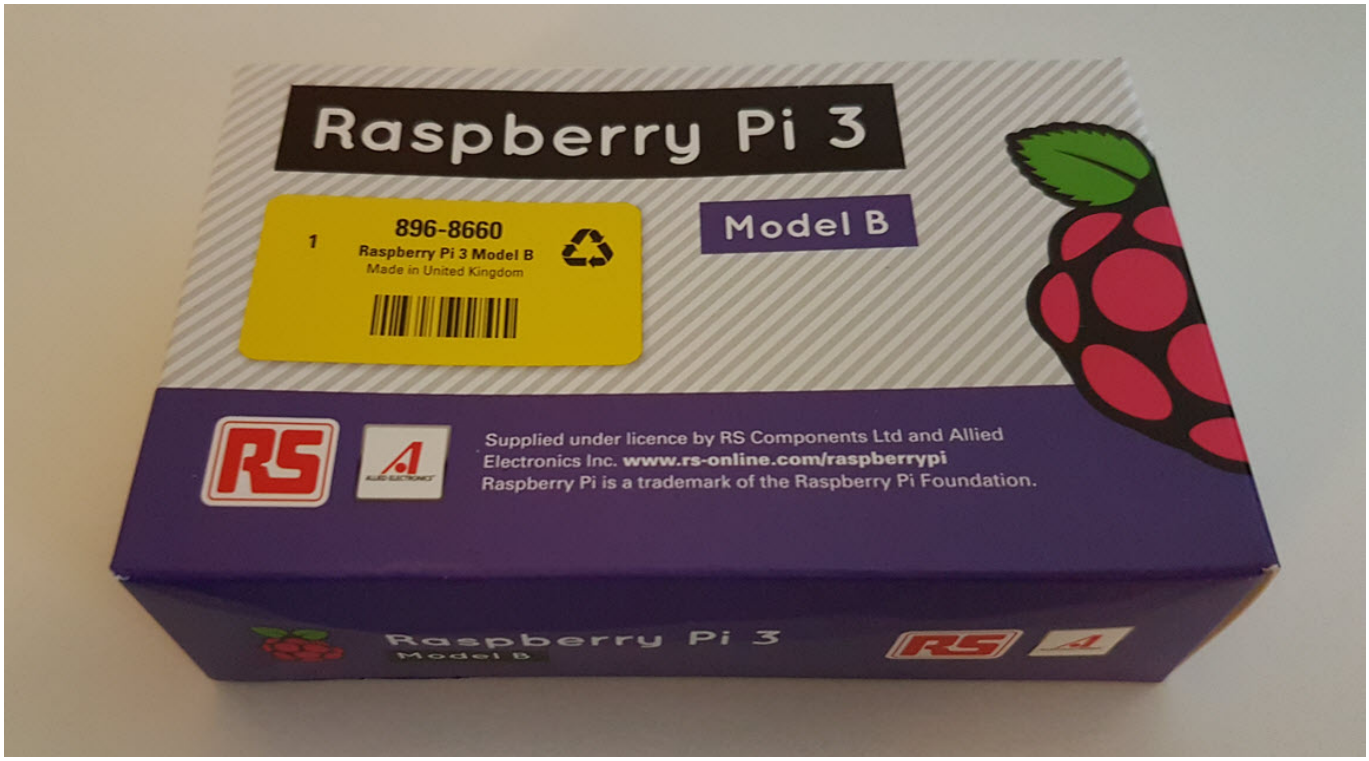
Pi Hediyem Var! #10

written by Mert SARICA | 27 January 2017

2017 yılının ilk Pi Hediyem Var siber güvenlik oyunu ile tekrar karşınızdayım. Bir önceki oyunu çözemeyenlerin bilenip, bu oyunu çözmek için ellerinden geleni ardına koymayacağını az çok tahmin edebiliyorum. :)

Önceki oyunlarda olduğu gibi, oyunu başarıyla tamamlayan üniversite öğrencileri arasında yapılacak çekiliş ile 1 adet Raspberry Pi 3'ü, 1 öğrenciye hediye edeceğim. Bu oyunun Pi sponsoru olan sevgili işverenim IBTech firmasına hem kendi adıma hem de oyunseverler adına teşekkür ederim.



Yeni oyunumuza gelecek olursak, kurumsal SOME çalışanı olan kahramanımız günün birinde İngiltere'de bir üniversiteye ait olan bir e-posta hesabından bir daveti konu olan bir e-posta alır. Sahte olmadığından emin olabilmek için gönderen kişiyi hem üniversitenin web sitesinde hem de Linkedin üzerinde araştırdığında, bu üniversitede gerçekten bu isim ve soyadda bir akademisyenin çalıştığını görür. Konu ilgisini çektiği için e-postayı gönderen kişi ile yazışmaya başlar. Birkaç defa yazıştıktan sonra gelen son e-postada yer alan bağlantı adresi ve doküman, güvenlik sistemlerindeki alarmları tetikler ve kahramanımız ne tür bir tehdit ile karşı karşıya kaldığını anlamak için hemen kolları sıvar.

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/g1pzyskv2iqjnz8/ctf10.zip?dl=0 adresinden incelenmesi gereken şüpheli yazılımı indirmelisiniz. (zip şifresi: infected)

Yönergeler & Sorular;

1. Analiz esnasında ihtiyaç duyacağınız tüm şüpheli dosyalar ctf10.zip dosyası içinde yer almaktadır.
2. Analize Application_Form dosyasından başlamanız ve daha sonrasında Windows üzerinde çalışacak zararlı yazılımın oluşturulmasına kadar olan akışın nasıl ilerlediğini, haberleştiği adreslere yer verecek şekilde açıklayınız.
3. Windows üzerinde çalışan zararlı yazılımın ne tür bir zararlı yazılım olduğunu elde ettiğiniz ipuçlarıyla birlikte açıklayınız.

Daha önce Raspberry Pi kazanmamış olup çekilişe katılmak isteyenler veya adını oyunu başarıyla tamamlayanlar listesine yazdırmak isteyenler, 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 30 Ocak Pazartesi Saat 09:00‘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.

Not: Bu oyunu çözerken zararlı yazılım analizi yaptığınızı hatırlatır, izole ve sanal bir sistem üzerinde çalışmanızı şiddetle tavsiye ederim.

Başarılar.

"Education is not the learning of facts, but the training of the mind to think."
-Albert Einstein