Cyber Threat Modelling by leveraging an open source attack graph and activity thread graph tool
(cti-stix-diamond-activity-attack-graph)

Author: Rukhsar Khan
rkhan@rukhsarkhan.de

***Abstract* – Ineffective approaches in incident preparation and security operations (detection, intrusion analysis and response) exist in many SOC organizations today. They further lack knowledge and expertise to comprehend and analyse a large cyber event chain consisting of multiple related events. Therefore, organizations fall short of defending against the risk cyber attackers pose to them.**

Leverage our tool (cti-stix-diamond-activity-attack-graph) to properly prepare for the current and future risks cyber attackers are posing against a client's organization. Upon detailed understanding of the threats by using attack graphs and attack trees, put the right defensive measures onto the client's prevention and detection security controls. These insights are consumed by various stakeholders to get an understanding of the attacker's complete modus operandi and how they would target a client's assets in a few glances.

1 Introduction

What customers actually need for improving the effectiveness of their defence preparation, threat detection, intrusion analysis and incident response capabilities is an end-to-end cyber defence methodology which helps them achieve a high maturity level. The maturity of SOC organizations is roughly defined in the following 5 levels:

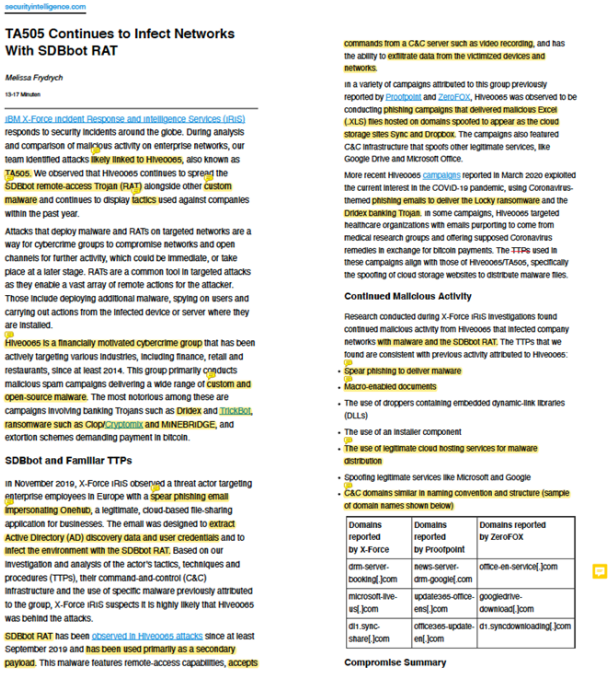
- Level 1: Initial (Processes are ad-hoc, chaotic, poorly defined; success depends on individual efforts and heroics)
- Level 2: Repeatable (Basic SOC processes and discipline established to repeat earlier success)
- Level 3: Defined (Standard Operating Procedures (SOP) are defined, documented and integrated across the organization)
- Level 4: Managed (Detailed process metrics are measured, proactive use cases as well as effective frameworks and cyber defence methodologies are implemented)
- Level 5: Optimized (Continuous process improvement is enabled. Automation leveraged by AI/ML)

SOC organizations are mostly lacking essential security operations skills [1], meaning that they are operating on a low maturity level. To increase their maturity level, they need to build threat-, system- and asset-centric cyber threat models and juxtapose these to one another. SOC organizations further need to operationalize the threat models for Threat Hunting and inferring effective SIEM detection rules.

2 Methodology
2.1 Modelling of the threat-centric part

At its core, our methodology is based on concepts from *The Diamond Model of Intrusion Analysis* [2]. This model facilitates the arrangement of all elements and objects related to a cyber-attack including their relationships in a meaningful way. It further proposes an effective underlying analysis methodology that integrates the art and science of intrusion analysis. A concept for consuming Threat Intelligence to infer Cyber Threat Models (CTMs) represented as attack graphs is part of the Diamond Model, however, it is different from our approach.

