Anexă la nr. 78184 din 04.12.2024 -STRICT SECRET-

~~Anexa la nr. 00784853 din 02.12.2024~~

NOTĂ

I. Acțiuni ale unui actor cibernetic statal asupra infrastructurilor IT&C suport pentru procesul electoral, găzduite de Autoritatea Electorală Permanentă (AEP) și Serviciul de Telecomunicații Speciale (STS).

Prin metode specifice, în data de 24.11.2024, SRI a obținut date cu privire la publicarea unor **credențiale de acces asociate *„bec.ro”*, *„roaep.ro”* și *„registrulelectoral.ro”*** în cadrul unor platforme de criminalitate cibernetică de sorginte rusă, date similare fiind identificate și în cadrul unui canal privat de Telegram recunoscut pentru diseminarea de date exfiltrate din foarte multe state, mai puțin Federația Rusă.

În urma verificărilor demarate s-a stabilit că exfiltrarea s-a realizat fie prin targetarea utilizatorilor legitimi către care au fost distribuite credențialele de tip utilizator/parola, fie prin exploatarea serverului legitim de instruire pus la dispoziție de către STS la adresa ***https://operatorsectie.roaep.ro***.

> Referitor la topologia infrastructurii, STS gestionează secvența principală aferentă procesului de votare: înregistrarea prezenței la vot, asigurarea corectitudinii numărării buletinelor de vot prin înregistrarea video a procesului de deschidere a urnelor și numărarea voturilor și centralizarea rezultatelor.
>
> Secvența de infrastructură gestionată de AEP deservește: afișarea în timp real a prezenței la vot, statistici referitoare distribuția votului pe diverse criterii (categorii, de vârstă, sex, mediu urban/rural etc.), precum și punerea la dispozitie a legislației electorale.

Aceste postări au fost efectuate după ce în data de 19.11.2024, un incident cibernetic a targetat și a afectat infrastructura IT&C a AEP, în urma căruia atacatori cibernetici au compromis un server de hărți (***gis.registrulelectoral.ro***), conectat atât în exterior, la internet, cât și la rețeaua internă a AEP.

În context, a fost identificat **un număr ridicat de atacuri cibernetice[1] (peste 85.000)**, care au vizat exploatarea vulnerabilităților existente la nivelul sistemelor informatice de suport pentru procesul electoral, în vederea **obținerii accesului la**

[1] *De tip*
- SQL Injection (SQLi) – Atac care presupune injectarea de cod malware de tip SQL într-o aplicație pentru a accesa și/sau modifica baza de date din spatele acesteia;
- Cross Site Scripting (XSS) - Atac care exploatează o vulnerabilitate ce se regăsește într-o pagină web și care permite unui atacator să introducă linii de cod în paginile web vizitate de alți utilizatori (victime), în scopul obținerii de date cu acces restricționat

datele din sistemele informatice, alterării integrității acestora, schimbării conținutului prezentat publicului larg și indisponibilizării infrastructurii.

Centrul Național Cyberint a derulat evaluări tehnice asupra sistemelor informatice conexe prin **analizarea fișierelor de jurnalizare aferente intervalului 20-26.11.2024**, generate de echipamentele de securitate cibernetică utilizate de:

- *prezenta.roaep.ro* – platformă de monitorizare și afișare statistici privind prezenta la vot;
- *voting.roaep.ro* – platformă cu tranzacții blockchain;
- *prezidentiale1-sicpv.bec.ro* – sistem informatic de centralizare al proceselor verbale;
- *simpv.bec.ro* – sistem informatic de monitorizare a prezenței la vot;
- *simpv.roaep.ro* – sistem informatic de monitorizare a prezenței la vot;
- *simpv.stsnet.ro* – sistem informatic de monitorizare a prezenței la vot.

Atacurile în cauză au continuat **într-un mod susținut, inclusiv în ziua alegerilor și în noaptea post alegeri (25.11.2024)**. Pentru lansarea atacurilor au fost utilizate **sisteme informatice din peste 33 de țări**, folosind metode de anonimizare avansate pentru a îngreuna procesul de atribuire.

Menționăm că au fost demarate investigații specifice împreună cu AEP și STS. Întrucât **evaluarea cu privire la atacul cibernetic este în derulare**, în prezent nu deținem date certe cu privire la atacator ori cu privire la afectarea procesului electoral.

