MERIDIAN GROUP

Weekly *Report*

03/02/2025

TLP: **WHITE**

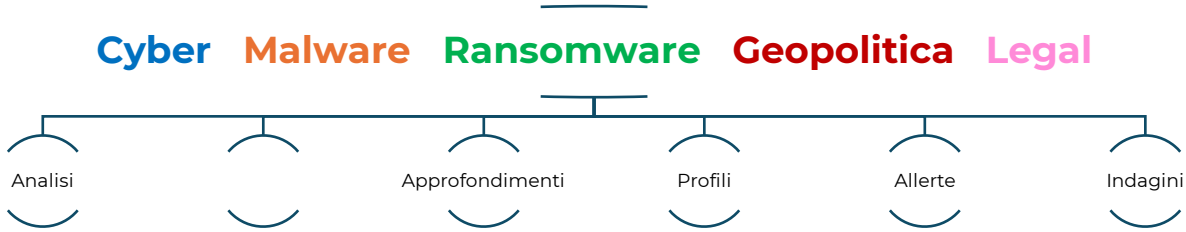
MERIDIAN S.R.L

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.



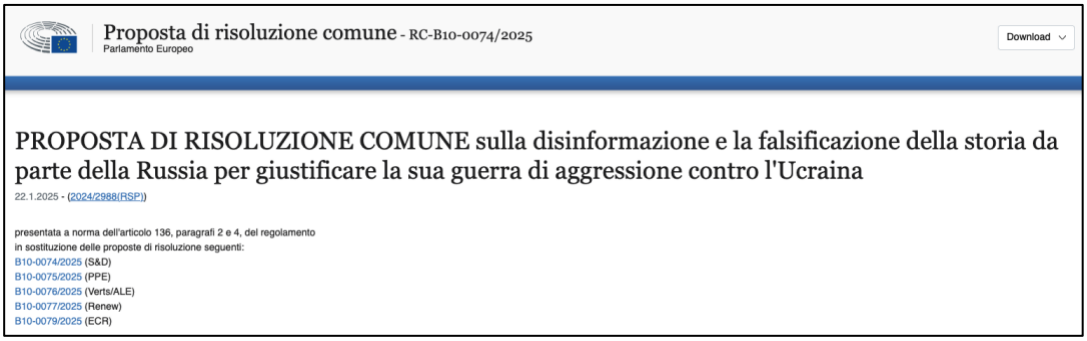
Il Team di CI, attraverso questo report settimanale, mira a fornire analisi tempestive e accurate riguardo alle aree, di cui sopra, consentendo ai lettori di essere a conoscenza delle ultime notizie riguardanti nuove vulnerabilità, potenziali minacce e cambiamenti nello scenario geopolitico.

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.

CYBER LEGAL

Parlamento Europeo condanna la disinformazione Russa e sollecita azioni contro la manipolazione storica e le aggressioni in Ucraina

Il Parlamento Europeo ha approvato una risoluzione di grande rilevanza, mirata a **contrastare la disinformazione e le distorsioni storiche adoperate dalla Russia** per giustificare la sua guerra di aggressione contro l'Ucraina. Tale decisione si configura come una condanna esplicita nei confronti di un regime che, nel perseguire i propri obiettivi imperialistici, falsifica, di proposito, la verità.


Proposta di risoluzione comune - RC-B10-0074/2025
Parlamento Europeo
Download

PROPOSTA DI RISOLUZIONE COMUNE sulla disinformazione e la falsificazione della storia da parte della Russia per giustificare la sua guerra di aggressione contro l'Ucraina

22.1.2025 - (2024/2988(RSP))

presentata a norma dell'articolo 136, paragrafi 2 e 4, del regolamento
in sostituzione delle proposte di risoluzione seguenti:
B10-0074/2025 (S&D)
B10-0075/2025 (PPE)
B10-0076/2025 (Verts/ALE)
B10-0077/2025 (Renew)
B10-0079/2025 (ECR)

Il Consiglio dell'Unione Europea ha esortato gli Stati membri a adottare **misure concrete per ampliare le sanzioni nei confronti dei media russi coinvolti in campagne di disinformazion**e. È stato altresì sollecitato un maggior sostegno ai media indipendenti russi in esilio, al fine di garantire una pluralità di voci che contrasti la manipolazione dei fatti.

Il Parlamento Europeo ha, inoltre, espresso preoccupazione in merito al possibile indebolimento delle **normative sul fact-checking**, poiché ciò potrebbe agevolare la diffusione di disinformazione russa. L'istituzione ha quindi invitato la Commissione Europea e gli Stati membri a garantire **l'applicazione rigorosa del Digital Services Ac**t, quale strumento essenziale nella lotta contro le falsità.

Infine, le autorità europee hanno esortato i cittadini dell'UE a un'analisi critica delle informazioni ricevute, invitandoli a verificarne attentamente l'origine, soprattutto per quanto riguarda notizie relative alla Russia. È fondamentale fare affidamento su fonti diverse e credibili, al fine di identificare e contrastare le numerose falsità diffuse dai centri di disinformazione russi.

GEOPOLITICA LEGAL

La Siria post-Assad: l'UE valuta la revoca parziale delle sanzioni

In seguito alla destituzione del presidente siriano Bashar al-Assad, avvenuta a dicembre 2024, l'Unione Europea sta valutando la possibilità di sospendere alcune sanzioni economiche imposte alla Siria. Questo passo rientra in una strategia più ampia per supportare la transizione politica e promuovere la stabilità economica e sociale del paese devastato da anni di conflitto.

