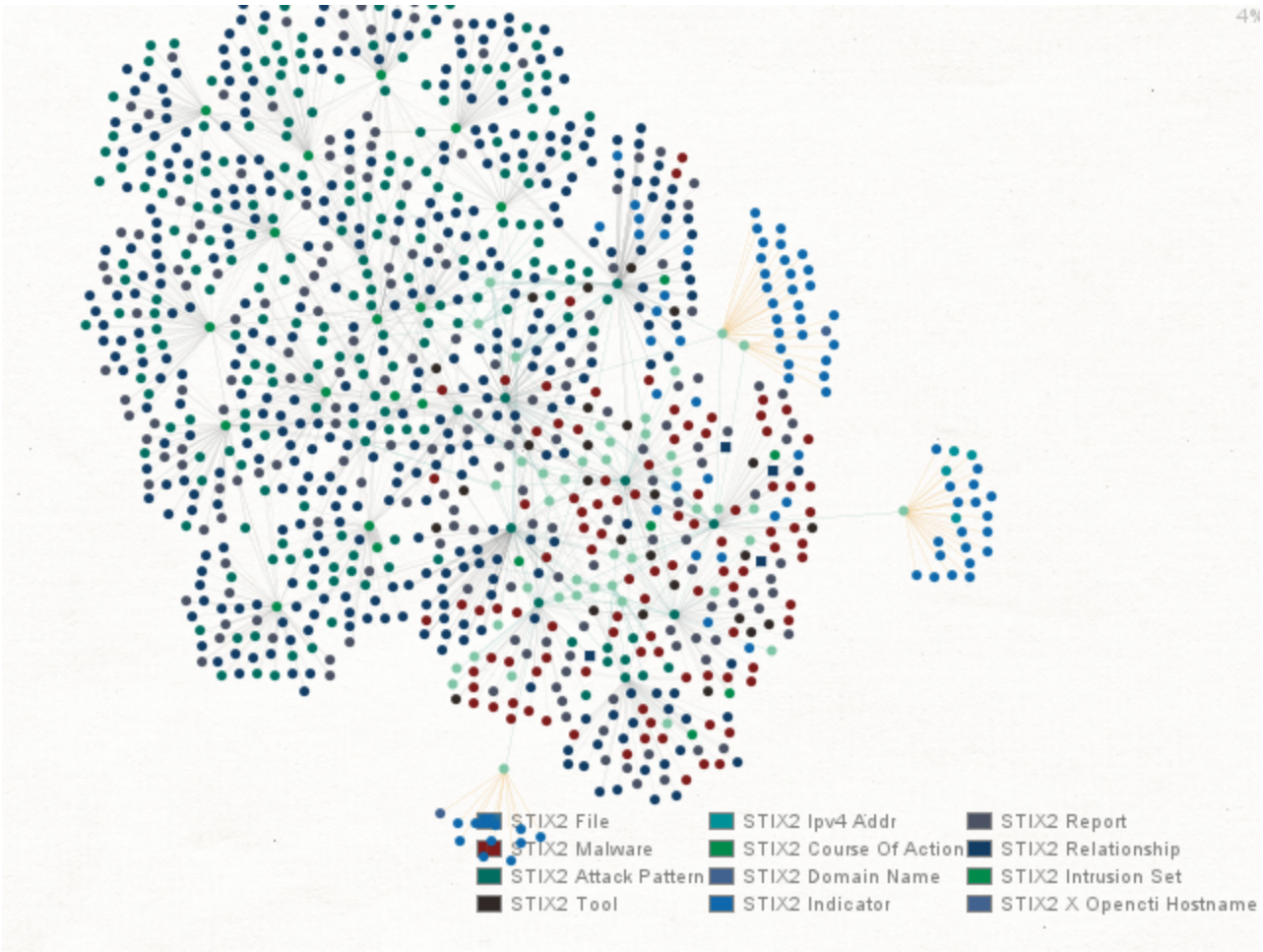
Investigating TA413 Threat Actor Group Using OpenCTI in Maltego

maltego.com/blog/investigating-ta413-threat-actor-group-using-opencti-in-maltego/



29 Apr 2021 Tutorial Cyber security investigation

Maltego Team

In Part 1 of the article series, we announced the new release of Maltego's STIX2 Entities and OpenCTI Hub item. **In this article, we will demonstrate how investigators can use STIX2 Entities and OpenCTI in Maltego by taking a look at TA413.**

Threat Actors have been steadily improving their Tactics, Techniques, and Procedures (TTP) over the last few years, allowing them to carry out complex campaigns against multiple targets with the same effort that it used to take to attack a single target.

A recent example is the "Solorigate" attack (commonly known as the SolarWinds Hack), which spread to the company's clients and went undetected for months. The attack allowed hackers to spy on private companies like the elite cybersecurity firm FireEye and important

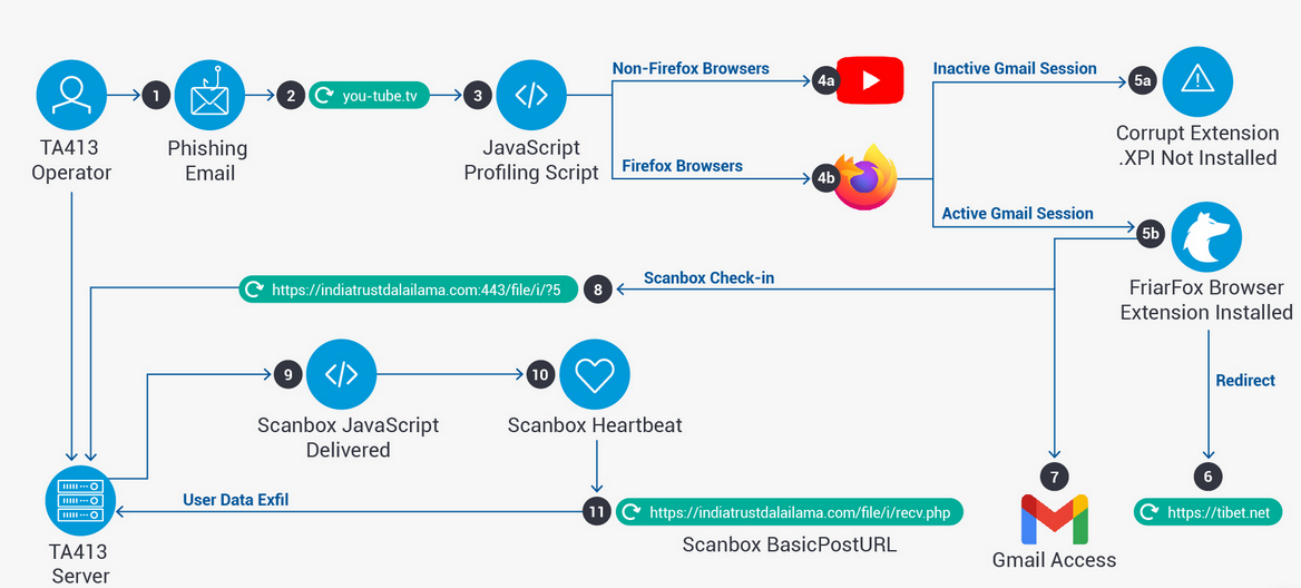
US Government entities, including the Department of Homeland Security and Treasury Department.

