JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

February 2022

REFERENCE IMPLEMENTATION REVISION 0 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

APL Research Team
- Suzanne Hassell
- Kurt Karolenko
- Nam Le
- Keat Ly
- Ali Shahegh
- Tim Zhan

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

FIGURES

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, 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 to allow both human analysts and automation to use the shared information to detect an adversary based on that adversary's observed behavior within the victim network.

2.1 Motivation for the Research

Previous APL work under the Integrated Adaptive Cyber Defense (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 while they are still viable for network defenders, 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

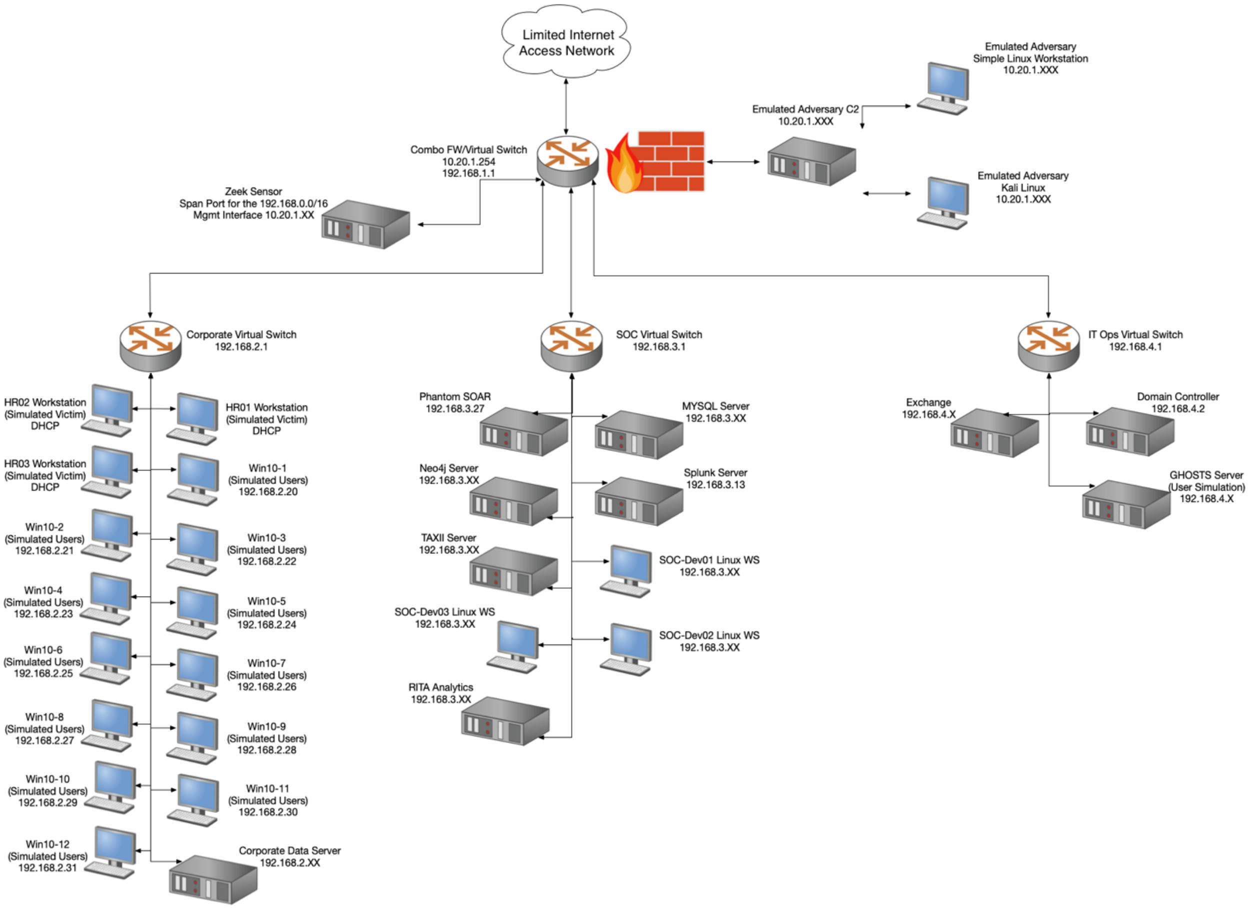

Limited Internet Access Network
Emulated Adversary Simple Linux Workstation 10.20.1.XXX
Emulated Adversary C2 10.20.1.XXX
Combo FW/Virtual Switch 10.20.1.254 192.168.1.1
Emulated Adversary Kali Linux 10.20.1.XXX
Zeek Sensor Span Port for the 192.168.0.0/16 Mgmt Interface 10.20.1.XX
Corporate Virtual Switch 192.168.2.1
SOC Virtual Switch 192.168.3.1
IT Ops Virtual Switch 192.168.4.1
HR02 Workstation (Simulated Victim) DHCP
HR01 Workstation (Simulated Victim) DHCP
HR03 Workstation (Simulated Victim) DHCP
Win10-1 (Simulated Users) 192.168.2.20
Win10-2 (Simulated Users) 192.168.2.21
Win10-3 (Simulated Users) 192.168.2.22
Win10-4 (Simulated Users) 192.168.2.23
Win10-5 (Simulated Users) 192.168.2.24
Win10-6 (Simulated Users) 192.168.2.25
Win10-7 (Simulated Users) 192.168.2.26
Win10-8 (Simulated Users) 192.168.2.27
Win10-9 (Simulated Users) 192.168.2.28
Win10-10 (Simulated Users) 192.168.2.29
Win10-11 (Simulated Users) 192.168.2.30
Win10-12 (Simulated Users) 192.168.2.31
Corporate Data Server 192.168.2.XX
Phantom SOAR 192.168.3.27
MYSQL Server 192.168.3.XX
Neo4j Server 192.168.3.XX
Splunk Server 192.168.3.13
TAXII Server 192.168.3.XX
SOC-Dev01 Linux WS 192.168.3.XX
SOC-Dev03 Linux WS 192.168.3.XX
SOC-Dev02 Linux WS 192.168.3.XX
RITA Analytics 192.168.3.XX
Exchange 192.168.4.X
Domain Controller 192.168.4.2
GHOSTS Server (User Simulation) 192.168.4.X

Figure 1: APL Reference Implementation Research Environment

The research environment was 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 Strike[3]
- An emulated corporate enclave containing:
  - Windows workstations automated with the Carnegie Mellon University (CMU) GHOSTS[4] agent to create benign user activity within the network
  - Splunk[5] Security Information and Event Management (SIEM) forwarders for SYSMON[6] and Windows event logs

[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

  - A file server to contain emulated sensitive information that would be the adversary's target for data exfiltration
- 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 Zeek[7] network sensor to analyze traffic
  - A Trusted Automated eXchange of Indicator Information (TAXII) server for the transmission of any shared STIX objects
  - A MySQL[8] 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

This 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.

