Open-Source Tool Report: Maltego

Introduction

Using search engines and grid techniques to gather information is a time-consuming process. Maltego is an open source cyber intelligence tool that saves considerable time by automating the extensive information gathering process. The graphical representation of the detected information greatly helps in identifying relationships between entities. Therefore, it can be used by a wide audience such as security professionals, penetration testers, forensic investigators, etc., providing support in various fields.

Maltego can be used to integrate information collection sources for threat intelligence. It also graphically displays information from these sources. This gives threat intelligence analysts a unique opportunity to correlate disparate indicators.

1. What is Maltego?

Maltego is a comprehensive tool that facilitates real-time data mining and information gathering processes, provides a holistic view of the data by presenting this collected information in a visual graph in a node structure, identifies connections, and can be used for link analysis. It increases access to confidential information thanks to a powerful search capability.

Maltego can easily combine data from various sources using Transforms. Through the Transformation Center, information from more than 30 data partners, various OSINT sources and investigator's data can be integrated.

Different versions of Maltego, data integrations, deployment and infrastructure options, support services and learning and training formats provide an extremely useful tool for information gathering.

In general, Maltego has two types of discovery options: infrastructural discovery and personal discovery. infrastructural discovery covers an area that includes name servers, email exchanges, DNS information such as DNS-to-IP resolution. Personal discovery includes personal information such as email addresses, phone numbers, profiles on social networks and friend connections.

Maltego uses a secure HTTPS connection, sending client data in XML format to seed servers. On the server side, this data is processed and the results are transmitted to the Maltego client.

2. Maltego Use Cases

Maltego is one of the most advanced and useful information gathering software available today and has both active and passive information gathering features.

Passive Information Collection: It is a process that is carried out without direct interaction with target organizations or individuals while collecting information over the Internet. These methods include research conducted through search engines, Whois, DNS query sites and social media platforms.

Active Information Collection: Using the information obtained in the passive information gathering process, system scans are performed and weak points in the system are identified.

Maltego is not command-line based, using a visual interface and classifies the data it collects and presents it in a visual way.

Maltego can collect information on various topics:

- Information about the network infrastructure and network devices: IP addresses, DNS records, network interfaces, etc.
- Information related to e-mail addresses and e-mail servers.
- Information related to websites and domain names: Owners, hosting companies, history, etc.
- Social media profiles and associated information: Facebook, Twitter, LinkedIn, etc.

Maltego also has the following capabilities:

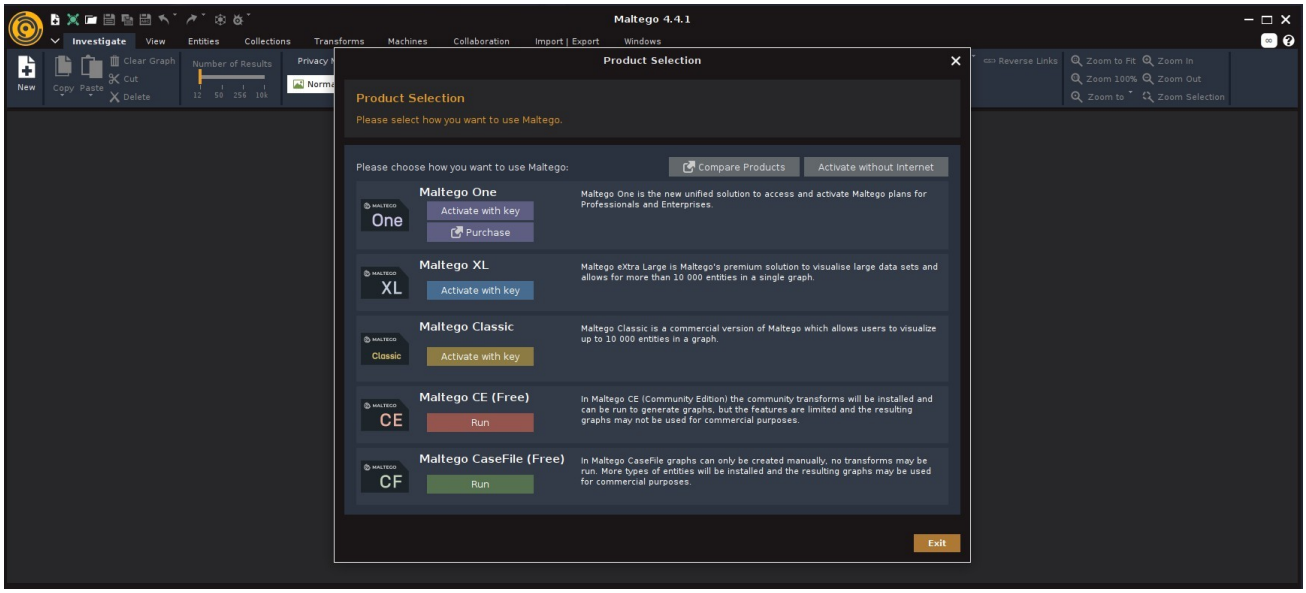
- Data visualization: Graphically visualize the collected information and analyze relationships.
- Integration capabilities: Collect and combine information from different data sources.
- Automated data collection and analysis: Automatically collect and analyze information relevant to a specific target.

