MERIDIAN GROUP

Weekly *Report*

TLP:GREEN **DATA REPORT: 16.09.2024**

— Contatti

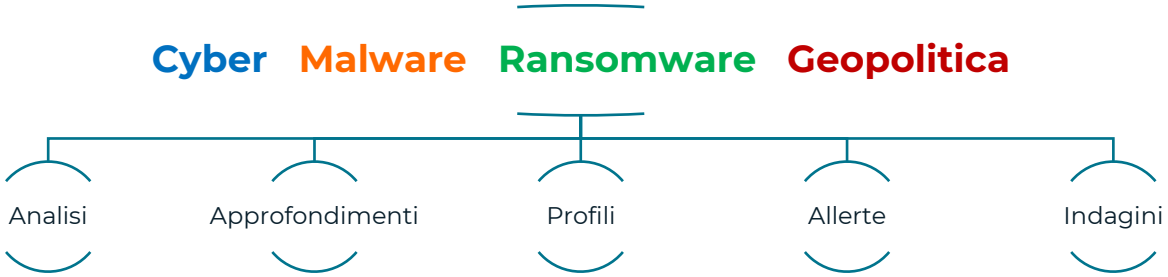
MERIDIAN SRL

+39 06 99706680 | Viale Erminio Spalla, 09 - 00142 Roma (RM) IT

P.IVA/C.F. 13693001003 - REA-RM-1465989

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.

Indice *Report*

SEVERITY

INFORMATIVO: Le informazioni "informative" non rappresentano una minaccia immediata, ma aiutano a mantenere la consapevolezza della sicurezza.

BASSO: Questo livello presenta un rischio limitato che deve essere monitorato, ma non è prioritario.

MEDIO: Le minacce "medie" hanno un rischio moderato e devono essere monitorate e risolte in tempi ragionevoli.

ALTO: Le minacce "alte" hanno un alto rischio di causare danni gravi e richiedono una rapida risposta.

CRITICO: Le minacce "critiche" rappresentano un rischio estremamente elevato e richiedono azioni immediate per evitare danni gravi o catastrofici.

TRAFFIC LIGHT PROTOCOL

WHITE: Queste informazioni possono essere condivise pubblicamente senza restrizioni. Non sono sensibili e possono essere diffuse liberamente. Non ci sono limitazioni alla condivisione.

GREEN: Queste informazioni possono essere condivise con altre organizzazioni di una comunità più ampia, ma non pubblicamente.

AMBER: Queste informazioni sono sensibili e possono essere condivise SOLO all'interno di una specifica comunità o organizzazione per affrontare problemi o mitigare rischi. La condivisione è limitata ai membri della comunità di fiducia.

RED: Queste informazioni sono altamente sensibili e devono essere condivise SOLO con persone specifiche all'interno dell'organizzazione. Sono informazioni critiche e la loro diffusione è limitata al minimo indispensabile, garantendo massima riservatezza e protezione.

NATO ADMIRAL CODE

Affidabilità della fonte

A: Fonte completamente affidabile

B: Fonte solitamente affidabile

C: Fonte abbastanza affidabile

D: Fonte non molto affidabile

E: Fonte inaffidabile

F: Affidabilità della fonte non determinabile

Accuratezza della fonte

1: Informazione confermata da altre fonti indipendenti

2: Informazione probabilmente vera

3: Informazione possibilmente vera

4: Informazione dubbia

5: Informazione improbabile

6: Accuratezza dell'informazione non determinabile

RANSOMWARE GEOPOLITICA

L’attore criminale Meow attacca le IDF e il Mossad

Attacco cibernetico del gruppo MEOW colpisce le infrastrutture critiche israeliane tra cui le Forze Armate israeliane (IDF) e il Mossad.

Martedì 10 settembre il gruppo di hacker MEOW ha intrapreso un massiccio attacco cibernetico contro le infrastrutture critiche israeliane, prendendo di mira le Forze Armate e le agenzie di intelligence, inclusa la leggendaria organizzazione del Mossad.

Secondo le prime ricostruzioni, l'attacco sarebbe stato portato avanti con una combinazione di tecniche avanzate di phishing e malware, progettate per infiltrarsi nelle reti governative e rubare informazioni sensibili. Il gruppo MEOW, noto per il suo modus operandi aggressivo e per l'uso di strumenti cibernetici non convenzionali, avrebbe sfruttato vulnerabilità sconosciute nei sistemi informatici delle Infrastrutture Essenziali (IE), paralizzando temporaneamente le comunicazioni interne e compromettendo dati di alto valore. Mentre si cerca di comprendere l'origine e le motivazioni dietro questo attacco, l'incidente solleva preoccupazioni sulla crescente capacità e audacia degli attori criminali nel cyberspazio. Il gruppo MEOW, che ha già rivendicato responsabilità per altri attacchi simili nel passato, sembra voler lanciare un messaggio chiaro alle autorità israeliane e alla comunità internazionale: nessuna organizzazione, per quanto protetta, è immune dal rischio di un’aggressione cibernetica.

