



July 2023

REFERENCE IMPLEMENTATION REVISION 2 FOR REPRESENTATION OF CYBER ADVERSARY BEHAVIOR IN STRUCTURED THREAT INFORMATION EXCHANGE (STIX) FORMAT

Prepared by:

The Johns Hopkins University
Applied Physics Laboratory
11100 Johns Hopkins Rd.
Laurel, Maryland 20723-6099

Authors:

Charles Frick, Charles.Frick@jhuapl.edu
Tim Zhan
Kurt Karolenko



APL Research Team

- Emma Lubes
- Jason O'Connor
- Ali Shahegh

Prepared for: The Cybersecurity and Infrastructure Security Agency

Distribution Statement A. Approved for public release: distribution unlimited.

Disclaimer: The views and conclusions contained in this document are those of the author and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security / Cybersecurity and Infrastructure Security Agency.

CONTENTS

1. Introduction	4
2. Behavior sharing research	4
2.1 Motivation for the Research	4
2.2 Research Environment.....	4
2.3 Initial Behavior Set Reference Implementation	6
3. Next steps	29
4. Acknowledgement.....	29
5. Conclusion.....	29
6. Appendix A: Acronymns.....	30
7. Appendix B: Complete behavior set STIX bundle.....	31

FIGURES

Figure 1: Reference implementation research environment.....5

Figure 2: Reference implementation emulated attack scenario.....7

Figure 3: Visualization of reference implementation behavior set STIX bundle.....9

Figure 4 Neo4J visualization of reference implementation data 10

Figure 5 Neo4J visualization of core reference implementation data elements 11

Figure 6: Simplified example of adversary behaviors.....21

Figure 7: Conceptual process for detection correlation logic.....25

Figure 8 Shared playbook for system quarantine29

1. INTRODUCTION

The Johns Hopkins University Applied Physics Laboratory (APL), under the sponsorship of the Cybersecurity and Infrastructure Security Agency (CISA), seeks to dramatically change the timeline and effectiveness of cyber defense via integration, automation, and information sharing. Towards this goal, Johns Hopkins APL is providing a reference implementation for our research into machine readable objects, in Structured Threat Information eXchange (STIX)¹ format, to represent cyber adversary behaviors on a network. This report provides an overview of the research methodology as well as a guide for understanding the content and concepts within the reference implementation object.

2. BEHAVIOR SHARING RESEARCH

The key focus of APL's adversary behavior research is the generation of machine-readable objects to represent adversary behavior on a target network. This is an evolution of previous APL research conducted for CISA and as part of the Integrated Adaptive Cyber Defense (IACD)² framework.

Previous research focused on designing the proper format to hold adversary behavior. The use of custom objects within STIX standard version 2.1 was the format chosen based on those efforts. For this reference implementation, APL research focused on the creation of the content for a robust machine-readable STIX bundle that could be shared throughout a community. This design allows both human analysts and automation to use the shared information to detect an adversary's observed behavior within the victim network.

2.1 Motivation for the Research

Previous APL work under the IACD program identified a significant gap in Cyber Threat Intelligence (CTI) sharing when that sharing is solely focused on Indicators of Compromise (IOCs). IOCs by their very nature have a limited time window of being actionable towards network defense. While significant progress with Security Orchestration, Automation and Response (SOAR) has been achieved to take action on IOCs within a viable timeline for network defense, there remains a clear need for sharing data that can help a community of network defenders proactively defend against advanced attacks.

2.2 Research Environment

APL maintains a robust virtualization testbed environment to support our research and experimentation efforts. Figure 1 provides a summary of how a dedicated enclave of that environment was configured for the development of the reference implementation.

¹ <https://oasis-open.github.io/cti-documentation/>

² <https://iacdautomate.org>

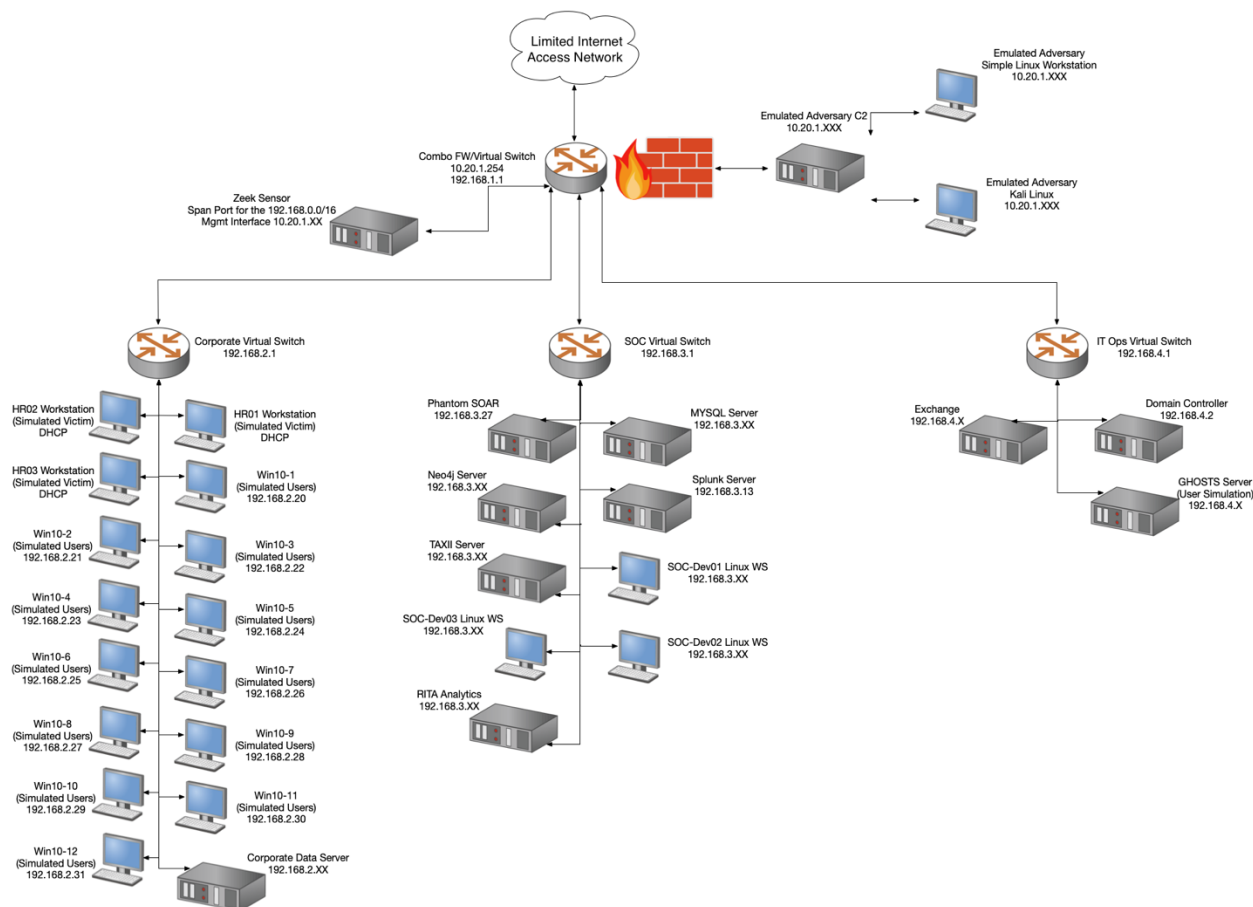


Figure 1: Reference implementation research environment

The research environment is sectioned into four main enclaves. The following description of the enclaves provides an overview of the tools used in creation of the reference implementation but is not provided as any form of endorsement for any singular technology or open-source project:

- An emulated adversary enclave implementing common threat emulation tools such as Cobalt Strike³
- An emulated corporate enclave containing:
 - Windows workstations automated with the Carnegie Mellon University (CMU) GHOSTS⁴ agent to create benign user activity within the network
 - Splunk⁵ Security Information and Event Management (SIEM) forwarders for SYSMON⁶ and Windows event logs
 - A file server to contain emulated sensitive information that would be the adversary's target for data exfiltration

³ <https://www.cobaltstrike.com>

⁴ <https://github.com/cmu-sei/GHOSTS>

⁵ <https://www.splunk.com>

⁶ <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

- An emulated Network Operations Center enclave containing:
 - Windows domain controller for Active Directory
 - Exchange email server
 - Command and control for the CMU GHOSTS agents
- An emulated Security Operations Center enclave containing:
 - A Zeek⁷ network sensor to analyze traffic
 - A Trusted Automated eXchange of Indicator Information (TAXII) server for the transmission of any shared STIX objects
 - A MySQL⁸ database server for holding STIX data internally to the network
 - This was done to simulate a very basic Threat Intel Platform (TIP) capability since the research for the reference implementation did not require all the features of a TIP
 - A Real Intelligence Threat Analytics (RITA)⁹ server for generation of beaconing alerts from the Zeek analytics
 - A Splunk SIEM for detecting adversary activity
 - Used in research analysis to develop a shared behavior object
 - Also used from the point of view as a recipient who would receive a bundle and translate that data into analytics for a SIEM
 - A Splunk SOAR platform for automating SOC activities
 - While not heavily used in the reference implementation, work was done to update and use SOAR to support future research on automating the behavior development process as well as executing future correlation and response actions

2.3 Initial Behavior Set Reference Implementation

APL's research focuses on creating STIX "behavior-set" bundles. These bundles represent sequences of observed adversary behaviors within a network that are not dependent on traditional IOCs (file hash, URL, IP address, etc.). Instead, the bundles include detection analytics for individual behaviors as well as information on how to correlate behaviors to better detect and prioritize a sequence of observed adversary behaviors. Additionally, this STIX bundle also provides information on observables used to generate the behaviors, detector descriptions, data components/sources, courses of actions to take once a sequence is detected, and shareable playbooks to achieve the shared courses of action.

Bundles such as the reference implementation are intended to augment a larger set of CTI within the STIX standard. As behaviors represent sequences of procedures conducted by an adversary, they are inherently linked to adversary tactics and techniques, represented within the MITRE ATT&CK^{®10} framework. The goal of the behavior sets and detection bundles is to provide more actionable detection techniques than those present in the ATT&CK description. Achieving this goal will make it easier for community and vendors to rapidly add detections for advanced

⁷ <https://github.com/zeek/zeek>

⁸ <https://www.mysql.com>

⁹ <https://github.com/activecm/rita>

¹⁰ <https://attack.mitre.org>

attacks that could assist with defense against multiple campaigns by a cyber adversary or set of adversaries.

A summary of the overall goals for the reference implementation research follows:

- Emulate threat behaviors
- Identify and create behavior objects
- Correlate behavior objects into behavior sets
- Create detection objects for behavior sets
- Develop a STIX bundle to include:
 - Behavior Set
 - Observables
 - Detections
 - Detectors
 - Detection Groups for correlation
 - Courses of Action
 - Playbooks
- Store and share the STIX bundle

2.3.1 Adversary Scenario

To properly capture a realistic set of adversary behaviors, APL required a representative sample adversary attack. Figure 2 provides a visual representation of the sample attack that was based on the “APT 37/Reaper”¹¹ campaign.

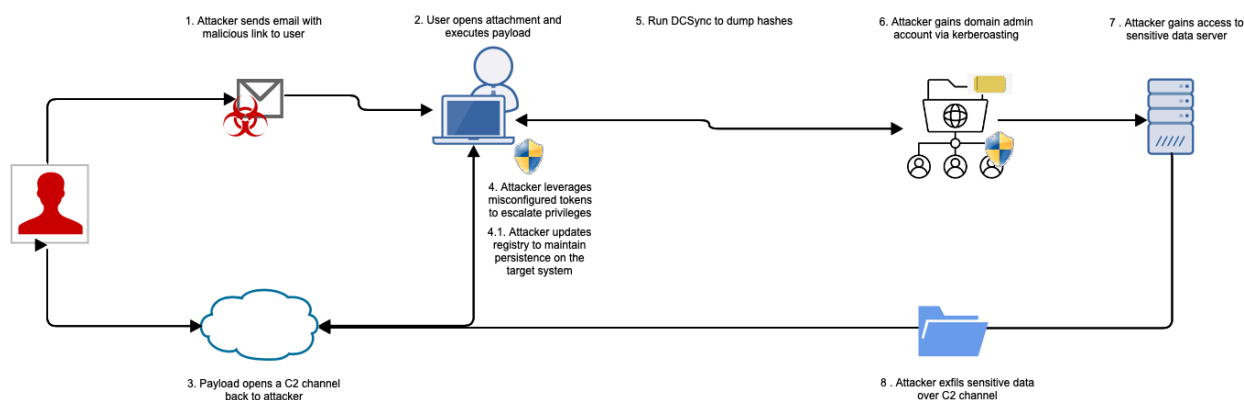


Figure 2: Reference implementation emulated attack scenario

The overall steps in this attack include:

1. Attacker sends an email to the target organization with a malicious link.
2. The user opens the attachment and executes a malicious office macro payload.

¹¹ https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

- The details of the file are traditionally shared as IOCs, but those details are often modified rapidly by the attacker, reducing the effectiveness of the IOC in enabling network defense across a community.
- 3. The payload establishes a command and control (C2) channel to adversary infrastructure.
 - The domains and/or IP addresses of the C2 server are traditionally shared as IOCs, but those details are often modified rapidly by the attacker, reducing the effectiveness of the IOC in enabling network defense across a community.
- 4. The attacker escalates privileges on the initial victim machine.
 - The attacker leverages misconfigured tokens to escalate privileges.
 - The attacker then updates the initial victim machine registry to maintain persistence.
- 5. The attacker uses the "DCSync"¹² capability to retrieve password hashes from the target network's domain controller.
- 6. The attacker then uses the "kerberoasting"¹³ technique to gain access as a domain administrator account.
- 7. The attacker uses this compromised administrator account to gain access to a sensitive data server.
- 8. The attacker then exfiltrates sensitive data via the established C2 channel.

2.3.2 Behavior Set STIX Bundle

The full text of the reference implementation STIX bundle for representing an adversary set of behaviors is provided in [Appendix B](#). Figure 3 provides a visualization of the bundle via the STIX visualizer from the OASIS standards group.¹⁴

Due to the complex set of information and relationships found within the reference implementation, the default view from the STIX visualizer may be difficult to read. To address this challenge, the IOB Sub-Project released an open source python script to translate this information into a Neo4J graph database.¹⁵ Figure 4 provides a visualization of all the included data within the reference implementation using the Neo4J browser and Figure 5 provides a visualization of the core elements within the reference implementation. It is important to note that the colors used for icons in the Neo4J visualization were chosen to improve readability in this specific documentation and are not the official colors used in the icon set provided by the OASIS standards body.

¹² <https://attack.mitre.org/techniques/T1003/006/>

¹³ <https://attack.mitre.org/techniques/T1558/003/>

¹⁴ <https://oasis-open.github.io/cti-stix-visualization/>

¹⁵ <https://github.com/opencybersecurityalliance/oca-iob/tree/main/STIX2NEO4J%20Converter>

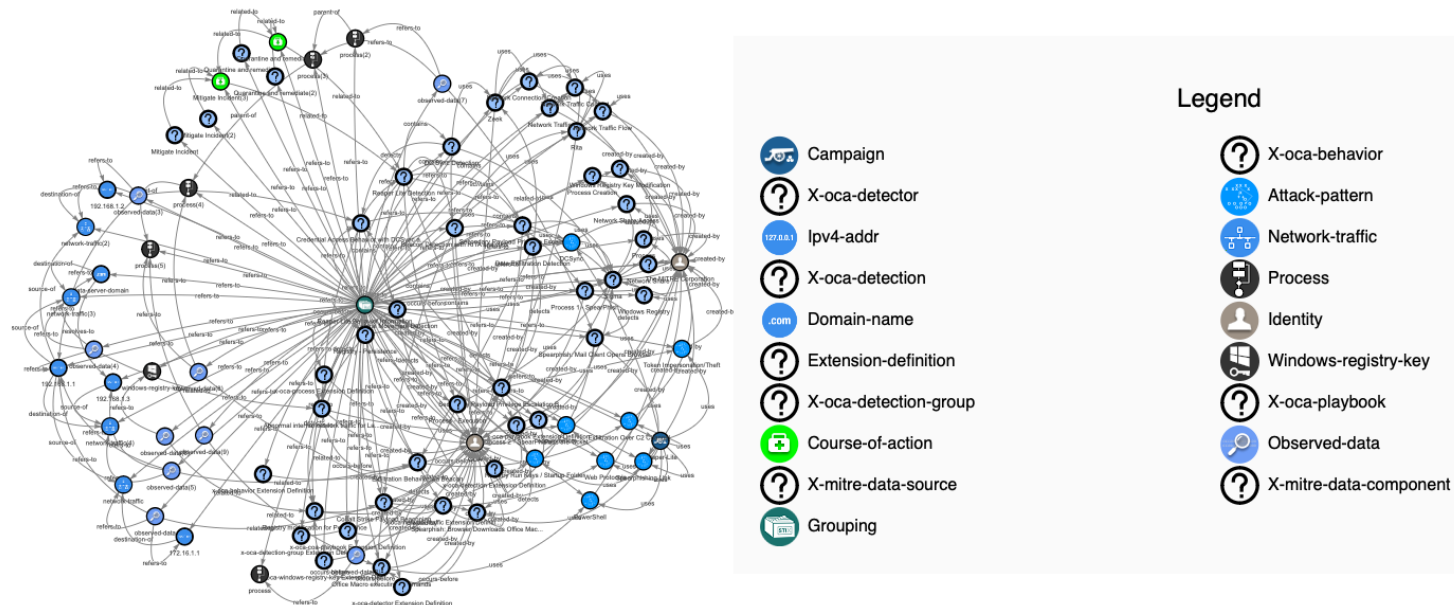


Figure 3: Visualization of reference implementation behavior set STIX bundle



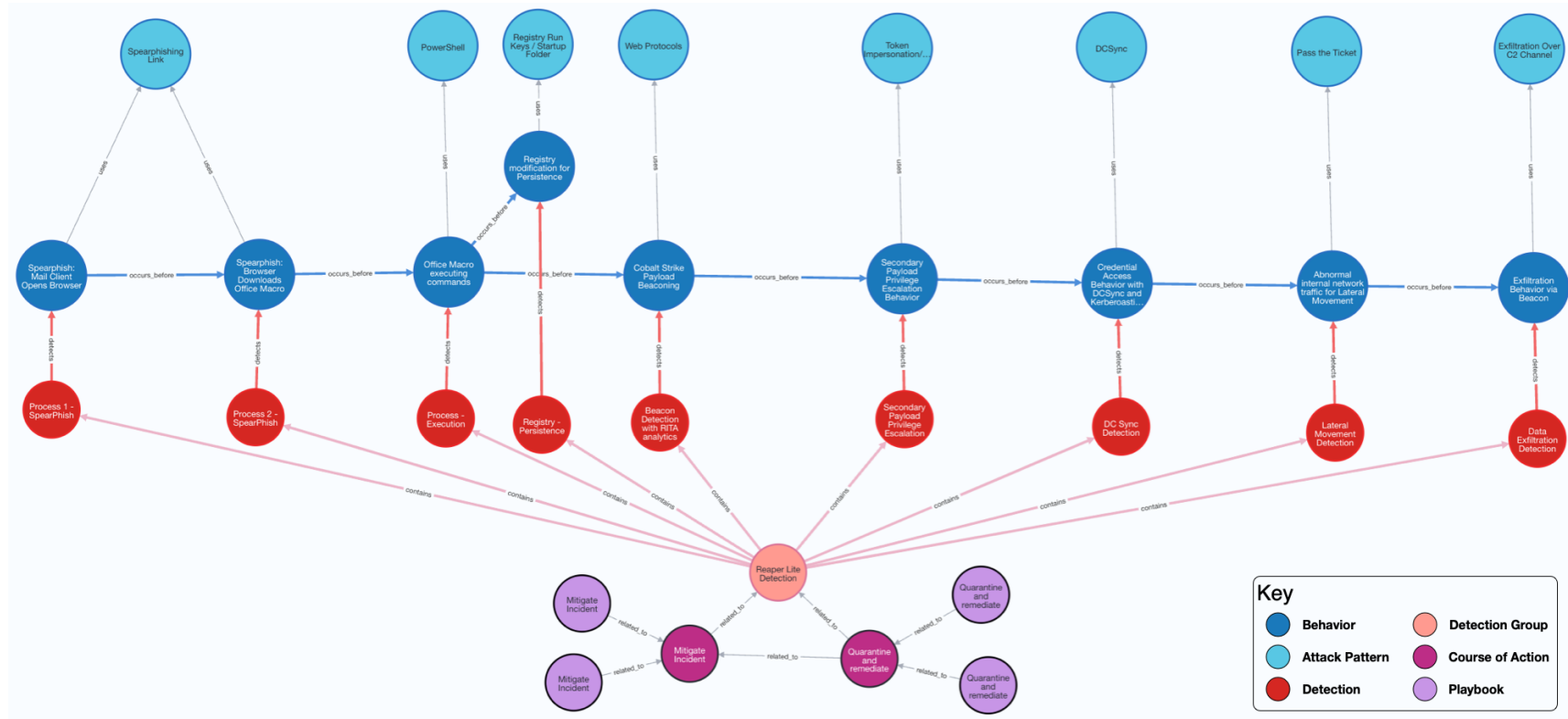




Figure 5 Neo4J visualization of core reference implementation data elements



This reference implementation bundle contains several custom SDOs as well as several custom SCOs. The standard SDO of a “grouping” object was used to represent the observed set of behaviors. The following descriptions of the custom objects provides a key for reading the diagram in Figure 4 with respect to the custom objects:




- Behavior SDO



-  Icon:
- Description: Behavior SDOs represent the observed adversary behaviors within a particular campaign. These consist of a sequence of actions characterized by multiple techniques (and sub-techniques) in pursuit of multiple tactical goals. As such, these objects may contain relationships to STIX Attack-Pattern SDOs that are traditionally used to represent entries in the MITRE ATT&CK framework. These objects exist to provide more actionable data for detection and response than what is currently found in the ATT&CK information.
- Fields within the object:
 - STIX type
 - STIX specification version
 - STIX ID
 - Created by reference
 - Created date
 - Description field
 - Behavior class
 - Modification date
 - Name
 - Tactic
 - Technique
 - First seen date
 - Platforms affected by the behavior
 - Extensions



