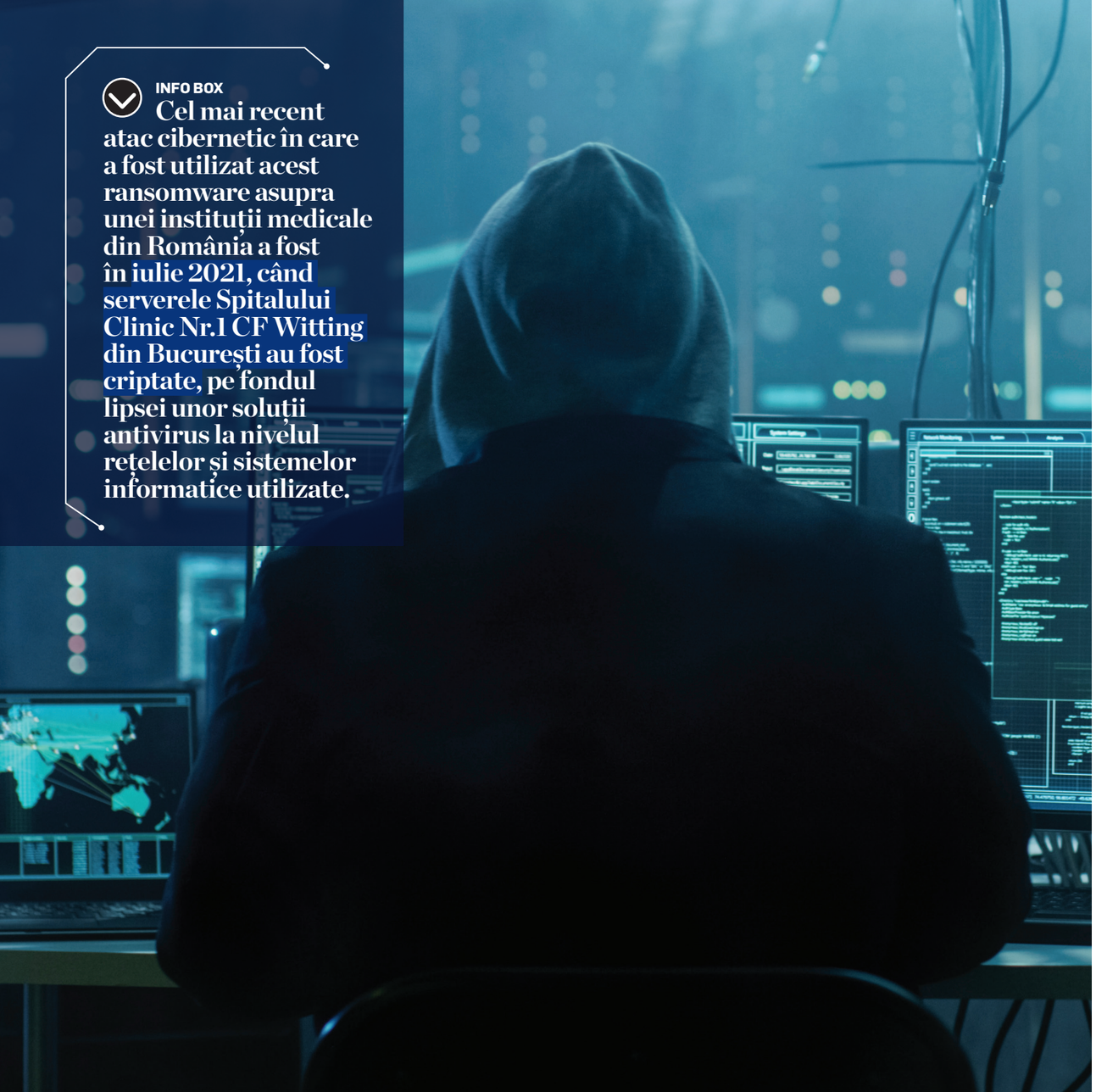
ROMANIA
SRI
Patria a priori
SERVICIUL ROMAN DE INFORMAȚII

NR_2_2021

BULETIN CYBERINT



INFO BOX

Cel mai recent atac cibernetic în care a fost utilizat acest ransomware asupra unei instituții medicale din România a fost în iulie 2021, când serverele Spitalului Clinic Nr.1 CF Witting din București au fost criptate, pe fondul lipsei unor soluții antivirus la nivelul rețelelor și sistemelor informatice utilizate.

IMPACTUL ATACURILOR RANSOMWARE ASUPRA UNITĂȚILOR MEDICALE – PHOBOS

Actorii cibernetici motivați financiar își actualizează constant modul de lucru și tacticile utilizate, astfel încât să își maximizeze profitul într-un timp cât mai scurt. Atacurile cibernetice de tip ransomware continuă să fie unul dintre cele mai întâlnite, actorii cibernetici exploatând nevoia utilizatorilor de a accesa sistemele informatice sau datele stocate la nivelul acestora.

Atacurile ransomware pot fi diferite, în funcție de complexitate, entitatea/gruparea responsabilă pentru dezvoltare sau sistemele targetate. Derularea unor astfel de atacuri asupra rețelelor și sistemelor informatice din cadrul entităților publice sau private poate avea un impact major atât din punct de vedere al afectării confidențialității, integrității și disponibilității datelor gestionate la nivelul acestora, cât și din perspectiva afectării capitalului de imagine asociat victimei.

La nivel național, peisajul atacurilor ransomware asupra unităților medicale a fost conturat de către aplicația malware PHOBOS, care a afectat atât funcționalitatea sistemelor informatice utilizate de spitale, cât și confidențialitatea, integritatea și disponibilitatea datelor gestionate la nivelul acestora.

PHOBOS este o aplicație de tip ransomware, care face parte din familia CrySiS, fiind identificat pentru prima dată în octombrie 2017. Ulterior criptării datelor, victimei i se solicită să trimită un mesaj la o adresă de e-mail utilizată de atacator în vederea stabilirii prețului pentru decriptare (acesta poate varia în funcție de profilul entității afectate).

Cel mai recent atac cibernetic în care a fost utilizat acest ransomware asupra unei instituții medicale din România a fost în iulie 2021, când serverele Spitalului Clinic Nr.1 CF Witting din București au fost criptate, pe fondul lipsei unor soluții antivirus la nivelul rețelelor și sistemelor informatice utilizate. Anterior, sistemele informatice ale altor 4 spitale din România au fost infectate cu ransomware-ul PHOBOS.

