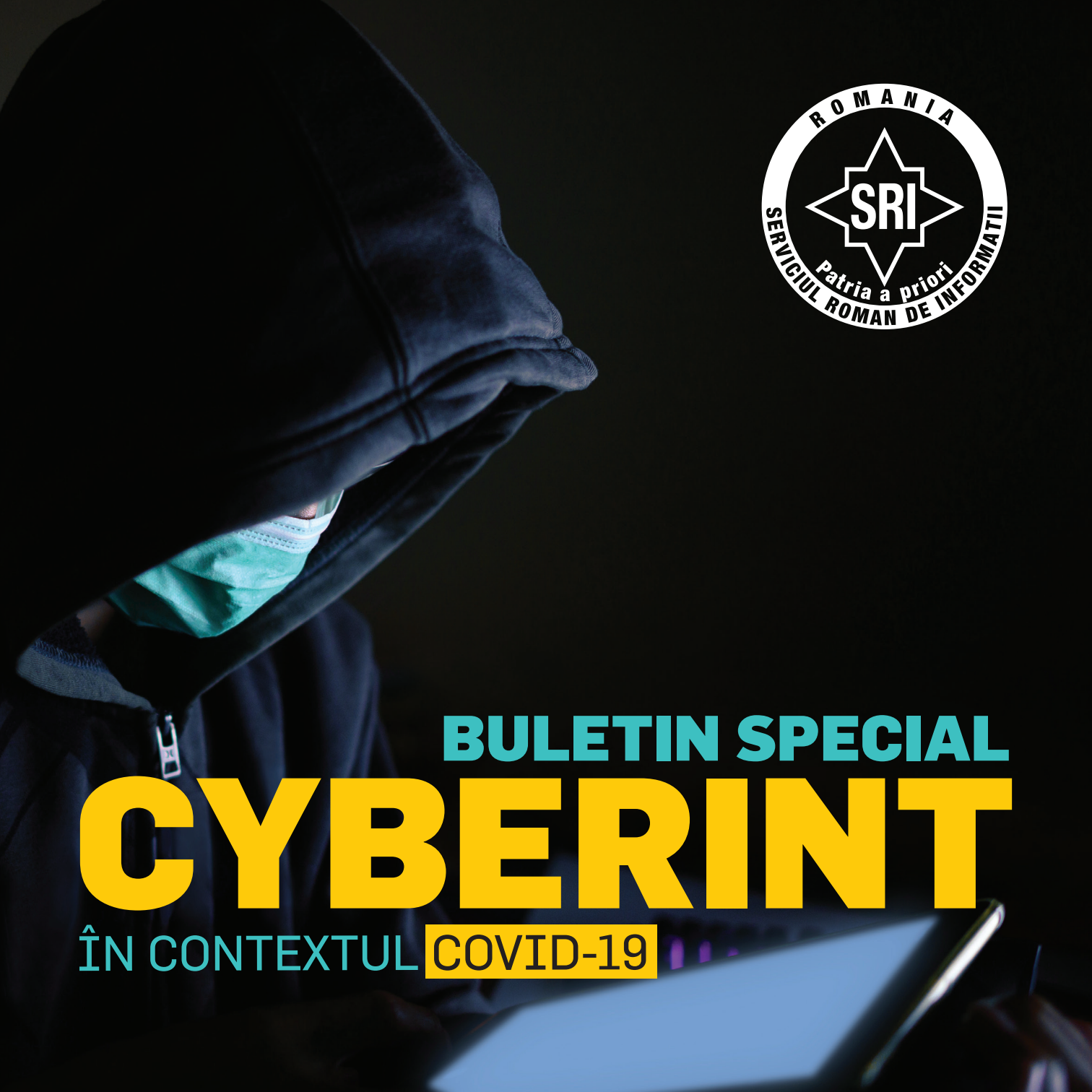

BULETIN SPECIAL

CYBERINT

ÎN CONTEXTUL COVID-19

ATACURI CIBERNETICE ÎN CONTEXTUL COVID-19

În contextul crizei COVID-19, la nivel global s-au intensificat activitățile ostile din spațiul cibernetic. Actorii cibernetici utilizează contextul social actual, atât prin derularea de atacuri cibernetice care au la bază tehnici de inginerie socială, cât și prin încercări de afectare a unor servicii din domenii cheie (sănătate, administrație publică, educație etc.) pentru gestionarea crizei COVID-19.

