MERIDIAN GROUP

Weekly *Report*

13/01/2025

TLP: WHITE

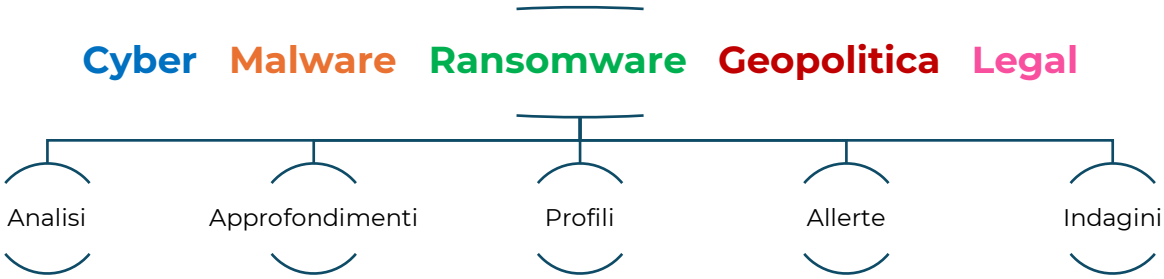
MERIDIAN S.R.L

Viale Erminio Spalla, 9-00142 Roma (RM) | +39 06 99 70 66 80 | P.IVA/CF 13693001003 | meridiangroup@legalmail.it | info@meridian-group.eu | www.meridian-group.eu |

Sommario

Metodologie e Risorse

Il team di *Cyber Intelligence* (CI) utilizza i seguenti metodi e risorse per l'analisi delle notizie e per l'acquisizione di informazioni utili al contenimento degli attacchi informatici.



Il Team di CI, attraverso questo report settimanale, mira a fornire analisi tempestive e accurate riguardo alle aree, di cui sopra, consentendo ai lettori di essere a conoscenza delle ultime notizie riguardanti nuove vulnerabilità, potenziali minacce e cambiamenti nello scenario geopolitico.

L'analisi giornaliera delle notizie sulla piattaforma Kitsune è essenziale per gli analisti di CI al fine di monitorare e comprendere i rischi emergenti nelle diverse categorie, sopra esposte, consentendo così di prevenire o mitigare le potenziali minacce alla sicurezza dei clienti.

GEOPOLITICA

La Russia ordina a Yandex di oscurare mappe e immagini di una raffineria strategica

UNA SENTENZA SENZA PRECEDENTI IMPONE AL COLOSSO TECNOLOGICO DI RIMUOVERE INFORMAZIONI SU UN IMPIANTO PETROLIFERO SENSIBILE, BERSAGLIO DI RIPETUTI ATTACCHI UCRAINI.

Un tribunale russo ha ordinato a Yandex, principale azienda tecnologica del paese, di rimuovere mappe e immagini relative a una delle più grandi raffinerie di petrolio della Russia. La decisione è stata motivata dai ripetuti attacchi di droni ucraini contro l'impianto.

Secondo l'agenzia statale TASS, questa è la prima sentenza che obbliga Yandex a eliminare informazioni su strutture strategiche legate all'industria della difesa. Yandex, spesso chiamata il "Google della Russia," gestisce il motore di ricerca più utilizzato nel paese, oltre a servizi come mappe, email, trasporti e commercio online.

La raffineria non è stata identificata nei documenti ufficiali, ma fonti indipendenti ritengono che si tratti dell'impianto di proprietà statale Rosneft a Ryazan. Durante il conflitto in Ucraina, Rosneft ha fornito materiali alle forze armate russe ed è stata colpita da quattro attacchi ucraini nell'ultimo anno, che hanno causato danni strutturali e ferito dipendenti.

Un'agenzia governativa ha avviato la causa contro Yandex dopo aver riscontrato che mappe e immagini dettagliate della raffineria erano pubblicamente accessibili. Non avendo raggiunto un accordo diretto con Yandex, l'agenzia ha chiesto l'intervento del tribunale.

La sentenza impone a Yandex di rimuovere o oscurare immagini di officine, stazioni di compressione, serbatoi e altre aree sensibili dell'impianto. Il tribunale ha dichiarato che la disponibilità pubblica di queste informazioni "compromette le capacità di difesa nazionale" e "ritarda la consegna dei materiali" alle forze armate. Inoltre, Yandex è stata multata.

Il problema della divulgazione di immagini strategiche riguarda sia la Russia sia l'Ucraina. Lo scorso novembre, l'Ucraina aveva accusato Google di aver esposto i propri siti militari in un aggiornamento delle mappe online. I funzionari ucraini avevano sottolineato i rischi di rivelare informazioni sensibili, come la posizione di sistemi di difesa aerea.

Google Ucraina ha replicato affermando che le immagini satellitari in questione risalivano a oltre un anno prima ed erano già pubblicamente disponibili. "Evitiamo di pubblicare immagini recenti delle zone di conflitto," ha dichiarato l'azienda.

MALWARE

FireScam: il malware Android che si traveste da Telegram Premium per rubare dati sensibili

UN SOFISTICATO ATTACCO INFORMATICO SFRUTTA SITI DI PHISHING E PERMESSI MALEVOLI PER SOTTRARRE CREDENZIALI, MONITORARE ATTIVITÀ E MANTENERE IL CONTROLLO REMOTO SUI DISPOSITIVI INFETTI.

Un sofisticato malware per Android, denominato FireScam, è stato individuato mentre si spacciava per una versione premium dell'app di messaggistica Telegram, con l'obiettivo di sottrarre dati sensibili e mantenere un controllo remoto persistente sui dispositivi infetti. FireScam si diffonde attraverso un sito di phishing ospitato su GitHub.io che imita RuStore, un noto app store russo gestito dal gigante tecnologico VK.

L'attacco inizia con il download di un file APK denominato GetAppsRu.apk, fornito attraverso il sito di phishing rustore-apk.github[.]io. Una volta installato, l'APK funge da "dropper," ossia un veicolo per consegnare il payload principale, progettato per sottrarre dati sensibili come notifiche, messaggi e altre informazioni app, inviandoli a un endpoint su Firebase Realtime Database.

