URL Reputation Tools

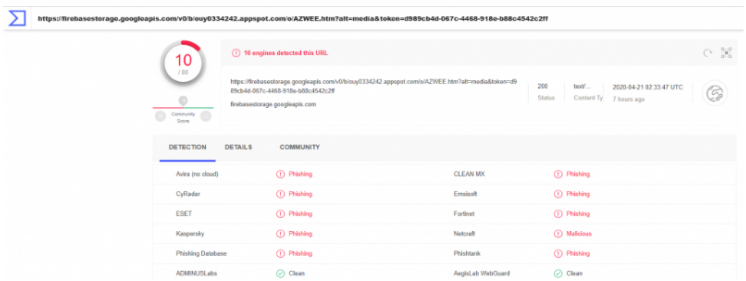
This lesson will cover how to perform reputation checks for potentially malicious URLs, helping us to decide if they are actually malicious or not. Whilst there are a number of free online reputation tools, we are going to be focusing on VirusTotal and URLScan.io, as they are the most complete and easy to use. Below we will cover how to use these tools to determine if URLs have been marked as malicious by the security community. **It is extremely important to remember that if something is not being identified as malicious by online reputation tools, it does not mean it is safe. We're sure you've heard of the phrase "innocent until proven guilty" – we need to use the opposite here. Assume that suspicious sites are malicious until you can prove it is safe to visit.**

While reputation sites can be a good resource, you need to remember they are not always effective, and further analysis is always needed. If a URL or domain has a malicious community score, it means the URL has been analyzed and reported as malicious before. Targeted and unique attacks will not have been analyzed by other security professionals, therefore URLs could come back with no negative comments, but could be extremely malicious.

VIRUSTOTAL

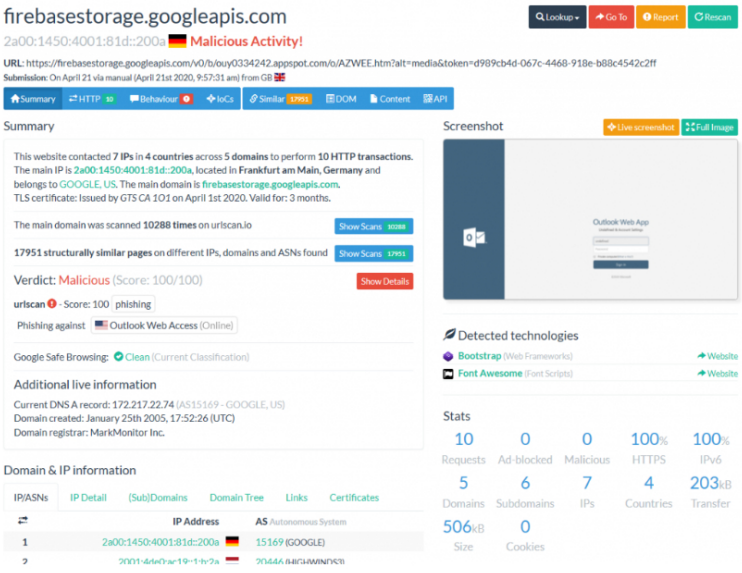
Head over to VirusTotal and you'll be met with the simple web GUI. Click on the URL tab, and you'll see the same as the below screenshot. Here we can enter malicious URLs to retrieve reputation scores.

Now I'm going to enter in a URL that I know goes to a live Outlook credential harvester. We can see that the URL has been recognized as malicious by a number of vendors, including Kaspersky, ESET, and Fortinet.



URLSCAN

URLScan is a service that can provide us with **tons** of information about a URL. To walk you through this tool, we're going to enter the same URL that we just saw was flagged as malicious on VirusTotal.

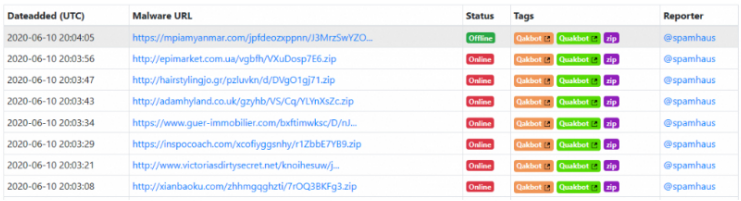


As you can see, we've been presented with so much useful information. From a reputation score to a screenshot, web technologies used on the site to domain and IP information. Whilst all of this information can be useful during high profile investigations, typically using URL2PNG for visualization will be enough.

