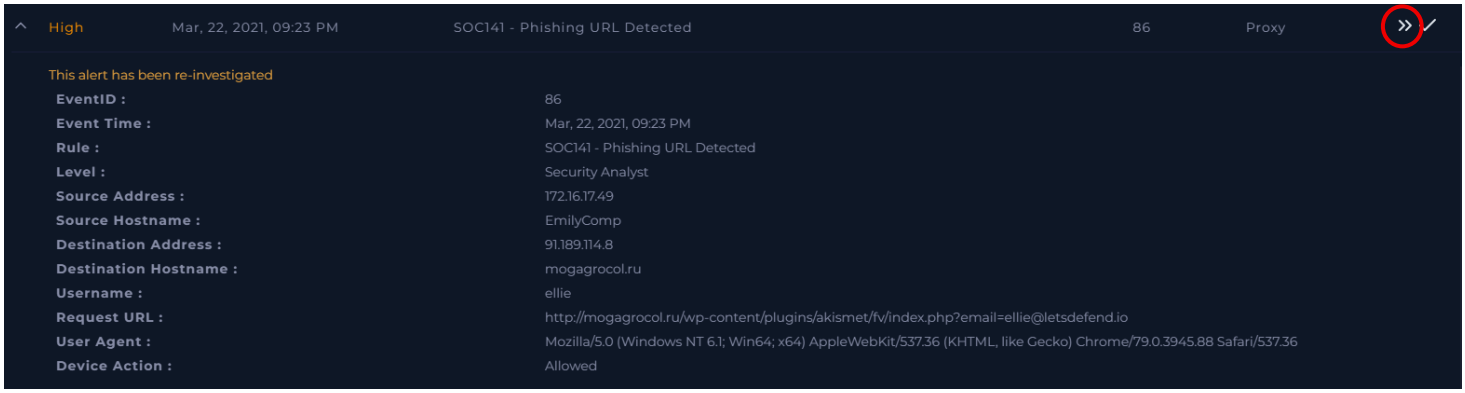
Kia ora! This is my walkthrough/documentation of my process in investigating LetsDefend's SOC alert for SOC141 – Phishing URL Detected.

Lets start with going to our investigation channel inside the LetDefend practice sector and create a case for this alert.

