

# 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 virustotal.

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

7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813

47/67 security vendors flagged this file as malicious

Reanalyze Similar More

7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2ff002d9f2e058813

Size 2.66 MB Last Analysis Date 1 day ago

ORDER SHEET & SPEC.xlsm

write-file macro-run-file auto-open open-file macros exe-pattern checks-user-input run-file detect-debug-environment cve-2017-11882 run-dll clipboard

long-sleeps executes-dropped-file calls-wmi exploit

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 22+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Code insights

This macro exhibits several behaviors commonly associated with malicious intent:

1. Obfuscation:

- The code uses heavily obfuscated variable and function names, making it difficult to understand its true purpose.

Show more

Crowdsourced AI

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

History	
Creation Time	2020-02-01 18:28:07 UTC
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
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 VirusShare analysis page for a file. At the top, a Crowdsourced AI section indicates the file is malicious. Below this, the Popular threat label is 'trojan.acao/docdl'. The Threat categories are 'trojan', 'downloader', and 'dropper'. The Family labels are 'acao', 'docdl', and 'valyria'. The Security vendors' analysis section shows a table of detections from various vendors. The BitDefender entry is highlighted with a red box, showing the detection name 'Trojan.GenericKD.36266294'.

Vendor	Detection
AhnLab-V3	OLE/Cve-2017-11882.Gen
AllCloud	Trojan:MSOffice/Downloader.ahm
Antiy-AVL	Trojan(Downloader)/MSOffice.Agent
Avast	VBA:Dropper-AN [Trj]
Avira (no cloud)	VBS/Dldr.Agent.VPNI
<b>BitDefender</b>	<b>Trojan.GenericKD.36266294</b>
ClamAV	Xls.Dropper.Valyria-10030821-0
Cynet	Malicious (score: 99)

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 'Dropped Files (29)' section of the VirusShare analysis page. It displays a table with columns for Scanned date, Detections, File type, and Name. The table lists 29 files that were dropped on the disk. The total number of files is 29, as indicated by the 'Dropped Files (29)' header.

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	9zwblq3Fsdfg
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.bts.cript1.vbs
2026-01-25	0 / 62	HTML	9zwblq3Fsdffg
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	77EC63BDA74BD0D0E0426DC8F8008506

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

979dde2aed02f077c16ae53546c6df9eed40e8386d6db6fc36aee9f966d2cb82

image1.emf

Size: 4.85 KB | Last Analysis Date: 1 day ago

**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

7bcd31bd41686c32663c7cabf42b18c50399e3b3b4533fc2f002d9f2e058813

ORDER SHEET & SPEC.xlsm

Size: 2.66 MB | Last Analysis Date: 1 day ago

Relations

Scanned	Detections	Status	URL
2025-11-28	0 / 98	200	http://ocsp.pki.goog/gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGGUABBTgXIsxbrv2lBKpPoiEVRE6ghlCnAQUm+HV2ccHsBqBt5ZLJot39wZh4CDQHjtJqhYqpgSVpULg=
2026-01-20	8 / 97	403	https://multiwaretecnologia.com.br/js/podaliri4.exe

**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.