Anexa la nr. 784184 din 04.12.2024 ~~STRICT SECRET~~

~~Anexa la nr. 00784853 din 02.12.2024~~

ROMANIA
AOM|MSTRAŢIA FDE?DEN)Ht
sEcREz'Ri4zuL cwsiJ.iuLui suPxcu
oc zPzeAeE zŢzRit
INTRARE IEŞIRE Nr. 2SN/1743
Ziua 04 Luna 12 Anul 2024

NOTA

I. **Azioni di un cyber attore** statale sulle infrastrutture IT&C a supporto del processo elettorale, ospitate dall'Autorità elettorale permanente (AEP) e dal Servizio speciale di telecomunicazioni (STS).

Utilizzando metodi specifici, in data 24.11.2024, SRI ha ottenuto i dati relativi alla pubblicazione delle **credenziali di** accesso associate a "Cec.ro", *"roaeP.ro"* e *"registrulelectoral.ro"* su piattaforme di criminalità informatica con base in Russia, con dati simili identificati su un canale Telegram privato riconosciuto per la diffusione di dati esfiltrati da molti Paesi, tranne la Federazione Russa.

In seguito alle verifiche, è stato stabilito che l'esfiltrazione è stata effettuata sia prendendo di mira gli utenti legittimi a cui sono state distribuite le credenziali di utente/password, sia sfruttando il server di formazione legittimo fornito dall'STS all'indirizzo *https-/1-fi'eratorsectie.roaefi'.ro.*

Per quanto riguarda la topologia dell'infrastruttura, il STS gestisce la sequenza principale del processo di voto: registrazione dell'affluenza, garanzia della correttezza del conteggio delle schede attraverso la videoregistrazione dell'apertura delle urne, conteggio dei voti e centralizzazione dei risultati.

La sequenza di infrastrutture gestita da AEP serve: visualizzazione in tempo reale dell'affluenza alle urne, statistiche sulla distribuzione del voto in base a vari criteri (categorie, età, sesso, urbano/rurale, ecc.), nonché la disponibilità della legislazione elettorale.

Questi messaggi sono stati emessi dopo che, il 19.11.2024, un incidente informatico ha preso di mira e colpito l'infrastruttura IT&C di AEP, a seguito del quale gli aggressori informatici hanno compromesso un server di mappe *(zis.registrulelectoraL.ro),* collegato sia all'esterno (a Internet) sia alla rete interna di AEP.

In questo contesto, è stato identificato un elevato numero di **"attacchi informatici"** (più di 85.000), che miravano a sfruttare le vulnerabilità dei sistemi informatici a supporto del processo elettorale per ottenere l'accesso a

---

Tipo.
- SQL Injection (SQLi) - Un attacco che prevede l'iniezione di codice SQL dannoso in un'*applicazione per accedere* e/o *modificare* il database *sottostante*;
- Cross Site Scripting (XSS) - Un attacco che sfrutta una vulnerabilità in una pagina web.
consente a un aggressore di inserire linee di codice nelle pagine web visualizzate da altri utenti (vittime), allo scopo *di di* lastre *ad accesso limitato.*

dati nei sistemi informativi, alterandone l' integrità, modificando il contenuto presentato al pubblico e rendendo l'infrastruttura non disponibile.

Il National Cyberint Centre ha effettuato valutazioni tecniche sui sistemi informativi correlati analizzando i file di log per il periodo 20-26.11.2024, generati dalle apparecchiature di cybersecurity utilizzate da:
- *prezenta.rooep.ro* - piattaforma per il monitoraggio e la visualizzazione delle statistiche sull'affluenza alle urne;
- *voting.roaep.ro* - piattaforma di transazioni della catena blocl:
- *prezidentialel-sicpv.bec.ro* - sistema informatico per la centralizzazione dei verbali;
- *simpv.bec.ro* - sistema computerizzato per il monitoraggio dell'affluenza alle urne;
- *simpv.roaep.ro* - sistema computerizzato per il monitoraggio dell'affluenza alle urne;
- simpv.stsnet.ro - sistema iriformatico per il monitoraggio dell'affluenza alle urne.

Questi attacchi sono continuati in modo prolungato, anche il giorno delle elezioni e la notte successiva (25 novembre 2024). Per sferrare gli attacchi sono stati utilizzati sistemi informatici di oltre 33 Paesi, utilizzando metodi avanzati di anonimizzazione per rendere più difficile il processo di attribuzione.

