the "Advanced Persistent Threat" (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms. Network defense techniques which leverage knowledge about these adversaries can create an intelligence feedback loop, enabling defenders to establish a state of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt. Using a kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering form the basis of intelligence-driven computer network defense (CND). Institutionalization of this approach reduces the likelihood of adversary success, informs network defense investment and resource prioritization, and yields relevant metrics of performance and effectiveness. The evolution of advanced persistent threats necessitates an intelligence-based model because in this model the defenders mitigate not just vulnerability, but the threat component of risk, too.

Keywords: incident response, intrusion detection, intelligence, threat, APT, computer network defense

1 Introduction

As long as global computer networks have existed, so have malicious users intent on exploiting vulnerabilities. Early evolutions of threats to computer networks involved self-propagating code. Advancements over time in anti-virus technology significantly reduced this automated risk. More recently, a new class of threats, intent on the compromise of data for economic or military advancement, emerged as the largest element of risk facing some industries. This class of threat has been given the moniker "Advanced Persistent Threat," or APT. To date, most organizations have relied on the technologies and processes implemented to mitigate risks associated with automated viruses and worms which do not sufficiently address focused, manually operated APT intrusions. Conventional incident response methods fail to mitigate the risk posed by APTs because they make two flawed assumptions: response should happen after the point of compromise, and the compromise was the result of a fixable flaw (Mitropoulos et al., 2006; National Institute of Standards and Technology, 2008).

APTs have recently been observed and characterized by both industry and the U.S. government. In June and July 2005, the U.K. National Infrastructure Security Co-ordination Centre (UK-NISCC) and the U.S.

[*]eric.m.hutchins@lmco.com

[†]michael.j.cloppert@lmco.com

[‡]rohan.m.amin@lmco.com

Computer Emergency Response Team (US-CERT) issued technical alert bulletins describing targeted, socially-engineered emails dropping trojans to exfiltrate sensitive information. These intrusions were over a significant period of time, evaded conventional firewall and anti-virus capabilities, and enabled adversaries to harvest sensitive information (UK-NISCC, 2005; US-CERT, 2005). Epstein and Elgin (2008) of Business Week described numerous intrusions into NASA and other government networks where APT actors were undetected and successful in removing sensitive high-performance rocket design information. In February 2010, iSec Partners noted that current approaches such as anti-virus and patching are not sufficient, end users are directly targeted, and threat actors are after sensitive intellectual property (Stamos, 2010).

Before the U.S. House Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities, James Andrew Lewis of the Center for Strategic and International Studies testified that intrusions occurred at various government agencies in 2007, including the Department of Defense, State Department and Commerce Department, with the intention of information collection (Lewis, 2008). With specificity about the nature of computer network operations reportedly emanating from China, the 2008 and 2009 reports to Congress of the U.S.-China Economic and Security Review Commission summarized reporting of targeted intrusions against U.S. military, government and contractor systems. Again, adversaries were motivated by a desire to collect sensitive information (U.S.-China Economic and Security Review Commission, 2008, 2009). Finally, a report prepared for the U.S.-China Economic and Security Review Commission, Krekel (2009) profiles an advanced intrusion with extensive detail demonstrating the patience and calculated nature of APT.

Advances in infrastructure management tools have enabled best practices of enterprise-wide patching and hardening, reducing the most easily accessible vulnerabilities in networked services. Yet APT actors continually demonstrate the capability to compromise systems by using advanced tools, customized malware, and "zero-day" exploits that anti-virus and patching cannot detect or mitigate. Responses to APT intrusions require an evolution in analysis, process, and technology; it is possible to anticipate and mitigate future intrusions based on knowledge of the threat. This paper describes an intelligence-driven, threat-focused approach to study intrusions from the adversaries' perspective. Each discrete phase of the intrusion is mapped to courses of action for detection, mitigation and response. The phrase "kill chain" describes the structure of the intrusion, and the corresponding model guides analysis to inform actionable security intelligence. Through this model, defenders can develop resilient mitigations against intruders and intelligently prioritize investments in new technology or processes. Kill chain analysis illustrates that the adversary must progress successfully through each stage of the chain before it can achieve its desired objective; just one mitigation disrupts the chain and the adversary. Through intelligence-driven response, the defender can achieve an advantage over the aggressor for APT caliber adversaries.

This paper is organized as follows: section two of this paper documents related work on phase based models of defense and countermeasure strategy. Section three introduces an intelligence-driven computer network defense model (CND) that incorporates threat-specific intrusion analysis and defensive mitigations. Section four presents an application of this new model to a real case study, and section five summarizes the paper and presents some thoughts on future study.

2 Related Work

While the modeling of APTs and corresponding response using kill chains is unique, other phase based models to defensive and countermeasure strategies exist.