For generating CTMs we follow the principles outlined in the *TIBER-EU* framework [3] to understand, and manually extract and relate entities and objects from natural language prose, essentially provided in strategic, operational and tactical cyber threat intelligence (CTI) reports.



securityintelligence.com

TA505 Continues to Infect Networks With SDBbot RAT

Melissa Frydrych

13-17 Minuten

IBM X-Force Incident Response and Intelligence Services (IRIS) responds to security incidents around the globe. During analysis and comparison of malicious activity on enterprise networks, our team identified attacks likely linked to Hiveooes, also known as TA505. We observed that Hiveooes continues to spread the SDBbot remote-access Trojan (RAT) alongside other custom malware and continues to display tactics used against companies within the past year.

Attacks that deploy malware and RATs on targeted networks are a way for cybercrime groups to compromise networks and open channels for further activity, which could be immediate, or take place at a later stage. RATs are a common tool in targeted attacks as they enable a vast array of remote actions for the attacker. Those include deploying additional malware, spying on users and carrying out actions from the infected device or server where they are installed.

Hiveooes is a financially motivated cybercrime group that has been actively targeting various industries, including finance, retail and restaurants, since at least 2014. This group primarily conducts malicious spam campaigns delivering a wide range of custom and open-source malware. The most notorious among these are campaigns involving banking Trojans such as Dridex and TrickBot, ransomware such as ClopCryptomix and MINEBRIDGE, and extortion schemes demanding payment in bitcoin.

SDBbot and Familiar TTPs

In November 2019, X-Force IRIS observed a threat actor targeting enterprise employees in Europe with a spear phishing email impersonating Onehub, a legitimate, cloud-based file-sharing application for businesses. The email was designed to extract Active Directory (AD) discovery data and user credentials and to infect the environment with the SDBbot RAT. Based on our investigation and analysis of the actor's tactics, techniques and procedures (TTPs), their command-and-control (C&C) infrastructure and the use of specific malware previously attributed to the group, X-Force IRIS suspects it is highly likely that Hiveooes was behind the attacks.

SDBbot RAT has been observed in Hiveooes attacks since at least September 2019 and has been used primarily as a secondary payload. This malware features remote-access capabilities, accepts commands from a C&C server such as video recording, and has the ability to exfiltrate data from the victimized devices and networks.

In a variety of campaigns attributed to this group previously reported by Proofpoint and ZeroFOX, Hiveooes was observed to be conducting phishing campaigns that delivered malicious Excel (.XLS) files hosted on domains spoofed to appear as the cloud storage sites Sync and Dropbox. The campaigns also featured C&C infrastructure that spoofs other legitimate services, like Google Drive and Microsoft Office.

More recent Hiveooes campaigns reported in March 2020 exploited the current interest in the COVID-19 pandemic, using Coronavirus-themed phishing emails to deliver the Locky ransomware and the Dridex banking Trojan. In some campaigns, Hiveooes targeted healthcare organizations with emails purporting to come from medical research groups and offering supposed Coronavirus remedies in exchange for bitcoin payments. The TTPs used in these campaigns align with those of Hiveooes/TA505, specifically the spoofing of cloud storage websites to distribute malware files.

Continued Malicious Activity

Research conducted during X-Force IRIS investigations found continued malicious activity from Hiveooes that infected company networks with malware and the SDBbot RAT. The TTPs that we found are consistent with previous activity attributed to Hiveooes:

- Spear phishing to deliver malware
- Macro-enabled documents
- The use of droppers containing embedded dynamic-link libraries (DLLs)
- The use of an installer component
- The use of legitimate cloud hosting services for malware distribution
- Spoofing legitimate services like Microsoft and Google
- C&C domains similar in naming convention and structure (sample of domain names shown below)

Domains reported by X-Force	Domains reported by Proofpoint	Domains reported by ZeroFOX
drm-server-booking[.]com	news-server-drm-google[.com	office-en-service[.]com
microsoft-live-es[.]com	updateses-office-ens[.]com	googledrive-download[.]com
dl1.sync-share[.]com	officeses-update-en[.]com	dl.syncdownloading[.]com

Compromise Summary

Figure 1 - CTI reports

We structure attack graphs in multiple levels of abstraction (x, y) by aggregating the DML1 to DML6 abstraction levels of the *DML model* [4] and cover therein the threat-centric part of an attack.