Astfel, au fost identificate, inclusiv în România, campanii de atacuri cibernetice de tip *ransomware* și *web defacement*, dar și atacuri cu aplicații de tip *troian bancar*, în acord cu motivațiile actorilor cibernetici implicați. Cu toate că scopurile atacurilor cibernetice sunt diferite și diversificate, **se remarcă faptul că în majoritatea cazurilor identificate s-au utilizat tehnici de inginerie socială, precum *phishing-ul, spear-phishing-ul* sau *smishing-ul*,** pentru a transmite victimelor link-uri sau atașamente ce conțin aplicații malware.

Precizări:

- ***Ransomware**: atac cibernetic prin care se vizează afectarea integrității și disponibilității datelor din cadrul sistemelor informatice, prin criptare, și implicit prin blocarea accesului la acestea, solicitând plata unei răscumpărări în monedă virtuală.*

- ***Web defacement** - atac cibernetic asupra unui website care constă în înlocuirea neautorizată a interfeței paginii web prin exploatarea unor vulnerabilități de securitate cibernetică. Elementele grafice introduse pot conține mesaje prin care se motivează atacul, autorul sau gruparea care a efectuat atacul, alte date compromise (precum conturi de utilizator și parole) sau eventuale link-uri către alte site-uri. În urma unui atac de tip defacement, forma legitimă a site-ului web este inaccesibilă, fiind necesară restaurarea lui, precum și verificarea breșelor de securitate care au permis atacul.*

- ***Troian bancar** – aplicație malware creată pentru a obține acces și pentru a extrage date despre conturile utilizatorilor sistemelor bancare online.*

TEHNICI DE INGINERIE SOCIALĂ

Atât incidența globală, cât și rata ridicată de succes a atacurilor ciberentice din perioada crizei COVID-19, pot fi argumentate prin faptul că pandemia a devenit cel mai discutat subiect de pe agenda publică internațională, ceea ce a generat o serie de emoții cu impact negativ în rândul populației. Prin definiție, **ingineria socială** presupune derularea de acțiuni de manipulare a factorului uman, în vederea atingerii unor etape intermediare necesare derulării unor atacuri cibernetice. În context, atacatorii cibernetici au făcut apel la starea emoțională a potențialelor ținte, prin subiecte special create în acest sens, pentru a-și atinge o serie de obiective nelegitime: *obținere de foloase financiare necuvenite, accesarea neautorizată și indisponibilizarea unor sisteme informatice și furt de date persoanale.*

În ultimele luni s-au utilizat și distribuit (ex. prin e-mail, SMS, aplicații de mesagerie instantă) mesaje special create, care făceau referire la subiectul COVID-19.

Câteva dintre **titlurile / subiectele abordate** în tentativele de inginerie socială din această perioadă au fost:

- *Numărul de persoane infectate cu Coronavirus în [nume de țară], astăzi [data din ziua transmiterii mesajului]*
- *Numărul de persoane infectate cu Coronavirus în [nume de țară]*
- *Propunere de finanțare pentru combaterea Coronavirus*
- *Fond de prevenire a Coronavirus – Organizația Mondială a Sănătății*
- *Vânzare măști de unică folosință*
- *Protecție împotriva Coronavirus prin utilizarea uleiului pentru imunitate*
- *COVID-19 UPDATE !!!*
- *COVID-19 – nCoV – Update Special – OMS*
- *Coronavirus: Informații importante și măsuri de precauție*
- *Detalii secrete! (COVID-19)*

Pentru a **diminua riscurile materializării unui atac cibernetic care folosește scheme de inginerie socială**, recomandăm:

