INCIDENT RESPONSE METHODOLOGIES

INTELLIGENCE DRIVEN DEFENSE® AND CYBER KILL CHAIN®

QUINCY TAYLOR

F2T2EA KILL CHAIN

Find: Identify a target.

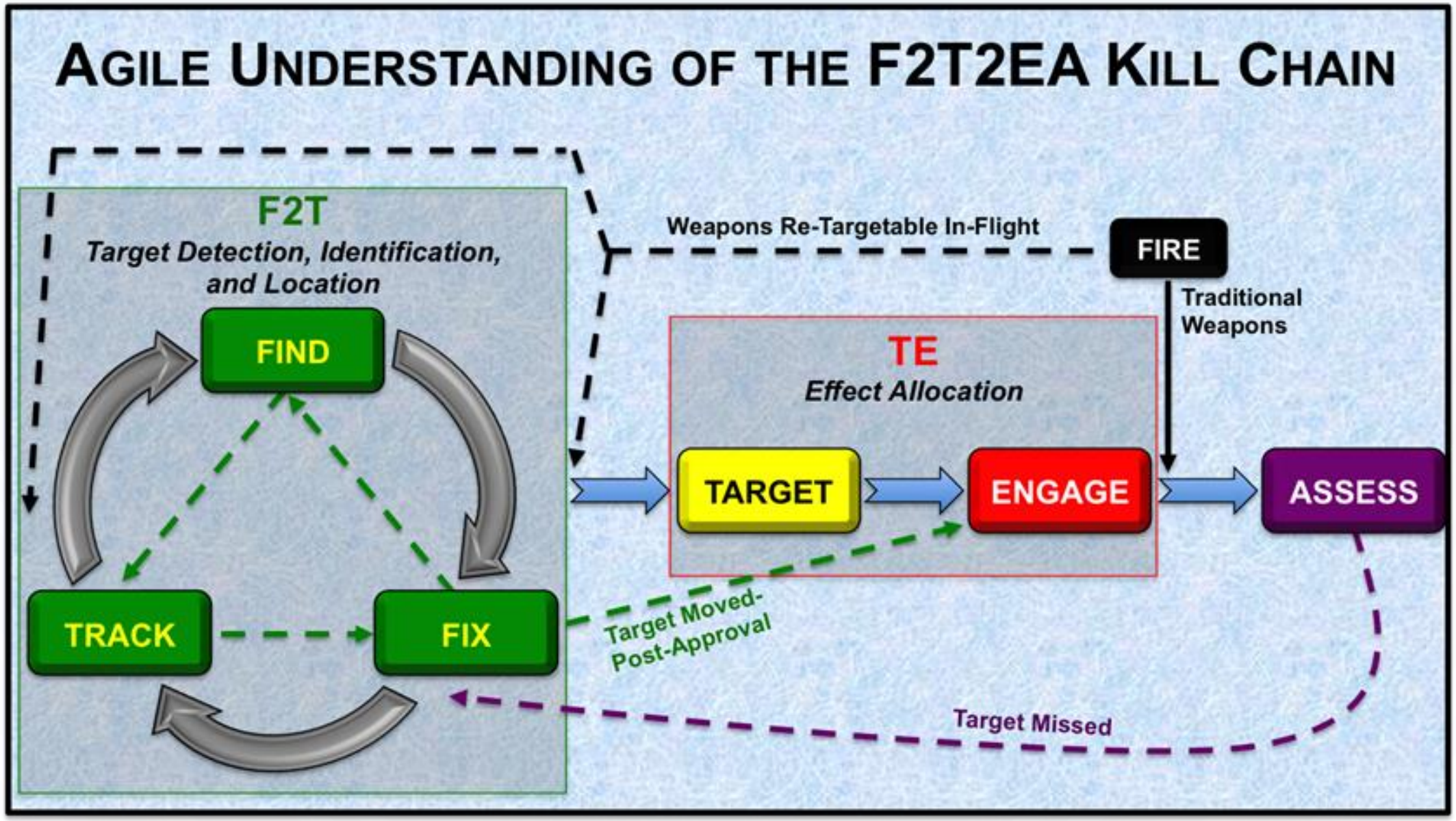
Fix: Fix the target's location.

Track: Monitor the target's movement.

