Google scopre vulnerabilità sugli iPhone, rubati dati personali degli utenti



Bastava visitare siti malevoli attraverso un iPhone per diventare bersaglio di cybercriminali che potevano prendere il controllo del telefono e attingere a dati personali degli utenti, posizione, foto. In pratica monitorarli. Lo riporta oggi il Guardian dove a scoprire, a febbraio scorso, le falle di sicurezza di Apple è stato un gruppo di ricercatori di **Google Project Zero**, il team che si occupa di attacchi informatici 'zero days' cioè quelli di cui non sono a conoscenza neanche gli sviluppatori o le aziende informatiche che hanno creato i software. **Cupertino**, dopo la segnalazione dei ricercatori ha corretto le vulnerabilità.

"*La semplice visita al sito compromesso era sufficiente affinché il server attaccasse il dispositivo e, in caso di successo, installasse un impianto di monitoraggio*", ha

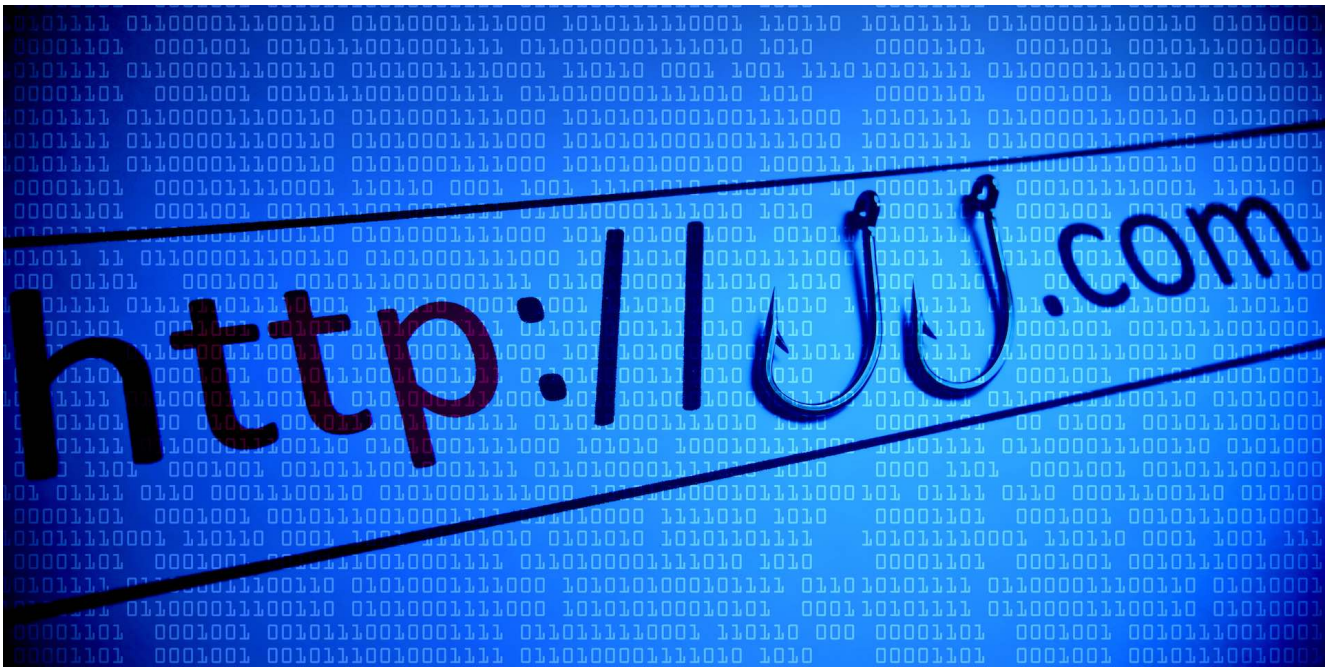
spiegato **Ian Beer** in un post pubblicato sul blog di Project Zero. In pratica, gli hacker potevano avere accesso all'iPhone, installando applicazioni dannose e anche monitorando l'attività dell'utente a sua insaputa. Per i ricercatori di Google, le vulnerabilità del sistema operativo sarebbero state sfruttate sia per rubare foto e messaggi, che per rintracciare la posizione in tempo reale di dispositivi e utenti. Gli esperti di Google hanno segnalato la scoperta a Cupertino lo scorso 1 febbraio. I vertici americani hanno subito rilasciato le correzioni per evitare problemi legati alla sicurezza, lanciando il 7 febbraio l'aggiornamento iOS 12.1.4, proprio per correggere i problemi riscontrati nelle versioni precedenti.

