

Remote Working [Let's Defend – Write-up]

Analysis XLS File

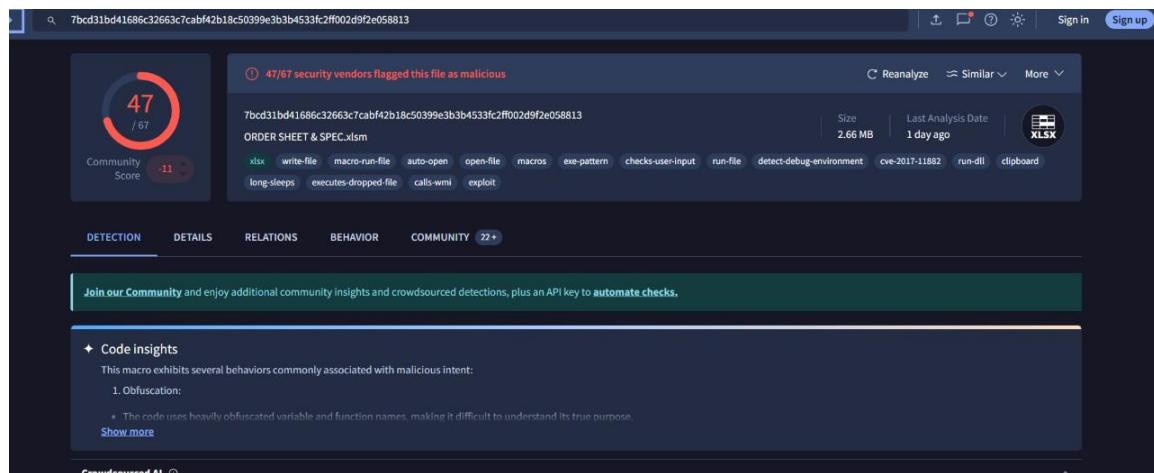
File link: /root/Desktop/ChallengeFiles/ORDER_SHEET_SPEC.zip

Password: infected

| Start investigation

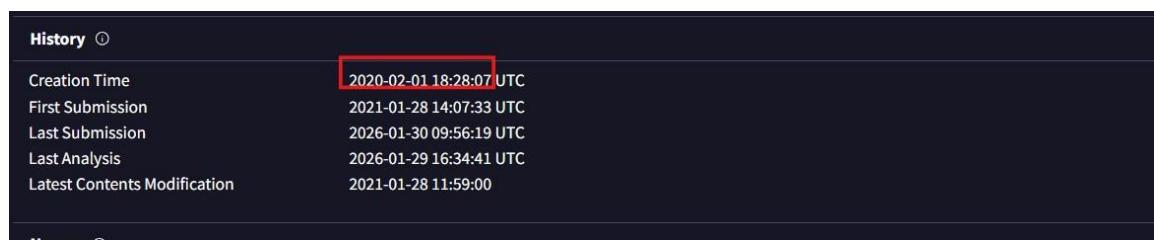
First, I want to calculate the hash so I can search on virstotal.

```
root@ip-172-31-14-26:~/Desktop/ChallengeFiles# sha256sum 'ORDER SHEET & SPEC.xlsx'
7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813  ORDER SHEET & SPEC.xlsx
root@ip-172-31-14-26:~/Desktop/ChallengeFiles#
```



The screenshot shows the Virstotal analysis interface for the file 'ORDER SHEET & SPEC.xlsx'. The file has a community score of 47/67. It is flagged as malicious by 47 security vendors. The file is an XLSX document (2.66 MB) last analyzed 1 day ago. The detection panel lists various behaviors: write-file, macro-run-file, auto-open, open-file, macros, exe-pattern, checks-user-input, run-file, detect-debug-environment, run-dll, and clipboard. A green bar at the bottom encourages joining the community.

**Q1: What is the date the file was created? (UTC) Answer Format:
YYYY-MM-DD HH:MM:SS**



The screenshot shows the Virstotal History section for the file. The creation time is listed as 2020-02-01 18:28:07 UTC. Other submission and analysis dates are also listed: First Submission (2021-01-28 14:07:33 UTC), Last Submission (2026-01-30 09:56:19 UTC), Last Analysis (2026-01-29 16:34:41 UTC), and Latest Contents Modification (2021-01-28 11:59:00).

Go to Details after that see the History.

Answer: 2020-02-01 18:28:07.

Q2: With what name is the file detected by Bitdefender antivirus?