Target: Select an appropriate weapon or asset to use on the target.

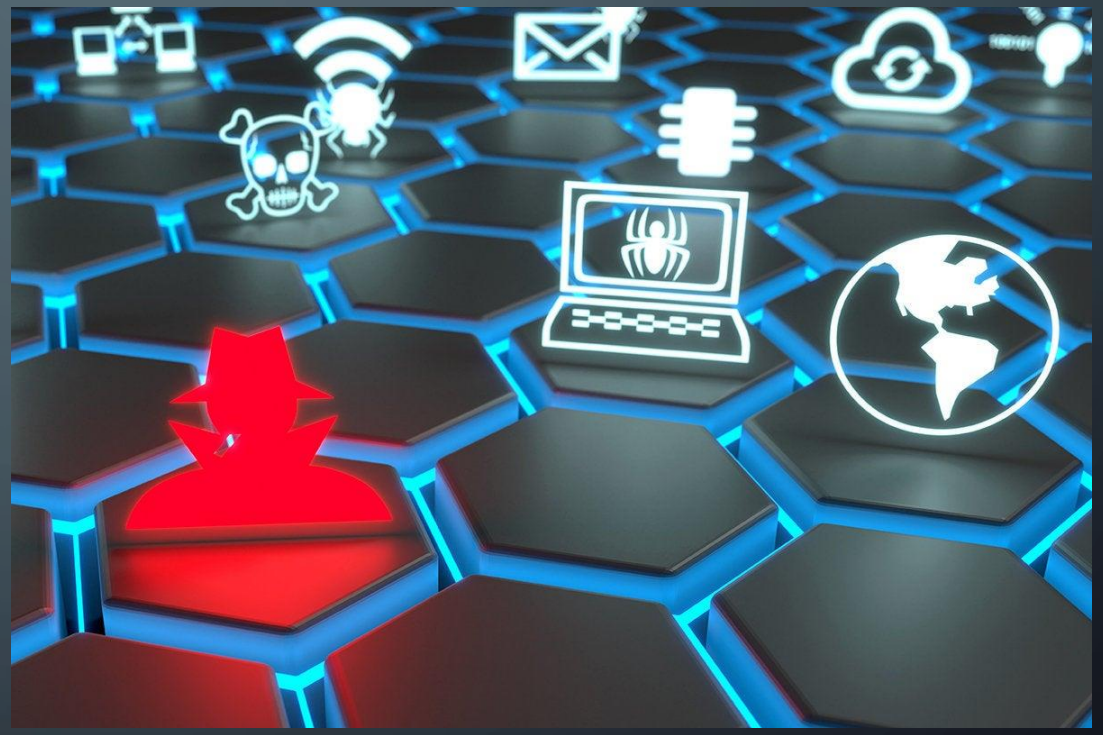
Engage: Apply the weapon to the target.

Assess: Evaluate effects of the attack.


AGILE UNDERSTANDING OF THE F2T2EA KILL CHAIN
F2T
Target Detection, Identification, and Location
FIND
TRACK
FIX
Weapons Re-Targetable In-Flight
FIRE
Traditional Weapons
TE
Effect Allocation
TARGET
ENGAGE
ASSESS
Target Moved-Post-Approval
Target Missed