L'app dropper richiede numerose autorizzazioni, tra cui la scrittura su memoria esterna e la possibilità di installare, aggiornare o eliminare app su dispositivi Android 8 o versioni successive. In particolare, sfrutta il permesso ENFORCE_UPDATE_OWNERSHIP, che consente di designare l'app come proprietaria degli aggiornamenti, bloccando così eventuali aggiornamenti legittimi provenienti da altre fonti e garantendo la persistenza del malware sul dispositivo.

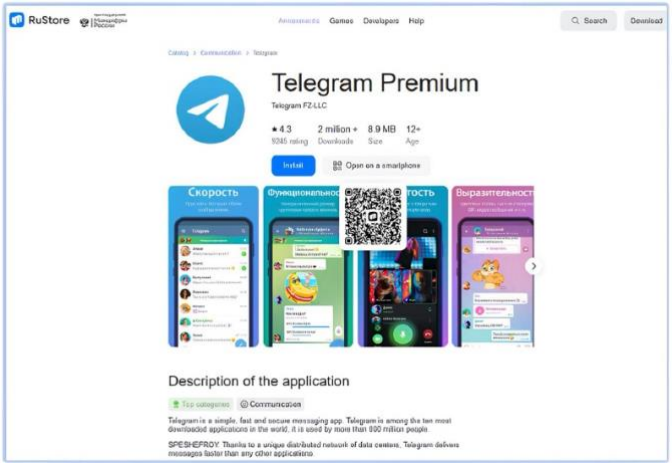


Figura 1 - Falsa app Telegram

FireScam utilizza metodi di offuscamento e anti-analisi per evitare il rilevamento. Una volta installato, monitora notifiche, attività dell'utente, contenuti della clipboard e transazioni di e-commerce, raccogliendo dati di interesse. È anche in grado di scaricare e analizzare immagini da URL specifici.

Quando l'app "Telegram Premium" viene lanciata, il malware richiede ulteriori permessi per accedere a contatti, registri delle chiamate e messaggi SMS. Successivamente, visualizza una pagina di login del sito ufficiale di Telegram tramite un WebView per sottrarre le credenziali dell'utente, avviando il processo di raccolta dati indipendentemente dal fatto che la vittima esegua l'accesso o meno.

Il malware registra, inoltre, un servizio per ricevere notifiche da Firebase Cloud Messaging (FCM), consentendo agli operatori di inviare comandi remoti e mantenere un accesso occulto al dispositivo. In parallelo, stabilisce una connessione WebSocket con un server di comando e controllo (C2) per esfiltrare dati e coordinare attività successive.

Infine, il dominio di phishing ospitava anche un altro artefatto dannoso chiamato CDEK, probabilmente riferito a un servizio russo di tracciamento pacchi e spedizioni. Tuttavia, la società non è riuscita ad analizzare questo componente al momento dell'indagine.

Non è ancora chiaro chi siano gli operatori di FireScam, come gli utenti vengano indirizzati a tali siti o se vengano utilizzate tecniche di phishing via SMS o campagne di malvertising.

CYBER

Nuova campagna di phishing a tema iCloud

EMAIL FRAUDOLENTE PROMETTONO SPAZIO DI ARCHIVIAZIONE GRATUITO PER INDURRE LE VITTIME A FORNIRE INFORMAZIONI PERSONALI E DETTAGLI DELLE CARTE DI CREDITO.

È stata recentemente individuata una sofisticata campagna di phishing avente come tema il servizio iCloud, mirata all'acquisizione fraudolenta di informazioni personali delle potenziali vittime, inclusi i dati delle carte di credito. Tale campagna, veicolata tramite email, persuade gli utenti a riscuotere un presunto premio, consistente nell'ottenimento gratuito di spazio di archiviazione aggiuntivo sul servizio Apple iCloud.

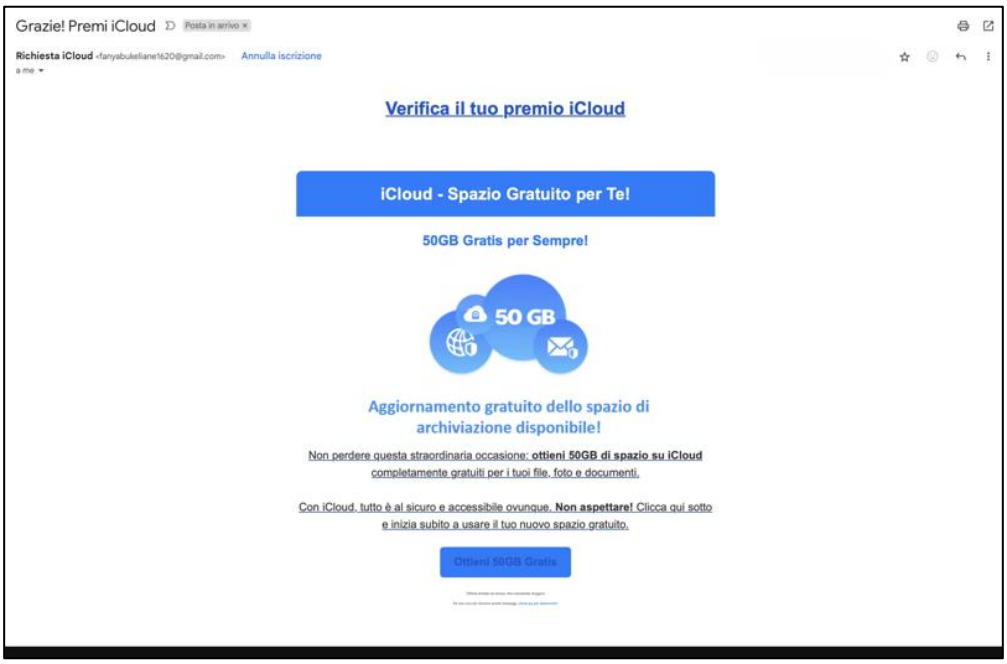


Figura 2 - Mail di phishing

Il collegamento ipertestuale presente nell'email conduce l'utente a un portale appositamente predisposto, in cui è enfatizzata la possibilità di acquisire 50 GB di spazio aggiuntivo al costo di soli 2 euro annui – un'incongruenza evidente rispetto a quanto dichiarato nel corpo della comunicazione.

