LUNA EUROPEANĂ A SECURITĂȚII INFORMATICE

CERT.RO

RAPORT

Amenințări cibernetice la adresa utilizatorilor din România

Raport realizat de către:

Bitdefender

în cadrul campaniei de conștientizare a riscurilor de securitate cibernetică derulată în Romania sub egida ECSM de către CERT-RO.

BE AWARE, BE SECURE.
www.enisa.europa.eu/cybersecmonth

www.cert-ro.eu/ecsm.php

Pagină albă

CUPRINS

Pagină albă

1. Despre BITDEFENDER

Bitdefender este producătorul uneia dintre cele mai performante și eficiente game de soluții de securitate informatică atestate pe plan internațional. Bitdefender protejează datele digitale ale aprox. 500 milioane de utilizatori individuali și companii din întreaga lume.

2. Scopul prezentului raport

Scopul raportului este obţinerea unei viziuni de ansamblu asupra naturii şi dinamicii tipurilor de amenințări cibernetice ce au afectat utilizatorii din România, în perioada 01.01 – 30.06.2013.

Prezentul document se vrea a fi o completare a "Raportului cu privire la alertele de securitate cibernetică primite de CERT-RO în primele 6 luni ale anului 2013"[1], raport elaborat și publicat de CERT-RO.

3. Despre sursele de date

Statisticile oferite de Bitdefender sunt bazate pe telemetria trimisă de clienții companiei atunci când produsele acestora blochează un atac informatic pe sistemul clientului.

4. Evoluția amenințărilor de natură cibernetică din spațiului cibernetic național

4.1. Phishing

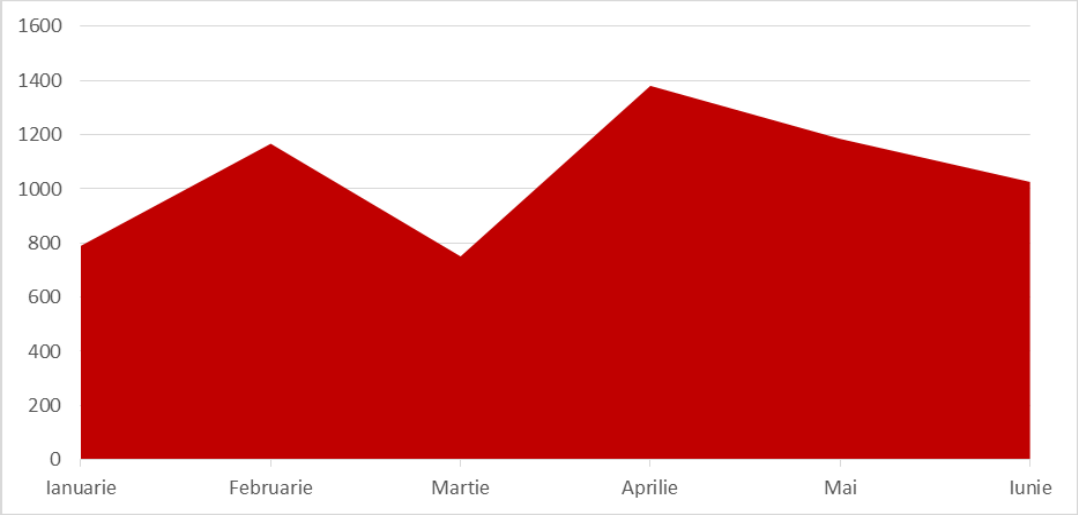

Fig. 1 – Evoluția paginilor de phishing găzduite în România (domeniu + IP)

[1] https://cert.ro/vezi/document/raport-alerte-primite-cert-ro-2013

Conform datelor Bitdefender în aprilie, numărul paginilor de phishing a atins un maxim absolut pe anul 2013, fiind înregistrate aproximativ 1400 de astfel de pagini pe sisteme compromise din România. În marea majoritate a cazurilor, paginile de phishing se află găzduite pe domenii care rulează soluții vulnerabile de gestionare a conținutului (CMS). În primele 6 luni ale anului Bitdefender a depistat aprox. 6400 de locații care găzduiesc pagini cu phishing, dintre care aproximativ 850 de pagini conțin text în română și sunt create pentru utilizatorii români.