PROFILUL TEHNIC AL APLICAȚIEI PHOBOS

În ceea ce privește profilul tehnic al ransomware-ului PHOBOS, acesta prezintă un nivel de complexitate medie-redusă. Infecția sistemelor targetate este realizată preponderent prin exploatarea conexiunilor de tip Remote Desktop Protocol (RDP), însă poate fi realizată inclusiv prin campanii de phishing / spear-phishing care au atașamente cu conținut malware.

După ce pătrunde în sistemul informatic, PHOBOS derulează acțiuni la nivelul acestuia în vederea:

- asigurării persistenței la nivelul sistemului infectat;
- dezactivării funcțiilor de recuperare ale sistemului de operare și ștergerea copiilor de siguranță ale fișierelor;
- dezactivării soluțiilor de securitate ale sistemului;
- inițierii procesului de criptare a fișierelor;
- generării unor fișiere specifice ce conțin instrucțiuni pentru răscumpărarea datelor.

În cazul atacului derulat asupra Spitalului clinic Nr. 1 CF Witting din București impactul a fost unul redus, unitatea continuând să deruleze activitatea specifică prin utilizarea registrelor offline.

Pentru a asigura reziliența cibernetică a instituțiilor în fața atacurilor de tip ransomware se recomandă implementarea unor politici și măsuri de securitate precum:

- utilizarea unei soluții de antivirus actualizate;
- Dezactivarea serviciului RDP de pe toate stațiile și serverele de lucru;
- Actualizarea sistemelor de operare și a tuturor aplicațiilor din rețea;
- Schimbarea frecventă a parolelor tuturor utilizatorilor, respectând recomandările de complexitate;
- Verificarea periodică a tuturor utilizatorilor înregistrați, pentru a identifica utilizatorii noi, adăugați în mod nelegitim;
- Realizarea unor copii de siguranță a datelor critice pe suporți de date offline;
- Păstrarea datelor criptate în eventualitatea în care ar putea apărea o aplicație de decriptare în mediul online.

ATRIBUIREA PUBLICĂ A CAMPANIEI CIBERNETICE ASUPRA COMPANIEI **SOLARWINDS**

În luna martie 2020, compania americană SolarWinds a fost ținta unui atac cibernetic complex, de tip supply-chain, ce a vizat compromiterea software-ului Orion, furnizat de către entitatea privată unui număr de peste 33.000 de clienți din domenii strategice precum energetic, financiar, educațional etc.

În urma modificărilor efectuate de către actorul cibernetic asupra software-ului companiei americane, estimările arată că au fost compromise aproximativ 18.000 de sisteme guvernamentale și private de la nivel global. La data de 15 aprilie 2021, National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA) și Federal Bureau of Investigation (FBI) au inițiat demersul de atribuire publică a campaniei cibernetice asupra companiei SolarWinds către Serviciul de Informații Externe al Federației Ruse (SVR).

România s-a raliat la demersul părții americane printr-un comunicat de presă al Ministerului Afacerilor Externe, publicat la aceeași dată.

ATRIBUIREA PUBLICĂ A CAMPANIILOR CIBERNETICE DERULATE DE APT 40 ȘI A **ATACURILOR CIBERNETICE DERULATE ASUPRA MICROSOFT EXCHANGE SERVER**

Gruparea APT40 derulează atacuri cibernetice încă din anul 2013, scopul acestora fiind de a obține date de interes strategic, care să sprijine obiectivele Republicii Populare Chineze. Printre domeniile vizate de grupare s-au regăsit în principal ingineria, transporturile și cel militar, în mod special acele segmente conexe tehnologiilor din domeniul maritim.

Suplimentar, în prima jumătate a anului 2021, a fost întreprinsă campania cibernetică HAFNIUM, care a vizat compromiterea unor ținte de interes strategic (din domenii precum economic, afaceri externe, transporturi sau justiție), prin exploatarea a patru vulnerabilități critice(CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 și CVE-2021-27065) de la nivelul serverelor Microsoft Exchange.

Ca urmare a acestor aspecte, statele membre UE și NATO au inițiat demersul de atribuire publică a campaniei cibernetice HANFIUM și a operațiunilor derulate de actorul cibernetic APT40 către Republica Populară Chineză. România s-a alăturat acestui demers printr-un comunicat public al Ministerului Afacerilor Externe, emis în data de 19 iulie 2021.

WANTED BY THE FBI

APT 40 CYBER ESPIONAGE ACTIVITIES

Conspiracy to Damage Protected Computers and Commit Economic Espionage; Criminal Forfeiture

Zhu Yunmin | Wu Shurong | Ding Xiaoyang | Cheng Qingmin

CAUTION

On May 28, 2021, a federal grand jury in the United States District Court for the Southern District of California returned an indictment against four People's Republic of China (PRC) citizens for their alleged roles in a long running campaign of computer network operations targeting trade secrets, intellectual property, and other high value information from companies, universities, research institutes, and governmental entities in the United States and abroad, as well as multiple foreign governments. The indictment alleges that Zhu Yunmin, Wu Shurong, Ding Xiaoyang, and Cheng Qingmin targeted the following sectors: aerospace/aviation, biomedical, defense industrial base, healthcare, manufacturing, maritime, research institutes, transportation (rail and shipping), and virus research from 2012 to 2018, on behalf of the PRC Ministry of State Security. Additionally, the indictment alleges the use of front companies by the PRC Ministry of State Security to conduct cyber espionage.

The four individuals are identified as:

ZHU Yunmin 朱允敏 (STC Codes: 2612/0336/2404) Alias: Zhu Rong

WU Shurong 吴淑荣 (STC Codes: 0702/3219/2837) Aliases: goodperson, ha0r3n, Shi Lei

DING Xiaoyang 丁晓阳 (STC Codes: 0002/2556/7122) Aliases: Ding Hao, Manager Chen

CHENG Qingmin 程庆民 (STC Codes: 4453/1987/3046) Alias: Manager Cheng

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: San Diego

www.fbi.gov

ASPECTE RECENTE PRIVIND CADRUL LEGISLATIV CU APLICABILITATE ÎN SPAȚIUL CIBERNETIC

1. În România, procesul inițiat pentru implementarea 5G a debutat la începutul anului 2019, când Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM) a supus consultării publice un document de poziție privind acordarea drepturilor de utilizare a spectrului radio aferent tehnologiei 5G.

Prin HG nr. 429 din 20 iunie 2019, a fost aprobată Strategia 5G pentru România și a fost constituit mecanismul de monitorizare a implementării acesteia, prin intermediul Comitetului de monitorizare a Strategiei 5G pentru România.

