
ROMANIA
SRI
Patria a Priori
SERVICIUL ROMAN DE INFORMAȚII
NR_1_2021
BULETIN
CYBERINT

INFO BOX

Un element specific anului 2020, generat în contextul pandemiei de COVID-19, îl reprezintă orientarea activității actorilor cibernetici statali către exfiltrarea de informații din domeniul medical, în special din cadrul companiilor farmaceutice și institutelor de cercetare care au dezvoltat vaccinuri împotriva virusului SARS-CoV-2.

EVOLUȚIA AMENINȚĂRII CIBERNETICE ÎN 2020

ACTORI CIBERNETICI CU MOTIVAȚIE STRATEGICĂ

În anul 2020, entități statale au continuat să deruleze atacuri cibernetice la adresa infrastructurilor IT&C cu valențe critice pentru securitatea națională, obiectivul principal al acestor atacuri rămânând exfiltrarea de informații de interes strategic.

Aceste atacuri au folosit aplicații malware cu un nivel ridicat de complexitate, instrumente cibernetice diversificate, adaptate scopului operațional astfel încât să asigure o rată cât mai mare de succes.

Un element specific anului 2020, generat în contextul pandemiei de COVID-19, îl reprezintă orientarea activității actorilor cibernetici statali către exfiltrarea de informații din domeniul medical, în special din cadrul companiilor farmaceutice și institutelor de cercetare care au dezvoltat vaccinuri împotriva virusului SARS-CoV-2.

ACTORI CIBERNETICI CU MOTIVAȚIE FINANCIARĂ

Activitatea actorilor cibernetici cu motivație financiară s-a menținut la un nivel ridicat, amenințarea fiind amplificată de pandemia de COVID-19 și efectele acesteia. A fost regândit modul de lucru și s-au diversificat TTP-urile folosite, în scopul valorificării contextului pandemic. De asemenea, aceștia au exploatat atât nevoia populației de informare cu privire la evoluția pandemiei, cât și aplicarea modelului work from home, ca parte a măsurilor de distanțare socială.

În planul atacurilor de tip ransomware, a fost observat un nou trend în rândul atacatorilor, aceștia recurgând la activități de extorcare a victimelor (double extortion). De asemenea, entități din sfera criminalității cibernetice au derulat unele campanii de tip ransom DDoS, prin care au amenințat victimele cu indisponibilizarea sistemelor IT&C prin atacuri de tip DDoS, în situația în care suma solicitată nu era plătită.

Pe parcursul anului 2020, prin campanii de inginerie socială (ex. phishing, spear-phishing și smishing) au fost transmise, cu frecvență și amploare ridicate, aplicații malware de tip troian, precum Emotet, Agent Tesla, Cerberus Android Banker și QBOT. Toate acestea au avut ca scop exfiltrarea datelor de interes ale victimelor, precum credențiale de acces la conturile personale/oficiale sau platforme online, Cerberus Android Banker și QBOT vizând preponderent domeniul financiar-bancar.

ACTORI CIBERNETICI CU MOTIVAȚIE IDEOLOGICĂ

În ceea ce privește fenomenul hacktivist autohton, s-a constatat o ușoară creștere a numărului de atacuri derulate, nivelul tehnologic al acestora fiind relativ redus. Exploatând contextul pandemic, exponenții mediului hacktivist autohton au derulat în 2020 atacuri cibernetice de tip Distributed Denial of Service (DDoS), SQL Injection și Web Defacement, care au vizat preponderent indisponibilizarea unor resurse IT&C de la nivelul unor instituții publice din România, inclusiv cu responsabilități în gestionarea pandemiei. Cu titlu de exemplu, în 2020 au fost identificate mai multe atacuri cibernetice de tip defacement și SQL Injection asupra mai multor website-uri ale unor instituții din România, realizate de către o grupare hacktivistă autohtonă. Membrii grupării au realizat inclusiv activități premergătoare derulării unor atacuri cibernetice de tip ransomware la adresa unor instituții din domeniul sănătății. Materializarea acestora ar fi fost în măsură să diminueze capacitatea de gestionare a efectelor pandemiei de COVID-19.

PROTECȚIA INFRASTRUCTURILOR IT&C CU VALENȚE CRITICE PENTRU SECURITATEA NAȚIONALĂ

Și în 2020, acest aspect a reprezentat o provocare, disfuncțiile și vulnerabilitățile de securitate cibernetică existente fiind exploatate inclusiv în contextul adoptării modelului work from home. Utilizarea unor tehnologii depășite și existența unor proceduri neactualizate grevează în continuare funcționarea infrastructurilor IT&C cu valențe critice pentru securitatea națională. De asemenea, lipsa personalului calificat în domeniul securității cibernetice și subfinanțarea domeniului accentuează starea precară în care se regăsesc aceste infrastructuri, făcându-le vulnerabile la atacuri cibernetice.

Anul 2020 ne-a demonstrat că digitalizarea este un proces extrem de important, inclusiv în ceea ce privește funcționalitatea serviciilor esențiale. Domenii precum cel al sănătății, financiar-bancar, energetic și al educației au beneficiat de o atenție sporită din partea specialiștilor în securitate cibernetică. Monitorizarea acestei problematici permite, pe de o parte, identificarea riscurilor și amenințărilor de securitate, iar, pe de altă parte, aplicarea măsurilor necesare creșterii rezilienței cibernetice.

Aplicarea unor măsuri la nivel global, în scopul limitării efectelor pandemiei de COVID-19, precum distanțarea socială, a creat necesitatea continuării activității în sectoarele esențiale, prin intermediul work from home. Această situație fără precedent a obligat entitățile care gestionează infrastructuri IT&C cu valențe critice pentru securitatea națională să se reorienteze rapid în reorganizarea propriilor activități. Tot în acest context, nivelul scăzut al culturii de securitate cibernetică în rândul angajaților a reprezentat un factor suplimentar de risc.

INFO BOX

Exponenții mediului hacktivist autohton au derulat în 2020 atacuri cibernetice de tip Distributed Denial of Service (DDoS), SQL Injection și Web Defacement

EMOTET
– AMENINȚARE CIBERNETICĂ PREVALENTĂ ÎN 2020

În România, una dintre cele mai des întâlnite aplicații malware utilizate de actorii cibernetici în 2020, a fost Emotet, cu un număr ridicat și diversificat de ținte.