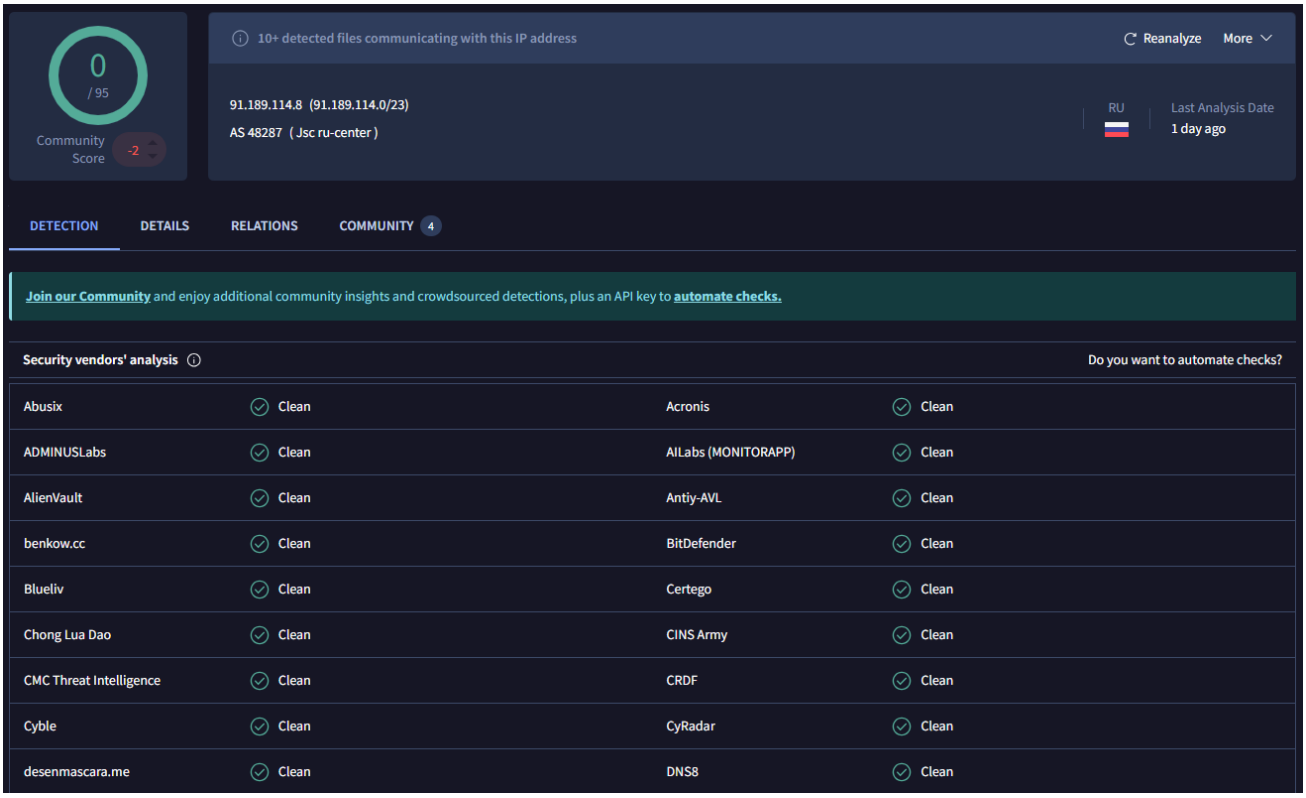


Make note of the details on this screen. I like to keep a separate notepad open to get down the source address/hostname, destination address/hostname, and any other information that might call out to me. In this case, I take note of the user agent and request URL.

Now that we've created the case, I recommend duplicating the tab before starting the playbook. This ensures that you can always refer back to the playbook without losing your progress.

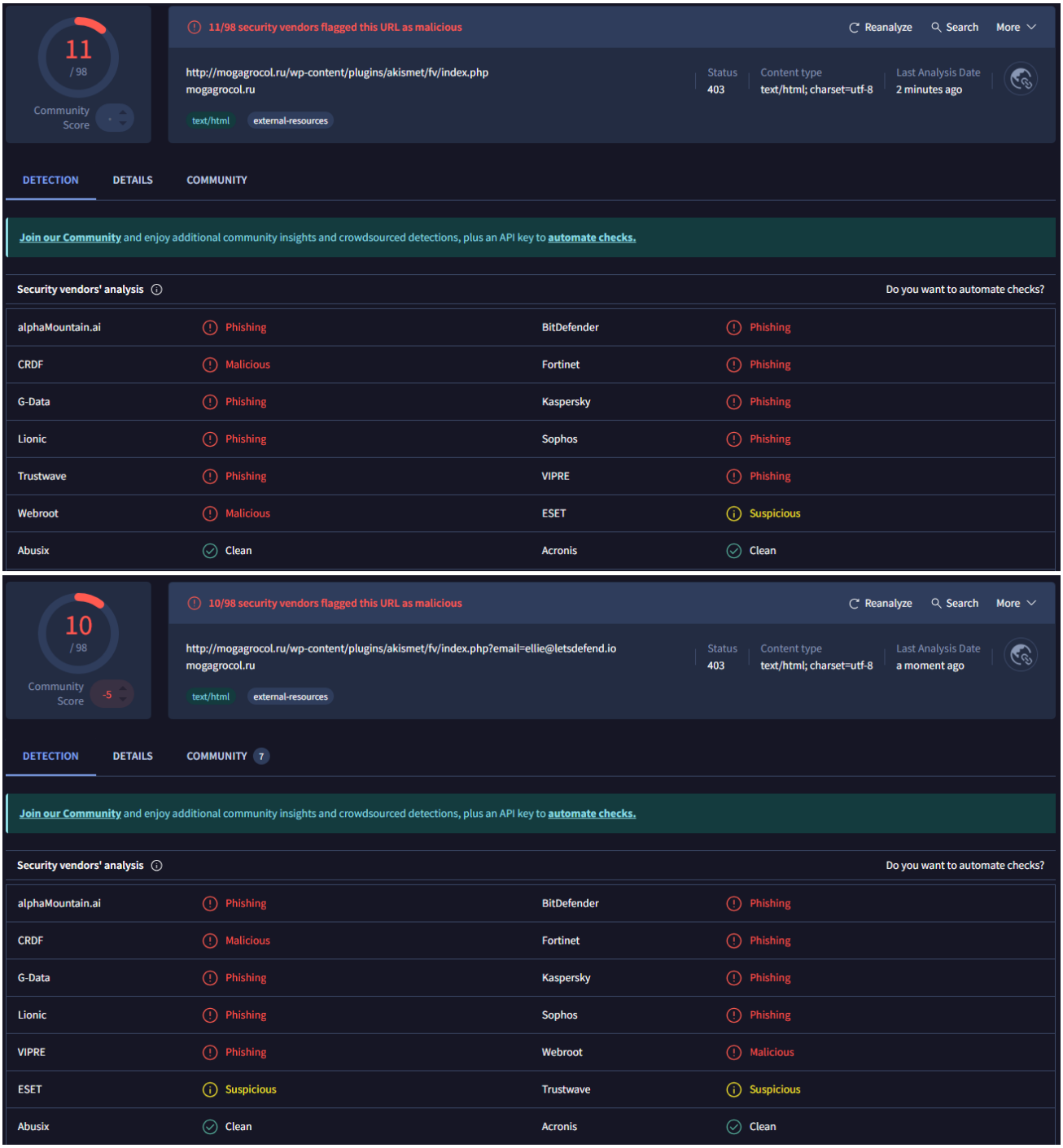
Personally, I like to do my investigation before going through the playbook. This is my process.

