CERT-RO

ROMÂNIA
1918-2018 | SĂRBĂTORIM ÎMPREUNĂ

Raport privind evoluția amenințărilor cibernetice în 2017

Cuprins

1. Context. Evoluția amenințărilor și a politicilor în domeniul securității cibernetice

2. Evoluția amenințărilor cibernetice la nivel global

   2.1 Malware

   2.2 Ransomware

   2.3 Botnets

   2.4 DoS/DDoS

   2.5 Phishing

3. Evoluția amenințărilor în spațiul cibernetic național

   3.1 Date statistice

   3.2 Principalele atacuri

4. Analiza alertelor procesate de CERT-RO

   4.1 Distribuția alertelor în funcție de clasa și tipul incidentului

   4.2 Tipuri de incidente notificate către CERT-RO

   4.3 Tipuri de sisteme informatice afectate

Taxonomia utilizată de CERT-RO pentru clasificarea alertelor și incidentelor de securitate cibernetică

Referințe

Raportul CERT-RO privind evoluția amenințărilor cibernetice în anul 2017 este rezultatul unei analize asupra informațiilor colectate și procesate de instituție pe parcursul anului 2017. Un element de noutate față de rapoartele din anii anteriori îl reprezintă introducerea unei analize asupra tendințelor în ceea ce privește evoluția amenințărilor cibernetice la nivel global.

Pentru realizarea raportului au fost analizate notificările primite de CERT-RO prin intermediul adresei de email destinate acestui scop (alerts@cert.ro), alertele colectate și procesate automat (feed-uri), informațiile și rapoartele primite de la organizațiile partenere, precum și cele mai relevante rapoarte publicate de companiile ce activează în domeniul securității cibernetice.

Prezentul raport este destinat atât managerilor și experților în securitate cibernetică din organizațiile publice și private din România, cât și decidenților politici, cercetătorilor, organizațiilor neguvernamentale și cetățenilor.

El prezintă o viziune de ansamblu asupra amenințărilor și vulnerabilităților din spațiul cibernetic național și recomandări pentru consolidarea capacităților de prevenire și reacție, care pot fi utilizate atât în procesul de definire a politicilor publice în domeniu, al politicilor organizaționale, cât și la nivel individual.

Cap.1 Context.

Evoluția amenințărilor și a politicilor în domeniul securității cibernetice

Anul 2017 a fost unul dinamic în ceea ce privește evoluția amenințărilor cibernetice, atât prin prisma atacurilor[1] cibernetice cu impact major asupra unor servicii esențiale, cât și prin prisma pierderilor de date confidențiale la scară largă[2]. La toate acestea s-au adăugat o serie de acuzații cu privire la utilizarea mediului online pentru influențarea proceselor democratice din anumite state, în speță a campaniilor electorale.

Amenințările, vulnerabilitățile și riscurile în spațiul cibernetic au apărut în prim plan mai mult ca oricând, pe măsură ce atacurile s-au multiplicat și au devenit din ce în ce mai sofisticate. Toate acestea în contextul în care un număr tot mai mare de dispozitive sunt conectate la Internet, estimările indicând aproximativ 23 de miliarde până în 2018 și 75 de miliarde până în 2025, în timp ce producătorii și dezvoltatorii lansează zilnic noi astfel de produse pe piață.

Piața produselor de securitate cibernetică este în continuă creștere, generată de intensificarea criminalității informatice și a pierderilor de date, cifrele indicând o creștere semnificativă în următorii ani, deși o mare parte din acestea rămân încă nedetectate[3].

În acest context, statele și organizațiile internaționale și-au intensificat eforturile în domeniul reglementării și al consolidării capacităților de prevenție și răspuns la incidente de securitate cibernetică.

Directiva privind un nivel comun ridicat de securitate a rețelelor și sistemelor informatice în Uniune **(Directiva NIS)** și ***Regulamentul General pentru Protecția Datelor cu Caracter Personal*** **(GDPR)**, care vor începe să producă efecte în luna mai a acestui an, vor determina organizațiile care intră sub incidența lor să adopte măsuri concrete, tehnice și organizatorice, pentru creșterea nivelului de securitate cibernetică și pentru protejarea datelor personale ale utilizatorilor.

Directiva NIS prevede măsuri minime de securitate și cerințe de notificare a incidentelor de securitate cu impact semnificativ pentru operatorii de servicii esențiale din șapte sectoare: energetic, bancar, sănătate, apă, transporturi, infrastructuri ale pieței financiare și infrastructură digitală, în timp ce ***GDPR*** afectează toate organizațiile care prelucrează date cu caracter personal. Ambele reglementări ar trebui să aducă o schimbare substanțială a culturii companiilor și utilizatorilor cu privire la gestionarea datelor personale și securitatea sistemelor informatice.

Strategia Uniunii Europene de Securitate Cibernetică este și ea în proces de revizuire și un nou pachet legislativ european este în curs de negociere, care are în vedere consolidarea Agenției Europene pentru Securitate Cibernetică (ENISA) și introducerea unor scheme de certificare europeană a produselor de securitate cibernetică, menite pe de o parte să crească încrederea consumatorilor în produse iar pe de altă parte să elimine problema fragmentării schemelor de certificare existente pe piața europeană.

La nivel național, în anul 2017 alertele de securitate cibernetică procesate de CERT-RO au vizat 2,89 milioane de IP-uri unice, reprezentând 33,71% din totalul IP-urilor alocate spațiului cibernetic național. Imaginea pe care aceste date o oferă nu este însă una completă – în absența unui cadru legal care să definească modalitățile de colectare a informațiilor cu privire la incidentele din infrastructurile cibernetice naționale, datele colectate de CERT-RO se bazează în foarte mică măsură pe informații primite de la organizații afectate din țară.

Tendința globală cu privire la diversificarea amenințărilor și vulnerabilităților de natură cibernetică s-a reflectat pe parcursul anului 2017 și în spațiul cibernetic național, aspect evidențiat prin faptul că în anul 2017, CERT-RO a introdus noi tipuri de alerte.

Majoritatea alertelor procesate de CERT-RO (83,63%) se referă la sisteme informatice vulnerabile (neactualizate, nesecurizate sau configurate necorespunzător), ceea ce indică un nivel relativ scăzut al culturii de securitate cibernetică în rândul utilizatorilor din România. 10.32 % din alertele procesate se referă la sisteme informatice compromise sau infectate cu diverse variante de malware (adesea botnet).

Oricare dintre cele două tipuri de sisteme informatice menționate mai sus pot fi folosite ca interfață (proxy) sau infrastructură pentru desfășurarea unor atacuri asupra unor ținte din afara țări reprezentând astfel potențiale amenințări la adresa altor sisteme conectate la Internet.

În acest context creșterea rapidă a numărului de dispozitive sau echipamente de rețea de uz casnic (precum routerele wireless), sau cele care fac parte din categoria Internet of Things (IoT) (camere web, smart TV, smartphone, imprimante etc.) conectate la Internet este problematică, acestea putând deveni ținta atacatorilor. Vulnerabilitățile acestora sunt de regulă exploatate pentru a compromite rețeaua din care fac parte sau pentru lansarea de atacuri asupra altor ținte din Internet.

România este atât o țară generatoare de incidente de securitate cibernetică, cât și cu rol de proxy (de tranzit) pentru atacatori din afara spațiului național prin prisma utilizării unor sisteme informatice vulnerabile sau compromise, ce fac parte din spațiul cibernetic național.

Cap.2 Evoluția amenințărilor cibernetice la nivel global

În această secțiune sunt analizate principalele 5 tipuri de amenințări cibernetice manifestate în anul 2017: malware, ransomware, botnets, DDoS și phishing. Acestea se regăsesc și în raportul[5] ENISA privind peisajul amenințărilor cibernetice pe anul 2017.

2.1 Malware

Malware-ul rămâne una dintre cele mai importante amenințări cibernetice și care înregistrează o permanentă evoluție ascendentă în ceea ce privește nivelul de sofisticare tehnologică, complexitate și diversitate.

