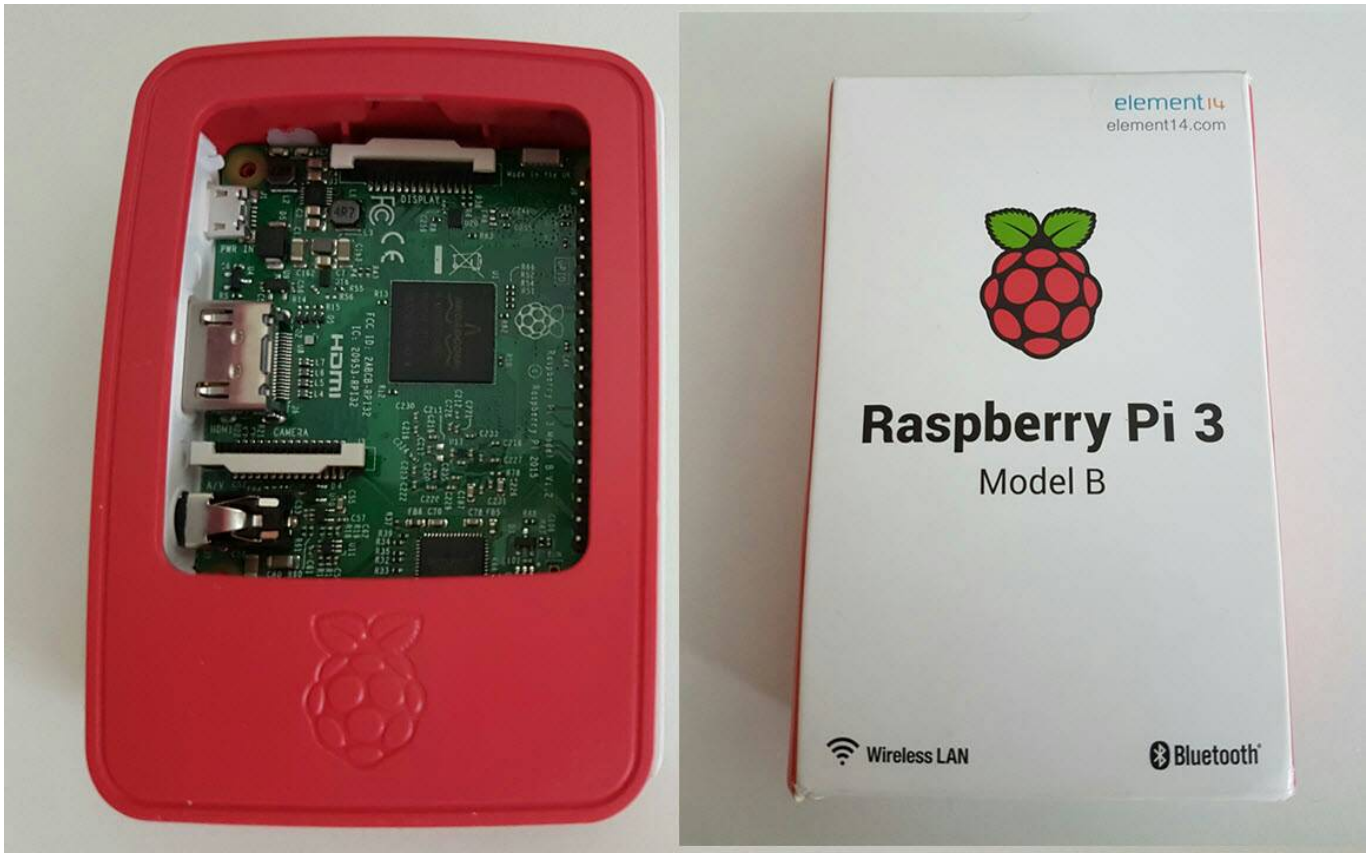
Pi Hediyem Var! #8

written by Mert SARICA | 30 September 2016
2016 yılının dördüncü Pi Hediyem Var güvenlik oyunu ile tekrar karşınızdayım!

