CUPRINS

Sumar executiv

Asociația Națională pentru Securitatea Sistemelor Informatice (ANSSI) a fost înființată în 2012 ca persoană juridică română, fiind o organizație de drept privat, nonprofit, fără scop patrimonial, neguvernamentală, profesională, independentă. Un rol important al ANSSI este de a promova bune practici în domeniul securității informațiilor și a sesiza factorilor cu competențe administrative dezechilibrele de pe piața IT, acționând pentru instituirea unei culturi etice și de securitate pe această piață prin coagularea unor forme de parteneriat public privat care să conducă la eficiență și operaționalitatea sistemelor IT implementate în România. În egală măsură, ANSSI se implică activ în domenii conexe, cum ar fi comunicațiile electronice, soluțiile și sistemele de e-guvernare și e-administrație, accesarea instrumentelor structurale sau standardele ocupaționale.

Prin prezentul document, ANSSI își propune să sintetizeze tendințele de evoluție ale riscurilor și amenințărilor de securitate cibernetică, prin raportarea spațiului virtual autohton la tendințele înregistrate la nivel global.

Scopul acestei evaluări îl reprezintă evidențierea unor indicatori relevanți în raport cu care membrii și partenerii noștri, atât din mediul privat, cât și din mediul public, să poată să-și orienteze strategiile și politicile proprii necesar a fi adaptate permanent pentru asigurarea unui nivel adecvat de securitate cibernetică. Totodată, prin evaluarea tendințelor înregistrate de categoriile de riscuri și amenințări evidențiate în document, pot fi identificate mai facil tipurile de măsuri concrete necesar a fi adoptate în plan tehnologic, precum și tipurile de competențe necesare pentru personalul specializat în domeniul securității cibernetice.

Materialul se dorește un document pragmatic, realizat pe baza datelor și contribuțiilor analitice furnizate de o parte a membrilor și partenerilor ANSSI, identificați ca atare în document.

Se pornește de la evoluțiile identificate la nivel global, se analizează prin comparație situația locală, inclusiv cadrul normativ, prezentându-se în final un set de propuneri și recomandări.

În prima secțiune se observă, la nivel macro, diversificarea entităților ostile, apariția și dezvoltarea (în tandem) a Cybercrime-as-a-Service și a finanțelor subterane, precum și impactul paradigmei IoT. Sunt prezentate principalele tendințe în domeniul amenințărilor cibernetice, detaliindu-se aspectele ce țin de kiturile de exploatare, Java și spam. De asemenea, se prezintă o analiză a percepției privind riscurile de securitate și a costului lipsei de securitate la nivelul utilizatorilor și al companiilor.

Prin raportare la tendințele globale, secțiunea următoare analizează peisajul local. Observăm astfel că:

- Cele mai notabile amenințări informatice la adresa utilizatorilor de Internet din România sunt reprezentate de virușii de tip crypto-ransomware și troienii bancari Tinba si Dridex
- Win32.Worm.Downadup ocupă primul loc în lista amenințărior informatice din 2015
- În zona de mobile, pe primul loc se află troienii de fraudă cu mesaje scurte la numere cu suprataxă (50% din cazuri), urmați la distanță de instrumentele de spionaj tip AndroRAT
- Spam-ul a rămas la un nivel relativ constant, pe primul loc (50% din cazuri) regăsindu-se mesajele care plasează produse farmaceutice și suplimentele alimentare, urmate de site-urile matrimoniale (10%) și produsele contrafăcute (7%)

- În ceea ce privește alertele CERT.ro, în prima jumătate a anului 2015 numărul acestora a ajuns la aproape 30 de milioane cu 1.7 milioane IP-uri unice

În ceea ce privește cadrul legislativ, se observă o evoluție convergentă cu tendințele europene, dar și o abordare (atât europeană cât și locală) ușor conservatoare, în pași mici, care permite însă evitarea erorilor și asimilarea lecțiilor anterioare.

În finalul materialului se prezintă o serie de propuneri și recomandări din care punctăm:

- Întregirea cadrului legal în domeniul securității cibernetice
- Dezvoltarea de CERT-uri sectoriale
- Definirea unui set de condiții tehnice minime de securitate pentru sistemele informatice
- Înființarea unui Cluster orientat pe securitate cibernetică, care să includă un Centru național de transfer tehnologic și un Centru specializat pentru evaluarea nivelului de securitate al soluțiilor hardware/software
- Oragnizarea unui Centru național de competențe care să asiste instituțiile publice în dezvoltarea sistemelor informatice
- Un cadru normativ pentru infrastructurile de tip Cloud
- Dezvoltarea de “hub-uri informaționale”, care să asigure schimbul securizat de informații între instituțiile publice, interconectate prin Intranetul guvernamental
- Oferirea de facilități (vouchere) care să permită actorilor economici să-și efectueze un audit minim de securitate
- Introducerea unor roluri de specialiști IT în toate instituțiile publice centrale și locale

Tendințe globale

Trăim astăzi într-o lume din ce în ce mai conectată și suntem înconjurați de device-uri din ce în ce mai inteligente. 90% din informația disponibilă online a fost introdusă în ultimul an, 85% din aplicațiile dezvoltate azi sunt pregătite pentru cloud, iar noi petrecem în medie 4 ore pe zi în fața unui ecran, fie că vorbim de laptop, desktop, tabletă sau smartphone. Timpul petrecut în spațiul virtual capătă o pondere din ce în ce mai mare, am învățat să ne "transferăm" o parte din activități și ne-am adaptat o serie de gesturi la mediul online: acum, nu doar căutăm și alegem haine online ținând cont de pozele din, ci putem să le "probăm" virtual, nu ne mai rezumăm la a căuta după cuvinte cheie, ci dialogăm cu un asistent electronic într-un limbaj (aproape) natural, iar pentru plăți folosim portofele electronice și monede virtuale.

Până în 2020 se estimează că numărul de telefoane inteligente va depăși 6 miliarde, în timp ce IoT va număra aproape 80 miliarde de device-uri. Nivelul de sofisticare va crește accelerat, la fel funcționalitățile, așa că soluțiile electronice vor câștiga teren în fața alternativei clasice. Implicit, furnizorii de servicii vor fi din ce în ce mai interesați de prezența și poziția lor în spațiul virtual, însoțindu-și astfel clienții potențiali.

Pentru furnizorii care își adaptează și își diversifică oferta introducând servicii electronice noi, succesul se măsoară prin numărul de utilizatori efectivi și prin frecvența utilizării soluției (și, în final, prin numărul de clienți ai serviciului sau produsului propriu-zis, fie că e vorba de clienții unui serviciu de Internet banking sau ai unui magazin virtual). Iar un consumator va folosi varianta online dacă știe cum, poate și vrea să o facă:

- ***Știe cum*** – Atrage atenția asupra setului minim de cunoștințe și competențe al utilizatorului, dar în egală măsură indică furnizorilor de servicii importanța ergonomiei interfeței (un exemplu relevant din zona B2B: 71% dintre achizitori ar cumpăra mai mult dacă aplicațiile ar permite o navigare mai facilă și ar simplifica procesul de cumpărare pentru companii – www.internetretailer.com).

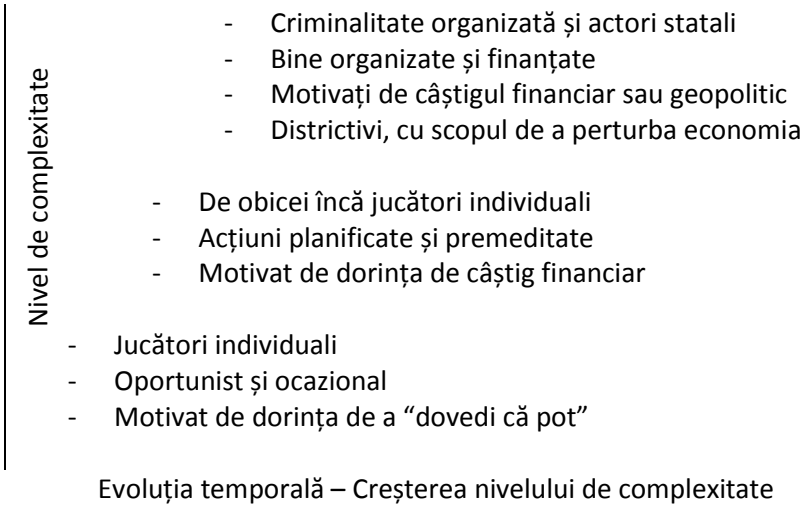
- ***Poate*** – Consumatorul dispune de resursele minime pentru a accesa serviciul online: echipament și conexiune Internet.

- ***Vrea*** – Aici trebuie să avem în vedere atât factorii motivaționali (de exemplu valoarea adăugată de serviciul electronic, așa cum este ea percepută de client), care acționează în sensul utilizării serviciului, cât și atributele care pot limita utilizarea acestuia (de exemplu, un nivel de securitate al sistemului perceput ca fiind insuficient, aspect asupra căruia ne vom și concentra în continuare).

Din aceste perspective, creșterea nivelului de conectivitate și sofisticare al device-urilor contribuie la dezvoltarea și diversificarea alternativei electronice dar, în același timp, induce riscuri de securitate suplimentare, cu efect opus, de limitare a utilizării serviciilor online.

Entitățile ostile

Privind retrospectiv, observăm că locul tânărului programator care realiza, acum 20 de ani, un virus doar pentru a-și dovedi că poate să o facă, este luat de grupuri organizate, formate deseori din specialiști din regiuni/țări diferite, motivate și de rezultate financiare sau de altă natură. Complexitatea, dimensiunea și frecvența virușilor a crescut de asemenea. Codul sursă al unui virus din 1995 ocupa câteva pagini și putea fi analizat de un singur specialist, în câteva ore, în timp ce un virus modern este "dezlegat" de o echipă întreagă, iar codul sursă s-ar putea întinde pe câteva sute de mii de pagini. În urmă cu 20 de ani, furnizorii de soluții antivirus se confruntau cu un virus nou o dată pe săptămână sau chiar mai rar, în timp ce azi apar peste 250.000 de viruși zilnic (incluzând și mutațiile).



Creșterea complexității implică costuri suplimentare, ajungându-se la valori foarte ridicate. În locul "scriitorului de viruși" din 1995, în general nemotivat financiar și nefinanțat, identificăm în prezent mai multe roluri, fiecare cu motivația sa (o entitate, grup sau persoană, poate cumula mai multe roluri simultan):

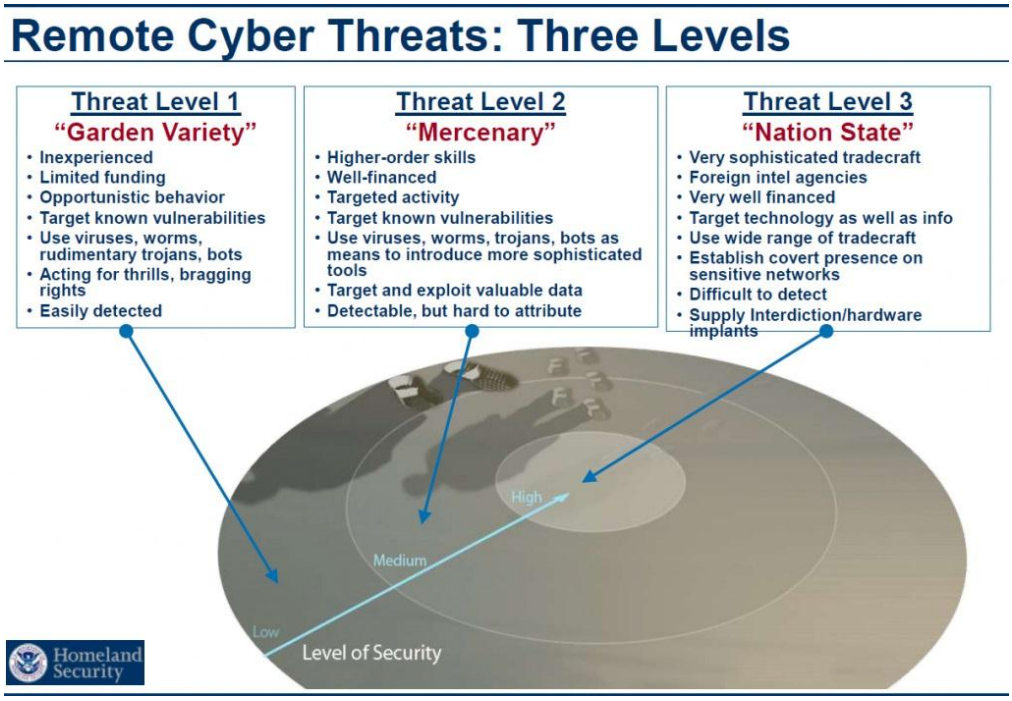
- ***Finanțatorul*** – Cel care susține financiar dezvoltarea unui instrument/mecanism de atac informatic, incluzând aici organizații teroriste, grupurile infracționale organizate și actorii statali

- ***Echipa care concepe și realizează malware-ul***

- ***"Distribuitorul"*** – Veriga în procesul (ilicit) de comercializare a malware-ului. Distribuitorul nu dorește să utilizeze respectivul instrument.

- ***Clientul*** – Cel care achiziționează malware-ul pentru a-l utiliza sau angajează CaaS (Cybercrime-as-a-Service)

După cum se menționează și în documentele NATO, până în prezent, cei mai periculoşi actori în domeniul cibernetic rămân statele-naţiuni, deși o largă diversitate de capabilităţi ofensive este acum accesibilă și actorilor non-statali, cum ar fi grupurile infracționale organizate sau grupările teroriste. Spionajul de stat sau sabotajul de înaltă sofisticare necesită, ca și până acum, hotărârea, raţiunea cost-beneficiu și capabilităţile unui stat-naţiune.



Nu există nicio îndoială că unele ţări, companii sau grupuri organizate investesc deja masiv în capabilităţi cibernetice care pot fi folosite și în scopuri militare. La prima privire, cursa digitală a înarmării se bazează pe o logică clară şi implacabilă, deoarece domeniul războiului cibernetic oferă numeroase avantaje: este asimetric, atrăgător prin costurile scăzute şi atacatorul deţine iniţial toate avantajele. Mai mult decât atât, nu există practic nicio formă reală de descurajare în cadrul războiului cibernetic, deoarece până şi identificarea atacatorului este extrem de dificilă şi, respectând dreptul internaţional, probabil, aproape imposibilă. În aceste condiţii, orice formă de retorsiune militară ar fi foarte problematică, atât din punct de vedere legal, cât şi din punct de vedere politic (www.nato.int).