I put through the destination address through various online tools such as VirusTotal and Hybrid Analysis. Let's see what hits we get.



Putting the destination address through VirusTotal comes back clean, but we still need to keep looking.

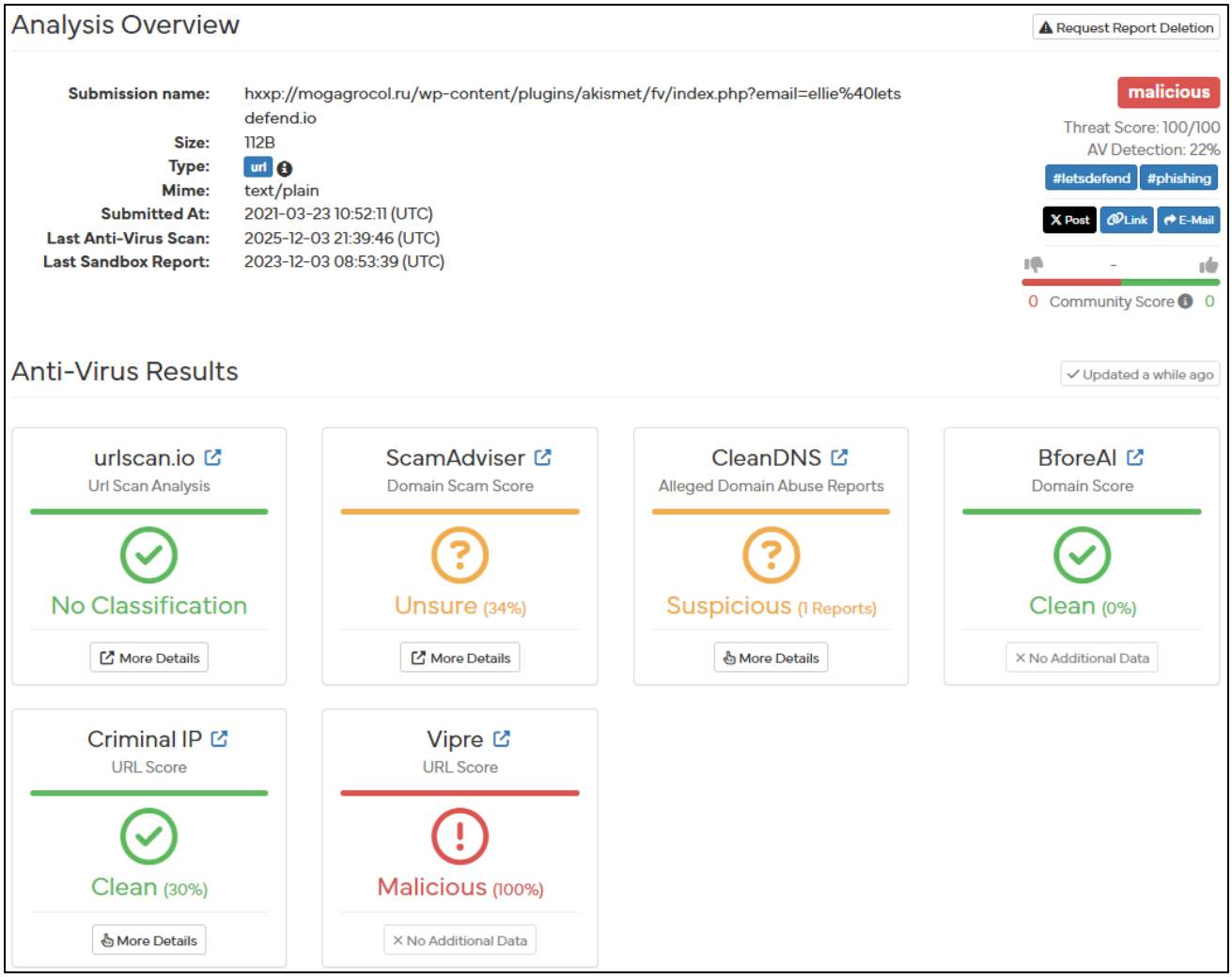
I searched the request URL twice, once with the typical phishing "?email=ellie@letsdefend.io" and another without, I want to take a look if there are any differences there.