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
- 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 which was based on the "APT 37/Reaper"[11] campaign.

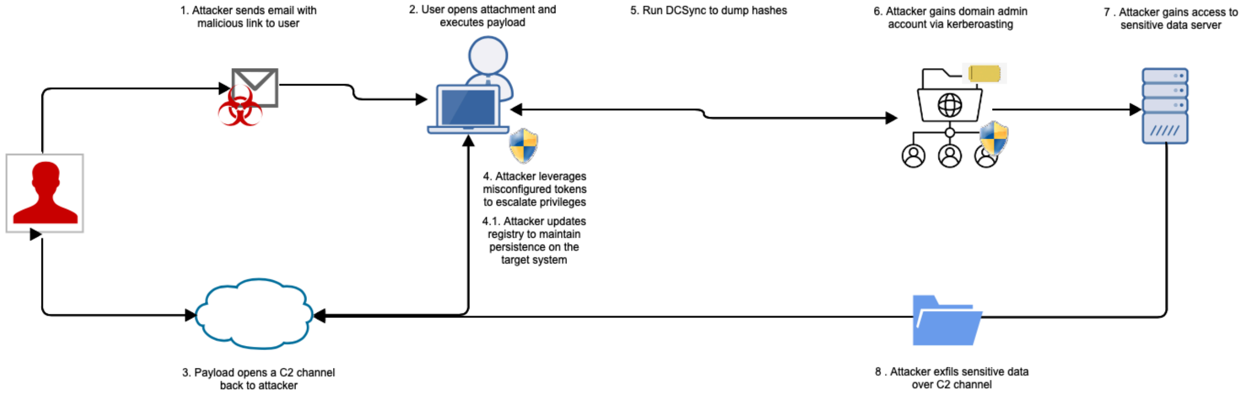

1. Attacker sends email with malicious link to user
2. User opens attachment and executes payload
5. Run DCSync to dump hashes
6. Attacker gains domain admin account via kerberoasting
7 . Attacker gains access to sensitive data server
4. Attacker leverages misconfigured tokens to escalate privileges
4.1. Attacker updates registry to maintain persistence on the target system
3. Payload opens a C2 channel back to attacker
8 . Attacker exfils sensitive data over C2 channel

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.
    - 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.

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

- 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 Data Construct

Previous APL research determined how to represent a single behavior within the STIX standard. However, as adversary actions are often better characterized as a sequence of events, APL determined it was necessary to combine multiple behaviors into a set.

Figure 3 provides a visual representation of the logical construct for the behavior set. The overall set is represented as a STIX “grouping” with each behavior STIX Domain Object (SDO) linked to a set of STIX Cyber Observables (SCOs) that are interrelated. This interrelation reveals key contextual insights to understanding the logic behind the construction shared detection analytics. APL includes this level of detail as the envisioned use of these objects spans multiple communities to include both intelligence analyst and network defender communities.

[12] https://attack.mitre.org/techniques/T1003/006/

[13] https://attack.mitre.org/techniques/T1558/003/

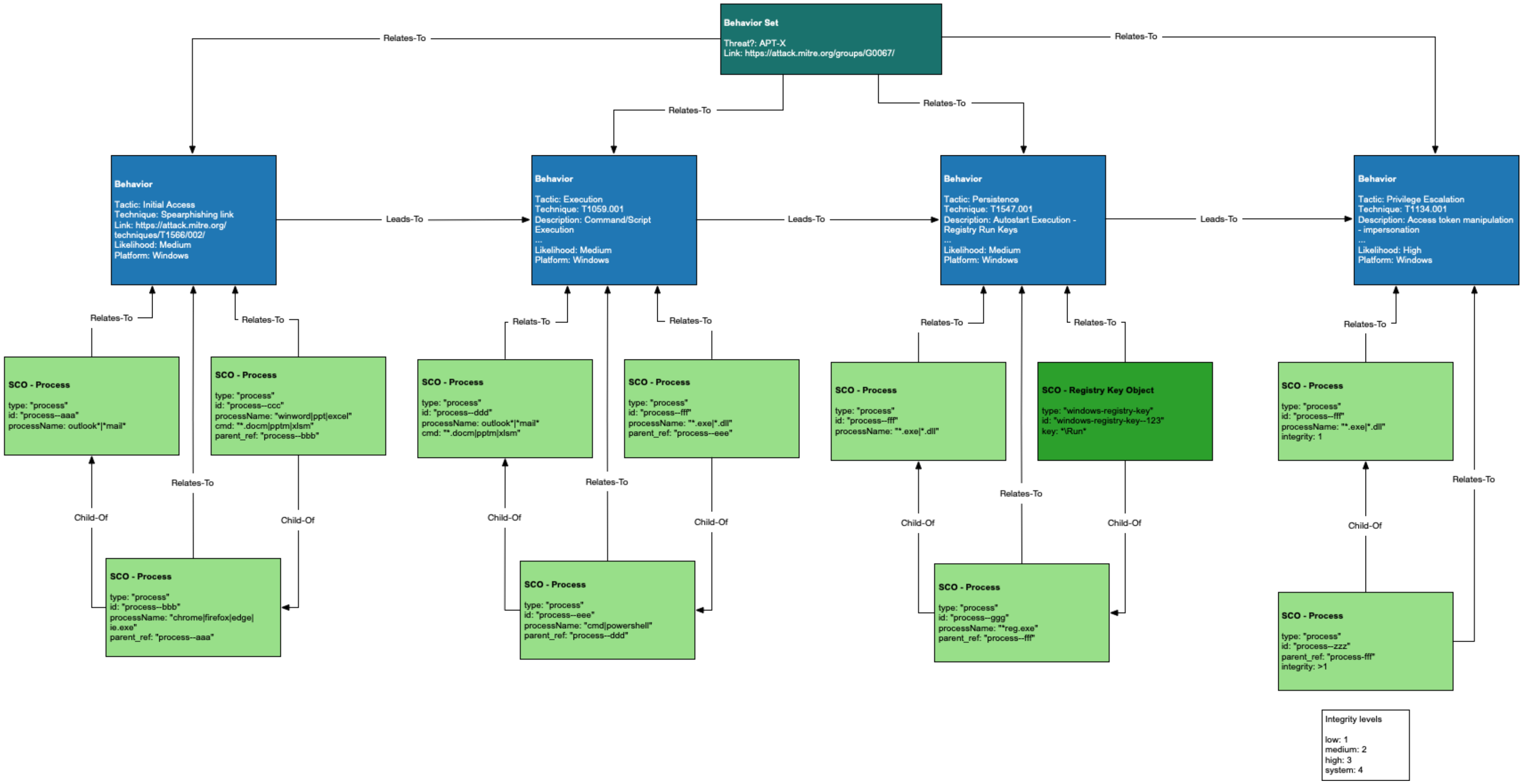


Figure 3: Logical Construct for Behavior Set

2.3.3 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 4 provides a visualization of the bundle via the STIX visualizer from the OASIS standards group [14].

