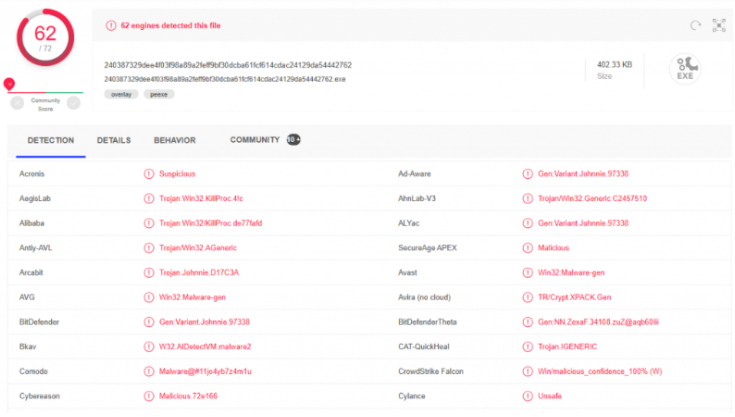
Artifact Analysis With PhishTool

This lesson is going to show how you can analyze artifacts from the PhishTool analysis console, including; WHOIS checks, VirusTotal reputation checks for MD5 hashes and URLs, URL visualization. Doing all of this within PhishTool keeps investigations streamlined and allows you to get the information you need in one place.

FILE ARTIFACT ANALYSIS

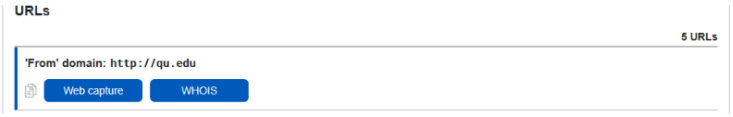
PhishTool will automatically retrieve the file name and MD5 hash from any email attachments, and the console has a button that allows us to search for the hash value in VirusTotal straight from the console. If the submitted email contains an attachment, click the following button on the right-hand side to submit it for a reputation check.

This will automatically generate a VirusTotal search query for the MD5 file hash, and open it in a new browser window.

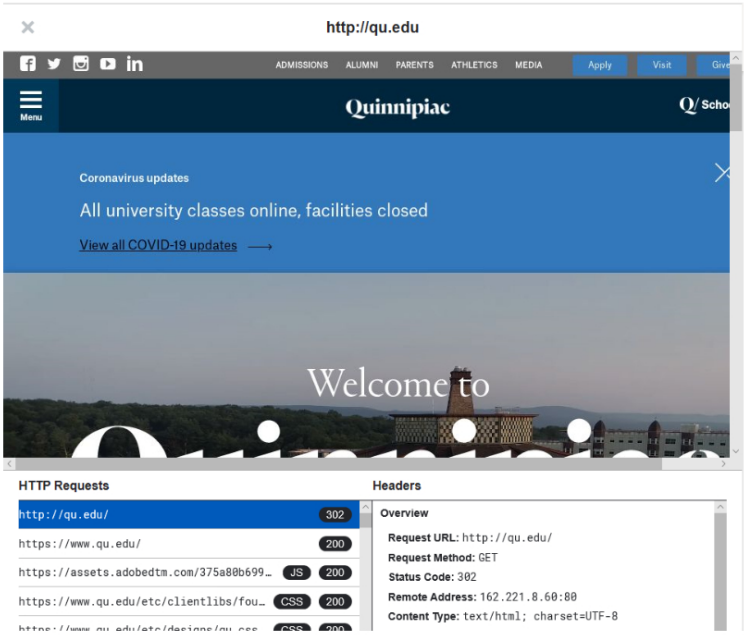


WEB ARTIFACT ANALYSIS

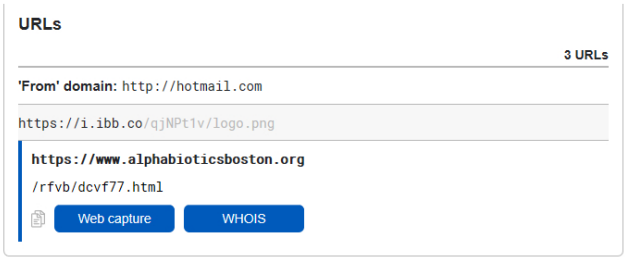
Similarly to how we use URL2PNG to visualize what is at the end of a URL, PhishTool has the ability to generate a live screenshot of a URL. If an email is submitted to PhishTool that includes any URLs, whether malicious or not, a web capture can be viewed by clicking on the URL, and selecting Web Capture.



This feature also kindly provides us with the HTTP requests made, and headers from the site.



Another analysis activity we can perform from within the PhishTool console is a WHOIS lookup, providing us with information about the domain such as where it's hosted, who owns the domain, how long it has been alive for, and contact information. Let's try a WHOIS search on a different URL from another phishing email.



Below is the sidebar that will come from the right-hand side of the analysis console, and provides us with valuable WHOIS data. From this we can see that the domain has been alive for 2643 days, the domain name was registered with Domain.com LLC, and we have some contact email addresses.

Name servers

ns3.a2hosting.com
ns4.a2hosting.com

Emails

compliance@domain-inc.net
support@ipage-inc.com

Previous Topic

Back to Lesson

Next Topic