Cybercrime-as-a-service

Dezvoltarea de malware sofisticat se bazează pe 2 componente esențiale:

- acces la o sursă de finanțare consistentă
- acces la capabilități tehnice relevante

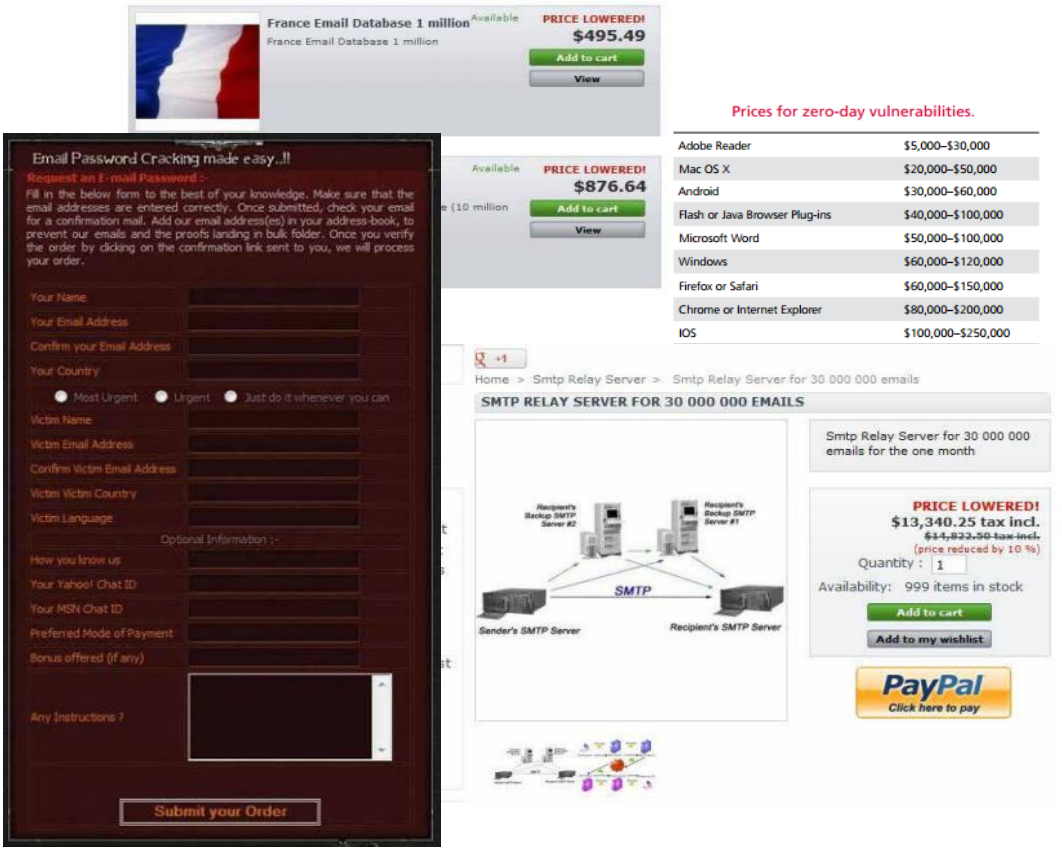
De curând, Europol a estimat că la nivel global există aproximativ 100 de "creiere" care pot realiza astfel de malware, majoritatea în fostele țări sovietice. Mai grav însă, o bună parte dintre aceste mecanisme informatice, odată construite și utilizate în sensul și pentru motivul pentru care au fost

elaborate, încep să fie disponibile pe o piață neagră dedicată. Infractorii cibernetici din ziua de azi nu mai au nevoie de cunoștințe tehnice specializate ci doar de un card de credit, putând să achiziționeze "arma" ca atare (și, din păcate, în lumea virtuală nu există conceptul de "permis port-armă") sau să angajeze serviciul de exploatare/utilizare al acesteia.

Serviciile oferite îmbracă mai multe forme (www.mcafee.com):

- ***Reasearch-as-a-Service*** – în acest caz nu se poate vorbi neapărat de o piață neagră, ci mai degrabă gri. Aici regăsim organizațiile care identifică și prezintă vulnerabilități 0-day către companii selectate după anumite criterii de eligibilitate. Totuși, nu se exclud intermediarii care nu mai aplică aceleași criterii stricte, informația putând ajunge la entități care o folosesc ulterior în scopuri infracționale.

- ***Crimeware-as-a-Service*** – identificarea și dezvoltarea de kit-uri de exploatare, instrumente suport (keyloggers, bots), soluții de mascare a conținutului malware (cryptors, polymorphic builders), roboți și chiar dispositive hardware conexe (skimmers).



- ***Cybercrime Infrastructure-as-a-Service*** – odată ce infractorii cibernetici obțin instrumentele necesare, pentru atacul propriu-zis aceștia pot închiria rețele de calculatoare pentru un atac DoS sau pot accesa platforme pe care să-și hosteze conținutul malware.

- ***Hacking-as-a-Service*** – având un cost superior alternativei în care se achiziționează componentele individuale, "cumpărarea" unui atac reprezintă varianta care necesită cele mai puține cunoștinte tehnice. Tot în această categorie regăsim cumpărarea de credențiale, date despre cardurile de credit etc.

10-th version.

Packages:

â€¢ Minimum: DDoS Bot, no free updates, no modules = $450
â€¢ Standart: DDoS Bot, 1 month free updates, password grabber module = $499
â€¢ Bronze: DDoS Bot, 3 months free updates, password grabber module, 1 free rebuild = $570
â€¢ Silver: DDoS Bot, 6 months free updates, password grabber module, 3 free rebuilds = $650
â€¢ Gold: DDoS Bot, lifetime free updates, password grabber + "hosts" editor modules, 5 free rebuilds, 8% discount on other products. = $699
â€¢ Platinum: DDoS Bot, lifetime free updates, password grabber, unlimited free rebuilds, 20% discount on other products. = $825
â€¢ Brilliant: DDoS Bot, lifetime free updates, unlimited free rebuilds, all modules for free, 25% discount on other products. = $999

Other:
â€¢ ReBuild (URLs changing) â€" $35.
â€¢ Sources - ~3500-5000$, discuss individually
â€¢ New features - discuss individually.
â€¢ Web-Panel reinstalling (1st time is free) - $50

Botnet services

CHEAP PROFESSIONAL DDOS SERVICE

Cheap Professional DDOS Service
Trusted
Strong/Fast Service
Takes down Large Website/Forum/Game Servers etc.
No time limit

PRICE

1 - 4 hours / 2$ per hour
5 - 24 hours / 4$ per hour
24 - 72 hours / 5$ per hour
1 month / 1000$ fix price

PAYMENT ACCEPTED

Paypal (Verified users only)
Liberty Reserve
Western Union
MoneyBookers

CONTACT

Yahoo Messenger :
Msn :
Skype :

credit card

	US			EU		
Visa Classic	$15	$80		$40	$150	
Master Card Standard		$90			$140	
Visa Gold/Premier	$25	$100	$200	$45	$160	$250
Visa Platinum	$30	$110		$50	$170	
Business/Corporate	$40	$130		$60	$170	
Purchasing/Signature	$50	$120		$70		
Infinite				$130	$190	
Master Card World		$140				
AMEX	$40			$60		
AMEX Gold	$70			$90		
AMEX Platinum	$50					

Finanțele subterane

Această economie paralelă s-a dezvoltat în special pentru că infractorii (și nu ne rezumăm la cei cibernetici) au nevoie să acceseze circuite financiare fără trasabilitate.

Economia digitală subterană, ca orice economie, se bazează pe fluxul liber de fonduri. Varietatea mecanismelor de plată disponibile și folosite de infractorii cibernetici este diversă, variază față de lumea reală, plățile fizice fiind efectuate către monede digitale nedetectabile.

Multe mecanisme de plată cu aspect important on-line oferă un număr de caracteristici care le face atractive ca și instrument financiar pentru organizațiile criminale - anonimatul, transferuri rapide, ieftine și ireversibile și tranzacțiile financiare disimulate.

În multe privințe, unele mecanisme de plată pot oferi un nivel de anonimat similar banilor, dar într-un mediu on-line.

În continuare se prezintă, sintetizat, modul în care sunt utilizate diversele mecanisme de plată (www.europol.europa.eu):

Payment purpose	*Payment for*	*Common payment mechanisms*	*Example*
Victim payment	Extorsion	Bitcoins, Bank Transfer, paysafecard	Payment extorted as a result of a ramsonware or DDoS attack
	Fraud	Bitcoins, Bank Transfer, Western Union	Loss to an online fraud/scam
Criminal to criminal payment	Counter AV	PayPal	Testing of malware against commercial AV products
	Data	Bitcoins, Ukash, Western Union, Webmoney	Purchase of compromosed financial data such as credit cards
	DDoS	Bitcoins	DDoS service for hire
	Hosting	Bitcoins	Purchase of hosting (including bulletproof)
	Malware	Visa, MasterCard, WebMoney, PayPal	Purchase of malware, such as RATS and banking trojans
	Trade on hidden service	Bitcoins, Ukash, paysafecard	Purchase of drugs or weapons
Payment for legitimate service		Bitcoins, Bank transfer, Visa, MasterCard	Hosting, hardware, software, travel, accomodation etc
Money movement		Bitcoins, Bank transfer, Western Union	Movement of money to maintain control of funds or hide/break a financial trail, including „cashing-out" of compromised financial accounts. This also includes exchange to, from or between virtual, digital and fiat currencies

IoT și IoBadT

Internet of Things este o paradigmă care schimbă abordarea tehnologiei, extinzând suprafaţa de atac. Dispozitivele IoT se regăsesc deja pretutindeni și din acest motiv industria IT trebuie să ţină cont de problemele de securitate și confidenţialitate. Un studiu recent a scos în evidenţă faptul că dispozitivele IoT casnice expun utilizatorii la o gamă variată de ameninţări, incluzând furtul de date și

sabotaje, iar proliferarea dispozitivelor IoT va avea o influenţă majoră asupra comportamentului uman, schimbând modul în care realizăm anumite activități, cum ar fi achizițiile online, plata online etc (www.veracode.com, www.cybersecuritytrends.ro).

Odată cu IoT a apărut și un al doilea concept, ***"Internet of Bad Things"***, reunind aici dispozitivele care conțin vulnerabilități intrinseci, greu de înlăturat, unele apărute încă din faza de design. Din această categorie fac parte *dispozitivele produse de companii în care presiunea departamentului de marketing-vânzări pentru încadrarea într-un calendar ferm face ca etapa de testare să fie redusă excesiv*, dar și *dispozitivele în care regăsim firmware vulnerabilizat voluntar de producător pentru a putea avea ulterior acces de la distanța la echipament*. În cazul IoBadT, eliminarea vulnerabilităților prin patch-uri ulterioare este dificilă sau chiar imposibilă.

Infractorii cibernetici, hackerii susţinuţi de state, hack-tiviștii și teroriștii cibernetici pot exploata defectele din arhitectura IoT și pot produce daune extinse în orice industrie. Infractorii cibernetici pot fi interesaţi să fure informaţii sensibile administrate de platformele IoT sau pot fi interesaţi să compromită obiectele inteligente și să le utilizeze în activităţi ilegale, cum ar fi derularea unor atacuri asupra unor terţe entităţi sau mineritul Bitcoin. În mod similar agenţiile de Intelligence sunt interesate să exploateze dispozitivele inteligente pentru a derula campanii de spionaj la scară largă, care utilizează routere, console de jocuri și smartphone-uri pentru a spiona persoanele vizate. Teroriștii cibernetici și hack-tiviștii pot fi de asemenea interesaţi să compromită dispozitivele IoT pentru a fura informaţii sensibile.

Specialiștii estimează că numărul atacurilor cibernetice împotriva obiectelor inteligente va crește rapid în anii care vor urma.

Principalele ameninţări cibernetice pentru dispozitivele IoT pot fi (www.symantec.com, www.cybersecuritytrends.ro):

- ***Denial of service*** - atacurile DDoS pot viza toate punctele unui scenariu de lucru determinând probleme serioase în reţeaua dispozitivelor inteligente și paralizând serviciul pe care acestea îl furnizează.

- ***Botneți și atacuri malware*** - acesta este scenariul cel mai comun și mai periculos, dispozitivele IoT sunt compromise de atacatori care abuzează de resursele lor. În mod uzual atacatorii utilizează cod specializat care să compromită software-ul care rulează pe dispozitivele IoT. Malware-ul poate fi utilizat pentru a infecta dispozitivele utilizate pentru controlul reţelei de dispozitive inteligente sau să compromită software-ul care rulează pe acestea. În cel de-al doilea scenariu atacatorii pot exploata prezenţa unor defecte în firmware-ul care rulează pe aceste dispozitive și să ruleze codul lor arbitrar care să deturneze componentele IoT spre o funcţionare neplanificată.

- ***Accesul neautorizat la date*** - atacatorii pot spiona comunicaţiile dintre dispozitivele IoT și să colecteze informaţii despre serviciile pe care acestea le implementează. Datele accesate prin intermediul dispozitivelor IoT pot fi utilizate în scopuri de spionaj cibernetic sau de către o agenţie de intelligence sau de către o companie privată în scopuri comerciale. Breșele de securitate reprezintă o problemă serioasă pentru organizaţiile sau persoanele care utilizează dispozitive inteligente.

- ***Breșe accidentale*** – Managementul datelor într-o arhitecutură care include dispozitive IoT este un aspect critic. Informaţiile sensibile pot fi expuse nu numai într-un atac cibernetic, ci pot fi expuse sau pierdute și în mod accidental.

- ***Protectie redusa la nivel de conexiune*** – Prin exploatarea unui defect în SmartTV-ul nostru atacatorul poate avea acces la reţeaua domestică și să dezactiveze orice sistem antifurt implementat pentru securitatea fizică.

