

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ

CERT-RO



# Evoluția malware-ului pentru dispozitive mobile în 2015

---

Pagină albă

## CUPRINS

1. Introducere .....	5
2. Cum suntem infectați? .....	6
2.1. Phishing, Spear-phishing, SMS-phishing, App-phishing .....	6
2.2. Rooting și Jailbreak .....	7
2.3. Conectarea la un punct de acces Wi-Fi compromis .....	7
2.4. Posesia unui dispozitiv modificat hardware sau software .....	8
3. Semne că am fost infectați .....	8
3.1. Facturi telefonice mai mari .....	9
3.2. Trafic de date crescut .....	9
3.3. Bateria se consumă rapid .....	9
3.4. Scăderea performanței terminalului .....	9
3.5. Apeluri întrerupte .....	9
3.6. Pattern-uri ale accesului la date neobișnuite .....	9
3.7. Aplicații necunoscute de utilizator .....	9
3.8. Dispozitivul mobil a fost supus procesului de rooting/jailbreaking .....	9
3.9. Soluția de securitate instalată este nefuncționabilă .....	9
4. Cum ne protejăm? .....	10
4.1. Parolarea dispozitivului .....	10
4.2. Actualizarea aplicațiilor descărcate și a sistemului de operare .....	10
4.3. Blocarea automată a terminalului .....	10
4.4. Descărcarea aplicațiilor doar din surse verificate .....	10
4.5. Examinarea cererilor de permisiuni ale aplicațiilor descărcate .....	11

4.6. Instalarea unui software de securitate.....	11
4.7. Scanarea aplicațiilor descărcate.....	11
4.8. Criptarea dispozitivului .....	11
4.9. Protecție anti-furt .....	11
4.10. Restricționarea apelurilor, mesajelor.....	12
4.11. Prevenirea rooting-ului .....	12
4.12. Verificarea link-urilor primite via SMS sau email.....	12
4.13. Accesarea doar a hot-spot-urilor sigure .....	12
4.14. Blocarea conectării automate la Wi-Fi .....	12
4.15. Blocarea conectării automate la Bluetooth.....	12
5. Studii de caz.....	13
5.1. Vulnerabilități Android OS .....	13
5.2. Vulnerabilități iOS.....	15

## 1. Introducere

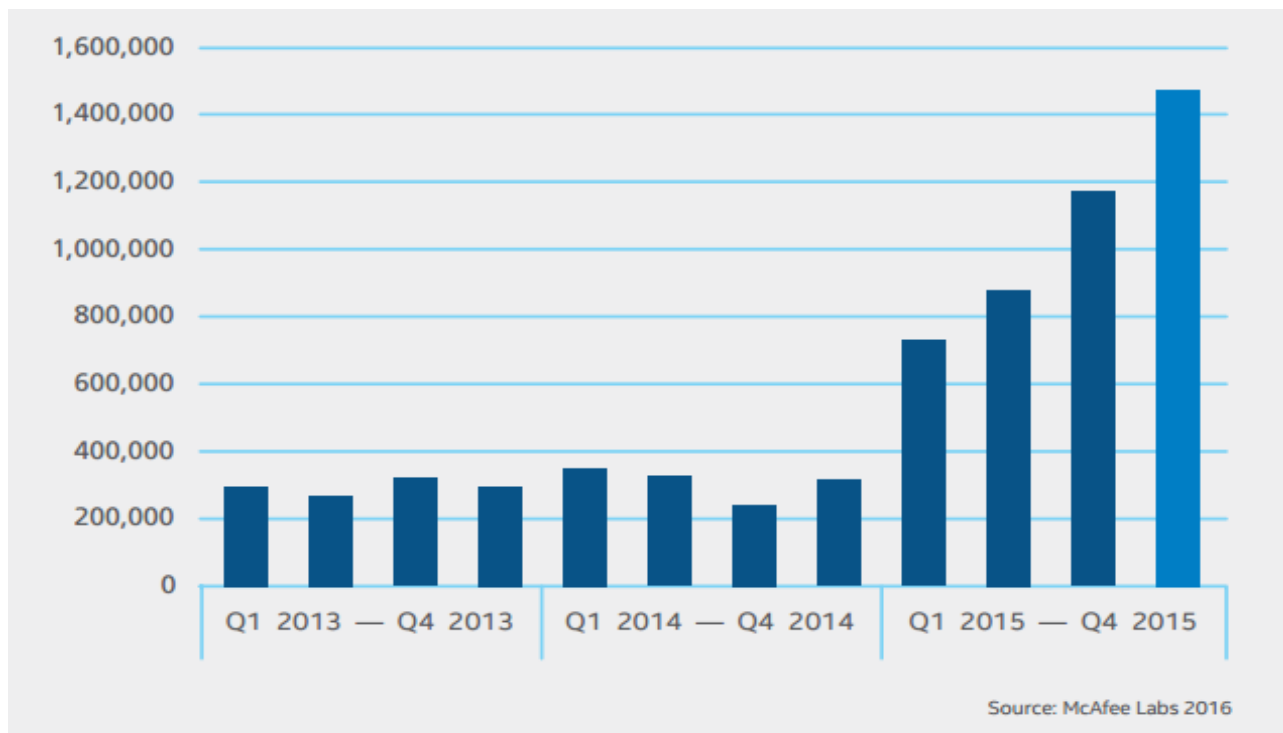
Au trecut mai bine de 10 ani de la momentul apariției primului cod malițios dezvoltat cu scopul de a compromite un dispozitiv mobil, însă acesta a devenit o amenințare serioasă la adresa securității utilizatorului final îndeosebi în ultimii ani. Creșterea exponențială a numărului de utilizatori de telefoane inteligente, respectiv tablete din ultimii ani a condus în mod inevitabil la captarea atenției și prezentarea unui interes sporit sectorului de dispozitive mobile din partea infractorilor din mediul cibernetic.

Mai mult decât atât, îmbunătățirea continuă a caracteristicilor privind viteza de transfer a datelor, puterea de procesare, memoria și bateria au reușit să atragă utilizatorii finali și să le ofere confortul de a fi mereu "conectați". Astfel, performanțele din ce în ce mai ridicate ale unui terminal mobil au dus la creșterea continuă a numărului de utilizatori care folosesc dispozitivele mobile pentru încheierea tranzacțiilor financiare, achitarea taxelor și impozitelor, efectuarea cumpărăturilor online, etc.