BEFORE KILL CHAIN

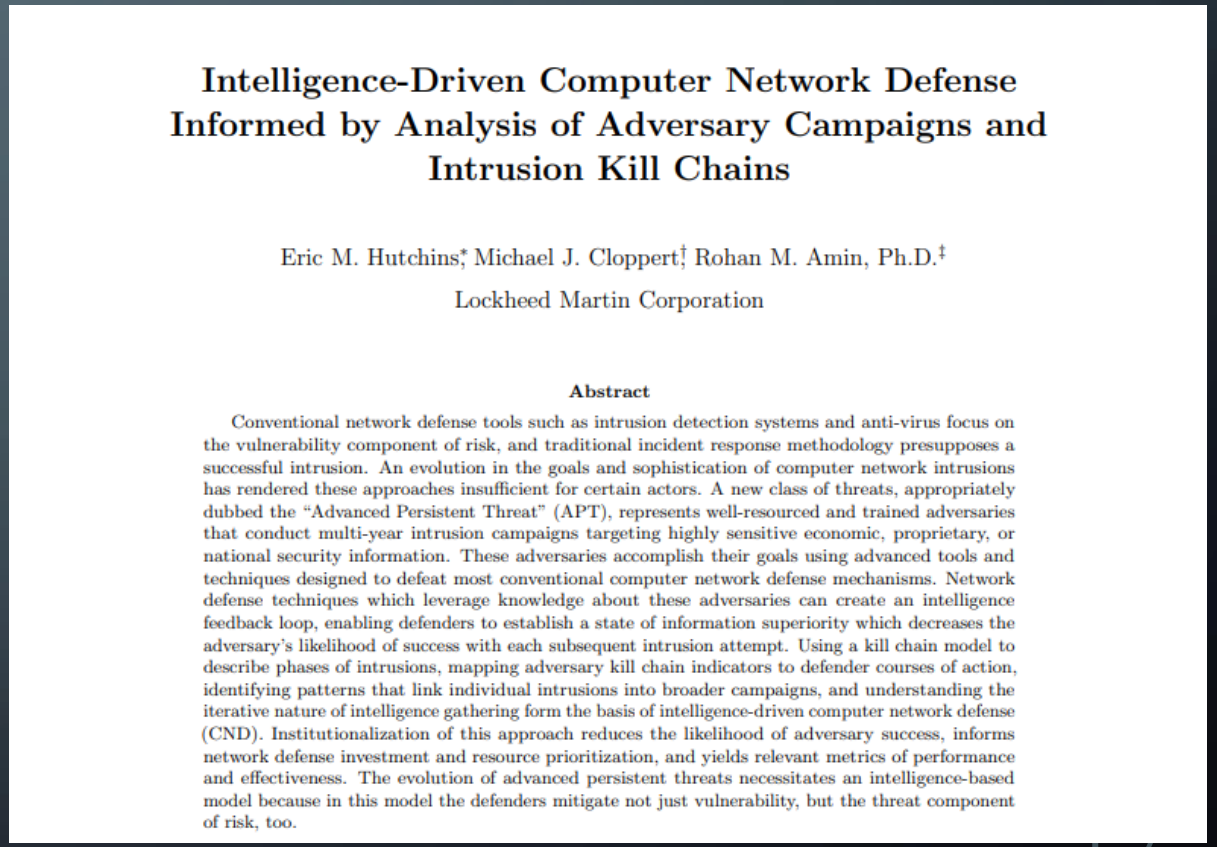
- Castle and moat analogy.
- Sought to put power in the hands of the defenders.
- New kind of threat: Advanced Persistent Threat (APT)



LOCKHEED MARTIN'S CYBER KILL CHAIN METHODOLOGY

- Remember there is no such thing as secure, only defendable.

- Defenders should have a home field advantage.
  - Visibility
  - Intelligence
  - Effect change



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.

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

1) RECONNAISSANCE

- Information gathering on target.
  - Passive: without interacting with the target. (Ex. OSINT)
  - Active: unauthorized access to the network and engages with the system directly to gather information.
- Attackers find weak points and vulnerabilities that allow penetration.

Mitigations

- Firewalls for perimeter security.
- Monitor points of entry and visitor logs.
- Employees trained to report.
- Limit the amount of publicly available company data.

2) WEAPONIZATION

- Find weakness that can be exploited.
- Malicious payload.
- Develop virus, worm, or zero-day as a weapon.
- Leg work for infiltration.

Mitigations

- Security awareness training.
- Analyze malware artifacts to check for similarities.
- Build detection tools for weaponizers

3) DELIVERY

- Gain entry into the victim's security perimeter.
- Supply chain compromise
- Spear phishing attachments
- External/remote services

Mitigations

- Protect from phishing attacks.
- Use patch management tools.
- Flag and investigate changes to files with file integrity monitoring (FIM).
- Monitor for odd login times or locations.
- Run penetration tests.

4) EXPLOITATION

- Intruders gain access.
- Install the necessary tools.
- Modify security certificates.
- Create script files.
- Look for further vulnerabilities to get a better foothold before starting the main attack

Mitigations

•Keep devices up to date.
•Use anti-virus software.
•Set up a host-based intrusion detection system to alert or block common installation paths.
•Conduct regular vulnerability scanning.