Introduction 🔗

We will use the public demo instance of OpenCTI (https://demo.opencti.io), which is open to the public. If you don't have an OpenCTI instance, all you need to do is create an account here to start exploring right away. Once you have registered, you will also get an API key that you can use with Maltego if you want to follow along.

What or Who is our target for this investigation? 🔗

A few weeks ago, Proofpoint published an excellent article about TA413 and how this group was targeting the Tibetan diaspora. The image below illustrates the attack vectors used by the TA413 group.



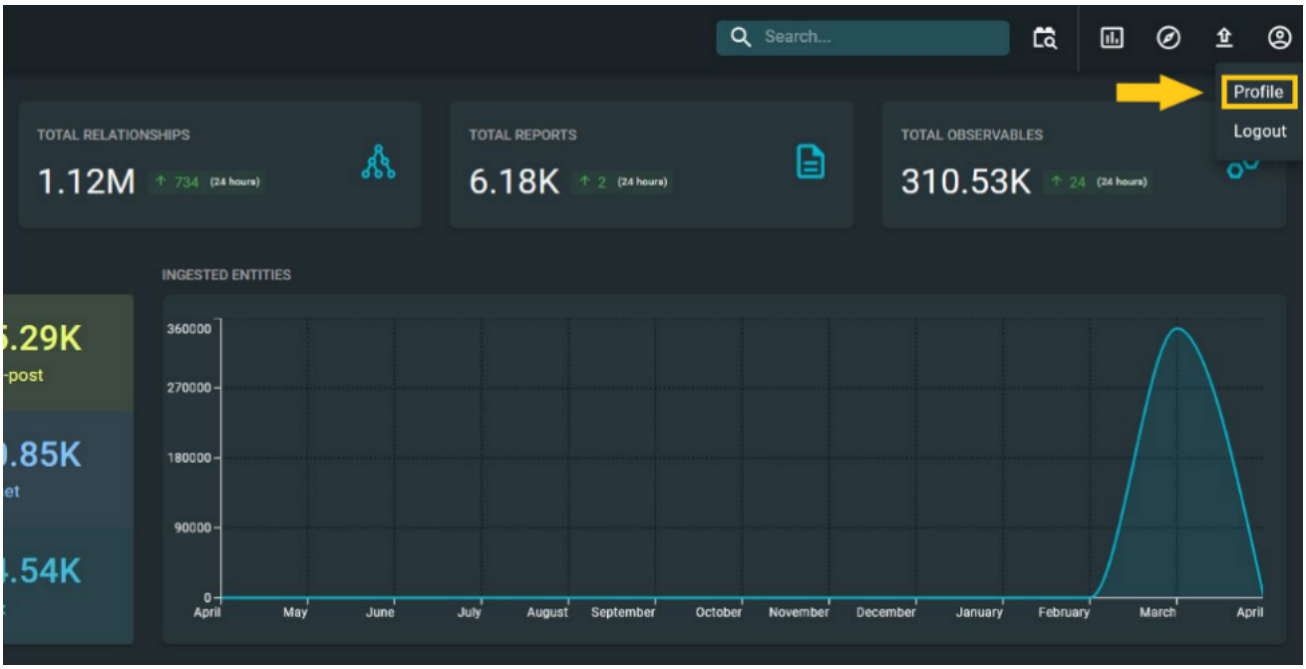
The APT group known as TA413 has been associated with the Chinese state. While they are regionally known for their attacks against the Tibetan diaspora, their worldwide renown came about in March 2020 when they began targeting Western economies that were suffering under the effects of COVID-19 to collect intelligence.

Based on Proofpoint's article, we will now attempt to map TA413's infrastructure while trying to find any additional IOCs (Indicators of Compromise) that the author of the article may have missed.

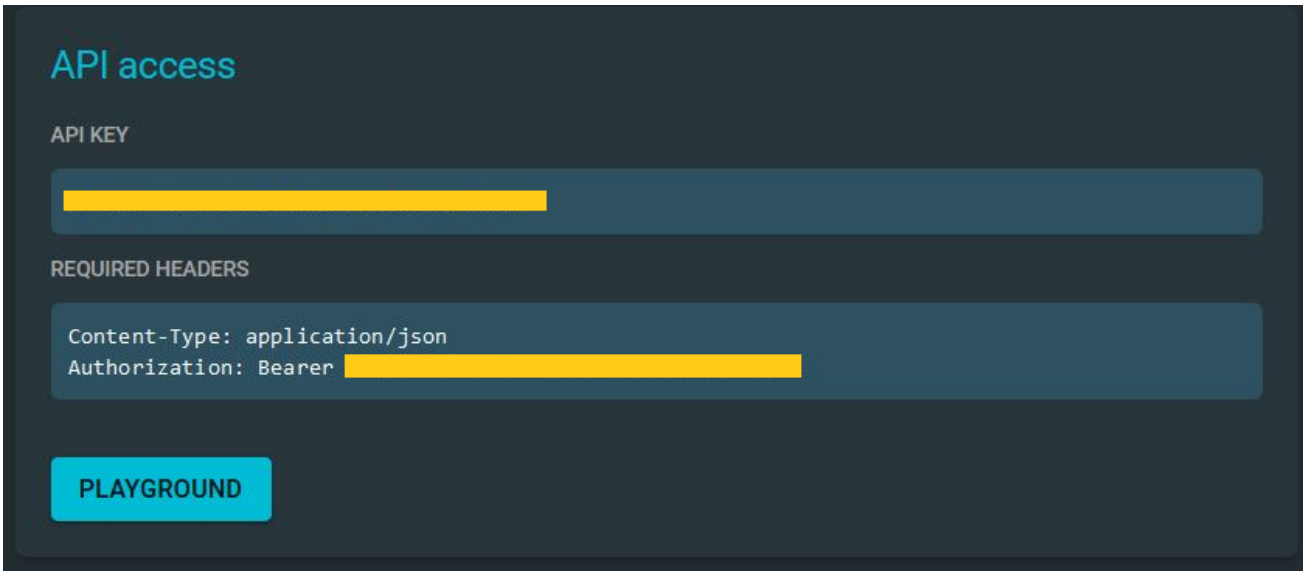
Let's Make Sure We Have Everything We Need for Our Investigation! 🔗

As previously mentioned, once you have created an OpenCTI account, you can sign into their demo instance to retrieve your API Key. The first thing you will see is a friendly dashboard, but to get the API key, all you need to do is go to the upper right corner of the

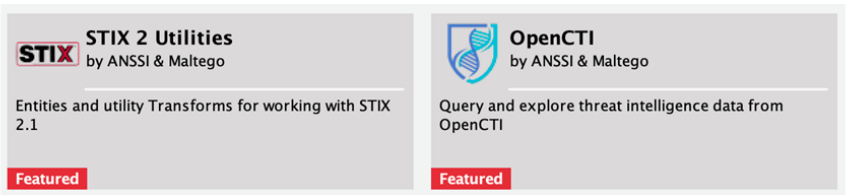
screen, click on the Account icon and then select the Profile option from the submenu.



