CYBER INTELLIGENCE REPORT

MERIDIAN GROUP

WEEKLY UPDATE

TLP: GREEN

DATA: 08.07.2024

Sommario

Indice delle figure

Company Overview

Meridian Group si posiziona come un leader nel campo della sicurezza informatica, offrendo consulenza aziendale di alto livello. Grazie alla nostra vasta esperienza e alla collaborazione con rinomate aziende nazionali e internazionali, abbiamo sviluppato una profonda comprensione delle specifiche esigenze nel settore della sicurezza informatica. La nostra capacità di stabilire relazioni significative con governi e istituzioni a livello globale ci contraddistingue, fornendo un prezioso supporto alle aziende nella ricerca di partnership industriali e commerciali.

Con una rete di oltre 50 partner professionisti in paesi chiave come Belgio, Italia, Francia, Regno Unito, Germania, Romania, Tunisia, Qatar, Brasile, Cina ed Emirati Arabi Uniti, Meridian Group si impegna a offrire soluzioni innovative ed etiche. Queste fondamenta sono alla base della nostra filosofia aziendale e guidano ogni nostra azione. La nostra costante attenzione all'innovazione ci spinge ad esplorare nuovi orizzonti nel campo della sicurezza informatica, mentre il nostro impegno verso la responsabilità assicura che ogni soluzione sia etica e sostenibile.

Offriamo ai nostri clienti servizi personalizzati e competitivi progettando soluzioni in grado non solo di soddisfare le aspettative ma anche di superarle. Il nostro approccio si basa su competenze avanzate, idee innovative e una pianificazione accurata al fine di creare un valore tangibile aggiuntivo.

La nostra missione consiste nel trasformare le sfide in opportunità, creando strategie efficaci che consentano ai nostri clienti di ottenere risultati tangibili e di successo.

Kitsune Platform

Kitsune è la piattaforma di cyber intelligence completamente italiana sulla quale il team di cyber intelligence eroga servizi as a service ai clienti di Meridian Group.

Kitsune monitora l'underground con oltre 1.300 fonti dirette ed oltre 50.000 canali pubblici e privati garantendo ai clienti una larga visibilità sul mondo del crimine informatico.

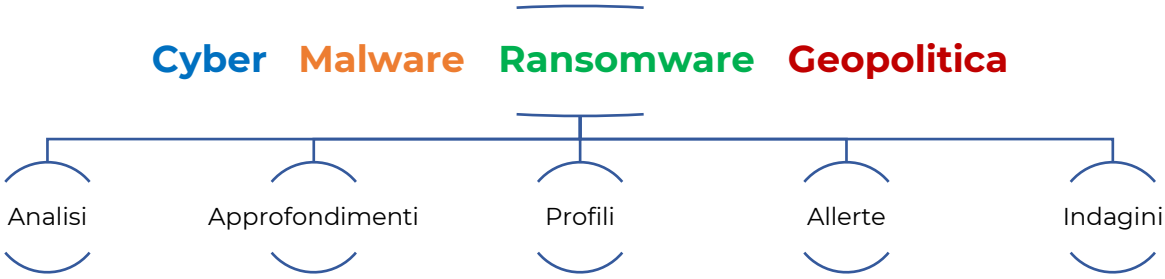
Kitsune è una piattaforma di Cyber Intelligence che si pone l'obiettivo di essere uno strumento indispensabile per gli analisti di intelligence.

La sua funzione principale è quella di raccogliere dati provenienti da diverse fonti e correlarli al fine di garantire un approccio proattivo nei confronti delle minacce che possono colpire aziende, istituzioni e persone. Kitsune offre agli analisti un ampio spettro di informazioni e strumenti avanzati per analizzare e comprendere le tendenze nel campo della sicurezza informatica. Attraverso l'utilizzo di tecniche avanzate di intelligenza artificiale e analisi dei dati, la piattaforma identifica potenziali minacce in tempo reale, consentendo agli analisti di adottare misure preventive tempestive.

Kitsune rappresenta quindi un valido alleato per gli analisti di intelligence, fornendo loro una panoramica completa delle minacce digitali e permettendo di agire in modo proattivo per mitigarle.

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.

La sicurezza cibernetica è una priorità del Governo italiano

Il Ministro degli Esteri, Antonio Tajani, evidenzia l'importanza della collaborazione internazionale e dell'innovazione tecnologica nella lotta contro la cyber criminalità e la disinformazione

Durante l'apertura della prima Conferenza Nazionale per la creazione di un ecosistema di "Cyber Capacity Building" alla Farnesina, il vicepresidente del Consiglio e ministro degli Esteri, Antonio Tajani, ha sottolineato l'importanza cruciale della sicurezza cibernetica per lo sviluppo della società italiana, dei suoi cittadini, delle imprese e della competitività del sistema industriale del Paese. Con l'espressione "cyber capacity building" ci si riferisce all'insieme di attività e iniziative volte a sviluppare, migliorare e potenziare le capacità di un Paese o di un'organizzazione nel campo della cybersecurity. A tal fine, Tajani ha evidenziato che la lotta alla criminalità informatica deve essere parte integrante di un'azione politica più ampia, volta a sostenere l'economia, la crescita industriale e la creazione di posti di lavoro in Italia.

"È necessario che l'Italia non si faccia trovare impreparata di fronte a questa sfida", ha affermato il ministro Tajani, "e per questo il governo fin dalle prime riunioni del consiglio dei ministri si è occupato prioritariamente di questo tema", evidenziando di come la criminalità contribuisca fortemente alla creazione di minacce alla cyber sicurezza, vista la sua sempre più capacità di adattamento allo sfruttamento di tecnologie avanzate e nuovi strumenti digitali legati all'Intelligenza Artificiale (AI).

"È importante dunque", ha continuato Tajani,

> "... affrontare queste minacce superando egoismi tra le varie burocrazie, facendo squadra tra le varie istituzioni, le imprese e il mondo della ricerca". In particolare, Tajani ha sottolineato come legato al tema della sicurezza cibernetica c'è quello dell'intelligenza artificiale utilizzata per manipolare l'informazione. "

Durante il G7 di Capri insieme al Segretario di Stato degli Stati Uniti, Antony Blinken, l'Italia ha firmato un accordo per contrastare la disinformazione, anche a difesa della rete delle nostre ambasciate, data la necessità di godere di norme che regolino tali novità.