- Detection SDO




-  Icon:
- Description: Detection SDOs provide information on how to detect a particular behavior observed from a campaign. These detections are presented as analytics referencing the SCOs related to the behavior object. The key distinction is that the analytics are designed to not be IOC specific so that they can relate to multiple occurrences of the behavior. It is possible to have more than a single detection for a behavior. The guidance on how to correlate these detections within a set of behaviors is defined in the Detection Group SDO.
- Fields within the object:
 - STIX type
 - STIX specification version
 - STIX ID
 - Created by reference

- Created date
 - Modification date
 - Name
 - Analytic for detection
 - Data sources to support analytic
- Detector SDO
 - Icon: 
 - Description: The detector SDO provides information on the capabilities used to create a detection. This information is shared so that CTI recipients and their automation can know what capabilities are needed to use an analytic shared within a detection object. This information can be used for detectors that may be more dynamic in nature.
 - Fields within the object:
 - STIX type
 - STIX specification version
 - STIX ID
 - Created by reference
 - Created date
 - Modification date
 - Valid until date
 - Name
 - Common Platform Enumeration for detector (when applicable)
 - Description field
 - Detection types applicable to this detector
 - Detection data categories that support this detector
 - Extensions used within the object
 - Detector product
 - Detector product URL (when applicable)
 - Detector product version
 - Detector vendor
 - Detector vendor URL (when applicable)
 - Data sources to support detector
- Data Source SDO
 - Icon: 
 - Description: To provide a more complete description of the data needed to support detectors/detection, the reference implementation includes examples using the “x-mitre-data-source” SDO from MITRE ATT&CK.
 - Fields within the object:
 - STIX type
 - STIX specification version
 - STIX ID
 - Created by reference
 - Created date
 - Modification date

- Name
- Description Field
- External references
- Object marking
- MITRE ATT&CK version
- MITRE collection layers
- MITRE domains
- Data Component SDO
 - Icon: 
 - Description: To provide a more complete description of the data needed to support detectors/detection, the reference implementation includes examples using the “x-mitre-data-component” SDO from MITRE ATT&CK.
 - Fields within the object:
 - STIX type
 - STIX specification version
 - STIX ID
 - Created by reference
 - Created date
 - Modification date
 - Name
 - Object marking
 - MITRE ATT&CK version
 - Data Source reference
 - MITRE domains
- Detection Group SDO
 - Icon: 
 - Description: The Detection Group SDO is intended to provide the guidance on how to correlate the multiple detections within a grouping of behavior SDOs. As of Spiral 26, APL is still refining the logic and required metadata for strong correlations but the version provided in the Spiral 26 reference implementation conveys the current status of the object.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Created date
 - Modification date
 - Name
 - Description field
 - Correlation workflows describing the correlation procedure
 - List of detection object STIX IDs to use for correlation
- Course of Action SDO
 - Icon: 


- Description: Once a sequence of behaviors from a Detection Group has been identified, the reference implementation includes Course of Action SDOs share recommended courses of action to take. This SDO has been extended to support the inclusion of playbooks as recommended by the CACAO project. The relevant playbooks are shared as independent SDOs as there can be a one-to-many relationship between a course of action and relevant playbooks.
- Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Created date
 - Modification date
 - Name
 - Description field
 - Extension
- Playbook SDO
 - Icon: 
 - Description: To provide additional context to shared courses of action, the reference implementation includes a playbook SDO to outline the steps required for implementing the course of action. This object structure was designed by the suggestions from the CACAO project.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Created date
 - Modification date
 - Name
 - Description field
 - Playbook abstraction
 - Playbook bin (base64 representation of playbook)
 - Playbook creator
 - Playbook format
 - Playbook type
 - Playbook revocation status
- Identity SDO
 - Icon: 
 - Description: The Identity SDO represents entities relevant to the CTI held in the bundle. The bundle contains an Identity SDO for MITRE Corporation, which produced the Attack-Pattern SDOs. The bundle also contains an Identity SDO for the targeted organization.
 - Fields within the object:
 - STIX type
 - STIX ID




- STIX specification version
 - Created date
 - Modification date
 - Name
- Grouping SDO
 -  Icon:
 - Description: The Grouping SDO is used to associate related STIX objects together. A Grouping SDO is used to group the Behavior SDOs observed during the attack.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Created date
 - Modification date
 - Context on how the objects within the Grouping are related
 - References to objects within grouping
- Attack-Pattern SDO
 -  Icon:
 - Description: The Attack-Pattern SDO describes adversary tactics, techniques, and procedures (TTPs). The Attack-Pattern SDOs in the bundle have been constructed by MITRE and include custom fields.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Name
 - Description field
 - Created by
 - Created date
 - Modification date
 - Kill chain phases
 - Object marking references
 - External references
 - MITRE custom fields
 - Data sources
 - MITRE version
 - Platforms
 - Flag to determine if the instance is a sub technique
 - Contributors
 - MITRE detection
 - MITRE ATT&CK specification version
 - Domains

- Modified by Identity reference
- Campaign SDO
 - Icon: 
 - Description: The Campaign SDO groups adversarial activity against specific targets over a period of time. The object is used to group the Attack-Pattern SDOs involved in the attack. In the bundle, the Campaign SDO also refers to the Grouping SDO containing the Behavior SDOs.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Created date
 - Modification date
 - Name
 - Description field
 - First seen date
 - Last seen date
- Observed Data SDO
 - Icon: 
 - Description: To provide support for those wishing to research detections through STIX patterning, the reference implementation includes the Observed Data SDO to be better compliant with the STIX standard
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Created date
 - Modification date
 - Name
 - Object references
- Process SCO
 - Icon: 
 - Description: Process SCOs are used for observed sequences of processes executed within an observed behavior. These is often low-level information found within target network log sources such as SYSMON.¹⁶ As opposed to traditional IoCs that may represent the name of a particular malicious process, these SCOs capture common processes within multiple target environments to describe when one process is creating a new process. For example, this is used to capture when something like office applications spawn new processes such as PowerShell or Windows Command Line via a malicious macro. The sequence of Process SCOs


¹⁶ <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

is key to developing the detection object for the behavior of new system process creation.

- Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Object marking refs
 - Granular markings
 - Flag to determine whether the referenced information in the process is “defanged”
 - Flag to determine if the SCO is hidden
 - Process ID (PID)
 - Created date
 - Current Working Directory (CWD)
 - Command line information for the process when available
 - Opened connection references
 - Creator user reference
 - Object reference to executable binary executed as the process image
 - Object reference to parent process
 - Object references to child processes
 - Extensions applied to the SCO
 - Action
 - User
 - Source
 - Creator process name: list of process names or patterns that may spawn the current process
 - New process name: list of process names or patterns that the creator processes may create
 - Windows event code
- Registry SCO
 - Icon: 
 - Description: The registry key SCO provides details for adversary behaviors that modify a particular registry key. It is intended to help restrict behavior alerts to adversary campaigns that modify a specific Windows Registry key. By linking it to the processes created within a chain of Process SCOs, detection is improved. The goal is to share the correlating fact that the process created by a chain of process SCOs is the same one that calls to the registry to make this change. This is different than sharing the name of a specific process from a single incident that calls “regedit.exe” as it provides the path to identify new processes in new campaigns.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version

- Registry key referenced
- Registry key values
- Extensions applied to SCO
 - Action performed on the key
 - New value of the key
 - ID of process that acted on the key
 - Name of process that acted on the key
- IPv4 Address SCO
 - Icon: 
 - Description: The IPv4 Address SCO represents an IPv4 address.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Value
- Network Traffic SCO
 - Icon: 
 - Description: The Network Traffic SCO represents network traffic between a source and destination.
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Source IP reference
 - Destination IP reference
 - Protocols
 - Extensions applied to SCO
 - Number of connections
 - Real Intelligence Threat Analysis (RITA)¹⁷ score
- Domain Name SCO
 - Icon: 
 - Description: The Domain Name SCO provides observable information of a domain utilized by threat activity
 - Fields within the object:
 - STIX type
 - STIX ID
 - STIX specification version
 - Domain Value
- Extension Definition SDO

¹⁷ <https://github.com/activecm/rita>

- Icon: 
- Description: When custom extensions are added to an SDO, the Extension Definition SDO provides a reference to the JSON schema used to represent the additional data.
- Fields within the object:
 - STIX type
 - STIX specification version
 - STIX ID
 - Created by reference
 - Created date
 - Modification date
 - Description field
 - Name
 - Link to extension schema
 - Version
 - List of extension types

2.3.3 Detailed Example for a Subset of the Behavior Bundle

A detailed subset of the first three observed behaviors from the reference implementation scenario shown in Figure 4 follows to better clarify the concepts and capabilities present within the behavior bundle. This example is intended to demonstrate how information in the shared behavior bundle can aid in detecting the sequence of attacker activities represented in Figure 6.

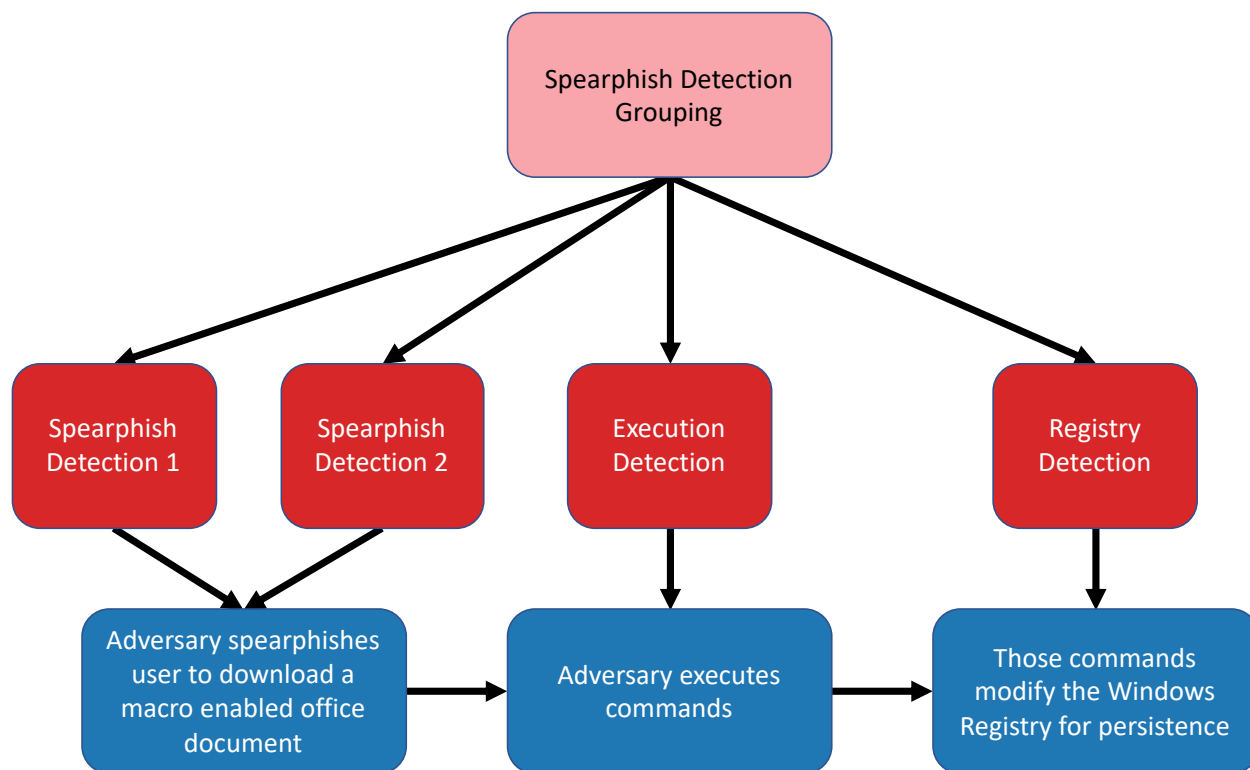


Figure 6: Simplified example of adversary behaviors

The first behavior is intended to represent the observable characteristics within the victim's network when a specific machine's email client (e.g., MS Mail, Outlook, Thunderbird) spawns a process to open a web browser (e.g., Chrome, Firefox, Edge) and download a macro-enabled office document (e.g., *.docm, *.pptm, *.xlsm). The specific types of processes observed in the behavior are common within multiple organizations using similar software. These processes can be commonly recorded via standard Microsoft Windows Log types, such as Windows Event Log and Sysmon. The behavior object also contains a link to a pair of analytics to determine this type of behavior. APL chose the Sigma¹⁸ common analytic format for log analysis to represent these connected analytics.

For the detection the email client opening a web browser, the following Sigma rule is provided:

```

---
date: 2021/06/07
detection:
  selection:
    EventCode: '4688'
    Creator_Process_Name|contains:
      - outlook
      - thunderbird
      - mail
    New_Process_Name|contains:

```

¹⁸ <https://github.com/SigmaHQ/sigma>

- edge
- chrome
- firefox

condition: selection
level: high
author: demo
description: Detects Office macro opening from browser.
id: spearphishing
falsepositives:
- Low
title: Spearphishing with Link
logsource:
 index: main
 product: windows
 category: process_event
status: experimental
tags:
- attack.initial_access
- attack.t1566.002

For the detection of the web browser downloading a macro-enabled office document, the following Sigma rule is provided:

date: 2021/06/07
detection:
 selection:
 Process_Command_Line|contains:

- docm
- xlsx
- pptm

 EventCode: '4688'
 Creator_Process_Name|contains:

- edge
- chrome
- firefox

 New_Process_Name|contains:

- winword
- excel
- powerpoint

 condition: selection
level: high
author: demo
description: Detects Office macro opening from browser.
id: spearphishing
falsepositives:
- Low
title: Spearphishing with Link
logsource:
 index: main
 product: windows

```
category: process_event
status: experimental
tags:
- attack.initial_access
- attack.t1566.002
```

The second behavior represents when the macro executes commands on the file system. It contains STIX Relationship Objects (SRO) to the process identified in the first behavior as well as to a detection object with the following Sigma rule:

```
---
date: 2021/06/07
detection:
  condition: run_macro and (not false_positive)
  run_macro:
    Creator_Process_Name|contains:
      - word
      - powerpoint
      - excel
    New_Process_Name|endswith:
      - ".exe"
      - ".dll"
    EventCode: '4688'
  false_positive:
    New_Process_Name|contains:
      - splwow64
level: high
author: demo
description: Detects Office macro execution
id: execution
falsepositives:
- Low
title: Execution
logsource:
  index: main
  product: windows
  category: process_event
status: experimental
tags:
- attack.execution
- attack.t1059
```

The third behavior object represents observed behaviors for the adversary establishing persistence on the initial target via modification of the Windows registry. It contains SROs to an SCO for the registry modification observed as well as one to a detection object represented in the following Sigma rule:

```
---
date: 2021/06/07
detection:
  selection:
    EventCode: '4657'
    Object_Name|contains:
      - Run
      - Shell Folders
  condition: selection
level: high
author: demo
description: Detects new registry run key created event.
id: registry_persistence
falsepositives:
  - High
title: Registry Run Keys
logsource:
  index: main
  product: windows
  category: registry_event
status: experimental
tags:
  - attack.persistence
  - attack.t1547
```

Any single detection object analytic by itself may not detect the behavior without significant numbers of false positives. The detection grouping is intended to provide the correlation logic to execute all of these queries and include the proper common fields between the queries to further increase the confidence of successfully detecting a behavior.

In the current reference implementation, the detection group object has the ability to contain multiple styles of correlation workflow. For the example provided in the reference implementation, correlation workflows are provided in Collaborative Automated Course of Action Operations (CACAO) format as well as base64 encoded Business Process Modeling Notation (BPMN). Figure 7 provides a visualization of the BPMN workflow when extracted and decoded from the reference implementation.

Figure 7: Conceptual process for detection correlation logic

2.3.4 Using a Received Behavior Set to Augment Network Defense Capability

Once the submitter of a threat intelligence bundle containing behaviors submits the information to a threat feed, the recipient organization can use the correlation information in the detection group to execute the individual queries from each analytic and apply the suggested logic to detect a behavior either automatically or manually, depending on the receiving organization's processes.

It is envisioned that automation will be heavily leveraged to conduct these detections and correlations. This is a key reason for selecting Sigma as there are free and open-source tools available to process Sigma rules to translate them to an organization's SIEM of choice. For example, a shared detection analytic from the earlier example:

```
---
date: 2021/06/07
detection:
  selection:
    Process_Command_Line|contains:
      - docm
      - xlsx
      - pptm
    EventCode: '4688'
    Creator_Process_Name|contains:
      - edge
      - chrome
      - firefox
    New_Process_Name|contains:
      - winword
      - excel
      - powerpoint
  condition: selection
level: high
author: demo
description: Detects Office macro opening from browser.
id: spearphishing
falsepositives:
  - Low
title: Spearphishing with Link
logsource:
  index: main
  product: windows
  category: process_event
status: experimental
tags:
  - attack.initial_access
  - attack.t1566.002
```

By providing this analytic in Sigma format, free tools can translate it to a variety of SIEM options that can be selected from the consumer of the bundle. This rule translates automatically into the following Splunk Query:

```
((Process_Command_Line="*docm*" OR Process_Command_Line="*xlsm*" OR
Process_Command_Line="*pptm*") EventCode="4688" (Creator_Process_Name="*edge*" OR
Creator_Process_Name="*chrome*" OR Creator_Process_Name="*firefox*")
(New_Process_Name="*winword*" OR New_Process_Name="*excel*" OR
New_Process_Name="*powerpoint*"))
```

It can also be automatically translated into another SIEM option such as Azure Sentinel:

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "workspace": {
      "type": "String"
    }
  },
  "resources": [
    {
      "id":
        "[concat(resourceId('Microsoft.OperationalInsights/workspaces/providers',
        parameters('workspace'),
        'Microsoft.SecurityInsights'), '/alertRules/spearphishing')]",
      "name":
        "[concat(parameters('workspace'), '/Microsoft.SecurityInsights/spearphishing')]",
      "type": "Microsoft.OperationalInsights/workspaces/providers/alertRules",
      "apiVersion": "2021-03-01-preview",
      "kind": "Scheduled",
      "properties": {
        "displayName": "Spearphishing with Link by demo",
        "description": "Detects Office macro opening from browser. Technique:
        T1566.002.",
        "severity": "high",
        "enabled": true,
        "query": "Windows | where ((Process_Command_Line contains 'docm' or
        Process_Command_Line contains 'xlsm' or Process_Command_Line contains 'pptm') and
        EventCode == \"4688\" and (Creator_Process_Name contains 'edge' or
        Creator_Process_Name contains 'chrome' or Creator_Process_Name contains
        'firefox') and (New_Process_Name contains 'winword' or New_Process_Name contains
        'excel' or New_Process_Name contains 'powerpoint'))",
        "queryFrequency": "PT30M",
        "queryPeriod": "PT30M",
        "triggerOperator": "GreaterThan",
        "triggerThreshold": 0,
        "suppressionDuration": "PT2H30M",
        "suppressionEnabled": true,
        "tactics": [
```

```

    "InitialAccess"
  ],
  "incidentConfiguration": {
    "createIncident": true,
    "groupingConfiguration": {
      "enabled": false,
      "reopenClosedIncident": false,
      "lookbackDuration": "PT2H30M",
      "matchingMethod": "AllEntities",
      "groupByEntities": [],
      "groupByAlertDetails": [],
      "groupByCustomDetails": []
    }
  },
  "eventGroupingSettings": {
    "aggregationKind": "SingleAlert"
  },
  "alertDetailsOverride": null,
  "customDetails": null,
  "templateVersion": "1.0.0"
}
]
}

```

Sigma is freely available via GitHub¹⁹ and at the time of the reference implementation analysis, the following tools were supported:

- ArcSight
- Azure Sentinel / Azure Log Analytics
- Devo
- ee-outliers
- Elastic X-Pack Watcher
- ElasticSearch Query DSL
- ElasticSearch Query Strings
- Grep with Perl-compatible regular expression support
- Kibana
- LimaCharlie
- LOGIQ
- Logpoint
- LogRhythm
- Microsoft Defender Advanced Threat Protection (MDATP)
- PowerShell
- QRadar
- Qualys
- RSA NetWitness

¹⁹ See section 2.3.4 for link to Sigma GitHub site.

- Splunk
- Structured Threat Information Expression (STIX)
- Sumologic
- uberAgent ESA

Once translated into the recipient's SIEM format, these rules can be used to detect the individual behaviors. These detections can then be translated into a series of SIEM alerts that can be forwarded to a new SIEM index. The correlation logic can then be transformed into an operational workflow (either manually executed or executed via automation) that can execute the correlation check when new alerts are generated. Once a medium or high confidence correlation is observed, a security operator can be notified to investigate the potential behavior sequence detection.

Once notified, the security operator can extract the recommend course of action and relevant playbook for execution either through manual or automated steps. Figure 8 displays the steps required to quarantine an affected system as identified in the shared playbook within the reference implementation.

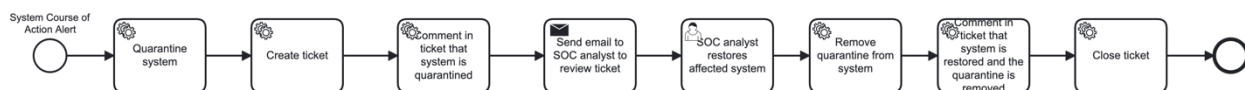


Figure 8 Shared playbook for system quarantine

3. NEXT STEPS

The next phase of this research will investigate the incorporation of the reference implementation into official repositories for the Cyber Threat Intelligence Technical Committee within the OASIS standards body. These changes will be submitted for consideration as inclusions for a future STIX version.

4. ACKNOWLEDGEMENT

The IOB Sub-Project wishes to thank Dr. Vasileios Mavroeidis and his teams at University of Oslo / Cyentific AS for their technical discussions on best practices to represent CACAO playbooks within STIX.

5. CONCLUSION

APL provides this reference implementation and report to facilitate collaboration on research regarding machine readable representations of adversary behavior and to share our work with the larger cyber defense community in the hope that the community can collectively accelerate development of capabilities to defend against the ever-growing speed and scale of cyber threat. For any questions regarding this report, please contact the author via email (Charles.Frick@jhuapl.edu).

6. APPENDIX A: ACRONYMS

APL	Johns Hopkins University Applied Physics Laboratory
BPMN	Business Process Modeling Notation
C2	Command and Control
CACAO	Collaborative Automated Course of Action Operations
CISA	Cybersecurity and Infrastructure Security Agency
CMU	Carnegie Mellon University
COA	Courses of Action
CTI	Cyber Threat Intelligence
CUI	Controlled Unclassified Information
CWD	Current Working Directory
IACD	Integrated Adaptive Cyber Defense
IOC	Indicator of Compromise
JSON	JavaScript Object Notation
MDATP	Microsoft Defender Advanced Threat Protection
PID	Process ID
RITA	Real Intelligence Threat Analytics
SCO	STIX Cyber Observables
SDO	STIX Domain Object
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SRO	STIX Relationship Object
STIX	Structured Threat Information eXchange
TAXII	Trusted Automated eXchange of Indicator Information
TIP	Threat Intel Platform

7. APPENDIX B: COMPLETE BEHAVIOR SET STIX BUNDLE

