TINEXTA CYBER

Come le Fake News influenzano le elezioni

SOMMARIO

Executive Summary

Il mondo delle fake news sta evolvendo in modi significativi, passando dalle fake news prodotte da attori statali a fake news meno convenzionali come i meme, i troll, o più in generale contenuti diffusi dagli utenti sui social network. Questa trasformazione è influenzata dalla crescente disponibilità di strumenti, come l'intelligenza artificiale, che facilitano la creazione e la propagazione di contenuti falsi. Le fake news s*tate sponsored* tendono a essere realizzate con una tecnica più sofisticata e pianificata attraverso la manipolazione delle informazioni e la loro disseminazione mirata mediante campagne di disinformazione ben studiate. Sembrerebbe, infatti, che la disinformazione nasca da paesi esterni (Russia/Cina) e non attacca un partito, ma il governo che è a favore dell'Ucraina. Queste operazioni richiedono risorse finanziarie e tecniche avanzate per creare un impatto strategico. D'altro canto, le fake news ad alto livello sono spesso create utilizzando le nuove tecnologie accessibili a chiunque. L'uso di strumenti semplici come app di editing di immagini e video, combinato con la viralità dei social media, consente a chiunque di creare e condividere contenuti falsi con facilità. Questo cambiamento è anche legato al fatto che, in un mondo sempre più interconnesso, le fake news possono diffondersi rapidamente e ampiamente, influenzando l'opinione pubblica in modo significativo. Inoltre, la tecnologia AI può essere utilizzata per creare deepfake, video e audio manipolati in modo convincente, che possono essere particolarmente dannosi in quanto possono essere difficili da individuare come falsi: in questo contesto, c'è da considerare infatti il fattore tempo. Il fattore tempo gioca un ruolo critico nell'influenzare l'impatto delle fake news durante le elezioni: se una fake news emerge proprio nel periodo delle elezioni, può avere un impatto significativo poiché c'è poco tempo per verificare la sua veridicità. Questo a sua volta influenza diversi fattori, quali:

- **la velocità di diffusione**: se una fake news emerge poco prima delle elezioni, c'è meno tempo per contrastare la sua diffusione. In questo modo, può raggiungere un pubblico più ampio prima che possano essere fornite informazioni accurate per smentirla.
- **Influenza sull'elettorato**: l'immediatezza delle notizie durante le elezioni può portare le persone a prendere decisioni basate su informazioni false o fuorvianti.
- **manovre strategiche**: alcuni attori potrebbero deliberatamente diffondere fake news durante le elezioni per influenzare i risultati. Se queste notizie sono diffuse poco prima del voto, possono avere un impatto diretto sulle decisioni degli elettori senza che ci sia abbastanza tempo per una reazione efficace.
- **difficoltà nella correzione**: anche se una notizia viene successivamente confermata come falsa, l'impatto iniziale potrebbe già aver avuto un effetto sul risultato delle elezioni. Inoltre, durante le elezioni, c'è spesso un aumento dell'attenzione mediatica e dell'interesse pubblico, il che significa che le fake news possono ottenere maggiore visibilità e circolazione in un breve periodo di tempo.

Strumenti e Obiettivi della disinformazione

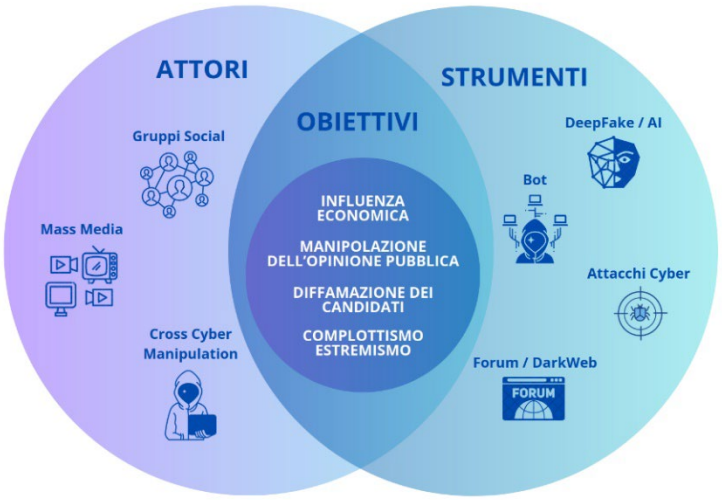
Nel corso delle elezioni degli ultimi anni è infatti diventato sempre più importante e critico l'aspetto delle fake news, ovvero false informazioni relative a nazioni, canditati e scandali atti a promuovere o demolire la reputazione dei candidati.

Gli obiettivi principali per la diffusione di fake news sono, ad esempio:

1) Influenza economica
2) Manipolazione dell'opinione pubblica
3) Diffamazione dei candidati
4) Complottismo/Estremismo

Gli strumenti utilizzati per raggiungere questi obiettivi sono:

1) DeepFake / AI
2) Gruppi Social
3) Forum Underground
4) Furti d'identità
5) Cross Cyber Manipulation
6) Mass Media
7) Bot



Gli strumenti

Nel contesto delle elezioni del 2024, l'emergenza relativa al proliferare delle fake news ha assunto un ruolo cruciale e sempre più preoccupante. Queste false informazioni, progettate per influenzare l'opinione pubblica e alterare il processo democratico, si sono diffuse a un ritmo allarmante. Le elezioni non sono solo una sfida per determinare il futuro di una nazione, ma anche un terreno fertile per la manipolazione e la diffusione di informazioni ingannevoli. Per raggiungere i loro obiettivi, coloro che diffondono fake news sfruttano una serie di strumenti sofisticati e tecniche ingannevoli, tra questi spiccano l'utilizzo di DeepFake / AI, i Gruppi Social, profili Bot e la diffusione di informazioni su Forum Underground e Mass Media.

Deepfake / AI

Con l'avvento dell'intelligenza artificiale (AI), la produzione e la diffusione delle fake news diventano ancora più facili e pericolose, in quanto l'AI può generare testi, immagini, video o audio falsi ma credibili, con una velocità e una numerosità senza precedenti. Questo fenomeno può avere gravi conseguenze per il contesto delle nuove elezioni, in cui i cittadini devono essere informati e consapevoli delle proposte e dei programmi dei candidati, senza essere manipolati o ingannati da informazioni false o tendenziose. Per contrastare le fake news, è necessario sviluppare strumenti di verifica e di fact-checking basati sull'AI, ma anche educare i cittadini a essere critici e responsabili nel consumo e nella condivisione delle informazioni.

Gruppi social

I gruppi social possono svolgere un ruolo significativo nell'influenzare le elezioni diffondendo rapidamente informazioni false o fuorvianti. Questi gruppi possono essere utilizzati per creare e diffondere narrazioni distorte o complottistiche su candidati o questioni politiche. Inoltre, possono agire come *echo chambers* ("camere dell'eco"), dove le persone vengono esposte solo a una prospettiva unilaterale, rinforzando le loro convinzioni esistenti e influenzando le loro decisioni di voto.

Forum underground

Essendo spazi digitali poco regolamentati, i forum underground facilitano la diffusione di data leak e informazioni personali come, ad esempio, liste di votanti così da poter avere informazioni utili per attacchi di disinformazione mirata, che possono influenzare l'opinione pubblica e distorcere il dibattito politico.
Gli utenti possono operare in modo anonimo, rendendo difficile tracciare l'origine della disinformazione o delle attività illecite. Questo anonimato favorisce la diffusione di contenuti dannosi, la coordinazione di attività illegali finalizzate a influenzare il processo elettorale, come la diffusione di malware o il tentativo di sabotaggio delle elezioni.

Furti d'identità

Nel contesto elettorale, la diffusione di malware InfoStealer può influenzare le elezioni in diversi modi. Il furto di informazioni sensibili come password e dati personali può compromettere la sicurezza delle comunicazioni tra candidati, partiti politici ed elettori. Questo potrebbe portare alla manipolazione delle informazioni, al sabotaggio delle campagne elettorali e alla diffusione di notizie false o compromettenti. Inoltre, il furto di identità e la perdita di dati possono minare la fiducia del pubblico nel processo elettorale, compromettendo così l'integrità delle elezioni.

Cross cyber manipulation

Con il termine "Cross Cyber Manipulation" si indicano tattiche sofisticate che coinvolgono l'interconnessione di più operatori cibernetici per influenzare le elezioni. Questo fenomeno si è manifestato in varie forme:
un nuovo filone sta infatti emergendo nell'ambito della manipolazione dell'opinione pubblica, caratterizzato dall'utilizzo di strumenti sofisticati per creare tensione e insicurezza. Questo approccio si basa sull'uso avanzato della tecnologia e delle strategie di comunicazione per influenzare le percezioni e le opinioni del pubblico. Gli attacchi informatici mirati vengono utilizzati per compromettere le infrastrutture critiche, diffondere virus informatici e rubare informazioni sensibili al fine di creare caos e instabilità. Questi attacchi possono essere perpetrati da attori statali o non statali con l'obiettivo di influenzare l'opinione pubblica e minare la fiducia nelle istituzioni democratiche. Attacchi distribuiti di denial of service (DDOS) perpetrati da gruppi di hacktivisti possono essere utilizzati per sovraccaricare i siti web delle autorità elettorali o dei partiti politici, rendendoli inaccessibili agli elettori o compromettendo la trasmissione di informazioni cruciali.

MASS media

I fake exit polls sono sondaggi realizzati nel periodo delle elezioni che possono influenzare l'opinione pubblica nel suo complesso, spingendo gli elettori a seguire presunte tendenze di voto. Questo può portare a un effetto di "*bandwagon*" (“carrozzone”) o "*underdog*" (“perdente”) e influenzare la copertura mediatica delle elezioni. Entrambi questi effetti possono essere influenzati dalla percezione pubblica dei sondaggi di opinione e dei risultati elettorali. I fake exit polls, se diffusi in modo tale da far sembrare un candidato o un partito in vantaggio o in svantaggio, possono amplificare questi effetti e influenzare il comportamento degli elettori. Inoltre, quando diversi siti web o piattaforme di social media condividono o riproducono la stessa notizia falsa, questa può sembrare più credibile agli occhi degli utenti, poiché viene presentata da fonti diverse, anche se tutte non attendibili. Questo fenomeno può amplificare l'effetto delle fake news, contribuendo a diffondere disinformazione su larga scala.

Profili bot

I profili bot sui social media possono essere programmati per diffondere messaggi politici o disinformazione in modo automatizzato e massivo. Possono essere utilizzati per amplificare contenuti favorevoli o sfavorevoli a determinati candidati, manipolare trending topics e influenzare il dibattito online. Poiché i bot possono operare in modo anonimo e veloce, possono avere un impatto significativo sull'opinione pubblica, rendendo difficile distinguere tra conversazioni genuine e manipolate.

L'utilizzo dei bot durante le elezioni è stato evidenziato da Meta, che ha individuato una rete di quasi 4.800 account falsi creati in Cina per sembrare appartenere a utenti americani, con foto, nomi e localizzazioni falsi. Invece di diffondere contenuti falsi, gli account ritrasmettevano post da X (precedentemente noto come Twitter), creati da politici, media e altri, sia liberali che conservatori. L'obiettivo sembrava essere quello di esacerbare le divisioni partigiane e alimentare la polarizzazione. Per sembrare autentici, gli account a volte pubblicavano contenuti su moda o animali domestici. Alcuni account hanno anche cambiato improvvisamente nome e foto profilo, suggerendo una residenza in India, iniziando a diffondere contenuti pro-cinesi su Tibet e India.

Meta non ha collegato pubblicamente questa rete cinese al governo cinese, ma ha rilevato che il contenuto diffuso dagli account è in linea con la propaganda e la disinformazione del governo cinese, mirata a gonfiare le divisioni partigiane negli Stati Uniti.

Gli account sono stati utilizzati per condividere i post di X creati da politici, organi di informazione e altri e hanno attinto contenuti da fonti sia liberali che conservatrici, un'indicazione del fatto che

l'obiettivo non era quello di sostenere una parte o l'altra, ma di esasperare le divisioni partitiche e infiammare ulteriormente la polarizzazione.

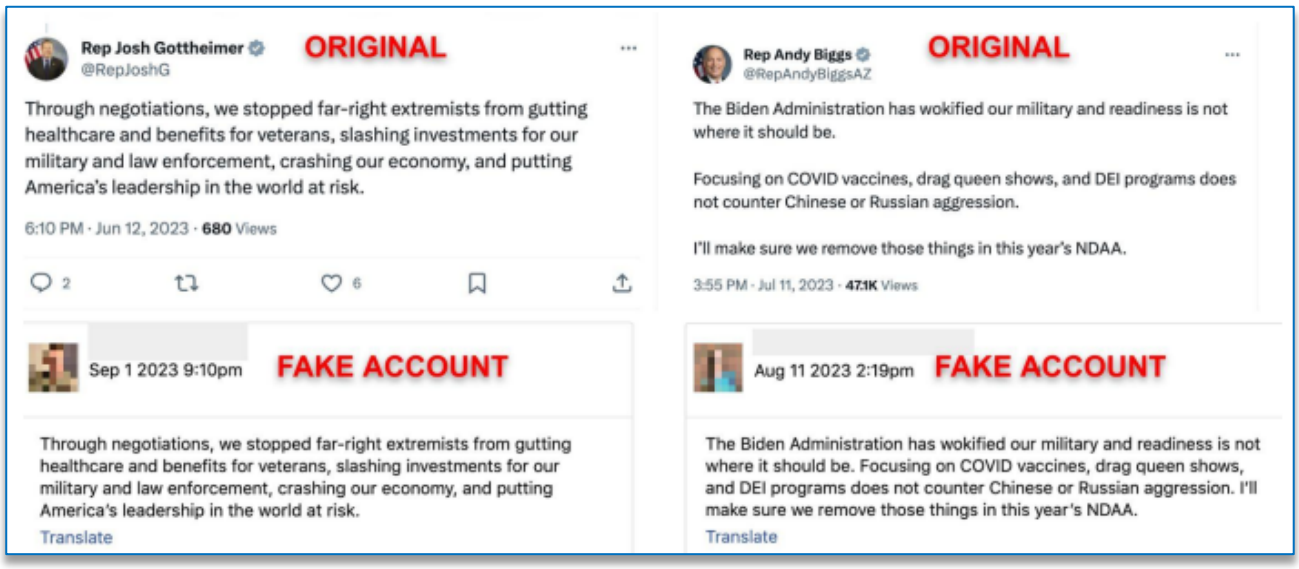
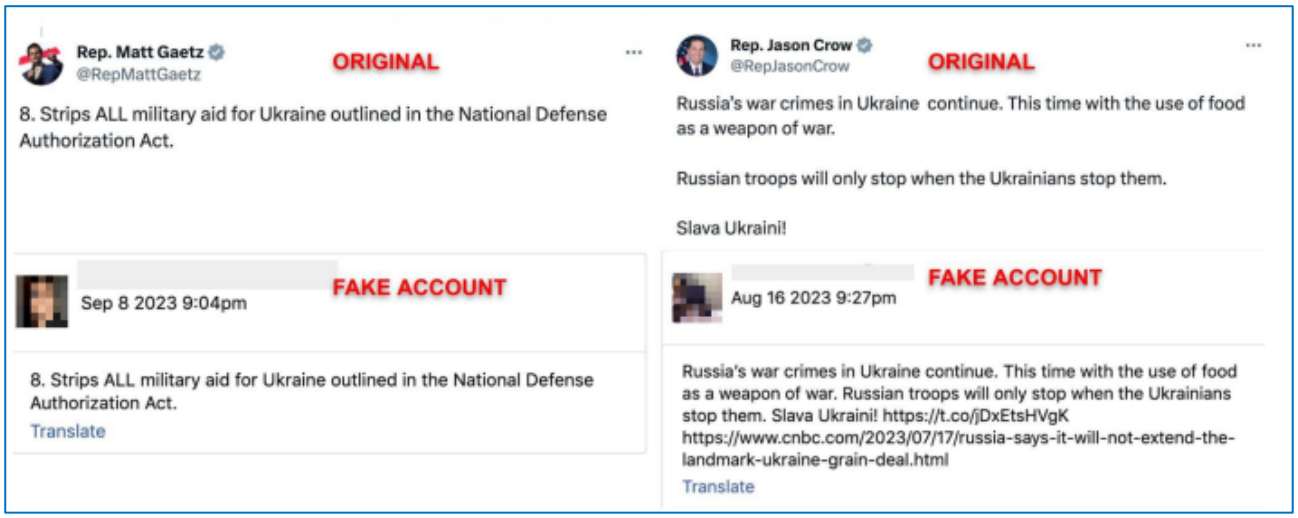
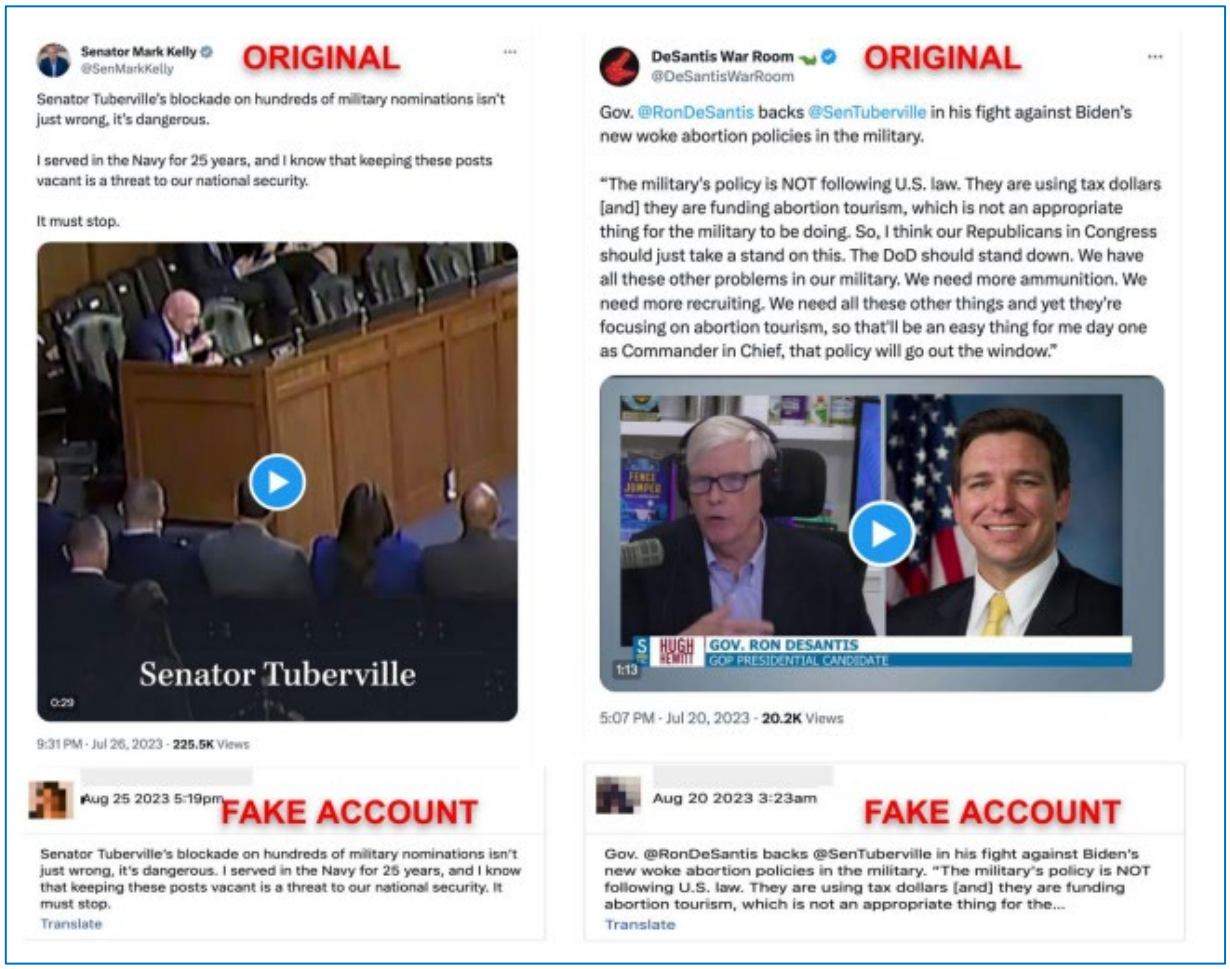


***Figura 1**:in alto i tweet dei rappresentanti Josh Gottheimer (D) e Andy Biggs (S). In basso i post su Facebook della rete di origine cinese, che copia/incolla i tweet di questi rappresentanti eletti. Da: Facebook*

Altri esempi:





Inoltre, un post su X ha guadagnato grande visibilità quando Alex Jones, noto per diffondere teorie del complotto, l'ha condiviso con i suoi 2,2 milioni di follower. L'account, con riferimento a "MAGA 2024", di provenienza cinese, ha diffuso un video della tv russa RT secondo il quale Biden e la Cia avrebbero mandato un gangster neonazista a combattere in Ucraina.