Firmele de securitate au observat o escaladare a atacurilor cibernetice împotriva dispozitivelor IoT, la scară globală. Cel mai întâlnit scenariu este utilizarea de botneţi alcătuiţi din mii de dispozitive din domeniul IoT, cunoscute și sub denumirea de thingboţi, care sunt utilizaţi pentru a trimite mesaje de spam sau pentru coordonarea unor atacuri DDoS. Rezumând, un thingbot poate fi utilizat pentru:

- a trimite spam.
- a coordona un atac împotriva unei infrastructuri critice.
- a furniza un malware.
- a funcţiona ca punct de intrare în reţeaua unei companii.

Doua vulnerabilități merită punctate aici:

1. ***Bash Bug*** (CVE-2014-6271) este un defect critic care poate fi exploatat de la distanţă și care afectează mașini Linux, Unix și Apple Mac OS X, inclusiv dispozitive IoT. Companiile de securitate confirmă faptul că vulnerabilitatea Bash Bug ar putea să fie deja utilizată de către infractori pentru afectarea dispozitivelor din diferite industrii.
2. ***Heartbleed***: prin exploatarea defectului Heartbleed un atacator poate citi de la distanţă memoria sistemelor care rulează versiuni vulnerabile ale popularei biblioteci OpenSSL. Un dispozitiv IoT vulnerabil conectat la un server poate fi compromis dacă este afectat de o vulnerabilitate Heartbleed prin simpla trimitere a unui mesaj Heartbeat către acesta. Dispozitivul IoT îi va răspunde trimiţând date suplimentare din memoria sa, putând expune credenţialele și alte date sensibile.

Amenințăr și vulnerabilități

Vendorii majori de tehnologie dispun de capabilitățile tehnice de colectare, agregare și analizare continuă a vulnerabilităților și amenințărilor (precum traficului malware), de-a lungul unui set global de date de telemetrie, rezultatele oferind perspective asupra unui posibil comportament criminal viitor. Principalele concluzii sunt prezentate mai jos (www.cisco.com):

- Atacatorii au devenit mai eficienți în a profita de brește de securitate pentru a-și ascunde activitatea.
- Operatorii de crimeware, precum ransomware, angajează și finanțează echipe de dezvoltare profesioniste pentru a-i ajuta să se asigure că tacticile lor rămân profitabile.
- Criminalii apelează la rețeaua de internet anonimă Tor și Proiectul Internetului Invizibil (I2P) pentru a transmite comunicațiile de tip comandă și control (command&control) în timp ce evită detectarea.
- Autorii malware au intensificat studierea tehnicilor precum detectarea în sandbox pentru a-și masca prezența pe rețea.

- Au fost exploatate 1% din vulnerabilitățile si expunerile comune (CVE – Common Vulnerabilities and Exposure) identificate prin alerte de extremă urgență. Asta înseamnă că organizațiile trebuie să-și stabilească prioritățile și să aplice corecțiile necesare acelui procent din vulnerabilități cât mai rapid. Dar chiar și cu tehnologie de securitate de vârf, excelența în procedurile interne este necesară pentru a adresa aceste vulnerabilități.
- De când kitul de exploatare Blackhole a fost abandonat în 2013, nici un alt kit de exploatare nu a fost capabil să obțină aceleași culmi ale succesului. Este insă posibil ca locul în top să nu mai fie la fel de râvnit de autorii kiturilor de exploatare precum era odată. Angler continuă să domine piața kiturilor de exploatare când vine vorba de sofisticare și eficacitate. Utilizatorii par să investească în special în kit-uri care-și dovedesc abilitatea de a evita detecția.
- Unii autori ai kiturilor de exploatare încorporează texte din romanul clasic al lui Jane Austen "Rațiune și simțire" în paginile web care le găzduiesc kiturile de exploatare. Este foarte probabil că antimalware-ul și alte soluții de securitate vor categorisi aceste pagini ca valide după "citirea" unui asemenea text.
- Adversarii folosesc din nou macrocomenzile Microsoft Office pentru a livra malware. Este o tehnică veche care acum a pierdut teren, dar este reluată pe măsură ce entități rău intenționate caută noi moduri de a contracara măsurile de protecție
- Exploatările Java au scăzut cu 34% pe măsură ce securitatea Java se îmbunătățește, iar atacatorii adoptă noi vectori de atac.
- Malware-ul din Flash poate interacționa acum cu JavaScript pentru a ajuta la camuflarea activității, fiind mult mai greu de detectat și analizat.
- Exploatarea vulnerabilităților lui Adobe Flash sunt în creștere, acestea fiind integrate regulat în kituri de exploatare utilizate la scară largă precum Angler și Nuclear.
- Volumul spam a crescut cu 250% în ultimul an. Spam-ul de tip Snowshoe, care implică trimiterea unor volume mici de spam de la o gamă largă de adrese IP pentru a evita detectarea, este o amenințare în dezvoltare. Volumul spam este în creștere în Statele Unite, China și Federația Rusă, dar rămâne relativ stabil în alte regiuni în primele cinci luni ale anului 2015
- Utilizatorii și echipele IT au devenit fără voie componente ale problemelor de securitate. Criminalii online se bazează pe faptul că utilizatorii vor instala malware sau vor ajuta la exploatarea lacunelor în securitate.
- Heartbleed, periculosul defect de securitate, este o amenințare critică pentru OpenSSL. Cu toate astea 56% din toate versiunile OpenSSL existente au mai mult de 50 luni vechime și de aceea sunt încă vulnerabile.
- Nivelul de conştientizare al riscurilor şi ameninţărilor cibernetice, competențele și capabilitățile utilizatorilor, coroborate cu campaniile focusate ale atacatorilor, plasează multe industrii într-o zonă cu risc crescut de expunere la malware. Pe primul loc, în ultimul an, regăsim industria farmaceutică și chimică.
- Creatorii malware folosesc add-on-urile de la browser ca un mediu pentru distribuirea malware și aplicații nedorite. Această abordare pentru distribuirea malware se dovedește a fi de succes pentru actorii implicați, pentru că mulți utilizatori au încredere automat în add-on-uri sau le consideră inofensive.
- Industria securității acordă mai multă atenție diminuării vulnerabilităților în soluțiile open source

A. *Exploatări Web: Pentru autorii kiturilor de exploatare, menținerea locului din top nu înseamnă că ești cel mai bun*

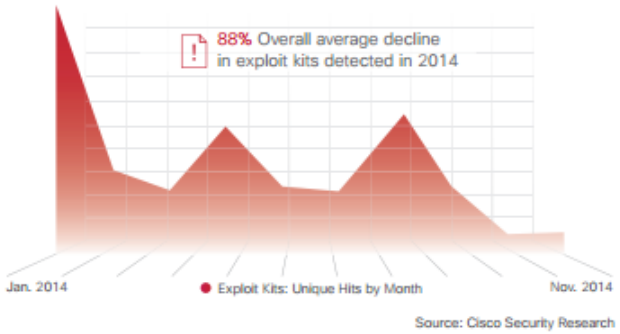
În lumea afacerilor, companiile doresc să fie cunoscuți ca lideri ai industriei. Dar pentru autorii kiturilor de exploatare care operează în așa numita ”economie subterană”, menținerea celei de-a patra sau a cincea poziție în cadrul topului kiturilor de exploatare poate fi un semn și mai distinctiv de indicare a succesului.

În cursul ultimului an și jumătate, Angler, Sweet Orange și Goon erau kiturile de exploatare observate cel mai des ”în acțiune”, potrivit experților de securitate.

- ***Angler*** a fost observat cel mai frecvent dar, din motive neclare, a ieșit în evidență foarte mult la sfîrșitul verii. Cercetarea atribuie popularitatea lui Angler deciziei autorului de a elimina cerința de a descărca un malware sub forma unui fișier executabil Windows. Includerea vulnerabilităților Flash, Java, Microsoft Internet Explorer (IE) și chiar și Silverlight in pachetul Angler face acest kit de exploatare unul ”de supravegheat”.

- ***Sweet Orange*** este de asemenea foarte dinamic; componentele se schimbă constant astfel încât Sweet Orange poate rămâne eficient și nedetectat. Asta califică Sweet Orange ca fiind kitul de exploatare cu cele mai mari șanse de reușită. Sweet Orange distribuie o gamă de malware către sistemele finale fără corecții și include exploatări pentru vulnerabilitățile din Adobe Flash Player, IE și Java. Atacatorii care folosesc Sweet Orange se bazează pe malvertising pentru a redirecționa utilizatorii către site-uri, inclusiv cele legitime, care găzduiesc kitul de exploatare. Utilizatorii sunt de obicei redirecționați de cel puțin două ori în acest proces. Site-urile compromise care rulează versiuni depășite ale sistemelor de gestionare al conținutului (CMS) precum WordPress și Joomla sunt cunoscute pentru găzduirea kitului Sweet Orange.

- ***Goon*** poate fi considerat drept ”cel mai organizat” kit comparativ cu restul kiturilor de exploatare. Inițial descoperit de cercetătorii în securitate în 2013, Goon, cunoscut ca și ”kitul de exploatare Goon\Infinity”, este un sistem de distribuție malware care generează exploatări pentru vulnerabilitățile browser-ului care țin de Flash, Java sau Silverlight pe platformele Mac și Windows.



În timp ce numărul aproximativ al kiturilor de exploatare detectate în teren a scăzut cu 87% în lunile următoare expunerii kitului Blackhole, numărul de kituri detectate a crescut în timpul verii anului trecut. În ultimele două săptămâni ale lunii august se observă o creștere semnificativă în numărul de detecții ale kitului de exploatare Angler. Însă, până în luna noiembrie, numărul general de detectări

ale kiturilor cunoscute a scăzut din nou, iar Angler și Goon\Infinity rămân cele care apar cel mai frecvent. Scăderea generală a numărului de kituri de exploatare este de 88%.

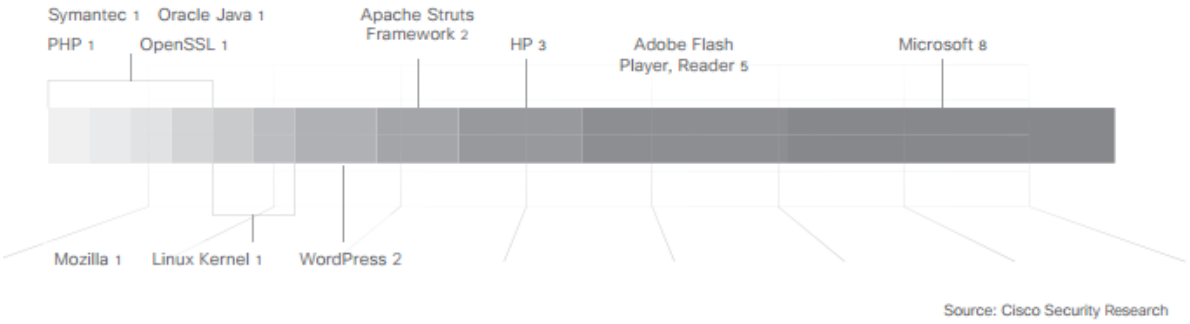
B. Amenințări și vulnerabilități: Java în declin ca vector de atac

În anii recenți, Java a jucat un rol principal nedorit în lista celor mai severe și predominante vulnerabilități de exploatat. Însă, Java începe să nu mai fie principala alegere a atacatorilor care caută cele mai rapide, ușoare și greu de detectat căi pentru a lansa exploatări folosind vulnerabilități software.

Din topul celor 25 de vulnerabilități legate de vendori și produse din ultimul an, numai unul era legat de Java. Comparând ultimii 2 ani, numărul de vulnerabilități Java a scăzut de la 54 la 19. Date provenite de la Baza de Date a Vulnerabilităților Naționale (NVD) arată un declin similar, de la 309 la 253.

Asta nu ar trebui să descurajeze criminalii din mediul online de la a continua să profite de popularitatea și eficiența utilizării acestor vulnerabilități vechi, dar care continuă să existe și în prezent.

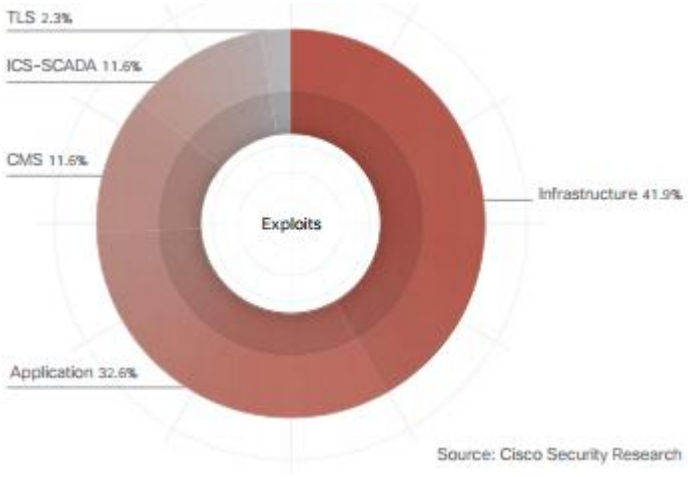
Ierarhia vulnerabilităților vendorilor și produselor:



Exploatările care implică vulnerabilități pe partea clientului în Adobe Flash Player și Microsoft IE au detronat Java, alături de exploatările care vizează servere (spre exemplu exploatări ce implică vulnerabilități în cadrul Apache Struts, sistemul open-source web). Numărul în creștere al exploatărilor Apache Struts este un exemplu al tendinței criminalilor de a compromite infrastructura online pentru a-și mări raza de acțiune și posibilitățile din timpul atacurilor.

Cadrul Apache Struts este un punct de pornire logic pentru exploatări, datorită popularității sale. Sistemele de gestionare al conținutului (CMS) sunt de asemenea ținte preferate; adversarii se bazează pe site-uri care rulează versiuni vechi de CMS pentru a facilita livrarea exploatării.

