LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

The Evolution of Cyber Hunt Processes

From IOCs to TTPs

06/17/2021

TLP: WHITE, ID# ***202106171300***

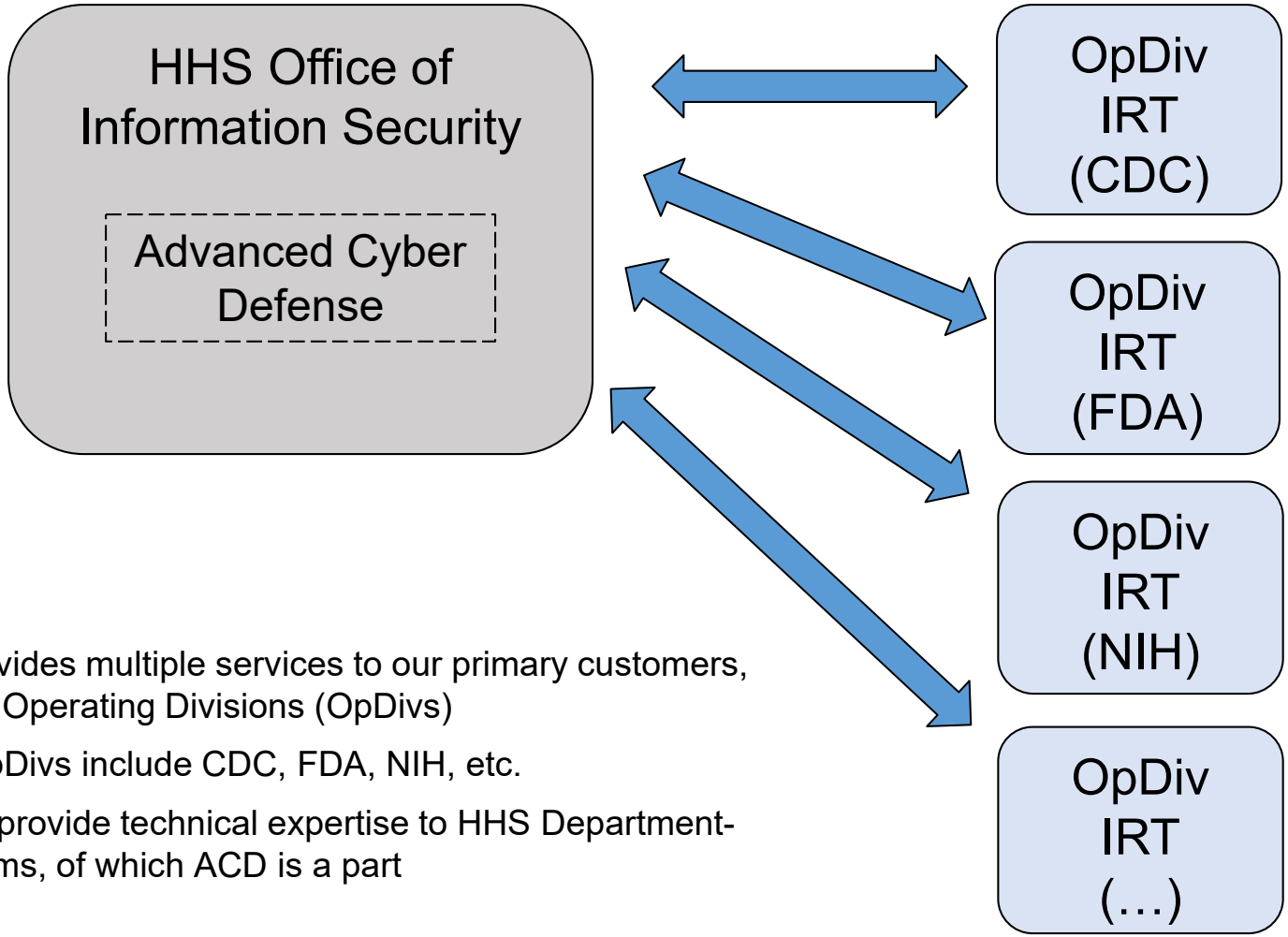
Agenda

- HHS OIS Organization
- The Early Days
- Malspam Grouping
- Hunting with TTPs
- Examples of Hunting with TTPs
- Hunting with TTPs: Frameworks (MITRE ATT&CK)
- Hunting with TTPs: SolarWinds
- Threat Hunting in a Federated Environment
- Threat Feeds
- STIX / TAXII
- STIX / TAXII: STIX
- STIX / TAXII: TAXII
- Collaborations
- Actionable Outcomes: “So What?”
- Metrics

