Maltego Handbook for Cyber Threat Intelligence

handbook

MALTEGO

Table of Content

About Cyber Threat Intelligence

Attacks are getting more sophisticated, and enterprises may be targeted from adversaries with various domains and motivations. Companies can no longer only work on an incident-by-incident basis, but must leverage information on previous incidents to react faster to future incidents identification and mitigation. Incident observa-tions and the intelligence gained from those events help to identify and possibly predict threats. With cyber threat intelligence, individ-uals as well as enterprises can apply and build their knowledge, skills, and experiences when engaging with attacks. While CTI is focused on the digital world, geopolitical parameters of the real world must not be left out to correctly understand an attack or threat and support decision makers in risk reduction.

Cyber threat intelligence is categorized into the following types:

Strategic Threat Intelligence: Helps to map the threat landscape and support decision makers. Usually, this information is handwrit-ten with less technical background.

Tactical Threat Intelligence: Helps to under-stand threat actors as it applies TTP's for ex-ample with the Mitre ATT&CK framework. Such information is technical and includes techni-cal context consumed by admins, security en-gineers, and security staffs. This information should also be used to improve security poli-cies and defend organizations.

Operational Threat Intelligence: Helps to understand cyber-attacks or malicious campaigns and is usually consumed by threat hunters and incident responders. It overlaps with tactical threat intelligence and includes information about attack vectors such as which domain is used to control infected systems.

With this categorization in place, each operational teams and personnel can consume the most relevant intelligence. All this information aims to support risk identification and risk reduction and may lead to actor attribution as they have various motivations.

Where to Use Cyber Threat Intelligence

Cyber threats are everywhere. The only way to truly protect your company and your clients is to have access to the right information. Cyber threat intelligence gives you the intelligence you need to stay ahead of hackers and keep your business safe.

It is important that cyber threat intelligence is tailored to the needs of each company. There are different types of intelligence platforms which can provide different types of information based on your area of business and what kind of data you are looking for.

Key Use Cases Involving Cyber Threat Intelligence

In this handbook, we will focus on the following 5 commonly known use cases that involve the usage of cyber threat intelligence:

1. IoC Collection for Specific Threats
2. Profiling Threat Actor Infrastructure
3. Profiling Threat Actors
4. Attack and TTP Analysis
5. Vulnerability or Attack Surface Assessment

Setting up Maltego

Set up your Maltego Desktop Client followings the simple five steps below.

Download Maltego

Download Maltego from our website for your Windows, Linux, or Mac machine.

Activate Maltego

Open Maltego and activate your license by inputting your license key.

Accept the License Agreement

Read and accept the license agreement.

Install Transform Servers

Select the Transform servers you need for Desktop Client: The Public Transform Server and/or the Local Transform Server.

Install Hub Items & Start Investigating!

Install the Maltego Standard Transforms and other third-party Hub items and start investigating!

Top Maltego Hub Items for Cyber Threat Intelligence

Here is a list of high-quality intelligence options for various CTI investigative scenarios that have proven to be amongst our end-users' favorites and are suitable for all budget sizes. The list is sorted in alphabetical order and doesn't indicate any ranking or preference.

Main Hub Items for Daily Use

Click-and-Run

1 **Intezer Analyze**
Automate end-to-end malware investigations with genetic malware analysis.

2 **OpenCTI**
Query and explore threat intelligence data from OpenCTI instances using STIX2 Entities.

3 **Shodan**
Gain access to intelligence about the global IoT and infrastructure data.

4 **VirusTotal Public API**
Leverage 15 years of malicious sightings to enrich your organization's malware observations and logs.

5 **WhoisXML API**
Leverage advanced IP and domain data to facilitate cybercrime detection, response, and prevention.

Commercial

1 **Recorded Future**
Gain full picture of threat actors, including known exploit kits, vulnerabilities, or other TTPs.

2 **Silobreaker**
Tap into deep & dark web for enrichment and investigations of malware, threat actors, TTPs, and more.

Supplementary Hub Items

Click-and-Run

1 Maltego Standard Transforms

2 NIST NVD

Discover context and insights around CVEs, CPEs, and CWEs for vulnerability and threat exposure assessment.

Commercial

1 GreyNoise Enterprise

Query IP address data and CVEs, Tags, or activities that an IP address has been observed scanning for.

Looking for more data sources? Explore and find your solutions in our Transform Hub now.

Use Case 1: Ioc Collection for Specific Threats

Context:

Our Threat Intel team wishes to gather IOCs on a particular threat actor. However, we do not have access to external intel feeds, or if we do, the intel feeds have little information about the said threat actor. We will try to gather IoCs using only the Maltego Standard Transforms.

Goal:

