Using Maltego for Open-Source Intelligence (OSINT) Gathering

Thu Duong

CS-444-Spring 2022

Table of Contents

1. Introduction

During the peak of the SARS-CoV-2 (Covid-19) pandemic, terminologies such as “flatten the curve” and “immune compromised” have become household concepts. When something so grand manifests itself in real life applications, the world has no other choice but to learn and adapt. In much the same way, in a world where our identities are no longer protected by the privacy of geographical locations, cybersecurity knowledge should be made mainstream, and its application made available to the layman. In other words, cybersecurity individuals ought not only be found working for internet security companies or in the IT section of national security laboratories. There should be an increase in public education in these areas much in the same way we regard the idea that financial literacy can positively impact the public as a whole.

In fact, intelligence gathering is not a new concept. However, one might ask for further details as to what this type of gathering this entails. Is it a mere search engine exercise or a battle of the wits to see who can cleverly garner much information about a particular website? The ordinary person might take much pride in obtaining hard to find information from online searches. However, to the forensics and cyber professional community, open-source intelligence (OSINT) is much more than search results due to diligence. To the reconnaissance practitioner, OSINT is a field that requires great knowledge of internet publishing and application programming interface (API)—or at least their potential use in scoping out a particular person or website of interest. To the national security individual, OSINT is a tool that can protect a nation from possible vulnerability attacks on major government sites, for example.

This paper presents the usefulness and can also be used as manual to Maltego, a cybersecurity and research tool designed for OSINT professionals to obtain more actionable knowledge in the field of cyber security operations, law enforcement, and trust and security. In the interest of the narrative of this paper, we will focus on the cyber side of Maltego. The promise of the software includes reducing cyber risk and increasing speed as well as precision of major security operation center (SOC) investigations (*Reduce Your Cyber Risk with Maltego | Maltego Solution*). The SOC is essentially a command center typically running as a 24/7 operation and is called on to perform investigations to protect its client or organization when there is a cyber-attack related, but not limited to internal network infrastructure, endpoint devices, databases, and internet traffic (Kienzle). Another part of what the SOC does is preemptive monitoring to detect penetrable flaws involving: monitoring and detection of potential threats; detection engineering; threat intelligence and incident response and threat hunting (Kienzle). As we can see here, such an operation requires complex and capable tools to scientifically pinpoint points of interest.

As mentioned in the abstract, OSINT should also be understood by the public for the sake of public good. Fortunately, while Maltego is a tool that is used by law enforcements as well as cyber security professionals, it is also available for download through its community edition (*Register a Maltego CE Account*). The software may be downloaded through the Kali Linux platform which is highly convenient for the practitioner who is already operating other cyber tools on the OS. Due to its graphical link analysis, Maltego proves to be a powerful tool in generating actionable insights.

Definitions

Entity- a name, domain, or icon resulting from a transform. The name suggests the subject of investigation on the graphical link analysis on the Maltego graphical interface.

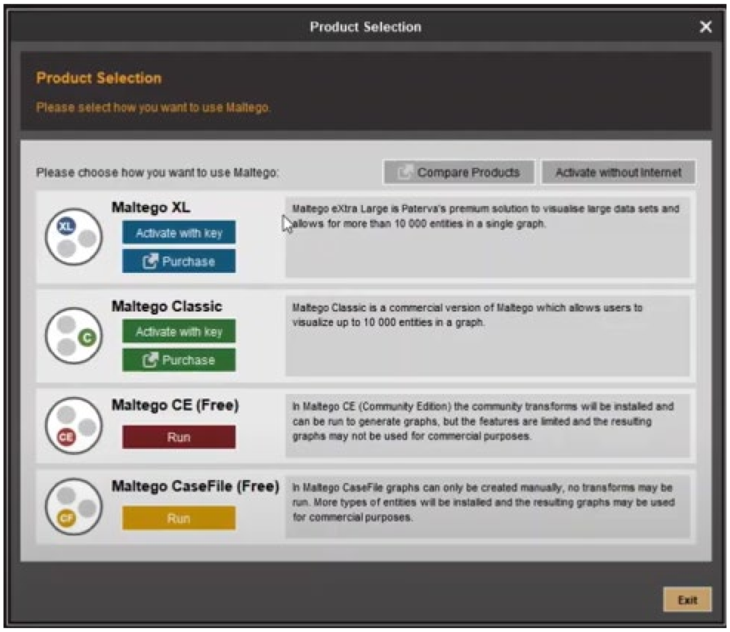
Transforms - A transform is code that can generate additional information based on already available information.