Conform datelor CERT-RO[2], în aceeași perioadă a anului, 5.678 domenii ".ro" au fost compromise, numărul reprezentând mai puțin de 1% din totalul domeniilor existente; 51% dintre acestea au suferit atacuri de tip defacement, iar 43% au fost infectate cu diverse variante de malware. Aprox. 4% dintre domeniile ".ro" raportate au fost clasificate în categoria "phishing".

4.2. Peisajul amenințărilor cu malware în România

În prima jumătate a anului 2013, cele mai importante amenințări cu malware în România au fost troienii, urmați de variante ale unor amenințări cunoscute deja, dar refolosite de atacatori prin tehnici specifice (reîmpachetare).

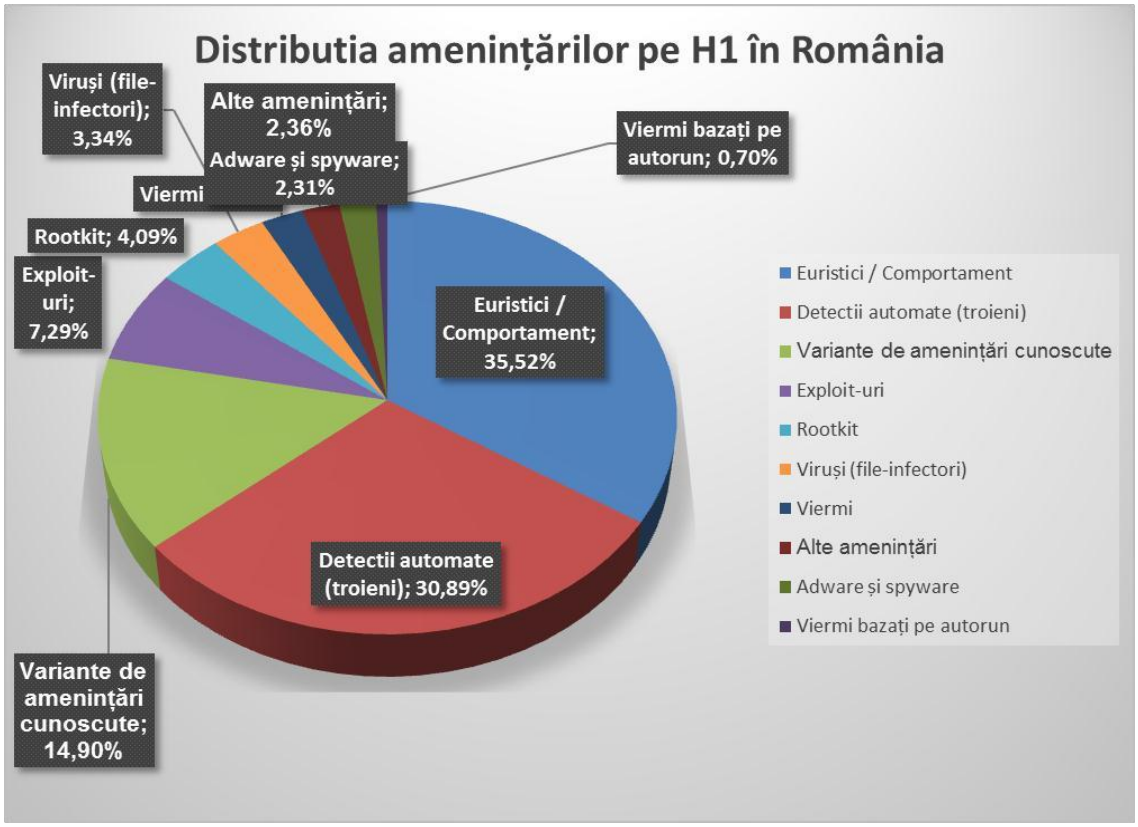

Fig. 2 – Distribuția amenințărilor informatice pe primele 6 luni ale anului

[2] https://cert.ro/vezi/document/raport-alerte-primite-cert-ro-2013

Exploiturile au cunoscut de asemenea o creștere semnificativă, în mod special în primul trimestru al anului, principalele aplicații vizate fiind Java (prin pluginul de web), Adobe Reader și Flash Player. Aceste vulnerabilități au fost folosite pe scară largă în România pentru livrarea virusului Poliția Română, un tip de aplicație ransomware care se folosește de elementele vizuale ale autorităților românești pentru a forța utilizatorii să plătească "o amendă" în valoare de până la 100 de euro.
Aceste exploituri sunt strâns legate de creșterea popularității kiturilor de exploatare precum BlackHole, Sakura, CrimePack sau Cool Exploit Kit, kituri ce permit hackerilor neexperimentați să exploateze utilizatori ce rulează versiuni vulnerabile ale aplicațiilor terțe menționate mai sus.
Un alt tip de malware care a cunoscut o creștere semnificativă în prima jumătate a anului este reprezentat de aplicațiile de tip Rootkit (malware care folosește sisteme avansate de protecție pentru a-și ascunde prezența în sistem față de utilizator, antivirus sau chiar de sistemul de operare). Cele mai prolifice familii de rootkiți în România sunt TDSS / Alureon și Sirefef / ZeroAccess.
În scădere masivă față de anii precedenți se află viermii ce se folosesc de funcția de AutoRun din Windows pentru a se propaga de pe medii detașabile de stocare pe sisteme neinfectate încă. Această involuție este strâns legată de faptul că noile sisteme de operare de la Microsoft au eliminat funcția de autorun pentru medile de stocare portabile, cu excepția celor optice.
Internetul a jucat un factor decisiv în propagarea infecțiilor din primul semestru, fiind vectorul preferat al atacatorilor. În contrast, doar 5,2% din mesajele e-mail primite de utilizatorii români sunt infectate cu malware sau conțin linkuri care duc către malware.

4.3. Clasificarea mesajelor de tip spam

Mesajele de tip spam, vehiculate în România, în prima jumătate a anului poate fi clasificată astfel:

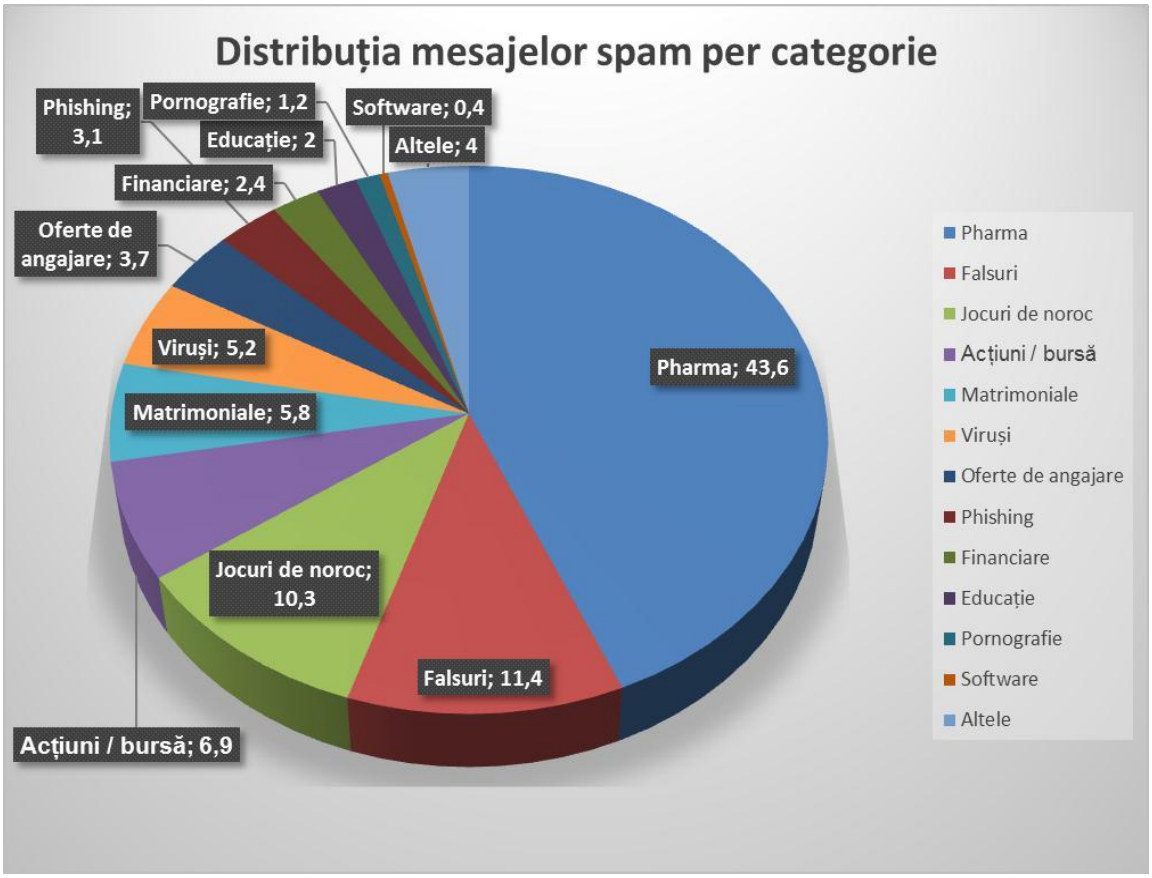

Fig. 3 – Distribuția mesajelor spam pe categorie

Ca de obicei, principalele TLD-uri de pe care se comit abuzuri sau se trimit spam sunt cele internaționale (.com, .net, .info etc), deoarece acestea sunt cele mai des folosite și înregistrate. Cu toate acestea, există un trend regional la nivel de TLD-uri folosite în activități ilegale. În 2011, principalele domenii folosite în infracționi erau .co.cc și co.kr, domenii second-level oferite gratuit. Anul acesta, proaspăt-introdusul TLD .pw a cunoscut cea mai mare creștere, de la 0 la 3.14% în mai puțin de trei luni.

