File Reputation Tools

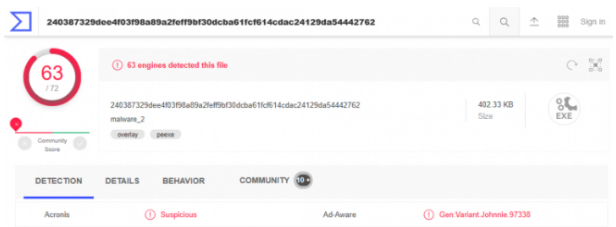
In this lesson, we will show you a couple of the many online services where you can upload suspicious attachments or their associated hashes in order to see their reputation within the security community. The tools we will cover are; VirusTotal and Talos File Reputation. This is a quick way to be able to identify if a file has been marked as malicious by the security community, without having to conduct a full analysis. **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 these files are malicious until you can prove it is safe to run.**

VIRUSTOTAL

VirusTotal is an incredible platform where you can upload files, search for IP addresses, domains, URLs, and other artifacts to retrieve a community-generated reputation value, and to see which security vendors have identified the searched artifact as malicious.

The feature we're interested in is the file upload function, where you can upload any kind of file to see more information about it.

In this example, we're going to upload an old piece of malware, which we know will be detected by a number of security vendors – this will allow you to see what malicious files look like once they've been submitted for analysis. In the below screenshot you can see that 63/72 vendors have detected this file to be malicious. In the top bar, it tells us that the file size is 402.33 KB and is a .exe file. If you upload a file that has even a few engines/vendors in red, then the file is most likely malicious in nature and defensive measures should be put in place (we'll cover this later).



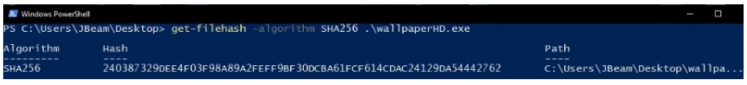
AegisLab	Trojan.Win32.KillProc.4lc	AhnLab-V3	Trojan/Win32.Generic.C2457510
Alibaba	Trojan:Win32/KillProc.da77fafd	ALYac	Gen:Variant.Johnnie.97338
Antiy-AVL	Trojan/Win32.AGeneric	SecureAge APEX	Malicious
Arcabit	Trojan.Johnnie.D17C3A	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/Crypt.XPACK.Gen
BitDefender	Gen:Variant.Johnnie.97338	BitDefenderTheta	Gen:NN.ZexaF.34104.zuZ@aqb60lii
Bkav	W32.AIDetectVM.malware2	CAT-QuickHeal	Trojan.IGENERIC
Comodo	Malware@#1ljo4yb7z4m1u	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.72e166	Cylance	Unsafe
Cyren	W32/Agent.AYT.gen!Eldorado	DrWeb	Trojan.Siggen8.20721
Emsisoft	Gen:Variant.Johnnie.97338 (B)	Endgame	Malicious (high Confidence)
eScan	Gen:Variant.Johnnie.97338	ESET-NOD32	A Variant Of Win32/Agent.VQU
F-Prot	W32/Agent.AYT.gen!Eldorado	F-Secure	Trojan.TR/Crypt.XPACK.Gen
FireEye	Generic.mg.0c4374d72e166f15	Fortinet	W32/Agent.VQU!tr
GData	Gen:Variant.Johnnie.97338	Ikarus	Trojan.Win32.Agent
Jiangmin	Trojan.Generic.cmvas	K7AntiVirus	Trojan (00497c8b1)
K7GW	Trojan (00497c8b1)	Kaspersky	HEUR:Trojan.Win32.KillProc.gen
Malwarebytes	Trojan.Dropper	MAX	Malware (ai Score=100)

It's important to remember that VirusTotal isn't a one-stop shop. A file that isn't flagging as malicious in VirusTotal could still be malicious – it just means that it hasn't been detected by security vendors yet. Whilst VT can give a good indicator as to the reputation of the file or other artifacts, further investigation should still be conducted to ensure that the file either is malicious or safe.

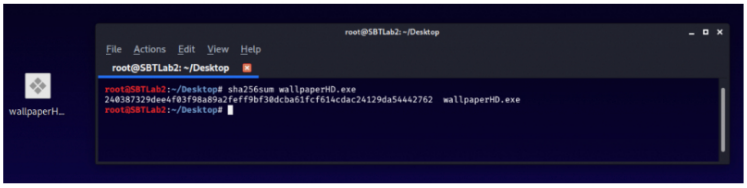
TALOS FILE REPUTATION

This service, offered by Cisco, allows us to search for SHA256 strings against their reputation database to determine if it has been classed as malicious by their products; AMP, FirePower, ClamAV, and open-source Snort product lines. This database of information is called the "Talos File Reputation system".

In the previous lesson, I covered how to retrieve file hashes in both Windows and Linux operating systems. So I'll generate a SHA256 hash using PowerShell on my Windows host, and plug that into Talos File Reputation. I'm using the same piece of malware that I submitted to VirusTotal, so we're expecting to see that it is recognized as malicious straight away.

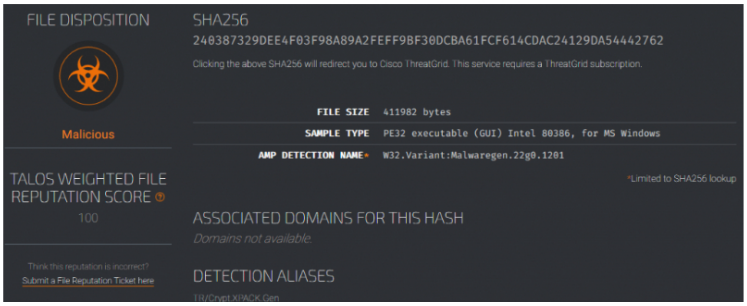


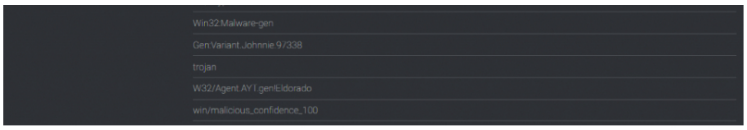
Using PowerShell on Windows to get the SHA256 hash using the "get-filehash" command with the "-algorithm sha256" switch.



Using Linux Command Line to get the SHA256 hash using the "sha256sum" command.

Now that we've retrieved the SHA256 hash value we can upload it to TFR to check the reputation of the file. The results clearly show that this file is malicious, with a score of 100 (left side). We are also provided with the file size, the type of file, the name used for detection, and other aliases used to track this specific piece of malware.





CONCLUSION

When investigating a phishing email that has an attachment, you should always include the reputation checks you performed in your report. In organizations with a dedicated security team, it is highly likely that they will have their own internal tools for sandboxing files that provide more accurate reputations cores, such as McAfee's Advanced Threat Defence (ATD). We will cover exactly how you should include this in your report in a future lesson.

Previous Topic

Back to Lesson

Next Topic