Altri quattro account simili con legami cinesi sono stati individuati, uno dei quali ha pagato per una sottoscrizione su una piattaforma che offre una spunta blu di verifica. Tutti condividevano contenuti pro-Trump e anti-Biden, inclusa la teoria QAnon e accuse di frode elettorale senza fondamento. Inoltre, hanno attaccato gli sforzi americani per vietare TikTok, considerandoli un "vero autoritarismo" orchestrato da Israele per danneggiare la Cina. Questi account spesso hanno amplificato contenuti dalla campagna di influenza cinese Spamouflage, iniziata nel 2019 e legata al Ministero della Pubblica Sicurezza cinese, un'operazione di influenza in corso e pluriennale che promuove gli interessi di Pechino. L'anno scorso, la società madre di Facebook, Meta, ha rimosso 7.704 account e 954 pagine identificate come parte dell'operazione Spamouflage, che ha descritto come "la più

grande operazione di influenza multipiattaforma conosciuta che [Meta] ha interrotto fino ad oggi". Spamouflage è attivo principalmente su X, ma anche su YouTube, Facebook, TikTok, Medium e altri forum, siti Web e piattaforme di social media. I termini di servizio di Facebook vietano una serie di comportamenti ingannevoli e non autentici, compresi i tentativi di nascondere lo scopo dell'attività sui social media o l'identità di coloro che ne sono responsabili.

L'ISD ha identificato quattro account collegati a Spamouflage che si spacciano, in modo convincente, come sostenitori di Donald Trump e del movimento MAGA, e un quinto che si spaccia per greco ma si occupa di argomenti politici americani. Sebbene tutti abbiano pubblicato quantità significative di contenuti e narrazioni di Spamouflage a sostegno del Partito Comunista Cinese, non vengono potenziati artificialmente dal resto della rete Spamouflage.

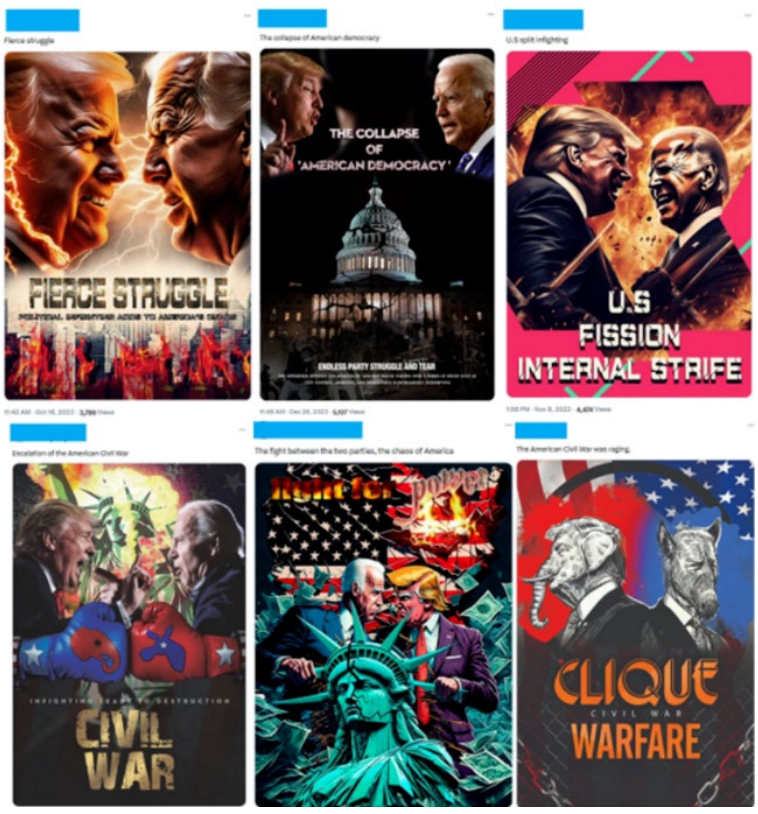
Stanno invece costruendo un autentico pubblico pro-Trump, anche attraverso la comunità MAGA " follow trains" in cui gli utenti dei social media accettano di seguirsi a vicenda e quindi aumentare il numero di follower reciproci. Hanno anche postato chiedendo più follower, ricevendo centinaia di likes.

Da gennaio 2024, i contenuti riguardanti le elezioni di Spamouflage si concentrano esclusivamente su Joe Biden e Donald Trump come i principali contendenti presidenziali. La ricerca condotta dall'ISD non ha individuato alcun contenuto che riguardi altri candidati repubblicani o eventuali sfidanti democratici al presidente Biden.

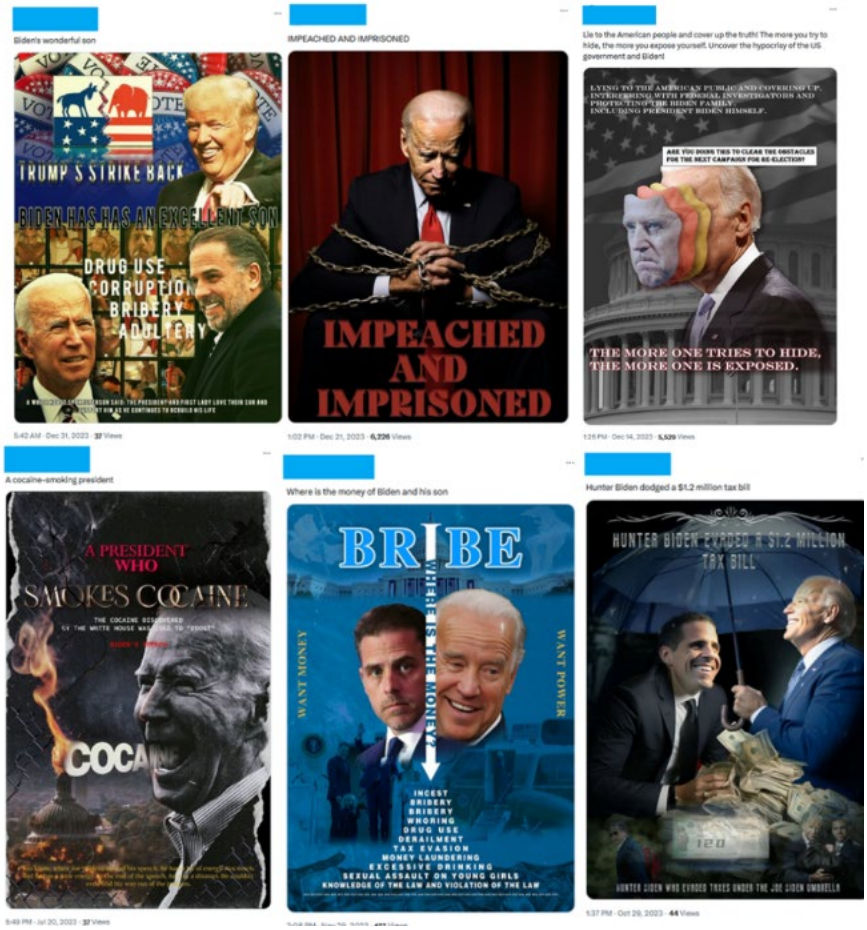
Tuttavia, la maggior parte dei contenuti sembra focalizzarsi su creare un senso di sconcerto riguardo allo stato attuale dell'America, senza una chiara inclinazione politica. Si affrontano temi come il degrado urbano, la crisi dell'oppio, l'inquinamento dell'acqua, la brutalità della polizia, la violenza armata e le infrastrutture in cattive condizioni. Sebbene non siano direttamente collegati alle elezioni, questi contenuti contribuiscono a generare insoddisfazione tra gli elettori riguardo allo stato del paese, oltre a potenzialmente alimentare un senso di caos negli Stati Uniti.

Le narrazioni principali includono:

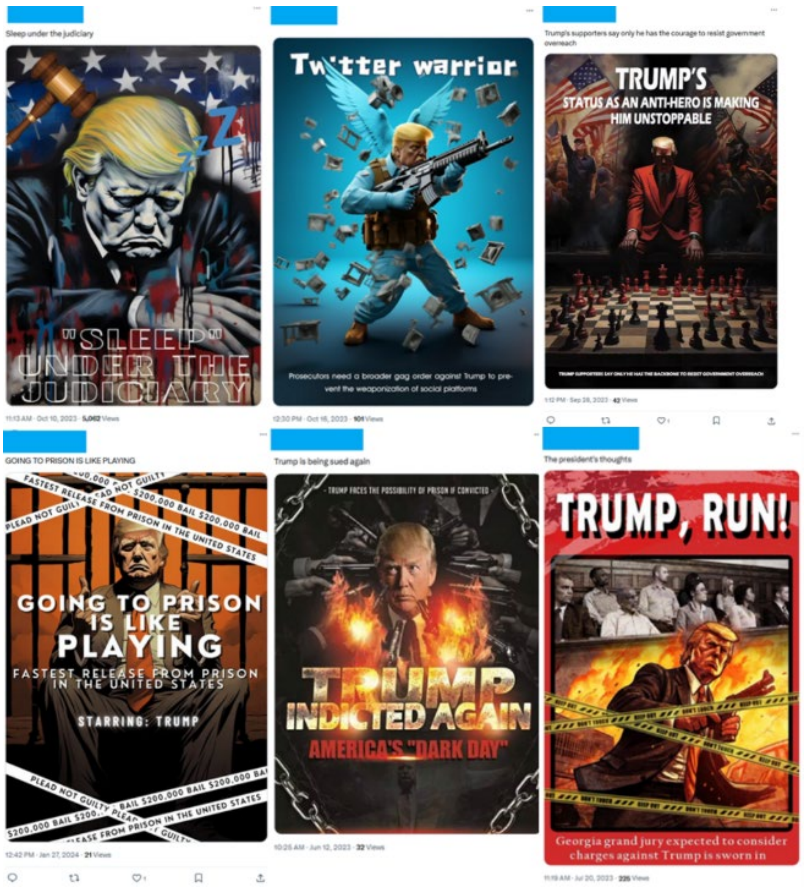
Creazione di divisioni e danni per l'America: L'intento sembra essere quello di descrivere le elezioni come fonte di divisione e conflitto, peggiorando i problemi esistenti negli Stati Uniti. Le immagini associate a questa narrazione spesso ritraggono Trump e Biden in faccia a faccia.



Narrazioni negative su Biden: oltre a dipingere le elezioni come divisive, le narrazioni negative sul presidente Biden sembrano essere l'altro obiettivo più significativo degli sforzi di Spamouflage legati alle elezioni a partire da gennaio 2024.



Narrazioni ambigue su Trump: le narrazioni relative a Trump sono meno comuni di quelle relative a Biden. È interessante notare che molti di essi sono anche alquanto ambigui: mentre gli autori potrebbero intenderli come negativi, i sostenitori di Trump potrebbero leggerli in modo diverso, come "Lo status di antieroe di Trump lo rende inarrestabile" e "Guerriero di Twitter".



Uno dei profili, @WubbaLubbaDub18, in attività dal 2020 come account standard di Spamouflage, si è principalmente dedicato alla promozione dei resoconti ufficiali del PCC e delle narrazioni pro-PCC, tra cui la diffamazione dei manifestanti pro-democrazia di Hong Kong in mandarino. Dopo un periodo di inattività tra aprile 2022 e maggio 2023, l'account è tornato attivo postando in inglese e condividendo contenuti generati dall'intelligenza artificiale. Potrebbe aver cambiato nome, immagine del profilo e biografia durante questo periodo.

Durante questo periodo, l'account ha regolarmente pubblicato "poster di film" generati dall'intelligenza artificiale di Spamouflage, insieme a testi anti-Biden e pro-Trump in inglese. Tuttavia, sembra che il 13 maggio 2023 l'operatore dell'account abbia risposto in mandarino a un tweet dell'account ufficiale della campagna Trump, dimenticando di tradurre i propri contenuti.

Inizialmente, i post dell'account non hanno suscitato alcun coinvolgimento, autentico o artificiale. Tuttavia, a metà maggio 2023, ha cominciato a interagire con veri sostenitori di Trump. Entro la fine di maggio, i suoi post hanno iniziato a ottenere coinvolgimenti a doppia cifra, continuando a mantenere un livello costante di coinvolgimento a doppia o tripla cifra sulla maggior parte dei post almeno fino a febbraio 2024.

Durante questo periodo, l'account ha anche aderito al servizio Premium di X, beneficiando presumibilmente di funzionalità come il potenziamento algoritmico nelle risposte. Numerosi rapporti hanno segnalato abusi del servizio X Premium da parte di operazioni di influenza legate allo Stato, organizzazioni terroristiche e individui coinvolti in truffe di vario genere.

Un altro account MAGAflage, @ktwsports, attivo dal 2010, ha iniziato a condividere post che implicavano che i politici, in particolare Joe Biden, fossero pedofili, collegati a Jeffrey Epstein e potenzialmente satanici (profilo sospeso)

Uno dei fulcri dell'attività di Spamouflage è rappresentato dalla community conosciuta come "The War of Somethings". Come parte della rete di Spamouflage, la comunità WoS è attiva durante le ore lavorative in Cina e sfrutta account non autentici, tra cui personaggi inventati e account compromessi, per promuovere i propri contenuti. A partire da luglio 2023, e forse anche prima, la rete WoS ha iniziato a pubblicare contenuti direttamente correlati alle imminenti elezioni americane. Questi contenuti includono testi, video, vignette politiche, fotografie e articoli di notizie che criticano coerentemente la politica interna ed estera degli Stati Uniti, allineandosi con le posizioni del Partito Comunista Cinese (PCC) e trattando anche delle elezioni americane del 2024.

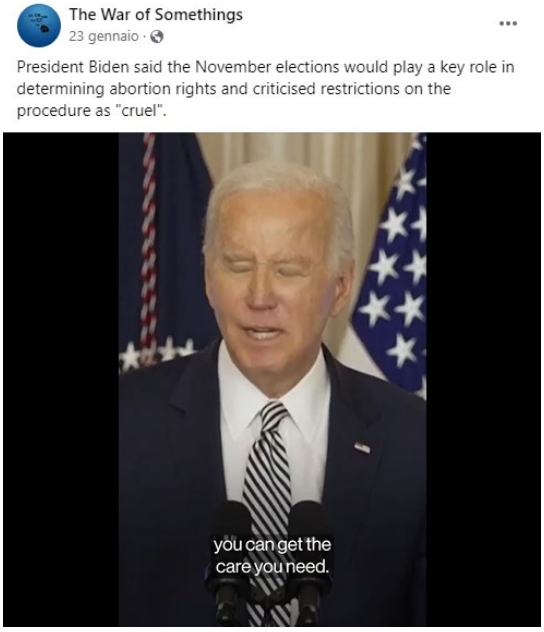


Figura 2: *https://www.facebook.com/reel/407829588286561*

Tratto distintivo della rete è anche l'utilizzo dell'intelligenza artificiale per creare immagini false, come nell'esempio di seguito che ritrae Guo Wengui trascinato dagli agenti di polizia.

