LUNA EUROPEANĂ A SECURITĂȚII INFORMATICE

CERT.RO

GHID

Amenințări generice la adresa securității cibernetice

Ghid realizat de către:

CERT.RO

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

https://cert.ro/tag/ecsm

-pagină albă-

Cuprins

1. Introducere

Amenințările cibernetice ajung să fie un impediment din ce în ce mai prezent în viețile noastre. Mai mult, unii specialiști vorbesc deja de un ''război cibernetic'', cel mai elocvent exemplu fiind reprezentat de Statele Unite ale Americii, care deja tratează conflictul cibernetic ca unul de tip terorist.[1]

Atunci când sisteme de comunicații, infrastructuri critice, instituții financiar-bancare sau organisme guvernamentale devin ținte ale atacatorilor, trebuie să tragem un semnal de alarmă în ceea ce privește căile prin ne putem apăra.

Amenințările cibernetice din mediul online sunt în continuă creștere. Spațiul cibernetic va fi mereu animat de cursa continuă dintre atacatori și cei care sunt afectați de aceste atacuri. Din nefericire, așa cum precizează ENISA, în acest moment infractorii cibernetici sunt cu un pas înainte.[1]

Pentru a ține pasul cu aceștia este esențial ca utilizatorul să fie informat corespunzător cu privire la metodele de atac cel mai des folosite. De aceea, ghidul de față se adresează utilizatorului obișnuit și conține informații cu privire la principalele amenințări din spațiul cibernetic, inclusiv un top al amenințărilor și o definire succintă termenilor cu care operăm. Pe langă acestea, dacă urmăriți tabelul de mai jos, puteți identifica evoluția amenințărilor informatice din 2012 și 2013, precum și principalele schimbări față de anul trecut.

Top Amenințări	Trend 2012	Trend 2013	
1. Drive-by exploits			
2. Viermi/Troieni			
3. Injecţie de Cod			
4. Kit-uri de Exploatare			
5. Botnet			

[1] *ENISA Threat Landscape 2012*, p.2

Denial of Service	
Phishing	
15.Manipularea motoarelor de căutare	
16. Certificate Digitale False	

Sursa: ENISA Threat Landscape Mid 2013

Legendă: Trend ascendent Trend descendent Trend stabil Schimbări interesante

2. Principalele amenințări cibernetice

8.Compromiterea informațiilor confidențiale	
9.Rogueware/Scareware	
10. Spam	
11. Atacuri direcţionate	
12. Furt/Pierderi/Distrugere Fizică	
13. Furt de identitate	
14. Scurgere de informaţii	

2.1 Drive-by exploits

Amenințările de tip Drive-by pot exploata în mod automat vulnerabilități existente în software-ul instalat pe un PC, fără a interacționa cu utilizatorul de drept. Atunci când un utilizator vizitează un site ce conține exploit-uri drive-by, se pot exploata vulnerabilități în browser, în plugin-urile acestuia sau în sistemul de operare pentru a instala malware pe PC fără știrea utilizatorului.

Dezinfectarea în acest caz este extrem de importantă tocmai prin faptul că infecția poate fi inițiată printr-o simplă navigare pe internet, care poate duce la vizitarea unui website ce conține un astfel de drive-by.

Mai există posibilitatea ca atacatorii să conceapă un site special (fake website sau chiar phishing) pentru a infecta pe cei ce îl accesează. Astfel, pentru a determina utilizatorii obișnuiți să îl viziteze, se apelează la o strategie bazată pe e-mail-uri de tip spam (trimiterea de mesaje nesolicitate de către destinatar) ce conțin link-uri către astfel de site-uri ilegale.

Distribuția de malware prin exploit-uri de tip drive-by se axează aproape în totalitate pe compromiterea website-urilor legitime[2]. În fiecare zi, atacatorii manipulează mii de site-uri web din întreaga lume și apoi injectează un cod malițios în conţinutul acestora. Aceste siteuri de regulă sunt compromise prin furtul datelor de autentificare. Analiștii care investighează serverele atacate adesea găsesc liste de credențiale pentru servere FTP extrase de la utilizatori. [3]

Exploit-urile de tip drive-by și-au extins aria de acțiune în 2012 și la terminalele mobile. Conform unor rapoarte date publicității de către companiile de securitate McAffe și FSecure începînd cu luna mai 2012 apar primele rapoarte cu privire la folosirea acestui instrument de către atacatori pentru exploatarea vulnerabilităților sistemului de operare Android.

