

Pi Hediye Var! #18

written by Mert SARICA | 21 February 2020

If you are looking for an English version of this writing, please visit [here](#).

2020 yılının ilk Pi Hediye Var oyunu ile tekrar karşınızdayım. Önceki oyunlarda olduğu gibi bu oyunu da başarıyla tamamlayan üniversite öğrencileri arasında yapılacak çekiliş ile 2 adet Raspberry Pi 4'ü hediye edeceğim. Bu oyunun Pi sponsoru olan Keepnet Labs Türkiye Ülke Müdürü Erdi BALCI'ya hem kendi adıma hem de tüm oyunseverler adına teşekkür ederim.

Oyunumuza gelecek olursam, kurumsal Android telefonunun ayarlarında bilinmeyen kaynaklardan uygulama yüklemeye izin vermiş olan üst düzey bir çalışan, kendisine gelen bir SMS'teki bağlantı adresine tıklayıp APK dosyasını indirdikten sonra çalıştırır. Aradan 1 hafta geçtikten sonra kurumun ağ güvenlik sisteminden zararlı yazılım trafiğine ilişkin bir alarm gelir ve Kurumsal SOME çalışanı olan kahramanımız konuya müdahil olur. Durumdan haberdar olan üst düzey çalışan, Kurumsal SOME'den hangi bilgilerinin çalındığını öğrenmek için yardım ister. Alarma konu olan HTTP trafiğini inceleyen kahramanımız, APK dosyasından faydalanarak çalınan veriyi tespit edebilme adına şifreli veriyi çözmek üzere işe koyulur ve hikayemiz burada başlar.

Oyunu başarıyla tamamlamak için aşağıdaki tüm soruların cevaplarını, kanıtları (kod parçaları, ekran görüntüleri vs.) ile birlikte detaylı olarak açıklamamız gerekmektedir.

Soruları yanıtlayabilmek için öncelikle

<https://www.dropbox.com/s/t6kakt8jsrsrsqy/ctf18.zip?dl=0> adresinden incelenmesi gereken şüpheli dosyayı indirmelisiniz. (zip şifresi: infected)

Yönergeler & Sorular;

1. APK dosyasını analiz ederek komuta kontrol merkezinin adresini bulunuz.
2. Aşağıdaki ws parametresinde yer alan verinin şifrelemesinde kullanılan anahtarı (private key) bulunuz.
3. Aşağıdaki ws parametresinde yer alan şifrelenmiş veriyi çözünüz.

POST / HTTP/1.1

Content-Length: 1118

Content-Type: application/x-www-form-urlencoded

User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; Google Nexus 6



YOUR **MIND** IS A WEAPON
KEEP IT LOADED

- JOHN WICK -