
Statistici
ATACURI CIBERNETICE
Domeniul sănătății vizat de campanii RANSOMWARE
Securitatea dispozitivelor mobile
ROMANIA
SRI
SERVICIUL ROMAN DE INFORMATII
Patria a priori
Blockchain
SRI va organiza a treia ediție a CYDEX
BULETIN CYBERINT
SEMESTRUL 2 - 2019

1

ROMÂNIA A DEVENIT NAȚIUNE-SPONSOR LA CENTRUL NATO DE EXCELENȚĂ PENTRU APĂRAREA CIBERNETICĂ **(CCDCOE)**

În 13 iunie 2019, **România a devenit națiune-sponsor** *(Sponsoring Nation/SN)* **la Centrul NATO de Excelență pentru Apărarea Cibernetică prin Cooperarae** *(Cooperative Cyber Defence Centre of Excellence/CCDCoE)* de la Tallinn, **prin Serviciul Român de Informații** și **Ministerul Apărării Naționale.**

CCDCoE a fost înființat în 2008 și are ca scop consolidarea cooperării, a capabilităților și a schimbului de informații în domeniul securității cibernetice între statele membre NATO.

Centrul organizează exerciții cibernetice, seminarii și conferințe pe teme legislative sau de *policy*, precum și cursuri tehnice destinate pregătirii NATO și a statelor membre ale Alianței în vederea gestionării amenințărilor cibernetice.

De asemenea, CCDCoE coordonează proiecte de cercetare în domeniul cibernetic.

Astfel, ca urmare a eforturilor depuse de la nivel național, în data de 13 iunie 2019, a avut loc ceremonia oficială de arborare a steagului României la sediul CCDCoE, România devenind SN prin SRI și MApN.
Obținerea de către România a statutului de **națiune-sponsor la CCDCoE** oferă o serie de oportunități:

1. DETAȘAREA UNOR **REPREZENTANȚI** NAȚIONALI ÎN CADRUL CCDCOE;
SRI a detașat încă din 1 septembrie 2018, în cadrul CCDCoE, un ofițer cu specializare tehnică. În prezent, urmare a rezultatelor excelente obținute, a fost promovat în funcția de Manager al Departamentului de Analiză Malware al CCDCoE, având totodată calitatea de instructor la două din dintre cursurile de specialitate organizate în cadrul Centrului NATO (Botnet Mitigation Course și Malware and Exploit Essentials).

2. PARTICIPAREA ROMÂNIEI LA **CEL MAI MARE EXERCIȚIU DE SECURITATE CIBERNETICĂ AL NATO** – *LOCKED SHIELDS* (ÎN ANUL 2019, AU PARTICIPAT MAI MULT DE 1200 DE PARTICIPANȚI, DIN 30 DE STATE);
Locked Shields este un exercițiu de tip Red Team vs. Blue Team care se focusează pe scenarii realiste, tehnologii de ultimă generație și în care se simulează întreaga complexitate a unui incident cibernetic complex la adresa infrastructurilor IT&C naționale.

3. PARTICIPAREA ROMÂNIEI LA EXERCIȚIUL DE SECURITATE CIBERNETICĂ AL NATO – **CROSSED SWORDS**;

Crossed Swords este un exercițiu cibernetic anual, de tip Red Team, la care participă experți în pentesting, digital forensics și situational awareness. Ediția din 2019 a întrunit mai mult de 100 de experți din 23 de țări participante. Scopul exercițiului este testarea capabilităților și cunoștințelor tehnice ale participanților, necesare în planificarea și executarea unei operațiuni cibernetice, în conexiune cu elemente din alte domenii.

4. POSIBILITATEA DE A BENEFICA DE **REZULTATELE PROIECTELOR DE CERCETARE**, CU APLICABILITATE ÎN DOMENIUL CIBERNETIC, DEZVOLTATE DE CCDCOE ÎN PLAN INTERN;

5. POSIBILITATEA DE A BENEFICIA DE EXPERTIZA **CCDCOE PE DOUĂ DOMENII IMPORTANTE: *STRATEGY*** ȘI ***LAW;***

La nivelul CCDCoE a fost elaborat **Manualul de la Tallinn** (ce a ajuns la versiunea 2.0) privind dreptul internațional aplicabil operațiunilor cibernetice.

6. POSIBILITATEA DE A PARTICIPA LA CONFERINȚELE ORGANIZATE LA **INTERNATIONAL CENTER FOR DEFENCE AND SECURITY / ICDS DIN TALLINN.**

CCDCOE

2

DOMENIUL SĂNĂTĂȚII
VIZAT DE CAMPANII
RANSOMWARE

Atacurile de tip ***ransomware*** reprezintă una dintre principalele activități la care recurg entități din mediul criminalității cibernetice, provocând pagube în **mod nediscriminatoriu**, prin afectarea unui **spectru larg de victime** la nivel internațional (instituții guvernamentale, entități private, organizații, utilizatori individuali).

Amploarea campaniilor ***ransomware*** din ultimii ani este un rezultat al fenomenului ***ransomware-as-a-service***, care presupune comercializarea de ***malware*** cu capabilități de tipul ***criptare fișiere*** către ***orice persoană/grupare interesată***, care nu trebuie să dețină, în mod obligatoriu cunoștințe tehnice. Forumurile de criminalitate informatică (publice, dar cu acces restricționat sau cele de pe **DarkWeb**), constituie mediul în care se comercializează ilegal astfel de servicii.

Ultimii ani au fost marcați de numeroase campanii ransomware, printre care amintim ***WannaCry, Locky, GoldenEye, Jaff, DMA Locker, Dharma, SamSam, Bad Rabbit, CryptoLocker, Fusob, Cerber, Ryuk, GandCrab etc.***

Pe 12 mai 2017, campania globală de ransomware WannaCry a afectat mai mult de 200,000 de calculatoare din cel puțin 100 de țări. În Regatul Unit, 80 din cele 236 de trusturi ale sistemului de asistență medicală de stat **National Health Service (NHS)** de pe teritoriul Angliei au fost afectate.