A United States Department of Defense Joint Staff publication describes a kill chain with stages find, fix, track, target, engage, and assess (U.S. Department of Defense, 2007). The United States Air Force (USAF) has used this framework to identify gaps in Intelligence, Surveillance and Reconnaissance (ISR) capability and to prioritize the development of needed systems (Tirpak, 2000). Threat chains have also been used to model Improvised Explosive Device (IED) attacks (National Research Council, 2007). The IED delivery chain models everything from adversary funding to attack execution. Coordinated intelligence and defensive efforts focused on each stage of the IED threat chain as the ideal way to counter these attacks. This approach also provides a model for identification of basic research needs by mapping existing capability to the chain. Phase based models have also been used for antiterrorism planning. The United States Army describes the terrorist operational planning cycle as a seven step process that serves as a baseline to assess the intent and capability of terrorist organizations (United States Army Training

and Doctrine Command, 2007). Hayes (2008) applies this model to the antiterrorism planning process for military installations and identifies principles to help commanders determine the best ways to protect themselves.

Outside of military context, phase based models have also been used in the information security field. Sakuraba et al. (2008) describe the Attack-Based Sequential Analysis of Countermeasures (ABSAC) framework that aligns types of countermeasures along the time phase of an attack. The ABSAC approach includes more reactive post-compromise countermeasures than early detection capability to uncover persistent adversary campaigns. In an application of phase based models to insider threats, Duran et al. (2009) describe a tiered detection and countermeasure strategy based on the progress of malicious insiders. Willison and Siponen (2009) also address insider threat by adapting a phase based model called Situational Crime Prevention (SCP). SCP models crime from the offender's perspective and then maps controls to various phases of the crime. Finally, the security company Mandiant proposes an "exploitation life cycle". The Mandiant model, however, does not map courses of defensive action and is based on post-compromise actions (Mandiant, 2010). Moving detections and mitigations to earlier phases of the intrusion kill chain is essential for CND against APT actors.

3 Intelligence-driven Computer Network Defense

Intelligence-driven computer network defense is a risk management strategy that addresses the threat component of risk, incorporating analysis of adversaries, their capabilities, objectives, doctrine and limitations. This is necessarily a continuous process, leveraging indicators to discover new activity with yet more indicators to leverage. It requires a new understanding of the intrusions themselves, not as singular events, but rather as phased progressions. This paper presents a new intrusion kill chain model to analyze intrusions and drive defensive courses of action.

The effect of intelligence-driven CND is a more resilient security posture. APT actors, by their nature, attempt intrusion after intrusion, adjusting their operations based on the success or failure of each attempt. In a kill chain model, just one mitigation breaks the chain and thwarts the adversary, therefore any repetition by the adversary is a liability that defenders must recognize and leverage. If defenders implement countermeasures faster than adversaries evolve, it raises the costs an adversary must expend to achieve their objectives. This model shows, contrary to conventional wisdom, such aggressors have no inherent advantage over defenders.

3.1 Indicators and the Indicator Life Cycle

The fundamental element of intelligence in this model is the *indicator*. For the purposes of this paper, an indicator is any piece of information that objectively describes an intrusion. Indicators can be subdivided into three types:

- **Atomic** - Atomic indicators are those which cannot be broken down into smaller parts and retain their meaning in the context of an intrusion. Typical examples here are IP addresses, email addresses, and vulnerability identifiers.
- **Computed** - Computed indicators are those which are derived from data involved in an incident. Common computed indicators include hash values and regular expressions.
- **Behavioral** - Behavioral indicators are collections of computed and atomic indicators, often subject to qualification by quantity and possibly combinatorial logic. An example would be a statement such as "the intruder would initially used a backdoor which generated network traffic matching [regular expression] at the rate of [some frequency] to [some IP address], and then replace it with one matching the MD5 hash [value] once access was established."

Using the concepts in this paper, analysts will reveal indicators through analysis or collaboration, mature these indicators by leveraging them in their tools, and then utilize them when matching activity is discovered. This activity, when investigated, will often lead to additional indicators that will be subject to the same set of actions and states. This cycle of actions, and the corresponding indicator states, form the indicator life cycle illustrated in Figure 1. This applies to all indicators indiscriminately, regardless of their accuracy or applicability. Tracking the derivation of a given indicator from its predecessors can be

time-consuming and problematic if sufficient tracking isn't in place, thus it is imperative that indicators subject to these processes are valid and applicable to the problem set in question. If attention is not paid to this point, analysts may find themselves applying these techniques to threat actors for which they were not designed, or to benign activity altogether.

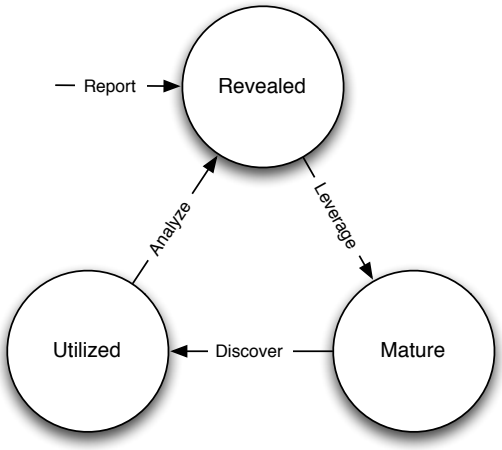

Figure 1: Indicator life cycle states and transitions

3.2 Intrusion Kill Chain

A kill chain is a systematic process to target and engage an adversary to create desired effects. U.S. military targeting doctrine defines the steps of this process as find, fix, track, target, engage, assess (F2T2EA): find adversary targets suitable for engagement; fix their location; track and observe; target with suitable weapon or asset to create desired effects; engage adversary; assess effects (U.S. Department of Defense, 2007). This is an integrated, end-to-end process described as a "chain" because any one deficiency will interrupt the entire process.