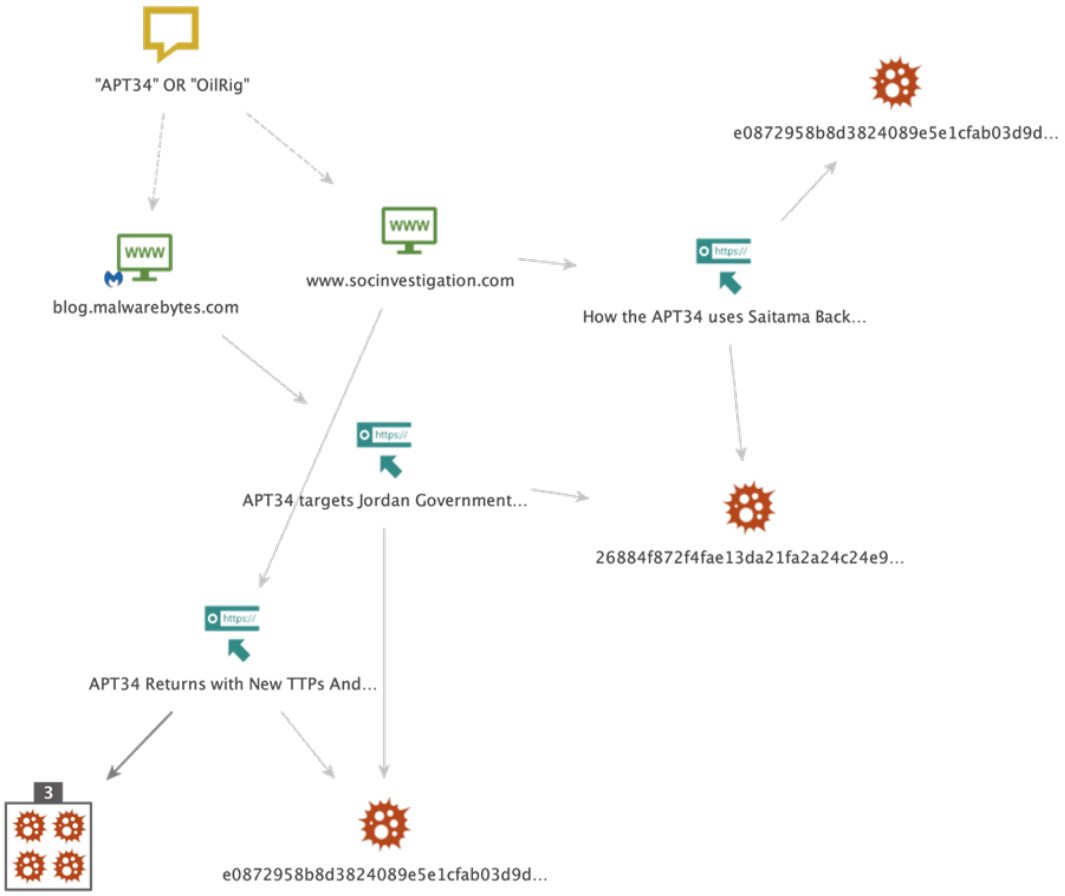
The Threat Intel team wants to gather IOCs associated with a particular threat actor.

Starting Points:

Names or alias of the said threat actors

Playbook:

1. Paste all known names and aliases of your target threat actors into Maltego. For example: APT34 is also known as OilRig, which gives us: "APT34" OR "OilRig".
2. Select the Phrase Entity containing the names and aliases and run the following Transform:
   - To Website [using Search Engine]
3. Select the Website Entities that looks relevant to your search, or alternatively, select all results with a weight higher than 70, and run:
   - To URLs [show Search Engine results]
4. Select all the URL Entities and automatically extract the IOCs from these pages using the following regular expressions:
   - To Regex Matches [Found on web page]
     - \b[A-Fa-f0-9]{32}\b
       (to search for MD5 hashes)
     - \b[A-Fa-f0-9]{64}\b
       (to search for SHA256 hashes)
     - [-a-zA-Z0-9()@:%_\+.~#?&\/=\[\]]*\[\.\][-a-zA-Z0-9()@:%_\+.~#?&\/=]*
       (to search for defanged domains or URLs)
     - \b[\d]{1,3}\[?\.\]?[\d]{1,3}\[?\.\]?[\d]{1,3}\[?\.\]?[\d]{1,3}(:\d+)?\b
       (to search for IP address, defanged or not, bearing a port or not)
5. Copy and paste the relevant domains, URLs and Ips to your text editor to “refang” them
6. Copy and paste them back to Maltego and change the Entity types to reflect their nature (e.g. change the hashes from a Phrase Entity to a Hash Entity).
7. Use other integrations such as Intezer Analyze, AlienVault OTX, VirusTotal, and more to gather other IOCs linked to the one you just collected



This is an example graph illustrating the process listed above. Several results have been removed from the graph above to increase its readability.

Use Case 2: Profiling Threat Actor Infrastructure

Context:

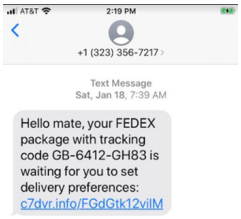
- SOC/CSIRT team is investigating phishing emails targeting different user communities in your organization.
- Phishing was not properly detected but notified by one of our users thanks to the security awareness training they have received

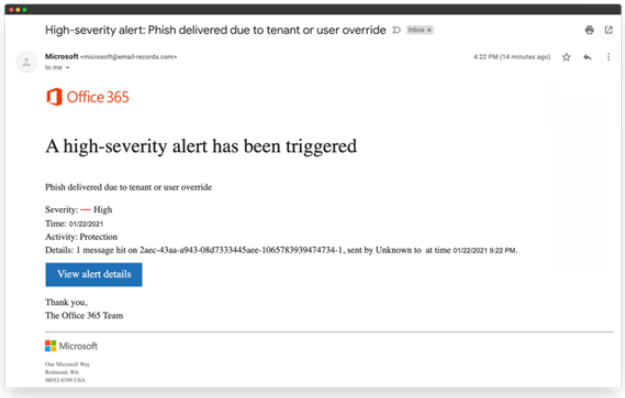
Goal:

- Map the phishing activity to an existing campaign/threat actor
- Understand the infrastructure:
  - Hosting of the phishing website
  - Sending of the phishing/SMS emails
- Discover other similar websites linked to the same campaign or threat actor

Starting Points:

- Original phishing email/SMS (including full headers)
- Source email addresses
- URLs embedded in the email





Playbook:

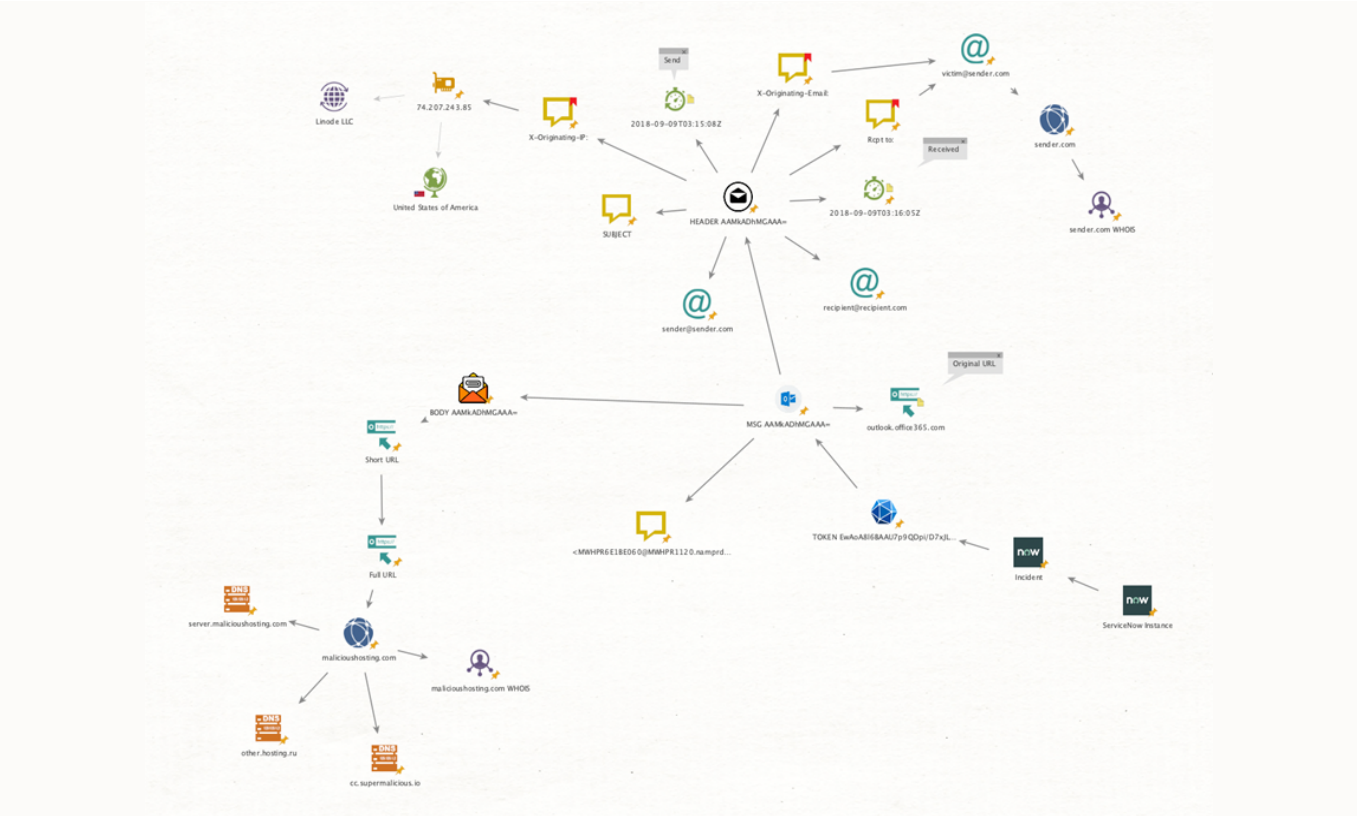
1. Observe the phishing emails or SMS and extract relevant information such as:
   - Source IP/DNS name of the MTA sending the email
     - X-originating-Email
     - X-originating-IP
   - Source mailbox
     - Return-path
     - From:
   - Source Phone
   - Links to URLs
   - Fixed parts of the message (avoiding codes)

```
X-Originating-Email: [bad_guy_spammer@spammy.com]
X-Originating-IP: [192.168.1.25]
X-Agari-Original-From: bad_guy_spammer@spammy.com
X-Agari-Original-To: buggln***@gmail.com
X-IronPort-Anti-Spam-Filtered: true
X-IronPort-AV: E=Sophos;i="5.26,359,1459832400";
   d="scan'208,217";a="15091714"
From: Mike McDuck <mmcduck***@outlook.com>
To: "buggln***@gmail.com" <buggln***@gmail.com>
Subject: New Update!
Date: Tue, 24 Apr 2016 08:59:23 -0700
Importance: Normal
MIME-Version: 1.0
X-OriginalArrivalTime: 24 Apr 2016 15:59:24.0506 (UTC)
FILETIME=[3E1ACBA0:01D1B5D5]
```

2. Identify targeted assets and potential risky connections
   - Search in Splunk/SIEM for the IoCs identified (source email and/or domain) to see how many mailboxes were targeted

Profiling IP/DNS/Phones

3. Obtain intelligence around the IPs involved
   - Select IPv4 addresses
     - Enrich them with Virustotal Address Risk Score
     - Map to ISP/Hosting with AbuseIPDB
     - Use Farsight Passive DNS to identify related DNS names



Data Integrations Used:

- Abuse IPDB
- Farsight Passive DNS
- Splunk
- Standard Transforms
- VirusTotal Public API

Use Case 3: Profiling Threat Actors

Context:

Our Cyber Treat Intel team wants to generate Intelligence about potential threats impacting our company. We specifically want to build a threat actor profile using social media intelligence.

Goal:

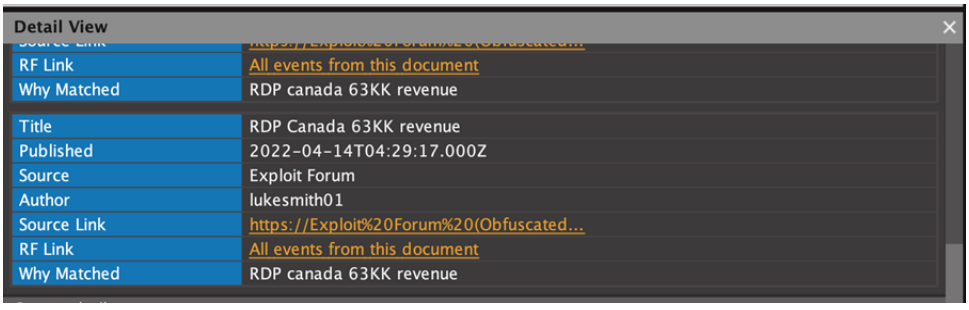
Understand our adversaries and the current and upcoming risks.

