The Mechanics of Cyber Threat Information Sharing

Session 229, February 23, 2017

Denise Anderson, President, National Health Information Sharing and Analysis Center (NH-ISAC)
Julie Connolly, Principal Cybersecurity Engineer, The MITRE Corporation
Speaker Introduction

Denise Anderson, MBA
President, National Health Information Sharing and Analysis Center (NH-ISAC)

Julie Connolly, CISSP
Principal Cybersecurity Engineer
The MITRE Corporation
Conflict of Interest

Denise Anderson, NH-ISAC, MBA
Julie Connolly, MITRE, B.S.

Have no real or apparent conflicts of interest to report.
Agenda

- A Review of **Cyber Threat Intelligence** (CTI)
- Thwarting cyber attackers by **anticipating** and **preventing attacks**
- **Tools** and **examples** of effective Cyber Threat Intelligence sharing
- Extending the Cyber Threat Intelligence model to the include **post-attack detection** and **response**
Learning Objectives

• Explain the **Structured Threat Information eXpression** (STIX) and **Trusted Automated eXchange of Indicator Information** (TAXII) standards and how they enable automated cyber threat sharing

• Identify and describe **threat sharing tools** that leverage STIX and TAXII and how they can be effectively used in your environment

• Discuss **STIX/TAXII use cases** and **implementation success stories** that showcase effective cyber threat sharing and highlight key lessons learned

• Describe what a **cyber threat–based defense** is and how it is effective in combatting sophisticated cyber adversaries
Realizing the Value of Health IT

Clinical accuracy & timeliness
By ensuring the integrity and confidentiality of patient data

Accurate, available PHI
Via a reduction in cybersecurity incidents on healthcare networks

Accurate, available PHI
Via a reduction in cybersecurity incidents on healthcare networks

TREATMENT/CLINICAL

REALIZING THE VALUE OF HEALTH IT
Health IT creates five kinds of value of benefit to patients, healthcare providers and communities.

S SATISFACTION
T TREATMENT/CLINICAL
E ELECTRONIC SECURE DATA
P PATIENT ENGAGEMENT AND POPULATION MANAGEMENT
S SAVINGS

TREATMENT/CLINICAL

ELECTRONIC SECURE DATA
Cyber Threat Intelligence
The Cyber Attack Lifecycle*

Cyber Threat Intelligence Sharing

How can my detection today aid your prevention tomorrow?
Cyber Threat Intelligence Sharing Enablers

Standardized Language

Standardized Exchange Mechanism
STIX is a **language** for the characterization and communication of cyber threat information.

TAXII defines a **set of service** for securely exchanging cyber threat information.

- Not a sharing program, database, or tool
  - But supports those use cases and more

- A set of specifications developed based on public feedback and offered freely to the public
Cyber Threat Intelligence Sharing Enablers: What they get you

• A structured framework to enable the analysis of full-spectrum cyber threat intelligence

• A common language in which to share cyber threat information across organizations and products

• A common set of services to share cyber threat information
### Constructs

<table>
<thead>
<tr>
<th>Atomic</th>
<th>What threat activity are we seeing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tactical</td>
<td>What threats should I look for on my networks and systems and why?</td>
</tr>
<tr>
<td>Operational</td>
<td>Where has this threat been seen?</td>
</tr>
<tr>
<td></td>
<td>What does it exploit?</td>
</tr>
<tr>
<td></td>
<td>What can I do about it?</td>
</tr>
<tr>
<td>Strategic</td>
<td>Who is responsible &amp; why are they doing it?</td>
</tr>
<tr>
<td></td>
<td>What are they doing and how can we characterize it?</td>
</tr>
</tbody>
</table>
The Exchange (TAXII Sharing Models)

- TAXII supports a wide variety of sharing models
  - Push or pull delivery
  - On-demand or subscription

Peer to Peer

Hub and Spoke

Peer A

Peer B

Peer C

Peer D

Peer E

Source

Hub

Subscriber

Spoke
  - (Consumer only)
  - (Consumer & Producer)
  - (Producer only)

Source/Subscriber

Peer to Peer (Consumer & Producer)
Putting It All Together

- Implement a Cyber Threat Intelligence based defense that includes sharing

- Adopt/use STIX/TAXII “compatible” tools and services

- Establish relationships with peer organizations
Putting it All Together: Multiple Use Cases

