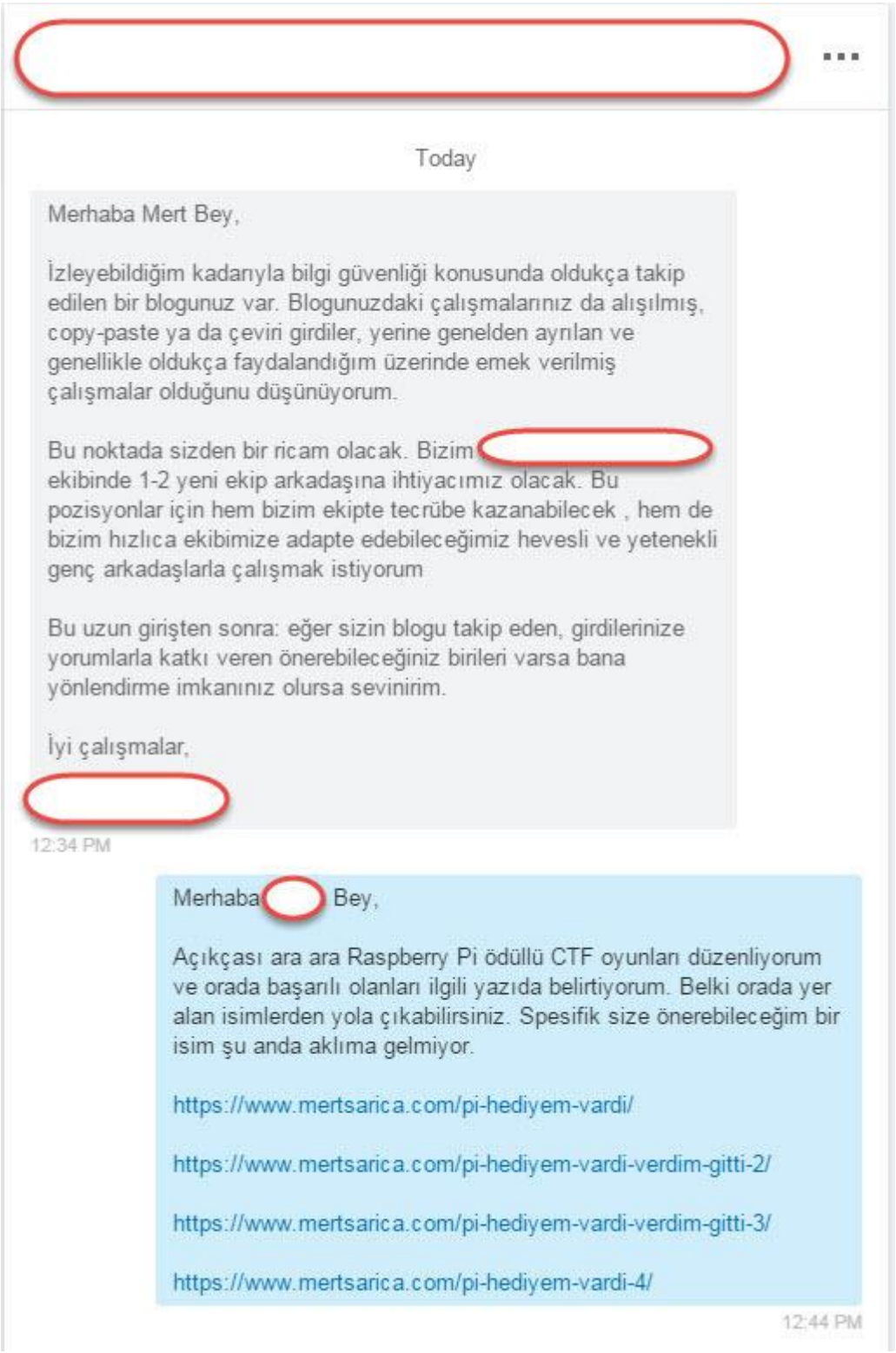
Pi Hediyem Var! #5

written by Mert SARICA | 26 March 2016

2016 yılının ilk Pi Hediyem Var güvenlik oyunu ile uzun bir aradan sonra tekrar karşınızdayım! Yeri gelmişken oyunlarda başarılı olup, Raspberry Pi kazanamayanların üzülmemeleri adına ufak bir ayrıntıyı da bu vesileyle sizlerle paylaşmak istedim ;)



Oyuna geçmeden önce öncelikle Bilgi Güvenliği Akademisi ‘ne Pi Hediyem Var oyunları için tam tamına 3 adet Raspberry Pi 3 Model B bağışladığı için hem kendi adıma hem de oyunlara katılacaklar adına teşekkürü bir borç bilirim.



Önceki oyunlarda olduğu gibi, oyunu başarıyla tamamlayan üniversite öğrencileri arasında yapılacak bir çekiliş ile 1 adet Raspberry Pi 3’ü bir kişiye hediye edeceğim. Merakla bekleyenler için lafı çok uzatmadan hemen oyuna ve kurallara geçiyorum.

Kurumsal SOME‘de çalışan kahramanımız (yani siz), kum havuzu (sandbox) analizi yapan bir sistemden alarm alır. Alarmı incelediğinde, kurum çalışanlarından birinin ziyaret etmiş olduğu bir web sitesinin hacklenmiş olduğunu ve bu sitenin bir şekilde ziyaretçileri istismar kiti yüklü olan başka bir siteye yönlendirdiğini görmüştür. İşi gereği bu yönlendirmenin nereden, nasıl gerçekleştiğini bulmak için kum havuzu sistemi üzerinden indirmiş olduğu ağ trafiği dosyasını (PCAP) incelemeye başlar ve oyunumuz başlamış olur.

Oyunu başarıyla tamamlamak için izlenmesi gereken adımlar;

1. https://www.mertsarica.com/ctf/ctf5.zip adresinden incelenmesi gereken PCAP dosyasını indirin. (zip şifresi: infected)
2. Hacklenmiş web sitesini tespit edin.
3. Zararlı kodları bulun ve okunaklı hale (decode) getirin.
4. Kod seviyesinde yönlendirmenin nasıl gerçekleştiğini detaylı bir şekilde açıklayın.
5. Bu zararlı kodların hangi istismar kitine ait olduğunu bulun.

Daha önce hediye kazanmamış olup çekilişe katılmak isteyenlerin, kanıtlarla (kod, ekran görüntüsü vs.) birlikte detaylı çözüm yolunu iletişim formu veya e-posta ile, adını, soyadını, kendini tanıtan ve Raspberry Pi ile güvenlik üzerine yapmayı düşündüğü çalışmalarını anlatan bir yazıyı 27 Mart 2016 Saat 24:00'a kadar iletmeleri gerekmektedir.

Oyunun çözüm yolu ve kazanan talihli, ilerleyen günlerde yine bu sayfa ve Twitter hesabım üzerinden duyurulacaktır. Twitter hesabım üzerinden zorlananlar için zaman zaman ipuçları yayınlanacaktır. Oyunu başarıyla tamamlayabilen oyuncu sayısı az olduğu taktirde oyunun süresi uzatılacaktır.

May the force be with you!