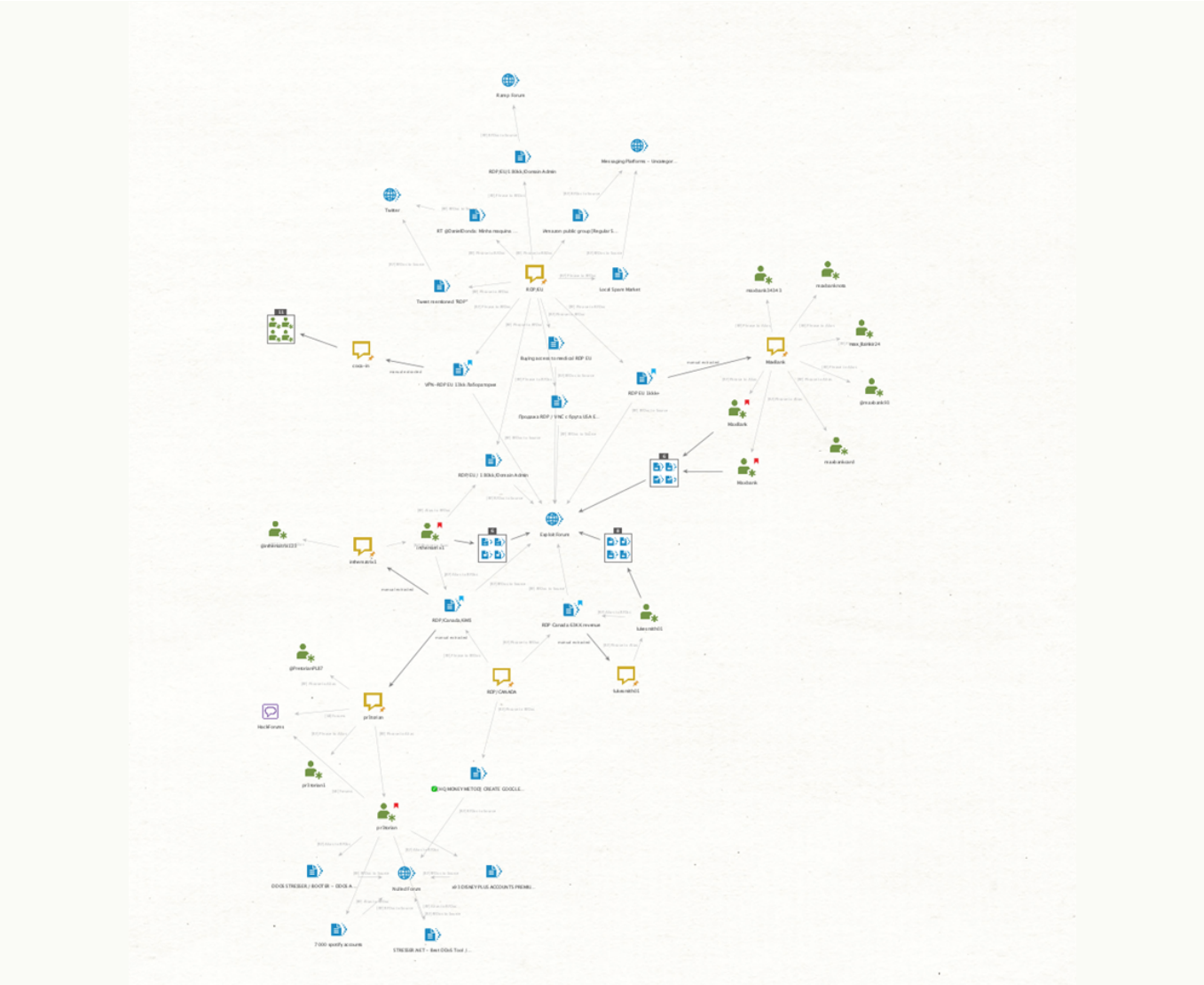
Starting Points:

1. Countries where the company has its HQ and subsidiary

Playbook:

1. 1. Paste the Phrase Entities containing the country names—in our case RDP/EU and RDP/Canada—onto your Maltego graph
2. Select the Phrase Entities and pivot to RF Docs using the Recorded Future Transform
   - [RF] To RF Doc
3. Select the RF Doc Entities and pivot to their sources using the Recorded Future Transform
   - [RF] RFDoc to Source
4. Select the RF Doc Entities from plausible sources like forums known for hacking activities
5. Extract the post author name from Detail View Pane and paste them as Phrase Entities to the graph
6. Link the nicknames manually to their original RF Doc Entities
7. Select the Phrase Entities and search for related aliases
   - [RF] Phrase to Alias
8. Select the most relevant Alias Entities and search for other RF Docs using the Recorded Future Transform:
   - [RF] Alias to RFDoc
9. Select the newly appeared RF Doc Entities and find out in which forums the nickname also appear
   - [RF] RFDoc to Source
10. Review if users appearing in different forums are using the same usernames and if there is overlap of goods that they are advertising.
11. To verify and find intelligence from other sources, select the all Phrase Entities containing a nickname and pivot to other forums using the Silobreaker Transform
    - [SB] Forums
12. Review the results and understand how this could be a risk or threat to your organization





Required Hub Items:

- Recorded Future
- Silobreaker

Use Case 4: Attacks and TTPs Analysis

Context:

Our Cyber Treat Intel team wants to generate Intelligence about previous incidents and find overlapping intelligence with publicly documented samples.

Goal:

The Cyber Threat Intelligence team needs to profile similar working malware with current and past behaviors of the adversaries.

