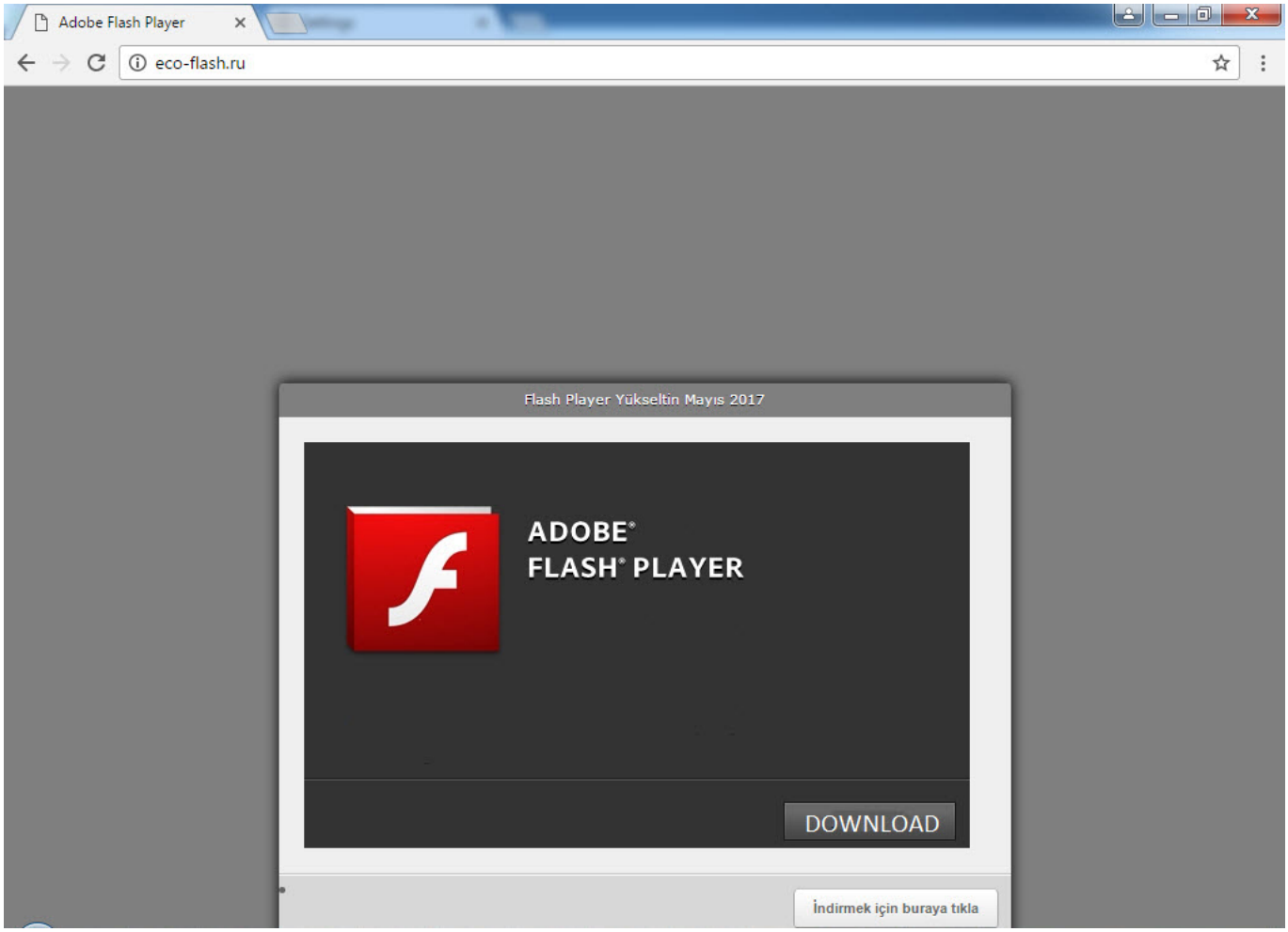
Pi Hediyem Var! #12

written by Mert SARICA | 17 June 2017

Önceki oyunlarda çıtayı fazlasıyla yükselttiğimin ve sizleri zorladığımın farkındayım ancak oyunlar çoğunlukla kurgu olsa da örnek dosyalar gerçek hayattan alıntı olduğu için bu oyunların sizleri gerçek hayata hazırladığını, amacıma hizmet ettiğine inanıyorum. Ne de olsa Rocky filmini izleyenleriniz, Rocky'i Rocky yapan büyük zaferlerin ardında zorlu idmanların olduğunu anımsayacaklardır. ;)

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 ve gizli kalmayı tercih eden bilişim gönüllüsü hayırsevere hem kendi adıma hem de tüm Pi Hediyem Var oyunseverleri adına teşekkür ederim.

Önceki oyunlara kıyasla daha kolay olan yeni oyunumuza gelecek olursam, internette sörf yapan kahramanımız karşısına çıkan aşağıdaki şüpheli web sayfasında belirtilen dosyayı (Flash-2017.js) indirip, incelemeye ve aklına takılan sorulara yanıt aramaya 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/tl2x2t34alakvgk/ctf12.zip?dl=0 adresinden incelenmesi gereken şüpheli dokümanı indirmelisiniz. (zip şifresi: infected)

Yönergeler & Sorular;

1. JScript üzerinde gizlenmiş (encoded) olarak saklanan en az 5 farklı karakter dizisinin (string) çözülmüş (decoded) halini gönderiniz.
2. JScript dosyası tarafından ana zararlı yazılımın indirildiği web adresi nedir ?
3. Diske kayıt edilen ve çalıştırılan zararlı yazılımın md5 hashi nedir ?
   Not: Komuta kontrol merkezi kapalı olduğu için http yanıt (response/body) paketi, ctf12.zip dosyasındaki http_body.txt dosyasında yer almaktadır.

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, adını,

soyadını, yaşını iletişim formu üzerinden veya e-posta adresine 17 Haziran Cumartesi Saat 22:00'a kadar iletmeleri gerekmektedir.

Oyunun çözüm yolunu içeren blog yazısı ilerleyen günlerde yayınlanacak olup, kazanan talihli bu sayfa ve Twitter hesabım üzerinden duyurulacaktır.

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.