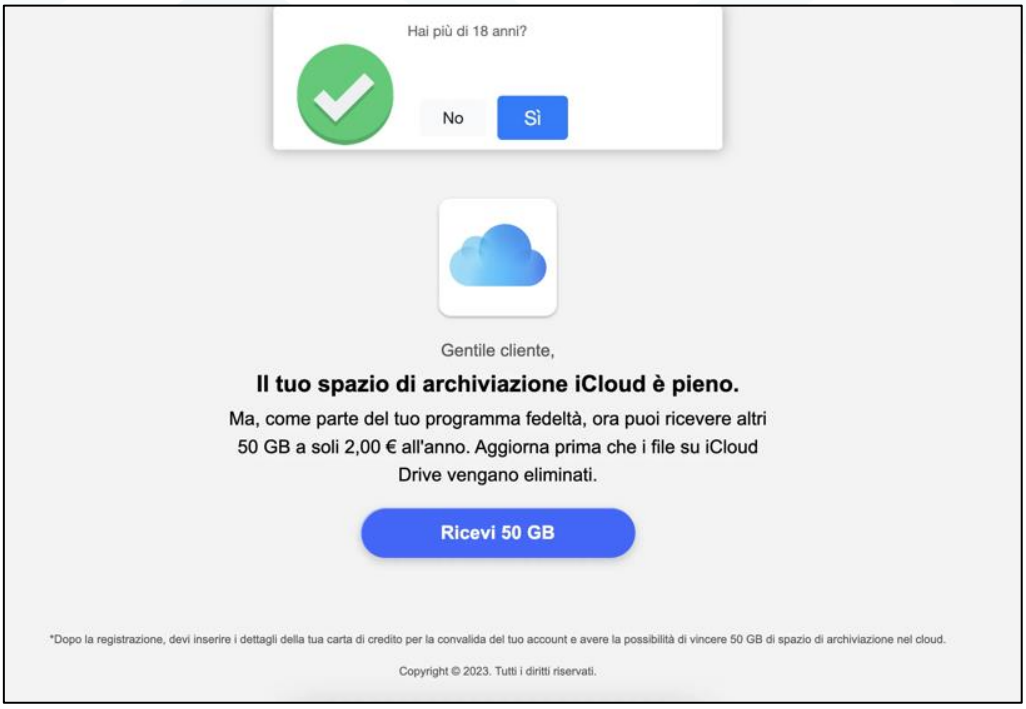


Figura 3 - Landing page di phishing

Cliccando sul pulsante "Ricevi 50 GB", la vittima è indotta a fornire informazioni sensibili, tra cui dati personali e dettagli relativi alla propria carta di credito, in modalità analoghe a quelle descritte nell'ambito della segnalazione AL01/250103/CSIRT-ITA.

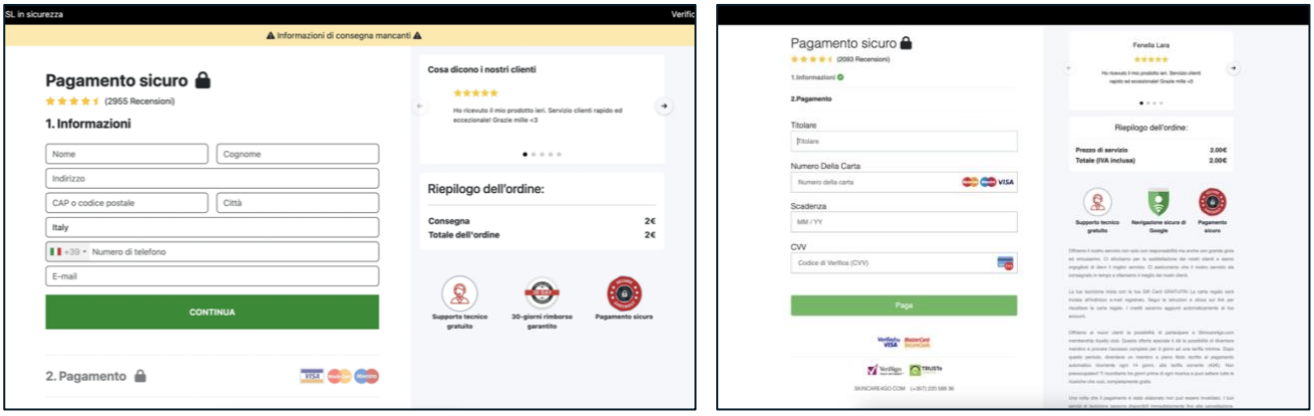


Figura 4 - Richiesta di inserimento dati e carta di credito

Successivamente, qualora i dati vengano inseriti, il sito fraudolento mostrerà una schermata che simula il fallimento del pagamento, accompagnata da un messaggio esplicativo sulle presunte cause della transazione non riuscita. In tale schermata è altresì presente una chat di supporto, gestita tramite un bot. Interagendo con questa funzionalità, il sistema

richiederà una descrizione del problema riscontrato, esortando poi la vittima a utilizzare ulteriori carte di pagamento e indirizzandola verso portali di pagamento alternativi appositamente allestiti per perpetrare la truffa.

