INDICATORS OF BEHAVIOR

Discovering the Indicators of Behavior:

Collaborative Integration with CACAO Roaster, STIX Shifter, TAXII, and Kestrel

Charlie Frick, IOB Sub-Project Chair
The Johns Hopkins University Applied Physics Laboratory

Talk for April 2024 CASP Cybersecurity Automation Village

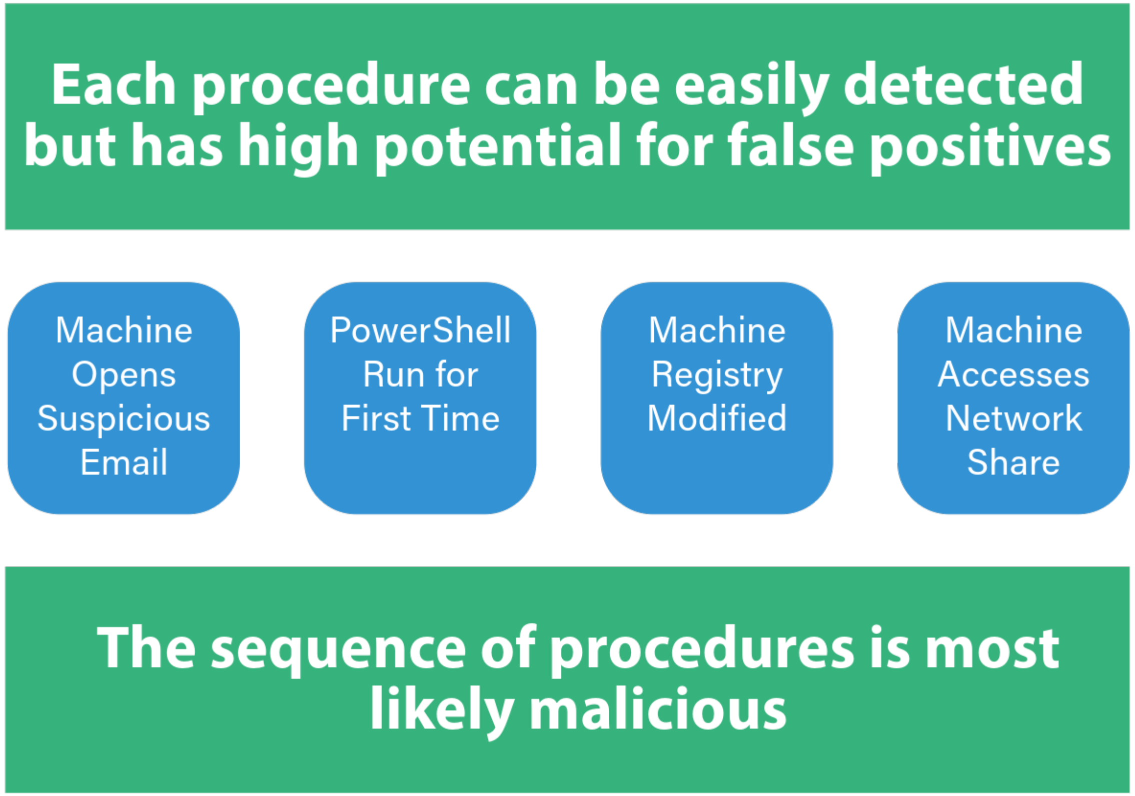
Agenda

- Short IOB background/overview
- Creating an Olympic Destroyer IOB
- Sharing STIX IOBs via TAXII
- Neo4J analysis of IOB contents
    - Kestrel and Stix-Shifter hunt elements
    - Playbooks shared in CACAO format
- Editing IOB with STIX-Modeler and CACAO-ROASTER
- Conclusion

Green = Open Source Projects / Standards

Indicator of Behavior Concept

- Indicator of Behavior (IOB) STIX bundles provide repeatable sets of observed adversary behaviors to help defender tools & capabilities
  - Intelligence context provided in machine-readable graph representation
  - Relationships to relevant ATT&CK attack pattern objects
  - Relationships to detection analytics
  - Includes correlation workflows to address false-positives
  - Includes response COAs and cybersecurity operations playbooks in standardized formats