- Evitarea transmiterii sau recepționării de informații sensibile prin e-mail
- Alegerea unui provider de e-mail care oferă o filtrare puternică anti-spam
- Acordarea unei atenții sporite la adresa de mail a expeditorului, verificând relația dintre expeditor și conținutul mesajului
- Evitarea deschiderii atașamentelor / accesării link-urilor nesolicitate sau provenind de la adrese aparent legitime, dar având mesaje cu subiect și conținut atipic. Dacă este absolut necesară deschiderea unui astfel de atașament, chiar și din e-mailuri legitime, acesta trebuie, în prealabil, descărcat și scanat cu soluția antivirus instalată și, ulterior, deschis cu aplicația asociată
- Evitarea accesării directe a link-urilor din cadrul unor mesaje e-mail, îndeosebi a celor care nu utilizează protocolul HTTPS
- Evitarea furnizării de răspunsuri la mesaje care conțin solicitări de date personale sau confidențiale (ex. cod PIN, parole, date asociate contului și cardului bancar)
- Utilizarea doar a site-urilor / platformelor oficiale pentru a obține informații referitoare la COVID-19

ATACURI CIBERNETICE DE TIP *RANSOMWARE*

În contextul COVID-19, actorii cibernetici au vizat utilizatorii individuali, dar mai ales organizațiile (instituții publice și entități private) din domenii cheie pentru gestionarea crizei epidemiologice, cel mai vizat fiind cel al *sănătății*. Au fost vizate, îndeosebi, spitale și alte instituții publice din domeniul sănătății, atacatorii exploatând necesitatea stringentă a acestora de a avea acces la sistemele informatice deținute.

Atacurile cibernetice de tip ransomware vizează sistemele informatice, atât prin transmiterea unor mesaje special create prin tehnici de inginerie socială, cât și prin exploatarea unor vulnerabilități de securitate cibernetică.

La nivel mondial, în perioada crizei COVID-19, au fost identificate o serie de atacuri cibernetice de tip *ransomware*, precum:

- **COVIDLOCK**, care se răspândește prin intermediul **aplicației mobile "COVID19 Tracker".** Aplicația criptează datele de pe dispozitivul mobil și solicită plata a 100 BTC pentru deblocarea acestora.

- **NETWALKER**, care este transmis prin intermediul unor mesaje de tip *phishing*. Această aplicație malware vizează sistemele informatice pe care rulează Windows 10 și are capabilități de evitare a detecției de către soluțiile de securitate cibernetică (ex. antivirus).

- **MAZE**, care se răspândește atât prin mesaje de tip *phishing*, cât și prin exploatarea unor vulnerabilități de securitate cibernetică, precum cele ale protocoalelor de comunicații de la distanță (*remote desktop protocol*). Comparativ cu alte atacuri de tip *ransomware*, în afară de criptarea datelor și de solicitarea unei recompense, MAZE realizează și sesiuni de exfiltrare de date, în vederea obținerii unor venituri consistente.

- **NEMTY,** care se răspândește prin mesaje de tip *spear-phishing*, inclusiv prin impersonarea unor entități medicale, cu relevanță în contextul COVID-19. Acest *ransomware* a vizat entități din domeniul sănătății.

Pentru a diminua riscurile de infectare cu aplicații malware de tip *ransomware*, recomandăm:

- Utilizarea pe toate sistemele din rețea a unei soluții de tip antivirus actualizate, care să dispună de module de protecție anti-ransomware activate.
- Realizarea zilnică de copii de siguranță (BACK-UP) pentru principalele sisteme din rețea care stochează date, dar și pentru serverele care găzduiesc domenii importante (în vederea restaurării facile în cazul unei compromiteri).

- Actualizarea tuturor sistemelor de operare din rețea, dar și a aplicațiilor principale utilizate (Suita MS Office, Adobe Acrobat, etc.).
- Folosirea celui mai redus nivel de privilegii necesare pentru executarea acțiunilor/operațiilor, atât pentru aplicații, cât și pentru utilizatori.
- Evitarea introducerii de date personale în cadrul unor pagini web (de ex.: adresă e-mail și parolă, detalii bancare, ș.a.).

ATACURI CIBERNETICE CU APLICAȚII MALWARE DE TIP *TROIAN BANCAR*

Actualul context a generat o creștere a gradului de utilizare al platformelor bancare online, de tip Internet Banking, sens în care actorii cibernetici ostili și-au intensificat activitățile de distribuire de aplicații malware care vizează obținerea de credențiale de acces la aceste platforme. Și în acest caz, sunt utilizate tehnici de inginerie socială prin care atacatorii cibernetici vizează infectarea dispozitivelor clienților băncilor.