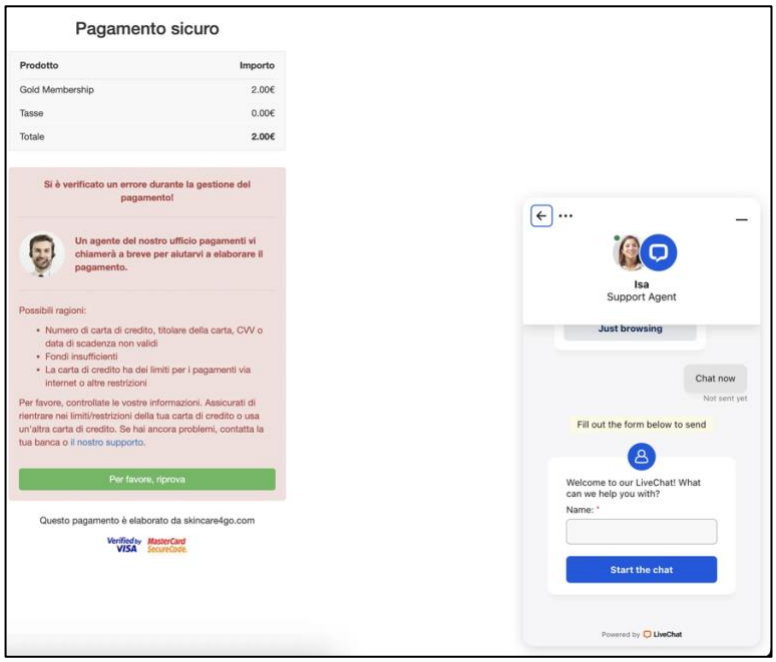


Figura 5 - Pagamento non riuscito e chat bot

GEOPOLITICA

Cresce l'alleanza tra Russia e Corea del Nord: rischio di scambio di tecnologie militari avanzate

MOSCA POTREBBE FORNIRE A PYONGYANG TECNOLOGIE SATELLITARI E SPAZIALI IN CAMBIO DI TRUPPE E ARMAMENTI, MENTRE AUMENTANO I TIMORI PER UNA POSSIBILE APPROVAZIONE DEL PROGRAMMA NUCLEARE NORDCOREANO.

La Russia potrebbe presto condividere tecnologie satellitari avanzate con la Corea del Nord, dopo che quest'ultima ha inviato truppe per sostenere l'offensiva di Mosca in Ucraina. Lo ha dichiarato il Segretario di Stato americano Antony Blinken lunedì 6 gennaio.

"La Corea del Nord sta già ricevendo equipaggiamenti militari e addestramento dalla Russia. Ora crediamo che Mosca voglia condividere tecnologie spaziali e satellitari avanzate con Pyongyang"

Blinken si trova in Corea del Sud per l'ultimo tour diplomatico prima dell'insediamento del presidente eletto Donald Trump. Le sue parole arrivano mentre la Corea del Nord ha testato un missile balistico di medio raggio, che si è schiantato nelle acque al largo della costa orientale della penisola coreana, secondo le autorità sudcoreane. Il Segretario di Stato ha anche avvertito che la Russia potrebbe accettare il programma nucleare della Corea del Nord, abbandonando il suo storico impegno per la denuclearizzazione della penisola coreana.

Gli Stati Uniti hanno espresso preoccupazione per l'alleanza sempre più stretta tra Pyongyang e Mosca. Nel giugno scorso, Putin e Kim Jong Un hanno firmato un importante accordo di difesa. La visita di Putin in Corea del Nord è stata vista come un tentativo di assicurarsi il sostegno di Kim, in un momento in cui la Russia fatica a rifornire le sue scorte di armi e subisce gravi perdite in Ucraina. Da allora, munizioni e missili sarebbero stati trasferiti dalla Corea del Nord alla Russia, sebbene entrambe le nazioni neghino tali scambi. Secondo fonti ucraine e occidentali, anche soldati nordcoreani stanno combattendo al fianco della Russia. Si teme inoltre che Mosca stia violando le sanzioni internazionali per aiutare la Corea del Nord a sviluppare il suo programma satellitare militare.

Inoltre, il Ministro della Difesa sudcoreano, Kim Yong Hyun, ha riferito che la Corea del Nord sta chiedendo alla Russia tecnologie per armi nucleari tattiche, missili balistici intercontinentali, satelliti di ricognizione e sottomarini nucleari, in cambio di supporto militare sul campo.

CYBER LEGAL

Google sotto accusa: violazione della privacy e raccolta dati senza consenso

UN GIUDICE DI SAN FRANCISCO HA APPROVATO UNA CLASS ACTION CONTRO GOOGLE PER PRESUNTA RACCOLTA NON AUTORIZZATA DI DATI PERSONALI, EVIDENZIANDO AMBIGUITÀ NELLE SUE INFORMATIVE. IL PROCESSO DEL 2025 POTREBBE AVERE IMPORTANTI CONSEGUENZE PER L'INDUSTRIA TECNOLOGICA.

Un giudice federale di San Francisco ha stabilito che Google dovrà affrontare una class action legale relativa alla presunta raccolta non autorizzata di dati personali dagli smartphone degli utenti, anche quando la funzione di tracciamento della posizione è disattivata. Il giudice capo Richard Seeborg ha respinto il tentativo dell'azienda di archiviare il caso, aprendo la strada a un possibile processo con giuria programmato per il 18 agosto 2025.

I querelanti sostengono che, nonostante le dichiarazioni pubbliche dell'azienda secondo cui gli utenti potevano disattivare il tracciamento della posizione, Google avrebbe continuato a registrare la cronologia di navigazione e le attività in background. Questo comportamento rappresenterebbe una violazione delle aspettative ragionevoli di privacy degli utenti, aggravata dal fatto che Google avrebbe deliberatamente oscurato queste pratiche nelle sue informative sulla privacy. La causa fa riferimento in particolare al California Invasion of Privacy Act (CIPA) e ad altre normative statali che proibiscono la raccolta di dati personali senza autorizzazione esplicita.