Categorii de produse exploatate:



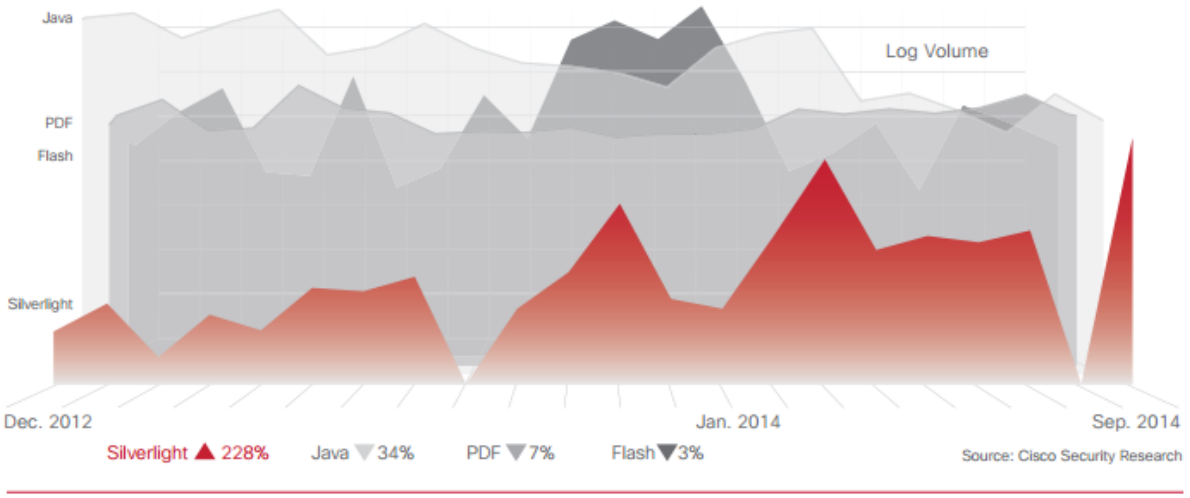
Obs. O zonă care impune o atenție sporită în viitor o reprezintă sisteme SCADA, atacurile asupra acestora dublându-se anual. Odată cu nevoia de deschidere și interconectare a rețelelor de monitorizare și control apar implicit și riscurile specifice rețelelor și sistemelor IP clasice. Această tendință de interconectare , procesare în cloud (cel mai probabil privat) și deschidere către terți a acestor rețele, considerate până acum sigure prin izolarea lor, va putea duce la incidente semnificative de securitate daca nu este efectuata din timp o analiza de risc și implementate controale specifice zonei de IT. Mare parte din aceste sisteme intra sub incidenta infrastructurii critice dar și in zona industriala privata efectele unui atac pe sistemele de control industrial poate duce la pierderi importante din punct de vedere financiar sau pot genera incidente cu impact asupra mediului de exemplu. Consideram că și aceasta zona ar trebui tratată distinctiv inclusiv în zona cadrului legislativ și reglementată din punct de vedere al securității cibernetice, mai ales în contextul creșterii amenințărilor teroriste și al atacurilor coordonate de alte națiuni.

Analiză: Factorii probabili pentru care adversarii au abandonat exploatarea Java

Cercetătorii sugerează că declinul în exploatările Java poate fi legat de faptul că exploatări Java de tip "zero day" nu au mai fost dezvăluite și prin urmare nu au mai fost disponibile pentru atacatori în anul 2014. Versiunile moderne Java sunt corectate automat, iar versiunile mai vechi și vulnerabile sunt blocate automat de către vendorii de browsere. Apple face un pas în plus și dezactivează versiunile vechi și vulnerabile și le corectează prin actualizări automate. În plus, Centrul de Răspuns la Incidente de Securitate Cibernetică SUA (US-CERT) a recomandat ca utilizatorii de calculatoare să securizeze, dezactiveze sau să înlăture Java.

Ultima versiune Java, Java 8, are controale mai puternice față de versiunile anterioare. Este și mai greu de exploatat pentru că acum necesită interacțiune umană, ca semnarea unui cod și o căsută de dialog prin care se cere activarea Java. Criminalii online au descoperit ținte mai ușoare și și-au îndreptat atenția către vectori non-Java care le oferă un profit mai mare al investiției. Spre exemplu, mulți utilizatori nu actualizează Adobe Flash sau cititoarele PDF în mod regulat, oferind criminalilor o gamă mai largă de vulnerabilități atât vechi, cât și noi. De asemenea, s-a observat că numărul kiturilor de exploatare care includ exploatări Silverlight este în creștere.

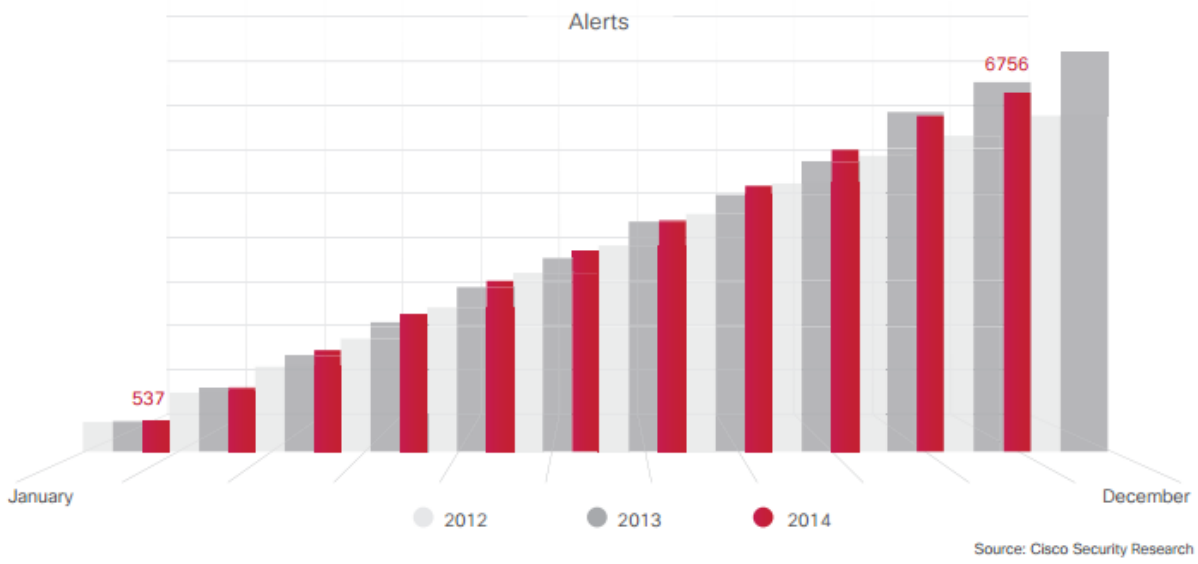
Figura următoare arată că „domnia” Java ca principalul vector de atac are o tendință în scădere de aproape 2 ani. Folosirea Flash pentru lansarea exploatărilor a fost oarecum dezordonată, cu punctul culminant în 2014. Utilizarea PDF a fost constantă, fiindcă mulți infractori cibernetici par să rămână concentrați pe lansarea campaniilor țintă prin intermediul emailurilor cu atașamente PDF. Atacurile Silverlight, deși încă mici la număr față de vectorii consacrați, sunt în creștere.



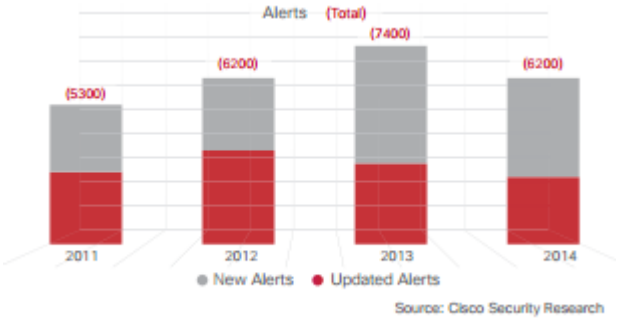
C. Alerte cumulative anuale în declin

Totalul alertelor anuale, ca sumă a vulnerabilităților noi și actualizate ale produselor raportate în 2014, pare să cunoască un declin (de 1.8%). Procentajul poate fi mic, dar este pentru prima oară în ultimii ani când alertele au scăzut comparativ cu anul precedent.

Cel mai probabil motiv pentru declin este atenția crescândă acordată de vendori testării și dezvoltării de software. Îmbunătățirile aduse ciclurilor de dezvoltare par să reducă numărul de vulnerabilități ce pot fi ușor exploatate de criminali.



Alerte noi vs. alerte actualizate: Numărul în creștere de alerte noi pentru anul 2013 și 2014 indică faptul că sunt raportate mai multe vulnerabilități noi față de anii precedenți, ceea ce înseamnă că vendorii, dezvoltatorii și cercetătorii în domeniul securității găsesc, repară și raportează noi vulnerabilități în produsele lor. Numărul total al alertelor noi și totalul anual sunt la egalitate sau scad ușor în 2014 comparativ cu anul 2013.



D. Pericolele unui software depășit și de ce corectarea nu e singura soluție

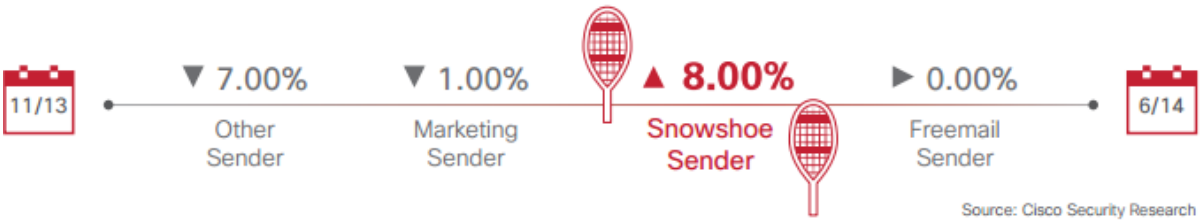
Tradițional, atacatorii adoptă cea mai ușoară cale disponibilă când determină unde și cum vor avea succes în exploatare. Aleg produse care prezintă o suprafață de atac mai mare; acele oportunități sunt în general create de folosirea unui software depășit sau fără corecții. Spre exemplu, aplicarea corecțiilor rămâne o provocare fiindcă există încă multe sisteme care sunt vulnerabile la un atac SSL Poodle. Bazat pe tendințele observate, cercetătorii sugerează că proliferarea versiunilor depășite a unui software exploatabil va continua să ducă la probleme de securitate de magnitudine mare.

O echipă de experți a folosit motoare de căutare pentru a examina dispozitivele conectate la internet care folosesc OpenSSL. S-a determinat că 56% din dispozitivele examinate foloseau versiuni OpenSSL care erau mai vechi de 50 luni. Asta înseamnă că în ciuda publicității oferită lui Heartbleed, defectul de securitate în manevrarea TLS (Transport Security Layer) descoperit în 2014, și a nevoii urgente de a actualiza la ultima versiune de OpenSSL pentru a evita asemenea vulnerabilități, organizațiile nu se asigură că rulează cele mai noi versiuni.

E. Spam: Spammerii adoptă strategia Snowshoe

Phishing-ul continuă să își dovedească valoarea ca unealtă pentru livrarea malware și furtul de credențiale deoarece utilizatorii cad pradă tacticilor de spam familiare. Atacatorii au realizat că este adesea mai ușor să exploatezi utilizatori la nivel de browser și email decât să le compromiți serverul, ceea ce înseamnă că spammerii continuă să inoveze.

Nu este neobișnuit să vezi un sistem anti-spam care detectează mai mult de 99% din spam. Majoritatea celor mai bune sisteme anti-spam fac asta. În acest mediu, spammerii încearcă aproape orice pentru a evita filtrele spam. Pentru a se asigura că acel spam ajunge la destinația menită, ei folosesc din ce în ce mai des noi tactici pentru a evita detecția bazata pe reputația IP-ului.



Spam snowshoe (incălțăminte de zăpadă): Comparația este potrivită deoarece snowshoe permite unei persoane să meargă prin zăpada adâncă prin distribuirea greutății sale pe o suprafață mai mare, astfel prevenind scufundarea piciorului în zăpadă. Spam-ul snowshoe este alcătuit din emailuri nesolicitate trimise prin intermediul unui număr mare de adrese IP, și la un volum mic per adresă IP, astfel prevenind anumite sisteme spam de la a-l detecta. Pentru a diminua spam-ul snowshoe, profesioniștii în securitate nu se pot baza pe soluții bazate pe reputație, din moment ce aceleași mesaje dintr-o campanie pot fi generate din sute sau chiar mii de locuri în cazul campaniilor ce utilizeaza botneti. Examinarea altor componente ale spam-ului poate oferi o detectare mai precisă.

Volumul de spam în funcție de țară:

F. Malvertising cu ajutorul add-on-urilor de la browser: provocarea pagubelor mici per utilizator pentru a colecta recompense mari

Analiza a arătat că această familie de add-on-uri este mult mai extinsă decât se credea și că, creatorii de malware folosesc o combinație de cod foarte sofisticat, scris în mod profesionist și un plan de afacere rafinat pentru a menține acel malware profitabil pe termen lung. Cu alte cuvinte, nu este necesar un control complet asupra gazdei țintă pentru a monetiza cu succes. Asta duce la o predominanță crescută a tipului de malware construit special pentru un impact scăzut asupra gazdei afectate și optimizat pentru monetizare pe termen lung pe seama unei largi populații afectate.