DATA	VITTIMA	ATTORE CRIMINALE	STATO
2024-09-10	IDF and Mossad agents	meow	

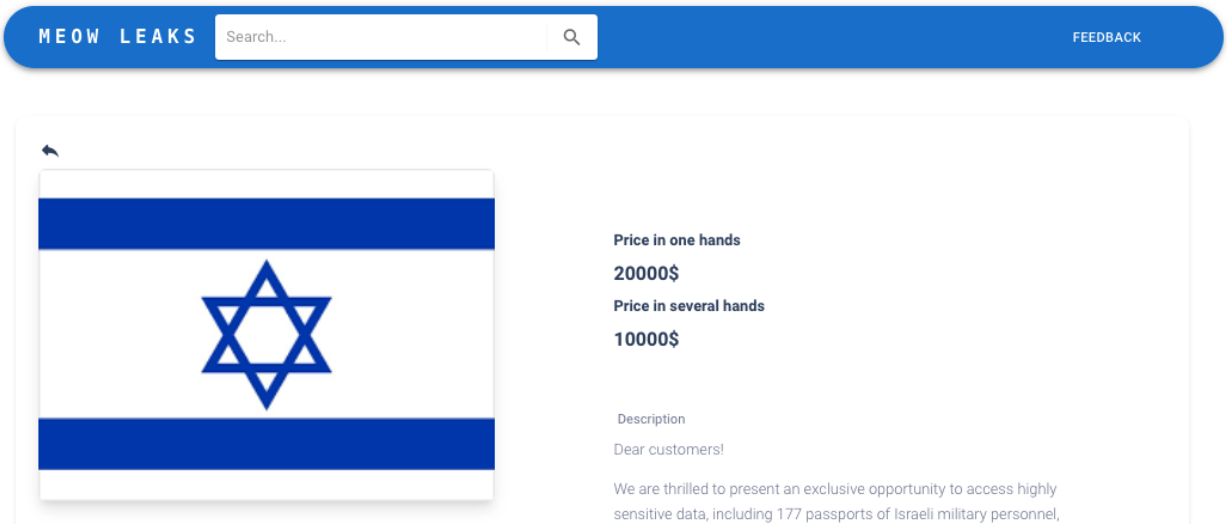


Figura 1 - Rivendicazione dell'attacco sul DLS di Meow

Inoltre, MEOW ha pubblicato, sul proprio Data Leak Site (DLS), un commento all'attacco spiegando l'importanza dei dati sottratti.

Dear customers!

We are thrilled to present an exclusive opportunity to access highly sensitive data, including 177 passports of Israeli military personnel, encompassing members of the Israeli Defense Forces (IDF) and operatives from Mossad, Israels renowned intelligence agency.

The IDF (Tzva HaHagana LeYisrael) is Israels military force, structured into three main branches:

Ground Forces: responsible for infantry, tanks, and artillery operations;
Air Force: conducting air support, reconnaissance, and airstrikes;
Navy: securing maritime borders and conducting naval operations.
All IDF soldiers are known for their rigorous training and discipline, with most Israeli citizens required to serve - 2.8 years for men and 2 years for women. They are tasked with safeguarding the country against both internal and external threats, conducting peacekeeping missions, and preventing terrorism.

Mossad is Israels external intelligence agency, playing a key role in protecting the country from foreign threats. It is involved in covert intelligence-gathering operations, sabotage, espionage, and the elimination of terrorist threats. Mossads missions are secretive and far-reaching, operating outside Israels borders.

The 177 passports in this data set provide sensitive information about Israeli military personnel, including soldiers and intelligence agents. This data is of great interest to intelligence professionals, political analysts, and other stakeholders seeking insights into Israels defense mechanisms.

Key data in this pack includes:

Passports of IDF soldiers and Mossad operatives
Personal details including names, birth dates, and nationalities
Intelligence and military-related documentation
To gain access to this exclusive data source, simply click the Buy button and provide your contact information for registration. Our team will promptly assist you in ensuring a smooth and confidential transaction process.

Dont miss this unique opportunity to uncover detailed information about Israels most guarded defense and intelligence assets!

Cari clienti!

Siamo entusiasti di presentare un'opportunità esclusiva di accesso a dati altamente sensibili, tra cui 177 passaporti di personale militare israeliano, tra cui membri delle Forze di difesa israeliane (IDF) e agenti del Mossad, la famosa agenzia di intelligence israeliana.

L'IDF (Tzva HaHagana LeYisrael) è la forza militare israeliana, strutturata in tre rami principali:

Forze di terra: responsabili delle operazioni di fanteria, carri armati e artiglieria;

Aeronautica Militare: effettuazione di supporto aereo, ricognizione e attacchi aerei;

Marina: protezione dei confini marittimi e conduzione di operazioni navali.

Tutti i soldati dell'IDF sono noti per il loro rigoroso addestramento e la loro disciplina, con la maggior parte dei cittadini israeliani tenuti a prestare servizio - 2,8 anni per gli uomini e 2 anni per le donne. Hanno il compito di salvaguardare il paese da minacce interne ed esterne, condurre missioni di mantenimento della pace e prevenire il terrorismo.

Il Mossad è l'agenzia di intelligence esterna di Israele, che svolge un ruolo chiave nella protezione del paese dalle minacce straniere. È coinvolta in operazioni segrete di raccolta di informazioni, sabotaggio, spionaggio ed eliminazione delle minacce terroristiche. Le missioni del Mossad sono segrete e di vasta portata, e operano al di fuori dei confini di Israele.

I 177 passaporti in questo set di dati forniscono informazioni sensibili sul personale militare israeliano, tra cui soldati e agenti dell'intelligence. Questi dati sono di grande interesse per i professionisti dell'intelligence, gli analisti politici e altri stakeholder che cercano approfondimenti sui meccanismi di difesa di Israele.

I dati chiave di questo pacchetto includono:

Passaporti di soldati dell'IDF e agenti del Mossad Dati personali, inclusi nomi, date di nascita e nazionalità Documentazione relativa all'intelligence e all'esercito Per accedere a questa esclusiva fonte di dati, è sufficiente fare clic sul pulsante Acquista e fornire le informazioni di contatto per la registrazione. Il nostro team ti assisterà tempestivamente per garantire un'esperienza fluida e riservata processo di transazione.

Non perdere questa opportunità unica di scoprire informazioni dettagliate sulle risorse di difesa e di intelligence più protette di Israele!