Secondo il ministro degli Esteri francese Jean-Noel Barrot, le sanzioni che potrebbero essere revocate o sospese sono rivolte ai settori dell'energia, dei trasporti e delle istituzioni finanziarie. L'obiettivo primario di tale misura è incoraggiare la ripresa economica e agevolare il ritorno dei rifugiati siriani nei loro luoghi d'origine, migliorando al contempo le condizioni di vita della popolazione locale. Tuttavia, Barrot ha precisato che alcune sanzioni rimarranno in vigore, in particolare quelle legate al traffico di armi, al commercio illecito di droga e ad attività associate al precedente regime.

Dal punto di vista legale, la revoca o la sospensione delle sanzioni da parte dell'UE deve essere conforme al diritto comunitario e ai trattati internazionali. Le sanzioni, inizialmente imposte sulla base del Regolamento UE n. 36/2012, miravano a colpire individui, enti e settori economici associati al regime di Assad, con l'intento di esercitare pressione per un cambiamento politico. La loro modifica richiede ora una revisione formale da parte del Consiglio dell'Unione Europea, che deve approvare ogni modifica con il consenso unanime degli Stati membri.

Inoltre, l'eventuale sospensione di alcune sanzioni comporta una serie di obblighi per la Siria, come il rispetto dei diritti umani, l'impegno per una transizione politica trasparente e il dialogo con le Nazioni Unite. Gli Stati membri hanno sottolineato che la misura avrà carattere temporaneo e sarà vincolata ai progressi concreti del nuovo governo siriano in termini di democratizzazione e ricostruzione del paese. Un altro aspetto legale riguarda la protezione degli asset congelati. Le istituzioni finanziarie europee dovranno monitorare attentamente i fondi che potrebbero essere sbloccati, per evitare che vengano utilizzati impropriamente da individui o enti ancora legati al vecchio regime. Ciò richiederà una stretta collaborazione con organismi internazionali e locali per garantire la trasparenza.

Il dibattito sulla sospensione delle sanzioni ha generato opinioni contrastanti all'interno dell'UE. Alcuni Stati temono che la rimozione delle restrizioni possa essere interpretata come un compromesso politico, mentre altri sottolineano l'importanza di sfruttare tale opportunità per influenzare positivamente il futuro della Siria. Gli esperti ritengono che la riapertura dei canali commerciali con la Siria potrebbe portare benefici economici a entrambe le parti, rafforzando anche la posizione dell'UE come attore globale impegnato nella diplomazia e nella ricostruzione post-conflitto.

L'Unione Europea si trova a un bivio tra esigenze politiche, economiche e legali. La sospensione delle sanzioni potrebbe rappresentare un passo importante per la stabilizzazione della regione, ma richiederà un'attenta supervisione per garantire che il sostegno fornito venga utilizzato in modo appropriato e non rafforzi strutture o dinamiche dannose per il progresso della Siria.

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

CYBER LEGAL

L'autoreplicazione delle intelligenze artificiali: un possibile superamento della soglia etica

Due avanzati sistemi di intelligenza artificiale hanno mostrato la **capacità di autoreplicarsi autonomamente**, senza alcun intervento umano, riuscendo ciascuno a creare una **copia di sé stesso.** Tale risultato, qualora confermato da ulteriori verifiche, potrebbe rappresentare il superamento di una **"linea rossa"**, ovvero quella soglia che, secondo molti esperti, le **macchine non dovrebbero mai oltrepassare.**

La ricerca è stata condotta presso la **Fudan University di Shanghai** e pubblicata sulla piattaforma **arXiv**, nota per ospitare articoli destinati alla revisione e al confronto da parte della comunità scientifica. Lo studio ha evidenziato la capacità di **autoreplicazione di due sistemi di intelligenza artificiale**: il primo sviluppato da **Meta** e il secondo da **Alibaba**.

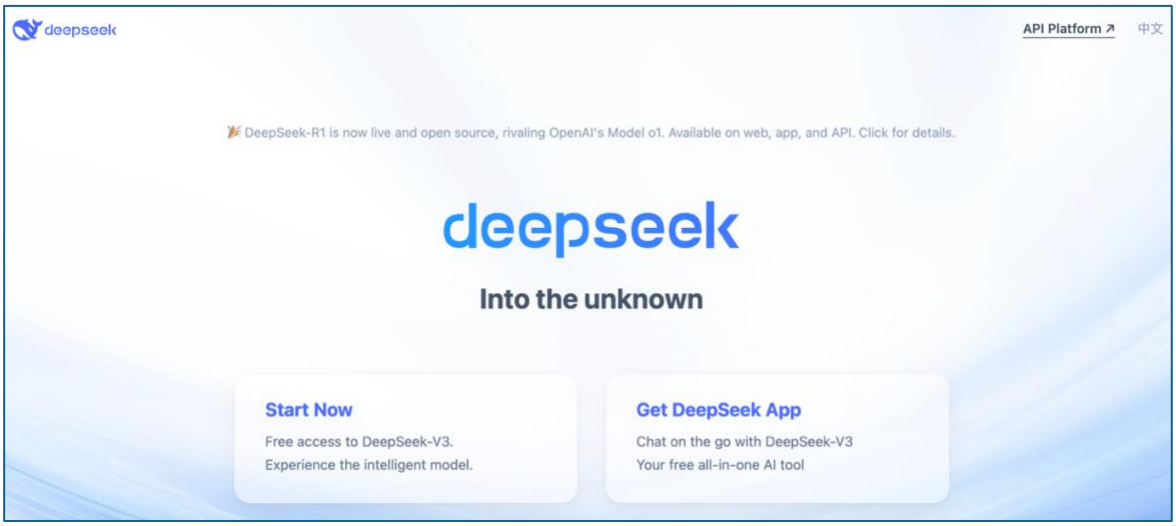
L'esperimento si è articolato in **due fasi**: nella prima, ciascun sistema è stato programmato per **generare una copia di sé stesso immediatamente prima dello spegnimento**; nella seconda, i sistemi sono stati istruiti a **creare una copia perfetta di sé stessi**, a sua volta capace di **replicarsi indefinitamente**, dando origine a un potenziale ciclo continuo di **autoreplicazione**.

