Amazon e l’“account bloccato”: attenzione alle email truffa, rubano dati e carte di credito



Il nostro utilizzo dei servizi di Amazon è aumentato notevolmente in questi ultimi mesi, sia per le consuete attività di *ecommerce*, sia per film e serie tv on demand.

L’emergenza Covid-19 ha poi favorito gli acquisti online di beni di prima necessità e questo non è passato inosservato agli occhi dei cyber criminali.

Amazon e l’account bloccato

Se tra i **messaggi di posta** trovate un avviso di Amazon, in cui si comunica che il vostro account è stato bloccato, bisogna

fare molta attenzione e mai eseguire le operazioni richieste, perché potrebbe essere una **truffa online** e un'azione di ***phishing***.

L'allarme arriva dalla Polizia postale e delle comunicazioni, che in questi giorni ha notato un aumento di questo tipo di cyber attacchi, finalizzati ad impossessarsi dei nostri dati personali, delle credenziali delle carte di pagamento e anche dei codici bancari se ce n'è occasione.

"***Il tuo account è stato bloccato!!!***" è il contenuto del messaggio. Il lettore, ignaro della truffa a cui sta andando incontro, prende per buono l'avviso ed inizia a seguire le indicazioni contenute nell'email.

La truffa

Indicazioni generiche, ma che potrebbero convincere i poco esperti. Di solito sì legge che a seguito di (inesistenti) tentativi di accesso non autorizzato, l'account sarebbe stato bloccato, e che per ottenerne lo sblocco occorrerebbe cliccare sul link indicato.

I cyber criminali hanno pensato a tutto, pur di ingannare l'utente, riproducendo al meglio il logo dell'azienda, sfruttando un falso indirizzo email del servizio clienti Amazon.

Cercando anche di simulare un avviso di emergenza proveniente dall'amministrazione, in cui si spinge l'utente ad eseguire il fantomatico sblocco dell'account.

In realtà, spiegano dal Commissariato online di Polizia, quando si apre una mail del genere ci si ritrova davanti ad un ambiente contraffatto, cioè un vero e proprio sito di *phishing*, in cui ci viene chiesto ad esempio di "*creare un nuovo account*", oppure "*avvia sezione*".

Una volta selezionate tali voci, l'utente viene indotto ad

inserire le proprie credenziali di accesso, dati personali e codici bancari o di carte di pagamento, che costituiscono il bottino finale a cui ambiscono i cyber-criminali.

https://www.key4biz.it/amazon-e-laccount-bloccato-attenzione-alle-email-truffa-rubano-dati-e-carte-di-credito/301747/

Criminal Hacker, in vendita sul web i dati di 3mila dipendenti UniCredit

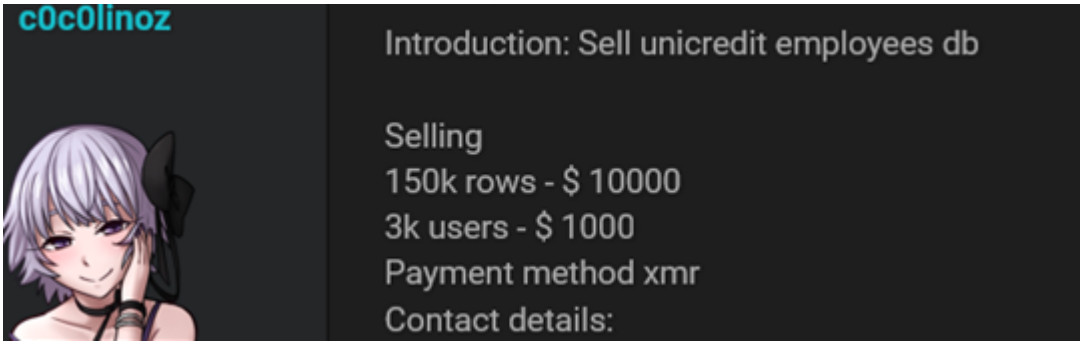
In vendita i dati di 3 mila dipendenti di **UniCredit** su un forum di hacker.

Lo ha scoperto **Telsy**, società italiana di cybersecurity di proprietà di **Telecom Italia**, una delle aziende strategiche del Governo italiano.