Each procedure can be easily detected but has high potential for false positives

Machine Opens Suspicious Email

PowerShell Run for First Time

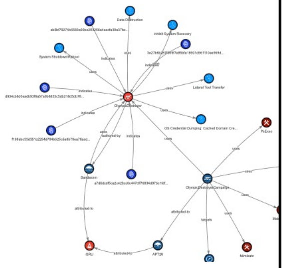
Machine Registry Modified

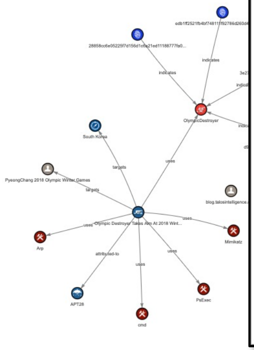
Machine Accesses Network Share

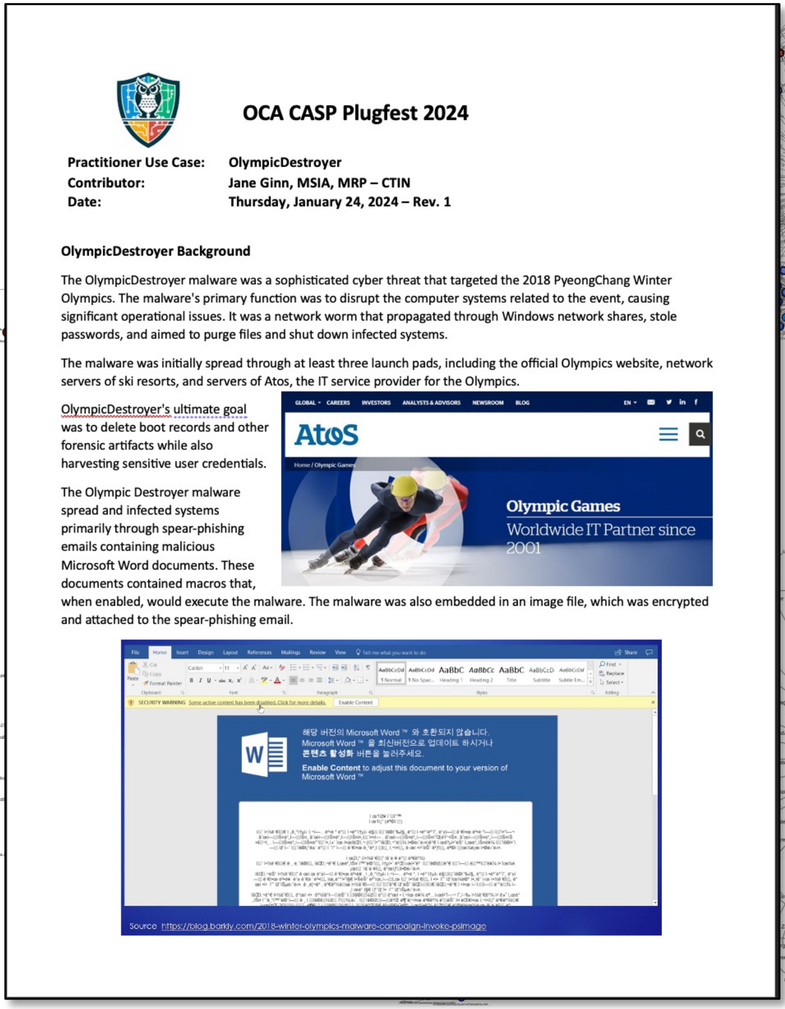
The sequence of procedures is most likely malicious

Creating an IOB Bundle for Olympic Destroyer

- Review existing CTI
  - STIX Bundles
  - Threat Reports







OCA CASP Plugfest 2024

Practitioner Use Case: OlympicDestroyer
Contributor: Jane Ginn, MSIA, MRP – CTIN
Date: Thursday, January 24, 2024 – Rev. 1

OlympicDestroyer Background

The OlympicDestroyer malware was a sophisticated cyber threat that targeted the 2018 PyeongChang Winter Olympics. The malware's primary function was to disrupt the computer systems related to the event, causing significant operational issues. It was a network worm that propagated through Windows network shares, stole passwords, and aimed to purge files and shut down infected systems.

The malware was initially spread through at least three launch pads, including the official Olympics website, network servers of ski resorts, and servers of Atos, the IT service provider for the Olympics.

OlympicDestroyer's ultimate goal was to delete boot records and other forensic artifacts while also harvesting sensitive user credentials.

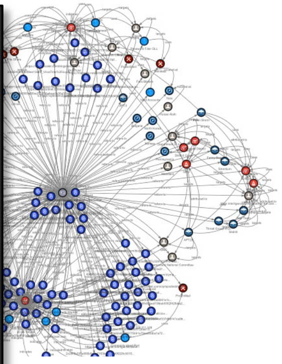
The Olympic Destroyer malware spread and infected systems primarily through spear-phishing emails containing malicious Microsoft Word documents. These documents contained macros that, when enabled, would execute the malware. The malware was also embedded in an image file, which was encrypted and attached to the spear-phishing email.

SECURITY WARNING Some active content has been disabled. Click for more details.

