BULETIN
CYBERINT

SEMESTRUL 1 - 2018

1) AMENINȚAREA CIBERNETICĂ - CONTEXT ȘI ACTORI

În mediul actual de securitate, caracterizat prin asimetrie și incertitudine, lista amenințărilor este completată cu un nou tip de amenințare – cibernetică – unde actorii sunt reprezentați de către entități statale și non-statale. Evoluțiile tehnologice generează noi riscuri și vulnerabilități în planul securității rețelelor și sistemele informatice.

Conform Strategiei de Securitate Cibernetică a României actorii statali, dar și cei nonstatali pot proiecta, amenințări la adresa securității cibernetice a României, prin exploatarea unor vulnerabilități de natură umană, tehnică și procedurală. În ceea ce privește categoria actorilor non-statali, amenințările cibernetice pot fi proiecate de hacktiviști, teroriști cibernetici și de către actori din spectrul criminalității cibernetice.

În ultimii ani, amenințarea cibernetică a reprezentat una dintre cele mai persistente și dinamice amenințări la adresa securității naționale a României, aflându-se într-o evoluție continuă, atât din punctul de vedere al numărului de agresiuni cibernetice, cât și al complexității metodelor specifice utilizate.

La nivelul României, cele mai importante amenințări sunt generate de actorii statali și de cei afiliați unor grupări de criminalitate cibernetică.

Atacurile cibernetice prezumat a fi derulate de către entități statale sunt de regulă de tip APT(Advanced Persistent Threat) și se caracterizează prin intensitate și complexitate tehnologică. Țintele strategice vizate, rezultatele obținute (în termeni de exfiltrare de informații strategice, de dezinformare și chiar de disrupere a serviciilor) și, nu în ultimul rând, motivația atacatorilor (care este politică, prin natura sa) atenționează asupra apartenenței lor la arsenalul amenințărilor de tip hibrid.

În 2017, atacurile derulate de către grupările de criminalitate cibernetică au cunoscut o amploare deosebită, fapt generat atât de creșterea numărului acestora cât și de varietatea țintelor vizate, de la utilizatori individuali la instituții publice. Atacatorii și-au divesificat metodele folosite și schemele de fraudare, au dezvoltat noi capabilități operaționale și s-au concentrat pe automatizarea proceselor acționale, în vederea maximizării beneficiilor financiare ale activităților criminale.

2) ACTORI STATALI

Atacurile cibernetice sponsorizate de actori statali au țintit de-a lungul timpului instituții publice de interes strategic din domenii precum afaceri externe, afaceri interne, apărare, economie, cercetare și dezvoltare sau energie. Principalul obiectiv al acestor atacuri este de a prelua controlul asupra rețelelor infectate pentru a colecta informații sensibile sau confidențiale, fenomen cunoscut și sub numele spionaj cibernetic.

Complexitatea infrastructurilor de atac, a modului de operare și a modalităților de exfiltrare folosite indică angrenarea unor resurse semnificative (umane, financiare și tehnologice) și converg către atribuirea atacurilor cibernetice unor entități asociate actorilor statali.

Cyber Kill Chain este o listă ordonată a fazelor unui atac cibernetic de tip APT, permițând experților în securitate cibernetică înțelegerea acestui tip de agresiune cibernetică, de la etapa planificării până la îndeplinirea obiectivelor.

2.1) CYBER KILL CHAIN

Reconnaissance - atacatorii testează rețelele vizate în vederea identificării unor vulnerabilități. Pe lângă acest fapt, aceștia ar putea viza captarea de credențiale necesare penetrării rețelelor informatice, dar și informații necesare unui atac de tip spearphishing.

Weaponization - crearea unei aplicații malware adaptată obiectivelor vizate în urma penetrării rețelei informatice a victimei.

Delivery - transmiterea respectivei aplicații malware printr-un mesaj de tip email sau printr-un link către o pagină web infectată.

Exploit - execuția aplicației în cadrul rețelei victimei.

Installation - instalarea aplicației pe rețeaua victimei.

Command and control - crearea unui canal de comunicare între atacator și rețeaua victimei, prin care atacatorul poate executa comenzi asupra acesteia de la distanță.

Actions - îndeplinirea scopului atacatorului.