```
{
  "type": "bundle",
  "id": "bundle--7482bcf3-61b1-4189-9c8a-c1f62b8abfc1",
  "objects": [
    {
      "type": "campaign",
      "id": "campaign--f3bf3827-d9c5-414d-b0f0-610146ff5d85",
      "created": "2022-03-31T13:00:00.000Z",
      "modified": "2022-03-31T13:00:00.000Z",
      "name": "Reaper-Lite",
      "description": "This is an emulated version of the APT37 Reaper Campaign. It was created to demonstrate the creation of machine readable STIX objects to represent adversary behavior.",
      "first_seen": "2022-03-31T13:00:00.000Z",
      "last_seen": "2022-03-31T13:00:00.000Z"
    },
    {
      "type": "x-oca-behavior",
      "spec_version": "2.1",
      "id": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2022-03-31T13:00:00.000Z",
      "modified": "2022-03-31T13:00:00.000Z",
      "name": "Spearphish: Mail Client Opens Browser",
      "description": "An email client has opened a web browser. Although most instances of this behavior are benign, it may indicate a victim clicking on a phishing link.",
      "behavior_class": "anomalous",
      "tactic": "INITIAL ACCESS",
      "technique": "T1566.002 Spearphishing Link",
      "first_seen": "2022-03-31T13:00:00.000Z",
      "platforms": [
        {
          "operating_system": "Microsoft Windows",
          "version": "10"
        }
      ],
      "extensions": {
        "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
          "extension_type": "new-sdo"
        }
      }
    },
    {
      "type": "x-oca-behavior",
      "spec_version": "2.1",
      "id": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bc",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2022-03-31T13:00:00.000Z",
      "modified": "2022-03-31T13:00:00.000Z",
      "name": "Spearphish: Browser Downloads Office Macro",
      "description": "A web browser downloads an Office file containing that contains Macros. Office Macros may contain malicious code.",
      "behavior_class": "anomalous",
      "tactic": "INITIAL ACCESS",
      "technique": "T1566.002 Spearphishing Link",
      "first_seen": "2022-03-31T13:00:00.000Z",
      "platforms": [
        {
          "operating_system": "Microsoft Windows",
          "version": "10"
        }
      ],
      "extensions": {
        "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
          "extension_type": "new-sdo"
        }
      }
    }
  ]
}
```

```
{
},
{
  "type": "x-oca-detector",
  "spec_version": "2.1",
  "id": "x-oca-detector--9441073d-119b-4ec9-aa08-8bdb1703ed56",
  "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
  "created": "2023-05-01T12:00:00.000Z",
  "modified": "2023-05-01T12:00:00.000Z",
  "name": "Rita",
  "description": "A network traffic analysis tool.",
  "cpe": "cpe:2.3:a:active_countermeasures:rita:4.7.0:*:*:*:*:*:*:*:",
  "vendor": "Active Countermeasures, Inc.",
  "vendor_url": "https://www.activecountermeasures.com",
  "product": "RITA",
  "product_url": "https://github.com/activecm/rita",
  "product_version": "4.7.0",
  "detection_types": ["beacon"],
  "detector_data_categories": ["network"],
  "detector_data_sources": ["zeek", "pcap"],
  "valid_until": "2027-05-01T12:00:00.000Z",
  "extensions": {
    "extension-definition--5cccb5c-0be4-450c-8672-b66e98515754": {
      "extension_type": "new-sdo"
    }
  }
},
{
  "type": "x-oca-detector",
  "spec_version": "2.1",
  "id": "x-oca-detector--67330653-ac02-46c8-b9c2-25b837a2ed6d",
  "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
  "created": "2023-05-01T12:00:00.000Z",
  "modified": "2023-05-01T12:00:00.000Z",
  "name": "Zeek",
  "description": "A network security monitoring tool.",
  "cpe": "cpe:2.3:a:zeek:zeek:5.0.9:*:*:*:*:*:*:*:",
  "vendor": "Zeek",
  "vendor_url": "https://zeek.org",
  "product": "Zeek",
  "product_url": "https://zeek.org/get-zeek/",
  "product_version": "5.0.9",
  "detection_types": ["dcsync"],
  "detector_data_categories": ["network"],
  "detector_data_sources": ["network tap"],
  "valid_until": "2027-05-01T12:00:00.000Z",
  "extensions": {
    "extension-definition--5cccb5c-0be4-450c-8672-b66e98515754": {
      "extension_type": "new-sdo"
    }
  }
},
{
  "type": "x-oca-detector",
  "spec_version": "2.1",
  "id": "x-oca-detector--f9ccd3d-2217-45fd-8e65-055da8e66c3e",
  "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
  "created": "2023-05-01T12:00:00.000Z",
  "modified": "2023-05-01T12:00:00.000Z",
  "name": "Sigma",
  "description": "A generic signature format for log files.",
  "cpe": "cpe:2.3:a:sigmahq:sigma:0.21:*:*:*:*:*:*:*:",
  "vendor": "SigmaHQ",
  "vendor_url": "https://github.com/SigmaHQ",
  "product": "Sigma",
  "product_url": "https://github.com/SigmaHQ/sigma",
  "product_version": "0.21",
  "detection_types": ["log"],
```



```

    "detector_data_categories": ["log"],
    "detector_data_sources": ["windows event log", "sysmon", "zeek", "rita"],
    "valid_until": "2027-05-01T12:00:00.000Z",
    "extensions": {
      "extension-definition--5cccba5c-0be4-450c-8672-b66e98515754": {
        "extension_type": "new-sdo"
      }
    }
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--ae96d1d8-41ab-4bf1-aad9-6bf704064404",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab",
    "target_ref": "attack-pattern--2b742742-28c3-4e1b-bab7-8350d6300fa7"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--7f91c908-73ea-40e2-91df-ec9d72e37005",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bc",
    "target_ref": "attack-pattern--2b742742-28c3-4e1b-bab7-8350d6300fa7"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--e38c15bc-224e-4d81-a899-dc3b6f8cee92",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "campaign--f3bf3827-d9c5-414d-b0f0-610146ff5d85",
    "target_ref": "attack-pattern--2b742742-28c3-4e1b-bab7-8350d6300fa7"
  },
  {
    "modified": "2023-05-09T14:00:00.188Z",
    "name": "Spearphishing Link",
    "description": "Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.\n\nAll forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly. Additionally, adversaries may use seemingly benign links that abuse special characters to mimic legitimate websites (known as an \"IDN homograph attack\").(Citation: CISA IDN ST05-016)\n\nAdversaries may also utilize links to perform consent phishing, typically with OAuth 2.0 request URLs that when accepted by the user provide permissions/access for malicious applications, allowing adversaries to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s.(Citation: Trend Micro Pawn Storm OAuth 2017) These stolen access tokens allow the adversary to perform various actions on behalf of the user via API calls. (Citation: Microsoft OAuth 2.0 Consent Phishing 2021)",
    "kill_chain_phases": [
      {
        "kill_chain_name": "mitre-attack",
        "phase_name": "initial-access"
      }
    ]
  },
],

```

```

"x_mitre_contributors": [
  "Philip Winther",
  "Shailesh Tiwary (Indian Army)",
  "Mark Wee",
  "Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services)",
  "Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC)",
  "Kobi Haimovich, CardinalOps",
  "Menachem Goldstein"
],
"x_mitre_deprecated": false,
"x_mitre_detection": "URL inspection within email (including expanding shortened links) can help
detect links leading to known malicious sites as well as links redirecting to adversary infrastructure
based by upon suspicious OAuth patterns with unusual TLDs.(Citation: Microsoft OAuth 2.0 Consent Phishing
2021). Detonation chambers can be used to detect these links and either automatically go to these sites to
determine if they're potentially malicious, or wait and capture the content if a user visits the
link.\n\nFiltering based on DKIM+SPF or header analysis can help detect when the email sender is
spoofed.(Citation: Microsoft Anti Spoofing)(Citation: ACSC Email Spoofing)\n\nBecause this technique
usually involves user interaction on the endpoint, many of the possible detections take place once [User
Execution](https://attack.mitre.org/techniques/T1204) occurs.",
"x_mitre_domains": [
  "enterprise-attack"
],
"x_mitre_is_subtechnique": true,
"x_mitre_platforms": [
  "Linux",
  "macOS",
  "Windows",
  "Office 365",
  "SaaS",
  "Google Workspace"
],
"x_mitre_version": "2.4",
"x_mitre_data_sources": [
  "Network Traffic: Network Traffic Flow",
  "Application Log: Application Log Content",
  "Network Traffic: Network Traffic Content"
],
"type": "attack-pattern",
"id": "attack-pattern--2b742742-28c3-4e1b-bab7-8350d6300fa7",
"created": "2020-03-02T19:15:44.182Z",
"created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
"revoked": false,
"external_references": [
  {
    "source_name": "mitre-attack",
    "url": "https://attack.mitre.org/techniques/T1566/002",
    "external_id": "T1566.002"
  },
  {
    "source_name": "ACSC Email Spoofing",
    "description": "Australian Cyber Security Centre. (2012, December). Mitigating Spoofed Emails
Using Sender Policy Framework. Retrieved October 19, 2020.",
    "url": "https://www.cyber.gov.au/sites/default/files/2019-
03/spoof_email_sender_policy_framework.pdf"
  },
  {
    "source_name": "CISA IDN ST05-016",
    "description": "CISA. (2019, September 27). Security Tip (ST05-016): Understanding
Internationalized Domain Names. Retrieved October 20, 2020.",
    "url": "https://us-cert.cisa.gov/ncas/tips/ST05-016"
  },
  {
    "source_name": "Trend Micro Pawn Storm OAuth 2017",
    "description": "Hacquebord, F.. (2017, April 25). Pawn Storm Abuses Open Authentication in
Advanced Social Engineering Attacks. Retrieved October 4, 2019.",
    "url": "https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-abuses-open-
authentication-advanced-social-engineering-attacks"
  }
],

```

```
{
  "source_name": "Microsoft OAuth 2.0 Consent Phishing 2021",
  "description": "Microsoft 365 Defender Threat Intelligence Team. (2021, June 14). Microsoft
delivers comprehensive solution to battle rise in consent phishing emails. Retrieved December 13, 2021.",
  "url": "https://www.microsoft.com/security/blog/2021/07/14/microsoft-delivers-comprehensive-
solution-to-battle-rise-in-consent-phishing-emails/"
},
{
  "source_name": "Microsoft Anti Spoofing",
  "description": "Microsoft. (2020, October 13). Anti-spoofing protection in EOP. Retrieved
October 19, 2020.",
  "url": "https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-
spoofing-protection?view=o365-worldwide"
}
],
"object_marking_refs": [
  "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
],
"x_mitre_attack_spec_version": "3.1.0",
"x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
"spec_version": "2.1"
},
{
  "type": "x-oca-behavior",
  "spec_version": "2.1",
  "id": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa",
  "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "name": "Office Macro executing commands",
  "description": "An Office Macro is executing commands. This may be malicious code being executed.",
  "behavior_class": "anomalous",
  "tactic": "EXECUTION",
  "technique": "T1059.001 Command/Script execution - VBA",
  "first_seen": "2022-03-31T13:00:00.000Z",
  "platforms": [
    {
      "operating_system": "Microsoft Windows",
      "version": "10"
    }
  ],
  "extensions": {
    "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
      "extension_type": "new-sdo"
    }
  }
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--399ee227-e888-4dcd-bbc8-b79cf5cff259",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa",
  "target_ref": "attack-pattern--970a3432-3237-47ad-bcca-7d8cbb217736"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--81da5956-d9ea-4a09-9e3d-ab09be3cc3eb",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "campaign--f3bf3827-d9c5-414d-b0f0-610146ff5d85",
  "target_ref": "attack-pattern--970a3432-3237-47ad-bcca-7d8cbb217736"
},
{

```

```

"modified": "2023-05-09T14:00:00.188Z",
"name": "PowerShell",
"description": "Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a
powerful interactive command-line interface and scripting environment included in the Windows operating
system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions,
including discovery of information and execution of code. Examples include the <code>Start-Process</code>
cmdlet which can be used to run an executable and the <code>Invoke-Command</code> cmdlet which runs a
command locally or on a remote computer (though administrator permissions are required to use PowerShell
to connect to remote systems).\n\nPowerShell may also be used to download and run executables from the
Internet, which can be executed from disk or in memory without touching disk.\n\nA number of PowerShell-
based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363),
[PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378),
and PSAttack.(Citation: Github PSAttack)\n\nPowerShell commands/scripts can also be executed without
directly invoking the <code>powershell.exe</code> binary through interfaces to PowerShell's underlying
<code>System.Management.Automation</code> assembly DLL exposed through the .NET framework and Windows
Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS
Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)",
"kill_chain_phases": [
  {
    "kill_chain_name": "mitre-attack",
    "phase_name": "execution"
  }
],
"x_mitre_contributors": [
  "Mayuresh Dani, Qualys",
  "Praetorian",
  "Ross Brittain"
],
"x_mitre_deprecated": false,
"x_mitre_detection": "If proper execution policy is set, adversaries will likely be able to define
their own execution policy if they obtain administrator or system access, either through the Registry or
at the command line. This change in policy on a system may be a way to detect malicious use of PowerShell.
If PowerShell is not used in an environment, then simply looking for PowerShell execution may detect
malicious activity.\n\nMonitor for loading and/or execution of artifacts associated with PowerShell
specific assemblies, such as System.Management.Automation.dll (especially to unusual process
names/locations).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)\n\nIt
is also beneficial to turn on PowerShell logging to gain increased fidelity in what occurs during
execution (which is applied to .NET invocations). (Citation: Malware Archaeology PowerShell Cheat Sheet)
PowerShell 5.0 introduced enhanced logging capabilities, and some of those features have since been added
to PowerShell 4.0. Earlier versions of PowerShell do not have many logging features.(Citation: FireEye
PowerShell Logging 2016) An organization can gather PowerShell execution details in a data analytic
platform to supplement it with other data.\n\nConsider monitoring for Windows event ID (EID) 400, which
shows the version of PowerShell executing in the <code>EngineVersion</code> field (which may also be
relevant to detecting a potential [Downgrade Attack](https://attack.mitre.org/techniques/T1562/010)) as
well as if PowerShell is running locally or remotely in the <code>HostName</code> field. Furthermore, EID
400 may indicate the start time and EID 403 indicates the end time of a PowerShell session.(Citation:
inv_ps_attacks)",
"x_mitre_domains": [
  "enterprise-attack"
],
"x_mitre_is_subtechnique": true,
"x_mitre_platforms": [
  "Windows"
],
"x_mitre_version": "1.3",
"x_mitre_data_sources": [
  "Process: Process Metadata",
  "Script: Script Execution",
  "Process: Process Creation",
  "Command: Command Execution",
  "Module: Module Load"
],
"x_mitre_remote_support": true,
"type": "attack-pattern",
"id": "attack-pattern--970a3432-3237-47ad-bcca-7d8cbb217736",
"created": "2020-03-09T13:48:55.078Z",
"created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
"revoked": false,

```

```

"external_references": [
  {
    "source_name": "mitre-attack",
    "url": "https://attack.mitre.org/techniques/T1059/001",
    "external_id": "T1059.001"
  },
  {
    "source_name": "Microsoft PSfromCsharp APR 2014",
    "description": "Babinec, K. (2014, April 28). Executing PowerShell scripts from C#. Retrieved
April 22, 2019.",
    "url": "https://blogs.msdn.microsoft.com/kebab/2014/04/28/executing-powershell-scripts-from-c/"
  },
  {
    "source_name": "SilentBreak Offensive PS Dec 2015",
    "description": "Christensen, L.. (2015, December 28). The Evolution of Offensive PowerShell
Invocation. Retrieved December 8, 2018.",
    "url": "https://web.archive.org/web/20190508170150/https://silentbreaksecurity.com/powershell-
jobs-without-powershell-exe/"
  },
  {
    "source_name": "FireEye PowerShell Logging 2016",
    "description": "Dunwoody, M. (2016, February 11). GREATER VISIBILITY THROUGH POWERSHELL LOGGING.
Retrieved February 16, 2016.",
    "url": "https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html"
  },
  {
    "source_name": "Github PSAttack",
    "description": "Haight, J. (2016, April 21). PS>Attack. Retrieved June 1, 2016.",
    "url": "https://github.com/jaredhaight/PSAttack"
  },
  {
    "source_name": "inv_ps_attacks",
    "description": "Hastings, M. (2014, July 16). Investigating PowerShell Attacks. Retrieved
December 1, 2021.",
    "url": "https://powershellmagazine.com/2014/07/16/investigating-powershell-attacks/"
  },
  {
    "source_name": "Malware Archaeology PowerShell Cheat Sheet",
    "description": "Malware Archaeology. (2016, June). WINDOWS POWERSHELL LOGGING CHEAT SHEET - Win
7/Win 2008 or later. Retrieved June 24, 2016.",
    "url": "http://www.malwarearchaeology.com/s/Windows-PowerShell-Logging-Cheat-Sheet-ver-June-
2016-v2.pdf"
  },
  {
    "source_name": "TechNet PowerShell",
    "description": "Microsoft. (n.d.). Windows PowerShell Scripting. Retrieved April 28, 2016.",
    "url": "https://technet.microsoft.com/en-us/scriptcenter/dd742419.aspx"
  },
  {
    "source_name": "Sixdub PowerPick Jan 2016",
    "description": "Warner, J.. (2015, January 6). Inexorable PowerShell \u2013 A Red Teamer\u2013s
Tale of Overcoming Simple AppLocker Policies. Retrieved December 8, 2018.",
    "url": "https://web.archive.org/web/20160327101330/http://www.sixdub.net/?p=367"
  }
],
"object_marking_refs": [
  "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
],
"x_mitre_attack_spec_version": "3.1.0",
"x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
"spec_version": "2.1"
},
{
  "type": "x-oca-behavior",
  "spec_version": "2.1",
  "id": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bb",
  "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
  "created": "2022-03-31T13:00:00.000Z",

```

```

    "modified": "2022-03-31T13:00:00.000Z",
    "name": "Cobalt Strike Payload Beacons",
    "description": "Network traffic matching a signature of Cobalt Strike's beaconing.",
    "behavior_class": "anomalous",
    "tactic": "Command and Control",
    "technique": "T1071.001 - Application Layer Protocol - Web Protocols",
    "first_seen": "2022-03-31T13:00:00.000Z",
    "platforms": [
      {
        "operating_system": "Microsoft Windows",
        "version": "10"
      }
    ],
    "extensions": {
      "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
        "extension_type": "new-sdo"
      }
    }
  },
  {
    "type": "ipv4-addr",
    "spec_version": "2.1",
    "id": "ipv4-addr--57a33521-9761-54a9-81de-3c11e441d86b",
    "value": "192.168.1.1"
  },
  {
    "type": "ipv4-addr",
    "spec_version": "2.1",
    "id": "ipv4-addr--bba1d187-08fb-5000-aed1-ef055c1dfd24",
    "value": "172.16.1.1"
  },
  {
    "type": "network-traffic",
    "spec_version": "2.1",
    "id": "network-traffic--15a157a8-26e3-56e0-820b-0c2a8e553a2c",
    "src_ref": "ipv4-addr--57a33521-9761-54a9-81de-3c11e441d86b",
    "src_port": 443,
    "dst_ref": "ipv4-addr--bba1d187-08fb-5000-aed1-ef055c1dfd24",
    "dst_port": 443,
    "protocols": [
      "ipv4",
      "tcp",
      "http",
      "https"
    ],
    "extensions": {
      "extension-definition--3b7505ce-2a18-496e-aa58-311dac6c1473": {
        "connections": 4022,
        "score": 0.834,
        "extension_type": "property-extension"
      }
    }
  },
  {
    "type": "x-oca-detection",
    "spec_version": "2.1",
    "id": "x-oca-detection--5899C5CC-CE20-44EE-806E-9F64EBA0B29F",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "Beacon Detection with RITA analytics",
    "data_sources": [
      {
        "LogName": "Rita",
        "Category": "show-beacons",
        "score_num": "> 0.7"
      }
    ]
  },
],

```

Page 39

"x_mitre_detection": "Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect application layer protocols that do not follow the expected protocol standards regarding syntax, structure, or any other variable adversaries could leverage to conceal data.(Citation: University of Birmingham C2)\n\nMonitor for web traffic to/from known-bad or suspicious domains. ",