Finalizarea, în luna februarie 2021, a proiectului de Lege privind adoptarea unor măsuri referitoare la infrastructuri informatice și de comunicații de interes național și condițiile implementării rețelelor 5G (Legea 5G), vine în întâmpinarea unor nevoi existente la nivel național privind transpunerea de măsuri strategice și tehnice cheie din setul de instrumente al UE (5G Toolbox) pentru atenuarea eficace a riscurilor și asigurarea securității rețelelor 5G necesare a fi implementate de România.

La 11 iunie a.c., președintele României a promulgat Legea 5G (Legea nr. 163/2021, publicată în Monitorul Oficial nr. 590 din 11.06.2021). Potrivit legii, furnizorii de comunicații vor putea utiliza în rețelele 5G doar tehnologii, echipamente și programe software de la producători autorizați, în prealabil, prin decizie a prim-ministrului României, pe baza avizului conform al Consiliului Suprem de Apărare a Țării.

INFO BOX

Furnizorii de comunicații vor putea utiliza în rețelele 5G doar tehnologii, echipamente și programe software de la producători autorizați, în prealabil, prin decizie a prim-ministrului României

Avizul se va emite prin raportare la obligațiile asumate de statul român în cadrul cooperării la nivelul organizațiilor internaționale în care țara noastră este prezentă, al UE și parteneriatelor strategice bilaterale, pentru evitarea unor riscuri care pot decurge din:

➡ controlul unui guvern străin asupra producătorului în lipsa unui sistem juridic independent;

➡ absența unei structuri transparente a acționariatului producătorului;

➡ lipsa unui istoric de conduită corporativă etică a producătorului;

➡ funcționarea producătorului într-un sistem juridic care nu impune practici corporative transparente.

2. În perspectiva îmbunătățirii cadrului legislativ național în domeniul securității cibernetice, în cursul anului 2021 au fost întreprinse demersuri pe linia:

➡ finalizării proiectului Legii privind securitatea și apărarea cibernetică a României;

➡ revizuirii Strategiei de Securitate Cibernetică a României.

Aceste documente sunt deosebit de

importante prin prisma rolului pe care îl au în stabilirea unei orientări clare și corecte la nivel național, în ceea ce privește securitatea cibernetică, ca parte componentă a securității naționale. Totodată, documentele în cauză țin cont de trendul ascendent și dinamica amenințărilor cibernetice și au în vedere reglementările europene și internaționale în domeniul securității cibernetice.

DIMENSIUNEA STRATEGICĂ A EDUCAȚIEI DE SECURITATE CIBERNETICĂ ÎN ROMÂNIA

Serviciul Român de Informații, prin Centrul Național CYBERINT, a susținut permanent proiecte cu scop de consolidare a rolului României de hub în domeniul securității cibernetice, prin inițiative care vizează aspecte precum consolidarea igienei cibernetice la nivel național sau formarea unei mase critice de specialiști în securitate cibernetică. Realizarea unor demersuri constante pe aceste coordonate va avea impact strategic și pe termen lung, beneficiile obținute la nivel național fiind de importanță majoră, atât în ceea ce privește domeniul securității cibernetice, cât și pe linia consolidării securității naționale.

➲ PROGRAME EDUCAȚIONALE UNIVERSITARE

Astfel, începând cu 2018, Centrul Național CYBERINT a cooperat cu Ministerul Educației și douăzeci de instituții de învățământ superior la nivel național, contribuind la conceperea și includerea în curricula universitară programe de masterat și cursuri post-universitare în domeniul securității cibernetice. La nivelul anului 2021, feedback-ul recepționat din partea zonei academice și din partea sectorului privat era foarte bun, eforturile fiind asociabile unor progrese în privința consolidării statutului României de hub regional în domeniul securității cibernetice.

➲ PROGRAME EDUCAȚIONALE PRE-UNIVERSITARE

Tot începând cu 2018, Centrul Național CYBERINT a început să desfășoare proiecte de familiarizare a elevilor de liceu cu noțiuni de securitate cibernetică, angrenând patru licee cu profil informatică intensiv –Tudor Vianu" din București, Grigore Moisil din Iași, Tiberiu Popoviciu din Cluj-Napoca și Grigore Moisil din Timișoara. Colaborarea a continuat inclusiv în anul școlar 2020-2021, experți din Centrul Național CYBERINT și din cadrul unor companii din mediul privat susținând prezentări online pentru elevii și profesorii din cele patru licee pe discipline de securitate cibernetică.

➲ PROIECTUL „VINEREA CYBER"

Proiectul a presupus derularea a

douăsprezece sesiuni online, susținute de experți ai Centrului Național CYBERINT și din cadrul unor companii private din domeniu (Orange, Thales, CISCO, Deloitte, IBM și FireEye), dedicate elevilor din clasele a X-a și a XI-a din cele patru licee. Sesiunile au vizat teme în domeniul securității cibernetice, precum securitatea aplicațiilor web, autoprotecția în mediul online și perspectivele de aprofundare a studiilor în domeniul securității cibernetice după absolvirea liceului.

În urma reacțiilor pozitive, Centrul Național CYBERINT a decis continuarea și extinderea proiectului în anul școlar 2021-2022, prin creșterea numărului de licee participante, în scopul obținerii unor beneficii pe termen mediu și lung, atât în domeniul educațional, cât și în cel al securității cibernetice.,

IMPLICAREA TINERELOR TALENTE ÎN COMPETIȚII DE SECURITATE CIBERNETICĂ

O temă recurentă a eforturilor educaționale desfășurate de Centrul Național CYBERINT este reprezentată de promovarea conștientizării, în mediul elevilor și studenților, a consecințelor legale ale propriilor acțiuni în mediul cibernetic. Dincolo de educarea acestora cu privire la principii etice, una dintre cele mai bune modalități de direcționare a abilităților tinerelor talente din domeniu către sporirea securității cibernetice o constituie competițiile de white hat hacking.

White hat hacker – expert în domeniul securității cibernetice, specializat în penetrarea rețelelor și sistemelor IT&C, cu acordul proprietarilor, în vederea raportării și remedierii vulnerabilităților. Termenul este folosit în contrast cu **black hat hacker** – specializat în penetrarea rețelelor și sistemelor IT&C, fără acordul proprietarilor, cu încălcarea cadrului legal.

România se află în plin proces de construire a unei tradiții de excelență în competițiile de acest gen la nivel internațional, după ce, în 2019, a găzduit și câștigat etapa finală a Campionatului European de Securitate Cibernetică - ediția 2019 (ECSC19), iar la competițiile din 2016 și 2017 a fost vicecampioană.

Serviciul Român de Informații s-a implicat direct în organizarea competiției de la București, dar și în preselecția și instruirea echipei României, beneficiind și de sprijinul CERT-RO și al Asociației Naționale pentru Securitatea Sistemelor Informatice.