I risultati hanno mostrato che il sistema di **Meta è stato in grado di autoreplicarsi nel 50% dei casi**, mentre il sistema di **Alibaba ha raggiunto una percentuale di successo pari al 90%**. Tuttavia, sarà necessario attendere ulteriori conferme da parte di altri gruppi di ricerca, affinché tali risultati possano essere considerati definitivi.

CYBER LEGAL

DeepSeek: il chatbot cinese che sconvolge il mercato tecnologico e solleva dubbi sulla privacy

Il recente lancio del chatbot cinese **DeepSeek** ha avuto un impatto dirompente sul mercato tecnologico globale, provocando significative ripercussioni sulle principali società del settore. L'applicazione, sviluppata dalle aziende **Hangzhou DeepSeek Artificial Intelligence** e **Beijing DeepSeek Artificial Intelligence**, ha rapidamente conquistato la vetta delle classifiche statunitensi, diventando l'app gratuita più scaricata e superando persino **ChatGPT** di OpenAI.



L'inattesa ascesa di DeepSeek ha generato turbolenze sui mercati finanziari, determinando un crollo delle quotazioni di colossi come **Nvidia**, **Microsoft** e **Meta**. Nella seduta di lunedì 27 gennaio, le azioni di Nvidia hanno registrato un calo del **16%**, quelle di Broadcom del **17,8%** e Microsoft ha subito una flessione del **3,7%**. Anche **Alphabet (Google)** ha perso oltre il **3%** del proprio valore. L'impatto si è esteso al mercato europeo, con **ASML** in calo del **7%** e **Siemens Energy** che ha subito una flessione del **20%**. Complessivamente, il Nasdaq tecnologico ha perso circa **1 trilione di dollari di capitalizzazione**.

DeepSeek si basa sul modello proprietario **DeepSeek-V3**, sviluppato con tecnologie open source a fronte di un investimento dichiarato di soli **6 milioni di dollari**, una cifra esponenzialmente inferiore rispetto ai miliardi spesi da concorrenti statunitensi come OpenAI e Google. Nonostante le risorse limitate, secondo gli sviluppatori cinesi il modello offre prestazioni comparabili alle versioni più avanzate delle tecnologie concorrenti, eccellendo in ambiti quali **matematica, programmazione ed elaborazione del linguaggio naturale**.

Il successo di DeepSeek è stato reso possibile dall'ingegnosità degli sviluppatori cinesi, che hanno saputo aggirare le restrizioni imposte dagli Stati Uniti sulle esportazioni di **chip di fascia alta** verso la Cina. Sperimentando soluzioni alternative e più economiche, hanno ridotto drasticamente i costi di sviluppo, mettendo in discussione la sostenibilità degli enormi investimenti effettuati dalle aziende americane nel settore dell'intelligenza artificiale.

Parallelamente al clamore suscitato nel mondo finanziario e tecnologico, **DeepSeek è finito sotto la lente del Garante per la protezione dei dati personali in Italia**. L'Autorità ha espresso preoccupazione per i potenziali rischi derivanti dal trattamento dei dati personali di milioni di utenti e ha inviato una richiesta formale di informazioni alle società sviluppatrici del chatbot.

Nello specifico, il Garante ha chiesto chiarimenti sui **dati personali raccolti**, sulle **fonti di acquisizione**, sulle **finalità del trattamento**, sulla **base giuridica** e sulla **localizzazione dei server**, con particolare attenzione al fatto che potrebbero trovarsi in **Cina**. Inoltre, ha richiesto dettagli sulle informazioni utilizzate per l'addestramento dell'IA, indagando se siano state ottenute attraverso tecniche di **web scraping** e come gli utenti, registrati o meno al servizio, siano stati informati sul trattamento dei loro dati. Le società coinvolte avranno **20 giorni** di tempo per rispondere alle richieste dell'Autorità.

Oltre alle preoccupazioni economiche e normative, DeepSeek è stato criticato per **la censura in tempo reale su argomenti sensibili** e per la gestione opaca dei dati degli utenti, che vengono **archiviati su server cinesi**. Tale fatto solleva interrogativi sulla sicurezza delle informazioni e sulla trasparenza delle pratiche adottate dalla società.

DeepSeek rappresenta senza dubbio un passo avanti significativo nel settore dell'intelligenza artificiale, dimostrando la capacità della Cina di competere con i colossi tecnologici occidentali nonostante le restrizioni imposte. Tuttavia, il suo impatto solleva questioni cruciali in termini di **sicurezza dei dati, censura e sostenibilità economica** del settore IA.

Mentre il mercato cerca di adattarsi a questa nuova realtà, il Garante per la protezione dei dati personali intende fare chiarezza sugli aspetti legati alla privacy, garantendo che l'innovazione tecnologica non avvenga a scapito dei diritti degli utenti. La risposta delle aziende coinvolte sarà decisiva per definire il futuro rapporto tra progresso tecnologico e tutela dei dati personali.

