Metadata Analysis

LCE

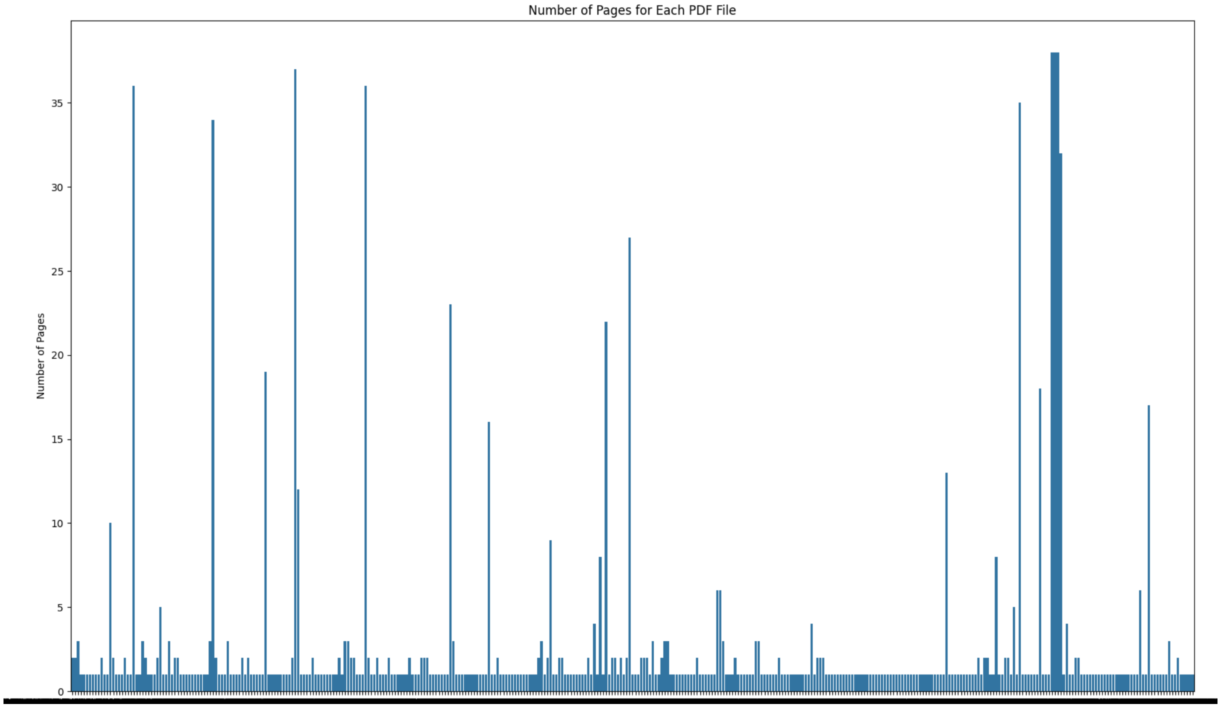
Domenic Lo Iacono

Table of Contents

Executive Summary

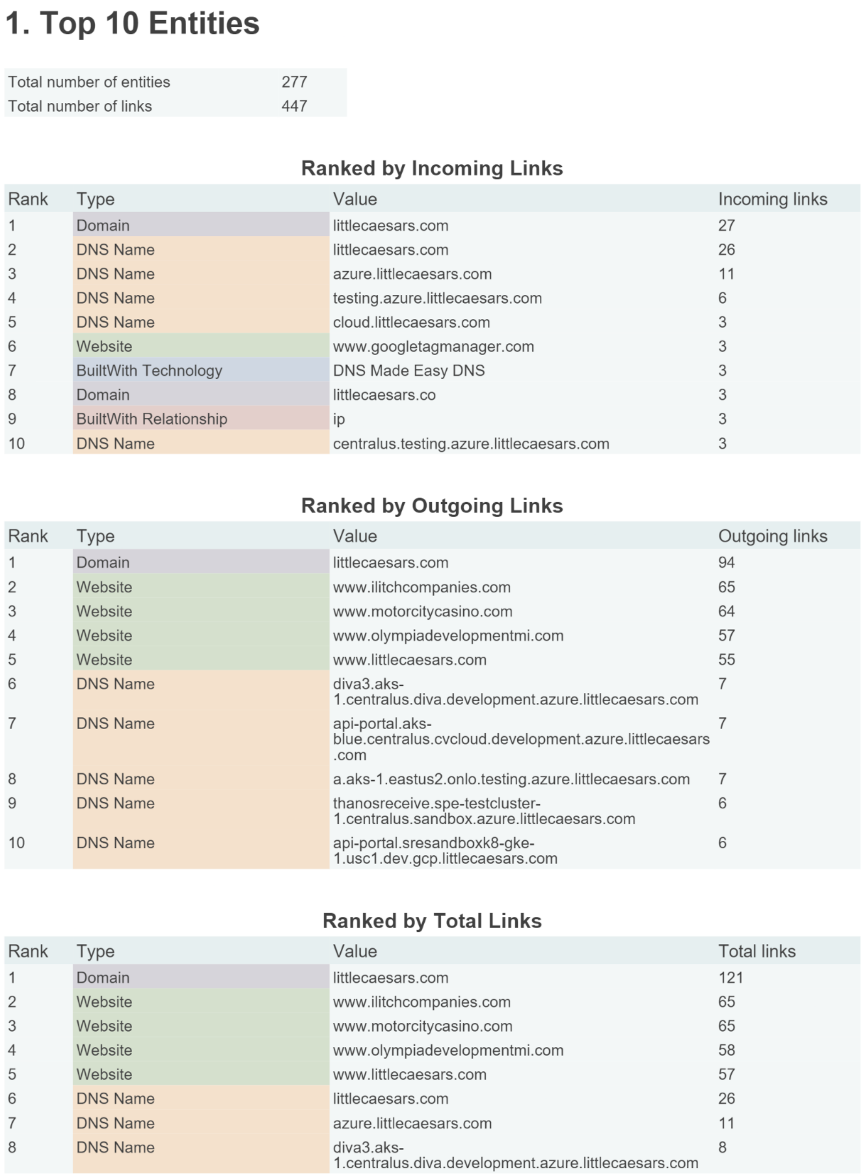
Findings

A total of 394 files were collected with a total size of 10.9MB. These files were collected via an advanced Google search within the domains of littlecaesars.com, motorcitycasino.com, 313presents.com, olympiadevelopmentmi.com, and ilitchcompanies.com. All of the files found are PDF files but searches were conducted for a variety of common file types across all domains. Using Exiftool and python, metadata was collected from the documents to reveal additional information including, but not limited to, the listed author, the software that was used to create the document, and the creation date. This data is stored as json files and can be used in tandem with python to create graphs and sort the data. One such graph is seen below which displays the number of pages each document has.



None of the documents themselves have any kind of PII or sensitive information and the metadata collected also does not contain any PII. Additionally, metadata revealed that a majority of the files collected were exported as a PDF and that the original file was created with a different extension like .docx or .ppt.

Another tool that was utilized to collect metadata across the listed domains was Maltego. Using Maltego DNS/Network metadata was collected to identify the domains and their connections amongst themselves as well as collect past versions of the site using the Wayback Machine from archive.org.



1. Top 10 Entities

Total number of entities	277
Total number of links	447

Ranked by Incoming Links

Rank	Type	Value	Incoming links
1	Domain	littlecaesars.com	27
2	DNS Name	littlecaesars.com	26
3	DNS Name	azure.littlecaesars.com	11
4	DNS Name	testing.azure.littlecaesars.com	6
5	DNS Name	cloud.littlecaesars.com	3
6	Website	www.googletagmanager.com	3
7	BuiltWith Technology	DNS Made Easy DNS	3
8	Domain	littlecaesars.co	3
9	BuiltWith Relationship	ip	3
10	DNS Name	centralus.testing.azure.littlecaesars.com	3

Ranked by Outgoing Links

Rank	Type	Value	Outgoing links
1	Domain	littlecaesars.com	94
2	Website	www.ilitchcompanies.com	65
3	Website	www.motorcitycasino.com	64
4	Website	www.olympiadevelopmentmi.com	57
5	Website	www.littlecaesars.com	55
6	DNS Name	diva3.aks-1.centralus.diva.development.azure.littlecaesars.com	7
7	DNS Name	api-portal.aks-blue.centralus.cvcloud.development.azure.littlecaesars.com	7
8	DNS Name	a.aks-1.eastus2.onlo.testing.azure.littlecaesars.com	7
9	DNS Name	thanosreceive.spe-testcluster-1.centralus.sandbox.azure.littlecaesars.com	6