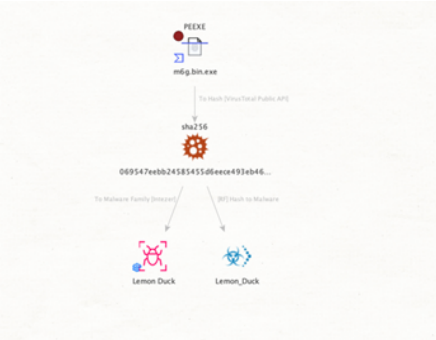
Starting Points:

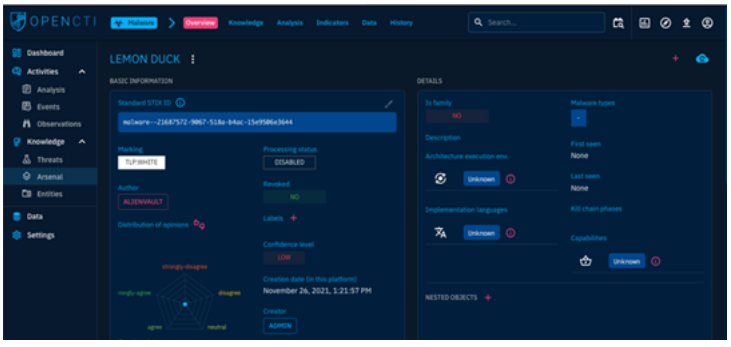
Hashes of faced attacks in our case we assume that we're hit by a crypto miner malware.

Playbook:

We start with the information that was provided by the IR team and want to verify with publicly available sources which malware type in the incident was used. To do so, we copy paste the sha256 hash to the canvas.

1. Select the hash entity and run:
   - To VirusTotal File [VirusTotal Public API]
   - [RF] Hash To Malware
   - To Malware Family [Intezer]

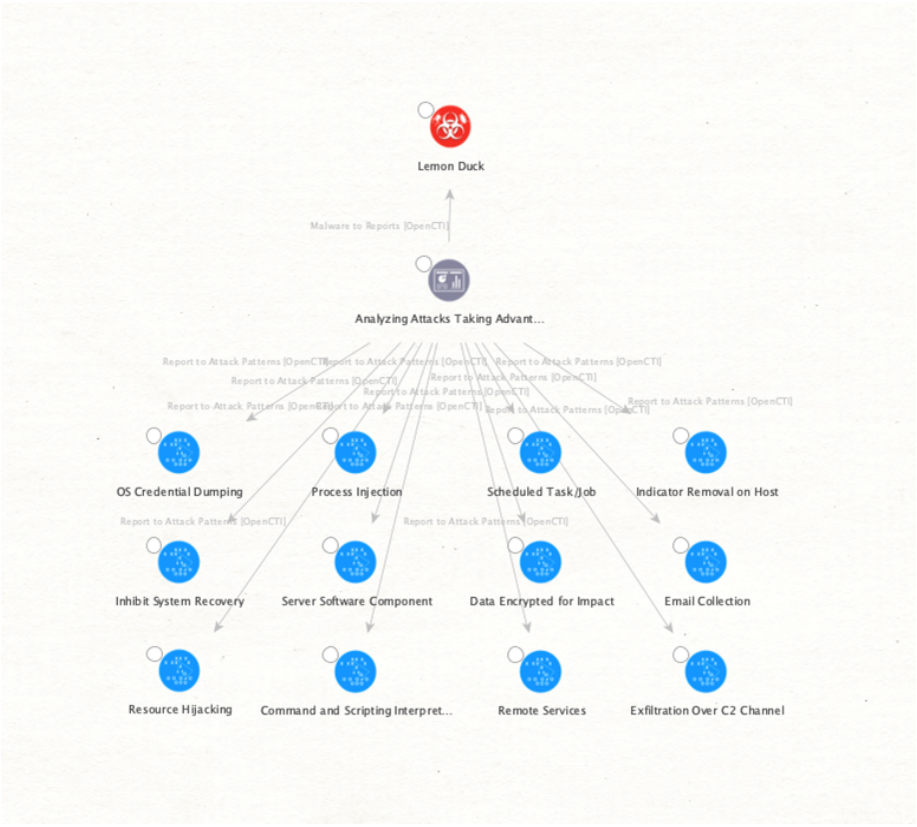




2. Get information from OpenCTI

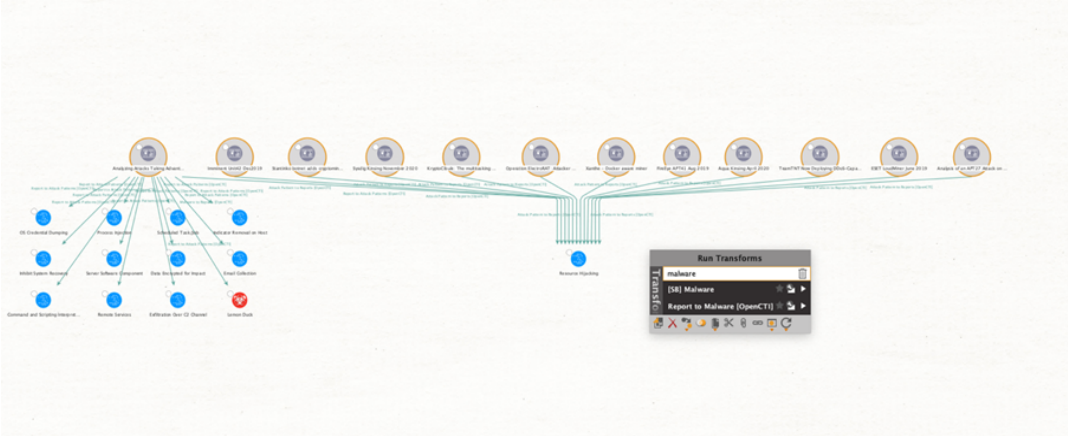
We copy the id “malware--21687572-9067-518a-b4ac-15e9506e3644” (please be aware could be different in your case) and paste it to the graph. We then run the following Transforms:

- To Details [OpenCTI]
- To Reports [OpenCTI]
- Report to Attack Patterns [OpenCTI]