Dal canto suo, Google ha sostenuto che le sue pratiche di raccolta dati sono conformi alla legge e che gli utenti erano adeguatamente informati attraverso le sue informative sulla privacy. Inoltre, l'azienda ha affermato che la raccolta di dati serviva a migliorare i servizi offerti, come le raccomandazioni personalizzate e le mappe in tempo reale, e ha sottolineato

che i querelanti non avrebbero dimostrato danni concreti derivanti da queste pratiche. Tuttavia, il giudice Seeborg ha respinto queste argomentazioni, sottolineando che le informative sulla privacy di Google potrebbero essere interpretate come ambigue e fuorvianti da un utente medio. Secondo il giudice, un utente ragionevole potrebbe considerare "altamente offensiva" la raccolta di dati personali effettuata senza consenso esplicito o in violazione delle dichiarazioni dell'azienda.

La decisione di Seeborg apre la strada a un processo che potrebbe avere implicazioni significative non solo per Google, ma per l'intera industria tecnologica. Negli ultimi anni, la società è stata coinvolta in numerose controversie legali legate alla privacy, tra cui una class action relativa al tracciamento degli utenti nella modalità "Incognito" del browser Chrome. Le accuse contro Google si inseriscono in un contesto più ampio di crescente attenzione verso le pratiche di raccolta dati delle grandi aziende tecnologiche, spinto anche dall'entrata in vigore di normative come il California Consumer Privacy Act (CCPA). Queste leggi stanno spingendo le aziende a rivedere le loro politiche per evitare sanzioni finanziarie e danni reputazionali.

Il processo programmato per il 2025 potrebbe rappresentare un punto di svolta, con la possibilità di stabilire un precedente importante per le future cause sulla privacy. Se i querelanti riuscissero a dimostrare che Google ha violato sistematicamente i diritti di privacy degli utenti, l'azienda potrebbe essere costretta a pagare danni significativi e a modificare profondamente le sue politiche di tracciamento. Inoltre, una sentenza sfavorevole potrebbe avere ripercussioni ben oltre i confini della California, influenzando la regolamentazione della privacy a livello nazionale e internazionale.

CYBER LEGAL

Il Tribunale UE crea un precedente: sanzionata la Commissione per dati personali

IL TRIBUNALE UE HA CONDANNATO LA COMMISSIONE EUROPEA PER VIOLAZIONE DEL GDPR, ORDINANDOLE UN RISARCIMENTO DI 400 EURO PER UN TRASFERIMENTO ILLECITO DI DATI A META. LA SENTENZA RIBADISCE CHE ANCHE LE ISTITUZIONI UE DEVONO RISPETTARE PIENAMENTE LE NORME SULLA PROTEZIONE DEI DATI.

Per la prima volta nella storia, il Tribunale Generale dell'Unione Europea ha stabilito che la Commissione Europea ha violato le proprie leggi sulla protezione dei dati, ordinandole di risarcire un cittadino tedesco con una somma di 400 euro. Questo caso rappresenta un passo significativo nel rafforzamento della protezione dei dati e del principio di responsabilità anche per le istituzioni europee.

La vicenda nasce dall'utilizzo della funzione "Accedi con Facebook" da parte della Commissione Europea su una delle sue piattaforme. Un cittadino tedesco aveva utilizzato questa opzione per registrarsi a una conferenza organizzata dall'UE. Tuttavia, l'impiego di questa funzione ha comportato il trasferimento dell'indirizzo IP dell'utente a Meta Platforms, l'azienda madre di Facebook, con sede negli Stati Uniti.

Questo trasferimento è avvenuto senza adeguate garanzie per la protezione dei dati personali dell'utente, una chiara violazione del Regolamento Generale sulla Protezione dei Dati (GDPR). L'utente ha deciso di portare la questione davanti al Tribunale Generale dell'Unione Europea, sostenendo che la Commissione non aveva rispettato le norme che essa stessa è chiamata a far applicare.

Il GDPR, entrato in vigore nel 2018, è considerato uno dei quadri normativi più rigorosi al mondo in materia di protezione dei dati personali. La sua applicazione è obbligatoria per tutte le istituzioni, gli Stati membri e le aziende che operano all'interno dell'Unione Europea. Alcuni dei principi fondamentali del GDPR includono: la limitazione delle finalità, secondo cui i dati personali possono essere raccolti solo per finalità specifiche e chiaramente definite; la minimizzazione dei dati, che prevede la raccolta solo delle informazioni strettamente necessarie; e la regolamentazione dei trasferimenti transfrontalieri, che vieta lo spostamento dei dati al di fuori dello Spazio Economico Europeo senza garanzie adeguate, come le clausole contrattuali standard.

Nel caso specifico, la Commissione Europea non ha implementato misure adeguate per garantire che il trasferimento dei dati a Meta Platforms fosse conforme a questi principi. La decisione del tribunale sottolinea che anche le istituzioni europee devono rispettare pienamente il GDPR.

La sentenza rappresenta un doppio precedente. Da un lato, conferma che il GDPR è applicabile anche alle istituzioni dell'UE, incluse la Commissione Europea e le sue agenzie. Dall'altro, ribadisce l'importanza di garantire che i dati personali dei cittadini europei siano protetti quando vengono trasferiti verso paesi terzi.

Il tribunale ha ritenuto che la violazione fosse relativamente limitata, come dimostrato dal risarcimento di soli 400 euro, ma ha comunque sottolineato la necessità di maggiore diligenza da parte delle istituzioni europee. Inoltre, questa decisione potrebbe incoraggiare altri cittadini a intraprendere azioni legali in caso di violazioni simili.

La sentenza del Tribunale Generale arriva in un contesto di crescente attenzione alla protezione dei dati personali e ai trasferimenti transfrontalieri di informazioni. La Corte di Giustizia dell'UE aveva già stabilito, con la decisione Schrems II del 2020, che il Privacy Shield – un accordo che regolava il trasferimento di dati tra UE e USA – non offriva sufficienti garanzie per la privacy degli utenti europei.

Questo caso rafforza l'idea che le istituzioni europee devono essere modelli di conformità alle leggi che esse stesse promuovono. Per prevenire futuri problemi legali, è probabile che la Commissione e altre istituzioni rivedano i loro processi interni per garantire una piena adesione al GDPR.

