Cyber Kill Chain

Mariano Ceccato

mariano.ceccato@univr.it

Attacks in the past

- Malicious users willing to exploit vulnerabilities existed since the beginning of global computer networks
- Initially, self-propagating code
- Anti-virus technology significantly reduced this automated risk

Modern day attackers

- A new class of threats, aiming at the compromising data for economic or military advancement
- Adversaries are more sophisticated, well-resourced, trained
  - Demonstrated their willingness to conduct destructive attacks
  - Their tools and techniques could defeat most common computer network defense mechanisms.
- Skillfully planned intrusion campaigns called **Advanced Persistent Threats** (APT)
- Nations security and prosperity depend on critical infrastructure
  - Protecting these assets requires a clear understanding of adversaries, their motivations and strategies.

Advanced Persistent Threats

- Conventional incident response methods fail to mitigate the risk posed by APTs
- Two invalid assumptions:
  - response should happen after the point of compromise
  - compromise was the result of a fixable flaw

Few examples

- June 2005
  - U.K. National Infrastructure Security Co-ordination Centre (UK-NISCC)
  - U.S. Computer Emergency Response Team (US-CERT)
- 2008
  - NASA (sensitive high-performance rocket design information)

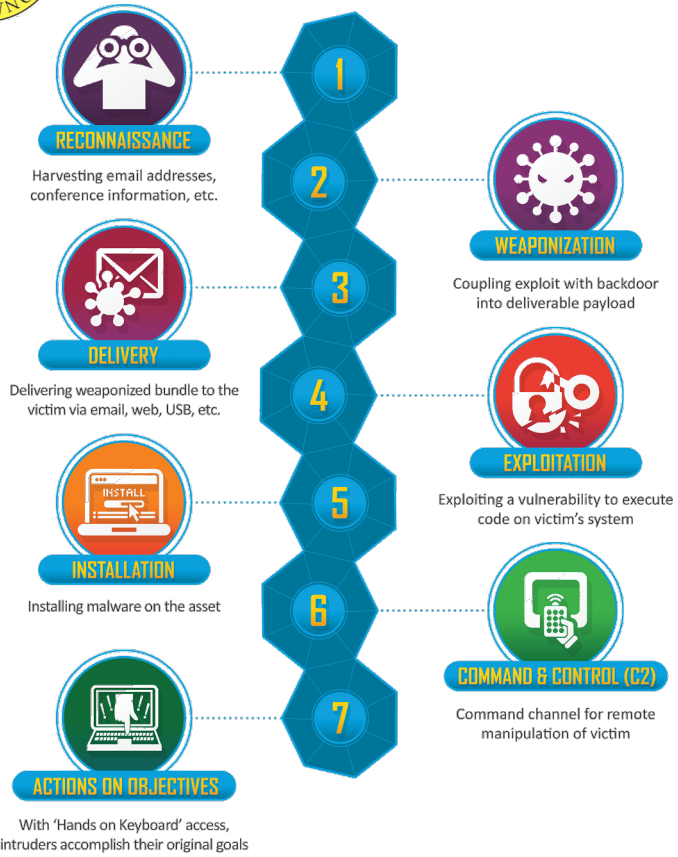
- Socially-engineered emails dropping trojans to exfiltrate sensitive information
  - Evaded conventional firewall and anti-virus capabilities
  - Enabled adversaries to harvest sensitive information
  - End users are directly targeted

How to cope with APT

- Attackers continually demonstrate the capability to compromise systems by using advanced tools
  - customized malware
  - “zero-day” exploits
  - 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
  - Intelligence-driven, threat-focused approach to study intrusions from the adversaries’ perspective
  - Defenders can develop resilient mitigations against intruders and intelligently prioritize investments in new technology or processes.

Cyber kill chain



- A model for the identification and prevention of cyber intrusions activity
- The model identifies what the adversaries must complete in order to achieve their objective
- Stopping adversaries at any stage breaks the chain of attack!
- Every intrusion is a chance to understand more about our adversaries and use their persistence to our advantage.

Cyber kill chain process

- Incorporating analysis of adversaries, capabilities, objectives, doctrine and limitations
- Continuous process to discover new activity
- New understanding of the intrusions themselves, not as singular events, but rather as phased progressions

- Model for actionable intelligence when defenders align enterprise defensive capabilities to the specific processes an adversary undertakes to target that enterprise
- Objective: base security decisions and measurements on a keen understanding of the adversary.