În 2019, infrastructuri **IT&C de pe teritoriul României** au continuat să fie ținta unor campanii ransomware, fiind vizat îndeosebi **domeniul sănătății**. Derularea de atacuri *ransomware* la adresa domeniului medical din România se subscrie unei **tendințe observate la nivel internațional**.

Orientarea atacatorilor către domeniul sănătății este justificată inclusiv de **rolul vital** al elementelor de **infrastructură IT&C** ce deservesc activitățile derulate în cadrul unor astfel de instituții. Un astfel de atac, poate afecta instituții din domeniul sănătăți prin criptarea datelor, inclusiv a celor cu privire la pacienți, blocarea accesului la acestea, motive pentru care pot apărea întârzieri în consultarea pacienților și în administrarea tratamentelor. Campaniile de *ransomware* creează pentru atacatori premisele unor câștiguri financiare consistente, prin răscumpărările ce trebuie achitate.

Pentru a **preveni** astfel de situații, este recomandat ca infrastructura IT&C din cadrul instituției să dispună de măsuri de protecție, precum implementarea unor **politici de securitate** privind accesarea unor e-mailuri provenite din surse necunoscute, realizarea de backup-uri, instalarea unor soluții de tip antivirus, realizarea în mod constant a actualizărilor de sistem și ale aplicațiilor utilizate.

Ulterior infecției, este importantă **raportarea incidentului către autorități** pentru a identifica cea mai bună soluție. Există situații în care în mediul online sunt disponibile deja cheile de decriptare necesare, publicate fie de autorități, companii de securitate și, uneori, chiar de atacatori.

În situațiile în care nu pot fi identificate chei de decriptare, trebuie menționat că **plata răscumpărării solicitate de atacator** (de cele mai multe ori în monede virtuale precum *Bitcoin - BTC sau Monero -XMR*) **nu asigură obținerea cheii**. Ba mai mult, plata acesteia poate atrage includerea instituției de către atacator pe o listă a plătitorilor și implicit vizarea acesteia în campanii *ransomware* ulterioare.

3

PROTECȚIA SISTEMELOR DE CONTROL INDUSTRIAL **SCADA** CU AJUTORUL INSTRUMENTELOR CE FOLOSESC INTELIGENȚA ARTIFICAIALĂ

Sistemele de control industrial **SCADA**[1] sunt sisteme de automatizare ce controlează și monitorizează procese tehnologice ce au loc în obiective industriale civile sau militare (ex. centrale nucleare, hidrocentrale, facilități de producere și distribuție a energiei electrice, sisteme de control trafic - rutier, feroviar, aerian, facilități de extracție și transport gaze naturale și țiței etc.), care, prin importanța și rolul lor, sunt asimilate infrastructurilor critice sau celor cu valențe critice.

Aducerea acestor sisteme în stare de neîntrebuințare sau de folosință în afara parametrilor optimi, constituie o **amenințare la adresa facilităților deservite**, generând un impact considerabil ce se poate traduce în pierderi economice, influențarea vieții socio-politice sau chiar pierderea de vieți omenești.

Odată cu evoluția tehnologică și din rațiuni de **reducere a costurilor și eficientizare a proceselor**, contrar recomandărilor de bune practici, sistemele SCADA au început să fie interconectate cu alte rețele, iar în unele cazuri la Internet.

Dat fiind faptul că în prezent, există entități care aleg să administreze de la distanță aceste sisteme, inclusiv folosind mediul Internet, **crește riscul de derulare a unor atacuri cibernetice care pot indisponibiliza sau compromite echipamentele industriale gestionate prin intermediul sistemelor SCADA**.

În context, infrastructurile critice ce folosesc sisteme de control industrial **SCADA au devenit ținte ale unor acțiuni ofensive derulate de regulă de actori statali**. Astfel, aceștia recurg la atacuri cibernetice de tip APT[2], care exploatează vulnerabilități tehnologice, procedurale și umane ale infrastructurilor țintă.

Aceste atacuri cibernetice sunt **extrem de complexe** și, în cele mai multe cazuri, sunt **nedetectabile de soluțiile de securitate clasice** (ex: antivirus). Astfel, avansul tehnologic a generat necesitatea dezvoltării și implementării unor instrumente actualizate care să sprijine demersurile de **prevenire și contracarare a amenințărilor cibernetice**. Printre soluțiile identificate în acest sens au fost cele bazate pe **inteligență artificială** ce folosesc **analiza comportamentală**[3].

---

[1] *Supervisory Control and Data Acquisition System.*
[2] *Advanced Persistent Threat.*
[3] *Analiza informațiilor rezultate din activitatea unei rețele IT&C, pentru a înțelege comportamentul și a identifica posibile patern-uri cu scopul de a îmbunătăți securitatea cibernetică sau a aplica măsuri de prevenire.*

Instrumentele în cauză sunt instalate în cadrul sistemelor SCADA sau în rețelele de perimetru, **învățând comportamentul din cadrul rețelei și** având posibilitatea de a identifica **modificări/ anomalii de trafic sau de funcționare**. Astfel, se creează posibilitatea detectării unor atacuri cibernetice derulate inclusiv în complicitate cu persoane care au acces autorizat la rețea.

Soluțiile de securitate ce folosesc analiza comportamentală își creează propriile **semnături de comportament** specifice rețelelor în care au fost instalate. În acest fel, ar putea fi posibilă detectarea unor atacuri cibernetice care exploatează **vulnerabilități necunoscute anterior (*zero day*)**, a unor **vulnerabilități tehnologice** sau ale **spectrului electromagnetic** care influențează funcționarea sistemelor SCADA precum și **a erorilor umane** ori a anomaliilor din rețea.