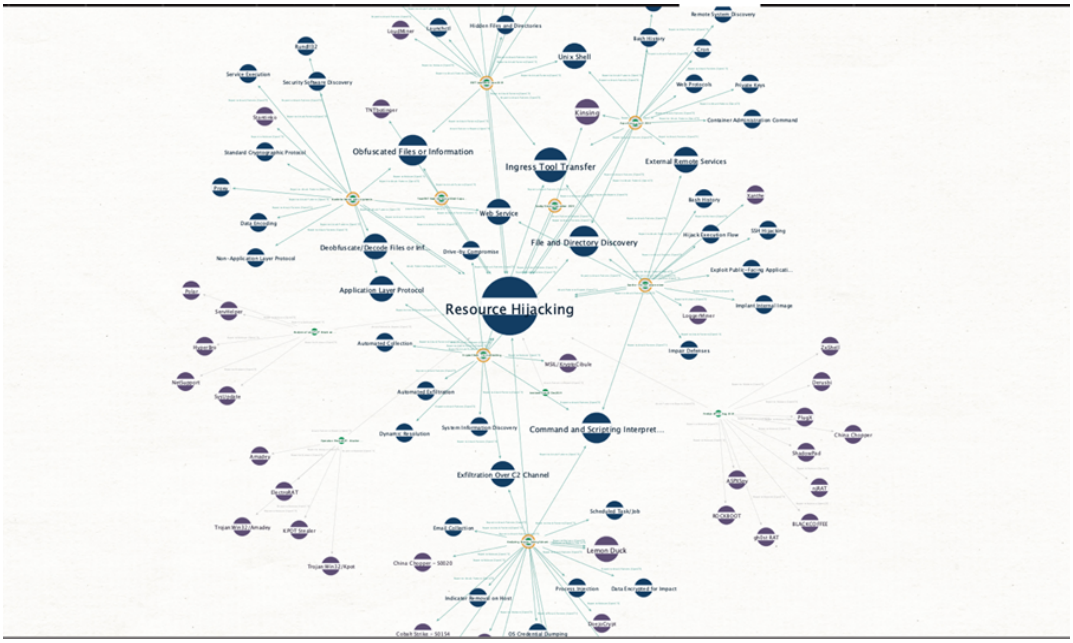


And from the results, we run the following Transforms:

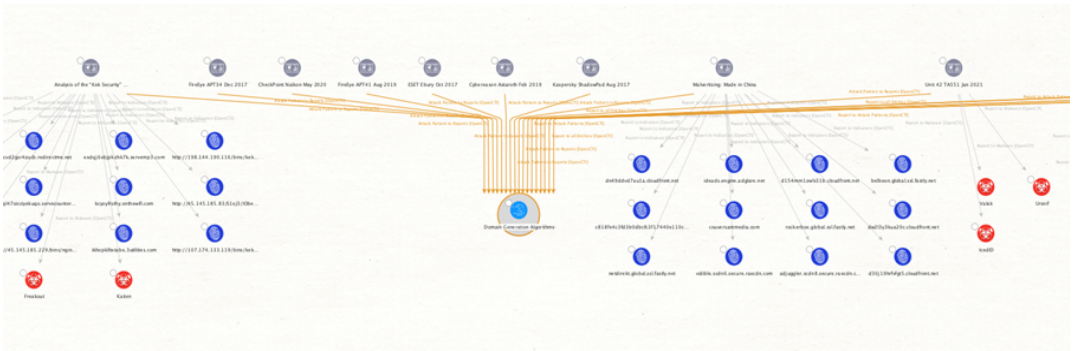
- Attack Pattern to Reports [OpenCTI]
- Report to Malware [OpenCTI]



Finally, we run the Report to Attack Pattern [OpenCTI] Transform again to acquire the following results:



This will provide an overview and overlap of our single sample to other malware that is known to make use of resource hijacking. With the OpenCTI integration, you can also easily search the other way around and start from a technique to malware. For instance, from DGA (Domain Generation Algorithms) to malware and IoC's.



Required Hub Items:

- OpenCTI
- Intezer Analyze
- Recorded Future
- VirusTotal

Use Case 5: Vulnerability & Attack Surface Assessment

Context:

- Threat Intel team is aware of a new vulnerability that could potentially impact in assets belonging to the organization
- Notification comes from an stakeholder including an intel provider, CSIRT/CERT alerts or just the vendor who pushed it to the organization

Goal:

Evaluating a new vulnerability considering a vendor/intel report. This implies, on one hand, to identify some IoCs of ongoing malicious activity to be considered for proactive protection and detection. On the other hand, we want to identify which assets based in public scanners and/or internal ones are exposed to it

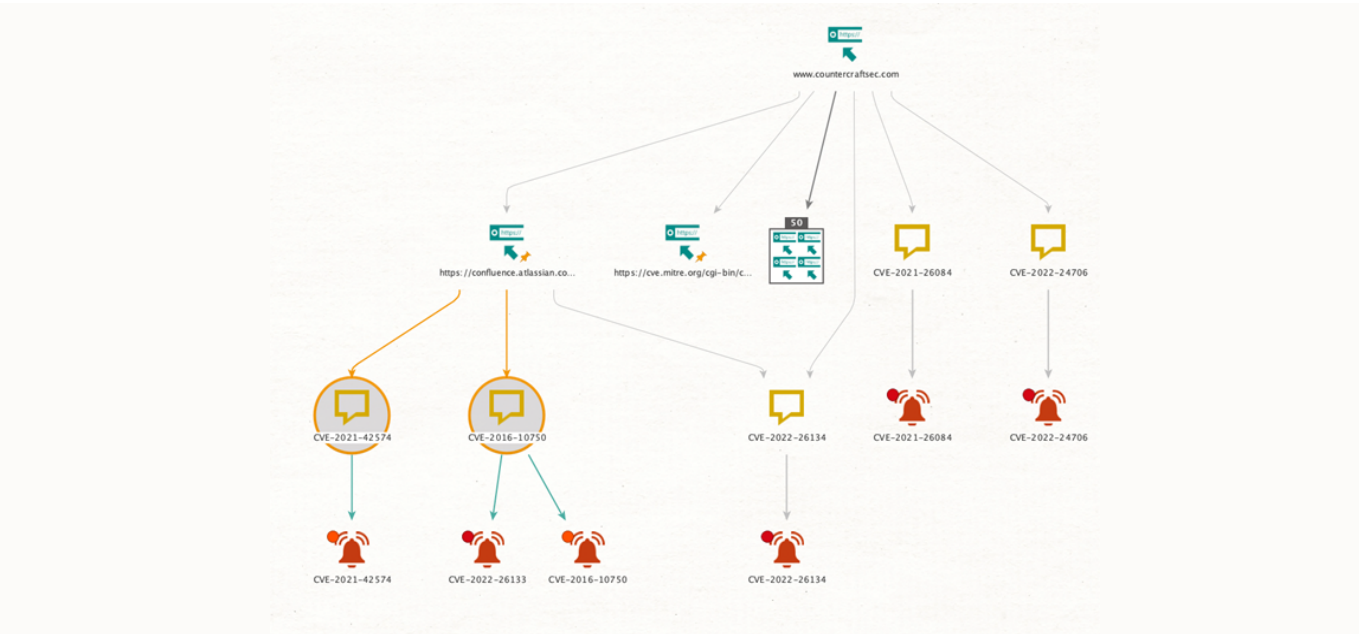
Starting Points:

- Product Security IRT (PSIRT) vulnerability alert website (Maltego URL Entities)
- List of the software names affected (Maltego Phrase Entities)
- Social Media, blog posts or notes (Maltego URL Entities)

Playbook:

Explore The Vulnerability Report To Obtain Links And Cves

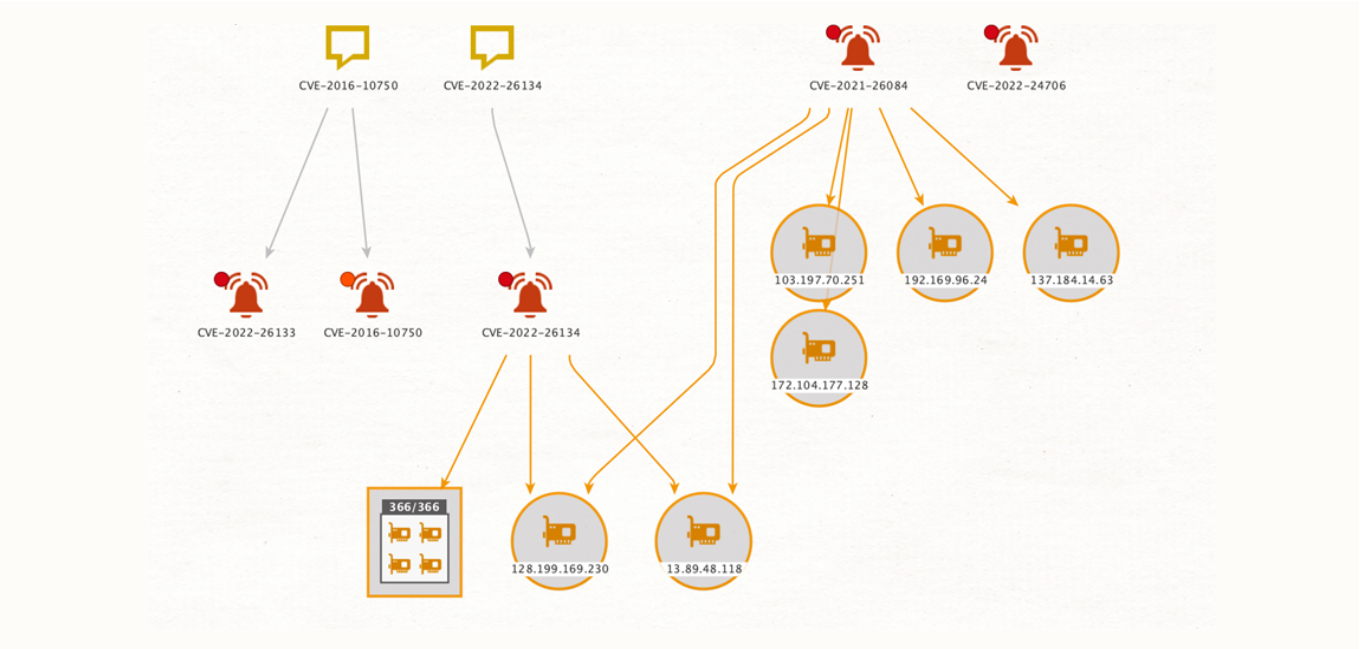
1. Paste the PSIRT URL onto a Maltego graph
2. Select the URL Entity and pivot using Maltego Standard Transforms to obtain related URLs
   - To Links found on website
3. Pin some of the websites linked to a vendor or relevant intelligence providers, such as Atlassian, Cisco, and Microsoft, and bookmark the Entities with a color
4. Select the relevant links bookmarked before and pivot using Standard Transforms to obtain other CVEs as Phrase Entities:
   - To Regex Matches [Found on web page] CVE-\d{4}-\d{4,7}



5. Select the CVE Phrase Entities and pivot using NIST NVD:
   - Search for CVEs [NIST NVD]

Identify Digital Assets Linked With Active Offensive Activity

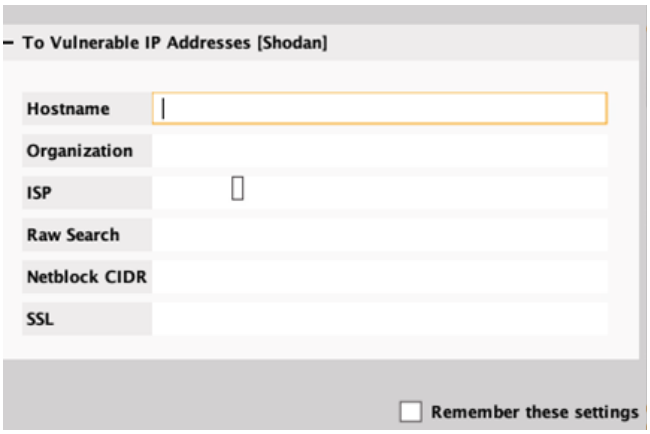
6. Select CVEs and pivot using GreyNoise Enterprise:
   - To Scanning IPs CVE [Greynoise]