2.2 Viermi/Troieni

- **Viermi:** programe care se pot auto-replica. Acestea folosesc rețeaua de calculatoare pentru a-și trimite propriile copii în alte noduri (calculatoare din rețea), reușind să facă acest lucru fără intervenția vreunui utilizator.

  Spre deosebire de un virus informatic, un vierme informatic nu are nevoie să fie atașat la un program existent. Viermii provoacă daune rețelei, chiar și prin simplul fapt că ocupă bandă, în timp ce virușii corup sau modifică aproape întotdeauna fișiere de pe computerul țintă.

[2] ENISA Threat Landscape 2012, p. 13

[3] Federal Office for Information Security, *The IT Security situation in Germany 2011*, p.8

- **Troieni:** aceste programe se prezintă sub forma unor programe legitime, care, în realitate, sunt create cu scopul de a fura date confidențiale, sau de a permite unor utilizatori sau programe neautorizate accesul la sistemul infectat. Conform *ENISA Threat Landscape 2012* [4], troienii constituie marea majoritate a infecțiilor (80%). Acest lucru arată că epidemia worm a devenit istorie și a fost substituită de către o invazie a troienilor.[5]

În ceea ce privește aria terminalelor mobile, un raport al F-Secure din 2012 arăta că 84% din amenințări sunt reprezentate de către Troieni, principala motivare pentru atacatori fiind una exclusiv bazată pe profit financiar.[6] Totodată, utilizatorul trebuie să fie atent și la modul cum operează în cadrul rețelelor de socializare. Acestea pot constitui totodată modalități prin care creatorii de malware să ajungă la ținta dorită.

2.3 Injecție de cod

Acest tip de amenințare include tehnici de atac binecunoscute împotriva aplicațiilor web, cum ar fi SQL Injection (SQLi), cross-site scripting (XSS), cross-site request forgery (CSRF), Remote File Inclusion (RFI) etc.

Atacatorii care generează un astfel de atac încearcă să extragă date, să fure credențiale, să preia controlul serverului web țintit sau să își promoveze activitățile malițioase prin intermediul exploatării vulnerabilităților de aplicații web.

În ultimii ani, cel mai frecvent vector de atac împotriva aplicațiilor web este SQL Injection. Mai mult de cât atât, atacurile de acest tip sunt populare în rândul grupurilor hacktivist (ex: Anonymus), grupurilor de hackeri (ex: LulzSec) și în rândurile infractorilor cibernetici (ex: LizaMoon25).

2.4 Kit-uri de exploatare

[4] *ENISA Threat Landscape 2012*,p.46

[5] Bitdefender - H1 2012 E-Threat Landscape Report, p.95

[6] F-Secure - Mobile Threat Report Q1 2012, p.103

Pe scurt, această categorie se referă la acele software-uri automatizate care ajută atacatorii, mai puțin experimentați, în compromiterea sistemelor prin exploatarea vulnerabilităților de tip client-side, în special a celor din browsere web sau aplicații ce pot fi accesate de site-uri web (ex: Adobe Reader, Flash, JRE etc.). Practic, aceste pachete "ready to use'' (gata de utilizare) automatizează procesul criminalității informatice.

De regulă acestea se bazează pe atacuri de tip drive-by download, în urma căruia codul malițios este injectat în site-urile web compromise. Aceste atacuri pot exploata vulnerabilități din broswer sau din plugin-urile acestuia. Mai mult decât atât, acest exploit kit poate utiliza o multitudine de canale de comunicare cu scopul distribuirii de malware către alți utilizatori web.

O caracteristică importantă a acestui exploit kit o reprezintă ușurința cu care acesta poate fi utilizat (de obicei printr-o interfață web) chiar și de către persoane fără cunoștințe tehnice.