The main graph (see Figure 2) categorizes entities and objects including their respective relationships and arranges them in a phase-ordered kill chain representing attacker Tactics and Techniques.

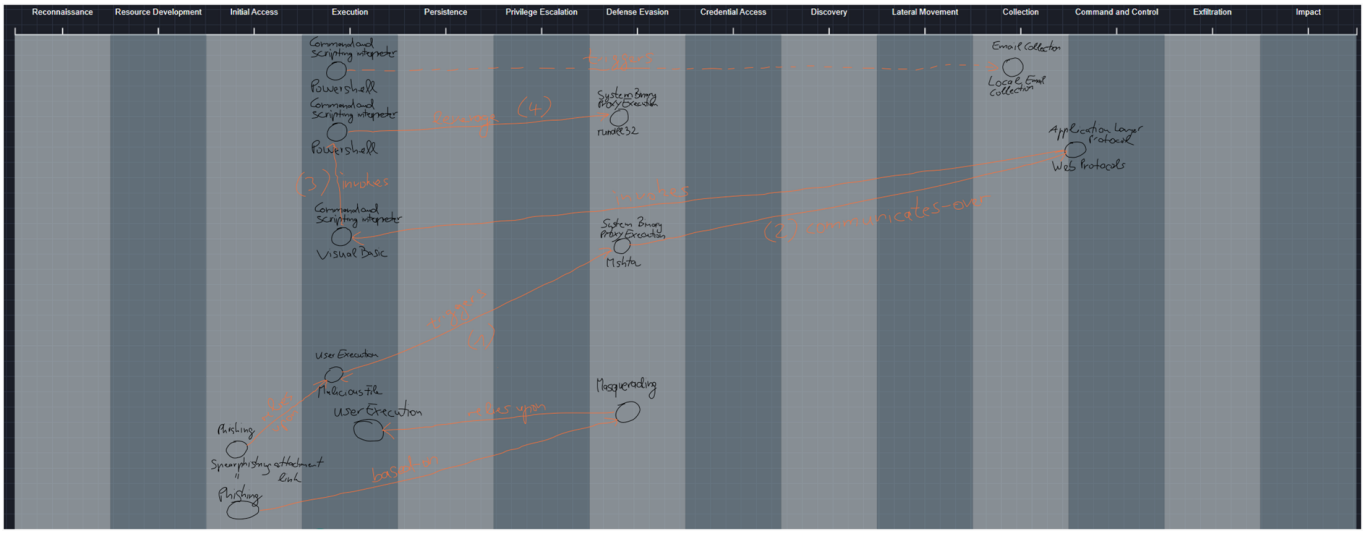


Figure 2 - Main graph (level x)

The subgraph (see Figure 3) represents the Procedure of a specific Technique, particularly on a tactical rather on a technical level.

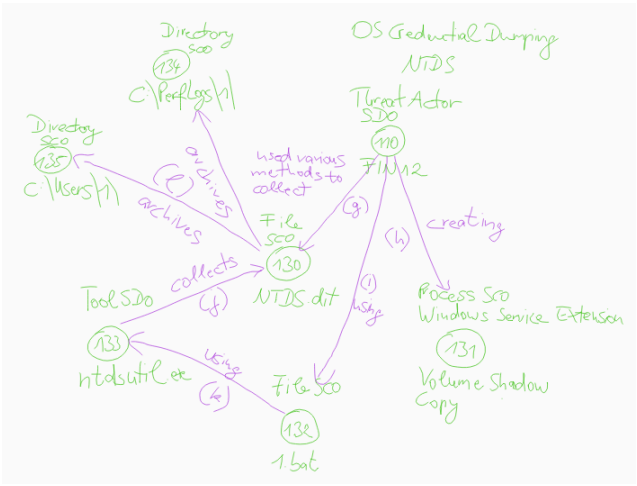


Figure 3 - Subgraph (level y)

The MITRE ATT&CK Matrix for Enterprise constitutes the taxonomy of the main graph. The taxonomy of the subgraph is mainly based on the Diamond Model (see Figure 4). The corpus of the main graph and subgraph are built on a defined ontology vocabulary that leverages Structured Threat Information Expression (STIX) language [5], more precisely STIX Domain Objects (SDO), STIX Relationship Objects (SRO), STIX Cyber-observable Objects (SCO) as well as STIX Extensions.