Emotet este un troian care infectează dispozitive informatice cu sisteme de operare Microsoft Windows. Acesta este distribuit prin campanii de phishing/spear-phishing, e-mail-urile utilizate având link-uri sau atașamente cu conținut malware. Adresele utilizate pentru expedierea acestor e-mail-uri sunt de două tipuri:

- par a fi legitime, impersonând persoane fizice sau instituții;
- sunt reale, fiind compromise anterior.

Emotet a targetat atât utilizatori individuali, cât și instituții publice din România. În cele mai multe dintre cazuri, infecțiile cu Emotet au fost realizate prin descărcarea unor fișiere Microsoft Office atașate e-mail-urilor, acestea conținând macro-uri care descarcă malware-ul. Suplimentar, malware-ul a utilizat funcționalitatea de loader, pentru livrarea de alte aplicații, printre care și Trickbot și Ryuk. Scenariul utilizat de actorii cibernetici în derularea atacurilor cibernetice cu un nivel de complexitate ridicat presupune o combinație care include troienii Emotet și Trickbot și ransomware-ul Ryuk

INFO BOX

Trickbot este un malware de tip troian, utilizat pentru derularea unor atacuri cibernetice asupra sectorului financiar-bancar, platformelor de tip exchange criptomonede, industriei farmaceutice, industriei petroliere, respectiv instituțiilor guvernamentale în scopul compromiterii stațiilor de lucru, obținerii credențialelor de acces, exfiltrării datelor de interes și realizării fraudelor financiare.

INFO BOX

Ryuk reprezintă un malware de tip ransomware, observat începând cu luna august 2018 și a vizat preponderent sectorul bancar, cel medical, de retail sau guvernamental.

Capabilitățile Emotet sunt utilizate pentru realizarea infecției inițiale, ulterior fiind livrat malware-ul Trickbot, care exfiltrează date de interes despre victimă. Ca parte finală a atacului, este descărcat și lansat în execuție ransomware-ul Ryuk, care criptează datele utilizatorului, atacatorul solicitând plata unei răscumpărări pentru decriptarea acestora.

În urma campaniilor cibernetice frecvente și de anvergură în care a fost utilizat Emotet, specialiștii în securitate cibernetică au dezvoltat o soluție software prin intermediul căreia este detectată infecția. Tool-ul poate fi descărcat de la adresa de GitHub https://github.com/JPCERTCC/EmoCheck.

Suplimentar, a fost dezvoltat un instrument online pentru scanarea adreselor de e-mail și a domeniilor web în vederea compromiterii acestora cu Emotet. Acesta este disponibil la adresa *https://www.haveibeenemotet.com.*

CENTRUL DE COMPETENȚE EUROPEAN INDUSTRIAL, TEHNOLOGIC ȘI DE CERCETARE ÎN MATERIE DE SECURITATE CIBERNETICĂ – IMPACT ÎN PLAN NAȚIONAL ȘI EUROPEAN

La data de 9 decembrie 2020, capitala României a fost aleasă de către reprezentanții statelor membre ale Uniunii Europene (UE) să găzduiască viitorul sediu al noului Centru de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC). Centrul va reprezenta o structură-cheie în contextul eforturilor de la nivelul UE de configurare a unui ecosistem în materie de securitate cibernetică, fiind în același timp prima Agenție Europeană de pe teritoriul României.

INFO BOX

Înființarea Centrului va oferi suport financiar sporit pentru cercetare, inovare, tehnologizare și dezvoltare industrială în domeniul securității cibernetice

Înființarea Centrului va oferi suport financiar sporit pentru cercetare, inovare, tehnologizare și dezvoltare industrială în domeniul securității cibernetice, în complementaritate cu activitatea structurilor europene deja existente (ex. Agenția Uniunii Europene pentru Securitate Cibernetică/ ENISA).

ECCC va avea rolul de implementare a Strategiei de Securitate Cibernetică a UE, contribuind astfel la creșterea nivelului de securitate cibernetică, prin echilibrarea și eliminarea diferențelor dintre statele membre. Totodată, Centrul va avea ca obiectiv transformarea UE într-un furnizor global de securitate cibernetică, concurând astfel cu SUA și state din zona Asiei.

Prin intermediul ECCC, Comisia Europeană vizează crearea unui pol european de expertiză tehnologică în materie de securitate cibernetică, în special în domenii precum criptografia, securitatea cibernetică a rețelelor/sistemelor IT&C, detectarea intruziunilor, securitatea programelor/

aplicațiilor informatice, precum și aspectele umane și societale ale securității și ale protecției vieții private.

Obiectivul Centrului este să susțină angajamentul UE în domeniul securității cibernetice, să dezvolte competențele în materie și să asigure accesul statelor membre la expertiza dobândită. De asemenea, ECCC va reprezenta principalul organism de gestionare a resurselor financiare ale UE dedicate securității cibernetice, în cadrul programelor Europa Digitală și Orizont Europa.

Programul Europa Digitală va asigura finanțare pentru proiecte din cinci domenii majore: supercalcul, inteligență artificială, securitate cibernetică, competențe digitale avansate, și utilizarea pe scară largă a tehnologiilor digitale la toate nivelurile economiei și societății.

Orizont Europa constituie programul cadru al UE pentru cercetare și inovare, în perioada 2021-2027, reprezentând continuarea programului Orizont 2020. Programul ar trebui să consolideze atât sectorul științei, cât și sectorul tehnologiei din UE, pentru a permite abordarea principalelor provocări globale precum sănătatea, îmbătrânirea populației, securitatea, poluarea și schimbările climatice.

INFO BOX

Obiectivul Centrului este să susțină angajamentul UE în domeniul securității cibernetice, să dezvolte competențele în materie și să asigure accesul statelor membre la expertiza dobândită.

EDUCAȚIE ÎN DOMENIUL 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, Serviciul Român de Informații a cooperat cu instituții publice și companii private pentru dezvoltarea unor programe de pregătire în domeniul securității cibernetice. Astfel, sunt în derulare proiecte pentru ciclurile pre-universitar, universitar și post-universitar, obiectivele principale ale acestora fiind:

➡ de a crea o masă critică de specialiști în securitate cibernetică;
➡ de a încuraja însușirea unor noțiuni de igienă în spațiul cibernetic, la nivel național.

LA NIVEL UNIVERSITAR / POST-UNIVERSITAR

Serviciul Român de Informații, prin Centrul Național CYBERINT, în cooperare cu Ministerul Educației Naționale și 20 de universități la nivel național, a demarat un proiect de operaționalizare a unor programe universitare și post-universitare de studii în domeniul securității cibernetice.

Au fost concepute și incluse în curricula universitară programe de masterat și cursuri post-universitare care cuprind o gamă largă de discipline subsumate domeniului securității cibernetice, astfel încât cei care urmează aceste programe de studiu să obțină competențele tehnice necesare specializării și integrării profesionale rapide.