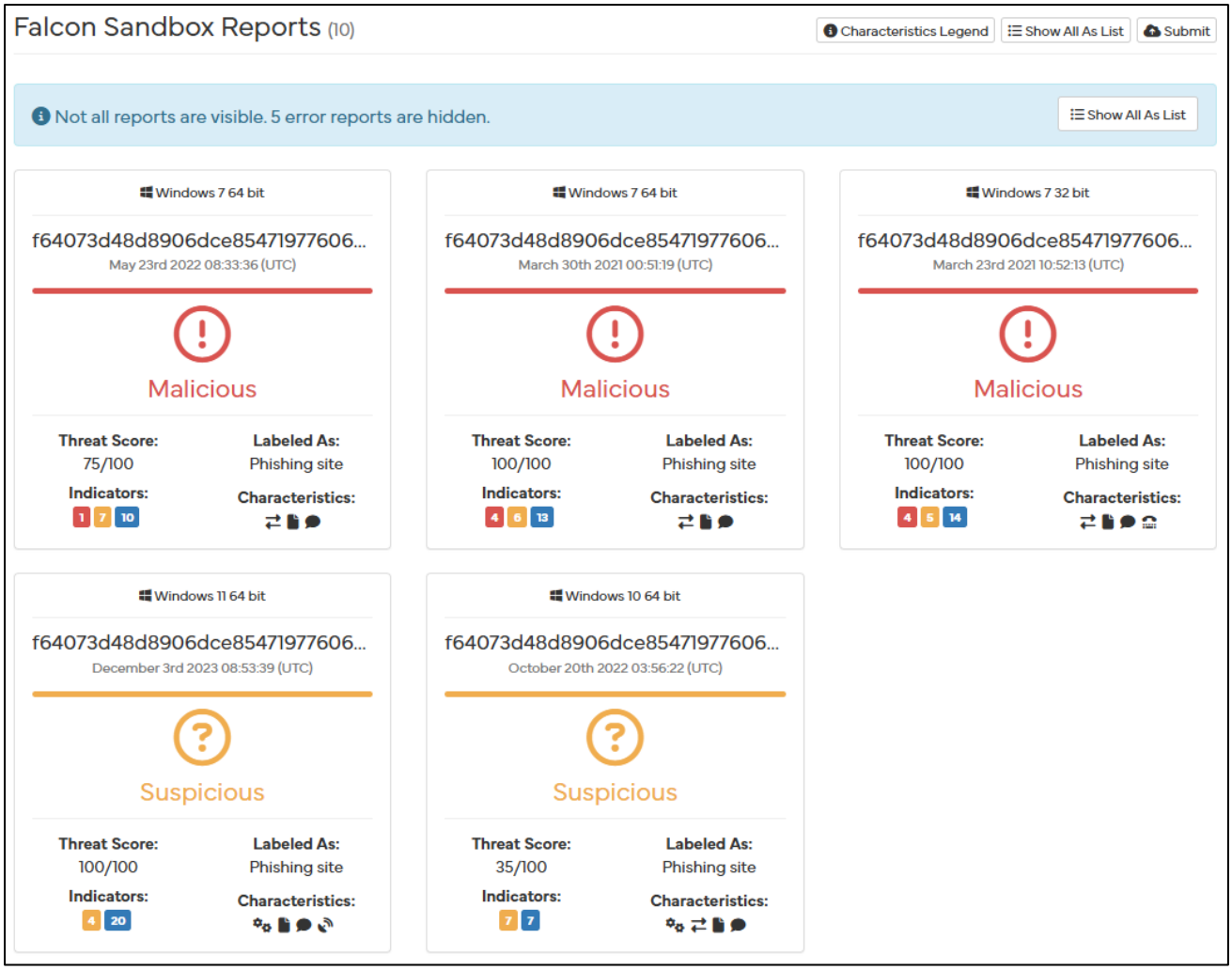
10-11 out of 98 vendors flagged this as malware. Checking the categories shows that this is suspected phishing and fraud according to the different vendors. We also see that the website is error code 403 (forbidden).

Another thing that is interesting is the different address in the HTTP response section. This is 195.24.68[.]4, putting this through shows that it communicates with a lot of risky executables, PDFs and other HTML files.