UniCredit: dati in vendita il 19 aprile

I dati sono stati messi in vendita il 19 aprile e contenevano informazioni riguardanti indirizzi email, numeri di telefono, password cifrate e nome e cognome dei dipendenti della banca.

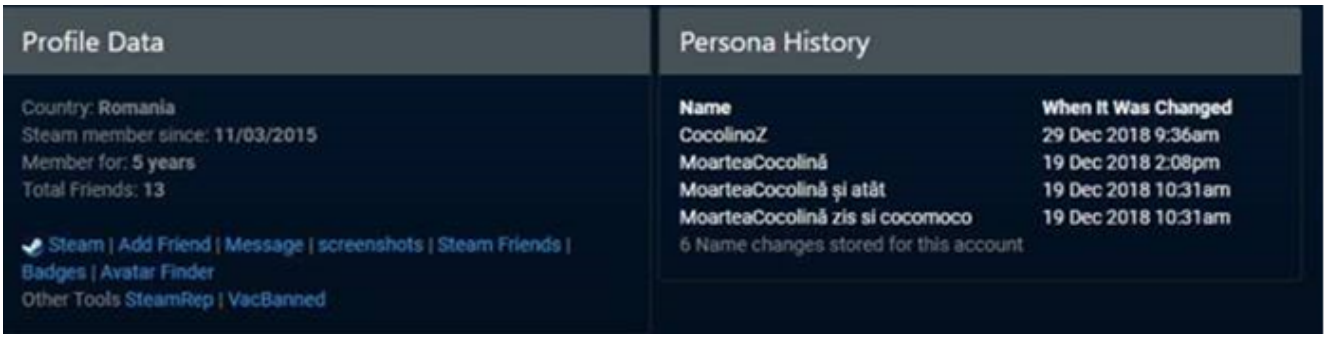
"*Il nickname del presunto hacker che ha messo in vendita tali dati è* ***c0c0linoz,*** spiega Telsy. "*Quest'ultimo avrebbe venduto 150.000 righe di dati per 10 mila dollari e sembra che contenessero proprio i dati di UniCredit risalenti al data breach del 2018.*"



Fonte: blog.telsy.com

“*Dai primi dettagli tecnici a disposizione, il database sembra genuino e appare come il possibile risultato di un attacco di tipo SQL injection, ovvero una tecnica di inserimento di codice malevolo per attaccare le applicazioni,* spiega in una nota la società di sicurezza informatica. “*Oppure potrebbe essere il risultato di una vasta compromissione della rete della banca con il successivo passaggio del database direttamente da uno dei server interni nelle mani degli hacker”.*

“*c0c0linoz*“, spiega Telsy, *“ha creato nuovi account appositamente per questa vendita su almeno un forum relativo alla cybercrime in cui ha mostrato alcuni dati parziali al fine di confermare l’autenticità di quelli in suo possesso. Un piccolo campione dei dati è stato fornito come garanzia all’eventuale compratore.*



Fonte: blog.telsy.com

Il data breach di ottobre 2018

Le informazioni rubate potrebbero risalire al data breach di **UniCredit** avvenuto il 21 ottobre 2018. Al tempo la banca

italiana aveva prontamente comunicato la violazione dei dati personali ai sensi dell'art. 33 del GDPR.

Tuttavia, spiega l'azienda di sicurezza informatica, non ci sono prove che evidenzino che la recente perdita di dati sia la conseguenza di questo stesso attacco.

"Come azienda Golden Power ci sentiamo in dovere di difendere le principali istituzioni del Paese, specialmente in questi momenti di difficoltà", ha dichiarato a Key4biz **Emanuele Spoto**, CEO di Telsy. "*Continua l'incessante impegno di tutto il team cyber contro lo spionaggio industriale e le cattive pratiche di intrusione informatica.*"

UniCredit, attraverso uno Statement rilasciato a **Bloomberg News**, ha dichiarato: "*Siamo a conoscenza del fatto che il nome UniCredit è stato citato in relazione a un presunto caso di data breach in Romania connesso con una piattaforma di recruiting HR fornita e gestita da una terza parte. Non c'è alcuna prova di alcun accesso in alcun sistema di Unicredit*".

