VirusTotal for SOC Analysts BY P3NGU1N

File Analysis with VirusTotal

🎯 According to the analysis report in the link, what is the creation date of the file?

https://www.virustotal.com/gui/file/415ba65e21e8de9196462b10dd17ab81d75b3e315759ecced5ea8f5812000c1b

Answer Format: YYYY-MM-DD

ANSWER: 2020-08-20

🎯 According to the VirusTotal result, how many URL addresses does the malicious file communicate with? You mus enter number.

https://www.virustotal.com/gui/file/415ba65e21e8de9196462b10dd17ab81d75b3e315759ecced5ea8f5812000c1b

ANSWER: 14

🎯 Examine the analysis report, what is the **Compilation Timestamp** of the file?

https://www.virustotal.com/gui/file/6c745b8c701574b32cce2cdec63de7e669127cc0aa6afa654165ebd46c4252b

ANSWER: 2022-07-17 22:57:46 UTC

Scanning URLs with VirusTotal

🎯 In which category is google.com classified according to Sophos?

https://www.virustotal.com/gui/url/cf4b367e49bf0b22041c6f065f4aa19f3cfe39c8d5abc0617343d1a66c6a26f5/

ANSWER: search engines

🎯 In which category is letsdefend.io classified according to Forcepoint ThreatSeeker?

https://www.virustotal.com/gui/domain/letsdefend.io/details

ANSWER: information technology

🎯 What is the name of the hash file "**349d13ca99ab03869548d75b99e5a1d0**" scanned in VirusTotal?
ANSWER: 1word.doc

Searching for IOC

🎯 Search VirusTotal for the MD5 value "**b92021ca10aed3046fc3be5ac1c2a094**". What is the First Submission date? (YYYY-MM-DD)
ANSWER: 2019-09-16

QUIZ:

🎯 **Which of the following cannot be obtained after a file analysis in VirusTotal?**
ANSWER: **File owner name**

🎯 **What information is not found in the "Details" tab after the file scan?**
ANSWER: RSA

🎯 **Which tab should we check to view the subprocesses created after the file is run?**
ANSWER: Behavior

🎯 **From which tab can we view the 'Headers' of a scanned URL address in VirusTotal?**
ANSWER: Details

🎯 **Which button should be clicked to rescan the URL/File found in an old report?**
ANSWER: **Re-analyse**

🎯 **Which of the following cannot be reached for malware scanned in VirusTotal?**
ANSWER: **The person who created the file**

🎯 **Which one is not found in the "Details > History" section of a scanned file report?**

ANSWER: **First infected date**

🎯 **What information can you access in the "Relations" tab of the analysis results?**

ANSWER: **Contacted Domains**

🎯 **Which one is not one of the tabs in the analysis reports?**

ANSWER: **Result**

🎯 **What is shown in the “Detection” tab in the reports?**

ANSWER: **Security Vendors analysis**