CYBER INTELLIGENCE REPORT

MERIDIAN GROUP

WEEKLY UPDATE

TLP: GREEN

DATA: 29.04.2024

Sommario

Indice 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.

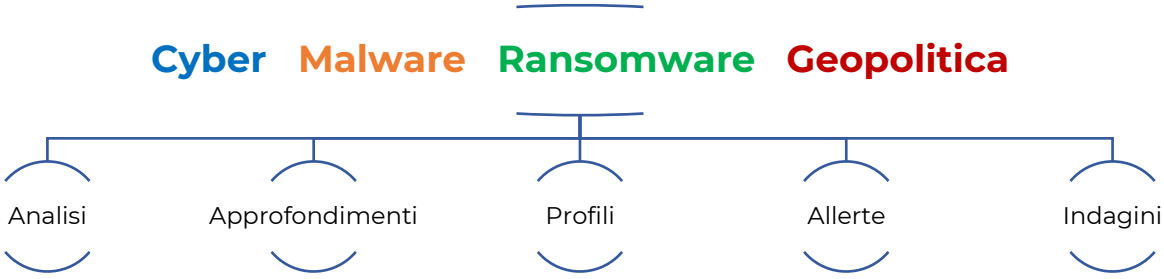
Kitsune è una piattaforma di Cyber Intelligence che si pone l'obiettivo di essere uno strumento indispensabile per gli analisti di intelligence.

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.

Il peso delle responsabilità: le dimissioni del Generale Haliva

Motivi e conseguenze delle dimissioni del capo dell'intelligence militare israeliana in seguito all'attacco di Hamas e alle risposte iraniane

Il generale israeliano Aharon Haliva ha deciso di dimettersi in seguito alla catastrofe avvenuta il 7 ottobre, quando Hamas è riuscita a superare un blocco che si riteneva insormontabile, causando la morte di 1.200 persone e la cattura di 253 ostaggi. In una mossa inaspettata, Haliva, che ricopriva il ruolo di capo della direzione dell'intelligence militare delle Forze Armate Israeliane (IDF), ha reso le sue dimissioni notificate al capo di stato maggiore Herzi Halevi attraverso una lettera, nella quale ha dettagliato le ragioni della sua decisione.

Figura 1 - Generale delle IDF Haliva

Il comunicato ufficiale delle forze armate ha rivelato che, in accordo con il capo di stato maggiore e con l'approvazione del ministro della difesa, Haliva lascerà la sua posizione e si ritirerà dall'IDF dopo aver garantito la nomina di un successore attraverso un processo organizzato e professionale. Sebbene resti in carica temporaneamente, è stato confermato che le sue dimissioni sono state accettate.

Tuttavia, la catena di errori e l'aver sottovalutato gravemente le capacità di Hamas costituiscono un peso sulla coscienza del generale e su tutta la gerarchia militare israeliana, che dovrà affrontare le conseguenze di tali errori, prima o poi. Questa responsabilità diventa ancora più evidente con il protrarsi dell'emergenza della crisi, che minaccia di estendersi con un'operazione terrestre a Rafah.

Inoltre, Haliva deve confrontarsi con un altro grave errore: nonostante un attacco mirato ai Pasdaran ospitati nell'ambasciata iraniana a Damasco, preparato con due mesi di anticipo e dopo un'analisi dettagliata delle possibili reazioni iraniane e delle contromisure israeliane necessarie, l'intelligence militare ha sottovalutato ampiamente la risposta dell'Iran. Per la prima volta, l'Iran ha colpito direttamente il suolo israeliano, penetrando l'Iron Dome.