해당 버전의 Microsoft Word ™ 와 호환되지 않습니다.
Microsoft Word ™ 을 최신버전으로 업데이트 하시거나
콘텐츠 활성화 버튼을 눌러주세요.

Enable Content to adjust this document to your version of Microsoft Word ™

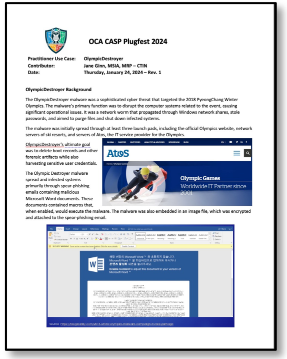
Source https://blog.barkly.com/2018-winter-olympics-malware-campaign-invoke-psimage



Creating an IOB Bundle for Olympic Destroyer

- Review existing CTI
  - STIX Bundles
  - Threat Reports
- Extract TTPs from Report

Note: IOB bundles utilize MITRE ATT&CK Attack Patterns



OCA CASP Plugfest 2024

Practitioner Use Case: **OlympicDestroyer**
Contributor: **Jane Ginn, MSIA, MRP – CTIN**
Date: **Thursday, January 24, 2024 – Rev. 1**

OlympicDestroyer Background

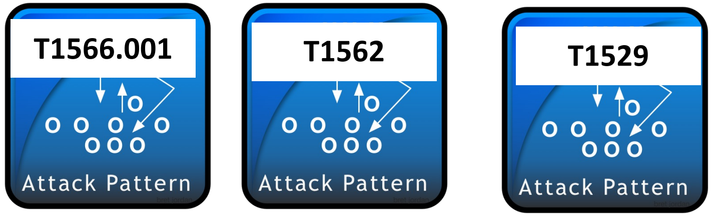
The OlympicDestroyer malware was a sophisticated cyber threat that targeted the 2018 PyeongChang Winter Olympics. The malware's primary function was to disrupt the computer systems related to the event, causing significant operational issues. It was a network worm that propagated through Windows network shares, stole passwords, and aimed to purge files and shut down infected systems.

The malware was initially spread through at least three launch pads, including the official Olympics website, network servers of ski resorts, and servers of Atos, the IT service provider for the Olympics.

OlympicDestroyer's ultimate goal was to delete boot records and other forensic artifacts while also harvesting sensitive user credentials.

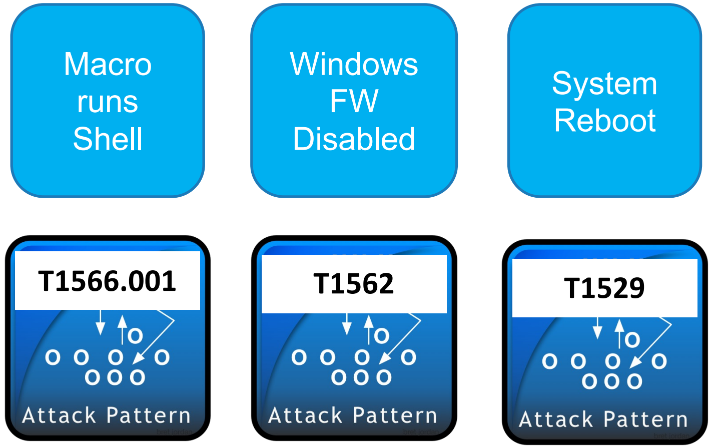
The Olympic Destroyer malware spread and infected systems primarily through spear-phishing emails containing malicious Microsoft Word documents. These documents contained macros that, when enabled, would execute the malware. The malware was also embedded in an image file, which was encrypted and attached to the spear-phishing email.

Atos
Olympic Games
Worldwide IT Partner since 2001
해당 버전의 Microsoft Word ™ 와 호환되지 않습니다.
Microsoft Word ™ 을 최신버전으로 업데이트 하시거나
콘텐츠 활성화 버튼을 눌러주세요.
Enable Content to adjust this document to your version of Microsoft Word ™
Source: https://blog.barkly.com/2018-winter-olympics-malware-campaign-invoke-psimage


T1566.001
Attack Pattern
T1562
Attack Pattern
T1529
Attack Pattern

Creating an IOB Bundle for Olympic Destroyer

- Review existing CTI
  - STIX Bundles
  - Threat Reports
- Extract TTPs from Report
- Identify and Create Behaviors