Serviciul Român de Informații a identificat o serie de campanii de acest fel la nivel național. Având în vedere că riscul generat de astfel de campanii la adresa sistemelor IT&C ale utilizatorilor este unul ridicat, SRI a realizat campanii de conștientizare publică referitoare la:

- **Cerberus Android Banker**, care vizează utilizatori individuali prin distribuirea unui mesaj tip text redactat în limba română, care conține sintagma „*Detalii secrete! (COVID-19)*". Principalul pericol este acela că troianul oferă acces ilicit la date din aplicațiile bancare. De asemenea, *Cerberus Android Banker* poate extrage date despre aplicațiile de mesagerie și poștă electronică instalate pe dispozitivul vizat (spre exemplu, Telegram, WhatsApp sau Gmail), precum și jurnalizarea apăsărilor de taste și exfiltrarea datelor astfel obținute.

- **Qbot**, care vizează utilizatori individuali prin transmiterea unor e-mailuri de tip *spear-phishing*, pentru a obține acces la date financiare. Mesajele de *spear-phishing* pot avea fie un link în conținut, fie un atașament. Atașamentul este un fișier de tip

zip, care conține un document MS Word ce rulează un macro prin care se descarcă troianul și se realizează infectarea dispozitivului.

Pentru a diminua riscurile de infectare cu aplicații malware de tip troian bancar, recomandăm:

- Utilizarea de soluții antivirus și actualizarea constantă a semnăturilor acestora.
- Actualizarea sistemului de operare și evitarea utilizării sistemelor de operare care nu mai primesc suport din partea producătorului.
- Verificarea conturilor bancare pentru a depista eventualele accesări neautorizate.

În plus, în situația în care este suspectată o eventuală compromitere a sistemelor IT&C utilizate, recomandăm:

- Schimbarea credențialelor de acces pentru autentificarea în dispozitiv și în aplicații.
- Resetarea dispozitivului mobil prin revenire la setările din fabrică.
- Notificarea băncii atunci când observați tranzacții bancare care nu vă aparțin.

ATACURI CIBERNETICE DE TIP *WEB DEFACEMENT*

Cu toate că atacurile de tip *web defacement* nu au un nivel ridicat de sofisticare și complexitate, acestea pot îngrădi / indisponibiliza accesul utilizatorilor care vor să acceseze o pagină web compromisă. În cazul afectării unei pagini web aparținând unei instituții publice pot fi afectate atât demersurile de comunicare publică pentru gestionarea crizei COVID-19, cât și funcționalitatea acesteia, efectele putând fi resimțite la nivelul societății.

Cu toate că nu s-a observat o predilecție a atacatorilor cibernetici motivați ideologic pentru postarea unor mesaje conexe crizei COVID-19, aceștia derulează atacuri la adresa unor instituții guvernamentale cu rol critic în acest context, în special fiind vizat domeniul sănătății, pentru a-și promova propriile mesaje.

Pentru a diminua riscurile de securitate cibernetică asociate atacurilor de tip *web defacement*, recomandăm organizațiilor:

- Investigarea serverului web, în scopul identificării semnelor de compromitere și a accesărilor la nivelul acestuia.
- Actualizarea la ultima versiune a serverului și aplicațiilor web aferente domeniului și subdomeniilor afectate.
- Definirea unei politici de acces prin blocarea porturilor la nivelul serverelor specifice, cu excepția porturilor strict necesare (de exemplu: HTTP, HTTPS etc.).
- Realizarea zilnică de copii de siguranță (BACK-UP) pentru principalele sisteme din rețea care stochează date, dar și pentru serverele care găzduiesc domenii importante (în vederea restaurării facile în cazul unei compromiteri).
- Setarea, cel puțin în cazul conturilor cu rol de administrator al infrastructurii IT&C, a unor credențiale de acces cu un grad ridicat de securitate.