Il ministro degli esteri Tajani conclude il suo intervento assicurando che la strategia nazionale in tema di sicurezza cibernetica ha l'obbiettivo anche di sostenere Paesi terzi alleati, come ad esempio Albania, Balcani e Mediterraneo, attraverso le eccellenze italiane nel settore.

Cuba e il nuovo sito radar: potenziali sviluppi per lo spionaggio cinese nei pressi della base militare USA

Il rapporto del think tank svela il potenziale impatto del nuovo sito radar cubano sulla sicurezza regionale e sugli interessi strategici della Cina.

Il Center for Strategic and International Studies (CSIS) di Washington ha rivelato, attraverso immagini satellitari, che Cuba sta attualmente costruendo un nuovo sito radar. Questo sito, situato a est della città di Santiago de Cuba vicino al quartiere El Salao, potrebbe avere la capacità di sorvegliare la vicina base navale statunitense di Guantanamo Bay. Secondo il rapporto di CSIS, pubblicato lunedì e successivamente citato dal Wall Street Journal, il sito radar rappresenta un'ulteriore espansione delle capacità di sorveglianza di Cuba, a lungo associate alla presenza di interessi cinesi.

Il Viceministro degli Esteri cubano, Carlos Fernandez de Cossio, ha respinto le accuse secondo cui Cuba ospiterebbe interessi militari cinesi, sottolineando come tali affermazioni siano prive di fonti verificabili o prove concrete.

La posizione geografica di Cuba, in prossimità degli Stati Uniti e delle loro basi militari nel sud, la rende un luogo strategico per la Cina, principale rivale strategico degli Stati Uniti, per raccogliere informazioni di intelligence. CSIS ha descritto il nuovo sito radar come uno strumento potente che, una volta operativo, potrebbe monitorare le attività aeree e marittime della militare statunitense.

Il sito è identificato come un array di antenne circolari con un diametro compreso tra 130 e 200 metri, con la capacità di rilevare segnali a distanze fino a 3.000-8.000 miglia nautiche (circa 3.452 - 9.206 miglia).

CSIS ha evidenziato che l'accesso a un tale avamposto offrirebbe alla Cina un punto di vantaggio strategico significativo vicino alla Base Navale di Guantanamo Bay, situata a 45 miglia (circa 73 km) a est di Santiago, la seconda città più grande di Cuba.

L'anno scorso, funzionari dell'amministrazione Biden hanno affermato che Pechino sta conducendo attività di spionaggio da Cuba da diversi anni e ha cercato di potenziare le sue capacità di raccolta di intelligence a partire dal 2019. Tuttavia, queste accuse sono state respinte sia da Pechino che da L'Avana.

Il portavoce del Dipartimento di Stato, Vedant Patel, ha rifiutato di commentare specificamente il rapporto, ma ha dichiarato durante un briefing che gli Stati Uniti stanno monitorando attentamente la presenza cinese a Cuba. L'ambasciata cinese a Washington ha respinto categoricamente le accuse statunitensi di spionaggio e sorveglianza da parte della Cina a Cuba, definendole calunnie senza fondamento.

CSIS ha anche riferito che le immagini satellitari del marzo 2024 mostrano come il principale sito cubano di intelligence di segnali a Bejucal, vicino a L'Avana, collegato a presunte attività di intelligence cinese, ha subito significativi aggiornamenti nell'ultimo decennio, indicando un chiaro impegno per migliorare le capacità operative.

Secondo CSIS, questi sistemi radar sono in grado di monitorare i lanci di razzi da Cape Canaveral e dal Kennedy Space Center della NASA, un aspetto di interesse per la Cina nel suo tentativo di rimanere competitiva nella tecnologia di lancio spaziale rispetto agli Stati Uniti.

Embargo colpisce la società francese di automazione elettronica Gerard Perrier Industrie

Grave violazione della sicurezza: sistemi compromessi e dati sensibili a rischio

Nella giornata di mercoledì 3 luglio il gruppo di cybercriminali Embargo ha rubato 1,4 T di dati alla società francese Gerard Perrier Industrie SA, leader nella fornitura di sistemi di automazione elettrica ed elettronica per l'industria, inclusi progettazione e produzione e installazione e manutenzione.