[14] https://oasis-open.github.io/cti-stix-visualization/

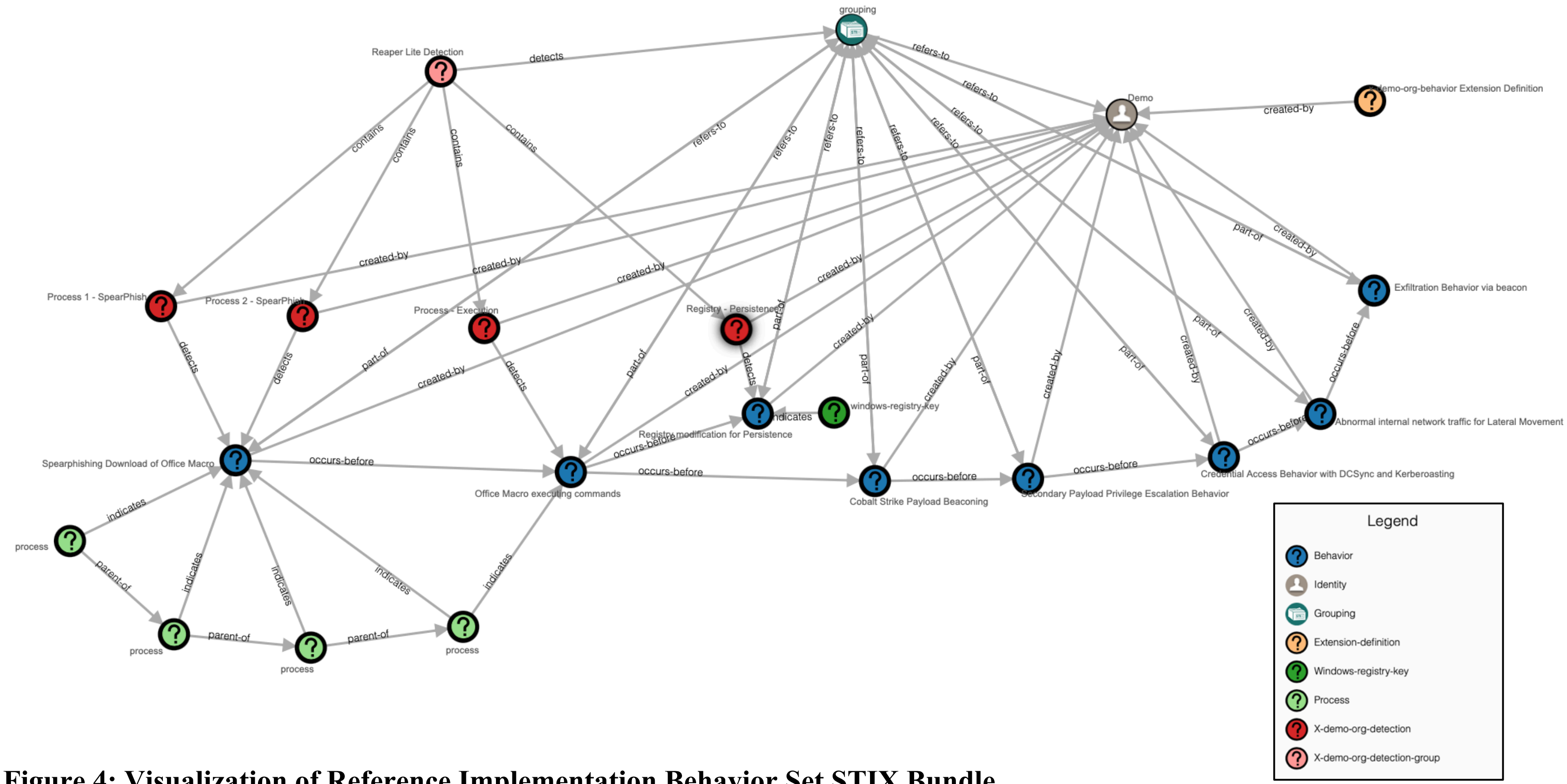

grouping
Reaper Lite Detection
detects
refers-to
Demo
x-demo-org-behavior Extension Definition
created-by
contains
part-of
Process 1 - SpearPhish
Process 2 - SpearPhish
Process - Execution
Registry - Persistence
Exfiltration Behavior via beacon
detects
windows-registry-key
indicates
Registry modification for Persistence
occurs-before
Abnormal internal network traffic for Lateral Movement
Spearphishing Download of Office Macro
Office Macro executing commands
Cobalt Strike Payload Beaconing
Secondary Payload Privilege Escalation Behavior
Credential Access Behavior with DCSync and Kerberoasting
process
parent-of
indicates
Legend
Behavior
Identity
Grouping
Extension-definition
Windows-registry-key
Process
X-demo-org-detection
X-demo-org-detection-group

Figure 4: Visualization of Reference Implementation Behavior Set STIX Bundle

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
    - Color: Blue
    - 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 ID
        - Extensions
        - First seen date
        - STIX specification version
        - Created date
        - Created by
        - Name
        - Technique
        - Modification date
        - Tactic
        - Periodicity
        - Platforms affected by the behavior
- Detection SDO
    - Color: Red
    - 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 ID
        - STIX specification version
        - Created date
        - Created by
        - Name
        - Modification date
        - Analytic for detection
        - Data Sources to support analytic

- Detection Group SDO
  - Color: Pink
  - Description: The Detection Group SDO is intended to provide the guidance on how to correlate the multiple detections within a grouping of behavior SDOs. APL is still refining the logic and required metadata for strong correlations but the version provided in the reference implementation conveys the current status of the object as of late 2021.
  - Fields within the object:
    - STIX ID
    - STIX specification version
    - Created date
    - Name
    - Modification date
    - Description field
    - Correlation confidence levels based on the number of detections that provide data
    - Detection objects to use for correlation
- Process SCO
  - Color: Light green
  - 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. 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 is key to developing the detection object for the behavior of new system process creation.
  - Fields within the object:
    - STIX ID
    - STIX specification version
    - Created date
    - Name
    - Modification date
    - Image references
    - Child object references
    - Flag to determine if the SCO is hidden
    - Process ID (pid)
    - Parent object references to determine if other SCOs are observed prior to this process
    - Granular markings
    - Current Working Directory (CWD)
    - Extensions applied to the SCO
      - Creator-Process-Name
      - New-Process-Name

        - Opened connection references
        - Creator user references
        - Flag to determine whether the referenced information in the process is "defanged"
        - Command line information for the process when available
- Registry SCO
    - Color: Dark green
    - 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 specify 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 ID
        - STIX specification version
        - Created date
        - Name
        - Referenced extensions
        - Registry key referenced
        - Registry key values
        - Action performed on the key
        - ID of process that acted on the key
        - Name of process that acted on the key
- Extension Definition SDO
    - Color: Peach
    - Description: When custom extensions are added to an SDO, the Extension Definition SDO provides the schema used to represent the additional data.
    - Fields within the object:
        - STIX ID
        - STIX specification version
        - Created by reference
        - Created date
        - Name
        - Modification date
        - Extension type definition
        - Link to extension schema
        - Version

2.3.4 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 5.