Nella sua lettera di dimissioni, Haliva ha assunto la piena responsabilità per il fallimento del 7 ottobre, impegnandosi a fare del suo meglio nel tempo che gli rimane in carica per perseguire gli obiettivi prestabiliti. Tra questi, vi è il ripristino del dominio militare nel nord e nel sud della Striscia di Gaza, il recupero degli ostaggi e la dissuasione dalle minacce iraniane e di altri nemici. Il generale ha condiviso il peso del "giorno nero" e del "dolore della guerra", riconoscendo che la divisione di intelligence sotto il suo comando non è stata all'altezza del compito assegnatogli.

La sua dimissione rappresenta soltanto il primo passo di un inevitabile processo di rendiconto per l'incidente del 7 ottobre. Anche il generale Herzi Halevi, capo di stato maggiore, si è dichiarato responsabile per il fallimento poco dopo il massacro. È ampiamente previsto che Halevi si dimetterà non appena avrà portato a termine il suo incarico. Le pressioni dell'opinione pubblica contro i vertici militari sono sempre più forti, non solo per l'incidente del 7 ottobre che ha scosso l'intero paese, ma anche per il mancato recupero degli ostaggi e per la fuga dell'insurrezionista Yayah Sinwar.

Non solo la catena di comando militare è chiamata a rispondere per gli errori commessi, ma anche il mondo politico ne subisce le conseguenze. Vladimir Beliak, del partito Yesh Atid dell'opposizione guidata da Lapid, ha twittato la richiesta di istituire immediatamente una commissione d'inchiesta statale e ha chiesto le dimissioni immediate del primo ministro.

Nuovo Malware mirato ai Professionisti IT: MadMxShell

Una nuova backdoor si diffonde attraverso pubblicità ingannevoli e tecniche avanzate, mettendo a rischio la sicurezza delle reti aziendali.

È stata individuata una nuova campagna malware mirata ai professionisti IT, che sfrutta annunci ingannevoli su note utilità online per introdurre una nuova backdoor chiamata MadMxShell.

Questa campagna è inziata a marzo di quest'anno, quando i cybercriminali hanno creato domini molto simili a quelli ufficiali di noti software per la scansione degli indirizzi IP e la gestione di reti, come Advanced IP Scanner e Angry IP Scanner. Una volta che l'utente fa click sull'annuncio viene reindirizzato a una pagina che sembra essere il sito ufficiale dello sviluppatore, nel quale è offerta la possibilità di scaricare un file dannoso che in realtà contiene la backdoor MadMxShell.

MadMxShell utilizza un processo complesso in diverse fasi per evitare la rilevazione da parte degli strumenti di sicurezza standard. Il processo di avvio avviene attraverso la tecnica del sideloading DLL, in cui un programma legittimo carica una DLL malevola, che a sua volta scarica componenti aggiuntivi per stabilire una comunicazione con il server di comando e controllo dei cybercriminali.

Un aspetto particolarmente importante di MadMxShell è l'uso di query DNS MX per comunicare con il server di gestione. Questa tecnica sfrutta il protocollo DNS in modo non convenzionale, rendendo difficile il monitoraggio delle attività dannose. Infine, MadMxShell utilizza tecniche di analisi anti-memoria, complicando il lavoro degli analisti nel comprendere il suo funzionamento.

GEOPOLITICA

Tensioni Cina-Taiwan

Analisi dei recenti eventi e delle strategie politiche nell'ambito del crescente confronto tra Cina e Taiwan

L'analisi odierna delle tensioni Cina-Taiwan si concentra sui tentativi del Partito Comunista Cinese (PCC) di ottenere il controllo su Taiwan e sugli sviluppi nello Stretto di Taiwan.