The Maltego tool can also find the following information about a person:

- First name and other identification information associated with the surname: Email addresses, phone numbers, addresses, etc.
- Associated persons and organizations: Family members, business partners, employers, etc.
- Social media profiles and activities: Shares, followers, likes, etc. Work history and education information: Previous workplaces, educational institutions, graduation dates, etc.

The links between this data are found using OSINT techniques by querying many sources and extracting their metadata. The data is visualized in various graphs that allow information to be clustered to see the relationships between the data, thus discovering hidden connections.

3. Maltego Products



The app is one of the most detailed information gathering tools. The app is available in free and paid versions.

The different versions of Maltego offer various features according to users' needs:

Maltego One:

- A commercial version, designed for larger-scale research and working on large datasets.

- It can return more results in a query and can do larger graph visualizations.
- It can run more Transforms and has wider data integration than other versions.

Maltego XL:

- The most comprehensive and advanced version of Maltego.
- It is ideal for large-scale enterprise environments and can handle millions of entities and results.
- It is optimized for working on very large datasets and has the widest range of Transform and integration options.

Maltego Classic:

- It is one of the commercial editions and provides full access to OSINT Transforms.
- It can return more results in a query and perform more extensive searches.
- However, the number of results returned in a query is still limited and some advanced features are not available in this version either.

Maltego CE:

- Community edition available free of charge.
- It has basic OSINT (Open Source Intelligence) capabilities.
- It can use transformations and plugins released by community members.
- However, it can return a limited number of results per query and lacks some advanced features.

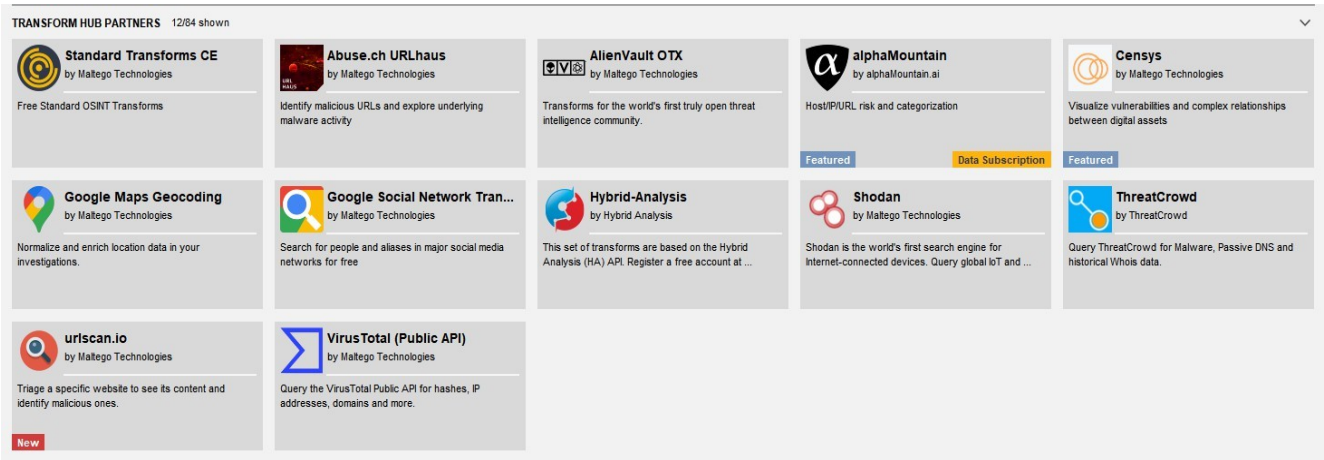
CaseFile: Free version for visualizing links in offline data and does not require the use of Transforms.

4. Using Maltego

The data that I will use in this research is the CVE-2023-22527 vulnerability. I did it on the domains in their IOCs. For the sake of being up to date I took into account the posts made in February. You can access the indicators I used from the links below.