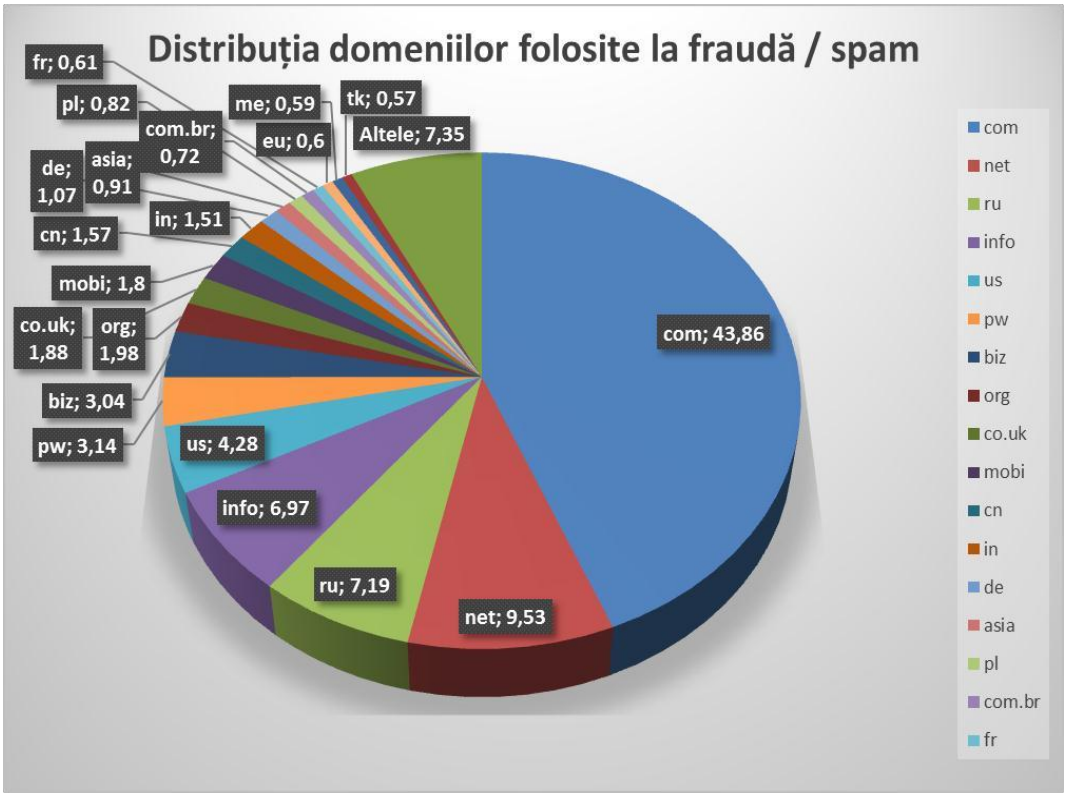

Fig. 4 – Distribuția domeniilor folosite la fraudă/spam.

4.4. Amenințări specifice dispozitivelor mobile din România

Din punct de vedere al securității dispozitivelor mobile, România ocupă locul trei în lume, ca număr de dispozitive infectate, după India și Vietnam. Majoritatea amenințărilor ce vizează platforma Android, înregistrate în România în prima jumătate a anului 2013, e formată din troieni cu comportamente diferite (încadrați în categoria "Altele"), precum și aplicații care încearcă să abuzeze de funcționalitățile SMS / apel pentru a genera costuri suplimentare.

Exploiturile împotriva platformei Android reprezintă 2,98% din totalul incidentelor înregistrate în prima jumătate a anului 2013, fiind folosite de diverse familii de malware pentru a prelua controlul asupra dispozitivului ca super-utilizator.

Instrumentele de hacking însumează 1,85% din evenimentele înregistrate în 2013, cele mai răspândite astfel de aplicații fiind Android.Hacktool.Pentr.B, Android.Hacktool.WifiKill.A și Android.Hacktool.Faceniff.A.