2.2) Atacuri notabile de tip APT

Red October (nivel mediu de tehnologizare): Tactics, Techniques and Procedures - TTP (spearphishing, inginerie socială, dropper, trojan), Motivație (spionaj cibenetic), Ținte (instituții guvernamentale diplomatice și organizații din domeniul cercetării științifice)

APT 28 (nivel foarte înalt de tehnologizare): TTP (spearphishing, inginerie socială, wattering hole, exploatare de vulnerabilități, backdoor), Motivație (spionaj cibenetic), Ținte (instituții guvernamentale din domeniile militar și politc, ONG-uri, jurnaliști și formațiuni politice din state membre NATO/UE)

APT 29 (nivel foarte înalt de tehnologizare): TTP (spearphishing, inginerie socială, aplicații customizate de tip backdoor), Motivație (spionaj cibenetic), Ținte (instituții guvernamentale, think-tank-uri, ONG-uri, agenții media)

Cosmic Duke (nivel mediu de tehnologizare): TTP (droppers, loaders, info-stealers, exploits, keylogger), Motivație (spionaj cibenetic), Ținte (instituții guvernamentale ale unor state membre NATO/UE)

Mini Duke (nivel înalt de tehnologizare): TTP (inginerie socială, dropper, backdoor customizat, arhitectură modulară), Motivație (spionaj cibenetic), Ținte (instituții guvernamentale din sectoarele afacerilor externe, diplomației, energiei, telecomunicațiilor și apărării)

Turla (nivel foarte înalt de tehnologizare): TTP (watering hole, 0-day exploits, inginerie socială, utilizarea unor comunicații prin satelit pentru exfiltrarea datelor), Motivație (spionaj cibenetic), Ținte (Ambasade, oficii consulare, organizații guvernamentale din domeniul afacerilor externe)

3) CYBER-CRIME

Referitor la activitatea grupărilor de criminalitate cibernetică, se pot distinge două categorii: "cyber - enabled crime" - activități ale indivizilor sau ale grupărilor de criminalitate cibernetică ce se folosesc de spațiul cibernetic pentru a-și îndeplini obiectivele, dar și de tipul "cyber-dependent crime" - activități ale indivizilor sau grupărilor de criminalitate cibernetică ce pot fi desfășurate doar în spațiul cibernetic.

Atacurile cibernetice derulate de astfel de grupări au înregistrat o amploare deosebită, instituțiile publice fiind incluse în spectrul de ținte vizate de atacatori. Începând cu luna aprilie 2017, au fost lansate mai multe atacuri ransomware și criptocurrency miner malware (sub forma unor campanii cunoscute sub numele WannaCry, Adylkuzz, GoldenEye, Locky, Bad Rabbit) care au vizat sisteme informatice de la nivel global, inclusiv din România.

Campaniile ransomware au generat riscuri de compromitere a datelor confidențiale gestionate de instituțiile publice și de afectare, cel puțin temporară, a activității acestora.

De asemenea, în 2017 s-au intensificat atacurile cibernetice realizate prin diseminarea de aplicații malware bancare (DRIDEX, Trickbot, Emotet) utilizate pentru sustragerea datelor personale/confidențiale și credențialelor de autentificare la conturile de internet banking.

3.1) Ransomware, criptocurrency miner malware, banking trojans

GoldenEye/NotPetya - În data de 27 iunie 2017, a fost lansată o campanie ransomware, denumită GoldenEye/NotPetya, care a vizat și afectat mai multe entități publice și private la nivel global, din domeniile telecomunicațiilor, transporturilor, energiei, mass-media și financiar. Această campanie s-a răspândit prin două modalități: phishing și exploatarea unor vulnerabilității ale Microsoft Windows.

Adylkuzz - Aplicația malware Adylkuzz, lansată la sfârșitul lunii aprilie 2017, folosește puterea de calcul a sistemelor informatice pentru a genera monedă virtuală (monero), fiind astfel un atac cibernetic de tipul cryptocurrency mining malware. Sistemele de operare care pot fi afectate sunt versiunile Windows, în cazul în care nu au aplicate actualizări de securitate la zi.

WannaCry/WannaCrypt - În prima jumătate a lunii mai 2017, un atac major de tip ransomware a afectat mai multe companii și organizații la nivel global. WannaCry/WannaCrypt a avut suport pentru 28 de limbi, criptând 179 de tipuri de fișiere și solicitând victimelor plata unei recompense în bitcoin (BTC), în valoare de 300$ – 600$.