Slides Key:

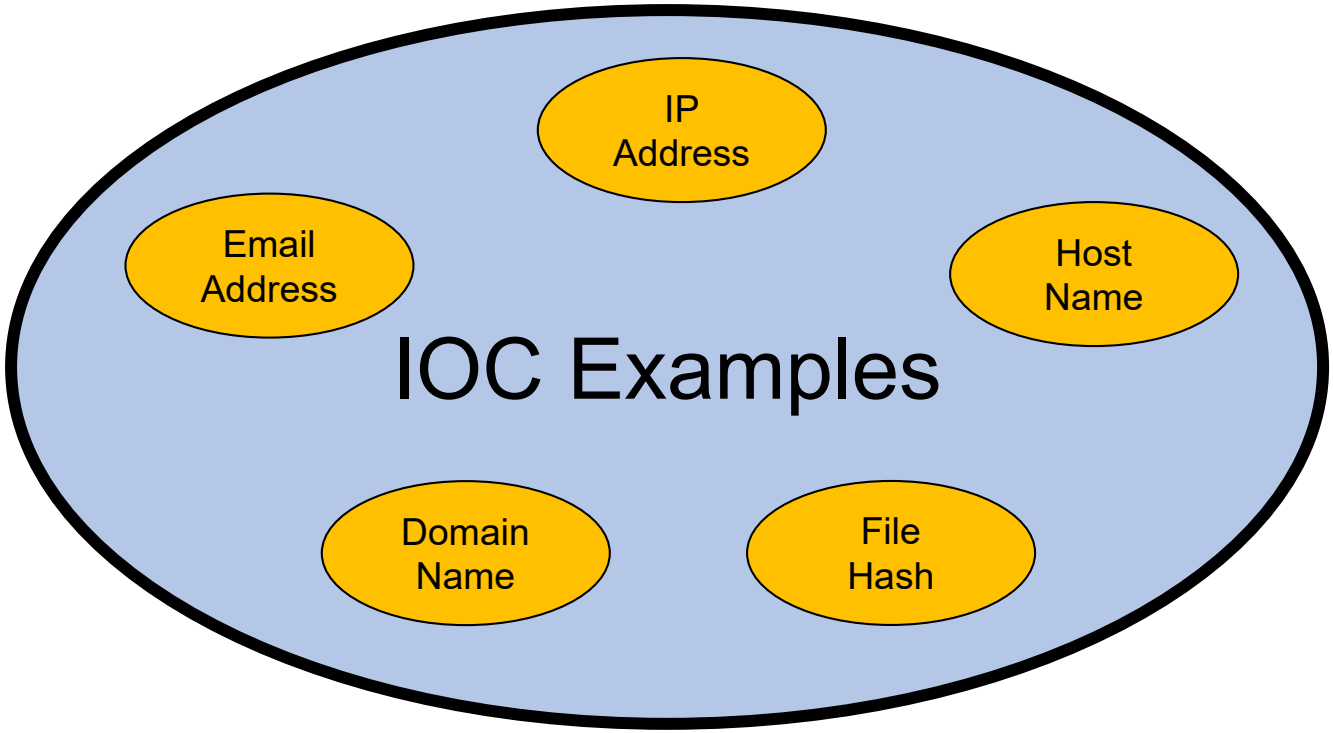
Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)



- ACD provides multiple services to our primary customers, the HHS Operating Divisions (OpDivs)
- Major OpDivs include CDC, FDA, NIH, etc.
- We also provide technical expertise to HHS Department-level teams, of which ACD is a part

- Indicators of Compromise (IOCs) were king
- A “win” was the ability to detect activity related to IOCs
- An even bigger win was the ability to extract new IOCs from malware samples
- The end goal was communication of IOCs so that IRTs could monitor or block them



Malspam Grouping

- Malicious spam emails (malspam) were grouped by subject lines or contents
- The primary driver was to cut down on analysts' workloads
- It also allowed us to observe patterns in the malspam
- This helped with "use and discard" IOCs

Campaign 1	Campaign 2	Campaign 3
New invoice #50670	Order #136-7354561-0126833	Invoice number 6428
New invoice #9214	Order #141-0033408-0135582	Invoice number 1875
New invoice #521203	Order #142-7248705-0404000	Invoice number 393540

"Tactics, Techniques, and Procedures" together refer to the behavior of an actor:

Tactic:

The highest level of behavior.