Modul de operare, precum și amploarea campaniei cibernetice conduc la concluzia că atacatorul dispune de resurse considerabile, **corelate cu un mod de operare specific unui atacator statal**. Totodată, infrastructura AEP rămâne afectată încă de vulnerabilități care, în măsura în care sunt exploatate de către atacatori, aceștia pot realiza acțiuni de escaladare a accesului în cadrul rețelei și asigurarea persistenței.

II. În contextul aspectelor vehiculate în mediul online, au fost obținute date care au relevat faptul că motivul creșterii masive în ritm accelerat a popularității lui **Călin GEORGESCU** la nivelul platformei sociale TikTok se datorează unei campanii de promovare foarte bine organizată.

Călin GEORGESCU a beneficiat de un tratament preferențial la nivelul platformei TikTok, deoarece conținutul postat de acesta **nu a fost marcat ca aparținând unui candidat**, aspect ce a favorizat diseminarea în masă, videoclipurile publicate nefiind asociate oficial cu campania electorală.

În consecință, **vizibilitatea acestuia a crescut preferențial în raport cu ceilalți candidați, ale căror postări au fost filtrate masiv, diminuând exponențial prezența acestora în online.**

Acest tratament preferențial a fost potențat de nerespectarea de către TikTok a Deciziei Biroului Electoral Central (BEC) nr.175D din 20.11.2024 prin care, la art.3,

dispunea "înlăturarea materialelor de propagandă electorală din mediul online ce îl ilustrează pe candidatul Călin Georgescu la alegerile pentru Președintele României din anul 2024, care nu conțin codul de identificare al mandatarului fiscal".

Solicitarea a fost transmisă către TikTok, prin intermediul AEP, în data de 21.11.2024 ora 08:00. Ulterior la cererea TikTok s-a făcut revenire cu codul CMF, care în urma analizei făcute de AEP nu se regăsea în nicio postare a candidatului.

În 22.11.2024, ora 13:47, TikTok a transmis AEP confirmarea eliminării postărilor care fac obiectul Deciziei BEC nr.175D din 20.11.2024, prin blocarea accesului vizual la acestea de pe teritoriul României, **ele rămânând vizibile în alte state și putând fi distribuite**.

De asemenea, conform informațiilor obținute la nivelul TikTok a fost realizată o analiză cu privire la activitățile online subsumate campaniei de promovare a lui Călin GEORGESCU.

Prima sesizare a TikTok cu privire la faptul că se desfășoară o campanie de promovare a lui Călin Georgescu a avut loc în 2020, iar, în anul 2021, a fost raportat de aceștia (cel mai probabil către conducerea TIK TOK) ca fiind o activitate suspectă.

Concluziile analizei actuale relevă următoarele:

- au fost identificate canale de Telegram și Discord unde se discută cum să se coordoneze și sa evite blocarea pe platformă, astfel că nu s a identificat o legătură directă între multiplele conturi de TikTok utilizate în promovarea lui Călin Georgescu, dat fiind că activitatea era desfășurată din geolocații multiple;
- **activitatea conturilor ar fi fost coordonată de către un actor statal**, care ar fi utilizat un canal alternativ de comunicare pentru „rostogolirea" mesajelor pe platformă;
- nu folosește ferme de boți pe platformă, ci operează mai discret din afară, ca să nu încalce politicile de utilizare a platformei;
- cei implicați în campania de promovare a celui în cauză dovedesc o cunoaștere foarte bună a politicilor de securitate ale TikTok, având și know-how-ul necesar pentru eludarea acestora;
- în spate este **o firmă foarte bună de digital marketing**;
- conturile care l-au promovat pe Călin Georgescu pe TikTok au diseminat mesaje identice, fără să existe coordonare pe platformă (nu au fost decelate amprente digitale care să conecteze dispozitivele utilizate).

Creșterea conturilor **nu a fost organică** (similară unor evenimente virale natural), astfel că TikTok apreciază că, practic, sunt **voluntari coordonați**

(„**mass guerilla political campaign**" sau „**forță brută de atac în cybersecurity**").

- diseminarea mesajelor în cadrul platformei TikTok s-a realizat în roiuri (*swarming*).

De asemenea, în ultimele zile, TikTok a mai identificat o activitate de promovare masivă, derulată în ultimele două săptămâni, pentru susținerea POT (Partidul Oamenilor Tineri), partid suveranist, înființat în anul 2023, care îl susține pe Călin GEORGESCU.