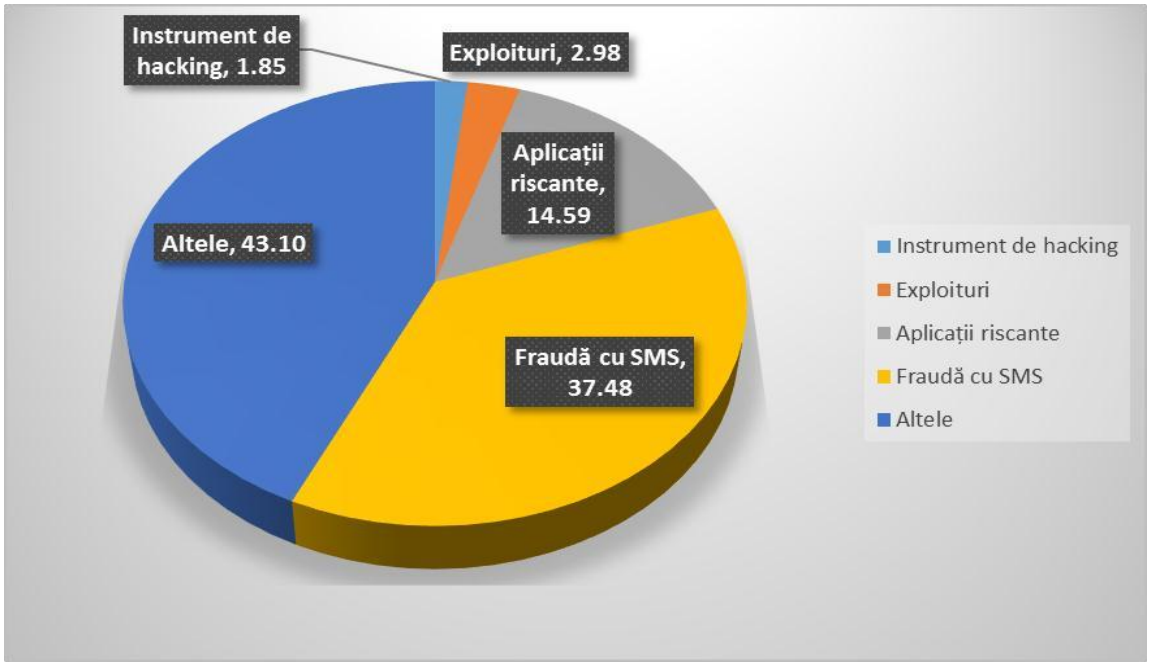

Figura 5: Distribuția amenințărilor de Android după tipul atacului

Cei mai răspândiți viruși în România, în perioada monitorizată, au fost Android.Trojan.FakeAV.G (un fals antivirus care îndeamnă victima să cumpere aplicația prin afișarea de false alarme de securitate), Android.Riskware.SMSReg.AA (o