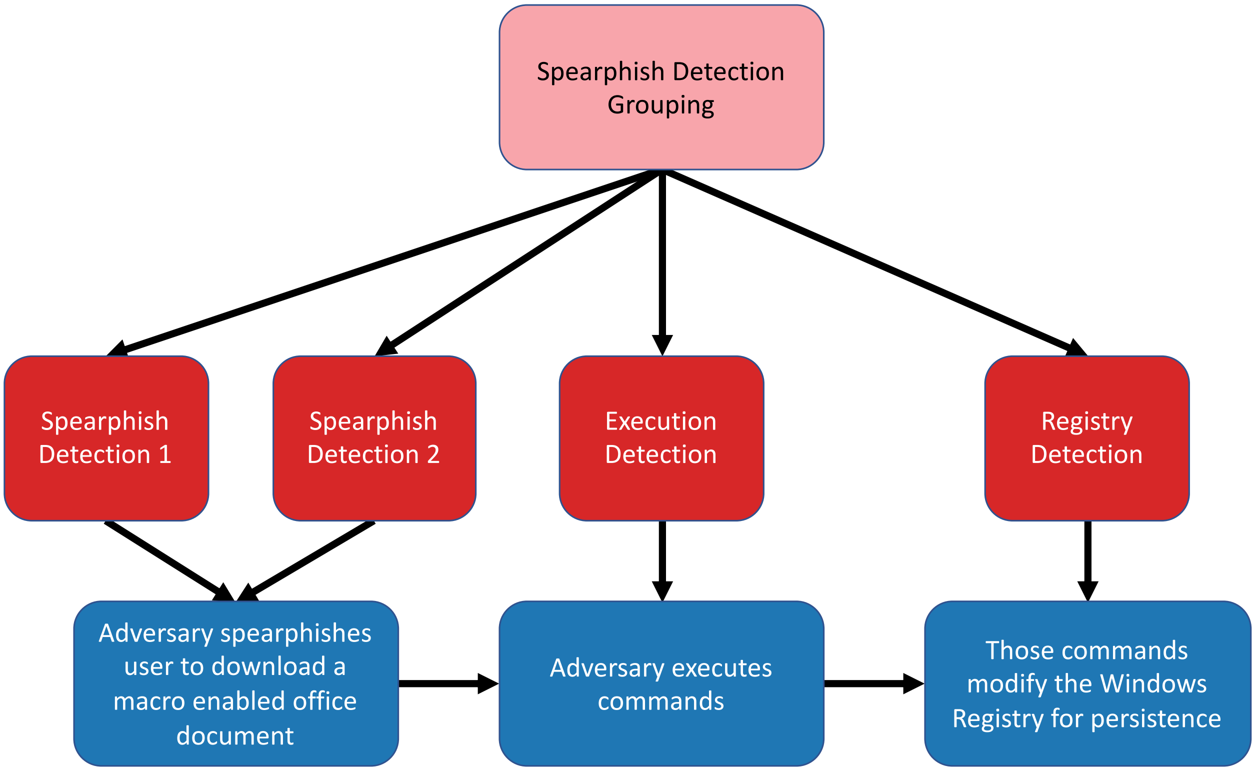

Spearphish Detection Grouping
Spearphish Detection 1
Spearphish Detection 2
Execution Detection
Registry Detection
Adversary spearphishes user to download a macro enabled office document
Adversary executes commands
Those commands modify the Windows Registry for persistence

Figure 5: 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, etc.) spawns a process to open a web browser (e.g., Chrome, Firefox, Edge, etc.) 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 Sigma[15] 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
```

[15] https://github.com/SigmaHQ/sigma

```
    - thunderbird
    - mail
    New_Process_Name|contains:
    - 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
    - xlsm
    - 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:

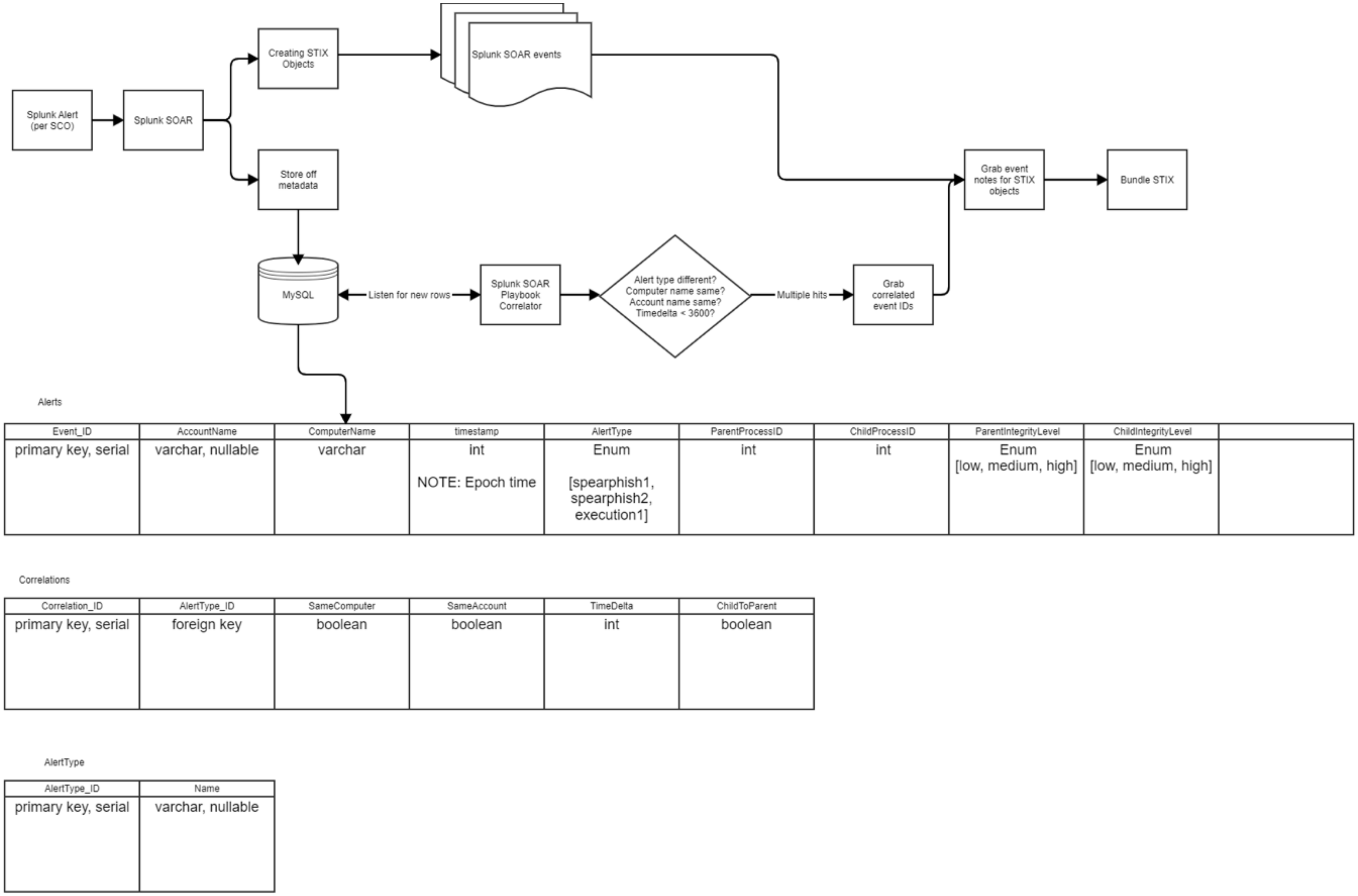
```
---
date: 2021/06/07
detection:
  selection:
    EventCode: '4657'
    Object_Name|contains:
    - Run
    - Shell Folders
  condition: selection
level: high
author: demo
description: Detects new registry run key created event.
id: registry persistence
falsepositives:
- High
title: Registry Run Keys
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.

It is important to note that the detection group in the reference implementation is not complete and does not include all the necessary fields for this correlation. These correlating factors are the subject of ongoing APL research and will be included in future revisions to the reference implementation. The following sample provides the current placeholder detection group structure:

```
{
    "type": "x-demo-org-detection-group",
    "spec_version": "2.1",
    "id": "x-demo-org-detection-group--58834c29-4ceb-42a1-a218-321103021999",
    "created": "2021-08-13T20:30:34Z",
    "modified": "2021-08-13T20:30:34Z",
    "name": "Reaper Lite Detection",
    "description": "This detection group detects spearphishing, execution, and
persistence",
    "confidence": {
      "low": 1,
      "medium": 2,
      "high": 3
    },
    "detection_ids": [
      "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021000",
      "x-demo-org-detection--458c02c9-3635-42e4-8873-6785e00517e7",
      "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021111",
      "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021222"
    ]
  }
```

The JSON format of the placeholder detection grouping provides a reference to all the detections to run and a confidence scoring rubric based on the number of detections required to return shared information in order to evaluate whether a behavior has been successfully detected. This format is not sufficient. Ongoing APL research aims to augment this construct by representing a sequential process for running and analyzing the multiple detections. An early concept of such a process is provided in Figure 6 to better illustrate the intent for these objects which will be refined a future revision to the reference implementation.


Splunk Alert (per SCO)
Splunk SOAR
Creating STIX Objects
Splunk SOAR events
Store off metadata
MySQL
Listen for new rows
Splunk SOAR Playbook Correlator
Alert type different? Computer name same? Account name same? Timedelta < 3600?
Multiple hits
Grab correlated event IDs
Grab event notes for STIX objects
Bundle STIX

Alerts

Event_ID	AccountName	ComputerName	timestamp	AlertType	ParentProcessID	ChildProcessID	ParentIntegrityLevel	ChildIntegrityLevel	
primary key, serial	varchar, nullable	varchar	int NOTE: Epoch time	Enum [spearphish1, spearphish2, execution1]	int	int	Enum [low, medium, high]	Enum [low, medium, high]	

Correlations

Correlation_ID	AlertType_ID	SameComputer	SameAccount	TimeDelta	ChildToParent
primary key, serial	foreign key	boolean	boolean	int	boolean

AlertType

AlertType_ID	Name
primary key, serial	varchar, nullable

Figure 6: Conceptual Process for Detection Correlation Logic

2.3.5 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
    - xlsm
    - 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 GitHub[16] 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
- Splunk

[16] See section 2.3.4 for link to Sigma GitHub site

- 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. APL's plan for future revisions to the reference implementation will follow a similar approach to share the correlation logic as a workflow in a standardized format so that recipients can execute correlations via the technologies they currently have in place.

3. NEXT STEPS

APL plans to create a future revision to the reference implementation that expands the behavior object work by developing a higher fidelity detection grouping, most likely through the inclusion of a correlation workflow. Additionally, APL plans to incorporate higher fidelity detections, testing of analytics against different emulated threats, and begin research on response objects to represent defensive courses of action. By sharing this reference implementation with the greater security community, APL hopes to receive community feedback that can shape additional features and capabilities in the reference implementation.

4. 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).

5. APPENDIX A: ACRONYMNS

APL	Johns Hopkins University Applied Physics Laboratory
C2	Command and Control
CISA	Cybersecurity and Infrastructure Security Agency
CMU	Carnegie Mellon University
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

6. APPENDIX B: COMPLETE BEHAVIOR SET STIX BUNDLE