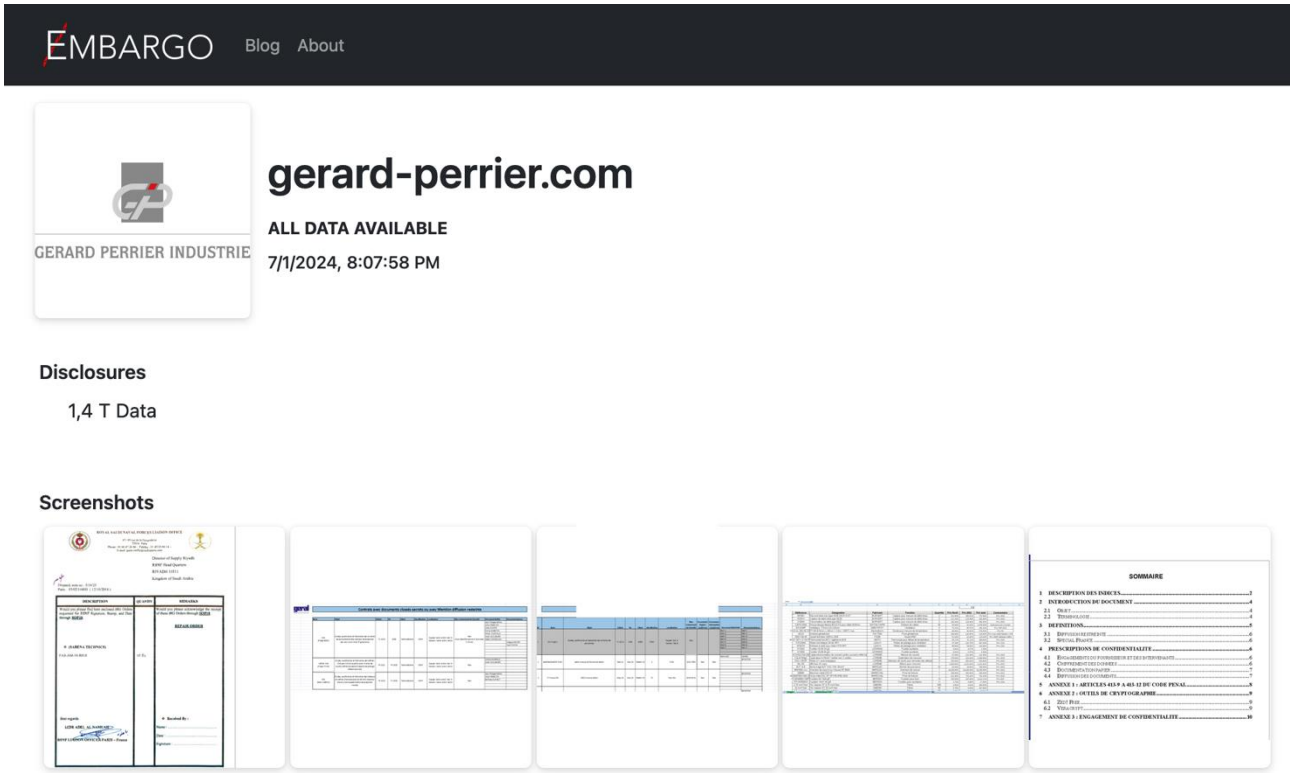


Figura 1 – Pubblicazione sul DLS di Embargo dell'attacco Gerard Perrier Industrie

Il gruppo di criminali informatici noto come Embargo rappresenta un attore malevolo molto conosciuto nel mondo del cybercrimine, contraddistinto per la sofisticatezza delle operazioni e per la portata su larga scala degli attacchi perpetrati. La composizione di Embargo è eterogenea, includendo individui altamente qualificati in svariate discipline della tecnologia e della criminalità informatica. La struttura del gruppo è fluida e decentralizzata, caratteristica che rende arduo per le forze dell'ordine il compito di tracciarne i movimenti e smantellarne l'organizzazione. Tra i membri del gruppo si annoverano hacker, ingegneri di rete, esperti di crittografia, sviluppatori di malware e ingegneri sociali.

Embargo adotta una molteplicità di tecniche per portare a termine le proprie operazioni criminali. Tali metodologie includono il phishing e lo spear phishing, con attacchi mirati a ottenere informazioni sensibili da individui specifici, lo sviluppo e la diffusione di malware quali ransomware, trojan e spyware, attacchi DDoS (Distributed Denial of Service) mirati a sovraccaricare server e reti rendendoli inaccessibili, lo sfruttamento di vulnerabilità zero-day per infiltrarsi nei sistemi attraverso falle di sicurezza non ancora note o risolte, e il controllo di reti BotNet per lanciare attacchi coordinati mediante computer infetti.

Gli obiettivi del gruppo Embargo spaziano tra una vasta gamma di entità. Tra essi si annoverano aziende e corporazioni, con l'intento di rubare dati sensibili, segreti commerciali e proprietà intellettuale; governi e infrastrutture critiche, soggetti a spionaggio, sabotaggio e interruzione dei servizi; e individui di alto profilo, i cui conti bancari, identità e privacy vengono compromessi.

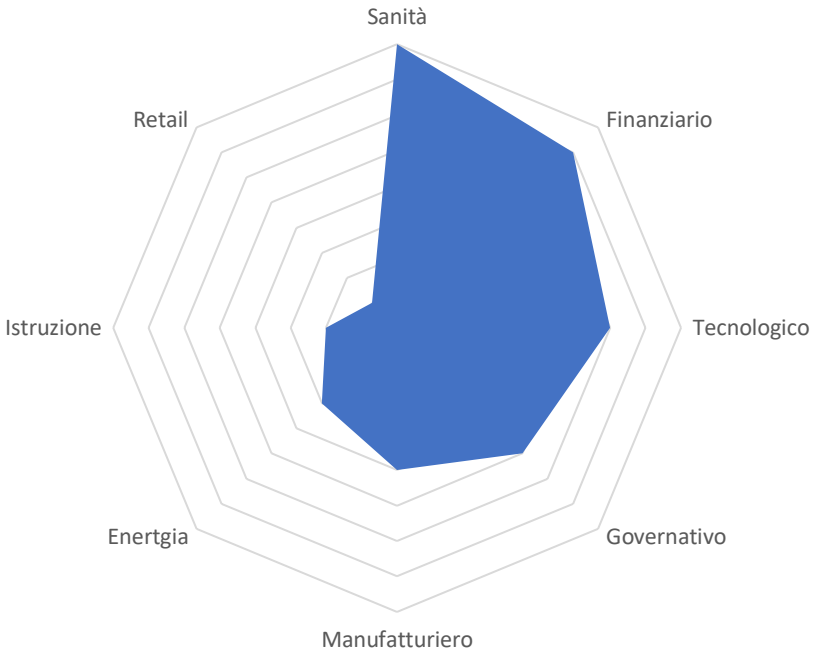


Figura 2 – Settori colpiti da Embargo

Le motivazioni che spingono Embargo ad agire sono principalmente finanziarie, sebbene non manchino ragioni politiche o ideologiche. Alcuni attacchi sono eseguiti per estorcere denaro attraverso il ransomware, mentre altri potrebbero essere commissionati da terze parti con interessi specifici. Embargo è rinomato per la capacità di eseguire attacchi di grande impatto con precisione chirurgica. Tra i colpi più noti si annoverano attacchi ransomware a ospedali, che hanno interrotto servizi medici critici costringendo le istituzioni a pagare ingenti riscatti e la manipolazione di mercati finanziari attraverso l'uso di informazioni rubate per influenzare i mercati e realizzare profitti illeciti.