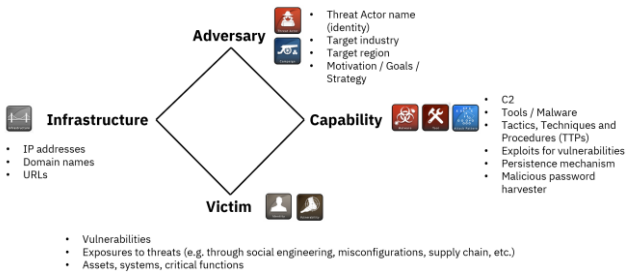


Figure 4 - Representing Diamond Model with STIX

This means that the manually extracted entities and objects including their corresponding relationships need to undergo a translation process into STIX language. Currently, this is also a manual endeavour which is described under section 6.

According to [6], cyber threat modelling can be approached from various directions. We follow the approach to first model the threat-centric part of an attack and then apply it to the asset- and system-centric part, the latter part also referred to as the operational environment.

2.2 Modelling of the asset- and system-centric part (operational environment)

The crown jewels of the operational environment along with their corresponding exposures are retrieved from a pre-filled critical functions table for threat modelling. This table also includes attack paths, network topology and intermediate endpoint information. Crown jewels including their direct and indirect exposures within this table are converted to individual attack trees [7]. The concept is much like in [8], however, based on common exposures like vulnerabilities (CVE), weaknesses (CWE), cyber-enabled application attack pattern (CAPEC), Tactics, Techniques and Procedures (TTPs) and more, a manual juxtaposing endeavour establishes a connection between an attack tree and a pre-defined threat-centric attack graph. Such a connection is captured as an n-tuple (attack graph, attack tree). Once completed, the attack tree is further incorporated into the corresponding attack graph. This builds the foundation of a **complete threat scenario** that represents how relevant threat actors would target the client's critical functions with their attack methodology, malware and tools.

2.3 Leveraging CTMs for security operations

We leverage CTMs to derive effective Security Information & Event Management (SIEM) detection rules which help reduce false-positive alerts. We further utilize CTMs for effective threat hunting, using the provided attack graphs to give clues to threat hunters and streamline the testing of pre-formulated hypotheses with corresponding pre-defined queries.

3 Tool description

The cti-stix-diamond-activity-attack-graph is an open-source tool designed to visualize STIX 2.1 content in both an Attack Graph and an Activity Thread Graph. It applies principles from The Diamond Model of Intrusion Analysis, as well as Tactics, Techniques, and Procedures (TTPs) from the MITRE ATT&CK v8.2 framework. Specifically, the Attack Graph provides a graphical representation of a known attack scenario sourced from Cyber Threat Intelligence (CTI) of a specific adversary, while the Activity Thread Graph represents local findings gathered during a hunt engagement. Both graphs feature a main graph and one or more sub-graphs, depending on the number of Techniques available. Users can access sub-graphs by clicking on individual Technique objects.

This tool is designed to assist Cyber Threat Hunters (Cyber Security Analysts) in gaining full visibility into an attack scenario. The tool primarily ingests Strategic, Operational and Tactical Threat Intelligence reports but also includes limited Technical Threat Intelligence feeds. The gathered intelligence is represented in the Attack Graph, helping analysts understand how an adversary executed a cyber threat campaign, which in turn aids in defending against it. The Activity Thread Graph enables analysts to chain locally identified attacker activities and visualize them on a timeline.

The tool is implemented using the HTML5 Boilerplate framework [9]. The complete visualization is built with d3.js [10], a JavaScript library for document manipulation, and the entire process is carried out in the browser without the need for a server (backend).

