Pi Hediyem 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 Hediyem 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 Erdinç 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 açıklamanız 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

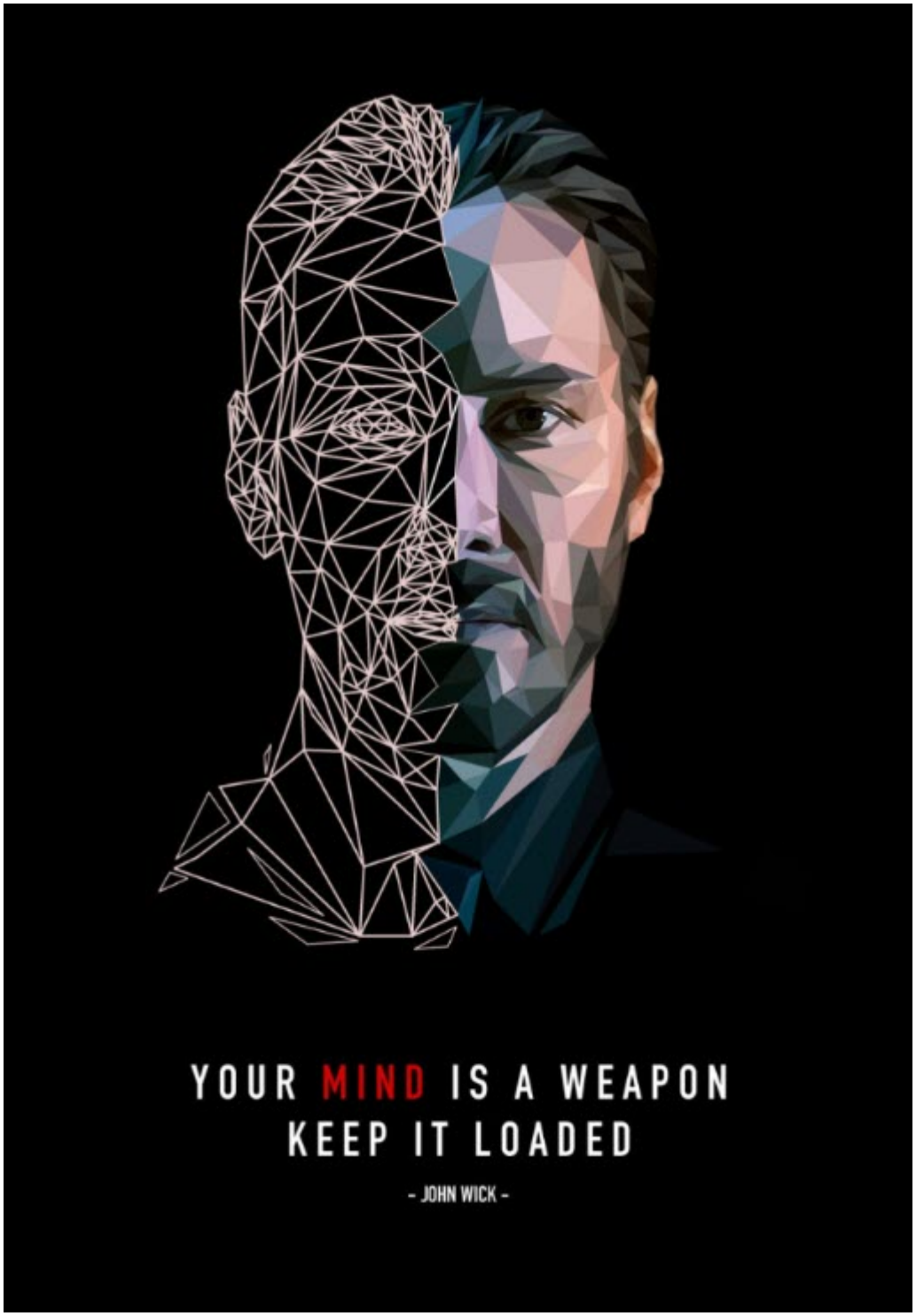
```
Build/OPR6.170623.017)
Host: xxxxxxxxxxxxxxx
Accept-Encoding: gzip
Connection: keep-alive

sti=006&q=saved_data_attacker&zip=q7&ws=ODYyMmYzNDRiMThjZDU3MzM3YWNmZmUw
MWNiZDZlNzk4NjdiZjA1MGY5NmY0NzIyYjJkMTBhYWM1MzhhNWQ2Nzc3MzRiMDgyMzgxZjI1
NTQ2ZGFkZTg4ODBhYjZkOWQwOWFiY2Y0NjU1MTJlM2JmMjllNDAwN2E4MDVkMWQwZjQxMWEw
MDY4ZWIyOTlhMGY4YWY3NDk4NWIxNmM5NDEyMjNmOTAyMzNhNGRhMDQ4MGM1YWUzN2NiYzVh
MzNhZTI1NzRjMTg4ODlmNGYwYThhMGRkMzYxYTk3OGNhOGU0NDI5YTI2Y2VjYzhiYzZlMWE2
OWRiMWI4ZDViMWM0Yjc5YjcyNjQ4NTZlNGJjNWZkYjhhZDY1MWVlMDBlYzM3MTM2NTk3ZTQz
ZDhiM2JmNWY2YjBkYzdkMDUxYWRmMjZiOTgzMTU3ZjZiMDhhNjE4ZTY2NDdhMzIyOTg3ODI1
ZmM2ZGNhMGU3MGM3OTMxZWE1ZWQwMzdhZDJlZjBlYjQ1ODdkNTc3ZDg2YTg0NzdiYWUyNWI4
OTAxZTQ2NzAxNDVhNjM1MTQ0ZjFiZmE0NWU2ZjlhYWZmMmY0N2MyY2ZjNGU5MWU5ZDk3OWY5
MDE5M2MzNzc2YmRmOTY4NWQ3NjhjOTIxMjk3OWVkYTUyYmJiNjkwZGYwMTIyODUxNzM5Mjc3
ODgxYTcyMmMzMDUwNjA2YTM0OGQ1NDUwMzg1ODk5NTlkOWVlZmY0ZDViNTYwMGZmOTllYjkz
ZjE3ODFiYmI0OTUyYzM3ZjQzYzA0NjUxYWFjNjMxMjU1OGNkMzUwYWY5NTMyYTRlMjM2NmE2
ZmYxMGU4M2QzZjc1MDk5NWE5MzVhZjVjODQwYjRiZjAwMGEwZWQ1YmQ0N2Y2ZGIzYWYxYTlj
NzFhYWRmZDE3M2U2NWU3MjY5NDQ0NzUzOWI1ZjhlYjEzOTZhNzJjN2U4N2ZhYjc1MDgzYzM2
NWFiZWRhOTQwODM5MmYzZTJkZjY2NDAyYWMwZmEyZjgxYTQ2NzVhM2JiYWNlODRjODAxNzlk
ZTdiNWViMDFmODgxNDkyOWZk
```

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 23 Şubat Pazar Saat 21:00'a kadar iletmeleri gerekmektedir. Doğru bilen çıkmadığı taktirde ilave süre verilecektir.

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


YOUR MIND IS A WEAPON
KEEP IT LOADED
- JOHN WICK -