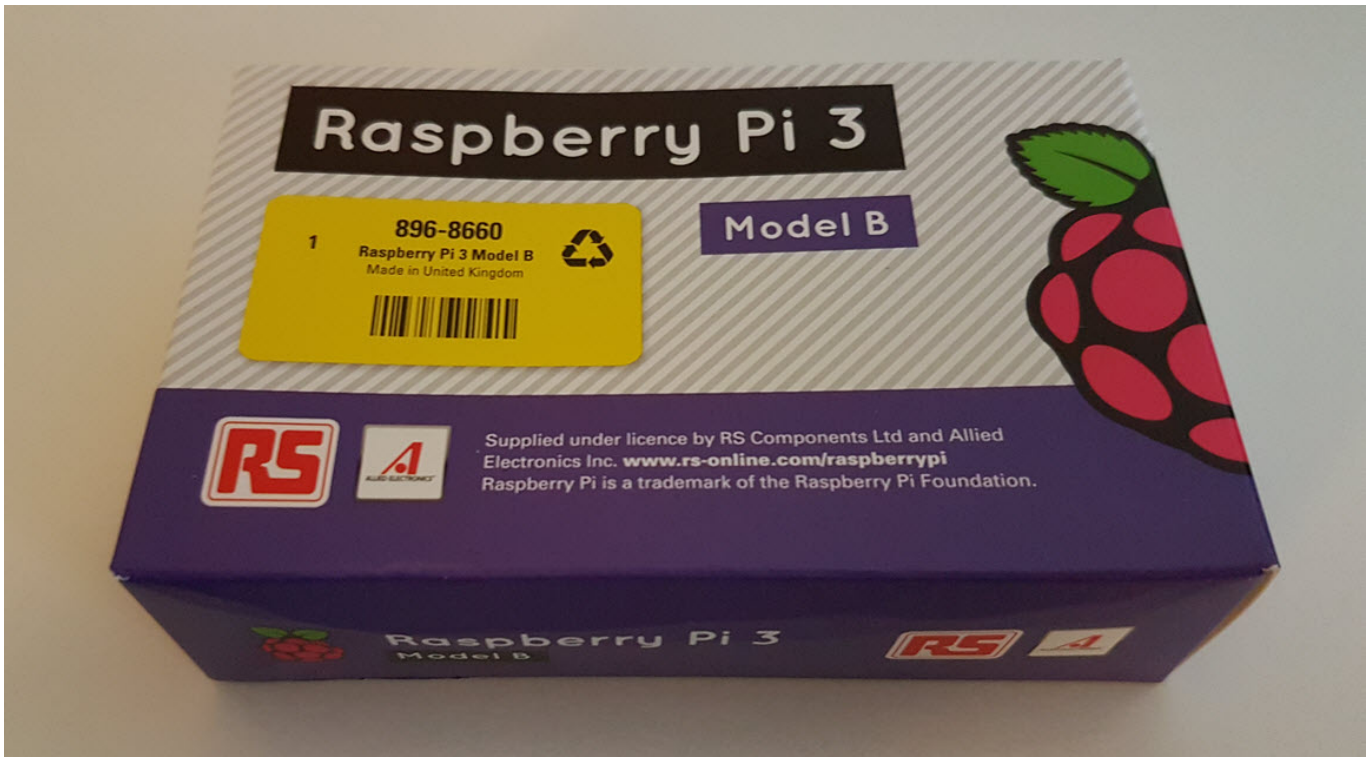
Pi Hediyem Var! #9

written by Mert SARICA | 2 December 2016
Ve 2016 yılının son Pi Hediyem Var siber güvenlik oyunu karşınızda!

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.