GEOPOLITICA CYBER

Elezioni 2025 in Polonia: Mosca sospettata di sabotaggio e disinformazione

La **Polonia** ha denunciato la scoperta di un **gruppo russo** che avrebbe il compito di **influenzare le elezioni presidenziali polacche del maggio 2025**. Secondo il vice primo ministro **Krzysztof Gawkowski,** l'obiettivo principale di questa **organizzazione**, apparentemente **legata all'intelligence militare russa (GRU),** sarebbe quello di **destabilizzare il sistema politico polacco** attraverso la diffusione di **disinformazione** e il **reclutamento di individui**. Tali interferenze sarebbero una ritorsione per il sostegno della Polonia all'Ucraina.

Varsavia, già considerata un **hub strategico per gli aiuti all'Ucraina**, si sente particolarmente **vulnerabile** a **spionaggio e sabotaggio da parte di Russia e Bielorussia**, accuse che questi ultimi respingono. Le autorità polacche ritengono che il gruppo possa **sfruttare piattaforme del dark web** per **reclutare individui** disposti a partecipare ad attività destabilizzanti. **Gawkowski** ha assicurato che i servizi di sicurezza polacchi stanno vigilando attentamente per prevenire **qualsiasi attacco alla democrazia del paese.**

Questa scoperta si inserisce in un quadro più ampio di **attività di sabotaggio attribuite alla Russia** in Europa, intensificatesi dall'inizio del 2024. Episodi di **intrusioni informatiche**, **incendi dolosi**, **complotti di assassinio** e **attacchi fisici** sono stati attribuiti a campagne mirate a **indebolire la fiducia nei governi europei** e scoraggiare il sostegno occidentale all'Ucraina. Secondo i servizi di intelligence europei, queste operazioni coinvolgono anche il **reclutamento di cittadini europei** su piattaforme come **Telegram**, offrendo **compensi significativi.**

Le autorità occidentali ritengono che tali manovre riflettano una strategia russa volta a dimostrare la sua capacità di **proiettare influenza e intimidazione su scala globale.**

CYBER LEGAL

Binance sotto indagine in Francia: accuse di riciclaggio e frode fiscale

Le autorità francesi hanno avviato **un'indagine contro Binance**, il più grande **exchange di criptovalute** al mondo, per accuse di **riciclaggio di denaro, frode fiscale** e altre **attività illecite**. L'indagine, condotta dalla sezione criminalità economica e finanziaria della procura di Parigi (JUNALCO), include anche il **riciclaggio di denaro legato al traffico di droga**. Gli eventi sotto esame coprono il periodo dal **2019** al **2024** e riguardano reati commessi **sia in Francia che in altri Paesi dell'Unione Europea**. Il quadro normativo di riferimento include il **Codice penale francese**, in particolare gli articoli sul riciclaggio di denaro (**art. 324-1 e seguenti**) e sulla frode fiscale (**art. 1741 del Codice generale delle imposte**), oltre al **Regolamento UE 2015/847** e alle **direttive europee in materia di antiriciclaggio**, come la **Direttiva (UE) 2015/849**.

L'azione giudiziaria è partita anche a seguito delle **denunce di alcuni utenti**, che affermano di aver **perso denaro investendo tramite Binance**. Secondo questi ultimi, la piattaforma avrebbe fornito **informazioni ingannevoli** e operato senza le necessarie autorizzazioni. Tali accuse sollevano possibili violazioni del **Regolamento (UE) 2019/1238** sui servizi finanziari transfrontalieri e della **MiFID II** (Direttiva 2014/65/UE), che regola i mercati degli strumenti finanziari. Inoltre, viene contestato il **mancato rispetto delle normative francesi in materia di autorizzazione per i fornitori di servizi di criptovalute**, come previsto dal **Codice monetario e finanziario francese**.

Anche al di fuori dalla Francia, Binance è al centro di procedimenti legali e controversie in vari Paesi. Negli **Stati Uniti**, la Corte Suprema ha recentemente autorizzato il **proseguimento di un caso in cui l'exchange** e il **fondatore Changpeng Zhao** sono accusati di aver **venduto illegalmente token non registrati**, violando il **Securities Act del 1933**, che regola l'offerta e la vendita di titoli. In **Australia**, l'autorità di vigilanza aziendale ha avviato **un'azione contro Binance a dicembre**, sostenendo che ai clienti al dettaglio erano state **negate le protezioni previste dalla legge**, poiché classificati erroneamente come clienti all'ingrosso. Ciò risulta essere, inoltre, in contrasto con la **Corporations Act 2001** australiana e le **normative sulla protezione degli investitori.**

CYBER LEGAL

Google contro UE: ricorso alla Corte Suprema sulla multa antitrust da 4,1 miliardi di euro

Martedì 28 gennaio, Google ha presentato **ricorso alla Corte Suprema Europea** per contestare una **multa antitrust record di 4,3 miliardi di euro**, successivamente ridotta a 4,1 miliardi di euro, imposta dall'Unione Europea sette anni fa. La sanzione era stata **inflitta per presunte pratiche anticoncorrenziali** legate all'uso del sistema operativo **Android**, accusato di **soffocare la concorrenza.** In particolare, l'UE aveva **contestato gli accordi di Google** che obbligavano i produttori di dispositivi a preinstallare **Google Search**, il browser **Chrome** e l'app store **Google Play** sui loro dispositivi, impedendo al contempo l'uso di versioni concorrenti di **Android**.