```
{
  "type": "bundle",
  "id": "bundle--9edb6354-d73f-4ba2-b774-3d76c6474b14",
  "objects": [
    {
      "type": "behavior",
      "spec_version": "2.1",
      "id": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2021-07-14T09:16:08.989000Z",
      "modified": "2021-07-14T09:16:08.989000Z",
      "name": "Spearphishing Download of Office Macro",
      "tactic": "INITIAL ACCESS",
      "technique": "T1566.002 Spearphishing Link",
      "first_seen": "2021-04-21T17:20:45",
      "platforms": [
        {
          "operating_system": "Microsoft Windows",
          "version": "10"
        }
      ],
      "extensions": {
        "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
          "extension_type": "new-sdo"
        }
      }
    },
    {
      "type": "behavior",
      "spec_version": "2.1",
      "id": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2021-07-14T09:16:08.989000Z",
      "modified": "2021-07-14T09:16:08.989000Z",
      "name": "Office Macro executing commands",
      "tactic": "EXECUTION",
      "technique": "T1059.001 Command/Script execution - VBA",
      "first_seen": "2021-04-21T17:20:45",
      "platforms": [
        {
          "operating_system": "Microsoft Windows",
          "version": "10"
        }
      ],
      "extensions": {
        "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
          "extension_type": "new-sdo"
        }
      }
    },
    {
      "type": "behavior",
      "spec_version": "2.1",
      "id": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bb",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2021-07-14T09:16:08.989000Z",
      "modified": "2021-07-14T09:16:08.989000Z",
      "name": "Cobalt Strike Payload Beaconing",
      "tactic": "Command and Control",
      "technique": "T1071.001 - Application Layer Protocol - Web Protocols",
      "first_seen": "2021-04-21T17:20:45",
      "platforms": [
        {
          "operating_system": "Microsoft Windows",
          "version": "10"
        }
      ],
      "extensions": {
        "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
          "extension_type": "new-sdo"
        }
      }
    },
    {
      "type": "behavior",
      "spec_version": "2.1",
      "id": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890cc",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2021-07-14T09:16:08.989000Z",
      "modified": "2021-07-14T09:16:08.989000Z",
      "name": "Registry modification for Persistence",
      "tactic": "Persistence",
      "technique": "T1547.001 - Autostart Execution - Registry Run Keys / Startup
Folder",
      "first_seen": "2021-04-21T17:20:45",
      "platforms": [
        {
          "operating_system": "Microsoft Windows",
          "version": "10"
        }
      ],
      "extensions": {
        "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
          "extension_type": "new-sdo"
        }
      }
    },
    {
      "type": "behavior",
      "spec_version": "2.1",
      "id": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890dd",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2021-07-14T09:16:08.989000Z",
      "modified": "2021-07-14T09:16:08.989000Z",
      "name": "Secondary Payload Privilege Escalation Behavior",
      "tactic": "Privilege Escalation",
      "technique": "T1134.001 - Access token manipulation - Token impersonation",
      "first_seen": "2021-04-21T17:20:45",
      "platforms": [
        {
          "operating_system": "Microsoft Windows",
          "version": "10"
        }
      ],
      "extensions": {
        "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
          "extension_type": "new-sdo"
        }
      }
    },
    {
      "type": "behavior",
      "spec_version": "2.1",
      "id": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ee",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2021-07-14T09:16:08.989000Z",
      "modified": "2021-07-14T09:16:08.989000Z",
      "name": "Credential Access Behavior with DCSync and Kerberoasting",
      "tactic": "Credential Access",
      "technique": "T1003.006 - OS Credential dumping - DCSync",
      "first_seen": "2021-04-21T17:20:45",
      "platforms": [
        {
          "operating_system": "Microsoft Windows",
          "version": "10"
        }
      ],
      "extensions": {
        "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
          "extension_type": "new-sdo"
        }
      }
    },
    {
      "type": "behavior",
      "spec_version": "2.1",
      "id": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ff",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2021-07-14T09:16:08.989000Z",
      "modified": "2021-07-14T09:16:08.989000Z",
      "name": "Abnormal internal network traffic for Lateral Movement",
      "tactic": "Lateral Movement",
      "technique": "T1550.003 - Pass the Ticket",
      "first_seen": "2021-04-21T17:20:45",
      "platforms": [
        {
          "operating_system": "Microsoft Windows",
          "version": "10"
        }
      ],
      "extensions": {
        "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
          "extension_type": "new-sdo"
        }
      }
    },
{
  "type": "behavior",
  "spec_version": "2.1",
  "id": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890gg",
  "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
  "created": "2021-07-14T09:16:08.989000Z",
  "modified": "2021-07-14T09:16:08.989000Z",
  "name": "Exfiltration Behavior via beacon",
  "tactic": "Exfiltration",
  "technique": "T1041 - Exfiltration over C2 Channel",
  "first_seen": "2021-04-21T17:20:45",
  "platforms": [
    {
      "operating_system": "Microsoft Windows",
      "version": "10"
    }
  ],
  "extensions": {
    "extension-definition--9c59fd79-4215-4ba2-920d-3e4f320e1e62": {
      "extension_type": "new-sdo"
    }
  }
},
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--b085a68a-bf48-4316-9667-37af78cba894",
  "created": "2021-10-01T20:03:34.105161Z",
  "modified": "2021-10-01T20:03:34.105161Z",
  "name": "Demo"
},
{
  "type": "grouping",
  "spec_version": "2.1",
  "id": "grouping--cb508d31-469c-41d0-ab3d-fb78ed60b61d",
  "created": "2021-10-13T14:23:19.018783Z",
  "modified": "2021-10-13T14:23:19.018783Z",
  "context": "Behavior Set",
  "object_refs": [
    "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-ed093e8279fe",
    "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab",
    "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa",
      "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bb",
      "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890cc",
      "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890dd",
      "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ee",
      "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ff",
      "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890gg",
      "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890hh",
      "identity--b085a68a-bf48-4316-9667-37af78cba894"
    ]
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
    "created": "2016-11-23T08:17:27.000Z",
    "modified": "2016-11-23T08:17:27.000Z",
    "relationship_type": "part-of",
    "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-ed093e8279fe",
    "target_ref": "grouping--cb508d31-469c-41d0-ab3d-fb78ed60b61d"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
    "created": "2016-11-23T08:17:27.000Z",
    "modified": "2016-11-23T08:17:27.000Z",
    "relationship_type": "part-of",
    "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab",
    "target_ref": "grouping--cb508d31-469c-41d0-ab3d-fb78ed60b61d"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
    "created": "2016-11-23T08:17:27.000Z",
    "modified": "2016-11-23T08:17:27.000Z",
    "relationship_type": "part-of",
    "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa",
    "target_ref": "grouping--cb508d31-469c-41d0-ab3d-fb78ed60b61d"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
    "created": "2016-11-23T08:17:27.000Z",
    "modified": "2016-11-23T08:17:27.000Z",
    "relationship_type": "part-of",
    "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bb",
    "target_ref": "grouping--cb508d31-469c-41d0-ab3d-fb78ed60b61d"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
    "created": "2016-11-23T08:17:27.000Z",
    "modified": "2016-11-23T08:17:27.000Z",
    "relationship_type": "part-of",
    "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890cc",
    "target_ref": "grouping--cb508d31-469c-41d0-ab3d-fb78ed60b61d"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a0ab",
    "created": "2016-11-23T08:17:27.000Z",
    "modified": "2016-11-23T08:17:27.000Z",
    "relationship_type": "part-of",
    "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890dd",
    "target_ref": "grouping--cb508d31-469c-41d0-ab3d-fb78ed60b61d"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
    "created": "2016-11-23T08:17:27.000Z",
    "modified": "2016-11-23T08:17:27.000Z",
    "relationship_type": "part-of",
    "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ee",
    "target_ref": "grouping--cb508d31-469c-41d0-ab3d-fb78ed60b61d"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "part-of",
      "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ff",
      "target_ref": "grouping--cb508d31-469c-41d0-ab3d-fb78ed60b61d"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "part-of",
      "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890gg",
      "target_ref": "grouping--cb508d31-469c-41d0-ab3d-fb78ed60b61d"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "part-of",
      "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890hh",
      "target_ref": "grouping--cb508d31-469c-41d0-ab3d-fb78ed60b61d"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "occurs-before",
      "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "occurs-before",
      "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bb"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "occurs-before",
      "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890cc"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "occurs-before",
      "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890bb",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890dd"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "occurs-before",