2.5 Botnet

Un botnet reprezintă un set de computere care se află sub controlul unui atacator. Aceste sisteme compromise poartă denumirea de 'bots' sau 'zombies'. Aceasta este o rețea de sisteme informatice infectate care sunt controlate de alte persoane/organizații decât deținătorii acestora.[9]

O rețea de tip botnet poate fi utilizată cu scopuri multiple: atacuri de tip „Distributed Denial of Service - DDoS", spamming, furt de identitate, distribuire de malware, infectarea sistemelor informatice etc.

În prezent botnet-ul poate fi folosit ca marfă. Părțile interesate pot chiar închiria o rețea de tip botnet pentru a-și atinge scopurile malițioase și inclusiv pentru a obține avantaje materiale. Mai mult, acestea pot acționa pe mai multe sisteme de operare. Spre exemplu, în 2012 botnet-ul ''Flashback'' a reușit să infecteze aproximativ 600.000 de computere Apple.

Conform raportului CERT-RO[7], peste 80% dintre alertele primite se referă la activităţi suspecte/maliţioase generate de reţelele de tip botnet.

2.6 Denial of Service

Un atac de tip Denial of Service este o încercare de a afecta disponibilitatea unor sisteme/servicii informatice sau comunicații electronice. Sistemul țintă este atacat prin transmiterea unui număr foarte mare de solicitări nelegitime, ce consumă resursele hardware sau software ale acestuia, făcându-l indisponibil pentru utilizatorii legitimi. [11] Conform raportului ENISA Threat Landscape din 2012, principalele motivări ale atacurilor de tip DDoS sunt hacktivismul, vandalismul și înşelăciunea.[8]

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

[8] *ENISA Threat Landscape 2012*, p. 17

2.7 Phishing

Phishing-ul este o formă de înșelăciune în mediul online care constă în folosirea unor tehnici de manipulare a identității unor persoane/organizații pentru obținerea unor avantaje materiale sau informații confidențiale.

Atacatorii folosesc diverse tehnici de social engineering pentru a-și determina victimele să-și dezvăluie date de autentificare. Țintele cele mai întâlnite sunt site-urile instituțiilor financiare, precum băncile. Alte ținte sunt reprezentate de serviciile de plată online, rețelele de socializare, furnizorii de servicii de internet, organizațiile non-profit, servicii de coletărie sau site-urile unor sectoare guvernamentale.[9]

2.8 Compromiterea informațiilor confidențiale

Compromiterea informațiilor confidențiale se referă la încălcări ale securității datelor care au apărut prin dezvăluirea (fie intenționată, fie neintenționată) de informații confidențiale de către agenți interni sau externi.

Această amenințate are ca țintă informații confidențiale din diferite sectoare, cum ar fi sectorul public de sănătate, organizații guvernamentale, întreprinderi mici și mijlocii etc. Scurgerea de informații se realizează de regulă prin hacking, distribuire de malware, atacuri de tip social engineering, atacuri fizice sau prin abuz de privilegii.[10]

2.9 Rogueware/scareware

Tip de amenințare ce îmbracă formă unui software fals utilizat de criminalii cibernetici pentru a atrage utilizatorii către scopurile lor malițioase.

[9] *ENISA Threat Landscape 2012*, p.17

[10] *ENISA Threat Landscape 2012*, p.18

Un caz particular de rogueware/scareware este un software fals de securitate care odată instalat în sistem furnizează alerte false de securitate și invită utilizatorul să cumpere o unealtă specială (tool) de dezinfecție.

Acest tip de amenințare se propagă prin diverse metode ca de exemplu tehnici de social engineering, troieni, exploatarea de vulnerabilități (în special java).

2.10 Spam

Mesaje electronice nesolicitate, de cele mai multe ori cu caracter comercial, care fac publicitate pentru produse și servicii, fiind folosite de către industria e-marketingului și de către proprietarii de site-uri cu conținut indecent.

De obicei mesajele spam sunt trimise de către calculatoare infectate cu troieni, care fac parte dintr-un botnet (o rețea de calculatoare compromise și utilizate pentru trimiterea de spam, sau atacuri asupra unor site-uri de internet, fără știrea posesorilor calculatoarelor respective).

Mesajele spam, deși nu reprezintă un program malițios în sine, pot include atașamente conținând astfel de programe, și trimit utilizatorii către pagini de internet periculoase.