În cazul în care sunt identificate anomalii de comportament ale rețelei, instrumentele bazate pe inteligența artificială alertează administratorul. Alerta de securitate poate reprezenta un **indicator inițial al unui atac cibernetic** la adresa infrastructurii deservite de sistemul SCADA, în acest caz, administratorul demarând acțiunile necesare în vederea **mitigării incidentului**.

Considerând rolul îndeplinit de **sistemele SCADA** este important ca acestora să le fie asigurată corespunzător **securitatea cibernetică prin aceste sisteme bazate pe inteligența artificială**, a căror analiza comportamentală generează un nivel sporit de securitate.

4

ROMÂNIA VA ORGANIZA
CAMPIONATUL EUROPEAN DE SECURITATE CIBERNETICĂ
EDIȚIA 2019

În perioada 09-11 octombrie 2019 va avea loc la Palatul Parlamentului din București etapa finală a **Campionatului European de Securitate Cibernetică ediția 2019 (ECSC19)**, competiție destinată tinerelor talente în domeniul *cyber*, la care România participă pentru al cincilea an consecutiv. În edițiile din 2016 și 2017, echipa României a obținut titlul de vice-campioană.

În procesul de selecție și antrenare a echipei naționale s-au implicat alături de *Serviciul Român de Informații, CERT-RO* și *Asociația Națională pentru Securitatea Sistemelor Informatice*, o serie de companii din zona privată - *Orange, BitSentinel, certSIGN, Cisco, Microsoft, Clico, Palo Alto Networks, Emag și Cybertas* - în calitate de parteneri/sponsori.

În aprilie 2019 a avut loc etapa de calificare online pentru selecția echipei României la ECSC19, care s-a desfășurat în cadrul poligonului cibernetic al Serviciului Român de Informații.

Concret, candidaților le-au fost testate cunoștințe în domenii precum **securitatea aplicațiilor web, apărarea cibernetică, criptografia, analiza traficului de rețea, reverse engineering și public speaking**. Ulterior, pentru a veni în sprijinul echipei selecționate să reprezinte România, SRI și partenerii organizează sesiuni de training pentru creșterea expertizei și dezvoltarea spiritului de echipă.

La concursul de anul acesta vor participa reprezentanți din **18 țări europene**, fiecare fiind reprezentată de câte o echipă formată din **10 concurenți împărțiți în două grupe de vârstă**: 16-20 de ani și 21-25 de ani, cu câte 5 concurenți fiecare.

5

SRI
VA ORGANIZA
A TREIA EDIȚIE A
CYDEX

În perioada **30 septembrie - 2 octombrie va avea loc CyDEx19**, singurul exercițiu de securitate cibernetică din Romania de tip *hands on* - axat pe componenta practică - ce asigură un nivel de realism extrem de avansat prin desfășurarea activităților într-un poligon de securitate cibernetică.

Exercițiul are ca principal obiectiv exersarea capacităților de apărare în domeniul securității cibernetice, împotriva amenințărilor la adresa infrastructurilor IT&C cu valențe critice pentru securitatea națională.

Demersul se înscrie în eforturile SRI de a crea un mecanism eficient de avertizare, alertă și reacție la incidentele cibernetice, precum și de a dezvolta cooperarea dintre sectorul public și cel privat în domeniul securității cibernetice.

Exercițiul de anul acesta va întruni aproximativ **100 de entități participante din mediul public, privat și academic**. În 2019, în comparație cu edițiile din anii anteriori, CyDEx va cuprinde scenarii mai complexe, etapizate, propuse și concepute, atât de entități din mediul public, cât și de cel privat. În plus, poligonul cibernetic pus la dispoziție de SRI va fi disponibil entităților participante timp de două săptămâni înainte de eveniment pentru ca participanții să se familiarizeze cu acesta.

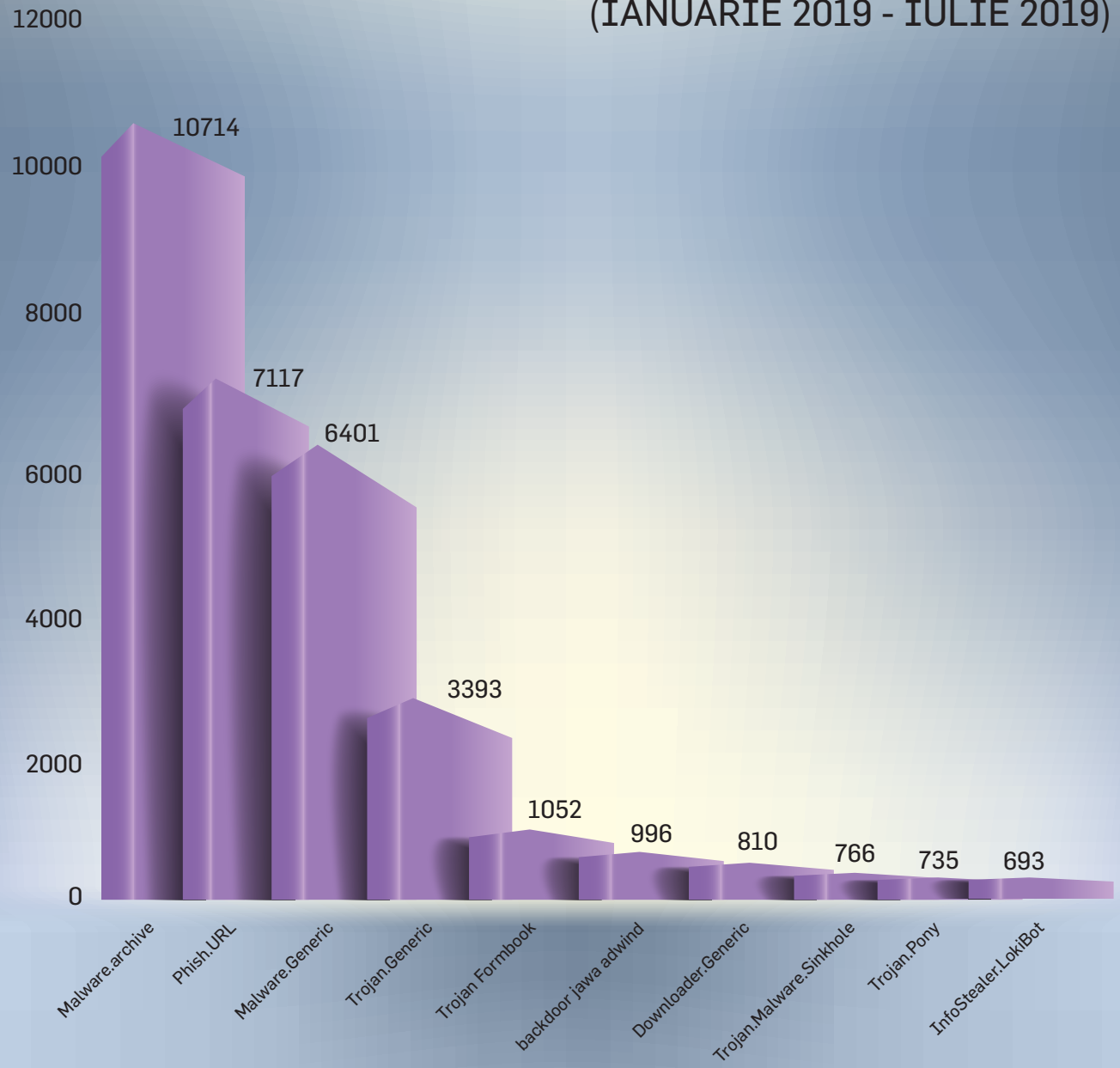
EXERCIȚIUL CYDEX19 VA PERMITE:

- verificarea și stimularea mecanismelor de cooperare între instituțiile publice cu responsabilități în domeniul securității naționale și, în general, între instituțiile publice, mediul privat și cel academic;
- dezvoltarea unui mecanism eficient de avertizare, alertă și reacție la incidente de securitate cibernetică;
- verificarea nivelului de expertiză tehnică al specialiștilor din cadrul entităților participante în cazul unui incident cibernetic major la nivel național;
- creșterea nivelului de conștientizare atât la nivelul instituțiilor publice, cât și la nivelul celor private cu privire la amenințările din spațiul cibernetic, precum și la efectele cauzate de un incident cibernetic major la nivel național.

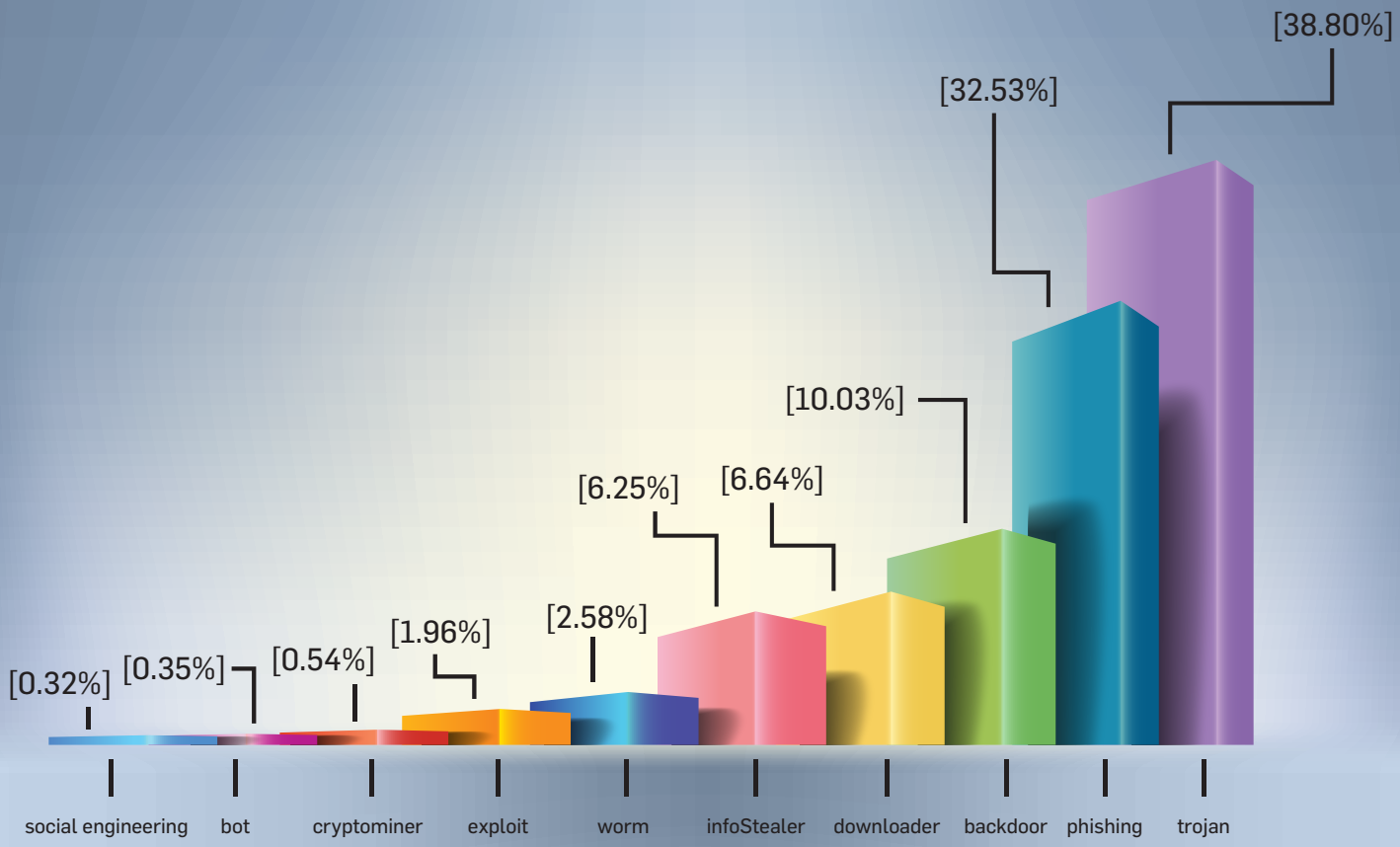
6

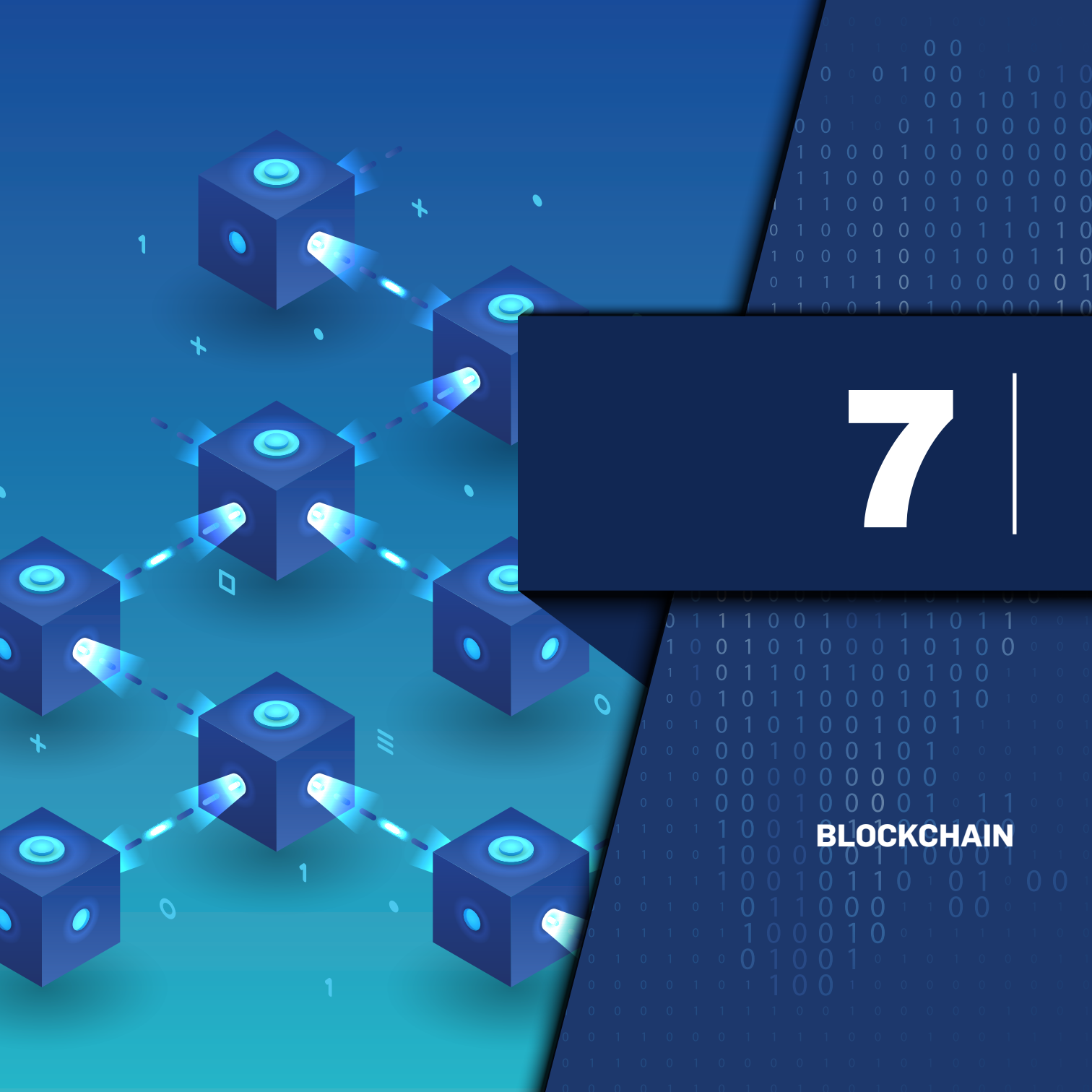
STATISTICI
ATACURI CIBERNETICE

TOP 10 CAMPANII MALWARE ÎN ROMÂNIA
(IANUARIE 2019 - IULIE 2019)



CELE MAI FRECVENTE TIPURI DE ATACURI





7

BLOCKCHAIN

Blockchain-ul sau tehnologia blocurilor, face parte din ansamblul rețelelor de tip **tehnologie a registrelor distribuite** (distributed ledger technology - DLT) și este un registru de date organizat în blocuri de informație înlănțuite, partajate, replicate și sincronizate între membrii rețelei. Principiile care stau la baza blockchain sunt **criptografia** și rețelele de tip **peer-to-peer** (absența unui intermediar).

Termenul și principiile blockchain au fost implementate pentru prima dată în proiectul de monedă virtuală **Bitcoin** (BTC) lansat în 2008 de o persoană/un grup de persoane sub numele de **Satoshi Nakamoto**.

*Toate tranzacțiile cu monedă **Bitcoin** care au avut vreodată loc în cadrul rețelei sunt **validate** de nodurile existente in rețea prin putere de calcul, generându-se noi unități de monedă. Ulterior, aceste tranzacții, utilizând criptografia, sunt organizate în blocuri și adăugate registrului blockchain.*

PRINTRE CARACTERISTICILE PRINCIPALE ALE ACESTEI TEHNOLOGII SE NUMĂRĂ:

Cu toate acestea, există situații în care arhitectul și dezvoltatorii unui blockchain pot reduce gradul de anonimitate pentru a spori transparența sau pentru a conferi alte beneficii utilizatorilor.

Toate aceste caracteristici ale tehnologiei blockchain asigura o securitate sporită a rețelelor prin implementarea criptografiei și prin asigurarea unui control distribuit asupra operațiunilor realizate la nivelul blocurilor.

DIN PUNCT DE VEDERE AL DEȚINERII ȘI ACCESULUI, BLOCKCHAIN-UL POATE FI DE TREI TIPURI:

PUBLIC - nimeni nu deține rețeaua, orice persoană/entitate având posibilitatea de a se conecta/efectua operațiuni în cadrul acesteia, respectiv de a deveni nod prin descărcarea, stocarea și actualizarea constantă a întregului registru de date.

PRIVAT - accesul în vederea înscrierii de date și dobândirii calității de nod în cadrul rețelei este restricționat către anumite persoane/entități în funcție de criterii stabilite de deținătorul rețelei.

Un nod reprezintă un participant în cadrul rețelei care îndeplinește una sau mai multe funcții conform arhitecturii blockchain-ului. În unele situația această funcție poate fi reprezentată de utilizarea puterii de calcul pentru validarea unor operațiuni.

CONSENSUS/SINDICAT - aparține unui grup definit de noduri stabilite anterior, acestea având calitatea de deținători și dreptul de a decide participanții în cadrul rețelei.

Încă de la apariția tehnologiei, companii private și-au orientat atenția către a integra blockchain-ul în activitățile pe care le derulează, în vederea eficientizării acestora.

Din perspectiva **sectorului public** și al **îmbunătățirii serviciilor furnizate cetățenilor**, implementarea unor tehnologii de tip blockchain ar putea aduce beneficii în ramuri precum **managementul identității** (documente de identitate, acte de căsătorie, pașapoarte, permis de conducere etc.), **optimizarea sistemului de vot**, (ex. Estonia, Elveția, Danemarca, Rusia), **optimizarea sistemului de colectare a taxelor** (Estonia), **gestionarea registrelor medicale, gestionarea în mod integrat a parcursului scolar al cetățenilor.**

Prin implementarea tehnologiei blockchain în sistemul de educație, cetățenii vor putea accesa în mediul digital registrele privind formele de învățământ absolvite, certificate de pregătire obținute, fișa matricolă, precum și alte informații introduse atât de profesori și instituții cât și de persoanele evaluate pe baza unui **sistem de validare** a acestora de către părțile implicate.

Implementarea unui **sistem digital** de colectare a taxelor, utilizând tehnologii ale registrelor distribuite ar permite cetățenilor să dețină un cont personal prin intermediul căruia să poată plăti contribuțiile către stat, transparența, imuabilitatea și caracterul distribuit al rețelei asigurând securitatea datelor și conturilor din cadrul rețelei.

Datele pot fi stocate într-un registru printr-un mecanism de consens între mai multe părți care să verifice acuratețea datelor. Toate tranzacțiile din cadrul registrului sunt imuabile și semnate digital, factor responsabilizator la adresa participanților rețelei. Accesul in cadrul rețelei se poate realiza, inclusiv, prin metode biometrice de identificare.

Principalul **risc** al tehnologiei blockchain este reprezentat de monopolizarea rețelei de o entitate care ar putea astfel să acceseze și să realizeze modificări asupra datelor înregistrate, fenomen cunoscut ca "**51% attack**".

Prin deținerea a 51% din puterea computațională necesară validării noile înregistrări în cadrul rețelei, **atacatorul** poate decide ce operațiuni să valideze, **alterând autenticitatea** datelor și **încrederea** membrilor în rețea și/sau în entitatea inițiatoare/deținătoare.

Cu toate acestea, un astfel de eveniment poate fi preîntâmpinat prin implementarea unor funcționalități care să descurajeze tentativele de atac asupra rețelei.

De asemenea, în cadrul unei rețele private sau de consorțiu, identitatea reală a membrilor poate fi cunoscută, astfel încât, cu ajutorul caracteristicii de transparență a tehnologiei, poate fi identificată entitatea responsabilă de alterarea datelor.

8

SECURITATEA
DISPOZITIVELOR MOBILE

Odată cu dezvoltarea tehnologiilor IT&C la nivel mondial, actorii cibernetici și-au extins aria de acțiune inclusiv asupra smartphone-urilor și tabletelor. Pe măsură ce utilizatorii își folosesc dispozitivele mobile pentru tranzacții bancare, platforme social media, precum și cumpărături online, actorii cibernetici își îndreaptă atenția către exploatarea vulnerabilităților sistemelor de operare iOS și Android.

Fiecare sistem de operare, inclusiv iOS și Android, este actualizat periodic de producător, în scopul înlăturării vulnerabilităților acestuia și a diminuării riscurilor de securitate cibernetică asociate. Cunoscând faptul că mulți utilizatori nu actualizează software-ul, atacatorii exploatează aceste vulnerabilități, reușind să deruleze activități pe sistemul țintă.

Astfel, alegerea sistemului de operare a devenit un aspect foarte important, întrucât fiecare dintre acestea prezintă o serie de avantaje și dezavantaje.

SISTEMUL DE OPERARE ANDROID

Android este foarte popular la nivel mondial, ceea ce oferă avantaje pentru utilizatori, întrucât dezvoltatorii software creează în mod constant aplicații care să poată fi rulate pe acest sistem de operare.

Principalele riscuri sunt generate de aplicațiile dezvoltate special pentru a infecta dispozitivele mobile care le utilizează. Aceste riscuri sunt amplificate de procesul prin care aplicațiile Google Play sunt verificate, acesta nefiind infailibil.

De asemenea, sistemul de operare Android oferă posibilitatea ca utilizatorul să permită instalarea de aplicații din alte surse, fiind astfel evitat procesul de verificare al acestora de către Google Play și crescând incidența atacurilor cibernetice.

Utilizatorii Android pot modifica inclusiv codul sursă al sistemului de operare, întrucât el este disponibil în mediul online. Acest aspect reprezintă un avantaj pentru utilizatorii care doresc flexibilitate în ceea ce privește personalizarea sistemului, însă există și posibilitatea ca, în urma alterării codului sursă, acesta să devină vulnerabil în fața posibililor atacatori.

Sistemul de operare Android este instalat pe dispozitive fabricate de mai multe companii. Acestea, la rândul lor, pot adăuga funcționalități, oferind avantaje și dezavantaje deopotrivă.

În context, modificarea codului sursă al sistemului de operare neînsoțită de actualizări de securitate eficiente, poate genera riscuri cibernetice.

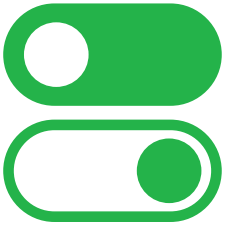
SISTEMUL DE OPERARE iOS

Rigurozitatea procesului de verificare al aplicațiilor din cadrul AppStore, magazinul oficial Apple, limitează tentativele dezvoltatorilor de a distribui aplicații cu conținut malware.

Apple nu face public codul sursă al sistemului de operare iOS și nu permite customizarea acestuia. Această restricție are drept efect un control mai strict al soft-urilor instalate pe dispozitive și o diminuare a riscurilor asociate amenințărilor cibernetice. Cu toate acestea, există posibilitatea modificării codului sursă, prin *jailbreak*. Deși această operațiune generează o experiență de utilizare personalizată, amplifică totodată riscurile de securitate cibernetică asociate.

Odată ce codul sursă al sistemului de operare este modificat, Apple nu mai oferă suport tehnic pentru remedierea eventualelor probleme, inclusiv furnizarea unor actualizări de securitate. În plus, pot fi instalate pe dispozitiv aplicații care nu sunt verificate de Apple, ceea ce induce riscuri de securitate suplimentare.

Există o serie de **riscuri de securitate asociate utilizării dispozitivelor mobile** care sunt independente de sistemul de operare folosit, printre care:



GESTIONAREA DEFECTUOASĂ A PERMISIUNILOR - deseori, utilizatorii oferă acces aplicațiilor la datele personale (ex. agenda telefonică, locație, cameră etc.), fără a analiza punctual necesitatea acordării acestor permisiuni (ex. solicitarea accesului la camera foto de către o aplicație de tip agregator de știri nu este justificată);

CONECTAREA LA REȚELE WI-FI NESECURIZATE - utilizatorii trebuie să evite accesarea serviciilor confidențiale sau personale, precum informațiile bancare, ce pot fi captate de terțe persoane care ar putea monitoriza rețeaua;

ATACURI CIBERNETICE CARE UTILIZEAZĂ TEHNICI DE INGINERIE SOCIALĂ - utilizarea în permanență a dispozitivelor mobile generează o reacție instantanee la conținutul vehiculat pe aceste terminale, reprezentând mediul propice pentru derularea de atacuri ce utilizează tehnici de inginerie socială. Unul dintre exemplele de atacuri în care se utilizează aceste tehnici este *phishing-ul*;

GESTIONAREA NEADECVATĂ A PAROLELOR - folosirea unor parole de complexitate redusă sau generice, adeseori pentru multiple conturi, creează riscul compromiterii, de către entități interesate, a datelor personale (ex. folosirea aceleiași parole pentru conturi de social media, precum și pentru accesarea aplicațiilor care gestionează date bancare);

LIPSA UTILIZĂRII UNOR SOLUȚII ANTI-VIRUS - în vederea prevenirii compromiterii terminalelor mobile, se recomandă utilizarea unor soluții anti-virus dedicate.

9

MINI-GLOSAR DE TERMENI
DIN DOMENIUL SECURITĂȚII CIBERNETICE

Advanced Persistent Threat (APT) Concept utilizat pentru a defini un atac cibernetic derulat, de regulă, de o entitate statală, ce vizează ținte strategice (din domeniul guvernamental, militar, al securității naționale și / sau al afacerilor), care prin intermediul tehnicilor, tacticilor și procedurilor de nivel ridicat, reușește să fie nedetectabil o perioadă lungă de timp cu scopul de a extrage date pentru a obține avantaje strategice sau financiare.

Apărare cibernetică (Defensivă cibernetică) Set agregat de tehnici, procese și proceduri desfășurate în spațiul cibernetic într-o manieră coordonată cu scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor și asigurării răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetice specifice apărării naționale.

Atribuire Procesul de analiză a dovezilor și indiciilor unui atac cibernetic, care are ca scop identificarea entității care l-a derulat.

Awareness în securitate cibernetică Derularea de măsuri pentru cunoașterea și înțelegerea, de către diferite categorii de public, a evenimentelor ce au loc în mediul virtual, cât și pentru conștientizarea riscurilor și amenințărilor la adresa securității cibernetice, cu scopul formării unor comportamente / deprinderi necesare creșterii nivelului culturii de securitate cibernetică.

Blockchain (tehnologia blocurilor) Registru de date organizat în blocuri de informație înlănțuite, partajate, replicate și sincronizate între membrii rețelelor de tip DLT. Principiile care stau la baza blockchain sunt criptografia și absența unui intermediar (rețelele de tip peer-to-peer). Este utilizat și în realizarea tranzacțiilor de criptomonedă.

Confidentiality, Integrity and Availability (CIA) Confidențialitatea, integritatea și disponibilitatea reprezintă cele mai importante cerințe de îndeplinit pentru asigurarea securității cibernetice.
Confidențialitatea - proprietatea unor date și informații de a rămâne cunoscute doar celor care au acest drept și a căror compromitere poate afecta negativ persoane și/sau organizații;
Integritatea - proprietatea unor date, informații și procese de a nu fi modificate sau distruse;
Disponibilitatea - proprietatea unor date, informații, echipamente sau servicii de a putea fi accesate și utilizate, la un anumit moment sau în permanență, fără restricții.