Dridex - Dridex este un trojan bancar faimos pentru nivelul de sofisticare, complexitate, dar și pentru capacitatea de a rămâne nedetectat pe dispozitivele pe care le infectează. Odată infectate, dispozitivele sunt incluse într-o rețea de boți (botnet) care poate fi utilizată pentru a desfășura și alte atacuri. În 2017, a apărut a patra versiune a acestui malware, care infectează utilizatorii finali prin distribuție de mesaje tip spam sau prin exploatarea unor vulnerabilități.

Bad Rabbit - La 24.10.2017, în Europa de Est și Asia, mai multe agenții guvernamentale, cât și entități private au fost afectate de către un nou tip de ransomware, asemănător cu Petya și NotPetya. Ransomware-ul, pe care cercetătorii l-au numit Bad Rabbit, a avut peste 200 de ținte din mai multe state, infecția fiind realizată printr-o aplicație malware care pretinde a fi un installer pentru Adobe Flash Player.

4) STATISTICI CYBERINT 2017

Trojan—Program informatic care pare a avea o funcție utilă, legitimă, dar deține și una ascunsă care scapă mecanismelor de securitate, uneori exploatând vulnerabilități ale sistemelor vizate. Astfel, odată rulat, programul poate derula activități nelegitime, precum sustragerea de informații, afectarea calculatorului gazdă sau crearea unor căi disimulate de acces de la distanță la sistemul infectat.

Botnet—O rețea de calculatoare infectate în mod intenționat prin diverse metode de către o persoană/entitate rău-intenționată în vederea utilizării acestora în folosul celui care controlează rețeaua (botmaster), pentru sustragerea de date confidențiale, de obicei financiar—bancare, pentru inițierea de atacuri de tip distributed-denial-of-service (DDoS), pentru spargerea parolelor sau pentru căutarea și exfiltrarea de informații.

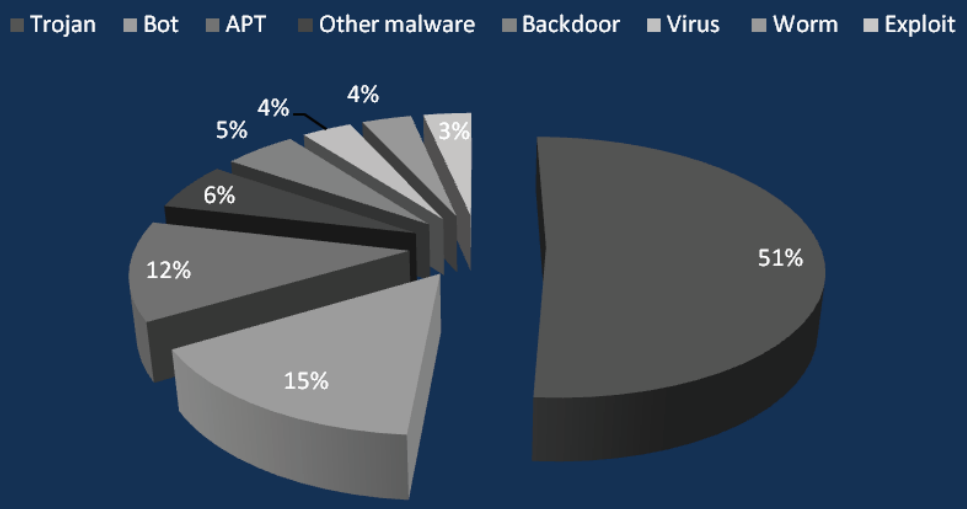
Backdoor—Program creat pentru a ocoli sistemele de securitate sau pentru autentificare neautorizată la un sistem/rețea.

Virus—Program care se poate autoreplica în cadrul unui sistem și care se poate propaga în alte calculatoare din rețea fără știința utilizatorului. Acesta poate afecta negativ funcționalitatea, integritatea, disponibilitatea sistemului sau datelor conținute de acesta.