În acest context, mostrele de malware destinate dispozitivelor mobile identificate în ultima perioadă încep să se asemeze din punct de vedere al complexității cu cele dezvoltate pentru compromiterea PC-urilor. Exemple din această categorie pot fi reprezentate de troienii utilizați în campanii de tip *Advanced Persistent Threat* (APT, ex. *SlemBunk*), în *Remote Access Tool*-urile (ex. *Adwind*) utilizate de atacatori pentru a accesa de la distanță terminalele compromise și în campaniile de *ransomware* (ex. *Svpeng*)[sursa: *McAfee Labs*].

Conform rapoartelor realizate de către companiile cunoscute specializate în securitate cibernetică, statisticile privind evoluția malware-ului destinat platformelor mobile indică o creștere îngrijorător de mare a numărului de mostre de cod malițios înregistrate în anul 2015. În intervalul 2004 – 2013 au fost detectate aproximativ 200000 de mostre de cod malițios, în anul 2014 aproximativ 300000, în timp ce în anul 2015 un număr de aproximativ 900000 de mostre unice de cod malițios pentru dispozitive mobile au fost înregistrate [sursa: *Kasperky Lab*].

Dezvoltatorii de cod malițios pentru dispozitivele mobile cunosc faptul că cea mai bună metodă de a infecta un număr maxim de dispozitive este de a ataca piețele principale de aplicații. Astfel, modul cel mai probabil prin care un dispozitiv mobil poate fi compromis este de a descărca o aplicație aparent legitimă, dar care inserează în codul sursă și cod malițios, care nu a fost verificată suficient.



## 2. Cum suntem infectați?

Suprafața de atac a dispozitivelor mobile este aproximativ identică pentru toate platformele mobile (*Android, iOS, Windows, etc.*) deoarece atacatorii au găsit modalități de a publica aplicații malițioase chiar și în magazinele online oficiale, sau de a ataca utilizatorii fie prin SMS, fie prin puncte de acces Wi-Fi compromise.

### 2.1. Phishing<sup>1</sup>, Spear-phishing, SMS-phishing, App-phishing

Platformele mobile sunt expuse în mod egal la atacuri de tip *phishing, spear-phishing, SMS-phishing* și *app-phishing*. De fapt, dispozitivele mobile expun organizațiile din ce în ce mai mult unor astfel de atacuri direcționale datorită mijloacelor propriu-zise de a ajunge la utilizatorul victimă vizat: conturi de email personale, contul de email de la locul de muncă, mesaje text de tip SMS și aplicații malițioase ce redirecționează victima către pagini web cu conținut malițios sau pagini web false (*app-phishing*).

Statisticile arată că utilizatorii de dispozitive mobile sunt de aproximativ trei ori mai susceptibili decât cei conectați într-o rețea administrată corespunzător. Utilizatorul de smartphone sau tabletă își verifică constant toate conturile configurate pe dispozitiv, accesează site-uri web care pot fi nesigure, probabilitatea de a fi compromis fiind una mai mare datorită lipsei de măsuri de

<sup>1</sup> O formă de activitate infracțională care constă în obținerea unor date confidențiale, cum ar fi date de acces pentru aplicații de tip bancar, aplicații de comerț electronic (ca eBay sau PayPal) sau informații referitoare la carduri de credit, folosind tehnici de manipulare a datelor identității unei persoane sau a unei instituții.

O înșelăciune electronică constă, în mod obișnuit, în trimiterea de către atacator a unui mesaj electronic, folosind programe de mesagerie instantanee sau telefon, în care utilizatorul este sfătuit să-și dea datele confidențiale pentru a câștiga anumite premii, sau este informat că acestea sunt necesare datorită unor erori tehnice care au dus la pierderea datelor originale. În mesajul electronic este indicată de obicei și o adresă de web care conține o clonă a sitului web al instituției financiare sau de trading. Majoritatea phisherilor folosesc această metodă pentru a obține date bancare.

protecție *anti-phishing* implementate, comparativ cu un sistem protejat din cadrul unei rețele ce respectă standardele de securitate actuale. În plus, ecranul mult mai mic al dispozitivelor mobile poate face mai dificilă observarea unui URL malițios.

## 2.2. Rooting<sup>2</sup> și Jailbreak<sup>3</sup>

Platformele mobile sunt susceptibile la programele utilizate de atacatori pentru a obține drepturi depline la resursele dispozitivului mobil vizat. Aceste software-uri sunt dezvoltate în scopul pătrunderii în sistemul de operare, prin exploatarea unei vulnerabilități, și elevarea privilegiilor. În timp ce producătorii software se străduiesc să protejeze utilizatorii prin izolarea acestora (a proceselor deschise de utilizator) într-un mediu sigur (*sandboxing*), cei din urmă încearcă să realizeze *rooting* (Android), respectiv *jailbreak* (iOS) pentru a eluda măsurile de securitate impuse de producător, astfel misiunea unui atacator devenind mult mai facilă. Utilizatorii platformelor mobile își doresc *rootarea* dispozitivelor din mai multe motive: descărcarea aplicațiilor care nu au fost aprobate de magazinele oficiale, modificarea configurărilor sistemului de operare, accesarea site-urilor web nesigure, descărcarea gratuită a aplicațiilor, etc.



## 2.3. Conectarea la un punct de acces Wi-Fi compromis

Un dispozitiv mobil ce suportă conectivitate wireless trece printr-un proces de descoperire prin care încearcă să se conecteze la o rețea Wi-Fi din proximitate. Acest proces poate fi fie pasiv - atunci când dispozitivul ascultă pentru a primi pachetele de broadcast de la rețele Wi-Fi, fie activ - atunci când dispozitivul trimite pachete în scopul identificării unei rețele la care să se conecteze. Este foarte probabil ca un smartphone să emită pachete de broadcast ce conțin numele rețelelor (SSID) pe care deja le are stocate în memorie. Astfel, un posibil atacator poate identifica locațiile