La multa inflitta alla Commissione Europea rappresenta un momento cruciale nel rafforzamento del regime legale sulla protezione dei dati personali nell'Unione Europea. La sentenza non solo garantisce una maggiore tutela per i cittadini, ma invia anche un messaggio chiaro: nessuno, neanche le istituzioni più alte dell'UE, è al di sopra della legge.

CYBER GEOPOLITICA

Elon Musk, l'AfD e le preoccupazioni europee: interferenze politiche e regolamentazione digitale

LA DIRETTA DI ELON MUSK SU X CON IL LEADER DELL'ESTREMA DESTRA TEDESCA ACCENDE IL DIBATTITO SU INTERFERENZE ELETTORALI, BIG TECH E L'URGENZA DI UNA RISPOSTA UE ATTRAVERSO IL DIGITAL SERVICES ACT

La decisione di Elon Musk, imprenditore statunitense e proprietario della piattaforma X, di ospitare Alice Weidel, leader del partito di estrema destra tedesco Alternative für Deutschland (AfD), in una diretta prevista per il 10 gennaio, ha acceso un acceso dibattito in Germania e nell'Unione Europea. Questo evento, che si inserisce in un contesto politico delicato con le elezioni parlamentari tedesche programmate per il 23 febbraio, sta sollevando preoccupazioni su possibili interferenze elettorali e sul ruolo delle grandi piattaforme digitali nella politica europea.

L'AfD, classificato come partito estremista di destra dai servizi di sicurezza tedeschi, è noto per le sue posizioni anti-immigrazione e anti-islamiche. Recentemente, ha visto una crescita nei sondaggi, raggiungendo il 21,5% delle preferenze e posizionandosi al secondo posto dietro ai conservatori. Musk, che ha apertamente lodato le politiche economiche del partito, è accusato di legittimare l'AfD e di rimuovere parte dello stigma che lo circonda. Le sue azioni, insieme alle sue dichiarazioni critiche nei confronti del cancelliere Olaf Scholz e del presidente Frank-Walter Steinmeier, hanno ulteriormente polarizzato il dibattito politico.

Figura 6 - Alice Weidel, co-leader del partito Alternative für Deutschland (AfD)

La diretta con Weidel sarà attentamente monitorata dalle autorità tedesche e dalla Commissione Europea, che valuteranno eventuali violazioni del Digital Services Act (DSA) e delle norme sul finanziamento delle campagne elettorali. Il DSA, progettato per bilanciare libertà di espressione e prevenzione di incitamenti all'odio o interferenze politiche, potrebbe diventare il fulcro delle risposte europee alle attività di Musk.

Figura 7 - Il CEO di tesla e proprietario della piattaforma social media X, Elon Musk

Nel frattempo, Francia e Spagna hanno chiesto all'UE di adottare un approccio più deciso contro le interferenze politiche. Il ministro degli Esteri francese, Jean-Noel Barrot, ha esortato la Commissione a rafforzare l'applicazione del DSA, mentre il primo ministro spagnolo Pedro Sanchez ha accusato Musk di minare la democrazia europea. Le dichiarazioni di Musk a favore di partiti populisti e le sue critiche ai leader europei, tra cui anche il primo ministro britannico Keir Starmer, hanno sollevato interrogativi sul confine tra libertà di espressione e influenza indebita

La Commissione Europea, pur ribadendo che Musk è libero di esprimersi, ha sottolineato che ogni attività deve rispettare i limiti legali. Una riunione del consiglio direttivo del DSA, prevista per il 24 gennaio, esaminerà le possibili risposte a questi sviluppi, cercando di garantire un equilibrio tra trasparenza, regolamentazione delle piattaforme digitali e tutela del processo democratico in Europa.

L'evento del 10 gennaio rappresenta quindi un banco di prova cruciale per la politica tedesca, il ruolo delle big tech e la capacità dell'UE di difendere la propria integrità elettorale in un'epoca di crescenti influenze esterne.

CYBER

CERT-AGID: supporto al formato ClamAV nel flusso IoC

UNA NUOVA FUNZIONALITÀ PER MIGLIORARE LA SICUREZZA INFORMATICA, RISPONDENDO ALLE ESIGENZE DELLA COMUNITÀ ACCADEMICA E ISTITUZIONALE.

A partire da oggi, il Flusso IoC del CERT-AGID offre il supporto al formato ClamAV, il celebre antivirus open source ampiamente utilizzato in ambiti accademici, istituzionali e aziendali. Questa nuova funzionalità è stata implementata per rispondere a una richiesta specifica della comunità dei sistemisti degli Atenei del GARR, che aveva sottolineato la necessità di arricchire il flusso già disponibile con un formato aggiuntivo, caratterizzato da personalizzabilità e semplicità d'uso, al fine di innalzare il livello di sicurezza dei sistemi gestiti.

Grazie a questa integrazione, è possibile utilizzare in modo diretto gli indicatori di compromissione (IoC) diramati dal CERT-AGID per rilevare file sospetti sui sistemi protetti da ClamAV. La gestione delle firme, inoltre, avviene in maniera trasparente e con un alto grado di flessibilità, come dettagliato nella relativa documentazione tecnica. Le pubbliche amministrazioni già accreditate al Flusso IoC possono beneficiare immediatamente del nuovo formato per ClamAV, semplicemente aggiungendo il parametro `type=clamav` all'URL ricevuto: *<URL_ricevuto>&type=clamav*