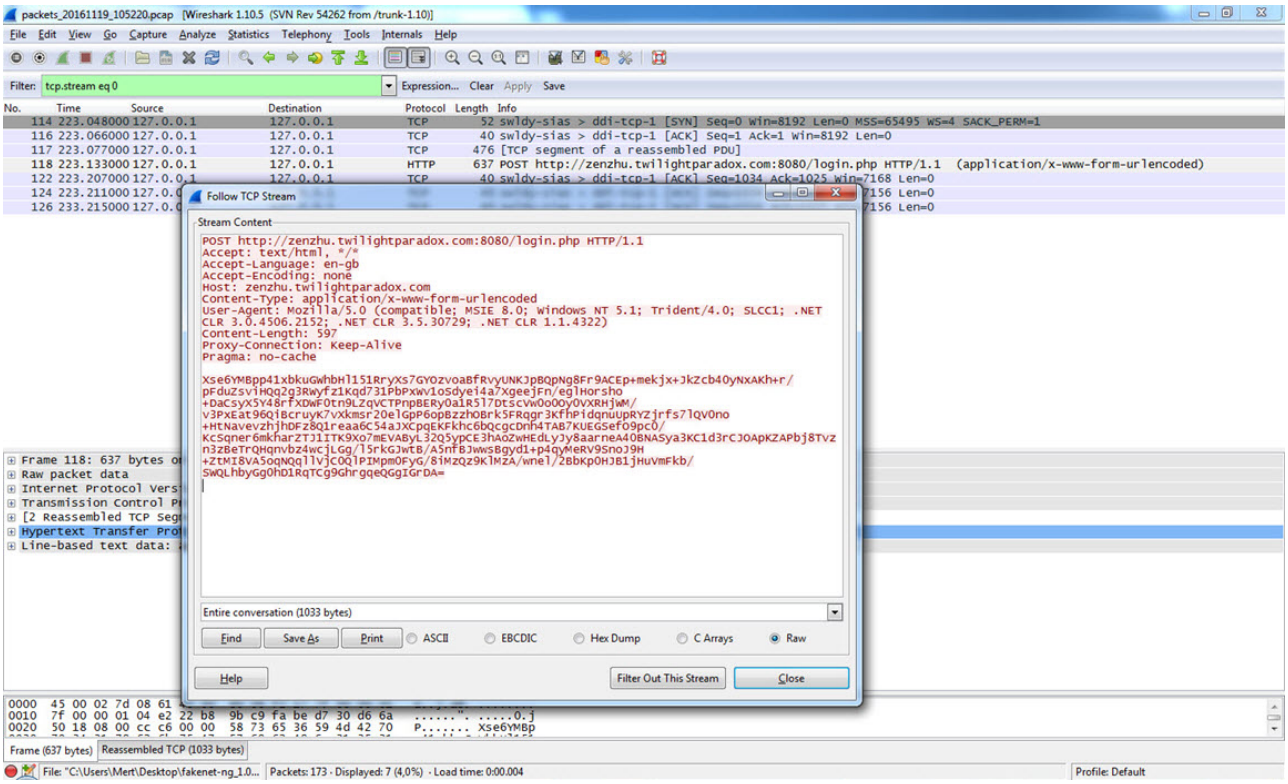
Oyunumuza gelecek olursak, geçmiş vakaların altından başarıyla kalkan kahramanımız bu defa bir devlet sitesini ziyaret ettiğinde kullanmış olduğu Antivirüs yazılımının vermiş olduğu JS/Kryptik.I alarmı ile irkilir. Alarmın http://pol.google.com.mooo.com/ajax/libs/jquery/jquery-2.1.5.ack.min.js sayfasından kaynaklandığını gören kahramanımız, VirusTotal üzerinde şüpheli JavaScript kodunu tarattığında, 57 tane antivirüs yazılımından sadece 3 tanesinin alarm ürettiğini görür ve konuyu derinlemesine incelemeye karar verir.

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/zrqbteyc56f78ny/ctf9.zip?dl=0 adresinden

incelenmesi gereken şüpheli yazılımı indirmelisiniz. (zip şifresi: infected)

Yönergeler & Sorular;

1. Analiz esnasında ihtiyaç duyacağınız tüm şüpheli dosyalar ctf9.zip dosyası içinde yer almaktadır.
2. Analize jquery-2.1.5.ack.min.js dosyasından başlamanız ve daha sonrasında Windows üzerinde çalışacak zararlı yazılımın oluşturulmasına kadar olan akışın nasıl ilerlediğini, zararlı web adreslerine de yer verecek şekilde açıklayınız.
3. Windows üzerinde çalışan zararlı yazılımın ne tür bir zararlı yazılım olduğunu örneklerle açıklayınız.
4. Son olarak Windows üzerinde çalışan bu zararlı yazılım tarafından komuta kontrol merkezine gönderilen aşağıdaki şifreli paketi nasıl çözdüğünüzü açıklayınız.



Xse6YMBpp41xbkuGWhbHl151RryXs7GYOzvoaBfRvyUNKJpBQpNg8Fr9ACEp+mekjx+JkZcb40yNxAKh+r/pFduZsviHQq2g3RWyfz1Kqd731PbPxWv1oSdyei4a7XgeejFn/eglHorsho+DaCsyX5Y48rfXDWF0tn9LZqVCTPnpBERy0a1R5l7DtscVw0o0Oy0VXRHjWM/v3PxEat96QiBcruyK7vXkmsr20elGpP6opBzzhOBrk5FRqgr3KfhPidqnuUpRYZjrfs7lQV0no+HtNavevzhjhDFz8Q1reaa6C54aJXCpqEKFkhc6bQcgcDnh4TAB7KUEGSefO9pc0/KcSq

```
ner6mkharZTJ1ITK9Xo7mEVAByL32Q5ypCE3hAoZwHEdLyJy8aarneA40BNASya3KC1d3rCJ
OApKZAPbj8Tvzn3z
BeTrQHqnvbz4wcjLGg/l5rkGJwtB/A5nfBJwwsBgyd1+p4qyMeRV9SnoJ9H+ZtMI8VA5oqNQ
qllVjC0QlPIMpm0F
yG/8iMzQz9KlMzA/wnel/2BbKp0HJB1jHuVmFkb/SWQLhbyGg0hD1RqTCg9GhrgqeQGgIGrD
A=
```

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 5 Aralık 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.