Macro runs Shell

Windows FW Disabled

System Reboot

T1566.001 Attack Pattern

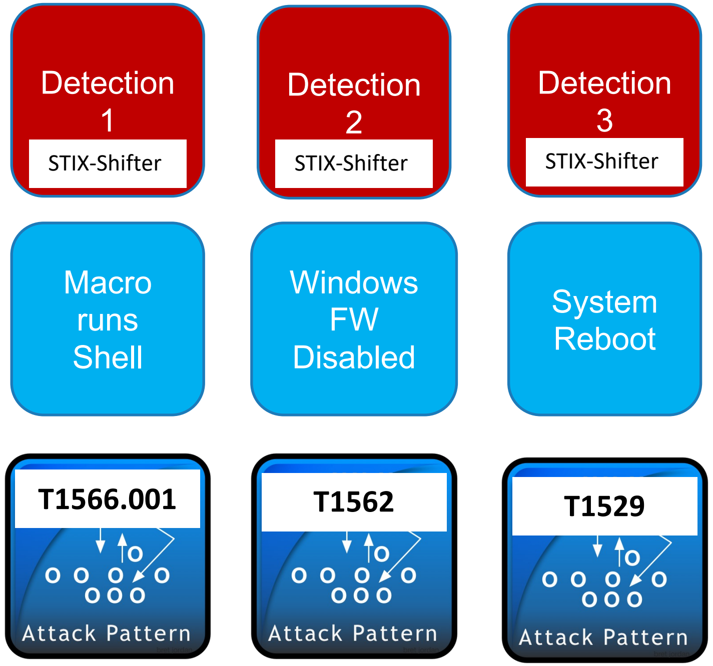
T1562 Attack Pattern

T1529 Attack Pattern

Creating an IOB Bundle for Olympic Destroyer

- Review existing CTI
  - STIX Bundles
  - Threat Reports
- Extract TTPs from Report
- Identify and Create Behaviors
- Develop Detections

Note: CASP 2024 example uses STIX-Shifter but other analytics can also be used as well



Detection 1
STIX-Shifter

Detection 2
STIX-Shifter

Detection 3
STIX-Shifter

Macro runs Shell

Windows FW Disabled

System Reboot

T1566.001
Attack Pattern

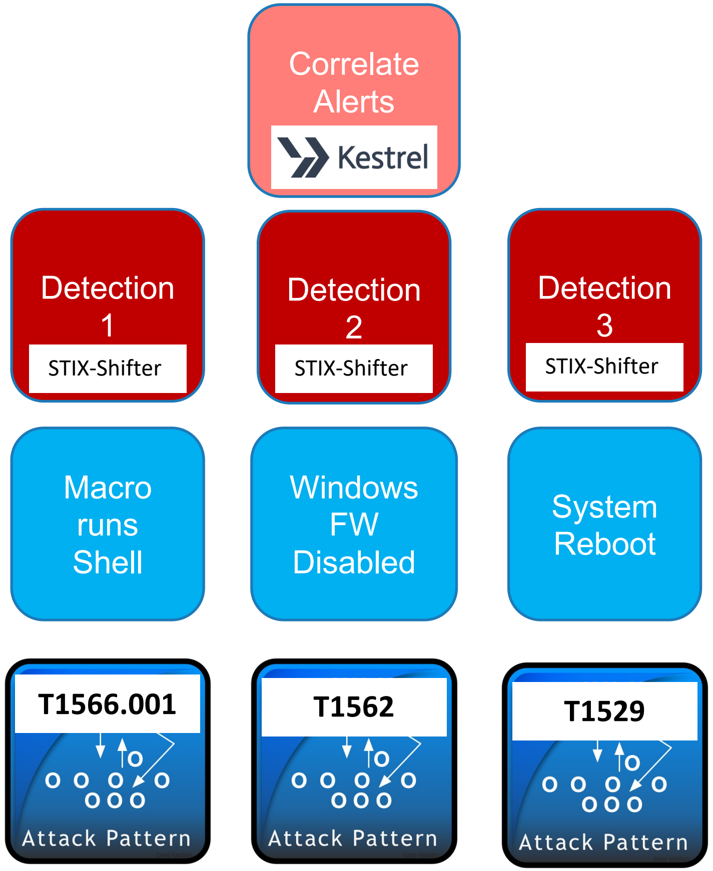
T1562
Attack Pattern

T1529
Attack Pattern

Creating an IOB Bundle for Olympic Destroyer

Note: CASP 2024 example uses Kestrel but other correlation engines can be used as well