Aceste programe de studii au fost demarate încă din 2018, existând deja primele promoții de absolvenți. Pentru a contribui efectiv la crearea unei mase critice de specialiști în securitate cibernetică, astfel de programe trebuie însă continuate și dezvoltate pe termen mediu și lung.

LA NIVEL PRE-UNIVERSITAR

Serviciul Român de Informații, în cooperare cu Ministerul Educației Naționale, și beneficiind de suportul unor universități și

firme din domeniul IT&C, au inițiat un proiect-pilot complementar, al cărui obiectiv constă în familiarizarea cu noțiuni aferente securității cibernetice a elevilor din patru licee cu profil informatică intensiv din București, Cluj-Napoca, Iași și Timișoara.

Proiectul reprezintă rezultatul unor demersuri realizate în parteneriat public-privat:
➡ cu reprezentanți ai unor universități din București, Iași, Cluj și Timișoara, care au derulat sesiuni de training pentru profesorii de informatică din cele patru licee;
➡ cu firme din domeniul IT&C și al securității cibernetice, care participă la proiect prin activități precum organizarea unor sesiuni de instruire pentru elevi și profesori.

Spre exemplu, începând cu luna octombrie 2020, experți din Serviciul Român de Informații / Centrul Național CYBERINT și din cadrul unor companii din mediul privat, susțin prezentări online pentru elevii și profesorii din cele patru licee, pe teme subsumate domeniului securității cibernetice. Până în prezent, în sesiunile online au fost abordate teme de interes la un nivel de complexitate adaptat ciclului liceal, precum „Top 10 riscuri de securitate cibernetică în securitatea aplicațiilor", „Tipologia atacurilor în zona serviciilor și aplicațiilor mobile", „Cum să ajungi să lansezi un start-up în cyber" și „Ce presupun Artificial Intelligence și Machine Learning".

BENEFICII

În scopul obținerii unor beneficii pe termen mediu și lung, atât în domeniul educațional, cât și în cel al securității cibernetice, este necesară continuarea și extinderea proiectelor în cadrul cât mai multor universități și licee pentru a:

➡ crește numărul de specialiști în domeniul securității cibernetice;
➡ expune tinerii la cunoștințe care le vor facilita demersul educațional ulterior;
➡ armoniza nivelul de pregătire între nivelul pre-universitar și cel universitar, prin conectarea tinerilor și profesorilor la tehnologiile și conceptele de ultimă generație;
➡ pregăti liceenii conform cerințelor pieței, prin integrarea/acomodarea rapidă a acestora cu programa academică din universitățile tehnice în care se abordează aspecte referitoare la securitatea cibernetică;
➡ asigura plierea demersului pe modul de predare în format online, impus atât de actualul context epidemiologic, cât și de evoluțiile în domeniul educațional existente la nivelul altor state;
➡ încuraja dobândirea unor noțiuni de igienă în spațiul cibernetic și de comportament responsabil încă de la începutul parcursului educațional.

NOUTĂȚI ÎN VIZIUNEA STRATEGICĂ A UE ÎN DOMENIUL **SECURITĂȚII CIBERNETICE**

La 16 decembrie 2020, Comisia Europeană și Înaltul Reprezentant al UE pentru Afaceri Externe și Politică de Securitate, Josep Borell, au prezentat Noua Strategie de Securitate Cibernetică a UE.

Prevederile documentului permit UE să se afirme ca lider în materie de norme și standarde internaționale în spațiul cibernetic și să consolideze cooperarea cu partenerii din întreaga lume pentru a promova un spațiu cibernetic global deschis, stabil și sigur, bazat pe valorile fundamentale ale UE: statul de drept, drepturile omului, libertățile fundamentale și valorile democratice.

Strategia cuprinde propuneri concrete de inițiative în materie de reglementare, de investiții și de politică, în principalele linii de acțiune ale UE:

1. Reziliență, suveranitate tehnologică și poziție de lider

Comisia propune revizuirea Directivei NIS, cu scopul de a întări reziliența cibernetică a sectoarelor publice și private critice: sistemul medical, rețelele energetice, domeniul transporturilor, centrele de date, administrațiile publice și laboratoarele de cercetare. De asemenea, se urmărește, la nivelul întregii UE, lansarea unei rețele de centre de operațiuni de securitate (SOC - Security Operations Center), bazate pe Inteligența Artificială (IA), care să constituie un adevărat scut de securitate cibernetică pentru UE. Acesta ar urma să dețină capabilități de detecție a semnalelor premergătoare unui atac cibernetic, permițând astfel adoptarea unor acțiuni proactive, menite să limiteze daunele.

2. Consolidarea capacității operaționale de prevenire, descurajare și răspuns

Comisia Europeană pregătește înființarea unei noi entități comune de securitate cibernetică. Aceasta va consolida coope-

rarea dintre organismele UE și autoritățile statelor membre responsabile de prevenirea și descurajarea atacurilor cibernetice și de răspunsul la acestea.

Tot în acest context, au fost prezentate propuneri de consolidare a setului de instrumente pentru diplomația cibernetică (folosirea resurselor diplomatice și a beneficiilor acțiunilor diplomatice pentru a proteja interesele naționale referitoare la spațiul cibernetic).

În noua viziune exprimată în Strategia de securitate cibernetică, UE va depune eforturi pentru a consolida cooperarea în domeniul apărării cibernetice și a dezvolta capabilități de apărare cibernetică de ultimă generație. În realizarea acestui deziderat, UE se va baza pe activitatea Agenției Europene de Apărare și va încuraja statele membre să utilizeze cooperarea structurată permanentă și Fondul european de apărare.

3. Promovarea unui spațiu cibernetic global deschis printr-o cooperare sporită

UE va promova normele și standardele internaționale care reflectă valorile fundamentale ale acesteia, în colaborare cu partenerii internaționali în cadrul Organizației Națiunilor Unite și al altor foruri relevante.

De asemenea, UE se angajează să sprijine implementarea noii Strategii de securitate cibernetică prin investiții fără precedent în tranziția digitală a UE, cu ajutorul unor programe precum Europa Digitală, Orizont Europa și Planul de redresare pentru Europa.

Obiectivul este de realiza investiții în valoare de până la 4,5 miliarde de euro din partea UE și a statelor membre, în special în cadrul Centrului de competențe în materie de securitate cibernetică, ce va avea sediul la București.