```

    "x_mitre_domains": [
      "enterprise-attack"
    ],
    "x_mitre_is_subtechnique": true,
    "x_mitre_platforms": [
      "Linux",
      "macOS",
      "Windows"
    ],
    "x_mitre_version": "1.1",
    "x_mitre_data_sources": [
      "Network Traffic: Network Traffic Content",
      "Network Traffic: Network Traffic Flow"
    ],
    "type": "attack-pattern",
    "id": "attack-pattern--df8b2a25-8bdf-4856-953c-a04372b1c161",
    "created": "2020-03-15T16:13:46.151Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "revoked": false,
    "external_references": [
      {
        "source_name": "mitre-attack",
        "url": "https://attack.mitre.org/techniques/T1071/001",
        "external_id": "T1071.001"
      },
      {
        "source_name": "CrowdStrike Putter Panda",
        "description": "CrowdStrike Global Intelligence Team. (2014, June 9). CrowdStrike Intelligence Report: Putter Panda. Retrieved January 22, 2016.",
        "url": "http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf"
      },
      {
        "source_name": "University of Birmingham C2",
        "description": "Gardiner, J., Cova, M., Nagaraja, S. (2014, February). Command & Control Understanding, Denying and Detecting. Retrieved April 20, 2016.",
        "url": "https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf"
      },
      {
        "source_name": "Brazking-Websockets",
        "description": "Shahar Tavor. (n.d.). BrazKing Android Malware Upgraded and Targeting Brazilian Banks. Retrieved March 24, 2023.",
        "url": "https://securityintelligence.com/posts/brazking-android-malware-upgraded-targeting-brazilian-banks/"
      }
    ],
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "x_mitre_attack_spec_version": "3.1.0",
    "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1"
  },
  {
    "type": "x-oca-behavior",
    "spec_version": "2.1",
    "id": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890cc",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "Registry modification for Persistence",

```



```

    "description": "Modification of the Windows Registry may indicate an adversary attempting to
    establish persistence.",
    "behavior_class": "anomalous",
    "tactic": "Persistence",
    "technique": "T1547.001 - Autostart Execution - Registry Run Keys / Startup Folder",
    "first_seen": "2022-03-31T13:00:00.000Z",
    "platforms": [
      {
        "operating_system": "Microsoft Windows",
        "version": "10"
      }
    ],
    "extensions": {
      "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
        "extension_type": "new-sdo"
      }
    }
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--8e796cf6-5401-4a23-9354-59b58155bd5e",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890cc",
    "target_ref": "attack-pattern--9efb1ea7-c37b-4595-9640-b7680cd84279"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--7a9afa0a-0c25-4dec-8f3d-db92e213643c",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "campaign--f3bf3827-d9c5-414d-b0f0-610146ff5d85",
    "target_ref": "attack-pattern--9efb1ea7-c37b-4595-9640-b7680cd84279"
  },
  {
    "modified": "2023-05-09T14:00:00.188Z",
    "name": "Registry Run Keys / Startup Folder",
    "description": "Adversaries may achieve persistence by adding a program to a startup folder or
    referencing it with a Registry run key. Adding an entry to the \"run keys\" in the Registry or startup
    folder will cause the program referenced to be executed when a user logs in.(Citation: Microsoft Run Key)
    These programs will be executed under the context of the user and will have the account's associated
    permissions level.\n\nPlacing a program within a startup folder will also cause that program to execute
    when a user logs in. There is a startup folder location for individual user accounts as well as a system-
    wide startup folder that will be checked regardless of which user account logs in. The startup folder path
    for the current user is <code>C:\\Users\\[Username]\\AppData\\Roaming\\Microsoft\\Windows\\Start
    Menu\\Programs\\Startup</code>. The startup folder path for all users is
    <code>C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\Startup</code>.\n\nThe following run keys
    are created by default on Windows systems:\n\n*
    <code>HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run</code>\n*
    <code>HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce</code>\n*
    <code>HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Run</code>\n*
    <code>HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce</code>\n\nRun keys may
    exist under multiple hives.(Citation: Microsoft Wow6432Node 2018)(Citation: Malwarebytes Wow6432Node 2016)
    The <code>HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnceEx</code> is also
    available but is not created by default on Windows Vista and newer. Registry run key entries can reference
    programs directly or list them as a dependency.(Citation: Microsoft Run Key) For example, it is possible
    to load a DLL at logon using a \"Depend\" key with RunOnceEx: <code>reg add
    HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnceEx\\0001\\Depend /v 1 /d
    \"C:\\temp\\evil.[.dll]\"</code> (Citation: Oddvar Moe RunOnceEx Mar 2018)\n\nThe following Registry keys
    can be used to set startup folder items for persistence:\n\n*
    <code>HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\User Shell
    Folders</code>\n* <code>HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Shell
    Folders</code>\n* <code>HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Shell
    Folders</code>\n* <code>HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\User
  
```

Shell Folders

The following Registry keys can control automatic startup of services during boot:

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices`

Using policy settings to specify startup programs creates corresponding values in either of two Registry keys:

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run`

The Winlogon key controls actions that occur when a user logs on to a computer running Windows 7. Most of these actions are under the control of the operating system, but you can also add custom actions here. The `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit` and `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell` subkeys can automatically launch programs. Programs listed in the load value of the registry key `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows` run when any user logs on. By default, the multistring `BootExecute` value of the registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager` is set to `autocheck autochk *`. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot. Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading] (<https://attack.mitre.org/techniques/T1036>) to make the Registry entries look as if they are associated with legitimate programs.",

```
"kill_chain_phases": [
  {
    "kill_chain_name": "mitre-attack",
    "phase_name": "persistence"
  },
  {
    "kill_chain_name": "mitre-attack",
    "phase_name": "privilege-escalation"
  }
],
"x_mitre_attack_spec_version": "2.1.0",
"x_mitre_contributors": [
  "Oddvar Moe, @oddvarmoe",
  "Dray Agha, @Purp1eW0lf, Huntress Labs"
],
"x_mitre_deprecated": false,
"x_mitre_detection": "Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Monitor the start folder for additions or changes. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders. (Citation: TechNet Autoruns) Suspicious program execution as startup programs may show up as outlier processes that have not been seen before when compared against historical data. Changes to these locations typically happen under normal conditions when legitimate software is installed. To increase confidence of malicious activity, data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.",
"x_mitre_domains": [
  "enterprise-attack"
],
"x_mitre_is_subtechnique": true,
"x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
"x_mitre_platforms": [
  "Windows"
],
"x_mitre_version": "1.2",
"x_mitre_data_sources": [
  "Windows Registry: Windows Registry Key Creation",
  "Windows Registry: Windows Registry Key Modification",
  "Command: Command Execution",
  "Process: Process Creation",
  "File: File Modification"
],
"x_mitre_permissions_required": [
  "Administrator",
  "User"
```

```

    ],
    "type": "attack-pattern",
    "id": "attack-pattern--9efb1ea7-c37b-4595-9640-b7680cd84279",
    "created": "2020-01-23T22:02:48.566Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "revoked": false,
    "external_references": [
      {
        "source_name": "mitre-attack",
        "url": "https://attack.mitre.org/techniques/T1547/001",
        "external_id": "T1547.001"
      },
      {
        "source_name": "Malwarebytes Wow6432Node 2016",
        "description": "Arntz, P. (2016, March 30). Hiding in Plain Sight. Retrieved August 3, 2020.",
        "url": "https://blog.malwarebytes.com/cybercrime/2013/10/hiding-in-plain-sight/"
      },
      {
        "source_name": "Microsoft Wow6432Node 2018",
        "description": "Microsoft. (2018, May 31). 32-bit and 64-bit Application Data in the Registry. Retrieved August 3, 2020.",
        "url": "https://docs.microsoft.com/en-us/windows/win32/sysinfo/32-bit-and-64-bit-application-data-in-the-registry"
      },
      {
        "source_name": "Microsoft Run Key",
        "description": "Microsoft. (n.d.). Run and RunOnce Registry Keys. Retrieved November 12, 2014.",
        "url": "http://msdn.microsoft.com/en-us/library/aa376977"
      },
      {
        "source_name": "Oddvar Moe RunOnceEx Mar 2018",
        "description": "Moe, O. (2018, March 21). Persistence using RunOnceEx - Hidden from Autoruns.exe. Retrieved June 29, 2018.",
        "url": "https://oddvar.moe/2018/03/21/persistence-using-runonceex-hidden-from-autoruns-exe/"
      },
      {
        "source_name": "TechNet Autoruns",
        "description": "Russinovich, M. (2016, January 4). Autoruns for Windows v13.51. Retrieved June 6, 2016.",
        "url": "https://technet.microsoft.com/en-us/sysinternals/bb963902"
      }
    ],
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "spec_version": "2.1"
  },
  {
    "type": "x-oca-behavior",
    "spec_version": "2.1",
    "id": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890dd",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "Secondary Payload Privilege Escalation Behavior",
    "description": "A privilege escalation has occurred which may indicate adversary activity.",
    "behavior_class": "anomalous",
    "tactic": "Privilege Escalation",
    "technique": "T1134.001 - Access token manipulation - Token impersonation",
    "first_seen": "2022-03-31T13:00:00.000Z",
    "platforms": [
      {
        "operating_system": "Microsoft Windows",
        "version": "10"
      }
    ],
    "extensions": {
      "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {

```



```

"type": "process",
"spec_version": "2.1",
"id": "process--3BCFB0A5-BAF5-411D-B9D0-8D4B4E09BA82",
"is_hidden": false,
"pid": 0,
"cwd": "C:\\Users\\jsmith.CBIS\\AppData\\Local\\",
"command_line": "C:\\Users\\jsmith.CBIS\\AppData\\Local\\Beacon.exe",
"extensions": {
  "extension-definition--f9dbe89c-0030-4a9d-8b78-0dc0a0de874": {
    "extension_type": "property-extension",
    "action": "created",
    "user": "SP25-TARGET$",
    "src_user": "jsmith",
    "win_event_code": "4688"
  }
},
"created_time": "2022-03-31T13:00:00.000Z",
"defanged": false
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--a7e2ab2a-cdf5-45d0-bbe2-e6ecdb95ca99",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890dd",
  "target_ref": "attack-pattern--86850eff-2729-40c3-b85e-c4af26da4a2d"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--4655b19d-c949-45be-8316-e8861c634cab",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "campaign--f3bf3827-d9c5-414d-b0f0-610146ff5d85",
  "target_ref": "attack-pattern--86850eff-2729-40c3-b85e-c4af26da4a2d"
},
{
  "modified": "2023-04-11T21:19:05.544Z",
  "name": "Token Impersonation/Theft",
  "description": "Adversaries may duplicate then impersonate another user's existing token to escalate privileges and bypass access controls. For example, an adversary can duplicate an existing token using `DuplicateToken` or `DuplicateTokenEx`. The token can then be used with `ImpersonateLoggedOnUser` to allow the calling thread to impersonate a logged on user's security context, or with `SetThreadToken` to assign the impersonated token to a thread.\n\nAn adversary may perform [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001) when they have a specific, existing process they want to assign the duplicated token to. For example, this may be useful for when the target user has a non-network logon session on the system.\n\nWhen an adversary would instead use a duplicated token to create a new process rather than attaching to an existing process, they can additionally [Create Process with Token](https://attack.mitre.org/techniques/T1134/002) using `CreateProcessWithTokenW` or `CreateProcessAsUserW`. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001) is also distinct from [Make and Impersonate Token](https://attack.mitre.org/techniques/T1134/003) in that it refers to duplicating an existing token, rather than creating a new one.",
  "kill_chain_phases": [
    {
      "kill_chain_name": "mitre-attack",
      "phase_name": "defense-evasion"
    },
    {
      "kill_chain_name": "mitre-attack",
      "phase_name": "privilege-escalation"
    }
  ],
  "x_mitre_contributors": [
    "Jonny Johnson"
  ],

```

```

    "x_mitre_deprecated": false,
    "x_mitre_detection": "If an adversary is using a standard command-line shell, analysts can detect token manipulation by auditing command-line activity. Specifically, analysts should look for use of the <code>runas</code> command. Detailed command-line logging is not enabled by default in Windows.(Citation: Microsoft Command-line Logging)\n\nAnalysts can also monitor for use of Windows APIs such as <code>DuplicateToken(Ex)</code>, <code>ImpersonateLoggedOnUser</code>, and <code>SetThreadToken</code> and correlate activity with other suspicious behavior to reduce false positives that may be due to normal benign use by users and administrators.",
    "x_mitre_domains": [
      "enterprise-attack"
    ],
    "x_mitre_is_subtechnique": true,
    "x_mitre_platforms": [
      "Windows"
    ],
    "x_mitre_version": "1.1",
    "x_mitre_data_sources": [
      "Command: Command Execution",
      "Process: OS API Execution"
    ],
    "x_mitre_defense_bypassed": [
      "Windows User Account Control",
      "System access controls",
      "File system access controls"
    ],
    "type": "attack-pattern",
    "id": "attack-pattern--86850eff-2729-40c3-b85e-c4af26da4a2d",
    "created": "2020-02-18T16:39:06.289Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "revoked": false,
    "external_references": [
      {
        "source_name": "mitre-attack",
        "url": "https://attack.mitre.org/techniques/T1134/001",
        "external_id": "T1134.001"
      },
      {
        "source_name": "Microsoft Command-line Logging",
        "description": "Mathers, B. (2017, March 7). Command line process auditing. Retrieved April 21, 2017.",
        "url": "https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/manage/component-updates/command-line-process-auditing"
      }
    ],
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "x_mitre_attack_spec_version": "3.1.0",
    "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1"
  },
  {
    "type": "x-oca-behavior",
    "spec_version": "2.1",
    "id": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ee",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "Credential Access Behavior with DCSync and Kerberoasting",
    "description": "A DCSync may have occurred, allowing an adversary access to the Domain Controller's credentials. The adversary may obtain password hashes via Kerberoasting and attempt to crack them.",
    "behavior_class": "anomalous",
    "tactic": "Credential Access",
    "technique": "T1003.006 - OS Credential dumping - DCSync",
    "first_seen": "2022-03-31T13:00:00.000Z",
    "platforms": [
      {
        "operating_system": "Microsoft Windows",

```

```

        "version": "10"
      }
    ],
    "extensions": {
      "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
        "extension_type": "new-sdo"
      }
    }
  },
  {
    "type": "x-oca-detection",
    "spec_version": "2.1",
    "id": "x-oca-detection--275bf485-736d-4aa5-b172-e34d28faa58c",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "DC Sync Detection",
    "data_sources": [
      {
        "data_type": "notice-too_small",
        "LogName": "/nsm/zeek/logs/current/notice.log"
      }
    ]
  },
  "analytic": {
    "type": "Sigma Rule",
    "rule": "
LS0tCnRpdGx1oiBEQ1N5bmMKaWQ6IGRjc3luYwpzdGF0dXM6IGV4cGVyaW1lbnRhbApkZXNjcmlwdGlvbjogRGV0ZWN0cyBuZXR3b3JrI
GFjdG12aXR5IHVzaW5nIERSU0dldE5DQ2hhbmdlcY4KdGFnZzoKICAtIGF0dGFjay5jcmVkbW50aWFsX2FjY2VzcwogIC0gYXR0YWNrLlQ
xMDAzLjAwNgphdXR0b3I6IGRlbW8KZGF0ZTogMjAyMS8wNi8wNwpsb2dzb3VyY2U6CiAgCHJvZHVjdDogemVlawogIGluZGV4O0iBtYWluC
iAgY2F0ZWdvcnk6IG5ldHdvcmRfZXZlbnQKZGV0ZWN0aW9uOgogIHNlbGVjdGlvbjogKICAgIG1zZz0gJ2Ryc3VhcGk6O0kRSU0dldE5DQ2h
hbmdlcycKICBjb25kaXRpb246IHNlbGVjdGlvbGpmYWxzZX8vc2l0aXZlczoKICAtIERvbWVpbiBDb250cm9sbGVyCmxldmVsOiBoaWdo"
      ",
      "extensions": {
        "extension-definition--c4690e13-107e-4796-8158-0dcf1ae7bc89": {
          "extension_type": "new-sdo"
        }
      }
    },
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--d993c3af-9443-44db-9478-b3a9d632d94d",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "detects",
    "source_ref": "x-oca-detection--275bf485-736d-4aa5-b172-e34d28faa58c",
    "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ee"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--d4ce259f-f595-4d1d-913c-e17454396dba",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ee",
    "target_ref": "attack-pattern--f303a39a-6255-4b89-aecc-18c4d8ca7163"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--ca57a603-b4d6-475e-be8d-7618fbd58fbb",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "campaign--f3bf3827-d9c5-414d-b0f0-610146ff5d85",
    "target_ref": "attack-pattern--f303a39a-6255-4b89-aecc-18c4d8ca7163"
  }
},

```



```
{
  "x_mitre_platforms": [
    "Windows"
  ],
  "x_mitre_domains": [
    "enterprise-attack"
  ],
  "x_mitre_contributors": [
    "ExtraHop",
    "Vincent Le Toux"
  ],
  "object_marking_refs": [
    "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
  ],
  "id": "attack-pattern--f303a39a-6255-4b89-aecc-18c4d8ca7163",
  "type": "attack-pattern",
  "created": "2020-02-11T18:45:34.293Z",
  "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "external_references": [
    {
      "source_name": "mitre-attack",
      "external_id": "T1003.006",
      "url": "https://attack.mitre.org/techniques/T1003/006"
    },
    {
      "url": "https://msdn.microsoft.com/library/cc228086.aspx",
      "description": "Microsoft. (2017, December 1). MS-DRSR Directory Replication Service (DRS) Remote Protocol. Retrieved December 4, 2017.",
      "source_name": "Microsoft DRSR Dec 2017"
    },
    {
      "url": "https://msdn.microsoft.com/library/dd207691.aspx",
      "description": "Microsoft. (n.d.). IDL_DRSGetNCChanges (Opnum 3). Retrieved December 4, 2017.",
      "source_name": "Microsoft GetNCCChanges"
    },
    {
      "url": "https://wiki.samba.org/index.php/DRSUAPI",
      "description": "SambaWiki. (n.d.). DRSUAPI. Retrieved December 4, 2017.",
      "source_name": "Samba DRSUAPI"
    },
    {
      "url": "https://source.winehq.org/WineAPI/samlib.html",
      "description": "Wine API. (n.d.). samlib.dll. Retrieved December 4, 2017.",
      "source_name": "Wine API samlib.dll"
    },
    {
      "url": "https://adsecurity.org/?p=1729",
      "description": "Metcalfe, S. (2015, September 25). Mimikatz DCSync Usage, Exploitation, and Detection. Retrieved August 7, 2017.",
      "source_name": "ADSecurity Mimikatz DCSync"
    },
    {
      "url": "http://www.harmj0y.net/blog/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/",
      "description": "Schroeder, W. (2015, September 22). Mimikatz and DCSync and ExtraSids, Oh My. Retrieved August 7, 2017.",
      "source_name": "Harmj0y Mimikatz and DCSync"
    },
    {
      "url": "https://blog.stealthbits.com/manipulating-user-passwords-with-mimikatz-SetNTLM-ChangeNTLM",
      "description": "Warren, J. (2017, July 11). Manipulating User Passwords with Mimikatz. Retrieved December 4, 2017.",
      "source_name": "InsiderThreat ChangeNTLM July 2017"
    },
    {
      "url": "https://github.com/gentilkiwi/mimikatz/wiki/module--lsadump",
      "description": "Deply, B., Le Toux, V. (2016, June 5). module ~ lsadump. Retrieved August 7, 2017.",
    }
  ]
}
```



```

    "source_name": "GitHub Mimikatz lsadump Module"
  },
  {
    "url": "https://msdn.microsoft.com/library/cc237008.aspx",
    "description": "Microsoft. (2017, December 1). MS-NRPC - Netlogon Remote Protocol. Retrieved
December 6, 2017.",
    "source_name": "Microsoft NRPC Dec 2017"
  },
  {
    "url": "https://msdn.microsoft.com/library/cc245496.aspx",
    "description": "Microsoft. (n.d.). MS-SAMR Security Account Manager (SAM) Remote Protocol
(Client-to-Server) - Transport. Retrieved December 4, 2017.",
    "source_name": "Microsoft SAMR"
  },
  {
    "url": "https://adsecurity.org/?p=1729",
    "description": "Metcalfe, S. (2015, September 25). Mimikatz DCSync Usage, Exploitation, and
Detection. Retrieved December 4, 2017.",
    "source_name": "AdSecurity DCSync Sept 2015"
  },
  {
    "url": "http://www.harmj0y.net/blog/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/",
    "description": "Schroeder, W. (2015, September 22). Mimikatz and DCSync and ExtraSids, Oh My.
Retrieved December 4, 2017.",
    "source_name": "Harmj0y DCSync Sept 2015"
  }
],
"modified": "2022-04-25T14:00:00.188Z",
"name": "DCSync",
"description": "Adversaries may attempt to access credentials and other sensitive information by
abusing a Windows Domain Controller's application programming interface (API)(Citation: Microsoft DRSR Dec
2017) (Citation: Microsoft GetNCCChanges) (Citation: Samba DRSUAPI) (Citation: Wine API samlib.dll) to
simulate the replication process from a remote domain controller using a technique called
DCSync.\n\nMembers of the Administrators, Domain Admins, and Enterprise Admin groups or computer accounts
on the domain controller are able to run DCSync to pull password data(Citation: ADSecurity Mimikatz
DCSync) from Active Directory, which may include current and historical hashes of potentially useful
accounts such as KRBTGT and Administrators. The hashes can then in turn be used to create a [Golden
Ticket](https://attack.mitre.org/techniques/T1558/001) for use in [Pass the
Ticket](https://attack.mitre.org/techniques/T1550/003)(Citation: Harmj0y Mimikatz and DCSync) or change an
account's password as noted in [Account
Manipulation](https://attack.mitre.org/techniques/T1098).(Citation: InsiderThreat ChangeNTLM July
2017)\n\nDCSync functionality has been included in the \"lsadump\" module in
[Mimikatz](https://attack.mitre.org/software/S0002).(Citation: GitHub Mimikatz lsadump Module) Lsadump
also includes NetSync, which performs DCSync over a legacy replication protocol.(Citation: Microsoft NRPC
Dec 2017)",
"kill_chain_phases": [
  {
    "kill_chain_name": "mitre-attack",
    "phase_name": "credential-access"
  }
],
"x_mitre_detection": "Monitor domain controller logs for replication requests and other unscheduled
activity possibly associated with DCSync.(Citation: Microsoft DRSR Dec 2017) (Citation: Microsoft
GetNCCChanges) (Citation: Samba DRSUAPI) Also monitor for network protocols(Citation: Microsoft DRSR Dec
2017) (Citation: Microsoft NRPC Dec 2017) and other replication requests(Citation: Microsoft SAMR) from
IPs not associated with known domain controllers.(Citation: AdSecurity DCSync Sept 2015)\n\nNote: Domain
controllers may not log replication requests originating from the default domain controller
account.(Citation: Harmj0y DCSync Sept 2015)",
"x_mitre_is_subtechnique": true,
"x_mitre_version": "1.0",
"x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
"x_mitre_data_sources": [
  "Network Traffic: Network Traffic Flow",
  "Network Traffic: Network Traffic Content",
  "Active Directory: Active Directory Object Access"
],
"x_mitre_permissions_required": [
  "Administrator"

```