The API key should be visible at the bottom of the screen. Remember that this key can often change with the demo instance, which means you will need to check your API key whenever you want to use it; otherwise, you may face issues with Maltego.



You will also need to install the OpenCTI Transforms and the STIX2 Utilities in Maltego.



Once you click on Install on the OpenCTI Hub item, you should get a prompt window asking you for the below information.

- OpenCTI Instance URL: Enter https://demo.opencti.io for the demo instance. In case you are using your own instance, you should add said URL here.
- OpenCTI API Token: Provided with your OpenCTI profile.
- Verify SSL (true or false): In this case, we will be using SSL, so you should enter "true".

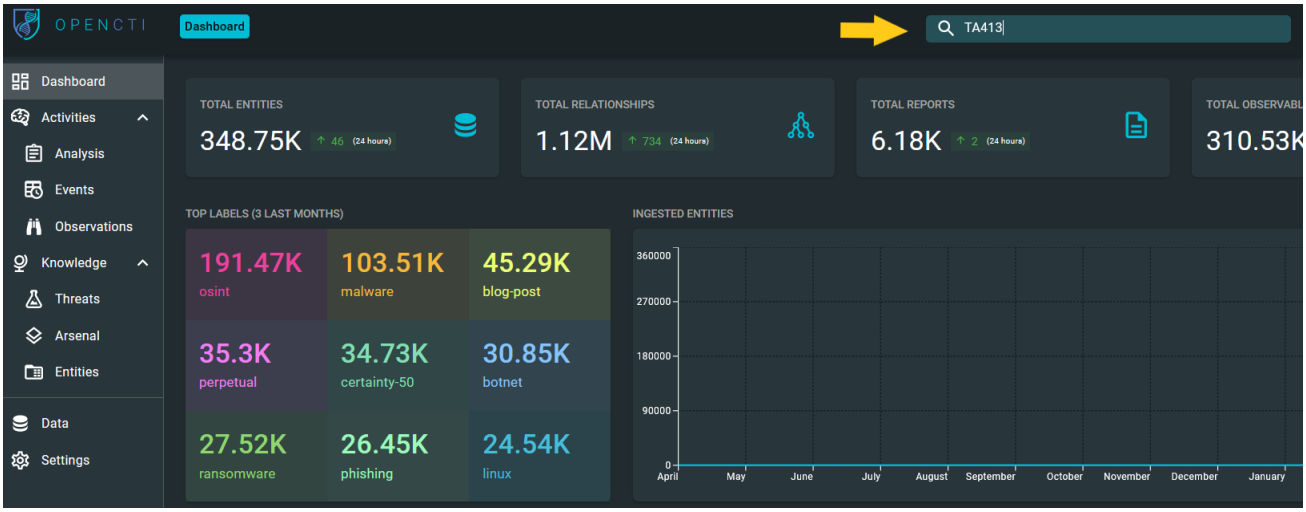
The installation for STIX2 Utilities is straightforward for this item since it does not require any custom settings.

We should be good to go now!

Investigating TA413 Using Maltego and OpenCTI🔗

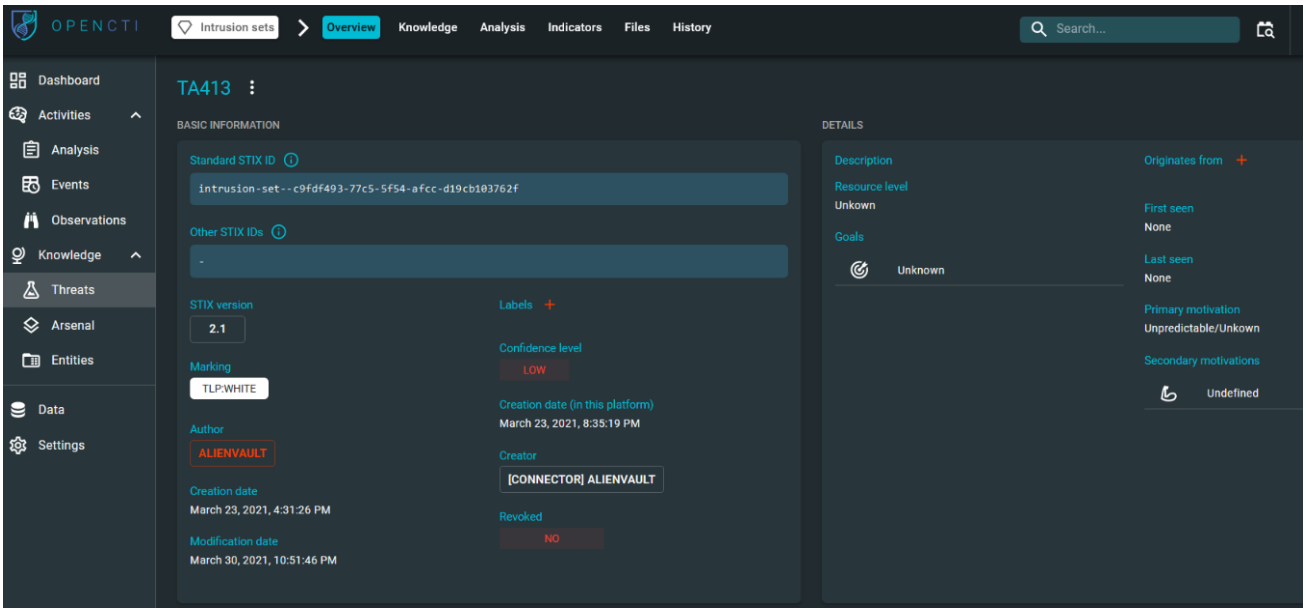
Finding Relevant Intelligence in OpenCTI🔗

We will start our investigation by looking into OpenCTI and seeing what general information we can find about TA413. To do so, we can use the search box on the upper right corner of the main dashboard, type in "TA413", and hit Enter.