Technique:

A more detailed description of behavior within context of the tactic.

Procedure:

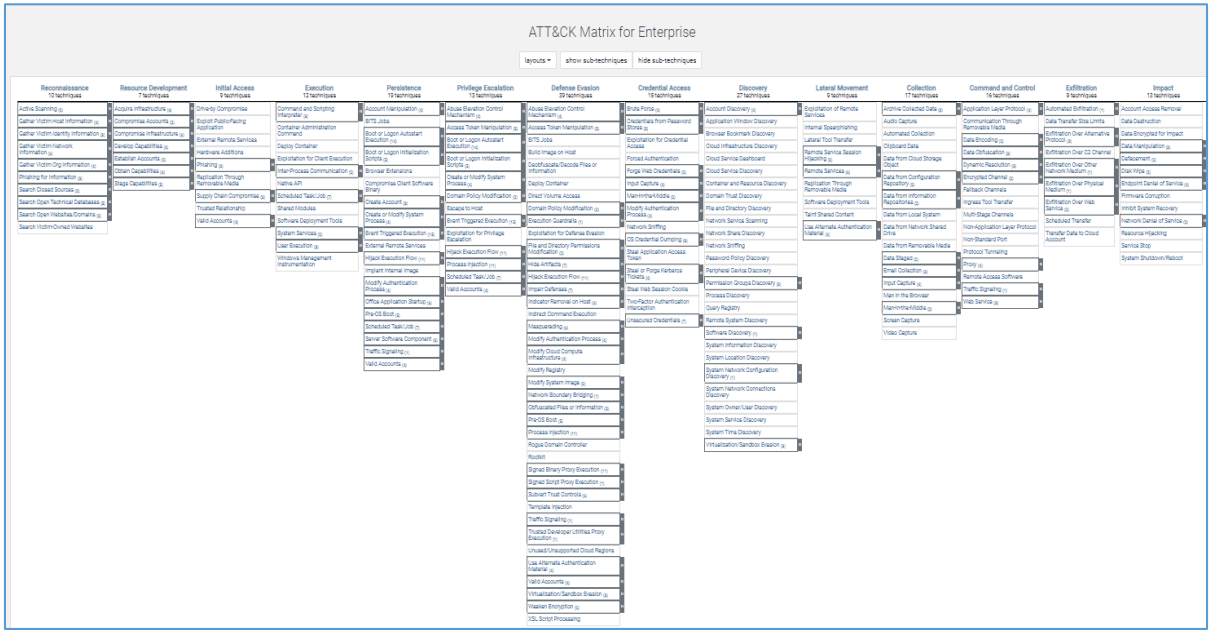
Lower level, highly detailed description in context of the technique.

Source: https://csrc.nist.gov/glossary/term/Tactics_Techniques_and_Procedures

Common TTPs:

- Ransomware delivered via email attachments
- Use of PowerShell scripts
- Adding malware to startup items folder
- Command & Control via HTTPS traffic
- Emails linking to credential harvesters

"MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations."