> *Criminal Hacker, in vendita sul web i dati di 3mila dipendenti UniCredit*

Dallo Zeroday al sistema di Intelligence

Molto spesso parliamo di **ZeroDay,** del loro valore, del fatto che possono essere rivenduti a prezzi esorbitanti.

Come spesso abbiamo detto, la privacy in questo periodo è oggetto della massima attenzione. Se ne parla al telegiornale,

se ne parlava a scuola, se ne parlava al bar (perdonatemi il passato, visto il regime di *lockdown*), ma di fatto la privacy inizia e finisce con l'avvento dei Social Network e con tutto quello che ruota attorno; e dopo il **Datagate, Vault7 e Crypto-Ag**, abbiamo abbondanti motivi per parlarne.

Gli Stati nazionali, sulla base delle loro costituzioni, acquistano strumenti di Intelligence per *"controllare il crimine, per investigare sul terrorismo e salvare centinaia di vite umane",* così si legge sulle home-page dei siti delle aziende che vendono questo genere di sistemi.

Ma è possibile che tutto questo avvenga alla luce del sole?

Di recente **Facebook ha fatto notizia denunciando la Israeliana NSO Group**, la quale vendette a enti governativi il sistema **Pegasus** (armato da un potente Zeroday per Whatsapp) che ha consentito di violare circa 1400 utenti tra i quali personaggi politici, attivisti, ecc.

Ma per capire tutto questo e come funziona, dobbiamo seguire un filo logico.

Oggi negli smartphone abbiamo tutto: dall'accesso alla nostra banca alle chat con i nostri amici, colleghi, conoscenti. Abbiamo l'accesso all'email dell'ufficio e a quelle personali; abbiamo le nostre foto, le coordinate di dove andiamo e dove siamo stati, le nostre perversioni, insomma **tutta la nostra vita.**

Immaginate se fossimo dei criminali e le forze di polizia accedessero a questo "ecosistema" di preziose informazioni, **saremmo pressoché rovinati** (e che "colpo grosso" sarebbe per le polizie di stato, vero?).

Ma accedere a un terminale di un individuo lo si può fare in diversi modi.

1. Il primo modo, se se ne è il legittimo proprietario;
2. il secondo, qualora lo smartphone venga perduto;
3. il terzo, Attraverso backdoor progettate per scopi di spionaggio (appannaggio dei governi e delle agenzie di Intelligence, come ad esempio NSA, CIA, GCHQ, IDF, ecc… parlando di software americano);
4. il quarto – il più ghiotto – sfruttando degli errori di scrittura del software, dei "bug" sconosciuti che fanno eseguire codice con i massimi privilegi su un software specifico o su terminale remoto.

Ecco appunto i famosi **zeroday no-click RCE** su sistemi quali **IoS, Whatsapp, Android**, che vengono acquisiti nel clear-web o nelle darknet a prezzi stratosferici da "**Broker zero-day"** con picchi di ricompense tra i **2 e i 3 milioni di dollari.**

Quindi, se noi fossimo una agenzia che produce *tool* di spionaggio (ma chiamiamoli, in modo più mite e pacato, di Intelligence), quale sarebbe il nostro canale di approvvigionamento?

1. Il ricercatore **scopre una vulnerabilità zero-day** che consente l'esecuzione di codice arbitrario su un WhatsApp senza l'interazione dell'utente;
2. il ricercatore **divulga privatamente** a un **Broker zero-day** la vulnerabilità che gli riconosce 2.5 milioni di dollari per la scoperta, pagando di fatto il suo silenzio;
3. il broker **rivende ad aziende che sviluppano tool di Intelligence** lo zero-day, magari attraverso un'asta privata. L'azienda che sviluppa sistemi di Intelligence si aggiudica lo zero-day a 4 milioni di dollari;
4. **su quello zero-day l'azienda sviluppa un sistema** (ovviamente per i soli enti governativi), che consente l'accesso completo ai dati di uno smartphone di ipotetica vittima (ad es. inviandogli un SMS o una chiamata WhatsApp senza avere interazione con l'utente), magari fornendo anche strumenti di controllo remoto e di

dashboard.
5. L’azienda rivende questo tool a 10 governi alla cifra di 2 milioni di dollari (passatemi il termine) a licenza.
6. le *revenue* è presto fatta.