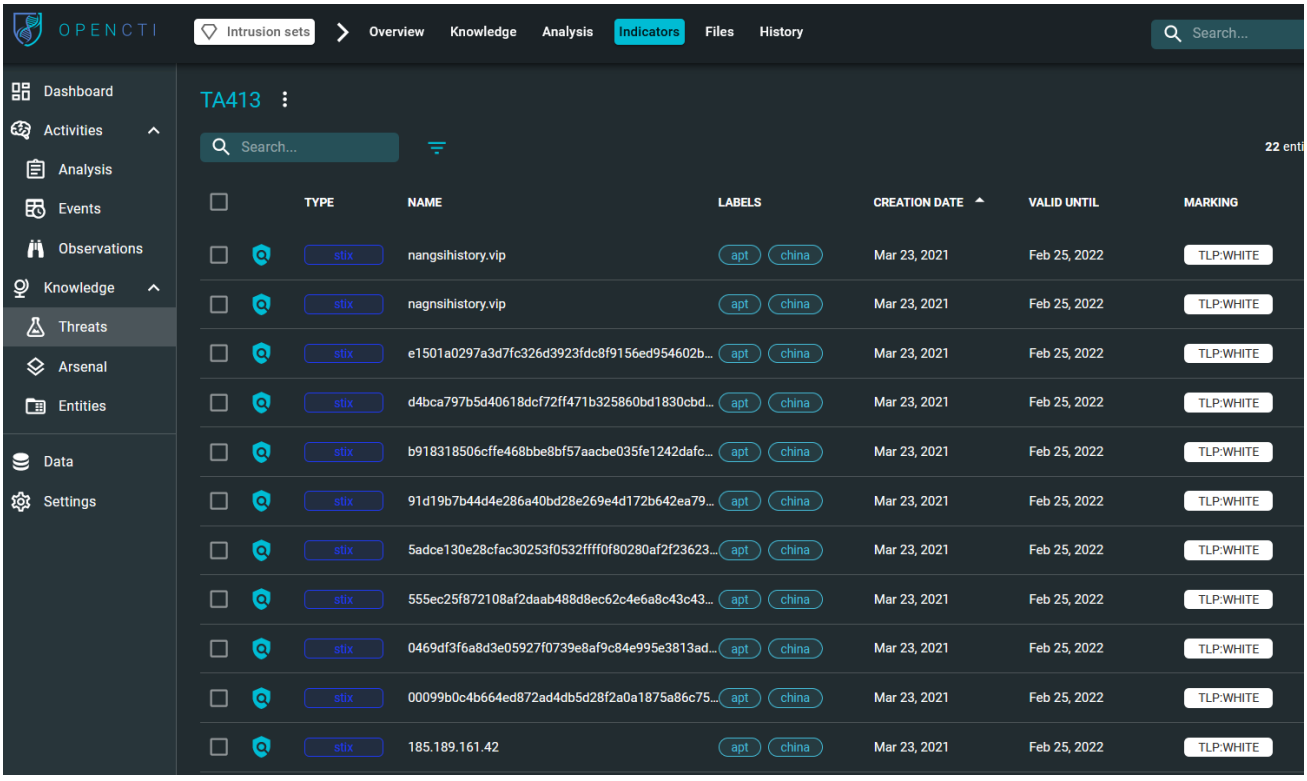


Below is a snapshot of the information found in OpenCTI for this Threat Actor, where we noticed that OpenCTI categorized this information as an "Intrusion Set."

According to Oasis, an Intrusion Set is a STIX2 Domain Object that represents a grouped set of adversarial behaviors and resources with common properties that are believed to be orchestrated by a single organization.

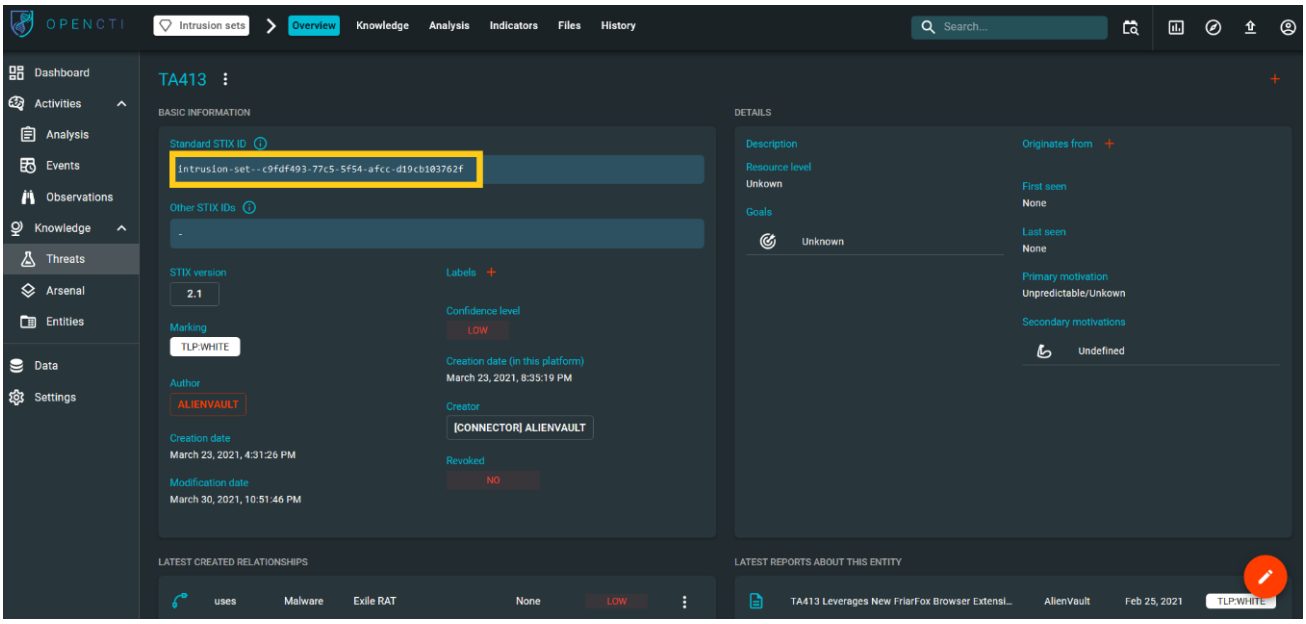


Let's now look for any observables for this intrusion set under the "Indicators" tab. As we can see, OpenCTI provides a comprehensive list of IOCs associated with TA413—some of them mentioned in Proofpoint's article—which will be helpful in our investigation.



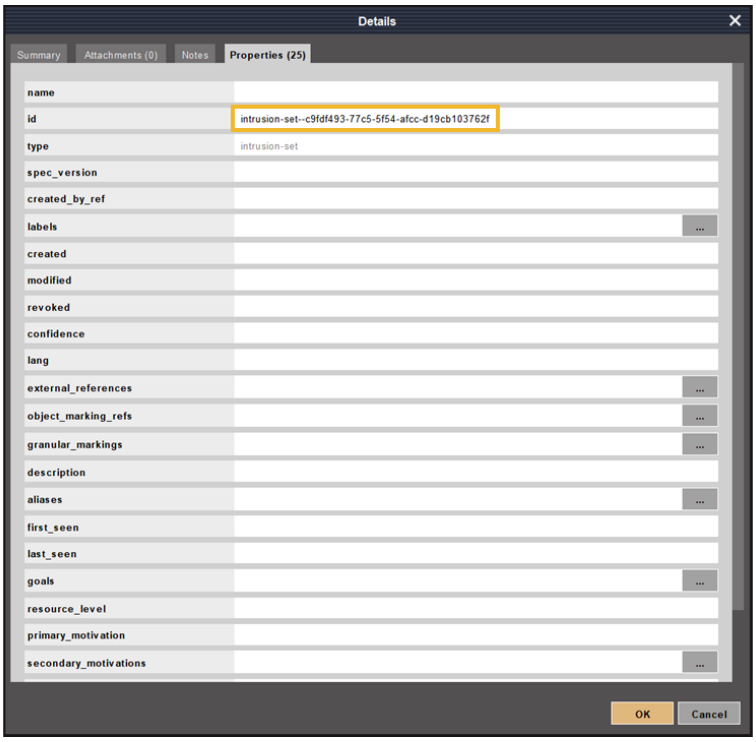
Enriching the STIX Standard IDs Using Maltego 🔗

We can now pivot into Maltego. To do so, let's go back to OpenCTI's overview tab and copy the STIX Standard ID associated with this Intrusion Set so we can drop it into Maltego.