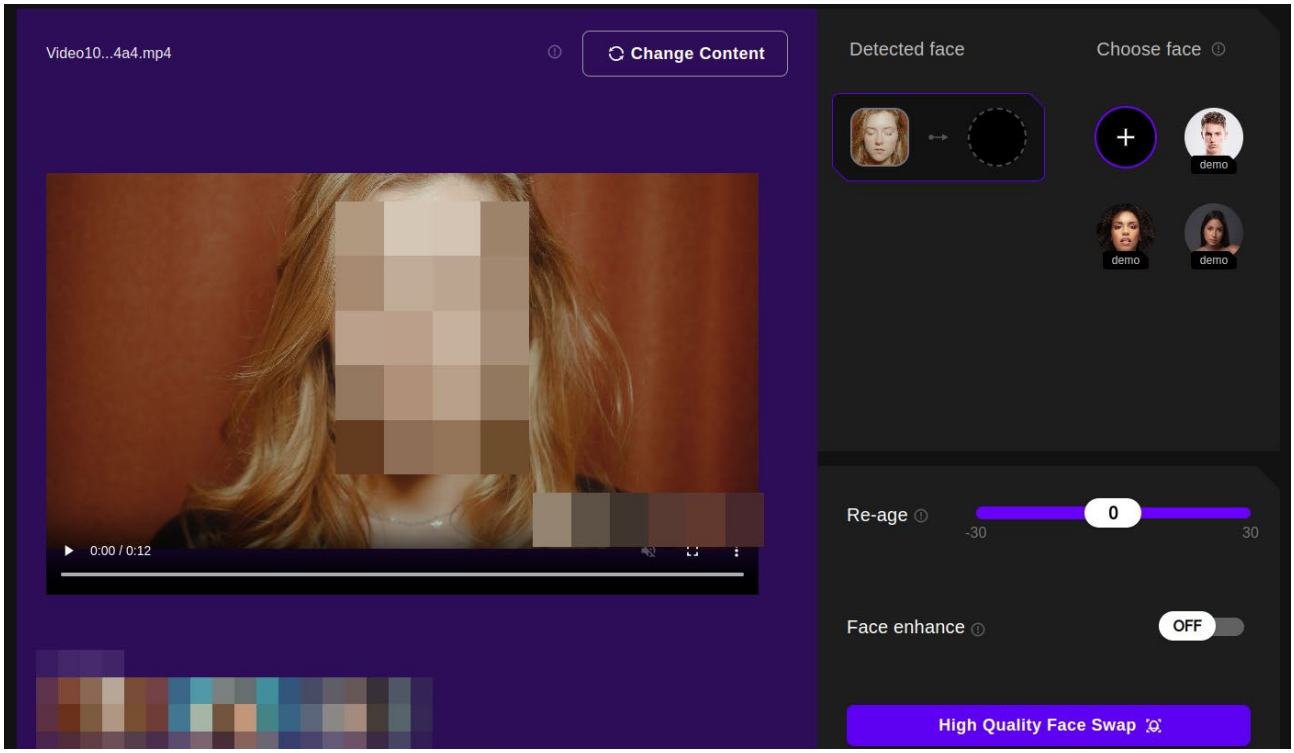
Figura 3: *https://ghostarchive.org/archive/WHMnz*

Facilità d’uso

I recenti sviluppi dell'intelligenza artificiale (AI) hanno reso più accessibili che mai gli strumenti per la creazione di contenuti falsi.

La proliferazione di piattaforme online che offrono servizi gratuiti basati sull’AI che rendono possibile la generazione o manipolazione di testi, immagini e video mantenendo una fedeltà agli originali disarmante.

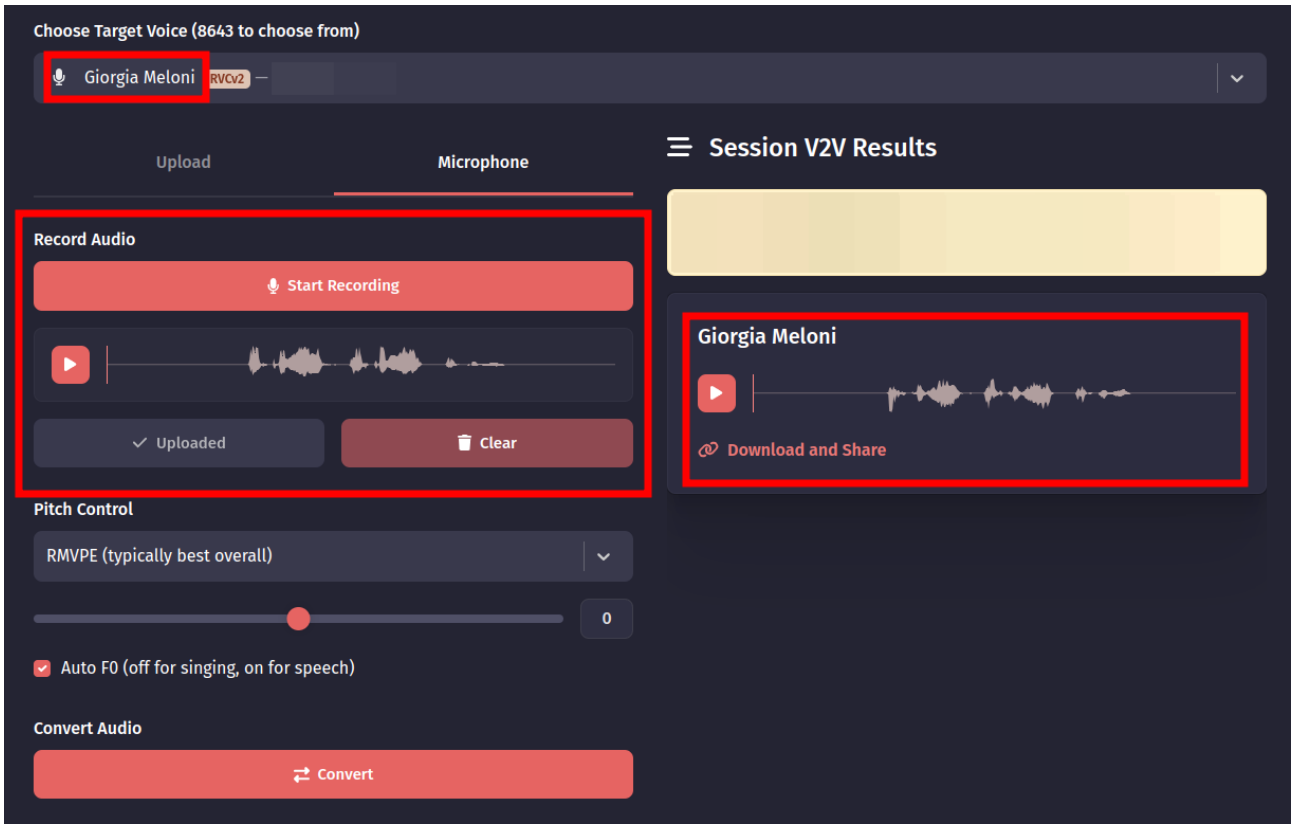
I servizi son molteplici, la maggior parte dei video deep fake è creata facendo face swapping, ovvero una sostituzione della faccia di una persona da un video. Questo il tool usato come esempio: https://akool.com/



Come mostrato nello screen, basta creare un qualunque video e l’immagine della faccia di una persona e dopo pochi minuti il deep fake video sarà disponibile.

Se non bastasse, ci sono altri strumenti che consentono anche di modificare la voce in maniera separata o congiunta con il video.

Questi strumenti inoltre hanno già dei pattern della voce di numerosi personaggi pubblici e grazie a registrazioni o brevi audio è possibile creare audio, di seguito un esempio con un pattern dell'attuale presidente del consiglio Giorgia Meloni:

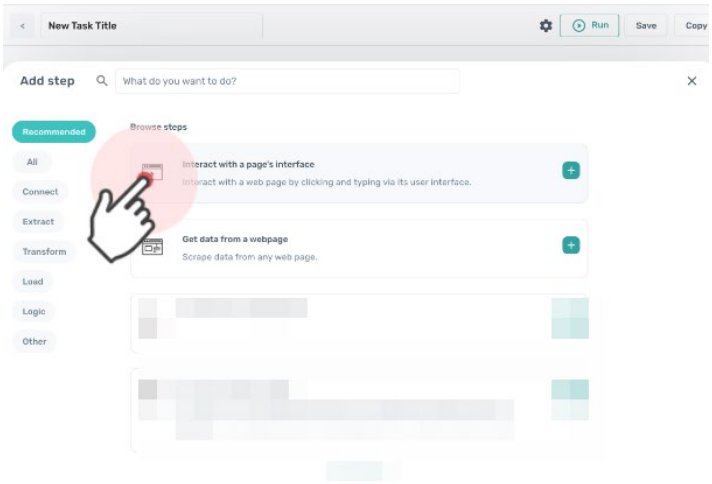


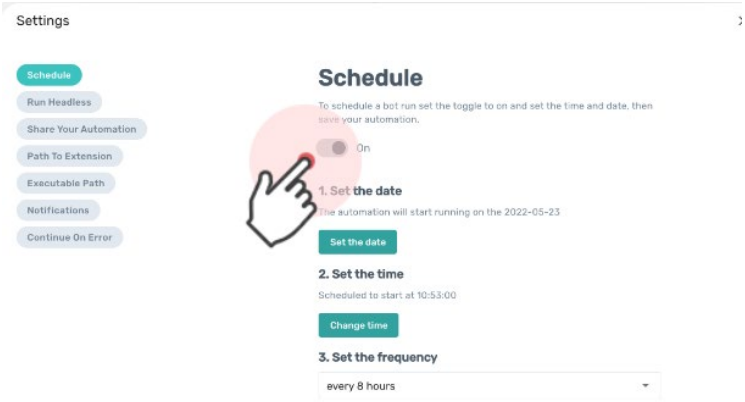
Tool: https://fakeyou.com/

A dar manforte alla disinformazione ci sono anche sondaggi la cui raccolta di informazioni è volutamente limitata a target specifici, ma vengono successivamente diffusi falsando la vastità dei target e quindi le conclusioni. Questi sondaggi vengono pubblicati successivamente sui vari social e resi appetibili con dichiarazioni e risultati tutt'altro che veritieri.

Per creare un sondaggio fasullo basta attingere da una delle numerose liste online che presentano contatti personali, spesso provenienti da databreach, dopodiché è possibile creare form reali o siti di phishing per la raccolta dati. Anche in questo caso le risorse per compiere queste azioni sono di facile utilizzo e reperibili online in maniera gratuita.

Correlato a quest'ultima modalità, c'è sicuramente l'utilizzo di bot, spesso utilizzati per citare informazioni false e aggiungere un commento che sia allettante per i lettori. Questi, nonostante le limitazioni applicate sui social, continuano ad esistere e ad essere funzionanti alimentando la diffusione delle fake news.



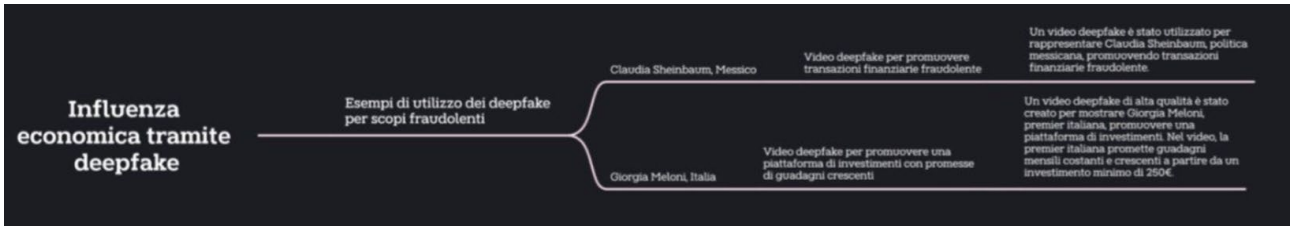


Gli obiettivi

Di seguito analizzeremo alcuni esempi per ciascun obiettivo della creazione e diffusione di FakeNews.

Influenza Economica

Uno degli obiettivi principali per la diffusione di fake news durante le elezioni è l'influenza economica: questo cluster fa riferimento alle fake news volte a manipolare la percezione pubblica dell'economia di una nazione o delle conseguenze economiche delle politiche adottate dai candidati. Le fake news possono infatti essere utilizzate per manipolare i mercati finanziari e ottenere vantaggi economici attraverso la diffusione di informazioni false o fuorvianti; gli individui o gruppi possono diffondere false informazioni su aziende o prodotti per influenzare le decisioni di investimento degli altri, manipolare i prezzi delle azioni e trarre profitto dalle fluttuazioni del mercato.



- Il caso di Claudia Sheinbaum in Messico, vittima di un deepfake, rappresenta un esempio significativo dell'impatto della disinformazione nelle elezioni politiche, con conseguenze potenzialmente gravi per la percezione pubblica e la stabilità politica. In questo caso, un video deepfake utilizza l'immagine della politica messicana per promuovere delle transazioni finanziarie fraudolente. Questo video falsificato, diffuso attraverso i social media, mira a ingannare i cittadini invitandoli ad investire denaro in un'impresa.

Figura 4: *Video originale da dove è stata presa l'immagine: https://www.google.com/search?q=canalcatorce+intervista+a+claudia+sheinbaum&rlz=1C1CHBF_itIT1099IT1099&oq=canalcatorce+entervist&gs_lcrp=EgZjaHJvbWUqCQgCECEYChigATIGCAAQRRg5MgkIARAhGAoYoAEyCQgCECEYChigA*

La candidata nel video enfatizza la possibilità d'investimento nell'industria Pemex petrolifera, investendo solo 4.000 pesos, circa 225€, promettendo un ritorno ingente.

A partire dal terzo trimestre del 2023, in Messico, si sono diffuse truffe in cui è stata falsificata l'identità di Petróleos Mexicanos (Pemex), con inviti al pubblico a investire nella compagnia statale a partire da mille pesos, promettendo rendimenti allettanti. La situazione è diventata così seria che i criminali informatici hanno diffuso sui social media video in cui apparivano il volto e la voce del presidente Andrés Manuel López Obrador, insieme a conduttori di notiziari in televisione, incoraggiando gli investimenti nell'azienda. Queste informazioni sono state successivamente smentite ufficialmente da Pemex. Recentemente sono stati diffusi video con il volto della governatrice del Banco de México (BdeM). banca centrale ha smentito categoricamente le informazioni diffuse e ha invitato la popolazione a ignorare il video falso per evitare di essere vittima di inganni che potrebbero portare a operazioni fraudolente.

La reazione di Sheinbaum, che ha denunciato pubblicamente il video e minacciato azioni legali, evidenzia l'urgenza nel contrastare la disinformazione politica e il crescente utilizzo di deepfake per

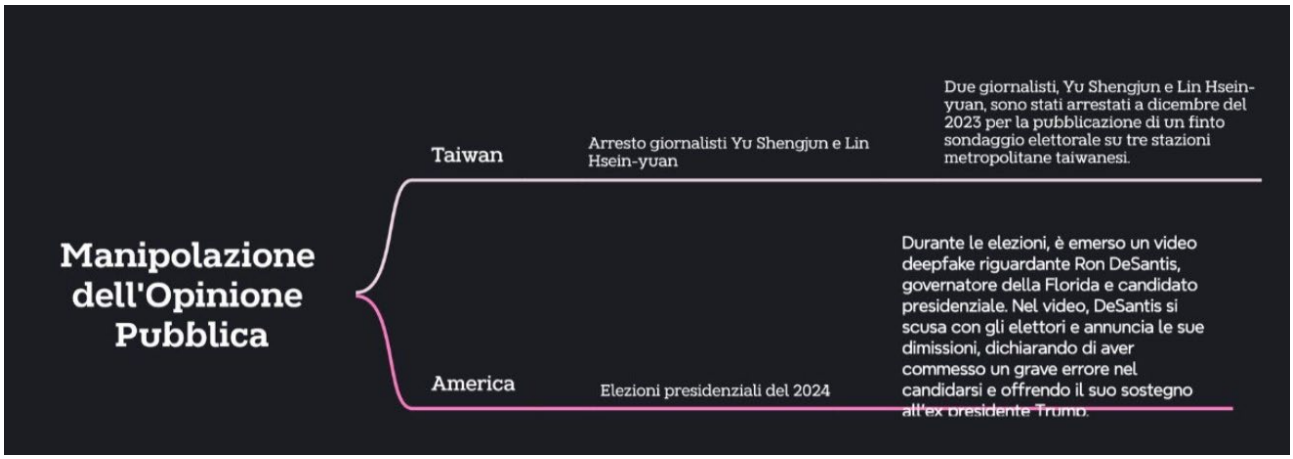
scopi fraudolenti. Il video manipolato presenta la voce della politica e l'immagine del suo ufficio vero, creando un'illusione di autenticità che potrebbe facilmente ingannare i cittadini meno informati.

L'uso del deepfake dilaga anche in Italia, in cui sono coinvolti politici, giornalisti, e conduttori televisivi. Il video in questione prende di mira la Premier italiana Giorgia Meloni, che a differenza dei precedenti mostra una qualità audio e video superiore. Nel video in questione mostra la Premier italiana promuovere una piattaforma di investimenti promettendo un guadagno mensile costante e crescente, partendo da un investimento di soli 250€.

Video: https://www.youtube.com/watch?v=ib8COtt9WB0&ab_channel=Adnkronos

Manipolazione dell'opinione pubblica

Un altro obiettivo significativo della diffusione di fake news durante le elezioni è la manipolazione dell'opinione pubblica: questo tipo di disinformazione comprende le fake news create per supportare o danneggiare specifici candidati o partiti politici. La diffusione di informazioni false viene infatti spesso utilizzata per influenzare l'opinione pubblica su questioni politiche, sociali o culturali, promuovendo una determinata agenda politica o ideologica. Gli individui o gruppi possono creare e diffondere informazioni false o manipolate per generare divisioni nella società, alimentare il dissenso e influenzare il processo decisionale degli elettori; questo può minare la fiducia nelle istituzioni democratiche e compromettere la coesione sociale. Spesso queste notizie false includono affermazioni esagerate sulle politiche proposte o sui successi di un candidato, oppure diffamazioni mirate contro avversari politici con lo scopo di manipolare l'opinione pubblica.



- L'arte della manipolazione elettorale risiede proprio nelle false notizie, ed un caso specifico è quando una testata giornalistica manipola il sondaggio delle elezioni. A dicembre del 2023 due giornalisti, Yu Shengjun e Lin Hsein-yuan, sono stati arrestati a causa della pubblicazione di un finto sondaggio casuale fatto su tre stazioni metropolitane taiwanesi su un totale di 900 persone. Il falso sondaggio avrebbe ingannato gli elettori sulla situazione reale elettorale e di conseguenza minato all'integrità del proprio paese, inserendo come principali canditati Hou Yu-ih e Jaw Shaw-kong per il Kuomintang, partito di centro destra favorevole ad un maggiore impegno con la repubblica cinese. Il finto sondaggio pubblicato da Fingermedia è diventato immediatamente virale sia a Taiwan che in Cina, grazie anche al supporto dei siti partner. Taiwan è al momento al centro dell'attenzione da parte di due grandi Nazioni, la Cina e l'America, lo squilibrio di potere tra le due influenze potrebbe portare a tensioni politiche. L'influenza da parte di finte notizie, in particolar modo in concomitanza delle elezioni taiwanesi potrebbe andare a rompere il sottile equilibrio creato nel tempo.