Ecco quindi che i governi possono beneficiare di questi strumenti per *“prevenire il crimine e il terrorismo, e poter vegliare sulle nazioni con un grande occhio vigile”.*

Ma dove è il confine tra legalità e illegalità?
Ogni fine giustifica un mezzo?
Rispetto alle possibili risposte esistono molte scale di grigio e non è facile rispondere.

Sicuramente, però, questa non è fantascienza.Parliamo di sistemi quali **Karma, Pegasus** e tanti altri ancora, creati in continuazione sfruttando questo sistema, fino a quando queste falle non verranno rese pubbliche da un ricercatore eticamente corretto o da una “spifferata”, in seguito a un eventuale ricatto, **verso le stesse aziende che producono spyware.**

Ma ricordiamoci di *Eternalblue* che ci insegna come passarono **5 lunghi anni prima che The Shadow Broket rubasse l’exploit dai server della NSA;** e se così non fosse stato, i nostri sistemi Windows **starebbero ancora ballando la Samba!** (Perdonatemi la battuta… ma ci stava bene).

Questa è la realtà di oggi: la racconto nella convinzione sia importante che tutti la conoscano bene.

Articolo a cura di **Massimiliano Brolli**

https://www.ictsecuritymagazine.com/articoli/dallo-zeroday-al-sistema-di-intelligence/

Sicurezza Nazionale, addio CERT-PA. Dal 6 maggio via al CSIRT Italia



Al via dal prossimo 6 maggio il trasferimento delle funzioni del **CERT-PA** e il **CERT Nazionale** allo **CSIRT Italia**, il nuovo team per gestire la cyber-difesa nazionale italiana istituito presso il Dipartimento Informazioni per la Sicurezza (**DIS**).

CSIRT Italia

Lo ha annunciato in una nota lo stesso CERT-PA in cui spiega come entrambe le strutture, che sino ad oggi hanno rispettivamente supportato le pubbliche amministrazioni e il settore privato nella prevenzione e nella risposta agli incidenti informatici, termineranno tutti i servizi proattivi e reattivi.

Entrambe passeranno con gradualità le consegne dal 6 maggio, da tale data, inoltre, i due CERT cesseranno contestualmente di esistere come soggetti autonomi.

La direttiva NIS

La decisione rientra nell'ambito del piano di attuazione della Direttiva NIS (Decreto legislativo 18 maggio 2018 n. 65), recante le misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione europea, che – tra le altre misure – prevede anche in Italia la costituzione di un **Computer Security Incident Response Team unico** (cosiddetto CSIRT).

L'attività dello CSIRT è disciplinata dal DPCM 8 agosto 2019 in materia di "*Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team – CSIRT italiano*", pubblicato in Gazzetta Ufficiale l'8 novembre 2019.

In tale quadro, i soggetti pubblici e privati, a partire dalla data menzionata, in caso di incidente cibernetico e/o di segnalazione di evento, avranno quale nuovo ed unico interlocutore lo CSIRT Italia, che già riceve le notifiche obbligatorie e volontarie degli operatori di servizi essenziali (cosiddetti OSE) e Fornitori di Servizi Digitali (cosiddetti FSD) ai sensi della Direttiva NIS.

I compiti del CSIRT

Il CSIRT è istituito presso il **Dis**, il Dipartimento delle informazioni per la Sicurezza, e ha il compito di:

- definire le procedure tecniche per la prevenzione e la gestione degli incidenti informativi
- ricevere le notifiche sugli incidenti, fornire a chi ha effettuato la notifica le informazioni per facilitare

una gestione efficace dell'evento ed informare gli altri Stati dell'Ue eventualmente coinvolti.
- Garantire la collaborazione nella rete Csirt, attraverso l'individuazione di forme di cooperazione appropriate, lo scambio di informazioni.