În ceea ce privește abordarea rezilienței cibernetice și fizice a entităților și a rețelelor critice, Comisia Europeană a înaintat două propuneri de directive:

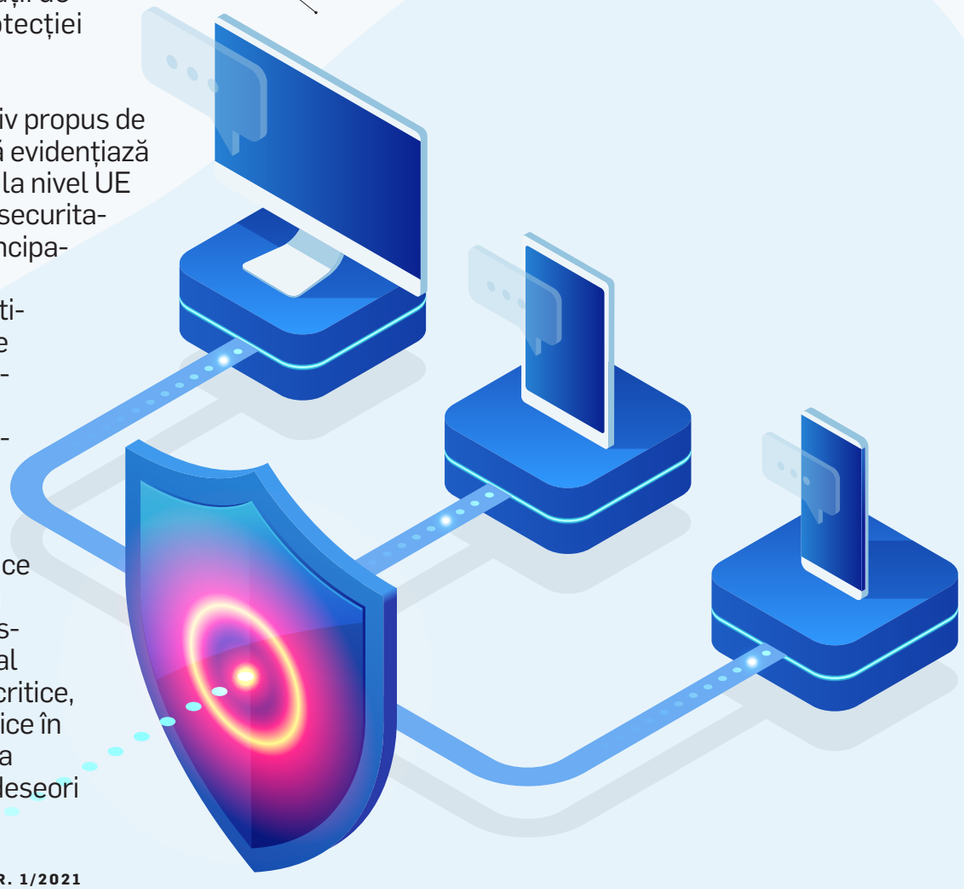
- Directiva privind măsuri pentru un nivel comun ridicat de securitate cibernetică în UE (NIS 2). Noua propunere legislativă introduce schimbări sistemice și structurale cadrului stabilit de Directiva 1148/2016. Comisia Europeană va oferi statelor membre mai multă flexibilitate în ceea ce privește identificarea și desemnarea entităților, care vor putea fi esențiale sau importante. De asemenea, în spectrul acoperit de NIS 2 vor fi adăugați noi operatori de servicii esențiale, din sectoare precum: spațiu, administrația publică, infrastructura digitală, servicii poștale și de curierat, alimentație.

Directiva privind reziliența entităților critice - extinderea și aprofundarea domeniului de aplicare al Directivei 114/2008, document ce vizează identificarea și desemnarea infrastructurilor critice europene (ICE) și evaluarea necesității de îmbunătățire a protecției acestora.

Noul cadru normativ propus de Comisia Europeană evidențiază dezideratul comun la nivel UE în ceea ce privește securitatea cibernetică, principalul obiectiv fiind revizuirea și eficientizarea proceselor de identificare, desemnare și protejare a infrastructurilor critice de pe teritoriul statelor membre. Asigurarea securității cibernetice este o componentă esențială a mecanismului de protecție al unei infrastructuri critice, sistemele informatice în baza cărora aceasta funcționează fiind deseori ținta unor atacuri.

INFO BOX

Asigurarea securității cibernetice este o componentă esențială a mecanismului de protecție al unei infrastructuri critice, sistemele informatice în baza cărora aceasta funcționează fiind deseori ținta unor atacuri.



STATISTICI

FRECVENȚA LUNARĂ A ACTIVITĂȚILOR DE PHISHING

IANUARIE	6291
FEBRUARIE	1609
MARTIE	243
APRILIE	156
MAI	157
IUNIE	26774
IULIE	22989
AUGUST	24515
SEPTEMBRIE	14884
OCTOMBRIE	19464
NOIEMBRIE	8046
DECEMBRIE	4535

În ceea ce privește tipurile de aplicații utilizate, s-a observat gradul ridicat al celor de tip downloader, întrucât acestea sunt necesare atacatorului pentru a distribui malware-ul în sistemele infectate. De asemenea, aplicațiile de tip troian bancar sau infostealer au înregistrat un număr mare de distribuiri la nivelul instituțiilor publice din România și a infrastructurilor IT&C cu valențe critice pentru securitatea națională. În contextul social al anului 2020, atacatorii au utilizat inclusiv aplicații ransomware pentru a targeta instituții din domeniul sănătății.

TOP 10 ALERTE MALWARE ÎN ROMÂNIA ÎN 2020

1	DOWNLOADER.EMOTET	60086
2	DOWNLOADER.AGENT	22753
3	INFOSTEALER.AGENTTESLA	10376
4	RANSOMWARE.LOCKY.DNS	9329
5	TROJAN.EMOTET	4559
6	TROJAN.TRICKBOT	2976
7	EXPLOIT.IOT.MIRAI	1593
8	INFOSTEALER.LOKIBOT	1225
9	TROJAN.FORMBOOK	1221
10	TOOL.COINMINER	942

În urma analizării alertelor generate de sistemul ȚIȚEICA, au fost identificate pe parcursul anului 2020 campanii malware ce au vizat instituții publice din România. Campaniile de distribuire a malware-ului EMOTET au fost cele mai numeroase la nivel național. De asemenea, s-a observat un grad ridicat de distribuire a aplicațiilor malware AGENT TESLA sau TRICKBOT, care au utilizat tehnici de inginerie socială și phishing pentru a compromite sistemele vizate.