Expanding on this concept, this paper presents a new kill chain model, one specifically for intrusions. The essence of an intrusion is that the aggressor must develop a payload to breach a trusted boundary, establish a presence inside a trusted environment, and from that presence, take actions towards their objectives, be they moving laterally inside the environment or violating the confidentiality, integrity, or availability of a system in the environment. The intrusion kill chain is defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives.

With respect to computer network attack (CNA) or computer network espionage (CNE), the definitions for these kill chain phases are as follows:

1. **Reconnaissance** - Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.

2. **Weaponization** - Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.

3. **Delivery** - Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors, as observed by the Lockheed Martin Computer Incident Response Team (LM-CIRT) for the years 2004-2010, are email attachments, websites, and USB removable media.

4. **Exploitation** - After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

5. **Installation** - Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.
6. **Command and Control (C2)** - Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have "hands on the keyboard" access inside the target environment.
7. **Actions on Objectives** - Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.

3.3 Courses of Action

The intrusion kill chain becomes a model for actionable intelligence when defenders align enterprise defensive capabilities to the specific processes an adversary undertakes to target that enterprise. Defenders can measure the performance as well as the effectiveness of these actions, and plan investment roadmaps to rectify any capability gaps. Fundamentally, this approach is the essence of intelligence-driven CND: basing security decisions and measurements on a keen understanding of the adversary.

Table 1 depicts a course of action matrix using the actions of detect, deny, disrupt, degrade, deceive, and destroy from DoD information operations (IO) doctrine (U.S. Department of Defense, 2006). This matrix depicts in the exploitation phase, for example, that host intrusion detection systems (HIDS) can passively *detect* exploits, patching *denies* exploitation altogether, and data execution prevention (DEP) can *disrupt* the exploit once it initiates. Illustrating the spectrum of capabilities defenders can employ, the matrix includes traditional systems like network intrusion detection systems (NIDS) and firewall access control lists (ACL), system hardening best practices like audit logging, but also vigilant users themselves who can detect suspicious activity.

Table 1: Courses of Action Matrix

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	

Here, completeness equates to resiliency, which is the defender's primary goal when faced with persistent adversaries that continually adapt their operations over time. The most notable adaptations are exploits, particularly previously undisclosed "zero-day" exploits. Security vendors call these "zero-day attacks," and tout "zero day protection". This myopic focus fails to appreciate that the exploit is but one change in a broader process. If intruders deploy a zero-day exploit but reuse observable tools or infrastructure

in other phases, that major improvement is fruitless if the defenders have mitigations for the repeated indicators. This repetition demonstrates a defensive strategy of complete indicator utilization achieves resiliency and forces the adversary to make more difficult and comprehensive adjustments to achieve their objectives. In this way, the defender increases the adversary's cost of executing successful intrusions.

Defenders can generate metrics of this resiliency by measuring the performance and effectiveness of defensive actions against the intruders. Consider an example series of intrusion attempts from a single APT campaign that occur over a seven month timeframe, shown in Figure 2. For each phase of the kill chain, a white diamond indicates relevant, but passive, detections were in place at the time of that month's intrusion attempt, a black diamond indicates relevant mitigations were in place, and an empty cell indicates no relevant capabilities were available. After each intrusion, analysts leverage newly revealed indicators to update their defenses, as shown by the gray arrows.

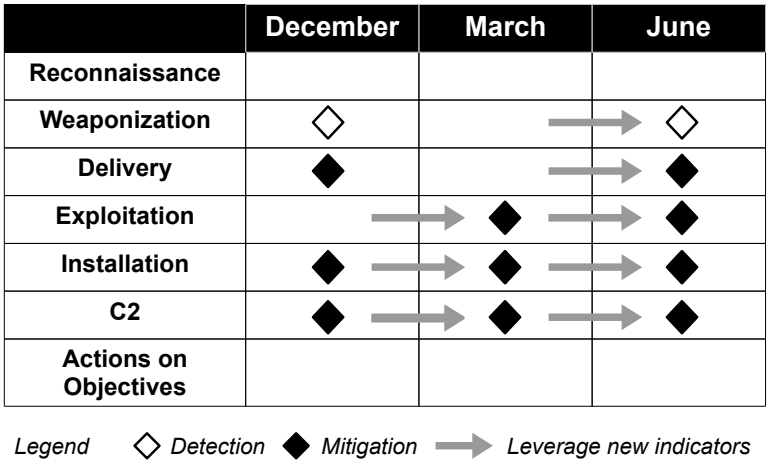

Figure 2: Illustration of the relative effectiveness of defenses against subsequent intrusion attempts

The illustration shows, foremost, that at last one mitigation was in place for all three intrusion attempts, thus mitigations were successful. However, it also clearly shows significant differences in each month. In December, defenders detect the weaponization and block the delivery but uncover a brand new, unmitigated, zero-day exploit in the process. In March, the adversary re-uses the same exploit, but evolves the weaponization technique and delivery infrastructure, circumventing detection and rendering those defensive systems ineffective. By June, the defenders updated their capabilities sufficiently to have detections and mitigations layered from weaponization to C2. By framing metrics in the context of the kill chain, defenders had the proper perspective of the relative effect of their defenses against the intrusion attempts and where there were gaps to prioritize remediation.