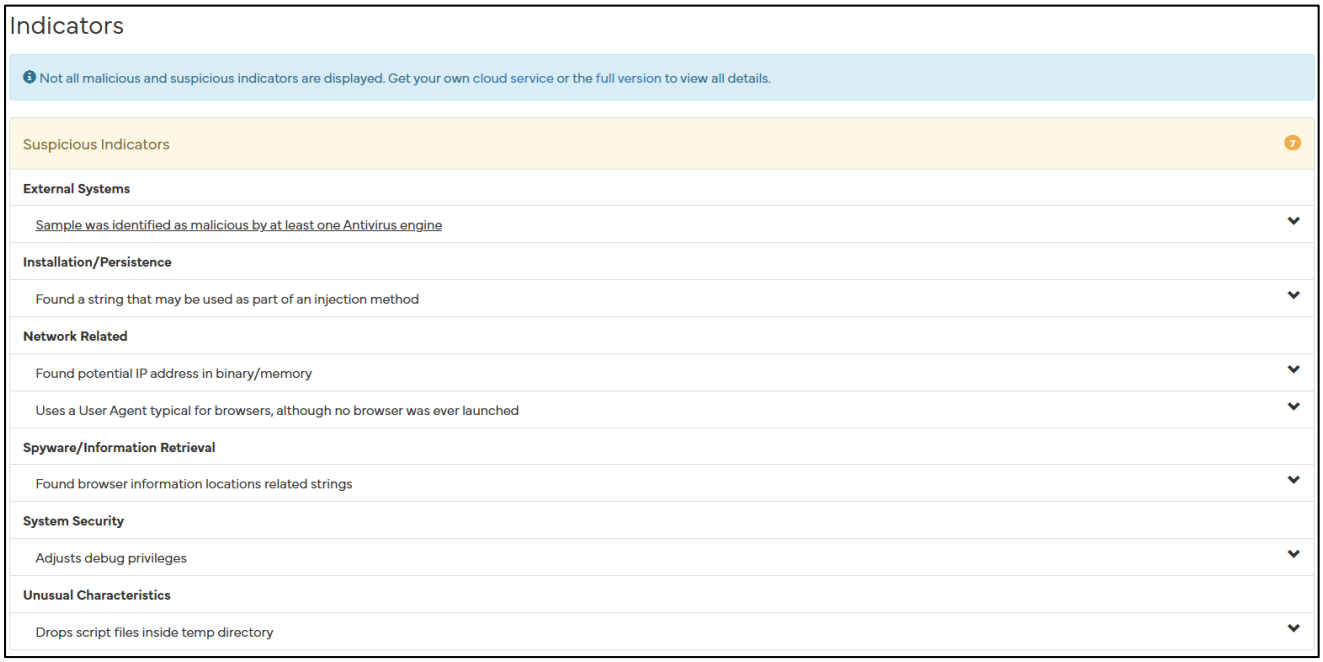
So VirusTotal is showing hits for it maybe being a phishing URL, lets take a look at Hybrid Analysis where it also runs it through a sandbox and can be a bit more detailed.



Threat score is 100/100 and the overall is malicious rating. Lets take a look at what the Falcon Sandbox reported.



Not good, safe to say that this is 100% a phishing site. Ignore the 5 error reports, those were in a Linux environment that didn't support the "sample.url" files. Lets choose one of these are see what indicators are showing up.



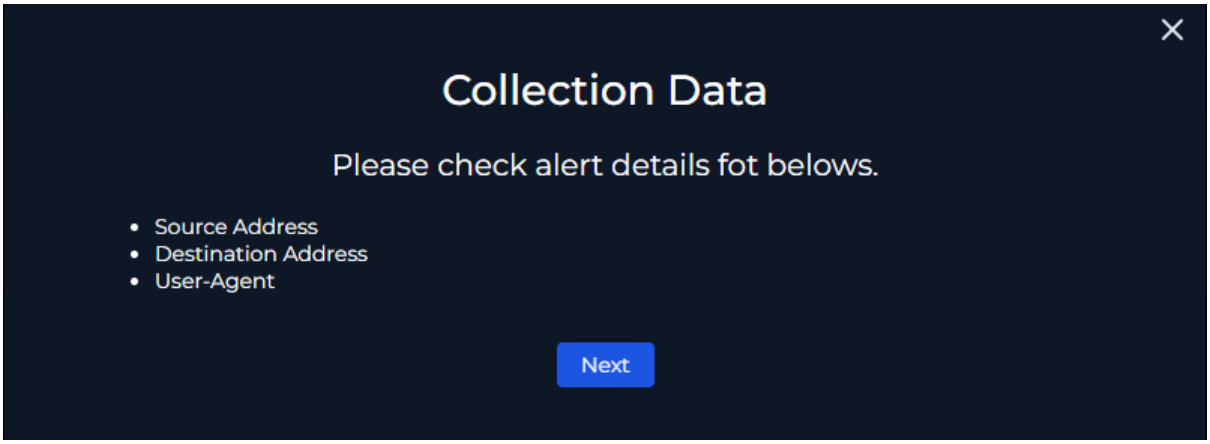
Here we can see the risk assessment and MITRE ATT&CK techniques used as well as indicators that show why its suspicious/malicious. Scrolling down to the contacted hosts shows the IP addresses from the original alert plus the one that was connected to the VirusTotal result from earlier.