aplicație care colectează printre altele informațiile despre telefon, precum și poziția acestuia determinată prin GPS) și Android.Trojan.FakeAV.B (un fals antivirus care colectează informații despre telefon și cardul de credit al utilizatorului).

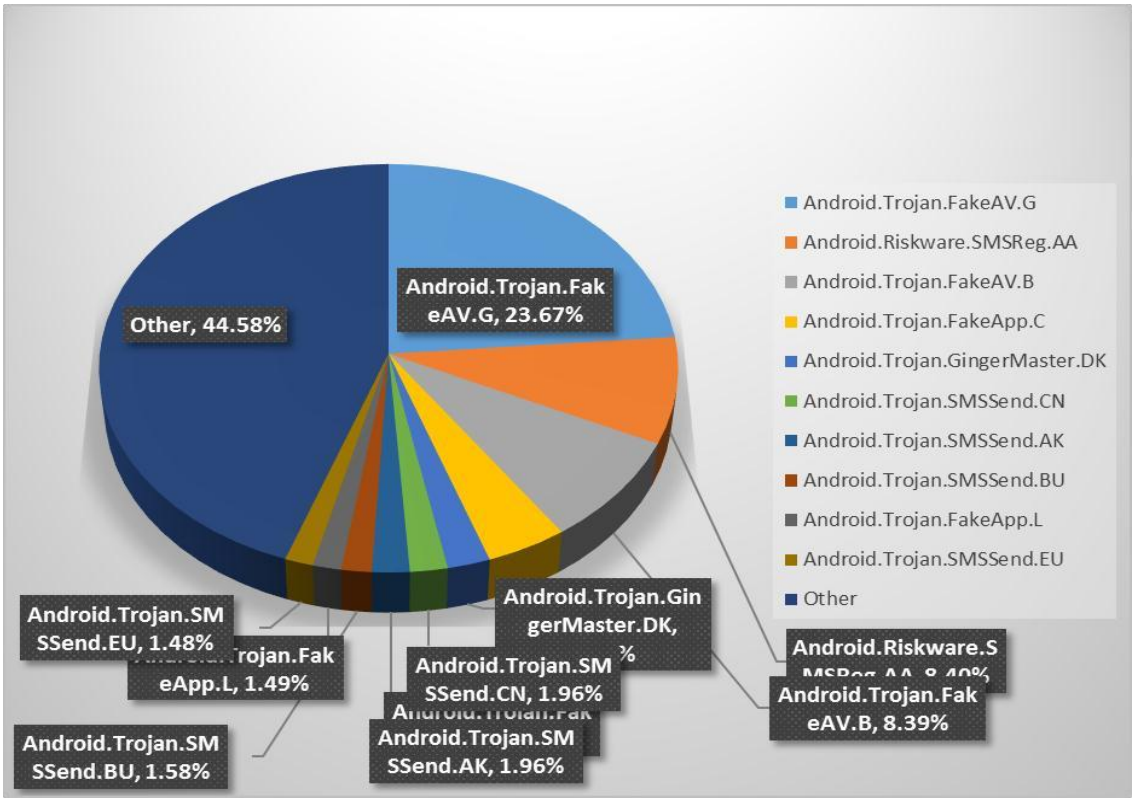

Figura 6: Cei mai răspândiți viruși pentru platforma Android