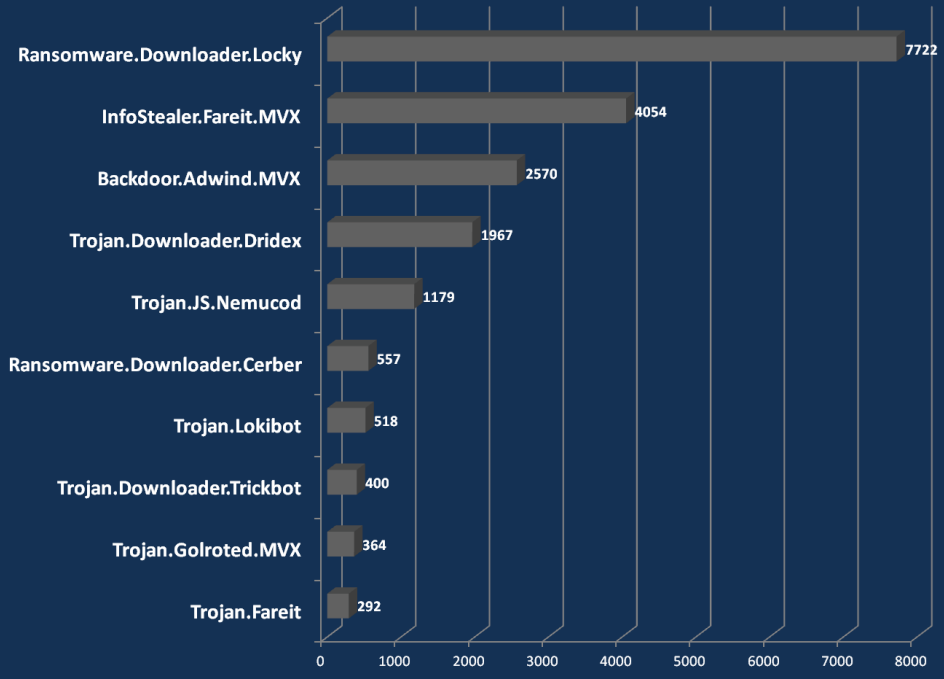
Worm—Malware care are capacitatea de a se autoreplica și propaga într-o rețea de calculatoare folosind resursele rețelei, fără a se atașa unui alt program sau proces.

Exploit—Un software sau o secvență de cod care folosește o vulnerabilitate a unei aplicații sau a unui sistem informatic cu scopul de a obține controlul asupra acestuia sau de a derula atacuri de tip denial-of-service (DOS).

CELE MAI FRECVENTE TIPURI DE ATACURI



TOP 10 CAMPANII MALWARE ÎN ROMÂNIA - 2017



5) BUNE PRACTICI

Soluțiile antivirus instalate în cadrul rețelelor informatice trebuie să aibă semnăturile actualizate la zi. Administratorii sau utilizatorii individuali trebuie să configureze scanări automate folosind soluțiile antivirus instalate, la intervale de timp regulate. În cazul unei suspiciuni legate de modul de funcționare al sistemului informatic, este recomandabilă o scanare manuală folosind soluția antivirus instalată.

Utilizatorii trebuie să fie vigilenți la deschiderea documentelor ce provin din surse necunoscute sau care nu sunt de încredere, în special prin folosirea accesului la mail.