Le vulnerabilità erano presenti in quasi tutte le versioni di iOS 10 e fino all'ultima versione di iOS 12, il sistema operativo per dispositivi mobili di Cupertino. "*Questo* – aggiunge Ian Beer – *indica che un gruppo stava compiendo uno sforzo prolungato per hackerare gli utenti di iPhone su un periodo di almeno due anni". Secondo i ricercatori, inoltre, alla base delle vulnerabilità ci sono "codici che sembra non abbiano mai funzionato"* oppure *"abbiano avuto pochi test o revisioni prima di essere resi disponibili agli utenti*".

https://www.key4biz.it/google-scopre-vulnerabilita-sugli-iphone-rubati-dati-personali-degli-utenti/269160/

Cybercrime, aumentano gli attacchi phishing in Italia.

Come difendersi



In Italia e nel mondo continuano ad aumentare gli attacchi del cybercrime di tipo phishing. Secondo gli esperti di cybersecurity il fenomeno è in crescita a causa di due elementi: da una parte la disponibilità di liste infinite di email, in vendita per pochi soldi sul dark web o sui forum degli hacker. Dall'altra la costante disattenzione degli utenti quando ricevono un messaggio o navigano su Internet.

Il phishing è una truffa veicolata tramite Internet, in cui si cerca di ingannare la vittima al fine di recuperare informazioni sensibili come username, password o dati bancari. Generalmente, il criminale informatico invia false comunicazioni al soggetto-vittima, fingendosi un Ente o un'azienda ben conosciuta o con cui è possibile che si stiano avendo conversazioni e relazioni, usando scuse plausibili per ottenere i dati personali della vittima.

6 consigli su come difendersi

1. **mantenere il proprio browser sempre aggiornato.** Installando le ultime versioni e inserendo dei filtri anti-spam, o degli appositi plug-in

2. **controllare il dominio da cui proviene la comunicazione.** Una società o un ente scriveranno sempre dal proprio dominio, bisogna controllare che corrisponda a quello ufficiale. Questa verifica non dà la massima garanzia di autenticità ma rappresenta un primo controllo da poter effettuare;
3. **fare attenzione a cliccare sui link nelle e-mail.** Come buona norma si consiglia di non cliccare mai sui link contenuti nella comunicazione ma digitare direttamente nel browser l'indirizzo del sito ufficiale del mittente della comunicazione e verificare sul sito il contenuto descritto nella comunicazione dell'e-mail;
4. **utilizzare più indirizzi e-mail.** Quando ci si iscrive a servizi, o siti web, di dubbia affidabilità, è preferibile utilizzare e-mail secondarie, in modo da non rischiare di contaminare la propria casella e-mail principale;
5. **contattare il servizio clienti.** Se arriva una e-mail ambigua e non si capisce con certezza se sia una frode o meno, è meglio contattare il servizio clienti dell'azienda a cui la mail fa riferimento.
6. **segnalare un sito di phishing** aiutando altri utenti a non cadere nella truffa.

Cybercrime, aumentano gli attacchi phishing in Italia. Come difendersi

---

Cyber Security, trasformare

l’anello debole in punto di forza

Tutti coloro che abbiano vissuto l’esperienza di aver avuto il proprio computer violato o infettato da un virus, hanno vivo il ricordo di quanto sia stato fastidioso e soprattutto quanto sia stato costoso in termini di tempo e denaro ripristinarlo Ciò dovrebbe rendere la disciplina della sicurezza informatica un’abitudine da seguire regolarmente. Eppure è rimandata in secondo piano una volta che il danno è stato risolto. Non solo gli individui, ma anche le aziende, le istituzioni pubbliche e persino i governi sono vittime del **crimine informatico**; per questi ultimi, le conseguenze possono essere ancora più gravi rispetto a quanto avviene per gli individui.

Nella primavera del 2017, il programma *WannaCry* (***ransomware***) si è infiltrato in aziende e organizzazioni in 150 paesi. Ha bloccato l’accesso ai file su qualsiasi computer infetto e ha chiesto all’utente di pagare un determinato importo per ottenere le chiavi di sblocco. Tra le sue vittime ci fu il servizio sanitario nazionale nel Regno Unito. Per molti pazienti britannici, ciò significò che le loro consultazioni furono cancellate, gli interventi chirurgici previsti impossibilitati ad essere compiuti. Su una scala più ampia, le perdite economiche derivanti da quest’attacco informatico sono state stimate in circa 4 miliardi di dollari USA. Questo è solo un esempio di violazione della sicurezza informatica. In realtà, esiste una varietà di approcci che gli aggressori usano per infettare computer e server.

