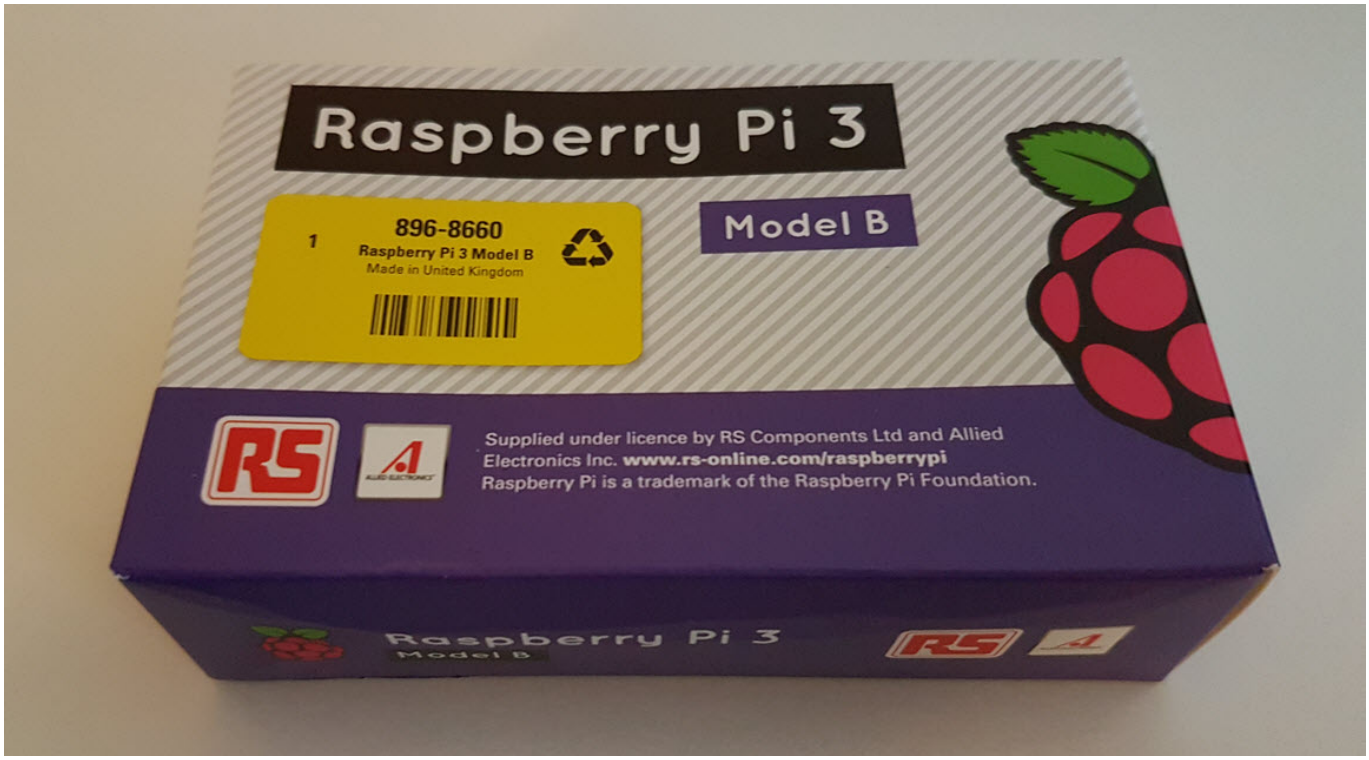
Pi Hediyem Var! #11

written by Mert SARICA | 25 March 2017

2017 yılının ikinci Pi Hediyem Var siber güvenlik oyunu ile tekrar karşınızdayım. 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 da Pi sponsoru olan sevgili işverenim IBTech firmasına hem kendi adıma hem de tüm Pi Hediyem Var oyunseverleri adına teşekkür ederim.



Yeni oyunumuza gelecek olursak, bir finans kurumunda kurumsal SOME çalışanı olarak görev yapan kahramanımız, FireEye (Mandiant) firması tarafından Mart ayında yayınlanan M-Trends raporunu okumaya başlar. Son zamanlarda Finans kurumlarına gerçekleştirilen siber saldırılarda, devlet destekli (nation state) siber saldırılarda olduğu gibi 0. gün zafiyetlerini istismar eden istismar kodlarının kullanıldığını öğrenir. Bunun üzerine son 1 ayda kurum çalışanlarına gönderilip, e-posta güvenlik sistemleri tarafından bloklanan e-postalara detaylı olarak baktığında, ekinde (Confirmation_letter.docx) istismar kodu tespit edildiği için bloklanan bir e-posta dikkatini çeker ve bu dokümanı analiz etmek için işe koyulur.