INFO BOX

White hat hacker – expert în domeniul securității cibernetice, specializat în penetrarea rețelelor și sistemelor IT&C, cu acordul proprietarilor, în vederea raportării și remedierii vulnerabilităților.

Amplificarea recentă a interesului în securitate cibernetică în rândul elevilor și studenților se reflectă inclusiv prin concursurile și platformele tehnice educaționale noi, apărute în 2020. O astfel de platformă este unbreakable.ro, creată cu ocazia primei ediții a concursului național de securitate cibernetică UNbreakable România, organizat în perioada 16-18.10.2020, de Universitatea Tehnică Gheorghe Asachi din Iași (UTI), cu susținerea unor parteneri din mediul privat. În aprilie 2021, platforma a desfășurat webinarii săptămânal, iar pe 14.05.2021 și 04.06.2021 au avut loc concursuri individuale și pe echipe.

În 2020, ca urmare a amânării celei de-a șasea ediții a ECSC, Serviciul Român de Informații, CERT-RO și ANSSI au organizat online Campionatului Național de Securitate Cibernetică 2020. Participarea la etapa finală, desfășurată pe 24.10.2020, a permis finaliștilor să ia parte, alături de concurenți din alte state europene, la o competiție de profil organizată de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), intitulată Hackfest.

CAMPIONATUL NAȚIONAL DE SECURITATE CIBERNETICĂ 2021

În 2021, Serviciul Român de Informații, Asociația Națională pentru Securitatea Sistemelor Informatice și CERT-RO, alături de parteneri din mediul privat, a organizat, în perioada 28-29 august 2021, cea de-a doua ediție a Campionatul Național de Securitate Cibernetică (ROCSC21). Competiția națională s-a desfășurat pe trei categorii de vârstă: juniori (16-21 ani), seniori (22-26 ani) și open (participanți care nu se încadrează în celelalte două categorii).

După ROCSC21, organizatorii vor iniția un proces de selecție pentru alcătuirea echipei României care va participa la ECSC21, ce va avea loc în Praga, în perioada 28.09-01.10.2021. Procesul de selecție va presupune testarea celor mai promițători participanți prin exerciții din domenii precum mobile & web security, crypto, reverse engineering și forensics. Pentru ECSC21, echipa României va fi formată din zece concurenți (cinci juniori și cinci seniori).

REZULTATELE STRATEGICE

Beneficiile implicării în demersuri educaționale, indiferent că este vorba despre prezentări ale fundamentelor domeniului securității cibernetice sau despre competiții internaționale și performanță la cel mai înalt nivel, sunt substanțiale și se reflectă la nivel strategic prin:

- creșterea gradului de conștientizare a riscurilor și implicațiilor legale asociate domeniului securității cibernetice;
- însușirea unor deprinderi specifice igienei cibernetice;
- racordarea abordării domeniului securității cibernetice a mediului universitar la cerințele existente pe piața forței de muncă;
- extinderea bazei de selecție a viitorilor experți în securitate cibernetică la nivel național.

Este necesar ca demersurile educaționale la nivel național în domeniul securității cibernetice să rămână conexate evoluțiilor recente din domeniu, dat fiind că acest aspect rămâne esențial inclusiv pentru digitalizarea statului român. Astfel, vor fi generate rezultate pe termen mediu și lung care se vor constitui în factori importanți pentru afirmarea statutului României ca hub regional în domeniul securității cibernetice.

BRAȘOV CYBER HUB

Rolul principal al unui hub de securitate cibernetică este acela de a concentra o serie de resurse și de inițiative în domeniu pentru a asigura eficiența acestora. O astfel de nevoie a fost resimțită și în România, pe fondul potențialului în domeniul securității cibernetice la nivel internațional.

În context, Centrul Național CYBERINT, Agenția Metropolitană Brașov - Primăria Municipiului Brașov, Universitatea Transilvania din Brașov și compania de securitate cibernetică Atos au pus bazele Brașov Cyber Hub care întrunește specialiști, profesori, cercetători, furnizori de servicii, oameni de afaceri și instituții, având ca scop comun să identifice soluții noi în domeniul securității cibernetice, adaptate specificului fiecărei entități participante.

Hub-ul a stabilit trei verticale esențiale pentru desfășurarea activității în domeniul securității cibernetice: educație, evenimente și inovare. Pe fiecare nișă de competență partenerii și-au prezentat și asumat rolul de contributor la demersurile de creștere a nivelului de securitate cibernetică la nivel regional și național.

La evenimentul de lansare din 11 mai 2021 au participat instituții, experți, studenți, decizionali și companii cu viziuni și atitudini proactive, conștienți că doar prin inovare și conlucrare devin mai puternici și mai pregătiți în fața provocărilor actuale și viitoare.

HUB-UL DE LA BRAȘOV POATE SPRIJINI ÎN MOD FUNDAMENTAL:

- creșterea rezilienței cibernetice la nivel local, regional și național;
- creșterea nivelului de expertiză de securitate cibernetică în rândul angajaților din instituțiile publice, unități de învățământ gimnazial, preuniversitar, (post)universitar;
- crearea unui mediu creativ pentru stimularea identificării unor soluții la cele mai complexe provocări de securitate cibernetică;
- testarea rezilienței sistemelor integrate la atacuri cibernetice și formularea unor recomandări privind politici de securitate personalizate fiecărei entități vizate.

DE ASEMENEA, HUB-UL URMĂREȘTE:

- organizarea de exerciții cibernetice de tip "capture the flag" și "hackathon", precum și încurajarea mediului public, privat dar mai ales a studenților și elevilor să participe și să își dezvolte cunoștințele în domeniul securității cibernetice;
- crearea oportunităților de interacțiune între furnizorii de servicii de securitate cibernetică (firme, start-up-uri, specialiști IT&C, experți, autorități naționale cu expertiză în domeniu, etc) și beneficiarii ce gestionează infrastructuri IT&C cu valențe critice (ex. primării, consilii județene, prefecturi, instituții de sănătate, rețeaua instituțiilor educaționale, instituții financiar-bancare, operatori de servicii publice esențiale, furnizori de infrastructuri de comunicații etc).

Deși aflat, la acest moment, la început de drum, Brașov Cyber Hub se bucură de atenție la nivel național, o serie de companii private susținând, în mod concret, misiunea proiectului.

Mai mult de atât, în contextul înființării viitorului Centru European de Competențe în domeniul securității cibernetice, Brașov Cyber Hub poate sprijini dezvoltarea proiectelor pentru creșterea rezilienței cibernetice, obținerea de fonduri necesare și implementarea acestora.