Percepția asupra riscurilor și amenințărilor cibernetice

Un studiu realizat pe 1700 de companii din 9 țări a scos la iveală câteva concluzii interesante (www.cisco.com):

- 59% dintreChief Information Security Officers (CISO) își consideră procesele de securitate optimizate, comparativ cu 46% dintre managerii insărcinați cu securitatea operațiunilor.
- Aproximativ 75% din CISO își văd soluțiile de securitate ca fiind foarte sau extrem de eficiente, iar aproximativ un sfert din ei percep soluțiile de securitate ca fiind oarecum eficiente.
- 91% dintre respondenții din cadrul companiilor cu securitate sofisticată sunt întru totul de acord că directorii companiei consideră securitatea o prioritate de top.
- Mai puțin de 50% din respondenți folosesc unelte standard precum corecția și configurarea pentru a ajuta prevenirea breșelor de securitate.
- Este mai probabil ca organizațiile mari și mijlocii să aibă abordări de securitate foarte sofisticate, comparativ cu organizațiile de alte dimensiuni incluse în studiu

Pe de altă parte însă, aproape jumătate din ***utilizatori*** confirmă că au întâlnit programe malware anul trecut și că în cele mai multe cazuri (81%) aceste incidente au avut consecințe negative asupra utilizatorilor și dispozitivelor lor (www.kaspersky.com, www.b2binternational.com, www.faravirusi.com). Astfel:

- 12% dintre utilizatori cred că echipamentul lor a fost infectat în urma accesării unui site web compromis
- 8% au menționat ca posibile cauze ale infecției folosirea unui stick de memorie USB care nu le aparține, un alt dispozitiv infectat sau instalarea unui malware deghizat într-un program legitim
- 7% dintre respondenți au declarat că dispozitivele lor au fost infectate în urma deschiderii unui fișier atasat la e-mail
- 13% nu au putut explica cum au ajuns programele malware pe dispozitivul lor

Studiul a arătat că patru din cinci infecții cu malware au cauzat probleme pentru cei afectați (rezultatele obținute în urma utilizării unui chestionar cu răspunsuri multiple):

- 35% din utilizatori s-au confruntat cu diminuarea randamentului echipamentului
- 30% dintre respondenți au observat anunțuri publicitare deranjante (de exemplu, browser-ul îi redirecționa către site-uri nedorite)
- 20% dintre cei intervievați au găsit programe nedorite pe dispozitivele lor
- 17% din cazuri au prezentat modificări la nivelul setărilor browser-ului sau sistemului de operare, efectuate fără cunoștința utilizatorului
- 10% - pierderea datelor cu caracter personal
- 9% - publicarea de mesaje neautorizate sau “like-uri” pe site-uri de socializare
- 8% - furtul datelor cu caracter personal
- 6% - hacking-ul camerei web

Mai mult decât atât, o parte dintre respondenți au fost nevoiți să plătească infractorii cibernetici după ce au fost infectate cu viruși de tip ransomware:

- 11% pentru a debloca dispozitivul

- 6% pentru a decripta fișierele personale

Per total, unul din trei utilizatori (33%) s-a confruntat cu pierderi financiare în urma unui atac malware. Pe lângă plata unei răscumpărări infractorilor, victimele au cheltuit bani pentru deblocarea unui dispozitiv sau a datelor, pentru a achiziționa un software care să elimine efectele infectării sau chiar pentru a cumpăra un dispozitiv nou. În cazurile în care s-au înregistrat pierderi financiare, costul mediu al unui atac s-a ridicat la 160 de dolari.

În ceea ce privește costul lipsei de securitate a ***companiilor*** un studiu pe 5500 de companii din 26 de țări (www.kaspersky.com, www.b2binternational.com, www.faravirusi.com) ne arată că:

- Cele mai costisitoare breșe de securitate sunt fraudele întreprinse de angajați, atacurile de spionaj cibernetic, intruziunile în rețea și deficiențele cauzate de furnizori externi;
- Bugetul mediu necesar pentru remedierea unei breșe de securitate poate ajunge la 551.000$ pentru întreprinderile mari și la 38.000$ pentru companiile mici și mijlocii;
- O breșă gravă în sistemele de securitate IT poate cauza multiple daune afacerii. Dată fiind varietatea posibilelor prejudicii, uneori este dificilă estimarea costurilor totale, chiar și de către victime. Companiile obișnuite trebuie să cheltuiască mai mult pentru servicii specializate (cum ar fi experți IT externi, avocați, consultanți etc.) și câștigă mai puțin ca urmare a oportunităților pierdute sau a perioadei de inactivitate;
- Pe langă cifrele deja menționate, companiile plătesc în medie de la 8.000$ (IMM-uri) la 69.000$ (companii mari) pentru optimizări la nivelul infrastructurii, al personalului și al pregătirii acestuia;
- Factura medie a unei companii afectate de o breșă:
    - Servicii specializate (IT, gestionarea riscului, avocați): până la 84.000$, cu o probabilitate de 88%,
    - Oportunități de business ratate: până la 203.000$, 29%,
    - Perioada de inactivitate: până la 1,4 milioane $, 30%,
    - Media totală: 551.000$,
    - Costuri indirecte: până la 69.000$,
    - Daune aduse reputației: până la 204.750$.

Big Data în detecție și prevenție

În 2015, s-au utilizat mult mai frecvent analizele de securitate folosind infrastructuri de tip "Big Data". Din păcate, creșterea complexității atacurilor cibernetice va conduce implicit la creșterea costurilor asociate cu mitigarea lor. Nimeni nu este imun. De exemplu, un site important este de obicei "testat" de 1 milion de ori în fiecare zi de părți terțe rău voitoare. Pare un număr mare, dar aceste atacuri sunt sesizate rar întrucât același site prelucrează milioane de alte evenimente pe secundă. Există o serie de abordări pentru a combate amenințări cunoscute. Provocarea este de a găsi corelații noi și modele pentru a identifica atacurile sofisticate, cum ar fi phishing și hacktivism.

Analiza de securitate în timp real într-un sistem de tip "Big Data" trebuie să filtreze și să analizeze milioane de evenimente pe secundă dintr-o varietate mare de surse de date, inclusiv surse tradiționale, cum ar fi fișierele jurnal sau de audit, și surse emergente, precum imagini, rețele sociale și e-mail.

Analiza de securitate bazată pe "Big Data" permite organizațiilor să exploateze cantități mari de date — date generate atât în interiorul cât și în afara organizației — și să descopere corelații, să construiască modele de detecție și să elimine amenințările de securitate. Mai mult, aceste rezultate sunt obtinute in timp real.

Predicția atacurilor cibernetice în timp real înseamnă că organizațiile pot descoperi noi amenințări înainte ca acestea să aibă un impact semnificativ și pot reacționa rapid înainte ca acestea să se propage. Scopul, așadar, este de prevenție și protecție.

Și politicile de confidențialitate pot fi îmbunătățite prin analize bazate pe "Big Data". De exemplu, o organizație poate monitoriza traficul Web și fluxurile din rețea. Rezultatul acestei analize poate evidenția exact care dintre serverele Web au fost infectate cu malware, să identifice domeniile suspecte, să detecteze scurgeri de documente și să identifice tipare de acces neautorizat.

Evoluția sistemelor de analiză în domeniul securității cibernetice:

- prima generație: sisteme de detectare a intruziunilor
- a doua generație: folosirea de sisteme de management al incidentelor și evenimentelor de securitate (SIEM)
- a treia generație: analiză de tip "Big Data" cuplată cu inteligența artificială (Machine Learning) - SIEM II

Prima generație (sisteme de detectare a intruziunilor) și-a atins limita atunci când oamenii au realizat că protejarea completă a unui sistem nu era posibilă. Nu există nicio modalitate de protejare perfectă a unui sistem. Sistemele de detectare a intruziunilor sunt în continuu dezvoltate de aproape trei decenii. Primele au fost foarte specifice, un fel de extensie a firewall-urilor. Ele folosesc pentru detecție semnături, bazându-se pe acestea pentru detectarea intruziunilor sau infecțiilor cu malware. Principala problema a acestor sisteme o reprezinta numărul mare de alerte false.

Pentru ca volumul și varietate de informații care trebuie să fie agregate și corelate au crescut foarte mult și pentru limitarea numărului de alarme false, au fost proiectate **sistemele de generația a doua (SIEM)**. S-au dezvoltat, de asemenea, astfel centre de operațiuni de securitate, capabilități în care se pot urmări centralizat toți indicatorii de securitate dintr-o rețea. La nivelul acestor centre, pe baza datelor colectate, se pot modela tendințe specifice.

Cea de **a treia generație** poate acomoda formate de date noi și permite analize pe date nestructurate cum ar fi conținut Web sau "mesaje Tweeter". Analiza datelor nestructurate este foarte dificilă pentru sistemele SIEM clasice.

Principalul avantaj al "Big Data" şi NoSQL este că acestea pot stoca date în structuri scalabile, permițând, în același timp, crearea de interogări specifice.

"Big Data" permite, de exemplu, investigația incidentelor de securitate prin *analiza tendințelor pe termen lung* folosind date istorice. Prin colectarea datelor pe scară largă și analizând tendințe istorice, se poate identifica când a început un atac și care au fost pașii pe care atacatorul i-a executat pentru a prelua controlul unui sistem. Chiar dacă nu a fost detectat atacul original de către sistemele clasice, analizând datele istorice putem identifica și contracara repetarea acestuia.

O altă caracteristică importantă este *eficiența interogărilor*. Atunci când se dorește identificarea de corelații, "Big Data" permite efectuarea de interogări complexe și generarea rezultatelor într-un timp rezonabil.

"Big Data" este abia la început, mai multe companii construind acum asemenea sisteme de analiză. Prin folosirea acestora se realizează evoluția de la metoda clasică de analiză descriptivă la analiza predictivă (orientată pe viitor, pe ceea ce urmează să se întâmple).

Diferențele dintre sistemele clasice și cele bazate pe “Big Data”, cum ar fi sistemul Hadoop pentru procesare distribuită în "batch-uri" și transformarea datelor în timp real pe măsură ce acestea ajung la sistem ("streaming data/ processing") sunt determinate de tehnologiile pe care sunt construite.

Intersecția dintre **ML ("Machine Learning") şi securitatea IT** se concentrează pe analiza datelor fără a se limita la generarea de rapoarte. ML permite o analiză automatizată și avansată a datelor putând să detecteze proverbialul "ac în carul cu fan", adică comportamentul anormal într-o cantitate uriașa de informații.

"Machine Learning", precum și "Big Data", câștigă popularitate datorită utilizării sale pe scară largă în multe companii de tehnologie din întreaga lume. Asemenea instrumente sunt folosite în sisteme ce tranzacționează volume mari de date (de exemplu, Netflix, Amazon), filtrele de spam (de exemplu Google) şi multe alte aplicații.

Dintr-o perspectivă cibernetică, *modelele generate trebuie să aibă putere predictivă*, să distingă automat între traficul de rețea normal și cel generat de o persoană potențial rău intenționată, care poate fi un indicator al unei infecții active, atac cibernetic sau malware. "Machine Learning" poate fi folosit pentru a construi clasificări, în scopul modelării și de a oferi un răspuns binar (de exemplu, bun sau rău) la traficul de rețea analizat.

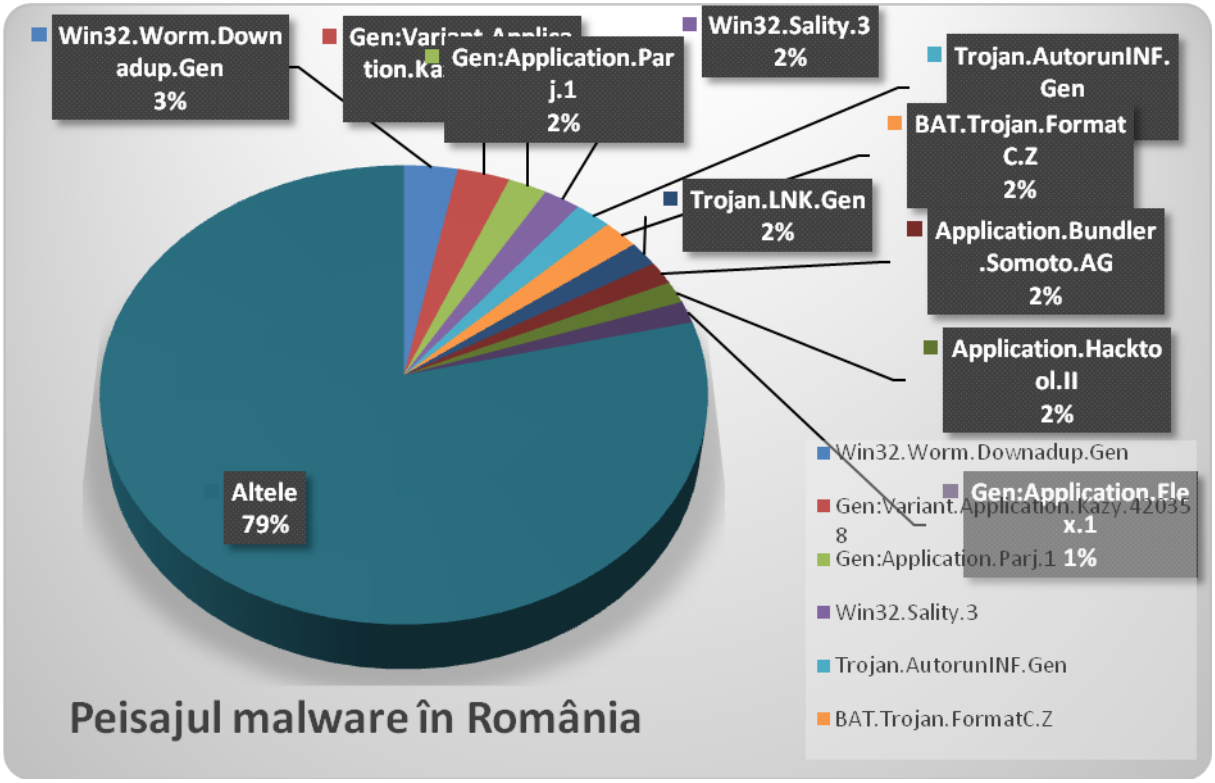
Peisajul local

Date malware

Cele mai notabile amenințări informatice la adresa utilizatorilor de Internet din România au fost virușii de tip crypto-ransomware și troienii bancari.

- Versiunea 3 a troianului ***Tinba***, precum și cele mai recente iterații ale familiei ***Dridex*** sunt două exemple de troieni bancari special concepuți pentru piața de e-banking din România. Aceste familii de viruși care, în trecut, activau pe piața internațională (USA, Franța, Germania), au fost modificate pentru a intercepta tranzacții pe portalurile de e-banking ale principalilor jucători bancari din România.