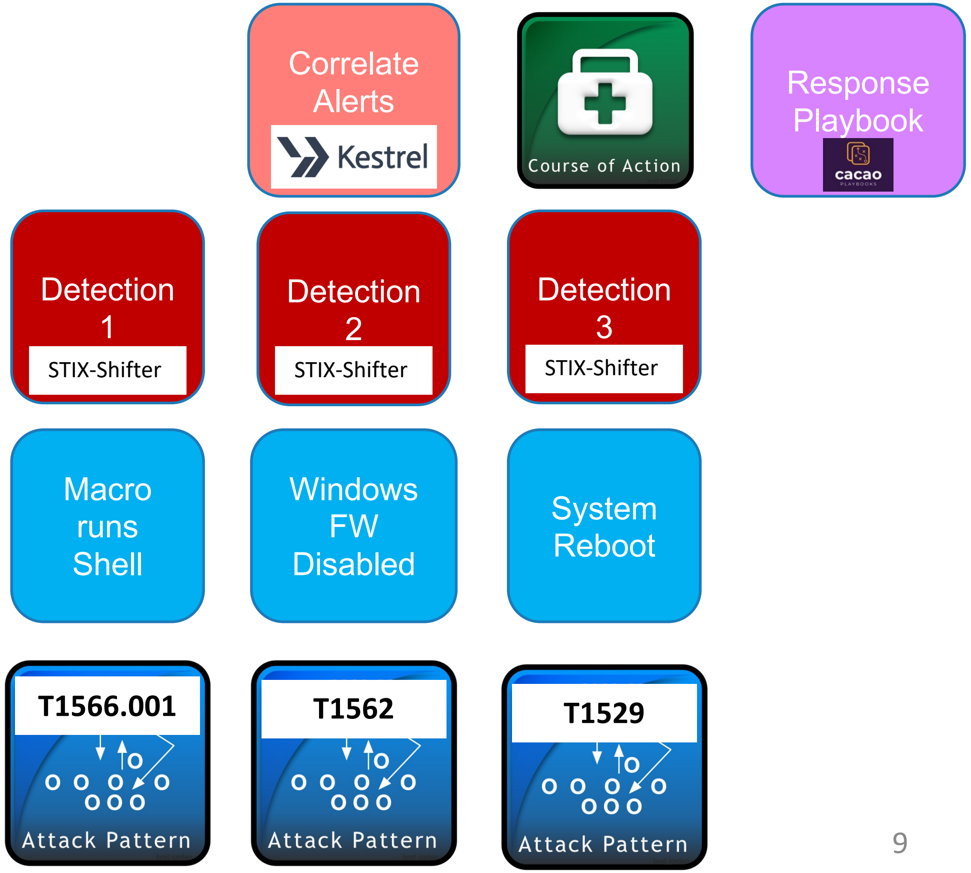
- Review existing CTI
  - STIX Bundles
  - Threat Reports
- Extract TTPs from Report
- Identify and Create Behaviors
- Develop Detections
- Develop Correlations



Creating an IOB Bundle for Olympic Destroyer

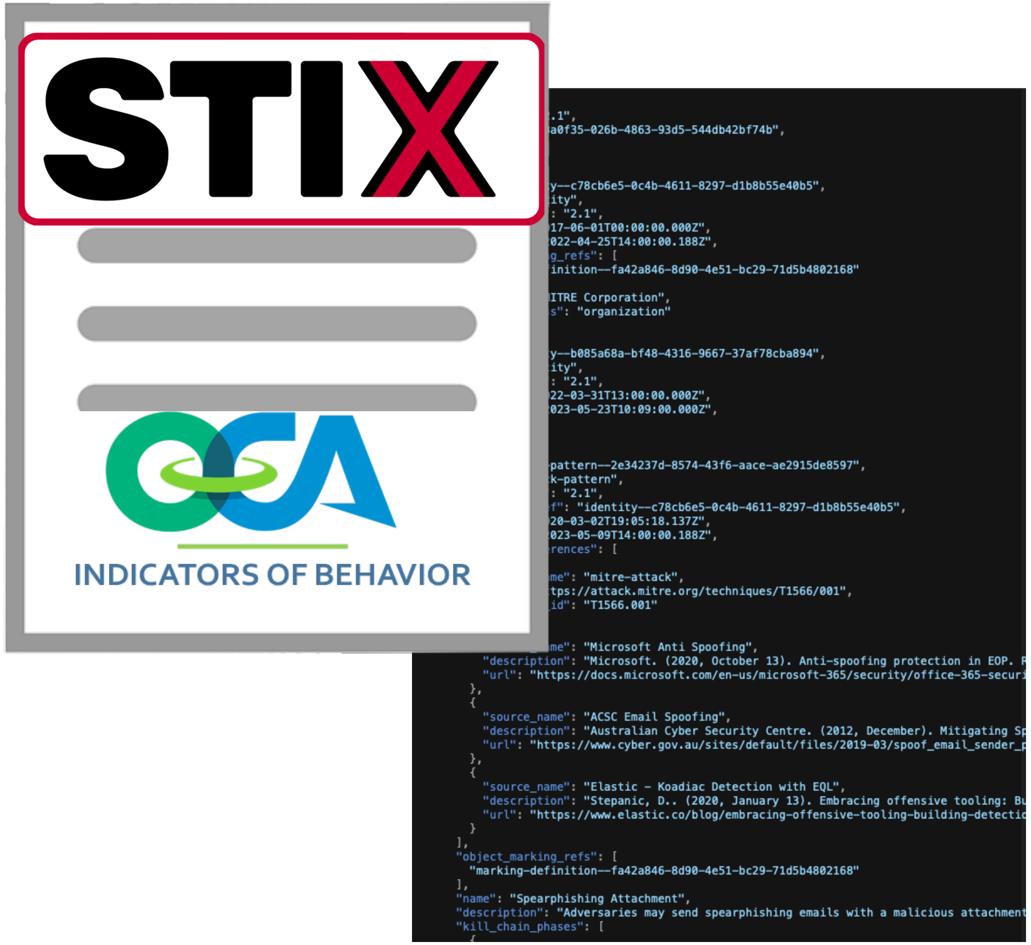
Note: CASP 2024 example uses CACAO but other playbooks could be used as well