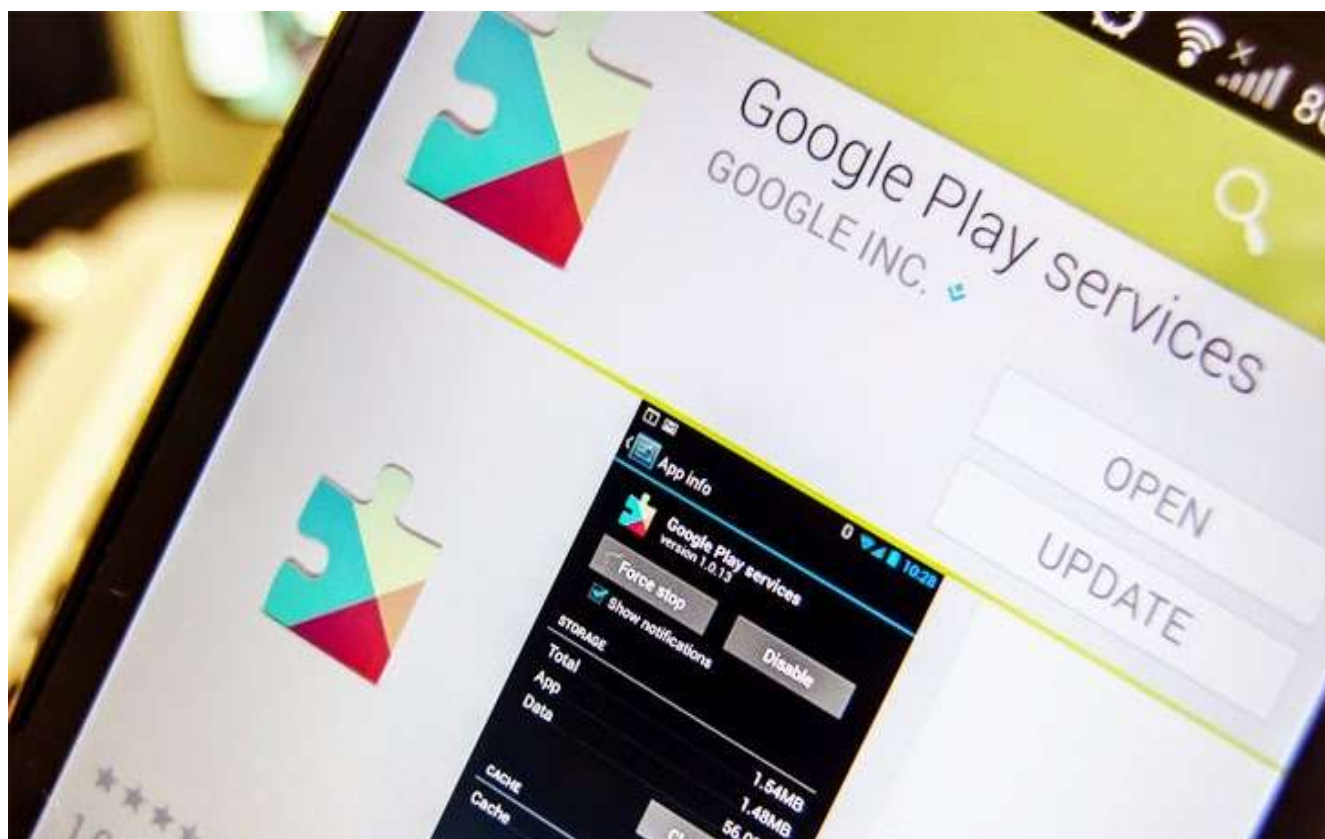
<sup>2</sup> *Rooting* este procesul prin care utilizatorii obțin drepturi de administrator (*root*) asupra sistemului de operare *Android*, pentru a avea acces complet la resursele platformei mobile.

<sup>3</sup> *Jailbreaking* reprezintă echivalentul procesului de *rooting* specific platformei *iOS*.

frecventate de proprietarul dispozitivului, numele rețelei de acasă, de la birou etc. În plus, atacatorul poate ulterior să configureze un punct de acces clonat (*rogue access point*), identic cu cel legitim din punct de vedere al configurării, în scopul forțării unei conexiuni din partea dispozitivului urmărit pentru a intercepta datele.

#### 2.4. Posesia unui dispozitiv modificat hardware sau software

Ofertele tentante pentru dispozitive performante ascund de multe ori un sistem afectat și controlat de infractorii cibernetici. Un caz relativ recent din această categorie este reprezentat de un smartphone echipat cu un program *spyware* chiar din fabrică distribuit în Europa și comercializat de marii retaileri online. Programul malware este deghizat ca aplicație *Google Play Store* și face parte din aplicațiile preinstalate. Acesta rulează în background și nu poate fi detectat de către utilizatori. Fără știrea utilizatorului, smartphone-ul trimite datele personale către un server de comandă și control și este capabil să instaleze pe ascuns aplicații suplimentare. Astfel, sunt posibile preluarea datelor personale, interceptarea apelurilor și a datelor de autentificare pe online banking, citirea emailurilor și a mesajelor text sau preluarea controlului camerei video și a microfonului, de la distanță. Pentru că programul *spyware* este integrat ca firmware al producătorului, acesta nu poate fi șters de pe dispozitiv.



### 3. Semne că am fost infectați

Deși atacatorii depun un efort din ce în ce mai mare pentru a rămâne nedetectați există însă câteva semne care trădează un telefon infectat:



### 3.1. Facturi telefonice mai mari

Adesea malware-urile pentru dispozitive mobile au ca scop trimiterea de mesaje text la numere cu suprataxă. Efectele se văd imediat în facturile telefonice, însă unele programe malițioase sunt mai discrete. Ele pot trimite câte un mesaj o dată pe lună pentru a nu trezi suspiciuni sau se pot dezinstala automat după o lovitură de proporții în bugetul utilizatorului.

### 3.2. Trafic de date crescut

Prin setarea unui volum de trafic limită vă puteți da seama rapid dacă terminalul este infectat cu un virus care vă fură date.

### 3.3. Bateria se consumă rapid

Unii viruși se pot da de gol prin faptul că generează un consum neobișnuit de ridicat al bateriei.

### 3.4. Scăderea performanței terminalului

Verificarea memoriei RAM (*Random Access Memory*) sau a consumului procesorului poate scoate la iveală prezența virușilor activi pe dispozitivul infectat (aceștia vor încerca să scrie, să citească sau să redirecționeze date).

### 3.5. Apeluri întrerupte

Convorbirile întrerupte sau alte interferențe neobișnuite pot scoate la iveală existența unor aplicații malițioase.

### 3.6. Pattern-uri ale accesului la date neobișnuite

Pentru a observa dacă dispozitivul mobil compromis transferă date către serverul de comandă și control, se recomandă verificarea periodică a traficului de date, respectiv a consumului acestuia per aplicație. Dacă se observă o diferență mai mare de 10MB între cât trafic crede utilizatorul că epuizează și cât trafic consumă aplicațiile în realitate, atunci este foarte probabil să fie vorba despre un consumator parazit, o aplicație malițioasă.

### 3.7. Aplicații necunoscute de utilizator

Dacă sunt observate aplicații care nu sunt instalate de utilizator în dispozitivul mobil, cel mai probabil acestea au fost descărcate de o altă aplicație malițioasă.