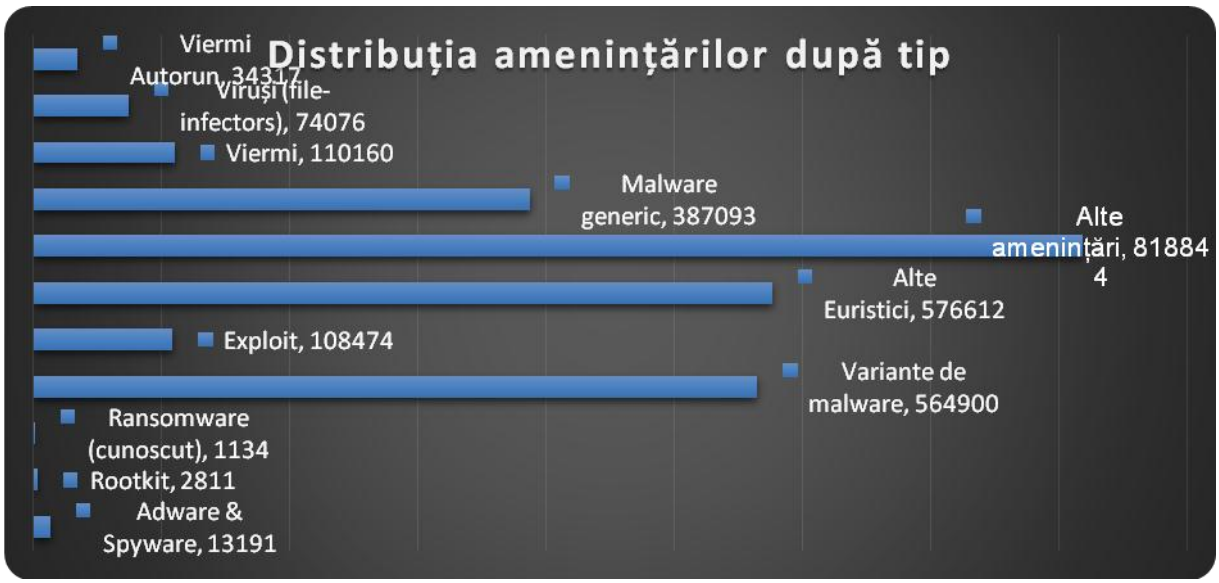
- Telemetria specialiștilor poziționează ***Win32.Worm.Downadup pe primul loc în amenințările informatice care au vizat România*** în prima jumătate a anului 2015 (www.bitdefender.ro).



- O apariție notabilă în topul amenințărilor informatice o reprezinta ***Win32.Sality***, un virus extrem de longeviv, care infectează fișiere executabile, apoi instalează un component de tip backdoor ce perimte accesul hackerilor. Botnet-ul Sality cuprinde peste un milion de calculatoare la nivel global și e activ din 2003.

- ***Trojan.AutorunINF*** și ***Win32.Worm.Downadup*** sunt două familii de malware care au supraviețuit din epoca Windows XP. Ambele amenințări sunt strict legate de această platformă și nu pot infecta calculatoare ce rulează sisteme de operare scoase pe piață după Windows XP. Acest lucru este posibil din cauza faptului că, în România, cota de piață a

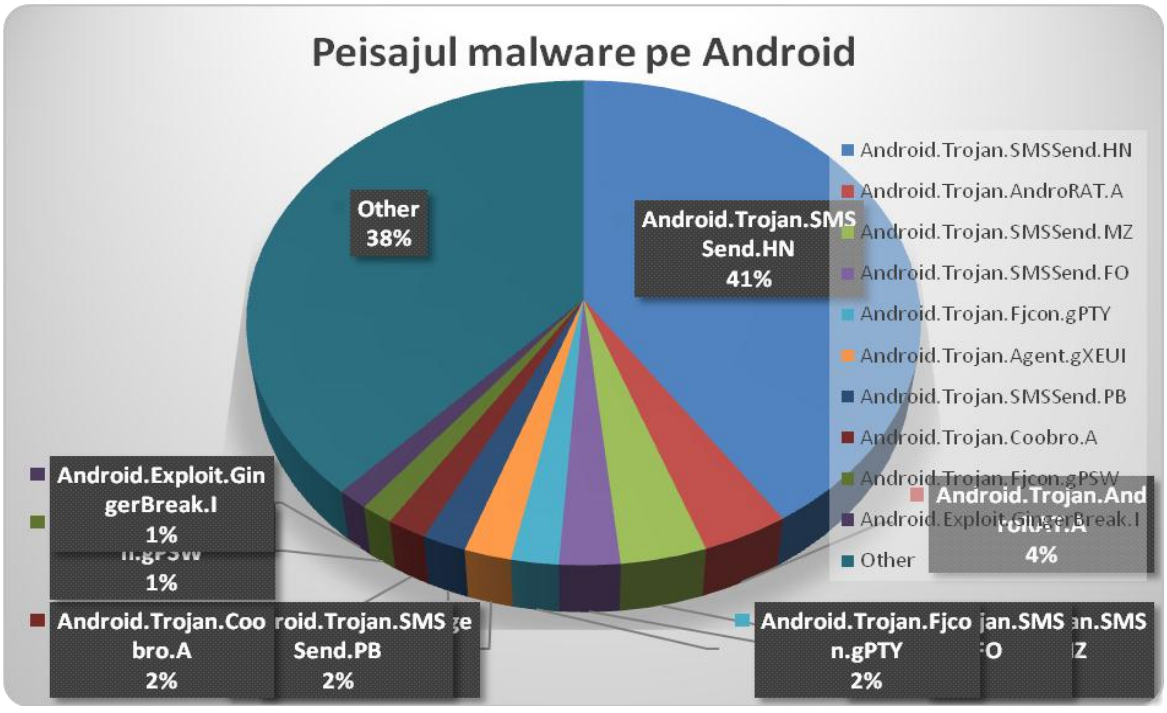
Windows XP s-a micșorat relativ puțin pe parcursul anului 2015, coborând doar 3.72 procente (de la 17.3% în ianuarie la 13.58% în septembrie).



Notă: ransomware-ul necunoscut e detectat comportamental și intră în categoria “Alte Euristici”.

Malware pe mobile

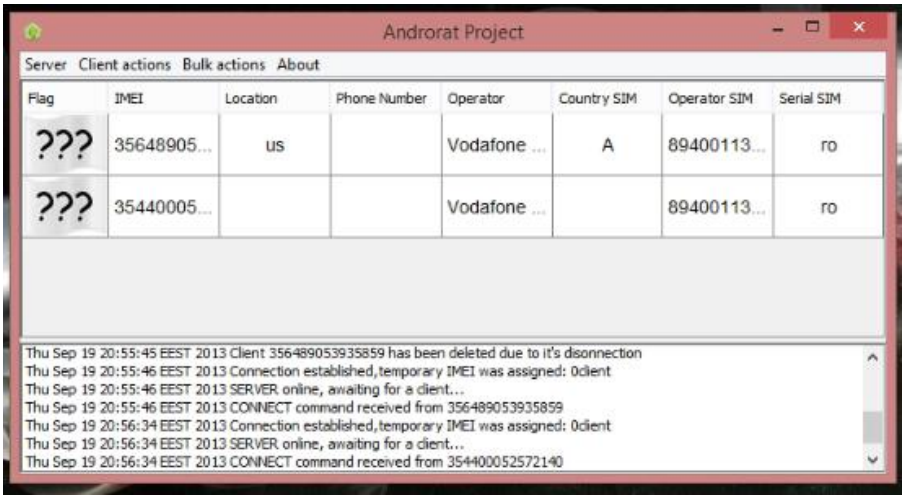
Terminalele mobile care rulează Android au devenit o țintă predilectă a atacatorilor. Principalele amenințări care au dominat topul malware în prima jumătate a anului 2015 sunt troienii care trimit mesaje la numere cu suprataxă (Android.Trojan.SMSSend.HN, Android.Trojan.SMSSend.MZ, Android.Trojan.SMSSend.FO șiAndroid.Trojan.SMSSend.PB), precum și instrumente de spionaj din familia AndroRAT (Android.Trojan:AndroRAT.A).



- ***Troienii de fraudă cu mesaje scurte la numere cu suprataxă însumează 49,18%*** din totalul amenințărilor informatice pe Android. Acești troieni sunt, de obicei, injectați în jocuri sau aplicații comerciale, apoi sunt distribuiți pe forumuri sau site-uri de torrente de unde pot fi descărcați în mod gratuit. Odată ce au fost instalate, aceste aplicații vor trimite mesaje premium pentru a abona victimele la diverse servicii care trimit mesaje contra cost (horoscop).

- ***Pe locul doi în topul celor mai frecvent întâlnite amenințări se află AndroRAT***, un instrument de acces de la distanță care permite unui atacator să preia controlul asupra funcțiilor importante ale dispozitivului. Inițial dezvoltat ca proiect educațional, AndroRAT a fost adaptat pentru a fi injectat în aplicații legitime, apoi diseminat prin market-uri terțe, unde aplicațiile nu sunt verificate.

Panou de comandă și control AndroRAT:



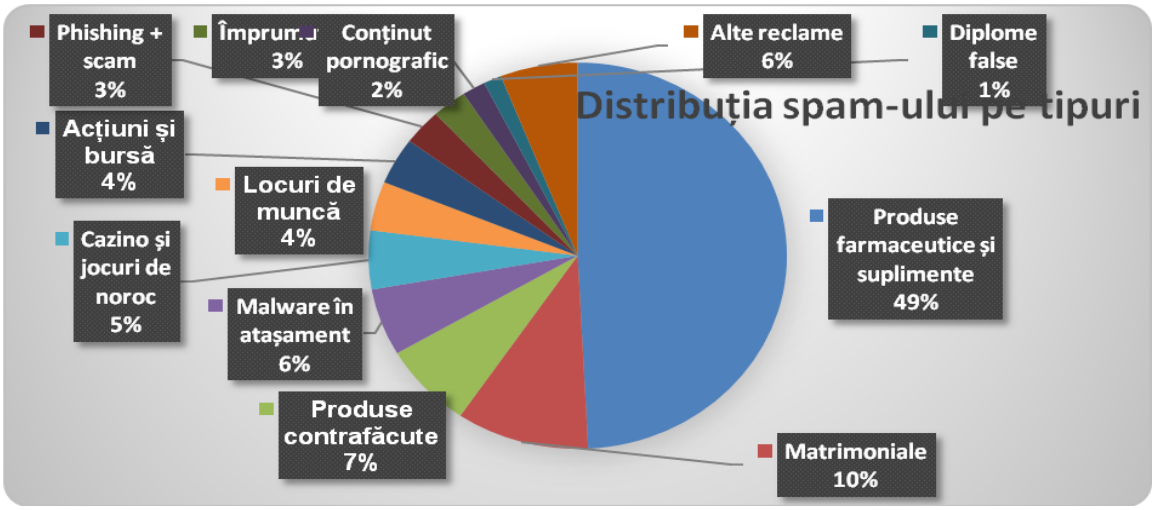
Spam

Distribuția mesajelor de tip spam pe tipuri a rămas relativ constantă în perioada ianuarie – iunie 2015, cu mici diferențe la nivel procentual.

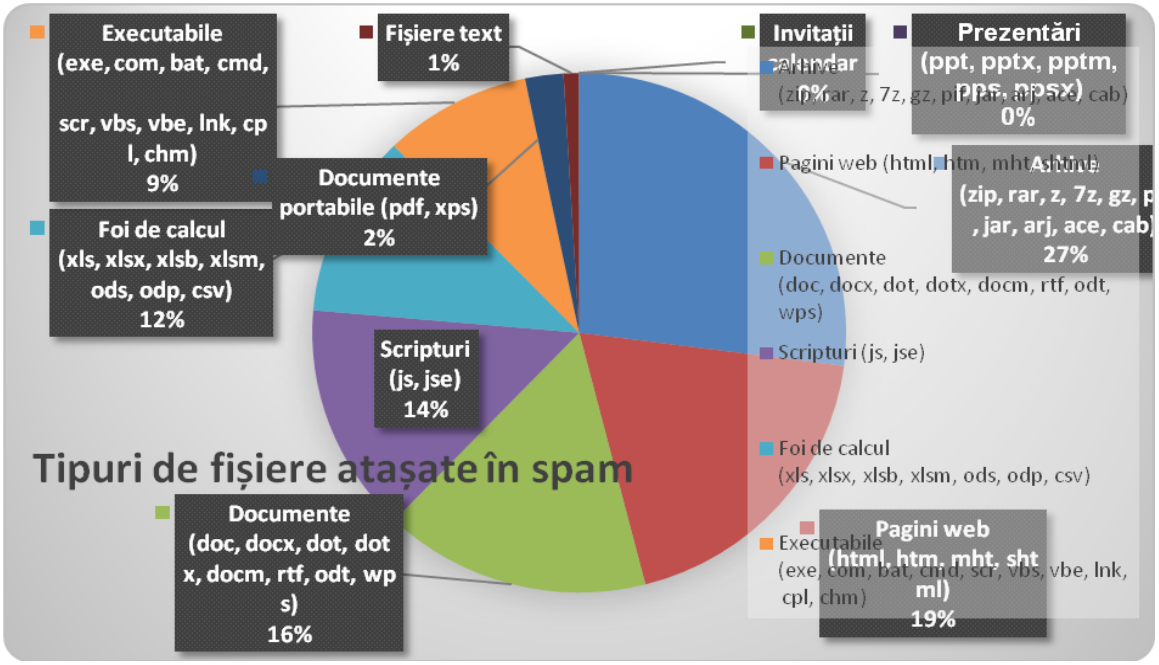
- ***Pe locul 1***, aproximativ jumătate din totalul mesajelor nesolicitate plasează ***produse farmaceutice și suplimente alimentare***.

- ***Pe locul 2*** ca volum se situează mesajele care promovează ***site-uri de matrimoniale***. Spam-ul axat pe matrimoniale a cunoscut o creștere ușoară în ultimul an (10.3% față de 6.8%).

- ***Pe locul 3,*** mesajele nesolicitate ce promovează ***produse contrafăcute*** au scăzut ca procent față de a doua jumătate a anului 2014 (7.1% față de 13.40%), dar activitatea în acest segment crește o dată cu apropierea sărbătorilor de iarnă.



- ***Mesajele infectate ocupă locul 4*** în topul celor mai frecvent întâlnite tipuri de spam. Mai bine de cinci procente din mesajele analizate de Bitdefender conțin atașamente malware, o creștere semnificativă față de a doua jumătate a anului 2014 (3.2%). Această creștere e alimentată de grupările care operează rețele de crypto-ransomware și troieni bancari, cele mai frecvente amenințări care se răspândesc prin intermediul e-mail-ului.