2.11 Atacuri direcționate

Tip de amenințare ce vizează o anumită persoană sau organizație. Are ca scop fie colectarea de date cu caracter personal/confidențial sau compromiterea sistemelor informatice țintă.

Acest tip de atac are în general o fază prin care atacatorul se informează prin diverse tehnici (ex. inginerie sociala) asupra sistemului informatic vizat și apoi declanşează atacul. De multe ori acțiunile lui par legitime deoarece par a fi venite din partea unei persoane de încredere.

Conform raportului CERT-RO[11] amenințările de tip APT, specifice campaniilor de spionaj cibernetic, au devenit o realitate și în România, în România fiind deja detectate o serie de astfel de atacuri.

2.12 Furt/Pierderi/Distrugere fizică

Furtul fizic, pierderea sau distrugerea efectivă pot fi considerate o amenințare la adresa securității cibernetice. Datorită mobilității crescute pe care o oferă laptopurile, telefoanele inteligente sau tabletele, acest tip de amenințare este pe cale să devină una majoră. În acest sens backup-ul consistent al datelor și criptarea conținutului pot fi o soluție de limitare a pierderilor efective de date sau de divulgare către persoane străine a datelor confidențiale.

2.13 Furt de identitate

Furtul de identitate este o amenințare reală într-un mediu ce devine pe zi ce trece cu preponderența online. Credențialele de acces sau datele cu caracter personal sunt astăzi ținta atacatorilor. Odată intrat în posesia acestora, atacatorul poate efectua tranzacții frauduloase (în special financiare) sau obține date cu caracter confidențial.

2.14 Scurgere de informații

Scurgerea de informații se referă la dezvăluirea în mod voit sau nu de informații către o persoană neautorizată. Odată ajunse în mâna unei persoane neautorizate aceste informații pot fi folosite fie pentru a porni un atac (targeted attacks), fie pentru a avea acces la surse suplimentare de informații.

Se cuvine a fi menționată aici și scurgerea de informații în mod voit prin instalarea de aplicații pe telefoanele mobile fără ca utilizatorul să se informeze suficient asupra datelor

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

la care aplicația are acces. Astfel informaţii cum ar fi geo-localizarea şi contactele din agendă pot ajunge cu uşurinţă în mâinile unor atacatori și folosite în scopuri frauduloase.

2.15 Manipularea motoarelor de căutare (SEP)

Acest tip de atac manipulează motoarele de căutare pentru a afișa rezultate de căutare care conțin referinţe către site-uri malițioase.

Există o multitudine de metode pentru a efectua SEP, unul din ele fiind preluarea controlului unor site-uri populare și includerea de link-uri sponsorizate către site-urile malițioase.

O altă metodă este SEP via Cross-Site Scripting, în acest caz un motor de căutare este forțat să returneze referințe către site-uri infestate cu Cross Site Scripting (XSS).

Astfel o pagină web infestată redirectează uşerii către site-uri malițioase iar în cazul în care victimele accesează site-urile respective îşi infestează computerele cu malware. De menționat că în acest caz atacatorul nu trebuie să spargă sau să preia controlul unui server aflat în schemă.

2.16 Certificate digitale false

Certificatele digitale false sunt folosite de către atacatori pentru semnarea digitală a resurselor (site-uri web, aplicații, coduri sursă etc.) folosite în diverse atacuri cibernetice, cu scopul de a trece nedetectabile de utilizatorul final. Acestea sunt des folosite pentru semnarea aplicațiilor web malițioase de tip e-banking sau e-commerce, ce folosesc protocolul HTTPS.

Un astfel de certificat poate fi creat sau furat prin exploatarea unor vulnerabilități ale asistemelor de tip PKI (Public Key Infrastructure) ale autorităților de certificare, care emit certificate digitale pentru site-uri web securizate.

Certificatele digitale sunt un mijloc de definire a încrederii în internet. Atacatorii pun în circulaţie certificate false (rogue certificates) care rup lanțul de încredere, oferindu-le astfel capacitatea de a se angaja în atacuri nedetectabile de utilizatorii finali.

Un astfel de certificat este văzut ca trusted de browsere deoarece apare ca fiind semnat de o autoritate de certificare root pe care browserele o consideră de încredere în mod implicit.