Exploratory link analysis - This is a type of analysis that helps the investigator to perform multiple transforms resulting in a tree-like graphical report which might reveal relationships and history of workflow.

2. Operating Maltego

2.1 Installation and activation

It is noted that there are only 2 free versions of Maltego as presented in this activation screen. One of the major differences between the free version and the paid versions are related to the visualization capabilities. For example, Maltego XL allows visualization of large data sets and the inclusion of over 10,000 entities on a graph. The free version as mentioned earlier is called “Maltego CE (Free)”, aka the Community Edition does allow for transforms to be installed and generation of graphics. However, the graphical analysis may not be used for commercial purposes. This is an important distinction on the software licensing aspect due to the nature of these highly technical analyses which would valuable in the consulting and SOC field. Getting Maltego installed and configured is the first step in getting started with the software.



Product Selection

Please select how you want to use Maltego.

Please choose how you want to use Maltego:

Maltego XL

Maltego eXtra Large is Paterva's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.

Maltego Classic

Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.

Maltego CE (Free)

In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.

Maltego CaseFile (Free)

In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.

Figure 1 Adapted from (Maltego, Maltego Essentials 3*), the company's channel on YouTube. Different Maltego versions available for activation after installation is complete.*

2.2 Running a transform

2.2.1 Investigate an email address

When a transform is run on Maltego, it does so on the server and not on our desktop. It ultimate yields data that can be stored on the server. The transform provides additional information based on available source given (Maltego, *Maltego Essentials 4*). A transform allows us to create graphical link analysis which originate from the original source of information. The resulting link analysis provides information to help us see relationships that are not previously made aware of.

First, look for the information, or entities, that we already have from the panel in the left. Examples of entities from the infrastructure category are IPv4 address (An IP version 4 address); MX Record (a DNS real exchange record); NS Record (a DNS name server record); Netblock (a range of IP 4 version addresses); a URL (an internet uniform resource locator); Tracking code (tracking code for a web service); or any other entity listed. Other categories of entities are devices, personal, groups, location, and penetration testing type entities (Maltego, *Maltego Essentials 4*).

Starting with the *personal* category, drag the Email entity onto the graph and change the email to a desired address. Double clicking or pressing F2 will allow the value of the entity to be changed. According to the company's video tutorial, the default email address was changed to support@maltego.com.

In order to figure out important information about the email address, one starts with any of the items under the Transforms dropdown bar. For example, choosing To Domain [DNS] transform removes the part in front of the @ symbol of the email to show the domain of that email. To run the transform, we can click the play button and in a few moments, Maltego will show a new icon on the graph displaying the domain: maltego.com.

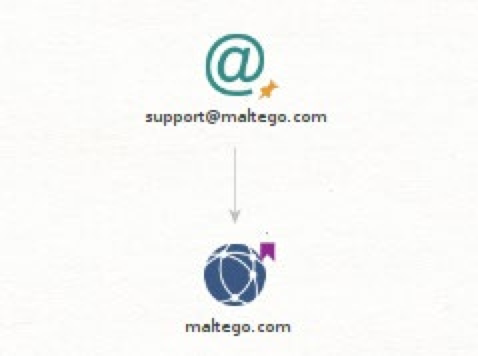
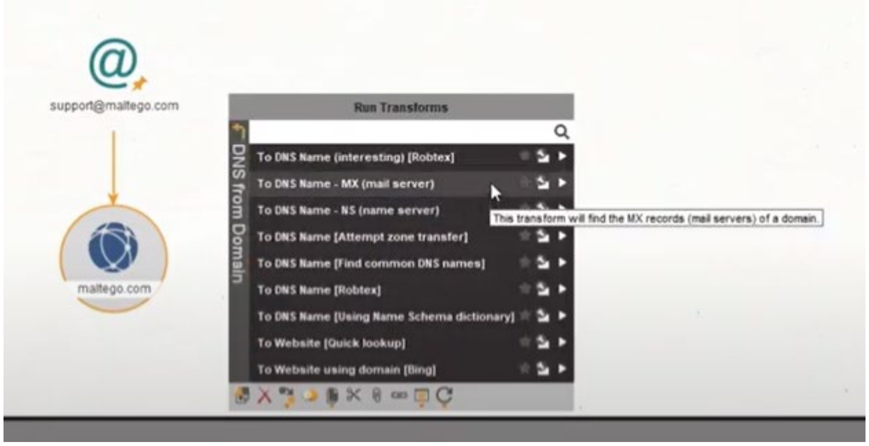


Figure 2. An example of a Domain DNS transform where the part in front of @ symbol is removed. The arrow shows the parent to child relationship in the graph.