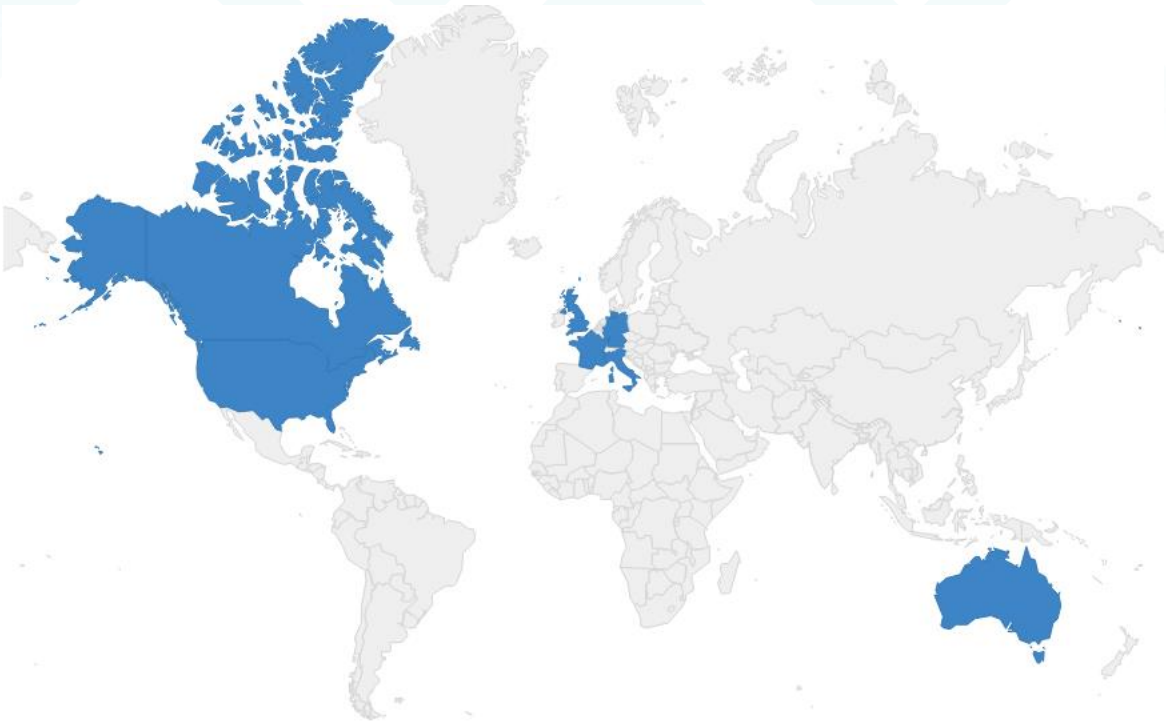


Figura 3 - Paesi colpiti da Embargo

Le forze dell'ordine e le agenzie di cybersecurity di tutto il mondo collaborano incessantemente per contrastare le attività di Embargo, ma l'elevata competenza tecnica del gruppo e la sua capacità di adattamento rendono arduo il compito della loro cattura.

Minacce Android: CapraRAT e l'inganno delle app popolari

Spyware camuffato da app di successo rappresenta un pericolo per gli utenti Android

Il gruppo di cybercriminali di origine pakistana noto come Transparent Tribe (o APT36) ha continuato a diffondere applicazioni Android infette da malware come parte di una strategia mirata di ingegneria sociale verso individui di interesse.

Queste applicazioni malevole, come "Crazy Game", "Sexy Videos", "TikToks" e "Weapons", contengono uno spyware chiamato CapraRAT, una versione modificata di AndroRAT. Questo spyware è stato utilizzato per più di due anni da Transparent Tribe in attacchi mirati al governo indiano e al personale militare. Il gruppo ha una storia di utilizzo di spear-phishing e watering hole per distribuire varie forme di spyware su Windows e Android.

CapraRAT sfrutta WebView per aprire URL verso YouTube o CrazyGames[.]com, mentre in background ottiene accesso non autorizzato a posizione, messaggi SMS, contatti, registri delle chiamate, può effettuare chiamate, scattare screenshot e registrare audio e video.

Una modifica significativa al malware è l'eliminazione di alcuni permessi, indicando un cambiamento verso l'uso dello strumento come mezzo di sorveglianza anziché come backdoor. I recenti aggiornamenti al codice di CapraRAT indicano un focus su maggiore affidabilità e stabilità, oltre a un adattamento per funzionare su versioni più recenti di Android.

Questo sviluppo evidenzia un'evoluzione delle tecniche di attacco impiegate da Transparent Tribe, con un'enfasi su dispositivi più moderni per continuare a prendere di mira obiettivi nel governo indiano e nel settore militare. La comparsa di nuovi tipi di malware come Snowblind, che sfruttano tecniche avanzate per eludere il rilevamento e compromettere dispositivi Android, sottolinea ulteriormente la crescente sofisticazione degli sviluppatori di malware nella regione del sud-est asiatico.

CYBER GEOPOLITICA

Nuovo malware che simula l'effetto della "bomba a grappolo" attivando centinaia di virus

La società di sicurezza Outpost24 rileva un'ondata di attacchi informatici provenienti dalla Russia, con migliaia di file infetti diffusi principalmente negli Stati Uniti, Germania e Turchia.

La società di sicurezza informatica Outpost24 ha identificato l'attività di un nuovo gruppo di cybercriminali di origine russa, denominato Unfurling Hemlock, che si distingue per le sue campagne di attacchi informatici principalmente contro obiettivi negli Stati Uniti, con attività significative anche in Germania e Turchia. Il gruppo utilizza una tecnica di attacco che simula l'effetto di una "bomba a grappolo", in grado di disperdere gli effetti della sua azione attivando centinaia di malware con un singolo attacco.

I ricercatori di sicurezza di KrakenLabs, una divisione di Outpost24, hanno analizzato questa tecnica di attacco, che consente agli aggressori di diffondere una varietà di file infetti attraverso alcuni infostealer come Redline, Mystic Stealer, RisePro, Amadey e SmokeLoad.

L'attività di Unfurling Hemlock sarebbe iniziata nel febbraio del 2023 e finora il gruppo avrebbe distribuito in rete almeno 50.000 file infetti.

Gli attacchi iniziano inducendo le vittime ad aprire un documento che contiene il malware iniziale, WeExtract.exe. Questo malware raggiunge i dispositivi di destinazione tramite e-mail di phishing o programmi utilizzati per scaricare software gratuito. Il file eseguibile contiene ulteriori file nidificati, ciascuno contenente vari campioni di malware. Una volta eseguito il primo file, gli altri vengono attivati in sequenza. Gli specialisti di Outpost24 hanno osservato fino a sette modalità differenti di esecuzione di questa tecnica di attacco "a grappolo", in base alla strategia di hacking adottata e alla vittima presa di mira.

GEOPOLITICA

La Cina richiede ai cittadini di non divulgare le informazioni sensibili

Crescenti misure per prevenire la fuga di informazioni sensibili attraverso i canali online

Il Ministero della Sicurezza dello Stato della Cina ha ufficialmente richiesto ai cittadini di interrompere la pubblicazione online di dettagli riguardanti i satelliti spia nazionali e le installazioni di sicurezza strategiche.

Nella giornata di lunedì, i media statali hanno ampiamente diffuso l'appello del Ministero, esortando gli utenti del web a non contrassegnare le posizioni delle strutture militari sulle mappe digitali e a evitare discussioni su temi militari nei forum online.

