Pi Hediyem Var! #17

written by Mert SARICA | 26 July 2019

Uzuuuun bir aradan sonra 2019 yılının ilk Pi Hediyem Var oyunu ile tekrar karşınızdayım. Önceki oyunlarda olduğu gibi bu oyunu da başarıyla tamamlayan üniversite öğrencileri arasında yapılacak çekiliş ile 3 adet Raspberry Pi 4'ü hediye edeceğim. Bu oyunun Pi sponsoru olan Keepnet Labs Türkiye Ülke Müdürü Erdinç BALCI'ya hem kendi adıma hem de tüm oyunseverler adına teşekkür ederim.

Oyunumuza gelecek olursam, kurum çalışanlarınızdan biri hizmet almak için ziyaret ettiği bir fırsat sitesine kredi kartı bilgilerini girdikten sonra farklı bir web sitesine yönlendirildiğini farkeder. Kredi kartı bilgilerinin çalındığından şüphe eden çalışan soluğu yanınızda alarak bu konuyu aydınlatmanıza dair sizden yardım ister. Son zamanlarda Magento e-ticaret platformu kullanan web sitelerine yönelik siber saldırılar gerçekleştirildiği ile ilgili haberler okuyan ve Kurumsal SOME ekibinde yer alan kahramanımız, sanal sisteminden bu web sitesini ziyaret ederek şüpheli kod tespitine yönelik web trafiğini analiz etmeye başlar ve hikayemiz burada başlamış olur.

Oyunu başarıyla tamamlamak için aşağıdaki tüm soruların cevaplarını, kanıtları (kod parçaları, ekran görüntüleri vs.) ile birlikte detaylı olarak açıklamanız gerekmektedir.
Soruları yanıtlayabilmek için öncelikle https://www.dropbox.com/s/yyfretoo11hopq8/ctf17.zip?dl=0 adresinden incelenmesi gereken şüpheli dosyayı indirmelisiniz. Dosyayı Fiddler aracı ile analiz edebilirsiniz. (zip şifresi: infected)

Yönergeler & Sorular;

1. Zararlı kodu içeren dosyaları bulunuz.
2. Gizlenmiş en az 50 karakter dizisini (strings) çözünüz. (Hazır program (deobfuscator) kullanmak yasaktır.)
3. Önceki adımdan yola çıkarak zararlı kodun çaldığı bilgileri hangi web adresine ilettiğini bulunuz.
4. Analizinizden yola çıkarak zararlı kodun müşteriye ait hangi bilgileri çalabileceğini (en az 5 bilgi) söyleyiniz.
5. Zararlı kodun hangi hacking grubu tarafından geliştirilmiş olabileceğini, kod analizinden elde ettiğiniz bilgilerden faydalanarak tahmin ediniz.

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 bana veya e-posta adresime 27 Temmuz Cumartesi 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.

Not: Bu oyunu çözerken zararlı yazılım, kod analizi yaptığınızı hatırlatır, izole ve yaması güncel olan sanal sistem yazılımı (vmware, virtualbox vs.) ile çalışmanızı şiddetle tavsiye ederim.

Başarılar


NO PAIN
THE ITALIAN STALLION
ROCKY IV