Tendințe și aspecte de interes

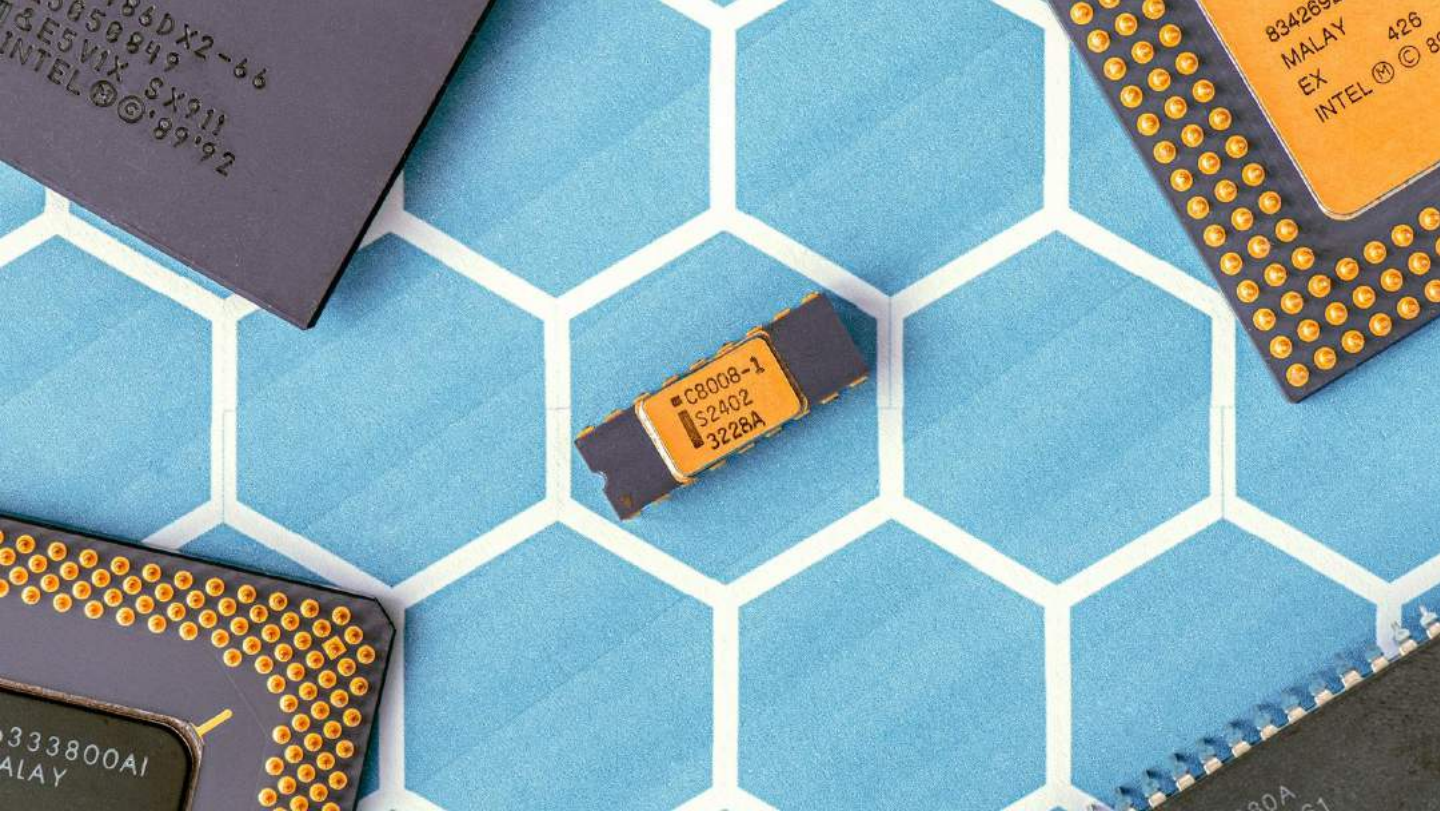
- **Malware rezident doar în RAM („fileless")[6]** – atacatorii preferă tot mai mult utilizarea de malware care nu lasă urmă pe discurile de stocare ale sistemelor infectate. Acest tip de malware este dificil de investigat prin metodologiile și cu uneltele clasice. Practic, malware-ul rezidă doar în memoria RAM, componentele acestuia devenind astfel foarte volatile;
- **Utilizarea uneltelor software pre-instalate („living off the land")[7]** – tot mai multe atacuri utilizează malware rezultat prin combinarea unor unelte software pre-instalate în sistemele țintă, precum: PowerShell, PSExec, WMI etc. Astfel, atacurile devin mai greu de detectat deoarece respectivele unelte sunt destinate în mod normal pentru derularea unor activități legitime de administrare a sistemelor informatice. Campania NotPetya[8] din vara anului 2017 este un exemplu relevant în acest sens;

- **Independență față de acțiunea utilizatorilor („click less”)** – Datorită creșterii eforturilor în direcția conștientizării riscurilor cibernetice în rândul utilizatorilor, atacatorii încep să se orienteze către mecanisme de infectare a sistemelor informatice fără a fi nevoie de vreo acțiune din partea utilizatorilor. Astfel, au fost identificate tot mai multe cazuri de infecții datorate simplei vizitări a unui site web, sau prin răspândirea automată în rețea (capabilități de tip „worm”). Campania WannaCry[9] este un exemplu relevant de malware care nu vreo acțiune din partea utilizatorilor pentru răspândire;

- **Malware-ul ce țintește szistemele MAC OS este în creștere** – Contrar percepției generale conform căreia sistemele de operare de tip Linux/Unix nu sunt afectate de malware, în ultimii ani au fost identificate din ce în ce mai multe variante de malware special create pentru MAC OS X. Mai mult, în anul 2017 rapoartele[10] arată aproape o dublare a acestui tip de malware, ceea ce arată o tendință evidentă a atacatorilor de a ținti și aceste sisteme, mai ales în contextul în care și cota de piață a acestor sisteme este în continuă creștere;

- **Exploatarea vulnerabilităților din hardware sau firmware** - Descoperirea a tot mai multe vulnerabilități de acest fel în ultimul timp a condus la apariția de malware care încearcă să le exploateze[11]. Un exemplu recent în acest sens îl reprezintă vulnerabilitățile de tip „side-channel”[12] cunoscute ca Spectre și Meltdown[13];

- **Exploatarea lanțului de aprovizionare („supply chain attacks”)** – Atacatorii au observat că uneori, în vederea atacării unor ținte anume sau a cât mai multor utilizatori și companii, este mult mai eficient să se compromită anumite mecanisme de producție, aprovizionare sau distribuire de hardware și software. Spre exemplu, inserarea de malware într-o unealtă software utilizată la scară largă este o metodă foarte eficientă de infectare în masă. Unul dintre cele mai relevante cazuri de anul trecut a fost compromiterea Cleaner[14]. Alte campanii au vizat mecanismul de actualizare al unor unelte software (precum în cazul M.E.Doc[15]), sau malware la nivel de firmware[16] (BIOS, UEFI).



Măsuri de prevenție și răspuns

CERT-RO recomandă:

- Utilizarea de produse/tehnologii antimalware care să acopere toată plaja de sisteme informatice din infrastructura IT: stații de lucru fixe și mobile, dispozitive mobile, servere (fișiere, baze de date, email, web etc.);
- Actualizarea în permanență a tuturor componentelor infrastructurii IT: sisteme de operare, aplicații, echipamente de rețea, soluții de protecție etc.;
- Asigurarea unei vizibilități adecvate în cadrul infrastructurii IT, utilizând soluții care să detecteze automat anomaliile sau activitățile suspecte, precum cele datorate unor infecții cu malware;
- Dezvoltarea și implementarea de proceduri eficiente și capabilități adecvate de răspuns la incidentele cibernetice, inclusiv în ceea ce privește infecțiile cu malware;
- Utilizarea unor unelte de analiză malware și unelte/platforme de schimb de informații privind malware-ul și metodele de contracarare, inclusiv a soluțiilor „open source” precum Cuckoo[17] și MISP[18].

2.2 Ransomware

Această formă de malware și-a făcut simțită prezența din plin și în anul 2017, când au fost identificate campanii cu un potențial distructiv mai pronunțat precum WannaCry sau NotPetya.

Tendințe și aspecte de interes

- **Atacuri țintite** – au fost înregistrate tot mai multe atacuri îndreptate împotriva unor organizații cât mai profitabile[19], precum cele din zona financiar-bancară, cererile de răscumpărare ajungând în medie la aproximativ 500 de mii de dolari.
- **„Ransomware-as-a-service" (Raas)** – începutul anului 2017 a fost marcat de creșterea alarmantă variantelor de ransomware oferite ca serviciu contra cost pe piața neagră precum forumurile de hacking. Astfel, anul trecut s-au înregistrat recorduri în ceea ce privește numărul de variante de ransomware și costurile generate de aceste tipuri de atacuri (peste un miliard de dolari)[20]
- **„Wipeware"** – Două dintre cele mai mediatizate campanii ransomware de anul trecut, WannaCry și NotPetya, s-au caracterizat printr-un potențial distructiv ridicat și mecanisme de răspândire rapidă. Pe de altă parte, s-a dovedit că acestea nu au fost de fapt concepute pentru a se putea decripta fișierele în urma plății răscumpărării ci mai degrabă pentru a genera un impact disruptiv cât mai ridicat[21].
- **Atacuri asupra dispozitivelor medicale („MEDJACK")** – Cercetătorii au descoperit o creștere a atacurilor de tip ransomware ce vizează dispozitivele medicale[22]. Acest lucru se datorează în primul rând tendinței de interconectare între sistemele IT clasice și cele cu destinație specială, de tip (OT – Operational Technology). Mai mult decât atât, sectorul medical în general devine una dintre țintele preferate ale atacurilor cu ransomware.

Măsuri de prevenție și răspuns

CERT-RO recomandă:

- Implementarea măsurilor de protecție anti-malware;
- Consultarea "Ghidului privind combaterea amenințărilor informatice de tip ransomware" elaborat de CERT-RO[23];
- Acordarea unei atenții deosebite procedurilor și soluțiilor de creare a copiilor de siguranță (backup) pentru datele importante, aceasta fiind cea mai eficientă strategie de limitare a efectelor unui eventual atac cu ransomware.

2.3 Botnets

Amenințările de tip botnet reprezintă în continuare o problemă serioasă, în anul 2017 înregistrându-se recorduri în ceea ce privește lățimea de bandă (peste 1Tbps) aferentă unor atacuri DDoS derulate cu ajutorul unor botneți de tip IoT (Internet of Things).

Tendințe și aspecte de interes

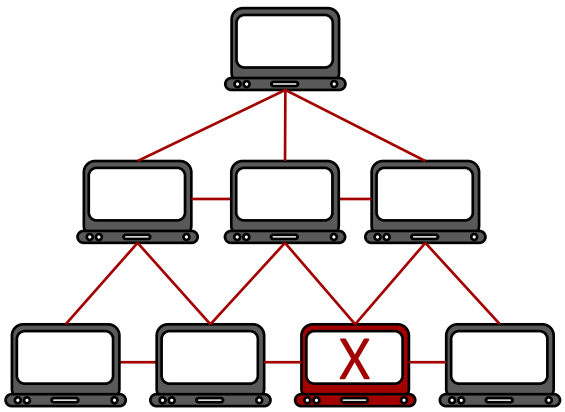
- **Migrarea către dispozitivele IoT** – Datele arată o tendință a malwarelului de tip botnet de a migra dinspre computerele personale către dispozitivele de tip IoT. Aceste dispozitive sunt preferate mai nou de botnet deoarece sunt în permanență conectate la Internet, au o securitate precară și numărul de dispozitive la nivel global crește exponențial. Între cei mai cunoscuți botneți din 2017 regăsim Mirai[24], Reaper[25] și Necurs[26], responsabili pentru unele dintre cele mai mari atacuri DDoS din istorie (detalii în secțiunea 1.2.4).