Il servizio fornirà un elenco in formato testuale conforme al modello `.hsb` utilizzato da ClamAV, omettendo la dimensione del file e sostituendola con il carattere jolly `*`. Per garantire una piena compatibilità retroattiva, il livello funzionale minimo richiesto è stato fissato alla versione 73 di ClamAV.

```
9a510395868bb9ffe02004ef6010738facba10ab65da2d70f6719a430537c525:*:FormBook:73
d97e22f94b96aa4eddbe315fe64f8379:*:Lumma:73
8dd9c8238f9a2da51c476fa09c68e8cf1316422c:*:Rhadamanthys:73
33162044ddd087dc5636406f8efa9ed9d3bb636b9f66f78a452235aae4ecce42:*:Irata:73
153635d66bd01a944dcd4661cec41896:*:KoiStealer:73
4be7ce58752d3d6c689441487d24933166c3decc:*:AsyncRat:73
81abb1776a5da5c7844a18f50a4f254eed232c6164b62e2a5fd69d4494c4b943:*:njRAT:73
a462535dd4c7d80f9b474eb2a67117563a9fcc8d73fc0592b7753fdf4191f758:*:FormBook:73
79a2a731aea9ede92ef449b25e910647:*:AgentTesla:73
ba889042212f5499eaac3dc6ed5862df:*:FormBook:73
34a8890e4998418150c23488eae537640fa236f0:*:Remcos:73
b21c95ebf34440ad8da30f6e4fe25badb871d61a:*:Rhadamanthys:73
116887b2ac34a05784dca6f2cac7cc03:*:Rhadamanthys:73
02c53e42858c9c99b5aef5552972954f26885209f9bf30b825403433ff28e513:*:Rhadamanthys:73
215ff81b6f3a50e48d9f5acfb89f5ea3a1afd59dddbb0666f7ce97a922f60326:*:KoiStealer:73
654c0c7e931356faa0396f064994dc50:*:FormBook:73
a99182cf7c27dda2a192598210339eb96f0612a6:*:Rhadamanthys:73
dc767ae22ec2c3aa37aac0fb59b96ea54eeb08d5:*:AsyncRat:73
dbcdba774b5330c06fde116ef1d1184f307d65ca:*:Rhadamanthys:73
0826938525ff0f4f400488819d1e7dc7:*:SpyNote:73
23f0f232c72231ee39a7df5d87bc1721:*:Rhadamanthys:73
4d63883ce64474b643f30b2e3e3876710a92a861c52a1a452c4d86955d1b5f1e:*:FormBook:73
31f30a8b7270e00247b64c28cab661f23660c398d0da80b953e6587d58e4a429:*:FormBook:73
755fb54225dd285b06c369a2f5e58082:*:Remcos:73
2079cc699607e1946c94d546ecf70609:*:Rhadamanthys:73
df7ffd20940c227dac2b37a2646e819cad5a52dd:*:Rhadamanthys:73
c16e7b591755e996a4fafb382453c7c8cfafc966:*:Rhadamanthys:73
95865bf569deef3fa8a68a642cf078e1572a03d4:*:QnodeService:73
517ec3bee4730f2b57b1e5d576d0f92749c32d6678ac7695670c7c2b4d86ae06:*:Lumma:73
ff82fd4a86eb8c8b36ff276a0078d6e1dd981b1b:*:Irata:73
e3439125d29714a7c9f8f4e8a36c2d0ffc4d5acd926589a4caf255c2b808758a:*:Rhadamanthys:73
```

Figura 8 - Esempio di Flusso IoC formato ClamAV

CYBER GEOPOLITICA

La sfida americana su TikTok: tra sicurezza nazionale e libertà digitale

LA PROPOSTA DI FRANK MCCOURT E IL DIBATTITO SUI RISCHI PER LA PRIVACY E LA LIBERTÀ DI ESPRESSIONE NEGLI STATI UNITI

TikTok si trova al centro di una complessa battaglia legale e politica negli Stati Uniti, con implicazioni che toccano la sicurezza nazionale, la libertà di espressione e il controllo del mercato tecnologico. Il consorzio guidato dall'imprenditore Frank McCourt, ex proprietario dei Los Angeles Dodgers, ha avanzato una proposta per acquisire le attività statunitensi della piattaforma di proprietà cinese ByteDance. Il termine ultimo per la vendita è fissato al 19 gennaio, in base a una legge firmata dal presidente

Joe Biden lo scorso aprile. Senza un accordo, TikTok rischia il divieto negli Stati Uniti. Il consorzio ha dichiarato di avere il sostegno di importanti investitori e banche statunitensi per completare l'acquisizione, con l'obiettivo di mantenere la piattaforma operativa senza l'attuale algoritmo e scongiurare un divieto. McCourt ha sottolineato l'intenzione di collaborare con ByteDance, il presidente eletto Donald Trump e la nuova amministrazione per garantire un accordo

vantaggioso. Nel frattempo, il destino di TikTok è oggetto di una disputa davanti alla Corte Suprema, che deve decidere se la legge che impone la vendita della piattaforma violi il Primo Emendamento sulla libertà di espressione. Il Dipartimento di Giustizia sostiene che TikTok rappresenta una minaccia per la sicurezza nazionale, citando il rischio che la Cina possa accedere ai dati sensibili degli utenti statunitensi o manipolare i contenuti diffusi sulla piattaforma. TikTok e ByteDance respingono queste accuse, definendo la legge un attacco alla libertà di parola. Il caso ha diviso l'amministrazione statunitense e il Congresso. Mentre molti repubblicani sostengono la necessità di limitare l'influenza cinese, il presidente eletto Trump ha chiesto una sospensione del divieto, definendo TikTok uno strumento importante per la comunicazione. Questo segna un'inversione rispetto al suo primo mandato, quando cercò di vietare la piattaforma. Il dibattito su TikTok si inserisce in un contesto di crescenti tensioni tra Stati Uniti e Cina e solleva questioni di principio sul futuro della libertà digitale e sulla regolamentazione delle piattaforme social. La decisione della Corte Suprema potrebbe avere ripercussioni significative, non solo per TikTok ma anche per altre app con legami internazionali, delineando il confine tra libertà di espressione e sicurezza nazionale.