- Review existing CTI
  - STIX Bundles
  - Threat Reports
- Extract TTPs from Report
- Identify and Create Behaviors
- Develop Detections
- Develop Correlations
- Develop Response



Creating an IOB Bundle for Olympic Destroyer

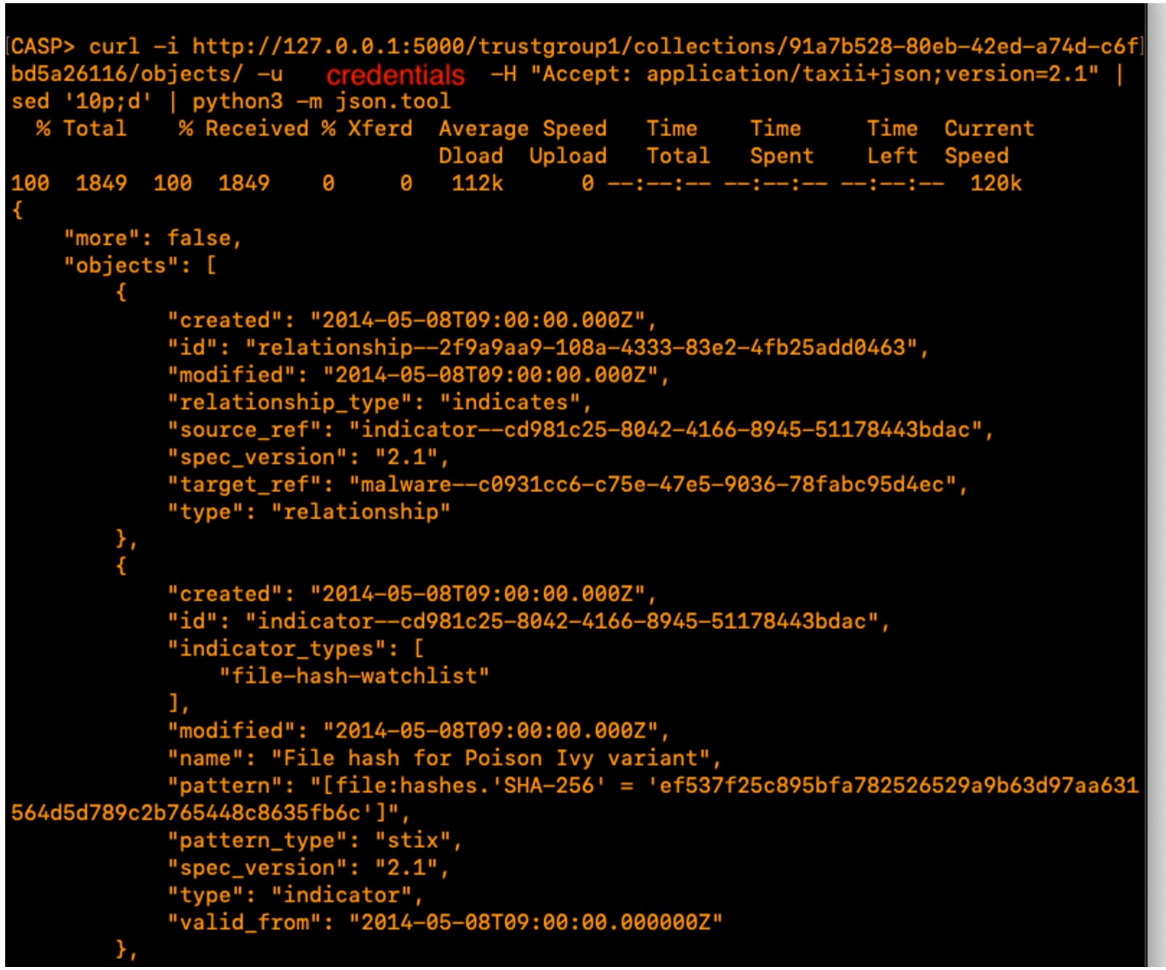
- Review existing CTI
    - STIX Bundles
    - Threat Reports
- Extract TTPs from Report
- Identify and Create Behaviors
- Develop Detections
- Develop Correlations
- Develop Response
- Combine into STIX IOB Bundle



```
.1",
a0f35-026b-4863-93d5-544db42bf74b",



y--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
ity",
: "2.1",
17-06-01T00:00:00.000Z",
022-04-25T14:00:00.188Z",
g_refs": [
inition--fa42a846-8d90-4e51-bc29-71d5b4802168"

ITRE Corporation",
s": "organization"


y--b085a68a-bf48-4316-9667-37af78cba894",
ity",
: "2.1",
22-03-31T13:00:00.000Z",
023-05-23T10:09:00.000Z",



pattern--2e34237d-8574-43f6-aace-ae2915de8597",
k-pattern",
: "2.1",
f": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
20-03-02T19:05:18.137Z",
023-05-09T14:00:00.188Z",
rences": [

me": "mitre-attack",
tps://attack.mitre.org/techniques/T1566/001",
id": "T1566.001"


me": "Microsoft Anti Spoofing",
      "description": "Microsoft. (2020, October 13). Anti-spoofing protection in EOP. R
      "url": "https://docs.microsoft.com/en-us/microsoft-365/security/office-365-securi
    },
    {
      "source_name": "ACSC Email Spoofing",
      "description": "Australian Cyber Security Centre. (2012, December). Mitigating Sp
      "url": "https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_p
    },
    {
      "source_name": "Elastic - Koadiac Detection with EQL",
      "description": "Stepanic, D.. (2020, January 13). Embracing offensive tooling: Bu
      "url": "https://www.elastic.co/blog/embracing-offensive-tooling-building-detectio
    }
  ],
  "object_marking_refs": [
    "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
  ],
  "name": "Spearphishing Attachment",
  "description": "Adversaries may send spearphishing emails with a malicious attachment
  "kill_chain_phases": [
    {
```

