Azure Storage Blobs OSINT

Introduction

Azure learned from the early days of AWS S3 and implemented a secure by a default setting for the access permission of objects within. By using the policy of default deny, you have to (just like AWS S3 now) explicitly set access permission for objects and containers.

What are we going to cover?

This chapter covers some common reconnaissance and attack techniques you can apply to find and work with Azure Blob Storage objects

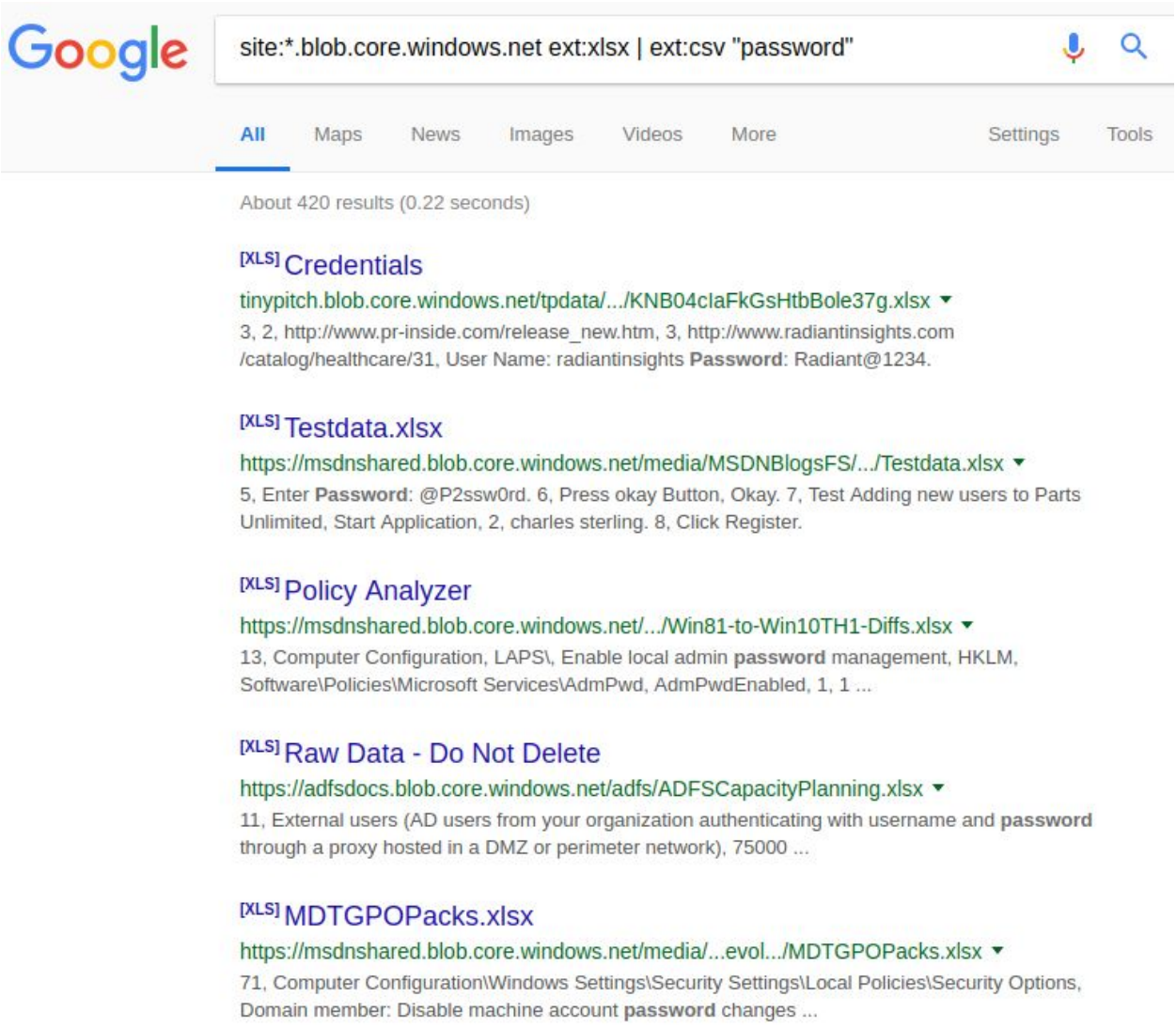
Attacking Azure Block Blobs

Let's take a look at some common techniques of identifying open Azure Block Blobs. The interesting thing about Azure Blob Storage's naming convention is that we can use DNS tools to identify if a Blob exists or not based on A records as all Blobs on Azure can be reached using a subdomain of blob.core.windows.net

Using Google to find Azure Blobs

1. Google search for site:*.blob.core.windows.net
2. This shows a list of Blob Storage that are deliberately or accidentally configured to be open to the Internet.
3. A specific search query to search for content inside Containers can be made such as the following query site:*.blob.core.windows.net ext:xlsx | ext:csv "password"

Do not click on any search results



Using DNS Enumeration

An Azure Blobs path is an FQDN and has an A record that is pointing to a Microsoft owned IP address. Therefore, any subdomain enumeration tool that either checks the existence of the A record for a domain name or checks for HTTP status codes can be used to find Azure Blobs.

We can use a tool like dnscan with a sample dictionary to see how this works. Also, for specific engagements, you will need to create custom dictionaries based on the target, the products or services they sell, etc.

On the attacker machine, clone the dnscan repo:

- git clone https://github.com/rbsec/dnscan.git

- cd dnscan
- pip install -r requirements.txt

1. Run the following command to use dnscan to identify Azure Blob names from the top 100 most common subdomain names

- python dnscan.py -d blob.core.windows.net -w subdomains-100.txt

Remember, the dictionary we used is a generic one. To obtain better results we would need to append/prepend/edit the names here.

OSINT to find interesting Azure SQL Databases

1. The Azure SQL database server endpoint name will be of the form ??.database.windows.net
2. Performing searches on the Internet for this particular string can yield interesting results. Essentially, database endpoint names and potential credentials can be found by using Google to search for:

- "database.windows.net" site:pastebin.com