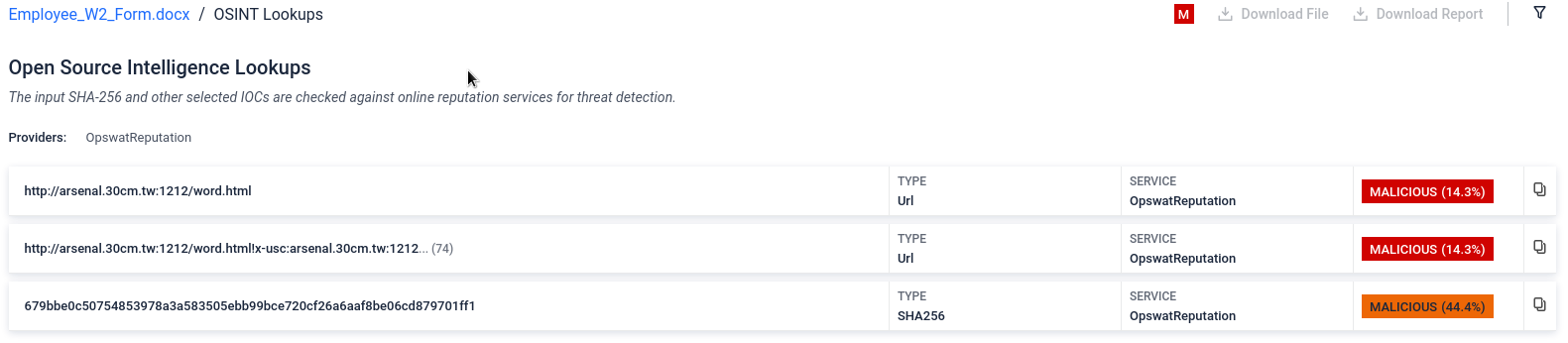
I’m going to be completing LetsDefend’s 2021's [0-Day MSHTML](https://app.letsdefend.io/challenge/mshtml) challenge.

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

By collecting the MD5 hash of the file using the md5sum command and inserting the result into [VirusTotal](https://www.virustotal.com/gui/file/ed2b9e22aef3e545814519151528b2d11a5e73d1b2119c067e672b653ab6855a/details), the top connecting IP result is 175.23.190.249.

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

Repeating the same steps from the previous question, placing the MD5 hash of the docx file into VirusTotal shows a [filescan](https://www.filescan.io/reports/679bbe0c50754853978a3a583505ebb99bce720cf26a6aaf8be06cd879701ff1/b03b8963-237c-4515-8bd8-acf632ba21fd/osint) result in the comment fields leading to several OSINT lookups. The resulting malicious domain being “arsenal.30cm.tw”.



1. Examining the Work\_From\_Home\_Survey.doc file, what is the malicious domain in the doc file?

Searching [VirusTotal](https://www.virustotal.com/gui/file/84674acffba5101c8ac518019a9afe2a78a675ef3525a44dceddeed8a0092c69) by the collected file’s MD5 hash, the top connected URL and malicious domain is “trendparlye.com”.

1. Examining the income\_tax\_and\_benefit\_return\_2021.docx, what is the malicious domain in the docx file?

Searching [VirusTotal](https://www.virustotal.com/gui/file/d0e1f97dbe2d0af9342e64d460527b088d85f96d38b1d1d4aa610c0987dca745) by the collected file’s MD5 hash, the top connected URL and malicious domain is “hidusi.com”.

1. What is the vulnerability the above files exploited?

When comparing the three VirusTotal results, the vulnerability that the filies exploited was cve-2021-40444