### 3.8. Dispozitivul mobil a fost supus procesului de rooting/jailbreaking

Obținerea drepturilor de administrator oferă utilizatorilor posibilitatea de a instala și folosi aplicații diverse, versiuni de sisteme de operare customizate, dar în același timp o aplicație malițioasă va rula cu drepturi de *root*.

### 3.9. Soluția de securitate instalată este nefuncționabilă

Oprirea bruscă a funcționării soluției de antivirus sau firewall poate semnifica prezența unei aplicații malițioase ce rulează pe dispozitivul mobil compromis.

## 4. Cum ne protejăm?

### 4.1. Parolarea dispozitivului

În pofida îngrijorării cu privire la infectarea terminalului mobil via Internet, cel mai simplu mod de compromitere a acestuia rămâne instalarea manuală a unui software malițios către o parte terță cu intenții malițioase. Blocarea accesului neautorizat asupra dispozitivului mobil prin parole, respectiv *pattern* sau *PIN*, este primul pas recomandat pentru o siguranță sporită a acestuia.

*Aplicații: LastPass, aWallet, Dashlane, DataVault, Keepass2Android*

### 4.2. Actualizarea aplicațiilor descărcate și a sistemului de operare

Actualizările pentru aplicații sau sisteme de operare deseori includ patch-uri ce repară vulnerabilitățile de securitate existente.

*Aplicații: Update me Smartphone, Software Updates, Smart Launcher 2*

### 4.3. Blocarea automată a terminalului

Majoritatea dispozitivelor mobile permit blocarea acestora după un interval de timp ales de utilizator. Se recomandă setarea acestui interval la mai puțin de 2 minute.

### 4.4. Descărcarea aplicațiilor doar din surse verificate

Se recomandă descărcarea și instalarea aplicațiilor pentru dispozitive mobile doar din surse oficiale ale producătorilor, precum *Google Play* și *App Store*.



#### 4.5. Examinarea cererilor de permisiuni ale aplicațiilor descărcate

Multe aplicații solicită mai mult decât permisiunile necesare (acces la SMS-uri, coordonate GPS, galerie foto, contacte etc.). Se recomandă verificarea listei de permisiuni pe site-ul oficial al producătorului și dezactivarea acestora dacă aplicația respectivă nu este utilizată. Există și o serie de instrumente software care pot verifica automat dacă o aplicație sau firmware-ul existent pe telefon sunt vulnerabile și permit escaladarea privilegiilor.

*Aplicații: SAndroid, WeChecker, DroidRay etc.*

#### 4.6. Instalarea unui software de securitate

Se recomandă căutarea aplicațiilor care protejează utilizatorul în special față de amenințări de tip malware, remote data wipe etc.

*Aplicații: Bitdefender Mobile Security & Antivirus, Avira Antivirus Security, , Kaspersky Internet Security, McAfee Antivirus & Security, Malwarebytes Anti-Malware, Avast Mobile Security etc.*

#### 4.7. Scanarea aplicațiilor descărcate

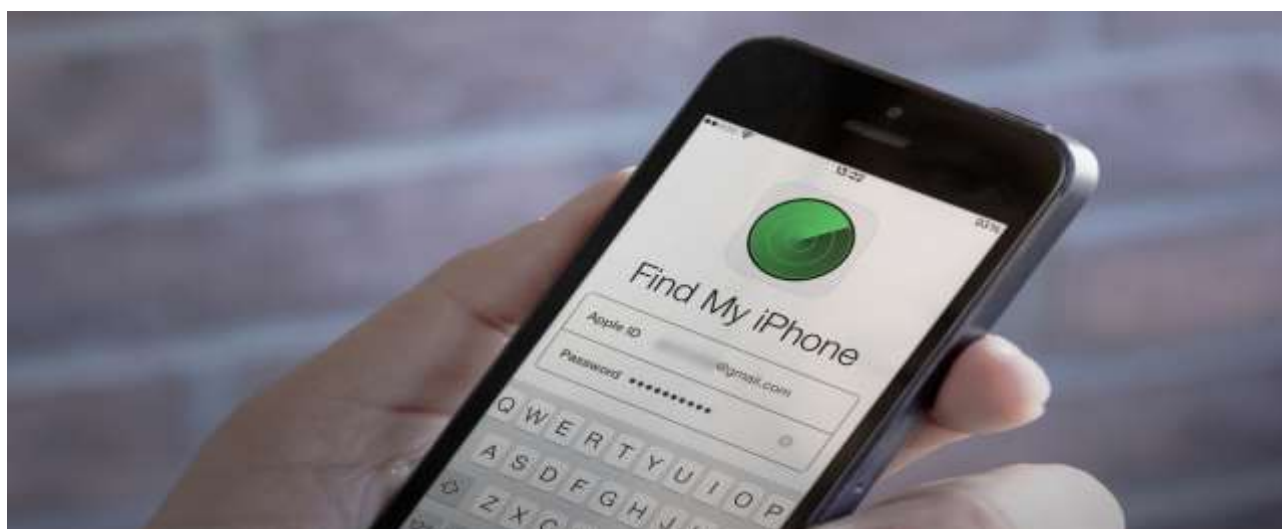
Indiferent de sursa aplicației, se recomandă scanarea acestora cu o soluție de securitate specifică terminalelor mobile.

*Aplicații: X-Ray, Android Network Toolkit – Anti, BullGuard Mobile Security*

#### 4.8. Criptarea dispozitivului

Riscul pierderii unui dispozitiv mobil este încă mai ridicat decât cel al infectării cu malware. Utilizarea criptării pentru datele stocate pe terminalul mobil previne accesul neautorizat la acestea.

*Aplicații: WiSeID, Lookout, Kaspersky Mobile Security, Silent Circle, Tiger Text*



#### 4.9. Protecție anti-furt

Protecția anti-furt a dispozitivului mobil oferă utilizatorului posibilitatea determinării locației terminalului sau a controlului de la distanță a acestuia.

*Aplicații: Find my iPhone, iHound, Android Anti-Theft Security, Prey Anti-Theft, Where's my Droid*

#### **4.10. Restricționarea apelurilor, mesajelor**

În cazul pierderii sau compromiterii dispozitivului mobil, un astfel de serviciu oferit din partea furnizorului poate limita considerent eventualele pagube aduse utilizatorului final.

*Aplicații: Call Control - Call Blocker, Call Blacklist, Call+SMS Filter, Clean Inbox*

#### **4.11. Prevenirea rooting-ului**

Obținerea drepturilor de administrator ale unui utilizator de terminale mobile, implică posibilitatea acordării acestor drepturi unei aplicații malițioase. Se recomandă verificarea terminalului dacă a trecut prin procesul de *rooting* (*jailbreak*) și readucerea acestuia dacă este cazul, la setările din fabrică.