TAXII Compliance

- By adhering to the open STIX standard, IOB bundles can be sent/received at machine speed via the open TAXII standard



```
[CASP> curl -i http://127.0.0.1:5000/trustgroup1/collections/91a7b528-80eb-42ed-a74d-c6f]
bd5a26116/objects/ -u    credentials  -H "Accept: application/taxii+json;version=2.1" |
sed '10p;d' | python3 -m json.tool
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1849  100  1849    0     0   112k      0 --:--:-- --:--:-- --:--:--  120k
{
    "more": false,
    "objects": [
        {
            "created": "2014-05-08T09:00:00.000Z",
            "id": "relationship--2f9a9aa9-108a-4333-83e2-4fb25add0463",
            "modified": "2014-05-08T09:00:00.000Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--cd981c25-8042-4166-8945-51178443bdac",
            "spec_version": "2.1",
            "target_ref": "malware--c0931cc6-c75e-47e5-9036-78fabc95d4ec",
            "type": "relationship"
        },
        {
            "created": "2014-05-08T09:00:00.000Z",
            "id": "indicator--cd981c25-8042-4166-8945-51178443bdac",
            "indicator_types": [
                "file-hash-watchlist"
            ],
            "modified": "2014-05-08T09:00:00.000Z",
            "name": "File hash for Poison Ivy variant",
            "pattern": "[file:hashes.'SHA-256' = 'ef537f25c895bfa782526529a9b63d97aa631
564d5d789c2b765448c8635fb6c']",
            "pattern_type": "stix",
            "spec_version": "2.1",
            "type": "indicator",
            "valid_from": "2014-05-08T09:00:00.000000Z"
        },
```