ATT&CK: Adversarial Tactics, Techniques, & Common Knowledge

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise			Boot or Logon Autostart	

Source: https://attack.mitre.org/

Hunting with TTPs: Frameworks (MITRE ATT&CK)

Home > Groups > Cobalt Group

Cobalt Group

Cobalt Group is a financially motivated threat group that has primarily targeted financial institutions. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. Cobalt Group has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. One of the alleged leaders was arrested in Spain in early 2018, but the group still appears to be active. The group has been known to target organizations in order to use their access to then compromise additional victims. [1] [2] [3] [4] [5] [6] [7] Reporting indicates there may be links between Cobalt Group and both the malware Carbanak and the group Carbanak. [8]

ID: G0080
Associated Groups: Cobalt Gang, Cobalt Spider
Version: 1.3
Created: 17 October 2018
Last Modified: 26 April 2021

Version Permalink

Associated Group Descriptions

Name	Description
Cobalt Gang	[1] [9] [10]
Cobalt Spider	[9]

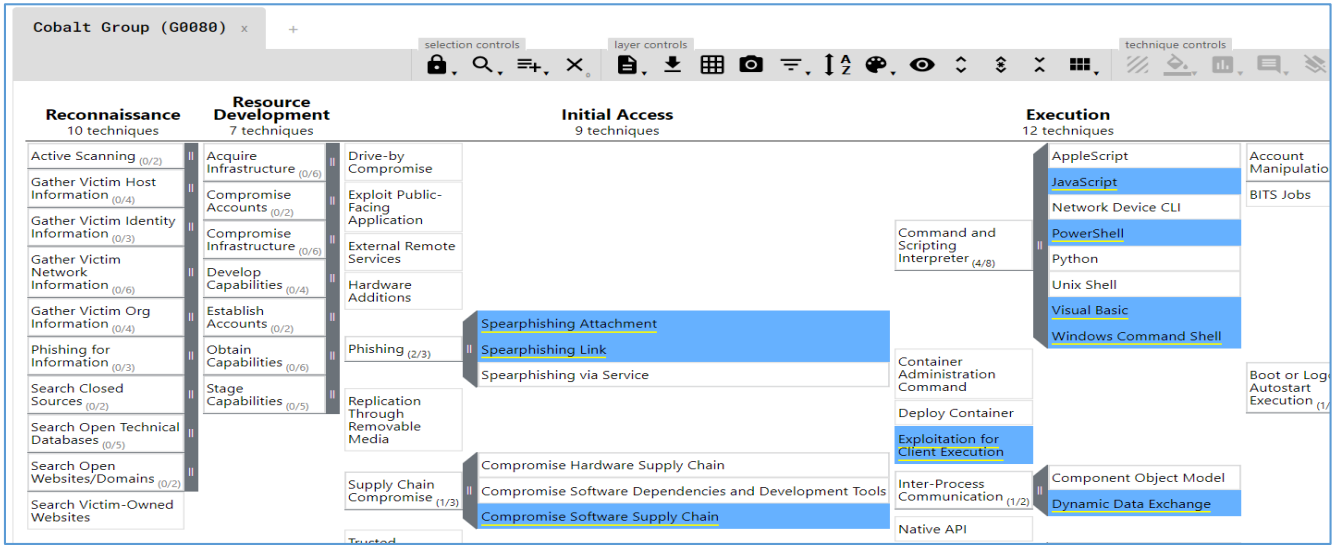
Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Account Control	Cobalt Group has bypassed UAC.[4]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Cobalt Group has used HTTPS for C2.[1][3][4]

MITRE provides information on a number of threat groups.

The ATT&CK Navigator shows which TTPs a group uses:



Source: https://attack.mitre.org/groups/G0080/

Initial indicators were random hostnames:

<random characters>[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com
<random characters>[.]appsync-api[.]us-west-2[.]avsvmcloud[.]com
<random characters>[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com
<random characters>[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com