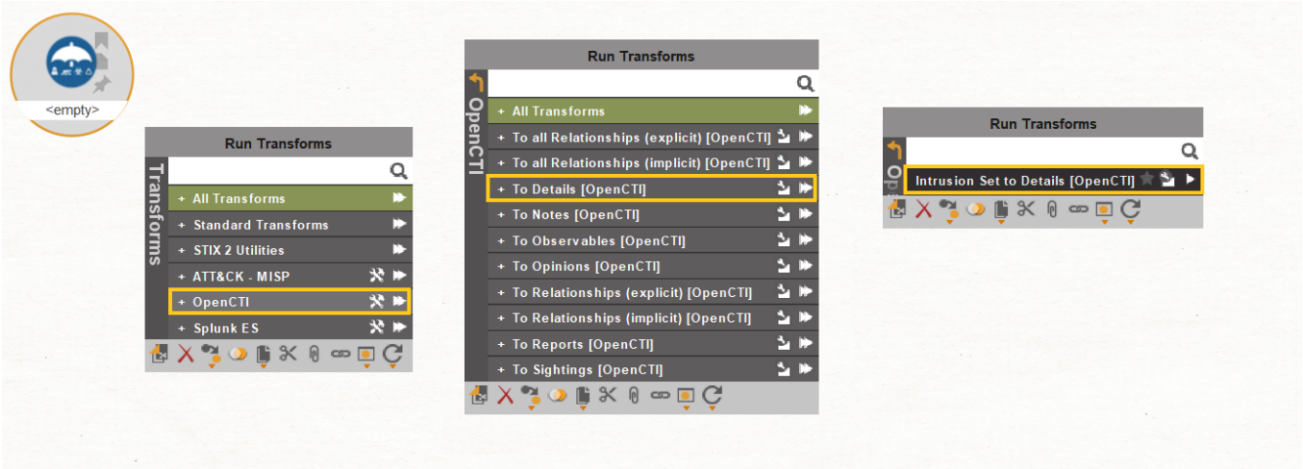


Maltego does a great job understanding the type of Entity that we need, as it automatically creates a **Maltego.STIX2.intrusion-set** Entity for us upon dropping the ID.

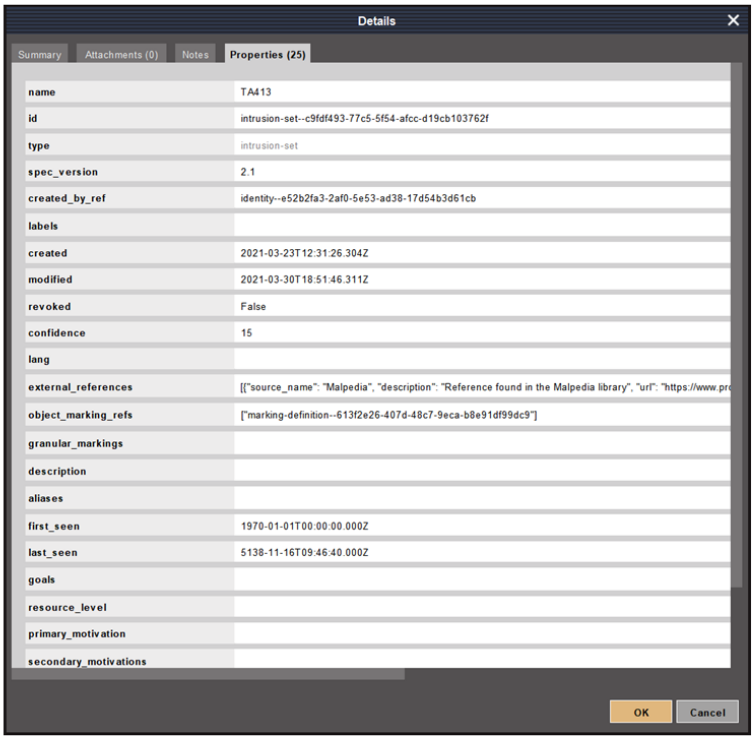
But wait, why is the new Entity showing up as ? It is important to note the Entity itself is not entirely devoid of information; if you double-click on it, and go to the Properties tab, you will find that the id and type fields are populated. We still need to query OpenCTI to retrieve the remaining details associated with the STIX Standard ID.



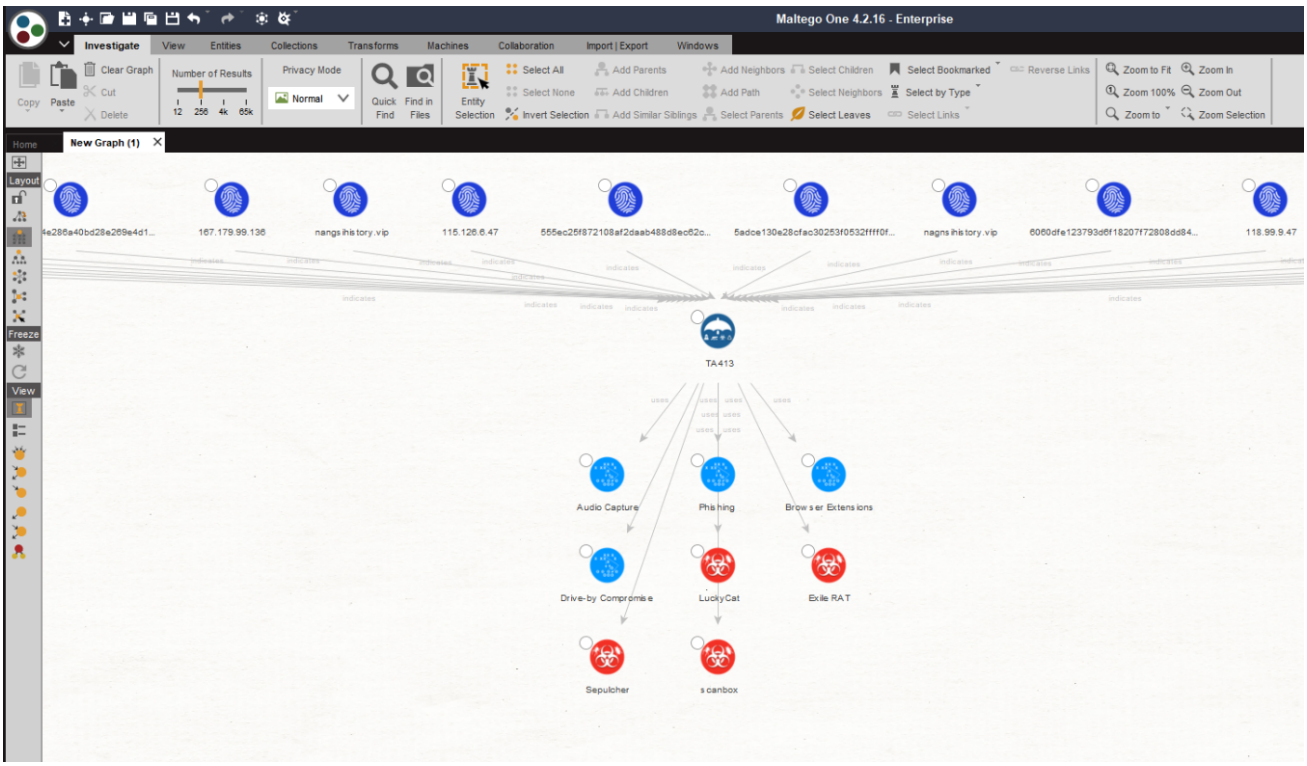
Let's close the Details window and request the details of this intrusion Set from OpenCTI. We can do this by selecting the **Maltego.STIX2.intrusion-set Entity** and running the **Intrusion Set to Details [OpenCTI]** Transform in the **To Details [OpenCTI] Transform set** of the OpenCTI Hub item.