Criptomonedă (Cryptocurrency) Monedă virtuală care utilizează tehnologia *blockchain* pentru a facilita plăți sigure și cu un grad mare de anonimitate, funcționând independent de sistemul bancar și guvernamental. *Exemple: Bitcoin, Ethereum, Monero etc.*

Dark web Componentă a mediului Internet care necesită software, configurări și autorizații speciale pentru accesare (ex. browser-ul TOR). Este o componentă a Deep Web-ului, în sensul în care conținutul nu este indexat de motoarele de căutare clasice.

Deep web Componentă a mediului World Wide Web care nu este indexată de motoarele tradiționale de căutare sau directoarele de resurse, paginile web putând fi accesate exclusiv prin intermediul unor mijloace specifice (ex. browser-ul TOR). Adresele paginilor web sunt caracterizate prin caractere alfaseminumerice (literele alfabetului și cifrele de la 2 la 7), și prin extensii specifice (ex. onion).

Distributed Denial of Service (DDoS) Atac prin care se urmărește indisponibilizarea, blocarea sau epuizarea resurselor unei rețele sau unui sistem IT&C.

Exploit Un software sau o secvență de cod care exploatează vulnerabilități ale sistemelor IT&C (ex. sisteme de operare/aplicații), în scopul compromiterii acestora.

Incident de securitate cibernetică Eveniment survenit în spațiul cibernetic, care afectează securitatea cibernetică. Acesta este de natură să pericliteze confidențialitatea, integritatea și/sau disponibilitatea unui sistem IT&C.

Inginerie socială (Social engineering) Acțiuni de manipulare a factorului uman, realizate pentru atingerea unor etape (obținerea de credențiale, accesarea unui fișier infectat, transmiterea unor sume de bani) din cadrul unor atacuri cibernetice.

Inteligența artificială Domeniu IT&C care urmărește conceperea, crearea și operaționalizarea unor instrumente care au capacitatea de a realiza sarcini asociate în mod tradițional unei ființe umane.

Jailbreak Înlăturarea restricțiilor de securitate impuse de producător unui dispozitiv (de obicei telefon mobil).

Malware (malicious software) Software realizat pentru a îndeplini scopuri nelegitime în momentul în care accesează un dispozitiv, rețea sau sistem IT&C, fără acordul sau cunoștința proprietarului. *Exemple: troian, virus, vierme, spyware, backdoor etc.*

Pen-testing (test de penetrare) Metodologie de testare a securității unei infrastructuri cibernetice, prin simularea unui atac din exteriorul și / sau interiorul acesteia, în vederea stabilirii potențialelor vulnerabilități și măsurilor necesare îmbunătățirii nivelului de securitate.

Phishing Reprezintă o formă de activitate infracțională ce are ca scop obținerea unor date confidențiale, cum ar fi credențiale (pentru aplicații de tip Internet banking, aplicații de comerț electronic, carduri de credit, etc.) prin folosirea tehnicii de inginerie socială. Se realizează prin intermediul mail-ului sau prin clonarea site-urilor și, ulterior, transmiterea de solicitări clienților referitoare la datele conturilor personale.

Politică de securitate cibernetică Document menit să reglementeze și consolideze normele legale în domeniul securității cibernetice. *Exemplu: Strategia de securitate cibernetică a României.*

Ransomware Software nelegitim care restricționează accesul și utilizarea dispozitivului, prin criptarea conținutului, până când nu este plătită o recompensă.

Reziliența infrastructurilor cibernetice Capacitatea componentelor infrastructurilor cibernetice de a reveni la starea de normalitate ca urmare a derulării unui atac cibernetic.

Spear phishing Reprezintă o tehnică asemănătoare cu phishing-ul clasic, diferența constă în faptul că ținta este bine determinată, iar atacul conține elemente personalizate de convingere a potențialelor victime. Metoda este utilizată, de regulă, în cadrul unui atac de tip APT, și constă în transmiterea de mesaje către un grup de utilizatori care au în comun anumite elemente (sunt angajații unei instituții sau companii). E-mailurile sunt concepute astfel încât destinatarul să perceapă expeditorul ca fiind o persoană cunoscută (de la care primește de regulă sau așteaptă corespondență). Atașamentele ce conțin malware (fișiere de tip word, excel, pdf) au denumiri similare domeniului de activitate al destinatarului.

Spionaj cibernetic Acțiune care vizează obținerea accesului neautorizat la informații cu caracter confidențial sau clasificat, stocate în cadrul unui sistem IT&C, cu scopul de a fi utilizate de o entitate străină.

Supervisory Control and Data Acquisition System (SCADA) Rețele sau sisteme IT&C folosite pentru comanda și controlul proceselor tehnologice ce au loc în obiective industriale civile sau militare (hidrocentrale, combinate electrice, chimice și petrochimice, centrale atomice etc.).

Tactics, Techniques and Procedures (TTP) Modul în care tehnicile, tacticile și procedurile au fost utilizate în cadrul unui atac cibernetic punctual.\

Troian Software care aparent are o funcție legitimă și utilă, dar deține și una ascunsă și potențial nelegitimă, care evită mecanismele de securitate, uneori exploatând vulnerabilități ale sistemelor vizate. Astfel, odată instalat, 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.

Vulnerabilitate de securitate cibernetică Punct slab al unui software sau sistem IT&C, pe care un atacator îl poate exploata pentru a compromite confidențialitatea, disponibilitatea și/ sau integritatea țintei.

Zero day exploit / vulnerability (0 day) Vulnerabilitate, a unei aplicații sau a unui sistem, care a fost descoperită de o persoană sau un grup restrâns de persoane, nefiind cunoscută de autorul acesteia și publicul larg, având posibilitatea de a o exploata (în scopuri rău intenționate), comercializa sau raporta.


www.sri.ro