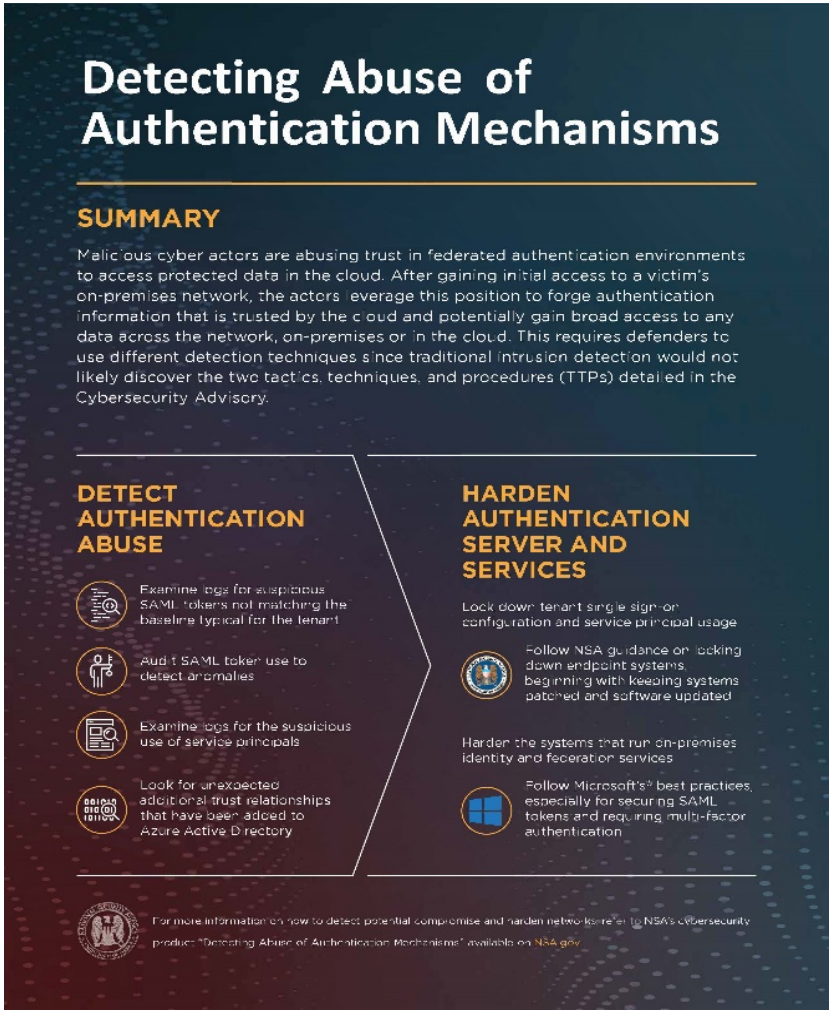
- Searching for the complete hostname has little value (IOC)
- Searching for hosts under the second level domain is actionable
- Example of a technique of using a Domain Name Generation algorithm under a single common domain

solarwinds

Source: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Multiple entities released information on detection opportunities:

https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html



https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2451159/nsa-cybersecurity-advisory-malicious-actors-abuse-authentication-mechanisms-to/#pop4744190

The ACD Hunt Team released toolset queries to the OpDivs to assist in their hunting efforts:

The distribution consisted of an executive summary, followed by queries for security tools used at HHS.

- Generally, ACD doesn't perform comprehensive cyber hunts.
- We produce methods of detection for vulnerabilities and malicious activity.
- OpDivs have granular expertise for their systems.
- Any activity uncovered during development will be handled as an incident with the appropriate IRTs.

Threat Feeds

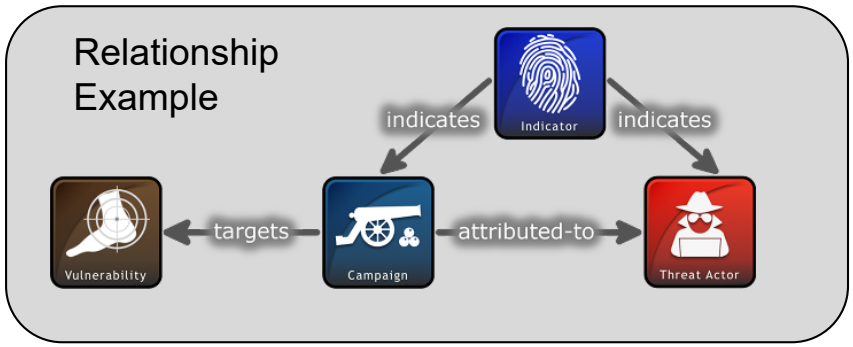
- Feeds of malicious indicators provide initial awareness and hopefully context
- At a basic level, they can be lists of bad IPs or email addresses
- More advanced feeds have additional context and TTPs
- One challenge is how to operationalize them:
  - They can be noisy if used as the basis of alerts, particularly if they are not high fidelity or generated using automated means
  - They can be an additional resource for forensic investigations
- Examples:
  - Vendor Feeds
  - Open Source Feeds
  - CISA CISCP/AIS Feeds