3.4 Intrusion Reconstruction

Kill chain analysis is a guide for analysts to understand what information is, and may be, available for defensive courses of action. It is a model to analyze the intrusions in a new way. Most detected intrusions will provide a limited set of attributes about a single phase of an intrusion. Analysts must still discover many other attributes for each phase to enumerate the maximum set of options for courses of action. Further, based on detection in a given phase, analysts can assume that prior phases of the intrusion have already executed successfully. Only through complete analysis of prior phases, as shown in Figure 3, can actions be taken at those phases to mitigate future intrusions. If one cannot reproduce the delivery phase of an intrusion, one cannot hope to act on the delivery phase of subsequent intrusions from the same adversary. The conventional incident response process initiates after our exploit phase, illustrating the self-fulfilling prophecy that defenders are inherently disadvantaged and inevitably too late. The inability to fully reconstruct all intrusion phases prioritizes tools, technologies, and processes to fill this gap.

Defenders must be able to move their detection and analysis up the kill chain and more importantly to implement courses of actions across the kill chain. In order for an intrusion to be economical, adversaries must re-use tools and infrastructure. By completely understanding an intrusion, and leveraging intelligence

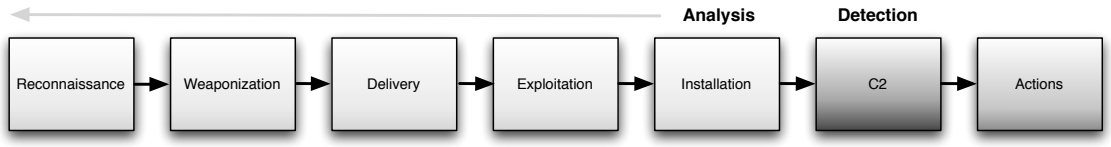

Figure 3: Late phase detection

on these tools and infrastructure, defenders force an adversary to change every phase of their intrusion in order to successfully achieve their goals in subsequent intrusions. In this way, network defenders use the persistence of adversaries' intrusions against them to achieve a level of resilience.

Equally as important as thorough analysis of successful compromises is synthesis of unsuccessful intrusions. As defenders collect data on adversaries, they will push detection from the latter phases of the kill chain into earlier ones. Detection and prevention at pre-compromise phases also necessitates a response. Defenders must collect as much information on the mitigated intrusion as possible, so that they may synthesize what might have happened should future intrusions circumvent the currently effective protections and detections (see Figure 4). For example, if a targeted malicious email is blocked due to re-use of a known indicator, synthesis of the remaining kill chain might reveal a new exploit or backdoor contained therein. Without this knowledge, future intrusions, delivered by different means, may go undetected. If defenders implement countermeasures faster than their known adversaries evolve, they maintain a tactical advantage.

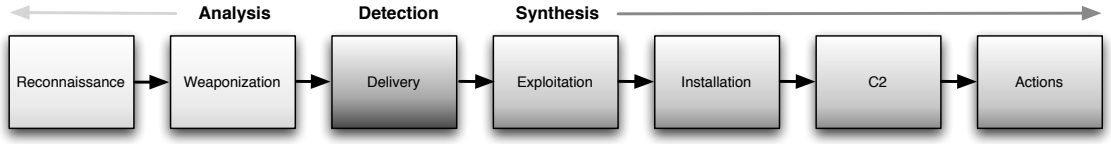

Figure 4: Earlier phase detection

3.5 Campaign Analysis

At a strategic level, analyzing multiple intrusion kill chains over time will identify commonalities and overlapping indicators. Figure 5 illustrates how highly-dimensional correlation between two intrusions through multiple kill chain phases can be identified. Through this process, defenders will recognize and define intrusion campaigns, linking together perhaps years of activity from a particular persistent threat. The most consistent indicators, the campaigns key indicators, provide centers of gravity for defenders to prioritize development and use of courses of action. Figure 6 shows how intrusions may have varying degrees of correlation, but the inflection points where indicators most frequently align identify these key indicators. These less volatile indicators can be expected to remain consistent, predicting the characteristics of future intrusions with greater confidence the more frequently they are observed. In this way, an adversary's persistence becomes a liability which the defender can leverage to strengthen its posture.

The principle goal of campaign analysis is to determine the patterns and behaviors of the intruders, their tactics, techniques, and procedures (TTP), to detect "how" they operate rather than specifically "what" they do. The defender's objective is less to positively attribute the identity of the intruders than to evaluate their capabilities, doctrine, objectives and limitations; intruder attribution, however, may well be a side product of this level of analysis. As defenders study new intrusion activity, they will either link it to existing campaigns or perhaps identify a brand new set of behaviors of a theretofore unknown threat and track it as a new campaign. Defenders can assess their relative defensive posture on a campaign-by-campaign basis, and based on the assessed risk of each, develop strategic courses of action to cover any gaps.