Now we can see an updated Entity in our graph and its populated properties in the Detail View.



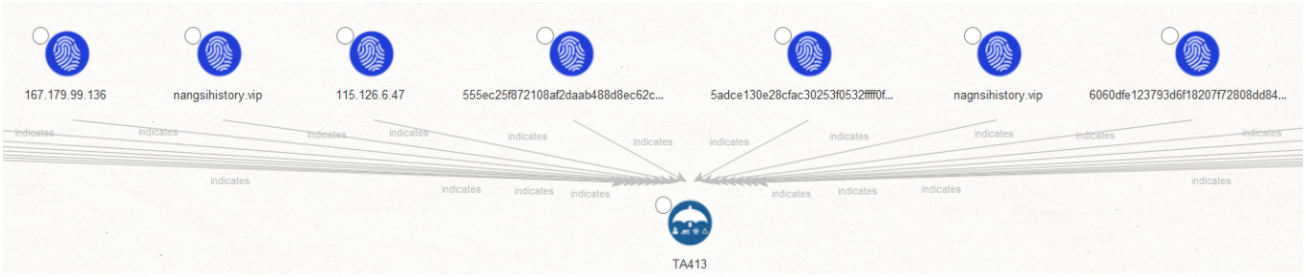
That was simple, but we should be able to get more details about this intrusion Set from OpenCTI. Let's select the Maltego.STIX2.intrusion-set Entity and run the **Intrusion Set to all Entities [OpenCTI]** Transform.



In just a few clicks, Maltego retrieved all the details from OpenCTI and pulled them into our graph. Let's take a minute to review these new Entities, which are based on and closely resemble the STIX2 Entities original Objects.

	Attack Pattern	A type of TTP that describe ways that adversaries attempt to compromise targets.
	Malware	A type of TTP that represents malicious code.
	Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.

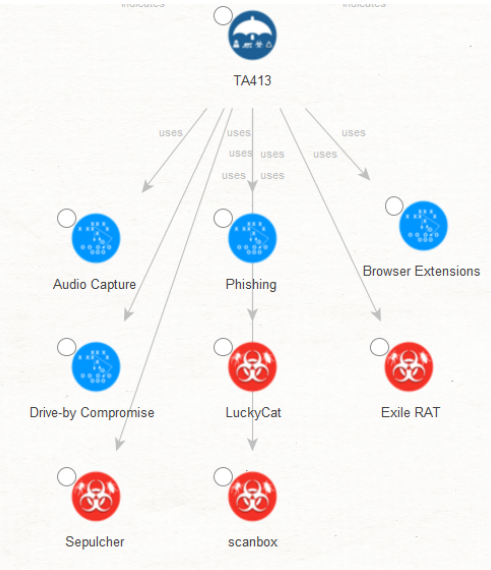
Let's take a minute to understand what we have found so far. In the upper half of our graph, where we can see that all Entities are STIX2 Indicator Entities and contain the same observables that we saw under the Indicators tab of OpenCTI.



We can also see an "indicates" label next to the links between the Indicator Entities and the Intrusion Set Entity, which follows the STIX2 Relationship Objects (SROs) structure.

Image from Oasis

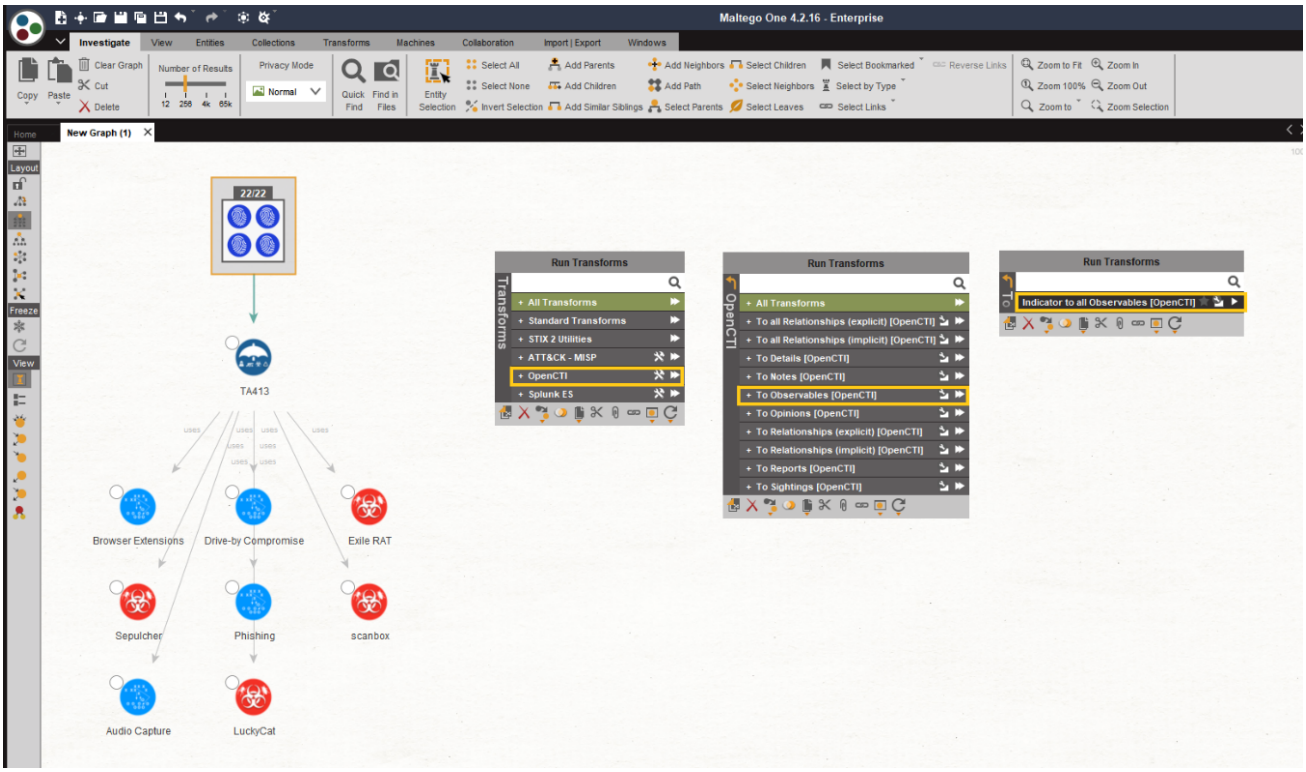
In the lower half of our graph, we see a few new **maltego.STIX2.attack-pattern** and **maltego.STIX2.malware** Entities, which will help us understand the Tactics and Techniques used by the TA413 group.