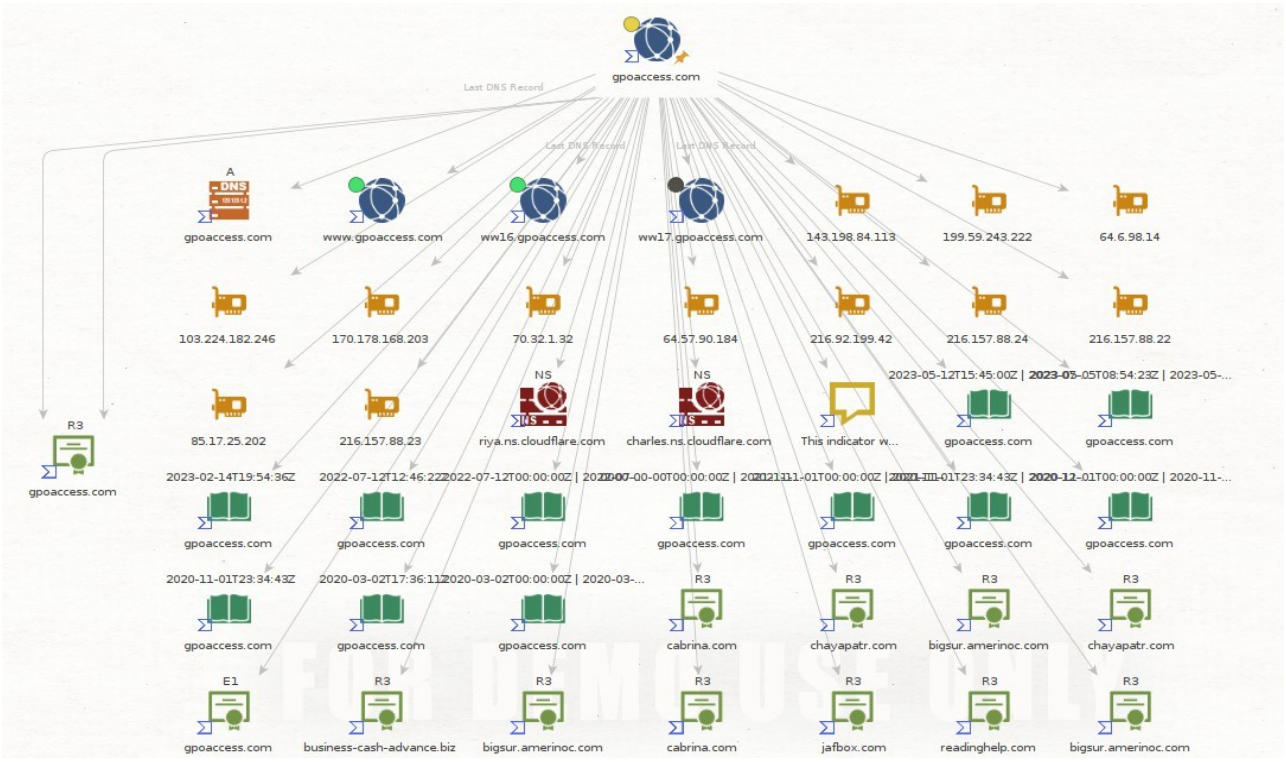
Modules Used

In my research, I used VirusTotal, Hybrid Analysis and AlienVault OTX modules on Maltego. For these integrations, APIs are needed on VirusTotal and Hybrid Analysis platforms. Integration can be easily realized with the API keys created. Other modules I use:

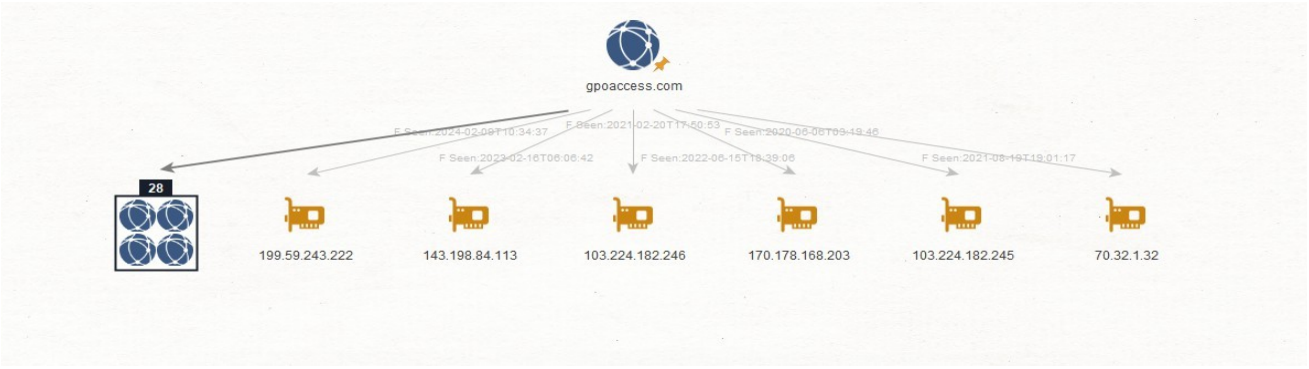


Details of the Research

- To analyze the domains in full detail, I first scanned the "gpoaccess[.]com" domain using the VirusTotal indicator.