Secondo quanto riportato dalle notizie, il Ministero ha sottolineato l'importanza di proteggere le informazioni sensibili relative alla sicurezza nazionale, evidenziando come la divulgazione di tali dettagli possa compromettere la sicurezza e gli interessi del Paese.

L'appello fa parte di una più ampia campagna del governo cinese volta a rafforzare la consapevolezza della sicurezza nazionale tra i cittadini e a prevenire la fuga di informazioni sensibili attraverso i canali online.

Il Ministero ha inoltre invitato i cittadini a segnalare qualsiasi attività sospetta o divulgazione non autorizzata di informazioni riservate alle autorità competenti, al fine di contribuire alla protezione della sicurezza nazionale.

Questa iniziativa si inserisce nel contesto delle crescenti tensioni geopolitiche e delle preoccupazioni riguardanti la sicurezza informatica a livello globale. La Cina sta adottando misure sempre più stringenti per salvaguardare i propri interessi strategici e prevenire potenziali minacce alla sicurezza nazionale.

ACN: le aziende devono rifiutare le richieste di riscatto e smettere di pagare i cybercriminali

Il direttore generale dell'Agenzia per la cybersicurezza Nazionale (ACN), Bruno Frattasi, insiste sull'importanza da parte delle aziende di investire sulla sicurezza informatica attraverso la formazione del personale, non cedendo al pagamento di riscatti

Il forte aumento di casi di attacchi ransomware nei confronti delle aziende e le estorsioni che da essi derivano, comporta la necessità di approcciarsi differentemente all'evento con misure più efficaci e che non danneggino fortemente l'azienda.

Secondo quanto dichiarato dal direttore generale dell'ACN, Bruno Frattasi, nel corso della discussione dei lavori del G7 cyber è emersa l'idea di rifiutare qualunque negoziazione con il cyber criminale, misura che le piccole medie imprese (PMI) fanno fatica ad attuare, desistendo dal pagare una qualsivoglia forma di estorsione.

Le PMI, afferma Frattasi, non si rendono conto che l'accettare le richieste di dell'attaccante pone le basi per una perpetuazione del fenomeno che viene alimentata proprio con il pagamento del riscatto, ricordando come la pratica di congelamento dei beni all'epoca della stagione dei sequestri funzionò.

Il Direttore generale dell'ACN prosegue dicendo di come:

> "...l'attacco ad una superficie digitale può avere effetti su altri soggetti legati nella catena di approvvigionamento. Il pericolo aumenta poi per l'avvento dei sistemi di Intelligenza artificiale: dobbiamo difenderci ancora più strenuamente".

Per questo motivo, afferma Frattasi, investire sulla sicurezza informatica da parte anche degli imprenditori di piccole aziende è fondamentale per proteggere i propri dati e sistemi interni, i dipendenti, e i propri clienti da qualunque minaccia informatica possa verificarsi, attraverso la formazione interna delle competenze e l'aumento del personale addetto, che in molte risulta essere insufficiente e non adeguatamente formato.

Operazione Morpheus: duro colpo al cybercrimine

L'Europol coordina un'operazione di polizia internazionale per smantellare 593 server usati in modo illegittimo per Cobalt Strike

Le forze dell'ordine, in collaborazione con il settore privato, hanno inferto un duro colpo ai cybercriminali che abusavano di Cobalt Strike, un legittimo strumento di sicurezza, per infiltrarsi nei sistemi informatici delle vittime. L'operazione, denominata MORPHEUS, si è svolta dal 24 al 28 giugno ed è stata coordinata dall'Europol.

Durante l'operazione, le autorità hanno segnalato ai fornitori di servizi online 690 indirizzi IP associati ad attività criminali, insieme a una serie di nomi di dominio utilizzati dai gruppi criminali. Entro la fine della settimana, 593 di questi indirizzi erano stati disabilitati, neutralizzando così le versioni non autorizzate di Cobalt Strike.

L'indagine, avviata nel 2021, è stata guidata dalla National Crime Agency del Regno Unito e ha coinvolto autorità di Australia, Canada, Germania, Paesi Bassi, Polonia e Stati Uniti. Europol ha svolto un ruolo chiave nel coordinare l'attività internazionale e nel fare da tramite con i partner del settore privato.

Cobalt Strike, sviluppato da Fortra, è uno strumento progettato per simulare attacchi e identificare punti deboli nella sicurezza. Tuttavia, versioni obsolete e crackate del software sono state utilizzate dai criminali per ottenere accesso non autorizzato ai sistemi e distribuire malware, tra cui RYUK, Trickbot e Conti.

La cooperazione con il settore privato è stata fondamentale per il successo di questa azione. Partner come BAE Systems Digital Intelligence, Trellix, Spamhaus, abuse.ch e The Shadowserver Foundation hanno fornito capacità avanzate di scansione, telemetria e analisi per identificare le attività malevole.

Grazie al regolamento emendato di Europol, l'agenzia può ora collaborare più efficacemente con il settore privato, accedendo a informazioni sulle minacce in tempo reale e acquisendo una prospettiva più ampia sulle tattiche dei cybercriminali. Questo approccio consente una risposta più coordinata e completa, migliorando la resilienza complessiva dell'ecosistema digitale europeo.

L'European Cybercrime Centre (EC3) di Europol ha fornito supporto analitico e forense, facilitando lo scambio di informazioni tra i partner tramite la Malware Information Sharing Platform. Durante l'intera indagine, sono state condivise oltre 730 informazioni sulle minacce, contenenti quasi 1,2 milioni di indicatori di compromissione.

L'operazione MORPHEUS dimostra l'importanza della collaborazione internazionale e del coinvolgimento del settore privato nella lotta al cybercrime. Le forze dell'ordine continueranno a monitorare e ad intraprendere azioni simili finché i criminali continueranno ad abusare di versioni obsolete di Cobalt Strike.

Scoperta una nuova BotNet Golang: Zergeca

Rivelato un potente strumento di attacchi DDoS con funzionalità avanzate e tecniche di evasione raffinate

É stata scoperta una nuova BotNet sviluppata con il linguaggio di programmazione Golang, denominata Zergeca, la quale è in grado di effettuare attacchi distribuiti di negazione del servizio (DDoS).

Nel maggio del 2024, è stato individuato un file ELF sospetto situato nel percorso /usr/bin/geomi, caricato dalla Russia su VirusTotal. Questo file era stato confezionato utilizzando una versione modificata di UPX, ma non era stato segnalato come dannoso. L'analisi dettagliata ha rivelato che il file rappresentava una botnet basata su Golang, chiamata "Zergeca".