Example

- A “zero-day” vulnerability is exploited to attack a computer system
  - E.g., a PDF file that attack the corporate PDF-reader
- No patch and no attack signature is available to defenders

- In case attackers reuse observable tools or infrastructure to deply a “zero-day” attack
  - E.g., a known IP or sender to dispatch malicious emails
- defenders have mitigations for the repeated indicators

Reconnaissance

Harvesting email addresses, conference information, etc.

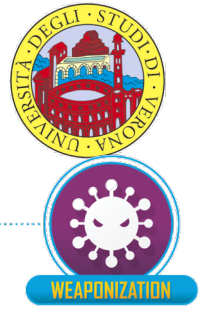
- **Goal:** Select and gather information about the target

- **Passive:** gather information without interacting with target
  - **Tools**: whois, Shodan, Google, Social Media
  - **Other sources**: press releases, conference attendance list

- **Active**: gather information with interacting with target
  - **Tools**: nmap, port scanning, vulnerability scanners

Reconnaissance

- **Defender:**
  - Detecting reconnaissance as it happens can be very difficult
  - When defenders discover recon (even well after the fact) it can reveal the intent of the adversaries
    - Website visitor logs for alerting and historical searching
    - Detections for browsing behaviors
    - Prioritize defenses based on recon activity.



Weaponization

- **Goal**: Find or create the deliverable attack to exploit a weakness
- **Tools:**
  - Metasploit
  - Exploit DB
  - Veil Framework
  - Social Engineering Toolkit
  - Cain and Abel
  - Aircrack
  - SQL Map

Weaponization

- **Defender**:
  - Cannot detect weaponization as it happens
  - Can infer by analyzing malware artifacts.
    - full malware analysis – not just what payload it drops, but how it was made
    - find new campaigns and new payloads - weaponizer toolkits are reused
    - Collect files and metadata for future analysis.
    - Determine which weaponizer artifacts are common to which APT campaigns.

Deliver

- **Goal:** Select which venue to deliver the exploit

Delivering weaponized bundle to the victim via email, web, USB, etc.

Web site

Email

USB

Social Media

Deliver

- **Defender:** most important opportunity to block the operation
  - Analyze delivery medium – understand upstream infrastructure.
  - Understand targeted servers and people, their roles and responsibilities, what information is available
  - Infer intent of adversary based on targeting
  - Leverage weaponizer artifacts to detect new malicious payloads at the point of Delivery
  - Analyze time of day of when operation began
  - Collect email and web logs for forensic reconstruction
    - Even if an intrusion is detected late, defenders must be able to determine when and how delivery began.

Exploitation

- **Goal:** Exploit an existing vulnerability (application or OS vulnerability) to gain access
- **Examples:**
  - SQL Injection
  - Buffer overflow
  - Malware
  - Javascript hijacking
  - User exploitation
  - OS feature to auto-execute code

Exploitation

- **Defender:**
  - User awareness
  - Secure coding training for developers
  - Regular vulnerability scanning and penetration testing
  - Endpoint hardening measures:
    - Restrict admin privileges
    - Use Microsoft EMET (Enhanced Mitigation Experience Toolkit)
    - Custom endpoint rules to block shellcode execution
  - Endpoint process auditing to forensically determine origin of exploit.

Installing malware on the asset

Installation

- **Goal:** Maintain persistence inside the environment
- **Techniques:**
  - DLL Hijacking
  - Meterpreter (interactive shell using Metasploit)
  - Remote Access Trojan
  - Registry Changes
  - PowerShell commands
  - Webshell on web server

Installation

- **Defender:** Endpoint instrumentation to detect and log installation activity
  - Alert or block on common installation paths
  - Auditing to discover abnormal file creations
  - Certificates of any signed executables.

Command and Control (C2)

Command channel for remote manipulation of victim

- **Goal:** Establish a command and control channel (C2) with the attacker to remotely manipulate the victim
  - "Hands on the keyboard" access inside the target environment.
- **Examples:**
  - Open two way communications channel to C2 infrastructure
  - Most common C2 channels are over web, DNS, and email protocols
  - C2 infrastructure may be adversary owned or another victim network itself

Command and Control (C2)

- **Defender:** by blocking the C2 channel is the last chance to block the operation
  - Discover C2 infrastructure thorough malware analysis.
  - Harden network, e.g., require proxies for all types of traffic (HTTP, DNS)
  - Conduct open source research to discover new adversary C2 infrastructure.