Un attacco informatico tecnologicamente semplice e tuttavia molto efficace è il ***phishing***. Quest’attacco avviane impiegando una e-mail, un messaggio di testo o un sito Web falsi, creati accuratamente per sembrare legittimi. Alcuni di tali attacchi hanno lo scopo di acquisire informazioni, nel testo del messaggio phishing si chiede di inserire i dettagli della

carta di credito o di confermare la password. Altri hanno la finalità di installare malware sul computer una volta aperto un allegato contenuto nel messaggio fasullo.

E in fine ci sono alcuni attacchi phishing in cui il messaggio falso è realizzato in modo da apparire proveniente da un superiore o da un amico e nel testo del messaggio si chiede di trasferire un determinato importo di denaro.



Uno studio ha scoperto che il 78% delle persone testate ha affermato di essere consapevole del rischio di una e-mail sconosciuta. Tuttavia, il 45% dei partecipanti ha effettuato comunque un click su un collegamento presente in una e-mail falsa. È interessante notare che, quando venga chiesto ai partecipanti se abbiano effettuato il click solo la metà conferma di averlo compiuto.

Un altro tipo di attacco è veicolato attraverso ***malware***. Il malware è un software che può essere scaricato da un'e-mail di phishing o facendo clic su un collegamento da un sito Web pubblicitario o anche direttamente da una chiavetta USB. Tale software è progettato per ottenere l'accesso in modo non autorizzato al sistema. Può alterare, eliminare o rubare informazioni da un dispositivo. Può anche potenzialmente diffondersi ad altri utenti sulla rete domestica o aziendale Esistono diverse sottocategorie appartenenti all'ampio ombrello di malware: virus, spyware o ransomware come nell'esempio di WannaCry. La maggior parte degli obiettivi di

tali attacchi sono le aziende che hanno dati preziosi da proteggere.

Un terzo tipo di attacco è noto con il suo acronimo **DDoS** (*Distribuited Denial of Service*). In questa tipologia di attacco un server viene preso di mira da una quantità soverchiante di richieste con l'obiettivo di impedirne l'operatività rendendo in tal modo indisponibili i servizi in esso ospitati. DDoS è un attacco relativamente più sofisticato rispetto ai precedenti, perché di solito coinvolge un hacker che, accedendo a molti dispositivi infetti, attiva l'invio di richieste contemporanee verso il server destinazione dell'attacco.

Un ultimo tipo di attacco, prevede che l'intruso entri in un'azienda durante una pausa pranzo, si sieda alla scrivania su cui un computer è sbloccato, installi un malware, rubi dati o invii un'e-mail, e quindi se ne vada. Semplice ma incredibilmente pericoloso.

L'elenco delle possibili minacce, dei tipi di veicoli d'infezione, delle motivazioni di attacco, degli attori nel ruolo di attaccanti evolve nel tempo. Nel migliore dei casi un attacco informatico è fastidioso. Nel peggiore dei casi, può totalmente interrompere il modo in cui i governi e le aziende gestiscono le loro operazioni quotidiane. Sebbene le aziende e le istituzioni pubbliche investano sempre più risorse in soluzioni di sicurezza informatica; tali investimenti non tengono il passo del numero di minacce che raddoppia circa ogni anno.

In particolare, in ambito governativo, legislativo e regolamentare sono stati profusi ingenti sforzi al fine di rafforzare la sicurezza informatica promovendo iniziative di scambi di informazioni, condivisioni di paradigmi di sicurezza, esercitazioni congiunte. Quanto fino ad ora indicato evidenzia la mancata corrispondenza tra una crescita esponenziale della tecnologia di offesa e una crescita lineare

della reazione del business.

Si rammenta spesso che l'anello debole nella catena di difesa informatica alloggi fra il monitor di un computer e la sedia della scrivania. Per affrontare in modo sostenibile il rischio cibernetico, tenendo conto dei differenti tassi di crescita tecnologica offensiva e di risposta del business, è necessario un approccio a livello di organizzazione che trasformi l'anello debole nel collante unico e prezioso per la difesa.

Quindi è necessario che attraverso una leadership situazionale sia promossa una crescita dello sviluppo della consapevolezza, della prevenzione, della capacità di risposta e dell'apprendimento su tutto ciò che riguarda la sicurezza informatica. Perché probabilmente non si tratta di se, ma quando una società sarà presa di mira dal crimine informatico.