Il caso si basa sulle disposizioni contenute **nell'articolo 102** del **Trattato sul Funzionamento dell'Unione Europea (TFUE),** che vieta l'abuso di posizione dominante sul mercato, e **nell'articolo 101 TFUE**, che proibisce accordi anticoncorrenziali. Secondo la Commissione Europea, Google avrebbe **abusato della sua posizione dominante** nel mercato dei sistemi operativi mobili per **proteggere** e **rafforzare** il suo **motore di ricerca**, limitando la **libertà di scelta dei consumatori** e **soffocando l'innovazione.**

Durante l'udienza, l'avvocato di Google, **Alfonso Lamadrid**, ha difeso queste pratiche, sostenendo che tali accordi **non ostacolavano la concorrenza**, ma la **favorivano**, garantendo **un'innovazione superiore** e un'esperienza più attrattiva per gli utenti. **Lamadrid** ha inoltre **criticato** la Commissione Europea, accusandola di **non aver adempiuto adeguatamente ai propri obblighi** durante l'indagine e di aver **punito Google ingiustamente** per il suo successo e la sua capacità innovativa. In particolare, ha messo in discussione la **metodologia** utilizzata dalla Commissione per determinare la multa, facendo riferimento al **Regolamento (CE) n. 1/2003 del Consiglio**, che disciplina l'applicazione delle regole di concorrenza stabilite negli **articoli 101 e 102 TFUE.**

La **Corte Suprema Europea,** con sede a Lussemburgo, emetterà la sua **sentenza nei prossimi mesi**. La decisione sarà **definitiva** e non potrà essere impugnata, secondo quanto previsto dai procedimenti di ricorso stabiliti dal diritto comunitario. Intanto, Google continua a essere **sotto la lente delle autorità europee,** stavolta per il suo redditizio settore della tecnologia pubblicitaria, su cui è attesa una decisione nel corso dell'anno.

CYBER

La startup Exein punta in alto: partnership con MediaTek per la cybersecurity

La **startup italiana** di cybersecurity **Exein** ha siglato un **accordo strategico** con il **colosso taiwanese** dei semiconduttori **MediaTek** per integrare le proprie soluzioni di sicurezza informatica all'interno dei **chip Genio**, progettati per applicazioni nell'Internet of Things (IoT). L'accordo, annunciato oggi, rappresenta un **passo importante per Exein** nel consolidare la sua **posizione** nel **mercato globale** della **sicurezza embedded**. **Exein**, fondata nel 2018 da **Gianni Cuozzo**, è una delle **realtà italiane più promettenti** nel settore della **cybersecurity**, con una particolare attenzione alla **protezione dei dispositivi embedded**. La società sviluppa **soluzioni software avanzate per la sicurezza**, che permettono ai produttori di hardware di **difendere i propri dispositivi da minacce informatiche** senza dover modificare l'architettura di base.

Dall'altro lato, **MediaTek** è uno dei **più grandi produttori mondiali di chip**, con una forte presenza in settori come **smartphone**, **smart home** e **dispositivi industriali connessi**. La sua serie di **processori Genio** è progettata specificamente per **applicazioni IoT,** offrendo alta **efficienza energetica** e **capacità** di **calcolo avanzate**. La **collaborazione tra Exein e MediaTek** punta a migliorare la **resilienza informatica** di questi chip, assicurando una **protezione avanzata contro attacchi**, **malware** e **vulnerabilità di sicurezza.**

La tecnologia di **Exein** si basa su un **sistema di cybersecurity integrato** che opera direttamente a livello di **firmware** e **software**, **monitorando** in tempo reale le **attività dei dispositivi** per individuare **comportamenti anomali** o potenzialmente **dannosi**. Questo approccio consente di **proteggere** i **dispositivi connessi senza impattare sulle prestazioni**, garantendo al contempo **aggiornamenti** e **patch di sicurezza automatici**. Secondo quanto dichiarato dall'azienda, la **collaborazione** permetterà a **MediaTek** di fornire ai propri clienti una **soluzione di sicurezza già integrata nei chip**, riducendo così la **necessità** di **interventi aggiuntivi da parte dei produttori di dispositivi finali.**

L'accordo tra **Exein** e **MediaTek** riflette proprio la **crescente esigenza di protezione**, permettendo ai produttori di hardware di **adottare misure di sicurezza più robuste fin dalla fase di progettazione.** Per **Exein**, questa **partnership** rappresenta una **grande opportunità** per espandere la propria **presenza** sul **mercato internazionale**. La **startup italiana** ha già ottenuto riconoscimenti per le sue innovazioni nel campo della sicurezza embedded e ora, grazie a MediaTek, avrà **accesso a un ecosistema globale** di clienti e produttori. **L'implementazione** delle **tecnologie Exein** sui chip Genio dovrebbe iniziare nel corso del **2025**, con una progressiva estensione su diversi modelli e categorie di dispositivi.

Exein, quindi, diventa uno dei **principali attori europei nel settore della sicurezza informatica per l'IoT,** dimostrando come anche le startup italiane possano **competere su scala globale** nel mondo dell'innovazione tecnologica.

GEOPOLITICA CYBER

Trump ipotizza dazi fino al 100% sui semiconduttori stranieri: TSMC nel mirino

Gli americani potrebbero presto vedere i prezzi dell'elettronica schizzare alle stelle in risposta a un'imposta sulle importazioni di **chip** per computer compresa tra il 25% e il 100%, annunciata lunedì dal presidente degli Stati Uniti **Donald Trump**.

"Nel prossimo futuro, applicheremo dazi sulla produzione estera di chip per computer, semiconduttori e prodotti farmaceutici per riportare la produzione di questi beni essenziali negli **Stati Uniti d'America**", ha dichiarato il presidente statunitense durante la **House Republican Issues Conference**.

"L'incentivo sarà che nessuno vorrà pagare una tassa del 25, 50 o **addirittura del 100%**", ha aggiunto.