```

    ],
    "spec_version": "2.1",
    "x_mitre_attack_spec_version": "2.1.0"
  },
  {
    "type": "network-traffic",
    "spec_version": "2.1",
    "id": "network-traffic--acffdf9a-bafd-5b74-a7d9-1a6d5a4e9c5a",
    "src_ref": "ipv4-addr--57a33521-9761-54a9-81de-3c11e441d86b",
    "dst_ref": "ipv4-addr--429ddae0-a1ff-543d-99b4-f12a4a144c70",
    "protocols": [
      "ipv4",
      "tcp",
      "smb"
    ]
  },
  {
    "type": "ipv4-addr",
    "spec_version": "2.1",
    "id": "ipv4-addr--429ddae0-a1ff-543d-99b4-f12a4a144c70",
    "value": "192.168.1.2"
  },
  {
    "type": "x-oca-behavior",
    "spec_version": "2.1",
    "id": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ff",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "Abnormal internal network traffic for Lateral Movement",
    "description": "Network traffic matching a pattern which may indicate lateral movement done by an
adversary.",
    "behavior_class": "anomalous",
    "tactic": "Lateral Movement",
    "technique": "T1558.001 - Steal Or Forge Kerberos Tickets - Golden Ticket",
    "first_seen": "2022-03-31T13:00:00.000Z",
    "platforms": [
      {
        "operating_system": "Microsoft Windows",
        "version": "10"
      }
    ],
    "extensions": {
      "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
        "extension_type": "new-sdo"
      }
    }
  },
  {
    "type": "x-oca-detection",
    "spec_version": "2.1",
    "id": "x-oca-detection--40a941cc-42df-4b2e-b607-6d74168084b9",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "Lateral Movement Detection",
    "data_sources": [
      {
        "data_type": "WinEventLog",
        "LogName": "WinEventLog:Security"
      }
    ]
  },
  "analytic": {
    "type": "Sigma Rule",
    "rule":
"YXV0aG9yOiBkZWlvcMhGU6IDIwMjIvMDMvMDQKZGVzY3JpcHRpb246IERldGVjdHMgcHJlLWVncjJlbGF0ZWQgZXZlbnRzIHRhZ2d1Z
CBhcyBwb3RlbnRyYWwR29sZGVuIFRyY2tldCBhdHRlbnRlcmlkOia5MmEYMWJlZi00MTM4LTQwYjYtYTk1NS00OTdiMGNlMDUxNTEKc3R
hdHVzOiBleHBlcm1tZW50YWwkdGFnczoKICAtIGF0dGFjay5jcMkZ50aWFSX2FjY2VzcwogIC0gYXR0YWNrLnQxNTU4LjAwMQpsb2dzb

```

```
3VyY2U6IAogIHByb2R1Y3Q6IHdpbmRvd3MKICBpbmRleDogbWVpbGogIGNhdGVnb3J5OibrZXJiZXJvcwpmZXRLY3Rpb246CiAgc2VsZWw
0aw9uOiAKICAgIHNdXGJjZXR5cGU6IGludGVybWFsX2FsZXJ0cwogICAgYWxlcnRfdHlwZXxb250YWluczogIkdvbGR1b1RpY2tldCIKI
CBjb25kaXRpb246IHNdGVjZGlvdGpmYWxzZXBvc2l0aXZlczoKICAtIERvbWVpb250cm9sbGVycwogIC0gRXhjaGFuZ2UKbGV2ZWw
6IGhpZ2g="
```

```
{
  "extensions": {
    "extension-definition--c4690e13-107e-4796-8158-0dcf1ae7bc89": {
      "extension_type": "new-sdo"
    }
  }
},
{
  "type": "domain-name",
  "spec_version": "2.1",
  "id": "domain-name--8713b93b-186e-524d-9224-db3b8f9fb9ef",
  "value": "data-server-domain",
  "resolves_to_refs": [
    "ipv4-addr--3d4ee4f2-a895-5781-a0cc-b5ba466f053d"
  ]
},
{
  "type": "network-traffic",
  "spec_version": "2.1",
  "id": "network-traffic--3564fb7d-d65c-5e02-9f55-a8a960f5c9f5",
  "src_ref": "ipv4-addr--57a33521-9761-54a9-81de-3c11e441d86b",
  "dst_ref": "domain-name--8713b93b-186e-524d-9224-db3b8f9fb9ef",
  "protocols": [
    "ipv4",
    "tcp",
    "smb"
  ]
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--19856de6-739c-4b31-b0cc-aaa6b0b751c8",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "detects",
  "source_ref": "x-oca-detection--40a941cc-42df-4b2e-b607-6d74168084b9",
  "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ff"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--c9a2a2b3-67f3-4b8a-ad40-17c8098f7205",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ff",
  "target_ref": "attack-pattern--7b211ac6-c815-4189-93a9-ab415deca926"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--baf7f0f2-1aa8-45cb-b306-cbca8dd863d1",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "campaign--f3bf3827-d9c5-414d-b0f0-610146ff5d85",
  "target_ref": "attack-pattern--7b211ac6-c815-4189-93a9-ab415deca926"
},
{
  "modified": "2023-03-30T21:01:38.108Z",
  "name": "Pass the Ticket",
  "description": "Adversaries may \u201cpass the ticket\u201d using stolen Kerberos tickets to move laterally within an environment, bypassing normal system access controls. Pass the ticket (PtT) is a method of authenticating to a system using Kerberos tickets without having access to an account's
```

password. Kerberos authentication can be used as the first step to lateral movement to a remote system.\n\nWhen performing PtT, valid Kerberos tickets for [Valid Accounts](https://attack.mitre.org/techniques/T1078) are captured by [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). A user's service tickets or ticket granting ticket (TGT) may be obtained, depending on the level of access. A service ticket allows for access to a particular resource, whereas a TGT can be used to request service tickets from the Ticket Granting Service (TGS) to access any resource the user has privileges to access.(Citation: ADSecurity AD Kerberos Attacks)(Citation: GentilKiwi Pass the Ticket)\n\nA [Silver Ticket](https://attack.mitre.org/techniques/T1558/002) can be obtained for services that use Kerberos as an authentication mechanism and are used to generate tickets to access that particular resource and the system that hosts the resource (e.g., SharePoint).(Citation: ADSecurity AD Kerberos Attacks)\n\nA [Golden Ticket](https://attack.mitre.org/techniques/T1558/001) can be obtained for the domain using the Key Distribution Service account KRBtgt account NTLM hash, which enables generation of TGTs for any account in Active Directory.(Citation: Campbell 2014)\n\nAdversaries may also create a valid Kerberos ticket using other user information, such as stolen password hashes or AES keys. For example, \"overpassing the hash\" involves using a NTLM password hash to authenticate as a user (i.e. [Pass the Hash](https://attack.mitre.org/techniques/T1550/002)) while also using the password hash to create a valid Kerberos ticket.(Citation: Stealthbits Overpass-the-Hash)",

```
"kill_chain_phases": [
  {
    "kill_chain_name": "mitre-attack",
    "phase_name": "defense-evasion"
  },
  {
    "kill_chain_name": "mitre-attack",
    "phase_name": "lateral-movement"
  }
],
"x_mitre_contributors": [
  "Vincent Le Toux",
  "Ryan Becwar"
],
"x_mitre_detection": "Audit all Kerberos authentication and credential use events and review for discrepancies. Unusual remote authentication events that correlate with other suspicious activity (such as writing and executing binaries) may indicate malicious activity.\n\nEvent ID 4769 is generated on the Domain Controller when using a golden ticket after the KRBtgt password has been reset twice, as mentioned in the mitigation section. The status code 0x1F indicates the action has failed due to \"Integrity check on decrypted field failed\" and indicates misuse by a previously invalidated golden ticket.(Citation: CERT-EU Golden Ticket Protection)",
"x_mitre_domains": [
  "enterprise-attack"
],
"x_mitre_is_subtechnique": true,
"x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
"x_mitre_platforms": [
  "Windows"
],
"x_mitre_version": "1.1",
"x_mitre_data_sources": [
  "Logon Session: Logon Session Creation",
  "User Account: User Account Authentication",
  "Active Directory: Active Directory Credential Request"
],
"x_mitre_defense_bypassed": [
  "System Access Controls"
],
"x_mitre_system_requirements": [
  "Kerberos authentication enabled"
],
"type": "attack-pattern",
"id": "attack-pattern--7b211ac6-c815-4189-93a9-ab415deca926",
"created": "2020-01-30T17:03:43.072Z",
"created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
"external_references": [
  {
    "source_name": "mitre-attack",
    "url": "https://attack.mitre.org/techniques/T1550/003",
    "external_id": "T1550.003"
  }
]
```

```

    },
    {
      "source_name": "ADSecurity AD Kerberos Attacks",
      "description": "Metcalfe, S. (2014, November 22). Mimikatz and Active Directory Kerberos Attacks. Retrieved June 2, 2016.",
      "url": "https://adsecurity.org/?p=556"
    },
    {
      "source_name": "GentilKiwi Pass the Ticket",
      "description": "Depledge, B. (2014, January 13). Pass the ticket. Retrieved June 2, 2016.",
      "url": "http://blog.gentilkiwi.com/securing/mimikatz/pass-the-ticket-kerberos"
    },
    {
      "source_name": "Campbell 2014",
      "description": "Campbell, C. (2014). The Secret Life of Krbtgt. Retrieved December 4, 2014.",
      "url": "http://defcon.org/images/defcon-22/dc-22-presentations/Campbell/DEFCON-22-Christopher-Campbell-The-Secret-Life-of-Krbtgt.pdf"
    },
    {
      "source_name": "Stealthbits Overpass-the-Hash",
      "description": "Warren, J. (2019, February 26). How to Detect Overpass-the-Hash Attacks. Retrieved February 4, 2021.",
      "url": "https://stealthbits.com/blog/how-to-detect-overpass-the-hash-attacks/"
    },
    {
      "source_name": "CERT-EU Golden Ticket Protection",
      "description": "Abolins, D., Boldea, C., Socha, K., Soria-Machado, M. (2016, April 26). Kerberos Golden Ticket Protection. Retrieved July 13, 2017.",
      "url": "https://cert.europa.eu/static/WhitePapers/UPDATED%20-%20CERT-EU_Security_Whitepaper_2014-007_Kerberos_Golden_Ticket_Protection_v1_4.pdf"
    }
  ],
  "object_marking_refs": [
    "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
  ],
  "x_mitre_attack_spec_version": "3.1.0",
  "spec_version": "2.1"
},
{
  "type": "x-oca-behavior",
  "spec_version": "2.1",
  "id": "x-oca-behavior--DE81EF18-55E6-4754-A761-6B929BF22395",
  "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "name": "Exfiltration Behavior via Beacon",
  "description": "Adversary exfiltrates data from the target network.",
  "behavior_class": "anomalous",
  "tactic": "Exfiltration",
  "technique": "T1041 - Exfiltration over C2 Channel",
  "first_seen": "2022-03-31T13:00:00.000Z",
  "platforms": [
    {
      "operating_system": "Microsoft Windows",
      "version": "10"
    }
  ],
  "extensions": {
    "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
      "extension_type": "new-sdo"
    }
  }
},
{
  "type": "x-oca-detection",
  "spec_version": "2.1",
  "id": "x-oca-detection--66aa9c25-8b56-4121-8630-dbe457393b27",
  "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",

```

```

"created": "2022-03-31T13:00:00.000Z",
"modified": "2022-03-31T13:00:00.000Z",
"name": "Data Exfiltration Detection",
"data_sources": [
  {
    "data_type": "zeek",
    "LogName": [
      "/nsm/zeek/logs/current/files.log",
      "SMB"
    ]
  }
],
"analytic": {
  "type": "Sigma Rule",
  "rule":
"YXV0aG9yOiBkZW1vcmRhdGU6IDIwMjIvMDMvMDQKZGVzY3JpcHRpb246IERldGVjdHMgYSBkb3dubG9hZCBmcm9tIGEgc2Vuc2l0aXZlI
G1vbm10b3JlZCBkaXJlY3RvcnkKaWQ6IDkyYTIxYmVmlTQxMzgtNDBiNi1hOTU1LTQ5N2IwY2UwNTE1MApzdGF0dXM6IGV4cGVyaW11bnR
hbAp0YWdzOgogIC0gYXR0YWNrLmV4ZmlsdHJhdGlvbGogIC0gYXR0YWNrLnQxMDQxcmxvZ3NvdXJjZTogCiAgcHJvZHVjdDogemVlawogI
GluZGV4OjBtYWluCiAgY2F0ZWdvcnk6IGZpbGVzcmRldGVjdGlvbjoKICBzZWx1Y3Rpb246IAogICAgc291cmNldHlwZTogemVlawogICA
gc291cmNldiAvbnNtL3plZWsvbG9ncy9jdXJyZW50L2ZpbGVzLmxvZWogICAgZmlsZW5hbWV8Y29udGFpbnM6ICJTW5zaXRpdmUgRGF0Y
SIKICBjb25kaXRpb246IHNlbGVjdGlvbGpmYWxzZXBvc2l0aXZlcz0KICAtIEFwcHJvdmVkJEFjY2Vzc29ycwpsZXZlbDogaGlnaA=="
  },
  "extensions": {
    "extension-definition--c4690e13-107e-4796-8158-0dcf1ae7bc89": {
      "extension_type": "new-sdo"
    }
  }
},
{
  "type": "ipv4-addr",
  "spec_version": "2.1",
  "id": "ipv4-addr--3d4ee4f2-a895-5781-a0cc-b5ba466f053d",
  "value": "192.168.1.3"
},
{
  "type": "network-traffic",
  "spec_version": "2.1",
  "id": "network-traffic--fcff628d-d69f-5d23-88b0-aecedcfb7da7c",
  "src_ref": "ipv4-addr--3d4ee4f2-a895-5781-a0cc-b5ba466f053d",
  "dst_ref": "ipv4-addr--57a33521-9761-54a9-81de-3c11e441d86b",
  "protocols": [
    "ipv4",
    "tcp"
  ]
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--94aaccf3-e8c4-41c0-985a-473f46312bb7",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "detects",
  "source_ref": "x-oca-detection--66aa9c25-8b56-4121-8630-dbe457393b27",
  "target_ref": "x-oca-behavior--DE81EF18-55E6-4754-A761-6B929BF22395"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--c4e4b439-2662-47e1-b961-2b6a6fae5241",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "x-oca-behavior--DE81EF18-55E6-4754-A761-6B929BF22395",
  "target_ref": "attack-pattern--92d7da27-2d91-488e-a00c-059dc162766d"
},
{
  "type": "relationship",
  "spec_version": "2.1",

```

```

    "id": "relationship--fd55f673-53b0-4ae1-915b-6f30b20c950b",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "campaign--f3bf3827-d9c5-414d-b0f0-610146ff5d85",
    "target_ref": "attack-pattern--92d7da27-2d91-488e-a00c-059dc162766d"
  },
  {
    "modified": "2023-05-09T14:00:00.188Z",
    "name": "Exfiltration Over C2 Channel",
    "description": "Adversaries may steal data by exfiltrating it over an existing command and control
channel. Stolen data is encoded into the normal communications channel using the same protocol as command
and control communications.",
    "kill_chain_phases": [
      {
        "kill_chain_name": "mitre-attack",
        "phase_name": "exfiltration"
      }
    ],
    "x_mitre_contributors": [
      "William Cain"
    ],
    "x_mitre_deprecated": false,
    "x_mitre_detection": "Analyze network data for uncommon data flows (e.g., a client sending
significantly more data than it receives from a server). Processes utilizing the network that do not
normally have network communication or have never been seen before are suspicious. Analyze packet contents
to detect communications that do not follow the expected protocol behavior for the port that is being
used. (Citation: University of Birmingham C2)",
    "x_mitre_domains": [
      "enterprise-attack"
    ],
    "x_mitre_is_subtechnique": false,
    "x_mitre_platforms": [
      "Linux",
      "macOS",
      "Windows"
    ],
    "x_mitre_version": "2.2",
    "x_mitre_data_sources": [
      "Network Traffic: Network Traffic Content",
      "Network Traffic: Network Traffic Flow",
      "File: File Access",
      "Network Traffic: Network Connection Creation",
      "Command: Command Execution"
    ],
    "x_mitre_network_requirements": false,
    "type": "attack-pattern",
    "id": "attack-pattern--92d7da27-2d91-488e-a00c-059dc162766d",
    "created": "2017-05-31T21:30:41.804Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "revoked": false,
    "external_references": [
      {
        "source_name": "mitre-attack",
        "url": "https://attack.mitre.org/techniques/T1041",
        "external_id": "T1041"
      },
      {
        "source_name": "University of Birmingham C2",
        "description": "Gardiner, J., Cova, M., Nagaraja, S. (2014, February). Command & Control
Understanding, Denying and Detecting. Retrieved April 20, 2016.",
        "url": "https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf"
      }
    ],
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "x_mitre_attack_spec_version": "3.1.0",

```

```

    "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1"
  },
  {
    "type": "identity",
    "spec_version": "2.1",
    "id": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2023-05-23T10:09:00.000Z",
    "name": "OCA"
  },
  {
    "type": "identity",
    "spec_version": "2.1",
    "id": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "created": "2017-06-01T00:00:00.000Z",
    "modified": "2022-04-25T14:00:00.188Z",
    "name": "The MITRE Corporation",
    "identity_class": "organization",
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "x_mitre_attack_spec_version": "2.1.0",
    "x_mitre_domains": [
      "enterprise-attack"
    ],
    "x_mitre_version": "1.0"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--d99350ec-bc5b-4d92-8990-ae6b08ffce7a",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "occurs-before",
    "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bc",
    "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--d3f134d4-bf65-477c-927e-1b0e87630e38",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "occurs-before",
    "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab",
    "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bc"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--3ad280cd-42f7-49b6-88ff-d2ee35a175b6",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "occurs-before",
    "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa",
    "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bb"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--0347363b-b476-4bff-8203-a585febf21bb",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "occurs-before",
    "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa",
    "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890cc"
  }
},

```



```
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--87c4aca0-6b97-4fe9-ab99-ab5ba7f3db95",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "occurs-before",
  "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bb",
  "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890dd"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--33da2e36-637b-47a7-ae95-d8ae192fb3d2",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "occurs-before",
  "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890dd",
  "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ee"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--72fc61e3-67d7-497e-900b-faf26173bd71",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "occurs-before",
  "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ee",
  "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ff"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--88ae0ce8-96d8-4886-a5aa-bbc0a32c3a3f",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "occurs-before",
  "source_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ff",
  "target_ref": "x-oca-behavior--DE81EF18-55E6-4754-A761-6B929BF22395"
},
{
  "type": "extension-definition",
  "spec_version": "2.1",
  "id": "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62",
  "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "name": "x-oca-behavior Extension Definition",
  "description": "This schema creates a new object type called x-oca-behavior. x-oca-behavior objects describe higher-level functionality than can be described using SCOs.",
  "schema": "https://raw.githubusercontent.com/opencybersecurityalliance/oca-iob/main/apl_reference_implementation_bundle/revision_2/schemas/sdos/behavior.json",
  "version": "1.0.0",
  "extension_types": [
    "new-sdo"
  ]
},
{
  "type": "extension-definition",
  "spec_version": "2.1",
  "id": "extension-definition--5cccba5c-0be4-450c-8672-b66e98515754",
  "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
  "created": "2023-05-01T12:00:00.000Z",
  "modified": "2023-05-01T12:00:00.000Z",
  "name": "x-oca-detector Extension Definition",
  "description": "This schema creates a new object type called detector, which describes software that is capable of performing detections.",
}
```

```

    "schema": "https://raw.githubusercontent.com/opencybersecurityalliance/oca-
iob/main/apl_reference_implementation_bundle/revision_2/schemas/sdos/detector.json",
    "version": "1.0.0",
    "extension_types": [
        "new-sdo"
    ]
},
{
    "type": "extension-definition",
    "spec_version": "2.1",
    "id": "extension-definition--c4690e13-107e-4796-8158-0dcf1ae7bc89",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "x-oca-detection Extension Definition",
    "description": "This schema creates a new object type called detection, which contain queries or
other actionable information that can identify an event or behavior.",
    "schema": "https://raw.githubusercontent.com/opencybersecurityalliance/oca-
iob/main/apl_reference_implementation_bundle/revision_2/schemas/sdos/detection.json",
    "version": "1.0.0",
    "extension_types": [
        "new-sdo"
    ]
},
{
    "type": "extension-definition",
    "spec_version": "2.1",
    "id": "extension-definition--f9dbe89c-0030-4a9d-8b78-0dcd0a0de874",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "x-oca-process Extension Definition",
    "description": "This schema extends the Process SCO with additional Windows Event Log fields.",
    "schema": "https://raw.githubusercontent.com/opencybersecurityalliance/oca-
iob/main/apl_reference_implementation_bundle/revision_2/schemas/observables/extended-process.json",
    "version": "1.0.0",
    "extension_types": [
        "property-extension"
    ]
},
{
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--e82c60ee-78e1-4056-a2e0-2ed73571605d",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "detects",
    "source_ref": "x-oca-detection--58834c29-4ceb-42a1-a218-336103021000",
    "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa"
},
{
    "type": "windows-registry-key",
    "spec_version": "2.1",
    "id": "windows-registry-key--c5a4244e-22d5-5797-8f78-c5fc3d1c0bde",
    "key": "\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run",
    "values": [
        {
            "name": "persist"
        }
    ],
    "extensions": {
        "extension-definition--2cf8c8c2-69f5-40f7-aa34-efcef2b912b1": {
            "action": "modify",
            "new_value": "true",
            "process_id": "0x0",
            "process_name": "C:\\Windows\\regedit.exe",
            "extension_type": "property-extension"
        }
    }
}

```