Cyber Security, trasformare l'anello debole in punto di forza

---

Italia nel mirino del cyber crime cinese, tra frodi digitali e spionaggio online

Spionaggio industriale e governativo, ricatti e sottrazione di risorse economiche, l'organizzazione **Apt41** con base in Cina da diversi anni sembra svolga, con molta disinvoltura, diversi compiti criminali, un po' spiando, un po' rubando, fino all'estorsione online.

A condurre le indagini internazionali è stata la società di sicurezza informatica FireEye che ha diffuso un **Rapporto** sulle

capacità cyber crime dell'organizzazione stessa: "*Apt41 è unica tra gli attori cinesi sottoposti a monitoraggio, dal momento che utilizza malware non pubblicamente noti e normalmente riservati alle operazioni di spionaggio in quelle che sembrano essere operazioni slegate da obiettivi strategici e statali*", ha spiegato al quotidiano *La Stampa* un portavoce dell'azienda.
"*Sulla base delle osservazioni fatte finora, sembra che Apt 41 sia particolarmente concentrato sull'industria dei videogiochi. Molto probabilmente sono interessati al guadagno personale o da interessi hobbistici*".

Stando a quanto riportato dal quotidiano, **è possibile che ci sia uno stretto legame tra il Governo di Pechino e Apt41**. È lo stesso Rapporto ad evidenziare una certa correlazione tra il Piano nazionale Made in China 2025 e gli obiettivi dei cyber criminali.

Il primo segue una strategia di transizione dell'industria cinese verso standard di qualità crescenti, in grado di competere con quelli dei Paesi più avanzati. I secondi hanno come obiettivo criminale i centri di ricerca e sviluppo delle aziende e delle industrie dei Paesi competitor di Pechino.
Ne discende la possibilità che la Cina tenga ancora molto in considerazione lo spionaggio industriale, strumento utile per accelerare la crescita e tenere ancora saldamente il pugno il timone della transizione.



Diversi i bersagli di Apt41, tra cui certamente Stati Uniti, Giappone, Francia, India, Regno Unito, Hong Kong e anche l'**Italia**. Al centro degli attacchi dell'organizzazione cinese il settore sanitario, high tech, telecomunicazioni, militare, automobilistico, governativo, con l'obiettivo di sottrarre informazioni strategiche e riservate, ma anche di compiere tradizionali crimini informatici.
In quest'ultimo caso, è il settore dei videogiochi quello più sensibile all'azione dei cybercriminali, dove sono emersi casi di frodi relative alle criptovalute e tentativi di attacchi ransomware.

> *Italia nel mirino del cyber crime cinese, tra frodi digitali e spionaggio online*

Intel, nuova vulnerabilità sui processori: interessa le Cpu dal 2012 in poi. Rilasciata da Windows 'patch'

Dopo Spectre e Meltdown, le due falle di sicurezza di cui il mondo è venuto a conoscenza nel gennaio 2018, i processori prodotti da **Intel** hanno un'altra vulnerabilità che permetterebbe a un criminale informatico di impossessarsi di informazioni rilevanti. A scoprire la nuova falla, simile alle due precedenti e chiamata **SwapGs**, è stata la società di sicurezza informatica **Bitdefender**. **Windows** ha già rilasciato una patch di sicurezza per evitare lo sfruttamento della vulnerabilità, mentre i computer **Mac** e **Linux** non sarebbero

interessati dal problema.

La falla riguarda tutte le Cpu prodotte da Intel a partire dal 2012, processori *"che sfruttano la tecnica di esecuzione speculativa, consentendo agli hacker di accedere a password, token, conversazioni private, file crittografati e altri dati sensibili degli utenti, sia di tipo privato che professionale"*, spiega Bitdefender in una nota. La vulnerabilità, si legge, apre a un *"attacco laterale che fornisce all'aggressore un metodo per accedere a tutte le informazioni contenute nella memoria del kernel del sistema operativo"*. L'attacco sfrutta l'esecuzione speculativa, una funzionalità che cerca di velocizzare la Cpu "educandola" a prevedere le istruzioni successive.

"I criminali a conoscenza di questi attacchi avrebbero il potere di individuare le informazioni più vitali e meglio protette sia di aziende che di privati in tutto il mondo, e la relativa facoltà di rubare, ricattare, sabotare e spiare", ha affermato **Gavin Hill**, vicepresidente di Bitdefender.