GEOPOLITICA

Crisi in Venezuela: Maria Corina Machado arrestata e rilasciata durante le proteste contro Maduro

ONDATA DI MANIFESTAZIONI IN TUTTO IL PAESE, REPRESSIONE GOVERNATIVA E ACCUSE DI FRODE ELETTORALE SEGNANO L'OPPOSIZIONE AL TERZO INSEDIAMENTO DEL PRESIDENTE NICOLAS MADURO

Maria Corina Machado, leader dell'opposizione venezuelana, è stata arrestata e successivamente rilasciata giovedì 9 gennaio dopo essere stata coinvolta in una protesta a Caracas segnata da tensioni e spari. Il suo arresto, avvenuto durante un'ondata di manifestazioni in tutto il Paese contro il presidente Nicolas Maduro in vista del suo terzo insediamento, ha sollevato condanne da parte di alleati politici e governi stranieri. Machado, durante la detenzione, è stata costretta a registrare video e ha annunciato che fornirà ulteriori dettagli.

Figura 9 - Maria Corina Machado, leader dell'opposizione venezuelana durante la protesta prima dell'insediamento di Nicolas Maduro

L'opposizione accusa Maduro di frode elettorale e di repressione sistematica, con arresti di leader politici e attivisti, mentre il governo difende la legittimità delle elezioni e accusa i dissidenti di complotti. Edmundo Gonzalez, candidato presidenziale dell'opposizione, è stato riconosciuto da molti come il "vero vincitore" delle elezioni e ha ricevuto sostegno internazionale, ma rischia l'arresto se torna in Venezuela.

Le proteste, diffuse in tutto il Paese e represse duramente, hanno coinvolto migliaia di persone, mentre il governo ha organizzato contromanifestazioni. In diverse città, le forze di sicurezza hanno disperso i manifestanti con gas lacrimogeni e arresti. Anche i venezuelani all'estero si sono mobilitati in solidarietà. Il clima di tensione riflette una profonda crisi politica, sociale ed economica che affligge il Venezuela sotto il regime di Maduro, sostenuto dall'esercito e dai servizi segreti.

CYBER LEGAL

Scandalo all'ICAO: divulgazione non autorizzata di informazioni sul reclutamento

L'ICAO, AGENZIA DELLE NAZIONI UNITE, INDAGA SU UNA FUGA DI DATI PERSONALI LEGATI AL RECLUTAMENTO, CON IMPLICAZIONI LEGALI E REPUTAZIONALI. L'ORGANIZZAZIONE COLLABORA CON AUTORITÀ INTERNAZIONALI E ADOTTA MISURE PER RAFFORZARE LA SICUREZZA INFORMATICA E PREVENIRE NUOVI INCIDENTI.

L'Organizzazione Internazionale dell'Aviazione Civile (ICAO), un'agenzia delle Nazioni Unite con sede a Montreal, sta attualmente indagando su una presunta fuga di dati sensibili relativi al reclutamento del personale. Secondo fonti vicine alla questione, l'indagine è incentrata sulla possibile divulgazione non autorizzata di informazioni personali dei candidati, che potrebbero includere dati identificativi, esperienze professionali e altre informazioni riservate raccolte durante il processo di selezione.

La presunta violazione dei dati personali solleva questioni giuridiche rilevanti, in particolare in relazione alle normative internazionali sulla protezione dei dati. In questo contesto, l'ICAO, pur essendo un'agenzia delle Nazioni Unite, deve garantire la conformità alle normative in vigore, come il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea, laddove i dati dei cittadini europei siano coinvolti, e altre leggi nazionali o regionali applicabili.

La fuga di dati potrebbe comportare una responsabilità legale per l'ICAO, considerando che l'agenzia ha l'obbligo, sia etico sia giuridico, di proteggere i dati personali raccolti e trattati. Inoltre, se la violazione fosse attribuibile a negligenze o a una mancata implementazione di adeguate misure di sicurezza, ciò potrebbe aggravare la responsabilità dell'organizzazione. Le conseguenze potrebbero includere possibili sanzioni amministrative, a seconda della giurisdizione applicabile, nonché rimedi per le vittime, che potrebbero intraprendere azioni legali per ottenere risarcimenti, specialmente se la fuga di informazioni ha causato danni materiali o morali. Anche gli impatti reputazionali e diplomatici potrebbero essere significativi, considerando che l'ICAO opera sotto il controllo e la supervisione di diversi Stati membri, i quali potrebbero richiedere maggiore trasparenza e interventi per evitare futuri incidenti.

L'ICAO ha dichiarato di aver avviato un'indagine interna per stabilire l'entità della violazione, le cause e identificare i responsabili. L'organizzazione ha sottolineato che, qualora emergessero responsabilità individuali, potrebbero essere adottate misure disciplinari severe, in linea con i regolamenti interni e le convenzioni internazionali. Inoltre, l'ICAO ha

precisato di aver già informato le autorità competenti nei paesi interessati, facilitando una collaborazione transnazionale per affrontare eventuali questioni legali.

Sebbene l'ICAO goda di un certo grado di immunità diplomatica come agenzia delle Nazioni Unite, tale status non esime l'organizzazione dal dover rispettare i principi internazionali di protezione dei dati. Inoltre, potrebbe essere necessaria una revisione delle politiche interne per allinearsi agli standard di sicurezza informatica più recenti e garantire un trattamento equo dei dati personali.

Per evitare il ripetersi di tali incidenti, l'ICAO ha annunciato l'intenzione di implementare una serie di misure preventive, tra cui il rafforzamento delle infrastrutture di sicurezza informatica, la revisione dei protocolli per il trattamento e la conservazione dei dati personali, l'introduzione di corsi di formazione obbligatori per il personale su come gestire informazioni sensibili in conformità alle leggi internazionali e la collaborazione con esperti legali e tecnici per sviluppare linee guida aggiornate e monitorare costantemente l'efficacia delle nuove politiche.

L'agenzia si è inoltre impegnata a garantire una comunicazione trasparente e regolare con i candidati, i dipendenti e le parti interessate, fornendo aggiornamenti tempestivi sull'indagine in corso e sulle misure adottate.

Questa vicenda rappresenta un richiamo significativo per le organizzazioni internazionali riguardo all'importanza cruciale della protezione dei dati e del rispetto delle normative globali, evidenziando come anche strutture di alto profilo siano vulnerabili a tali incidenti.