Acest tip amenințare este folosit și pentru obținerea de date confidențiale prin spargerea tunelurilor SSL folosind tehnici de tip ''man in the middle''.

Mai mult decât atât, certificatele rogue pot fi folosite pentru a semna malware, astfel încât malware-ul devine legitim și se sustrage mecanismelor de detectare.

Ca şi măsura de prevenire a atacurilor, autoritățile de certificare trebuie să pună în aplicare, să revizuiască şi să adapteze permanent politicile de securitate conform celor mai bune practici în domeniu.

Diverse distribuții de malware, precum cele folosite de Stuxnet, Duqu sau Flame, se bazează pe certificate digitale false furate de la diverse autorități de certificare.

3. Schimbări interesante față de anul 2012

Drive-by-exploits: Se constată o tendință de migrare a atacurilor de la Botnets spre URLuri infestate, acestea devenind calea preferată de distribuție a malware-ului în ultima perioadă, fiind raportată o creștere a ratei de URL-uri infestate față de 2012. Atacurile bazate pe browser sunt cele mai raportate în ultima perioadă iar exploatarea vulnerabilităților din platforma java este cea mai utilizată cale de materializare a acestor tipuri de amenințări.

Injecțe de cod: un aspect important în ceea ce privește acest tip de amenințare sunt atacurile îndreptate împotriva platformelor populare de tip Content Management System

(CMS). Având în vedere utilizarea pe scară largă a platformelor CMS, mediul oferit de acestea au atras atenția criminalilor cibernetici. Pe parcursul anului 2013 se constată ca principal vector de atac folosirea mediilor cloud ale furnizoriilor de servicii pentru acest tip de amenințări.

Botnets: deși se constată o orientare a preferinței atacatorilor către URL-uri infestate pentru distribuția de malware, se constată o evoluție interesantă în ceea ce privește acest tip de amenințare. Deși folosirea rețelelor P2P ca mediu pentru răspândirea vectorilor de infecţie de tip botnet nu reprezintă o noutate, totuşi se constată accentuarea acestui fenomen.

Un exemplu concret în acest sens îl reprezintă utilizarea infrastructurii Bitcoins. În luna aprilie a acestui an, compania de securitate Fortinet anunța că în perioada 1 ianuarie-31 martie 2013, botnetul Zero Access (reţea botnet de exploatare a operaţiunilor cu moneda virtuală Bitcoin) a reprezentat principala amenințare înregistrată de deviceurile FortiGate la nivel mondial.[12]

Rețele P2P oferă o infrastructură larg distribuită geografic pentru reţelele botnet, fiind dificil astfel de a localiza și neutraliza acest tip de amenințare. Totodată se constată crearea de infrastructuri de tip botnet prin exploatarea vulnerabilităților din platformele /dispozitivele larg utilizate (telefoane mobile, browsere etc).

Denial of Service : conform Spamhaus atacurile de tip DNS reflection attack au câștigat în popularitate în 2013.

Deși DNS reflection attack este o tehnică relativ veche, aceasta a revenit în actualitate. Atacatorii par să fi adoptat această tehnică de reflexie DNS pentru a lansa atacuri amplificate, astfel lățimea de bandă pentru aceste tipuri de atacuri practic s-a dublat de la începutul acestui an, atingând chiar un vârf de 300Gbs (putem spune ca e cazul spamhaus).

[12] http://www.fortinet.com/press_releases/

Rogueware / scareware. În 2013, a existat o creștere a raportărilor de rogueware / scareware. Rapoartele analizate furnizează dovezi clare că există o creștere în ceea ce privește ransomware.

Unul dintre motivele pentru creșterea de ransomware și de programe antivirus false sunt platformele mobile cum ar fi Android. Specialiştii în securitate consideră că era o problemă de timp până ce acest tip de atac va migra inclusiv pe terminalele mobile[13], în special pe platforma mobilă a Google, care a devenit în ultimul timp una din ţintele preferate ale atacatorilor din pricina vulnerabilităţilor de securitate[14].

Este de remarcat faptul că disponibilitatea de servicii de plată anonime pentru a canaliza profituri ilicite obținute prin acest tip de amenintare este un factor cheie pentru acest tip de fraudă.

