We have known malicious domain registrations from the Area 1 Burisma report:

- cubenergy-my-sharepoint.com
- soros-my-sharepoint.com
- hudsonorg-my-sharepoint.com
- mail.esco-plvnlch.com
- kub-gas.com
- mail.kub-gas.com

What is the information we have about these domains?

Zone File

DomainTools.com

DNS queries

DNS Enumeration

.COM Domains with "-sharepoint" or "-my-sharepoint" in them

GitHub Notebook Link

Found a lot less than I thought I would. Waiting to hear back about update zone file data

3rd level doppleganger total search.

Use data from Rapid7 to create domain names and search for them.

Frequency Analysis. Trying to find delimiters in order to algorithmically create combinations of 3rd and 2nd.

Question:
Can we algorithmically find **"-my-"?**

GitHub Notebook Link

3rd/2nd level domain name analysis.

Question: is this domain name a good representation? For example using williams.com

williams-my-sharepoint.com
Yes, because "williams" legit:
sharepoint: legit
-my-: legit delimiter

mail-williams.com
Yes, because "williams" legit.
mail: legit

Allen-Williams.com
No
"williams" legit:
allen: not a top 3rd level or existing 3rd level.

tedWilliams.com
Maybe
Yes if ted.williams.com is found in Rapid7.
No if not found.

Is Rapid7 valid for a base line?

Where does Rapid7 data come from?

DNS Enumeration

Downloaded Kali. Trying their DNS Enumeration tools

SubBrute

Use Kali Tools

Analyze Log file:

GitHub Link