Another core objective of campaign analysis is to understand the intruders' intent. To the extent that defenders can determine technologies or individuals of interest, they can begin to understand the adversarys mission objectives. This necessitates trending intrusions over time to evaluate targeting patterns and closely examining any data exfiltrated by the intruders. Once again this analysis results

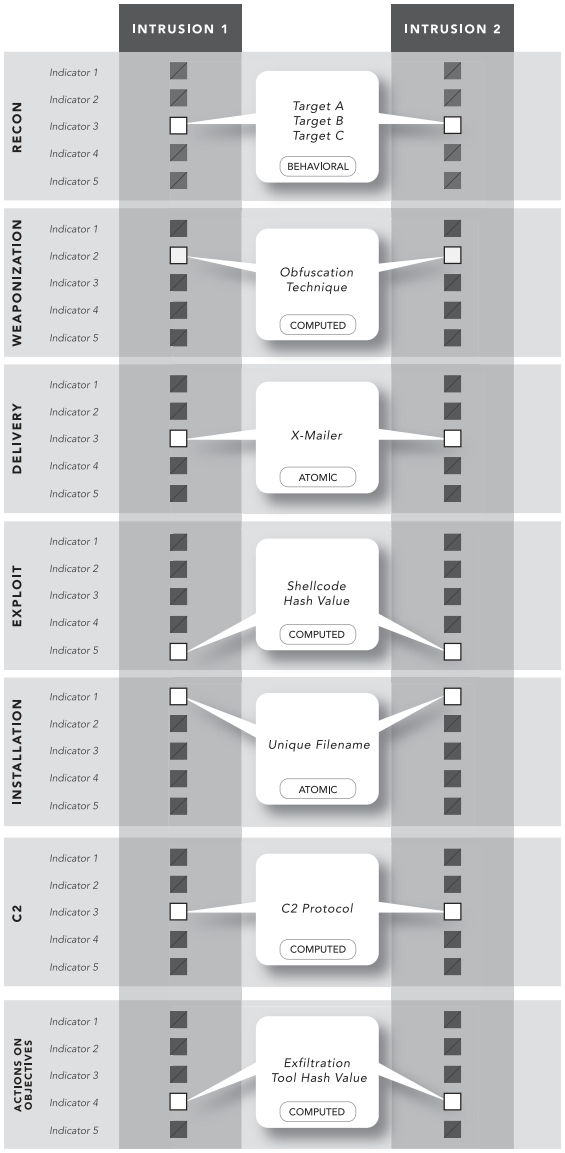

Figure 5: Common indicators between intrusions

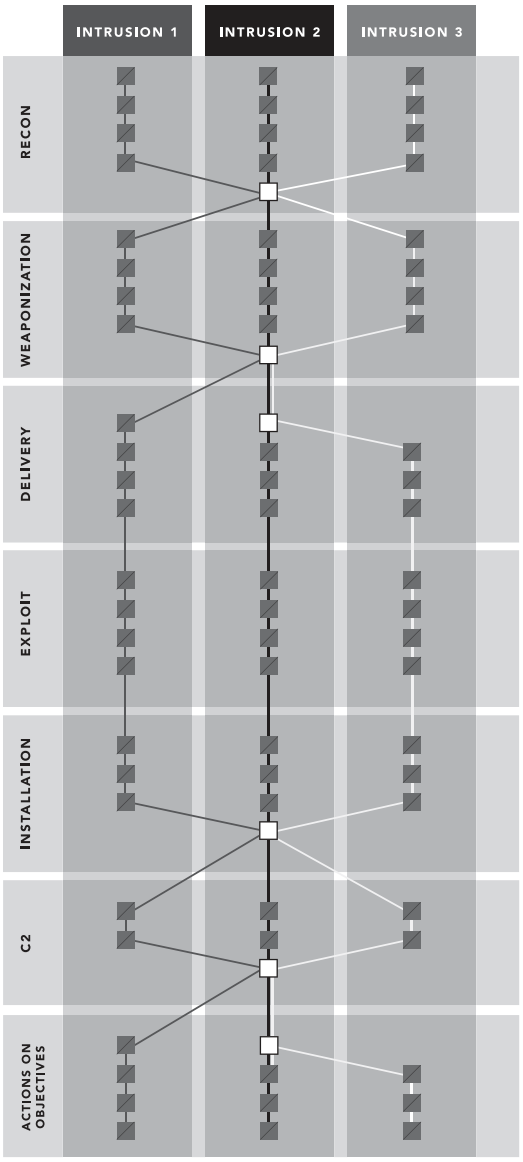

Figure 6: Campaign key indicators

in a roadmap to prioritize highly focused security measures to defend these individuals, networks or technologies.