Figura 2 - Commento sull'attacco pubblicato da Meow

GEOPOLITICA CYBER

CIA e MI6 sfruttano l'AI generativa per individuare i gruppi cybercriminali

I capi dei servizi segreti pubblicano la prima dichiarazione congiunta della storia, per denunciare come Russia e Cina sfruttino i nuovi mezzi tecnologici per seminare caos e confusione in tutto il mondo

Il direttore della CIA Bill Burns e il capo del Secret Intelligence Service (SIS) del Regno Unito, Richard Moore, hanno per la prima volta scritto insieme un articolo in cui rivelano che le loro agenzie hanno adottato l'intelligenza artificiale generativa. "Stiamo ora utilizzando l'IA, inclusa l'IA generativa, per migliorare le attività di intelligence – dalla sintesi all'ideazione fino all'aiuto nell'identificare informazioni chiave in un mare di dati", hanno dichiarato i due sul Financial Times.

> "Stiamo addestrando l'IA per aiutare a proteggere e testare le nostre operazioni per garantire la segretezza quando necessario. Stiamo utilizzando tecnologie cloud affinché i nostri brillanti data scientists possano sfruttare al massimo i nostri dati, e stiamo collaborando con le aziende più innovative negli Stati Uniti, nel Regno Unito e in tutto il mondo"

I due hanno anche parlato con la direttrice del Financial Times, Roula Khalaf, sabato e in quella sessione Moore ha rivelato che il MI6 utilizza modelli linguistici di grandi dimensioni per navigare nella vasta quantità di contenuti estremisti presenti su Internet e decifrare il gergo criminale più recente, in modo che i suoi agenti possano interagire credibilmente con quella comunità.

I capi dell'intelligence hanno sottolineato di operare in un momento in cui la tecnologia presenta sfide uniche che mettono in pericolo l'ordine internazionale "in un modo che non si vedeva dai tempi della Guerra Fredda". La guerra in Ucraina ha evidenziato come la tecnologia, se utilizzata insieme agli armamenti tradizionali, "possa alterare il corso di una guerra", secondo Moore e Burns. I due hanno affermato che il conflitto ha visto la combinazione di immagini satellitari, tecnologia dei droni, guerra informatica ad alta e bassa sofisticazione, social media, software e intelligence open source, veicoli aerei e navali senza equipaggio e operazioni informative a un "ritmo e scala incredibili".

Ma oltre all'Ucraina, i capi della CIA e del SIS hanno sottolineato che continuano a collaborare per interrompere sia le campagne di disinformazione della Russia sia la sua "spericolata campagna di sabotaggio in tutta Europa." Nel frattempo, la Cina rappresenta "la principale sfida di intelligence e geopolitica del XXI secolo", hanno scritto Moore e Burns. Inoltre, quest'ultimo ha detto che la CIA ha triplicato il proprio budget negli ultimi tre anni per affrontare il furto di tecnologia e questioni di sicurezza simili provenienti dalla Cina. La "sfida cinese" ora rappresenta il 20 percento del budget complessivo dell'agenzia. "Stiamo dedicando molta attenzione e posso tranquillamente prevedere che continueremo a farlo per il prossimo decennio", ha affermato Burns.

RANSOMWARE

Pubblicati i dati dell'Università di Genova sul DLS di RansomHub

RansomHub pubblica senza soluzione di continuità vittime sul proprio Data Leaks Site: tra le vittime più recenti spicca l'Università di Genova

RansomHub è uno dei gruppi in più rapida ascesa nel panorama cybercriminale. Dal suo debutto, nel mese di febbraio 2024, il gruppo ha mantenuto ritmi elevatissimi, attirando l'attenzione delle forze dell'ordine di tutto il mondo, tra cui anche CISA, FBI, HHS e MS-ISAC che, a tal proposito, hanno pubblicato la campagna #STOPRANSOMWARE la scorsa settimana.

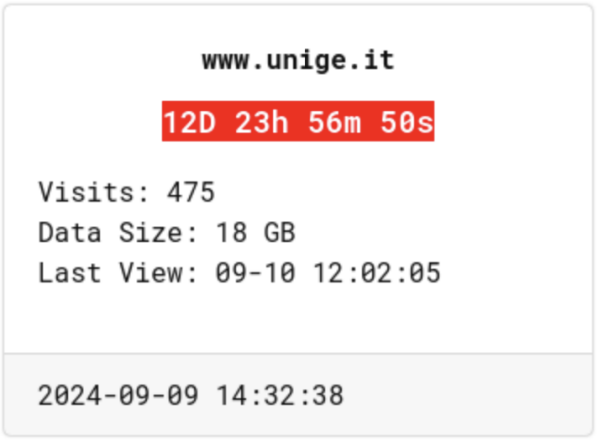


Figura 3 - Post su DLS RansomHub

Solamente nelle ultime 48 ore sono state pubblicate diverse vittime sul proprio DLS, tra cui l'ateneo genovese. I dati dovrebbero essere pubblicati per intero in data 23 settembre 2024, come annunciato nella miniatura del post.

VITTIMA	ATTORE CRIMINALE	STATO
www.pokerspa.it	ransomhub	

Removal.AI	ransomhub	

Removal.AI

PUBLISHED

Visits: 3162
Data Size: 12 GB
Last View: 09-09 14:58:36

Schneider	ransomhub	

www.schneider.ch

PUBLISHED

Visits: 3089
Data Size: 300gb
Last View: 09-09 14:59:36

Kawasaki.eu	ransomhub	

kawasaki.eu

PUBLISHED

Visits: 5394
Data Size: 487GB
Last View: 09-16 07:04:28

GEOPOLITICA CYBER

Vertice globale a Seoul chiede misure di sicurezza per l'uso militare dell'IA

Esperti e funzionari di 90 paesi si riuniscono per discutere la creazione di un quadro normativo internazionale che garantisca un uso responsabile e sicuro delle tecnologie IA nel settore militare.

Al vertice globale tenutosi a Seoul è stata ribadita l'urgenza di definire misure di sicurezza per l'impiego dell'intelligenza artificiale (AI) in ambito militare. L'AI sta infatti rimodellando le strategie militari moderne, come testimoniato dai conflitti in Ucraina e in Medio Oriente, con applicazioni che spaziano dalle armi autonome alla logistica, fino alla cybersicurezza e ai processi decisionali strategici. Tuttavia, l'assenza di un quadro normativo condiviso a livello internazionale per l'uso militare dell'AI ha creato un pericoloso vuoto, sollevando timori circa le possibili minacce alla stabilità globale derivanti dall'uso incontrollato di tali tecnologie.