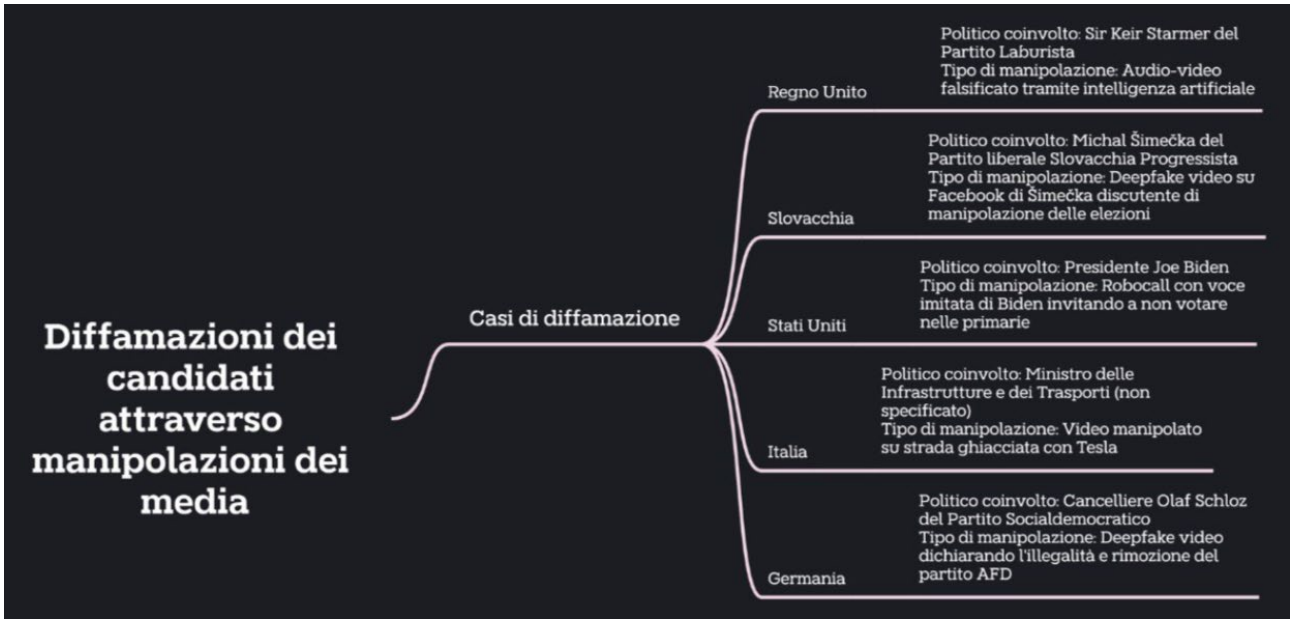
I fatti descritti da *Asia Fact Check Lab*: un individuo è stato incaricato da Zhi Dong New Media Co. Ltd. di condurre un sondaggio dal 27 novembre al 1 dicembre. Questo sondaggio coinvolgeva 900 interviste "casuali" con elettori di età superiore ai 20 anni nelle stazioni ferroviarie di Taiwan settentrionale, centrale e meridionale, con un margine di errore del ± 4%. Tuttavia, il campione selezionato non rappresentava accuratamente la popolazione, poiché ignorava le opinioni delle persone al di fuori delle aree metropolitane. Inoltre, Fingermedia è stato associato a campagne di influenza del Partito Comunista Cinese nel 2019 e a legami con organizzazioni mediatiche sostenute dal Partito. Nel luglio 2019, il Liberty Times di Taiwan e altri media hanno riferito che 23 media online taiwanesi hanno ripubblicato simultaneamente articoli dei media statali cinesi che criticavano il presidente di Taiwan Tsai Ing-wen. L'incidente è stato definito parte di una "guerra rossa dell'informazione" dal palazzo presidenziale di Taiwan, dal Consiglio di sicurezza nazionale e da altre agenzie. Dei 23 siti web citati, 15 erano gestiti dalla società madre di Fingermedia, Zhi Dong Technology Co., Ltd.

I risultati del sondaggio sono diventati virali a Taiwan e sono circolati anche in Cina, cosa insolita per Fingermedia, con sede a Taichung. I resoconti del sondaggio, infatti, si sono diffusi rapidamente a Taiwan sotto l'hashtag "Hou Yu-ih sorpassa" e anche nei notiziari in Cina, tra cui Taiwan.cn, che è affiliato con l'Ufficio cinese per gli affari di Taiwan, Sina Hong Kong e iFeng.

- AMERICA: Un altro video deepfake emerso durante le elezioni riguarda Ron DeSantis, attuale governatore della Florida e candidato alle elezioni presidenziali. Nel video il candidato si scusa con i propri elettori e sostenitori, ammettendo di aver commesso un grave errore nel candidarsi, motivo per il quale decide di dimettersi. Il video mostra Ron DeSantis che dichiara di voler abbandonare la corsa, offrendo sostegno all'ex presidente Trump.

Diffamazione dei candidati

Durante le campagne elettorali, le fake news vengono diffuse per diffamare e danneggiare la reputazione dei candidati avversari, minando così la loro credibilità agli occhi degli elettori e influenzando il loro voto. Le fake news vengono infatti utilizzate per diffamare i candidati politici, diffondendo informazioni false o fuorvianti sulla loro reputazione, etica o capacità. In questo caso, gli individui o gruppi possono diffondere false accuse, montare campagne di denigrazione o manipolare la percezione pubblica di un candidato al fine di danneggiarne la credibilità e le possibilità di successo elettorale. La diffamazione dei candidati attraverso la diffusione di fake news mina la qualità del dibattito politico e può influenzare negativamente l'esito delle elezioni.



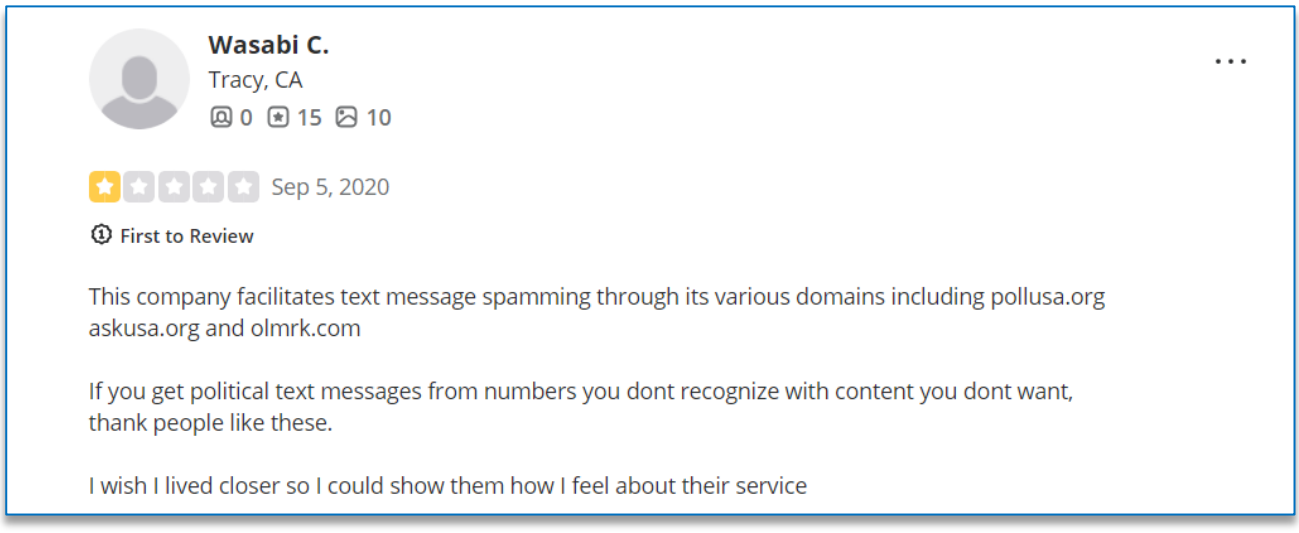
- Durante la conferenza annuale del Partito Laburista, sono stati diffusi video con audio falsificato tramite intelligenza artificiale che mostrava Sir Keir Starmer in momenti di ira e abuso verbale verso il suo staff. Questo attacco mirava a danneggiare l'immagine del leader laburista mentre si preparava per la campagna elettorale, che vedeva il suo partito in vantaggio nei sondaggi rispetto ai Conservatori. Il contenuto diffamatorio è stato pubblicato su Twitter da un account con pochi follower, ottenendo poi un'ampia visibilità. Questo episodio si inserisce in un trend più ampio di utilizzo di deep fake per influenzare le elezioni, come dimostrato da un caso simile in Slovacchia poco prima delle elezioni legislative, dove

un deep fake su Facebook ha mostrato Michal Šimečka, leader del partito liberale Slovacchia Progressista, che discuteva di manipolazione delle elezioni con una giornalista. Anche se entrambi hanno immediatamente denunciato il video come falso, il silenzio elettorale imposto dalle leggi slovacche ha reso difficile contrastarne la diffusione su Facebook.

- AMERICA: Inoltre, un'indagine è stata avviata dopo che è stata riportata la diffusione di un robocall che imita il presidente Joe Biden, invitando i destinatari a non votare nelle elezioni primarie presidenziali del martedì. Il messaggio, che sembra un'imitazione o una manipolazione digitale della voce del presidente, avverte che il voto favorirebbe i repubblicani nel loro tentativo di eleggere di nuovo Donald Trump. L'ufficio del procuratore generale del New Hampshire ha dichiarato che sta indagando su quanto appare essere un "tentativo illegale" di soppressione degli elettori. Il numero personale di un prominente democratico del New Hampshire è comparso sui display degli ID chiamanti di coloro che hanno ricevuto la chiamata. Il messaggio telefonico del robocall inizia con l'espressione "What a bunch of malarkey", eco di un termine preferito usato da Biden in passato.

Successivamente è emerso come questa chiamata sia stata apparentemente architettata da Steve Kramer con presupposto supporto di due compagnie, la texana Life Corporation e Lingo Telecom del Michigan.

Come possiamo notare dalle review online su Life Corporation di Walter Monk, possiamo osservare come siano già noti per condurre certi tipi di attività.



Kramer inoltre riporta come abbia sfruttato l'intelligenza artificiale per clonare la voce del presidente Biden, è necessaria difatti una semplice ricerca su Google per trovare decine di prodotti che possono replicare la voce di un personaggio famoso, come Biden, in pochi minuti.

Biden Voice Clone - https://www.vidnoz.com/ai-solutions/joe-biden-ai-voice.html

Inoltre, conferma come una campagna di disinformazione come questa richieda delle competenze sia a livello tecnico sia a livello infrastrutturale non indifferenti difatti Kramer abuserebbe le compagnie sopracitate per raggiungere l'obiettivo.

A novembre 2023, alcuni utenti online hanno affermato che i nonni di Ursula Von Der Leyen erano nazisti e che si era concessa un aumento di stipendio del 15% come presidente della Commissione dell'Unione europea.

Di seguito il post condiviso da Norman Finkelstein, uno studioso americano, scrittore e attivista politico, conosciuto principalmente per i suoi scritti controversi sul conflitto israelo-palestinese e sull'uso politico della memoria dell'Olocausto. Finkelstein non risulta supporter di nessuna fazione politica americana, tuttavia, è noto per le sue critiche alla politica israeliana risultando quindi in supporto della Palestina. Il post ha ottenuto oltre 2.3 milioni di visualizzazioni, 12 mila retweet e oltre 40 mila like.

https://twitter.com/normfinkelstein/status/1727500224136949829

Il post è iniziato a circolare poi in rete ottenendo decine di migliaia di visualizzazioni. Nel seguente esempio possiamo notare come una pagina di propaganda anti UE e pro Russia abbia condiviso la notizia ottenendo oltre 30 mila visualizzazione e 300 repost.

Ignorance, the root and stem of all evil
@ivan_8848

📸 A photo of Ursula von der Leyen's grandmother with Adolf Hitler is going viral on social media.

The grandfather of the Chairman of the European Commission was SS General Karl Albrecht Oberg. In September 1941, Karl Oberg was appointed "Chief of the SS and Police" (SSPf) in the Radom district of Poland, where he promoted the extermination of Jews and Slavs, as well as the purge of Poles.

On May 5, 1942, Oberg was appointed HSSPf of France. He arrived in Paris and took office on May 12 to lead the fight against French resistance networks and be in charge of the "Jewish Question." He and his staff made wearing the "yellow star" mandatory, regulated and ordered the deportation of about 100,000 people to death camps. Despite several death sentences, Karl Oberg died in his bed.

Earlier, a similar story about the family of the German Foreign Minister made headlines in the European media.

Norman Finkelstein @normfinkelstein · 12h
A Photo from Ursula von der Leyne's Family Album

"My Sweet Granny Didn't Wash Her Hand for a Month after This Precious Occasion"

https://x.com/ivan_8848/status/1769788145329910137

Il tweet sostiene che il nonno della presidente della Commissione europea fosse un generale delle SS di nome Karl Albrecht Oberg. Il post è accompagnato da una foto in bianco e nero che mostrerebbe la nonna della von der Leyen mentre stringe la mano ad Adolf Hitler, con una presunta citazione della stessa von der Leyen, che dice: "La mia dolce nonna non si è lavata le mani per un mese dopo questa preziosa occasione".

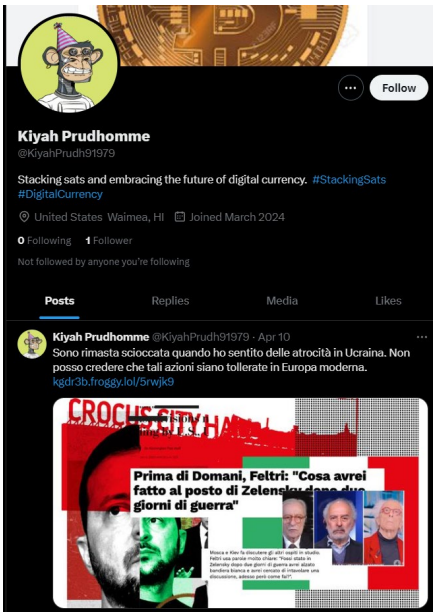
Ancora, il sito web "Repubblica.in" ha pubblicato tre articoli contro il sostegno del governo Meloni all'Ucraina, con titoli come "La guerra all'italiana: solo perdite" e "Gli Stati Uniti e l'UE hanno imposto manovre pericolose all'Italia". Tuttavia, questo non è il legittimo sito web della testata giornalistica "Repubblica", bensì un clone con dominio indiano che sembra essere coinvolto in attività di truffa politica gestita dall'estero a sostegno della propaganda russa. Gli articoli sono stati diffusi tramite una rete di account Twitter. Oltre a Repubblica.in esistono anche i siti LaStampa.in e Corriere.in. Questi casi evidenziano un tentativo di diffondere disinformazione politica attraverso cloni di siti web noti: si sospetta che questa attività sia parte di una campagna più ampia di propaganda russa e di inganno politico gestita dall'estero.

Il seguente esempio, di un profilo apparentemente legato alla scena delle cryptovalute, presenta oltre 700 report per la notizia falsa[1]:

[1] Analisi: https://www.open.online/2024/04/13/falsi-articoli-contro-governo-meloni-sostegno-ucraina-testate-italiane-fc/

https://twitter.com/AsterReppe17242

Lo stesso vale per il seguente esempio, l'account sembra essere legato al mondo delle crypto, 1 solo follower e 0 pagine o profili seguiti. Anche in questo caso il post ha ottenuto quasi 4 mila retweet:



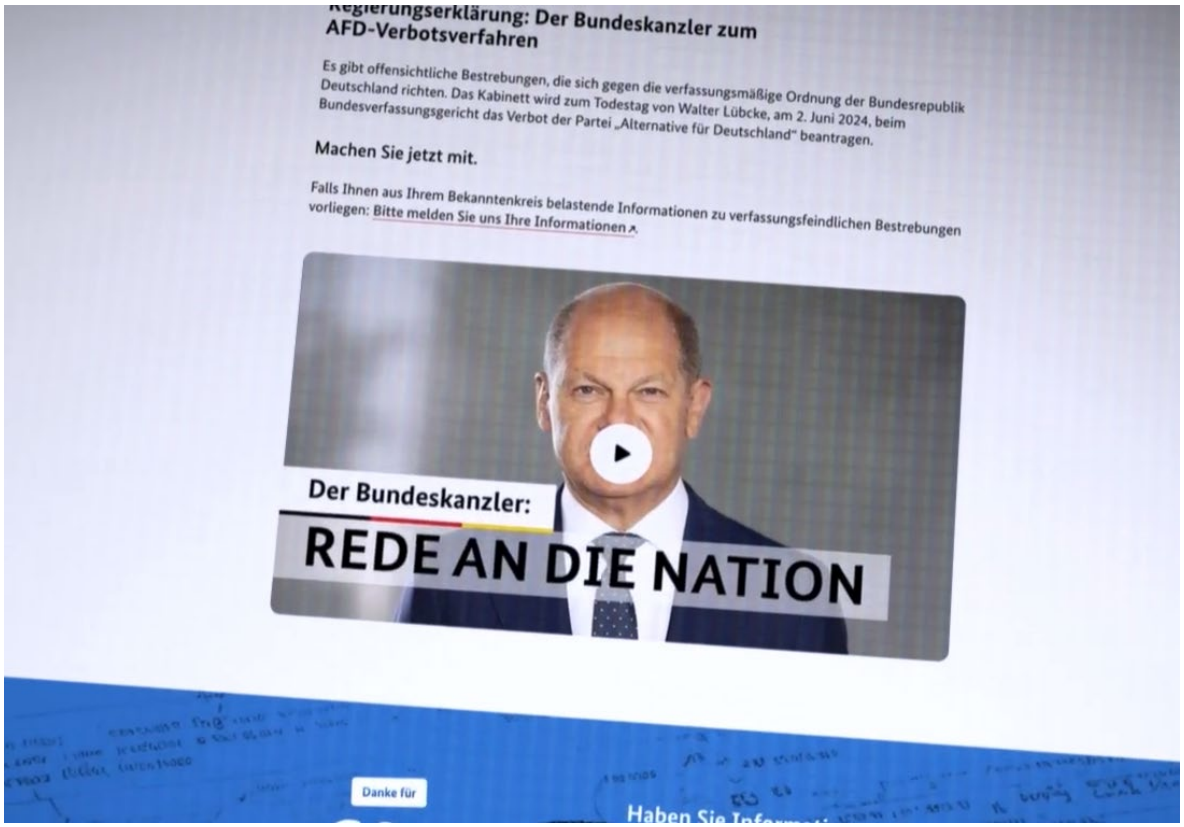
https://twitter.com/KiyahPrudh91979

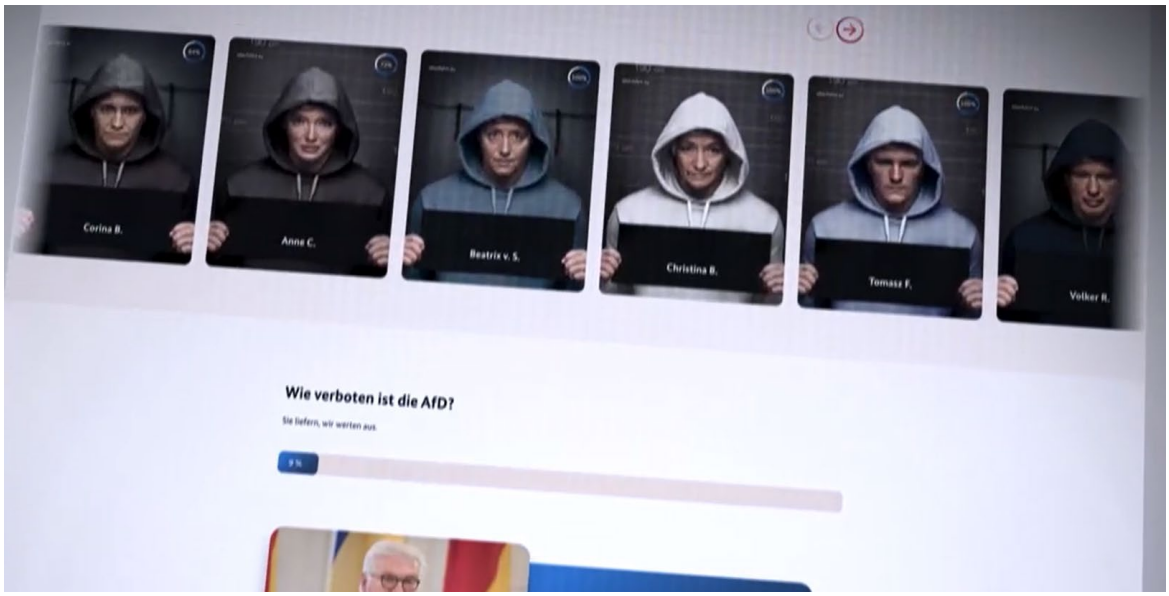
Inoltre, Il rapporto del German Marshall Fund mette in luce che il Dipartimento del Tesoro degli Stati Uniti ha imposto sanzioni[2] a 26 persone e 7 entità coinvolte nella disseminazione di false notizie riguardanti l'Ucraina. Tra di essi figurano la Strategic Culture Foundation, InfoRos, NewsFront, SouthFront, tutti accusati da Washington di avere legami con l'intelligence russa. Lo stesso si applica ad altre fonti di informazione come il New Eastern Outlook e l'Oriental Review, sospettate di essere legate al Cremlino. United World International e Geopolitica sarebbero invece associate alla sfera di Alexander Dugin, l'ideologo di Vladimir Putin[3].

