

# MSHTML [Let's defend – Write-up]

2021's 0-Day MSHTML

file location: /root/Desktop/ChallengeFiles/Employee\_W2\_Form.docx  
file location2: /root/Desktop/ChallengeFiles/Employees\_Contact\_Audit\_Oct\_2021.docx  
file location3: /root/Desktop/ChallengeFiles/Work\_From\_Home\_Survey.doc  
file location4: /root/Desktop/ChallengeFiles/income\_tax\_and\_benefit\_return\_2021.docx

## | Start Investigation

```
root@ip-172-31-3-35:~/Desktop/Tools# python3 zipdump.py /root/Desktop/ChallengeFiles/Employees_Contact_Audit_Oct_2021.docx
Index Filename          Encrypted Timestamp
 1 [Content_Types].xml      0 1980-01-01 08:00:00
 2 _rels/                  0 2021-09-01 23:23:30
 3 _rels/.rels              0 1980-01-01 08:00:00
 4 docProps/               0 2021-09-01 23:23:30
 5 docProps/app.xml        0 1980-01-01 08:00:00
 6 docProps/core.xml       0 1980-01-01 08:00:00
 7 word/                   0 2021-09-01 23:23:30
 8 word/_rels/              0 2021-09-01 23:23:30
 9 word/_rels/document.xml.rels 0 2021-09-10 16:37:10
10 word/document.xml       0 2021-09-01 23:23:30
11 word/fontTable.xml     0 1980-01-01 08:00:00
12 word/media/             0 2021-09-01 23:23:30
13 word/media/image1.wmf   0 1980-01-01 08:00:00
14 word/settings.xml       0 1980-01-01 08:00:00
15 word/styles.xml         0 1980-01-01 08:00:00
16 word/theme/             0 2021-09-01 23:23:30
17 word/theme/theme1.xml   0 1980-01-01 08:00:00
18 word/webSettings.xml    0 1980-01-01 08:00:00
root@ip-172-31-3-35:~/Desktop/Tools#
```

To enhance our analysis, we can pipe the output into another powerful tool developed by Didier Stevens: re-search.py.

re-search.py is a specialized utility that leverages regular expressions (regex) to parse and search through data. It allows you to utilize a built-in library of common patterns or define your own custom expressions for more targeted searches.

By combining zipdump and re-search, we can execute a command that dumps all file indexes from the sample and pipes them directly into the search tool. We will then apply specific filters to automatically identify and extract all unique IPv4 addresses from the output.

## Q1: Examining the Employees\_Contact\_Audit\_Oct\_2021.docx file, what is the malicious IP in the docx file?

Analyzing OOXML Files with zipdump.py

Since .docx files are essentially compressed ZIP archives, we can explore their internal structure using zipdump.py (by Didier Stevens), as recommended in the SANS cheat sheet.

To examine the contents of the document, run the following command:

```
python3 zipdump.py  
/root/Desktop/ChallengeFiles/Employees_Contact_Audit_Oct_2021.docx
```

```
root@ip-172-31-3-35:~/Desktop/Tools# python3 zipdump.py -D /root/Desktop/ChallengeFiles/Employees_Contact_Audit_Oct_2021.docx | python3 re-search.py -n -u ipv4  
175.24.190.249  
root@ip-172-31-3-35:~/Desktop/Tools#
```

**Answer:** 175.24.190.249.

## Q2: Examining the Employee\_W2\_Form.docx file, what is the malicious domain in the docx file?

To answer the question, I extracted the file hash and searched in Virustotal.

```
root@ip-172-31-3-35:~/Desktop/ChallengeFiles# ls  
Employee_W2_Form.docx          Work_From_Home_Survey.doc  
Employees_Contact_Audit_Oct_2021.docx  income_tax_and_benefit_return_2021.docx  
root@ip-172-31-3-35:~/Desktop/ChallengeFiles# md5sum Employee_W2_Form.docx  
45e7d6562bfddb816d45649dd667abde  Employee_W2_Form.docx  
root@ip-172-31-3-35:~/Desktop/ChallengeFiles#
```

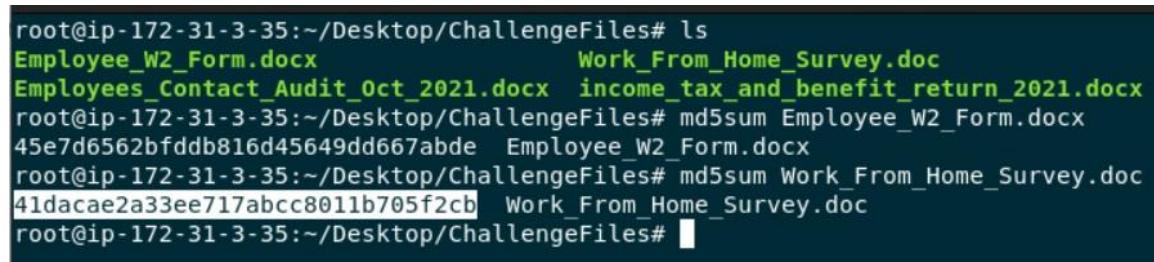
The screenshot shows the Virustotal analysis interface for the file 679bbe0c50754853978a3a583505eb99bce720cf26a6aa8be06cd879701ff1. It displays three analysis reports:

- Joe Sandbox Analysis:** Verdict: MAL, Score: 64/100, Threat Name: CVE-2021-40444. Domains: prod-wus-resolver.naturallanguageeditorservice.osi.office.net.akadns.net s-0005.dual-s-msedge.net mira-ofc.tm-4.office.com editor.svc.cloud.microsoft roaming.svc.cloud.microsoft Hosts: 52.110.2.130 72.154.7.38. HTML Report: <https://www.joesandbox.com/analysis/1857440/0/html>. PDF Report: <https://www.joesandbox.com/analysis/1857440/0/pdf>. Executive Report: <https://www.joesandbox.com/analysis/1857440/0/executive>.
- FileScanIO Analysis:** Verdict: MALICIOUS, Confidence: 100/100. Tags: docx,oxml. Domains: arsenal.30cm.tw. Hosts: 128.199.107.104,128.199.107.104. Report: <https://www.filescan.io/reports/679bbe0c50754853978a3a583505eb99bce720cf26a6aa8be06cd879701ff1/e005d7c3-4b01-4456-bb5d-38af2b8a4a66>.
- VirusShare Analysis:** Verdict: UNKNOWN, Confidence: 0/100. Domains: arsenal.30cm.tw. Hosts: 128.199.107.104,128.199.107.104. Report: <https://virusshare.com/report/679bbe0c50754853978a3a583505eb99bce720cf26a6aa8be06cd879701ff1>.

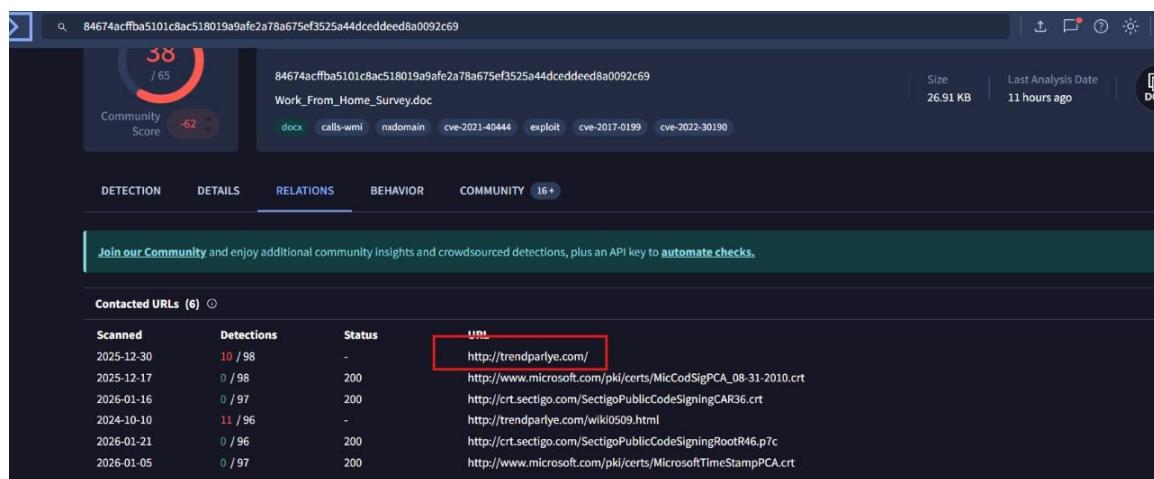
**Answer:** arsenal.30cm.tw

### **Q3: Examining the Work\_From\_Home\_Survey.doc file, what is the malicious domain in the doc file?**

Also to answer this question, I extracted the file hash and searched in Virustotal.



```
root@ip-172-31-3-35:~/Desktop/ChallengeFiles# ls
Employee_W2_Form.docx          Work_From_Home_Survey.doc
Employees_Contact_Audit_Oct_2021.docx  income_tax_and_benefit_return_2021.docx
root@ip-172-31-3-35:~/Desktop/ChallengeFiles# md5sum Employee_W2_Form.docx
45e7d6562bfddb816d45649dd667abde  Employee_W2_Form.docx
root@ip-172-31-3-35:~/Desktop/ChallengeFiles# md5sum Work_From_Home_Survey.doc
41dacae2a33ee717abcc8011b705f2cb  Work_From_Home_Survey.doc
root@ip-172-31-3-35:~/Desktop/ChallengeFiles#
```