To use this tool as intended, certain specific requirements related to STIX 2.1 objects, as outlined below, MUST be met.

4 How to access the tool

To quickly explore the output and functionalities of the tool, visit https://yukh1402.github.io/cti-stix-diamond-activity-attack-graph/ and load the partial Ryuk Ransomware scenario example STIX 2.1 bundle into the Attack Graph. You can use this URL to access the online version of the tool.

If you'd prefer to deploy your own instance of the application, we recommend setting up a Docker container. The docker image is available on Docker Hub. To activate the image and mount it to port 80 in your environment, use the following command on your Docker system:

```
docker run -d -p 80:80 1402/cti-stix-diamond-activity-attack-graph:latest
```

5 Graph types

In this tool, STIX objects are visually represented by simply providing a STIX 2.1 Bundle. Based on the selected graph type, STIX information is displayed either in an Attack Graph (Figure 5) or an Activity Thread Graph (Figure 6). The Attack Graph is timeless and displays multiple Techniques in the context of the MITRE ATT&CK Matrix for Enterprise. The Activity Thread Graph, on the other hand, considers the timestamps of local findings and generates a correlated Timeline-Technique graph. By selecting a Technique, the corresponding subgraph (Figure 7) with all related STIX objects is displayed.

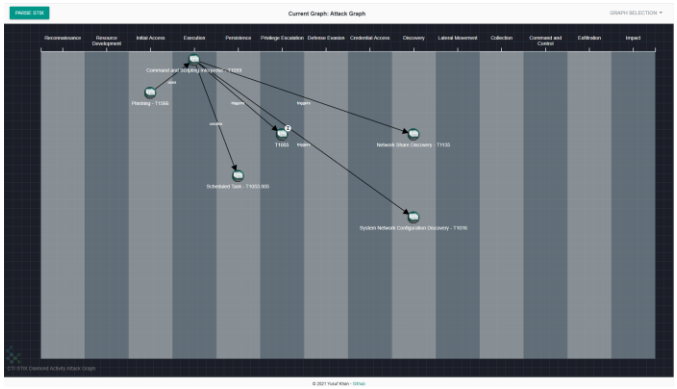


Figure 5 - Main graph (level x)

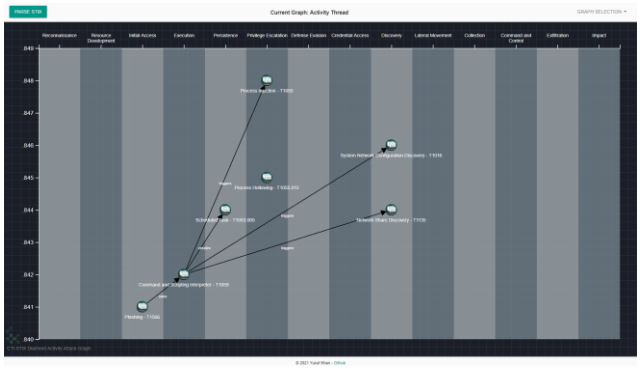


Figure 6 - Activity Thread graph

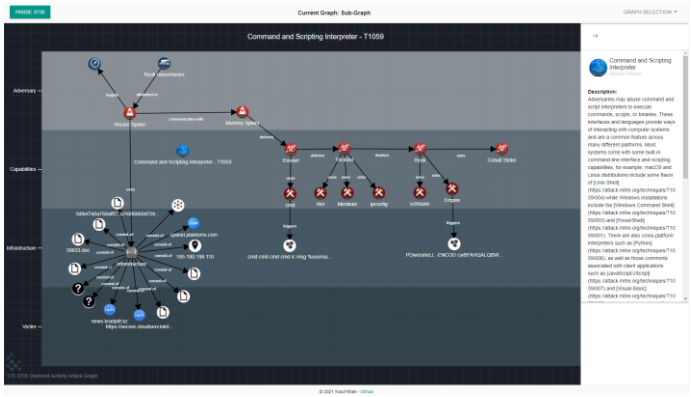


Figure 7 - Subgraph (level y)

6 Tool usage

As described under https://github.com/yukh1402/cti-stix-diamond-activity-attack-graph, follow the instructions for using the tool:

“The STIX Bundle MUST have a structured schema with at least one or multiple STIX Domain Objects (SDO) of type Grouping. All other SDOs, STIX Relationship Objects (SROs) and STIX Cyber-observable Objects (SCOs) that are related or employed in the same context will be referenced via id in the "object_refs" field of the associated Grouping

SDO."