Astfel, Hub-ul creează perspective de dezvoltare a domeniului securității cibernetice la nivel regional și reprezintă un bun exemplu de coordonare și mobilizare a eforturilor comune ce poate fi extins și chiar replicat la nivel național.

CE ESTE?
Cel mai mare exercițiu național de securitate cibernetică axat pe componenta practică

CARE ESTE OBIECTIVUL?
Exersarea capacităților de apărare în domeniul securității cibernetice împotriva amenințărilor la adresa infrastructurilor IT&C cu valențe critice pentru securitatea națională

CÂND?
Perioada 5 - 7 octombrie 2021

CINE VA PARTICIPA?
Instituții publice, entități private și mediul academic

Ajuns la a cincea ediție, se preconizează că în cadrul CyDEx21 vor participa peste 100 de entități, comparativ cu prima ediție din anul 2017 care s-a desfășurat live în poligonul cibernetic al Centrului Național CYBERINT, la care au participat 60 de entități. În ediția din 2021, participanții vor lua parte la cele 6 scenarii practice sau teoretice:

1. LIVE FIRE ÎN POLIGONUL CIBERNETIC

- nivel de dificultate: mediu-dificil

Fiecare echipă va avea acces complet la câte un segment dedicat, reprezentând rețeaua proprie. Participanții trebuie să îi asigure securitatea, precum și să identifice și să sanitizeze eventuale sisteme vulnerabile/compromise.

2. FORENSICS CHALLENGES (CTF)

- nivel de dificultate: foarte ușor-foarte dificil

Scenariul disponibil pe o platformă Capture The Flag (CTF) va pune la încercare abilități tehnice din mai multe domenii ale securității cibernetice.

3. INCIDENT DE SECURITATE CIBERNETICĂ SCADA

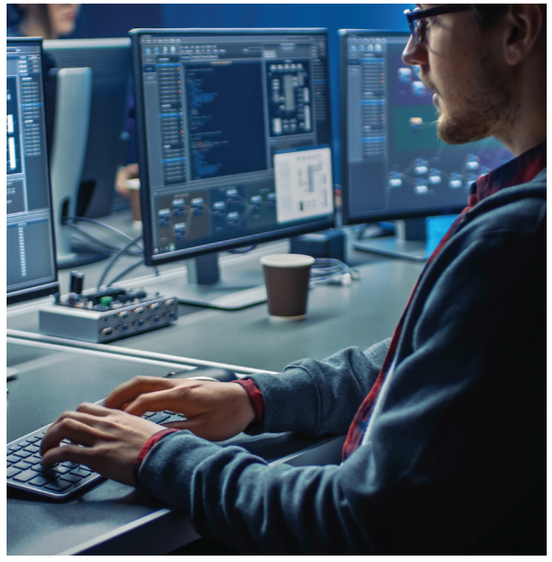
- nivel de dificultate: ușor-mediu

Scenariul prezintă un incident care a avut loc în cadrul unei Stații de Reglare și Măsurare (SRM) a gazelor naturale care asigură alimentarea cu gaze. Participanții trebuie să analizeze traficul, să se familiarizeze cu protocoalele de comunicație folosite în mediul industrial și cu echipamentele specifice, să identifice și să elimine cauza incidentului, precum și să realizeze un raport cu privire la acesta.

4. ATAC INFRASTRUCTURĂ CRITICĂ

- nivel de dificultate: ușor-mediu

Jucătorul face parte dintr-o echipă de răspuns rapid la incidente de securitate care investighează o scurgere de date la un laborator de cercetare care studia un posibil candidat pentru un vaccin împotriva SARS-COV-2. Această echipă este însărcinată cu demonstrarea modului în care actorii cibernetici au reușit exfiltrarea datelor, descrierea vulnerabilităților utilizate și propunerea de remedieri.



5. TABLE TOP

- nivel de dificultate: ușor

Conform denumirii, acest scenariu este unul de tip Table Top, exercițiu care presupune evaluarea planului de răspuns la incidente în cadrul unei organizații și se joacă în contextul adoptării Legii 362/2018 (care transpune Directiva NIS) și a legislației subsecvente.

6. SCENARIUL INDIVIDUAL ONEMAN

- nivel de dificultate: ușor-mediu

Scenariul poate fi abordat de către o singură persoană și presupune descrierea unor incidente de securitate raportate, identificarea pașilor de atac și a indicatorilor de compromitere.

Principalul avantaj pe care îl aduce ediția de anul acesta îl constituie existenta scenariului individual OneMan, care se adresează inclusiv celor care au avut rol de observator la edițiile anterioare. Scenariul se va desfășura pe parcursul celor 3 zile ale exercițiului și va presupune exersarea capacităților de identificare și raportare a incidentelor cibernetice.

STATISTICI

PENTRU PRIMA PARTE A ANULUI 2021

TOP 10 CAMPANII MALWARE ÎN ROMÂNIA (IANUARIE - IUNIE 2021)

În anul 2021, prin analiza alertelor generate de sistemul ȚIȚEICA, au fost identificate numeroase campanii malware ce au vizat instituții publice din România. Campaniile de distribuire a ransomware-ului Locky au fost cele mai frecvente la nivel național.

Locky este o aplicație malware observată începând cu luna februarie 2016. Acesta infectează echipamentele cu sistemul de operare Windows, criptând datele victimelor, până când acestea plătesc răscumpărarea. Aplicația este distribuită folosind tehnici de inginerie socială, preponderent e-mail-uri de tip phishing ale căror atașamente creează aparența unor facturi de plată legitime.

Deși inițial Locky a fost una dintre cele mai cunoscute și complexe aplicații de tip ransomware, în prezent, aceasta are o complexitate redusă și nu mai reprezintă o amenințare. Toate tentativele de

1	RANSOMWARE.LOCKY.DNS	16682
2	INFOSTEALER.MSIL.AGENTTESLA	11860
3	TROJAN.FORMBOOK	6810
4	DOWNLOADER.EMOTET	2785
5	TOOL.COINMINER	2694
6	BACKDOOR.MSIL.NANOCORE	2090
7	INFOSTEALER.LOKIBOT	1759
8	TROJAN.BRONTOK	1336
9	EXPLOIT.IOT.MOZI	994
10	TROJAN.PONY	465

compromitere a sistemelor și rețelelor informatice din cadrul instituțiile publice din România beneficiare în cadrul Sistemului ȚIȚEICA au fost blocate.

De asemenea, similar anului 2020, distribuirea aplicației Agent Tesla s-a menținut la un nivel ridicat în prima jumătate a anului 2021, tehnicile de inginerie socială utilizate de actorii cibernetici fiind diversificate în mod constant.