- **Mașinile virtuale reprezintă mai nou o țintă[27]** – Odată cu creșterea în amploare a serviciilor de găzduire de mașini virtuale în cloud, oferite de companii precum Google, Microsoft sau Amazon, atacatorii vizează tot mai mult compromiterea acestor mașini virtuale și includerea lor în rețele de tip botnet. Mașinile virtuale din cloud sunt atrăgătoare pentru botneți deoarece sunt în permanență conectate la Internet și de cele mai multe ori împărtășesc vulnerabilități comune ce facilitează infectarea în masă a acestora.

Măsuri de prevenție și răspuns

CERT-RO recomandă:

- Implementarea măsurilor de protecție anti-malware recomandate în prezentul raport;
- Utilizarea unor soluții de protecție perimetrală a rețelei (NGFW – Next Generation Firewall);
- Utilizarea unor soluții de protecție specifice diferitelor categorii de servicii: email (Email Gateway), web (Web Gateway), webserver (WAF – Web Application Firewall) etc.
- Implementarea de soluții de filtrare a traficului de tip IP/URL „blacklisting”.



2.4 DoS/DDoS

Atacurile de tip DoS (Denial of Service), prin care atacatorii vizează afectarea disponibilității unor sisteme informatice sau întreruperea unor servicii furnizate prin intermediul sistemelor IT, constau de cele mai multe ori în inundarea sistemului/serviciului țintă cu cereri la nivel de rețea astfel încât să se ajungă la supraîncărcarea sistemului care nu va mai putea răspunde la cererile legitime. Unele dintre cele mai atacate sisteme prin DoS sunt site-urile web.

Atacurile DDoS (Distributed Denial of Service) înregistrează o evoluție ascendentă; Acestea se caracterizează prin faptul că traficul care inundă sistemul țintă cu cereri de rețea este generat de un număr mare de surse – adesea sisteme informatice care fac parte dintr-o rețea de tip botnet. Datorită numărului mare de surse implicate în generarea traficului malițios, contracararea acestor tipuri de atacuri este de cele mai multe ori problematică și implică resurse/costuri mari.

Tendințe și aspecte de interes

- **Atacurile DDoS înregistrează o evoluție ascendentă** – Conform unor studii, atacurile de tip DDoS sunt în creștere, aproximativ 33% din companii fiind afectate de un astfel de atac în 2017, față de 17% în anul 2016;
- **Atacuri DDoS în valuri (Pulse Wave Attacks)[28]** – Unii dintre atacatorii din spatele unor rețele botnet utilizate pentru DDoS preferă să nu mai concentreze toate resursele de atac disponibile asupra unei singure ținte, preferând să direcționeze traficul malițios în valuri, pe perioade mai scurte, către mai multe ținte. Față de sfârșitul anului 2016, când s-au înregistrat atacuri cu lățimi de bandă de 1 Tbps (OVH[29]) și 665 Gbps (websiteul https://krebsonsecurity.com, deținut de jurnalistul Brian Krebs[30]), în anul 2017 lățimile de bandă au fost mai mici, însă s-au înregistrat atacuri în valuri.;
- **Costurile serviciilor de tip „DDoS as-a-service" sunt în continuă scădere** – Conform unor studii[31], costurile unui atac DDoS de o oră au ajuns să coste nu mai mult de 4 USD, făcând ca aceste atacuri să fie din ce în ce mai accesibile;
- **Serviciile de schimb de monezi virtuale (Bitcoin Exchange) sunt printre ținte** – Rapoartele[32] arată că începând cu Iunie 2017 s-a înregistrat o evoluție crescătoare în ceea ce privește atacurile DDoS îndreptate împotriva serviciilor de tip „Bitcoin Exchange" și a magazinelor online care acceptă plăți în monedă virtuală;
- **Câteodată atacurile DDoS maschează alte tipuri de atacuri** – Conform unui studiu[33], 53% dintre victimele atacurilor DDoS din prima jumătate a anului 2017 au declarat că acele atacuri au acoperit de fapt alte atacuri: infecții cu malware, exfiltrări de date, intruziuni sau tranzacții financiare frauduloase.

Măsuri de prevenție și răspuns

CERT-RO recomandă:

- Crearea și implementarea unei politici de securitate care să includă detecția și reacția la atacurile DoS/DDoS;
- Utilizarea unor mecanisme și tehnologii de protecție la atacurile DoS/DDoS: balansarea traficului/cererilor, Firewall, utilizarea listelor de control acces (ACL), IPS/IDS, WAF, IDMS (Intelligent DDoS mitigation systems), servicii anti DDoS bazate pe tehnologii cloud.

2.5 Phishing

Phishing-ul reprezintă o încercare a răufăcătorilor de a obține informații confidențiale (credențiale de acces la un sistem sau serviciu, date aferente cardurilor de credit etc.), prin deghizarea ca o persoană sau organizație de încredere și prin utilizarea unor tehnici de inginerie socială.

Cea mai întâlnită formă de phishing este cea în care atacatorii creează o copie aproape identică a unei pagini web asociate unui serviciu legitim (online banking, o rețea de socializare, un serviciu de webmail etc.) și trimit emailuri către utilizatori prin care-i îndeamnă pe aceștia să se autentifice la aceste pagini false, sau să-și completeze/actualizeze datele personale. Astfel, datele introduse de utilizatori pe acele pagini false sunt preluate de atacatori și utilizate în diferite scopuri frauduloase: tranzacții financiare în numele utilizatorilor, preluarea abuzivă a conturilor online sau chiar furt de identitate.

Tendințe și aspecte de interes

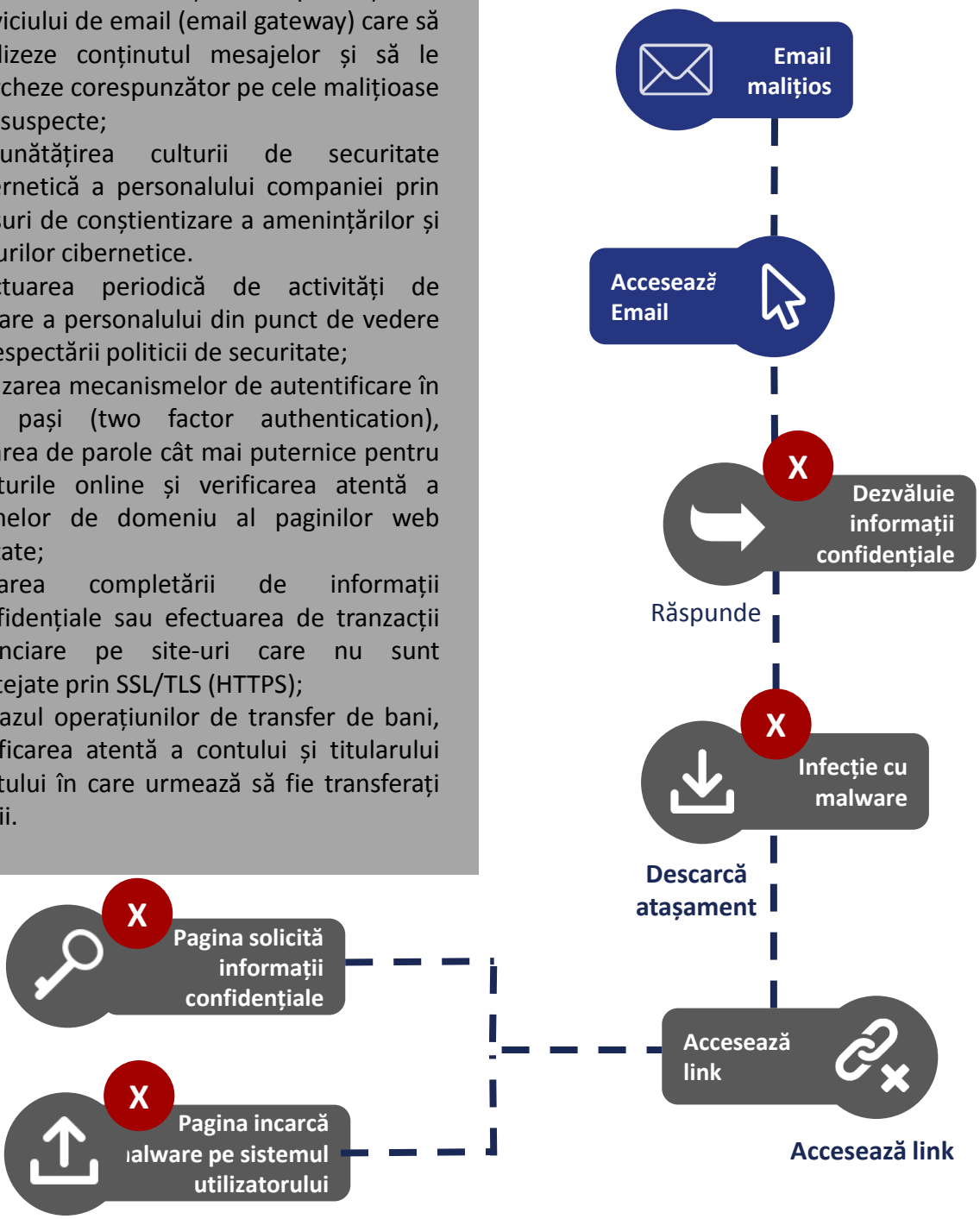
- **Atacuri țintite (spear phishing)** – Spre deosebire de acum câțiva ani, când marea majoritate a atacurilor de tip phishing se bazau pe trimiterea de emailuri în masă la cât mai mulți destinatari, în ultima perioadă aceste atacuri devin tot mai țintite[34]. Astfel, atacatorii personalizează atacul în funcție de profilul țintelor, începând cu limba în care este redactat textul de phishing și continuând cu detalii care fac mesajul mai credibil pentru ținte: subiecte de interes, deghizarea în expeditori cunoscuți cu care țintele relaționează de obicei etc;
- **Phishing care livrează malware** – Rapoartele[35] arată că în ultima perioadă mesajele de tip phishing conțin atașamente sau link-uri (URL) care, odată accesate de utilizatori, încearcă infectarea cu malware a sistemelor;
- **Utilizarea de mecanisme de evitare a detecției** – Deoarece în ultimii ani eforturile de contracarare a atacurilor de tip phishing s-au întețit, spre exemplu prin includerea paginilor identificate ca fiind de phishing în diferite liste negre (black lists), sau chiar afișarea de atenționări în browser, atacatorii au început să utilizeze mai multe resurse pentru o campanie[36] (spre exemplu mai multe URL-uri malițioase). O altă tehnică utilizată este aceea de a compromite mai întâi site-uri legitime și apoi inserarea de pagini de phishing în cadrul acestora.