"For providing a valid STIX Bundle schema that can be processed in the tool, three requirements are necessary:

1. Each Grouping SDO MUST have one Attack Pattern SDO reference. The Attack Pattern SDO schema is derived from the MITRE ATT&CK framework and can be found on the MITRE CTI repository or pulled from the MITRE ATT&CK TAXII Server. See example below:"


```
{
 "id": "bundle--70d2c497-5717-5a3a-8b03-d2c1f74df433",
"type": "bundle",
 "objects": [
  {
   "id": "grouping--b5df7982-fb4f-4f73-aac8-c8e22dd8f76d",
   "context": "Test",
   "object_refs": [
     "attack-pattern--b99dc28b-b1bc-41f1-b707-
b1b50a2118ea"
   ],
   "type": "grouping",
   "spec_version": "2.1",
   "created": "2021-04-18T06:18:03.030108Z",
   "modified": "2021-04-18T06:18:03.030108Z",
   "revoked": false
  },
  {
   "id": "attack-pattern--b99dc28b-b1bc-41f1-b707-
b1b50a2118ea",
   "name": "Spearphishing Attachment",
   "type": "attack-pattern",
   "created": "2020-03-02T19:05:18.137Z",
   "revoked": false,
   "modified": "2020-10-18T01:52:25.316Z",
   "description": "Adversaries may send spearphishing emails
with a malicious attachment in an attempt to gain access to
victim systems. Spearphishing attachment is a specific
variant of spearphishing. Spearphishing attachment is
different from other forms of spearphishing in that it employs
the use of malware attached to an email. All forms of
spearphishing are electronically delivered social engineering
targeted at a specific individual, company, or industry. In this
scenario, adversaries attach a file to the spearphishing email
and usually rely upon [User Execution]
(https://attack.mitre.org/techniques/T1204) to gain
execution.\n\nThere are many options for the attachment
such as Microsoft Office documents, executables, PDFs, or
archived files. Upon opening the attachment (and potentially
clicking past protections), the adversary's payload exploits a
vulnerability or directly executes on the user's system. The
text of the spearphishing email usually tries to give a
plausible reason why the file should be opened, and may
explain how to bypass system protections in order to do so.
The email may also contain instructions on how to decrypt an
attachment, such as a zip file password, in order to evade
email boundary defenses. Adversaries frequently manipulate
file extensions and icons in order to make attached
executables appear to be document files, or files exploiting
one application appear to be a file for a different one.",
  "spec_version": "2.1",
 "kill_chain_phases": [
  {
     "phase_name": "initial-access",
     "kill_chain_name": "mitre-attack"
    }
   ],
   "external_references": [
    {
     "external_id": "T1566.001",
     "source_name": "mitre-attack"
    }
   ]
  }
 ]
}
```


