Pi Hediyem Var! #7

written by Mert SARICA | 27 August 2016
2016 yılının üçüncü Pi Hediyem Var güvenlik oyunu ile tekrar karşınızdayım!

Önceki oyunlarda olduğu gibi, oyunu başarıyla tamamlayan üniversite öğrencileri arasında yapılacak bir çekiliş ile 1 adet Raspberry Pi 3'ü, 1 öğrenciye hediye edeceğim. Önceki oyunda olduğu gibi bu oyunun da Pi sponsoru olan Sinara Labs ekibine hem kendi adıma hem de oyunseverler adına tekrar teşekkür ederim.

Oyunumuza gelecek olursak, kahramanımızın çalıştığı kurumun CEO'su, geçtiğimiz hafta bir konferansa katılmak için üç günlüğüne yurt dışına gitmiştir. Internete bağlanmak için konakladığı oteldeki kablosuz ağı kullanan CEO, bir web sitesini ziyaret etmeye çalıştığında siteyi görüntülemek için Adobe PDF Reader uygulamasını güncellenmesi gerektiğini içeren bir uyarı mesajı ile karşılaşmıştır. Bu uyarının yer aldığı web sitesinden indirdiği Adobe PDF Reader programını çalıştıran CEO'nun kullandığı Windows işletim sistemi, şüpheli davranışlar sergilediği için konu hemen kurumsal SOME çalışanı olan kahramanımıza aktarılmıştır. Otellerin kablosuz ağlarına bağlanan CEOları oltalama saldırıları ile hedef alan bir APT grubundan haberdar olan kahramanımız, CEO'nun indirmiş olduğu sahte Adobe PDF Reader programının bir kopyasını alarak hemen şüpheli programı analiz etmeye başlar.

Kahramanımız ilk iş olarak programda yer alan karakter dizilerini (strings) Windows Sysinternals'ın strings aracı ile listelediğinde, çoğu karakter dizisinin aşağıdaki gibi gizlenmiş (encoded) olduğunu farkeder ve IDA yazılımı ile bu gizlenmiş karakter dizilerini çözmek için işe koyulur.

```
Yeljce(hR_
j[_dhIU(eo9[)cMjikcf
[DWc
d_jedY)Y(7MkU
99EKAE
[ihk
D8N:#7EI
^]_AjdZi_
```

Oyunu başarıyla tamamlamak için aşağıdaki tüm soruları, kod parçalarını ve

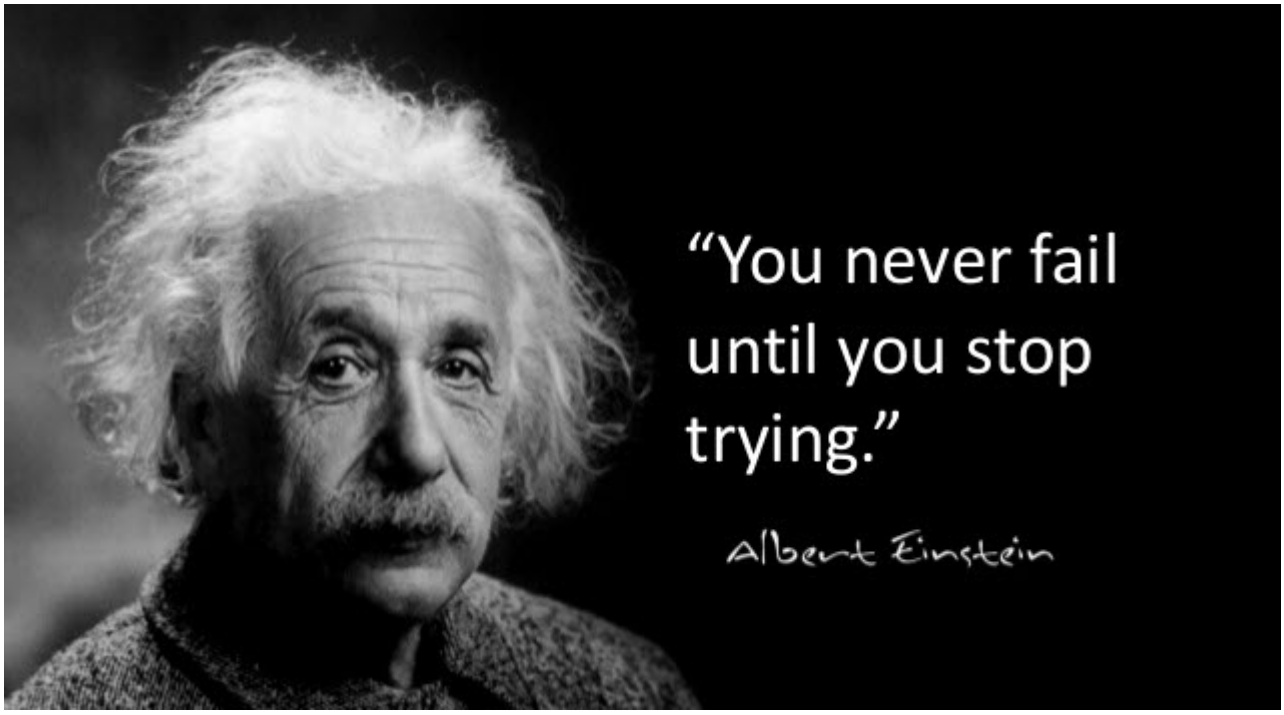
ekran görüntülerini içerecek şekilde detaylı olarak yanıtlamanız gerekmektedir. Soruları yanıtlayabilmek için öncelikle https://www.dropbox.com/s/lu22c36fj2ujbwk/ctf7.zip?dl=0 adresinden incelenmesi gereken şüpheli yazılımı indirmelisiniz. (zip şifresi: infected)

Sorular;

1. Gizlenmiş karakter dizilerini (encoded strings) çözen fonksiyonun adı (sub_xxxxx) nedir ?
2. idapython eklentisinde çalışabilen Python kodu ile en az 75 gizlenmiş karakter dizisini otomatik olarak çözebilen betik dosyasını (script) hazırlayınız.
3. Hazırladığınız betik dosyasını, en az 75 tane çözülmüş karakter dizisi ve betik dosyasının nasıl çalıştığını açıklayan bir yazıyı ile birlikte tarafıma gönderiniz.

Daha önce hediye kazanmamış olup çekilişe katılmak isteyenlerin, kanıtlarla (kod, ekran görüntüsü vs.) birlikte detaylı çözüm yolunu iletişim formu üzerinden veya e-posta ile adını, soyadını, yaşını, kendini tanıtan ve Raspberry Pi ile güvenlik üzerine yapmayı düşündüğü çalışmalarını anlatan bir yazıyı 31 Ağustos 2016 Saat 21:00'a kadar iletmeleri gerekmektedir.

Oyunun çözüm yolunu içeren blog yazısı ilerleyen günlerde yayınlanacak olup, kazanan talihli bu sayfa ve Twitter hesabım üzerinden duyurulacaktır. Ayrıca zorlananlar için Twitter hesabım üzerinden zaman zaman ipuçları da yayınlanacaktır.


“You never fail until you stop trying.”
Albert Einstein