Cyber Defense Overview

Attack Patterns Aligned to Cyber Kill Chain

John Franco
Electrical Engineering and Computing Systems

Attackers Leave Trails

Stages of Attack (Cyber kill Chain):

Reconnaissance: gather information on the target
social media, email addresses, intellectual property

Weaponization: trojan coupled with exploitable application
weaponized deliverable: adobe pdf, MS office documents

Delivery: get the weapon to the target environment
email attachments, USB removable media, websites

Exploitation: intruder's code activated, auto-exec'ed by OS?

Installation/spread: backdoor or trojan, persistence
hide existence from security devices

Command & Control: channels to send and receive info

Accomplish Mission: theft of money, theft of IP, destruction
exfiltration: collect, encrypt, extract info from target
use target to compromise other machines

Defender Capabilities

Defensible Actions:

- **Detect:** verify that some attacker is looking around
- **Deny:** prevent the attacker from gaining information
- **Disrupt:** stop or change outbound traffic (to attacker)
- **Degrade:** attack attacker's command & control
- **Deceive:** interfere with command & control
- **Contain:** network segmentation changes

Defender Tools

Mostly Review:

NIDS: Network Intrusion Detection

NIPS: Network Intrusion Prevention

HIDS: Host Intrusion Detection

EPP: Endpoint Protection Platform
Firewall, anti-virus, anti-spyware, behavioral blocking

ACL: Access Control List

AV: anti-virus

DNS Redirect: serve different web page than was requested
Attacker may seek CC channel through page with malware
But redirection may kill this chance

DLP: Data Loss Prevention
Stop exfiltration to untrusted locations, control what data users can transfer

Defender Tools

Mostly Review:

Tarpit: purposeful introduction of delays to network traffic
idea: bad guys may give up if things are taking too long

Honeypot: seems to belong to but is isolated from network
idea: divert malicious traffic to protect and to discover attack intentions

chroot jail: change root directory of current running process
idea: limit access of process to data and software

Proxy filter: intermediary for client requests
idea: hide network information from the attacker

Quality of Service: classify traffic - how to treat?; level of traffic; check for bottlenecks, selectively drop packets;

Trust Zones: level of trust associated with system parts

Queuing: form of tarpit on incoming traffic

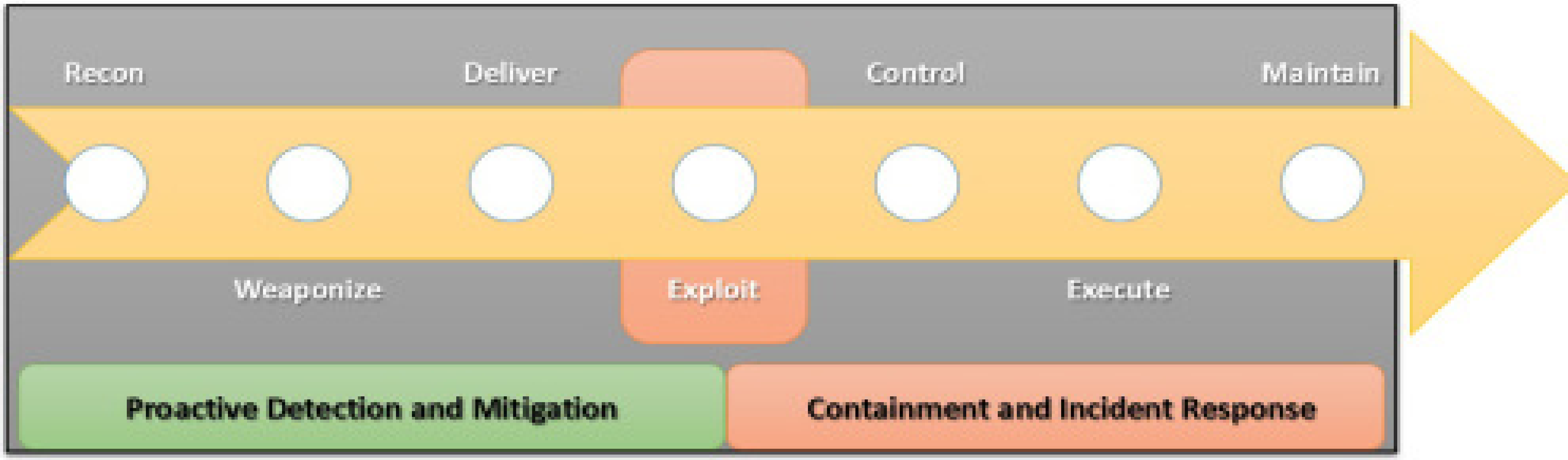
Defensible Actions Matrix
Aligned to the Cyber Kill Chain