Alright so we've done a bit of an indepth research using the online tools available and we can conclude that this is a malicious piece of software. There's another section that I would like you to take a look at – the URL itself:

[http://mogagrocol.ru/wp-content/plugins/akismet/fv/index[.]php?email=ellie@letsdefend.io]

Please look at the highlighted part, the plugin "Akismet" used for anti-spam does not have a directory /fv. This directly indicates the use of a compromised site as well as hiding in plain sight. Uses for this could be a backdoor with index.php.

Well, this seems like a substantial amount of information from the top layer, lets go onto the playbook and following along with it.

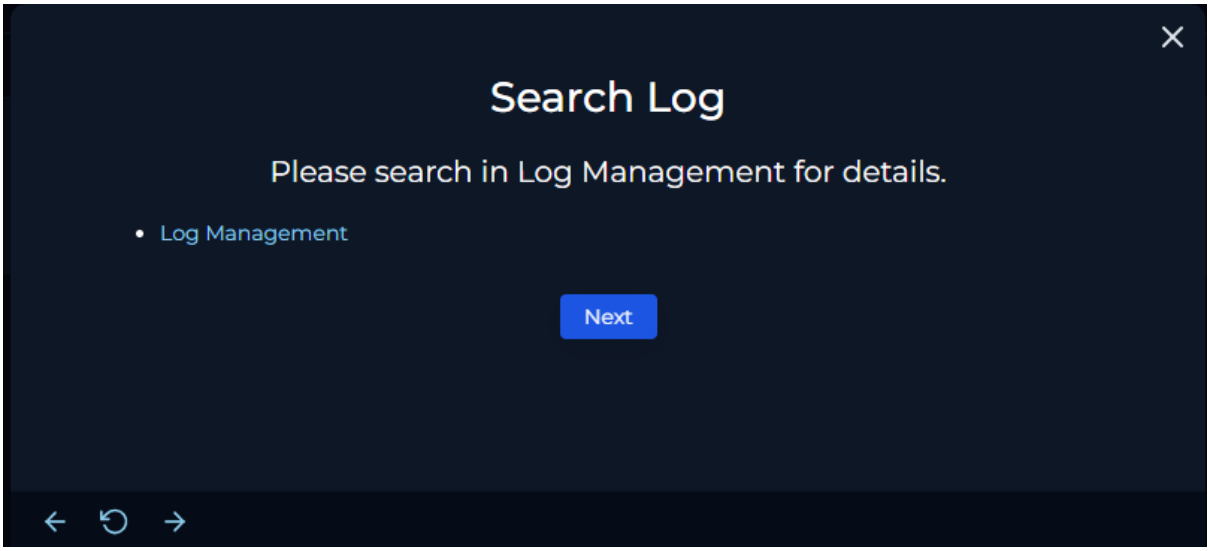


We already have all this information, something to note is the User-Agent here

[Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36]

We see that Emily is using outdated versions of Windows 7 (Windows NT 6.1 is the same thing) and the browser information being Chrome 79 (we are currently at Chrome version 143). This poses great risks, and should be taken note of for the remediation process.