      "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890dd",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ee"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "occurs-before",
      "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ee",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ff"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959a4c",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "occurs-before",
      "source_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ff",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890gg"
    },
    {
      "type": "extension-definition",
      "spec_version": "2.1",
      "id": "extension-definition--8185be67-a588-4791-b62a-968cd8c4bcd4",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2021-10-05T17:22:31.25295Z",
      "modified": "2021-10-05T17:22:31.25295Z",
      "name": "x-demo-org-behavior Extension Definition",
      "schema": "tbd",
      "version": "1.0.0",
      "extension_types": [
        "new-sdo"
      ]
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959111",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "indicates",
      "source_ref": "windows-registry-key--c5a4244e-22d5-5797-8f78-c5fc3d1c0bde",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890cc"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959222",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "indicates",
      "source_ref": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcaaa",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959333",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "indicates",
      "source_ref": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcbbb",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959444",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "indicates",
      "source_ref": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcccc",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959555",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "indicates",
      "source_ref": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcddd",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959555",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "indicates",
      "source_ref": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcddd",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890aa"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959666",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "detects",
      "source_ref": "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021000",
      "target_ref": "x-demo-org-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": {
        "x-winregkey-ext": {
          "action": "modify",
          "new_value": "true",
          "process_id": "0x2498",
          "process_name": "C:\\Windows\\regedit.exe"
        }
      }
    },
    {
      "id": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcaaa",
      "type": "process",
      "spec_version": 2.1,
      "object_marking_refs": [],
      "granular_markings": [],
      "is_defanged": false,
      "is_hidden": false,
      "pid": 0,
      "created": "2021-06-03T18:42:29-04:00",
      "cwd": "",
      "command_line": "",
      "opened_connection_refs": [],
      "creator_user_ref": "",
      "image_ref": "",
      "parent_ref": "",
      "child_refs": [],
      "extensions": {
        "extension-definition--f9dbe89c-0030-4a9d-8b78-0dcd0a0de874": {
          "extension_type": "toplevel-property-extension",
          "action": "created",
          "new-process-name": [
            "*outlook*",
            "thunderbird",
            "*mail*"
          ],
          "win-event-code": "4688"
        }
      }
    },
    {
      "id": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcbbb",
      "type": "process",
      "spec_version": 2.1,
      "object_marking_refs": [],
      "granular_markings": [],
      "is_defanged": false,
      "is_hidden": false,
      "pid": 0,
      "created": "2021-06-03T18:42:29-04:00",
      "cwd": "",
      "command_line": "",
      "opened_connection_refs": [],
      "creator_user_ref": "",
      "image_ref": "",
      "parent_ref": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcaaa",
      "child_refs": [],
      "extensions": {
        "extension-definition--f9dbe89c-0030-4a9d-8b78-0dcd0a0de874": {
          "extension_type": "toplevel-property-extension",
          "action": "created",
          "creator-process-name": [
            "*outlook*",
            "thunderbird",
            "*mail*"
          ],
          "new-process-name": [
            "*edge*",
            "*chrome*",
            "*firefox*"
          ],
          "win-event-code": "4688"
        }
      }
    },
    {
      "id": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcccc",
      "type": "process",
      "spec_version": 2.1,
      "object_marking_refs": [],
      "granular_markings": [],
      "is_defanged": false,
      "is_hidden": false,
      "pid": 0,
      "created": "2021-06-03T18:42:29-04:00",
      "cwd": "",
      "command_line": "*.docm|*.pptm|*.xlsm",
      "opened_connection_refs": [],
      "creator_user_ref": "",
      "image_ref": "",
      "parent_ref": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcbbb",
      "child_refs": [],
      "extensions": {
        "extension-definition--f9dbe89c-0030-4a9d-8b78-0dcd0a0de874": {
          "extension_type": "toplevel-property-extension",
          "action": "created",
          "creator-process-name": [
            "*edge*",
            "*chrome*",
            "*firefox*"
          ],
          "new-process-name": [
            "*word*",
            "*powerpoint*",
            "*excel*"
          ],
          "win-event-code": "4688"
        }
      }
    },
    {
      "id": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcddd",
      "type": "process",
      "spec_version": 2.1,
      "object_marking_refs": [],
      "granular_markings": [],
      "is_defanged": false,
      "is_hidden": false,
      "pid": 0,
      "created": "2021-06-03T18:42:29-04:00",
      "cwd": "",
      "command_line": "",
      "opened_connection_refs": [],
      "creator_user_ref": "",
      "image_ref": "",
      "parent_ref": "process--862e625d-48bb-489e-8d4e-f7d8cd2fcccc",
      "child_refs": [],
      "extensions": {
        "extension-definition--f9dbe89c-0030-4a9d-8b78-0dcd0a0de874": {
          "extension_type": "toplevel-property-extension",
          "action": "created",
          "creator-process-name": [
            "*word*",
            "*powerpoint*",
            "*excel*"
          ],
          "new-process-name": [
            "powershell.exe",
            "cmd.exe"
          ],
          "win-event-code": "4688"
        }
      }
    },
    {
      "type": "x-demo-org-detection",
  "spec_version": "2.1",
  "id": "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021111",
  "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
  "created": "2021-08-13T20:30:34Z",
  "modified": "2021-08-13T20:30:34Z",
  "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": {
      "title": "Spearphishing with Link",
      "id": "spearphishing",
      "status": "experimental",
      "description": "Detects Office macro opening from browser.",
      "tags": [
        "attack.initial_access",
        "attack.t1566.002"
      ],
      "author": "demo",
      "date": "2021/06/07",
      "logsource": {
        "product": "windows",
        "index": "main",
        "category": "process_event"
      },
      "detection": {
            "selection": {
              "EventCode": "4688",
              "Creator_Process_Name|contains": [
                "outlook",
                "thunderbird",
                "mail"
              ],
              "New_Process_Name|contains": [
                "edge",
                "chrome",
                "firefox"
              ]
            },
            "condition": "selection"
          },
          "falsepositives": [
            "Low"
          ],
          "level": "high"
        },
        "type": "Sigma Rule"
      }
    },
    {
      "type": "x-demo-org-detection",
      "spec_version": "2.1",
      "id": "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021222",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2021-08-13T20:30:34Z",
      "modified": "2021-08-13T20:30:34Z",
      "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": {
        "title": "Spearphishing with Link",
        "id": "spearphishing",
        "status": "experimental",
        "description": "Detects Office macro opening from browser.",
        "tags": [
          "attack.initial_access",
          "attack.t1566.002"
        ],
        "author": "demo",
        "date": "2021/06/07",
        "logsource": {
          "product": "windows",
          "index": "main",
          "category": "process_event"
        },
        "detection": {
          "selection": {
            "EventCode": "4688",
            "New_Process_Name|contains": [
              "winword",
              "excel",
              "powerpoint"
            ],
            "Process_Command_Line|contains": [
              "docm",
              "xlsm",
              "pptm"
            ],
            "Creator_Process_Name|contains": [
              "edge",
              "chrome",
              "firefox"
            ]
          },
          "condition": "selection"
        },
        "falsepositives": [
          "Low"
        ],
        "level": "high"
      },
      "type": "Sigma Rule"
    }
  },
  {
    "type": "x-demo-org-detection",
    "spec_version": "2.1",
    "id": "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021000",
    "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2021-08-13T20:30:34Z",
    "modified": "2021-08-13T20:30:34Z",
    "name": "Process - Execution",
    "data_sources": [
      {
        "EventCode": "4688",
        "LogName": "Security",
        "TaskCategory": "Process Creation",
        "data_type": "WinEventLog:Security",
        "Creator_Process_Name": [
          "*word*",
          "*powerpoint*",
          "*excel*"
        ],
        "New_Process_Name": [
          "*.exe",
          "*.dll"
        ]
      }
    ],
    "analytic": {
```