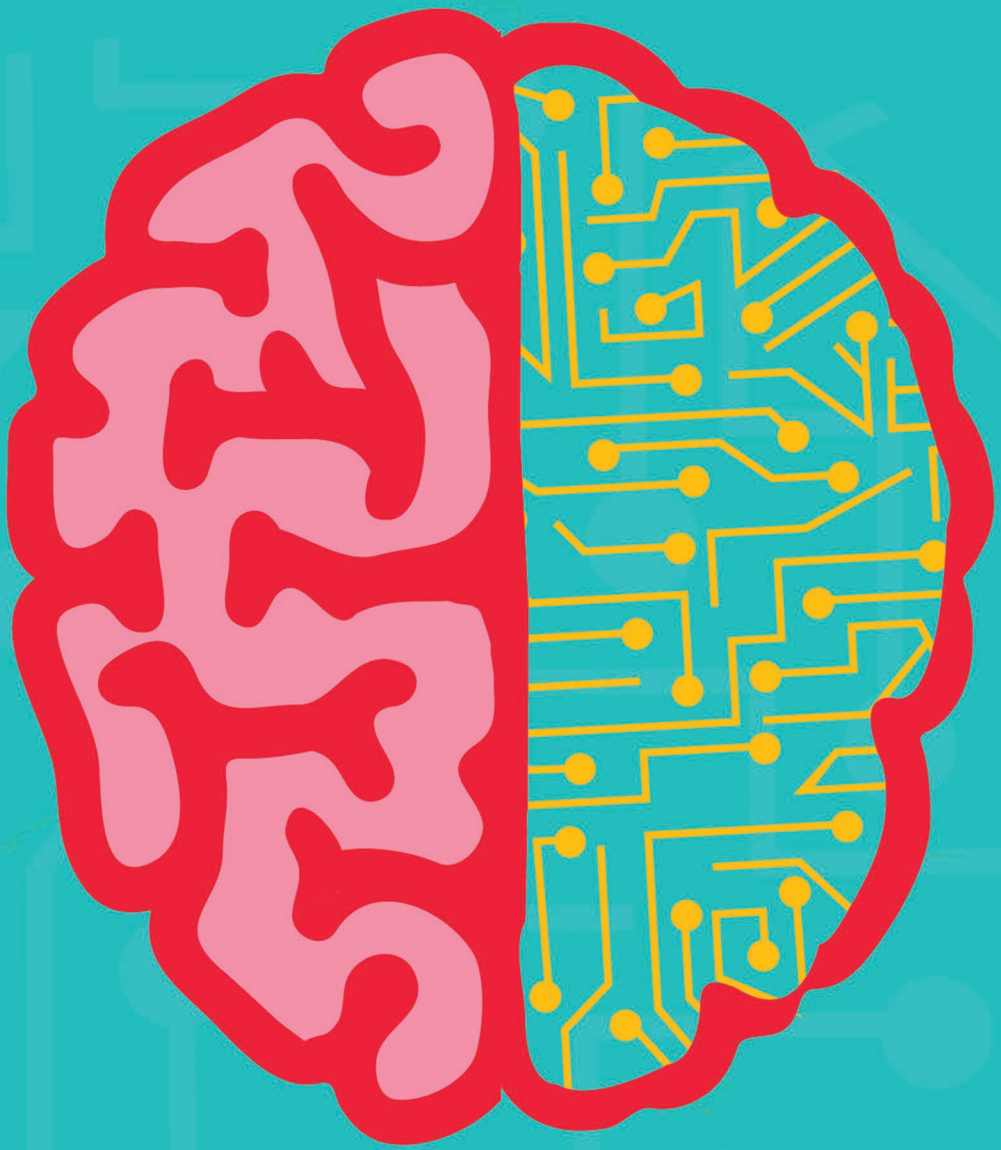
De asemenea, este o practică folosită de administratorii de sisteme informatice să configureze serverul de email pentru a bloca sau șterge acele emailuri care au ca atașamente fișiere ale căror extensii apar în listele cunoscute de fișiere ce răspândesc aplicații malware.

Este recomandată efectuarea back-up-ului de sistem, atât de către administratorii sistemelor informatice, cât și de utilizatorii individuali, la intervale de timp regulate, în scopul minimizării pierderilor generate de potențiale aplicații malware.

Administratorii de sistem trebuie să aloce privilegiile minimale necesare desfășurării unei activități. De asemenea, atunci când un program solicită utilizatorului parola de administrator pentru a-și continua execuția, acesta trebuie să fie vigilent și să se asigure că este vorba despre un program legitim.

În cazul infectării, în urma unor campanii de distribuție a unor aplicații malware, trebuie să se evite pe cât posibil plata recompensei cerute.

Este necesară actualizarea aplicațiilor sau a sistemelor de operare utilizate, deoarece versiunile mai vechi ale acestora conțin vulnerabilități de securitate, exploatate pe scară largă de către distribuitorii de malware.



6) INTERNET OF THINGS

Internet of Things (IoT) desemnează obiecte ce încorporează dispozitive electronice inteligente, inter-conectate prin intermediul Internetului. Astfel, printre miliardele de dispozitive care utilizează această tehnologie, putem regăsi obiecte folosite în activitățile de zi cu zi (cuptor inteligent, expresor inteligent, televizor inteligent, sisteme de iluminat inteligente, etc.).
Riscurile în această zonă vor deveni mai complexe și mai dificil de gestionat, având în vedere că:

- acțiunile ofensive desfășurate în spațiul cibernetic folosesc metode de atac adaptate permanent evoluțiilor tehnologice și vulnerabilităților identificate;
- nu există un număr ridicat de soluții disponibile pentru preîntâmpinarea unor astfel de incidente.