Măsuri de prevenție și răspuns

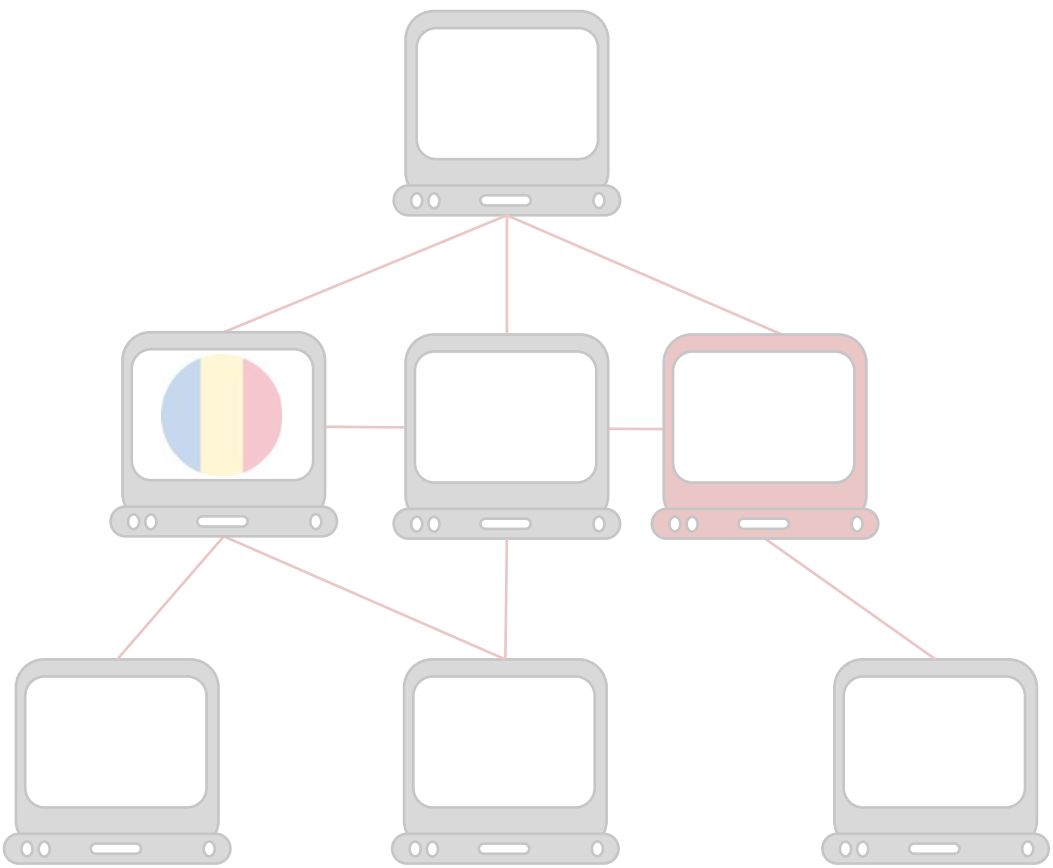
CERT-RO recomandă:

- Utilizarea de soluții de protecție a serviciului de email (email gateway) care să analizeze conținutul mesajelor și să le marcheze corespunzător pe cele malițioase sau suspecte;
- Îmbunătățirea culturii de securitate cibernetică a personalului companiei prin cursuri de conștientizare a amenințărilor și riscurilor cibernetice.
- Efectuarea periodică de activități de testare a personalului din punct de vedere al respectării politicii de securitate;
- Utilizarea mecanismelor de autentificare în doi pași (two factor authentication), setarea de parole cât mai puternice pentru conturile online și verificarea atentă a numelor de domeniu al paginilor web vizitate;
- Evitarea completării de informații confidențiale sau efectuarea de tranzacții financiare pe site-uri care nu sunt protejate prin SSL/TLS (HTTPS);
- În cazul operațiunilor de transfer de bani, verificarea atentă a contului și titularului contului în care urmează să fie transferați banii.

Parcursul tipic al unui atac de tip phishing din perspectiva utilizatorului



Cap.3 Evoluția amenințărilor în spațiul cibernetic național



3.1. Date statistice

33,71% (2,89 mil.) din totalul IP-urilor unice alocate spațiului cibernetic național au fost implicate în cel puțin o alertă de securitate cibernetică procesată de CERT-RO în anul 2017, în scădere față de anul 2016, când s-a înregistrat procentul de 38,72% (2,92 mil.);

83,63% (115,60 mil.) din alertele procesate vizează sisteme informatice vulnerabile, în sensul că sunt neactualizate, nesecurizate sau configurate necorespunzător, fiind astfel expuse atacurilor cibernetice care vizează exploatarea vulnerabilităților acestora.

10,32% (14,33 mil.) din alertele procesate se referă la sisteme informatice compromise, în sensul că fie au fost infectate cu diferite forme de malware, fie au fost exploatate și utilizate de atacatori în diferite tipuri de atacuri și campanii de trimitere de Spam, marea majoritate fiind înregistrate în listele cu resurse blocate (Realtime Blackhole Lists - RBL);

5,88% (8,17 mil.) din alertele procesate vizează sisteme informatice infectate cu malware de tip botnet, acesta din urmă fiind caracterizat de faptul că dispune de mecanisme ce permit atacatorilor să controleze de la distanță sistemele informatice infectate. Astfel, se constată o scădere semnificativă față de anul 2016 când s-a înregistrat procentul de **12,81% (14,12 mil.),** confirmându-se tendința descendentă a fenomenului botnet la nivel internațional;

1.709 de domenii web „.ro" au fost raportate la CERT-RO ca fiind compromise, în scădere cu aproximativ 84% față de anul 2016 (10.639). Numărul reprezintă aproximativ 0,18% din totalul domeniilor ".ro" înregistrate în România în luna decembrie 2017 (944.145) [37] și aproximativ 0,38% din totalul domeniilor ".ro" active (438.366)[38].

2017 CERT-RO
DATE STATISTICE

138M ALERTE

2.89M IP-uri (34%)

83% SISTEME VULNERABILE

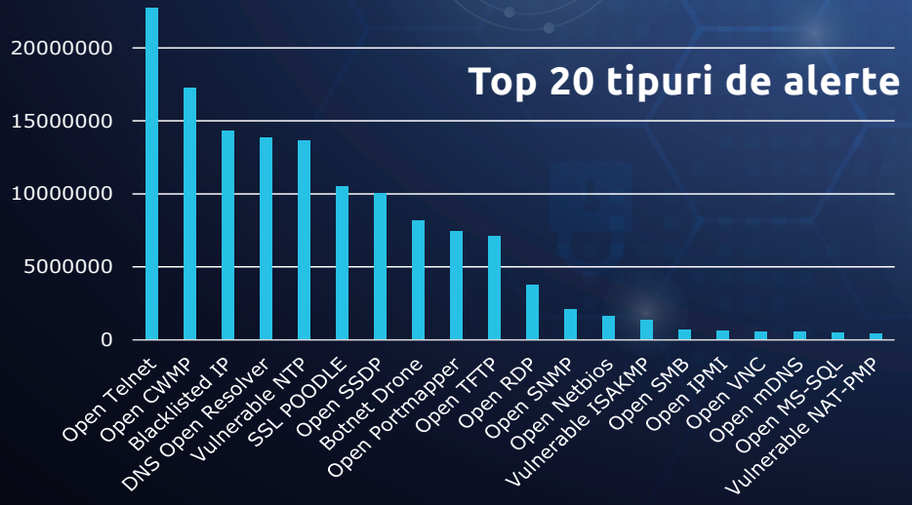
25% CREȘTERE ÎN NR. DE ALERTE

1.7k DOMENII .RO

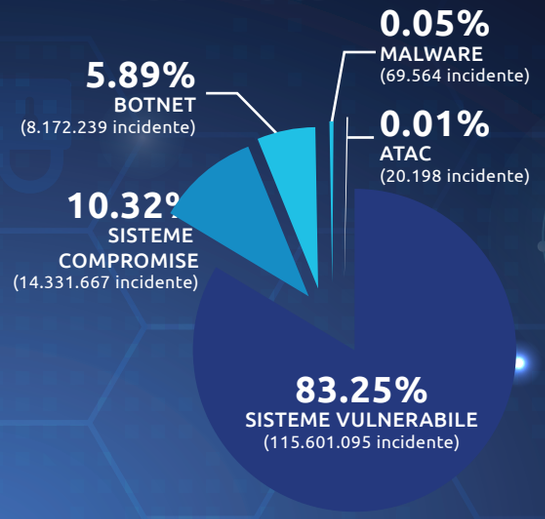
CERT-RO a colectat și procesat 138.217.026 alerte, înregistrând o creștere de 25% față de 2016. Totalul IP-urilor unice a fost 8.590.269, de la 7.540.736 în 2016, corelate cu tendința ascendentă a alertelor primite.