La botnet DDoS Zergeca è capace di effettuare sei diversi tipi di attacchi e offre ulteriori funzionalità come proxying, scansione, auto-aggiornamento, persistenza, trasferimento di file, shell inversa e raccolta di informazioni sensibili sui dispositivi compromessi. Tra le sue caratteristiche uniche si annoverano vari metodi di risoluzione DNS, con preferenza per il DNS over HTTPS (DoH) per la risoluzione del comando e controllo (C2), e l'utilizzo dell'inedita libreria Smux per la comunicazione C2, cifrata tramite XOR.

L'analisi ha inoltre rivelato che l'indirizzo IP associato al C2 di Zergeca, è stato collegato ad almeno due BotNet Mirai dal settembre 2023. I ricercatori ipotizzano che l'autore di Zergeca abbia maturato esperienza operando precedentemente con botnet Mirai.

Tra l'inizio e la metà di giugno 2024, la BotNet è stata impiegata per lanciare attacchi DDoS contro organizzazioni situate in Canada, Stati Uniti e Germania. Il tipo principale di attacco rilevato è stato l'ackFlood (atk_4), e gli esperti hanno osservato che le vittime erano distribuite in diversi paesi e appartenenti a vari sistemi autonomi (ASN).

La botnet è strutturata in quattro moduli distinti, denominati rispettivamente persistenza, proxy, silivaccine e zombie. Il modulo silivaccine consente alla botnet di eliminare malware concorrenti, mentre il modulo 'zombie' racchiude l'intera gamma di funzionalità della botnet. Quest'ultimo modulo invia informazioni sensibili dal dispositivo compromesso al C2 e attende comandi, supportando sei tipi di attacchi DDoS, scansione, reverse shell e altre funzioni. Zergeca mantiene la persistenza sui dispositivi infetti aggiungendo un servizio di sistema denominato geomi.service, il quale permette alla botnet di generare automaticamente un nuovo processo geomi in caso di riavvio del dispositivo o terminazione del processo.

CYBER GEOPOLITICA

Apple blocca 25 applicazioni VPN nell'App Store russo su richiesta di Roskomnadzor

Dallo scorso marzo, la Russia ha vietato la diffusione di informazioni su strumenti per aggirare il blocco di contenuti illegali. Confermate le rimozioni di Le VPN, Red Shield VPN, Proton VPN e NordVPN.

I rappresentanti di Roskomnadzor hanno informato i mass media che, su richiesta precisa del dipartimento, Apple ha proceduto a bloccare 25 applicazioni di diversi servizi VPN disponibili nell'App Store della Federazione Russa.

Secondo l'ufficio stampa di RKN, a partire dal 1° marzo 2024, è stato vietato in Russia di diffondere online informazioni che pubblicizzano o favoriscono strumenti per aggirare il blocco di accesso a contenuti illegali. Di conseguenza, Apple ha bloccato le applicazioni mobili di 25 servizi VPN nell'App Store russo, in accordo con le direttive di Roskomnadzor.

La rimozione delle applicazioni è stata confermata dagli sviluppatori di Le VPN e Red Shield VPN, i quali hanno ricevuto una comunicazione da Apple per risolvere la questione in collaborazione con i rappresentanti di Roskomnadzor.

Oltre a Red Shield VPN e Le VPN, sono stati rimossi anche Proton VPN e NordVPN dall'App Store russo, come segnalato da Anton Gorelkin, vicepresidente del comitato per la politica dell'informazione della Duma di Stato, tramite il proprio canale Telegram.

Nel suo intervento, Gorelkin ha sottolineato che Apple è una delle poche aziende americane che si impegna attivamente nel rispettare la legislazione russa e nel mantenere un dialogo costruttivo con l'autorità di regolamentazione. Ha espresso fiducia nel fatto che questo approccio è guidato dal desiderio di consolidare a lungo termine la propria presenza sul mercato russo, pur mantenendo stabili le proprie relazioni commerciali.

Secondo quanto riportato dai media, tra le applicazioni rimosse figurano anche Planet VPN, Hidemy.Name VPN e PIA VPN. Ma, al momento, Roskomnadzor non ha ancora pubblicato i nomi degli altri servizi VPN bloccati nell'App Store.

Nuova minaccia informatica in Italia: Malware VCRuntime

Utilizzo fraudolento della PEC per diffondere software dannoso attraverso falsi messaggi dell'Agenzia delle Entrate

In Italia sta prendendo piede una nuova minaccia informatica denominata VCRuntime, la quale sfrutta la Posta Elettronica Certificata (PEC) per diffondersi. Questo attacco, segnalato dal CERT-AGID, è particolarmente pericoloso in quanto sfrutta la fiducia degli utenti nella PEC, considerata un canale ufficiale e sicuro di comunicazione.