STATISTICI

CELE MAI FRECVENT ÎNTÂLNITE APLICAȚII MALWARE

DOWNLOADER	68.3%
TROJAN	10.45%
INFOSTEALER	9.56%
RANSOMWARE	7.7%
EXPLOIT	3.32%
BACKDOOR	0.5%
WORM	0.17%

Campaniile de distribuție de phishing rămân principalul vector de infecție în derularea atacurilor cibernetice. Referitor la frecvența lunară a activităților de phishing identificate de-a lungul anului 2020, s-a remarcat tendința atacatorilor de a crește exponențial numărul atacurilor între lunile iunie și octombrie. Acest lucru a fost cauzat de starea de incertitudine prezentă în rândul cetățenilor și cantitatea mare de informații referitoare la pandemia COVID-19 și efectele acesteia. Suplimentar, creșterea activităților de phishing poate fi cauzată și de intensificarea utilizării serviciilor online (precum cele comerciale sau de curierat), atacatorii cibernetici impersonând în repetate rânduri identitățile unor astfel de entități private.

INTERVIU
DAN CÎMPEAN

DIRECTOR CERT-RO

Sunteți absolvent al Universității din București, Facultatea de Fizică. Cum ați ales să vă construiți o carieră în domeniul securității cibernetice?

Probabil sunt un exemplu relevant al necesității de a ne adapta continuu și rapid la noile realități ale profesiei. Aceasta a evoluat foarte rapid în ultimii ani și a devenit un magnet pentru specialiști care au identificat securitatea cibernetică drept o oportunitate reală din punct de vedere al carierei. Domeniul securității cibernetice este unul complex, în transformare rapidă și care necesită multiple calități, tipuri de cunoștințe – tehnice și non-tehnice. Pentru a construi echipe cyber puternice, azi este nevoie și de manageri, de juriști, specialiști în comunicare și cooperare, în plus față de aptitudinile tehnice fundamentale.

Deținеți experiență de peste 20 de ani în domeniul securității cibernetice și ați ocupat diverse poziții în companii private de notorietate la nivel

internațional. Care credeți că sunt principiile pe care le-ați deprins ca urmare a experienței din mediul privat și pe care le transpuneți în activitatea dumneavoastră de director al CERT-RO?

Mediul privat nu este mult mai simplu, dar nici mai complex, față de sectorul public sau de cel guvernamental. Sunt însă unele practici și principii profesionale care cred că pot fi adoptate cu succes la o instituție cum este CERT-RO. Printre acestea, o prioritate personală este încurajarea principiului inițiativei și a colaborării la toate nivelurile: individual, de servicii, de direcții, de instituții. Am observat că, în multe situații, colegi din CERT-RO au încă ezitări în a-și prezenta ideile, sugestiile, inițiativele – sunt convins că practici și modalități de lucru deja validate în mediul privat vor ajuta la deblocarea potențialului creativ și de colaborare. Un alt principiu pe care încerc să îl transpun la CERT-RO este cel al eficienței – aici putem cu siguranță învăța multe din experiența sectorului privat, îndeosebi în modul în care utilizăm timpul de lucru, una dintre resursele cele mai prețioase, în special în domeniul securității cibernetice.

Ați ocupat o serie de poziții în domeniul securității cibernetice în cadrul unei companii din "Big4" și v-ați desfășurat aproape toată activitatea profesională în afara României. Care considerați că sunt principalele diferențe în ceea ce privește modul în care este văzut domeniul în România, comparativ cu alte state?

Cred că atât în România, cât și în alte țări, domeniul cyber este recunoscut ca unul transversal, tehnic dar și cu un potențial remarcabil. Privind aceasta, nu sunt diferențe majore, ceea ce este normal pentru un domeniu profesional ce nu are granițe și nu depinde în mod strict de limitări de natură tehnică sau lingvistică. Sunt însă unele diferențe de abordare cu privire la urgența și necesitatea unui efort național de investiție în dezvoltarea acestui domeniu. Câteva țări europene (ex. Franta, Germania, Luxemburg) sau din afara UE (ex. Israel) au recunoscut cu ani în urmă importanța strategică a investițiilor pe termen lung în domeniul securității cibernetice – iar acum beneficiază de un efect pozitiv de multiplicare a acestor investiții, inclusiv în domenii conexe: digitalizare pe ansamblu, educație, dezvoltare de noi tehnologii.

Ocupați funcția de Director al CERT-RO de aproximativ un an. Care considerați că sunt temele de importanță majoră și zonele problematice pentru domeniul securității cibernetice din România?

Cu siguranță, asigurarea unui nivel corespunzător al capabilităților și resurselor cyber la nivel național este de o importanță vitală pentru România. O altă temă de dezbatere pregnantă în comunitate este deopotrivă educația digitală a utilizatorilor din România. Există o diferență de expertiză majoră între ceea ce noi numim 'utilizatorul obișnuit' și specialistul de cyber. La nivel internațional, România este extrem de apreciată pentru talentele pe care le propunem în domeniu. Din păcate, acești oameni extrem de capabili de multe ori sunt recrutați de companii străine puternice și, fie se mută peste hotare, fie lucrează remote pentru acestea. Astfel, unul din obiectivele pe care le avem la CERT-RO este chiar stoparea acestei hemoragii de creiere peste hotare, pentru că deja ne confruntăm cu o cerere din piața forței de muncă mult peste ce avem în acest moment la dispoziție pentru recrutare. La polul opus acestor specialiști, extrem de căutați și apreciați în comunitatea de cybersecurity, se află utilizatorul obișnuit, care nu are pregătirea necesară să facă față dinamicii amenințărilor din online și care trebuie informat și instruit treptat, deoarece mediul educațional nu propune momentan, cel puțin la nivel pre-universitar, cursuri adecvate vremurilor în care trăim.

Care considerați că sunt principalele realizări pe care le-ați avut ca director al CERT-RO?

Cred că realizările, sau nerealizările mele ca director al CERT-RO vor putea fi estimate mult mai bine de un observator neutru din afara instituției. Personal, sunt însă foarte mulțumit că, în cele 10 luni de când m-am alăturat CERT-RO, am reușit să reconstruiesc încrederea echipei de conducere în viziunea proprie privind rolul și viitorul acestei instituții. Este esențial ca o organizație civilă de nivel național în domeniul securității cibernetice să poată avea claritate și încredere în propriul rol, în modul în care conducerea acesteia o poziționează printre actorii instituționali naționali sau europeni.

În situația în care identificați o vulnerabilitate critică de securitate cibernetică, care sunt pașii concreți pe care CERT-RO îi urmează în gestionarea unei astfel de provocări?