Actions and Objectives

- **Goal:** Take actions to achieve their original objectives
- **Possible actions:**
  - Collect user credentials
  - Privilege escalation
  - Internal reconnaissance
  - Lateral movement through environment
  - Collect and exfiltrate data
  - Destroy systems
  - Overwrite or corrupt data
  - Surreptitiously modify data

Actions and Objectives

- **Defender:** detect this stage as quickly as possible by using forensic evidence, for damage assessment
  - Detect data exfiltration, lateral movement, unauthorized credential usage
  - Network package capture to recreate activity
  - Conduct damage assessment with subject matter experts.

Course of actions

- Model for actionable intelligence
- Defenders align enterprise defensive capabilities to the specific processes an adversary undertakes to target that enterprise
- Defenders can measure the performance and the effectiveness of these actions
- Defenders can plan investment roadmaps to rectify any capability gaps

Example

- Context: U.S. Department of Defense, 2006

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	

Host intrusion detection systems (HIDS) can passively detect exploits

patching denies exploitation

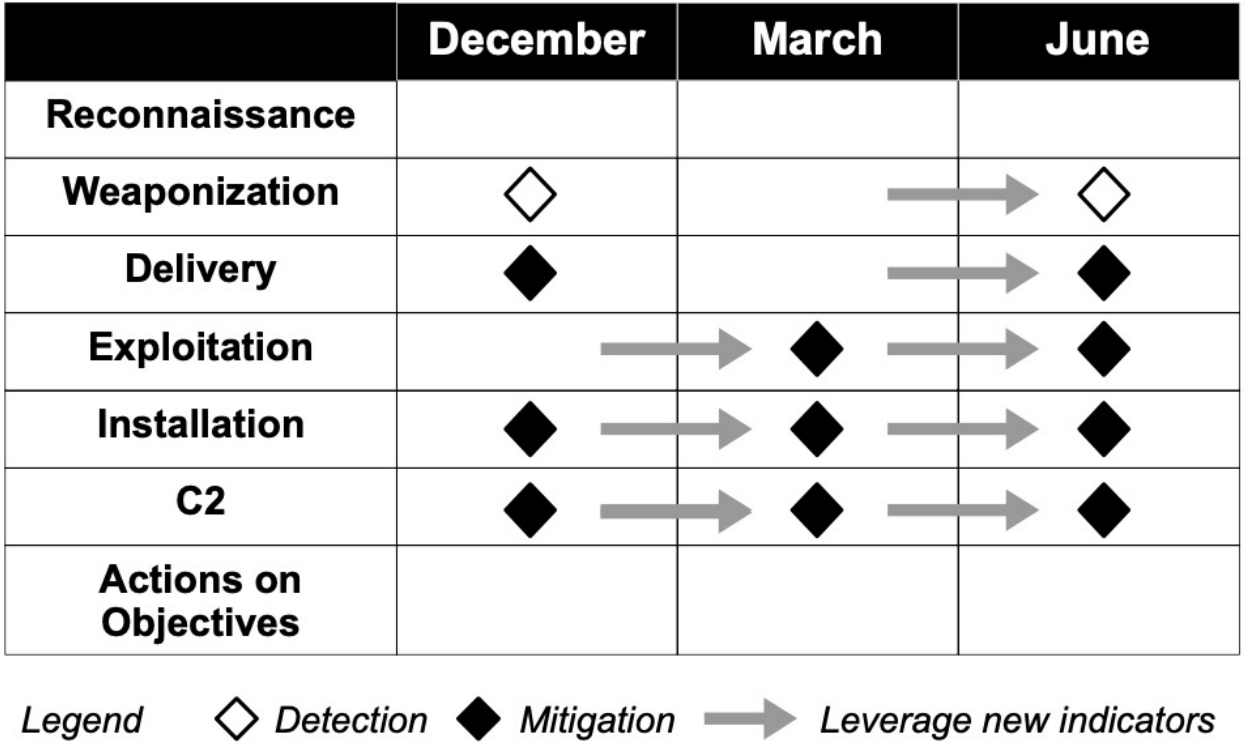
data execution prevention (DEP) can disrupt the exploit once it initiates

Best practices

Long-lasting process

- Analysis of multiple intrusion cyber kill chains over time draws attention to similarities and overlapping indicators
- Defenders learn to recognize and define intrusion campaigns and understand the intruder's mission objectives
  - what are they looking for, why are they targeting me?
- This will help identify how to best protect yourself from the next attack.
  - You can't get ahead of the threat unless you understand the campaign.
  - The threats will come back again. Learn how they got in and block it for the future.

