Domain Name Management Deadlock

written by Mert SARICA | 1 November 2019

Domain name (domain) management can sometimes become an insurmountable issue for large and medium-sized organizations when the process is not well managed. The ability of business and information technology units to independently purchase domain names in accordance with their needs, manage and renew these domains, and use these domain names in their correspondence with customers, from websites to email templates, as a link in their signatures, can turn into an opportunity for malicious individuals if there is even the slightest communication problem between units, causing the domain name inventory to be out of date.

Let’s consider a scenario: a domain name used in campaigns for years by an organization, embedded in the main website’s theme and email templates, has been retired over the years and therefore, its registration has been deleted because it was not renewed. Since the relevant parties were not aware of this situation, the domain name continued to be included as a link on the website and in emails sent to customers. Because this domain name belonged to the organization for many years, it was added to the exception lists of the organization’s security systems for various reasons over time. Although this scenario might seem far-fetched, encountering similar examples in the real world is not a low probability.

Especially in watering hole attacks, the goal of malicious individuals is to take control of the systems of the targeted organization’s employees and/or its customers by hacking the systems that the external link addresses used on the organization’s websites point to, thereby indirectly targeting those visiting these sites. All the information these malicious individuals need is simply a list of the external link addresses on the organization’s websites. If they are able to detect any domain names among these whose registrations have been deleted, all they need to do to achieve their malicious objectives is to wait for visitors or direct their targets to that address through a social engineering attack.

The first thing that should be done to mitigate this risk for organizations is to properly manage the domain name process, but it’s also true that things

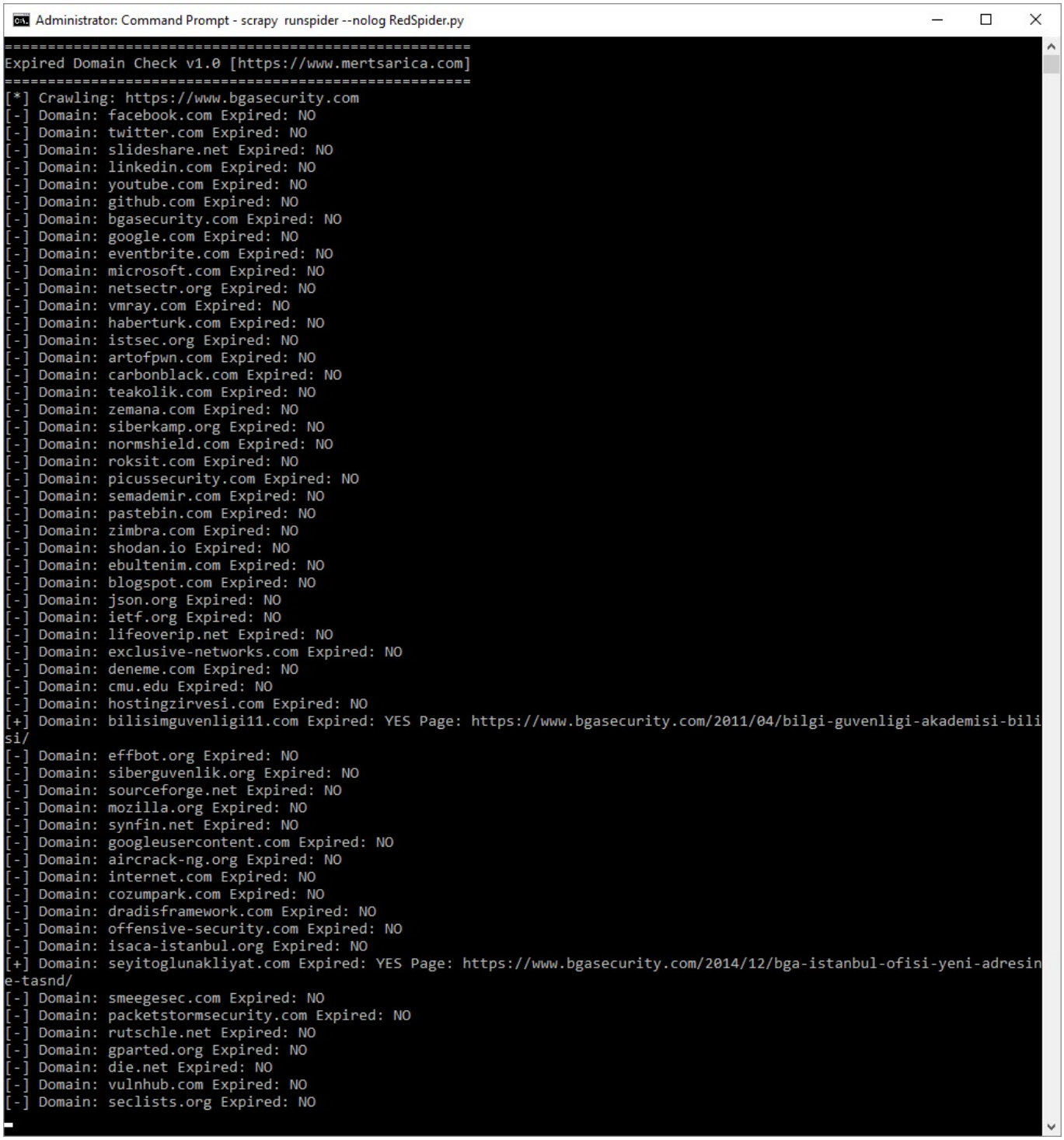
don’t always go as desired. Based on this, I decided to develop a tool to help both organizations detect these domain names and to assist red team members in security tests.

The basic expectation from this tool was to crawl the target website, check whether the detected domain names are registered by looking at their WHOIS information, and generate a warning if they are not registered. To avoid reinventing the wheel, instead of preparing a web browser with Python, I started looking for an existing software framework and soon came across Scrapy, a name I had heard before.

Scrapy is a fast, simple, and extensible open-source software framework frequently used by security researchers and penetration testing experts to crawl websites and gather data. Its installation is as easy as executing a single command: pip install scrapy.

The tool I named RedSpider visits the target website and, thanks to the Scrapy software framework, it scans the entire site. Then, it identifies all link addresses and queries the domain names found in external link addresses, excluding .tr extensions, via the whois.com.tr website. It writes the results of the queries into a logs.txt file in the current directory and issues a warning via the command line if it detects a domain name that has expired or is not registered.

When it came time to test the tool after developing it, I decided to give a fitting response to the BGA employees who had made it a habit to always test on my website over the years by deciding to do my test on BGA’s website. :) After running the command ‘scrapy runspider RedSpider.py‘ in the command line to start the test, the RedSpider tool was successfully able to detect that the domain name ‘bilisimguvenligi11.com‘, mentioned in a blog post from 2011, had expired and its registration had been deleted.



After successfully passing the test phase, I decided to share the RedSpider tool with you, believing that a wide range of people from security experts to red team members could benefit from it. Those who want to make use of the RedSpider tool can download it from my GitHub page.

Hope to see you in the following articles.