CELE MAI FRECVENTE APLICAȚII MALWARE

Referitor la tipurile de aplicații malware utilizate, comparativ cu anul 2020, a fost observată predilecția actorilor cibernetici pentru cele de tip ransomware și infostealer.

Aceste aplicații asigură atacatorilor beneficii financiare fie în urma plății răscumpărării de către victime pentru recăpătarea accesului la datele proprii, în cazul ransomware, fie prin vânzarea pe forumuri cybercrime a datelor furate, în cazul infostealer.

De asemenea, aplicațiile de tip troian au înregistrat un număr mare de distribuiri la nivelul instituțiilor publice din România și a infrastructurilor IT&C cu valențe critice pentru securitatea națională. Pentru distribuirea acestor aplicații, actorii cibernetici au derulat preponderent campanii de phishing, fiind înregistrată o medie de 3813 e-mail-uri de phishing în prima jumătate a anului 2021.

RANSOMWARE	**35.03%**
INFOSTEALER	**28.95%**
TROJAN	**20.67%**
DOWNLOADER	**5.93%**
BACKDOOR	**4.36%**
EXPLOIT	**4.23%**
WORM	**0.83%**

PERSPECTIVA MEDIULUI ACADEMIC ASUPRA SECURITĂȚII CIBERNETICE

Având în vedere nivelul ridicat al amenințării cibernetice care vizează infrastructuri IT&C din cadrul instituțiilor publice și al companiilor private, dar și utilizatori individuali, începând cu 2018, Serviciul Român de Informații a cooperat cu Ministerul Educației și companii private pentru dezvoltarea unor programe de pregătire în domeniul securității cibernetice. Pentru a identifica beneficiile aduse de acest demers, dar și pentru a putea extrage un set de bune practici, rectorii a 4 dintre universitățile implicate în acest proiect au participat la un interviu care marchează rezultatele de etapă obținute, dar și perspectivele asupra viitorul domeniului de securitate cibernetică.

CUM A DECURS IMPLEMENTAREA PROIECTULUI LA NIVELUL INSTITUȚIEI PE CARE O CONDUCEȚI?

UNIVERSITATEA POLITEHNICĂ DIN BUCUREȘTI

Universitatea Politehnică din București a implementat cursuri cu profil de securitate cibernetică atât în cadrul programelor de licență, cât și în cadrul programelor de master, în special în cadrul facultăților de profil: Facultatea de Automatică și Calculatoare și Facultatea de Electronică, Telecomunicații și Tehnologia Informației, dar și în cadrul altor facultăți din domenii conexe.

În cazul Facultății de Automatică și Calculatoare, se desfășoară cursuri cu profil de securitate cibernetică atât în cadrul programelor de licență din domeniile Calculatoare și Tehnologia Informației și Ingineria Sistemelor, cât și în cadrul programelor de master. De asemenea, în cadrul facultății se desfășoară și programe

de master dedicate domeniului de securitate: Securitatea Rețelelor Informatice Complexe și Sisteme Avansate de Securitate (program în limba engleză).

UNIVERSITATEA TEHNICĂ „GHEORGHE ASACHI" DIN IAȘI

În cadrul acestui proiect, la Facultatea de Electronică, Telecomunicații și Tehnologia Informației, din Universitatea Tehnică „Gheorghe Asachi" din Iași, s-a implementat infrastructura necesară desfășurării cursurilor de securitate cibernetică și au demarat formalitățile de organizare a programelor post-universitare cu acest specific, întârziate de situația pandemică din 2020 și 2021.

De asemenea, în același context, au fost elaborate module de securitate cibernetică și incluse în planurile de învățământ de la două programe de master, deja acreditate, care funcționează în cadrul facultății, începând cu anul universitar 2019-2020 și au continuat online în 2020-2021. Este vorba de „Rețele de calculatoare și securitate cibernetică" predată la programul de studii de master „Rețele de comunicații", precum și de disciplina „Networking, cloud computing and cybersecurity" inclusă în planul de învățământ al programului de master cu predare în limba engleză „Information Technology for Telecommunications", ambele discipline fiind predate în anul I de studii, semestrul al doilea.

În paralel, câțiva studenți de la doctorat, din cadrul Școlii doctorale a universității, abordează domeniul securitatii cibernetice și participă la orele practice de la programele de master pentru prezentarea unor aplicații specifice. Aprofundarea cunoștințelor prin activitățile de documentare din cadrul programelor de doctorat este deosebit de importantă întrucât creează premisele formării de specialiști bine instruiți și care sunt la curent cu toate tendințele și evenimentele din acest domeniu.

UNIVERSITATEA DE VEST DIN TIMIȘOARA

Apreciem că implementarea programului de master de Securitate Cibernetică a completat cu succes oferta de programe masterale din cadrul Universității de Vest din Timișoara, reprezentând unul dintre domeniile de mare interes astăzi în informatică, atât din punct de vedere al cercetării academice, cât și din punct de vedere al cerințelor pe piața forței de muncă. Prin acest program, Universitatea de Vest a răspuns cu succes numeroaselor solicitări de pregătire a viitorilor specialiști în domeniul securității cibernetice, un domeniu cu un factor de impact exponențial

crescător în ultimul deceniu, atât din prisma necesității specializărilor în cadrul cererii pe piața muncii, dar și din prisma atractivității acestui domeniu pentru tinerii care doresc să își construiască o carieră de succes în această direcție.

UNIVERSITATEA „OVIDIUS" DIN CONSTANȚA

Preocuparea Universității „Ovidius" din Constanța (UOC) pentru domeniul Cybersecurity s-a intensificat odată cu desfășurarea la Constanța, în anul 2017, a primei ediții a „Black Sea and Balkans Security Forum". În calitate de co-organizator, în toate cele 3 ediții, UOC a fost preocupată de paneluri în care s-au abordat subiecte actuale din zona securității cibernetice.

Astfel, după ce Serviciul Român de Informații prin Centrul Național Cyberint, alături de companii din domeniul IT&C, a inițiat demersurile pentru dezvoltarea unor programe de învățământ în domeniul securității cibernetice, Universitatea „Ovidius" din Constanța a achiesat la acest demers, propunând un plan pe 4 paliere: un modul cu 6 cursuri de câte un semestru dedicate Cybersecurity pentru 500 de studenți din anii terminali ai domeniului Informatică, pe o

perioadă de 2 ani, un modul pentru cadrele didactice specializate din învățământul universitar, un modul pentru cadrele didactice de informatică din învățământul preuniversitar și un modul general de conștientizare pentru cadrele didactice universitare, din domenii netehnice. Cel mai mare avantaj al acestor module a fost faptul că în fiecare dintre ele, componenta aplicativă a fost susținută de către specialiștii Centrului Național Cyberint (CNC).