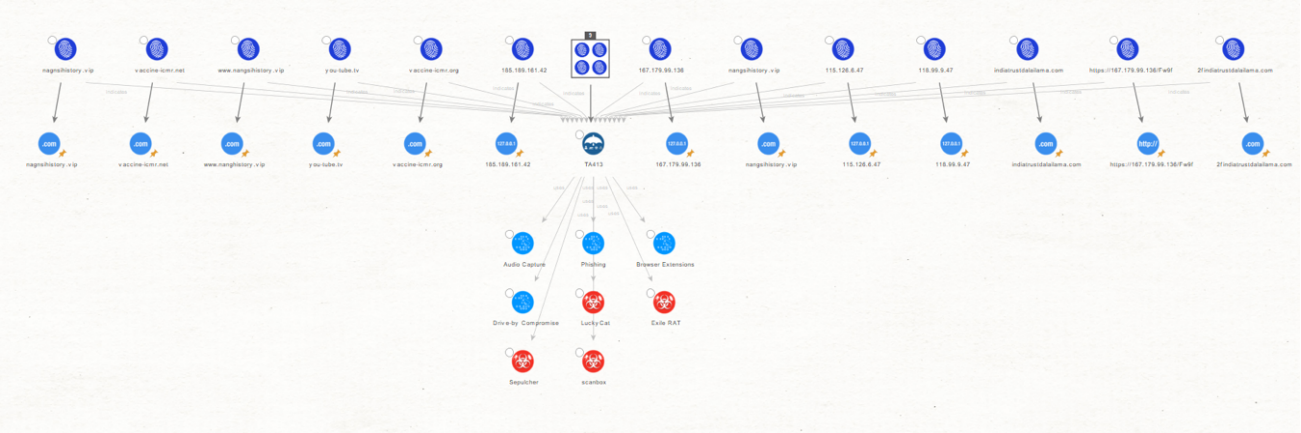
We now have an excellent idea of how this Threat Actor operates and its infrastructure, but let's see how we can leverage some of our other Transforms to further enrich the information we have on TA413's infrastructure.

First, we use the Collections feature of Maltego to simplify our graph by grouping Entities based on their type, grouping all the Observable Entities into a single box.

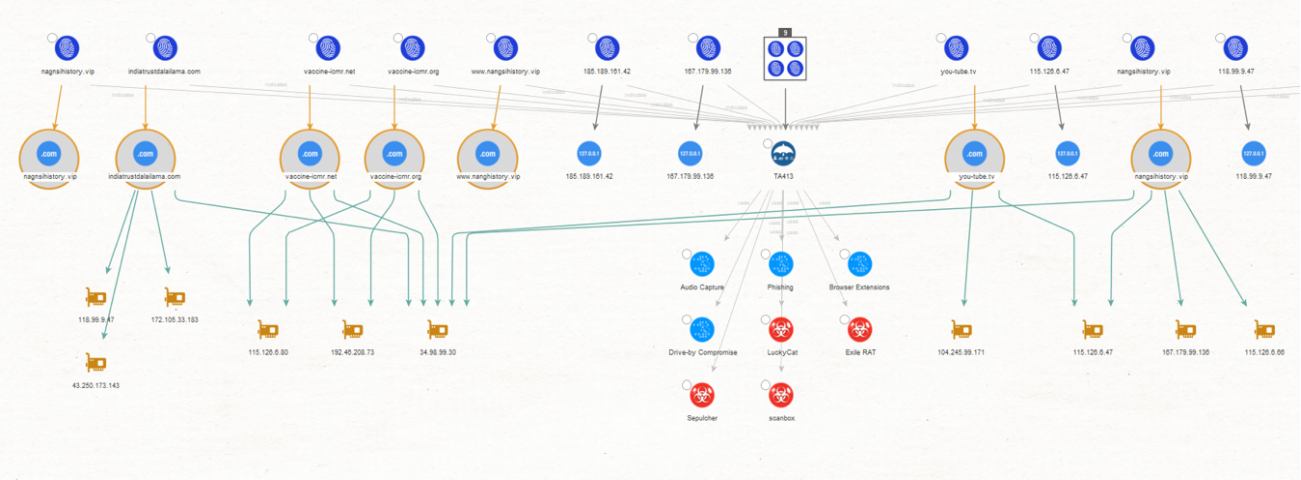
We then select the Collection Node and run the **Indicator to all Observables [OpenCTI]** Transform. This will allow us to use our existing Transforms to find additional infrastructure associated with TA413 and not listed in the report nor OpenCTI.



As we can see, Maltego returned a few STIX2 Domain Name Entities to most of the selected Observables.



We will select the STIX2 Domain Name Entities and run the **To Resolved IPs [VirusTotal Public API]** Transform to see if VirusTotal knows about any additional IP addresses associated with these domains.

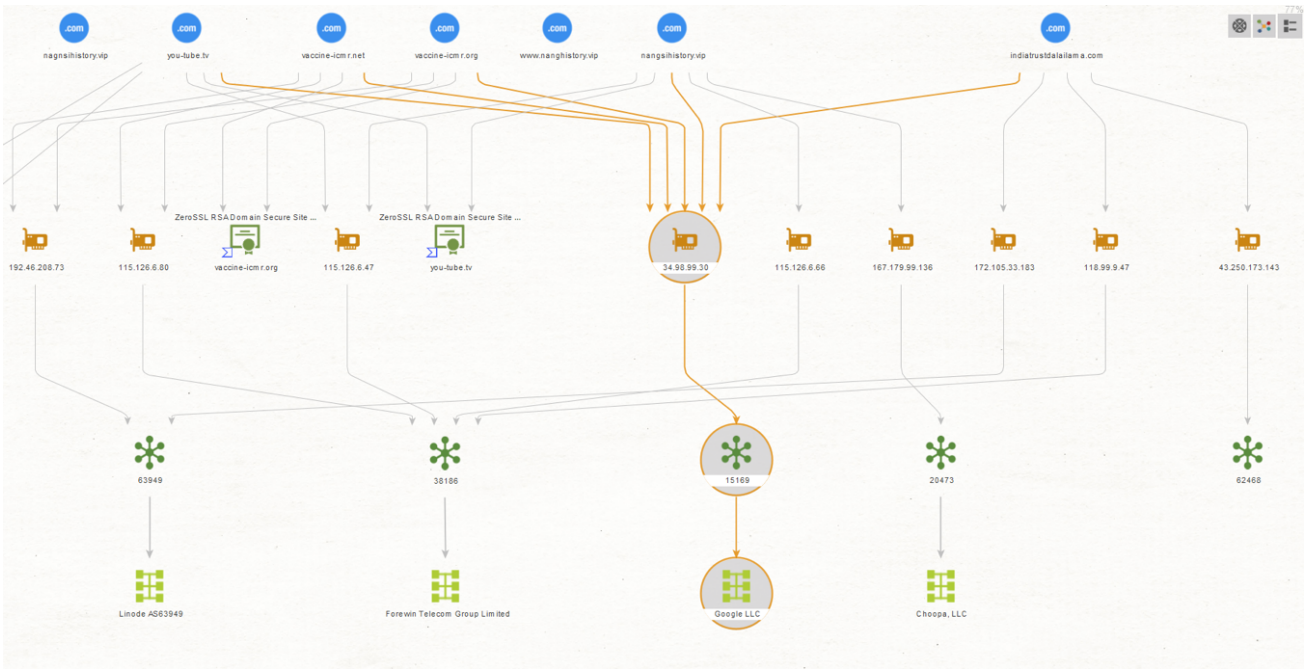


It looks like we have found some additional IP addresses. We will try to further expand our results by looking for suspicious file names or hashes associated with TA413.