- In particolare la Repubblica Popolare Cinese (RPC) ha aperto unilateralmente due rotte aeree in direzione est vicino allo spazio aereo di Taiwan sopra le isole Kinmen e Matsu. Questa azione potrebbe far parte degli sforzi del PCC per mettere pressione alla consapevolezza situazionale di Taiwan riguardo al proprio spazio aereo, specialmente in vista dell'insediamento del nuovo governo di Lai Ching-te.
- I dazi imposti dalla RPC sulle esportazioni di policarbonato di Taiwan potrebbero essere parte di una campagna di pressione prima dell'inaugurazione presidenziale di Lai Ching-te il 20 maggio.
- L'ex presidente della ROC Ma Ying-jeou ha incontrato il presidente del Kuomintang Eric Chu il 16 aprile per discutere di modifiche a una legge che contrasta l'interferenza politica della RPC a Taiwan.
- L'Esercito di Liberazione del Popolo (PLA) ha diviso la Forza di Supporto Strategico in tre branche distinte per raggiungere il "dominio dell'informazione" e una maggiore superiorità operativa attraverso l'integrazione delle forze.
- Il Ministero degli Affari Esteri della RPC ha sottolineato l'importanza di affrontare le sanzioni statunitensi contro le aziende cinesi durante la visita del Segretario di Stato Antony Blinken in Cina.
- Il portavoce del Ministero degli Affari Esteri della RPC ha criticato il dispiegamento da parte dell'esercito degli Stati Uniti del missile da crociera terrestre Typhon e del lanciatore di missili di difesa aerea sull'isola filippina di Luzon, descrivendolo come "provocatorio".
- La RPC ha aperto due rotte aeree in direzione est vicino allo spazio aereo taiwanese sopra le isole Kinmen e Matsu, probabilmente come parte degli sforzi del PCC per esercitare pressione su Taiwan prima dell'inaugurazione del nuovo governo di Lai Ching-te. La Civil Aviation Administration of China (CAAC) ha anche modificato la rotta M503 a gennaio 2024, spostandola più vicino alla linea mediana dello Stretto di Taiwan e annunciando la possibilità di voli in direzione est lungo le rotte W122 e W123 il 19 aprile.
- L'amministrazione dell'aviazione civile di Taiwan ha condannato queste nuove rotte e ha promesso di rispondere a eventuali incursioni nello spazio aereo senza autorizzazione. Un funzionario taiwanese ha dichiarato che queste azioni fanno parte di un modello di pressioni politiche sulla nuova amministrazione di Lai Ching-te.

Dev Popper: campagna di hacking mirata agli sviluppatori di software

Analisi di un sofisticato attacco di ingegneria sociale che distribuisce trojan di accesso remoto tramite finte opportunità di lavoro.

Una recente campagna di hacking denominata Dev Popper ha preso di mira gli sviluppatori di software, utilizzando tattiche sofisticate di ingegneria sociale per compromettere i loro sistemi. Gli aggressori si spacciano per datori di lavoro legittimi, pubblicizzando posizioni IT fittizie per attirare potenziali vittime.

L'obiettivo principale di questa campagna è distribuire un pericoloso trojan di accesso remoto (RAT) basato su Python sui computer delle vittime. Durante una falsa fase di colloquio, i candidati sono stati indotti a completare un "compito di test" che consisteva nello scaricare ed eseguire codice da un repository su GitHub.

L'attacco è stato orchestrato in diverse fasi, inizialmente con il suggerimento di scaricare un archivio ZIP contenente un pacchetto di supporto NPM, completo di file README.md e cartelle separate per il codice client e server.

Successivamente, un file JavaScript mascherato denominato imageDetails.js nella directory backend è stato attivato. Questo file, eseguito tramite Node.js, ha utilizzato comandi curl per scaricare un archivio ZIP crittografato da un server esterno.

All'interno di questo archivio ZIP si trovava il componente principale dell'attacco: uno script Python nascosto, ovvero il Trojan stesso. Una volta installato sulla macchina infetta, il RAT raccoglieva informazioni di base sul sistema operativo, nome host e dati di rete, inviandoli al server degli aggressori.

Oltre alla raccolta di dati, il Trojan forniva funzionalità avanzate, inclusa una comunicazione stabile per il controllo remoto, comandi per rilevare e rubare file dal sistema, possibilità di eseguire codice dannoso a distanza, trasferimento diretto dei dati tramite FTP e cattura delle sequenze di tasti e dati degli appunti per rubare credenziali.