Additionally, transforms can be performed using the mouse right button. Right clicking the mouse brings up a 'run transform' menu consisting of dropdowns for All Transforms, DNS form Domain, Domain owner detail, Email addresses for domain, Files and Documents from domain, and Machines (Maltego, *Maltego Essentials 4*).


support@maltego.com
maltego.com
Run Transforms
DNS from Domain
To DNS Name (interesting) [Robtex]
To DNS Name - MX (mail server)
To DNS Name - NS (name server)
To DNS Name [Attempt zone transfer]
To DNS Name [Find common DNS names]
To DNS Name [Robtex]
To DNS Name [Using Name Schema dictionary]
To Website [Quick lookup]
To Website using domain [Bing]

This transform will find the MX records (mail servers) of a domain.

Figure 3. Right clicking the mouse will also bring up a list of possible transforms.

If we click on 'To DNS Name – MX (Mail Server), another entity is added to the display pointing from the domain name (the source of which we previously performed the 'To DNS Name – MX (Mail Server) towards the child MX icon labeled "maltego.com mail protection…". To further transform the maltego.com icon, continue right clicking on the icon and choose ‘To DNS Name – NS (name server)’ which will cause the transform to find the NS records (name servers) of a domain. The resulting added children icons showing “ns59.domaincontrol.com” and “ns60.domaincontrol.com” which are names servers of the selected domain name icon. Now, one might be wondering if this exact process is needed to be performed on multiple entities individually. While individual transformation will work expected, we can also highlight the entire group of entities and simultaneously perform a desired transform on each of the selected entities. For example, after highlighting all three of the children’s entities of maltego.com domain, and right clicking, we can choose ‘resolve to IP’ to look for “ToIP Address [DNS]” transform, which further returns several results at a time with mail exchange producing 2 children icons and each of the name servers producing a child icon of their own giving a total four IP addresses.

Now, if we are interested in knowing where the servers for each of the IP addresses are located, we can highlight all of the IP addresses icons and perform a transform on them accordingly. Note that we can also highlight all of the same type of entities by choosing ‘IPv4 addresses’ under the drop-down “select by type”. Briefly, if we want to find out where the IP addresses are located, we can run a ‘To Location [country]’ under the ‘IP owner detail” drop-down. The resulting returns show several different countries: the US (for the name servers), Finland and Austria (for the mail exchange). In Maltego’s graphical link analysis, all entity results that are the same are connected at one icon, and thereby simplifying relationships. So far, we have performed multiple transforms on an initial email for Maltego’s support account. Each of the transforms that was performed only took a few seconds to return resulting child entities. Also, no additional information is needed other than the original email address: support@maltego.com.