In risposta a questa crescente preoccupazione, rappresentanti di governi, esperti internazionali e funzionari della difesa si sono riuniti a Seoul per il Summit 2024 sull'Intelligenza Artificiale Responsabile nel Settore Militare (REAIM). Tale evento, organizzato congiuntamente dal Ministero degli Affari Esteri e dal Ministero della Difesa Nazionale della Corea del Sud, è stato il secondo del suo genere, dopo l'edizione del 2023 tenutasi all'Aia, nei Paesi Bassi. Quest'anno l'organizzazione è stata coadiuvata anche da Paesi Bassi, Singapore, Kenya e Regno Unito, attirando circa 2.000 partecipanti provenienti da 90 paesi sotto il tema "AI Responsabile per un Futuro più Sicuro." Nel suo discorso inaugurale, il Ministro degli Esteri Cho Tae-yul ha indicato tre principi chiave per garantire l'uso etico e sicuro dell'AI in ambito militare: valutazione, applicazione e ancoraggio della governance. Ha sottolineato come l'intelligenza artificiale stia trasformando non solo le operazioni militari, ma anche il ruolo stesso dei comandanti e dei soldati, richiedendo una riflessione globale sulla creazione di un quadro normativo adeguato.

Il Ministro della Difesa Kim Yong-hyun ha ulteriormente evidenziato la duplice natura dell'AI, descrivendola come una "lama a doppio taglio". Se da un lato potenzia le capacità operative, dall'altro, in mancanza di norme precise, può portare a gravi conseguenze. Ha quindi ribadito l'impegno del Ministero della Difesa della Corea del Sud nel collaborare con la comunità internazionale per definire standard etici rigorosi. La cerimonia di apertura ha dato il via a una serie di dibattiti su temi centrali, tra cui le implicazioni dell'AI per la pace e la sicurezza globali, con interventi di alti ufficiali militari e accademici di rilevanza mondiale. Le discussioni hanno messo in luce il rapido impatto dell'AI sui campi di battaglia moderni e la necessità di una cooperazione tra produttori, governi e utilizzatori per colmare il divario tra l'evoluzione tecnologica e le normative. Il vertice si concluderà con l'adozione del "Blueprint for Action", un documento che sintetizza le linee guida emerse durante i lavori, e un tavolo di discussione a livello ministeriale, finalizzato a favorire uno scambio di idee su una governance condivisa e responsabile dell'IA militare. La Russia non è stata invitata al REAIM per il secondo anno consecutivo, in seguito alla condanna internazionale per l'invasione dell'Ucraina, mentre Stati Uniti e Cina, protagonisti nella competizione per il controllo dell'AI militare, hanno partecipato attivamente all'evento.

CYBER

Pubblicato il DPCM per la ripartizione dei fondi della Strategia Nazionale di Cybersicurezza 2024-2026

Un finanziamento di 347 milioni di euro per rafforzare la resilienza cibernetica dell'Italia, migliorare la protezione delle infrastrutture critiche e promuovere l'autonomia tecnologica nel contesto digitale.

É stato pubblicato nella Gazzetta Ufficiale n. 207 il Decreto del Presidente del Consiglio dei ministri (DPCM) concernente la ripartizione dei fondi destinati all'attuazione della Strategia Nazionale di Cybersicurezza per il triennio 2024-2026. Tale provvedimento rappresenta un elemento fondamentale per assicurare il finanziamento delle misure previste dal Piano di implementazione della strategia, con l'assegnazione di circa 347 milioni di euro alle Amministrazioni pubbliche competenti.

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 8 luglio 2024

Ripartizione del Fondo per l'attuazione della strategia nazionale di cybersicurezza e del Fondo per la gestione della cybersicurezza. (24A04539) (GU Serie Generale n.207 del 04-09-2024)

La Strategia Nazionale di Cybersicurezza, sviluppata per il periodo 2022-2026, costituisce il quadro di riferimento delle politiche italiane in materia di sicurezza cibernetica. Essa si pone come obiettivo primario il rafforzamento della resilienza del Paese rispetto alle minacce cyber, attraverso la protezione delle infrastrutture critiche nazionali e il miglioramento delle capacità di difesa, prevenzione e risposta agli attacchi informatici. L'attuazione di tale strategia è strettamente connessa agli obiettivi fissati dal Piano Nazionale di Ripresa e Resilienza (PNRR), che contempla investimenti significativi per la trasformazione digitale e la modernizzazione del settore pubblico e privato, creando un'opportunità senza precedenti per potenziare le capacità cibernetiche dell'Italia.

Il Piano di implementazione individua una serie di interventi prioritari, tra i quali si annoverano il rafforzamento delle infrastrutture critiche mediante investimenti volti a migliorare la sicurezza di settori strategici come l'energia, i trasporti, le telecomunicazioni, la sanità e la finanza, settori questi maggiormente esposti a rischi di attacchi informatici. Si prevede inoltre la promozione dell'autonomia tecnologica, sostenendo lo sviluppo di soluzioni tecnologiche nazionali e riducendo la dipendenza da tecnologie estere, specialmente in ambiti quali il cloud computing, l'intelligenza artificiale e la crittografia avanzata. È altresì prevista la crescita delle competenze digitali attraverso il finanziamento di programmi di formazione avanzata per il personale della pubblica amministrazione, la creazione di nuove figure professionali

specializzate in cybersicurezza e la promozione di borse di studio, corsi di aggiornamento e collaborazioni con università e centri di ricerca. Infine, si mira a rafforzare la cooperazione internazionale tramite la partecipazione attiva dell'Italia alle iniziative europee e globali per la sicurezza cibernetica, facilitando lo scambio di informazioni, la condivisione di best practices e contribuendo allo sviluppo di norme internazionali.