Numărul alertelor colectate de CERT-RO

Top 20 tipuri de alerte



138 217 026 alerte de securitate cibernetică



Tipuri de sisteme de operare afectate

LINUX **41.02%**

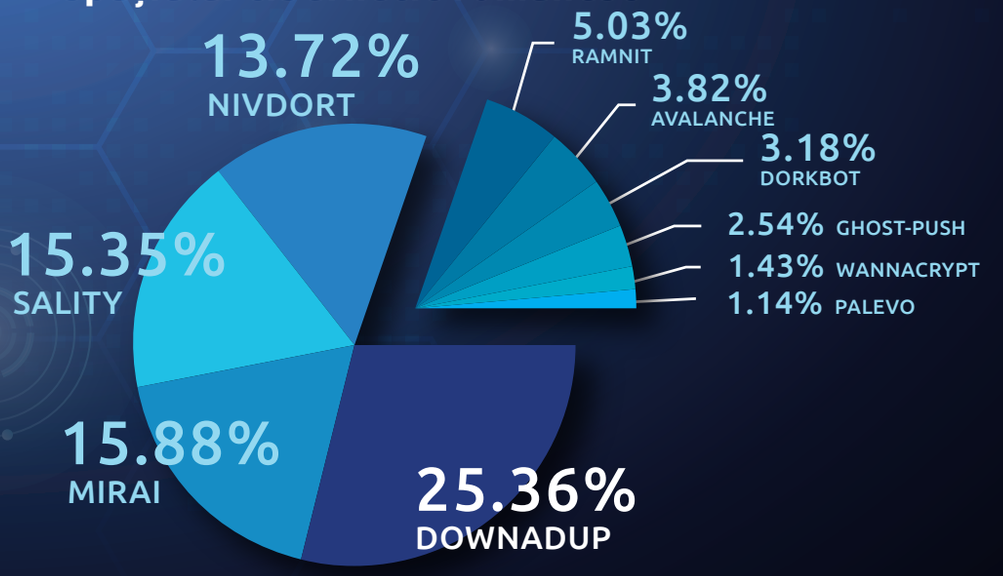
UNIX **30.13%**

DISPOZITIVE CONECTATE ÎN REȚEA FIRMWARE/OS **20.65%**

UPNP/1.0 **7.76%**

WINDOWS **0.44%**

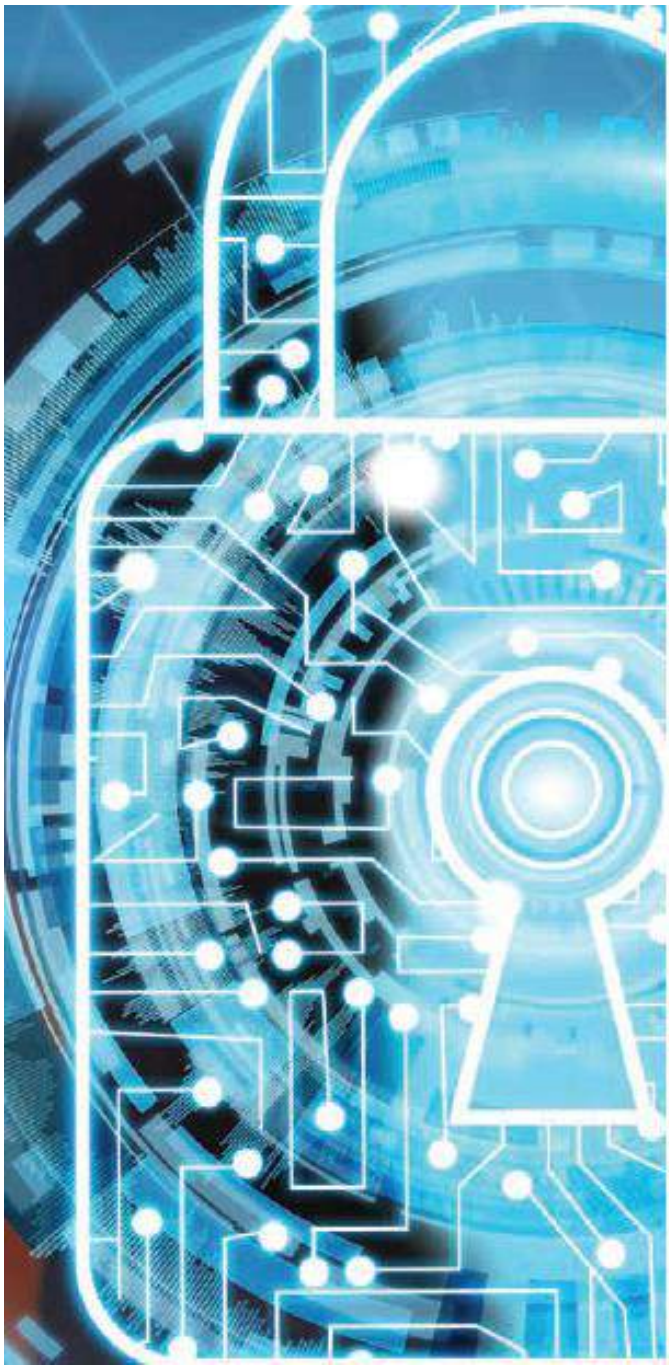
Top 10 tipuri de malware specifice spațiului cibernetic românesc



3.2 Principalele atacuri

Pierderile de date și campaniile de ransomware la scară largă au fost în prim plan în anul 2017.

Marile companii din domeniu indicau o dublare a infecțiilor cu ransomware în 2017 (Symantec) și o proporție de aproape 60% din totalul atacurilor cu malware în rândul companiilor în primul semestru din 2017 (Malwarebytes), în timp ce la începutul anului 2018 estimările FBI indicau 4,000 de atacuri ransomware pe zi[39] .



Două campanii majore de ransomware – **WannaCry[40] și NotPetya[41]** au fost în prim plan și pe agenda publică din România, după ce au afectat sute de mii de sisteme din sectoare diverse precum sănătate, transport, manufactură și administrație publică din aproximativ 150 țări. CERT-RO a publicat alerte, actualizări și recomandări pe parcursul celor două campanii, în vederea prevenirii infectării utilizatorilor din România sau a remedierii în caz de infectare.

Wannacry

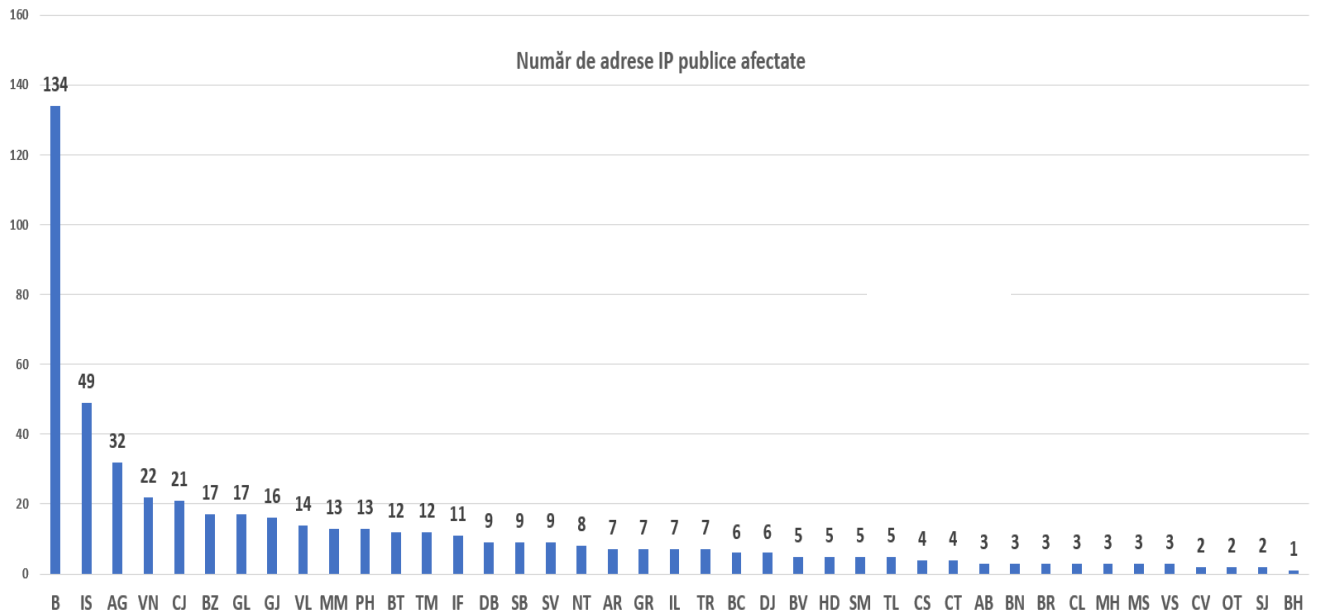
Începând cu 12 Mai 2017, numeroase organizații din întreaga lume au fost afectate de o nouă variantă de ransomware, cu denumirea de WannaCry. Printre victime s-au numărat companii-gigant precum FedEx, operatorul de comunicații Telefonica din Spania, sau chiar sistemul de sănătate din Marea Britanie (National Health Service).