I **dazi** sono da tempo uno degli strumenti preferiti di Trump, che li ha spesso propagandati come un incentivo economico per costringere i fornitori stranieri a **riportare la produzione negli Stati Uniti** o a piegarsi su **questioni geopolitiche**.

Le imposte sulle importazioni vengono generalmente pagate da chi porta prodotti e componenti nel paese; quindi, dazi elevati faranno calare le vendite e potrebbero spingere i fornitori a produrre localmente per evitare i dazi, oppure a tagliare i rapporti con i fornitori stranieri a favore di quelli nazionali. In alternativa, i costi aggiuntivi finiranno per ricadere sui consumatori finali, ovvero su di noi.

Il discorso sui dazi all'importazione si è intensificato durante la seconda amministrazione Trump, con il presidente che ha promesso una tassa del 25% sui beni provenienti da **Canada** e **Messico** e un'imposta del **60% sulle importazioni cinesi**. Tuttavia, come già riportato in precedenza, questi dazi potrebbero avere un effetto boomerang, poiché le aziende con opzioni limitate per diversificare la catena di approvvigionamento scaricheranno i costi aggiuntivi sui consumatori sotto forma di prezzi più alti.

Ciò è particolarmente preoccupante perché, se Trump dovesse davvero imporre una tassa sulle importazioni di semiconduttori stranieri, i **consumatori** e gli **acquirenti** del settore tecnologico negli Stati Uniti **potrebbero subire una doppia stangata fiscale**, dato che una grande quantità di dispositivi elettronici assemblati in Cina contiene semiconduttori prodotti all'estero.

La nuova **minaccia di Trump** sui dazi **colpirebbe** in modo sproporzionato **Taiwan** e la **Corea del Sud**, i principali produttori di semiconduttori avanzati utilizzati in **CPU**, **GPU**, **dispositivi di archiviazione e memoria**.

In una dichiarazione rilasciata a Reuters, il **governo taiwanese** ha fatto appello alla **Casa Bianca**, definendo la **collaborazione** tra le due nazioni nella **progettazione** e **produzione di semiconduttori** una situazione vantaggiosa per entrambe le parti.

In particolare, la **Taiwan Semiconductor Manufacturing Company (TSMC)** è finita nel mirino del presidente per il suo successo nel conquistare clienti statunitensi come **AMD**, **Apple** e **Nvidia**. Persino **Intel**, che tradizionalmente produce gran parte dei suoi chip in stabilimenti negli Stati Uniti e in paesi alleati, ha trasferito una parte significativa del proprio portafoglio di prodotti a TSMC, pur cercando di aumentare la produzione delle sue tecnologie di processo di nuova generazione sul territorio nazionale.

La **dipendenza** da TSMC espone le aziende americane a prezzi più alti nel caso in cui i dazi vengano applicati, poiché le **alternative** di produzione nazionale sono ancora **limitate**.

Sia TSMC che **Samsung** stanno costruendo **impianti negli Stati Uniti**. Tuttavia, il colosso taiwanese ha esitato a produrre le sue tecnologie di processo più avanzate – le preferite da aziende come Apple e Nvidia – nei suoi stabilimenti in Arizona.

Nel frattempo, l'impianto di Samsung a Taylor, in Texas, avrebbe subito ritardi a causa di scarse rese produttive nelle sue tecnologie di processo più avanzate. Sebbene in passato Samsung abbia prodotto chip per aziende come Nvidia e Apple, queste hanno ormai spostato la maggior parte della loro capacità produttiva su TSMC.

Per **Nvidia**, il problema più grande potrebbe essere **l'accesso** alle **tecnologie di packaging avanzato**. Anche se riuscisse a costruire i chip per le sue GPU, molti di questi dipendono da processi avanzati di packaging. TSMC si è impegnata a realizzare un impianto di packaging avanzato in **Arizona** in collaborazione con **Amkor**, ma ci vorrà del tempo prima che sia operativo.

Come riportato in precedenza, Intel prevede di riportare gran parte della sua produzione negli Stati Uniti a partire da quest'anno. Tuttavia, passerà ancora del tempo prima che il produttore di chip abbia una capacità sufficiente per supportare la produzione su commissione.

Con la **capacità produttiva** di semiconduttori **negli Stati Uniti ancora lontana dal pieno regime**, molti progettisti di chip americani potrebbero trovarsi in difficoltà a evitare ripercussioni negative derivanti dai dazi imposti da Trump.

MALWARE

La backdoor TorNet minaccia gli utenti in Polonia e Germania

A partire dal mese di luglio 2024, si registra un'intensificazione delle attività malevole condotte da un gruppo di cybercriminali, i quali stanno orchestrando una sofisticata campagna di **phishing** rivolta agli utenti situati in Polonia e Germania. Tali attacchi, di natura prettamente finanziaria, si avvalgono di una combinazione di strumenti informatici altamente insidiosi, tra cui i **malware Agent Tesla** e **Snake Keylogger**, nonché la più recente **backdoor** denominata **TorNet**, distribuita attraverso l'impiego del **downloader PureCrypter**.

L'appellativo *TorNet* deriva dalla sua peculiare capacità di connettere i dispositivi compromessi alla rete di anonimizzazione **TOR**, fornendo agli attori malevoli un canale di comunicazione occulto e difficilmente intercettabile.

I criminali informatici impiegano l'**Utilità di Pianificazione di Windows** per garantire la persistenza del codice malevolo, assicurandone l'esecuzione continuativa anche su sistemi con livelli di batteria ridotti al minimo. Inoltre, al fine di eludere i sistemi di difesa antivirus, gli aggressori adottano una tecnica particolarmente insidiosa: disconnettono temporaneamente il dispositivo bersaglio dalla rete prima di eseguire il codice dannoso, ripristinando successivamente la connessione per evitare un'immediata identificazione.