Sono state avviate indagini specifiche con l'AEP e l'STS. Poiché la valutazione dell'attacco informatico è in corso, al momento non disponiamo di dati certi sull'aggressore o sull'impatto sul processo elettorale.

Il modus operandi e la portata della campagna informatica portano a concludere che l'aggressore dispone di risorse considerevoli, unite a un modus operandi specifico di un aggressore statale. Allo stesso tempo, l'infrastruttura di CEPOL è ancora affetta da vulnerabilità che, se sfruttate dagli aggressori, possono aumentare l'accesso alla rete e la persistenza.

ll. Nel contesto delle questioni circolate nell'ambiente online, sono stati ottenuti dati che hanno rivelato che la ragione della crescita massiccia e accelerata della popolarità di cslin GEORGESCU sulla piattaforma sociale TikTok è dovuta a una campagna promozionale molto ben organizzata.

Călin GEORGESCU ha beneficiato di un trattamento preferenziale sulla piattaforma TikTok perché i contenuti da lui postati non erano contrassegnati come appartenenti a un candidato, il che ha favorito la diffusione di massa, in quanto i video pubblicati non erano ufficialmente associati alla campagna elettorale.

Di conseguenza, la sua visibilità è aumentata in modo preferenziale rispetto agli altri candidati, i cui post sono stati massicciamente filtrati, diminuendo esponenzialmente la loro presenza online.

Questo trattamento preferenziale è stato rafforzato dal mancato rispetto da parte di TikTok della decisione dell'Ufficio elettorale centrale (BEC) n. 175D del 20.11.2024 che, all'art. 3

ha ordinato la rimozione del materiale di propaganda elettorale online che illustra il candidato Călin Georgescu alle elezioni del 2024 per la presidenza della Romania, che non contiene il codice di identificazione dell'agente fiscale autorizzato".

La richiesta è stata inviata a TikTok, tramite l'AEP, in data 21.1 1.2024 alle 08:00. Successivamente, su richiesta di TikTok, è stato restituito il codice CMF, che dopo l'analisi di AEP non è stato trovato in nessuno dei post del candidato.

Il 22.1.2024, alle 13:47, TikTok ha inviato ad AEP la conferma della rimozione dei post soggetti alla decisione BEC n. J75D del 20.1.2024, bloccando l'accesso visivo ad essi dalla Romania, mentre **rimangono visibili in altri Paesi e possono** essere **distribuiti.**

Inoltre, in base alle informazioni ottenute a livello di TikTok, è stata effettuata un'analisi delle attività online che rientrano nella campagna promozionale di Călin GEORGESCU.

La prima segnalazione di TikTok di una campagna di promozione di Călin Georgescu è avvenuta nel 2020 e nel 2021 è stata segnalata da loro (molto probabilmente alla direzione di TIK TOK) come attività sospetta.

Le conclusioni dell'analisi attuale sono le seguenti:

- Sono stati individuati canali Telegram e Discord in cui si discuteva di come coordinarsi ed evitare il blocco sulla piattaforma, quindi non è stato individuato un collegamento diretto tra i molteplici account TikTok utilizzati per la promozione di Călin Georgescu, dato che l'attività è stata svolta da più geolocalizzazioni;
- L'attività degli account sarebbe stata coordinata da un attore statale, che avrebbe utilizzato un canale di comunicazione alternativo per "rollare" i messaggi sulla piattaforma;
- non utilizza bot farm sulla piattaforma, ma opera in modo più discreto dall'esterno, per non violare le politiche di utilizzo della piattaforma;
- coloro che sono coinvolti nella campagna di promozione di quello in questione hanno un'ottima conoscenza delle politiche di sicurezza di TikTok e il know-how per aggirarle;
- è un'ottima azienda di marketing digitale;
- gli account che hanno promosso Călin Georgescu su TikTok hanno diffuso messaggi identici, senza alcun coordinamento sulla piattaforma (non sono state rilevate impronte digitali per collegare i dispositivi utilizzati).

L'aumento dei conti non è stato organico (come per alcuni dei suoi eventi TikTok Pratica, volontariato r ti naturale), in modo da apprezzare che, sunt co

("guerriglia di massa guerriglia politica"). campagna" o "forza bruta di attacco in sicurezza informatica").

- la diffusione dei messaggi all'interno della piattaforma TikTok è avvenuta in sciami *(sciamatura).*

Inoltre, negli ultimi giorni, TikTok ha individuato una massiccia attività promozionale, svolta nelle ultime due settimane, a sostegno del POT (Partito dei Giovani), un partito sovranista, fondato nel 2023, che sostiene Călin GEORGESCU.