Echipa CERT-RO a dezvoltat un program denumit CVD (Coordinated Vulnerability Disclosure - Divulgarea Coordonată a Vulnerabilităților) care este de fapt o formă de cooperare dintre deținătorii sau producătorii de servicii, sisteme și programe informatice și raportorii de vulnerabilități (terțe persoane care identifică și/sau raportează vulnerabilități ale serviciilor, programelor și sistemelor informatice). Prin intermediul acestui program, cele două părți se coordonează în remedierea vulnerabilităților, înainte de divulgarea publică a informațiilor care ar permite comunității largi de utilizatori, producători și cercetători în securitate informatică să adopte măsurile necesare eli-

minării riscurilor de securitate. Practic, CERT-RO acționează ca un soi de mediator între raportorul vulnerabilității și producătorii sau furnizorii acelor servicii afectați de această vulnerabilitate.

Așadar, dacă ați descoperit o vulnerabilitate, primul pas pe care trebuie să-l faceți este să ne transmiteți un e-mail la cvd@cert.ro în care să documentați vulnerabilitatea, precum și pașii/tehnicile necesare pentru punerea în evidență a acesteia. Totodată, va fi nevoie să descrieți modalitatea prin care ați descoperit vulnerabilitatea. Ulterior, dacă raportarea întrunește condițiile necesare, CERT-RO va contacta deținătorul/producătorul și va oferi părților actualizări periodice referitoare la stadiul cazului raportat. După ce acea vulnerabilitate a fost remediată, raportorul va fi notificat cu privire la rezolvarea cazului și la eliminarea restricției de publicare, după caz.

Cum procedează instituția dumneavoastră în eventualitatea în care vulnerabilitatea respectivă nu se regăsește în categoria serviciilor esențiale conform Legii nr.362/2018?

Programul CVD pentru raportarea de vulnerabilități nu este dedicat exclusiv operatorilor de servicii esențiale și furnizorilor de servicii digitale, așa cum sunt ei definiți în Directiva NIS, implementată în legislația națională prin Legea nr. 362/2018. Divulgarea vulnerabilităților către deținătorii sau producătorii de servicii, sisteme și programe informatice funcționează pe baza aceluiași regulament, neexistând proceduri separate pentru situațiile în care serviciile afectate intră sub incidența Directivei NIS.

Ați propus Guvernului României un proiect legislativ privind crearea Directoratului Național de Securitate Cibernetică. Care considerați că ar fi principalele avantaje pentru România în cazul operaționalizării acestui organism?

Directoratul Național de Securitate Cibernetică este recomandat a fi creat printr-o ordonanță de urgență, pentru a se reuși operaționalizarea imediată a acestei noi instituții civile ce va înlocui CERT-RO, îndeosebi în acest moment când importanța domeniului cyber la nivelul UE a crescut semnificativ. Proiectul de OUG pentru înființarea Directoratului oferă un design instituțional și o bază legislativă moderne, pe care foarte puține țări le-au adoptat până acum.

Un avantaj evident va fi crearea unui pol de atractivitate pentru noua generație de talente și competențe cyber din România, inclusiv pentru femeile care activează în această profesie. Aceasta va permite alocarea resurselor necesare pentru atragerea de specialiști de top din mediul privat, dar și a unui număr mare de tineri absolvenți / debutanți, pentru menținerea în țară a forței de muncă înalt calificate.

În plus față de atribuțiile ce vor fi moștenite de la CERT-RO, Directoratul va avea responsabilități și va derula activități la nivelul celor mai avansate organizații civile din acest domeniu, contribuind semnificativ la creșterea nivelului de securitate cibernetică la nivel național.

Directoratul va avea capacitatea de a se autofinanța integral, de a aduce bani la bugetul de stat, așa cum o fac instituții similare din alte țări UE.

Prin crearea acestei noi instituții, statul român va consolida și dezvolta semnificativ parteneriatul intre mediul public-privat-universitar în securitate cibernetică, generând o dezvoltare sustenabilă a acestui domeniu la nivel național cu efecte benefice directe și imediate în economia națională.

Crearea Directoratului va asigura capabilitățile și performanța necesară în domeniul securității cibernetice la nivel național pentru o perioadă de cel puțin 10 ani.

La 09.12.2020, capitala României a fost desemnată de reprezentanții guvernelor statelor membre ale UE pentru a găzdui sediul noului Centru de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică. Care credeți că este impactul acestei decizii la nivel național, regional și european?

Să nu uităm, țara noastră nu găzduia nicio agenție a Uniunii Europene, deși România și-a adus un aport substanțial la transformarea digitală, la creșterea nivelului securității și rezilienței cibernetice a economiei și societății europene. Găzduirea la București a Centrului european cyber este un rezultat remarcabil și o recunoaștere la nivel european a rolului, capabilităților și potențialului pe care țara noastră le are în acest domeniu de vârf. Zona securității cibernetice a crescut semnificativ ca importanță, dar și ca și vizibilitate, la toate nivelurile, de la cel european până la cel local sau de sector economic.

Este un fapt cunoscut că acest Centru european va lansa și derula numeroase programe și proiecte finanțate din fonduri europene pe domeniul securității cibernetice și va fi un catalizator al inovării, cercetării si colaborării din domeniul securității cibernetice pentru statele membre ale UE. Inerent, un nivel semnificativ crescut al proiectelor și

inițiativelor majore, al cercetării și dezvoltării derulate prin Centrul european, plasează „de facto" România în centrul activităților cyber al Europei. Va trebui să reușim să capitalizăm aceasta în interes național, prin urmare, un pas important din partea autorităților competente române va fi să ia decizia a se implica și de a se coordona în mod eficace cu industria, cu mediul universitar, cu cel de cercetare, inclusiv cu autoritățile desemnate prin Directiva NIS (CERT-RO, în cazul României).

Având în vedere experiența dumneavoastră din mediul privat, în special cea din afara României, care credeți că sunt carențele legislative ale țării noastre în materie de securitate cibernetică în comparație cu legislația altor state europene?

România a avut deja întârzieri în implementarea corespunzătoare a legislației europene, spre exemplu a Directivei NIS, ceea ce a afectat piața de servicii de audit și de consultanță de securitate cibernetică. Această paradigmă poate fi schimbată, iar țara noastră ar putea deveni unul din statele membre ale UE ce poate adopta sau operaționaliza rapid noile directive și reglementări europene din domeniu.