Il DPCM stabilisce la ripartizione delle risorse finanziarie mediante due fondi principali. Il Fondo per l'Attuazione della Strategia Nazionale di Cybersicurezza, istituito dall'articolo 1, comma 899, della legge n. 197/2022 (Legge di Bilancio 2023), è destinato a sostenere gli investimenti necessari al raggiungimento dell'autonomia tecnologica nel contesto digitale. Tale fondo mira ad innalzare i livelli di sicurezza dei sistemi informativi nazionali, promuovendo progetti di innovazione tecnologica, ricerca e sviluppo, e l'acquisizione di tecnologie avanzate. Esso finanzia anche il potenziamento delle infrastrutture di difesa cibernetica, il miglioramento della protezione dei dati sensibili e favorisce l'interoperabilità e la condivisione delle informazioni tra enti pubblici e privati.

Il Fondo per la Gestione della Cybersicurezza, anch'esso istituito dalla legge n. 197/2022, è invece dedicato alla gestione operativa delle attività correlate alla sicurezza cibernetica. Esso finanzia la gestione delle emergenze cibernetiche, la formazione e l'addestramento del personale, lo sviluppo delle capacità di risposta rapida e il coordinamento tra le varie agenzie ed enti governativi. Inoltre, supporta la creazione di un ecosistema cibernetico integrato, in cui la cooperazione tra il settore pubblico, il privato e il mondo accademico risulta essenziale per rafforzare la resilienza complessiva.

La ripartizione dei fondi, secondo quanto stabilito dal decreto, avviene in base a una serie di criteri, quali la priorità degli interventi, con particolare attenzione a quelli che hanno un impatto diretto sulla protezione delle infrastrutture critiche come reti energetiche, telecomunicazioni e sanità, poiché questi settori sono considerati essenziali per la sicurezza nazionale e necessitano di maggiori risorse. Viene inoltre valutato il livello di rischio cibernetico associato a ciascun settore o ente, privilegiando con finanziamenti proporzionalmente maggiori le organizzazioni che gestiscono dati sensibili o infrastrutture ad alta esposizione a minacce cibernetiche. La capacità delle amministrazioni di utilizzare efficacemente i fondi assegnati rappresenta un ulteriore criterio determinante nella ripartizione, favorendo quegli enti che hanno dimostrato solide capacità operative e una storia di gestione efficace di progetti complessi.

L'allocazione dei circa 347 milioni di euro stanziati per il triennio 2024-2026 è distribuita tra le Amministrazioni centrali dello Stato, quali il Ministero dell'Interno, il Ministero della Difesa, il Ministero dell'Economia e delle Finanze, e l'Agenzia per la Cybersicurezza Nazionale (ACN), che hanno il compito di coordinare la protezione delle infrastrutture critiche, sviluppare politiche nazionali di sicurezza cibernetica e garantire l'integrità e la resilienza dei sistemi governativi. Ulteriori risorse sono destinate alle Regioni e agli Enti Locali per progetti specifici, come la protezione delle reti di trasporto, dei servizi pubblici locali e delle infrastrutture sanitarie, in coordinamento con le linee guida nazionali. Una parte dei fondi è inoltre assegnata al settore privato e ai partner industriali attraverso bandi di gara e progetti di partenariato pubblico-privato per incentivare l'adozione di tecnologie di sicurezza avanzate, specialmente in settori critici come l'energia, le telecomunicazioni, la finanza e la difesa. Infine, una quota è riservata a programmi di ricerca e sviluppo per nuove tecnologie di cybersicurezza, promuovendo l'innovazione tecnologica tramite collaborazioni con università, centri di ricerca e startup specializzate.

Il decreto specifica una serie di attività che possono beneficiare dei finanziamenti stanziati, includendo l'implementazione di sistemi di sicurezza avanzati, come soluzioni di rilevamento delle intrusioni, tecnologie di

crittografia avanzata e strumenti di analisi delle minacce; programmi di formazione per il personale delle amministrazioni pubbliche, per sviluppare competenze avanzate in materia di sicurezza cibernetica; il miglioramento della governance cibernetica mediante la creazione e il rafforzamento di strutture organizzative per la sicurezza a livello nazionale e locale; e il supporto alle iniziative di cooperazione internazionale in ambito cibernetico, inclusa la partecipazione a reti di scambio di informazioni e la collaborazione con organismi europei e internazionali.

Il DPCM prevede un sistema di monitoraggio e verifica per garantire l'utilizzo efficiente e trasparente dei fondi. Le misure adottate includono la presentazione di rapporti periodici da parte delle amministrazioni beneficiarie sui progressi dei progetti finanziati, audit regolari da parte della Corte dei Conti e di altre autorità di controllo per verificare la conformità alle disposizioni del decreto, e l'adozione di indicatori di performance specifici per valutare l'efficacia degli interventi finanziati, come la riduzione degli incidenti di sicurezza, l'incremento della protezione delle infrastrutture critiche e il potenziamento delle competenze del personale.

Oltre ai fondi specifici per la cybersicurezza, il Piano beneficia delle risorse del PNRR, che prevede investimenti significativi per la digitalizzazione e la sicurezza delle infrastrutture critiche del Paese. La combinazione delle risorse del PNRR con i fondi della Strategia Nazionale di Cybersicurezza crea una sinergia strategica volta ad accelerare la transizione digitale del settore pubblico, incentivare l'innovazione tecnologica, creare ecosistemi digitali resilienti e promuovere l'adozione di standard di sicurezza più elevati in tutto il settore pubblico e privato.

GEOPOLITICA CYBER

Le strategie occidentali contro la cyberpropaganda Russa

Gli Stati Uniti e i loro alleati intensificano gli sforzi per contrastare gli attacchi informatici e le operazioni di disinformazione orchestrate dal GRU. Sequestri di domini, sanzioni e l'uso di IA sono al centro della lotta contro la minaccia digitale che mira a destabilizzare democrazie e manipolare l'opinione pubblica.