Nel caso specifico a livello nostrano, verso la fine di Gennaio del 2024 è iniziato a circolare un video di un uomo all'apparenza molto simile al nostro ministro delle infrastrutture e dei trasporti, bloccato su una strada ghiacciata mentre cerca di ripartire con la sua tesla. Nel video si nota le risate e la derisione della persona che ha registrato la scena. Il video in questione è stato utilizzato come "meme" al fine di schernire il ministro italiano, che ha provveduto a rispondere sui social "Si inventano pure video-fake pur di attaccare me e la Lega".

[2] https://home.treasury.gov/news/press-releases/jy0628
[3] https://www.open.online/2024/04/29/usa-report-propaganda-russa-salvini/

Un caso di diffamazione nella politica Europea risiede in Germania attraverso un deepfake del Cancelliere Olaf Schloz, membro del partito socialdemocratico. Il video in questione mostra il cancelliere affermare di rendere illegale e rimuovere il partito AFD(Alternative für Deutschland), partito politico di estrema destra, suscitando numerose reazioni e dissensi da parte dell'opposizione. La creazione del video ha l'obiettivo di screditare il partito di destra, già conosciuto per le sue tensioni con il cancelliere. Analizzando il video si possono notare dei difetti, a partire dalla voce monotono fino ad arrivare alle numerose pause non in linea con il Cancelliere. Inoltre, per aumentare la credibilità del video, i creatori del deepfake hanno creato una finta pagina https://afd-verbot.de/, pagina ancora attiva in cui afferma che il cancelliere mette al bando il partito di opposizione e modificato a seguito della conferma della veridicità del video. L'obiettivo del sito era quello di raccogliere consensi e firme per mettere al bando il partito di estrema destra. Ad oggi il sito si presenta come un archivio di prove contro il partito AFD, catalogandole e numerandole.


Regierungserklärung: Der Bundeskanzler zum AFD-Verbotsverfahren
Es gibt offensichtliche Bestrebungen, die sich gegen die verfassungsmäßige Ordnung der Bundesrepublik Deutschland richten. Das Kabinett wird zum Todestag von Walter Lübcke, am 2. Juni 2024, beim Bundesverfassungsgericht das Verbot der Partei „Alternative für Deutschland" beantragen.
Machen Sie jetzt mit.
Falls Ihnen aus Ihrem Bekanntenkreis belastende Informationen zu verfassungsfeindlichen Bestrebungen vorliegen: Bitte melden Sie uns Ihre Informationen
Der Bundeskanzler:
REDE AN DIE NATION
Danke für


Corina B.
Anne C.
Beatrix v. S.
Christina B.
Tomasz F.
Volker R.
Wie verboten ist die AfD?
Sie liefern, wir werten aus.

POLITISCHE SCHÖNHEIT

inizio | Prove | persone | Notificare | Uscita dell'AfD | Donare

Visualizzazione elenco | Vista a griglia

Complottismo/Estremismo

Un altro obiettivo importante della diffusione di fake news durante le elezioni è la promozione del complottismo ed estremismo: questo obiettivo mira a creare divisioni nella società attraverso la diffusione di teorie del complotto e ideologie estremiste, includendo le fake news propagate da gruppi complottisti o estremisti, che spesso diffondono teorie del complotto senza fondamento o informazioni estremamente polarizzate per influenzare l'opinione pubblica o radicalizzare gli elettori, alimentando ideologie estremiste, diffondendo informazioni false o manipolate su eventi storici, questioni politiche o sociali. A tale scopo, gli individui o gruppi possono utilizzare la disinformazione per radicalizzare gli individui, alimentare la diffidenza verso le istituzioni e promuovere ideologie estremiste o violente.

- Il 7 febbraio 2024, l'utente di X Javed Iqbal (@javediqbalpk1), ha diffuso un audio in cui affermava che Imran Khan, fondatore del PTI, avesse annunciato un boicottaggio delle elezioni previste per l'8 febbraio. Nell'audio, Khan denuncia presunte persecuzioni contro il suo partito e accusa le forze dell'ordine di detenere e torturare i lavoratori del PTI, per un totale di 302 retweet e 285 citazioni su Twitter.

  "Miei cari pakistani: con l'avvicinarsi della data delle elezioni, è in corso un giro di vite nei confronti del nostro partito. Il simbolo del nostro partito è stato confiscato e ogni giorno i nostri lavoratori vengono detenuti e arrestati. I titolari di biglietti PTI, comprese le donne, rischiano la tortura. Nonostante sia in prigione, sono ben informato. La polizia e altre istituzioni sono complici e la Commissione elettorale è compromessa. Senza alcuna speranza di giustizia, abbiamo deciso di boicottare le elezioni a causa della situazione attuale".

  Tuttavia, il partito ha avvertito i suoi sostenitori di diffidare delle tattiche ingannevoli utilizzate nei giorni precedenti le elezioni e li ha esortati a concentrarsi sul voto.

Inoltre, un caso emblematico di Cross Cyber Manipulation è avvenuto a Taiwan, dove è stata emessa un'allerta a livello nazionale dopo che un satellite cinese ha sorvolato il suo spazio aereo meridionale giorni prima di un'elezione presidenziale cruciale. Tutti coloro presenti sul territorio hanno ricevuto un messaggio di avviso per la loro sicurezza, segnalando un presunto missile in volo nello spazio aereo, sebbene il ministero della Difesa abbia rapidamente smentito l'ipotesi di un attacco. Questo evento significativo, che si è verificato mentre il ministro degli Esteri Joseph Wu teneva una conferenza stampa a Taipei in vista delle elezioni, è stato spiegato come il passaggio di un satellite cinese con il rischio di detriti in caduta. Quello che abbiamo già osservato con RedAlert nel caso della guerra di Hamas evidenzia i rischi associati a un nuovo filone che può essere sfruttato per manipolare e influenzare la disinformazione, dove strumenti che generano tensione e insicurezza possono infatti essere usati per manipolare l'opinione pubblica: a tal proposito, è importante considerare che dietro pseudonimi o schermate anonime potrebbero celarsi gruppi con legami istituzionali più elevati nei rispettivi Paesi di origine.

Quando si tratta di attacchi DDoS e gruppi di hacktivisti, infatti, è essenziale comprendere il potenziale impatto su eventi politici come le elezioni. Gli attacchi DDoS possono mirare a sovraccaricare i sistemi informatici delle istituzioni coinvolte nelle elezioni, rendendo difficile o impossibile l'accesso ai siti web ufficiali per informazioni o per il voto online. Questo può influenzare negativamente la partecipazione elettorale o compromettere la trasparenza e l'integrità del processo stesso. I gruppi di hacktivisti, utilizzando le proprie competenze tecniche, potrebbero tentare di compromettere i sistemi informatici legati alle elezioni al fine di alterare i risultati o diffondere disinformazione attraverso la manipolazione di dati sensibili.

AMERICA: L'annuncio della candidatura ufficiale del Presidente Joe Biden per la rielezione è stato accompagnato da un attacco pubblicitario dei Repubblicani. Questo annuncio, intitolato "Sconfiggi Biden", immagina una vittoria di Biden e della Vice Presidente Kamala Harris nel 2024 e presenta

una serie di eventi immaginati, accompagnati da immagini e video generati interamente da intelligenza artificiale, che si suppone siano il risultato della loro rielezione.

- Il video, creato dal Comitato Nazionale Repubblicano, ritrae eventi allarmanti come un'invasione cinese a Taiwan, la chiusura di centinaia di banche regionali negli Stati Uniti e il blocco della città di San Francisco a causa della criminalità, tutti attribuiti alla vittoria elettorale di Biden.

Altri casi: attività di hacking – APT 31

Di recente si è sentito molto parlare di un processo di accusa verso alcuni membri del gruppo di Advanced Persistent Threat noto come APT31, che avrebbero attaccato infrastrutture critiche negli USA e nel Regno Unito, mirando a governi, aziende e individui dal 2010. Sono accusati di furto di dati e spionaggio su vasta scala, incluso il tentativo di hack delle e-mail dei parlamentari britannici e l'accesso a dati della Commissione elettorale britannica.

Analizzando i capi d'incriminazione formale si nota come vengano accusati di intrusione informatica e frode elettronica a sostegno degli obiettivi di intelligence straniera ed economica del Ministero per la Sicurezza dello Stato (MSS) della Repubblica Popolare Cinese (PRC). Queste attività includono il furto di informazioni sensibili, l'accesso non autorizzato a computer protetti, e lo sfruttamento di vulnerabilità informatiche contro una vasta gamma di bersagli negli Stati Uniti e altrove, compresi funzionari governativi, industrie della difesa e dell'economia, e attivisti per la democrazia.

Le accuse sono dirette a diversi imputati, tra cui NI GAOBIN, WENG MING, CHENG FENG, PENG YAOWEN, SUN XIAOHUI, XIONG WANG, e ZHAO GUANGZONG, i quali hanno operato sia individualmente sia come parte di un gruppo noto con vari nomi, tra cui "Advanced Persistent Threat 31", "Zirconium", "Violet Typhoon", "Judgment Panda", e "Altaire". L'attività di hacking è stata condotta per conto dell'Hubei State Security Department (HSSD), un braccio dell'MSS nella provincia di Hubei, Cina. Tra le operazioni dettagliate, l'HSSD ha creato una società di facciata, Wuhan Xiaoruizhi Science & Technology Co., per facilitare le sue attività di intrusione informatica.

L'indagine rivela come questi imputati abbiano mirato a svariati obiettivi strategici per la Cina, utilizzando tecniche sofisticate di malware e strategie di phishing per accedere e rubare informazioni sensibili. Le operazioni coprono un ampio spettro di obiettivi, tra cui funzionari governativi degli Stati Uniti e di altri paesi critici nei confronti delle politiche del PRC, industrie chiave come la difesa, l'IT, le telecomunicazioni, la produzione, il commercio, la finanza, il consulting, il legale e la ricerca, oltre a individui e gruppi legati ai movimenti democratici di Hong Kong e alla critica del governo cinese.

Oltre alle specifiche tecniche delle intrusioni, l'indagine descrive dettagliatamente le accuse di cospirazione per commettere intrusioni informatiche e frode elettronica, fornendo esempi di atti

compiuti dai cospiratori per avanzare i loro obiettivi illeciti, come il mantenimento dell'accesso non autorizzato a reti selezionate, l'uso di malware per rubare informazioni, e il tentativo di influenzare eventi politici e processi democratici.

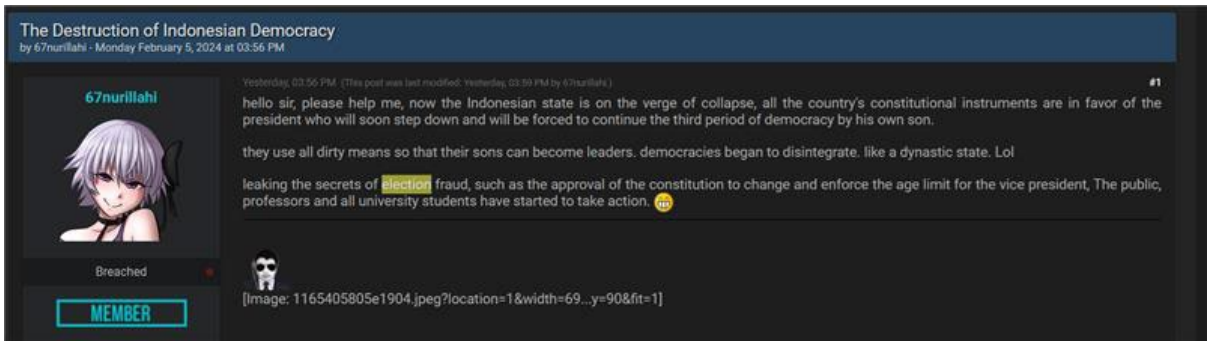
Infine, il documento include allegazioni di confisca criminale contro gli imputati, per cui gli Stati Uniti intendono richiedere la confisca di qualsiasi proprietà derivata direttamente o indirettamente come risultato delle loro attività illecite, nonché qualsiasi proprietà utilizzata o destinata a essere utilizzata per commettere o facilitare tali reati.

Forum underground

I forum sul deepweb e sul darkweb offrono un terreno fertile per la diffusione della disinformazione, della manipolazione dell'opinione pubblica e persino del reclutamento di hacker per sabotare i sistemi elettorali, diventando inoltre un mercato per la vendita di dati rubati che possano essere utilizzati per compromettere la sicurezza e l'integrità delle elezioni.

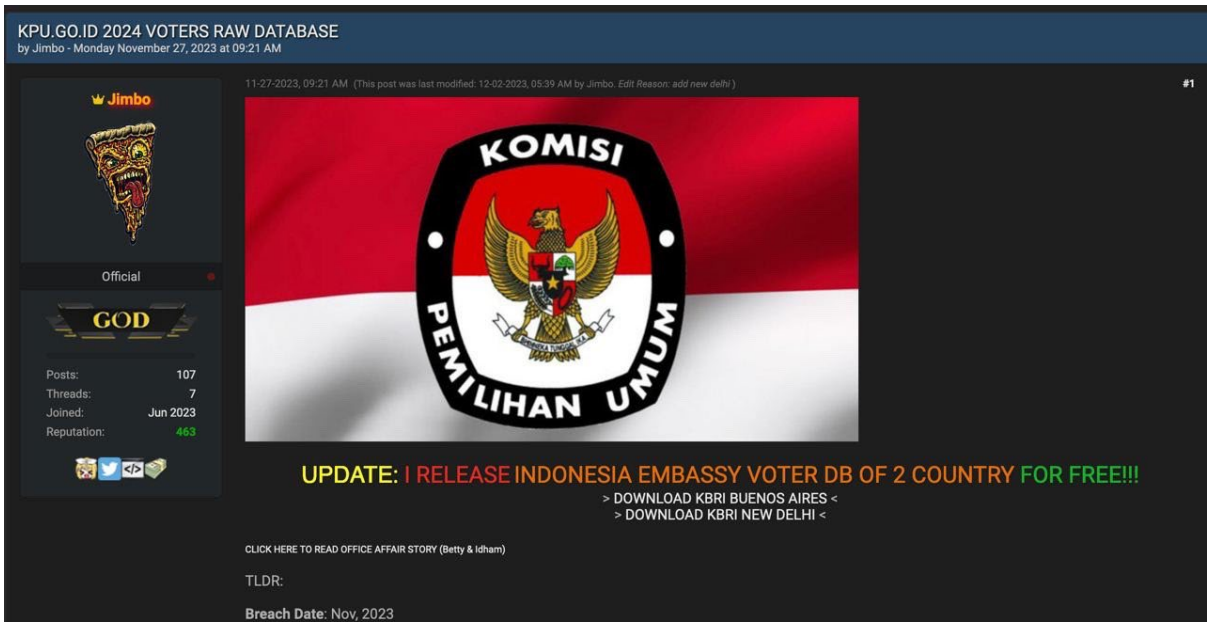
I dati sulle elezioni che possono essere ritrovati sul deep web e sul dark web includono informazioni sensibili come elenchi di elettori, informazioni di registrazione degli elettori, risultati elettorali precedenti, software e strumenti per compromettere i sistemi elettorali, e persino informazioni su campagne politiche e strategie di comunicazione. Questo fenomeno rappresenta una minaccia crescente per la democrazia, poiché le informazioni distorte e le manipolazioni online possono influenzare l'esito delle elezioni in modo significativo, minando la fiducia del pubblico nel processo democratico.