Începând din a doua jumătate a anului 2016, a fost înregistrată diseminarea aplicației malware „Mirai", pe o gamă variată de dispozitive IoT, în vederea creării unor rețele de boți. Aceste rețele pot fi utilizate pentru derularea de atacuri cibernetice de mare amploare.

Din punct de vedere legislativ, la nivelul UE se derulează demersuri pentru etichetarea dispozitivelor IoT, după modelul etichetelor energetice, scopul fiind de a clasifica aceste dispozitive în funcție de nivelul de securitate cibernetică al acestora.


PENTRU SECURIZAREA DISPOZITIVELOR IoT ȘI EVITAREA COMPROMITERII ACESTORA SE RECOMANDĂ:
01
schimbarea parolei implicite;
02
utilizarea cu precădere a unei interfețe HTTPS pe calculatorul care gestionează dispozitivele din categoria IoT;
03
închiderea protocoalelor de conexiune suplimentare ale dispozitivelor;
04
evaluarea necesității includerii unui nou dispozitiv IoT în rețeaua proprie. În unele cazuri, dispozitivele IoT includ o serie de funcționalități care nu optimizează activitățile curente.

7) PROIECȚII PENTRU 2018 ÎN DOMENIUL CYBER

Tehnologiile din domeniile inteligenței artificiale (IA) și machine learning (ML) vor începe să fie utilizate și pentru realizarea de agresiuni cibernetice.

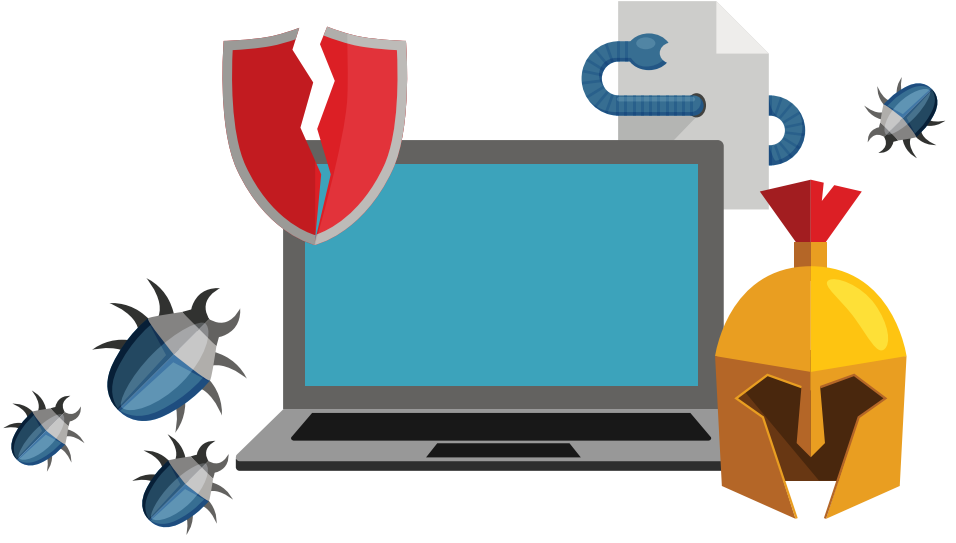
Se vor perfecționa metodele de anonimizare ale unor atacuri cibernetice complexe, folosindu-se tehnicile file-less și file-light malware.

Actorii statali vor încerca să desfășoare și operațiuni de tip false-flag.

Tehnologia pe care se bazează cripto-monedele, blockchain, va face parte din arsenalul grupărilor de criminalitate cibernetică.

Troienii bancari vor fi cauza mai multor pierderi financiare decât aplicațiile de tip ransomware.

Dispozitivele IoT, în special cele cu o valoare de piață ridicată, vor fi vizate de campanii ransomware și vor fi utilizate ca infrastructură pentru desfășurarea unor atacuri persistente și îndelungate.



www.sri.ro