```

    }
  },
  {
    "type": "process",
    "spec_version": "2.1",
    "id": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcaaa",
    "is_hidden": false,
    "pid": 0,
    "cwd": "C:\\Program Files\\Microsoft Office\\Office14\\",
    "command_line": "C:\\Program Files\\Microsoft Office\\Office14\\OUTLOOK.EXE",
    "extensions": {
      "extension-definition--f9dbe89c-0030-4a9d-8b78-0dcd0a0de874": {
        "extension_type": "property-extension",
        "action": "created",
        "new_process_name": [
          "OUTLOOK.EXE"
        ],
        "win_event_code": "4688"
      }
    },
    "created_time": "2022-03-31T13:00:00.000Z",
    "defanged": false
  },
  {
    "type": "process",
    "spec_version": "2.1",
    "id": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcbbb",
    "is_hidden": false,
    "pid": 0,
    "cwd": "C:\\Program Files\\Microsoft Office\\Office14\\",
    "command_line": "C:\\User\\jsmith.CBIS\\AppData\\Local\\Google\\Chrome\\Application\\chrome.exe --
single-argument https://172.25.1.19/download/test.docm",
    "parent_ref": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcaaa",
    "extensions": {
      "extension-definition--f9dbe89c-0030-4a9d-8b78-0dcd0a0de874": {
        "extension_type": "property-extension",
        "action": "created",
        "creator_process_name": [
          "OUTLOOK.EXE"
        ],
        "new_process_name": [
          "chrome.exe"
        ],
        "win_event_code": "4688"
      }
    },
    "created_time": "2022-03-31T13:00:00.000Z",
    "defanged": false
  },
  {
    "type": "process",
    "spec_version": "2.1",
    "id": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcccc",
    "is_hidden": false,
    "pid": 0,
    "cwd": "C:\\User\\jsmith.CBIS\\AppData\\Local\\Google\\Chrome\\Application\\",
    "command_line": "'C:\\Program Files\\Microsoft Office\\Office14\\WINWORD.EXE' /n
'C:\\Users\\jsmith.CBIS\\Downloads\\test.docm'",
    "parent_ref": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcbbb",
    "extensions": {
      "extension-definition--f9dbe89c-0030-4a9d-8b78-0dcd0a0de874": {
        "extension_type": "property-extension",
        "action": "created",
        "creator_process_name": [
          "chrome.exe"
        ],
        "new_process_name": [
          "WINWORD.EXE"
        ]
      }
    }
  }
}

```

```

    ],
    "win_event_code": "4688"
  },
  {
    "type": "process",
    "spec_version": "2.1",
    "id": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcddd",
    "is_hidden": false,
    "pid": 0,
    "cwd": "C:\\Program Files\\Microsoft Office\\Office14\\",
    "command_line": "C:\\Users\\JSMITH.CBIS\\AppData\\Local\\Temp\\rad99952.tmp.exe",
    "parent_ref": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcccc",
    "extensions": {
      "extension-definition--f9dbe89c-0030-4a9d-8b78-0dcd0a0de874": {
        "extension_type": "property-extension",
        "action": "created",
        "creator_process_name": [
          "WINWORD.EXE"
        ],
        "new_process_name": [
          "C:\\Users\\JSMITH.CBIS\\AppData\\Local\\Temp\\rad99952.tmp.exe"
        ],
        "win_event_code": "4688"
      }
    },
    "created_time": "2022-03-31T13:00:00.000Z",
    "defanged": false
  },
  {
    "type": "x-oca-detection",
    "spec_version": "2.1",
    "id": "x-oca-detection--58834c29-4ceb-42a1-a218-336103021111",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "Process 1 - SpearPhish",
    "data_sources": [
      {
        "EventCode": "4688",
        "LogName": "Security",
        "TaskCategory": "Process Creation",
        "data_type": "WinEventLog:Security",
        "Creator_Process_Name": [
          "*outlook*",
          "*thunderbird*",
          "*mail*"
        ],
        "New_Process_Name": [
          "*edge*",
          "*chrome*",
          "*firefox*"
        ]
      }
    ],
    "analytic": {
      "rule": "
LS0tCnRpdGx1OiBTcGVhcnBoaXNoaW5nIHdpdGggTGluawppZDogc3BlYXJwaGlzaGluZwpzdGF0dXM6IGV4cGVyYW1lbnRhbApkZXNjc
mlwdGlvbjogRGV0ZW90cyBPZmZpY2UgbWFWjcm8gb3BlbmlyZyBmcm9tIGJyb3dzZXIuCnRhZ3M6Ci0gYXR0YWNRlmluaXRpYXxYWNjZXN
zCi0gYXR0YWNRlLnQxNTY2LjAwMgphdXRob3I6IGRlbW8KZGF0ZTogMjAyMS8wNi8wNwpsb2dzb3VyY2U6CiAgcHJvZHVjdDogd2luZG93c
wogIGluZGV4Q0iBtYWluCiAgY2F0ZWdvcmk6IHByb2Nlc3NfZXZlbnQKZGV0ZW90aW9uOgogIHNlbGVjdGlvbjokICAgIEV2ZW50Q29kZTo
gJzQ2ODgnCiAgICBDcmVhdG9yX1Byb2Nlc3NfTmFtZXxjb250YWluczoKICAgIC0gb3V0bG9vawogICAgLSB0aHVuZGVyYmlyZAogICAgL
SBtYWlsCiAgICB0ZXdfUHJvY2Vzc190YW11fGNvbnRhaw5zOgogICAgLSB1ZGdlCiAgICAtIGNocm9tZQogICAgLSBmaXJlZm94CiAgY29
uZGl0aW9uOiBzZwly3Rpb24KZmFsc2Vwb3NpdG12ZXM6Ci0gTG93Cm9ldmVsOiBoawdo",
      "type": "Sigma Rule - base64 encoded YAML file"
    }
  }
]

```

```

    },
    "extensions": {
      "extension-definition--c4690e13-107e-4796-8158-0dcf1ae7bc89": {
        "extension_type": "new-sdo"
      }
    }
  },
  {
    "type": "x-oca-detection",
    "spec_version": "2.1",
    "id": "x-oca-detection--58834c29-4ceb-42a1-a218-336103021222",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "Process 2 - SpearPhish",
    "data_sources": [
      {
        "EventCode": "4688",
        "LogName": "Security",
        "TaskCategory": "Process Creation",
        "data_type": "WinEventLog:Security",
        "Creator_Process_Name": [
          "*edge*",
          "*chrome*",
          "*firefox*"
        ],
        "Creator_Command_Line": [
          "*docm*",
          "*pptm*",
          "*xlsm*"
        ],
        "New_Process_Name": [
          "*word*",
          "*powerpoint*",
          "*excel*"
        ]
      }
    ],
    "analytic": {
      "rule": "LS0tCnRpdGx1OiB0TcGVhcnBoaXNoaW5nIHdpdGggTGluawppZDogc3BlYXJwaGlzaGluZWpzdzGF0dXM6IGV4cGVyaW1lbnRhbmApkZXNjcmlwdGlvbjogRGV0ZW90cyBPZmZpY2UgbWFiYjcm8gb3BlbmlyZyBmc9tIGJyb3dzZXIuCnRhZ3M6Ci0gYXR0YWNRlmluaXRpYWxfYWVjZXNzCi0gYXR0YWNRlnQxNTY2LjAwMgphdXRob3I6IGRlbW8KZGF0ZTogMjAyMS8wNi8wNWpsb2dzb3VyY2U6CiAgcHJvZHVjdDogd2luZG93cwogIGluZGV4OjBTYWluCiAgY2F0ZWdvbnk6IHByb2Nlc3NfZXZlbnQKZGV0ZW90aW9uogogIHNlbGVjdGlvbjokICAgIEV2ZW50Q29kZTo gJzQ2ODgnCiAgICBOZXdfuHJVY2Vzc190YW1lfGNvb3RhaW5zOGogICAgLSB3aW53b3JkCiAgICAtIGV4Y2VsCiAgICAtIHBvd2VycG9pb nQKICAgIFByb2Nlc3NFQ29tbWFuZF9MaW5lfGNvb3RhaW5zOGogICAgLSBkb2NtCiAgICAtIHhsaW50KICAgIC0gcHB0bQogICAgQ3JlYXR vcl9Qcm9jZXNzX05hbWV8Y29udGFpbmM6CiAgICAtIGVkZ2UKICAgIC0gY2hyb21lCiAgICAtIGZpcmb3gKICBjb25kaXRpb246IHNlb GVjdGlvbgpmYWxzZXhvc2l0aXZlczoKLSEBMb3cKbGV2ZWw6IGhpZ2g=",
      "type": "Sigma Rule - base64 encoded YAML file"
    },
    "extensions": {
      "extension-definition--c4690e13-107e-4796-8158-0dcf1ae7bc89": {
        "extension_type": "new-sdo"
      }
    }
  },
  {
    "type": "x-oca-detection",
    "spec_version": "2.1",
    "id": "x-oca-detection--58834c29-4ceb-42a1-a218-336103021000",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "Process - Execution",
    "data_sources": [
      {
        "EventCode": "4688",
        "LogName": "Security",

```


Page 63

Page 64

[illegible]

[illegible]

Page 67

Page 68

[illegible]

[illegible]

Page 71

[illegible]

[illegible]

[illegible]

[illegible]

Page 76

[illegible]

[illegible]

UNCLASSIFIED

[illegible]

Page 81

Page 82

Page 83

```

"x-oca-detection--58834c29-4ceb-42a1-a218-336103021222",
"x-oca-detection--5899C5CC-CE20-44EE-806E-9F64EBA0B29F",
"x-oca-detection--275bf485-736d-4aa5-b172-e34d28faa58c",
"x-oca-detection--f27cb358-d747-47ba-a6c4-e5b8debab157",
"x-oca-detection--40a941cc-42df-4b2e-b607-6d74168084b9",
"x-oca-detection--66aa9c25-8b56-4121-8630-dbe457393b27"
],
"extensions": {
  "extension-definition--dbbce349-3550-4cdd-8a7b-af58bc12de6c": {
    "extension_type": "new-sdo"
  }
}
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--64726807-5082-43C3-B975-1484B60B963C",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "contains",
  "source_ref": "x-oca-detection-group--58834c29-4ceb-42a1-a218-321103021999",
  "target_ref": "x-oca-detection--66aa9c25-8b56-4121-8630-dbe457393b27"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--d8935337-1917-446c-9c63-ac0a36438712",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "contains",
  "source_ref": "x-oca-detection-group--58834c29-4ceb-42a1-a218-321103021999",
  "target_ref": "x-oca-detection--40a941cc-42df-4b2e-b607-6d74168084b9"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--eb6fd1a1-00bb-44c0-bba5-6c3a335c6cb6",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "contains",
  "source_ref": "x-oca-detection-group--58834c29-4ceb-42a1-a218-321103021999",
  "target_ref": "x-oca-detection--275bf485-736d-4aa5-b172-e34d28faa58c"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--64726807-5082-43C3-B975-1484B60B963D",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "contains",
  "source_ref": "x-oca-detection-group--58834c29-4ceb-42a1-a218-321103021999",
  "target_ref": "x-oca-detection--f27cb358-d747-47ba-a6c4-e5b8debab157"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--64726807-5082-43C3-B975-1484B60B963B",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "contains",
  "source_ref": "x-oca-detection-group--58834c29-4ceb-42a1-a218-321103021999",
  "target_ref": "x-oca-detection--5899C5CC-CE20-44EE-806E-9F64EBA0B29F"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--731021e2-e7a8-4863-ba41-65c893d7c564",
  "created": "2022-03-31T13:00:00.000Z",

```

```

    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "contains",
    "source_ref": "x-oca-detection-group--58834c29-4ceb-42a1-a218-321103021999",
    "target_ref": "x-oca-detection--58834c29-4ceb-42a1-a218-336103021000"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--3437bf91-0115-4c05-bfda-d9abf9954f8e",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "contains",
    "source_ref": "x-oca-detection-group--58834c29-4ceb-42a1-a218-321103021999",
    "target_ref": "x-oca-detection--458c02c9-3635-42e4-8873-6785e00517e7"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--e60900fc-e47e-44f3-aac2-4a5ca9be7c78",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "contains",
    "source_ref": "x-oca-detection-group--58834c29-4ceb-42a1-a218-321103021999",
    "target_ref": "x-oca-detection--58834c29-4ceb-42a1-a218-336103021111"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--535d743b-0b78-4891-a515-8ec92e65d42b",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "contains",
    "source_ref": "x-oca-detection-group--58834c29-4ceb-42a1-a218-321103021999",
    "target_ref": "x-oca-detection--58834c29-4ceb-42a1-a218-336103021222"
  },
  {
    "type": "extension-definition",
    "spec_version": "2.1",
    "id": "extension-definition--3b7505ce-2a18-496e-aa58-311dac6c1473",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "x-oca-network-traffic Extension Definition",
    "description": "This schema extends the Network Traffic SCO with beacon scoring information from
    Real Intelligence Threat Analytics (RITA).",
    "schema": "https://raw.githubusercontent.com/opencybersecurityalliance/oca-
    iob/main/apl_reference_implementation_bundle/revision_2/schemas/observables/extended-network-
    traffic.json",
    "version": "1.0.0",
    "extension_types": [
      "property-extension"
    ]
  },
  {
    "type": "extension-definition",
    "spec_version": "2.1",
    "id": "extension-definition--dbbce349-3550-4cdd-8a7b-af58bc12de6c",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "x-oca-detection-group Extension Definition",
    "description": "This schema creates a new object type called detection-group.",
    "schema": "https://raw.githubusercontent.com/opencybersecurityalliance/oca-
    iob/main/apl_reference_implementation_bundle/revision_2/schemas/sdos/detection-group.json",
    "version": "1.0.0",
    "extension_types": [
      "new-sdo"
    ]
  }
]

```

Page 86

[illegible]

[illegible]

[illegible]

Page 90

ZaIIC8+CiAgICAgIDwvYnBtBmRpOkJQTU5FZGd1PgogICAgICA8YnBtBmRpOkJQTU5FZGd1IGlkPSJGbG93XzF0aenNyOGdfZGkiIGJwbW5FbGVtZW50PSJGbG93XzF0aenNyOGciPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXMTTE1iB5PSiXMDIwIiAvPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXNDkwIiB5PSiXMDIwIiAvPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXNDkwIiB5PSi20DgiIC8+CiAgICAgICAgPGJwbW5kaTpCUE10TGFIZWw+CiAgICAgICAgICA8ZGM6Qm91bmRIZH9IjEjEMjIiIHk9IjEjEMDIwIiHdpZHRoPSiXNSiGagVpZ2h0PSiXNCiGIZ4KICAgICAgICA8L2JwbW5kaTpCUE10TGFIZWw+CiAgICAgICAgIDwvYnBtBmRpOkJQTU5FZGd1PgogICAgICA8YnBtBmRpOkJQTU5FZGd1IGlkPSJGbG93XzAwZW16YzRfZGkiIGJwbW5FbGVtZW50PSJGbG93XzAwZW16YzQiPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXMTTE1iB5PSi3NTAiIC8+CiAgICAgICAgPGRPOndheXBvaW50IHg9IjE0T0AiIHk9Ij1cMCIgZl4KICAgICAgICA8ZGk6d2F5cG9pbNqgeD0iMTQ5MCIgeT0iNjg4IiAvPgogICAgICAgIDxicG1uZGk6QlBNTkxhYmVsPgogICAgICAgICAgPGRjOgKjVdW5kcyB4PSiXMTIiB5PSi3MjgiHdpZHRoPSiXNSiGagVpZ2h0PSiXNCiGIZ4KICAgICAgICA8L2JwbW5kaTpCUE10TGFIZWw+CiAgICAgICAgIDwvYnBtBmRpOkJQTU5FZGd1PgogICAgICA8YnBtBmRpOkJQTU5FZGd1IGlkPSJGbG93XzAzYzZ5YXlFZGkiIGJwbW5FbGVtZW50PSJGbG93XzAzYzZ5YXkiPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXMDkwIiB5PSiXNjuiIC8+CiAgICAgICAgICAgPGRPOndheXBvaW50IHg9IjEwOTAiIHk9Ij1cMCIgZl4KICAgICAgICA8YnBtBmRpOkJQTU5MYWJlbd4KICAgICAgIDxkYzpbCb3VuZHMgeD0iMTA5NyIgeT0iMTk3IiB3aWR0aD0iMTgiGhlaWdodD0iMTQiIC8+CiAgICAgICAgICAgPC9icG1uZGk6QlBNTkxhYmVsPgogICAgICAgICA8L2JwbW5kaTpCUE10RWRRnZT4KICAgICAgPGJwbW5kaTpCUE10RWRRnZSBpZD0iRmxvd18waGU0a2R4X2R2IjBiBicG1uRwXlbnVudD0iRmxvd18waGU0a2R4Ij4KICAgICAgICA8ZGk6d2F5cG9pbNqgeD0iNjcwIiB5PSi20TUuiIC8+CiAgICAgICAgPGRPOndheXBvaW50IHg9IjY3MCIgeT0iNzUwIiAvPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSi4MTAiIHk9Ij1cMCIgZl4KICAgICAgPC9icG1uZGk6QlBNTkVkJkZ2U+CiAgICAgIDxicG1uZGk6QlBNTkVkJkZ2UgagWQ9IkJzsb3dfMHYzbnG1nM19kaSiGyYnBtbkVsZw1lbnQ9IkJzsb3dfMHYzbnG1nMi+CiAgICAgICAgICAgPGRPOndheXBvaW50IHg9IjEjEMDIwIiIHk9Ij1cMCIgZl4KICAgICAgICA8ZGk6d2F5cG9pbNqgeD0iMTQ5MCIgeT0iODg1IiAvPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXNDkwIiB5PSi20DgiIC8+CiAgICAgICAgIDwvYnBtBmRpOkJQTU5FZGd1PgogICAgICA8YnBtBmRpOkJQTU5FZGd1IGlkPSJGbG93XzAydHhlaZfZGkiIGJwbW5FbGVtZW50PSJGbG93XzAydHhlaZeiPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXMTQwIiB5PSiXMTUwIiAvPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXNDkwIiB5PSiXMTUwIiAvPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXNDkwIiB5PSi20DgiIC8+CiAgICAgICAgIDwvYnBtBmRpOkJQTU5FZGd1PgogICAgICA8YnBtBmRpOkJQTU5FZGd1IGlkPSJGbG93XzBxYnAyeTRfZGkiIGJwbW5FbGVtZW50PSJGbG93XzBxYnAyeT0iPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXNTA4IiB5PSi2NzAiIC8+CiAgICAgICAgICAgPGRPOndheXBvaW50IHg9IjE2MTAiIHk9Ij1cMCIgZl4KICAgICAgPC9icG1uZGk6QlBNTkVkJkZ2U+CiAgICAgIDxicG1uZGk6QlBNTkVkJkZ2UgagWQ9IkJzsb3dfMTFld2VuN19kaSiGyYnBtbkVsZw1lbnQ9IkJzsb3dfMTFld2VuNi+CiAgICAgICAgICAgPGRPOndheXBvaW50IHg9IjEwOTAiIHk9Ij1cMCIgZl4KICAgICAgICA8ZGk6d2F5cG9pbNqgeD0iMTA5MCIgeT0iNDEiIiAvPgogICAgICA8L2JwbW5kaTpCUE10RWRRnZT4KICAgICAgPGJwbW5kaTpCUE10RWRRnZSBpZD0iRmxvd18wbG9mXBMx2R2IjBiBicG1uRwXlbnVudD0iRmxvd18xbm9mXBMiIj4KICAgICAgICA8ZGk6d2F5cG9pbNqgeD0iMT0MCIgeT0iNTMwIiAvPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXNDkwIiB5PSi1MzAiIC8+CiAgICAgICAgICAgPGRPOndheXBvaW50IHg9IjE0T0AiIHk9Ij1YMiGIZl4KICAgICAgPC9icG1uZGk6QlBNTkVkJkZ2U+CiAgICAgIDxicG1uZGk6QlBNTkVkJkZ2UgagWQ9IkJzsb3dfMX3xdGNwa19kaSiGyYnBtbkVsZw1lbnQ9IkJzsb3dfMX3xdGNwai+CiAgICAgICAgICAgPGRPOndheXBvaW50IHg9IjEjEMTUuiIHk9Ij1cMCIgZl4KICAgICAgICA8ZGk6d2F5cG9pbNqgeD0iMTQ5MCIgeT0iMTQwIiAvPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXNDkwIiB5PSi2NTIiIiIC8+CiAgICAgICAgICAgPGJwbW5kaTpCUE10TGFIZWw+CiAgICAgICAgICA8ZGM6Qm91bmRIZH9IjEjEMjIiIHk9IjEjEMDIwIiHdpZHRoPSiXNSiGagVpZ2h0PSiXNCiGIZ4KICAgICAgIDwvYnBtBmRpOkJQTU5MYWJlbd4KICAgICAgPC9icG1uZGk6QlBNTkVkJkZ2U+CiAgICAgIDxicG1uZGk6QlBNTkVkJkZ2UgagWQ9IkJzsb3dfMHZjdG14ZF9kaSiGyYnBtbkVsZw1lbnQ9IkJzsb3dfMHZjdG14ZCI+CiAgICAgICAgICAgPGRPOndheXBvaW50IHg9IjEjEMTUuiIHk9Ij1cMCIgZl4KICAgICAgICA8ZGk6d2F5cG9pbNqgeD0iMTUwMiIgeT0iNjU3IiAvPgogICAgICAgIDxkaTp3YXlwb2ludCB4PSiXNTEyIiB5PSi2NDUuiIC8+CiAgICAgIDwvYnBtBmRpOkJQTU5FZGd1PgogICAgPC9icG1uZGk6QlBNTLBSYW5lPgogIDwvYnBtBmRpOkJQTU5EaWFncmFtPgo8L2JwbW46ZGVmaW5pdGlvbnM+Pg=="