Le tattiche utilizzate nella campagna Dev Popper potrebbero essere attribuite a gruppi hacker della Corea del Nord noti per l'uso di ingegneria sociale. Tuttavia, al momento non ci sono prove sufficienti per attribuire direttamente questi attacchi alle autorità della RPDC.

Gli aggressori sfruttano abilmente la fiducia degli specialisti IT nel processo di assunzione, inducendoli a seguire istruzioni apparentemente legittime per non perdere opportunità di lavoro potenzialmente vantaggiose. Questo approccio ha reso l'attacco particolarmente efficace nell'ingannare le vittime.

Progress Flowmon: CVE-2024-2389

Una nuova pericolosa vulnerabilità è stata rilevata per il noto software di monitoraggio e analisi delle prestazioni di rete.

La falla di sicurezza, identificata come CVE-2024-2389, è una vulnerabilità che consente ad un possibile utente malintenzionato l'accesso non autenticato a Flowmon, una soluzione di monitoraggio delle prestazioni di rete utilizzata da oltre 1.500 aziende in tutto il mondo, tramite API. La pericolosità in particolare è dovuta al fatto che una volta eseguito l'accesso, l'utente si ritrova di fronte l'interfaccia di gestione di Flowmon e può eseguire comandi di sistema arbitrari, mettendo a rischio i dati sensibili e le configurazioni di rete.

L'importanza di Flowmon risiede nel suo ruolo nel supportare le aziende nell'ottimizzazione delle infrastrutture di rete, nella individuazione e prevenzione delle anomalie e nel controllo del traffico per proteggere i dati. Tuttavia, la scoperta di questa vulnerabilità mette in evidenza i rischi associati a software critici utilizzati per la sicurezza e la gestione delle reti.

Per mitigare il rischio, Progress Software ha prontamente informato gli utenti della vulnerabilità e ha rilasciato patch di sicurezza per le versioni di Flowmon precedenti alla 11.1.14 e alla 12.3.5. L'aggiornamento è fondamentale per eliminare la possibilità di sfruttamento della vulnerabilità e prevenire attacchi dannosi che potrebbero compromettere dati e configurazioni di rete.

Infine, l'incidente sottolinea l'importanza di implementare una strategia di sicurezza informatica completa, che include monitoraggio costante delle attività anomale, l'uso di firewall, antivirus e backup regolari, oltre a educare i dipendenti e i clienti sulle buone pratiche di sicurezza informatica.

Violati i sistemi Volkswagen: rubati oltre 19.000 documenti

Hacker cinesi prendono di mira lo sviluppo tecnologico dell'iconico produttore automobilistico tedesco per oltre cinque anni

Gli aggressori, di probabile provenienza cinese, hanno preso di mira, con successo, il gigante automobilistico tedesco Volkswagen rubando oltre 19.000 documenti, nel periodo compreso tra il 2010 e il 2015, riguardanti:

- dati sulla mobilità elettrica;
- lo sviluppo di motori a benzina;
- la ricerca sulle trasmissioni a doppia frizione.

Analizzando gli indirizzi IP degli aggressori, il software utilizzato e il fuso orario è stata effettuata l'azione di hacking è stato possibile ipotizzare che il gruppo criminale sia localizzato in Cina.

Sandworm mira a destabilizzare le organizzazioni critiche in Ucraina

Nuovi attacchi contro i sistemi informatici di organizzazioni fornitrici di acqua, energia e riscaldamento

Il gruppo di cybercriminali Sandworm ha attaccato circa venti infrastrutture critiche in Ucraina. Secondo il Computer Emergency Response Team (CERT) ucraino, i criminali informatici - tra cui BlackEnergy, Seashell Blizzard, Voodoo Bear e APT44 - sono associati al Direttorato principale dello Stato Maggiore delle Forze Armate (GRU) della Russia, e mirano a creare caos nelle infrastrutture del paese. Il mese scorso, APT44 ha violato i sistemi informatici dei fornitori di acqua, energia e riscaldamento in 10 regioni dell'Ucraina. E la stessa situazione sembra essersi ripetuta per altre organizzazioni, colpite dal malware di Sandworm.