4 Case Study

To illustrate the benefit of these techniques, a case study observed by the Lockheed Martin Computer Incident Response Team (LM-CIRT) in March 2009 of three intrusion attempts by an adversary is considered. Through analysis of the intrusion kill chains and robust indicator maturity, network defenders successfully detected and mitigated an intrusion leveraging a "zero-day" vulnerability. All three intrusions leveraged a common APT tactic: targeted malicious email (TME) delivered to a limited set of individuals, containing a weaponized attachment that installs a backdoor which initiates outbound communications to a C2 server.

4.1 Intrusion Attempt 1

On March 3, 2009, LM-CIRT detected a suspicious attachment within an email discussing an upcoming American Institute of Aeronautics and Astronautics (AIAA) conference. The email claimed to be from an individual who legitimately worked for AIAA, and was directed to only 5 users, each of whom had received similar TME in the past. Analysts determined the malicious attachment, tcnom.pdf, would exploit a known, but unpatched, vulnerability in Adobe Acrobat Portable Document Format (PDF): CVE-2009-0658, documented by Adobe on February 19, 2009 (Adobe, 2009) but not patched until March 10, 2009. A copy of the email headers and body follow.

```
Received: (qmail 71864 invoked by uid 60001); Tue, 03 Mar 2009 15:01:19 +0000
Received: from [60.abc.xyz.215] by web53402.mail.re2.yahoo.com via HTTP; Tue,
03 Mar 2009 07:01:18 -0800 (PST)
Date: Tue, 03 Mar 2009 07:01:18 -0800 (PST)
From: Anne E... <dn...etto@yahoo.com>
Subject: AIAA Technical Committees
To: [REDACTED]
Reply-to: dn...etto@yahoo.com
Message-id: <107017.64068.qm@web53402.mail.re2.yahoo.com>
MIME-version: 1.0
X-Mailer: YahooMailWebService/0.7.289.1
Content-type: multipart/mixed; boundary="Boundary_(ID_Hq9CkDZSoSvBMukCRm7rsg)"
X-YMail-OSG:

Please submit one copy (photocopies are acceptable) of this form, and one
copy of nominee's resume to: AIAA Technical Committee Nominations,
1801 Alexander Bell Drive, Reston, VA 20191. Fax number is 703/264-
7551. Form can also be submitted via our web site at www.aiaa.org, Inside
AIAA, Technical Committees
```

Within the weaponized PDF were two other files, a benign PDF and a Portable Executable (PE) backdoor installation file. These files, in the process of weaponization, were encrypted using a trivial algorithm with an 8-bit key stored in the exploit shellcode. Upon opening the PDF, shellcode exploiting CVE-2009-0658 would decrypt the installation binary, place it on disk as `C:\Documents and Settings\[username]\Local Settings\fssm32.exe`, and invoke it. The shellcode would also extract the benign PDF and display it to the user. Analysts discovered that the benign PDF was an identical copy of one published on the AIAA website at `http://www.aiaa.org/pdf/inside/tcnom.pdf`, revealing adversary reconnaissance actions.

The installer `fssm32.exe` would extract the backdoor components embedded within itself, saving EXE and HLP files as `C:\Program Files\Internet Explorer\IEUpd.exe` and `IEXPLORE.hlp`. Once active, the backdoor would send heartbeat data to the C2 server 202.abc.xyz.7 via valid HTTP requests. Table 2 articulates the identified, relevant indicators per phase. Due to successful mitigations, the adversary never took actions on objectives, therefore that phase is marked "N/A."

Table 2: Intrusion Attempt 1 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

4.2 Intrusion Attempt 2

One day later, another TME intrusion attempt was executed. Analysts would identify substantially similar characteristics and link this and the previous day's attempt to a common campaign, but analysts also noted a number of differences. The repeated characteristics enabled defenders to block this activity, while the new characteristics provided analysts additional intelligence to build resiliency with further detection and mitigation courses of action.

```
Received: (qmail 97721 invoked by uid 60001); 4 Mar 2009 14:35:22 -0000
Message-ID: <552620.97248.qm@web53411.mail.re2.yahoo.com>
Received: from [216.abc.xyz.76] by web53411.mail.re2.yahoo.com via HTTP; Wed,
04 Mar 2009 06:35:20 PST
X-Mailer: YahooMailWebService/0.7.289.1
Date: Wed, 4 Mar 2009 06:35:20 -0800 (PST)
From: Anne E... <dn...etto@yahoo.com>
Reply-To: dn...etto@yahoo.com
Subject:  7th Annual U.S. Missile Defense Conference
To: [REDACTED]
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="0-760892832-1236177320=:97248"

Welcome to the 7th Annual U.S. Missile Defense Conference
```

The sending email address was common to both the March 3 and March 4 activity, but the subject matter, recipient list, attachment name, and most importantly, the downstream IP address (216.abc.xyz.76) differed. Analysis of the attached PDF, `MDA_Prelim_2.pdf`, revealed an identical weaponization encryption algorithm and key, as well as identical shellcode to exploit the same vulnerability. The PE installer in the PDF was identical to that used the previous day, and the benign PDF was once again an identical copy of a file on AIAA's website (`http://www.aiaa.org/events/missiledefense/MDA_Prelim_09.pdf`). The adversary never took actions towards its objectives, therefore that phase is again marked "N/A." A summary of indicators from the first two intrusion attempts is provided in Table 3.