2. "All STIX objects (SDOs, SROs, SCOs) which are considered in the same context MUST belong to one Grouping SDO. The references of these objects will be registered in the "object_refs" field of the Grouping SDO. SROs that are in the same context MUST be registered in the "object_refs" field as well."


```
{
 "id": "bundle--70d2c497-5717-5a3a-8b03-d2c1f74df433",
 "objects": [
  {
   "id": "grouping--b5df7982-fb4f-4f73-aac8-c8e22dd8f76d",
   "context": "Test",
   "object_refs": [
     "attack-pattern--b5d88165-5de1-4b36-94b3-
a7b272256088",
     "malware--beab30f1-4219-4efb-a533-0ae1a2aa1c6b",
     "tool--736dcf51-f123-434b-9a34-08208e856c94",
     "threat-actor--8f82ccac-ff89-4307-9661-547aaa4eaa77",
     "infrastructure--dc7e9a67-4667-4c75-b5d0-
776b54c54ced",
     "relationship--e9966e1b-1574-474b-a2b4-
cfe0ccac1cc2",
     "relationship--74654ae6-42b9-48cb-b6c1-
390b6f844acf"
   ],
   "type": "grouping",
   "spec_version": "2.1",
   "created": "2021-04-18T06:18:03.030108Z",
   "modified": "2021-04-18T06:18:03.030108Z",
   "revoked": false
  },
  {
   "id": "attack-pattern--b5d88165-5de1-4b36-94b3-
a7b272256088",
   "name": "System Network Configuration Discovery",
   "type": "attack-pattern",
   "created": "2017-05-31T21:30:27.342Z",
   "revoked": false,
   "modified": "2020-03-15T00:55:33.136Z",
   "description": "Adversaries may look for details about the
network configuration and settings of systems they access or
through information discovery of remote systems. Several
operating system administration utilities exist that can be
used to gather this information. Examples include
[Arp](https://attack.mitre.org/software/S0099),
[ipconfig](https://attack.mitre.org/software/S0100)/[ifconfi
g](https://attack.mitre.org/software/S0101)
   , [nbtstat](https://attack.mitre.org/software/S0102),
   and
[route](https://attack.mitre.org/software/S0103).\n\nAdve
rsaries may use the information from [System Network
Configuration
Discovery](https://attack.mitre.org/techniques/T1016)
during automated discovery to shape follow-on behaviors,
including whether or not the adversary fully infects the target
and/or attempts specific
```

```
   actions.",
   "spec_version": "2.1",
   "kill_chain_phases": [
    {
     "phase_name": "discovery",
     "kill_chain_name": "mitre-attack"
    }
   ],
   "external_references": [
    {
     "external_id": "T1016",
     "source_name": "mitre-attack"
    }
   ]
  },
  {
   "id": "malware--beab30f1-4219-4efb-a533-
0ae1a2aa1c6b",
   "name": "Emotet",
   "type": "malware",
   "created": "2021-04-18T05:52:49.754214Z",
   "revoked": false,
   "modified": "2021-04-18T05:52:49.754214Z",
   "is_family": true,
   "capabilities": [
     "anti-disassembly",
     "anti-emulation"
   ],
   "spec_version": "2.1",
   "malware_types": [
     "backdoor",
     "bot"
   ]
  },
  {
   "id": "tool--736dcf51-f123-434b-9a34-08208e856c94",
   "name": "schtasks",
   "type": "tool",
   "created": "2021-04-18T05:52:49.759204Z",
   "revoked": false,
   "modified": "2021-04-18T05:52:49.759204Z",
   "tool_types": [
     "exploitation"
   ],
   "spec_version": "2.1"
  },
  {
   "id": "threat-actor--8f82ccac-ff89-4307-9661-
547aaa4eaa77",
   "name": "Wizard Spider",
   "type": "threat-actor",
   "goals": [
     "trying to steal info"
   ],
   "roles": [
     "director"
   ],
   "created": "2021-04-18T05:52:49.765003Z",
   "revoked": false,
   "modified": "2021-04-18T05:52:49.765003Z",
   "spec_version": "2.1",
   "x_target_industry": [
     "government-national"
   ],
   "primary_motivation": "dominance",
   "threat_actor_types": [
     "activist",
     "nation-state"
   ],
   "secondary_motivations": [
     "organizational-gain"
   ]
  },
  {
   "id": "infrastructure--dc7e9a67-4667-4c75-b5d0-
776b54c54ced",
   "name": "Infrastructure",
   "type": "infrastructure",
   "created": "2021-04-18T05:52:49.766474Z",
   "revoked": false,
   "modified": "2021-04-18T05:52:49.766474Z",
   "spec_version": "2.1",
   "infrastructure_types": [
     "phishing"
   ]
  },
  {
   "id": "relationship--e9966e1b-1574-474b-a2b4-
cfe0ccac1cc2",
   "type": "relationship",
   "created": "2021-04-18T05:56:30.51424Z",
   "revoked": false,
   "modified": "2021-04-18T05:56:30.51424Z",
   "spec_version": "2.1",
   "source_ref": "infrastructure--dc7e9a67-4667-4c75-b5d0-
776b54c54ced",
   "relationship_type": "consist-of",
   "target_ref": "malware--beab30f1-4219-4efb-a533-
0ae1a2aa1c6b"
  },
  {
   "id": "relationship--74654ae6-42b9-48cb-b6c1-
390b6f844acf",
   "type": "relationship",
   "created": "2021-04-18T05:56:30.514686Z",
   "revoked": false,
   "modified": "2021-04-18T05:56:30.514686Z",
   "spec_version": "2.1",
   "source_ref": "threat-actor--8f82ccac-ff89-4307-9661-
547aaa4eaa77",
   "relationship_type": "uses",
   "target_ref": "tool--736dcf51-f123-434b-9a34-
08208e856c94"
  }
 ],
 "type": "bundle"
}
```