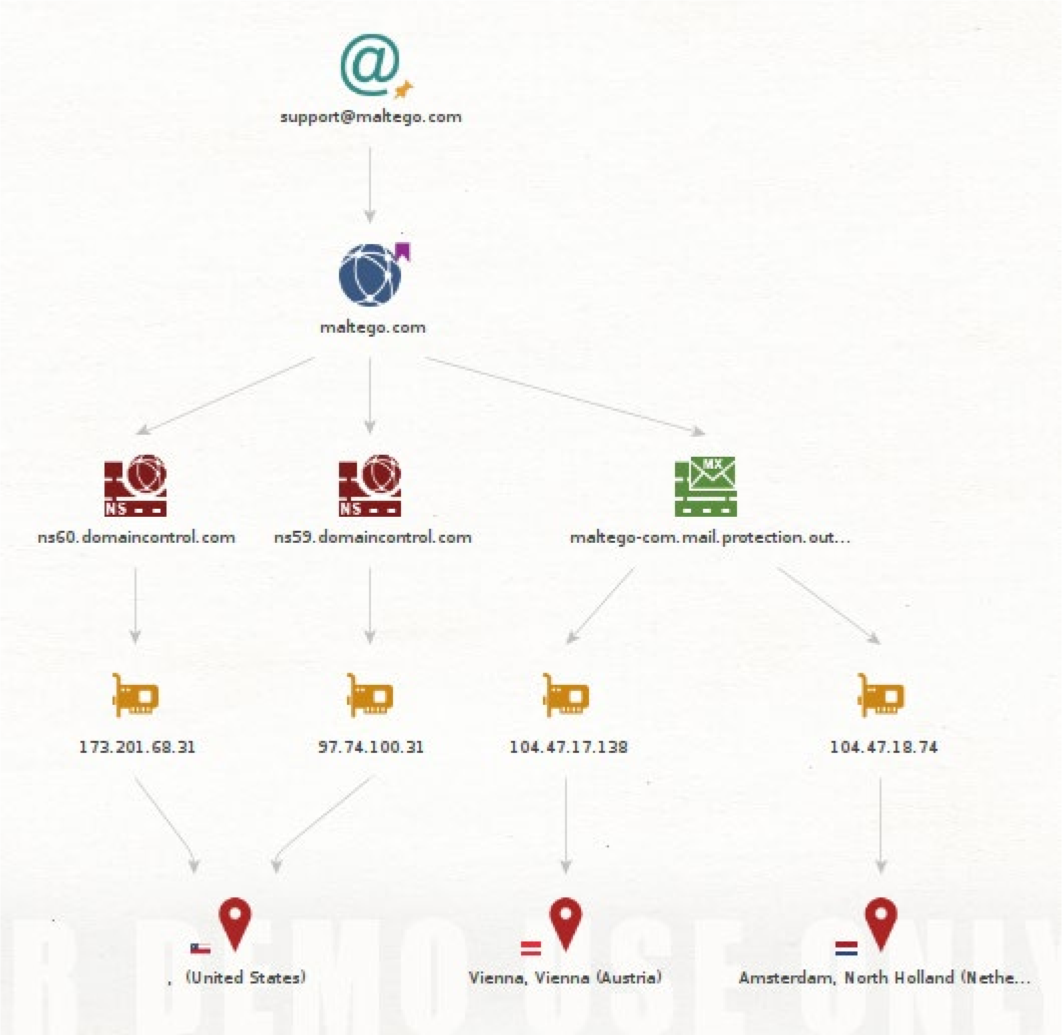


Figure 4. Example IP address transform followed by location transform. Note that two of the IP addresses have the same location and therefore Maltego shows the US having 2 arrows pointing at converging at it. Also, during this email address investigation example, no additional information is needed to be entered other than during the initial step where support@maltego.com was entered (Maltego, Maltego Essentials 4*).*

2.2.2 Investigate a domain name system (DNS)

One of the useful utilities of Maltego is to investigate further information about the DNS that appears in our network traffic log. It is helpful to know who has been visiting our sites. Features that allow the us to see our visitors have been in existence in professional social media sites such as LinkedIn. However, even when we do see who has been visiting us, will not know much information beyond that insight.

OSINT allows us much deeper knowledge about these sites and provides usual information about websites of interest. Here we will use an example posted by Maltego investigating relay.CIA.gov. To start, click and drag the ‘DNS Name’ entity to the graph and a DNS icon should appear. Here we can change the value of the icon to ‘relay.cia.gov’. like many address, our example can come with different numbers or enumerations (ie. relay1.cia.gov or relay2.cia.gov). In order to find this out, we can bring up and search for the transform name ‘To DNS Name [Enumerate hostname numerically]’. A popup window will appear prompting for additional settings information. Here, since there are not any suggestions for new adjustments, we can run the transform using the default settings. Now, in order to figure out the IP addresses of each of the enumerated hostnames, we can perform a ‘To IP Address [DNS]’ transform just like the one we did in the previous example. Once the transform has run, we notice that it returns 3 different IP addresses. We can further analyze where they originate through ‘To Netblock [using natural boundaries]’ transform which returns a common netblock.