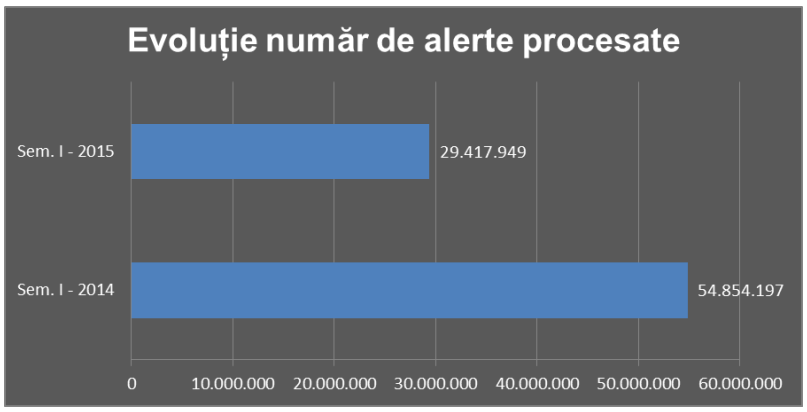


Alerte CERT.ro

În perioada 01.01.2015 – 30.06.2015, la CERT-RO au fost primite sesizări (alerte), astfel:

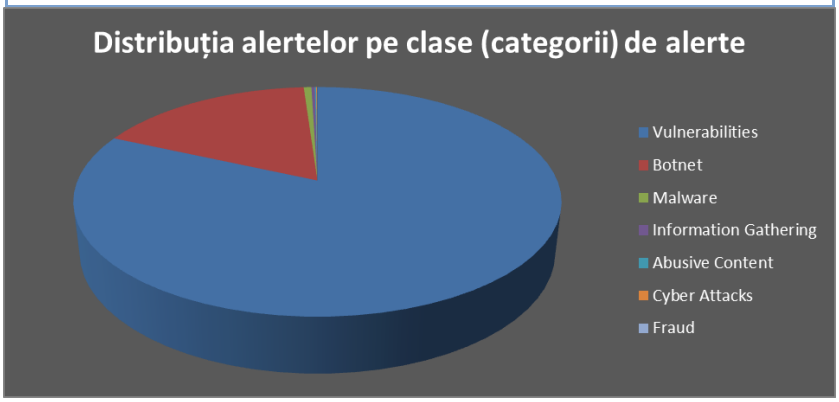
- Număr total de alerte procesate: 29.417.949 (automate: 29.417.302, alerte colectate manual: 647);
- Număr total de IP-uri unice extrase din totalul alertelor: 1.717.304.

Numărul alertelor primite de CERT-RO în prima jumătate a anului 2015, a scăzut cu 46% (29.417.949) față de prima jumătate a anului 2014 (54.854.197), scăderea fiind expusă în tabelul de mai jos.



Distribuția primelor 7 tipuri de alerte primite, pe clase de alerte:

Nr.	*Clasă alerte*	*Număr alerte*	*Procent*
1	Vulnerabilities	24.037.554	81,71 %
2	Botnet	5.061.753	17,21 %
3	Malware	178.958	0,61 %
4	InformationGathering	78.828	0,27 %
5	AbusiveContent	31.400	0,11 %
6	CyberAttacks	24.027	0,08 %
7	Fraud	5.413	0,02 %



Tipuri de malware caracteristice spațiului cibernetic românesc (identificarea tipului de malware a fost posibilă în 17% din numărul alertelor primite):

Nr. Crt.	*Tip Malware*	*Procent (%)*
1	Downadup	48,73 %
2	ZeroAccess	12,28 %
3	Sality	9,39 %
4	Virut	8,41 %
5	Ramnit	7,83 %

6	Zeus	2,82 %
7	Conficker	0,64 %
8	Citadel	0,62 %
9	Kins	0,50 %
10	Pushdo	0,35 %

Distribuția detaliată a alertelor pe clase și tipuri:

Nr.	*Clasa alerte*	*Tip alertă*	*Alerte manuale*	*Alerte automate*	*Total*	*Procent*
1	Vulnerabilities	SSL POODLE	0	7218138	7218138	24,54
2	Vulnerabilities	VulnerableNTP	0	5665385	5665385	19,26
3	Botnet	BotnetDrone	32	5060033	5060065	17,20
4	Vulnerabilities	OpenResolver	0	4996489	4996489	16,98
5	Vulnerabilities	OpenSSDP	0	1877859	1877859	6,38
6	Vulnerabilities	OpenNetBIOS	0	1274440	1274440	4,33
7	Vulnerabilities	OpenSNMP	0	1159835	1159835	3,94
8	Vulnerabilities	FREAK	0	804709	804709	2,74
9	Vulnerabilities	OpenIPMI	0	372086	372086	1,26
10	Vulnerabilities	OpenNATPMP	0	287705	287705	0,98
11	Vulnerabilities	OpenMsSql	0	230124	230124	0,78
12	Malware	MaliciousUrl	100	178721	178821	0,61
13	Information Gathering	Scanner	96	78730	78826	0,27
14	Vulnerabilities	OpenChargen	0	41588	41588	0,14
15	Vulnerabilities	Open NAT PMP	0	36087	36087	0,12
16	AbusiveContent	Spam	25	31372	31397	0,11
17	Vulnerabilities	NetisVulnerability	0	23856	23856	0,08
18	CyberAttacks	Bruteforce	9	23460	23469	0,08
19	Vulnerabilities	OpenQOTD	0	18163	18163	0,06
20	Vulnerabilities	OpenMongodb	0	17233	17233	0,06
21	Vulnerabilities	OpenRedis	0	10596	10596	0,04
22	Fraud	Phising	192	5217	5409	0,02
23	Vulnerabilities	OpenProxy	0	3236	3236	0,01
24	Botnet	BotnetCCServer	4	1684	1688	0,01
25	CyberAttacks	APT	1	502	503	0,00
26	Malware	InfectedIP	105	30	135	0,00
27	CyberAttacks	ExploitAttempt	35	0	35	0,00
28	Vulnerabilities	OpenElasticsearch	0	22	22	0,00
29	CyberAttacks	DDoS	20	0	20	0,00
30	Compromised Resources	Compromised Network/System	9	0	9	0,00

31	Compromised Resources	Compromised Website	4	0	4	0,00
32	Fraud	UnlawfuleCommerce/ Services	3	0	3	0,00
33	Compromised Resources	Compromised Router	1	2	3	0,00
34	AbusiveContent	DisclosureOf ConfidentialData	3	0	3	0,00
35	Malware	MalwareSample	2	0	2	0,00
36	Information Gathering	SocialEngineering	2	0	2	0,00
37	Vulnerabilities	OpenDB	2	0	2	0,00
38	Fraud	FinancialFraud	1	0	1	0,00
39	Vulnerabilities	ExposedPLC	1	0	1	0,00
	TOTAL		**647**	**29.417.302**	**29.417.949**	100,00%

Cadrul legal și instituțional

Creșterea nivelului de securitate cibernetică implică acțiuni pe mai multe planuri:

- Organizațiile par să își fi îmbunătățit capabilitățile prin adoptarea unor unelte mai sofisticate pentru prevenirea atacurilor și reducerea impactului lor, dar și prin achiziționarea de competențe tehnice conexe.
- La rândul lor, vendorii de tehnologie sunt de asemenea mai atenți către găsirea și rezolvarea vulnerabilităților în produsele proprii, oferind atacatorilor mai puține oportunități.
- Vendorii de soluții de securitate tind să formeze coaliții, prin care aceștia își pun în comun capabilități complementare pentru a putea realiza soluții de securitate capabile să facă față unor atacuri din ce în ce mai sofisticate. Posibil ca în viitorul imediat să asistăm chiar la o migrare spre o arhitectură de apărare integrată.
- Cadrul legal evoluează și tratează întreaga complexitate a securității cibernetice, cu teme aparte cum ar fi, de exemplu:
    - Atacuri transfrontaliere, intersectând arii cu legislații diferite, de exemplu: inițiate dintr-un stat non-UE, folosind o infrastructură dintr-un alt stat non-UE și care afectează sistemele informatice dintr-un stat UE
    - Infracțiunile cibernetice nu trebuie să fie tratate independent de acțiunile din lumea reală – ciclul infracțiunii pornește din lumea reală, poate avea o verigă/etapă/componentă sau mai multe cu desfășurare în mediul online, în final însă consecințele se manifestă în mediul fizic
    - Asigurarea că instituțiile responsabile cu apărarea intereselor cetățenilor au acces la instrumente și mecanisme digitale cu măcar același nivel de sofisticare ca și cele ale atacatorilor
- Cadrul instituțional care definește rolurile și responsabilitățile actorilor implicați
- Cadrul de cooperare public-privat, cultura de colaborare

În cele ce urmează, vom analiza direcțiile de acțiune așa cum sunt ele stabilite prin strategia de securitate cibernetică a UE și proiectul de directivă NIS, precum și principalii pași făcuți în acest sens în România. De asemenea, vom trata probabil cea mai spinoasă temă a momentului – confidențialitatea datelor.

Strategia de securitate cibernetică a Uniunii Europene (www.consilium.europa.eu)

Strategia de securitate cibernetică stabilește abordarea UE privind cea mai bună modalitate de prevenire și reacție la perturbările și atacurile cibernetice. Strategia detaliază o serie de acțiuni pentru a consolida reziliența cibernetică a sistemelor informatice, a reduce criminalitatea informatică și a consolida politica internațională a UE în materie de securitate cibernetică și apărarea cibernetică.

Pentru ca spațiul cibernetic să rămână deschis și liber, aceleași norme, principii și valori pe care Uniunea Europeană le susține offline ar trebui să se aplice și online. Drepturile fundamentale și democrația au nevoie de protecție în spațiul cibernetic. Libertatea și prosperitatea noastră depind din ce în ce mai mult de un internet robust și inovator, iar acesta va continua să se dezvolte dacă

inovațiile din sectorul privat și societatea civilă îi vor sprijini creșterea. Libertatea online presupune însă deopotrivă siguranță și securitate. Spațiul cibernetic ar trebui să fie protejat de incidente, activități rău intenționate și utilizare abuzivă. Administrațiile naționale joacă un rol semnificativ în asigurarea unui spațiu cibernetic liber și sigur. Ele au mai multe sarcini: să salvgardeze accesul și deschiderea, să respecte și să protejeze drepturile fundamentale online și să mențină fiabilitatea și interoperabilitatea internetului. Sectorul privat deține și exploatează însă o parte semnificativă a spațiului cibernetic și, prin urmare, orice inițiativă care dorește să aibă succes în domeniu trebuie să recunoască rolul central jucat de acesta.

Tehnologia informației și comunicațiilor (TIC) a devenit coloana vertebrală a creșterii economice și reprezintă o resursă de importanță majoră pe care se bazează toate sectoarele economiei. TIC stă în prezent la baza sistemelor complexe care asigură funcționarea economiilor noastre, în sectoare cheie cum ar fi finanțele, sănătatea, energia și transporturile, în timp ce multe modele comerciale sunt construite pornind de la premiza disponibilității neîntrerupte a internetului și a bunei funcționări a sistemelor informatice.

Priorități strategice:

- realizarea rezilienței cibernetice;
- reducerea drastică a criminalității cibernetice;
- dezvoltarea politicii și a capacităților de apărare cibernetică legate de politica de securitate și apărare comună (PSAC)
- dezvoltarea resurselor industriale și tehnologice în materie de securitate cibernetică;
- instituirea unei politici internaționale coerente a Uniunii Europene privind spațiul cibernetic și promovarea valorilor fundamentale al UE.

Una dintre principalele acțiuni ale strategiei este proiectul de directivă privind securitatea rețelelor și a informației.

Proiectul de directivă NIS

Proiectul de directivă privind securitatea rețelelor și a informației (NIS) este un element important al strategiei de securitate cibernetică. Aceasta ar impune tuturor statelor membre ale UE, principalilor operatori de internet și operatori de infrastructură, cum ar fi platformele de comerț electronic, rețelele sociale și serviciile de transport, serviciile bancare și serviciile de asistență medicală, să garanteze un mediu digital sigur și de încredere în întreaga UE. Având în vedere că actuala abordare a NIS se bazează pe acțiunea voluntară, capacitățile naționale și gradul de implicare și pregătire al sectorului privat variază considerabil de la un stat membru la altul. Proiectul de directivă vizează crearea unor condiții de concurență echitabile prin introducerea unor norme armonizate care să se aplice în toate țările UE.

Măsurile propuse includ:

- cerința ca statele membre ale UE să adopte o strategie privind NIS și să desemneze o autoritate NIS națională care să dispună de resurse adecvate pentru a preveni, gestiona și soluționa riscurile și incidentele NIS;

- crearea unui mecanism de cooperare între statele membre și Comisie pentru a transmite alertele timpurii referitoare la riscuri și incidente, a face schimb de informații și a contracara amenințările și incidentele legate de NIS;
- cerința pentru anumite societăți și servicii digitale să adopte practici de gestionare a riscurilor și să raporteze incidentele majore de securitate informatică autorității naționale competente.

Cerința de a raporta incidente de securitate informatică urmărește să dezvolte o cultură a gestionării riscurilor și să asigure că informațiile sunt partajate între sectoarele public și privat. Cerința include:

- operatorii infrastructurilor critice din anumite sectoare, cum ar fi servicii financiare, transporturi, energie și sănătate;
- societăți de servicii informatice, inclusiv magazine de aplicații, platforme de comerț electronic, platforme de plăți pe internet, platforme de cloud computing, motoare de căutare și rețele sociale;
- administrații publice.

Pe plan național au fost elaborate mai multe acte normative, pe paliere diferite (strategii, legi, hotărâri ale guvernului), unele atingând nivelul de maturizare, altele necesitând adaptări suplimentare.

Strategia de Securitate cibernetică a României (HG nr.271/2013)

Stabilește 4 direcții majore de acțiune:

1. Stabilirea cadrului conceptual, organizatoric şi acţional necesar asigurării securităţii cibernetice

- constituirea şi operaţionalizarea unui sistem naţional de securitate cibernetică;
- completarea şi armonizarea cadrului legislativ naţional în domeniu, inclusiv stabilirea şi aplicarea unor cerinţe minimale de securitate pentru infrastructurile cibernetice naţionale;
- dezvoltarea cooperării între sectorul public şi cel privat, inclusiv prin stimularea schimbului reciproc de informaţii, privind ameninţări, vulnerabilităţi, riscuri, precum şi cele referitoare la incidente şi atacuri cibernetice.