Le iniziative messe in atto dagli Stati Uniti e dai loro alleati per contrastare la disinformazione russa e le minacce informatiche riconducibili ai gruppi APT (Advanced Persistent Threat) affiliati al GRU, in particolar modo all'Unità 29155, si sono intensificate. Tale gruppo ha perpetrato attacchi cibernetici contro infrastrutture critiche, in particolare nel settore energetico e governativo, con un focus specifico sull'Ucraina e sui paesi membri della NATO. Uno degli strumenti principali utilizzati in questi attacchi è il malware noto come WhisperGate, particolarmente distruttivo. A fronte di tali minacce, le organizzazioni responsabili della gestione di infrastrutture critiche sono state esortate a rafforzare le misure di sicurezza dei propri sistemi.

Contestualmente, gli Stati Uniti hanno intensificato gli sforzi per contrastare la propaganda russa, sequestrando 32 domini web utilizzati nell'ambito dell'operazione Doppelgänger. Questo gruppo, connesso al governo russo, ha sfruttato il cybersquatting per replicare siti web di note testate giornalistiche, diffondendo informazioni false al fine di manipolare l'opinione pubblica. Attraverso l'uso di falsi influencer creati grazie all'intelligenza artificiale, Doppelgänger ha propagato narrazioni favorevoli alla Russia su piattaforme come TikTok, Instagram e X.

Il cybersquatting è stato uno strumento centrale di tale operazione, in cui sono stati creati falsi siti che imitavano fedelmente quelli di rinomate testate come il *Washington Post* e *Fox News*, con l'intento di ingannare gli utenti e minare la fiducia nei media tradizionali. I contenuti manipolati venivano poi disseminati sui social media attraverso account falsi, alimentando la disinformazione e generando interazioni che ne amplificavano ulteriormente la portata.

L'operazione è stata supervisionata da Sergei Kiriyenko, un alto funzionario dell'amministrazione russa, e coordinata da organizzazioni come la Social Design Agency e la Structura National Technology. Questi enti si sono occupati della creazione e gestione dei siti che hanno subito il typosquatting, diffondendo propaganda al fine di influenzare le elezioni in diverse nazioni, tra cui gli Stati Uniti. L'obiettivo era ridurre il sostegno all'Ucraina e promuovere candidati favorevoli alla Russia.

La disinformazione diffusa attraverso meme, storie false e commenti sui social media ha mirato a influenzare gli elettori, spingendo narrazioni favorevoli alla linea russa. Un aspetto innovativo di questa operazione è stato l'uso dell'intelligenza artificiale per creare contenuti propagandistici, tra cui immagini e video, al fine di manipolare in modo più efficace l'opinione pubblica.

Come conseguenza dell'operazione Doppelgänger, sono state imposte sanzioni alle organizzazioni russe coinvolte e sequestrati i domini malevoli negli Stati Uniti, con l'intento di ridurre la capacità operativa di tali entità. Tuttavia, l'uso di tecniche avanzate come VPN e server privati ha reso difficile il loro completo smantellamento.

Questo caso mette in luce come l'uso della tecnologia digitale possa rappresentare una minaccia per la stabilità politica e influenzare negativamente il processo democratico delle elezioni. Il cybersquatting e l'utilizzo dell'intelligenza artificiale per la diffusione di disinformazione rappresentano minacce in continua evoluzione, che richiedono strategie altrettanto sofisticate per essere contrastate. La difesa della democrazia e della sicurezza informatica si dimostra fondamentale, poiché il fenomeno della disinformazione, se non affrontato in modo adeguato, potrebbe avere ripercussioni gravi e durature.

RANSOMWARE

Medusa attacca Technolog S.r.l.

Nuovo attacco ransomware contro l'azienda italiana Technolog S.r.l. specializzata in software per la gestione di magazzini e automazione industriale

L'attacco ransomware condotto dal gruppo criminale noto come Medusa ai danni dell'azienda italiana Technolog S.r.l. rappresenta un caso emblematico di cybercriminalità avanzata. Medusa ha sfruttato vulnerabilità nei sistemi informatici dell'azienda per penetrare nella rete interna e criptare file critici, rendendoli inaccessibili.

Una volta penetrati nei sistemi interni, gli aggressori hanno operato in modo silente, muovendosi lateralmente attraverso la rete per identificare i file più sensibili e i sistemi critici da compromettere. Tale approccio ha permesso a Medusa di raccogliere informazioni preliminari e di preparare il terreno per il criptaggio su vasta scala dei dati. Nell'attacco Medusa ha utilizzato un algoritmo di cifratura per bloccare l'accesso a documenti, progetti, dati finanziari e informazioni sensibili. I file chiave dell'azienda sono stati criptati e una nota di riscatto è stata lasciata sui sistemi compromessi, nella quale veniva richiesto un pagamento in criptovaluta per ottenere la chiave di decrittazione.

Medusa ha inoltre minacciato Technolog S.r.l. di divulgare o vendere sul dark web i dati aziendali sottratti se il riscatto non fosse stato pagato entro un periodo di tempo limitato. Questa tattica di doppia estorsione aumenta la pressione sull'azienda, costringendola a valutare non solo il danno economico e operativo, ma anche le ripercussioni sulla sua reputazione e la possibile violazione delle normative sulla protezione dei dati.