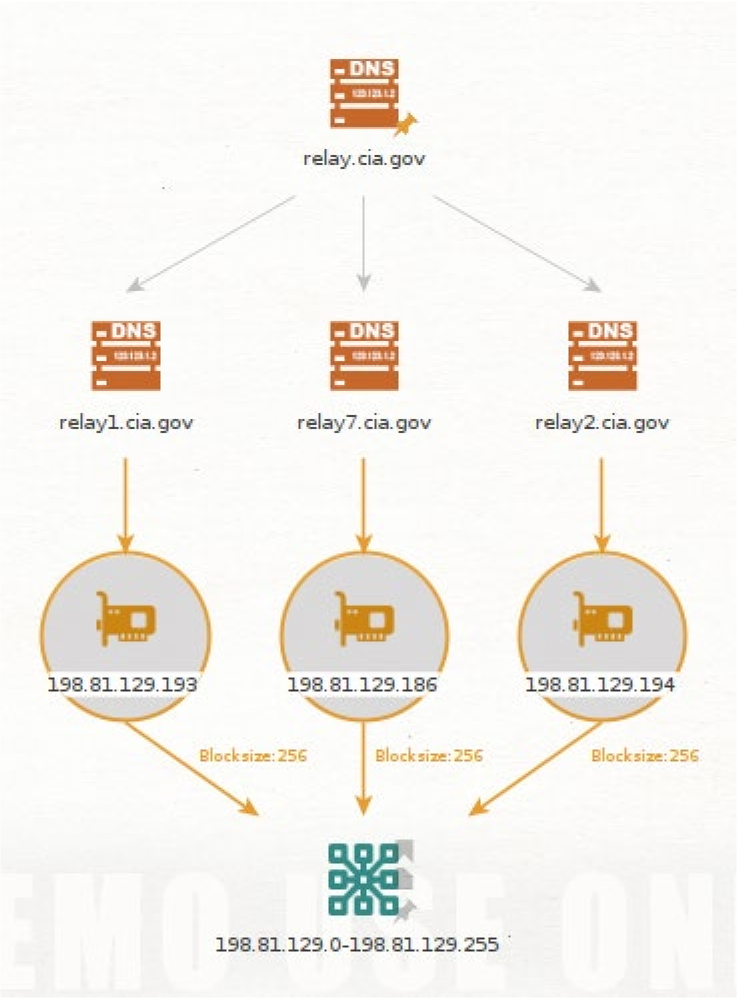


Figure 4. Example investigation of a Domain Name System (DNS) showing the three resulting enumerated hostnames which can further be transformed to reveal IP addresses. The IP addresses belong to a common netblock (Maltego, Maltego Essentials 4*).*

Running a transform is the first and foremost activity for the Maltego practitioner apart from setting up the tool. As noted, a transform is a code that, once implemented, can reveal additional information about the original entity of interest. Importantly, as shown in figures 3 and 4, we see that if a transform returns a child value belonging to 2 different parent entities, the arrows coming from the parent entities converge at one point (ie. locations of IP addresses or common netblock of 3 different IP addresses). This is an important feature as a result of the graphical link analysis capability of Maltego. An example of the usefulness of this type of investigation could arise post Distributed Denial-of-Service (DDoS) attacks. DDoS attacks are where a server is being flooded with disingenuous traffic disrupting the service or business website's operation, perhaps as a way to make statement or to harass the business(“What Is a DDoS Attack?”). In this situation, the SOC can determine the source of this traffic by pulling out samples of DNS that appears from the network traffic log and performing location or netblock transforms to determine a common source.

2.3 Investigate Phishing campaigns

One of the important uses of Maltego is to investigate an entity of interest to preemptively protect our systems and networks. Social engineering or the use of deception through planning and predicting our behaviors, in order to manipulate victims to give up or click malicious links can be a major issue in many corporations and institutions. Organizations that turn a blind eye to these activities thinking that that they may not ever be a victim to any phishing campaigns can not only put themselves at risk, but also their employees and their clients.

Phishing campaigns is one of the results of malicious social engineering activities. The attacker manipulates the victim to voluntarily click on links in putting them and their computers at risk. Phishing campaigns typically are interested in collecting information such as credentials, financial data, identities from the victim(s). If a malware successfully infiltrates a computer, drive by downloads can occur where the victim does not know that the download is taking place. This is just one of the many examples of a phishing attack (Maltego, *How to Investigate Phishing Campaigns Using Maltego in 5 Minutes*).

