Gün 4

Not defteri:	Zararlı Yazılım Analizine Giriş		
Oluşturulan:	28.01.2020 09:43	**Güncellen...**	2.02.2020 17:27
Yazar:	Özlem Körpe		

Android Zararlı Yazılım Türleri

Kötü Amaçlı Bankacılık Yazılımları: Saldırganlar para transferi ve fatura ödeme dahil olmak üzere tüm işlerini mobil cihazlarından yürütmeyi tercih eden kullanıcıları ele geçirmeye çalışıyor. Truva atlarının çoğu, cihazlara sızıp yerleşerek bankacılık oturum açma bilgilerini ve parolaları toplamak ve komuta-kontrol (C&C) sunucusuna göndermek için tasarlandı.

Mobil Fidye Yazılımı: Önceleri PC'lerde popüler olan fidye yazılımı belge, fotoğraf ve videolar gibi önemli kullanıcı verilerini şifreleyip "kilitler" ve ardından kötü amaçlı yazılım oluşturucularına bir fidye ödenmesini talep eder. Fidye (genellikle Bitcoin cinsinden) zamanında ödenmezse tüm dosyalar silinir veya kilitlenir ve kullanıcı bunlara sonsuza dek erişemez. Fidye yazılımı, en kalıcı tehditlerden biriydi ve kötü amaçlı yazılım oluşturucuları, cihazlara virüs bulaştırmak ve depolanan verileri şifrelemek için hem iyileştirilmiş akıllı telefon performansından hem de anonim Tor ağından faydalandı.

Spyware & Mobil Casus Yazılım: Cihazınıza program olarak yüklenen casus yazılım etkinliğinizi izler, konumunuzu kaydeder ve e-posta hesaplarının veya e-ticaret sitelerinin kullanıcı adları ve parolaları gibi önemli bilgileri kaldırır. Çoğu durumda casus yazılım, görünüşte iyi olan yazılımlara eklenir ve arka planda sessizce veri toplar. Cihaz performansı düşene veya tablet ya da telefonunuzda kötü amaçlı yazılımdan koruma tarayıcısı çalıştırana kadar casus yazılımın varlığını bile fark etmeyebilirsiniz.

MMS Kötü Amaçlı Yazılımı: Kötü amaçlı yazılım oluşturucular da kötü amaçlı yazılım göndermenin bir yolu olarak mesaj tabanlı iletişimden faydalanmanın yollarını arıyor. CSO Online'a göre, Android'in medya kitaplığındaki Stagefright adlı bir güvenlik açığı, saldırganların herhangi bir cep telefonu numarasına kötü amaçlı yazılım içeren bir mesaj göndermesini sağladı. Kullanıcılar mesajı açmasa veya kabul etmese bile kötü amaçlı yazılım yerleşerek saldırganların mobil cihazınızın kök dizinine erişmesine olanak tanıdı. Sorun hızla yamalandı ancak mesaj tabanlı virüslerin kanıtını sundu.

Adware % Mobil Reklam Yazılımı: Reklam yazılımları sinir bozucu açılır pencereler ve veri toplamanın çok ötesine geçti. Çoğu reklam yazılımı oluşturucunun geliri, aldığı tıklama ve indirme sayısına bağlıdır. ZDNet'e göre ise bazıları cihazınıza virüs bulaştırıp kök dizinine ulaşabilen, böylece belirli reklam yazılımı türlerini indirmesine ve saldırganların kişisel bilgileri çalmasına olanak tanıyan bir "kötü amaçlı reklam" kodu oluşturdu.

SMS Truva atları: Siber suçlular, kullanıcıların telefonlarıyla ilgili en çok sevdiği şeyi, metin mesajlarını avlayarak mobil cihazlara virüs bulaştırıyor. SMS Truva atları, dünya genelinde premium numaralara SMS mesajları göndererek ve kullanıcıların telefon faturalarını yükselterek büyük finansal zarar verir. 2015 yılında bazı Android kullanıcıları finansal bilgileri içeren metin mesajlarını durdurup metin mesajının bir kopyasını e-posta yoluyla gönderen ve böylece siber suçlulara finansal hesaplara sızmaları için gerekli tüm bilgileri sunan bir bankacılık Truva atı kaptılar.

Kaynak: https://www.kaspersky.com.tr/resource-center/threats/mobile

Frida

-U: USB modu

-f: Manuel olarak başlatmak

https://github.com/frida/frida/releases/download/12.8.9/frida-server-12.8.9-android-x86.xz

```
adb push frida-server-vvv /data/local/tmp
adb shell
cd /data/local/tmp
chmod +x frida-server-vvv
./frida-server-vv &

frida-ps -U
```

Del.js Dosyası

```
// install package with adb install package.name
// do not open application
// use -f force option
// frida -U -f package.name -l del.js
Java.perform(function() {


    var f = Java.use("java.io.File")
    f.delete.implementation = function(a){
        if(this.getAbsolutePath().includes("jar")){
            console.log("[+] Delete catched =>" +this.getAbsolutePath())
        }
        return true
    }
})
```

```
frida -U -f com.paket.adi -l del.js
```

Minesweeper for Frida

https://github.com/anirudhrata/Minesweeper-Frida

Mine Detector Script for Mine

```
setImmediate(function() { //prevent timeout
    console.log("[*] Starting script");
    Java.performNow(function() {
       Java.choose("Draziw.Button.Mines.MainActivity", {
            onMatch: function (instance) {

    for(var x =0; x< 16;x++){
                    var line = ""
                    for(var y = 0;y<11;y++)
                    {
                      var cell = instance.a(x,y)
                      if(cell== 10)
                        line += '\x1b[31mX\x1b[0m'
                      else {
                          var n = 0
                          if(cell == 1)       n = '\x1b[34m'
                          else if(cell == 2)  n = '\x1b[32m'
                          else if(cell == 3)  n = '\x1b[35m'
                          else if(cell == 4)  n = '\x1b[36m'
                          else if(cell == 5)  n = '\x1b[37m'
                          else  n = '\x1b[37m'
                          line += n + cell + '\x1b[0m'
                      }
                      //console.log(" " + instance.a(x,y))
                    }
                    console.log(line)
                }
            },
              onComplete: function () {
               }
        });
    })
})
```