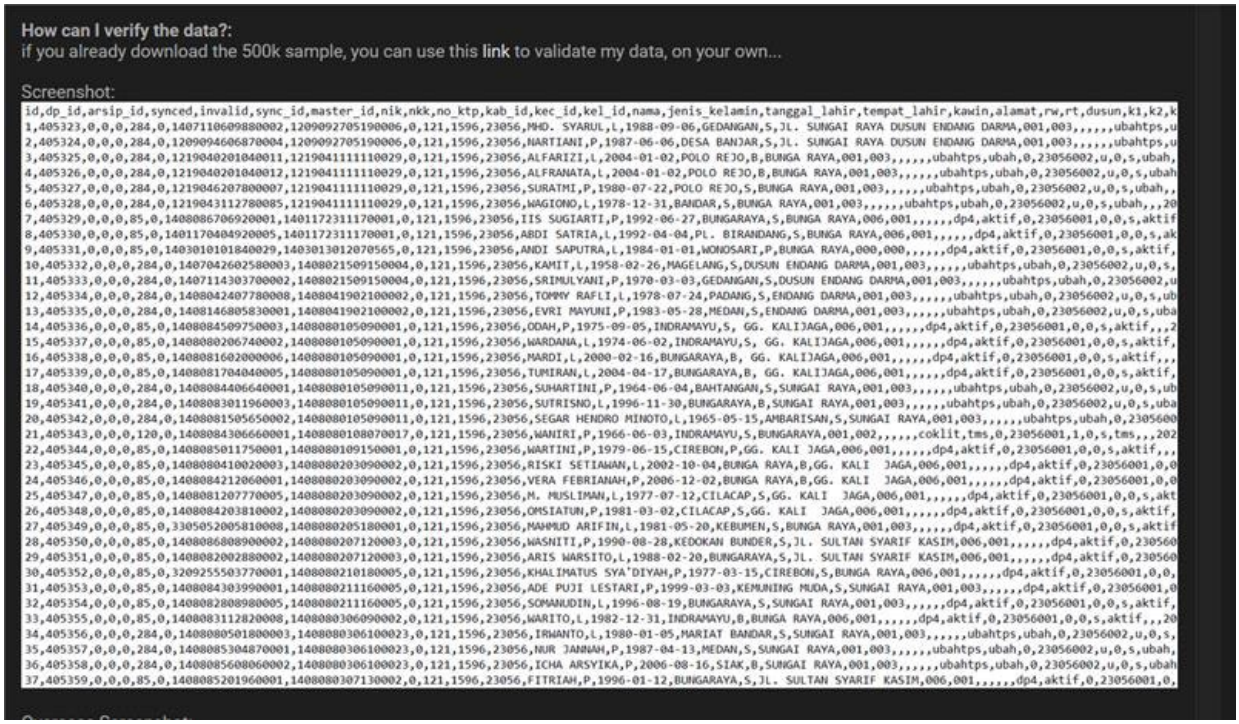
- Di seguito un post che fa riferimento ad una situazione politica problematica in Indonesia, con accuse di corruzione e manipolazione delle elezioni a vantaggio del presidente in carica e del suo successore designato, presunto figlio:



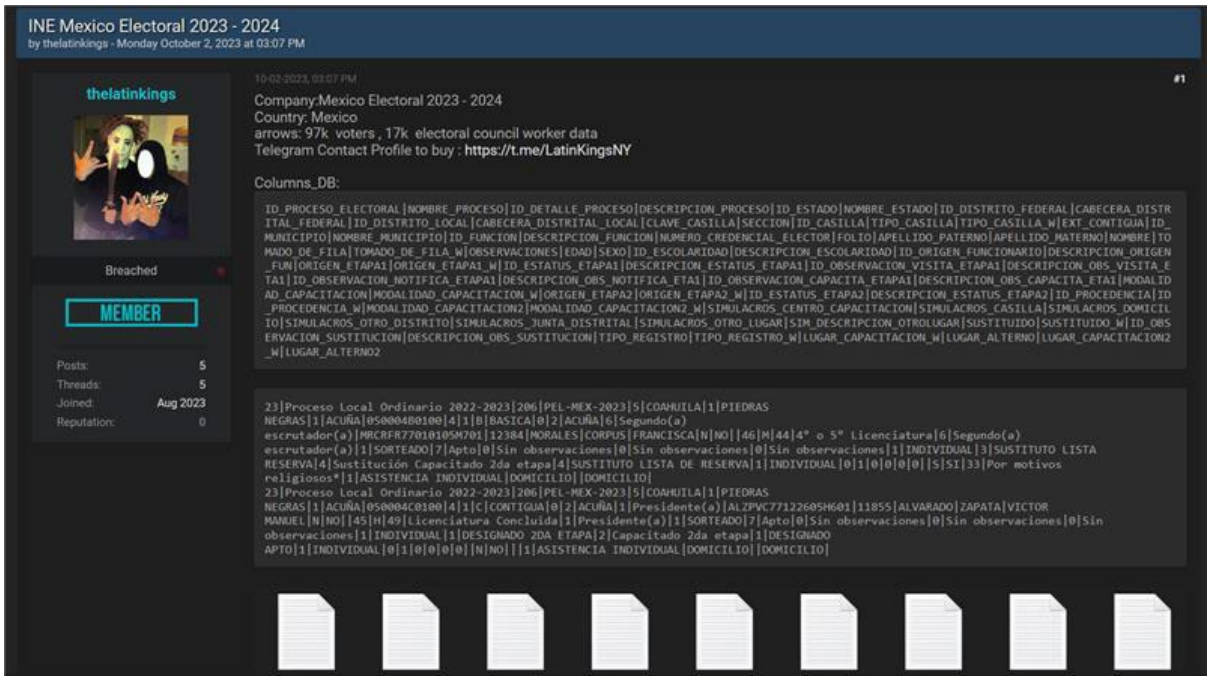
- Un altro post pubblicato a novembre 2023 fa riferimento ad una violazione che coinvolge dati personali appartenenti agli elettori indonesiani. Il numero totale di righe, superiore a 252 milioni, suggerisce la portata di questa violazione. I dati compromessi includono informazioni sensibili come numeri di identificazione, dettagli dei passaporti, nomi e indirizzi. L'origine dei dati sembra essere il sito web ufficiale della Commissione Elettorale Nazionale Indonesiana (*.kpu.go.id). Tuttavia, l'aspetto più inquietante di questa violazione è la sua natura commerciale. Il post offre questi dati rubati in vendita a un prezzo notevole, indicando che l'obiettivo principale potrebbe essere il profitto finanziario. Inoltre, la possibilità di rivendere i dati altrove sottolinea questo mercato di informazioni personali rubate, amplificando il rischio di abusi e violazioni della privacy su vasta scala.

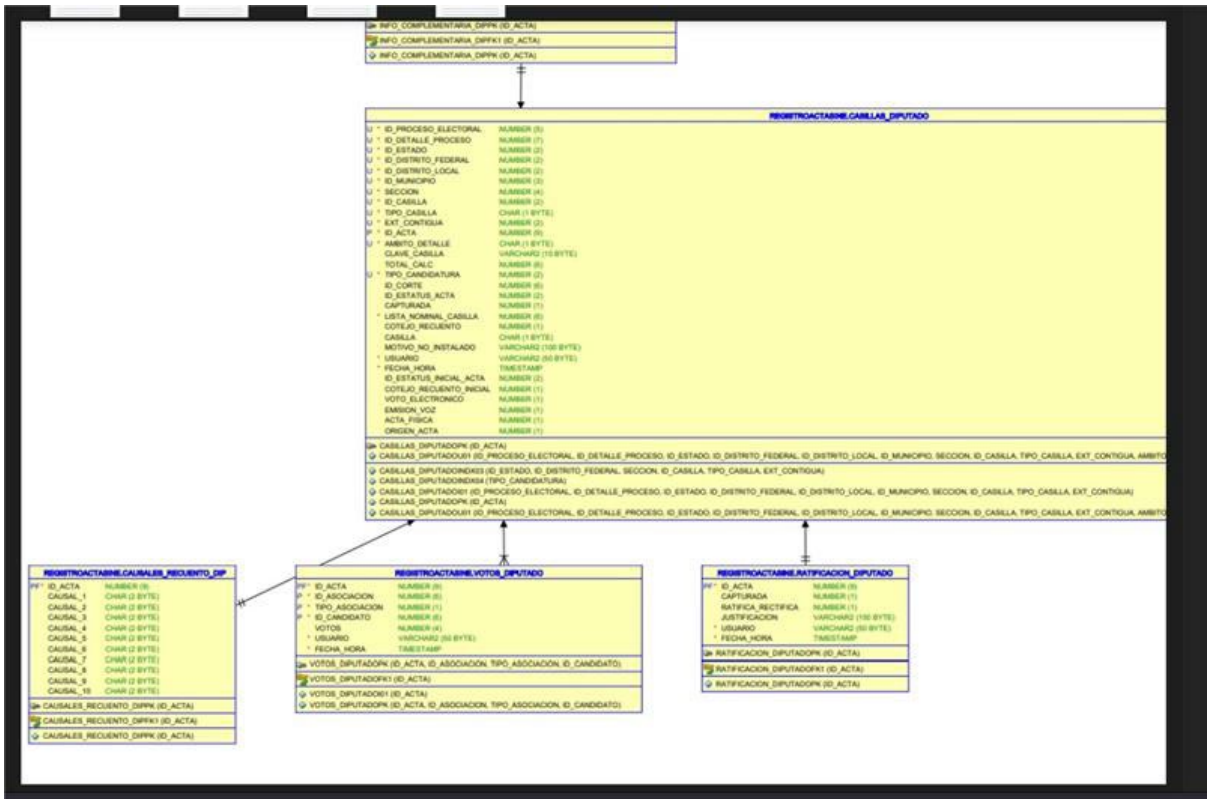
L’autore del post invita inoltre a contattarlo privatamente per ulteriori dettagli sull'accesso al sito.


KPU.GO.ID 2024 VOTERS RAW DATABASE
by Jimbo - Monday November 27, 2023 at 09:21 AM
Jimbo
Official
GOD
Posts: 107
Threads: 7
Joined: Jun 2023
Reputation: 463
11-27-2023, 09:21 AM (This post was last modified: 12-02-2023, 05:39 AM by Jimbo. Edit Reason: add new delhi)
#1
KOMISI PEMILIHAN UMUM
UPDATE: I RELEASE INDONESIA EMBASSY VOTER DB OF 2 COUNTRY FOR FREE!!!
> DOWNLOAD KBRI BUENOS AIRES <
> DOWNLOAD KBRI NEW DELHI <
CLICK HERE TO READ OFFICE AFFAIR STORY (Betty & Idham)
TLDR:
Breach Date: Nov, 2023


How can I verify the data?:
if you already download the 500k sample, you can use this link to validate my data, on your own...
Screenshot:
id,dp_id,arsip_id,synced,invalid,sync_id,master_id,nik,nkk,no_ktp,kab_id,kec_id,kel_id,nama,jenis_kelamin,tanggal_lahir,tempat_lahir,kawin,alamat,rw,rt,dusun,k1,k2,k
1,405323,0,0,0,284,0,1407110609880002,1209092705190006,0,121,1596,23056,MHD. SYARUL,L,1988-09-06,GEDANGAN,S,JL. SUNGAI RAYA DUSUN ENDANG DARMA,001,003,,,,,ubahtps,u
2,405324,0,0,0,284,0,1209094606870004,1209092705190006,0,121,1596,23056,NARTIANI,P,1987-06-06,DESA BANJAR,S,JL. SUNGAI RAYA DUSUN ENDANG DARMA,001,003,,,,,ubahtps,u
3,405325,0,0,0,284,0,1219040201040011,1219041111110029,0,121,1596,23056,ALFARIZI,L,2004-01-02,POLO REJO,B,BUNGA RAYA,001,003,,,,,ubahtps,ubah,0,23056002,u,0,s,ubah,
4,405326,0,0,0,284,0,1219040201040012,1219041111110029,0,121,1596,23056,ALFRANATA,L,2004-01-02,POLO REJO,B,BUNGA RAYA,001,003,,,,,ubahtps,ubah,0,23056002,u,0,s,ubah
5,405327,0,0,0,284,0,1219046207800007,1219041111110029,0,121,1596,23056,SURATMI,P,1980-07-22,POLO REJO,S,BUNGA RAYA,001,003,,,,,ubahtps,ubah,0,23056002,u,0,s,ubah,,
6,405328,0,0,0,284,0,1219043112780085,1219041111110029,0,121,1596,23056,WAGIONO,L,1978-12-31,BANDAR,S,BUNGA RAYA,001,003,,,,,ubahtps,ubah,0,23056002,u,0,s,ubah,,,20
7,405329,0,0,0,85,0,1408086706920001,1401172311170001,0,121,1596,23056,IIS SUGIARTI,P,1992-06-27,BUNGARAYA,S,BUNGA RAYA,006,001,,,,,dp4,aktif,0,23056001,0,0,s,aktif
8,405330,0,0,0,85,0,1401170404920005,1401172311170001,0,121,1596,23056,ABDI SATRIA,L,1992-04-04,PL. BIRANDANG,S,BUNGA RAYA,006,001,,,,,dp4,aktif,0,23056001,0,0,s,ak
9,405331,0,0,0,85,0,1403010101840029,1403013012070565,0,121,1596,23056,ANDI SAPUTRA,L,1984-01-01,WONOSARI,P,BUNGA RAYA,000,000,,,,,dp4,aktif,0,23056001,0,0,s,aktif,
10,405332,0,0,0,284,0,1407042602580003,1408021509150004,0,121,1596,23056,KAMIT,L,1958-02-26,MAGELANG,S,DUSUN ENDANG DARMA,001,003,,,,,ubahtps,ubah,0,23056002,u,0,s,
11,405333,0,0,0,284,0,1407114303700002,1408021509150004,0,121,1596,23056,SRIMULYANI,P,1970-03-03,GEDANGAN,S,DUSUN ENDANG DARMA,001,003,,,,,ubahtps,ubah,0,23056002,u
12,405334,0,0,0,284,0,1408042407780008,1408041902100002,0,121,1596,23056,TOMMY RAFLI,L,1978-07-24,PADANG,S,ENDANG DARMA,001,003,,,,,ubahtps,ubah,0,23056002,u,0,s,ub
13,405335,0,0,0,284,0,1408146805830001,1408041902100002,0,121,1596,23056,EVRI MAYUNI,P,1983-05-28,MEDAN,S,ENDANG DARMA,001,003,,,,,ubahtps,ubah,0,23056002,u,0,s,uba
14,405336,0,0,0,85,0,1408084509750003,1408080105090001,0,121,1596,23056,ODAH,P,1975-09-05,INDRAMAYU,S, GG. KALIJAGA,006,001,,,,,dp4,aktif,0,23056001,0,0,s,aktif,,2
15,405337,0,0,0,85,0,1408080206740002,1408080105090001,0,121,1596,23056,WARDANA,L,1974-06-02,INDRAMAYU,S, GG. KALIJAGA,006,001,,,,,dp4,aktif,0,23056001,0,0,s,aktif,
16,405338,0,0,0,85,0,1408081602000006,1408080105090001,0,121,1596,23056,MARDI,L,2000-02-16,BUNGARAYA,B, GG. KALIJAGA,006,001,,,,,dp4,aktif,0,23056001,0,0,s,aktif,,,
17,405339,0,0,0,85,0,1408081704040005,1408080105090001,0,121,1596,23056,TUMIRAN,L,2004-04-17,BUNGARAYA,B, GG. KALIJAGA,006,001,,,,,dp4,aktif,0,23056001,0,0,s,aktif,
18,405340,0,0,0,284,0,1408084406640001,1408080105090011,0,121,1596,23056,SUHARTINI,P,1964-06-04,BAHTANGAN,S,SUNGAI RAYA,001,003,,,,,ubahtps,ubah,0,23056002,u,0,s,ub
19,405341,0,0,0,284,0,1408083011960003,1408080105090011,0,121,1596,23056,SUTRISNO,L,1996-11-30,BUNGARAYA,B,SUNGAI RAYA,001,003,,,,,ubahtps,ubah,0,23056002,u,0,s,uba
20,405342,0,0,0,284,0,1408081505650002,1408080105090011,0,121,1596,23056,SEGAR HENDRO MINOTO,L,1965-05-15,AMBARISAN,S,SUNGAI RAYA,001,003,,,,,ubahtps,ubah,0,2305600
21,405343,0,0,0,120,0,1408084306660001,1408080108070017,0,121,1596,23056,WANIRI,P,1966-06-03,INDRAMAYU,S,BUNGARAYA,001,002,,,,,coklit,tms,0,23056001,1,0,s,tms,,,202
22,405344,0,0,0,85,0,1408085011750001,1408080109150001,0,121,1596,23056,WARTINI,P,1979-06-15,CIREBON,P,GG. KALI JAGA,006,001,,,,,dp4,aktif,0,23056001,0,0,s,aktif,,,
23,405345,0,0,0,85,0,1408080410020003,1408080203090002,0,121,1596,23056,RISKI SETIAWAN,L,2002-10-04,BUNGA RAYA,B,GG. KALI JAGA,006,001,,,,,dp4,aktif,0,23056001,0,0
24,405346,0,0,0,85,0,1408084212060001,1408080203090002,0,121,1596,23056,VERA FEBRIANAH,P,2006-12-02,BUNGA RAYA,B,GG. KALI JAGA,006,001,,,,,dp4,aktif,0,23056001,0,0
25,405347,0,0,0,85,0,1408081207770005,1408080203090002,0,121,1596,23056,M. MUSLIMAN,L,1977-07-12,CILACAP,S,GG. KALI JAGA,006,001,,,,,dp4,aktif,0,23056001,0,0,s,akt
26,405348,0,0,0,85,0,1408084203810002,1408080203090002,0,121,1596,23056,OMSIATUN,P,1981-03-02,CILACAP,S,GG. KALI JAGA,006,001,,,,,dp4,aktif,0,23056001,0,0,s,aktif,
27,405349,0,0,0,85,0,3305052005810008,1408080205180001,0,121,1596,23056,MAHMUD ARIFIN,L,1981-05-20,KEBUMEN,S,BUNGA RAYA,001,003,,,,,dp4,aktif,0,23056001,0,0,s,aktif
28,405350,0,0,0,85,0,1408086808900002,1408080207120003,0,121,1596,23056,WASNITI,P,1990-08-28,KEDOKAN BUNDER,S,JL. SULTAN SYARIF KASIM,006,001,,,,,dp4,aktif,0,230560
29,405351,0,0,0,85,0,1408082002880002,1408080207120003,0,121,1596,23056,ARIS WARSITO,L,1988-02-20,BUNGARAYA,S,JL. SULTAN SYARIF KASIM,006,001,,,,,dp4,aktif,0,230560
30,405352,0,0,0,85,0,3209255503770001,1408080210180005,0,121,1596,23056,KHALIMATUS SYA'DIYAH,P,1977-03-15,CIREBON,S,BUNGA RAYA,006,001,,,,,dp4,aktif,0,23056001,0,0,
31,405353,0,0,0,85,0,1408084303990001,1408080211160005,0,121,1596,23056,ADE PUJI LESTARI,P,1999-03-03,KEMUNING MUDA,S,SUNGAI RAYA,001,003,,,,,dp4,aktif,0,23056001,0
32,405354,0,0,0,85,0,1408082808980005,1408080211160005,0,121,1596,23056,SOMANUDIN,L,1996-08-19,BUNGARAYA,S,SUNGAI RAYA,001,003,,,,,dp4,aktif,0,23056001,0,0,s,aktif,
33,405355,0,0,0,85,0,1408083112820008,1408080306090002,0,121,1596,23056,WARITO,L,1982-12-31,INDRAMAYU,B,BUNGA RAYA,006,001,,,,,dp4,aktif,0,23056001,0,0,s,aktif,,,20
34,405356,0,0,0,284,0,1408080501800003,1408080306100023,0,121,1596,23056,IRWANTO,L,1980-01-05,MARIAT BANDAR,S,SUNGAI RAYA,001,003,,,,,ubahtps,ubah,0,23056002,u,0,s,
35,405357,0,0,0,284,0,1408085304870001,1408080306100023,0,121,1596,23056,NUR JANNAH,P,1987-04-13,MEDAN,S,SUNGAI RAYA,001,003,,,,,ubahtps,ubah,0,23056002,u,0,s,ubah,
36,405358,0,0,0,284,0,1408085608060002,1408080306100023,0,121,1596,23056,ICHA ARSYIKA,P,2006-08-16,SIAK,B,SUNGAI RAYA,001,003,,,,,ubahtps,ubah,0,23056002,u,0,s,ubah
37,405359,0,0,0,85,0,1408085201960001,1408080307130002,0,121,1596,23056,FITRIAH,P,1996-01-12,BUNGARAYA,S,JL. SULTAN SYARIF KASIM,006,001,,,,,dp4,aktif,0,23056001,0,