Table 3: Intrusion Attempts 1 and 2 Indicators

Phase	Intrusion 1	Intrusion 2
Reconnaissance	[Recipient List] Benign File: tcnom.pdf	[Recipient List] Benign File: MDA_Prelim_09.pdf
Weaponization	Trivial encryption algorithm: Key 1	
Delivery	Downstream IP: 60.abc.xyz.215 Subject: AIAA Technical Committees [Email body]	Downstream IP: 216.abc.xyz.76 Subject: 7th Annual U.S. Missile Defense Conference [Email body]
	dn...etto@yahoo.com	
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	N/A

4.3 Intrusion Attempt 3

Over two weeks later, on March 23, 2009, a significantly different intrusion was identified due to indicator overlap, though minimal, with Intrusions 1 and 2. This email contained a PowerPoint file which exploited a vulnerability that was not, until that moment, known to the vendor or network defenders. The vulnerability was publicly acknowledged 10 days later by Microsoft as security advisory 969136 and identified as CVE-2009-0556 (Microsoft, 2009b). Microsoft issued a patch on May 12, 2009 (Microsoft, 2009a). In this campaign, the adversary made a significant shift in using a brand new, "zero-day" exploit. Details of the email follow.

```
Received: (qmail 62698 invoked by uid 1000); Mon, 23 Mar 2009 17:14:22 +0000
Received: (qmail 82085 invoked by uid 60001); Mon, 23 Mar 2009 17:14:21 +0000
Received: from [216.abc.xyz.76] by web43406.mail.sp1.yahoo.com via HTTP; Mon,
23 Mar 2009 10:14:21 -0700 (PDT)
Date: Mon, 23 Mar 2009 10:14:21 -0700 (PDT)
From: Ginette C... <ginette.c...@yahoo.com>
Subject: Celebrities Without Makeup
To: [REDACTED]
Message-id: <297350.78665.qm@web43406.mail.sp1.yahoo.com>
MIME-version: 1.0
X-Mailer: YahooMailClassic/5.1.20 YahooMailWebService/0.7.289.1
Content-type: multipart/mixed; boundary="Boundary_(ID_DpBDtBoPTQ1DnYXw29L2Ng)"

<email body blank>
```

This email contained a new sending address, new recipient list, markedly different benign content displayed to the user (from "missile defense" to "celebrity makeup"), and the malicious PowerPoint attachment contained a completely new exploit. However, the adversaries used the same downstream IP address, 216.abc.xyz.76, to connect to the webmail service as they used in Intrusion 2. The PowerPoint file was weaponized using the same algorithm as the previous two intrusions, but with a different 8-bit key. The PE installer and backdoor were found to be identical to the previous two intrusions. A summary of indicators from all three intrusions is provided in Table 4.

Leveraging intelligence on adversaries at the first intrusion attempt enabled network defenders to prevent a known zero-day exploit. With each consecutive intrusion attempt, through complete analysis, more indicators were discovered. A robust set of courses of action enabled defenders to mitigate subsequent

Table 4: Intrusion Attempts 1, 2, and 3 Indicators

Phase	Intrusion 1	Intrusion 2	Intrusion 3
Reconnaissance	[Recipient List] Benign PDF	[Recipient List] Benign PDF	[Recipient List] Benign PPT
Weaponization	Trivial encryption algorithm		
	Key 1		Key 2
Delivery	[Email subject] [Email body]	[Email subject] [Email body]	[Email subject] [Email body]
	dn...etto@yahoo.com		ginette.c...@yahoo.com
	60.abc.xyz.215	216.abc.xyz.76	
Exploitation	CVE-2009-0658 [shellcode]		[PPT 0-day] [shellcode]
Installation	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp		
C2	202.abc.xyz.7 [HTTP request]		
Actions on Objectives	N/A	N/A	N/A

intrusions upon delivery, even when adversaries deployed a previously-unseen exploit. Further, through this diligent approach, defenders forced the adversary to avoid all mature indicators to successfully launch an intrusion from that point forward.

Following conventional incident response methodology may have been effective in managing systems compromised by these intrusions in environments completely under the control of network defenders. However, this would not have mitigated the damage done by a compromised mobile asset that moved out of the protected environment. Additionally, by only focusing on post-compromise effects (those after the Exploit phase), fewer indicators are available. Simply using a different backdoor and installer would circumvent available detections and mitigations, enabling adversary success. By preventing compromise in the first place, the resultant risk is reduced in a way unachievable through the conventional incident response process.

5 Summary

Intelligence-driven computer network defense is a necessity in light of advanced persistent threats. As conventional, vulnerability-focused processes are insufficient, understanding the threat itself, its intent, capability, doctrine, and patterns of operation is required to establish resilience. The intrusion kill chain provides a structure to analyze intrusions, extract indicators and drive defensive courses of actions. Furthermore, this model prioritizes investment for capability gaps, and serves as a framework to measure the effectiveness of the defenders' actions. When defenders consider the threat component of risk to build resilience against APTs, they can turn the persistence of these actors into a liability, decreasing the adversary's likelihood of success with each intrusion attempt.