Attacks can range from a personal scale to massive, institutionalized launches. The results of these attacks, if successful, can be detrimental to a wide range of people. Therefore, it is crucial to include phishing campaign investigations within any or all of the organizations that depend on IT infrastructures.

It is possible that an attacker would launch parallel phishing campaigns in order to effectively bring down the organization. Therefore, we recommend that OSINT should be used to investigate these attacks in order to pinpoint additional relationship that might easily be missed.

Maltego allows for a free ‘Standard Transforms’ hub which connects with several OSINT third-party data. Third party data integration is an extremely useful activity in order to aid the phishing campaign investigations by utilizing sources such as Whois, VIRUSTOTAL, and Recorded Future (Maltego, *How to Investigate Phishing Campaigns Using Maltego in 5 Minutes*).

First, we start with the Domain entity whiling entering in the value of the phishing domain. Then we look for the transform name ‘To DNS Name Transform’ using the method discussed previously. A DNS Name icon appears as a child to the parent domain icon. We can then proceed to run the ‘To IP Address [DNS] Transform]’ which give us the IP address. Now, in order to find what websites are hosting on the same IP address, we can run the ‘To Website using IP [Bing] Transform’ which will return a number of associated websites that are connected to the same attacker behind the phishing domain name. These IP addresses can then be further transformed.

Two additional transforms may be run on these associated websites. According to Maltego’s video tutorial, Mirror ‘External links found’ and ‘Email addresses found’ transforms can help identify external links email addresses, respectively, in the html source code. At this point, we have seen what Matego can do in terms of investigating phishing campaigns. Additional transforms are available to provide information on the attacker’s SSL certificate, the attack date and a whole host of other possible intelligence (Maltego, *How to Investigate Phishing Campaigns Using Maltego in 5 Minutes*).

3. Conclusion

OSINT is the utilization of information that are available from the internet but requires additional tools and expertise to gather. The internet has opened doors to many opportunities for investigators to perform reconnaissance on a website, an institution, and attacker’s phishing website. At the same time, it also created possible for malicious actors in the field. Therefore, it is important for us remember that while we do not need to celebrate too early for having advanced research and investigative OSINT tools because attackers can also use them, but we also do not need to mourn the existence of these attacks as well by virtue of the same reasoning that we now have capable tools with only a few clicks.

Educating the public and companies regarding OSINT tools such as Maltego can not only help protect these companies’ IT infrastructures, but also our nation’s security. While protecting individual data is extremely important and a noble cause, it is even more important to protect credentials to prevent certain security breaches that could allow people (or nations) with malicious intent to manipulate certain infrastructures to crumple, or even worse, give up control. OSINT can therefore be used as a penetration testing tool as well as an SOC investigative tool. While the information involved in OSINT tools are available to the public (in the form of APIs, for example), one must practice caution when utilizing these tools and consider their uses’ legal and ethical ramifications. As we have seen, Maltego is a powerful tool which provides graphical link analyses—a valuable feature to any investigations.

References

Kienzle, Julian. “What Is a Security Operations Center (SOC)?” *LogPoint*, 27 Aug. 2020, https://www.logpoint.com/en/blog/security-operations-center/.

Maltego. *How to Investigate Phishing Campaigns Using Maltego in 5 Minutes*. 2021. *YouTube*, https://www.youtube.com/watch?v=9-cd4W7Jl3g.

Maltego Essentials 3: How to Install and Activate Maltego - Official Tutorial Series for Beginners. 2020. *YouTube*, https://www.youtube.com/watch?v=6ZJ_4zjeZ7k.

Maltego Essentials 4: Running Your First Transform - Official Tutorial Series for Beginners. 2020. *YouTube*, https://www.youtube.com/watch?v=GwBiJqa_nEc.

Reduce Your Cyber Risk with Maltego | Maltego Solution. https://www.maltego.com/reduce-your-cyber-security-risk-with-maltego/. Accessed 26 Apr. 2022.

Register a Maltego CE Account. https://www.maltego.com/ce-registration/. Accessed 9 Mar. 2022.

“What Is a DDoS Attack? DDoS Meaning, Definition & Types.” *Fortinet*, https://www.fortinet.com/resources/cyberglossary/ddos-attack. Accessed 3 May 2022.