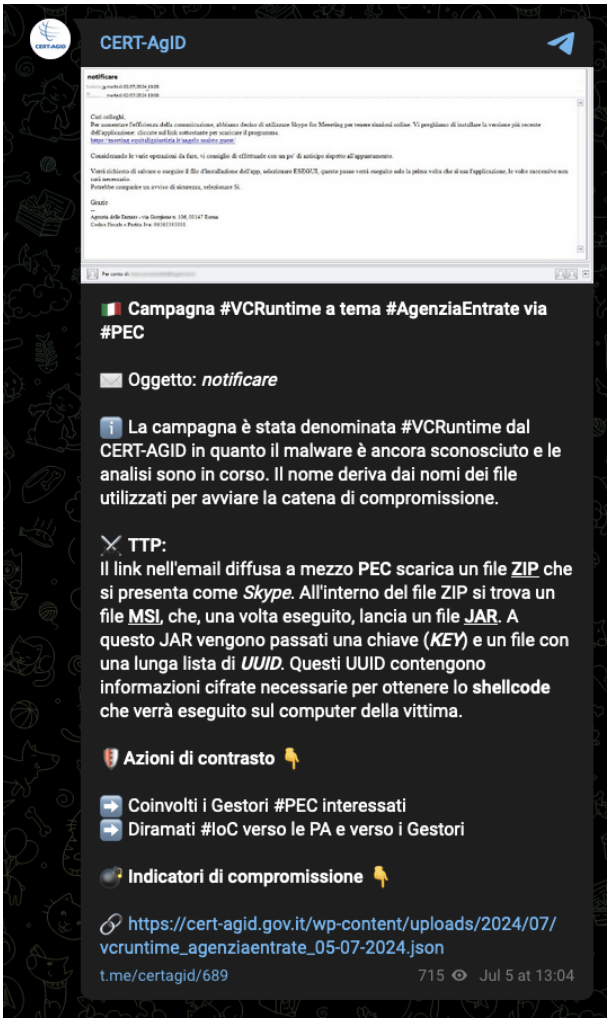
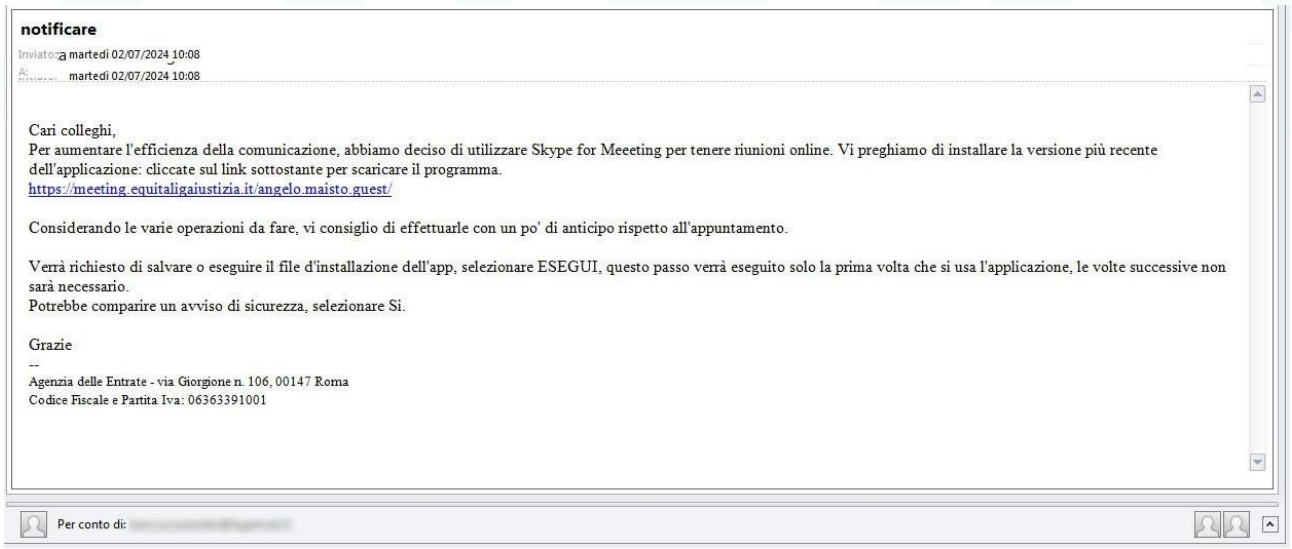


Figura 4 - Post Telegram di CERT-AGID

La modalità di attacco avviene tramite un'e-mail inviata attraverso la PEC, apparentemente proveniente dall'Agenzia delle Entrate. Il messaggio contiene un link che, una volta cliccato, conduce al download di un file ZIP mascherato da Skype. All'interno di questo ZIP si trova un file MSI che avvia un file JAR. Il file JAR, a sua volta, riceve in input una chiave (KEY) e un file contenente una lunga lista di UUID.


notificare

Inviato: martedì 02/07/2024 10:08

A: martedì 02/07/2024 10:08

Cari colleghi,
Per aumentare l'efficienza della comunicazione, abbiamo deciso di utilizzare Skype for Meeeting per tenere riunioni online. Vi preghiamo di installare la versione più recente dell'applicazione: cliccate sul link sottostante per scaricare il programma.
https://meeting.equitaligaiustizia.it/angelo.maisto.guest/

Considerando le varie operazioni da fare, vi consiglio di effettuarle con un po' di anticipo rispetto all'appuntamento.

Verrà richiesto di salvare o eseguire il file d'installazione dell'app, selezionare ESEGUI, questo passo verrà eseguito solo la prima volta che si usa l'applicazione, le volte successive non sarà necessario.
Potrebbe comparire un avviso di sicurezza, selezionare Si.

Grazie
--
Agenzia delle Entrate - via Giorgione n. 106, 00147 Roma
Codice Fiscale e Partita Iva: 06363391001

Per conto di:

Figura 5 - Testo della mail fraudolenta

Team Underground mette nel mirino il settore farmaceutico

La vittima è Ethypharm, azienda farmaceutica internazionale di medie dimensioni in forte crescita negli ultimi anni

Ethypharm è la nuova vittima del gruppo cybercriminale Underground. Come si può evincere dal post pubblicato all'interno del loro Data Leak Site (DLS), Underground ha messo in vendita 875 GB di dati. All'interno del post viene comunicato che i dati in questione includono:

- Dati confidenziali dei dipendenti
- Documenti di assunzioni
- Dati dei partner commerciali
- Fatture
- Progetti
- Dati di laboratorio
- Business plan
- Database SQL e Oracle

Figura 6 - Annuncio su DLS di Team Undergrond

Ethypharm conta più di 1500 dipendenti in tutta Europa, con sedi operative in Francia, Inghilterra, Spagna e Italia e dispone di una presenza commerciale diretta nei mercati di Asia Pacifica, Africa, Medio Oriente, Europa e America.

Per quanto riguarda il gruppo, Underground è attivo da metà 2023 e opera soprattutto con azioni di ingegneria sociale come vettore di attacco iniziale. Una volta ottenuto l'accesso al sistema, procede con la cifratura di tutti i file utilizzando l'algoritmo 3DES per poi rilasciare sul computer delle vittime un file "readme.txt", specificando di essere disposti ad aiutarle a migliorare la sicurezza della loro rete.