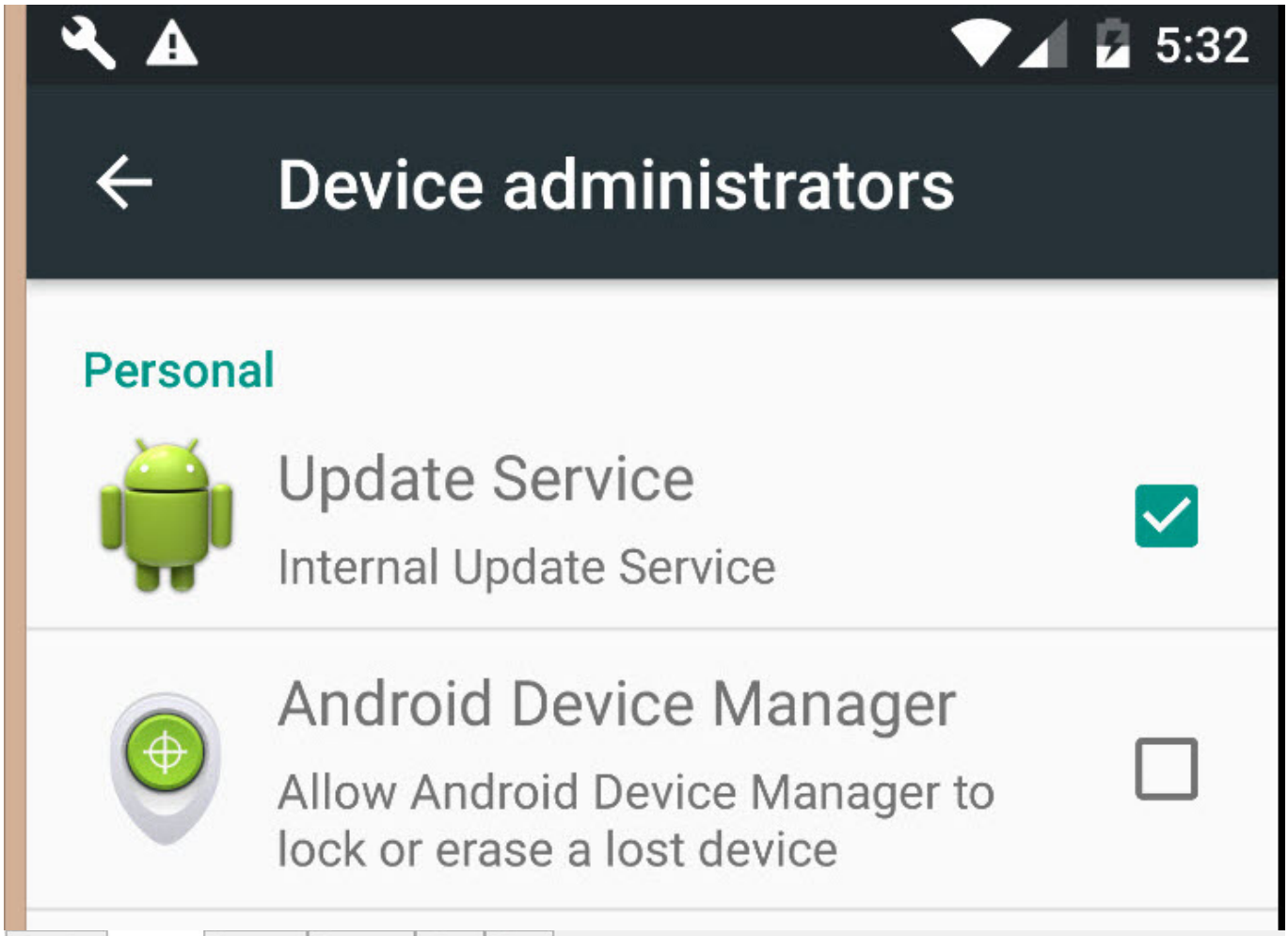
Önceki oyunlarda olduğu gibi, oyunu başarıyla tamamlayan üniversite öğrencileri arasında yapılacak çekiliş ile 1 adet Raspberry Pi 3'ü, 1 öğrenciye hediye edeceğim. Bu oyunun Pi sponsoru olan, ESET firmasının Türkiye temsilcisi Stratus Bilişim firmasına ve Sayın Erkan TUĞRAL'a hem kendi adıma hem de oyunseverler adına teşekkür ederim.