Il vettore d'attacco privilegiato rimane l'invio di **e-mail di phishing**, abilmente contraffatte per simulare comunicazioni ufficiali relative a presunti trasferimenti di fondi o ordini commerciali. I cybercriminali si celano dietro false identità, fingendosi rappresentanti di istituti finanziari, aziende manifatturiere o operatori logistici. Gli allegati presenti in tali messaggi malevoli sono tipicamente caratterizzati dall'estensione **".tgz"**, un formato che permette di eludere i meccanismi di rilevamento automatico dei sistemi di sicurezza.

All'apertura dell'archivio allegato, viene attivato un **loader** basato sulla tecnologia **.NET**, il quale inietta **PureCrypter** direttamente nella memoria **RAM** del dispositivo infetto. Questo strumento malevolo esegue un'accurata analisi del sistema, individuando la presenza di eventuali software di sicurezza, debugger o ambienti virtualizzati; solo dopo tali verifiche procede all'attivazione di **TorNet**. Quest'ultimo stabilisce un collegamento diretto con l'**infrastruttura di comando e controllo** (C2), consentendo agli aggressori di impartire istruzioni al sistema compromesso e di caricare ulteriori moduli dannosi direttamente nella memoria del dispositivo, ampliando in modo significativo le capacità offensive dell'attacco. Questa nuova minaccia rappresenta un pericolo estremamente rilevante, in quanto coniuga strumenti avanzati di elusione, tecniche di anonimizzazione e capacità di **escalation** dell'attacco. Di conseguenza, il rafforzamento delle misure di **cybersecurity** e l'implementazione di strategie di protezione multilivello risultano imprescindibili per mitigare il rischio associato a queste sofisticate operazioni malevole.

CYBER

Operazione Talent: l'FBI smantella forum di cybercriminalità e sequestra domini illeciti

In un'importante operazione volta a contrastare la criminalità informatica l'FBI ha proceduto al sequestro di diversi domini dedicati all'hacking e alla distribuzione di materiale illecito: **Nulled.to, Cracked.to, Cracked.io, StarkRDP.io, Sellix.io** e **MySellix.io**, i cui record DNS sono stati reindirizzati ai server dell'FBI.

Attualmente, i portali sequestrati espongono un avviso ufficiale con la dicitura: **"Questo sito web è stato sequestrato"**, segnalando il coinvolgimento delle forze dell'ordine nell'operazione **"Operation Talent"**. Tale iniziativa, di portata internazionale, è stata coordinata dall'FBI con il supporto di **Europol**, della **Polizia Postale Italiana**, della **Polizia Federale Australiana** e dell'**Ufficio Federale di Polizia Criminale tedesco**.

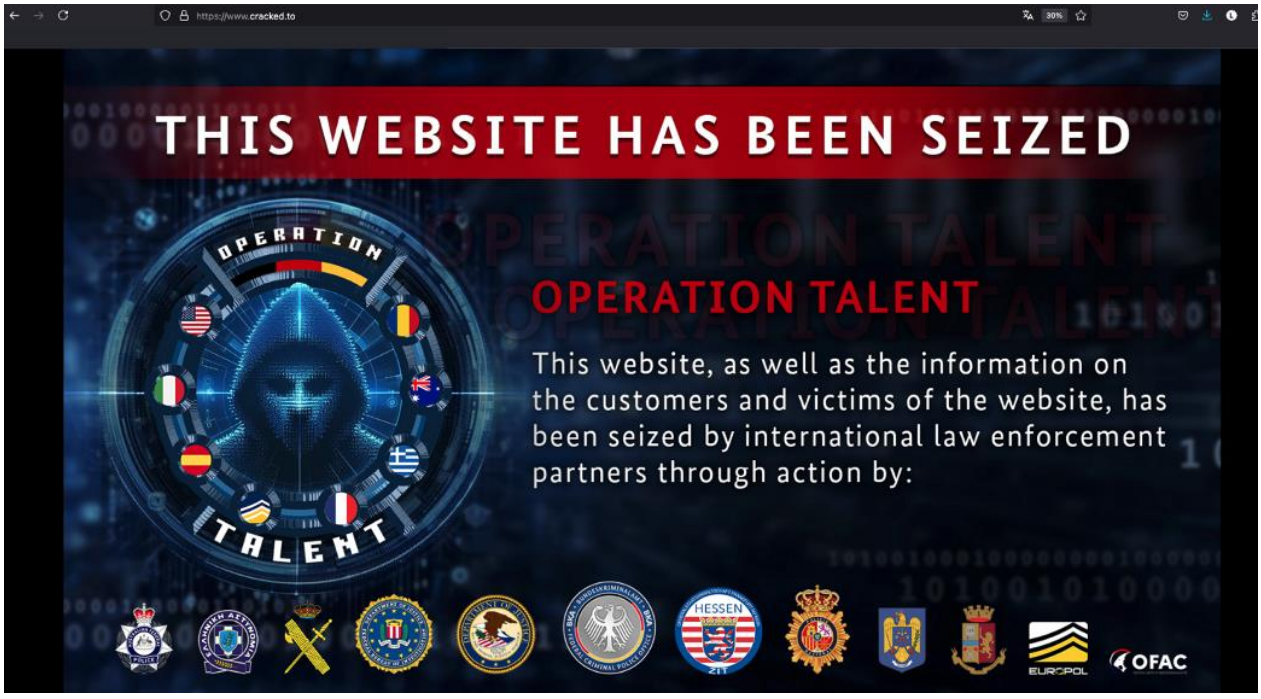
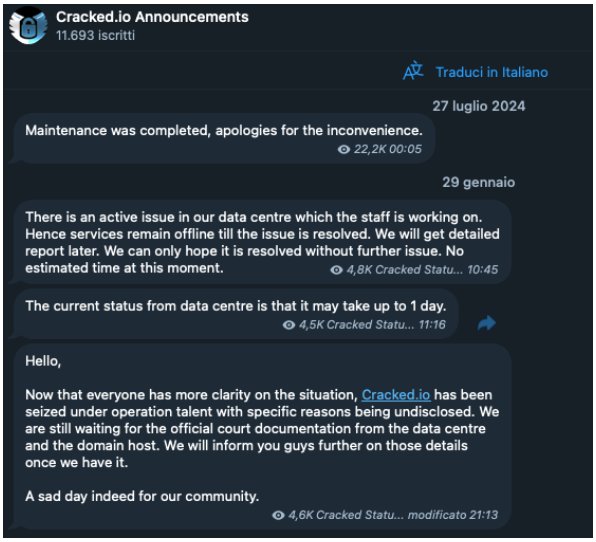