Open tools to support IOB analysis and creation

STIX2NEO4J Script

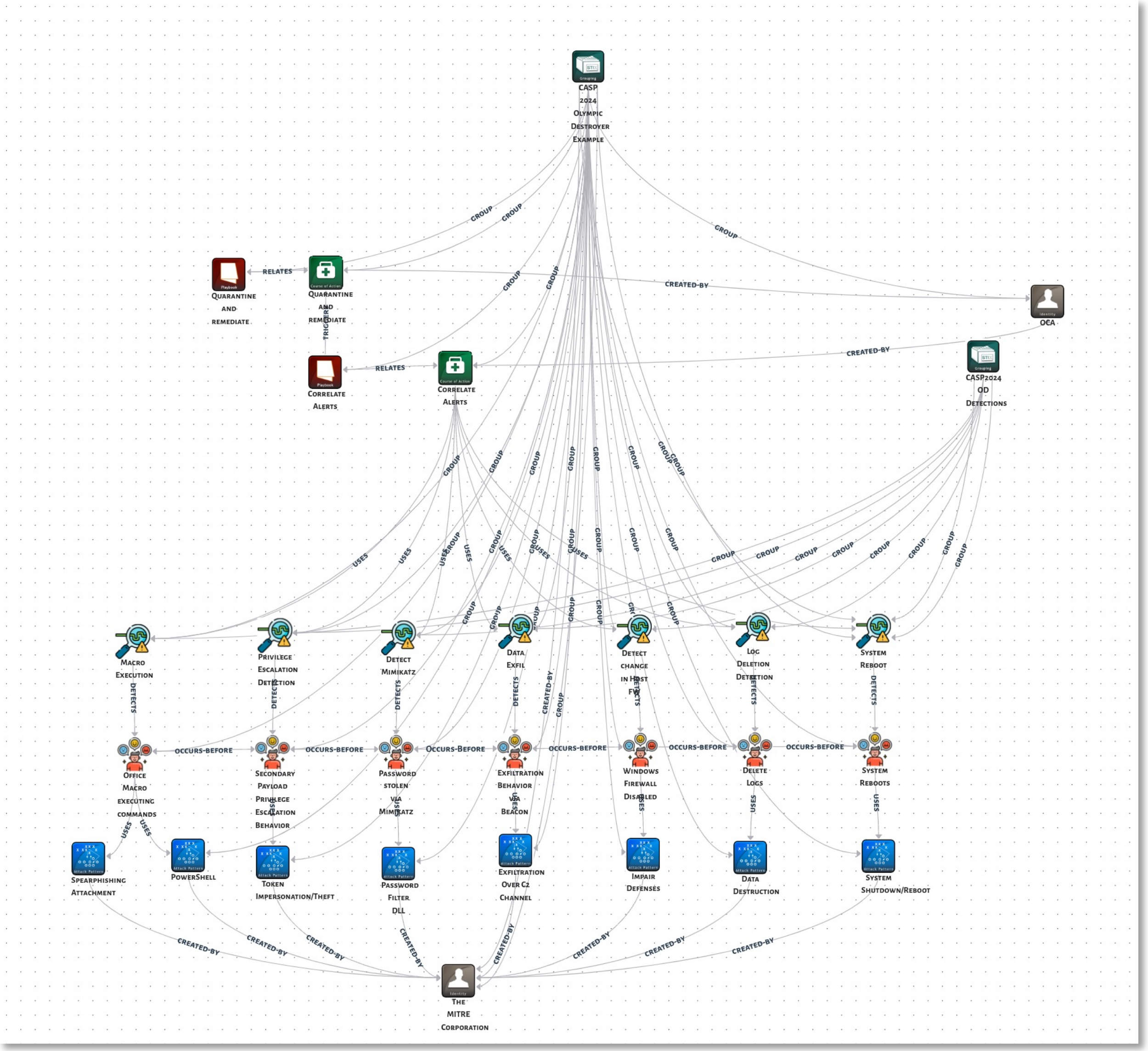
- Python script for analyzing STIX 2.x bundles in a neo4j graph database
- Provides additional analytical capabilities for investigating raw STIX messages without major modification of the data
- Threat Intel Platforms often make significant changes to data model upon import
- Released on an Apache2 license through the Open Cybersecurity Alliance Indicator of Behavior Sub-Project
- Script repository link on GitHub:
  - https://github.com/opencybersecurityalliance/oca-iob/tree/main/STIX2NEO4J%20Converter

INDICATORS OF BEHAVIOR

SCAN ME

STIX Modeler

- IOB work on edits to Open Source STIX-Modeler Project on GitHub
  - https://github.com/STIX-Modeler/UI
  - IOB edits currently in release review with planned submission to GitHub later in 2024
- GUI-based editor for creating STIX without coding
- Modernized code dependencies and visualization framework
- Created support for STIX extensions and custom STIX objects and relationships



Demonstration

Receiving an IOB Bundle
Extracting data via Neo4J
Integration into Kestrel, CACAO-Roaster
Editing of Data via STIX Modeler

For More Information

- IOB Project page: https://opencybersecurityalliance.org/iob/
- IOB GitHub for documentation, use cases, reference implementation https://github.com/opencybersecurityalliance/oca-iob