Python’u Seviyorum :)

written by Mert SARICA | 25 March 2010
If you are looking for an English version of this article, please visit here.

Korsancılık oynayan herkes gibi bende yıllarca C programlama dili ile haşır neşir oldum, çok kaynak kodu inceledim çok program yazdım ve çoğu kez iyiki C programlama dili öğrenmişim dedim çünkü ne zaman başka bir programlama dili ile yazılmış kaynak koduna göz atsam kolayca anlamamda hep faydasını gördüm.

Zaman içinde, yazılan istismar araçlarının (exploit) C’den Python’a geçmesi Python‘a karşı olan ilgimi arttırmıştı. Bir gün aklıma esti ve Python dünyasına adım atmaya karar verdim. Ne zaman bir güvenlik testinde bir programa ihtiyaç duysam ne kadar doğru bir karar verdiğimi anlıyorum çünkü programa ihtiyaç duymam ile programı kodlamam ve kullanmam arasında geçen süre, programın karmaşıklığına göre ortalama en fazla 1-2 gün en az 15 dakika alabiliyor.

Bu programları C ile yazmaya çalışsam eminimki 2 katı daha fazla kod yazmam ve zaman harcamam gerekecek ama neyseki Python var. İşte Python’un güçlü yanları;

- Sentakslar (syntax) ile çok fazla uğraşmıyorsunuz, { } ( ) ;
- 100 saat derlemek ile uğraşmıyorsunuz, kodla ve çalıştır.
- 1 dünya modül ile geliyor, import et ve fonksiyonu çağır.
- Yazdığınız kodlar daha okunaklı, code re-use için daha verimli.
- Platform bağımsız, windowsta kodla, linuxte test et, mac’te kullan.
- Diğer dillerdeki gibi data tipleri ile uğraşmıyorsunuz, “1” + “1” = “11”, 1 + 1 = 2

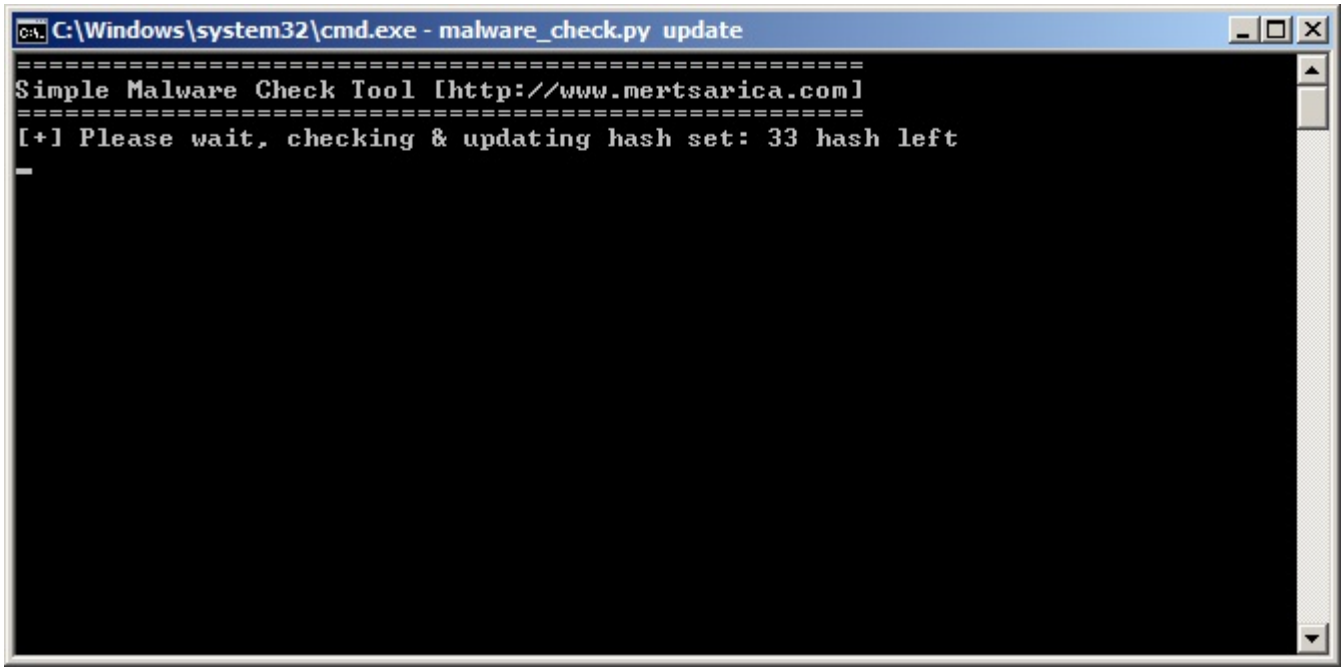
Gerek günlük işlerde olsun gerek canım sıkıldığında ve “ya şöyle bir program yazsam vatana millete hayırlı olur mu acaba” diye düşündüğümde hemen ortaya bir program çıkmış oluyor. Sizde Python dünyasına adım atmak istiyorsanız, Google’ın kendi çalışanlarına vermiş olduğu Python derslerine ait videoları izlemenizi şiddetle tavsiye ederim.

İşte yine bir can sıkıntısı ve yukardaki düşünce ile python ile bir program yazsam ve bu program gitse Avira‘nın sitesindeki tüm listelenen zararlı programların md5 hash bilgilerini toplasa ve bir dosyaya kayıt etse, diskimde belirttiğim herhangi bir dosyanın md5 hashini alsa ve zararlı içeriğe sahip olup olmadığını bu hash kümesi ile tespit etse hatta daha da ileriye gitsem

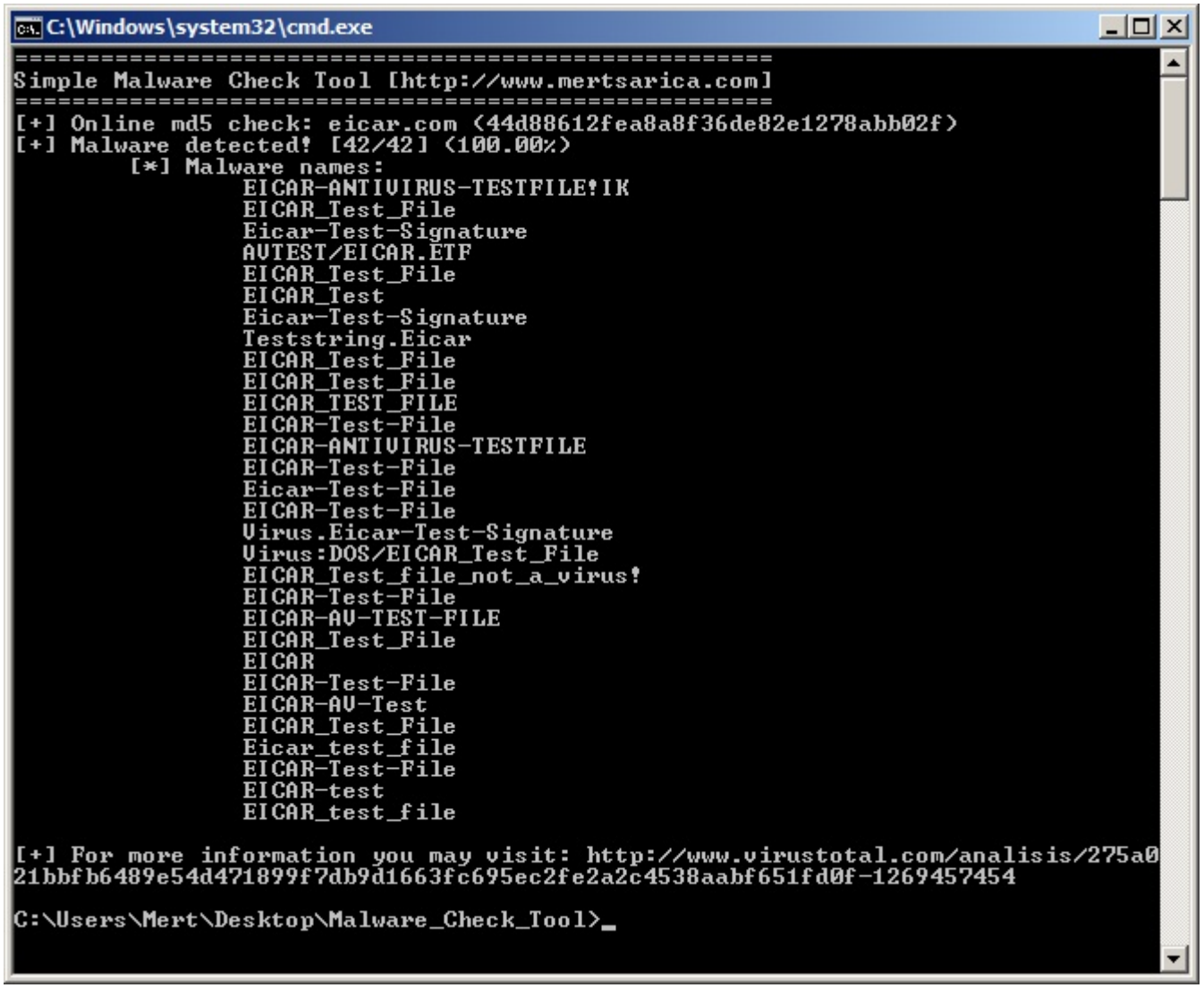
bir de aldığı bu md5 hashi Virustotal sitesine gönderse neticesini gösterse ve bir de Avira hash kümesini update etme özelliğine sahip olsa gerçekten faydalı bir eser olur mu dedim ve ortaya içinde proxy desteği de olan Malware Check Tool uygulaması çıkıverdi.