"*Viene così a comporsi un altro tassello importante dell'architettura nazionale cyber* – aveva sottolineato il Dipartimento delle Informazioni per la Sicurezza lo scorso novembre – *che, con la collocazione del Csirt presso il Dis, favorirà una più efficace gestione tecnica degli incidenti a livello nazionale e internazionale, grazie alle sinergie garantite dalle altre funzioni già assicurate dal Dipartimento in tale ambito, quali il 'punto di contatto unico nazionale Nis' per la gestione operativa di incidenti transfrontalieri, il 'Nucleo per la Sicurezza Cibernetica (Nsc)' per la gestione operativa di incidenti che hanno un impatto sulla sicurezza nazionale, e le attivazioni che deriveranno dal cosiddetto 'Perimetro di sicurezza nazionale cibernetica'.*"

Per lo svolgimento dei propri compiti, il **CSIRT** si avvarrà dell'AgID ai sensi del decreto legislativo NIS.

https://www.key4biz.it/sicurezza-nazionale-addio-cert-pa-dal-6-maggio-via-al-csirt-italia/301290/

Netflix, oltre 700 false repliche della piattaforma per sottrarre identità e

carte di credito



Le piattaforme a pagamento per vedere film e serie tv hanno visto aumentare il proprio pubblico durante questa epidemia di Coronavirus. Il mercato ne ha tratto beneficio, certamente, ma anche i criminali digitali non sono stati con le mani in mano e ne hanno approfittato.

Obiettivo Netflix

Secondo uno studio Mimecast, **sono più di 700 i falsi siti web che hanno tentato di replicare Netflix**, attribuibili a organizzazioni cyber criminali. L'obiettivo della contraffazione in rete è sempre lo stesso: **sottrarre soldi, codici di carte di credito e dati sensibili**.

Tra il 2 ed il 12 aprile 2020, i ricercatori hanno individuato centinaia di fake site apparentemente simili a Netflix, tra cui **4 falsi siti web dedicati a Disney+.** Graficamente la contraffazione sembra funzionale, anche nei particolari, ma

molto a desiderare hanno lasciato i testi all'interno, pieni di errori grammaticali e spesso grossolani nelle comunicazioni.

"*Abbiamo visto un aumento drastico di domini web sospetti che tentano di assomigliare il più possibile alle grandi piattaforme di streaming online, con l'unico obiettivo di realizzare guadagni illeciti*", ha spiegato **Carl Wearn**, responsabile unità eCrime.

"*Molto spesso* – ha precisato l'esperto – *questi siti web fantoccio cercano di attirare il maggior numero di utenti pubblicizzando accessi gratuiti o particolari offerte promozionali, con il solo scopo di rubare soldi, identità e credenziali degli ignari utenti di rete*".

I brand più sfruttati dal phishing

Secondo un'indagine sui cyber attacchi, condotta da Check Point Software, invece, **Netflix è il brand più sfruttato per gli attacchi di phishing nel mondo dopo Apple**. Questo perché si tratta delle aziende più popolari al mondo, con un gran numero di utenti.

Netflix, con i suoi 160 milioni di utenti (di cui 7 milioni appena registrati alla fine del primo trimestre 2020) e un valore di mercato pari a 192 miliardi di dollari, è un brand irresistibile per la criminalità online.

Questo accade perché Apple e Netflix, in questo caso, rappresentano un bacino enorme in cui pescare per i cyber criminali, che attraverso tecniche più o meno sofisticate di falsificazione e *scamming* riescono a rubare le credenziali di carte di credito e i dati sensibili degli stessi utenti (spesso sempre attraverso pagine contraffatte che replicano le originali).

Secondo l'indagine, infine, più del 10% dei tentativi di

phishing hanno utilizzato come esca falsi doppioni di siti Apple, il 9% di Netflix, il 6% di Yahoo e Whatsapp, nel 5% dei casi di PayPal.

