What You Need to Know

- Recognize and understand how to interpret data tagged to the Cyber Threat Framework (CTF)
- Understand how to tag reporting to the Cyber Threat Framework
- Understand how CTF-tagged reporting can be used in analysis
Cyber Threat Framework (CTF) Overview

The Cyber Threat Framework was developed by the US Government to enable consistent categorization and characterization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries. The framework captures the adversary life cycle from (a) “PREPARATION” of capabilities and targeting, to (b) initial “ENGAGEMENT” with the targets or temporary nonintrusive disruptions by the adversary, to (c) establishing and expanding the “PRESENCE” on target networks, to (d) the creation of “EFFECTS and CONSEQUENCES” from theft, manipulation, or disruption. The framework categorizes the activity in increasing “layers” of detail (1-4) as available in the intelligence reporting.
Cyber Threat Framework (v4) Layers 1 and 2

The progression of cyber threat actions over time to achieve objectives

**Stages**
- Preparation
  - Plan activity
  - Conduct research & analysis
  - Develop resources & capabilities
  - Acquire victim specific knowledge
  - Complete preparations
- Engagement
  - Deploy capability
  - Interact with intended victim
  - Exploit vulnerabilities
  - Deliver malicious capability
- Presence
  - Establish controlled access
  - Hide
  - Expand presence
  - Refine focus of activity
  - Establish persistence
- Effect/Consequence
  - Enable other operations
  - Deny access
  - Extract data
  - Alter data and/or computer, network or system behavior
  - Destroy HW/SW/data

**Objectives**
- Pre-execution actions
- Operational actions
- Internal actions
- External actions

**Layers**
- Layer 1
- Layer 2
The progression of cyber threat actions over time to achieve objectives

**Stages**
- Preparation
- Engagement
- Presence
- Effect/Consequence

**Objectives**
- Plan activity
- Conduct research & analysis
- Develop resources & capabilities
- Acquire victim specific knowledge
- Complete preparations

**Actions**
- Deploy capability
- Establish controlled access
- Interact with intended victim
- Hide
- Exploit vulnerabilities
- Expand presence
- Refine focus of activity
- Deliver malicious capability
- Establish persistence

**Pre-execution actions**
- Plan activity
- Conduct research & analysis
- Develop resources & capabilities
- Acquire victim specific knowledge
- Complete preparations

**Operational actions**
- Deploy capability
- Establish controlled access
- Interact with intended victim
- Hide
- Exploit vulnerabilities
- Expand presence
- Refine focus of activity
- Deliver malicious capability
- Establish persistence

**Layer 1**
- Enable other operations
- Deny access
- Extract data
- Alter data and/or computer, network or system behavior
- Destroy HW/SW/data

**Layer 2**
- Pre-execution actions
- Operational actions

**Layer 3**
- Actions
  - • Dedicate resources
  - • Create capabilities
  - • Establish partnerships
  - • Persuade people to act on the threat actors behalf (e.g., conduct social engineering)
  - • Obtain a legitimate user account
  - • Increase user privileges
  - • Move laterally
  - • Establish command and control node
  - • Establish hop point
  - • Add victim system capabilities to botnet
  - • Exfiltrate passwords, credentials
The progression of cyber threat actions over time to achieve objectives

Pre-execution actions
- Preparation
  - Plan activity
  - Conduct research & analysis
  - Develop resources & capabilities
  - Acquire victim specific knowledge
  - Complete preparations

Operational actions
- Engagement
  - Deploy capability
  - Interact with intended victim
  - Exploit vulnerabilities
  - Deliver malicious capability

Internal actions
- Presence
  - Establish controlled access
  - Hide
  - Expand presence
  - Refine focus of activity
  - Establish persistence

External actions
- Effect/Consequence
  - Enable other operations
  - Deny access
  - Extract data
  - Alter data and/or computer, network or system behavior
  - Destroy HW/SW/data

Stages
- Layer 1
  - Plan activity
  - Conduct research & analysis
  - Develop resources & capabilities
  - Acquire victim specific knowledge
  - Complete preparations
  - Deploy capability
  - Interact with intended victim
  - Exploit vulnerabilities
  - Deliver malicious capability
  - Establish controlled access
  - Hide
  - Expand presence
  - Refine focus of activity
  - Establish persistence

Objectives
- Layer 2
  - Preparation
  - Engagement
  - Presence
  - Effect/Consequence

Actions
- Layer 3
  - Pre-execution actions
    - Plan activity
    - Conduct research & analysis
    - Develop resources & capabilities
    - Acquire victim specific knowledge
    - Complete preparations
  - Operational actions
    - Deploy capability
    - Interact with intended victim
    - Exploit vulnerabilities
    - Deliver malicious capability
  - Internal actions
    - Establish controlled access
    - Hide
    - Expand presence
    - Refine focus of activity
    - Establish persistence

Indicators
- Layer 4
  - Company XXX reported to have created Malware QQ

These are representative Actions that can contribute to achieving the Layer 2 Objectives.

This is a simple example of the multitude of potential Indicators of threat actor Actions.
Cyber Threat Framework Representations

• The Cyber Threat Framework’s presentation can be adjusted to include only the information of most interest to an intended audience.
• Products tagged to the Cyber Threat Framework may be represented in a variety of ways on products. Presented layers can be adjusted to fit the intended audience.
Tagging Information to the Cyber Threat Framework

Tools to help you

• Cyber Threat Framework one page overview
• Cyber Threat Framework Lexicon outline
• Cyber Threat Framework Lexicon
### Cyber Threat Framework (v4)

**The progression of cyber threat actions over time to achieve objectives**

**Stages**
- Preparation
- Engagement
- Presence
- Effect/Consequence

**Objectives**
- Plan activity
- Conduct research & analysis
- Develop resources & capabilities
- Acquire victim specific knowledge
- Complete preparations
- Deploy capability
- Establish controlled access
- Establish persistence
- Enable other operations
- Hide
- Refine focus of activity
- Deny access
- Extract data
- Expand presence
- Alter data and/or computer, network or system behavior
- Destroy HW/SW/data

**Actions**
- Pre-execution actions: "Left of Intrusion"
- Operational actions: "Right of Intrusion"

**Indicators**
- Discrete cyber threat intelligence data

This one page outline can help identify layer 1 or layer 2 category of reported information.
Cyber Threat Framework (v4) Lexicon Outline

- The outline provides a multilayer view of a segment of the entire framework.

<table>
<thead>
<tr>
<th>Enable other activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny access</td>
</tr>
<tr>
<td>Disrupt/degrade communication links</td>
</tr>
<tr>
<td>Conduct Denial of Service (DoS) and/or</td>
</tr>
<tr>
<td>Distributed Denial of Service (DDoS) attack</td>
</tr>
<tr>
<td>Disrupt/degrade the network</td>
</tr>
<tr>
<td>Execute ransomware</td>
</tr>
<tr>
<td>Extract data</td>
</tr>
<tr>
<td>Relocate and store data on victim's computer, information system(s), network(s), and/or data stores.</td>
</tr>
<tr>
<td>Exfiltrate data/information</td>
</tr>
<tr>
<td>Alter data and/or computer, network, and/or system behavior</td>
</tr>
<tr>
<td>Alter data stored on the victim's system(s)</td>
</tr>
<tr>
<td>Change process run-state on victim system(s)</td>
</tr>
<tr>
<td>Change decisions</td>
</tr>
<tr>
<td>Change machine-to-machine (MtM)</td>
</tr>
<tr>
<td>communications</td>
</tr>
<tr>
<td>Destroy hardware/software/data</td>
</tr>
</tbody>
</table>
# Cyber Threat Framework (v4) Lexicon

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 1 Stages</td>
<td>The progression of cyber threat actions over time to achieve objectives.</td>
</tr>
<tr>
<td>Layer 2 Objectives</td>
<td>The purpose of conducting an action or a series of actions.</td>
</tr>
<tr>
<td>Layer 3 Actions</td>
<td>Activity and associated resources used by a threat actor to satisfy an objective.</td>
</tr>
<tr>
<td>Layer 4 Indicators</td>
<td>Exemplars of discrete, measurable, cyber threat data, i.e., presence of malicious software, named Malware, and/or reported instances of malicious actions or activities, that connotes a threat actor’s attempt to take or having taken an action, or to achieve an objective.</td>
</tr>
</tbody>
</table>

### Preparation

**Activities undertaken by a threat actor, their leadership and/or sponsor to prepare for conducting malicious cyber activities, e.g., establish governance and articulating intent, objectives, and strategy; identify potential victims and attack vectors; securing resources and develop capabilities; assess intended victim’s cyber environment; and define measures for evaluating the success or failure of threat activities.**

<table>
<thead>
<tr>
<th>Plan activity</th>
<th>Steps taken by a threat actor before conducting malicious cyber activity to: define intent; establish policy limitations; identify funding; coordinate intended activities; establish initial objectives and parameters for measuring progress/success towards meeting them; and the steps taken to update plans, activities, and requirements based upon insights gained during the eventual victim engagement.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify intended target(s) and the purpose for the malicious cyber activity</td>
<td>The initial step in the planning process that produces a list of intended victim(s), and defines the intent for and desired outcome of the malicious cyber activity.</td>
</tr>
<tr>
<td>Outline where and how the malicious activity is to be conducted</td>
<td>Actions taken by a threat actor (individual, team or government-sponsored agency), their sponsor and/or leadership to establish the overall strategy for, policy limitations of, and the requisite resources and capabilities needed to conduct the intended malicious cyber activity, (e.g., information needs, resources and capabilities, and partnerships), along with the criteria for evaluating the eventual success/failure (measures of performance, merit, and effectiveness [MoP/MoM/MoE]) of the activity.</td>
</tr>
<tr>
<td>Establish a projected timeline for the malicious activity</td>
<td>The last step in the initial planning process in which the threat actor establishes a projected time for executing the planned malicious activity.</td>
</tr>
</tbody>
</table>

Includes definitions of exemplar terms to aid in accurate data classification; as a living document, the number of terms will increase based on user input.
Sample Report #1

- According to a local report, last year over 120 million personnel files were electronically exfiltrated by an identified nation state cyber actor.
Sample Report #1 Highlighted

- According to a local report, last year over 120 million personnel files were electronically exfiltrated by an identified nation state cyber actor.
According to a local report, last year over 120 million personnel files were exfiltrated by an identified nation state cyber actor.
According to a local report, last year over 120 million personnel files were exfiltrated by an identified nation state cyber actor.
Sample Report #2

• Recent reporting indicates suspected cyber actors working on behalf of country X are planning a possible spearphishing campaign against the US Government, with the goal of gaining access to personnel records.
Sample Report #2 Highlighted

- Recent reporting indicates suspected cyber actors working on behalf of country X are planning a possible spearphishing campaign against the US Government, with the goal of gaining access to personnel records.
suspected cyber actors working on behalf of country X are planning a possible spearphishing campaign... with the goal of gaining access to personnel records.
suspected cyber actors working on behalf of country X are planning a possible spearphishing campaign... with the goal of gaining access to personnel records.
sample report #2 tagged to layers 1, 2, and 3

the progression of cyber threat actions over time to achieve objectives

stages

preparation

plan activity

conduct research & analysis

develop resources & capabilities

acquire victim specific knowledge

complete preparations

engagement

deploy capability

interact with intended victim

exploit vulnerabilities

deliver malicious capability

presence

establish controlled access

hide

expand presence

refine focus of activity

establish persistence

effect/consequence

enable other operations

deny access

extract data

alter data and/or computer, network or system behavior

destroy hw/sw/data

the purpose of conducting an action or a series of actions

objectives

the progression of cyber threat actions over time to achieve objectives

actions and associated resources used by an threat actor to satisfy an objective

actions

identify intended target(s)

outline where & how to conduct the activity

establish timeline for activity

establish strategy

suspected cyber actors working on behalf of country x are planning a possible spearphishing campaign... with the goal of gaining access to personnel records.

each of the layer 3 actions contains a number of embedded actions; this is but one example.
Sample Report #3

- Hackers attacked a self-driving car, bringing the car to a complete stop. Investigation showed that the hackers targeted the laser ranging system, spoofed thousands of objects, and overwhelmed the system’s ability to process information.
Sample Report #3 Highlighted

• Hackers attacked a self-driving car, bringing the car to a complete stop. Investigation showed that the hackers targeted the laser ranging system, spoofed thousands of objects, and overwhelmed the system’s ability to process information.

The framework allows the user to capture all activity surrounding an event. Assuming this was a cyber event, there are two activities: the first was when the car stopped; the second, determined through subsequent forensic analysis, was the specific targeting of the laser ranging system. Both actions should be recorded. The user must determine how to link the two activities to the single event.
The purpose of conducting an action or a series of actions

Actions and associated resources used by a threat actor to satisfy an objective

The progression of cyber threat actions over time to achieve objectives

Sample Report #3 Fact 1 Tagged to Layers 1 and 2

The car stopped
Sample Report #3 Fact 1 Tagged to Layers 1, 2 and 3

The progression of cyber threat actions over time to achieve objectives

Stages
- Preparation
- Engagement
- Presence
- Effect/Consequence

Objectives
- Plan activity
- Conduct research & analysis
- Develop resources & capabilities
- Acquire victim specific knowledge
- Complete preparations
- Deploy capability
- Interact with intended victim
- Exploit vulnerabilities
- Deliver malicious capability
- Establish controlled access
- Hide
- Expand presence
- Refine focus of activity
- Establish persistence
- Enable other operations
- Deny access
- Extract data
- Alter data and/or computer, network or system behavior
- Destroy HW/SW/data

Actions
- The car stopped

Steps taken by a threat actor to alter the operation of the victim information system:
- Disrupt/degrade communications links
- DDoS
- Disrupt/degrade the network
- Execute ransomware
Sample Report #3 Fact 2 Tagged to Layers 1, 2, and 3

The progression of cyber threat actions over time to achieve objectives

- Stages
  - Preparation
  - Engagement
  - Presence

- Pre-execution actions
  - Plan activity
  - Conduct research & analysis
  - Develop resources & capabilities
  - Acquire victim specific knowledge
  - Complete preparations

- Operational actions
  - Deploy capability
  - Interact with intended victim
  - Exploit vulnerabilities
  - Deliver malicious capability

- Internal actions
  - Establish controlled access
  - Hide
  - Expand presence
  - Refine focus of activity
  - Establish persistence

- External actions
  - Effect/Consequence
    - Enable other operations
    - Deny access
    - Extract data
    - Alter data and/or computer, network or system behavior
    - Destroy HW/SW/data

- Objectives
  - The purpose of conducting an action or a series of actions

- Actions
  - Spoofted thousands of objects and overwhelmed the laser ranging system’s ability to process information.

Steps taken by a threat actor that prevents access to a telecommunications system.

- Disrupt/degrade communications links
- DDoS
- Disrupt/degrade the network
- Execute ransomware

3/13/2017
Spoofed thousands of objects and overwhelmed the laser ranging system’s ability to process information.
Analysis

• Depending on the information selected and its presentation, one can begin to conduct a variety of analysis:
  – Trends – change over time
    • What caused the change
  – Predictive – what’s next
  – Environmental
    • Was the threat different than expected
    • What vulnerabilities were missed
    • How to optimize remedial action
  – Vulnerability – risk analysis
  – Defensive posture
## Cyber Threat Activity – CTF Layer 1 Stages Exemplar

<table>
<thead>
<tr>
<th>Threat Actor</th>
<th>Preparation</th>
<th>Engagement</th>
<th>Presence</th>
<th>Effect/Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Actor A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor D</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor E</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor F</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor G</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor H</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Reporting Period:** January – March 2016
## CTF (v4) Layer 2 Objectives Exemplar

<table>
<thead>
<tr>
<th>Layer 1 Stages</th>
<th>Layer 2 Objectives</th>
<th>Threat Actor A</th>
<th>Threat Actor B</th>
<th>Threat Actor C</th>
<th>Threat Actor D</th>
<th>Threat Actor E</th>
<th>Threat Actor F</th>
<th>Threat Actor G</th>
<th>Threat Actor H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conduct research &amp; analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop resources &amp; capabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acquire victim specific knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complete preparations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop capability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interact with intended victim</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit vulnerabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deliver malicious capability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish controlled access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hide</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expand presence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Refine focus of activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish persistence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable other operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deny Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extract data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alter data and/or computer, network or system behavior</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destroy HW/SW/data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Threat Actor A**
- Plan activity
- Develop capability
- Establish controlled access
- Enable other operations

**Threat Actor B**
- Conduct research & analysis
- Interact with intended victim
- Hide
- Extract data

**Threat Actor C**
- Develop resources & capabilities
- Exploit vulnerabilities

**Threat Actor D**
- Acquire victim specific knowledge
- Deliver malicious capability

**Threat Actor E**
- Complete preparations
- Refine focus of activity

**Threat Actor F**
- Establish persistence

**Threat Actor G**
- Deny Access

**Threat Actor H**
- Expand presence
- Destroy HW/SW/data
## Trend Analysis - Threat Activity Over Time

Level 2 Cyber Threat Activity by Threat Actor, Report Date, and Country of Threat Origin

<table>
<thead>
<tr>
<th>Reporting Period: Jan – Apr 2015</th>
<th>January</th>
<th>February</th>
<th>March</th>
<th>April</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country D</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor D</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor E</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor F</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor G</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Actor H</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Reporting Period:
- **January**
- **February**
- **March**
- **April**
Summary

• The Cyber Threat Framework can be represented in a variety of products tailored to a specific audience

• Important to understand how tagging cyber threat information to the Cyber Threat Framework works

• Cyber Threat Framework-tagged reporting can be used to produce insightful, consistent analysis from a variety of information sources
Questions?