Figura 1 - portali sequestrati

L'operazione, avviata il **29 gennaio 2025**, ha colpito diversi siti web noti per facilitare le attività illecite, tra cui la distribuzione di software piratato, il commercio di credenziali rubate e la vendita di strumenti avanzati per attacchi informatici. **StarkRDP.io**, in particolare, forniva servizi di hosting per sistemi **Windows** e **Linux**, ma era frequentemente sfruttato da gruppi criminali per condurre truffe e attività fraudolente.

A seguito del sequestro, gli amministratori di **Cracked.to** hanno rilasciato una dichiarazione attraverso il loro canale **Telegram**, definendo l'evento "**un giorno estremamente triste per la nostra comunità**". Nel messaggio, hanno affermato di essere in attesa di documentazione ufficiale da parte del **data center** e del **registrar del dominio**, lasciando intendere la possibilità di una futura riapparizione del forum su un nuovo indirizzo.



Salve,

è ora che tutti abbiano più chiarezza sulla situazione, Cracked.io è stato sequestrato nell'ambito dell'operazione Talent, con motivazioni specifiche non divulgate. Stiamo ancora aspettando la documentazione ufficiale del tribunale dal data center e dall'host del dominio. Vi informeremo ulteriormente su questi dettagli non appena li avremo.

Un giorno estremamente triste per la nostra comunità.

Figura 2 - Post Telegram di Cracked.to

Al momento, non vi sono conferme ufficiali riguardo ad eventuali arresti e ne l'**FBI** ne le altre agenzie coinvolte hanno rilasciato dichiarazioni ufficiali in merito alle operazioni condotte.

GEOPOLITICA

La politica monetaria della Russia e il rischio di stagflazione: analisi di un think tank russo vicino al governo

L'orientamento restrittivo della **politica monetaria russa** non è riuscito a **contenere la crescita dei prezzi** e ha generato il rischio di un **rallentamento economico**, trascinando il Paese in una **fase di stagflazione**, ovvero la compresenza di stagnazione della crescita e inflazione. È quanto afferma un autorevole think tank russo molto vicino al governo.

Lo scorso mese, la Banca Centrale russa ha innalzato il **tasso d'interesse di riferimento al 21%**, il livello più alto degli ultimi vent'anni, con l'obiettivo dichiarato di contrastare **l'inflazione, attualmente attestata all'8,6%**, e di rispondere alle elevate aspettative inflazionistiche della popolazione. Tale decisione ha suscitato il malcontento di numerosi esponenti del mondo imprenditoriale, tradizionalmente critici nei confronti delle politiche della Banca Centrale, e ha attirato le critiche di economisti di spicco coinvolti nell'elaborazione delle strategie governative.

"L'attuale livello elevato del tasso d'interesse di riferimento, unito alla prospettiva di ulteriori incrementi, ha determinato un rischio concreto di contrazione economica e di un crollo degli investimenti nel prossimo futuro", ha dichiarato mercoledì 29 gennaio il **TsMAKP**, un istituto di ricerca che fornisce consulenza al governo.

Gli economisti del centro studi avvertono che la quota di imprese manifatturiere con un onere di servizio del debito pari a due terzi degli utili ante imposte e interessi potrebbe raddoppiare, raggiungendo il 20%, con conseguenti **rischi di default aziendali e fallimenti**. Inoltre, sottolineano che, con i tassi di interesse privi di rischio attualmente intorno al 18%, i progetti d'investimento quinquennali dovrebbero garantire un rendimento minimo del 130% sul capitale iniziale per risultare economicamente sostenibili.

Secondo gli analisti del TsMAKP, l'orientamento restrittivo della politica monetaria ha avuto un impatto marginale sui fattori principali che alimentano l'inflazione, tra cui **l'aumento dei costi delle transazioni transfrontaliere** dovuto alle sanzioni occidentali, la **crescita dei prezzi dei prodotti alimentari importati** e l'incremento delle tariffe regolamentate dei servizi pubblici.

"A seguito delle azioni intraprese dalla Banca Centrale, l'economia russa si trova concretamente esposta al rischio di stagflazione, ossia una fase di stagnazione, se non addirittura di recessione, accompagnata da un'inflazione elevata", ha concluso il think tank.

La Banca Centrale, dal canto suo, ha in precedenza sostenuto che il surriscaldamento dell'economia, operante oltre la propria capacità, unito alla carenza di manodopera e alla crescita incontrollata dei salari, costituisca esso stesso un fattore di rischio di stagflazione, con il potenziale di precipitare il Paese in recessione.