Figura 2 - Logo del gruppo Sandworm

All'interno del rapporto tecnico del CERT si legge che i cybercriminali russi sono riusciti a violare gli obiettivi a causa delle cattive pratiche di sicurezza informatica delle infrastrutture, che non avrebbero curato i sistemi come dovuto.

I tecnici del CERT, successivamente, hanno scelto di adottare "misure per informare tutte le imprese identificate, e per indagare e contrastare le minacce informatiche nei sistemi ICS pertinenti". Più nel dettaglio, una volta identificato il malware, gli esperti di sicurezza si sono occupati prima di rimuoverlo e poi di installare un'adeguata tecnologia di sicurezza. Allo stato attuale delle cose, quindi, la situazione sembrerebbe essere tornata normale per buona parte delle infrastrutture colpite. Ma è abbastanza chiaro che la cybergang Sandworm abbia un obiettivo chiaro: compromettere la serenità delle organizzazioni critiche ucraine, infiltrandosi nei loro sistemi.

Nuovo Trojan Bancario Brokewell

Brokewell il malware che si nasconde dietro falsi aggiornamenti per chrome

È stato individuato un nuovo software dannoso di tipo trojan bancario, noto come Brokewell. Questo malware si presenta come falsi aggiornamenti per Chrome e ha la capacità di monitorare ogni azione che avviene sul dispositivo, inclusi clic, informazioni visualizzate sullo schermo, testo inserito e applicazioni avviate dall'utente. Il creatore di Brokewell è un hacker noto con il soprannome di Baron Samedit, dedito da almeno due anni alla vendita di strumenti per il controllo di account rubati.

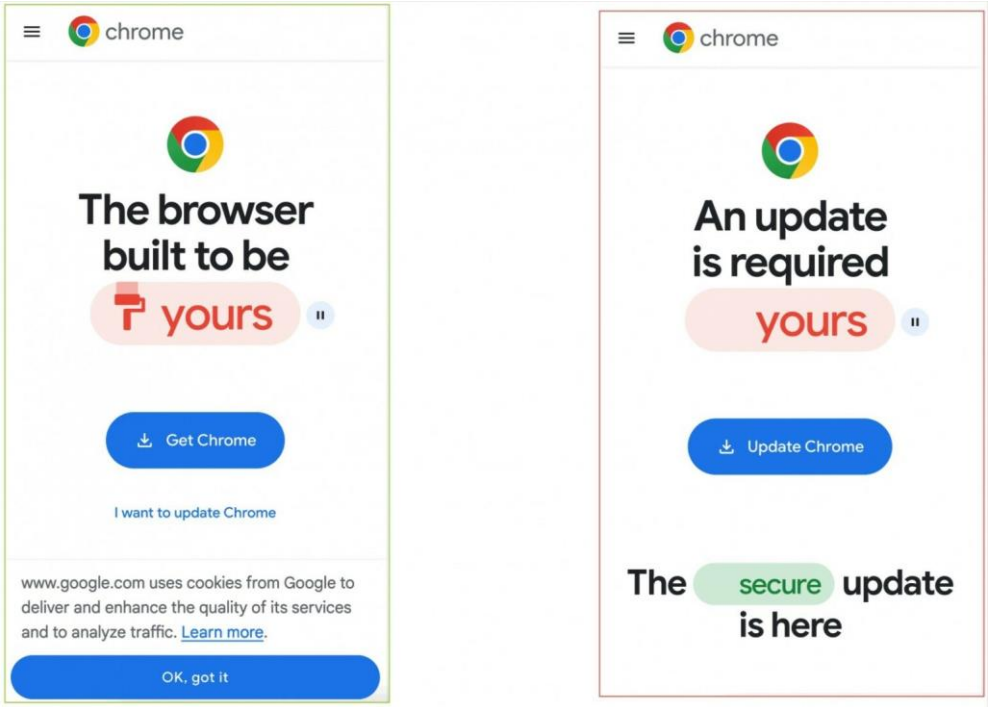


Figura 3 - Pagina Chrome reale (a sinistra) e aggiornamento falso (a destra)