The kill chain shows an asymmetry between aggressor and defender, any one repeated component by the aggressor is a liability. Understanding the nature of repetition for given adversaries, be it out of convenience, personal preference, or ignorance, is an analysis of cost. Modeling the cost-benefit ratio to intruders is an area for additional research. When that cost-benefit is decidedly imbalanced, it is perhaps an indicator of information superiority of one group over the other. Models of information superiority may be valuable for computer network attack and exploitation doctrine development. Finally, this paper presents an intrusions kill chain model in the context of computer espionage. Intrusions may represent a broader problem class. This research may strongly overlap with other disciplines, such as IED countermeasures.

References

Adobe. APSA09-01: Security Updates available for Adobe Reader and Acrobat versions 9 and earlier, February 2009. URL http://www.adobe.com/support/security/advisories/apsa09-01.html.

F. Duran, S. H. Conrad, G. N. Conrad, D. P. Duggan, and E. B. Held. Building A System For Insider Security. *IEEE Security & Privacy*, 7(6):30–38, 2009. doi: 10.1109/MSP.2009.111.

Keith Epstein and Ben Elgin. Network Security Breaches Plague NASA, November 2008. URL http://www.businessweek.com/print/magazine/content/08_48/b4110072404167.htm.

LTC Ashton Hayes. Defending Against the Unknown: Antiterrorism and the Terrorist Planning Cycle. *The Guardian*, 10(1):32–36, 2008. URL http://www.jcs.mil/content/files/2009-04/041309155243_spring2008.pdf.

Bryan Krekel. Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, October 2009. URL http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

James Andrew Lewis. Holistic Approaches to Cybersecurity to Enable Network Centric Operations, April 2008. URL http://armedservices.house.gov/pdfs/TUTC040108/Lewis_Testimony040108.pdf.

Mandiant. M-Trends: The Advanced Persistent Threat, January 2010. URL http://www.mandiant.com/products/services/m-trends.

Microsoft. Microsoft Security Bulletin MS09-017: Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340), May 2009a. URL http://www.microsoft.com/technet/security/bulletin/ms09-017.mspx.

Microsoft. Microsoft Security Advisory (969136): Vulnerability in Microsoft Office PowerPoint Could Allow Remote Code Execution, April 2009b. URL http://www.microsoft.com/technet/security/advisory/969136.mspx.

Sarandis Mitropoulos, Dimitrios Patsosa, and Christos Douligeris. On Incident Handling and Response: A state-of-the-art approach. *Computers & Security*, 5:351–370, July 2006. URL http://dx.doi.org/10.1016/j.cose.2005.09.006.

National Institute of Standards and Technology. Special Publication 800-61: Computer Security Incident Handling Guide, March 2008. URL http://csrc.nist.gov/publications/PubsSPs.html.

National Research Council. Countering the Threat of Improvised Explosive Devices: Basic Research Opportunities (Abbreviated Version), 2007. URL http://books.nap.edu/catalog.php?record_id=11953.

T. Sakuraba, S. Domyo, Bin-Hui Chou, and K. Sakurai. Exploring Security Countermeasures along the Attack Sequence. In *Proc. Int. Conf. Information Security and Assurance ISA 2008*, pages 427–432, 2008. doi: 10.1109/ISA.2008.112.

Alex Stamos. "Aurora" Response Recommendations, February 2010. URL https://www.isecpartners.com/files/iSEC_Aurora_Response_Recommendations.pdf.

John A. Tirpak. Find, Fix, Track, Target, Engage, Assess. *Air Force Magazine*, 83:24–29, 2000. URL http://www.airforce-magazine.com/MagazineArchive/Pages/2000/July%202000/0700find.aspx.

UK-NISCC. National Infrastructure Security Co-ordination Centre: Targeted Trojan Email Attacks, June 2005. URL https://www.cpni.gov.uk/docs/ttea.pdf.

United States Army Training and Doctrine Command. A Military Guide to Terrorism in the Twenty-First Century, August 2007. URL http://www.dtic.mil/srch/doc?collection=t3&id=ADA472623.

US-CERT. Technical Cyber Security Alert TA05-189A: Targeted Trojan Email Attacks, July 2005. URL http://www.us-cert.gov/cas/techalerts/TA05-189A.html.

U.S.-China Economic and Security Review Commission. 2008 Report to Congress of the U.S.-China Economic and Security Review Commission, November 2008. URL http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf.

U.S.-China Economic and Security Review Commission. 2009 Report to Congress of the U.S.-China Economic and Security Review Commission, November 2009. URL http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf.

U.S. Department of Defense. Joint Publication 3-13 Information Operations, February 2006. URL http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

U.S. Department of Defense. Joint Publication 3-60 Joint Targeting, April 2007. URL http://www.dtic.mil/doctrine/new_pubs/jp3_60.pdf.

Robert Willison and Mikko Siponen. Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM*, 52(9):133–137, 2009. doi: http://doi.acm.org/10.1145/1562164.1562198.