Pornind de la acest format, UOC a câștigat o finanțare pentru desfășurarea tuturor modulelor prin proiectul Proinfo (http://proinfo.univ-ovidius.ro/), context prin care au putut fi recompensați specialiștii și experții implicați în dezvoltarea curriculei, susținerea tuturor activităților timp de 2 ani, dar și pentru achiziționarea unor echipamente utile pentru laboratorul de securitate cibernetică existent la nivelul instituției.

Demersului susținut de CNC la nivelul UOC i s-a alăturat, în anul 2020, și compania Orange România, care prin experții săi în securitate cibernetică a susținut 2 semestre de training-uri și workshop-uri suplimentare curriculei furnizate în cadrul proiectului Proinfo.

Recent, și alte companii regionale s-au alăturat proiectului pornit în parteneriat cu CNC, extinzând pregătirea, dar mai ales deschizând și domeniul cercetării în securitatea cibernetică.

CUM EVALUAȚI IMPACTUL ACESTOR DEMERSURI ÎN PIAȚA FORȚEI DE MUNCĂ? DAR ÎN DOMENIUL CERCETARE-DEZVOLTARE?

UNIVERSITATEA POLITEHNICĂ DIN BUCUREȘTI

Actori importanți pe piața forței de muncă încep să includă din ce în ce mai multe oferte de locuri de muncă în domeniul securității cibernetice. În acest context, includerea cursurilor universitare de specialitate și specializarea în cadrul unor programe de master reprezintă o necesitate. Pregătirea de bază dar și specializarea în domeniu oferă posibilitatea integrării facile a absolvenților de studii universitare, atât în echipe care proiectează, cât și în echipe care administrează sistemele de securitate cibernetică ale companiilor.

Domeniul de cercetare în securitate cibernetică a cunoscut o creștere semnificativă în ultima perioadă. Rezultatele cercetărilor sunt aplicate în dezvoltarea unor sisteme de securitate cibernetică independente, dar sunt integrate și în cadrul unora existente precum sisteme de comunicații, sisteme de operare sau sisteme informaționale. Un subdomeniu cu o evoluție importantă este și cel al simulatoarelor.

UNIVERSITATEA TEHNICĂ „GHEORGHE ASACHI" DIN IAȘI

Impactul activităților din cadrul acestui proiect asupra absolvenților noștri, ulterior angajați la diferite companii, este unul esențial în ceea ce privește responsabilizarea și specializarea lor în asigurarea securității datelor și infrastructurilor instituționale respective, precum și implicarea lor activă în implementarea strategiilor în vederea identificării și soluționării incidentelor și evenimentelor de securitate cibernetică.

Cadrele didactice și studenții doctoranzi au desfășurat împreună activități de cercetare în acest domeniu și au publicat o serie de articole în reviste și în volumele unor manifestări științifice de profil în care au fost prezentate diverse aplicații dezvoltate de către aceștia.

UNIVERSITATEA DE VEST DIN TIMIȘOARA

Implementarea unor programe pentru stimularea interesului în domeniul securității cibernetice, respectiv creșterea gradului de conștientizare a importanței

acestuia în rândul viitorilor specialiști în informatică, atât în mediul privat cât și cel public, va determina în viitorul apropiat o răspândire și îmbunătățire semnificativă nu doar a normelor de protecție eficiente împotriva amenințărilor cibernetice, dar și a metodelor de prevenție și mitigare a acestora. Apreciem că diversificarea forței de muncă prin prisma pregătirii specialiștilor dedicați securității cibernetice are efecte colaterale nu doar prin evitarea costurilor ridicate ca urmare a potențialelor breșe de securitate în mediile publice și private, dar și prin prisma echilibrării cererii pieței cu o ofertă adecvată acesteia, într-un context economic în care există o nevoie reală de astfel de specialiști în domeniu.

În domeniul de cercetare-dezvoltare, observăm un trend încurajator de specializare a viitorilor profesioniști pe numeroase nișe de cercetare relevante în contextul securității cibernetice, cu precădere în rândul viitorilor doctoranzi. Acest lucru ne face să credem că acest program a fost și este de real interes în rândul tinerilor masteranzi, doctoranzi și postdoctoranzi, și ne bucurăm că s-a materializat într-un context care nu putea decât să puncteze foarte bine importanța socială, economică și juridică a diverselor aspecte pe care securitatea cibernetică le implică, la nivel național și internațional.

UNIVERSITATEA „OVIDIUS” DIN CONSTANȚA

Pe fondul deficitului imens de forță de muncă în domeniul securității cibernetice, crearea unei mase critice de specialiști este baza unei construcții sănătoase, care să facă față noilor provocări de personal din companiile private, dar și eventual pentru Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică, cu sediul în București.

Multe din proiectele viitoare ale Centrului de Inovare Digitală de la Constanța (CiTyInnoHub) au ca arie de cercetare securitatea cibernetică per-se, precum și domeniile conexe în care aceasta se extinde din ce în ce mai mult.

CUM VEDEȚI EVOLUȚIA DOMENIULUI SECURITATE CIBERNETICĂ ÎN MEDIUL UNIVERSITAR? DAR LA NIVELUL SOCIETĂȚII CIVILE?

UNIVERSITATEA POLITEHNICA DIN BUCUREȘTI

Securitatea cibernetică a căpătat o importanță deosebită, atât datorită evoluției sistemelor informatice inclusiv a celor asociate dispozitivelor mobile, a sistemelor de comunicații și a sistemelor încorporate ce utilizează tehnologii internet, dar și a comerțului electronic. Evoluția pandemiei COVID care a determinat tranziția unui număr semnificativ de activități către mediul virtual și a utilizării internetului pentru conectarea la sisteme ce permit desfășurarea de activități de la distanță.

Pe termen mediu și lung, învățământul universitar va fi marcat de o creștere atât a numărului de cursuri, cât și a numărului de programe de studii în domeniul securității cibernetice.

La nivelul societății civile, securitatea cibernetică va căpăta un rol din ce în ce mai important, atât din perspectiva protecției datelor cu caracter personal, cât și a protecției datelor confidențiale, a aplicațiilor și a mesajelor transmise prin internet. Pe lângă cele enumerate, o nouă dimensiune a securității cibernetice va capătă o amploare deosebită, odată cu interconectarea lucrurilor, a bunurilor și a infrastructurilor în cadrul general oferit de internetul lucrurilor (Internet of Things).

UNIVERSITATEA TEHNICĂ „GHEORGHE ASACHI” DIN IAȘI

În perioada următoare, domeniul securității cibernetice va fi unul din ce în ce mai mult abordat în programele de studii universitare, de la toate nivelurile (licență, postuniversitar, master, doctorat) întrucât riscurile de securitate cibernetică sunt tot mai mari și cerințele societății civile și a mediului

economic, precum și din alte domenii de activitate, pentru specialiști în acest domeniu, justifică organizarea cursurilor de profil.