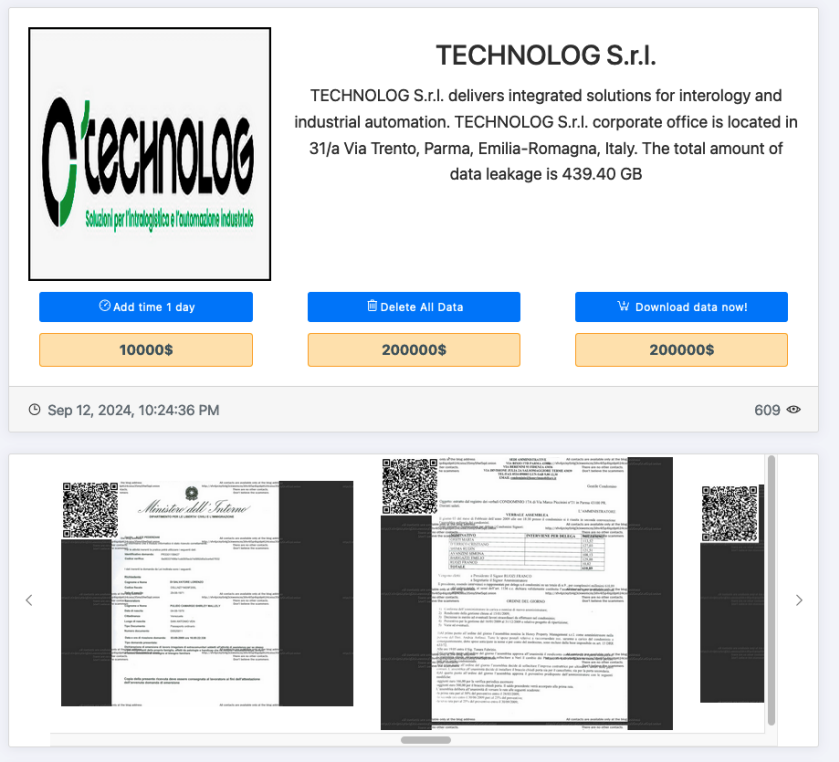


Figura 4 - Pubblicazione sul DLS di medusa dell'attacco

Medusa è un gruppo ransomware che opera come Ransomware-as-a-Service (RaaS), scoperto per la prima volta nel settembre 2019 e da allora ha mietuto molte vittime in diversi settori e locate in più Stati.

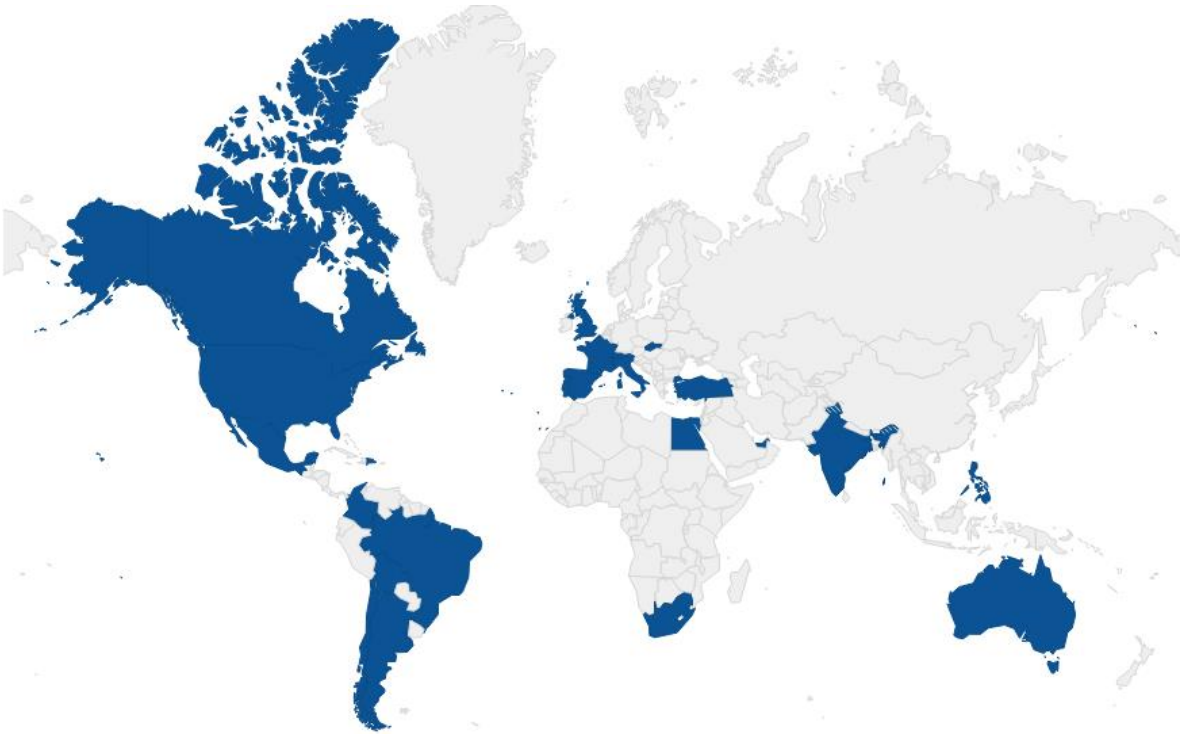


Figura 5 - Stati attaccati da Medusa

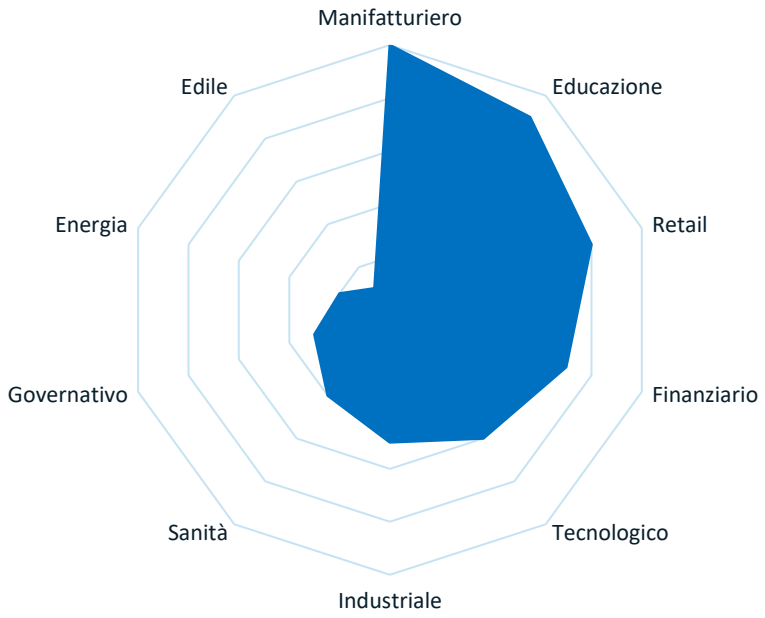


Figura 6 – Settori colpiti da Medusa

L'attacco iniziale avviene infiltrandosi nella rete aziendale delle vittime, sfruttando configurazioni errate del desktop remoto (RDP), mediante l'utilizzo di un file batch per eseguire codice PowerShell, precedentemente inserito dai criminali informatici. Questo codice cripta i file e i cybercriminali minacciano di divulgarli sul loro Data Leak Site (DLS) denominato