La vulnerabilità è simile e collegata a Spectre e Meltdown, ma le misure di sicurezza messe in campo per neutralizzare quelle due falle sono inefficaci contro la nuova minaccia. Microsoft, come detto, ha rilasciato una patch, e Bitdefender ha messo a disposizione una soluzione per mitigare l'attacco sui sistemi Windows senza patch.



https://www.key4biz.it/intel-nuova-vulnerabilita-sui-processori-interessa-le-cpu-dal-2012-in-poi-rilasciata-da-windows-patch/268314/

Ecco i mHackeroni, lo special team italiano di cybersecurity che volerà al Defcon

Tra i più forti *ethacal hacker* nazionali e non solo, i **mHackeroni** sono il team italiano che l'anno scorso ha sfidato i big mondiali della ***cybersecurity***, posizionandosi settimi (su 16 finalisti) alla prestigiosa manifestazione americana "*Defcon – Capture The Flag*" di Las Vegas.
Per l'edizione di quest'anno addirittura hanno rischiato di non poter partecipare, perché non avevano i soldi per l'iscrizione.

Avevano una copertura parziale, il resto lo dovevano tirar fuori di tasca propria.
Fortunatamente, sponsor, finanziamenti privati e pubblici arrivati dall'Università La Sapienza di Roma e il Politecnico di MIlano, nonché grazie al crowdfunding.
In questo modo i nostri mHackeroni prenderanno parte anche al DEF CON 2019, che inizia venerdì prossimo.

> *We are sincerely thankful to our sponsor that make it possible for the mHACKeroni team to take part in the DEF CON 27 CTF in Las Vegas: https://t.co/KxRkRozQQO*
>
> *— mhackeroni (@mhackeroni) August 2, 2019*

"Anche quest'anno saremo tra i finalisti: abbiamo infatti confermato gli ottimi risultati ottenuti nel 2018. Dopo il secondo posto alle selezioni su 600 squadre provenienti da tutto il mondo, ed il settimo posto alla finale mondiale, ad agosto torneremo a Las Vegas grazie alla nostra vittoria in Germania allo storico Chaos Communication Congress, punto di riferimento europeo per la sicurezza informatica – con un primo posto su oltre 600 squadre provenienti da tutto il mondo", si legge nella pagina aperta su *gofundme* per raccogliere soldi.

I mhackeroni sono circa 40 tra i migliori studenti e ricercatori italiani in cybersecurity, provenienti dal mondo accademico – Politecnico di Milano, La Sapienza Roma, Università degli Studi di Padova, Ca' Foscari Venezia, TU Wien, ETH Zurich – e da affermate realtà industriali.



Ora andranno al Defcon di quest'anno e parteciperanno al contest *Campture The Flag*, gara a squadre che prevede una serie di giochi di attacco e difesa che richiedono rapidità e sagacia, doti psicologiche non comuni, strategie avanzate, elevate competenze informatiche e capacità di lavorare in squadra e soprattutto sotto stress.

Il Defcon è una celebre manifestazione che si svolge a Los Angeles dal 1993 e mette assieme i migliori hacker etici per sviluppare strategie e soluzioni difensive in chiave di cyber sicurezza. In particolare, *Capture The Flag* è una gara in cui

le squadre devono affrontare una serie di situazioni critiche, sia di difesa, sia di attacco, verso obiettivi sensibili.

> *Ecco i mHackeroni, lo special team italiano di cybersecurity che volerà al Defcon*

Capital One, UniCredit smentisce il data leak: 'Nessuna violazione'

Dopo aver condotto un'indagine interna, **UniCredit** ha rivelato che non sussisterebbe alcuna prova del suo coinvolgimento nella violazione dei dati di **Capital One**. Lo ha dichiarato l'Istituto bancario in una nota interna indirizza ai dipendenti.

L'azienda ha infatti affermato di non aver trovato prove di violazione, sottolineando come i dati dei propri clienti non siano stati salvati sui server **Amazon** hackerati.

La violazione a Capital One

Il 30 luglio **Capital One**, holding bancaria con Sede in Virginia, ha dichiarato di aver subìto una data leak che ha coinvolto circa 100 milioni di persone negli Stati Uniti e 6 milioni in Canada.

Secondo la banca americana i criminali informatici sono riusciti a sfruttare una "*vulnerabilità di configurazione*" nella strutture informatiche dell'azienda rubando dati

sensibili quali: nomi, indirizzi, numeri di telefono ed estratti conto.



L'azienda ha però precisato che gli hacker non sono arrivati ad avere accesso ai numeri di conto corrente collegati ai numeri di carte di credito.