Mai mult, instituții cheie cum ar fi CERT-RO funcționează pe baza unei legislații învechite, neactualizată de aproape 10 ani. Este necesar ca legislația națională să fie actualizată corespunzător pentru a permite ca autoritățile și instituțiile publice să țină pasul cu dinamica amenințărilor cibernetice. Așa cum alte state membre ale UE au făcut-o deja, și România poate legifera cu prioritate domeniul securității cibernetice pentru a asigura crearea de capabilități (tehnice, organizaționale, operaționale), a unor platforme naționale de conștientizare și cooperare, programe de educație, de cercetare-dezvoltare, precum și a unor mecanisme de certificare, conformitate și standardizare.

Actuala Strategie de Securitate Cibernetică a României datează din 2013. Dat fiind faptul că domeniul este unul dinamic, având impact în toate celelalte domenii ale vieții sociale și economice, care considerați că ar trebui să fie principalele linii strategice pe care ar trebui să le urmeze România în următorii 5 ani, pe zona de cyber security?

Sunt de părere că este important ca România să aibă o strategie națională actualizată de securitate cibernetică care, pe de o parte să sprijine îndeplinirea obiectivele naționale de securitate și a angajamentelor asumate de România la nivel NATO și UE, iar pe de altă parte să creeze cadrul necesar poziționării domeniului securității cibernetice pentru a sprijini societatea românească, economia, dar și zona educațională și de cercetare.

În principal, va fi esențial ca noua strategie națională de securitate cibernetică a României să redefinească un cadru normativ și instituțional robust și consolidat, care va permite instituțiilor cu responsabilități în acest domeniu să activeze cu un nou aplomb, mult mai dinamic și mai coerent.

Desigur, obiectivul de a avea rețele și sisteme informatice sigure și reziliente, atât la nivel național, cât și la nivel de sector economic, de instituție sau de organizație, este unul încă foarte valabil, dar unul care necesită un efort semnificativ crescut față de acum 5-10-15 ani. Dezvoltarea de parteneriate pragmatice între mediul public și privat va fi instrumentală pentru un astfel de obiectiv.

Mai mult, prin găzduirea la București a noului Centru de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică, relevanța României ca actor-cheie în arhitectura internațională de cooperare în domeniul securității cibernetice a crescut semnificativ. Este un moment optim ca statul român să răspundă proporțional încrederii arătate de Uniunea Europeană către potențialul și rolul României, prin decizii și investiții inteligente în cyber.

Având în vedere evoluția continuă a mediului de securitate cibernetică, a amenințărilor, precum și ritmul accelerat de digitalizare, generat inclusiv de contextul pandemiei COVID-19, care considerați că sunt principalele cinci bune practici pe care utilizatorii ar trebui să le adopte?

Utilizatorul uman este una dintre verigile cheie, dar, paradoxal, cea mai vulnerabilă din ecosistemul de securitate cibernetică. Educarea utilizatorului final în a aplica un simplu set de reguli de „igienă cibernetică" poate reduce semnificativ riscurile de securitate cu care ne confruntăm.

Prima practică pe care o recomand utilizatorului obișnuit este să își formeze și să aplice în mod consecvent o rutină de securitate zilnică, ce ar trebui să includă o atenție sporită pentru evitarea unor acțiuni online executate în mod pripit, în special atunci când sunt implicate date sensibile, personale sau confidențiale. Este necesar ca utilizatorul să fie atent, vigilent și răbdător atunci când activează online și să conștientizeze existenta unor riscuri inerente.

O a doua practică recomandată se referă la gestionarea corectă a parolelor și protejarea datelor de acces la conturile de utilizator. Folosirea unor parole complexe, precum și a

unei aplicații de management al parolelor, împreună cu activarea unui pas de autentificare suplimentar (2FA) reprezintă o soluție ce poate limita multe dintre riscurile implicate.

În această perioadă, majoritatea dintre noi organizăm sau participăm la teleconferințe. Acestea ar trebui să fie întotdeauna efectuate pe platforme verificate și protejate împotriva accesului neautorizat. Pe perioada pandemiei COVID-19 este evident că un volum mult mai mare de informații sensibile este transmis prin facilitățile de teleconferință, prin urmare utilizarea unor platforme ce au un număr redus de vulnerabilități este esențială pentru o securitate adecvată a informațiilor. În plus, participanții la teleconferință ar trebui autentificați atât prin mijloace tehnice, cât și prin mijloace procedurale, de exemplu prin utilizarea codurilor PIN și validarea corespunzătoare a participanților reali verificând lista de invitați confirmați.

Este important să se adopte un set de controale stricte asupra configurațiilor echipamentelor folosite pentru conectarea la distanță, pentru a preveni utilizarea rău intenționată a acestora. De exemplu, utilizatorii finali nu ar trebui să aibă drepturi de administrare pe echipamente, să accepte scanările de securitate periodice și utilizarea unor soluții de securitate actualizate (ex. VPN) pentru accesul la distanță.

Nu în ultimul rând, în special în această perioadă în care o mare parte dintre noi lucrează de la distanță (telemuncă), se recomandă respectarea strictă a politicilor, regulilor și procedurilor de securitate ale organizației din care facem parte. Mulți utilizatori uită că lucrul de la distanță creează riscuri și vulnerabilități suplimentare, pentru care este vitală o disciplină crescută a utilizatorului obișnuit. Suntem responsabili nu doar în ceea ce privește datele noastre, ci și ale organizației cu care sau pentru care lucrăm.

VIZIUNEA INDUSTRIEI PRIVATE CU PRIVIRE LA MEDIUL DE SECURITATE CIBERNETICĂ - BITDEFENDER

DE CĂTĂLIN COSOI - HEAD OF INVESTIGATION AND FORENSICS UNIT, BITDEFENDER

Anul 2020 a venit la pachet cu multe surprize pentru industria securității cibernetice, în măsura în care peste 50% dintre organizații nu erau pregătite a face fata scenariului în care trebuie să-și migreze întreaga forță de muncă într-un mod de lucru hibrid sau de acasă.

SARS-CoV-2 a impactat enorm modul în care organizațiile își desfășoară activitatea ceea ce a deschis calea atacatorilor către o pluralitate de vulnerabilități și configurări eronate, ce urmau să apară inerent având în vedere viteza cu care organizațiile au trebuit să se replieze astfel încât să supraviețuiască pandemiei.