*Aplicații: Root Checker, Root Checker Pro, SuperSU, Speruser*

#### **4.12. Verificarea link-urilor primite via SMS sau email**

Fiind una dintre cele mai uzuale metode folosite de atacatori, se recomandă acordarea unei atenții sporite link-urilor sau atașamentelor primite via SMS, respectiv via email.

*Aplicații: Sophos, AVG Antivirus Security, ESET Mobile Security and Antivirus*

#### **4.13. Accesarea doar a hot-spot-urilor sigure**

Hotspot-urile wireless publice sunt vulnerabile interceptărilor de trafic și răspândirii virușilor, întrucât nu sunt protejate de parole și pot fi accesate de oricine. Imaginați-vă că cineva aflat în apropiere vă interceptează pachetele de date și vede tot ce faceți pe Internet. Asigurați-vă că funcțiile Wi-Fi și Bluetooth sunt oprite atunci când nu le utilizați. Acestea vor consuma bateria și pot facilita accesul neautorizat la datele de pe dispozitivul mobil.

*Aplicații: WiFiFoFum – WiFi Scanner, Network Signal Info, WiFi Manager, AVAST SecureLine VPN, HOTSPOT SHIELD*

#### **4.14. Blocarea conectării automate la Wi-Fi**

Conectarea automată la puncte de acces Internet necriptate nu consumă doar bateria, ci înseamnă practic acordarea accesului oricui pe dispozitivul mobil.

#### **4.15. Blocarea conectării automate la Bluetooth**

Conectarea automată la Bluetooth lasă o ușă deschisă pentru orice persoană interesată să acceseze informații private, liste de contacte, parole stocate etc. de pe dispozitivul mobil. Pentru a evita furtul de informații, se recomandă utilizarea doar a conexiunilor Bluetooth despre care se cunoaște sigur că sunt securizate.

## 5. Studii de caz

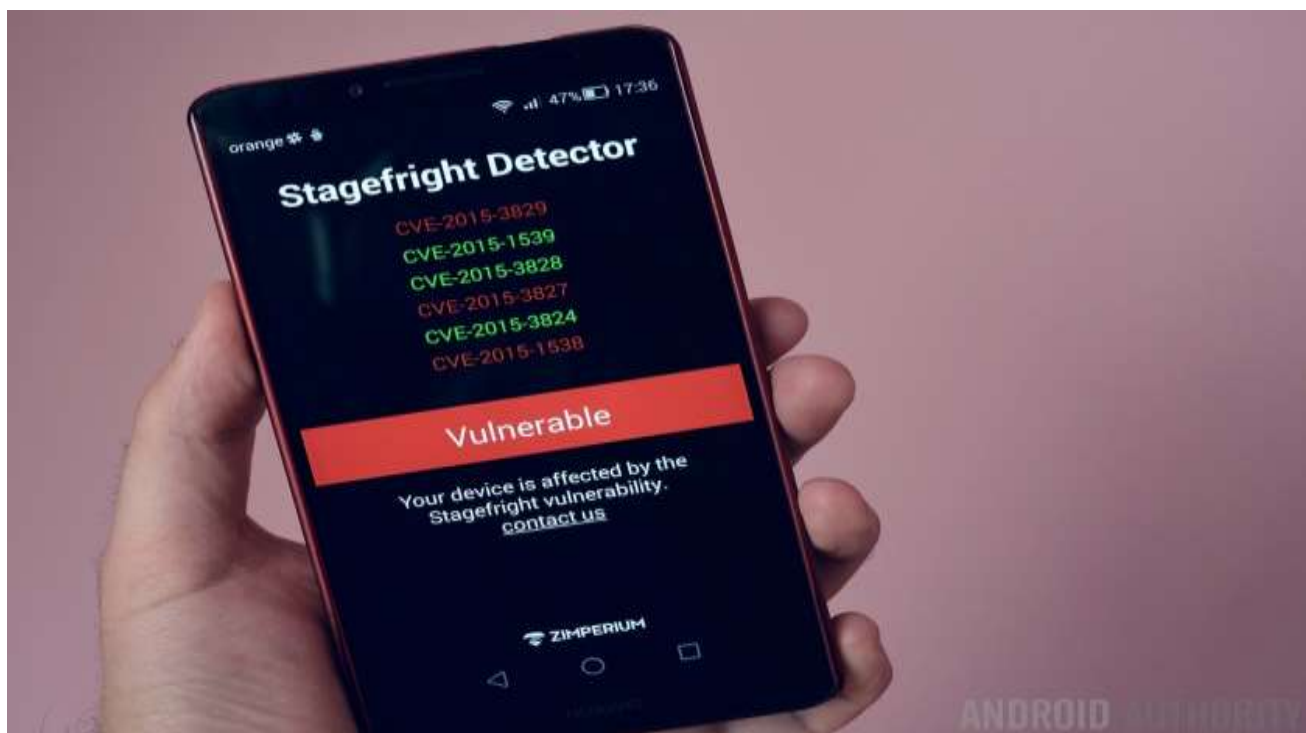
### 5.1. Vulnerabilități Android OS

Principală atracție pentru atacatori este reprezentată de platforma mobilă Android, aceasta fiind cea mai dinamică dintre platformele mobile cunoscute, beneficiind de cel mai mare număr de utilizatori, dar și pentru faptul că prezintă o piață deschisă de aplicații.

La nivel *enterprise*, utilizatorii sistemului de operare Android sunt mai expuși vulnerabilităților decât spre exemplu, utilizatorii dispozitivelor *Apple*. Un studiu recent efectuat de specialiștii din cadrul companiei de securitate *Appthority* din San Francisco arată că un procent de 88% din aplicațiile specifice Android prezintă un comportament funcțional predispus la vulnerabilități care ar conduce la eventuale scurgeri de date, comparativ cu 50% din aplicațiile pentru *iOS*.

În vara anului trecut, cu puțin timp înainte de celebra conferință *Black Hat* susținută în Las Vegas, au fost descoperite un număr consistent de vulnerabilități ale sistemului de operare Android cunoscute sub denumirea "*Stagefright*" (numele unor biblioteci de funcții din Android OS utilizate de mai multe aplicații mobile).

Conform experților din cadrul companiei de securitate *Zimperium Mobile Security*, aproximativ 95% din dispozitivele Android sunt expuse unor vulnerabilități critice identificate în cadrul bibliotecii de funcții utilizate pentru procesarea formatelor multimedia *Stagefright*.