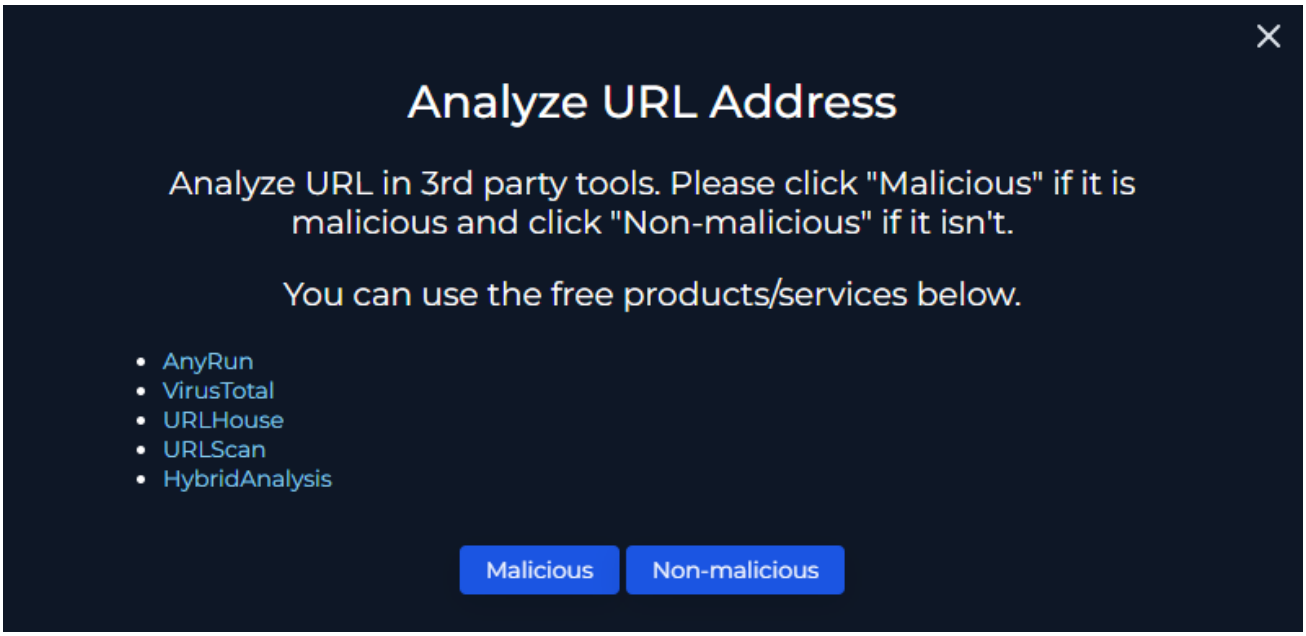
Let's click next to continue through the playbook.



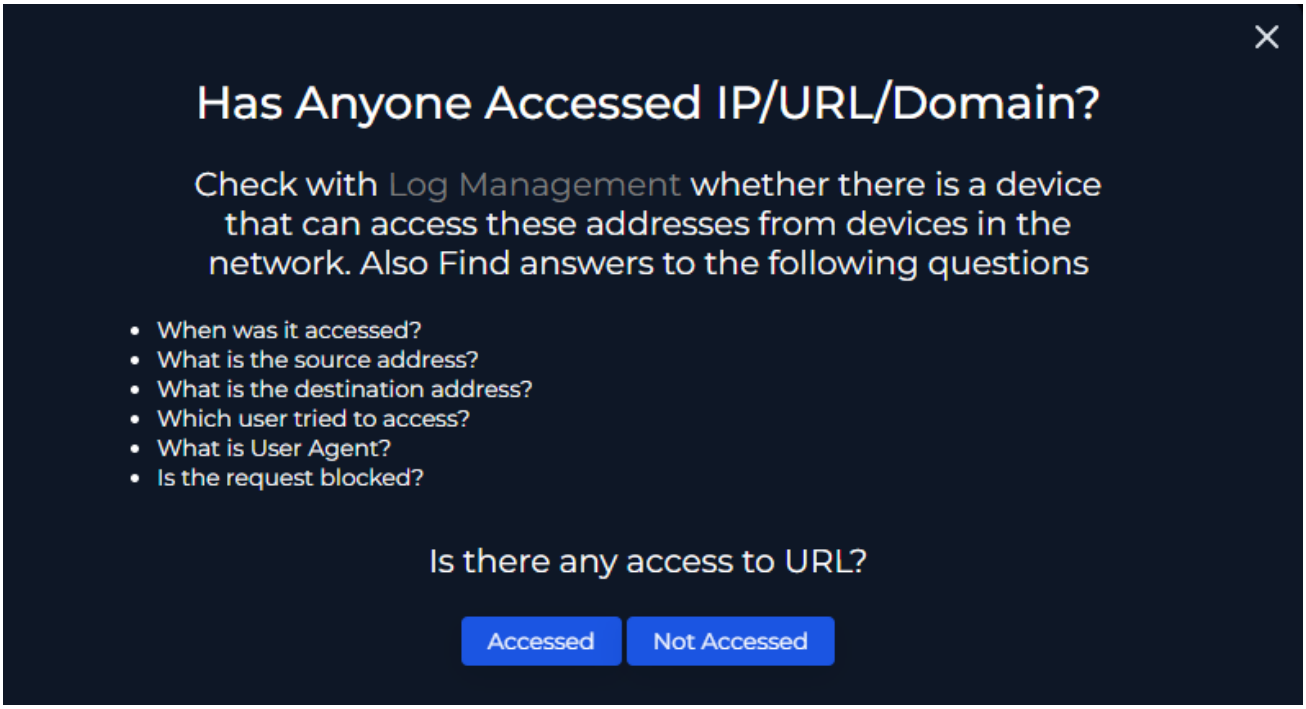
In that duplicated tab, go to Log Management and look at the destination address along with the source address.