First, we will check if any of the IP addresses belong to prominent hosting providers, as these tend to be shared or reassigned rather quickly, and we could save time and focus our attention on relevant IOCs by ignoring these noisy IP addresses for now.

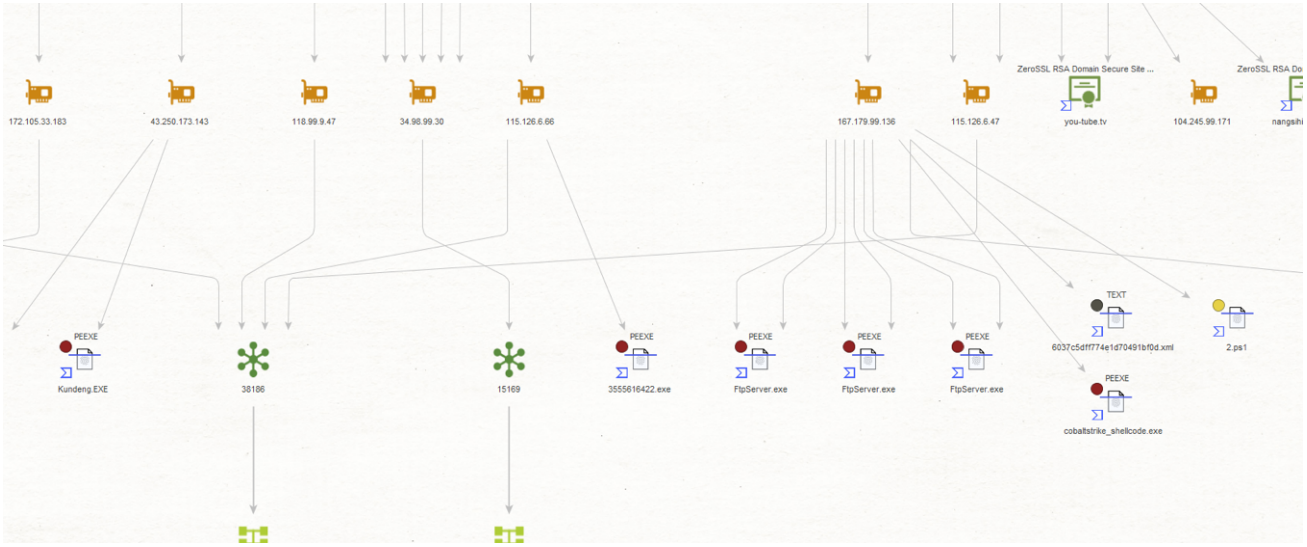
Selecting the IP Address Entities, we run the **To AS Number [VirusTotal Public API]** Transform and on the resulting AS Entities, the **To Network [Peering DB]** Transform.

We can immediately observe one specific IP associated with Google. We will exclude this IP from our next step.

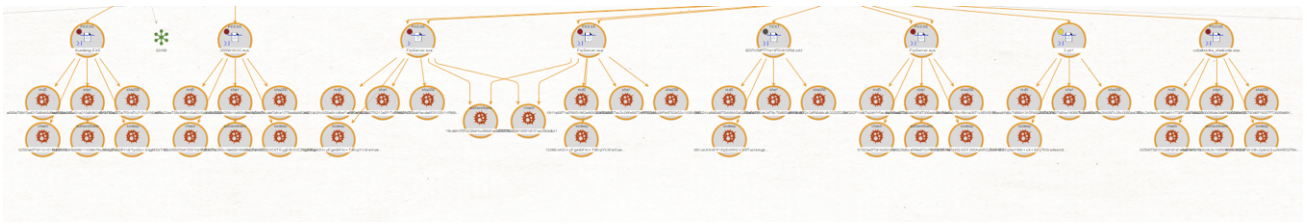


We will select the IP Address Entities again and run the **Communication Relationships [VirusTotal Public API]** Transform.

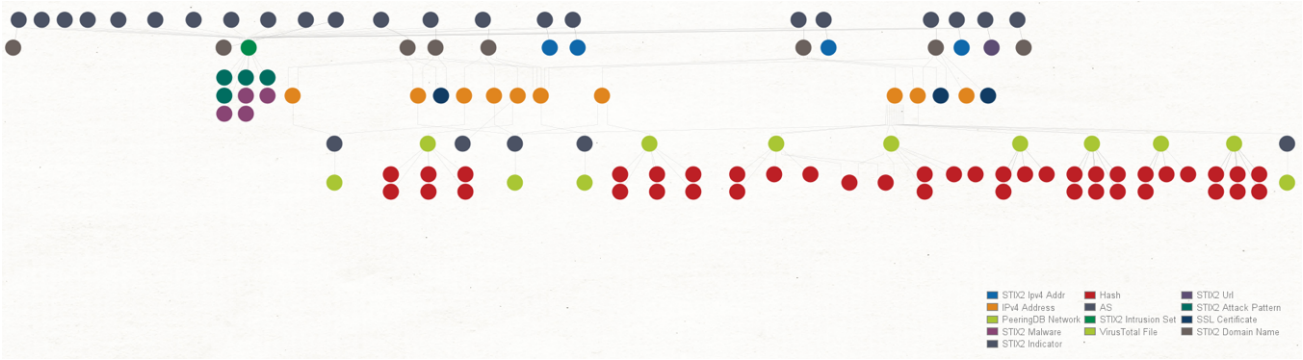
In this case, VirusTotal returned a set of malicious files, including one linked to Cobalt Strike, a threat emulation software heavily abused by threat actors.



Finally, we can run the **To Hash [VirusTotal Public API]** Transform to retrieve the hashes associated with these files. These will be of great help as we can use them for blocking and alerting any sightings of these in our network.



And that wraps up our OpenCTI Transform demonstration!



Start Using the Maltego OpenCTI Transforms to Unleash Your Threat Intelligence Investigations 🔗

Throughout this investigation, we found additional infrastructure used by TA413 for their campaigns, such as domains, IP addresses, file names and hashes.

These are very relevant as we can now use them to feed our Threat Intelligence and Threat Hunting processes and also for blocking and alerting purposes.

Maltego elevates your investigations to the next level by allowing you to visually analyze what the attack looked like as it took place and can help you to find patterns and additional infrastructure used by these attackers, all within a single interface.

Don’t forget to follow us on Twitter and LinkedIn and sign up for our email newsletter to stay updated on the latest news, tutorials, and events.

Happy Threat Hunting!