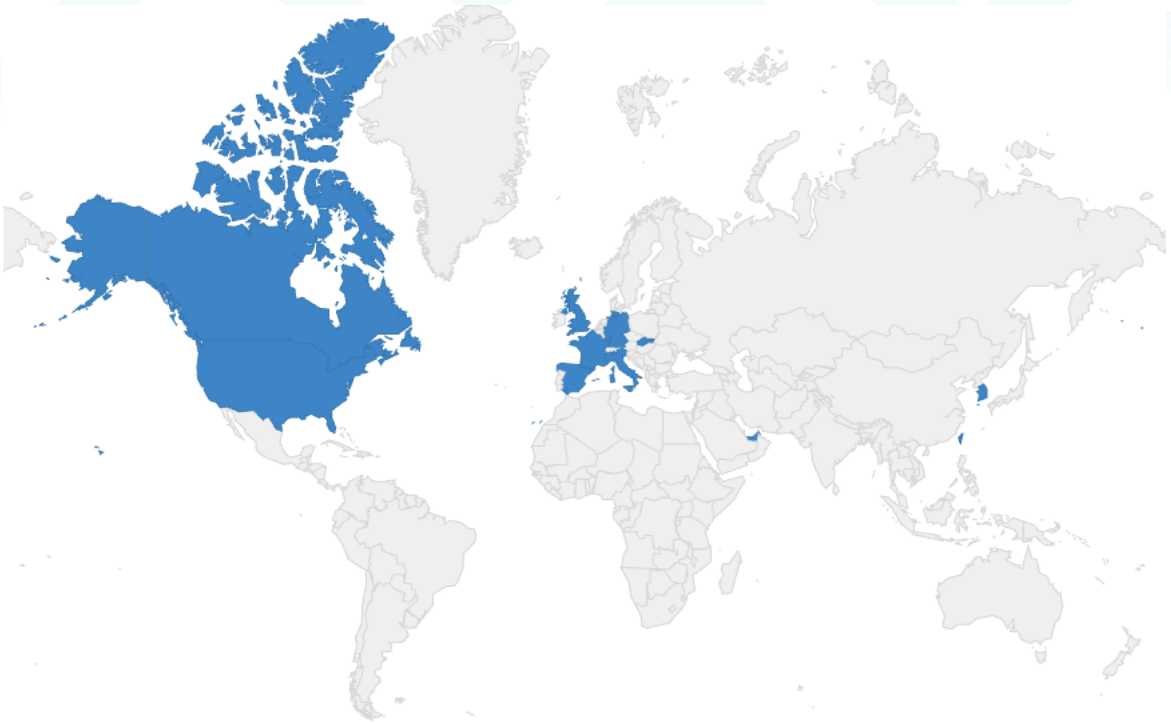


Figura 7 – Paesi colpiti da Underground

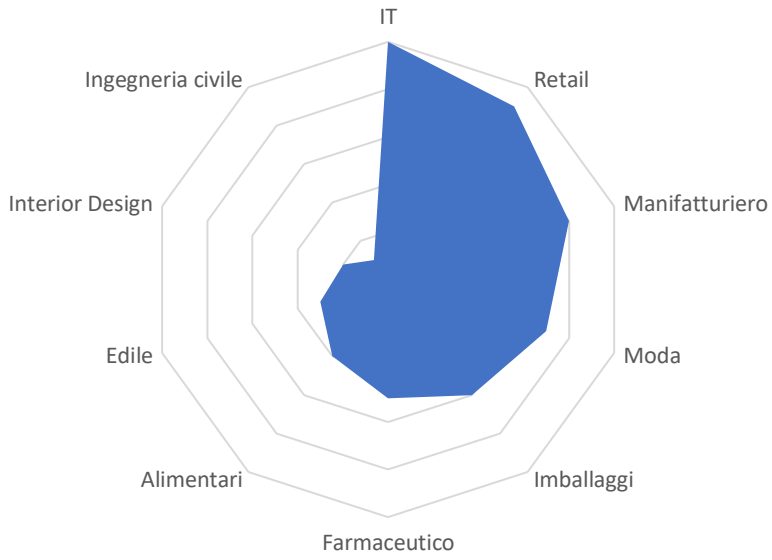


Figura 8 – Settori colpiti da Underground

Prima d'ora, Underground si è reso noto per attacchi in altri settori come ad esempio quello tecnologico, manifatturiero o edile, ma non aveva mai prima d'ora preso di mira quello farmaceutico.

Il futuro della guerra: la rivoluzione del comandante militare virtuale in Cina

Preparazione attraverso simulazioni avanzate e riflessioni sull'impatto dell'Intelligenza Artificiale

La Cina ha presentato il primo comandante militare virtuale al mondo, che sta partecipando a simulazioni di giochi di guerra virtuali per prepararsi al futuro. Questo comandante AI sta apprendendo ed emulando i modelli di pensiero dei comandanti militari reali e ha ricevuto un'eccezionale autorità di comando nei giochi di guerra su larga scala presso l'Università di Shijiazhuang, nella provincia di Hebei.

A differenza degli Stati Uniti, dove l'AI funge da supporto decisionale per i comandanti umani senza prendere decisioni finali, il comandante virtuale cinese può agire autonomamente durante le simulazioni, operando senza interferenze umane nei confini del laboratorio. Tale innovazione risponde alla necessità della Cina di prepararsi a possibili conflitti, come quelli nei territori di Taiwan e nel Mar Cinese Meridionale.

Il team di ricerca, guidato dall'ingegnere senior Jia Chenxing, sostiene che le simulazioni offrano preziose intuizioni su come tali scenari potrebbero evolversi nella realtà. Durante le simulazioni, il comandante AI può assumere ruoli diversi e imitare gli stili di comando di vari generali dell'Esercito Popolare di Liberazione, come il Generale Peng Dehuai e il Generale Lin Bao, ciascuno con approcci distinti alla strategia militare.

Il profilo del comandante virtuale è stato progettato per riflettere quello di uno stratega esperto e calmo, capace di analizzare situazioni con precisione e senza emozioni, fornendo piani pratici basati su decisioni simili prese in passato. Questa tecnologia rappresenta una risposta alla crescente importanza dell'AI nella guerra moderna, anche se persistono preoccupazioni riguardo all'autonomia delle macchine nella gestione di armamenti letali senza un controllo umano adeguato.

L'uso dell'AI nelle operazioni militari è oggetto di dibattiti internazionali, inclusi i suoi potenziali impatti sull'uso delle armi nucleari. Mentre tecnologie avanzate come i velivoli pilotati dall'AI stanno già rivoluzionando l'aviazione militare, rimane fondamentale stabilire regolamenti rigorosi per il loro impiego etico e sicuro.

Sebbene la Cina stia spingendo i confini dell'intelligenza artificiale applicata alla guerra, è chiaro che il controllo finale delle decisioni strategiche e delle operazioni militari rimarrà in mano umana, nonostante il continuo sviluppo di tecnologie che aumentano la capacità di elaborazione e di decisione delle macchine.

MERIDIAN GROUP

MERIDIAN SRL
Viale dell'Oceano Atlantico,
182 – Roma – Italy

p.Iva: 13693001003

www.meridian-group.eu
info@meridian-group.eu