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/f9hmagl7d3ks31r/ctf11.zip?dl=0 adresinden incelenmesi gereken şüpheli dokümanı indirmelisiniz. (zip şifresi: infected)

Yönergeler & Sorular;

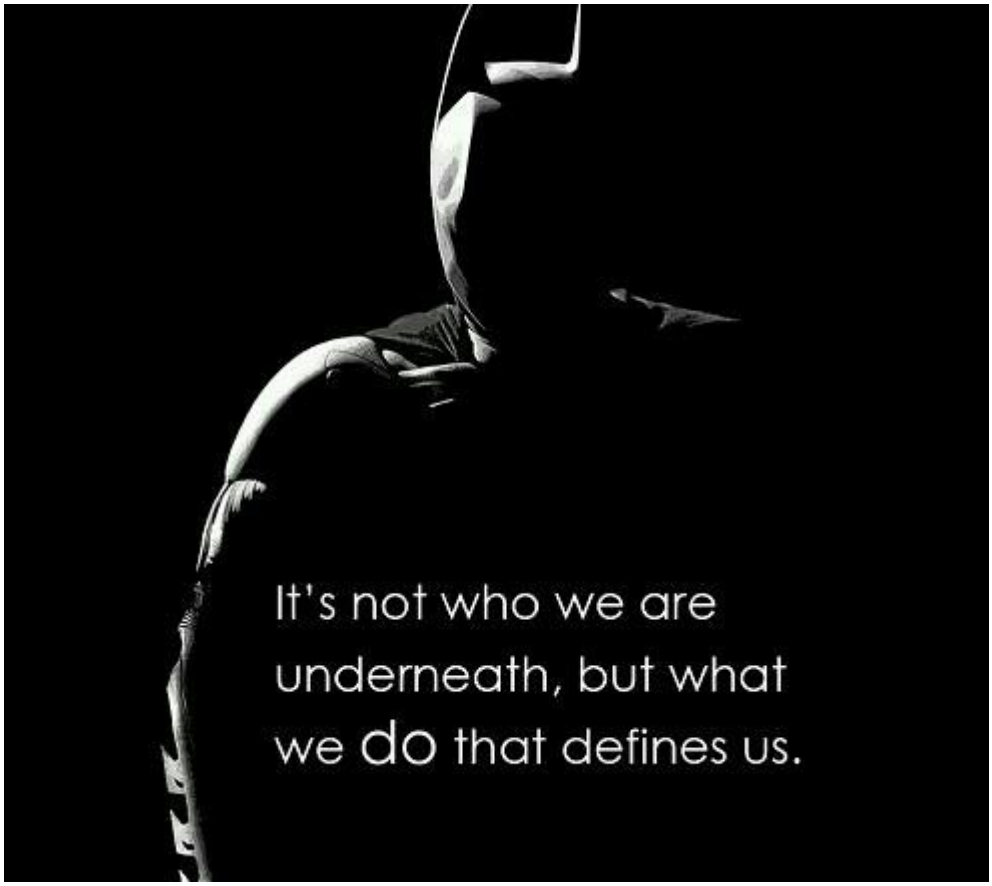
1. Doküman içinde kaç tane istismar kodu bulunmakta ve hangi zafiyeti veya zafiyetleri istismar etmektedir ?
2. İstismar kodu tarafından çalıştırıldıktan sonra sisteme yüklenen zararlı yazılımın türünü kanıtları ile birlikte söyleyiniz.
3. Zararlı yazılım, hangi güvenlik yazılımının sistemde çalışıp, çalışmadığını kontrol etmektedir? Güvenlik yazılımı sistem üzerinde çalışıyor ise ne tür bir davranış sergilemektedir ?
4. Zararlı yazılımın haberleştiği komuta kontrol merkezinin ip adresi nedir ?
5. Kod analizinden faydalanarak -08-03-2017 dosyasının içinde yer alan gizlenmiş veriyi çözünüz.

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 2 Nisan Pazar Saat 20:00'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 yaması güncel olan sanal sistem yazılımı (vmware, virtualbox vs.) ile çalışmanızı şiddetle tavsiye ederim.

Başarılar.


It's not who we are
underneath, but what
we do that defines us.