When looking at the destination address, we see that Ellie did access this URL at March 22nd 2021 09:23pm. Thankfully no other users also accessed this URL. As a precaution I also input the other IP addresses that we saw earlier, but no logs are returned.

We can go next through the playbook and with our knowledge answer whether this is malicious or non-malicious.



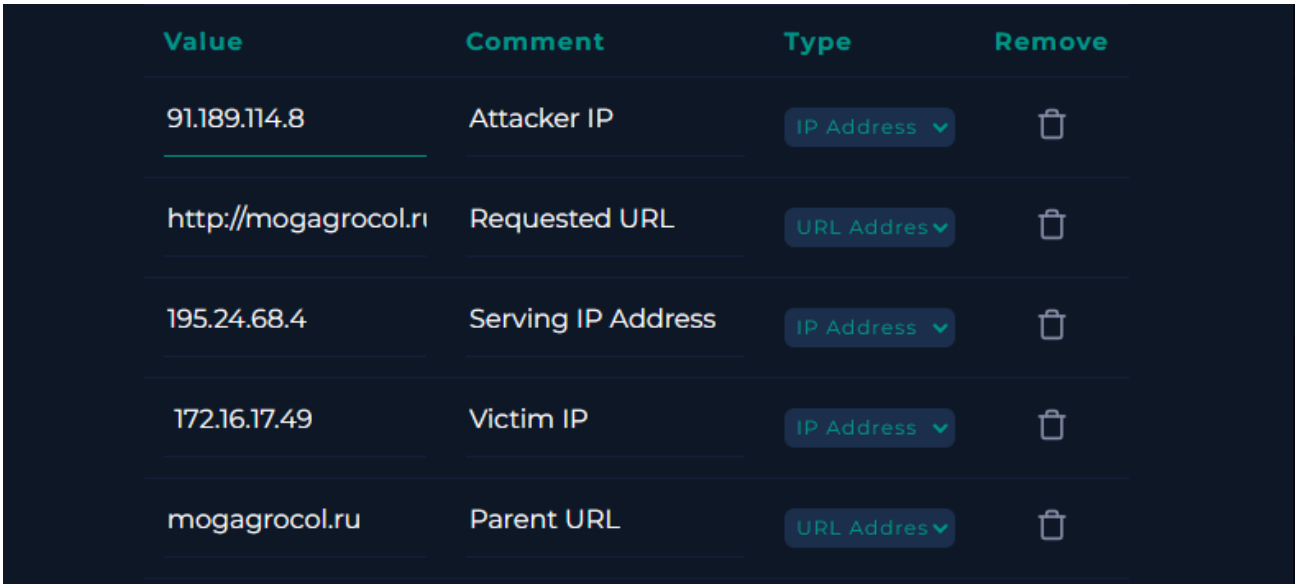
Now we must determine if anyone has accessed the IP/URL/Domain.



With our information and the log management section we can confidently answer all these questions. The last one can be a bit confusing if you are new to this, but we can see that the firewall allowed this URL.

Go to the end point security and contain the threat before continuing.

Now we can enter all the artifacts that we acquired during this investigation.



Fill out your analysis comments and complete the playbook. We can now close the alert and make a note to explain your result.

Congratulations! That's the SOC141 – Phishing URL Detected alert completed. As a part of good practice, we should think about some further remediation.

1. Block the IP addresses and URL

Make this into a firewall rule to ensure that no one else gets this URL and possibly contaminates their system.

2. Update Emily/Ellie's computer OS

This event time was in March of 2021, and Windows 7 ended support back in January of 2020, meaning this was very high risk of vulnerabilities. The system must be either updated or upgraded immediately – upgraded if the phish attack is serious.

We must also ensure that the Chrome version is also updated to the most recent version at that time, which would've been Chrome 89 (March 2nd 2021)

3. Train the Employees

A mandatory training exercise for the employees of the company to teach them the risks of clicking on untrusted URLs to raise awareness.