2. Dezvoltarea capacităţilor naţionale de management al riscului în domeniul securităţii cibernetice şi de reacţie la incidente cibernetice în baza unui program naţional, vizând:

- consolidarea, la nivelul autorităţilor competente potrivit legii, a potenţialului de cunoaştere, prevenire şi contracarare a ameninţărilor şi minimizarea riscurilor asociate utilizării spaţiului cibernetic;
- asigurarea unor instrumente de dezvoltare a cooperării dintre sectorul public şi cel privat, în domeniul securităţii cibernetice, inclusiv pentru crearea unui mecanism eficient de avertizare şi alertă, respectiv de reacţie la incidentele cibernetice;
- stimularea capabilităţilor naţionale de cercetare, dezvoltare şi inovare în domeniul securităţii cibernetice;
- creşterea nivelului de reziliență a infrastructurilor cibernetice;
- dezvoltarea entităţilor de tip CERT, atât în cadrul sectorului public, cât şi în sectorul privat.

3. Promovarea şi consolidarea culturii de securitate în domeniul cibernetic
- derularea unor programe de conştientizare a populaţiei, a administraţiei publice şi a sectorului privat, cu privire la ameninţările, vulnerabilităţile şi riscurile specifice utilizării spaţiului cibernetic;
- dezvoltarea de programe educaţionale, în cadrul formelor obligatorii de învăţământ, privind utilizarea sigură a internetului şi a echipamentelor de calcul;
- formarea profesională adecvată a persoanelor care îşi desfăşoară activitatea în domeniul securităţii cibernetice şi promovarea pe scară largă a certificărilor profesionale în domeniu;
- includerea unor elemente referitoare la securitatea cibernetică în programele de formare şi perfecţionare profesională a managerilor din domeniul public şi privat.

4. Dezvoltarea cooperării internaţionale în domeniul securităţii cibernetice
- încheierea unor acorduri de cooperare la nivel internaţional pentru îmbunătăţirea capacităţii de răspuns în cazul unor atacuri cibernetice majore;
- participarea la programe internaţionale care vizează domeniul securităţii cibernetice;
- promovarea intereselor naţionale de securitate cibernetică în formatele de cooperare internaţională la care România este parte.

Strategia de Securitate cibernetică definește, de asemenea, Sistemul naţional de securitate cibernetică (SNSC), cadrul general de cooperare care reuneşte autorităţi şi instituţii publice, cu responsabilităţi şi capabilităţi în domeniu, în vederea coordonării acţiunilor la nivel naţional pentru asigurarea securităţii spaţiului cibernetic, inclusiv prin cooperarea cu mediul academic şi cel de afaceri, asociaţiile profesionale şi organizaţiile neguvernamentale.

Misiunea SNSC constă în asigurarea elementelor de cunoaştere, prevenire şi contracarare a ameninţărilor, vulnerabilităţilor şi riscurilor specifice spaţiului cibernetic care pot afecta securitatea infrastructurilor cibernetice naţionale, inclusiv managementul consecinţelor.

Pentru îndeplinirea obiectivelor prezentei strategii, SNSC funcţionează ca un mecanism unitar şi eficient de relaţionare şi cooperare interinstituţională, în vederea adoptării şi aplicării cu celeritate a deciziilor.

Funcţiile principale ale SNSC se realizează prin informare, monitorizare, diseminare, analizare, avertizare, coordonare, decizie, reacţie, refacere şi conştientizare, precum şi prin adoptarea de măsuri proactive şi reactive.

Coordonarea SNSC se realizeaza de către Consiliul operativ de securitate cibernetică (COSC).

Suveranitatea, localizarea și confidențialitatea datelor

Suveranitatea datelor (conceptul care spune că datele se supun jurisdicției țării în care sunt localizate și nu a guvernelor străine sau tribunalelor care pot căuta acces unilateral la ele) și localizarea datelor (obligații legale pentru ca datele să fie depozitate într-o anumită locație) au devenit probleme aprinse.

Unele țări au început să caute modalități de a-și localiza datele ca o modalitate de a preveni accesul guvernelor străine la datele cetățenilor și compun cerințe care specifică faptul că datele rămân în țara lor, iar companiile folosesc echipament produs local.

O consecință potențial negativă a inițiativelor care obligă localizarea datelor – creând legislație care nu este interoperabilă – este că toate companiile multinaționale pot fi supuse unor cerințe legale conflictuale. O obligație de a se supune cererilor unei țări de a produce, reține sau distruge date poate viola cererile unei alte țări.

În afară de riscul de a crea obligații legale conflictuale, cerințele localizării datelor are potențialul de a limita fluxul de date peste granițe. Asta poate crea confuzie, dar și provocări semnificative în administrarea rețelelor. Este un aspect al lanțului de aprovizionare și aici: mai mulți operatori ai lanțului de aprovizionare global adoptă tehnologii bazate pe cloud pentru a-i conecta pe toți partenerii din lume. Localizarea datelor ar putea împiedica sau preveni schimbul de date în acele rețele și activitățile peste hotare ar putea fi vulnerabile la criminalitatea cibernetică. În plus, unele țări aleg să folosească numai tehnologii natale, sau plasează restricții semnificative privind persoanele care pot manevra datele cetățenilor, apărând riscul de a se izola singure de grupul de talente global și pot risca astfel o pierdere a inovației aduse de contactul cu idei noi. Câteva companii tehnologice de top din Statele Unite speră că folosirea criptării end-to-end va fi o cale de satisfacere a grijilor clienților cu privire la datele lor personale în spațiul web.

Atitudinea unei persoane sau organizații când vine vorba de confidențialitatea datelor poate varia în funcție de locul din lume în care se află. Aceste puncte de vedere variate afectează felul în care guvernele gestionează confidențialitatea datelor și felul în care întreprinderile fac afaceri atunci când aceste reglementări se contrazic.

Discuția legată de compatibilitatea confidențialității datelor – adică crearea abordărilor globale consistente – a devenit mai urgentă datorită creșterii serviciilor cloud. Spre exemplu, dacă o companie bazată în SUA cumpără cloud storage de la o companie din India și îl folosește pentru a stoca date pentru clienți cu domiciliul în Germania, legile cărui țări se aplica?

Alte drivere a compatibilității confidențialității datelor sunt Internetul Lucrurilor (IoT) și Big Data. Pe măsură ce întreprinderile iau în considerare noi modalități de a conecta dispozitive și folosesc seturi masive de date pentru a lua decizii profesionale, au nevoie de structură și reguli pentru felul în care aceste date pot fi manevrate la scară globală.

Diverse eforturi au fost lansate pentru armonizarea cerințelor legate de confidențialitatea datelor pe teritoriul unei regiuni sau grup de țări. Spre exemplu, legislația Uniunii Europene este modificată în prezent și va actualiza structura actuală de protecție a datelor – Reglementarea privind protecția datelor generale, cerând o armonizare a reglementărilor privind confidențialitatea datelor. Se intensifică eforturile pentru a ajunge la un acord privind confidențialitatea datelor și armonizare a legilor legate de suveranitatea datelor. O astfel de armonizare mai bună ar fi binevenită, dar este de asemenea important ca textul final sa fie în acord cu celelalte regiuni și să respecte realitatea tehnologiilor. Regiunea Asia-Pacific a dezvoltat Acordul privind impunerea confidențialității peste granițe din cadrul Cooperării Economice Asia-Pacific (APEC), care facilitează împărțirea datelor în economiile locale. Mai multă muncă trebuie depusă de guverne în scopul creării de regimuri

compatibile pentru confidențialitatea datelor și securitate, ancorate în standarde recunoscute global care promovează un internet deschis cu transmisii libere de date peste granițe naționale și regionale.

Pe măsură ce țările și regiunile clarifică abordările privind confidențialitatea datelor, întreprinderile vor fi capabile să aplice practici de confidențialitate consistente la nivel global și vor implementa sisteme eficiente de confidențialitate ”by design”, în care capacitățile sunt integrate în produse și servicii de la început. Sisteme reglementate de confidențialitate, clare și consistente, ar ajuta companiile să îndeplinească și depășească cerințele de confidențialitate, fără a se ține cont de locația unde se aplică oferta, astfel încurajând dezvoltarea produselor inovative și folosirea datelor.

În urma sondajului privind protecția datelor realizat de experți globali în confidențialitate din America de Nord, Uniunea Europeană și regiunea Asia-Pacific despre reglementările de date din regiunile lor, practici guvernamentale, conținutul utilizatorilor și standardele de securitate, răspunsurile au arătat un nivel ridicat de consistență în înțelegerea sensului de confidențialitate a datelor și valoarea standardelor globale de confidențialitate.

- Rezidența și suveranitatea datelor: răspunzătorii au identificat datele personale și informațiile de identificare personale (PII) ca datele care trebuie să rămână în țara de origine;
- Interceptarea legală: răspunzătorii au arătat o interpretare universală a modurilor în care datele pot fi interceptate – spre exemplu, când sunt necesare într-o investigație penală;
- Conținutul utilizatorului: 73% din răspunzători au fost de acord că trebuie o declarație a drepturilor privind confidențialitatea consumatorilor care este globală, nu regională. 65% au afirmat că Națiunile Unite ar trebui să joace un rol activ în crearea unei asemenea declarații;
- Principii de confidențialitate: răspunzătorii au fost întrebați dacă principiile de confidențialitate de la Organizația pentru Cooperare Economică și Dezvoltare ar facilita armonizarea datelor, sau ar crea tensiuni mai mari. Experții participanți la sondaj erau în favoarea adoptării acestor principii.

În rezumat, sondajul privind confidențialitatea datelor arată că experții sunt de acord în privința principiilor de bază care, dacă ar fi adoptate la scară globală, ar putea înlesni afacerile. Rezultatele indică și faptul că experții au un interes comun în ”coacerea” acestor principii de confidențialitate pentru soluții tehnologice noi, în loc să se încerce modificarea lor pentru a acomoda cerințele. Însă, actualele sisteme de reglementări privind confidențialitatea sunt relativ noi și se dezvoltă rapid.

Recomandări

1. Întregirea cadrului legal în domeniul securității cibernetice, asigurându-se compatibilitatea cu cadrul UE și NATO cu accent pe:
    a. Operaționalizarea Sistemului Național de Securitate Cibernetică (SNSC);
    b. Definirea criteriilor de clasificare a infrastructurilor;
    c. Stabilirea mecanismelor, rolurilor și procedurilor care vor permite o reacție rapidă în cazul identificării unor incidente de securitate la nivelul unei infrastructuri critice;
    d. Asigurarea eficienței acțiunilor instituțiilor abilitate prin eliminarea unor bariere procedural;
    e. Asigurarea accesului instituțiilor responsabile la instrumente cibernetice cu măcar același nivel de sofisticare ca și cele aflate la dispoziția atacatorilor.

2. Introducerea de-a lungul verticalelor în care regăsim infrastructuri critice a unor elemente de reglementare care să asigure dezvoltarea sau achiziționarea de competențe și capabilități tip CERT

3. O lege și normele tehnice aferente privind infrastructurile de tip Cloud:
    a. Condițiile minime de securitate;
    b. Modalitățile de acces;
    c. Rolurile în gestionarea cloud-ului;
    d. Principiul “cloud first”.

4. Un cadru normativ care să trateze:
    a. Definirea, actualizarea și garantarea unui set de condiții tehnice minime (de referință) de securitate pentru sistemele informatice, raportat la natura informațiilor gestionate și tranzacționate;
    b. Evidențierea transparentă a costurilor pentru securitatea sistemelor și subsistemelor cibernetice;
    c. SLA-uri cadru, prin care vendorii de tehnologie și integratorii își asumă răspunderea și oferă garanții privind securitatea echipamentelor și aplicațiilor, inclusiv absența backdoor-urilor “voluntare”.

5. În contextul unei reorganizări prin introducerea unui nivel de unități administrative regionale, în vederea asigurării interoperabilității securizate între sistemele informatice:
    a. Dezvoltarea de “hub-uri informaționale” regionale, care să asigure schimbul de informații între instituțiile publice;
    b. Interconectarea acestora într-un punct central (hub central), firesc într-un stat național unitar.

6. Dezvoltarea intranetului guvernamental care să deservească toate instituțiile publice centrale și locale, prin exploatarea eficientă, unificată, a resurselor de comunicații deținute de companii naționale sau entități publice.

7. Dezvoltarea unei capabilități centralizate care să asiste toate instituțiile publice în pregătirea proiectelor în domeniul Societății Informaționale, inclusiv în cadrul procedurilor de achiziție

publică (putând efectua chiar achiziții centralizate), asigurându-se astfel nivelul optim de securitate și interoperabilitate.

8. Definirea standardelor ocupaționale specifice domeniului securității IT.

9. Dezvoltarea sau achiziționarea de capabilități tehnice minimale, prin raportare la infrastructură și informațiile gestionate, atât în zona publică cât și în sectorul privat:
    a. Norme, criterii și necesități pentru introducerea rolurilor de specialist IT și specialist securitate IT în cadrul tuturor instituțiilor administrației publice locale și centrale, ținând cont de specificul activităților prestate (colectarea și introducerea datelor, identificarea necesarului de echipamente și soluții IT, organizare, raportare etc) sau, alternative, asigurarea acestor capabilități din surse externe;
    b. Mentenanța continuă a soluțiilor de securitate efectuată de specialiști bine pregătiți atât pe soluția tehnică folosită cât și cu cunoștințe mai largi de securitate IT;
    c. Proceduri și sisteme adecvate;
    d. Auditare periodic.

10. Oferirea de facilități (eventual bazate pe instrumente structurale) care să permită actorilor economici să-și efectueze un audit minim de securitate.

11. Înființarea unui Cluster orientat pe securitate cibernetică, care să includă un centru național de transfer tehnologic și un centru specializat și procedurat pentru evaluarea nivelului de securitate al soluțiilor hardware/software.

12. Sprijinirea unei schimbări culturale în sensul securității cibernetice, cu accent pe informare/conștientizare, instruire, cooperare public-privat.