Oyunumuza gelecek olursak, boş vaktinde Mr. Robot dizisini izleyen kahramanımız, dizinin üçüncü bölümünde E Corp firmasındaki bir üst düzey yöneticinin kurumun başka bir çalışanının cep telefonuna casus yazılım yüklediği bir sahneye tanıklık eder. Bu sahneden oldukça etkilenen kahramanımız, Android 6.0 işletim sistemi yüklü olan cep telefonunda casus yazılım ihtimaline karşın araştırma yapmaya başlar.

Çok geçmeden Android'in cihaz yöneticisi menüsünde Update Service isimli şüpheli bir uygulamanın yönetici yetkisine sahip olduğunu görür. Yüklü uygulamalar arasında bu uygulamaya dair bir simge/ikon da göremedikten sonra indirilenler klasörüne baktığında, 3 gün önce bt.apk isimli şüpheli bir

uygulamanın indirildiğini görür. Kilit ekranı ve güvenlik menüsünde, bilinmeyen kaynaklardan uygulama yüklenmesine de izin verildiğini gören kahramanımız, vakit kaybetmeden cep telefonunun HTTP trafiğini bilgisayarında çalışan Charles Proxy aracına yönlendirir. Çok geçmeden cep telefonunun https://a.thd.cc/apiv4/send/phoneinfojson adresine okunaklı olmayan (encoded) veri gönderdiğini görür ve bt.apk uygulamasını Android simülatörde inceleyerek bu paketi çözmek için işe koyulur.



Overview | Request | Response | Summary | Chart | Notes

```
POST /apiv4/send/phoneinfojson HTTP/1.1
Connection: close
Content-Type: application/x-www-form-urlencoded;
Account-Hash: [redacted]
Build-Version: 4.18.3
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; Samsung Galaxy S6 - 6.0.0 - API 23 - 1440x2560 Build/MRA58K)
Host: a.thd.cc
Accept-Encoding: gzip
Content-Length: 487

hash=cabdd9cbc542a9f483a67170d1fe8b78&imei=000000000000000&auth_id=[redacted]&api_revision=2&data_id=0&data=H4sIA
AAAAAAAAFWRQW6EMAxF75I1HRFgGMSuJ4kMMa3VEKMkwwytevc6aoXSLLL4_s5_dr5UohXV
qLtb1-p2aldKcTQ7hkjs1aj6S60qNUFKGA7jcEcn7ktdKflieXAmcYlsNrdrXyl8_pdLJ-xADiaX
A3U_6MJdIKTjQQuZmb3HOaFVYwp3rNTKEzks9QVczlVI0WZafZXT5LsTahJdxFbXTV-fRwq8YYDE
QYqv3gYmK2JgLrLyWj7ZC86L7rpamGDbTPacqRZ3mtGAXcmfiHE7zAceE0Ow5h4LyBIWSS0H_W2J
7_wwNOdt_zmfG0ujgTnRDuWc8i20HCaToM9vnLhvm4kYMk-UBX7_AOOMoKfXAQAA
```

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/uxd8e001etdvnt1/ctf8.zip?dl=0 adresinden incelenmesi gereken şüpheli yazılımı indirmelisiniz. (zip şifresi: infected)