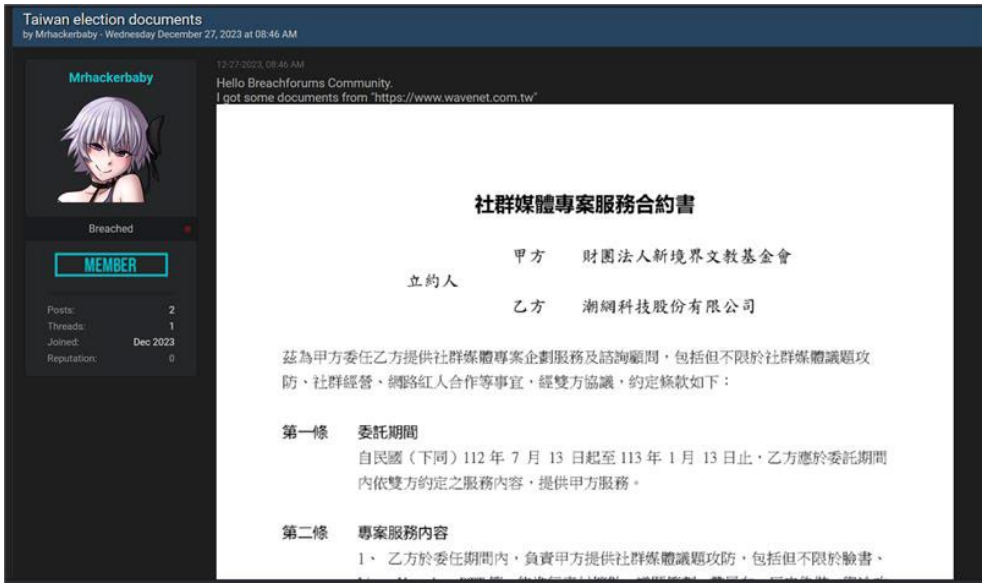
- Anche nel post di seguito vengono offerti dati riguardanti il processo elettorale in Messico del 2023-2024. Vengono elencati dati come il numero di votanti, i dettagli dei lavoratori del consiglio elettorale, i distretti elettorali e le informazioni personali degli elettori, come nome, cognome, età, sesso, istruzione e numero di credenziale elettorale. La loro vendita su un forum underground indica un'attività criminale organizzata e potenzialmente dannosa per l'integrità del processo democratico.
  Il link Telegram fornito è un punto di contatto per acquistare ulteriori informazioni. Queste informazioni dettagliate potrebbero essere estremamente sensibili e utili per individui o gruppi che cercano di influenzare o manipolare il processo elettorale.


INE Mexico Electoral 2023 - 2024
by thelatinkings - Monday October 2, 2023 at 03:07 PM
thelatinkings
Breached
MEMBER
Posts: 5
Threads: 5
Joined: Aug 2023
Reputation: 0
10-02-2023, 03:07 PM
#1
Company:Mexico Electoral 2023 - 2024
Country: Mexico
arrows: 97k voters , 17k electoral council worker data
Telegram Contact Profile to buy : https://t.me/LatinKingsNY
Columns_DB:
ID_PROCESO_ELECTORAL|NOMBRE_PROCESO|ID_DETALLE_PROCESO|DESCRIPCION_PROCESO|ID_ESTADO|NOMBRE_ESTADO|ID_DISTRITO_FEDERAL|CABECERA_DISTRITAL_FEDERAL|ID_DISTRITO_LOCAL|CABECERA_DISTRITAL_LOCAL|CLAVE_CASILLA|SECCION|ID_CASILLA|TIPO_CASILLA|TIPO_CASILLA_W|EXT_CONTIGUA|ID_MUNICIPIO|NOMBRE_MUNICIPIO|ID_FUNCION|DESCRIPCION_FUNCION|NUMERO_CREDENCIAL_ELECTOR|FOLIO|APELLIDO_PATERNO|APELLIDO_MATERNO|NOMBRE|TOMADO_DE_FILA|TOMADO_DE_FILA_W|OBSERVACIONES|EDAD|SEXO|ID_ESCOLARIDAD|DESCRIPCION_ESCOLARIDAD|ID_ORIGEN_FUNCIONARIO|DESCRIPCION_ORIGEN_FUN|ORIGEN_ETAPA1|ORIGEN_ETAPA1_W|ID_ESTATUS_ETAPA1|DESCRIPCION_ESTATUS_ETAPA1|ID_OBSERVACION_VISITA_ETAPA1|DESCRIPCION_OBS_VISITA_ETA1|ID_OBSERVACION_NOTIFICA_ETAPA1|DESCRIPCION_OBS_NOTIFICA_ETA1|ID_OBSERVACION_CAPACITA_ETAPA1|DESCRIPCION_OBS_CAPACITA_ETA1|MODALIDAD_CAPACITACION|MODALIDAD_CAPACITACION_W|ORIGEN_ETAPA2|ORIGEN_ETAPA2_W|ID_ESTATUS_ETAPA2|DESCRIPCION_ESTATUS_ETAPA2|ID_PROCEDENCIA|ID_PROCEDENCIA_W|MODALIDAD_CAPACITACION2|MODALIDAD_CAPACITACION2_W|SIMULACROS_CENTRO_CAPACITACION|SIMULACROS_CASILLA|SIMULACROS_DOMICILIO|SIMULACROS_OTRO_DISTRITO|SIMULACROS_JUNTA_DISTRITAL|SIMULACROS_OTRO_LUGAR|SIM_DESCRIPCION_OTROLUGAR|SUSTITUIDO|SUSTITUIDO_W|ID_OBSERVACION_SUSTITUCION|DESCRIPCION_OBS_SUSTITUCION|TIPO_REGISTRO|TIPO_REGISTRO_W|LUGAR_CAPACITACION_W|LUGAR_ALTERNO|LUGAR_CAPACITACION2_W|LUGAR_ALTERNO2
23|Proceso Local Ordinario 2022-2023|206|PEL-MEX-2023|5|COAHUILA|1|PIEDRAS NEGRAS|1|ACUÑA|050004B0100|4|1|B|BASICA|0|2|ACUÑA|6|Segundo(a) escrutador(a)|MRCRFR770101O5M701|12384|MORALES|CORPUS|FRANCISCA|N|NO||46|M|44|4° o 5° Licenciatura|6|Segundo(a) escrutador(a)|1|SORTEADO|7|Apto|0|Sin observaciones|0|Sin observaciones|0|Sin observaciones|1|INDIVIDUAL|3|SUSTITUTO LISTA RESERVA|4|Sustitución Capacitado 2da etapa|4|SUSTITUTO LISTA DE RESERVA|1|INDIVIDUAL|0|1|0|0|0|0||S|SI|33|Por motivos religiosos*|1|ASISTENCIA INDIVIDUAL|DOMICILIO||DOMICILIO|
23|Proceso Local Ordinario 2022-2023|206|PEL-MEX-2023|5|COAHUILA|1|PIEDRAS NEGRAS|1|ACUÑA|050004C0100|4|1|C|CONTIGUA|0|2|ACUÑA|1|Presidente(a)|ALZPVC77122605H601|11855|ALVARADO|ZAPATA|VICTOR MANUEL|N|NO||45|H|49|Licenciatura Concluida|1|Presidente(a)|1|SORTEADO|7|Apto|0|Sin observaciones|0|Sin observaciones|0|Sin observaciones|1|INDIVIDUAL|1|DESIGNADO 2DA ETAPA|2|Capacitado 2da etapa|1|DESIGNADO APTO|1|INDIVIDUAL|0|1|0|0|0|0|N|NO||1|ASISTENCIA INDIVIDUAL|DOMICILIO||DOMICILIO|



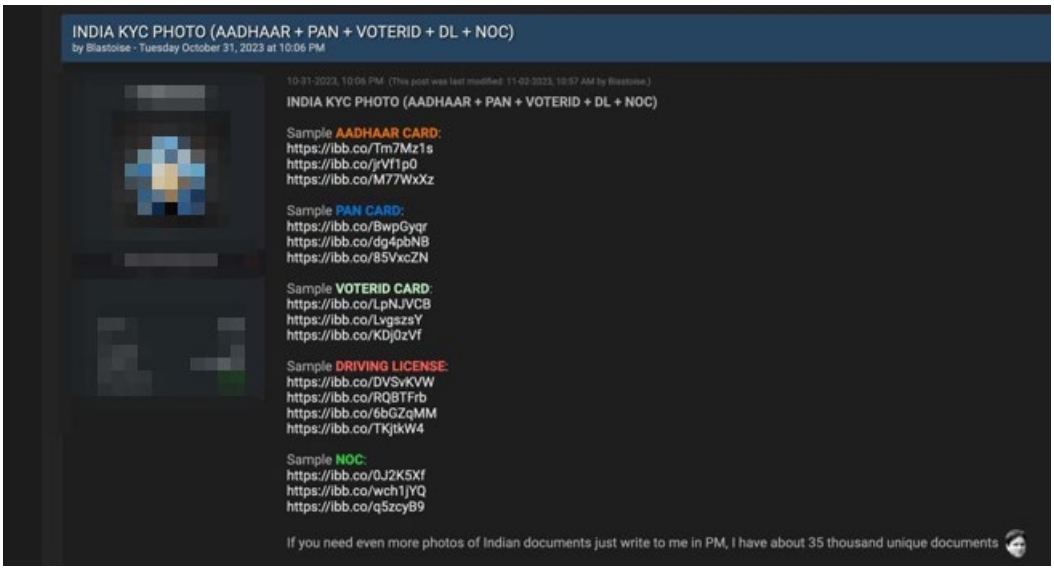
```
ID_FUNCIONARIO|INTERNO_IFE|CLAVE_ELECTOR|RFC|CURP|NOMBRE|APELLIDO_PATERNO|APELLIDO_MATERNO|GENERO|FECHA_NACIMIENTO|ID_ESTADO_NACIMIEN
TO|ESTADO_CIVIL|PROGRAMA|ID_SISTEMA|ESTATUS_FUNCIONARIO|FECHA_ANTIGUEDAD_SPEN|USUARIO|FECHA_HORA|CORREO_ELECTRONICO1|CORREO_ELECTRONI
CO2|ID_TRATAMIENTO


19|S|RDLPAD66021525H600|ROLA6602152U8|ROLA660215HSLDPD03|Adán|Rodríguez|López|H|15/02/1966|25||A|1|H|01/06/1993|antonio.fernandez|17
/08/2022 18:12:51|adan.rodriguez@ine.mx||4
20|S|MRRTAD6005141 4H500|MORA6005141L0|MORA600514HJCRTD06|Adolfo|Morán|Rito|H|14/05/1960|14||A|1|H|01/02/1991|ddbd.unicom|20/03/2020
19:00:00|adolfo.moran@ine.mx||
21|S|PRCSAD77030915H100|PECA770309MJ8|PECA770309HTLRSD02|Adolfo Antonio|Pérez|Castilla|H|09/03/1977|15||F|1|H|16
/09/2011|cesia.gomez|19/07/2022 15:05:41|adolfo.perez@ine.mx||4
22|S|GLCRAD8305302 1M700|GACA830530UJ4|GACA830530MPLLRD04|Adriana|Galeana|Carrasco|M|30/05/1983|21|C||1|H|01
/09/2014|antonio.fernandez|16/04/2023 20:35:53|adriana.galeanac@ine.mx|jorebabino@hotmail.com|3
23|S|MRPRAD63030214M500|MAPA630302 8Z9|MAPA630302MJCRRD02|Adriana Araceli|Martínez|Pérez|M|02/03/1963|14||F|1|H|28
/11/2001|ddbd.unicom|27/09/2020 19:00:00|adriana.martinez@ine.mx||1
24|S|MLSNAD66072511M100|MESA660725JV9|MESA660725MGTLND04|Adriana|Meléndez|Sánchez|M|25/07/1966|11|S||1|H|01/09/2014|cesia.gomez|07
/03/2022 13:09:24|adriana.melendez@ine.mx|paolacristi2002@hotmail.com|25
25|S|RDRDAD76092109M300|RORA760921000|RORA760921MDFDDD06|Adriana|Rodríguez|Rodríguez|M|21/09/1976|9||F|1|H|16
/10/2008|alejandro.aguila|03/01/2023 10:20:48|adriana.rodriguezr@ine.mx||3
26|S|ARCBAD74111011H500|AECA741110QT8|AECA741110HGTRBD06|Adrián|Arredondo|Cabrera|H|10/11/1974|11||F|1|H|31/01/2000|cintya.meza|07
/04/2020 20:00:00|adrian.arredondo@ine.mx||4
27|S|SLAYAD83100409M100|SAAA831004IL2|SAAA831004MDFLYD08|Adriana|Salazar|Ayala|M|04/10/1983|9|||1|H|01/09/2014|cesia.gomez|22/02/2022
12:35:55|adriana.salazar@ine.mx|adi_axs@hotmail.com|3
28|S|VRRBAD78041509M300|VARA7804156Y2|VARA780415MDFRBD05|Adriana|Vargas|Rubio|M|15/04/1978|9||F|1|H|01/12/2011|rosario.chavez|14
/06/2022 12:31:21|adriana.vargasr@ine.mx||1
29|S|PRCRAD88102220H700|PECA881022UC5|PECA881022HOCRRD06|Adrián Donato|Pérez|Carrillo|H|22/10/1980|20||F|1|H|01
/02/2009|cesia.gomez|28/02/2022 18:00:24|adrian.perez@ine.mx||6
30|S|SRVRAD76070811H600|SUVA760708J2|SUVA760708HGTRRD05|Adrián|Suárez|Vargas|H|08/07/1976|11||F|1|H|16/09/2001|juan.sosar|14/03/2020
18:00:00|adrian.suarez@ine.mx||4
31|S|ALGRAL66052830H300|AAGA660528001|AAGA660528HVZLRG04|Agustín Alejandro|Al
```

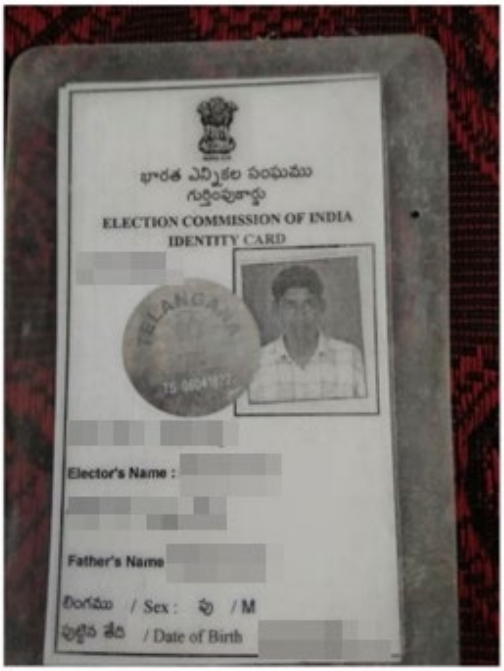
- Anche per Taiwan sono emersi dati e documenti relativi agli elettori venduti dal sito "https://www.wavenet.com.tw"

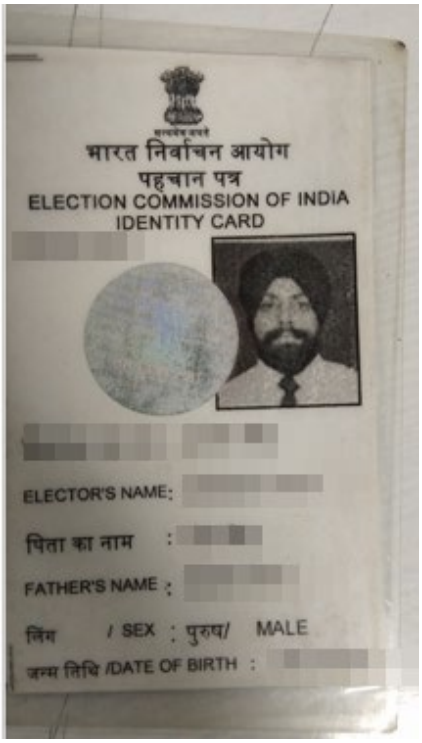


潮網科技股份有限公司社群媒體專案服務報價單						
類別	項目	內容概要	單位	數量	單價	總價（未稅）
社群攻防	臉書	素材擴散（每次擴散至不少於二百個社團，吃到飽）	月	6	200,000	1,200,000
		粉專帶風向（粉專粉絲量不少於一萬，數量不少於二十個，吃到飽）	月	6	400,000	2,400,000
		按讚、留言（帳號數量不少於一千，可根據要求製作留言內容，吃到飽）	月	6	500,000	3,000,000
	PTT	八卦板、政黑板洗板（一個月上限十次）	月	6	200,000	1,200,000
		回文推、噓（回文帳號數量不少於三百，吃到飽）	月	6	400,000	2,400,000
		寫手文章（攻擊、反串、假中立、帳號肉搜，吃到飽）	月	6	500,000	3,000,000
					小計	13,200,000
社群經營	臉書	即時支援、文案產出（吃到飽）	月	6	80,000	480,000
	臉書	即時圖卡製作（吃到飽）	月	6	80,000	480,000
	臉書	即時影片剪輯（一個月上限四次，不含拍攝）	月	6	150,000	900,000
	I G	限時動態製作（吃到飽）	月	6	100,000	600,000
	I G	素材轉換（吃到飽）	月	6	80,000	480,000
	Line@	即時圖卡製作（吃到飽）	月	6	80,000	480,000
	Youtube	頻道維運（吃到飽）	月	6	100,000	600,000
					小計	4,020,000

- La pubblicazione di informazioni sensibili come i documenti di identità (AADHAAR, PAN, VoterID, patente di guida) e NOC su un forum underground comporta rischi significativi per la privacy e la sicurezza degli individui. Questi dati possono essere utilizzati per scopi fraudolenti, come l'identità rubata, la frode finanziaria e l'accesso non autorizzato a servizi e informazioni sensibili. Inoltre, la vendita di tali informazioni può alimentare un mercato nero per il furto di identità e contribuire alla proliferazione di attività criminali. La diffusione di questi documenti durante le elezioni può, come anticipato, minare l'integrità del processo elettorale, consentendo a individui non autorizzati di votare o influenzare le elezioni.





