Zararlı Siteler Artık Cebinizde :)

written by Mert SARICA | 31 August 2010

Daha öncede paylaştığım üzere uzun zamandan beri vakit buldukça Certified Reverse Engineering Analyst (CREA) sertifika sınavına hazırlanmaya çalışıyorum. Sınavın bir bölümü zararlı yazılım analizinden oluştuğu için sınava hazırlanma adına vakit buldukça yerli malı zararlı yazılımlar inceliyorum.

Geçtiğimiz günlerde yine yerli malı zararlı bir yazılım keşfetme gayesiyle yelken açtığım web sitelerinde aradığımı bulamadım ve kara kara düşünmeye başladım. Ellerimin boş kalmasının sebebi yurdumda zararlı kod yayan sitelerin azlığı mıydı yoksa bunların arama motorları tarafından tespit edilmesi ve belleğe alınması ile sitenin yayından kaldırılması arasında geçen süre mi çok azdı ?
Bunun dışında memleketimde zararlı içeriğe sahip olan sitelerin halka açık olarak kayıt altına alınmadığını farkettim ve hemen işe koyuldum.

Bildiğiniz üzere eskiden web siteleri şan, şöhret ve kitlelere sesini duyurmak isteyen korsanlar tarafından hack edilirken günümüzde bunların yerini sitelere zararlı kod yerleştiren ve bu siteleri ziyaret eden kullanıcıları ağlarına düşüren art niyetli kişiler aldı.

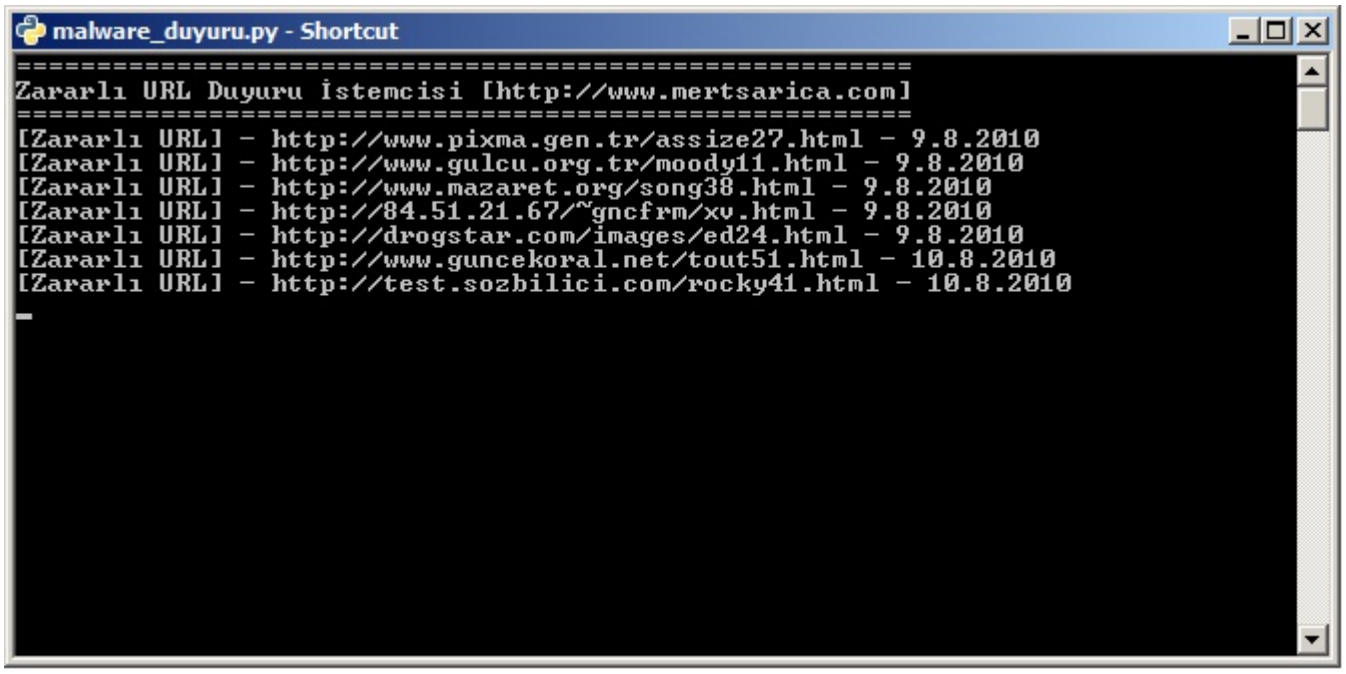
Yola çıkış noktam sınava hazırlık olsada işin sosyal boyutu ağır bastı ve zararlı kod yayan siteler konusunda ne kadar çok insanı haberdar edebilirsem o kadar az mağduriyet yaşanır diyerek Python ile hem kendim için hem de insanlar için faydalı olabileceğini düşündüğüm bir program hazırlamaya karar verdim.

Yaptığım ufak bir araştırma neticesinde zararlı kod yayan siteleri tespit eden ve alan adlarını yayınlayan fazla sayıda halka açık site olduğunu farkettim. Amacım sadece yerli malı siteler olduğu için halka açık bu siteleri gezen, sonuçları toplayan ve lokasyon olarak sadece Türkiye'de barınan bu siteleri yayınlayan bir program olacaktı. Günümüzde çoğu kişinin mobil cihazlar üzerinden Twitter'a ve Friendfeed'e bağlandığını göz önünde bulundurarak bu siteler üzerinden insanları haberdar etmenin daha hızlı olacağını düşündüm ve ortaya zararlı siteleri Twitter/Friendfeed üzerinden

duyuran bir istemci programı çıkmış oldu.

Program saat başı bu siteleri ziyaret ederek zararlı kod yayan yerel site adreslerini tespit edilme tarihi ile birlikte Twitter/Friendfeed üzerinden yayınlıyor.

Bu sitelerden haberdar olmak isteyenleriniz için adres: http://twitter.com/hack4career veya http://friendfeed.com/hack4career



Not: 16.01.2015 tarihi itibariyle bu çalışma sonlandırılmıştır.