Pi Hediyem Var! #6

written by Mert SARICA | 28 June 2016

2016 yılının ikinci Pi Hediyem Var güvenlik oyunu ile tekrar karşınızdayım! Pi Hediyem Var oyunlarının işe alım uzmanları tarafından da yakından takip edildiğini ve oyunu başarıyla tamamlayanlara iş teklifinde bulunulduğunu da yeri gelmişken oyunseverlere tekrar hatırlatmak isterim. ;)

G

[redacted]

Alıcılar:

Ayrıntıları gizle

Gönderen: [redacted]

Tarih: 18 Nis 2016 17:01

Merhabalar,

Pi Hediyem Var adlı oyunda başarı gösterdiğiniz için, Mert Sarıca tarafından isminiz ve mail adresiniz tarafımıza yönlendirildi. Yeni mezun sürecimizle ilgilenirseniz, CV'nizi bu mail adresine ileterek, aşağıdaki linkten başvurunuzu oluşturabilirsiniz.

Deloitte Türkiye Yeni Mezun İş Başvurusu: New Graduate Hire 2016 - Job Search Details - Turkey

Görüşmek dileğiyle,

[redacted]

Human Resources

DRT Yönetim Hizmetleri A.Ş.

Deloitte Values House

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

Oyunumuza gelecek olursak, geçtiğimiz oyunun kahramanı olan SOME çalışanımız (yani siz), bu defa kendisine gelen bir ihbarı değerlendirmeye karar verir. Bu ihbarda bir kullanıcı, müşterisi olduğu bankaların internet şubelerine girişi esnasında cep telefonu numarası isteyen bir pencere ile karşılaştığı bilgisini kahramanımız ile paylaşmıştır. Bankaların, internet şubeye giriş esnasında müşterilerinden cep telefonu numarası istemediğini bilen kahramanımız hemen bu şüpheli durumu araştırmaya başlar.

Kahramanımız, kullanıcının sisteminde msconfig komutunun çalıştırıp Başlatma sekmesi altında Komutlar kolonuna baktığında,
"C:\Users\kullanici\AppData\Roaming\Apple_Updater\lsasss.exe"
"C:\Users\kullanici\AppData\Roaming\Apple_Updater\safe" satırı dikkatini çekmiştir. Kahramanımız bu satıra konu olan iki dosyayı incelemeye başlar ve maceramız burada başlar.

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/392hss34pwrq3kz/ctf6.zip?dl=0 adresinden incelenmesi gereken şüpheli yazılımları indirmelisiniz. (zip şifresi: infected)

Sorular;

1. lsasss.exe programının sistem üzerinde oluşturduğu dosyalar hangileridir ?
2. lsasss.exe programının sistem üzerinde oluşturduğu şifreli dosyanın parolası nedir ?
3. Bankacılık zararlı yazılımının haberleştiği komuta kontrol merkezinin adresi nedir ?
4. Bankacılık zararlı yazılımı hangi bankaları hedef almaktadır ?
5. Bankacılık zararlı yazılımı kullanıcının hangi bilgilerini çalmaktadır ?

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 1 Temmuz 2016 Saat 09:00'a kadar iletmeleri gerekmektedir.

Oyunun çözüm yolunu içeren blog yazısı 1 Temmuz 2016 tarihinde yayınlanacak olup, kazanan talihli, ilerleyen günlerde yine bu sayfa ve Twitter hesabım üzerinden duyurulacaktır. Ayrıca zorlananlar için Twitter hesabım üzerinden zaman zaman ipuçları da yayınlanacaktır.