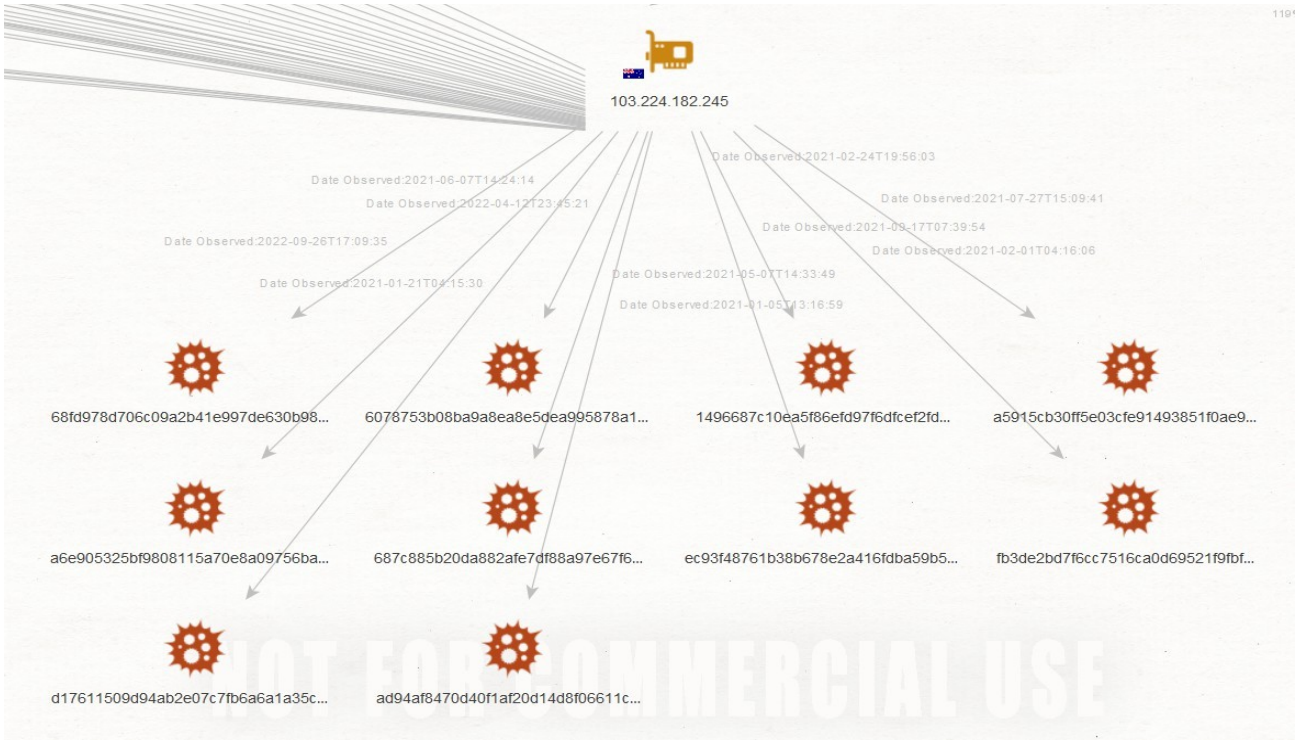


- When I do an IP search with the VirusTotal indicator, I see that it is associated with multiple IPs.