3. “Relationships (SROs) between Grouping SDOs MUST NOT be registered in the "object_refs" field of the Grouping SDO. They MUST appear as indivisdual objects inside the bundle "objects".”


```
{
"id": "bundle--70d2c497-5717-5a3a-8b03-d2c1f74df433",
"objects": [
 {
  "id": "grouping--e1e278ff-671d-44e1-add5-
42be17562663",
  "context": "Test1",
  "object_refs": [
     ...
  ],
  "type": "grouping",
  "spec_version": "2.1",
  "created": "2021-04-18T06:18:03.030108Z",
  "modified": "2021-04-18T06:18:03.030108Z",
  "revoked": false
 },
 {
  "id": "grouping--b5df7982-fb4f-4f73-aac8-c8e22dd8f76d",
```

```
  "context": "Test2",
  "object_refs": [
     ...
  ],
  "type": "grouping",
  "spec_version": "2.1",
  "created": "2021-04-18T06:18:03.030108Z",
  "modified": "2021-04-18T06:18:03.030108Z",
  "revoked": false
},
{
  "id": "relationship--74654ae6-42b9-48cb-b6c1-
390b6f844acf",
  "type": "relationship",
  "created": "2021-04-18T05:56:30.514686Z",
  "revoked": false,
  "modified": "2021-04-18T05:56:30.514686Z",
  "spec_version": "2.1",
  "source_ref": "grouping--e1e278ff-671d-44e1-add5-
42be17562663",
  "relationship_type": "uses",
  "target_ref": "grouping--b5df7982-fb4f-4f73-aac8-
c8e22dd8f76d"
 }
],
"type": "bundle"
}
```


References

[1] "The State of Cybersecurity 2023: The Business Impact of Adversaries," Sophos, 2023.

[2] S. Caltagirone, A. Pendergast and C. Betz, "The Diamond Model of Intrusion Analysis," https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf, 2013.

[3] "TIBER-EU Guidance for Target Threat Intelligence Report," European Central Bank, https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf, 2020.

[4] A. Jøsang, S. Bromander and M. Eian, "Semantic Cyberthreat Modelling," http://folk.uio.no/josang/papers/BJE2016-STIDS.pdf, 2016.

[5] "Introduction to STIX," OASIS Open, https://oasis-open.github.io/cti-documentation/stix/intro.html, 2017-2023.

[6] "Cyber Threat Modeling: Survey, Assessment, and Representative Framework," Homeland Security Systems Engineering and Development Institute (HSSEDI), https://www.mitre.org/news-insights/publication/cyber-threat-modeling-survey-assessment-and-representative-framework, 2018.

[7] B. Schneier, "Modeling security threats," 1999. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html.

[8] "Asset-Centric Analysis and Visualization of Attack Trees," Goethe University Frankfurt, University of Siegen, 2020.

[9] R. Larsen and C. Oliff, "HTML5 Boilerplate," https://html5boilerplate.com/.

[10] "The JavaScript library for bespoke data visualization," Mike Bostock and Observable, Inc., https://d3js.org/.