10	DNS Name	api-portal.sresandboxk8-gke-1.usc1.dev.gcp.littlecaesars.com	6

Ranked by Total Links

Rank	Type	Value	Total links
1	Domain	littlecaesars.com	121
2	Website	www.ilitchcompanies.com	65
3	Website	www.motorcitycasino.com	65
4	Website	www.olympiadevelopmentmi.com	58
5	Website	www.littlecaesars.com	57
6	DNS Name	littlecaesars.com	26
7	DNS Name	azure.littlecaesars.com	11
8	DNS Name	diva3.aks-1.centralus.diva.development.azure.littlecaesars.com	8

Above is a collection of tables that outlines some entities and their links. Using this in combination with the original graph reveals some data about the network architecture including different DNS servers, services that are related to those servers, and more.

Analysis

Analysis of the documents collected revealed several points of interest that could be used in the aid of a cyber attack. This includes but is not limited to, author(s) of the document, the software and its version used to create the document, and finally email addresses and usernames. This combination of data is not a complete exploit of any kind but could be used to build an attack. In other words the data collected is part of what an attacker would perform as reconnaissance. Using techniques related to a social engineering attack against those identified in the metadata a plan of attack could be created. This can be mapped out using the MITRE ATT&CK framework.

1. (Search Open Websites/Domains) https://attack.mitre.org/techniques/T1593/
2. (Stage Capabilities) https://attack.mitre.org/techniques/T1608/
3. (Develop Capabilities) https://attack.mitre.org/techniques/T1587/
4. (Phishing) https://attack.mitre.org/techniques/T1566/

The framework can be used past the point of initial access but is out of scope for this analysis.

A similar approach can be followed for metadata collected using Maltego. A majority of the data collected from this approach was network related and as such would be better utilized for a network or web application based attack in order to obtain initial access.

1. (Search Open Websites/Domains) https://attack.mitre.org/techniques/T1593/
2. (Stage Capabilities) https://attack.mitre.org/techniques/T1608/
3. (Develop Capabilities) https://attack.mitre.org/techniques/T1587/
4. (Exploit Public-Facing Application) https://attack.mitre.org/techniques/T1190/
5. (External Remote Services) https://attack.mitre.org/techniques/T1133/

Furthermore, a combination of the metadata collected could be used in tandem to create an attack that may be more effective. Although it should be noted that in a full scale penetration test additional data collection would likely be collected.