Brokewell è stato scoperto dopo aver identificato una pagina fraudolenta di aggiornamento per Chrome che trasportava il codice malevolo del malware. In passato Brokewell si è camuffato da servizi di "acquista ora, paga dopo" e si è presentato come l'applicazione di autenticazione digitale austriaca ID Austria.

Le funzionalità principali di Brokewell, attualmente in fase di sviluppo attivo, si concentrano sul furto di dati e sulla possibilità di consentire agli aggressori di controllare remotamente un dispositivo infetto. Brokewell offre tutte le caratteristiche standard dei trojan bancari e consente anche l'accesso remoto agli aggressori.

Inoltre, è stato scoperto un altro strumento correlato chiamato Brokewell Android Loader, anch'esso creato da Baron Samedit e ospitato su uno dei server di controllo di Brokewell. Questo downloader è in grado di eludere le restrizioni introdotte da Google in Android 13 e versioni successive per contrastare l'abuso del servizio di accessibilità da parte di APK caricati al di fuori del Google Play Store.

Utenti Apple sotto attacco

È in corso una nuova campagna di attacchi multi fattore per ottenere l'accesso agli account degli utenti Apple

Gli utenti di dispositivi Apple sono stati recentemente messi in guardia riguardo a una campagna di attacchi di autenticazione multi-fattore. Questa campagna sembra essere mirata a individui specifici, che vengono inondati di richieste di reimpostazione della password. L'obiettivo di questi attacchi, simile ad altri avvenuti nel corso degli anni, è quello di far arrivare il maggior numero di notifiche di approvazione agli utenti fino a far si che erroneamente facciano click su una di esse per consentire a qualcuno di cambiare la loro password.

Un esempio di come funziona questo attacco è stato fornito da Parth Patel, un imprenditore di AI. Circa 15 minuti dopo aver cancellato le notifiche, Patel ha riferito di essere stato chiamato da qualcuno che falsificava il proprio ID chiamante per fingere di chiamare dalla linea di supporto effettiva di Apple. Il chiamante ha informato Patel che il suo account era sotto attacco e gli ha chiesto di verificare le sue informazioni e fornire un codice di reimpostazione una tantum.

Tuttavia, Patel, sospettoso della natura della chiamata, ha chiesto loro di verificare alcune delle sue informazioni personali, e il chiamante è stato in grado di farlo, per la maggior parte. Fortunatamente per Patel, controlla regolarmente quali delle sue informazioni personali sono disponibili online e in questo caso le sue informazioni erano state ottenute dall'azienda americana, PeopleDataLabs.

Il fatto che il truffatore abbia chiamato Patel direttamente suggerisce che erano in grado di inviare richieste di reimpostazione della password utilizzando la pagina iForgot di Apple. Il volume di richieste solleva la possibilità che Apple possa avere un difetto di limitazione del tasso di richieste consentite nel suo sistema iForgot che consente di bombardare gli utenti con richieste di reimpostazione ripetute.

In conclusione, è importante che gli utenti di Apple siano consapevoli di questi attacchi e prendano le misure necessarie per proteggere i loro account. Questo può includere l'aggiornamento delle impostazioni di sicurezza, la verifica delle richieste di reimpostazione della password e la segnalazione di qualsiasi attività sospetta all'assistenza clienti di Apple

MERIDIAN GROUP

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

p.Iva: 13693001003

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