Atacuri direcționate. În prima jumătate a anului 2013 , acest tip de atac și-a demonstrat eficiența în realizarea propriilor obiective. În special , atacurile de spionaj cibernetic au ajuns la o dimensiune care a depășit cu mult așteptările. Și în acest caz se constată că dispozitivele mobile au oferit un mediu propice pentru proliferarea acestor tipuri de amenințări.

Este de remarcat faptul că aplicațiile mobile de tip spyware ar putea deveni instrumente deosebit de puternice pentru astfel de atacuri în mediile în care angajații pot folosi deviceurile proprii pentru accesarea informațiilor din interiorul companiei.

Furtul de identitate. Această amenințare a dus la unele dintre cele mai de succes atacuri. Aceste tipuri de atacuri au avut la bază troieni financiari (ex. Zeus, SpyEye, Citadel) implementați pentru platformele de telefonie mobilă. O sursă importantă pentru aplicarea acestei amenințări rămâne conţinutul media social.

De asemenea se constată o creștere a extensiilor malițioase pentru browsere care au scopul de a fura date prin intermediul conturilor de rețelele sociale.

[13] http://www.infoworld.com/t/mobile-security/ransomware-android-it-was-only-matter-of-time-221285

[14] http://www.infoworld.com/t/security/android-malware-and-cloud-abuse-among-top-threats-2013-209188

Manipularea motoarelor de căutare. În prima jumătate a anului 2013 acest tip de amenințare a fost foarte rar raportată. Una din cauze fiind o apărare mai bună împotriva acestei amenințări a principalului motor de căutare de la Google. Se remarcă și în cazul acestui tip de amenințare o migrare către platformele de telefonie mobilă, fiind raportate tot mai multe aplicații malware care proliferează astfel de atacuri.

4. Concluzii

Analizând comparativ evoluția incidentelor de securitate cibernetică din 2012 și ulterior din prima jumătate a anului 2013, putem sesiza evoluții interesante în ceea ce privește peisajul amenințărilor.

- Infractorii cibernetici ajung să folosească metode din ce în ce mai avansate pentru a implementa vectori de atac care sunt nedetectabili și dificil de neutralizat. Un rol important în acest caz îl joacă tehnologiile de anonimizare și utilizarea tehnologiilor distribuite pentru structuri mai rezistente, cum ar fi P2P (Peer to peer).

- Este din ce în ce mai clar că tehnologia mobilă este și va deveni din ce în ce mai exploatată de către infractorii cibernetici. Amenințări deja cunoscute și rulate în spațiul tradițional IT vor prevala și pe terminalele mobile. Proliferarea dispozitivelor mobile va conduce la o amplificare a abuzurilor generate prin intermediul social media.

- Activitatea infracțională ce se desfășoară în mediul online are în acest moment noi perspective: consumerizarea malware-ului, instrumente și servicii de cyberhacking, apariția valutei digitale și servicii de plată anonime.

- Așa cum raporta ENISA în 2012[15], atacurile cibernetice au ajuns pe locul 6 într-un clasament al celor mai probabile cauze ale întreruperilor survenite în infrastructurile

[15] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annualreports/annualincident-reports-2012/at_download/fullReport

de telecomunicații. Ca număr de utilizatori afectați în acest sector, impactul este unul considerabil.

- Luând în considerare incidentele ce au survenit de la începutul acestui an și totodată evoluția amenințărilor de tip „denial of service", se constată în 2013 o creștere a amenințărilor care au ca țintă infrastructura.

Bibliografie

Surse principale folosite în realizarea prezentului ghid:

1. ENISA Threat Landscape 2012
2. ENISA Threat Landscape 2013

Alte surse:

1. Raport cu privire la alertele de securitate cybernetică primite de CERT-RO în primele 6 luni ale anului 2013
2. Bitdefender - H1 2012 E-Threat Landscape Report
3. F-Secure - Mobile Threat Report Q1 2012
4. Federal Office for Information Security, *The IT Security situation in Germany 2011*
5. SOPHOS Security Threat Report 2012
6. www.enisa.europa.eu
7. www.fortinet.com
8. www.infoworld.com
9. www.cert.ro