5) INSTALLATION

- Windows remote management
- Pseudo attack
- SSH hijacking
- Shared webroot
- Process injection
- Path interception
- Internal spear phishing
- Access token manipulation

Mitigations

- Implement Zero Trust security
- Use network segmentation to isolate individual systems.
- Eliminate the use of shared accounts.
- Enforce password security best practices.
- Audit all suspicious activities of privileged users.

6) COMMAND & CONTROL

- Attacks operate and monitor his attack remotely.
- Obfuscation is when the attacker tries to cover his tracks, making it look like nothing has happened.

Mitigations

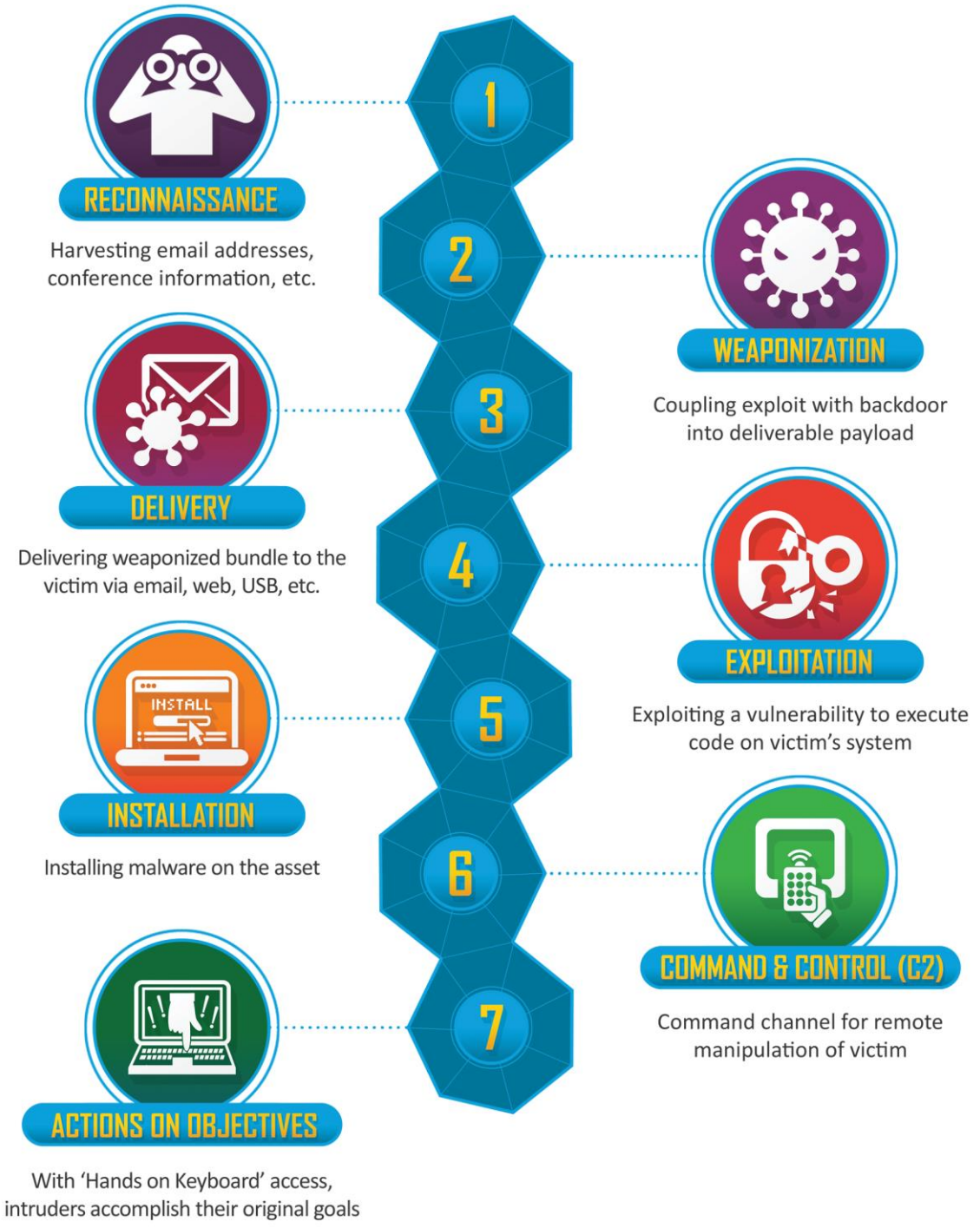
•Look for C2 infrastructures when analyzing malware.
•Demand proxies for all types of traffic (HTTP, DNS).
•Continuously scan for threats.
•Set intrusion detection systems to alert on all new programs contacting the network.

7) ACTION ON OBJECTIVE

- Data Exfiltration over alternative protocol
- Data Exfiltration over a physical medium
- Data encrypted
- Data compressed

Mitigations

- Create an incident response playbook.
- Use tools to detect signs of ongoing data exfiltration.
- Run immediate analyst responses to all alerts.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

PROBLEMS + OTHER METHODOLOGIES

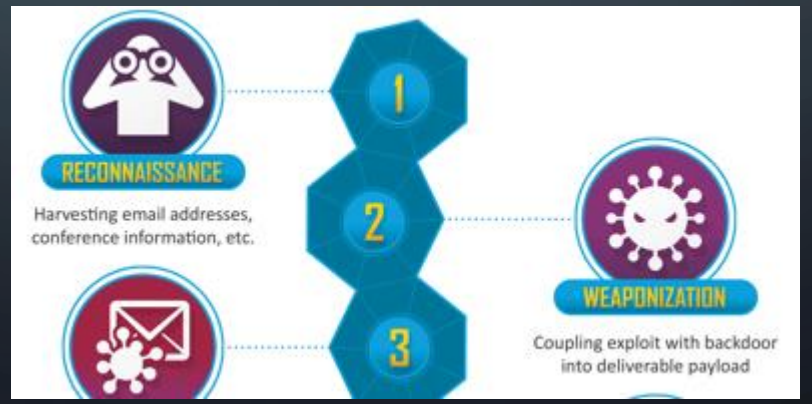
CKC fails to consider…

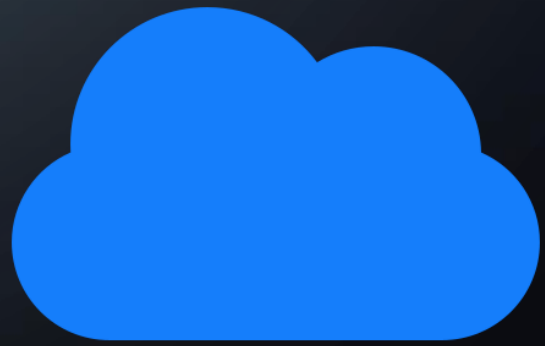
- Insider threats
- Cloud security
- Identifying Threats During the First and Second Phases

Alternative Methodologies

- Unified Kill Chain

MITRE ATT&CK™





ACTIVITY

https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/

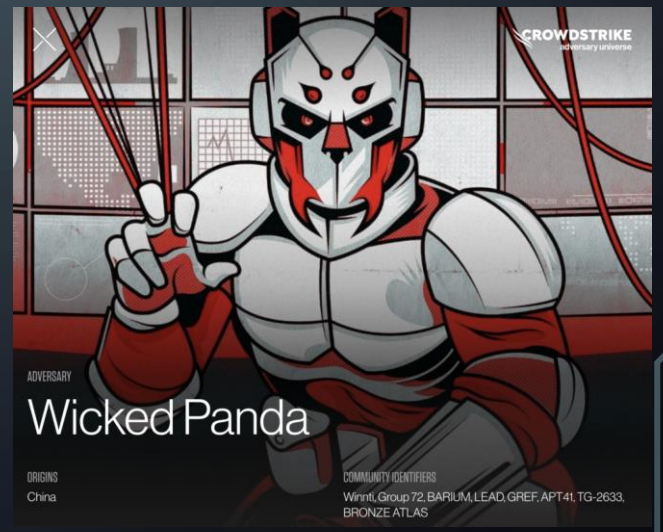
APT 27 – Goblin Panda

APT 28 – Fancy Bear

APT 29 – Fancy Bear

APT 32 – Ocean Buffalo

APT 34 – Helix Kitten



APT 41 – Wicked Panda