- Structured Threat Information Expression (STIX)
- Trusted Automated eXchange of Indicator Information (TAXII)
- A set of specifications facilitating cyber intel sharing
- Handled by the OASIS Cyber Threat Intelligence (CTI) Technical Committee (https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti)
- Currently at Version 2.1

Information Type	Data / Language	Transfer Mechanism
Web:	HTML	HTTP
CTI:	STIX	TAXII

STIX is a language and format to exchange cyber threat intel, and defines a number of domain objects:

STIX also defines two relationship objects:

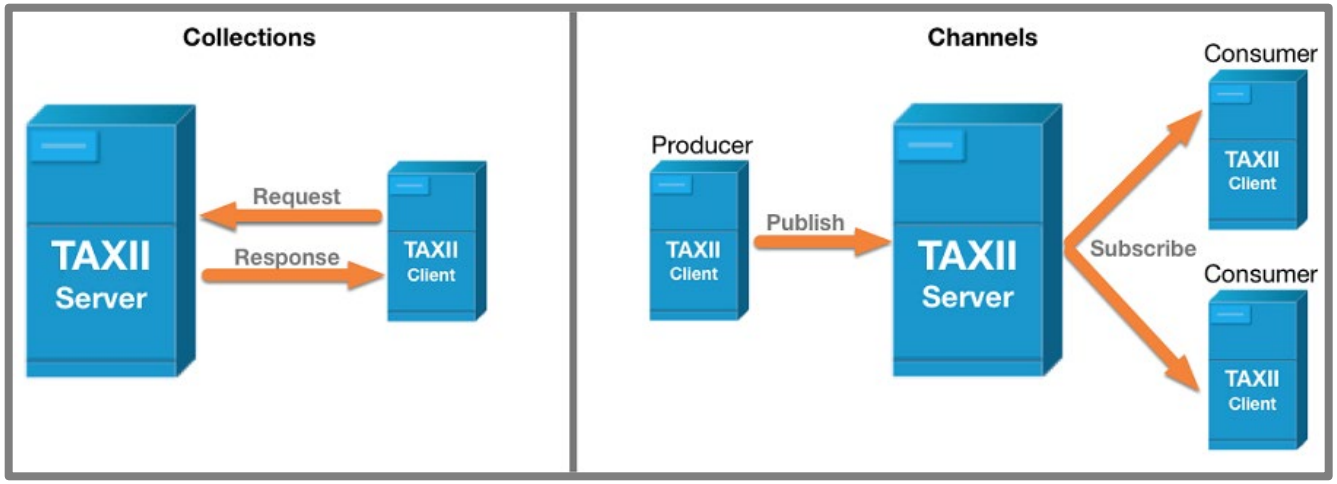


Source: https://oasis-open.github.io/cti-documentation/stix/intro

TAXII is a protocol for exchanging cyber threat intel.

Services:

- Collections – An interface to a logical repository with information exchanged in a request/response model.
- Channels:
  - Producers can push data to many consumers
  - Consumers can receive data from many producers