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Contain
Reconnaissance	Web Analytics	Firewall ACL				Firewall ACL
Weaponization	NIDS	NIPS				NIPS
Delivery	Vigilant User	Proxy Filter	Inline AV	Queuing		App-Aware Firewall
Exploitation	HIDS	Patch	DEP			Inter-Zone NIPS
Installation	HIDS	'*chroot*' Jail	AV			EPP
Command & Control	NIDS	Firewall ACL	NIPS	Tarpit	DNS Redirect	Trust Zones
Actions on Targets	Audit Logs	Outbound ACL	DLP	Quality of Service	Honeypot	Trust Zones

Cost to adversary increases as more indicators are revealed, used

From: Defensible Security Posture, Nige the Security Guy

Security Control Types
Aligned to the Cyber Kill Chain



From: Defensible Security Posture, Nige the Security Guy

Attack Patterns

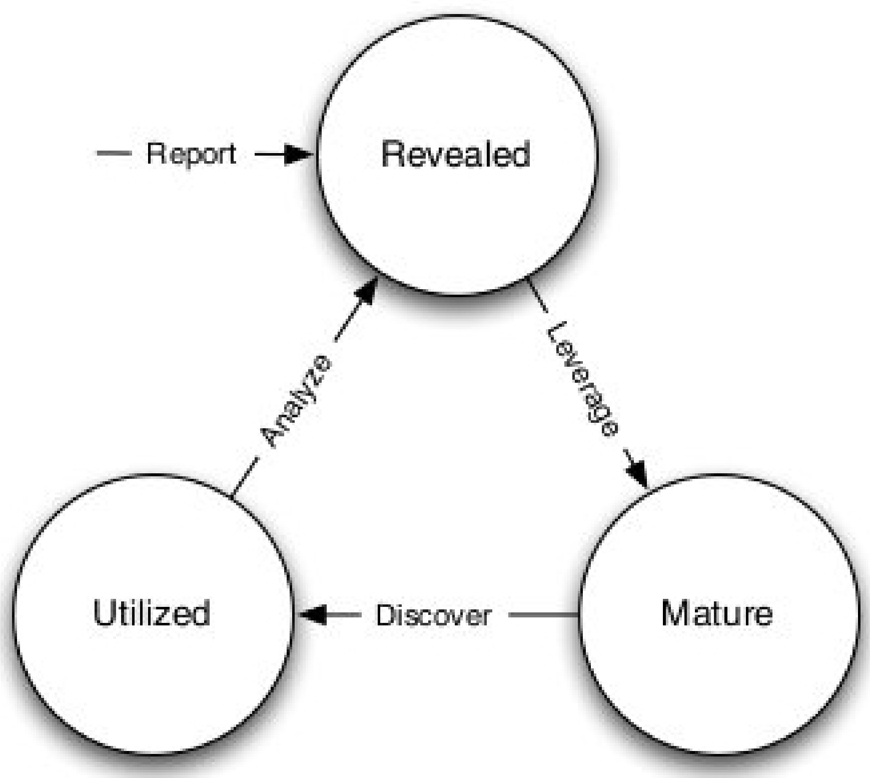
Indicators:

- any piece of information that describes an intrusion
- **atomic:**
  ip addresses, email addresses, vulnerability identifiers
- **computed:**
  * derived from data collected during an incident
  * e.g. hash values
- **behavioral:**
  * collections of atomic and computed indicators
  * AI over the aggregate is used to suggest mal behaviors
  * rule example:
    "intruder initially uses a backdoor to generate network traffic matching [regular expression] at the rate of [some frequency] to [some IP address], and then replaces it with a module matching the MD5 hash [value] once access was established"

Attack Patterns

Indicators:

- analysts reveal indicators through analysis or collaboration
- mature indicators by leveraging them in tools
- utilize them when matching activity is discovered
- form additional indicators subject to same actions and states



Attack Patterns

Reconnaissance and weaponization:

- sudden increase in network traffic (analytics/firewall)
- sudden increase in outbound transfers (analytics/firewall)
- unusual patterns of activity (analytics/firewall to stop)
  * large transfers of data outside normal office hours
  * large transfers to unusual locations
- unusual searches of directories, files of interest to attacker
  * source code repositories (NSM/firewall to stop)
- unrecognized, large outbound files that have been compressed, encrypted password-protected
- scans (NSM/firewalls)
- increased volume of IDS events/alerts (NSM/firewall)

Attack Patterns

Delivery:

- vulnerable UDP/TCP port used to load malware (NIDS/NIPS) communication channel established with master controller
- repeated queries to dynamic DNS names
- use URL filtering (outbound – deny access to sites) and DNS monitoring (inbound) to discover/deny attacker access
  * if new attack, protection is built on-the-fly while the UDP port is under repair
  * other enterprises should be warned

Attack Patterns

Exploitation:

- unexplained changes in configurations of platforms, routers or firewalls

Attack Patterns

Installation:

- DNS server is set up as a launching point for finding other vulnerable hosts
- Unusual traffic between servers that usually don’t talk to one another can be detected, examined, blocked by intelligent sensors

Attack Patterns

Command and Control:

- inbound commands are sent to the exploited DNS server which returns outbound traffic and/or begins identifying other vulnerable devices within the organization to exploit.
- changes to the system show up in logs and traffic reports
- intelligent tools pick up and report on unusual connections between servers and devices, to-from locations
- types of traffic and the ports used show up in logs
- tools capture suspect traffic between the servers for further examination, including decrypting packets and examining contents, when required.
- patterns of repeated downloads, uploads or lateral movement of files is suspect and can be killed bfore sensitive data leaves

Attack Patterns

Mission accomplished/exfiltration of data:

- attacker controls target system, sends data outbound
- outbound traffic monitoring catches this stage of attack
- but, criminals have learned to send their data from unsuspected, even trusted servers and use low and slow bursts to try and thwart outbound protections
- advanced tools make determinations on outbound traffic based on traffic type, to-from pathways, and other patterns to detect sensitive outbound data in outbound traffic

Defensible Actions Matrix
Aligned to the Cyber Kill Chain

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Contain
Reconnaissance	Web Analytics	Firewall ACL				Firewall ACL
Weaponization	NIDS	NIPS				NIPS
Delivery	Vigilant User	Proxy Filter	Inline AV	Queuing		App-Aware Firewall
Exploitation	HIDS	Patch	DEP			Inter-Zone NIPS
Installation	HIDS	'*chroot*' Jail	AV			EPP
Command & Control	NIDS	Firewall ACL	NIPS	Tarpit	DNS Redirect	Trust Zones
Actions on Targets	Audit Logs	Outbound ACL	DLP	Quality of Service	Honeypot	Trust Zones

Cost to adversary increases as more indicators are revealed, used

From: Defensible Security Posture, Nige the Security Guy

Example 1

See Page 9 of

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

by

Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Lockheed Martin Corporation

pdf file: LM-intel-driven-defense.pdf

Example 2

See Page 10 of

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

by

Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Lockheed Martin Corporation

pdf file: LM-intel-driven-defense.pdf

Example 3

See Page 11 of

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

by

Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin,
Lockheed Martin Corporation

pdf file: LM-intel-driven-defense.pdf