Programın kullanımı oldukça basit, 3 tane komut ile çalışıyor; online, offline ve update.

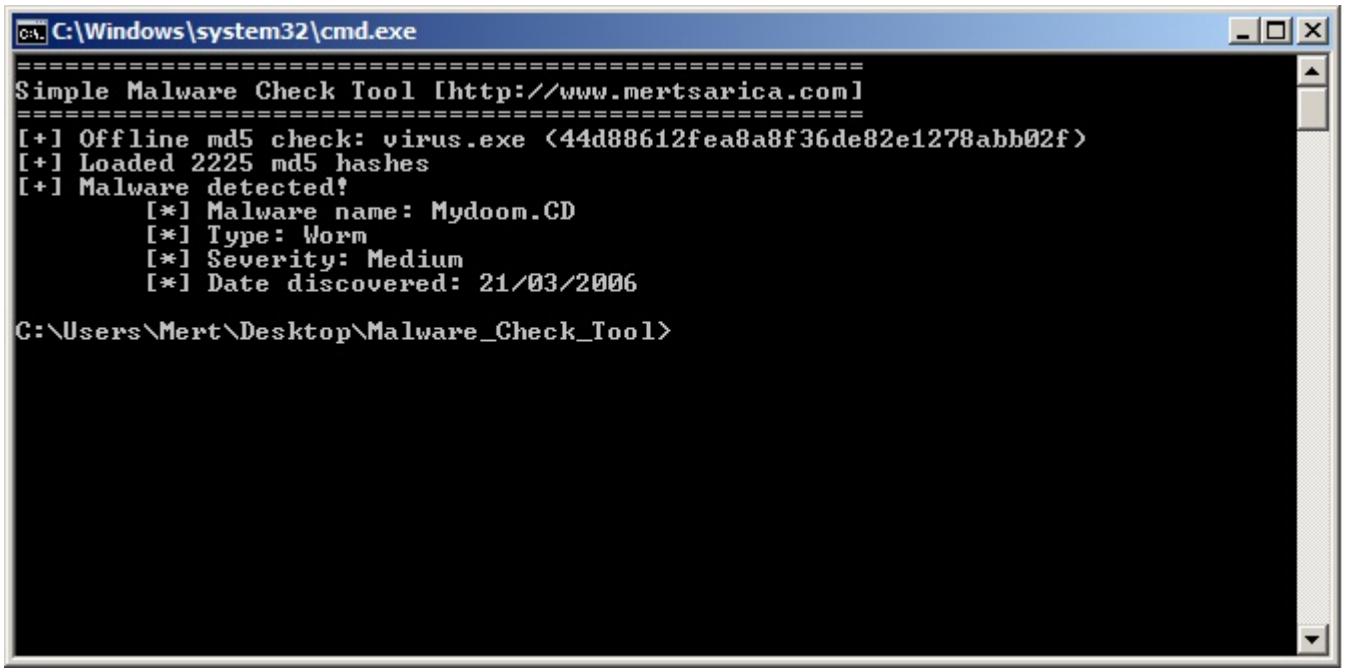
Update komutu (örnek: malware_check.py update) ile program zararlı içerik tespiti için kullandığı hash kümesini Avira'nın sitesini ziyaret ederek son sürüme güncelliyor.



Online komutu (örnek: malware_check.py online eicar.com) ile programı çalıştırdığınız taktirde belirtmiş olduğunuz dosyanın md5 hashini Virustotal sitesine göndererek size sonucu gösteriyor.



Offline komutu ile (örnek: malware_check.py offline virus.exe) ile programı çalıştırdığınız taktirde ise belirtmiş olduğunuz dosyasının md5 hashini, lokal disk üzerindeki hash kümesinde arayarak sonucunu size gösteriyor.



Programa http proxy özelliğide koydum, proxy ayarları için malware_check.py dosyasının içinde yer alan aşağıdaki kısmı değiştirmeniz gerekmektedir.

```
proxy_info = {
‘user’ : ‘test’, # proxy username
‘pass’ : ‘test’, # proxy password
‘host’ : “127.0.0.1”, # proxy host (leave it empty if no proxy is in use)
‘port’ : 8080 # proxy port
}
```

Bu haftalık benden bu kadar, Malware Check programına buradan ulaşabilirsiniz, şimdiden herkese iyi haftasonları…