iPhone Mobil Uygulamalardaki SSL Pinning Korumasını Bypass'lama ve Trafiklerini Burp ile Alabilme

Problem:

Mobil telefonun trafiği proxy ayarı ile bilgisayardaki burpsuite'e yönlendirildiğinde örneğin mobil telefondaki web tarayıcı http ve https trafiği bilgisayardaki burp arayüzüne gelirken mobil telefondaki X mobil uygulamasının http / https trafiği bilgisayardaki burp arayüzüne gelmemekte.

Neden:

Mobil telefondaki mobil uygulama eğer ssl pinning kullanıyorsa bu durumda istemci taraflı ssl sertifika doğrulaması yapıyor demektir. Bu ise araya MITM ile giren ve sahte sertifika ile haberleşmeyi çözümleyen proxy tool'ları kullanımı durumunda mobil uygulamanın trafiği başlamadan sonlanmakta. Çünkü mobil uygulamanın istemci taraflı sertifika doğrulaması başarısız olmakta. Bu ise proxy aracının mobil uygulama https trafiğini alamamasına sebep olmakta.

Çözüm:

SSL Pinning korumalı mobil uygulamaların https trafiğini alabilmek için mobil telefondaki istemci taraflı ssl sertifika doğrulamasını disable eden SSL Kill Switch jailbrak uygulaması kullanılmalıdır. Bu uygulamanın son sürümü github'dan mobil uygulamaya kurulmalıdır.

(Not: Cydia mağazasından MTerminal terminal uygulaması önce kurulmalıdır ve MTerminal başlatılmalıdır.)

MTerminal Console Uygulaması:

Root Erişimi Yapma (parola: alpine)
> su

SSL Kill Switch Son Stabil Sürümünü Github'dan Mobil Telefona İndirme
> wget https://github.com/nabla-c0d3/ssl-kill-switch2/releases/download/0.14/com.nablac0d3.sslkillswitch2_0.14.deb -O ssl.deb

SSL Kill Switch Deb Paketini Mobil Telefonda Kurma
> dpkg -i ssl.deb

Spring Board'u Restart'lama
> killall -HUP SpringBoard

Uyarı:

SSL Kill Switch 2 jailbreak uygulaması cydia mağazasından indirildiğinde işe yaramamakta ve ssl pinning korumalı mobil uygulamaların trafiği bilgisayardan burp ile alınamamakta. Fakat SSL Kill Switch 2 jailbreak uygulaması son sürümü github'dan mobil telefona indirildiğinde ve yukarıdaki gibi kurulduğunda ssl pinning korumalı mobil uygulamaların (örn; X Kurumu A Uygulaması veya App Store) https trafiği bilgisayardan burp ile alınabilmekte.

Bu adımlar neticesinde iPhone -> Settings’de SSL Kill Switch tweak’i listelenen uygulamalar arasında yerini alacaktır. Böylece mobil telefonda internet proxy ayarı girildiğinde ve bilgisayarda burpsuite ile trafik izlemeye başlandığında ssl pinning koruması olan mobil uygulamaların https trafiği alınabilir olacaktır ve trafikte düzenlemeler yapılabilecektir.

Kaynaklar:

https://github.com/nabla-c0d3/ssl-kill-switch2
https://github.com/nabla-c0d3/ssl-kill-switch2/releases/tag/0.14
https://medium.com/@yogendra_h1/ios-application-security-jailbreak-12-4-5e3fc0dc0726