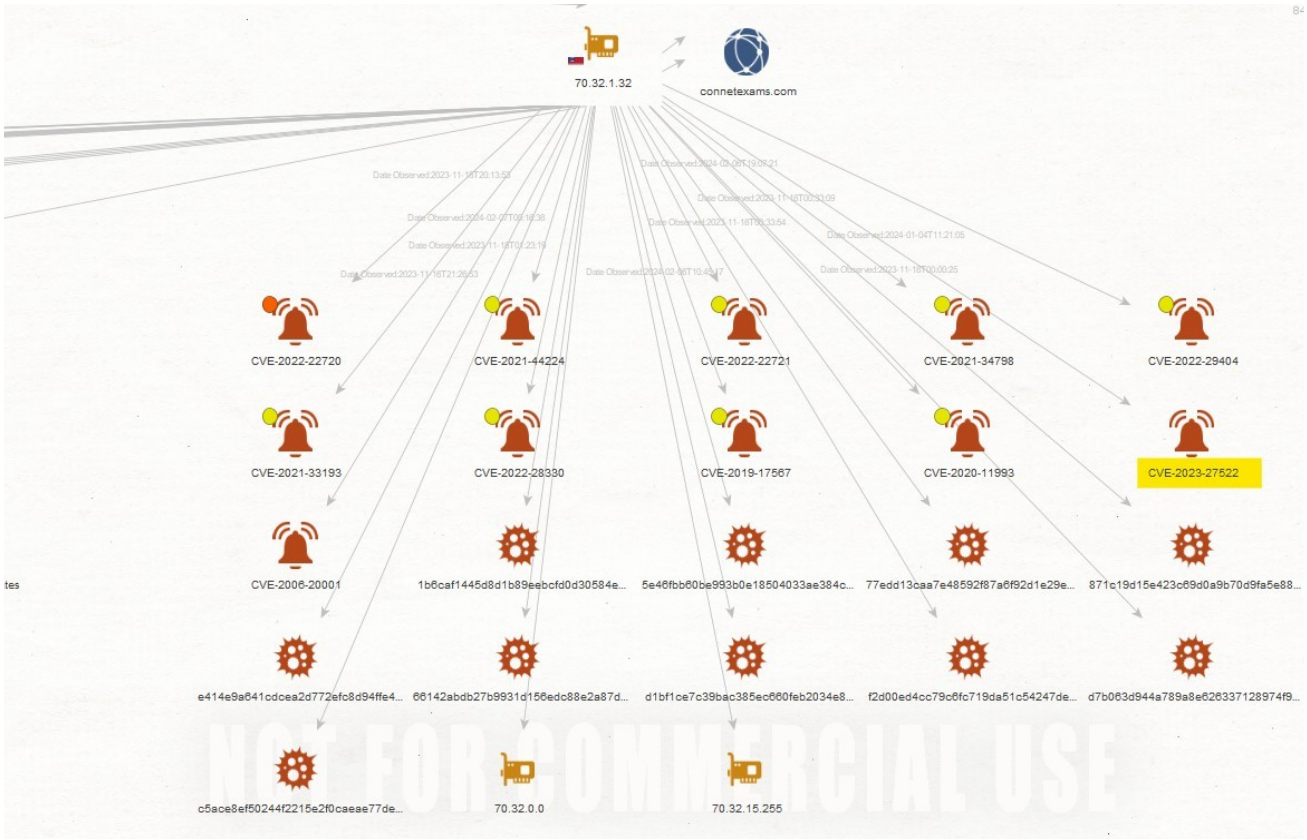


As a result of the analysis performed with the IP address, the files that have been associated with it and contain samples that have been associated with different vulnerabilities in the past understandable. The expansion of our indicator pool also provides us with extra examples and information for analysis.

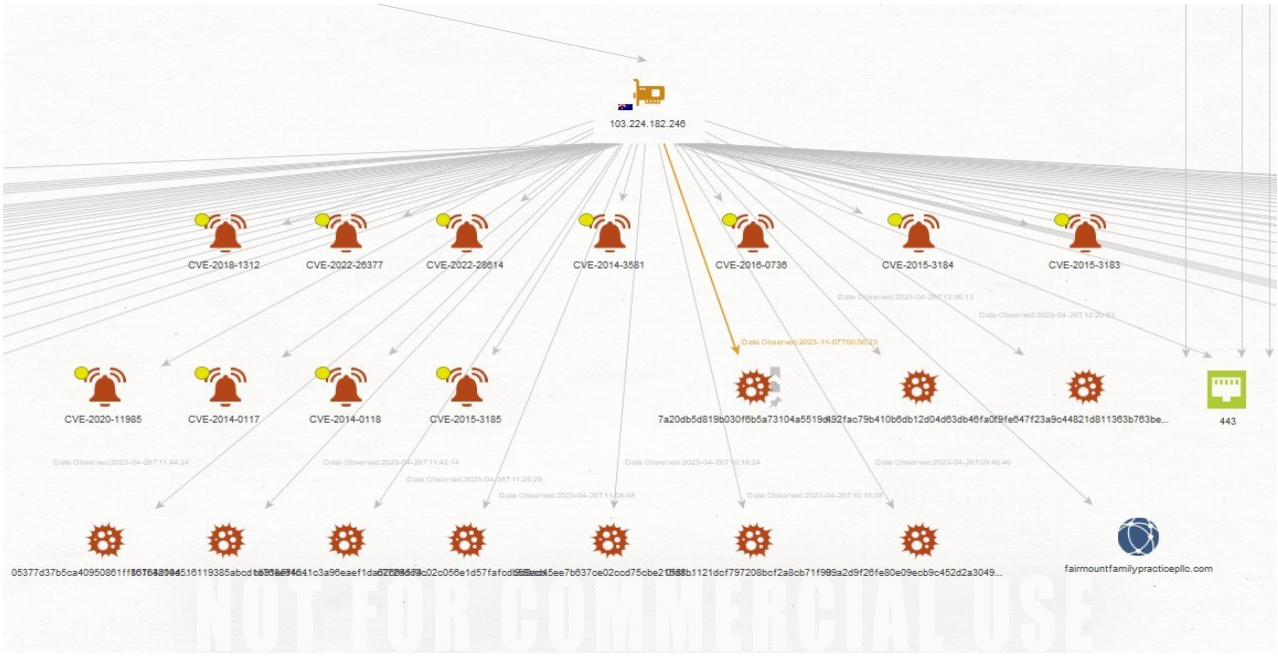
- The result of the analysis of the IPv4 address 103.224.182[.]245:



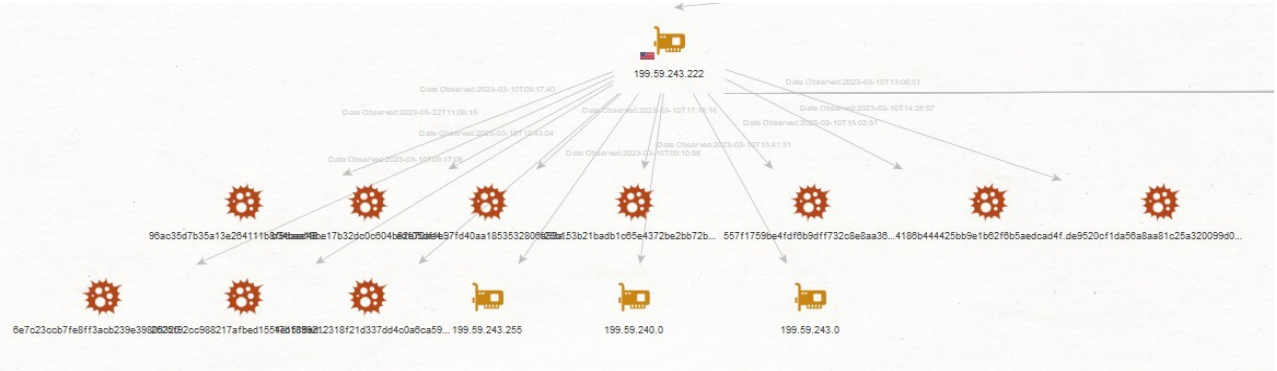
- The result of the analysis of the IPv4 address 70.32.1[.]32:



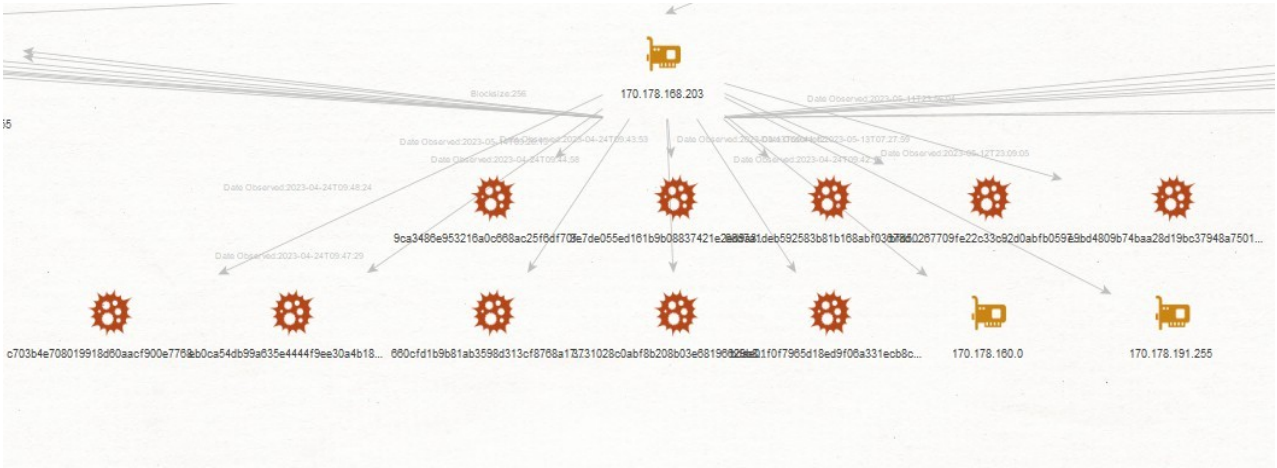
- The result of the analysis of the IPv4 address 103.224.182[.]246:



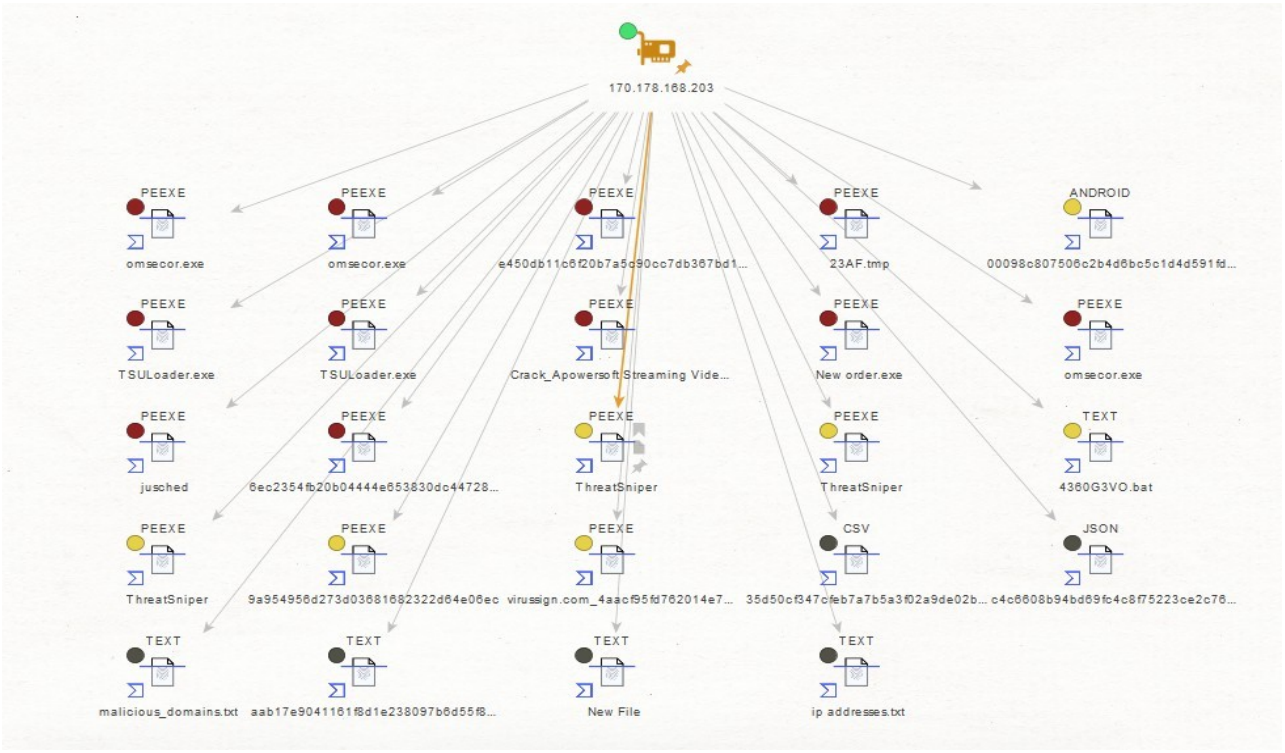
- The result of the analysis of the IPv4 address 199.59.243[.]222:



- The result of the analysis of the IPv4 address 170.178.168[.]203:

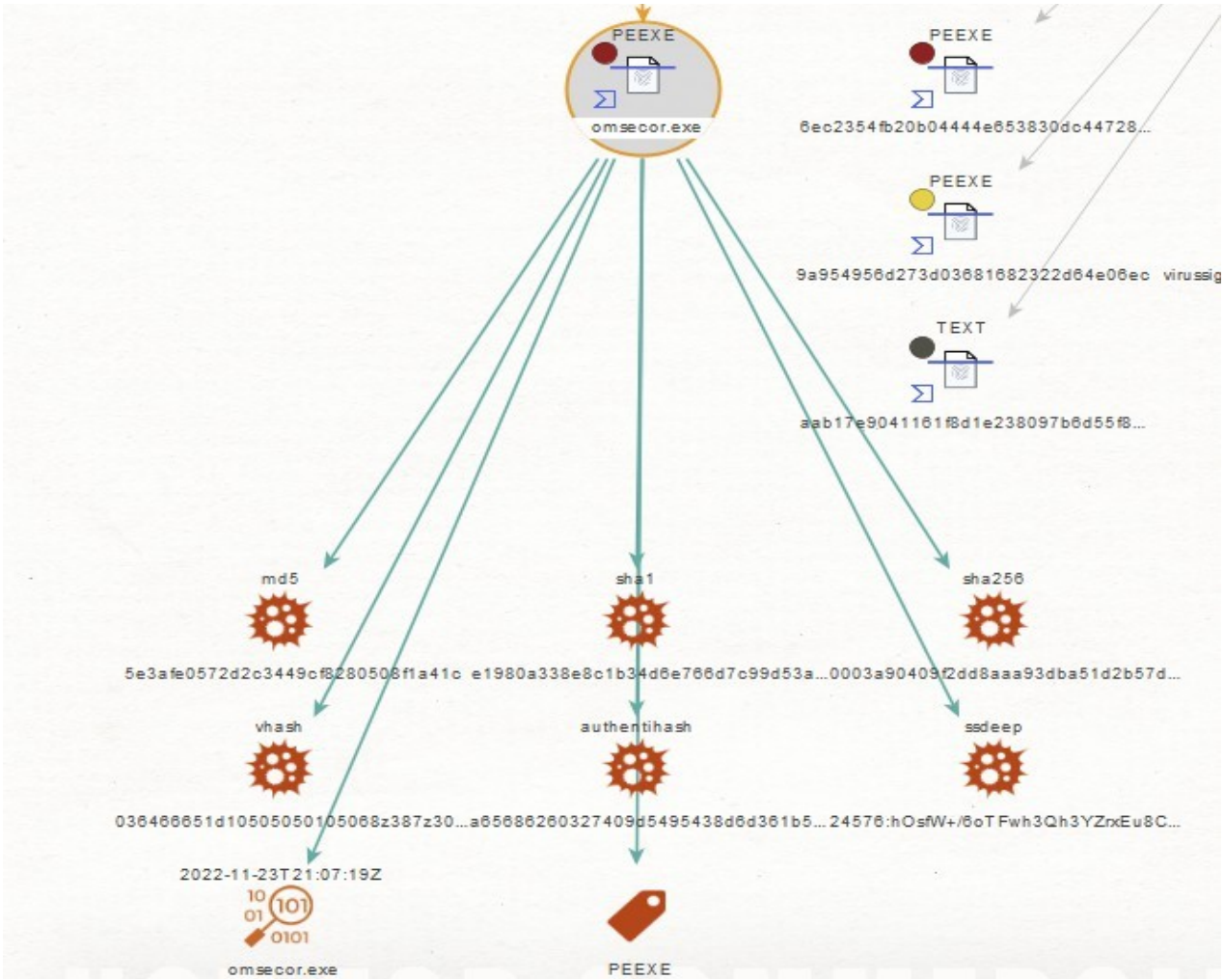


170.178.168[.]203 Result-1



170.178.168[.]203 Result-2

- When the file named "omsecor.exe" is examined as an example from the files we have identified above, it is understood that it is malware.



Conclusion

The existence of a comprehensive tool such as Maltego in the field of cyber security provides a significant advantage in information gathering and analysis processes. Maltego is available by default on the Kali Linux operating system and appeals to a wide user base with its user-friendly interface. Maltego, which is frequently preferred in penetration testing and information gathering processes, visually represents the information it collects and presents complex relationships in a more understandable way.

The focus of Maltego is to search and collect publicly available information on the internet. This information can be about individuals or organizations and is collected from various data sources. The collected information is visualized graphically, revealing relationships and connections. This allows users to analyze more effectively and refine their reports.

Maltego's custom entity types allow users to represent any type of information they want. Furthermore, transformations allow penetration testers to save significant time in their discovery process. This convenience provided by Maltego allows users to work more efficiently than with manual searches.

As a result, Maltego's comprehensive features and user-friendly interface make it the tool of choice for cybersecurity professionals and information gathering experts. These advantages of Maltego make information gathering processes more effective and play an important role in detecting and preventing vulnerabilities.

REFERENCES

Sol González. (2023, July 6). Maltego: Check how much you are exposed online. https://antivirus.com.tr/maltego-cevrimici-ortamda-ne-kadar-ifsa-oldugunuzu-kontrol-edin/

Avci, M. T. (2023, March 8). MALTEGO | Intelligence Tool. https://www.linkedin.com/pulse/maltego-istihbarat-arac%C4%9F-mert-tayfun-avci/

Pamuk, O. (2020, Jul 17). Domain Analysis of TA505 APT Group with Maltego. https://oguzcanpamuk.medium.com/maltego-ile-ta505-apt-grubuna-ait-domain-incelemesi-47cc5d0c7942

Redfox Security. (2022, October 18). OSINT with Maltego. https://redfoxsec.com/blog/osint-with-maltego/

Securium Solutions. (2023, February 16). MALTEGO – OSINT TOOL. https://securiumsolutions.com/maltego-osint-tool/

StationX. (2023, October 23). How to Use Maltego: A Beginner's Guide to OSINT Analysis. https://www.stationx.net/how-to-use-maltego/

TechLatest. (2023, February 17). MALTEGO: Unraveling the Power of Open-Source Intelligence(OSINT). https://medium.com/@techlatest.net/maltego-unraveling-the-power-of-open-source-intelligence-5e8000a2f996

WhisperLab. (2023, March 15). Open Source Intelligence (OSINT) with Maltego. https://whisperlab.org/introduction-to-hacking/notes/maltego

WondersmithRae. (2019, August 7). A Beginner's Guide to OSINT Investigation with Maltego. https://wondersmithrae.medium.com/a-beginners-guide-to-osint-investigation-with-maltego-6b195f7245cc

CyCognito. What is Maltego? https://www.cycognito.com/glossary/maltego.php

GlossaryTech. What is Maltego? https://glossarytech.com/terms/tools/maltego

Maltego. Maltego for Cyber Threat Intelligence. https://www.maltego.com/solutions/cyber-threat-intelligence/