The screenshot shows the Crowdsource AI interface. At the top, it says "Hispasec flags this file as malicious" with a note: "The macros extracted from the document exhibit several signs of malicious intent, as outlined below." Below this, there's a "Show more" link. The interface includes popular threat labels (trojan.acao/docdl), threat categories (trojan, downloader, dropper), and family labels (acao, docdl, valyria). A section for "Security vendors' analysis" lists various vendors and their detections. BitDefender is highlighted with a red box around its entry: "BitDefender | Trojan.GenericKD.36266294". Other entries include AhnLab-V3, AliCloud, Antiy-AVL, Avast, Avira (no cloud), ClamAV, and Cynet. To the right, there's a section for "Do you want to automate checks?" with a "Yes" button.

In Home page of Virstotal I get the answer.

Answer: trojan.generickd.36266294

Q3: How many files are dropped on the disk?

The screenshot shows the Virstotal interface with a table titled "Dropped Files (29)". The columns are "Scanned", "Detections", "File type", and "Name". The data is as follows:

Scanned	Detections	File type	Name
2025-07-14	0 / 61	HTML	identification
2024-08-05	0 / 65	JSON	SOPHIA.json
2025-03-06	18 / 61	PHP	asc.txt:script1.vbs
2026-01-25	0 / 62	HTML	9zwb1q3Fsd1g
2025-07-14	30 / 62	VBA	xx
2025-02-28	21 / 61	HTML	q
2024-06-05	0 / 62	JSON	SOPHIA.json
2026-01-20	0 / 61	XML	0AD2E627-3991-4646-B250-5A814425C9AD
2026-01-29	2 / 62	Windows Enhanced Metafile	image1.emf
2025-06-16	0 / 62	Text	?????? ?? ??????? 000000709 ?? 05.03.2024.pdf.Zone.Identifier

Go to Details after that see the Dropped Files above the Total.

Answer: 29

Q4: What is the sha-256 hash of the file with emf extension it drops?

Dropped Files (29)			
Scanned	Detections	File type	Name
2025-07-14	0 / 61	HTML	identification
2024-08-05	0 / 65	JSON	SOPHIA.json
2025-03-06	18 / 61	PHP	asc.txt;script1.vbs
2026-01-25	0 / 62	HTML	9zwbh3f5dfg
2025-07-14	30 / 62	VBA	xx
2025-02-28	21 / 61	HTML	q
2024-06-05	0 / 62	JSON	SOPHIA.json
2026-01-20	0 / 61	XML	0AD2E627-3991-4646-B250-5A814425C9AD
2026-01-29	2 / 62	Windows Enhanced Metafile	image1.emf
2025-06-16	0 / 62	Text	?????? ? ??????? 000000709 ?? 05.03.2024.pdf;Zone.Identifier
2026-01-09	0 / 61	HTML	403.html
2026-01-10	0 / 61	CAB	77EC63BDA74BD00D0E0426DC8F8008506

in drooped files just click on it after that you will get the hash above.

The screenshot shows a malware analysis interface. At the top, a search bar contains the hash: 979dde2aed02f077c16ae53546c6df9eed40e8386d6db6fc36aee9f966d2cb82. Below the search bar, a circular 'Community Score' icon shows a score of 2/62. A message indicates that 2/62 security vendors flagged this file as malicious. The file name 'image1.emf' is listed, along with its extension 'emf'. To the right, file details are shown: Size 4.85 KB and Last Analysis Date 1 day ago. Below the main content, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY, with the DETECTION tab currently selected. A green banner at the bottom encourages joining the community.

Answer: 979dde2aed02f077c16ae53546c6df9eed40e8386d6db6fc36aee9f966d2cb82

Q5: What is the exact url to which the relevant file goes to download spyware?

Go to Relations after that you will see the Url

The screenshot shows a malware analysis interface for the file 'ORDER SHEET & SPEC.xlsx'. The file is flagged as malicious by 47/67 security vendors. The file details include a size of 2.66 MB and a last analysis date of 1 day ago. Below the file details, a list of detected behaviors includes: xlsx, write-file, macro-run-file, auto-open, open-file, macros, exe-pattern, checks-user-input, run-file, detect-debug-environment, long-sleeps, executes-dropped-file, calls-wmi, exploit, cve-2017-11882, run-dll, clipboard. Below the file details, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY, with the RELATIONS tab currently selected. A green banner at the bottom encourages joining the community. Under the RELATIONS tab, a section titled 'Contacted URLs (2)' lists two URLs. The second URL, 'https://multiwaretecnologia.com.br/js/podaliri4.exe', is highlighted in red.

Answer: https://multiwaretecnologia.com.br/js/podaliri4.exe

Summary

This investigation into the ORDER_SHEET_SPEC sample was highly educational and greatly improved my malware analysis workflow. It taught me how to effectively pivot between VirusTotal's tabs to extract deep forensic details, such as tracking file creation history and identifying specific antivirus detections like Bitdefender's Trojan labels. I also gained practical experience in mapping out the 'Dropped Files' section to find specific artifacts, such as the .emf file and its SHA-256 hash.