În ceea ce privește societatea civilă, sunt necesare acțiuni de conștientizare a riscurilor cibernetice pentru întreaga populație, prin mass-media sau alte mijloace de informare. Evident, responsabilitatea organizării acestora le revine tot specialiștilor și organizațiilor abilitate din acest domeniu.

UNIVERSITATEA DE VEST DIN TIMIȘOARA

Dacă în urmă cu doar câțiva ani, securitatea cibernetică era un domeniu de cercetare în plină dezvoltare, cu numeroase direcții, dintre care puține clar identificate și stabilite, astăzi amenințările de tip ransomware, phishing, social engineering etc. sunt doar câțiva dintre numeroșii factori implozivi care au condus la conștientizarea importanței acestui domeniu, atât în cadrul învățământului superior pentru pregătirea specialiștilor pe piața forței de muncă, dar și la nivelul societății, prin educația aferentă interacțiunii în siguranță cu echipamentele electronice folosite, a rețelei de internet etc.

Evolutiv, apreciem că securitatea cibernetică este un domeniu în continuă schimbare, cu un grad de polimorfism, respectiv adaptabilitate, accentuate de extinderea rețelei de internet și a gradului de acces la aceasta în rândul populației la nivel global, dar și de prezența tehnologiei în tot mai multe aspecte dominante ale societății civile în prezent și viitor, de la roboți inteligenți și mașini autonome, la mass-media și sisteme financiare descentralizate.

UNIVERSITATEA „OVIDIUS" DIN CONSTANȚA

Începând cu acest an universitar, în baza bunelor practici avute în proiectele anterioare de securitate cibernetică, UOC demarează un masterat în limba engleză intitulat Cybersecurity and Machine Learning, ce va asigura continuitatea și formarea continuă în educație, dar mai ales în cercetarea aplicată în zona universitară, precum și în zona privată.

Prin Centrul de Inovare Digitală (CiTyInooHub) UOC, alături de parteneri de elită, și-a asumat rolul de lider regional pentru activitățile de conștientizare a societății civile, a instruirii personalului din administrația publică locală și județeană.

Nu în ultimul rând, rezultatele ascendente cantitativ, dar mai ales calitativ ale echipelor noastre participante la diverse competiții din domeniul securității cibernetice, ne face încrezători că împreună cu partenerii regionali, ne vom dezvolta și vom deveni un pol regional ce poate oferi o gamă largă de servicii dedicate companiilor locale.

Listăm mai jos câteva dintre rezultatele studenților noștri ce încununează munca în echipă, într-un colectiv coordonat de colegul nostru Asist.univ.dr. Dorin Iordache:

1. CyDEX 20: Lucian Plăcintă și Doru Gavrilă, INFO III, Antonio-Gabriel Vasile și Irinel Cătălin Istrătoae, CS III.

2. UNbreakable România, 16-18 octombrie 2020, clasare în primii 11% din 380 de participanți: Lucian Plăcintă, INFO III, Antonio-Gabriel Vasile, CS III.

3. UNbreakable România, 15-16 mai 2021, concurs individual, clasare în primii 4% din 700 de participanți: Iustin-Alexandru Vîlcu - INFO II, Alexandru Chiriacescu - INFO II, Marius-Paul Boldeanu - CS II, Andrei Ispas - CS I, Costin-Tiberiu Vasilescu - CS I

4. UNbreakable România, 4-6 iunie 2021, concurs pe echipe: Blackout și G2OVI.

INFRASTRUCTURA DE ATAC

Succesul unui atac cibernetic, precum și securitatea operațiunilor desfășurate de un atacator cibernetic depind de o serie de factori, unul dintre cei mai relevanți fiind infrastructura utilizată.

Când vine vorba de o grupare, fie ea motivată financiar sau ideologic, sau de un actor statal de tip Advanced Persistent Threat (APT), care urmărește obținerea unor avantaje strategice prin campanii cibernetice, infrastructura utilizată poate îndeplini mai multe roluri.

Odată cu evoluția tehnologică, dar și a domeniului securității cibernetice, autoritățile au devenit din ce în ce mai eficiente în prevenirea și contracararea amenințărilor, iar atacatorii sunt obligați să își dezvolte constant operațiunile derulate și să adapteze modul de operare.

În acest sens, o măsură cu un nivel crescut de eficiență este reprezentată de crearea unei infrastructuri complexe și sigure și segmentarea acesteia în funcție de rolul pe care îl îndeplinește: infrastructură utilizată în distribuirea de malware, în exfiltrarea datelor sau pentru asigurarea comunicațiilor între membrii unei grupări.

O infrastructură de atac performantă presupune eforturi suplimentare din partea atacatorilor, motiv pentru care, anterior inițierii unor campanii cibernetice, aceștia analizează necesitatea și decid dacă este mai benefic să dezvolte o infrastructură proprie sau să închirieze astfel de servicii de la alți actori cibernetici.

Un tip de infrastructură de atac este botnet-ul, ce reprezintă o rețea de echipamente infectate anterior, asupra cărora un actor deține controlul.

Rețelele de boți au cunoscut o creștere semnificativă odată cu dezvoltarea tehnologică și cu apariția dispozitivelor de tip

Internet of Things (IoT). De cele mai multe ori, astfel de dispozitive au un nivel redus de securitate cibernetică, fapt ce facilitează infectarea de către atacator în vederea includerii într-un botnet.

Actorii cibernetici de nivel înalt recurg inclusiv la crearea unor rețele de boți proprii prin exploatarea sistemelor victimă, pentru a se asigura că rețeaua funcționează la parametri optimi și că dețin controlul total asupra acesteia.

Acest mod de operare îngreunează activitatea autorităților orientată spre cunoașterea, prevenirea și contracararea atacurilor cibernetice, destructurarea unui botnet implicând resurse considerabile și fiind posibilă doar prin eforturi conjugate, cu implicarea atât a unor structuri naționale, cât și a mediului privat.

Includerea sistemelor informatice în cadrul unei rețele de boți poate avea mai multe efecte negative, printre care afectarea funcționalității acestora, includerea lor pe blacklist, fapt ce ar împiedica accesarea unor resurse internet, respectiv afectarea imaginii statului la nivel internațional.


ROMANIA
SRI
Patria a priori
SERVICIUL ROMAN DE INFORMAȚII
SIGURANȚĂ
PENTRU ROMÂNIA
WWW.SRI.RO/CYBERINT