```

      "playbook_abstraction": "template",
      "playbook_creation_time": "2022-03-31T13:00:00.000Z",
      "playbook_modification_time": "2022-03-31T13:00:00.000Z",
      "revoked": false,
      "playbook_creator": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "extensions": {
        "extension-definition--809C4D84-7A6E-4039-97B4-DA9FEA03FCF9": {
          "extension_type": "new-sdo"
        }
      }
    },
    {
      "type": "course-of-action",
      "spec_version": "2.1",
      "id": "course-of-action--94D890AC-3E24-4DEC-8ACB-C603FA4A7B20",
      "created": "2022-03-31T13:00:00.000Z",
      "modified": "2022-03-31T13:00:00.000Z",
      "name": "Mitigate Incident",
      "description": "Analyst mitigates the alert by blocking malicious IPs, sharing data, and/or remediating the affected system.",
      "extensions": {
        "extension-definition--BBC1D5C8-7DDC-4E89-BE9C-F33AD02D71DD": {
          "extension_type": "property-extension",
          "playbooks": {
            "CACA0": "x-oca-playbook--AE16A784-BAC9-4334-A09F-7CB63053A6D7",
            "BPMN": "x-oca-playbook--720E5E68-3959-4EE0-99DE-87A4EAA39F44"
          }
        }
      }
    }
  ]
}

```


Page 92

Page 93

[illegible]

```

    "playbook_abstraction": "template",
    "playbook_creation_time": "2022-03-31T13:00:00.000Z",
    "playbook_modification_time": "2022-03-31T13:00:00.000Z",
    "revoked": false,
    "playbook_creator": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "extensions": {
      "extension-definition--809C4D84-7A6E-4039-97B4-DA9FEA03FCF9": {
        "extension_type": "new-sdo"
      }
    }
  },
  {
    "type": "course-of-action",
    "spec_version": "2.1",
    "id": "course-of-action--4E202C5A-C1DF-42D8-9AEF-809A8E172AE3",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "Quarantine and remediate",
    "description": "Remediate by quarantining and performing analyst guided steps",
    "extensions": {
      "extension-definition--BBC1D5C8-7DDC-4E89-BE9C-F33AD02D71DD": {
        "extension_type": "property-extension",
        "playbooks": {
          "CACAO": "x-oca-playbook--9880DF48-09A7-4E99-8070-0DB8F4C946D0",
          "BPMN": "x-oca-playbook--32F52089-9943-4231-BBA3-5C02BA654755"
        }
      }
    }
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--282D26EF-0FA0-4975-81FC-69B5946F47D2",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "related-to",
    "source_ref": "x-oca-playbook--9880DF48-09A7-4E99-8070-0DB8F4C946D0",
    "target_ref": "course-of-action--4E202C5A-C1DF-42D8-9AEF-809A8E172AE3"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--84606E92-B52C-4BCA-908C-7D01C498F90C",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "related-to",
    "source_ref": "x-oca-playbook--32F52089-9943-4231-BBA3-5C02BA654755",
    "target_ref": "course-of-action--4E202C5A-C1DF-42D8-9AEF-809A8E172AE3"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--D487D30C-1326-4C3E-943D-883498DDCC8F",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "related-to",
    "source_ref": "course-of-action--4E202C5A-C1DF-42D8-9AEF-809A8E172AE3",
    "target_ref": "x-oca-detection-group--58834c29-4ceb-42a1-a218-321103021999"
  }
]

```



```

    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--98CC25CE-EBDA-4BC2-9D0C-57173B321198",
      "created": "2022-03-31T13:00:00.000Z",
      "modified": "2022-03-31T13:00:00.000Z",
      "relationship_type": "related-to",
      "source_ref": "course-of-action--94D890AC-3E24-4DEC-8ACB-C603FA4A7B20",
      "target_ref": "x-oca-detection-group--58834c29-4ceb-42a1-a218-321103021999"
    },
    {
      "type": "extension-definition",
      "spec_version": "2.1",
      "id": "extension-definition--809C4D84-7A6E-4039-97B4-DA9FEA03FCF9",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2022-03-31T13:00:00.000Z",
      "modified": "2022-03-31T13:00:00.000Z",
      "name": "x-oca-playbook Extension Definition",
      "description": "This schema creates a new object type called x-oca-playbook.",
      "schema": "https://raw.githubusercontent.com/opencybersecurityalliance/oca-
iob/main/apl_reference_implementation_bundle/revision_2/schemas/sdos/playbook.json",
      "version": "1.0.0",
      "extension_types": [
        "new-sdo"
      ]
    },
    {
      "type": "extension-definition",
      "spec_version": "2.1",
      "id": "extension-definition--BBC1D5C8-7DDC-4E89-BE9C-F33AD02D71DD",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2022-03-31T13:00:00.000Z",
      "modified": "2022-03-31T13:00:00.000Z",
      "name": "x-oca-coa-playbook Extension Definition",
      "description": "This schema extends the Course of Action SDO with playbook information.",
      "schema": "https://raw.githubusercontent.com/opencybersecurityalliance/oca-
iob/main/apl_reference_implementation_bundle/revision_2/schemas/sdos/course-of-action.json",
      "version": "1.0.0",
      "extension_types": [
        "property-extension"
      ]
    },
    {
      "type": "observed-data",
      "spec_version": "2.1",
      "id": "observed-data--3a418c06-bf5d-48b7-9e91-84bff7e0846a",
      "created": "2022-03-31T13:00:00.000Z",
      "modified": "2022-03-31T13:00:00.000Z",
      "first_observed": "2022-03-31T13:00:00.000Z",
      "last_observed": "2022-03-31T13:00:00.000Z",
      "number_observed": 1,
      "object_refs": [
        "ipv4-addr--57a33521-9761-54a9-81de-3c11e441d86b",
        "ipv4-addr--bba1d187-08fb-5000-aed1-ef055c1dfd24",
        "network-traffic--15a157a8-26e3-56e0-820b-0c2a8e553a2c"
      ]
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--2d967554-6995-4bfe-bb6e-d1efeb990570",
      "created": "2022-03-31T13:00:00.000Z",
      "modified": "2022-03-31T13:00:00.000Z",
      "relationship_type": "related-to",
      "source_ref": "observed-data--3a418c06-bf5d-48b7-9e91-84bff7e0846a",
      "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bb"
    },
  ],
}

```



```
{
  "type": "observed-data",
  "spec_version": "2.1",
  "id": "observed-data--4a551d1b-8c08-46bb-b1b8-79b4caa638e2",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "first_observed": "2022-03-31T13:00:00.000Z",
  "last_observed": "2022-03-31T13:00:00.000Z",
  "number_observed": 1,
  "object_refs": [
    "process--3BCFB0A5-BAF5-411D-B9D0-8D4B4E09BA82"
  ]
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--c901c890-c96c-46ca-bf5e-6eca1352ccbc",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "related-to",
  "source_ref": "observed-data--4a551d1b-8c08-46bb-b1b8-79b4caa638e2",
  "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890dd"
},
{
  "type": "observed-data",
  "spec_version": "2.1",
  "id": "observed-data--0e28ca31-6b10-4156-9678-4121b0c09a43",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "first_observed": "2022-03-31T13:00:00.000Z",
  "last_observed": "2022-03-31T13:00:00.000Z",
  "number_observed": 1,
  "object_refs": [
    "network-traffic--acffdf9a-bafd-5b74-a7d9-1a6d5a4e9c5a",
    "ipv4-addr--57a33521-9761-54a9-81de-3c11e441d86b",
    "ipv4-addr--429ddae0-a1ff-543d-99b4-f12a4a144c70"
  ]
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--f2fec843-0fef-44e9-a799-930495a55479",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "relationship_type": "related-to",
  "source_ref": "observed-data--0e28ca31-6b10-4156-9678-4121b0c09a43",
  "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ee"
},
{
  "type": "observed-data",
  "spec_version": "2.1",
  "id": "observed-data--08bd537f-69d9-44e0-90c9-13dc784c4eef",
  "created": "2022-03-31T13:00:00.000Z",
  "modified": "2022-03-31T13:00:00.000Z",
  "first_observed": "2022-03-31T13:00:00.000Z",
  "last_observed": "2022-03-31T13:00:00.000Z",
  "number_observed": 1,
  "object_refs": [
    "ipv4-addr--57a33521-9761-54a9-81de-3c11e441d86b",
    "network-traffic--3564fb7d-d65c-5e02-9f55-a8a960f5c9f5",
    "domain-name--8713b93b-186e-524d-9224-db3b8f9fb9ef"
  ]
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--6befc841-7b3b-4680-b7d6-7c743327d150",
  "created": "2022-03-31T13:00:00.000Z",
```

```

    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "related-to",
    "source_ref": "observed-data--08bd537f-69d9-44e0-90c9-13dc784c4eef",
    "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ff"
  },
  {
    "type": "observed-data",
    "spec_version": "2.1",
    "id": "observed-data--f8dc1a7e-33ec-4dc1-8076-739bdcc7358b",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "first_observed": "2022-03-31T13:00:00.000Z",
    "last_observed": "2022-03-31T13:00:00.000Z",
    "number_observed": 1,
    "object_refs": [
      "network-traffic--fcff628d-d69f-5d23-88b0-aedc7b7da7c",
      "ipv4-addr--3d4ee4f2-a895-5781-a0cc-b5ba466f053d",
      "ipv4-addr--57a33521-9761-54a9-81de-3c11e441d86b"
    ]
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--175473ba-1bf9-4168-a339-65454db013b2",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "related-to",
    "source_ref": "observed-data--f8dc1a7e-33ec-4dc1-8076-739bdcc7358b",
    "target_ref": "x-oca-behavior--DE81EF18-55E6-4754-A761-6B929BF22395"
  },
  {
    "type": "observed-data",
    "spec_version": "2.1",
    "id": "observed-data--1419d15e-65e8-4707-9311-25a8b571e7de",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "first_observed": "2022-03-31T13:00:00.000Z",
    "last_observed": "2022-03-31T13:00:00.000Z",
    "number_observed": 1,
    "object_refs": [
      "windows-registry-key--c5a4244e-22d5-5797-8f78-c5fc3d1c0bde"
    ]
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--0e0da782-5c16-485c-ab7d-1447d1851342",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "related-to",
    "source_ref": "observed-data--1419d15e-65e8-4707-9311-25a8b571e7de",
    "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890cc"
  },
  {
    "type": "observed-data",
    "spec_version": "2.1",
    "id": "observed-data--7646a2bc-514c-4599-ae87-ddb8afa89a51",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "first_observed": "2022-03-31T13:00:00.000Z",
    "last_observed": "2022-03-31T13:00:00.000Z",
    "number_observed": 1,
    "object_refs": [
      "process--862e625d-48bb-489e-8d4e-f7d8cd2fcaaa",
      "process--862e625d-48bb-489e-8d4e-f7d8cd2fcbbb"
    ]
  },
  },
  {

```

```

    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--e55308a4-db4e-4a00-a136-a0ccd26178ff",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "related-to",
    "source_ref": "observed-data--7646a2bc-514c-4599-ae87-ddb8afa89a51",
    "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab"
  },
  {
    "type": "observed-data",
    "spec_version": "2.1",
    "id": "observed-data--1a0ce5cc-0115-4108-b30b-8919efa2925c",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "first_observed": "2022-03-31T13:00:00.000Z",
    "last_observed": "2022-03-31T13:00:00.000Z",
    "number_observed": 1,
    "object_refs": [
      "process--862e625d-48bb-489e-8d4e-f7d8cd2fcccc",
      "process--862e625d-48bb-489e-8d4e-f7d8cd2fcddd"
    ]
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--22083b73-9546-41fd-a150-beb3e062766e",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "related-to",
    "source_ref": "observed-data--1a0ce5cc-0115-4108-b30b-8919efa2925c",
    "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bc"
  },
  {
    "type": "observed-data",
    "spec_version": "2.1",
    "id": "observed-data--12d2cf2b-5f87-4efc-b8cd-c70d719e351a",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "first_observed": "2022-03-31T13:00:00.000Z",
    "last_observed": "2022-03-31T13:00:00.000Z",
    "number_observed": 1,
    "object_refs": [
      "process--862e625d-48bb-489e-8d4e-f7d8cd2fcddd"
    ]
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--117e35be-a2ba-4b8f-b0ed-cbd22b14940e",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "relationship_type": "related-to",
    "source_ref": "observed-data--12d2cf2b-5f87-4efc-b8cd-c70d719e351a",
    "target_ref": "x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--ac03ff3c-a51c-4637-bbd9-0f59900a1872",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detection--5899C5CC-CE20-44EE-806E-9F64EBA0B29F",
    "target_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e"
  },
  {
    "type": "relationship",

```

```

    "spec_version": "2.1",
    "id": "relationship--4ca132b3-f40d-4e38-9d32-a5dc8e91efb0",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detection--5899C5CC-CE20-44EE-806E-9F64EBA0B29F",
    "target_ref": "x-oca-detector--9441073d-119b-4ec9-aa08-8bdb1703ed56"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--3089c0c1-2a6b-4ab0-b274-25d375362892",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detection--58834c29-4ceb-42a1-a218-336103021111",
    "target_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--958b9180-7270-493f-942e-33d0798572f7",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detection--58834c29-4ceb-42a1-a218-336103021222",
    "target_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--cab1e466-64c3-4752-bbce-134bae74b43f",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detection--58834c29-4ceb-42a1-a218-336103021000",
    "target_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--f5e74b96-093f-4942-a8c3-a05ee36023ec",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detection--458c02c9-3635-42e4-8873-6785e00517e7",
    "target_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--37777af9-db8b-46ca-b1d5-3abc5724d8f2",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detection--f27cb358-d747-47ba-a6c4-e5b8debab157",
    "target_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--c7eac063-5707-406b-ad43-2a83e5344d61",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detection--275bf485-736d-4aa5-b172-e34d28faa58c",
    "target_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e"
  }
},

```

```
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--23ffdaa4-8be9-4eb3-b251-e82e605e2795",
  "created": "2023-05-15T13:00:00.000Z",
  "modified": "2023-05-15T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "x-oca-detection--275bf485-736d-4aa5-b172-e34d28faa58c",
  "target_ref": "x-oca-detector--67330653-ac02-46c8-b9c2-25b837a2ed6d"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--f2c14bce-581c-4b1d-9ea6-941c2e4a4880",
  "created": "2023-05-15T13:00:00.000Z",
  "modified": "2023-05-15T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "x-oca-detection--40a941cc-42df-4b2e-b607-6d74168084b9",
  "target_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--63b586d2-9d36-48f2-a8f3-36350abe66b6",
  "created": "2023-05-15T13:00:00.000Z",
  "modified": "2023-05-15T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "x-oca-detection--66aa9c25-8b56-4121-8630-dbe457393b27",
  "target_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--12fc0865-9f15-4e79-858a-1ac25ba2ff1f",
  "created": "2023-05-15T13:00:00.000Z",
  "modified": "2023-05-15T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "x-oca-detection--66aa9c25-8b56-4121-8630-dbe457393b27",
  "target_ref": "x-oca-detector--67330653-ac02-46c8-b9c2-25b837a2ed6d"
},
{
  "x_mitre_platforms": [
    "Windows"
  ],
  "x_mitre_domains": [
    "enterprise-attack",
    "ics-attack"
  ],
  "x_mitre_collection_layers": [
    "Host"
  ],
  "object_marking_refs": [
    "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
  ],
  "id": "x-mitre-data-source--0f42a24c-e035-4f93-a91c-5f7076bd8da0",
  "type": "x-mitre-data-source",
  "created": "2021-10-20T15:05:19.273Z",
  "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "external_references": [
    {
      "source_name": "mitre-attack",
      "url": "https://attack.mitre.org/datasources/DS0024",
      "external_id": "DS0024"
    },
    {
      "source_name": "Microsoft Registry",
      "description": "Microsoft. (2018, May 31). Registry. Retrieved September 29, 2021.",
      "url": "https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry"
    }
  ]
}
```

```

    }
  ],
  "modified": "2022-05-11T14:00:00.188Z",
  "name": "Windows Registry",
  "description": "A Windows OS hierarchical database that stores much of the information and settings
for software programs, hardware devices, user preferences, and operating-system configurations(Citation:
Microsoft Registry)",
  "x_mitre_version": "1.0",
  "x_mitre_attack_spec_version": "2.1.0",
  "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "spec_version": "2.1"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--417693ec-1543-48a4-be84-a238bf8dfb8d",
  "created": "2023-05-15T13:00:00.000Z",
  "modified": "2023-05-15T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e",
  "target_ref": "x-mitre-data-source--0f42a24c-e035-4f93-a91c-5f7076bd8da0"
},
{
  "object_marking_refs": [
    "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
  ],
  "id": "x-mitre-data-component--da85d358-741a-410d-9433-20d6269a6170",
  "type": "x-mitre-data-component",
  "created": "2021-10-20T15:05:19.273Z",
  "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "modified": "2022-04-25T14:00:00.188Z",
  "name": "Windows Registry Key Modification",
  "description": "Changes made to a Registry Key and/or Key value (ex: Windows EID 4657 or Sysmon EID
13|14)",
  "x_mitre_data_source_ref": "x-mitre-data-source--0f42a24c-e035-4f93-a91c-5f7076bd8da0",
  "x_mitre_version": "1.0",
  "x_mitre_attack_spec_version": "2.1.0",
  "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "spec_version": "2.1",
  "x_mitre_domains": [
    "enterprise-attack"
  ]
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--8a7f7654-5346-4897-b102-df81246af61e",
  "created": "2023-05-15T13:00:00.000Z",
  "modified": "2023-05-15T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e",
  "target_ref": "x-mitre-data-component--da85d358-741a-410d-9433-20d6269a6170"
},
{
  "modified": "2023-04-20T18:38:26.515Z",
  "name": "Process",
  "description": "Instances of computer programs that are being executed by at least one thread.
Processes have memory space for process executables, loaded modules (DLLs or shared libraries), and
allocated memory regions containing everything from user input to application-specific data
structures(Citation: Microsoft Processes and Threads)",
  "x_mitre_platforms": [
    "Linux",
    "Windows",
    "macOS",
    "Android",
    "iOS"
  ],
  "x_mitre_deprecated": false,

```



```

    "x_mitre_domains": [
      "enterprise-attack",
      "mobile-attack"
    ],
    "x_mitre_version": "1.1",
    "x_mitre_contributors": [
      "Center for Threat-Informed Defense (CTID)"
    ],
    "x_mitre_collection_layers": [
      "Host"
    ],
    "type": "x-mitre-data-source",
    "id": "x-mitre-data-source--e8b8ede7-337b-4c0c-8c32-5c7872c1ee22",
    "created": "2021-10-20T15:05:19.272Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "revoked": false,
    "external_references": [
      {
        "source_name": "mitre-attack",
        "url": "https://attack.mitre.org/datasources/DS0009",
        "external_id": "DS0009"
      },
      {
        "source_name": "Microsoft Processes and Threads",
        "description": "Microsoft. (2018, May 31). Processes and Threads. Retrieved September 28,
2021.",
        "url": "https://docs.microsoft.com/en-us/windows/win32/procthread/processes-and-threads"
      }
    ],
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "x_mitre_attack_spec_version": "3.1.0",
    "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--d811f064-2df1-46d3-954c-4011e74425da",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e",
    "target_ref": "x-mitre-data-source--e8b8ede7-337b-4c0c-8c32-5c7872c1ee22"
  },
  {
    "modified": "2022-10-07T16:15:56.932Z",
    "name": "Process Creation",
    "description": "The initial construction of an executable managed by the OS, that may involve one or
more tasks or threads. (e.g. Win EID 4688, Sysmon EID 1, cmd.exe > net use, etc.)",
    "x_mitre_data_source_ref": "x-mitre-data-source--e8b8ede7-337b-4c0c-8c32-5c7872c1ee22",
    "x_mitre_deprecated": false,
    "x_mitre_version": "1.1",
    "type": "x-mitre-data-component",
    "id": "x-mitre-data-component--3d20385b-24ef-40e1-9f56-f39750379077",
    "created": "2021-10-20T15:05:19.272Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "revoked": false,
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "x_mitre_attack_spec_version": "2.1.0",
    "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1",
    "x_mitre_domains": [
      "enterprise-attack"
    ]
  }
]

```