```
  "rule": {
    "title": "Execution",
    "id": "execution",
    "status": "experimental",
    "description": "Detects Office macro execution",
    "tags": [
      "attack.execution",
      "attack.t1059"
    ],
    "author": "demo",
    "date": "2021/06/07",
    "logsource": {
      "product": "windows",
      "index": "main",
      "category": "process_event"
    },
    "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"
        ]
      }
    },
    "falsepositives": [
      "Low"
    ],
    "level": "high"
  },
  "type": "Sigma Rule"
```

```
      }
    },
    {
      "type": "x-demo-org-detection",
      "spec_version": "2.1",
      "id": "x-demo-org-detection--458c02c9-3635-42e4-8873-6785e00517e7",
      "created_by_ref": "identity--b085a68a-bf48-4316-9667-37af78cba894",
      "created": "2021-07-30T02:04:37Z",
      "modified": "2021-07-30T02:04:37Z",
      "name": "Registry - Persistence",
      "data_sources": [
        {
          "EventCode": "4657",
          "LogName": "Security",
          "Message": "A registry value was modified.\n\nSubject:\n\tSecurity
ID:\t\tS-1-5-21-1102256457-2379380313-1247321256-500\n\tAccount
Name:\t\tAdministrator\n\tAccount Domain:\t\tSP17\n\tLogon
ID:\t\t0x1A1ADFE8\n\nObject:\n\tObject
Name:\t\t\\REGISTRY\\MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\n\tOb
ject Value Name:\tpersist\n\tHandle ID:\t\t0x918\n\tOperation Type:\t\tNew registry
value created\n\nProcess Information:\n\tProcess ID:\t\t0x18f0\n\tProcess
Name:\t\tC:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\n\nChange
Information:\n\tOld Value Type:\t\t-\n\tOld Value:\t\t-\n\tNew Value
Type:\t\tREG_SZ\n\tNew Value:\t\tTrue",
          "TaskCategory": "Registry",
          "data_type": "WinEventLog:Security"
        }
      ],
      "analytic": {
        "rule": {
          "title": "Registry Run Keys",
          "id": "registry persistence",
          "status": "experimental",
          "description": "Detects new registry run key created event.",
          "tags": [
            "attack.persistence",
            "attack.t1547"
          ],
          "author": "demo",
          "date": "2021/06/07",
          "logsource": {
            "product": "windows",
            "index": "main",
            "category": "registry_event"
          },
          "detection": {
            "selection": {
              "EventCode": "4657",
              "Object_Name|contains": [
                "Run",
                "Shell Folders"
              ]
            },
            "condition": "selection"
          },
          "falsepositives": [
            "High"
          ],
          "level": "high"
        },
        "type": "Sigma Rule"
      }
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959666",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "detects",
      "source_ref": "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021111",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959666",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "detects",
      "source_ref": "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021222",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890ab"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-914343959666",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "detects",
      "source_ref": "x-demo-org-detection--458c02c9-3635-42e4-8873-6785e00517e7",
      "target_ref": "x-demo-org-behavior--edc99806-f8e9-4ee3-b2d4-1234567890cc"
    },
    {
      "type": "x-demo-org-detection-group",
      "spec_version": "2.1",
      "id": "x-demo-org-detection-group--58834c29-4ceb-42a1-a218-321103021999",
      "created": "2021-08-13T20:30:34Z",
      "modified": "2021-08-13T20:30:34Z",
      "name": "Reaper Lite Detection",
      "description": "This detection group detects spearphishing, execution, and
persistence",
      "confidence": {
        "low": 1,
        "medium": 2,
        "high": 3
      },
      "detection_ids": [
        "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021000",
        "x-demo-org-detection--458c02c9-3635-42e4-8873-6785e00517e7",
        "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021111",
        "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021222"
      ]
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-111111111111",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "detects",
      "source_ref": "x-demo-org-detection-group--58834c29-4ceb-42a1-a218-
321103021999",
      "target_ref": "grouping--cb508d31-469c-41d0-ab3d-fb78ed60b61d"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-111111111222",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "contains",
      "source_ref": "x-demo-org-detection-group--58834c29-4ceb-42a1-a218-
321103021999",
      "target_ref": "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021000"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-111111111333",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "contains",
      "source_ref": "x-demo-org-detection-group--58834c29-4ceb-42a1-a218-
321103021999",
      "target_ref": "x-demo-org-detection--458c02c9-3635-42e4-8873-6785e00517e7"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-111111111444",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "contains",
      "source_ref": "x-demo-org-detection-group--58834c29-4ceb-42a1-a218-
321103021999",
      "target_ref": "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021111"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--37ac0c8d-f86d-4e56-aee9-111111111555",
      "created": "2016-11-23T08:17:27.000Z",
      "modified": "2016-11-23T08:17:27.000Z",
      "relationship_type": "contains",
      "source_ref": "x-demo-org-detection-group--58834c29-4ceb-42a1-a218-
321103021999",
      "target_ref": "x-demo-org-detection--58834c29-4ceb-42a1-a218-336103021222"
    }
  ]
}
```