Astfel, dispozitivele mobile care rulează o versiune a sistemului de operare Android, cuprinsă între versiunea 2.2 și versiunea 5.1.1\_r4, conțin multiple vulnerabilități ale motorului de redare fișiere multimedia *Stagefright*. Exploatarea acestor vulnerabilități poate permite unui atacator să acceseze fișiere multimedia sau să preia controlul asupra unui dispozitiv vulnerabil.

Utilizatorii rău intenționați pot exploata această vulnerabilitate prin trimiterea unui mesaj multimedia (MMS) modificat care inserează conținut malițios. Acest set de vulnerabilități sunt extrem de periculoase deoarece codul malițios poate fi executat fără interacțiunea utilizatorului victimă.

Spre deosebire de un atac clasic, precum cel prin care utilizatorul trebuie să deschidă un fișier malițios primit via email, vulnerabilitățile identificate de *Zimperium* pot fi exploatare de la distanță, prin execuția codului în mod automat de către funcțiile din biblioteca vulnerabilă, deoarece *Stagefright* procesează mesajul multimedia odată ce acesta a fost primit pe dispozitivul Android înainte ca utilizatorul să îl deschidă.

Dispozitivele Android clasificate drept vulnerabile sunt cele care rulează pe toate versiunile sistemului de operare Android începând cu versiunea 2.2 (*Froyo*) inclusiv până la versiunea 5.1.1\_r5 (*Lollipop*). Dintre acestea, cele mai expuse sunt cele anterioare Android 4.1 (*Jelly Bean*) deoarece nu au implementat sistemul ASLR (*Address Space Layout Randomization*), un mecanism de protecție utilizat împotriva vectorilor de atac de tip buffer overflow (exploatarea erorilor de memorie).

Un atacator care deține numărul de telefon al unui utilizator legitim poate trimite către cel din urmă mesaje multimedia modificate (MMS) al căror conținut malițios poate fi procesat necorespunzător de către aplicația *Stagefright*. Astfel, atacatorul poate executa de la distanță cod arbitrar malițios pe dispozitivul Android afectat, implicit poate obține acces neautorizat asupra acestuia.

În România, numărul utilizatorilor terminalelor cu sisteme de operare Android afectați de amenințările din spațiul cibernetic este în creștere. Potrivit *Bitdefender*, în ultimele trei luni din 2015, aplicațiile de tip *adware HiddenAds* și *HiddenApp* au putut crea trafic suplimentar consistent către site-urile selectate de către atacatori și, în consecință, au reprezentat un mod facil de a genera recurent încasări substanțiale cu un efort minim.

În lipsa folosirii unei soluții software pentru asigurarea securității terminalului, utilizatorilor le este dificil să identifice momentul în care au descărcat astfel de aplicații malițioase sau să le înlăture după ce sunt instalate.

Un studiu realizat de *Bitdefender* la finalul anului 2014 a arătat că una din trei rețele de publicitate online ar putea servi malvertising, un tip de atac ce poate infecta utilizatorii cu viruși, prin reclame găzduite chiar și pe site-uri legitime. Cercetarea asupra fenomenului a relevat și că aproximativ 7% din numărul total de reclame online infectează utilizatorii cu viruși sau îi păcălesc cu fraude, spam și phishing.

Deși nu se regăsesc între primele cinci amenințări la adresa terminalelor care folosesc Android, din ultimul trimestru al anului 2015, amenințările de tip *ransomware* vor continua să producă pagube utilizatorilor români în 2016. Clasa de viruși *ransomware* a vizat în mai 2015 circa 1.000 de terminale din România, prin atacuri originare de la servere localizate în Ucraina, așa cum *Bitdefender* a comunicat la momentul respectiv. Aproximativ 48% dintre utilizatorii români



infecțați ar plăti o recompensă medie de 550 de lei pentru a-și debloca datele criptate de *ransomware*, conform unui sondaj *iSense* realizat la comanda *Bitdefender* în noiembrie 2015[sursa: *bitdefender.ro*].



## 5.2. Vulnerabilități iOS

Anul 2015 ne-a demonstrat însă că platforma *Apple iOS* nu mai este atât de sigură din punct de vedere al securității cibernetice, așa cum se credea în urmă cu câțiva ani. Recent, se presupunea că mai mult de 39 de aplicații malițioase au eludat mecanismele de verificare ale *App Store* și sunt disponibile pentru a fi descărcate de către utilizatorii *Apple*. Acest lucru a fost posibil nu din cauza faptului că atacatorii ar fi spart magazinul online *Apple*, ci pentru că o versiune malițioasă a setului de instrumente *Xcode* utilizat pentru dezvoltarea aplicațiilor destinate platformei *iOS* a fost distribuită de către părți-terțe neautorizate, iar diferiți producători de astfel de aplicații au preferat să descarce această versiune (cunoscută sub denumirea de *XcodeGhost*) de pe serverele acestora.

Cea mai cunoscută dintre aplicațiile malițioase disponibile în *App Store* a fost reprezentată de *WeChat*, o versiune gratuită de *messenger* instalată pe aproximativ 700 de milioane de dispozitive mobile. Compania *Apple* a eliminat aplicațiile malițioase identificate, dar versiunea compromisă a platformei de dezvoltare *Xcode* a fost disponibilă pe Internet mai bine de 6 luni. Mai mult decât atât, codul sursă al *XcodeGhost* a fost publicat pe *Github*.

