

**Blue Team Level 1 Certification
(Standard)****Introduction to BTL1**

Welcome to Blue Team Level 1

4 Topics

Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN

Introduction to Security Fundamentals

1 Topic

Soft Skills

7 Topics

Security Controls

5 Topics 1 Quiz

Networking 101

6 Topics 1 Quiz

Management Principles

4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

PA2) Types of Phishing Emails

10 Topics 2 Quizzes

PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

Section Introduction: Analysing Artifacts

Visualization Tools

URL Reputation Tools

File Reputation Tools

Malware Sandboxing

[Video] Manual Artifact Analysis

Artifact Analysis With PhishTool

[Video] Artifact Analysis with PhishTool

Activity: End of Section Review: Analysing Artifacts

PA6) Taking Defensive Actions

12 Topics 1 Quiz

PA7) Report Writing

7 Topics 1 Quiz

PA8) Phishing Response Challenge

3 Topics 1 Quiz

THREAT INTELLIGENCE DOMAIN

TI1) Introduction to Threat Intelligence

7 Topics

TI2) Threat Actors & APTs

6 Topics 2 Quizzes

TI3) Operational Threat Intelligence

7 Topics 1 Quiz

File Reputation Tools

Blue Team Level 1 Certification (Standard) > PA5) Analysing URLs, Attachments, and Artifacts > Fil...

COMPLETE



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.

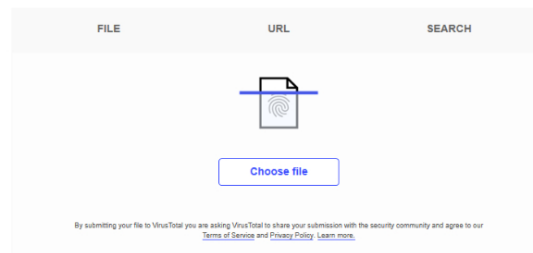
VIRUSTOTAL

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.

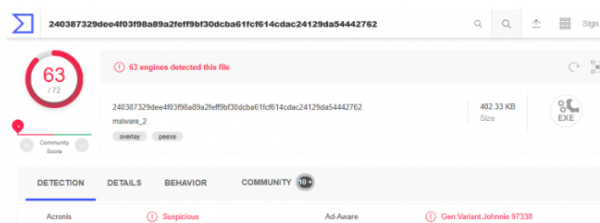
The feature we're interested in is the file upload function, where you can upload any kind of file to see more information about it.



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community



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).



I14) Iactical Threat Intelligence

7 Topics1 Quiz

T15) Strategic Threat Intelligence

5 Topics1 Quiz

T16) Malware and Global Campaigns

6 Topics1 Quiz

DIGITAL FORENSICS DOMAIN

DF1) Introduction to Digital Forensics

5 Topics

DF2) Forensics Fundamentals

10 Topics5 Quizzes

DF3) Digital Evidence Collection

8 Topics1 Quiz

DF4) Windows Investigations

3 Topics3 Quizzes

DF5) Linux Investigations

4 Topics2 Quizzes

DF6) Volatility

3 Topics1 Quiz

DF7) Autopsy

4 Topics1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM

7 Topics1 Quiz

SI2) Logging

6 Topics2 Quizzes

SI3) Aggregation

2 Topics1 Quiz

SI4) Correlation

6 Topics1 Quiz

SI5) Using Splunk

5 Topics2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response

8 Topics1 Quiz

IR2) Preparation Phase

10 Topics2 Quizzes

IR3) Detection and Analysis Phase

7 Topics4 Quizzes

IR4) Containment, Eradication, and Recovery Phase

5 Topics1 Quiz

IR5) Lessons Learned and Reporting

7 Topics

IR6) MITRE ATT&CK

13 Topics2 Quizzes

BTL1 EXAM

Exam Preparation

Using RDP and SSH

How to Start Your Exam

AngidLab	Trojan.Win32.KillProc.4tc	AbotLab-V3	Trojan.Win32.Generic.C2457510
Alibaba	Trojan.Win32.KillProc.da77af4d	ALYac	Gen.Variant.Johnnie.97338
Avily-AVL	Trojan.Win32.A.Generic	SecureAge APEX	Malicious
Accabit	Trojan.Johnnie.D17C3A	Avast	Win32.Malware-gen
AVG	Win32.Malware-gen	Avira (no cloud)	TR/Crypt.XPACK.Gen
BitDefender	Gen.Variant.Johnnie.97338	BitDefender.Theta	Gen.NN.Zenaf.34104.cz2@ap6008
Blav	W32.ADetect.VM.malware2	CAT-QuickHeal	Trojan.KOGENERIC
Comodo	Malware@f11p4y474e1fa	CrowdStrike Falcon	Win32.malicious_confidence_100% (W)
Cybereason	Malicious.72e166	Cylance	Unsafe
Cyren	W32/Agent.AYT.gen/Eldorado	DrWeb	Trojan.Siggen8.20721
Emisoft	Gen.Variant.Johnnie.97338 (B)	Endgame	Malicious (High Confidence)
eScan	Gen.Variant.Johnnie.97338	ESET-NOD32	A Variant Of Win32/Agent.VGU
F-Proit	W32/Agent.AYT.gen/Eldorado	F-Secure	Trojan.TR/Crypt.XPACK.Gen
FireEye	Generic.mg.6c4374d72e166f15	Fortinet	W32/Agent.VQJfr
GData	Gen.Variant.Johnnie.97338	Ikarus	Trojan.Win32.Agent
Jiangmin	Trojan.Generic.cmas	K7AntiVirus	Trojan (09497db1)
K7GW	Trojan (09497db1)	Kaspersky	HELR.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.

```
PS C:\Users\JBeam\Desktop> get-filehash -algorithm SHA256 .\wallpaperHD.exe
Algorithm Hash Path
-----
SHA256 240387329DEE4F03F98A89A2FEFF9BF30DCBA61FCF614CDAC24129DA54442762 C:\Users\JBeam\Desktop\wallpa...
```

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

```
root@SBTLab2: ~/Desktop
File Actions Edit View Help
root@SBTLab2: ~/Desktop
root@SBTLab2:~/Desktop# sha256sum wallpaperHD.exe
240387329DEE4F03F98A89A2FEFF9BF30DCBA61FCF614CDAC24129DA54442762 wallpaperHD.exe
root@SBTLab2:~/Desktop#
```

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.

FILE DISPOSITION

Malicious

SHA256

240387329DEE4F03F98A89A2FEFF9BF30DCBA61FCF614CDAC24129DA54442762

Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

FILE SIZE

411982 bytes

SAMPLE TYPE

PE32 executable (GUI) Intel 80386, for MS Windows

AMP DETECTION NAME

W32.Variant:Malwaregen.22g@.1201

TALOS WEIGHTED FILE REPUTATION SCORE

100

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available

DETECTION ALIASES

(1) (Copy to Clipboard)

Think this reputation is incorrect?

Submit a File Reputation Ticket here

Limited to SHA256 lookup

Win32/Malware.gen
GenVariant.Johnna.9/2008
Trojan
W32/Agent.AV1.gen/Idonado
win/malicious_confidence.100

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 >](#)[Privacy & Cookies Policy](#)