"Medusa Blog", su rete Tor, qualora la vittima non accetti il pagamento richiesto per il riscatto. Inoltre, il ransomware Medusa impedisce l'esecuzione contemporanea di più istanze di sé stesso per evitare rilevamenti e, grazie a una chiave di registro di Windows, previene la crittografia multipla degli stessi file.

Successivamente, per rimanere attivo nel sistema, il malware crea un'attività programmata che lo avvia regolarmente e, come gli altri ransomware, elimina i backup, le copie shadow e disabilita l'avvio del sistema operativo in modalità provvisoria. In aggiunta a ciò, se un file è ancora bloccato all'avvio del processo di crittografia, il malware utilizza Windows Restart Manager per sbloccarlo.

GEOPOLITICA | CYBER

Lo Stato Islamico rilascia video di propaganda: esortazione al jihad in Russia

Un nuovo video di 13 minuti rilasciato da centro media al-Furat mostra i prigionieri responsabili dell'attacco a Volgograd, che esortano ad intraprendere il jihad contro soprusi ed ingiustizie subite dal governo russo

Il 9 settembre, lo Stato Islamico ha pubblicato online un video di 13 minuti dove vengono mostrati 4 prigionieri affiliati a Islamic State (IS) che hanno condotto l'attacco all'interno del carcere di massima sicurezza IK-19 a Surovikino nella regione di Volgograd. Inoltre, sono stati condivisi alcuni nuovi estratti in cui dichiarano una sorta di manifesto ideologico esortando ad intraprendere il jihad in Russia, come "vendetta" per i conflitti con i musulmani e la proibizione di molte pratiche religiose dell'Islam.

Nel video sono stati inclusi alcuni filmati dell'attacco terroristico al centro commerciale Crocus.

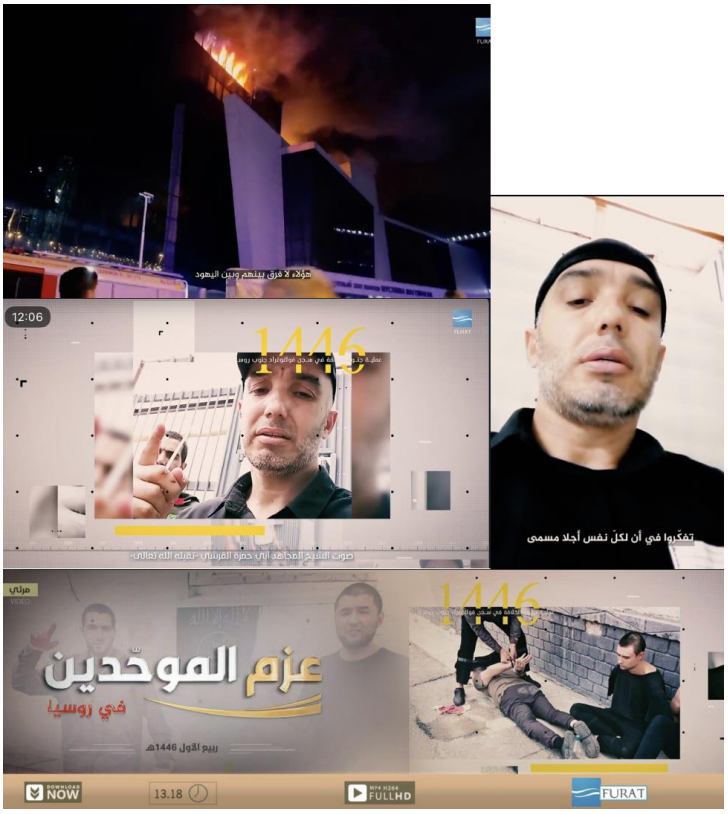


Figura 7 - Frame del video rilasciato su al-Furat

Tale strategia risulta infatti in linea con le attività operative di IS come:

- Guerra di logoramento: installazione e detonazione di IED, uso di SVBIED, organizzazione di imboscate e agguati, operazioni di assassinio con cecchini, assassinii, assassinii di leader sociali e politici, rapimenti, incendi di case e fattorie, attacchi alle forze di sicurezza e alle milizie paramilitari, attacchi a infrastrutture civili, religiose e private, attacchi contro sciiti, minoranze, sostenitori o collaboratori del governo e popolazioni non musulmane;

- Breaking the Walls: operazioni ed offensive militari contro prigioni, finalizzate a liberare prigionieri appartenenti allo Stato islamico o nuove leve da reclutare. IS con una certa regolarità incita i propri sostenitori e combattenti attraverso la propria propaganda di effettuare attacchi contro strutture penitenziari, come la rivolta all'interno del carcere di massima sicurezza sicurezza IK- 19 Surovikino, Volgograd Oblast, a sud della Russia, il 23 agosto;

- Attacchi diretti a cristiani e sciiti.

I luoghi che hanno subito attentati terroristici nel periodo analizzato sono il tempio di Wadi Al-Kabir, città di Muscat nell'Oman; la città di Soligen in Germania; il carcere di massima sicurezza IK- 19 Surovikino, Volgograd Oblast, a sud della Russia.