UniCredit

UniCredit ieri ha dichiarato di aver avviato un'indagine sulla vicenda dopo che il nome della banca è stato citato in un blog come un possibile obiettivo della presunta hacker, **Paige A. Thompson,** una ex dipendente di Amazon.

Secondo Capital One, Thompson "*ha utilizzato le credenziali del firewall dell'applicazione Web per raggiungere il database del clienti della banca e di altre organizzazioni finanziarie*".

Non solo UniCredit, ma anche la **Ford** ha avviato indagini per accertare se i propri dati siano stati hackerati durante l'hackeraggio alla holding bancaria, ma la casa automobilistica americana al momento non ha ancora rilasciato dichiarazioni ufficiali.

https://www.key4biz.it/capital-one-unicredit-smentisce-il-data-leak-nessuna-violazione/267809/

Capital One, anche UniCredit coinvolta? Cosa sappiamo sul data breach

Sono stati hackerati dati personali di milioni di persone di **Capital One,** banca americana con Sede in **Virginia**. L'azienda, attraverso un comunicato diffuso il 30 luglio, ha dichiarato che l'incidente ha colpito circa 100 milioni di persone negli Stati Uniti e 6 milioni in Canada.

Nomi, indirizzi, numeri di telefono, storia bancaria, estratti conto, entità di prestiti ed altro sono tra i dati sottratti, ha reso noto l'azienda, precisando che gli hacker non sono arrivati però ad avere accesso ai numeri di conto corrente collegati ai numeri di carte di credito.

Secondo la banca, l'hackeraggio è stato rilevato il 19 luglio, precisando che l'hacker, apparentemente già arrestata, è riuscita a "*sfruttare*" una "vulnerabilità di configurazione" nella strutture informatiche dell'azienda. Il presidente di Capital One, **Richard Fairbank**, si è scusato dicendosi "*grato che la responsabile sia stata catturata*", ma "*profondamente dispiaciuto per quanto è accaduto*".

Cosa è successo

Il 29 luglio, agenti dell'FBI hanno arrestato **Paige A. Thompson** con il sospetto di aver scaricato circa **30 GB di dati** relativi alle richieste di credito di Capital One da un server.



Tali dati includevano circa 140.000 numeri di previdenza sociale e circa 80.000 numeri di conti bancari su consumatori statunitensi e circa 1 milione di numeri di previdenza sociale (SIN) per clienti di carte di credito canadesi.

"*È importante sottolineare che nessun numero di conto della carta di credito o credenziali di accesso è stato compromesso e oltre il 99% dei numeri di previdenza sociale non è stato compromesso*", ha dichiarato Capital One in una nota pubblicata sul suo sito.

"*La più ampia categoria di informazioni a cui si è avuto accesso sono state le informazioni sui consumatori e le piccole imprese dal momento in cui hanno richiesto uno dei nostri prodotti con carta di credito dal 2005 all'inizio del 2019*", continua la nota. "*Queste informazioni includevano informazioni personali che Capital One raccoglie regolarmente nel momento in cui riceve le richieste di carte di credito, inclusi nomi, indirizzi, codici postali, numeri di telefono, indirizzi e-mail e date di nascita*."

Il profilo della ex dipendente di Amazon

Il responsabile del databreach a Capital One è stato un ex dipendente della società di web hosting **Amazon**.

Presumibilmente il dipendente “*infedele ha utilizzato le credenziali del firewall dell’applicazione Web per ottenere l’escalation dei privilegi e raggiungere il database del clienti della banca e di altre organizzazioni finanziarie*“.

Capital One ha dichiarato di aspettarsi costi per sanare l’incidente compresi tra 100 e 150 milioni. La compagnia ha una polizza assicurativa a rischio cibernetico con una franchigia di 10 milioni e una copertura di 400 milioni di dollari.

Unicredit: “Stiamo effettuando gli approfondimenti necessari”

La banca italiana **UniCredit** e la casa automobilistica americana **Ford** hanno avviato indagini per accertare se i loro dati siano stati hackerati dalla violazione della sicurezza dei dati di Capital One,

Secondo quanto riporta quotidiano statunitense “**Wall Street Journal**”, la banca italiana sta esaminando se una directory che si trova su un server cloud è stata raggiunta senza autorizzazione.

UniCredit, la più grande banca italiana, ha dichiarato in una nota di aver contattato le autorità competenti e di effettuare tutti gli approfondimenti necessari.