WORK FROM HOME

Foarte multe instituții publice și companii private au adoptat în această perioadă modelul *work from home*, accesarea de la distanță a rețelelor acestor entități devenind o necesitate pentru asigurarea respectării distanțării sociale. Astfel, prin eliminarea interacțiunilor dintre angajați a fost diminuat riscul răspândirii excesive a virusului SARS-CoV2, însă a crescut riscul expunerii infrastructurilor IT&C folosite la atacuri cibernetice.

Work from home presupune conectarea de la distanță la rețele în cadrul cărora sunt vehiculate informații de la nivelul instituțiilor și companiilor private care au implementat acest model de lucru. Astfel, în cadrul entităților care au stabilit măsuri și proceduri care să le permită angajaților să își poată exercita atribuțiile de serviciu de la distanță este recomandată implementarea unor politici de securitate adaptate pentru menținerea unui nivel optim al securității cibernetice și diminuarea riscurilor generate de incidentele de securitate cibernetică.

Recomandări privind infrastructurile și sistemele IT&C în contextul adoptării modelului work from home:

- Administrarea rețelei să nu fie realizată de la distanță, fiind astfel evitat riscul compromiterii infrastructurii IT.
- Accesarea rețelei prin utilizarea exclusivă a unor conexiuni securizate prin soluții de tip Virtual Private Network (VPN).
- Accesarea serviciilor din rețea (remote desktop, e-mail, servere de fișiere etc.) doar după conectarea prin intermediul VPN-ului, fiind evitată astfel expunerea în Internet a acestora.
- Crearea de politici de securitate în echipamentele de tip *firewall*, astfel încât utilizatorii care se conectează prin VPN la rețea să aibă acces doar la resursele și serviciile necesare desfășurării activității.
- Separarea utilizatorilor la nivelul logic al rețelei și al resurselor disponibile, în funcție de necesități și de specificul activităților și al departamentelor.
- Utilizarea unor zone tampon care conțin doar datele necesare desfășurării activității și neaccesarea de la distanță a *share-urilor* de fișiere existente anterior în rețea.
- Utilizarea exclusivă a sistemelor informatice deținute de organizație pentru accesarea rețelei acesteia, folosind dispozitive precum laptopul de serviciu. Este absolut necesar ca sistemele în cauză să dețină *antivirus* și *firewall* activat, iar software-ul instalat să fie actualizat la zi.
- Jurnalizarea tuturor activităților utilizatorilor care se conectează de la distanță.

Recomandările nu elimină complet posibilitatea apariției unor atacuri cibernetice, acestea fiind doar măsuri care reduc riscurile generate de implementarea modelului *work from home* la nivelul instituțiilor publice sau companiilor private.

INFORMAREA DIN SURSE OFICIALE

Atât la nivelul instituțiilor abilitate să gestioneze criza generată de COVID-19, cât mai ales la nivelul populației, **este recomandată doar informarea din surse oficiale**.

Pe de o parte, fenomenul *fake-news* s-a intensificat în perioada pandemiei de COVID-19, pe fondul necunoscutelor privind apariția, răspândirea, tratarea și combaterea virusului SARS-CoV2. Multitudinea de opinii neavizate din mediul Internet generează o intoxicare cu informații false, care poate crea panică și conduce la luarea unor decizii bazate pe informații eronate, diminuând semnificativ efectele vizate de măsurile impuse de autorități.

Pe de altă parte, distribuirea pe scară largă a unor atașamente/link-uri provenite din surse neoficiale crește riscul expunerii utilizatorilor la atacurile cibernetice care folosesc tehnici de inginerie socială.

În contextul necesității asigurării unui flux ridicat de furnizare a informațiilor pe tema crizei epidemiologice, este necesar ca platformele web create și utilizate în acest scop să respecte un set minim de recomandări de securitate cibernetică, precum:

- Asigurarea unei capabilități de gestionare a unui volum mare de cereri.
- Folosirea unei conexiuni criptate.
- Utilizarea parolelor cu o complexitate ridicată în cadrul tuturor serviciilor (autentificare, bază de date, server etc.).
- Actualizarea permanentă a modulelor/plugin-urilor utilizate, doar din surse oficiale.
- Asigurarea protecției împotriva atacurilor de tip Distributed Denial of Service (DDoS).


ROMANIA
SRI
Patria a priori
SERVICIUL ROMAN DE INFORMATII
www.sri.ro