```

    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--913ea5e0-0ec0-4885-b241-6f53526a98e5",
      "created": "2023-05-15T13:00:00.000Z",
      "modified": "2023-05-15T13:00:00.000Z",
      "relationship_type": "uses",
      "source_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e",
      "target_ref": "x-mitre-data-component--3d20385b-24ef-40e1-9f56-f39750379077"
    },
    {
      "x_mitre_platforms": [
        "Linux",
        "Windows",
        "macOS"
      ],
      "x_mitre_domains": [
        "enterprise-attack"
      ],
      "x_mitre_contributors": [
        "Center for Threat-Informed Defense (CTID)"
      ],
      "x_mitre_collection_layers": [
        "Host"
      ],
      "object_marking_refs": [
        "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
      ],
      "id": "x-mitre-data-source--ba27545a-9c32-47ea-ba6a-cce50f1b326e",
      "type": "x-mitre-data-source",
      "created": "2021-10-20T15:05:19.274Z",
      "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "external_references": [
        {
          "source_name": "mitre-attack",
          "url": "https://attack.mitre.org/datasources/DS0033",
          "external_id": "DS0033"
        },
        {
          "source_name": "Microsoft NFS Overview",
          "description": "Microsoft. (2018, July 9). Network File System overview. Retrieved September 28, 2021.",
          "url": "https://docs.microsoft.com/en-us/windows-server/storage/nfs/nfs-overview"
        }
      ],
      "modified": "2022-03-30T14:26:51.806Z",
      "name": "Network Share",
      "description": "A storage resource (typically a folder or drive) made available from one host to others using network protocols, such as Server Message Block (SMB) or Network File System (NFS)(Citation: Microsoft NFS Overview)",
      "x_mitre_version": "1.0",
      "x_mitre_attack_spec_version": "2.1.0",
      "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "spec_version": "2.1"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--8c9b87b9-4b26-4235-b992-6a6b87a1a91a",
      "created": "2023-05-15T13:00:00.000Z",
      "modified": "2023-05-15T13:00:00.000Z",
      "relationship_type": "uses",
      "source_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e",
      "target_ref": "x-mitre-data-source--ba27545a-9c32-47ea-ba6a-cce50f1b326e"
    },
    {
      "object_marking_refs": [

```

```

    "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
  ],
  "id": "x-mitre-data-component--f5468e67-51c7-4756-9b4f-65707708e7fa",
  "type": "x-mitre-data-component",
  "created": "2021-10-20T15:05:19.275Z",
  "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "modified": "2022-04-25T14:00:00.188Z",
  "name": "Network Share Access",
  "description": "Opening a network share, which makes the contents available to the requestor (ex:
Windows EID 5140 or 5145)",
  "x_mitre_data_source_ref": "x-mitre-data-source--ba27545a-9c32-47ea-ba6a-cce50f1b326e",
  "x_mitre_version": "1.0",
  "x_mitre_attack_spec_version": "2.1.0",
  "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "spec_version": "2.1",
  "x_mitre_domains": [
    "enterprise-attack"
  ]
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--cc07695b-ddbe-4c76-b41a-5eae1e78bb2a",
  "created": "2023-05-15T13:00:00.000Z",
  "modified": "2023-05-15T13:00:00.000Z",
  "relationship_type": "uses",
  "source_ref": "x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e",
  "target_ref": "x-mitre-data-component--f5468e67-51c7-4756-9b4f-65707708e7fa"
},
{
  "modified": "2023-04-20T18:38:13.356Z",
  "name": "Network Traffic",
  "description": "Data transmitted across a network (ex: Web, DNS, Mail, File, etc.), that is either
summarized (ex: Netflow) and/or captured as raw data in an analyzable format (ex: PCAP)",
  "x_mitre_platforms": [
    "IaaS",
    "Linux",
    "Windows",
    "macOS",
    "Android",
    "iOS"
  ],
  "x_mitre_deprecated": false,
  "x_mitre_domains": [
    "enterprise-attack",
    "mobile-attack"
  ],
  "x_mitre_version": "1.1",
  "x_mitre_contributors": [
    "Center for Threat-Informed Defense (CTID)",
    "ExtraHop"
  ],
  "x_mitre_collection_layers": [
    "Cloud Control Plane",
    "Host",
    "Network"
  ],
  "type": "x-mitre-data-source",
  "id": "x-mitre-data-source--c000cd5c-bbb3-4606-af6f-6c6d9de0bbe3",
  "created": "2021-10-20T15:05:19.274Z",
  "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "revoked": false,
  "external_references": [
    {
      "source_name": "mitre-attack",
      "url": "https://attack.mitre.org/datasources/DS0029",
      "external_id": "DS0029"
    }
  ]
}

```

```

    ],
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "x_mitre_attack_spec_version": "3.1.0",
    "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--7b86d9f4-a599-4434-8b7a-170d50ec1662",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detector--9441073d-119b-4ec9-aa08-8bdb1703ed56",
    "target_ref": "x-mitre-data-source--c000cd5c-bbb3-4606-af6f-6c6d9de0bbe3"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--df076a56-f728-48b0-ac85-cbfa55d62dbe",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detector--67330653-ac02-46c8-b9c2-25b837a2ed6d",
    "target_ref": "x-mitre-data-source--c000cd5c-bbb3-4606-af6f-6c6d9de0bbe3"
  },
  {
    "modified": "2022-10-20T20:18:06.745Z",
    "name": "Network Connection Creation",
    "description": "Initial construction of a network connection, such as capturing socket information
with a source/destination IP and port(s) (ex: Windows EID 5156, Sysmon EID 3, or Zeek conn.log)",
    "x_mitre_data_source_ref": "x-mitre-data-source--c000cd5c-bbb3-4606-af6f-6c6d9de0bbe3",
    "x_mitre_deprecated": false,
    "x_mitre_version": "1.1",
    "type": "x-mitre-data-component",
    "id": "x-mitre-data-component--181a9f8c-c780-4f1f-91a8-edb770e904ba",
    "created": "2021-10-20T15:05:19.274Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "revoked": false,
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "x_mitre_attack_spec_version": "2.1.0",
    "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1",
    "x_mitre_domains": [
      "enterprise-attack"
    ]
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--a3d7b535-fe76-47b2-ac2b-a620e65fe04f",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detector--9441073d-119b-4ec9-aa08-8bdb1703ed56",
    "target_ref": "x-mitre-data-component--181a9f8c-c780-4f1f-91a8-edb770e904ba"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--4a7a74a4-9f4b-4e33-9e61-f052ca3ea48a",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",

```

```

    "source_ref": "x-oca-detector--67330653-ac02-46c8-b9c2-25b837a2ed6d",
    "target_ref": "x-mitre-data-component--181a9f8c-c780-4f1f-91a8-edb770e904ba"
  },
  {
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "id": "x-mitre-data-component--3772e279-27d6-477a-9fe3-c6beb363594c",
    "type": "x-mitre-data-component",
    "created": "2021-10-20T15:05:19.274Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "modified": "2022-04-25T14:00:00.188Z",
    "name": "Network Traffic Content",
    "description": "Logged network traffic data showing both protocol header and body values (ex:
PCAP)",
    "x_mitre_data_source_ref": "x-mitre-data-source--c000cd5c-bbb3-4606-af6f-6c6d9de0bbe3",
    "x_mitre_version": "1.0",
    "x_mitre_attack_spec_version": "2.1.0",
    "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1",
    "x_mitre_domains": [
      "enterprise-attack"
    ]
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--05461c91-0a8b-4eac-b134-21ba631c10d0",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detector--9441073d-119b-4ec9-aa08-8bdb1703ed56",
    "target_ref": "x-mitre-data-component--3772e279-27d6-477a-9fe3-c6beb363594c"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--4bac4ea6-4826-40da-8a5c-d89b7e2f54cc",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detector--67330653-ac02-46c8-b9c2-25b837a2ed6d",
    "target_ref": "x-mitre-data-component--3772e279-27d6-477a-9fe3-c6beb363594c"
  },
  {
    "object_marking_refs": [
      "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
    ],
    "id": "x-mitre-data-component--a7f22107-02e5-4982-9067-6625d4a1765a",
    "type": "x-mitre-data-component",
    "created": "2021-10-20T15:05:19.274Z",
    "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "modified": "2022-04-25T14:00:00.188Z",
    "name": "Network Traffic Flow",
    "description": "Summarized network packet data, with metrics, such as protocol headers and volume
(ex: Netflow or Zeek http.log)",
    "x_mitre_data_source_ref": "x-mitre-data-source--c000cd5c-bbb3-4606-af6f-6c6d9de0bbe3",
    "x_mitre_version": "1.0",
    "x_mitre_attack_spec_version": "2.1.0",
    "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
    "spec_version": "2.1",
    "x_mitre_domains": [
      "enterprise-attack"
    ]
  },
  {
    "type": "relationship",
    "spec_version": "2.1",

```



```

    "id": "relationship--4c0dc183-3372-4e99-be15-e7e46682bede",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detector--9441073d-119b-4ec9-aa08-8bdb1703ed56",
    "target_ref": "x-mitre-data-component--a7f22107-02e5-4982-9067-6625d4a1765a"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--d44f3f49-071a-455e-9da6-bd7fb521897f",
    "created": "2023-05-15T13:00:00.000Z",
    "modified": "2023-05-15T13:00:00.000Z",
    "relationship_type": "uses",
    "source_ref": "x-oca-detector--67330653-ac02-46c8-b9c2-25b837a2ed6d",
    "target_ref": "x-mitre-data-component--a7f22107-02e5-4982-9067-6625d4a1765a"
  },
  {
    "type": "grouping",
    "spec_version": "2.1",
    "id": "grouping--35058fc1-2126-41c3-b1fc-e2ebc39f50c2",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "name": "Reaper Lite Behavior Information",
    "context": "suspicious-activity",
    "object_refs": [
      "attack-pattern--2b742742-28c3-4e1b-bab7-8350d6300fa7",
      "attack-pattern--7b211ac6-c815-4189-93a9-ab415deca926",
      "attack-pattern--86850eff-2729-40c3-b85e-c4af26da4a2d",
      "attack-pattern--92d7da27-2d91-488e-a00c-059dc162766d",
      "attack-pattern--970a3432-3237-47ad-bcca-7d8cbb217736",
      "attack-pattern--9efb1ea7-c37b-4595-9640-b7680cd84279",
      "attack-pattern--df8b2a25-8bdf-4856-953c-a04372b1c161",
      "attack-pattern--f303a39a-6255-4b89-aecc-18c4d8ca7163",
      "campaign--f3bf3827-d9c5-414d-b0f0-610146ff5d85",
      "course-of-action--4E202C5A-C1DF-42D8-9AEF-809A8E172AE3",
      "course-of-action--94D890AC-3E24-4DEC-8ACB-C603FA4A7B20",
      "domain-name--8713b93b-186e-524d-9224-db3b8f9fb9ef",
      "extension-definition--2cf8c8c2-69f5-40f7-aa34-efcef2b912b1",
      "extension-definition--3b7505ce-2a18-496e-aa58-311dac6c1473",
      "extension-definition--5cccb5c-0be4-450c-8672-b66e98515754",
      "extension-definition--809C4D84-7A6E-4039-97B4-DA9FEA03FCF9",
      "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62",
      "extension-definition--BBC1D5C8-7DDC-4E89-BE9C-F33AD02D71DD",
      "extension-definition--c4690e13-107e-4796-8158-0dcf1ae7bc89",
      "extension-definition--dbbce349-3550-4cdd-8a7b-af58bc12de6c",
      "extension-definition--f9dbe89c-0030-4a9d-8b78-0dcd0a0de874",
      "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
      "ipv4-addr--3d4ee4f2-a895-5781-a0cc-b5ba466f053d",
      "ipv4-addr--429ddae0-a1ff-543d-99b4-f12a4a144c70",
      "ipv4-addr--57a33521-9761-54a9-81de-3c11e441d86b",
      "ipv4-addr--bba1d187-08fb-5000-aed1-ef055c1dfd24",
      "network-traffic--15a157a8-26e3-56e0-820b-0c2a8e553a2c",
      "network-traffic--3564fb7d-d65c-5e02-9f55-a8a960f5c9f5",
      "network-traffic--acffdf9a-bafd-5b74-a7d9-1a6d5a4e9c5a",
      "network-traffic--fcff628d-d69f-5d23-88b0-aeedcfb7da7c",
      "observed-data--08bd537f-69d9-44e0-90c9-13dc784c4eef",
      "observed-data--0e28ca31-6b10-4156-9678-4121b0c09a43",
      "observed-data--12d2cf2b-5f87-4efc-b8cd-c70d719e351a",
      "observed-data--1419d15e-65e8-4707-9311-25a8b571e7de",
      "observed-data--1a0ce5cc-0115-4108-b30b-8919efa2925c",
      "observed-data--3a418c06-bf5d-48b7-9e91-84bfff7e0846a",
      "observed-data--4a551d1b-8c08-46bb-b1b8-79b4caa638e2",
      "observed-data--7646a2bc-514c-4599-ae87-ddb8afa89a51",
      "observed-data--f8dc1a7e-33ec-4dc1-8076-739bdcc7358b",
      "process--3BCFB0A5-BAF5-411D-B9D0-8D4B4E09BA82",
    ]
  }

```

"process--862e625d-48bb-489e-8d4e-f7d8cd2fcaaa",
"process--862e625d-48bb-489e-8d4e-f7d8cd2fcbbb",
"process--862e625d-48bb-489e-8d4e-f7d8cd2fcccc",
"process--862e625d-48bb-489e-8d4e-f7d8cd2fcddd",
"relationship--0347363b-b476-4bfb-8203-a585feb21bb",
"relationship--05461c91-0a8b-4eac-b134-21ba631c10d0",
"relationship--0e0da782-5c16-485c-ab7d-1447d1851342",
"relationship--117e35be-a2ba-4b8f-b0ed-cbd22b14940e",
"relationship--12fc0865-9f15-4e79-858a-1ac25ba2ff1f",
"relationship--175473ba-1bf9-4168-a339-65454db013b2",
"relationship--18568ee3-837f-48d3-b807-a5f64ab3b9d8",
"relationship--19856de6-739c-4b31-b0cc-aaa6b0b751c8",
"relationship--22083b73-9546-41fd-a150-beb3e062766e",
"relationship--23ffdaa4-8be9-4eb3-b251-e82e605e2795",
"relationship--258248c6-6363-461a-9b8b-452d0518b2a9",
"relationship--282D26EF-0FA0-4975-81FC-69B5946F47D2",
"relationship--2d967554-6995-4bfe-bb6e-d1efeb990570",
"relationship--3089c0c1-2a6b-4ab0-b274-25d375362892",
"relationship--33da2e36-637b-47a7-ae95-d8ae192fb3d2",
"relationship--3437bf91-0115-4c05-bfda-d9abf9954f8e",
"relationship--37777af9-db8b-46ca-b1d5-3abc5724d8f2",
"relationship--399ee227-e888-4dcd-bbc8-b79cf5cfff259",
"relationship--3ad280cd-42f7-49b6-88ff-d2ee35a175b6",
"relationship--3e3295b7-c616-4ee1-8210-002093589884",
"relationship--417693ec-1543-48a4-be84-a238bf8dfb8d",
"relationship--45dcf923-f8b1-45bf-8788-055a7033d6ee",
"relationship--4655b19d-c949-45be-8316-e8861c634cab",
"relationship--4a7a74a4-9f4b-4e33-9e61-f052ca3ea48a",
"relationship--4bac4ea6-4826-40da-8a5c-d89b7e2f54cc",
"relationship--4c0dc183-3372-4e99-be15-e7e46682bede",
"relationship--4ca132b3-f40d-4e38-9d32-a5dc8e91efb0",
"relationship--535d743b-0b78-4891-a515-8ec92e65d42b",
"relationship--603e1426-49d7-42ea-a73a-263a963e6db0",
"relationship--6317A9AC-6763-4551-B004-CA2AA45B3510",
"relationship--63b586d2-9d36-48f2-a8f3-36350abe66b6",
"relationship--64726807-5082-43C3-B975-1484B60B963B",
"relationship--64726807-5082-43C3-B975-1484B60B963C",
"relationship--64726807-5082-43C3-B975-1484B60B963D",
"relationship--6befc841-7b3b-4680-b7d6-7c743327d150",
"relationship--6d65615b-b7f6-4169-9226-6b70509f8f38",
"relationship--72fc61e3-67d7-497e-900b-faf26173bd71",
"relationship--731021e2-e7a8-4863-ba41-65c893d7c564",
"relationship--7a9afa0a-0c25-4dec-8f3d-db92e213643c",
"relationship--7b86d9f4-a599-4434-8b7a-170d50ec1662",
"relationship--7f91c908-73ea-40e2-91df-ec9d72e37005",
"relationship--81da5956-d9ea-4a09-9e3d-ab09be3cc3eb",
"relationship--84606E92-B52C-4BCA-908C-7D01C498F90C",
"relationship--87c4aca0-6b97-4fe9-ab99-ab5ba7f3db95",
"relationship--88ae0ce8-96d8-4886-a5aa-bbc0a32c3a3f",
"relationship--8a7f7654-5346-4897-b102-df81246af61e",
"relationship--8c9b87b9-4b26-4235-b992-6a6b87a1a91a",
"relationship--8DE4A689-FDA3-45B9-8FE2-4A519884CEA7",
"relationship--8e796cf6-5401-4a23-9354-59b58155bd5e",
"relationship--913ea5e0-0ec0-4885-b241-6f53526a98e5",
"relationship--92C59855-392E-490A-964C-F9E3B3D202BF",
"relationship--94aaccf3-e8c4-41c0-985a-473f46312bb7",
"relationship--958b9180-7270-493f-942e-33d0798572f7",
"relationship--98CC25CE-EBDA-4BC2-9D0C-57173B321198",
"relationship--a3d7b535-fe76-47b2-ac2b-a620e65fe04f",
"relationship--a7e2ab2a-cdf5-45d0-bbe2-e6ecd9b95ca99",
"relationship--ac03ff3c-a51c-4637-bbd9-0f59900a1872",
"relationship--ae96d1d8-41ab-4bf1-aad9-6bf704064404",
"relationship--baf7f0f2-1aa8-45cb-b306-cbca8dd863d1",
"relationship--C4CBC936-2936-450F-9E79-CE8E2F795A3D",
"relationship--c4e4b439-2662-47e1-b961-2b6a6fae5241",
"relationship--c7eac063-5707-406b-ad43-2a83e5344d61",
"relationship--c901c890-c96c-46ca-bf5e-6eca1352ccbc",
"relationship--c9a2a2b3-67f3-4b8a-ad40-17c8098f7205",

```

"relationship--ca57a603-b4d6-475e-be8d-7618fbd58fbb",
"relationship--cab1e466-64c3-4752-bbce-134bae74b43f",
"relationship--cc07695b-ddbe-4c76-b41a-5eae1e78bb2a",
"relationship--d3f134d4-bf65-477c-927e-1b0e87630e38",
"relationship--d44f3f49-071a-455e-9da6-bd7fb521897f",
"relationship--D4B7D30C-1326-4C3E-943D-883498DDCC8F",
"relationship--d4ce259f-f595-4d1d-913c-e17454396dba",
"relationship--d811f064-2df1-46d3-954c-4011e74425da",
"relationship--d8935337-1917-446c-9c63-ac0a36438712",
"relationship--d99350ec-bc5b-4d92-8990-ae6b08ffce7a",
"relationship--d993c3af-9443-44db-9478-b3a9d632d94d",
"relationship--df076a56-f728-48b0-ac85-cbfa55d62dbe",
"relationship--e38c15bc-224e-4d81-a899-dc3b6f8cee92",
"relationship--e55308a4-db4e-4a00-a136-a0ccd26178ff",
"relationship--e60900fc-e47e-44f3-aac2-4a5ca9be7c78",
"relationship--e82c60ee-78e1-4056-a2e0-2ed73571605d",
"relationship--eb6fd1a1-00bb-44c0-bba5-6c3a335c6cb6",
"relationship--f2c14bce-581c-4b1d-9ea6-941c2e4a4880",
"relationship--f2fec843-0fef-44e9-a799-930495a55479",
"relationship--f5e74b96-093f-4942-a8c3-a05ee36023ec",
"relationship--fd55f673-53b0-4ae1-915b-6f30b20c950b",
"windows-registry-key--c5a4244e-22d5-5797-8f78-c5fc3d1c0bde",
"x-mitre-data-component--181a9f8c-c780-4f1f-91a8-edb770e904ba",
"x-mitre-data-component--3772e279-27d6-477a-9fe3-c6beb363594c",
"x-mitre-data-component--3d20385b-24ef-40e1-9f56-f39750379077",
"x-mitre-data-component--a7f22107-02e5-4982-9067-6625d4a1765a",
"x-mitre-data-component--da85d358-741a-410d-9433-20d6269a6170",
"x-mitre-data-component--f5468e67-51c7-4756-9b4f-65707708e7fa",
"x-mitre-data-source--0f42a24c-e035-4f93-a91c-5f7076bd8da0",
"x-mitre-data-source--ba27545a-9c32-47ea-ba6a-cce50f1b326e",
"x-mitre-data-source--c000cd5c-bbb3-4606-af6f-6c6d9de0bbe3",
"x-mitre-data-source--e8b8ede7-337b-4c0c-8c32-5c7872c1ee22",
"x-oca-behavior--DE81EF18-55E6-4754-A761-6B929BF22395",
"x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa",
"x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab",
"x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bb",
"x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bc",
"x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890cc",
"x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890dd",
"x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ee",
"x-oca-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ff",
"x-oca-detection--275bf485-736d-4aa5-b172-e34d28faa58c",
"x-oca-detection--40a941cc-42df-4b2e-b607-6d74168084b9",
"x-oca-detection--458c02c9-3635-42e4-8873-6785e00517e7",
"x-oca-detection--58834c29-4ceb-42a1-a218-336103021000",
"x-oca-detection--58834c29-4ceb-42a1-a218-336103021111",
"x-oca-detection--58834c29-4ceb-42a1-a218-336103021222",
"x-oca-detection--5899C5CC-CE20-44EE-806E-9F64EBA0B29F",
"x-oca-detection--66aa9c25-8b56-4121-8630-dbe457393b27",
"x-oca-detection--f27cb358-d747-47ba-a6c4-e5b8debab157",
"x-oca-detection-group--58834c29-4ceb-42a1-a218-321103021999",
"x-oca-detector--67330653-ac02-46c8-b9c2-25b837a2ed6d",
"x-oca-detector--9441073d-119b-4ec9-aa08-8bdb1703ed56",
"x-oca-detector--f9ccdd3d-2217-45fd-8e65-055da8e66c3e",
"x-oca-playbook--32F52089-9943-4231-BBA3-5C02BA654755",
"x-oca-playbook--720E5E68-3959-4EE0-99DE-87A4EAA39F44",
"x-oca-playbook--9880DF48-09A7-4E99-8070-0DB8F4C946D0",
"x-oca-playbook--AE16A784-BAC9-4334-A09F-7CB63053A6D7"
]
}
]
}

```