“*Il 30 luglio UniCredit è venuto a conoscenza del fatto che il suo nome è stato menzionato in relazione all’emissione di Capital One*“, ha dichiarato il portavoce in una nota. “*La sicurezza dei dati e la privacy sono le priorità chiave da sempre. UniCredit ha contattato le autorità interessate e sta effettuando tutti gli approfondimenti necessar*i”.

https://www.key4biz.it/capital-one-anche-unicredit-coinvolta-cosa-sappiamo-sul-data-breach/267627/

Nexi e i database pubblicati su Pastebin, dubbi sul data-leak. La società, “Nessuna violazione informatica”

Ieri sera ***Pastebin***, popolare piattaforma di condivisione di codici sorgente, software, data set e altri contenuti a volte molto sensibili, mostrava al suo pubblico una serie di **elenchi di utenti** riferiti a **Nexi**. Elenchi completi di nomi e cognomi, indirizzi, codici fiscali, addirittura il numero del telefono personale. Insomma, veri e propri database completi di clienti del gigante dei pagamenti digitali in Italia, prova di un **attacco informatico** in piena regola.

> *https://t.co/XSImXbmMLA*
>
> *— Pawel ‘okno’ Zorzan Urban (@pawelzorzan) July 29, 2019*

Sul fatto si sta ovviamente cercando di fare luce, perché i dubbi sull’autenticità dell’attacco sono ancora molti. L’*ethical hacker* **Pawel Zorzan Urban** si è già messo al lavoro e ieri sera è stato tra i primi a far girare la notizia, rilanciando il messaggio dei presunti cyber criminali: “*Dati personali clienti Nexi Spa. Un saluto a Paolo Bertoluzzo, Luca Biancardi, Alessandro Cocciolo. Un abbraccio dagli schiavetti di Montefeltro*”.

Si tratta davvero della traccia di un attacco hacker?
Si tratta di ***data breach*** e ***data leak*** assieme? Quindi di sottrazione illecita e divulgazione non autorizzata di dati sensibili?

A giudicare dal messaggio, come ha anche suggerito Zorzan Urban, si potrebbe dedurre che l'attacco possa provenire dall'interno, o che comunque sia un fatto nato e consumato dentro Nexi (Vendetta personale? Cliente insoddisfatto? Faida interna?).
Ci sono riferimenti a singole persone e a quello che pare "*un gruppo*" specifico di persone ("*gli schiavetti di Montefeltro*").
Su questo indagheranno Polizia Postale e la stessa società vittima dell'ipotetico attacco.



Al momento, a seguito dell'analisi condotta a caldo da Zorzan Urban, "*L'analisi delle prime porzioni di database ha portato ad un totale di 14.241 record privati esposti. 1.709 record comprendono numeri di cellulare associati a persone fisiche*".
Si parla di **diverse liste con migliaia di utenti, oltre 10.000 in totale** quelli che parrebbero coinvolti.

È anche vero, però, che nelle ultime ore, ulteriori indagini hanno portato ad un "*ridimensionamento*" dell'evento. Come ha scritto stamattina Simone Cosimi su *La Repubblica*: "*Ancora, potrebbe trattarsi di un sottoinsieme, cioè dei clienti di uno specifico servizio di Nexi, o più semplicemente di informazioni datate, visto che nel corso della notte diversi utenti hanno analizzato gli elenchi, che non contengono comunque informazioni finanziarie di alcun genere, e non sono riusciti a individuarsi*".

In base all'ultimo aggiornamento diffuso sulla pagina LinkedIn di Zorzan Urban, **sembra che i suddetti link incriminati siano scomparsi**: "*Aggiornamento ore 03:10 30 Luglio 2019 – Rimossi link da Pastebin*".