Spre deosebire de alte campanii ransomware din trecut, Wannacry dispunea și de capabilități de răspândire în rețea (lateral movement) prin exploatarea unei vulnerabilități a protocolului SMBv1.

Această amenințare s-a propagat prin intermediul unor mesaje email care conțineau atașamente și link-uri malițioase, atacatorii utilizând tehnici de inginerie socială pentru a determina utilizatorii să acceseze resursele malițioase.

Odată infectată o stație de lucru dintr-o rețea, malware-ul încerca să se răspândească în interiorul rețelei prin intermediul protocolului SMB, utilizând porturile UDP/37, UDP/138, TCP/139 și TCP/445. Procesul de răspândire se realiza prin exploatarea unei vulnerabilități a protocolului SMBv1 din cadrul Windows, cunoscută ca CVE-2017-0145.

Microsoft a publicat încă din luna Martie 2017 o actualizare de securitate pentru rezolvarea vulnerabilității exploatată de acest ransomware pentru răspândire, cunoscută ca MS17-010.
Anumite sisteme de operare, precum Microsoft Windows Vista SP2, Microsoft Windows Server 2008 SP2 și R2 SP1, Microsoft Windows 7, Microsoft Windows 8.1, Microsoft Windows RT 8.1, Microsoft Windows Server 2012 și R2, Microsoft Windows 10, Microsoft Windows Server 2016, Microsoft Windows XP, Microsoft Windows Server 2003, au fost pasibile de a fi afectate de această amenințare în cazul în care nu au fost actualizate.



Conform informațiilor deținute de CERT-RO, campania ransomware WannaCry a fost urmată de multiple atacuri bazate pe exploatarea aceleiași vulnerabilități de Windows SMBv1, cunoscută ca EternalBlue (CVE-2017-0145), dar care aveau comportamente diferite post-exploatare, cele mai importante fiind cunoscute sub denumirile de EternalRocks (sau BlueDoom), UIWIX și Adylkuzz.

Mai mulți specialiști au susținut că ar exista variante multiple a ransomware-ului WannaCry, cu domenii diferite inserate în script sau fără acel buton de 'stop' (kill switch) pentru propagarea malware-ului. Comunitatea de specialitate a raportat cel puțin două domenii cu funcție de buton de stop (kill switch) pentru campanie.

În total, aproximativ 300.000 de computere din aproximativ 150 de țări au fost afectate de această campanie. Atacatorii au beneficiat de un număr de aproximativ 100 de plăți, cifrate la suma de aproximativ 26.000 de dolari.

În România, din datele deținute de CERT-RO la momentul respectiv, 514 IP-uri au fost afectate, 10 dintre acestea aparținând unor instituții publice. În absența unui cadru legal care să oblige companiile și instituțiile publice să raporteze aceste incidente, o evaluare exactă a situației la nivel național nu ar fi fost posibilă. În perioada campaniei, CERT-RO a primit doar cinci notificări oficiale de la organizații afectate din România.

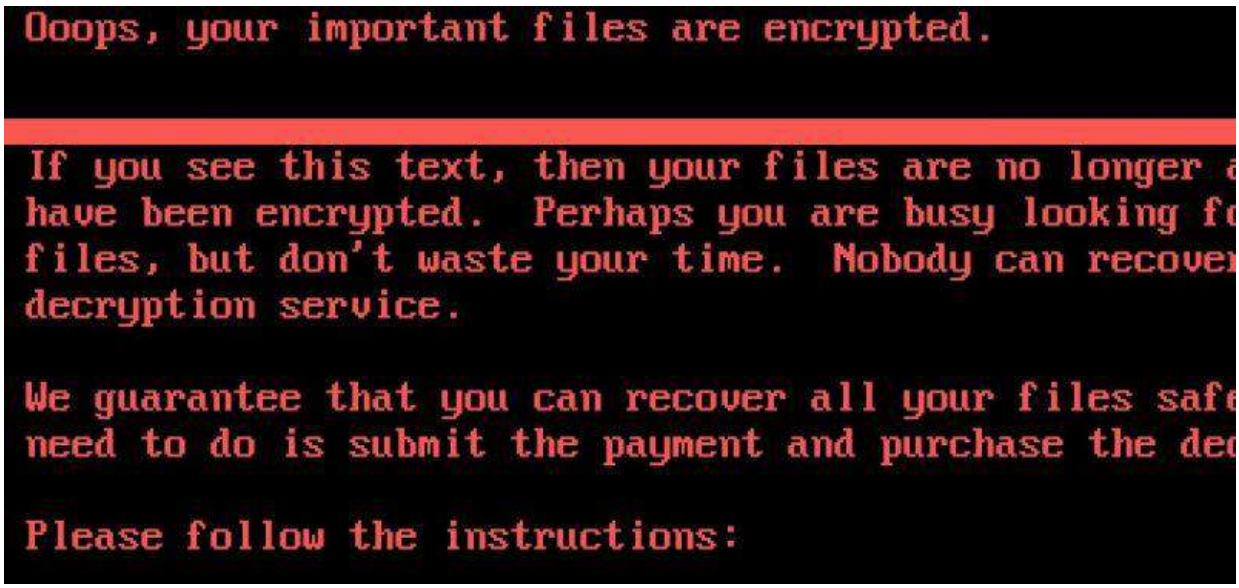
NotPetya

Începând cu data de 26 iunie 2017, utilizatori și companii din întreaga lume, dar mai cu seamă Ucraina, au fost afectați de un nou virus de tip ransomware denumit Petya, cunoscut și ca Petrwrap.

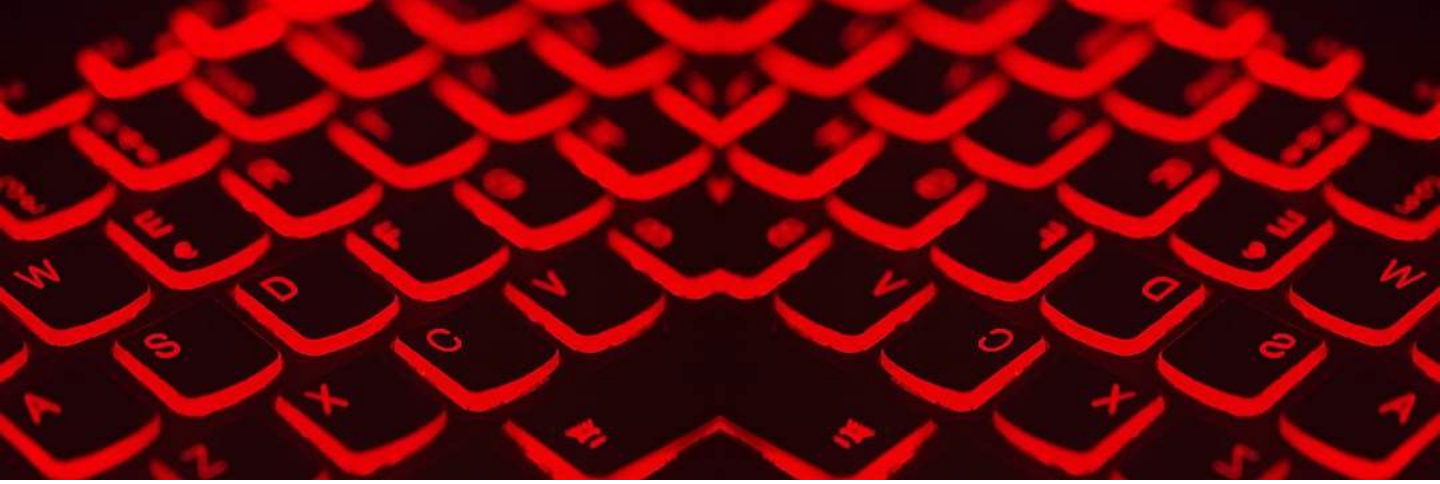
Infecția inițială a sistemelor se realiza prin intermediul unor documente atașate unor mesaje email de tip phishing, pe care utilizatorii erau îndemnați să le deschidă. De asemenea, conform unor informații publicate pe rețelele de socializare de autoritățile din Ucraina, virusul s-a răspândit și prin intermediul mecanismului de actualizare al aplicației MeDoc (populară în Ucraina), această variantă fiind confirmată și într-o postare de pe blogul companiei de securitate Kaspersky.

Ca și în cazul WannaCry, odată infectată o stație de lucru dintr-o rețea, virusul utiliza multiple tehnici de răspândire laterală în rețeaua internă unde a avut loc infecția inițială a unei stații de lucru, utilizând următoarele tehnici de identificare a altor sisteme țintă:

- Identificarea plăcilor de rețea de pe sistemul infectat;
- Citirea denumirilor altor sisteme din NetBIOS;
- Citirea informațiilor aferente DHCP (lease time)
- Toate sistemele identificate de virus în rețelele adiacente sunt scanate pe porturile TCP/445 și TCP/139 (utilizate de protocolul SMB), iar dacă porturile sunt deschise încercă exploatarea vulnerabilităților descrise anterior.



Analiza principalelor alerte procesate de CERT-RO



În 2017, CERT-RO a colectat și procesat 138.217.026 de alerte de securitate cibernetică, în creștere cu 25% față de anul 2016 (110.194.890), dintre care:

- alerte colectate și procesate automat (feed-uri): **138.215.593**;
- alerte colectate și procesate manual (email tiketing): **1.433**.

Prin alertă de securitate cibernetică, în contextul prezentului raport, înțelegem orice semnalare ce conține o adresă IP sau un domeniu web (URL), referitoare la un posibil incident sau eveniment de securitate cibernetică, ce implică sau poate implica sisteme informatice din spațiul cibernetic național deținute/administrate de persoane fizice sau juridice din România.
Numărul alertelor de securitate cibernetică procesate de CERT-RO în anul 2017 a crescut cu 25% față de anul 2016, păstrându-se tendința de creștere de la un an la altul.