Cyber Threat Information

Other Sources
- Sensors
- Cyber Threat Data

Cyber Threat Data

UC1: Analyzing Cyber Threats
- Observables & Context
- Courses of Action & Context
- Operational Cyber Threat Information

UC2: Specifying Indicator Patterns for Cyber Threats
- Indicators
- Cyber Ops (SOC/CERT)
- Cyber Threat Analyst

UC4: Sharing Cyber Threat Information
- Indicators
- Policy: what to Share with whom
- Cyber Decision Maker

Internal Organizational Scope
- Sharing Communities

Managing Cyber Threat Response Activities
- UC3.1 Cyber Threat Prevention
- UC3.2 Cyber Threat Detection
- UC3.3 Incident Response

Approved for Public Release; Distribution Unlimited. Case Number 17-0041
Putting It All Together: Adoption and Use

FS-ISAC, NH-ISAC, and the Multi-State ISAC are currently sharing operational data using STIX/TAXII

DHS’ National Cybersecurity and Communications Integration Center (NCCIC) and US-CERT are currently publishing reports in STIX/TAXII

DHS’s free Automated Indicator Sharing (AIS) capability uses STIX/TAXII to enable machine-to-machine communication
Putting it All Together: Tools

Example commercial vendors that have or are developing products that support STIX & TAXII:

See complete current list at https://wiki.oasis-open.org/cti/Products
Examples in Healthcare
The Cyber Attack Lifecycle

- Recon
- Deliver
- Control
- Maintain

Left of Exploit: Weaponize, Exploit
Right of Exploit: Execute, Maintain

Going Deeper: Post-attack Detection and Response
Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™)*

- Persistence
- Privilege Escalation
- Credential Access
- Host Enumeration
- Defense Evasion
- Lateral Movement
- Execution
- Command and Control
- Exfiltration

Threat data informed adversary model

Higher fidelity on right-of-exploit, post-access phases

Describes behavior sans adversary tools

*http://attack.mitre.org
The ATT&CK Model

- Consists of:
  1. Tactic phases derived from Cyber Attack Lifecycle
  2. List of techniques available to adversaries for each phase
  3. Possible methods of detection and mitigation
  4. Documented adversary use of techniques

- Publically available adversary information is a problem
  - Not granular enough
  - Insufficient volume

Image source: www.mrpotatohead.net

Mr. Potato Head is a registered trademark of Hasbro Inc.
Persistence – New Windows Service

- **Description**: When Windows starts, it also starts programs called services. A service's configuration information, including the service's executable, is stored in the registry. Adversaries may install a new service which will be executed at startup by directly modifying the registry or by using tools.

- **Platform**: Windows

- **Permissions required**: Administrator, SYSTEM

- **Effective permissions**: SYSTEM

- **Use**: Part of initial infection vector or used during operation to locally or remotely execute persistent malware. May be used for privilege escalation.

- **Detection**: Monitor new service creation. Look for out of the ordinary service names and activity that does not correlate with known-good software, patches, etc. New services may show up as outlier processes that have not been seen before when compared against historical data.

**Data Sources**: Windows Registry, process monitoring
ATT&CK Use Cases

• Gap analysis with current defenses
• Prioritize detection/mitigation of heavily used techniques
  – Current analytics can detect over 16 publicly reported adversary groups and over 30 publicly available attacker tools
• Information sharing
  – Leveraging STIX/TAXII to enable sharing of post-attack intelligence
• Track a specific adversary’s set of techniques
• Simulations, exercises
• New technologies, research
ATT&CK and Healthcare
Summary

• Cyber Threat Intelligence and Sharing is the key to a robust cyber defense
  – Cyber Attack Lifecycle is a useful construct for conceptualizing adversary behavior and concomitant defensive strategies
• STIX and TAXII standards – and the products and services that use them -- enable seamless cyber threat intel sharing and more
• ATT&CK model enumerates adversary post-exploit behavior
• Healthcare sector is and should continue to espouse and expand CTI sharing using STIX and TAXII
• The Healthcare sector is exploring ways to adapt ATT&CK to further bolster its post-exploit detection and response capabilities
Summary: Realizing the Value of Health IT

Clinical accuracy & timeliness
By ensuring the integrity and confidentiality of patient data

Accurate, available PHI
Via a reduction in # cybersecurity incidents on healthcare networks
Questions

• Denise Anderson, President, NH-ISAC  
  www.nhisac.org

• Julie Connolly, CISSP, MITRE  
  jconnoll@mitre.org