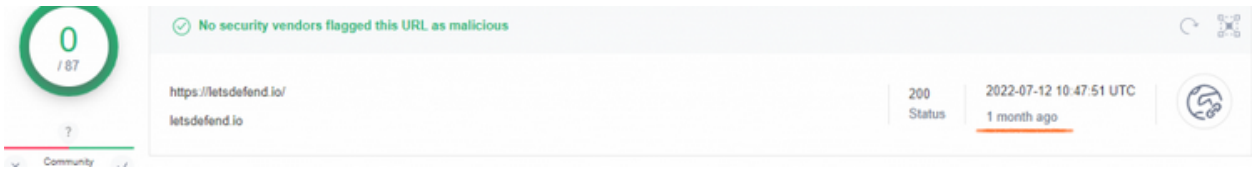
Key Points to Know

By: Ryan Stewart

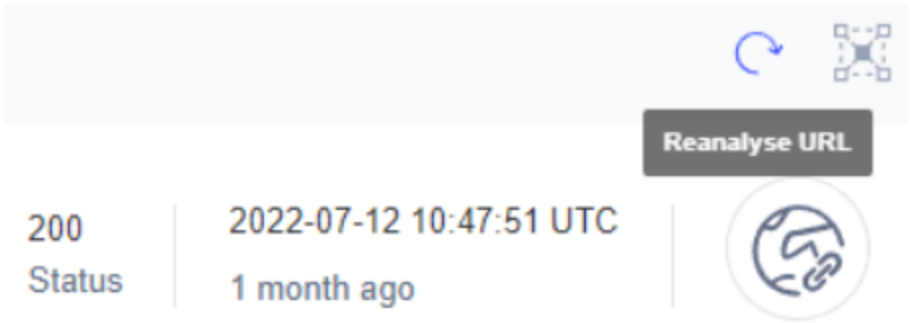
VirusTotal is frequently used by SOC Analysts during the day, the data provided by the platform quickly makes the analysts' job much easier. If care is not taken in some matters, the data obtained may cause incorrect analysis. It is very important that you read the following section **carefully** and **avoid this common mistake.**

Old Analysis Results

When you start a scan/search on VirusTotal, old results, if any, are shown for faster results. For example, if you scan the URL "letsdefend.io", you may see a result like the one below.



If you pay attention to the area in the image above, you are viewing the scan result **1 month ago.** Since attackers know that you use the VirusTotal platform a lot, they can follow this method: Generate a harmless URL address and scan it in VirusTotal (For example letsdefend.io/file). It then replaces the content of the URL with something that is harmful. **An amateur SOC analyst thinks the address is harmless** when he sees a green screen (where all security vendors give the result Clean) when he searches VirusTotal.



But in this case, the analyst falls into the trap of the attacker. All it needs to do is start a new query and view the analysis results of the current content in the URL address. By clicking the "**Reanalyse**" button, the analysis is performed again.

Detection Tags

One of the points to consider when deciding whether a file is malicious or not via VirusTotal is how **AV companies label it.**

A file may have a detection rate of 10/52 on VirusTotal, but when you examine the tags, you can see that it's not actually harmful. The most common example of this situation is setup files. In the setup files, there may be advertisements that appear on the setup screen from time to time. Since AV engines generally work on a rule-based basis, they can mark files with these ads as "Adware". For this reason, you may see these types of files as "red" on VirusTotal.