Alan Adı Yönetimi Sarmalı

written by Mert SARICA | 1 November 2019
If you are looking for an English version of this article, please visit here.

Alan adı (domain) yönetimi, sürecin iyi yönetilemediği büyük ve orta ölçekli kurumlar için kimi zaman içinden çıkalamaz bir hale gelebilmektedir. İhtiyaçları doğrultusunda iş birimi ile bilgi teknolojileri biriminin birbirinden bağımsız olarak alan adı satın alabilmeleri, bu alan adlarını yönetmeleri, yenilemeleri, web sitelerinden e-posta şablonlarına kadar bu alan adlarını müşterileriyle olan yazışmalarında, imzalarında bağlantı adresi olarak (link) kullanmaları, birimler arası en ufak bir iletişim problemi yaşanması durumunda alan adı envanterinin güncel olmamasına sebebiyet vererek art niyetli kişiler için fırsata dönüşebilmektedir.

Şöyle bir senaryo düşünelim, bir kurum tarafından yıllarca kampanyalarında kullanılmış, ana web sitesinin temasına ve ayrıca e-posta şablonuna gömülmüş bir alan adı yıllar içinde emekliye ayrılmış dolayısıyla yenilenmediği için de kaydı silinmiş olsun. Bu durumdan ilgili partilerin haberi olmadığı için de alan adı hem web sitesinde hem de müşterilere gönderilen e-postalarda bağlantı olarak yer almaya devam etmiş. Bu alan adının yıllarca kuruma ait olması sebebiyle yine zaman içinde kurumun güvenlik sistemlerinin istisna listelerine çeşitli sebeplerden dolayı eklenmiş. Düşündüğümüzde bu senaryo akla hayal ürünü gibi gelse de gerçek dünyada örneklerine fazla rastlamamız çok da düşük bir ihtimal değildir.

Özellikle su kaynağı (watering hole) saldırılarında art niyetli kişilerin amacı, hedef alınan kurumun web sitelerinde kullanılan dış bağlantı adreslerinin (external links) işaret ettiği sistemleri (links) hackleyerek dolaylı yoldan orayı ziyaret eden kurum çalışanlarını ve/veya kurumun müşterilerinin sistemlerini ele geçirmektir. Bunun için art niyetli kişilerin ihtiyaç duydukları bilgi sadece ve sadece kurumun web sitelerinde yer alan dış bağlantı adreslerinin bir listesidir. Bunlar arasından kaydı silinmiş alan adlarını tespit etmeleri durumunda kötü emellerine ulaşmak için sadece ziyaretçileri beklemek veya sosyal mühendislik saldırısı ile hedeflerini o adrese yönlendirmeleri gerekecektir.

Kurumlar için risk teşkil edebilecek bu duruma karşı yapılması gereken ilk iş alan adı yönetimi sürecini iyi bir şekilde işletmektir ancak işlerin her zaman arzu edildiği gibi ilerlemediği de bir gerçektir. Bundan yola çıkarak

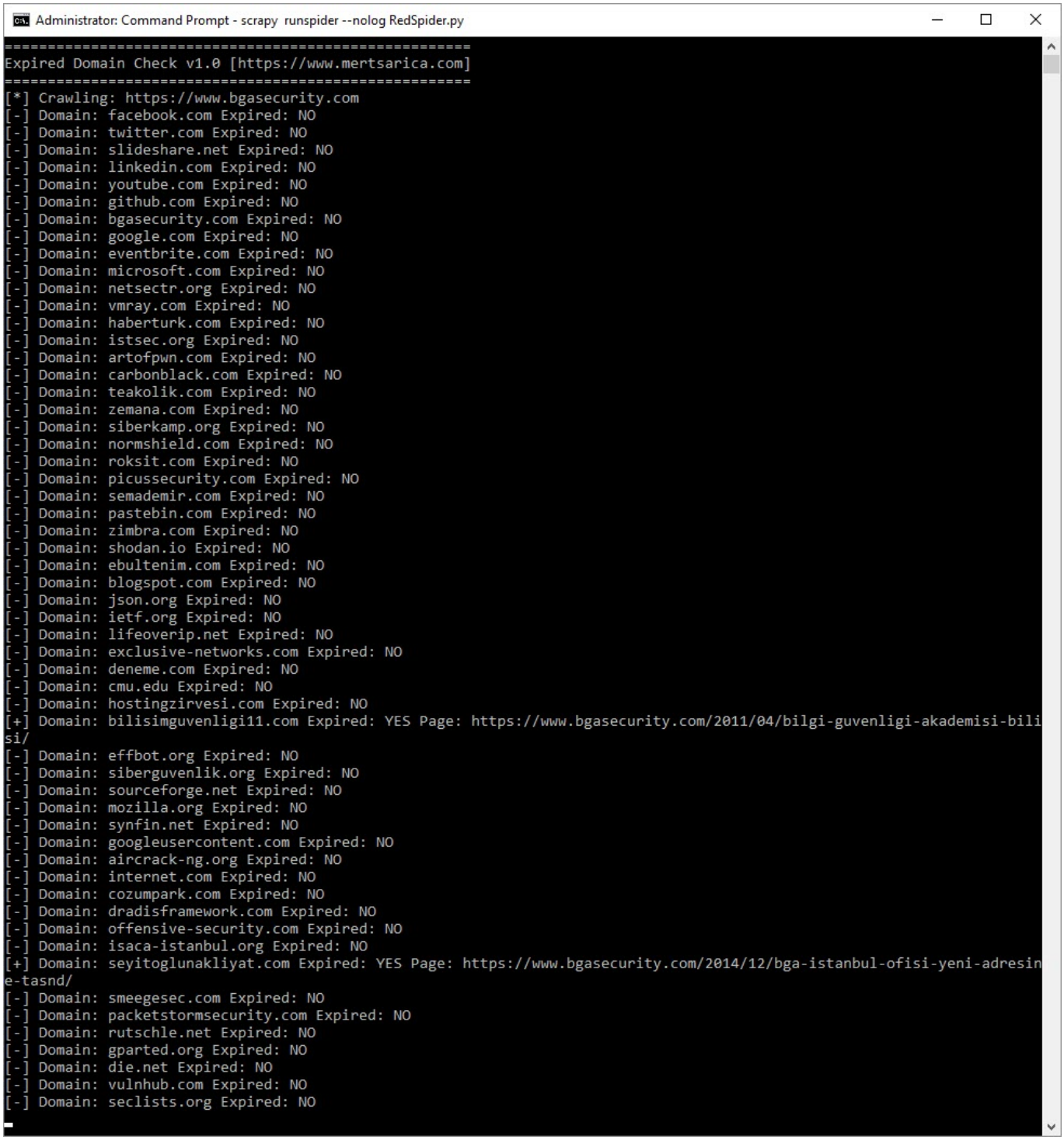
hem kurumlara bu alan adlarını tespit edebilmelerinde fayda sağlaması hem de güvenlik testlerinde kırmızı takım çalışanlarına yardımcı olması adına bir araç geliştirmeye karar verdim.

Bu araçtan temel olarak beklenen, hedef web sitesini taramak (crawling) , tespit edilen alan adlarının WHOIS bilgisine bakarak kayıtlı olup olmadığını kontrol etmek ve kayıtlı değil ise uyarı üretmekti. Tekerleği yeniden icat etmemek için Python ile bir web tarayıcısı hazırlamak yerine mevcutta bir yazılım iskeleti (framework) aramaya başladım ve çok geçmeden daha önce de adını duyduğum Scrapy ile karşılaştım.

Scrapy, güvenlik araştırmacıları ve sızma testi uzmanları tarafından da web sitelerini taramak, veri toplamak amacıyla sıklıkla kullanılan, hızlı, basit ve genişletilebilir açık kaynak kodlu bir yazılım iskeletidir. Kurulumu ise tek bir komutla gerçekleştirilebilecek kadar kolaydır; pip install scrapy

RedSpider adını verdiğim bu araç hedef web sitesini ziyaret ettikten sonra Scrapy yazılım iskeleti sayesinde tüm siteyi taramakta ardından tüm bağlantı adreslerini tespit edip, .tr uzantılı alan adları hariç dış bağlantı adreslerinde yer alan alan adlarını whois.com.tr web sitesi üzerinden sorgulamaktadır. Sorguların sonucunu, bulunduğu klasördeki logs.txt dosyasına yazmakta ve zaman aşımına uğramış, kayıtlı olmayan bir alan adı tespit etmesi durumunda komut satırı üzerinden uyarı vermektedir.

Aracı geliştirdikten sonra sıra test etmeye geldiğinde yıllardır her daim testlerini benim web sitem üzerinde yapmayı alışkanlık haline getirmiş BGA çalışanlarına misliyle karşılık vermek için ben de testimi BGA‘nın web sitesinde yapmaya karar verdim. :) Komut satırında scrapy runspider RedSpider.py komutunu çalıştırarak teste başladıktan kısa bir süre sonra RedSpider aracı, 2011 yılından kalma bir blog yazısında geçen bilisimguvenligi11.com alan adının zaman aşımına uğrayarak kaydının silindiğini başarıyla tespit edebildi.



Test aşamasını başarıyla geçtikten sonra RedSpider aracından güvenlik uzmanlarından, kırmızı takım çalışanlarına kadar geniş bir kitlenin faydalanabileceğine inanarak sizlerle paylaşmaya karar verdim. RedSpider aracından faydalanmak isteyenler GitHub sayfam üzerinden aracı indirebilirler.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.