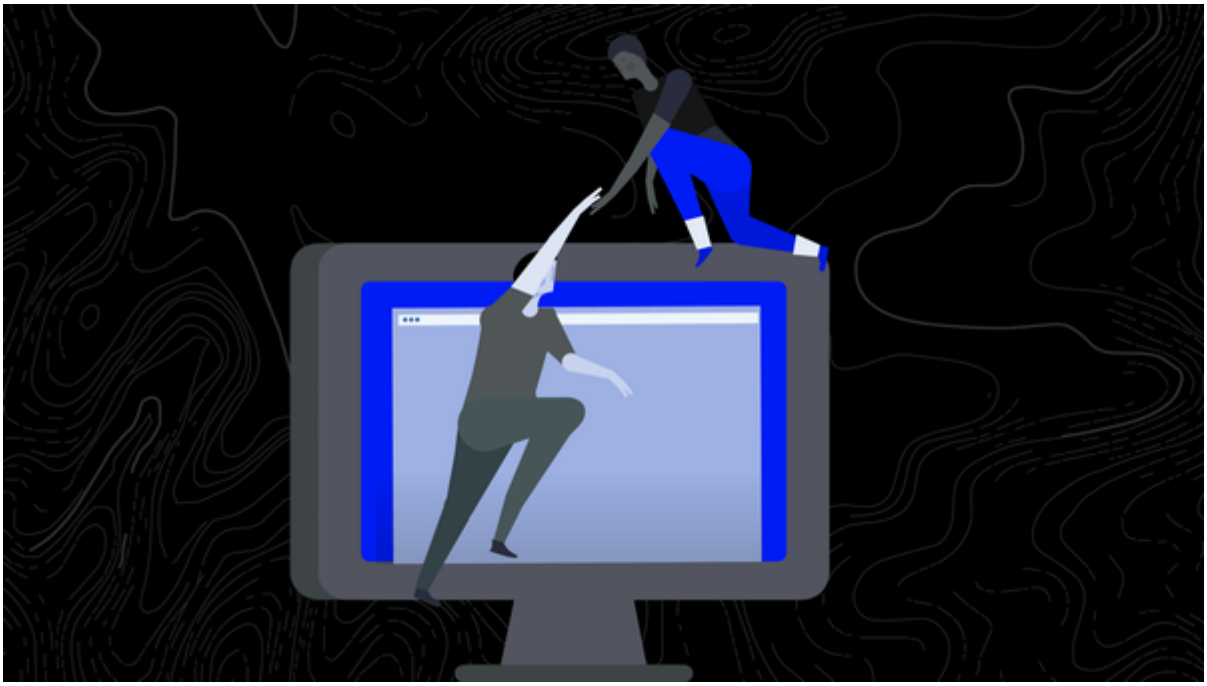
Stamattina, su TGCom24 è stata pubblicata la **notizia della denuncia di Nexi alle autorità** per "*presunto attacco hacker ai suoi danni, senza rilevare però alcuna violazione ai propri sistemi informatici e, soprattutto, alla sicurezza delle carte di pagamento da essa gestite*".
Sembrerebbe inoltre che Nexi abbia deciso di dare notizia del presunto attacco su un sito internet straniero, parlando di "*un post anonimo contenente una lista di circa 18mila nominativi corredati da dati personali di presunti clienti Nexi*".
"*In molti casi* – secondo quanto dichiarato da Nexi e riportato dall'Ansa – *i dati anagrafici contenuti nel sito non trovavano corrispondenza con quelli contenuti nei propri sistemi informatici*". Questo non ha impedito all'Azienda di "*diffidare immediatamente il sito internet che ha pubblicato i dati*", che a sua volta li ha "*prontamente rimossi*".

Nexi gestisce più di 41 milioni di carte di credito nel nostro Paese, attraverso 150 Istituti bancari partner (circa l'80% degli sportelli dell'interno sistema bancario nazionale), 1,4 milioni di terminali pos e 13.400 atm. Da aprile 2019 è una società quotata in Borsa.

> *Nexi e i database pubblicati su Pastebin, dubbi sul data-leak. La società, "Nessuna violazione informatica"*

Cybersecurity Visuals Workshop and Challenge (31 July only)

31 July 2019
Brooklyn, New York



The Cybersecurity Visuals Workshop and Challenge hosted by OpenIDEO is an excellent opportunity for recent graduates and designers to participate in brainstorming new ways to re-visualize cybersecurity perception by using visuals that are more appealing and friendly, unlike the dark and dreary images we're used to seeing.

"Many technologists don't understand how people learn or interact with computers and that-ignoring the human factor-is the original sin that got us into many problems on the internet." —Laurin Buchanan, Principal Investigator for Secure Decisions and an industry leader in cybersecurity awareness.

- 6:45pm: Networking
- 7:00pm: Workshop begins and discuss the challenge brief

- 7:10pm: Background into Design Thinking and generate new visual ideas with your team
- 7:30pm: Ideas pitch
- 8:00pm: Story refinement and second pitch
- 8:30pm: Understand how to submit your ideas to OpenIDEO for the chance to win funding.

Participants are encouraged to sign up for the OpenIDEO challenge answering the question, “how might we reimagine a more compelling and relatable visual language for cybersecurity?”

Sign up for the one day workshop on 31 July
Ask for the “Maker Event Space” when you check in with security

https://www.shillingtoneducation.com/blog/cybersecurity-visuals-workshop-and-challenge-31-july/