7. Enrich or curate the provided IP addresses with other Maltego Hub items
   - AbuseIPDB
   - VirusTotal
   - MISP
8. Provide the identified IoCs to your Protect/Detection functions to contain and/or detect potential campaigns or attacks

Identify Our Digital Assets Exposed By The Vulnerability

9. Select CVEs and while running the Shodan Transform, Include your organization name and/or netblocks CIDR in the appropriate fields
   - To Vulnerable IP Addresses [Shodan]



10. Identify which metadata fingerprints a service with the vulnerability exposed, i.e. Strings, HTTP information, etc.
11. Use identified fingerprints for dorking via Standard Transforms using a Phrase Entity
    - site:companydomain.tld AND intitle:"STRING" AND inurl:"text"
12. Select websites identified and pivot to URLs using Standard Transforms
    - To URLs [Search Engine Results]
13. Select URLs and pivot to technologies using Standard Transforms
    - To Web Technologies [BuiltWith]
14. Curate the results to verify which websites belong to your organization and are really using the vulnerable technology

Internal Verification Of Vulnerable Assets

15. Use your custom local Transform to verify in your internal assets databases (CMDB) which systems have the vulnerable software
16. Use your custom local Transform to complete a vulnerability scan over them to verify if they are online and vulnerable

Data Integrations Used:

Maltego Hub Items

- Standard Transforms
- NIST National Vulnerability Database (NIST NVD)
- Shodan
- Greynoise Enterprise

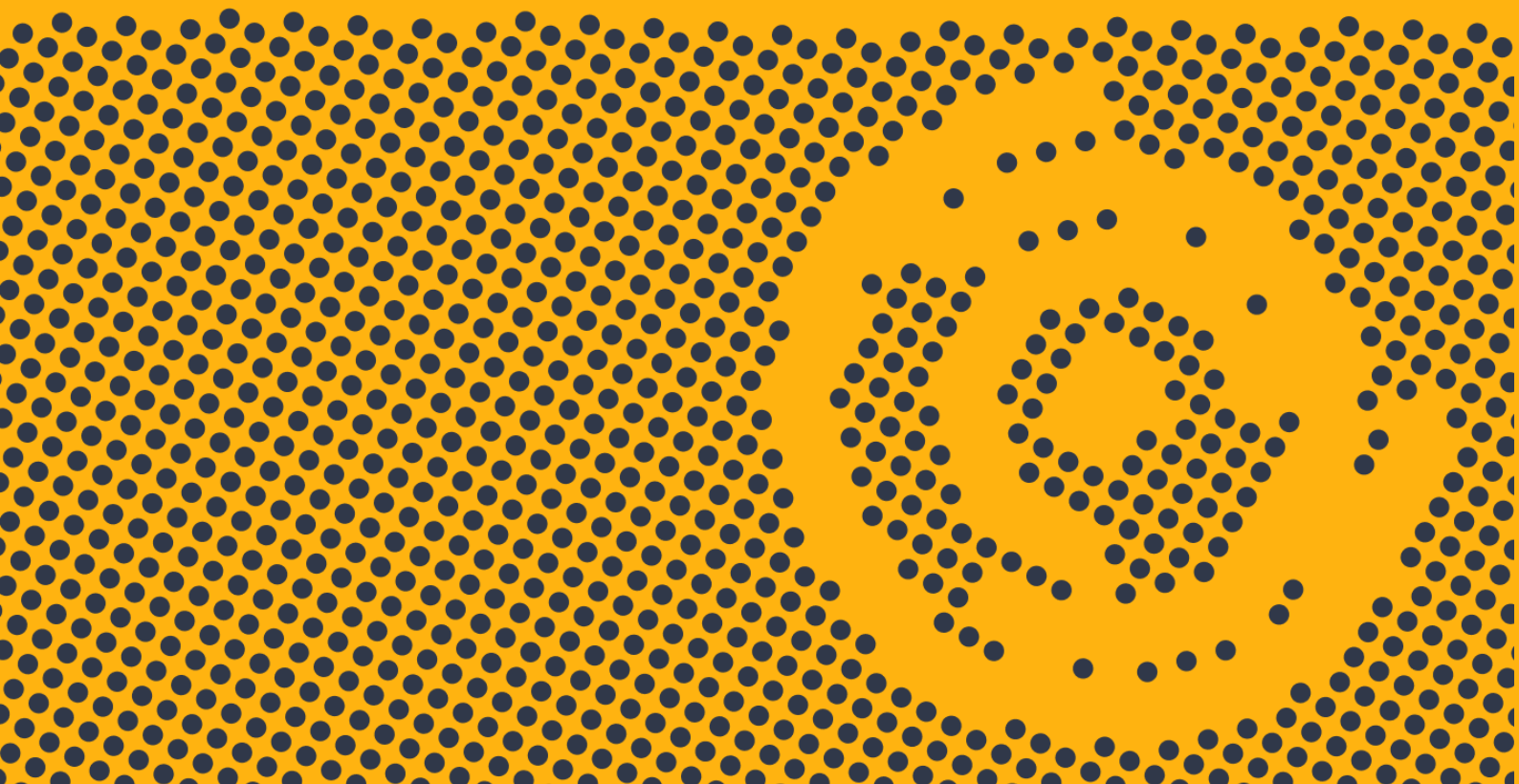
Internal / Custom Integrations

- Internal CMDB
- Nessus Scanning

For more information, please visit
maltego.com

Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable. With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape. Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over 30 data partners, a variety of public sources (OSINT) as well as your own data. Our different Desktop Client versions, data sources, and server solutions enable you to tailor Maltego to your specific needs in terms of data access, functionalities, and security requirements.

MINE • MERGE • MAP / DATA



Maltego Technologies GmbH
Address: Paul-Heyse-Strasse 29, 80336 Munich
Email: contact@maltego.com
Phone: +49-89-24418490

MALTEGO