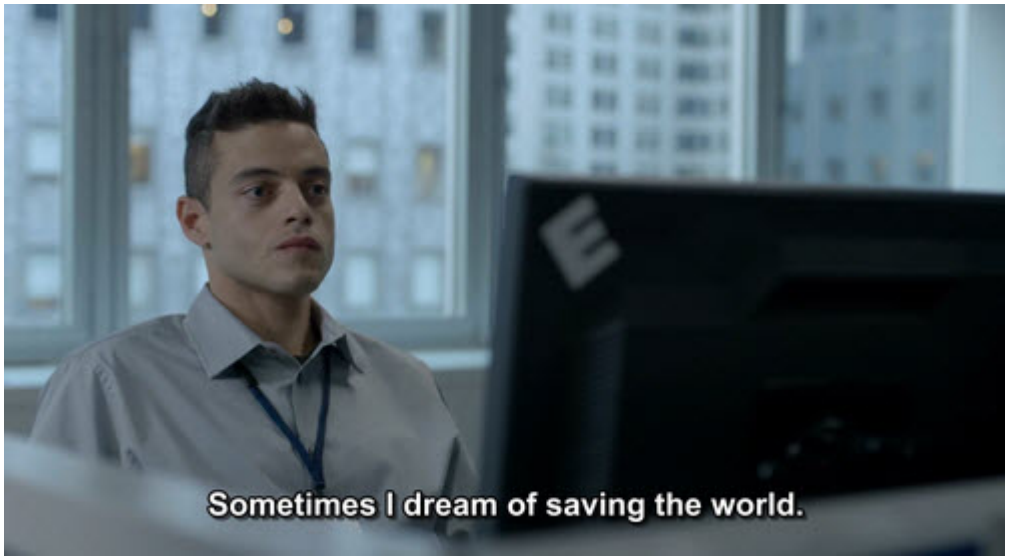
Sorular;

1. bt.apk uygulaması Android işletim sistemi yüklü simülatöre yüklenip çalıştırıldıktan sonra data parametresindeki gizlenmiş (encoded) veriyi oluşturan fonksiyon hangisidir ?
2. Bu fonksiyonun gizlenmiş veriyi nasıl oluşturduğunu ekran görüntülerine de yer vererek detaylı bir şekilde açıklayınız.
3. Bu fonksiyondan yola çıkarak aşağıdaki data parametresinde yer alan gizlenmiş veriyi (encoded) çözen betik dosyasını oluşturup, verinin çözülmüş hali ile birlikte tarafıma gönderiniz.
   data=H4sIAAAAAAAAAFWRQW6EMAxF75I1HRFgGMSuJ4kMMa3VEKMkwwytevc6aoXSLLL4_s5_dr5UohXVqLtb1-p2aIdKcTQ7hkjs1aj6S60qNUFKGA7jcEcn7ktdKfIieXAmcYIsNrdrXyl8_pdLJ-xADiaXA3U_6MJdlKTjQQuZmb3HOaFVYwp3rNTKEzks9QVczIVI0WZafZXT5LsTahJdxFbXTV-fRwq8YYDEQYqv3gYmK2JgLrLyWj7ZC86L7rpamGDbTPacqRZ3mtGAXcmfiHE7zAceE0Ow5h4LyBlWSS0H_W2J7_wwNOdt_zmfG0ujgTnRDuWc8i20HCaToM9vnLhvm4kYMk-UBX7_AOOMoKfXAQAA

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 3 Ekim 2016 Saat 19:00'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: bt.apk dosyasını IDA Pro ile dinamik olarak analiz edenler, hata ayıklama esnasında "Oops! internal error 1201 occured." hatası almamak için ida_android_fix.zip dosyasında yer alan plugins klasörünü IDA'nın yüklü olduğu klasöre kopyalamalıdırlar.


Sometimes I dream of saving the world.