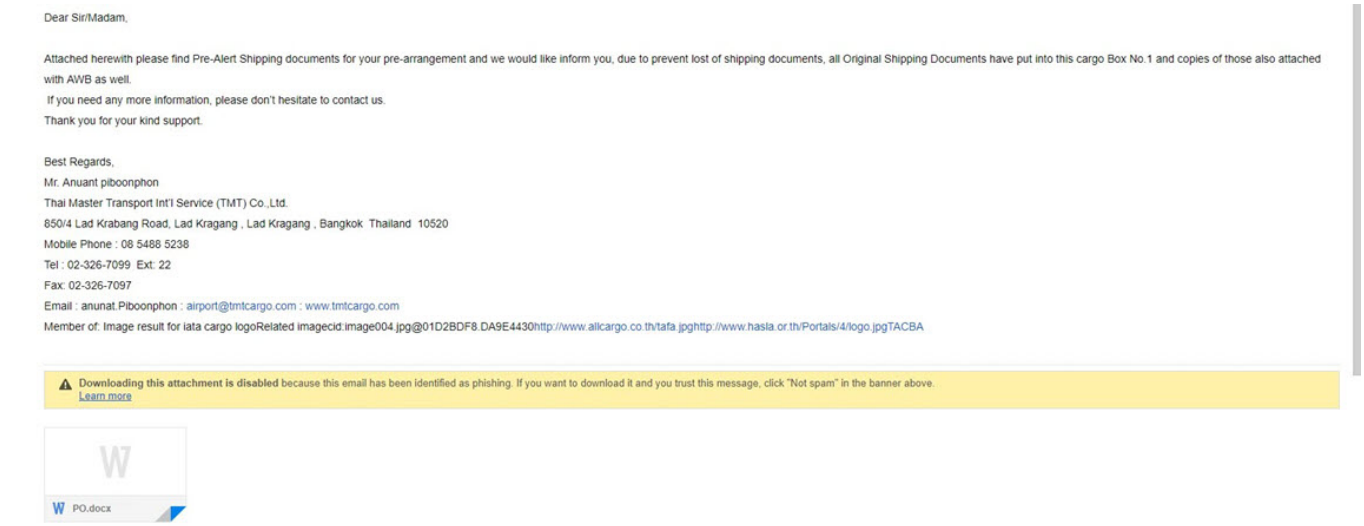
Pi Hediyem Var! #13

written by Mert SARICA | 23 February 2018

2018'in ilk Pi Hediyem Var oyunu ile uzun bir aradan sonra nihayet karşınızdayım. Önceki oyunlarda olduğu gibi bu oyunu da başarıyla tamamlayan üniversite öğrencileri arasında yapılacak çekiliş ile 1 adet Raspberry Pi 3'ü, 1 öğrenciye hediye edeceğim. Bu oyunun Pi sponsoru olan IBTech'e hem kendi adıma hem de tüm Pi Hediyem Var oyunseverleri adına teşekkür ederim.

Bu oyunun konusuna gelecek olursam, uzun yıllardan beri Gmail hesabına sahip olan kahramanımız son zamanlarda SPAM klasöründe çok sayıda şüpheli e-posta olduğunu görür. E-postalardan birinin ekinde şüpheli bir dosya (PO.docx) olduğunu gören kahramanımız, bu dosyayı analiz etmek için işe koyulur ve maceramız burada başlar.


Dear Sir/Madam,

Attached herewith please find Pre-Alert Shipping documents for your pre-arrangement and we would like inform you, due to prevent lost of shipping documents, all Original Shipping Documents have put into this cargo Box No.1 and copies of those also attached with AWB as well.
If you need any more information, please don't hesitate to contact us.
Thank you for your kind support.

Best Regards,
Mr. Anuant piboonphon
Thai Master Transport Int'l Service (TMT) Co.,Ltd.
850/4 Lad Krabang Road, Lad Kragang , Lad Kragang , Bangkok Thailand 10520
Mobile Phone : 08 5488 5238
Tel : 02-326-7099 Ext: 22
Fax: 02-326-7097
Email : anunat.Piboonphon : airport@tmtcargo.com : www.tmtcargo.com
Member of: Image result for iata cargo logoRelated imagecid:image004.jpg@01D2BDF8.DA9E4430http://www.allcargo.co.th/tafa.jpghttp://www.hasla.or.th/Portals/4/logo.jpgTACBA

Downloading this attachment is disabled because this email has been identified as phishing. If you want to download it and you trust this message, click "Not spam" in the banner above.
Learn more

PO.docx

Oyunu başarıyla tamamlamak için aşağıdaki tüm soruların cevaplarını, kod parçalarını ve ekran görüntülerini içeren kanıtları ile birlikte detaylı olarak açıklamanız gerekmektedir. Soruları yanıtlayabilmek için öncelikle https://www.dropbox.com/s/yq1chfhouef924d/ctf13_fixed.zip?dl=0 adresinden incelenmesi gereken şüpheli dokümanı indirmelisiniz. (zip şifresi: infected)

Yönergeler & Sorular;

1. PO.docx dosyası hangi zafiyeti istismar etmektedir ?
2. Oyuna konu olup sistem üzerinde çalışan zararlı yazılımların isimleri (PO.docx vs.) ve çalışma sıraları (PO.docx, x zararlı yazılımını çalıştırdı. X, y zararlı yazılımını çalıştırdı gibi) nedir ?

3. Sistem üzerinde en son çalışan, ana zararlı yazılımın adı (PoisonIvy gibi) ve türü nedir (spyware gibi) ?

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 26 Şubat Pazartesi Saat 23:00'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.

Güncelleme (24.02.2018 15:11): ctf13.zip dosyasındaki bozuk PO.docx dosyasını düzeltip tekrar yükledim. Bu hatam sebebiyle oyunun süresini 26 Şubat Pazartesi saat 23.00'a uzattım.

Matruşka, Rus yapımı bir oyuncak bebek türüdür. Ahşap el yapımı olan bebekler ortasından açıldığında başka bir bebek çıkar, onu açtığınızda yine başka bir bebek çıkar. Tek anne figürünün içerisinde iç içe yerleştirilmiş beş veya yedi bebekten oluşur. Kimi zararlı yazılımlar da aynı Matruşka bebeklerine benzerler. :)
Başarılar