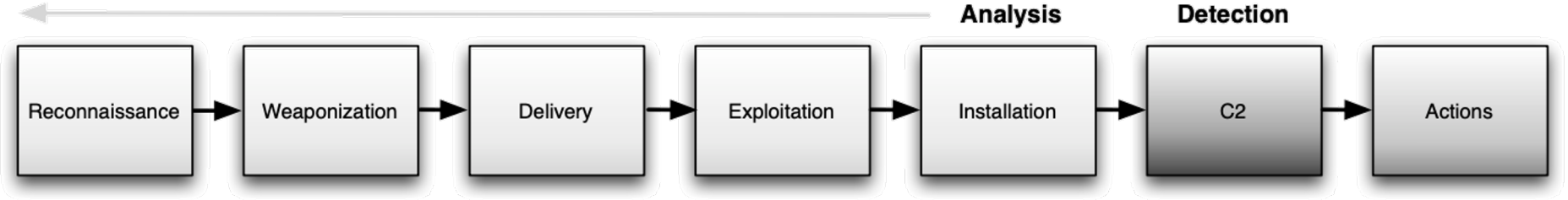
Example - a series of intrusion attempts



Intrusion reconstruction

- Based on detection in a given phase, analysts can assume that prior phases of the intrusion have already executed successfully
- Complete analysis of prior phases is needed to take actions 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.

- In order for an intrusion to be economical, adversaries must re-use tools and infrastructure.
- By completely understanding an intrusion, and leveraging intelligence 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.



Case study

- Observed by the Lockheed Martin Computer Incident Response Team (LM-CIRT) in March 2009
- 3 intrusion attempts by an adversary
- Using analysis of the intrusion cyber kill chains, network defenders successfully detected and mitigated an intrusion leveraging a “zero-day” vulnerability

- APT tactic:
  - Targeted malicious email (TME) delivered to a limited set of individuals
  - Emails contained a weaponized attachment that installs a backdoor
  - It initiates outbound communications to a C2 server

Intrusion attempt 1: March 3rd, 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 (Target Malicious Emails) 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.

The fishing email

```
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
```

The attack

- Encrypted using a trivial algorithm with an 8-bit key stored in the exploit shellcode
- When opening the file, shellcode would
  - Decrypt the binary
  - Save it as C:\Documents and Settings\[username] \Local Settings\fssm32.exe, saving EXE and HLP files as C:\Program Files\Internet Explorer\IEUpd.exe and IEXPLORE.hlp.
  - Invoke it
    - Connect to C2 server 202.abc.xyz.7 via valid HTTP requests.
  - Display the benign PDF: same file from AIAA website revealing adversary reconnaissance actions

The Cyber Kill Chain of the attack

- **Reconnaissance**
  - Email address and benign pdf file
- **Weaponization**
  - Malicious PDF, Encryption Key
- **Delivery**
  - Phishing email with the attachment
- **Exploitation**
  - CVE-2009-0658 Buffer overflow (shellcode)
- **Installation**
  - C:\...\fssm32.exe, C:\...\IEUpd.exe, C:\...\IEXPLORE.hlp
- **C2**
  - HTTP Request to 202.abc.xyz.7

Intrusion attempt 2: next day

```
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 Cyber Kill Chain of the 2 attacks

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

Intrusion attempt 3: March 23rd

```
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>
```

Significant shift: “zero-day” exploit

- The mail contained a PowerPoint file which exploited a vulnerability that was not known to the vendor or network defenders
  - Publicly acknowledged 10 days later by Microsoft as security advisory 969136 and identified as CVE-2009-0556
  - Microsoft issued a patch on May 12, 2009

Differences than previous attempts

- New email sending address
- New recipient list
- Different benign content displayed to the user (from “missile defense” to “celebrity makeup”),
- Malicious PowerPoint attachment contained a completely new exploit

Similarities with previous attempts

- Same downstream IP address, 216.abc.xyz.76, to connect to the webmail service (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 installer and backdoor were identical to the previous two intrusions

Leveraging intelligence on adversaries at the first intrusion attempt enabled network defenders to prevent a known zero-day exploit.

The Cyber Kill Chain of the 3 attacks

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

Summary

- Conventional, vulnerability-focused processes are insufficient
- Understanding the threat, its intent, capability, doctrine, and patterns of operation is required to establish resilience
- The intrusion cyber kill chain supports analysis of intrusions and drive defensive courses of actions.

Resources

- Eric M. Hutchins, Michael J. Clopperty, Rohan M. Amin, Ph.D.z. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.