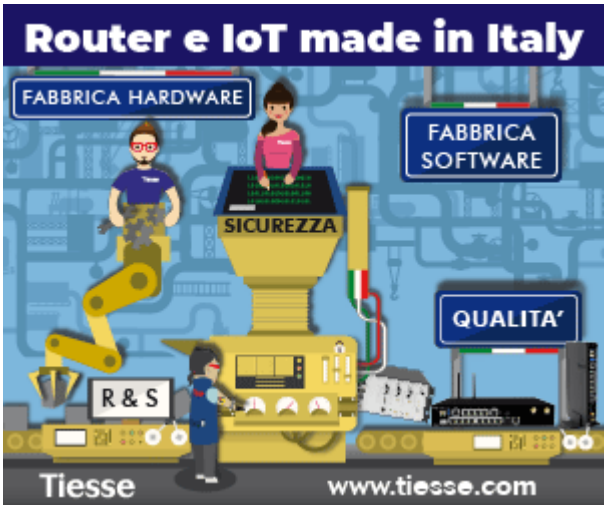
Il brand Netflix risulta anche quello più utilizzato per sferrare attacchi di phishing sia su web (2° posto), sia su rete mobile (1° posto).

https://www.key4biz.it/netflix-oltre-700-false-repliche-della-piattaforma-per-sottrarre-identita-e-carte-di-credito/301199/

Domini infetti, crescono del +600% quelli contenenti le parole “Coronavirus” e “Covid-19”

Il cyber crime sfrutta sempre ogni nuova opportunità per colpire semplici utenti, aziende, amministrazioni pubbliche e altre organizzazioni attive in diversi settori economici, con il solo scopo di sottrarre dati sensibili e assicurarsi profitti.

La pandemia di Coronavirus a livello mondiale ha subito rappresentato un’occasione per fare business illecitamente. Secondo un Report Yarix c’è stato un imponente **aumento di registrazioni di nuovi domini, intorno al +600%, contenenti parole chiave come ‘*Covid*’ e ‘*Coronavirus*’**.



I domini

L'azione di cyber crime è stata portata avanti in associazione ad altri termini generalmente utilizzati per attività di malware, phishing e scam (es. login, recovery, access, password, account…).

Lo studio ha preso in esame oltre 100.000 domini che in media vengono registrati ogni giorno nel mondo, per un lasso di tempo che va dal 23 febbraio alla metà di marzo.

Un dominio web altro non è che il nome con cui si contraddistinguono siti e piattaforme online (*www.nomesitoweb.it*). Un nome facile da ricordare associato a un indirizzo IP fisico su Internet. Il nome di domino corrisponde al nome univoco che compare dopo il simbolo @ negli indirizzi email e dopo www. negli indirizzi web.

Per questo, in un momento in cui le persone cercano informazioni online sull'epidemia di Coronavirus, è ancora più minacciosa l'azione dei cyber criminali che prevede di sfruttare le parole "*Coronavirus*" e "*Covid-19*".

Gli attacchi

Gli strumenti più usati, per questo tipo di attacchi informatici, portati via dominio infetto, sono il ***phishing***,

l’estorsione, i ***malware*** e le campagne per rubare soldi alle persone sfruttando anche le raccolte fondi per aiutare le popolazioni più vulnerabili all’epidemia.

Ricorrendo in particolare a tecniche di *phishing*, è spiegato in una nota allegata all’indagine, “*gli hacker stanno inviando mail ‘malevole’ inserendo come finto mittente il richiamo a ospedali o istituzioni sanitarie*”.

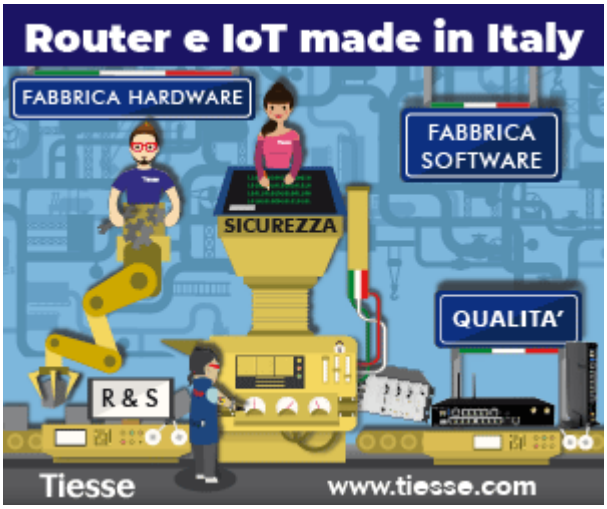
Altrettanto diffusi, nei dati rilevati, sono i tentativi di truffa, contenenti minacce di diffusione di dati personali e di contagio Covid19, ai danni di quanti si sono rifiutati di pagare i riscatti in bitcoin (nel caso di un attacco *ransomware*).