O altă surpriză a anului precedent a fost atacul asupra producătorului american de software SolarWinds, ce oferă o suită completă enterprise de monitorizare, management, securitate a infrastructurilor IT, prin care, o grupare de hackeri presupus ruși au reușit să compromită peste 100 de companii private sau de stat care utilizează serviciile aceste companii. Acesta este probabil unul dintre cele mai mari hack-uri din istoria securității, printre victime numărându-se companii de securitate, companii producătoare de software și sisteme de operare și o multitudine de organizații de stat americane, precum Departamentul Apărării, al Energiei, Homeland Security, Trezoreria și multe altele. Vor mai trece multe luni până când se vor cunoaște toate implicațiile acestui atac.

Iar peste aceste două puncte de mai sus au tronat în continuare atacurile de tip ransomware, profitând de pe urma vulnerabilităților și a erorilor de configurare pentru a cripta infrastructurile companiilor victimelor și a le decripta dacă victima plătește, sau a face publice informațiile confidențiale furate dacă victima refuza sa plătească.

Pentru 2021, Bitdefender anticipează că vom asista la un peisaj cu amenințări informatice din ce în ce mai agresive, iar atacatorii vor exploata orice oportunitate de a face bani cât mai ușor.

Atacatorii se vor concentra în direcții strategice unde vom asista la schimbări importante. Routerele și calculatoarele de acasă vor continua să fie atacate și compromise. Odată infectate, aceste dispozitive vor fi închiriate de către atacatori unor grupări interesate să le folosească în orchestrarea unor atacuri mai ample. În plus, creșterea valorii criptomonedelor va alimenta asemenea practici și pentru crearea unor rețele de calculatoare și servere a căror putere de procesare va fi folosită ilegal pentru a mina monede virtuale fără ca proprietarul de drept să știe. De asemenea, tot mai multe amenințări informatice vor infecta dispozitive MacOS și Android, inclusiv prin campanii derulate în magazinul oficial Google Play.

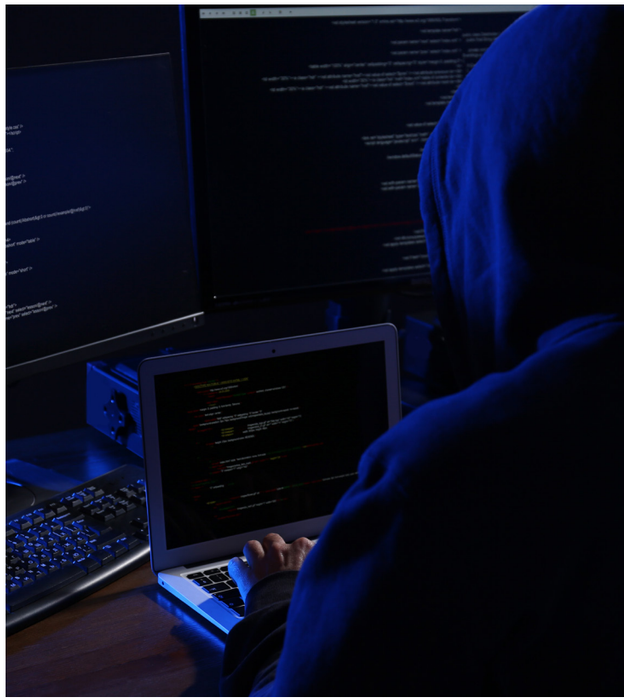
Breșele de securitate sunt la ordinea zilei, iar companiile alocă resurse însemnate pentru a păstra în siguranță infrastructurile IT. Pe măsură ce tot mai mulți oameni lucrează de acasă din cauza pandemiei, angajații vor continua să facă anumite compromisuri din comoditate. Dispozitivele personale securizate necorespunzător, precum routerele, dar și transferul de informații confidențiale prin canale neautorizate, cum ar fi serviciile de mesagerie online, adresele personale de e-mail sau serviciile de tip cloud de trimitere a documentelor, vor juca un rol cheie în scurgerile de date și vor alimenta apariția de noi breșe.

În paralel, presiunea pe departamentele IT din companii va crește constant, astfel că atacatorii vor primi o mână de ajutor și de la servere configurate necorespunzător din infrastructurile cloud, baze de date expuse incorect sau date de acces stocate fără protecție.

Atacurile informatice care vizează sistemul de operare din dispozitive smart, altădată percepute ca fiind complexe și greu de dus la capăt, vor deveni din ce în ce mai frecvente. Folosirea abuzivă a unor instrumente specializate precum RwEverything va determina sporirea atacurilor firmware, mai ales la adresa sistemelor unde producătorii nu au configurat corect arhitectura astfel încât să poată preveni rescrieri neautorizate. Dezvoltatorii de ransomware se vor folosi de asemenea erori ca să paralizeze complet anumite dispozitive până ce victima achită o recompensă.

Încă din 2014, amenințările de tip ransomware, care blochează accesul la date și apoi cer recompensă pentru deblocare, au însemnat un business profitabil pentru infractori și au inspirat tot mai mulți atacatori să folosească acest tip de atac. Concurența dintre grupările infracționale pentru o cotă de piață cât mai mare este o veste cât se poate de proastă pentru oamenii de rând și companii, întrucât va duce la crearea unor amenințări informatice din ce în ce mai sofisticate și, deci, și mai greu de decriptat. Dacă până acum atacatorii doar blocau datele și cereau recompensă, datele Bitdefender arată că cea mai nouă tendință e să le și copieze înainte de a le bloca, ceea ce poate crea o presiune în plus la adresa victimei odată ce este amenințată cu dezvăluirea în spațiul public a informațiilor confiscate.

Atacatorii informatici se vor concentra pe lanțul de aprovizionare a țintelor vizate și nu vor ataca direct victime de calibru. Exemple recente precum cel al atacării „lanțului rece" de aprovizionare cu noul vaccin anti-COVID și cel asupra autorităților de reglementare care gestionau documentația antidotului arată tendința atacatorilor de a găsi veriga slabă din preajma țintei mai mari și compromiterea acesteia. Domeniile vizate vor fi mai ales cercetare-dezvoltare, servicii medicale și farma. În plus, grupările specializate în spionaj industrial vor apela la amenințări avansate pentru a infecta ținte atent alese, mizând pe tehnici avansate de inginerie socială capabile să păcălească până și cea mai precaută persoană.



Criminalitatea online disponibilă ca serviciu pentru cei interesați va atinge un vârf al ofertei în 2021. Dezvoltatorii de amenințări informatice și infractorii se vor concentra pe conceperea unor amenințări sofisticate și imposibil de detectat de către soluțiile de securitate și le vor vinde celor care plătesc cel mai mult. Companiile vor fi nevoite să adopte metode ultra avansate de protecție, similare celor la care apelează țintele strategice vizate în mod curent de asemenea arme cibernetice.


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