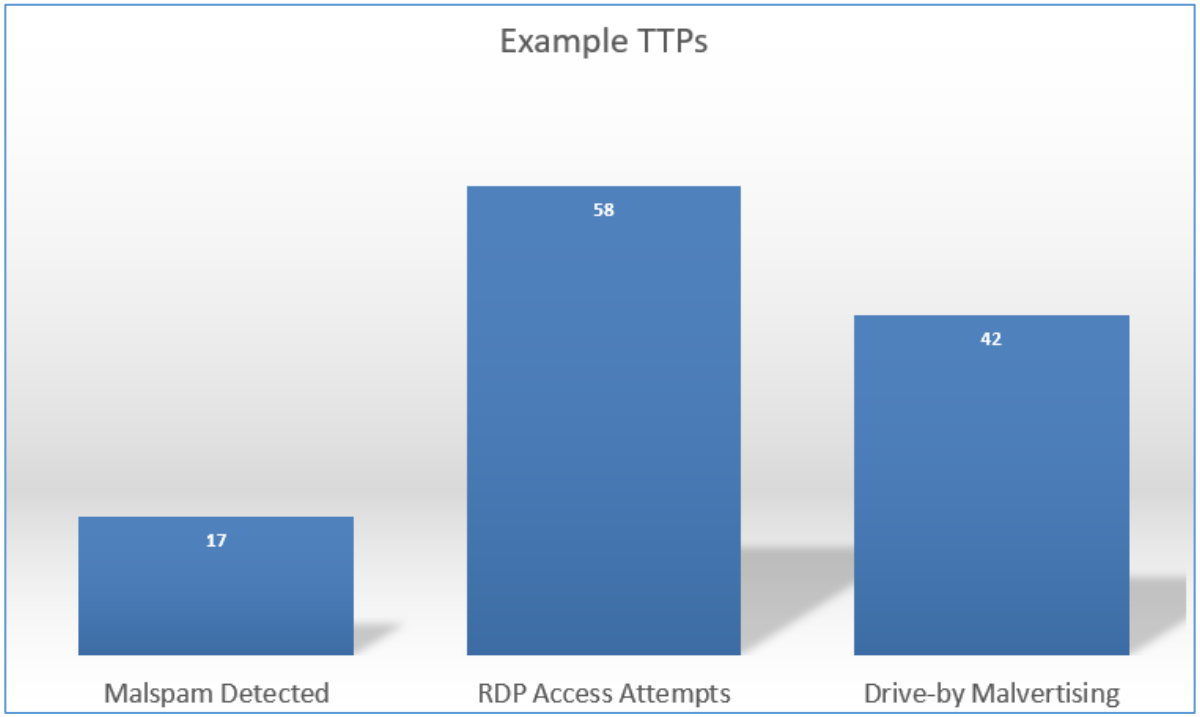
Source: https://oasis-open.github.io/cti-documentation/taxii/intro.html

- Customers / Partners:
  - OpDivs
  - CISA
  - Federal Healthcare Partners
  - HPH Sector
  - HHS Department-level Management
  - Law Enforcement

- Communication may include:
  - Automated means, such as feeds
  - Webinars
  - Notifications
  - Reports and distributions
  - Analyst-to-analyst collaboration
  - Sharing restrictions

- How would knowing IOCs be translated into protecting the Department's information and systems?
- It is best to prevent attacks at the earliest step
- Defense in depth addresses protections at multiple attack steps

- It is easy to count the number of IOCs observed
- It is hard to count things that did not happen (prevented attacks)
- Metrics on particular observed TTPs, along with gap analysis, can help prioritize defenses



Reference Materials

References

- FireEye. 2020. *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST backdoor | FireEye Inc.* December 13. Accessed June 14, 2021. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.

- MITRE. 2021. *Cobalt Group, Cobalt Gang, Cobalt Spider, Group G0080 | MITRE.* April 26. Accessed June 14, 2021. https://attack.mitre.org/groups/G0080.

- —. 2021. *MITRE ATT&CK.* May 20. Accessed June 14, 2021. https://attack.mitre.org.

- NIST Computer Security Resource Center. n.d. *Tactics, Techniques, and Procedurs (TTP) - Glossary.* Accessed June 14, 2021. https://csrc.nist.gov/glossary/term/Tactics_Techniques_and_Procedures.

- NSA. 2020. *NSA Cybersecurity Advisory: Malicious Actors Abuse Authentication Mechanisms to Access Cloud Resources > National Security Agency Central Security Service > Article.* December 17. Accessed June 14, 2021. https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2451159/nsa-cybersecurity-advisory-malicious-actors-abuse-authentication-mechanisms-to/#pop4744190.

- OASIS Open. 2021. *Introduction to STIX.* May 20. Accessed June 14, 2021. https://oasis-open.github.io/cti-documentation/stix/intro.

- —. 2021. *Introduction to TAXII.* May 20. Accessed June 14, 2021. https://oasis-open.github.io/cti-documentation/taxii/intro.html.

- —. n.d. *OASIS Cyber Threat Intelligence (CTI) TC | OASIS.* Accessed June 14, 2021. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti.

Questions

Upcoming Briefs

- 7/8 – Conti Ransomware

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**.

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at **HHS.GOV/HC3**.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV