Cyber Threat Framework (version 4)
How to Use
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.
The purpose of conducting an action or a series of actions

**Stages**
- Preparation:
  - 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
- External actions “Left of Intrusion”:
  - Establish controlled access
  - Hide
  - Expand presence
  - Refine focus of activity
  - Expose or establish presence
  - Deliver malicious capability
- Internal actions “Right of Intrusion”:
  - Establish persistence
  - Enable other operations
  - Deny access
  - Extract data
  - Alter computer, network or system behavior
  - Destroy HW/SW/data

**Objectives**
- **Pre-execution actions**
- **Operational actions**
- **Effect/Consequence**

The progression of cyber threat actions over time to achieve objectives

Layer 1
Layer 2
Cyber Threat Framework (v4) Layer 3 Exemplars

The progression of cyber threat actions over time to achieve objectives

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

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

**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 purpose of conducting an action or a series of actions

Actions and associated resources used by a threat actor to satisfy an objective
The purpose of conducting an action or a series of actions

The progression of cyber threat actions over time to achieve objectives

Stages

Preparation

Engagement

Presence

Effect/Consequence

External actions “Left of Intrusion”

Operational actions

Internal actions “Right of Intrusion”

Objectives

Pre-execution actions

Actions

Layer 1

Layer 2

Layer 3

Layer 4

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

The purpose of conducting an action or a series of actions

Stages

Preparation

Engagement

Presence

Effect/Consequence

External actions “Left of Intrusion”

Operational actions

Internal actions “Right of Intrusion”

Objectives

Pre-execution actions

Actions

Layer 1

Layer 2

Layer 3

Layer 4

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

The progression of cyber threat actions over time to achieve objectives

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.

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.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Stage</th>
<th>Objective</th>
<th>Action</th>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Executive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Executive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Tactical</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Tactical</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(U) Cyber Threat Framework
Reading the Framework

- 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
The purpose of conducting an action or a series of actions is 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 computer, network or system behavior
- Destroy HW/SW/data

**Actions**
- Layer 1
- Layer 2
- Layer 3
- Layer 4

**Indicators**
- Discrete cyber threat intelligence data

This one page outline can help identify layer 1 or layer 2 category of reported information.
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 Distributed Denial of</td>
</tr>
<tr>
<td>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</td>
</tr>
<tr>
<td>system(s), network(s), and/or data stores.</td>
</tr>
<tr>
<td>Exfiltrate data/information</td>
</tr>
<tr>
<td>Alter computer, network, and/or system behavior</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) communications</td>
</tr>
<tr>
<td>Destroy hardware/software/data</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.
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.
Sample Report #1 Tagged to Layers 1, 2, and 3

The progression of cyber threat actions over time to achieve objectives

The purpose of conducting an action or a series of actions

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

Stages

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
- "Left of Intrusion"
- Establish controlled access
- Hide
- Expand presence
- Refine focus of activity
- Establish persistence

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

Objectives

Actions

According to a local report, last year over 120 million personnel files were exfiltrated by an identified nation state cyber actor.

Activities
- Relocate and store data
- Exfiltrate data/information
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.
Sample Report #2 Tagged to Layers 1, 2, and 3

The progression of cyber threat actions over time to achieve objectives

Stages

Preparation

External actions "Left of Intrusion"

Operational actions

Internal actions "Right of Intrusion"

Layer 1

Layer 2

Layer 3

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

External actions

Enable other operations

Deny access

Expand presence

Extract data

Alter data

Alter computer, network or system behavior

Destroy HW/SW/data

The progression of cyber threat actions over time to achieve objectives

Stages

Preparation

External actions "Left of Intrusion"

Operational actions

Internal actions "Right of Intrusion"

Layer 1

Layer 2

Layer 3

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The progression of cyber threat actions over time to achieve objectives

Stages

Preparation

External actions "Left of Intrusion"

Operational actions

Internal actions "Right of Intrusion"

Layer 1

Layer 2

Layer 3

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The purpose of conducting an action or a series of actions

Objectives

Pre-execution actions

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

Establish persistence

Layer 1

Layer 2

Layer 3

Effect/Consequence

The progression of cyber threat actions over time to achieve objectives

The progression of cyber threat actions over time to achieve objectives

The progression of cyber threat actions over time to achieve objectives

The progression of cyber threat actions over time to achieve objectives

The progression of cyber threat actions over time to achieve objectives

The progression of cyber threat actions over time to achieve objectives

The progression of cyber threat actions over time to achieve objectives

The progression of cyber threat actions over time to achieve objectives

The progression of cyber threat actions over time to achieve objectives

The progression of cyber threat actions over time to achieve objectives

The progression of cyber threat actions over time to achieve objectives

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.

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

The progression of cyber threat actions over time to achieve objectives

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

**Objectives**
- The purpose of conducting an action or a series of actions
- Actions and associated resources used by a threat actor to satisfy an objective

**Actions**
- 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**
- Pre-execution actions
  - Preparation
    - 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
  - Presence
    - Establish controlled access
    - Hide
    - Expand presence
    - Refine focus of activity
    - Establish persistence
- Effect/Consequence
  - Enable other operations
  - Deny access
  - Extract data
  - Alter computer, network or system behavior
  - Destroy HW/SW/data

**Objectives**
- External actions “Left of Intrusion”
- Internal actions “Right of Intrusion”

**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

The purpose of conducting an action or a series of actions

Actions and associated resources used by a threat actor to satisfy an objective
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
- Operational actions
- Presence
- Effect/Consequence

**Objectives**
- 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

**Actions**
- Steps taken by a threat actor that prevents access to a telecommunications system.
  - Disrupt/degrade communications links
  - DDoS
  - Disrupt/degrade the network
  - Execute ransomware

**Spoofed thousands of objects and overwhelmed the laser ranging system’s ability to process information.**
Spoofed 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.

Program used to spoof the laser ranging system.
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>Preparation</td>
<td>Plan activity</td>
<td></td>
<td>★</td>
<td>★</td>
<td></td>
<td></td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Conduct research &amp; analysis</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Develop resources &amp; capabilities</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Acquire victim specific knowledge</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Complete preparations</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Engagement</td>
<td>Develop capability</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Interact with intended victim</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Exploit vulnerabilities</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Deliver malicious capability</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Presence</td>
<td>Establish controlled access</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Hide</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Expand presence</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Refine focus of activity</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Establish persistence</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td>Effect/Consequence</td>
<td>Enable other operations</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Deny Access</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Extract data</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Alter/manipulate computer, network or system behavior</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
<tr>
<td></td>
<td>Destroy HW/SW/data</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
<td>★</td>
</tr>
</tbody>
</table>

Threat Actor A

Threat Actor B

Threat Actor C

Threat Actor D

Threat Actor E

Threat Actor F

Threat Actor G

Threat Actor H

1/30/2017

ODNI Public Affairs Office
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>Country</th>
<th>January</th>
<th>February</th>
<th>March</th>
<th>April</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Threat Actor A**

**Threat Actor B**

**Threat Actor C**

**Threat Actor D**

**Threat Actor E**

**Threat Actor F**

**Threat Actor G**

**Threat Actor H**
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?