Un număr de **2.896.269 de adrese IP unice și 1.709 de domenii web „.ro”** au fost vizate de alertele procesate de CERT-RO în anul 2017.
Numărul total de IP-uri unice alocat organizațiilor din România este de 8.590.378[42], în creștere față de anul 2016 (7.540.736), revenind aproximativ la aceeași cifră din 2015 (8.958.498), însă în continuare mult sub nivelele înregistrate în 2014 (aprox. 10 mil.) și mai ales 2013 (aprox. 13,5 mil.).

Distribuția alertelor în funcție de clasa și tipul incidentului

Alertele procesate de CERT-RO au fost clasificate în baza unei taxonomii în care au fost definite clase și tipuri de incidente (o clasă de incident reprezentând o categorie generică ce poate îngloba mai multe tipuri specifice de incident). Descrierea tipurilor de alerte procesate de CERT-RO (taxonomia) se regăsește anexată prezentului raport.

Cele mai frecvente 5 clase de incidente, în ordinea frecvenței alertelor:

- Sistem vulnerabil
- Sistem compromis
- Botnet
- Malware
- Atac

În tabelul de pe pagina următoare se regăsesc toate tipurile de alerte colectate de CERT-RO în anul 2017, evidențiate după clasa și tipul incidentului. Față de anul 2016, **CERT-RO a procesat 7 noi tipuri de alerte**: **Blacklisted IP, Trackback SPAM, Open SMB, Open VNC, Open MS-SQL, Open Memcached, Open LDAP.**

4.1 Distribuția alertelor procesate de CERT-RO în 2017

	Clasă incident	Tip incident	Nr. alerte	Procent
1	Vulnerable System	Open Telnet	22.746.467	16,45707%
2	Vulnerable System	Open CWMP	17.245.057	12,47680%
3	Compromised System	Blacklisted IP	14.297.113	10,34396%
4	Vulnerable System	DNS Open Resolver	13.877.359	10,04027%
5	Vulnerable System	Vulnerable NTP	13.679.953	9,89744%
6	Vulnerable System	SSL POODLE	10.515.032	7,60762%
7	Vulnerable System	Open SSDP	10.041.893	7,26531%
8	Botnet	Botnet Drone	8.169.009	5,91028%
9	Vulnerable System	Open Portmapper	7.460.953	5,39800%
10	Vulnerable System	Open TFTP	7.105.127	5,14056%
11	Vulnerable System	Open RDP	3.799.358	2,74884%
12	Vulnerable System	Open SNMP	2.118.977	1,53308%
13	Vulnerable System	Open Netbios	1.637.249	1,18455%
14	Vulnerable System	Vulnerable ISAKMP	1.340.317	0,96972%
15	Vulnerable System	Open SMB	711.579	0,51483%
16	Vulnerable System	Open IPMI	663.362	0,47994%
17	Vulnerable System	Open VNC	606.589	0,43887%
18	Vulnerable System	Open mDNS	548.395	0,39676%
19	Vulnerable System	Open MS-SQL	530.279	0,38366%
20	Vulnerable System	Vulnerable NAT-PMP	414.407	0,29982%
21	Vulnerable System	Open Memcached	272.752	0,19734%
22	Vulnerable System	Open LDAP	119.536	0,08648%
23	Malware	Malicious URL	69.864	0,05055%
24	Vulnerable System	SSL FREAK	39.262	0,02841%
25	Compromised System	Compromised Webserver	34.651	0,02507%
26	Vulnerable System	Open MongoDB	34.304	0,02482%
27	Vulnerable System	Open Chargen	30.482	0,02205%
28	Vulnerable System	Open QOTD	21.296	0,01541%
29	Fast-Flux	Fast-Flux IP	19.327	0,01398%
30	Attack	Bruteforce	13.838	0,01001%
31	Vulnerable System	Open Elasticsearch	12.010	0,00869%
32	Vulnerable System	Unsecured Proxy	11.675	0,00845%
33	Vulnerable System	Vulnerable Netcore/Netis	6.739	0,00488%
34	Attack	Trackback SPAM	6.373	0,00461%
35	Vulnerable System	Open XDMCP	4.882	0,00353%
36	Vulnerable System	Open Redis	4.859	0,00352%
37	Botnet	Botnet C2 Server	3.265	0,00236%
38	Phishing	Phishing URL	1.184	0,00086%
39	Vulnerable System	Open DB2	945	0,00068%
40	Spam	Spam URL	933	0,00068%
41	Malware	Malware Infection	341	0,00025%
42	Attack	Scan	23	0,00002%
43	Attack	DDoS	10	0,00001%
	TOTAL		138.217.026	100%

4.2 Tipuri de incidente notificate către CERT-RO

Alături de alertele automate, analiștii CERT-RO au preluat o serie de notificări referitoare la diferite tipuri de incidente de securitate cibernetică, raportate direct de către persoane sau organizații din țară sau străinătate. Acestea sunt considerabil mai puține decât alertele automate, dar conțin informații complete și mai relevante despre incidente, organizația afectată, sursa atacului și metoda de atac. În majoritatea cazurilor datele sunt colectate de la entitățile afectate (persoane fizice sau juridice din țară sau străinătate), de către analiștii CERT-RO, odată cu raportarea incidentului.

CERT-RO a colectat **1.433 de notificări de incidente**, repartizate astfel:

	Clasă incident	Tip incident	Număr notificări	% notificări
1	Phishing	Phishing URL	673	46,96%
2	Malware	Malware Infection	341	23,80%
3	Malware	Malicious URL	239	16,68%
4	Compromised System	Compromised Webserver	97	6,77%
5	Botnet	Botnet Drone	31	2,16%
6	Attack	Scan	23	1,61%
7	Attack	Bruteforce	13	0,91%
8	Attack	DDoS	10	0,70%
9	Botnet	Botnet C2 Server	4	0,28%
10	Spam	Spam URL	2	0,14%

3.3.3. Tipuri de malware caracteristice spațiului cibernetic național

Un procent de 4,16% (5,77 mil.) din totalul alertelor colectate și procesate de CERT-RO în anul 2017 conțin informații referitoare la tipul de malware asociat alertei (precum alertele de tip botnet sau cele referitoare la URL-uri malițioase).

	Tip Malware	Număr de alerte	Procent (%)
1	Downadup	1.465.355	25,36%
2	Mirai	917.580	15,88%
3	Sality	886.722	15,35%
4	Nivdort	792.761	13,72%
5	Ramnit	290.420	5,03%
6	Avalanche	220.683	3,82%
7	Dorkbot	183.568	3,18%
8	Ghost-Push	146.875	2,54%
9	WannaCrypt	82.584	1,43%

4.3 Tipuri de sisteme informatice afectate

Un procent de 15% din totalul alertelor colectate și procesate de CERT-RO în anul 2017 conțin informații referitoare la sistemul de operare al sistemelor informatice vizate de alerte.

	Familie sistem de operare	Procent (%)
1	Linux	41,02%
2	Unix	30,13%
3	Network Devices Firmware/OS	20,65%
4	UPnP/1.0	7,76%
5	Windows	0,44%

Taxonomia utilizată de CERT-RO pentru clasificarea alertelor și incidentelor

Clasă alertă	Tip alertă	Descriere
Abusive Content	Spam	Comunicări electronice (email) nesolicitate cu caracter comercial.
Botnet	Botnet C&C Server	Sisteme informatice utilizate pentru controlul victimelor (drone, zombie) din cadrul unei rețele de tip botnet.
	Botnet Drone	Rețea de sisteme informatice infectate controlate de alte persoane/organizații decât deținătorii acestora.
Cyber Attacks	Bruteforce	Metodă automată de spargere a parolelor, folosită în scopul aflării credențialelor legitime ale utilizatorilor unui sistem informatic. Practic, prin intermediul unor mecanisme automate, se generează și se testează un număr foarte mare de combinații de parole, până la aflarea credențialelor reale.
	Trackback SPAM	O formă de Spam care se bazează pe un mecanism care constă în trimiterea unui mesaj automat către un domeniu, atunci când acest domeniu este referențiat într-un site/blog extern (de obicei printr-un comentariu).
	DDoS	Un atac de tip DDoS (Distributed Denial of Service) este un atac ce vizează afectarea sau chiar întreruperea unor servicii expuse în internet (site-uri web, servere etc.).
Fraud	Phishing	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.
Compromised System	Blacklisted IP	Adrese IP care au fost înregistrate în listele cu resurse blocate (Realtime Blackhole Lists - RBL), adesea datorită faptului că au fost identificate ca sursa unor atacuri, infecții cu malware, trimitere de Spam etc.

Clasă alertă	Tip alertă	Descriere
Information Gathering	Scanner	Sisteme care scanează clase întregi de IP-uri din Internet, în scopul identificării sistemelor vulnerabile, asupra cărora poate fi lansat ulterior un atac cibernetic. Faza de scanare este faza incipientă în majoritatea atacurilor cibernetice.
Malware	Infected IP	Sisteme/servicii informatice cu rol de vector de infectare pentru alte sisteme informatice. Sistemele/serviciile practic găzduiesc, cu sau fără voia administratorului, diverse mostre de malware ce pot infecta alți utilizatori legitimi.
	Ransomware	Ransomware este un software care blochează accesul la fișierele stocate într-un sistem informatic, solicitând plata unei sume de bani în schimbul re-dobândirii accesului la acestea.
	Malicious URL	Site-uri compromise, de cele mai multe ori fără voia administratorului, ce găzduiesc diverse tipuri de malware, facilitând infectarea altor utilizatori legitimi ce vizitează linkurile respective.
Vulnerabilities	Open Protocols and Services: *Portmapper, NTP, SSDP, TFTP, CWMP, SNMP, NetBIOS, Telnet, RDP, IPMI, MsSql, NAT-PMP, mDNS, ISAKMP, Mongodb, Redis, Chargen, QOTD, Elasticsearch, Xdmcp, DB2, Open SMB, Open VNC, Open MS-SQL, Open Memcached, Open LDAP*	Protocoale sau servicii care rulează pe diferite sisteme informatice, adesea servere, care nu sunt configurate corespunzător sau reprezintă versiuni neactualizate și cu probleme de securitate cunoscute. Aceste sisteme informatice sunt vulnerabile la diferite amenințări ce pot exploata vulnerabilitățile respective.

Clasă alertă	Tip alertă	Descriere
Vulnerabilities	SSL_POODLE	Atacul POODLE folosește faptul că, atunci când o încercare de conexiune securizată eșuează, serverele vor negocia folosirea unor protocoale mai vechi, cum ar fi SSL 3.0. Un atacator care poate declanșa o eroare de conexiune, poate forța apoi utilizarea SSL 3.0 și exploatarea vulnerabilității.
	FREAK	O nouă vulnerabilitate SSL/TLS - FREAK, acronim pentru Factoring RSA Export Keys. Această vulnerabilitate permite atacatorilor să intercepteze conexiuni de tip HTTPS între clienții vulnerabili și serverele web, forțându-i să utilizeze criptografia de tip „export-grade”.
	Malicious URL	Site-uri compromise, de cele mai multe ori fără voia administratorului, ce găzduiesc diverse tipuri de malware, facilitând infectarea altor utilizatori legitimi ce vizitează linkurile respective.

Notă: Tabelele de mai sus conțin tipurile de alertele de securitate cibernetică raportate frecvent la CERT-RO. Deși gama de amenințări cibernetice este mult mai variată, nu toate se regăsesc în raportările primite de instituția noastră. Sunt menținute denumirile în limba engleză a claselor și tipurilor de alerte pentru a nu pierde sensul anumitor categorii prin traducere în limba română.

Referințe

[1] *The Biggest Cybersecurity Disasters of 2017 So Far*. Wired, iulie 2017 - https://www.wired.com/story/2017-biggest-hacks-so-far/

[2] *Data Breach Investigations Report*. Verizon, iulie 2017 - https://www.wired.com/story/2017-biggest-hacks-so-far/

[3] *https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/*

[4] *The True Cost of Cybercrime for Businesses.* Forbes, iulie 2017 - https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/

[5] *ENISA Threat Landscape. Forbes, iulie 2017 - https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/*

[6] *Fileless Malware: A Hidden Threat.* TrendMicro, 2017 - https://blog.trendmicro.com/fileless-malware-a-hidden-threat/

[7] *Attackers are increasingly living off the land.* Symantec Blog, iulie 2017 - https://www.symantec.com/connect/blogs/attackers-are-increasingly-living-land

[8] *Alertă Petya/Petwarp ransomware! O nouă amenințare informatică vizează utilizatorii sistemelor de operare Windows.* CERT-RO, iulie 2017 - https://www.cert.ro/citeste/alerta-petya-ransomware

[9] *WannaCry' - Situația la zi și Wanakiwi - un posibil instrument de decriptare!.* CERT-RO, iulie 2017 - https://www.cert.ro/citeste/review-campanie-wannacry

[10] *Mac malware more than doubled in 2017.* Computer Weekly, martie 2018, http://www.computerweekly.com/news/252436453/Mac-malware-more-than-doubled-in-2017

[11] *Hundreds Of Meltdown, Spectre Malware Smaples Found in the Wild.* Tom's hardware, februarie 2019 - http://www.tomshardware.com/news/meltdown-spectre-malware-found-fortinet,36439.html

[12] *Reading privileged memory with a side-channel. Project Zero, ianuarie 2018 - https://googleprojectzero.blogspot.ro/2018/01/reading-privileged-memory-with-side.html*

[13] *Spectre și Meltdown - Vulnerabilități CPU. CERT-RO, ianuarie 2018 - https://www.cert.ro/citeste/spectre-meltdown-vulnerabilitati-cpu*

[14] *Un număr semnificativ de utilizatori ai aplicației CCleaner sunt expuși riscului de a avea PC-urile infectate cu malware.* CERT-RO, septembrie 2017 - https://cert.ro/citeste/versiuni-ccleaner-cu-malware

[15] *The MeDoc Connection.* Talos Intelligence, iulie 2017 - *http://blog.talosintelligence.com/2017/07/the-medoc-connection.html*

[16] *UEFI malware: how to exploit a false sense of security.* We LiveSecurity, octombrie 2017 - https://www.kaspersky.com/about/press-releases/2017_kaspersky-lab-identifies-ransomware-actors-focusing-on-targeted-attacks-against-businesses

[17] *https://cuckoosandbox.org/*

[18] *http://www.misp-project.org/*

[19] *Kaspersky Lab identifies ransomware actors focusing on targeted attacks against businesses.* KasperskyLab, aprilie 2017 - https://www.kaspersky.com/about/press-releases/2017_kaspersky-lab-identifies-ransomware-actors-focusing-on-targeted-attacks-against-businesses

[20] *Ransomware-as-a-Service: Rampant in the Underground Black Market.* Fortinet, februarie 2017 - https://www.fortinet.com/blog/threat-research/ransomware-as-a-service-rampant-in-the-underground-black-market.html?utm_source=dlvr.it&utm_medium=twitter ;

[21] *Petya.2017 is a wiper not a ransomware.* Comae Technologies Blog, iunie 2017 - https://blog.comae.io/petya-2017-is-a-wiper-not-a-ransomware-9ea1d8961d3b ;
ExPetr/Petya/NotPetya is a Wiper, Not Ransomware. Securelist, iunie 2017 - https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

[22] https://www.rsaconference.com/events/us17/agenda/sessions/4518-medjack-3-new-research-on-attacks-on-hospital
[23] *GHID privind combaterea amenințărilor informatice de tip „ransomware".* CERT-RO, martie 2016 - https://cert.ro/vezi/document/ghid-protectie-ransomware
[24] *Mirai: o amenințare de tip botnet utilizată recent pentru derularea celor mai însemnate atacuri DDoS din istorie.* CERT-RO, noiembrie 2016 - https://cert.ro/citeste/mirai-botnet-ddos
[25]*The Reaper IoT Botnet Has Already Infected a Million Networks.* WIRED, octombrie 2017, https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/
[26] *The Many Tentacles of the Necurs Botnet.* CISCO blogs, ianuarie 2018, https://blogs.cisco.com/security/talos/the-many-tentacles-of-the-necurs-botnet
[27] *Microsoft Warns that Virtual Machines Could Be Turned into Botnets.* BizTech, ianuarie 2017 - https://biztechmagazine.com/article/2017/01/microsoft-warns-virtual-machines-could-be-turned-botnets
[28] *Attackers Use DDoS Pulses to Pin Down Multiple Targets.* Imperva, august 2017 - https://www.incapsula.com/blog/pulse-wave-ddos-pins-down-multiple-targets.html
[29] *OVH suffers 1.1Tbps DDoS attack.* SC Media, septembrie 2016 - https://www.scmagazineuk.com/ovh-suffers-1tbps-ddos-attack/article/532197/
[30]*Hit With Record DDoS.* KrebsOnSecurity, martie 2016 - https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
[31]*The cost of launching a DDoS attack.* Securelist, martie 2017 - https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/
[32] *Bitcoin Exchanges Under Fire.* Radware, iunie 2017 - https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/cryptocurrencies-trade-under-fire/
[33] *Kaspersky Lab Research Shows DDoS Devastation on Organizations Continues to Climb.* KasperskyLab, octombrie 2017 - https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-research-shows-ddos-devastation-on-organizations-continues-to-climb
[34] *2017 Phishing Trends & Intelligence Report.* Phishlab, februarie 2017 - https://www.phishlabs.com/phishlabs-2017-phishing-trends-intelligence-report-hacking-the-human/
[35] *New Locky Ransomware Phishing Attacks Beat Machine Learning Tools.* DarkReading, septembrie 2017 - https://www.darkreading.com/attacks-breaches/new-locky-ransomware-phishing-attacks-beat-machine-learning-tools/d/d-id/1330010
2017 Threat Landscape Survey: Users on the Front Line. SANS Institute - https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910
New Backdoor targets Russian businesses in apparent spear phishing campaign . SC Media, august 2017 - https://www.scmagazine.com/new-backdoor-targets-russian-businesses-in-apparent-spear-phishing-campaign/article/680268/
[36] *Quarterly Threat Trends Report.* Webroot, septembrie 2017 - https://s3-us-west 1.amazonaws.com/webroot-cms cdn/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf
[37] Conform datelor ICI-ROTLD publicate la http://www.rotld.ro/
[38] http://viewdns.info/data/
[39] *Cyber Incident & Breach Trends Report.* Online Trust Alliance, ianuarie 2018 - https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf
[40] *'WannaCry' - Situația la zi și Wanakiwi - un posibil instrument de decriptare!, CERT-RO, mai 2017 –* https://cert.ro/citeste/review-campanie-wannacry
[41] *Alertă Petya/Petwarp ransomware! O nouă amenințare informatică vizează utilizatorii sistemelor de operare Windows. CERT-RO, iunie 2017 - https://cert.ro/citeste/alerta-petya-ransomware*
[42] *https://www.countryipblocks.net/allocation-of-ip-addresses-by-country.php*

www.cert.ro
+4031-6202187
cooperation@cert.ro
8-10 Mareșal Averescu Blvd., 011455 Bucharest, Romania