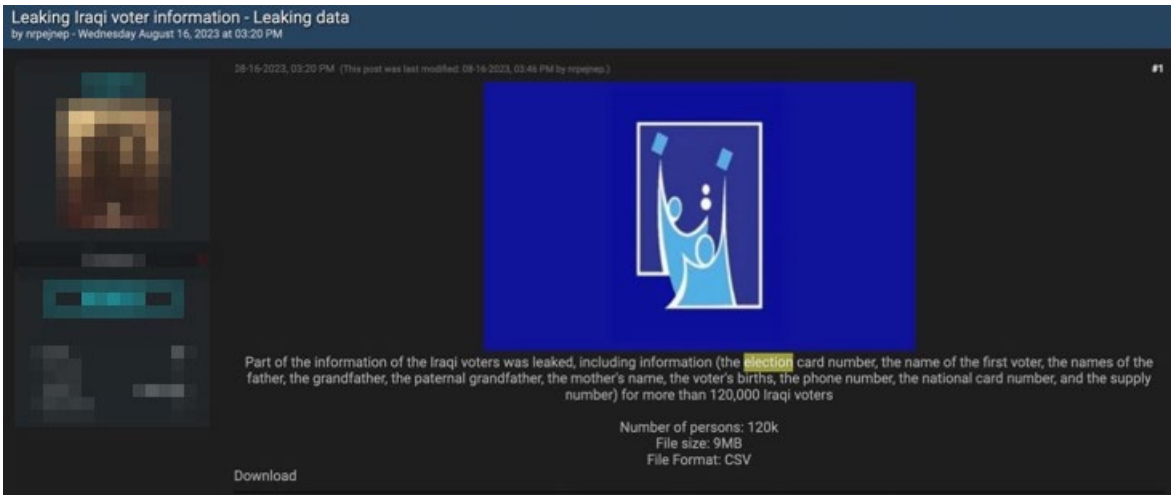


- Altro esempio è la pubblicazione di dati sensibili relativi agli elettori iracheni su forum underground costituisce una grave minaccia per l'integrità delle elezioni e il diritto democratico dei cittadini di esprimere la propria volontà. I dati compromessi includono informazioni personali estremamente sensibili, come numeri di carta d'identità, numeri di

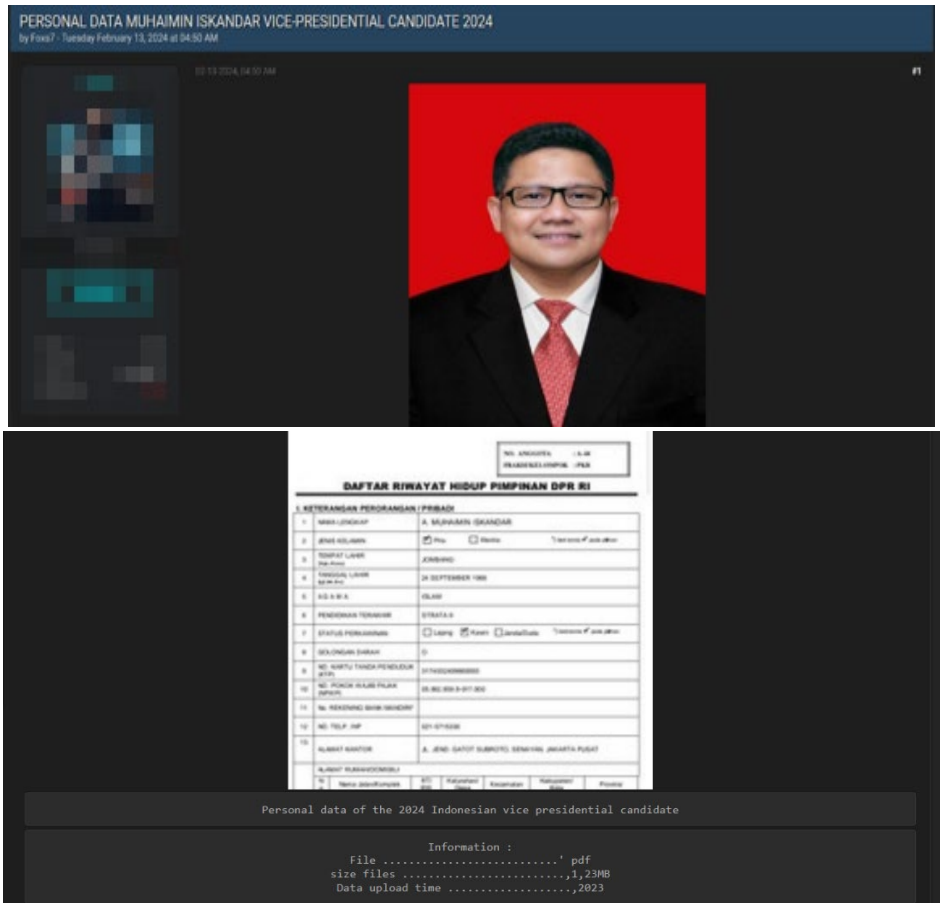
telefono e dati biografici completi, che possono essere utilizzati per scopi fraudolenti e manipolatori durante il processo elettorale

.

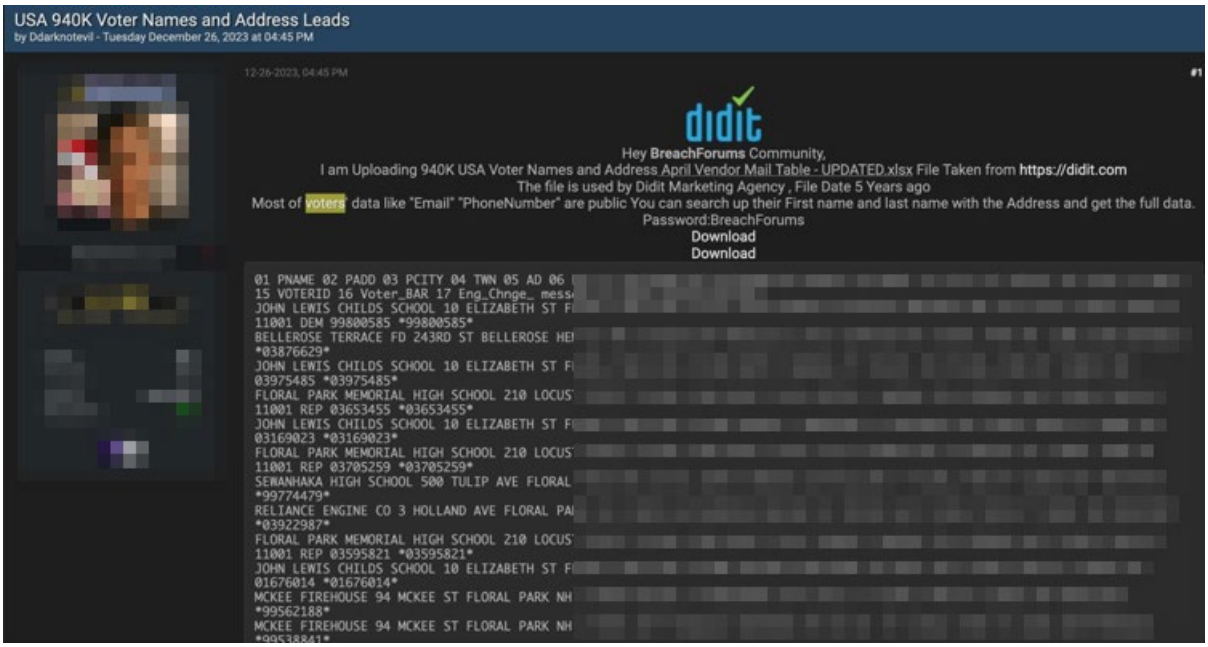
La scala della violazione è estremamente preoccupante, coinvolgendo oltre 120.000 elettori iracheni, per 9GB di file. Questo aumenta il rischio che tali informazioni vengano sfruttate in modo massiccio per influenzare il processo elettorale e minare la fiducia pubblica nell'integrità delle elezioni.



- Di seguito un altro esempio di vendita di informazioni personali relative al vicepresidente dell'Indonesia.

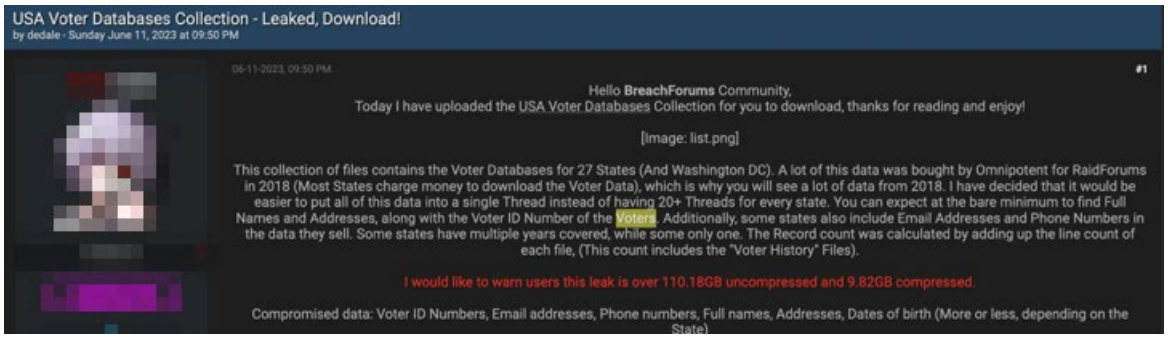


- AMERICA: Inoltre, la pubblicazione di informazioni sensibili relative agli elettori statunitensi su forum sul deep e dark web presenta rischi significativi per la sicurezza nazionale e l'integrità del processo democratico. La violazione riportate di seguito contiene i nomi e gli indirizzi di oltre 940.000 elettori, presumibilmente provenienti da una fonte nota come Didit Marketing Agency, con dati datati di circa cinque anni fa. I dati compromessi includono informazioni sensibili come nomi, indirizzi, numeri di telefono e altri dettagli personali che possono essere utilizzati per scopi fraudolenti. Ad esempio, l'accesso a informazioni come l'appartenenza politica degli individui può essere sfruttato per influenzare le elezioni o per condurre campagne di disinformazione mirate. Inoltre, la disponibilità di dati come indirizzi e numeri di telefono rende gli elettori vulnerabili al phishing, alla truffa e al furto d'identità.



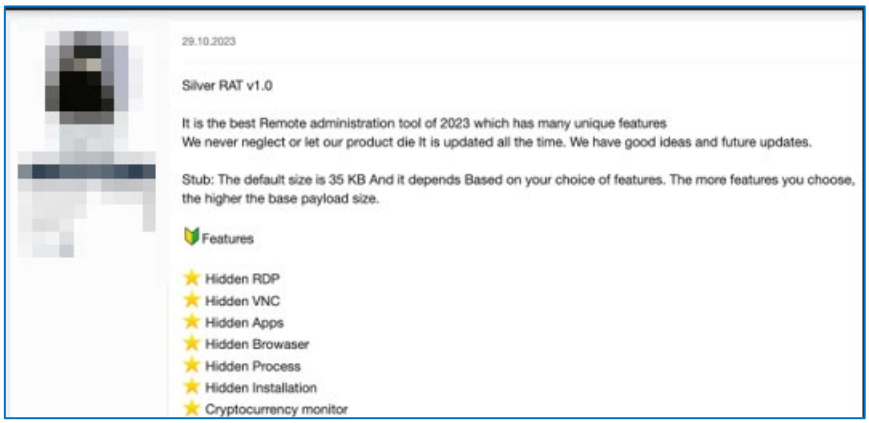
- Anche nel post di seguito è stato pubblicato un annuncio di una raccolta che comprende dati elettorali provenienti da 27 Stati degli Stati Uniti e dal Distretto di Columbia, con alcuni dati che risalgono al 2018.

- Anche in questo caso ci sono informazioni estremamente sensibili come numeri di identificazione degli elettori, indirizzi email, numeri di telefono, nomi completi, indirizzi e, in alcuni casi, date di nascita. La pubblicazione di informazioni così sensibili su forum come BreachForums mette a repentaglio non solo la sicurezza degli individui, ma anche la fiducia nell'integrità delle elezioni e nel sistema democratico nel suo complesso. Gli attori malintenzionati potrebbero sfruttare questi dati per influenzare le elezioni, condurre campagne di disinformazione o mettere a rischio la sicurezza nazionale degli Stati Uniti.



Un altro problema riguarda la diffusione di malware Infostealer nel Deep e Dark Web, dove è possibile acquistarli da chiunque con l'intento di condurre campagne malevole contro gli elettori. Questa situazione presenta diversi rischi rilevanti per l'integrità delle elezioni e per il processo democratico nel suo complesso. Prima di tutto, l'accessibilità ai malware da parte di individui malintenzionati aumenta il rischio di manipolazione delle elezioni attraverso attacchi informatici mirati. Gli aggressori potrebbero utilizzare questi strumenti per compromettere i sistemi informatici legati alle elezioni, influenzare l'opinione pubblica attraverso la diffusione di disinformazione o interferire direttamente con il processo di voto online. Inoltre, l'accesso ai dispositivi compromessi da parte di tali malware consente agli aggressori di estrarre informazioni sensibili sugli elettori.

Due esempi di software InfoStealer con funzionalità di Remote Access Trojan facilmente reperibili su un forum sono DanaBot e Silver RAT. Questi programmi non solo rubano informazioni come fanno gli InfoStealer tradizionali, ma offrono anche un vero e proprio Trojan che consente agli attaccanti di eseguire codice sul dispositivo infetto.



Anche Continental Stealer segue lo stesso modello di vendita. Tuttavia, è interessante notare che in questo caso il prodotto viene commercializzato anche verso utenti meno esperti, evidenziando chiaramente il pericolo rappresentato da questi malware. La facilità d'uso di tali tecnologie aumenta notevolmente il rischio associato alla loro diffusione.

Malware di tipo Infostealer potrebbero dunque essere sfruttati per rubare le credenziali di accesso agli account online, compresi quelli utilizzati dai candidati per le loro campagne elettorali o dagli elettori per accedere a servizi correlati alle elezioni, per intercettare le comunicazioni tra i candidati, i membri del loro staff e gli elettori, consentendo agli aggressori di raccogliere informazioni sensibili o pianificare azioni di interferenza. Allo stesso tempo, gli Infostealer possono anche raccogliere informazioni personali dagli elettori, come dettagli di contatto, indirizzi, informazioni finanziarie e altro ancora, che potrebbero essere utilizzate per influenzare o manipolare il processo elettorale. In aggiunta, il malware potrebbe essere programmato per prendere il controllo degli account social dei candidati e pubblicare contenuti, quali messaggi falsi o diffamatori per danneggiare la reputazione del candidato, o pubblicare informazioni riservate, foto compromettenti o documenti falsificati. Utilizzando i dati raccolti, gli aggressori potrebbero manipolare l'opinione pubblica attraverso campagne di disinformazione mirate, influenzando le decisioni degli elettori o danneggiando la reputazione dei candidati.

In sintesi, l'utilizzo di malware Infostealer non solo minaccia la privacy e la sicurezza degli elettori e dei candidati, ma può anche essere sfruttato per compromettere la legittimità e l'integrità delle elezioni attraverso azioni di defacement e manipolazione dei contenuti online.

Conclusioni

L'ascesa delle fake news durante le elezioni ha posto una sfida significativa per la salute della democrazia e la coesione sociale. Utilizzando una serie di strumenti avanzati come DeepFake / AI, gruppi social, bot e forum underground, gli attori malintenzionati sono in grado di diffondere disinformazione e manipolare l'opinione pubblica in vari modi. Questi strumenti sono stati impiegati per raggiungere diversi obiettivi, tra cui l'influenza economica, la manipolazione dell'opinione pubblica, la diffamazione dei candidati e la promozione del complottismo ed estremismo, tutti obiettivi che riflettono una serie di motivazioni, che vanno dall'ottenere profitti finanziari all'influenzare il risultato delle elezioni e promuovere ideologie estreme.

L'ampia diffusione delle fake news continua a minare la fiducia nelle istituzioni democratiche, danneggiando la reputazione dei candidati e alimentando divisioni e tensioni nella società. Affrontare efficacemente questo fenomeno richiede un impegno collettivo da parte delle istituzioni governative, delle piattaforme online, dei media e dei cittadini stessi.

In risposta alle crescenti preoccupazioni, infatti, diversi attori stanno adottando misure proattive per contrastare questo fenomeno. Tuttavia, nonostante questi sforzi, è chiaro che sono necessarie ulteriori misure per contrastare efficacemente la diffusione di fake news durante le elezioni. Una possibile soluzione potrebbe essere l'introduzione di modifiche legislative, come quelle proposte dal governo indiano per regolare l'intelligenza artificiale e le aziende di AI. Questo potrebbe includere disposizioni specifiche per regolare i deepfake e i contenuti sintetici, insieme a obblighi per le piattaforme di social media per addestrare e verificare i loro modelli di AI.

Infine, è importante promuovere l'educazione mediatica e il pensiero critico tra i cittadini per aiutarli a riconoscere e sfidare la disinformazione durante le elezioni. Le piattaforme di social media devono continuare ad intensificare i loro sforzi per identificare e rimuovere tempestivamente i contenuti falsi e manipolati, garantendo così un ambiente online più sicuro e affidabile durante il periodo elettorale.

Credits

Analysis by:

Riccardo D'Ambrosio
Riccardo Michetti
Martina Fonzo

Technical Contributors:

Soc team Swascan di Tinexta Cyber

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

Milano
+39 0278620700
www.swascan.com
info@swascan.com
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI