Pi Hediyem Var! #16

written by Mert SARICA | 5 October 2018

Kısa bir aradan sonra yeni bir Pi Hediyem Var oyunu ile tekrar 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 FireEye Türkiye ekibine ve FireEye Türkiye Ülke Müdürü Ümit NADİM'e hem kendi adıma hem de tüm Pi Hediyem Var oyunseverleri adına teşekkür ederim.

Ayrıca isteğe bağlı olarak oyunu başarıyla tamamlayanlar arasında yapılacak çekiliş ile bir kişi, FireEye firmasının 16 Ekim 2018 Salı günü İstanbul Çırağan Palace Kempinski'de gerçekleştireceği yarım günlük "CyberSecurity through Human, Technology & Intelligence" başlıklı etkinliğine benimle birlikte katılma, siber olay müdahale ve tehdit raporları ile dünyaca ünlü olan FireEye'ın Mandiant ekibinin Teknik Direktörü ile tanışma fırsatı yakalayacaktır.

Etkinlik Takvimi:

09:30 – 10:00 Kayıt ve Kahve Arası
10:00 – 10:10 Regional & Corporate Update – Marco Riboli – Vice President Southern Region at FireEye, Inc.
10:10 – 10:20 İnsan, Teknoloji ve İstihbarat ekseninde Siber Güvenlik – Umit Nadim – Country Sales Manager at FireEye, Inc.
10:20 – 10:30 FireEye ile Başarılı İşbirliği – Levent Ortaköylüoğlu – Yönetici Ortak, Dereka & Natica
10:30 – 11:30 How Was That Breach Detected – Jeff Hamm – Technical Director Mandiant
11:30 – 11:50 Kahve Arası
11:50 – 12:10 Güvenlik Yönetiminde Saha Deneyimlerim – Selim Öziş – Siber Güvenlik Mimarı, Dereka & Natica
12:10 – 12:40 FireEye Global Servisleri ve İstihbarat – Umit Nadim – Country Sales Manager at FireEye, Inc.
12:40 – 13:00 Tartışma
13:00 – 14:00 Öğle Yemeği

Oyunumuza gelecek olursam, bir kurumda üst düzey yetkili olan bir çalışan, e-posta kutusunda bir bankadan geldiği süsü verilen şüpheli bir e-posta bulur. E-postada yer alan resim dosyasına tıkladığında, internet tarayıcısı

üzerinden bir adresten havale.jar dosyasının indirilmeye çalıştığını farkederek durumu hemen kurumun SOME ekibi ile paylaşır. Kurumsal SOME izleme ve müdahale ekibinde yer alan kahramanımız, dosyayı indirdikten sonra hızlıca analiz etmeye başlar ve hikayemiz burada başlamış olur.

From: [redacted] BANKASI A.S [mailto:kabriestore@yahoo.com]
Sent: Tuesday, September 4, 2018 2:56 PM
Subject: Emailing: Re-Confirm Details

Hello Sir,

FYI

Best Regards
[redacted] BANKASI A.S
Remittance Department
Business Banking | Enterprise Cash Management

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/q4pm5c296k2ocj5/ctf16.zip?dl=0 adresinden incelenmesi gereken şüpheli dokümanı indirmelisiniz. (zip şifresi: infected)

Yönergeler & Sorular;

1. Şüpheli JAR dosyasını analiz ediniz.
2. JAR dosyası içinde kullanılan şifreleme algoritmasını tespit ediniz.
3. Şifrelenmiş en az 10 class dosyasının şifresini çözüp, kaynak koduna çeviriniz. (decompile)
4. Zararlı yazılımın adını, türünü ve iletişime geçtiği komuta kontrol merkezini Java sınıfı (class) seviyesinde bulunuz.

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 7 Ekim Pazar 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, kod analizi yaptığınızı hatırlatır, izole ve yaması güncel olan sanal sistem yazılımı (vmware, virtualbox vs.) ile çalışmanızı şiddetle tavsiye ederim.

Başarılar

WHY DO WE FALL?

SO WE CAN LEARN TO PICK OURSELVES UP