THREAT FEEDS

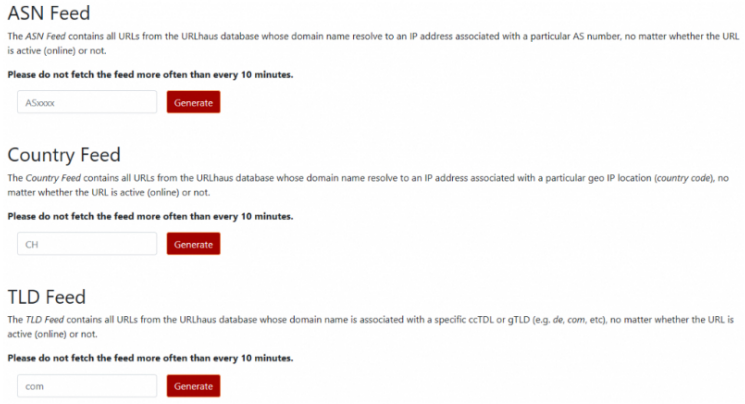
There are a number of public threat feeds that can provide security teams with intelligence regarding phishing attacks and malicious artifacts that can be used to power blacklists for email security products. Examples of these feeds include URLhaus and PhishTank. Let's explore them both below.

Firstly, let's look at the URLhaus Database, a huge collection of malicious URLs reported by researchers. In this screenshot, you can see the date the URL was added to the database, the malicious URL, the status showing whether this resource is still available on the internet or not, tags that show at a glance what the malware is (in these URLs we can see they're hosting Quakbot), and the final column shows which user reported these URLs.

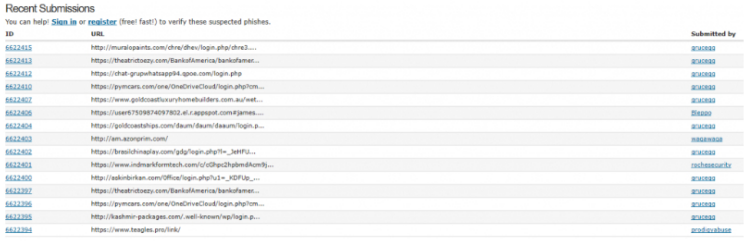


Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2020-06-10 20:04:05	https://mpiamyanmar.com/jpfdeozxppnn/J3MrzSwYZO...	Offline	Qakbot Quakbot zip	@spamhaus
2020-06-10 20:03:56	http://epimarket.com.ua/vgbfh/VXuDosp7E6.zip	Online	Qakbot Quakbot zip	@spamhaus
2020-06-10 20:03:47	http://hairstylingjo.gr/pzluvkn/d/DVgO1gj71.zip	Online	Qakbot Quakbot zip	@spamhaus
2020-06-10 20:03:43	http://adamhyland.co.uk/gzyhb/VS/Cq/YLYnXsZc.zip	Online	Qakbot Quakbot zip	@spamhaus
2020-06-10 20:03:34	https://www.guer-immobilier.com/bxftimwksc/D/nJ...	Online	Qakbot Quakbot zip	@spamhaus
2020-06-10 20:03:29	https://inspocoach.com/xcofiyggsnhy/r1ZbbE7YB9.zip	Online	Qakbot Quakbot zip	@spamhaus
2020-06-10 20:03:21	http://www.victoriasdirtysecret.net/knoihesuw/j...	Online	Qakbot Quakbot zip	@spamhaus
2020-06-10 20:03:08	http://xianbaoku.com/zhhmggghzti/7rOQ3BKFg3.zip	Online	Qakbot Quakbot zip	@spamhaus

URLhaus offers a number of threat feeds that can provide specific information, and as mentioned above can be used to generate blacklists of malicious URLs that can be blocked proactively to prevent users from visiting these known malicious sites.



PhishTank operates like URLhaus, and allows users to submit phishing artifacts which are then verified by the wider community. In the below screenshot you can see what looks like the URLhaus database.



Previous Topic
Back to Lesson
Next Topic