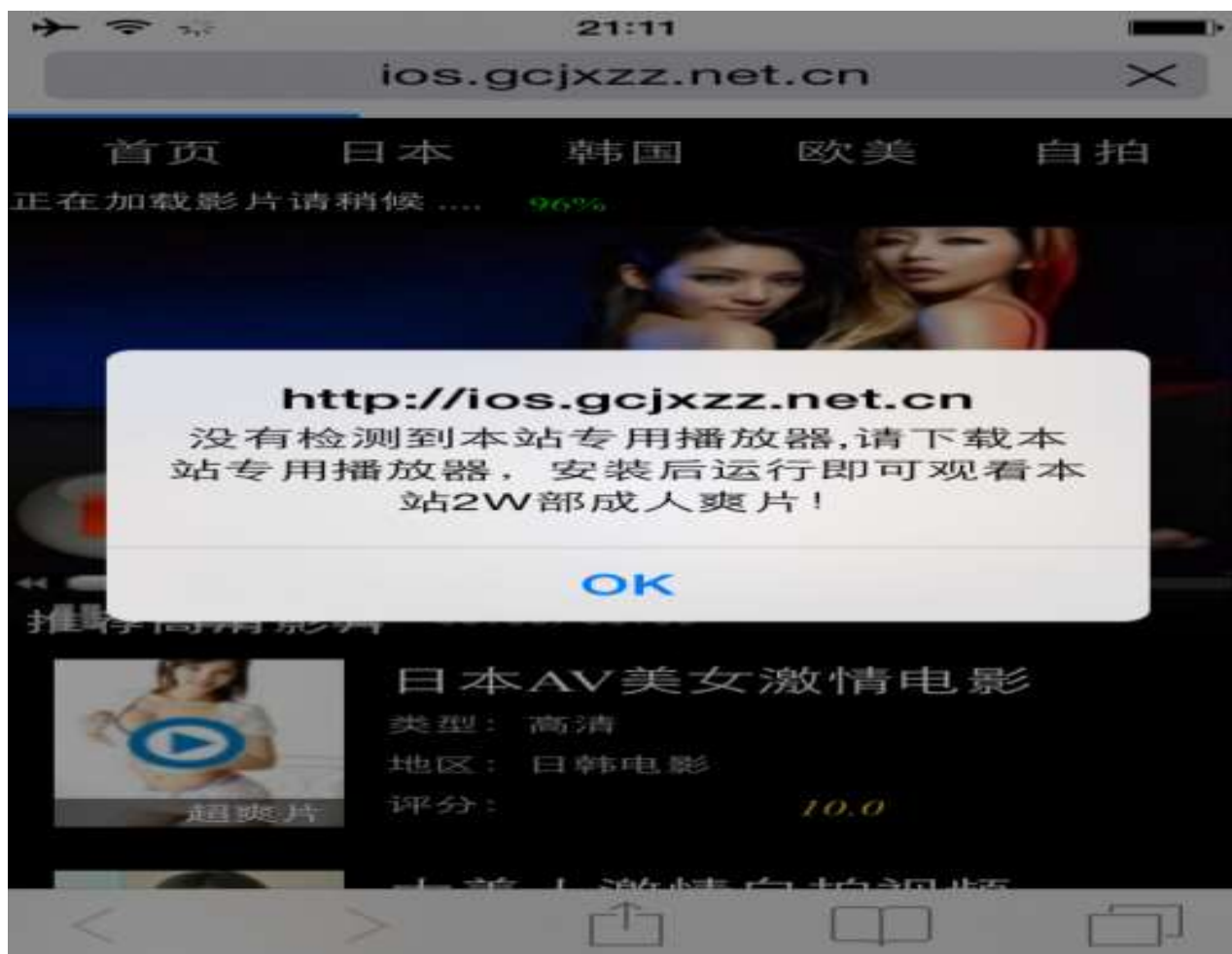
Utilizatorii de terminale mobile cu sistem de operare *iOS* au fost mereu atenționați asupra pericolelor de securitate la care se supun atunci când aleg varianta *jailbreak* pentru customizarea sistemului de operare și instalarea de aplicații neverificate, fără nici un cost. Ulterior, utilizatorul este capabil să modifice parametrii și setări ale sistemului care în mod normal nu pot fi accesate.

În cele mai multe cazuri unealta folosită pentru *jailbreak* va instala un nou magazin de aplicații numit *Cydia*, unde se regăsesc *tweak*-uri (aplicații terțe, neoficiale pentru care Apple nu le recomandă și pentru care nu oferă suport). Cu toate acestea, de multe ori se găsesc aplicații a căror variantă oficială presupune achiziționare contra unei sume de bani, ori aplicații care oferă servicii neacoperite de magazinul oficial *App Store*.

Ceea ce e important de știut de către utilizatori este faptul că optând pentru o astfel de soluție, aceștia pot pierde garanția în cazul în care dispozitivul se va defecta, dar operațiunea nu este ilegală. Până în 2015, toate variantele de malware ce atacau utilizatorii de sisteme de operare iOS au venit din surse neoficiale, din magazine nerecomandate, instalate prin *jailbreak*.

Cu toate acestea, în octombrie 2015 compania *Palo Alto Networks* a identificat o variantă de malware pentru *iOS* care afectează deopotrivă utilizatorii cu dispozitive cu sau fără *jailbreak*: *YiSpecter*. Momentan, campania malware a fost identificată exclusiv în Asia, afectând clienții Apple din China și Taiwan.

Propagarea malware-ului se produce prin metode neuzuale, ce presupune deturnarea traficului de la furnizorii de internet naționali, utilizarea unei variante de malware de tip worm SNS pentru Windows, dar și instalarea de aplicații offline. *YiSpecter* deține 4 componente diferite. Aceste componente se descarcă și se instalează pe rând, una cu ajutorul fiecăreia de la un server de comandă și control (C2).



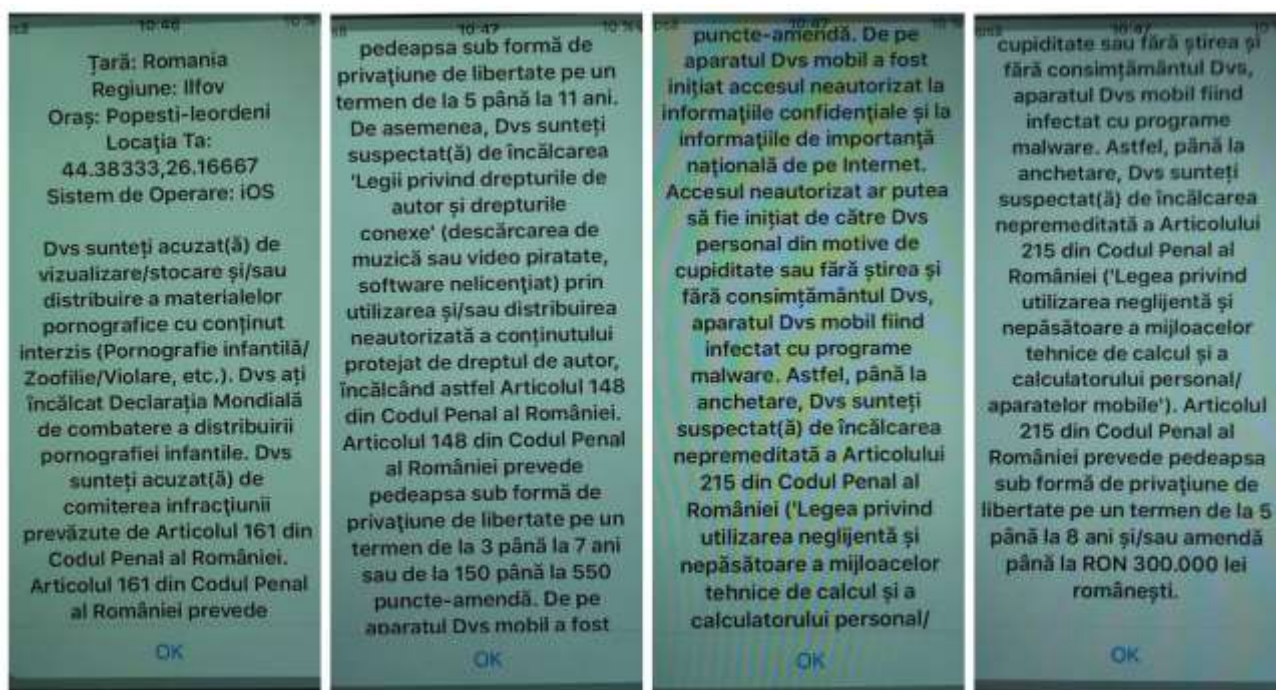


[<http://researchcenter.paloaltonetworks.com/2015/10/yispecter-first-ios-malware-attacks-non-jailbroken-ios-devices-by-abusing-private-apis/>]

Trei dintre aceste componente reușesc să păcălească sistemul astfel încât icoanele aplicațiilor malițioase abia instalate să nu devină vizibile pentru utilizator, pentru ca acesta să nu le poată înlătura. În același timp, *Yispecter* este capabil să înlătore aplicații, să afișeze reclame în interiorul aplicațiilor legitime, poate să înlocuiască motorul de căutare din browser-ul de internet Safari și să urce informații despre utilizator către servere remote.

În cazul utilizatorilor români ai serviciilor Apple, nu s-au întâlnit momentan campanii de malware pe *iOS* dedicate acestui spațiu, în care să fie utilizată exclusiv limba română.

Recent însă, CERT-RO a descoperit cazuri de utilizatori care sunt vizați de o campanie de tip Scam (înșelătorie) prin intermediul browser-ului Safari. Mai precis, la deschiderea Safari, utilizatorilor li se afișează un mesaj prin care sunt anunțați că li se aduc acuzații cu privire la faptul că au “vizualizat/stocat/distribuit materiale pornografice cu conținut interzis”, astfel că vor fi anchetați pentru aceste fapte și sunt pasibili de o “pedeapsă sub formă de privațiune de libertate pe un termen de la 5 până la 8 ani și/sau amendă până la 300.000 de RON”.



Aici aveți textul complet al înșelătoriei așa cum este afișat pe dispozitivele Apple:

*Dvs sunteți acuzat(ă) de vizualizare/stocare și/sau distribuire a materialelor pornografice cu conținut interzis (Pornografie infantilă/Zoofilie/Violare, etc.). Dvs ați încălcat Declarația Mondială de combatere a distribuirii pornografiei infantile. Dvs sunteți acuzat(ă) de comiterea infracțiunii prevăzute de Articolul 161 din Codul Penal al României.*

*Articolul 161 din Codul Penal al României prevede pedeapsa sub formă de privațiune de libertate pe un termen de la 5 până la 11 ani.*

*De asemenea, Dvs sunteți suspectat(ă) de încălcarea “Legii privind drepturile de autor și drepturile conexe” (descărcarea de muzică sau video piratate, software nelicențiat) prin utilizarea și/sau distribuirea neautorizată a conținutului protejat de dreptul de autor, încălcând astfel Articolul 148 din Codul Penal al României.*

*Articolul 148 din Codul Penal al României prevede pedeapsa sub formă de privațiune de libertate pe un termen de la **3** până la **7** ani sau de la **150** până la **550** puncte-amendă. De pe calculatorul Dvs a fost inițiat accesul neautorizat la informațiile confidențiale și la informațiile de importanță națională de pe Internet.*

*Accesul neautorizat ar putea să fie inițiat de către Dvs personal din motive de cupiditate sau fără știrea și fără consimțământul Dvs, calculatorul Dvs fiind infectat cu programe malware. Astfel, până la anchetare, Dvs sunteți suspectat(ă) de încălcarea nepremeditată a Articolului 215 din Codul Penal al României (“Legea privind utilizarea neglijentă și nepăsătoare a mijloacelor tehnice de calcul și a calculatorului personal/aparatelor mobile”). Articolul 215 din Codul Penal al României prevede pedeapsa sub formă de privațiune de libertate pe un termen de la **5** până la **8** ani și/sau amendă până la **RON 300.000** lei românești.*

La o primă analiză a textului afișat este evident că atacatorii l-au preluat de la o altă campanie ce încerca înșelarea utilizatorilor din România: virusul Poliția Română, adaptând-ul pentru utilizatorii de terminale mobile. După cum se poate observa, textul este scris într-o limbă română aproximativă, cu greșeli gramaticale și de ortografiere, cel mai probabil tradus dintr-o limbă străină cu ajutorul unor instrumente automate de traducere cum ar fi *Google Translate*.

În plus, mesajul conține informații cu privire la localizarea destinatarului telefonului, precum Țara/Regiune (județ)/Oraș și coordonate GPS. Aceste elemente au rolul de a acorda o impresie de autenticitate mesajului afișat. Utilizatorilor li se cere înaintarea unei sume de bani pentru rezolvarea problemei. Sub nici o formă **NU transmiteți suma cerută către atacatori!** După cum se poate observa, aceștia doar simulează o problemă serioasă cu privire la funcționalitatea telefonului. **Atât terminalul mobil utilizat, cât și informațiile de pe el sunt în continuare în deplină siguranță și nu au fost compromise!**

Acest proces se derulează exclusiv atunci când utilizați *Safari* web browser și funcționează ca o fereastră de tip pop-up. De fiecare dată când veți dori să utilizați Safari acesta va rula automat o căutare a paginii respective, care va funcționa ca pagină principală a browser-ului.

Cu alte cuvinte, funcționalitatea telefonului/dispozitivului nu este deloc afectată, ci doar navigarea pe internet prin intermediul Safari. Utilizatorii care s-au confruntat cu această problemă au vizitat în prealabil URL-uri cu conținut malițios, dar rezolvarea problemei este cât se poate de simplă. Deoarece la fiecare deschidere a *Safari* vă va apărea o fereastră pop-up cu acest mesaj, va fi nevoie doar de ștergerea datelor de navigare pentru ca pagina de pornire să nu mai afișeze automat acest mesaj.

## SURSE

<http://www.bitdefender.ro>

<https://cert.ro>

<http://www.kaspersky.ro>

<http://www.mcafee.com/us/mcafee-labs.aspx>

<http://researchcenter.paloaltonetworks.com>