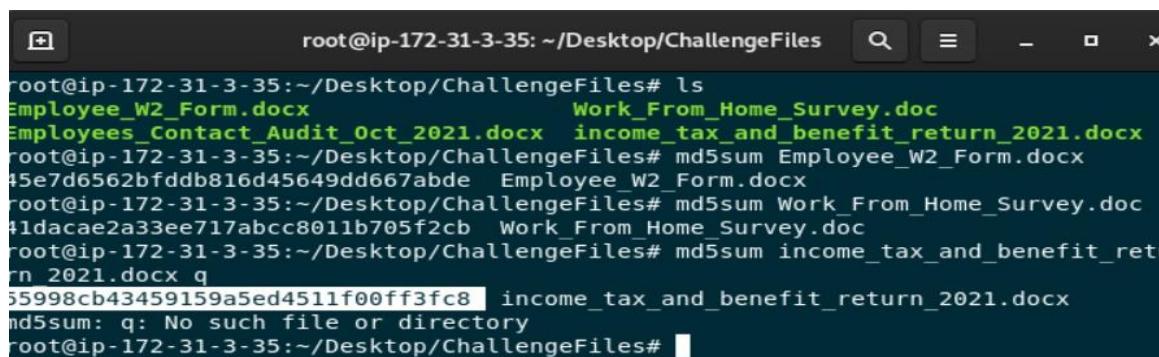
The screenshot shows the VirusTotal analysis page for the file 84674acffba5101c8ac518019a9afe2a78a675ef3525a44dceddeed8a0092c69. The file is a Microsoft Word document (docx). The analysis results show detections from various sources, including Trend Micro (10/98), Microsoft (0/98), Sectigo (0/97), and TrendParty (11/96). The file size is 26.91 KB and was last analyzed 11 hours ago. A table titled "Contacted URLs (6)" lists the URLs that were detected in the file:

Scanned	Detections	Status	URL
2025-12-30	10 / 98	-	http://trendparlye.com/
2025-12-17	0 / 98	200	http://www.microsoft.com/pki/certs/MicCodSigPCA_08-31-2010.crt
2026-01-16	0 / 97	200	http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt
2024-10-10	11 / 96	-	http://trendparlye.com/wiki0509.html
2026-01-21	0 / 96	200	http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c
2026-01-05	0 / 97	200	http://www.microsoft.com/pki/certs/MicrosoftTimeStampPCA.crt

**Answer:** trendparlye.com

### **Q4: Examining the income\_tax\_and\_benefit\_return\_2021.docx, what is the malicious domain in the docx file?**

Also to answer this question, I extracted the file hash and searched in Virustotal.



```
root@ip-172-31-3-35:~/Desktop/ChallengeFiles# ls
Employee_W2_Form.docx          Work_From_Home_Survey.doc
Employees_Contact_Audit_Oct_2021.docx  income_tax_and_benefit_return_2021.docx
root@ip-172-31-3-35:~/Desktop/ChallengeFiles# md5sum Employee_W2_Form.docx
45e7d6562bfddb816d45649dd667abde  Employee_W2_Form.docx
root@ip-172-31-3-35:~/Desktop/ChallengeFiles# md5sum Work_From_Home_Survey.doc
41dacae2a33ee717abcc8011b705f2cb  Work_From_Home_Survey.doc
root@ip-172-31-3-35:~/Desktop/ChallengeFiles# md5sum income_tax_and_benefit_return_2021.docx
55998cb43459159a5ed4511f00ff3fc8  income_tax_and_benefit_return_2021.docx
md5sum: q: No such file or directory
root@ip-172-31-3-35:~/Desktop/ChallengeFiles#
```

The screenshot shows the VirusTotal analysis page for the file `income_tax_and_benefit_return_2021.docx`. The file was uploaded on 2022-01-30. It has a community score of -36 and a size of 23.61 KB. The last analysis date is 4 days ago. The file type is docx, and it is associated with CVE-2021-40444, CVE-2022-30190, CVE-2017-0199, exploit, and calls-wmi. The detection tab is selected, showing no detections. The relations tab is also present.

Answer: hidusi.com

## Q5: What is the vulnerability the above files exploited?

The answer is also found in VirusTotal.

The screenshot shows the VirusTotal analysis page for the same file. The community score is now 45. There are 45 detections from 67 security vendors. The file was uploaded on 2022-01-30. It has a size of 23.61 KB and a last analysis date of 4 days ago. The file type is docx, and it is associated with CVE-2021-40444, CVE-2022-30190, CVE-2017-0199, exploit, and calls-wmi. The detection tab is selected, showing multiple detections. The details tab is also present.

Answer: cve-2021-40444

## **Summary**

By analyzing multiple samples like Employee\_W2\_Form.docx and Work\_From\_Home\_Survey.doc, I learned how to use zipdump.py and re-search.py to peel back the layers of OOXML structures and extract hidden malicious IPs and domains. This lab was particularly beneficial because it demonstrated the "real-world" transition from a simple document to a network-based attack, showing me how to pivot from local file analysis to global threat intelligence tools like VirusTotal to identify specific vulnerabilities.