> *Domini infetti, crescono del +600% quelli contenenti le parole “Coronavirus” e “Covid-19”*

Zoom, 500mila account in vendita sul dark web

Le informazioni sugli account appartenenti ad almeno mezzo milione di utenti **Zoom** sono state pubblicate, scambiate e, in alcuni casi, vendute sul dark web.

Secondo quanto riportato dal sito Bleeping Computer, l’archivio è stato identificato ad inizio aprile da **Cyble**, una società di sicurezza informatica che ha scoperto e successivamente acquistato più di 530.000 credenziali Zoom rubate attraverso un forum di hacker.



La tecnica del Credential Stuffing

Cyble ha dichiarato a Bleeping Computer che gli hacker sono stati in grado di ottenere gli indirizzi e-mail, le password, i collegamenti URL e le chiavi host degli utenti Zoom tramite uno schema di attacchi informatici chiamato "***Credential stuffing***", in cui i dati precedentemente trapelati da un'altra fonte online vengono estratti da aree del dark web e usate per compromettere nuovi account.

È qui che gli hacker utilizzano i dettagli dell'account rubati da hack di altri siti per ottenere l'accesso, poiché le persone spesso riutilizzano le stesse password su più siti.

Account venduti per 0,002 centesimi

Alcuni degli account Zoom venivano offerti gratuitamente, mentre altri per meno di 0,002 centesimi ciascuno "*in modo che gli hacker possano usarli in scherzi e attività criminale,* spiega il sito." Si dice anche che gli hacker offrano account gratuiti per "*acquisire una maggiore reputazione nella comunità degli hacker*".

I conti stessi erano vari, molti dei quali riguardavano indirizzi universitari ma includevano anche conti per società ben note, tra cui **JPMorgan Chase Bank N.A. e Citigroup Inc.**

Le colpe di Zoom

È bene precisare che la vicenda non nasce da un attacco diretto a Zoom, ma si basa sullo sfruttamento di **credenziali** già finite nelle mani sbagliate da tempo. Ci sono però dei modi per fornire una sicurezza maggiore agli utenti, come ad esempio l'introduzione dell'**autenticazione a due fattori.** In questo modo infatti, si aggiungerebbe una barriera all'ingresso contro i cybercriminali.

Zoom e Covid-19

Durante la pandemia **COVID-19**, Zoom è emerso alla ribalta, arrivando in cima ai download delle applicazioni. Con questa popolarità sono anche uscite allo scoperto le sue pratiche di sicurezza, rivelatesi carenti.

A parte i problemi di sicurezza, Zoom è una delle poche aziende che ha superato bene la pandemia di coronavirus. Il prezzo delle azioni di Zoom ha raggiunto il picco di 159,56 dollari lo scorso 23 marzo, anche se le questioni di sicurezza hanno attenuato leggermente l'interesse degli investitori.

https://www.key4biz.it/zoom-500mila-account-in-vendita-sul-dark-web/300083/

Coronavirus, come difendersi dai principali vettori di

attacco hacker



Non è una novità purtroppo, potreste aver già letto di come i **Criminal Hacker** stiano capitalizzando la pandemia di **coronavirus** in corso nel tentativo di infettare i computer e dispositivi mobile con malware o anche solo di portare a termine vari tipi di truffe.

Criminal hacker e Covid-19

Sfortunatamente, in una certa misura, sta funzionando. Questo perché la superficie di attacco sta cambiando e si sta espandendo rapidamente, dato che molte organizzazioni e aziende si stanno digitalizzando senza molta preparazione, esponendosi a più minacce potenziali.

La maggior parte dei recenti Cyber attacchi sfruttano principalmente i timori legati all'epidemia di COVID-19, alimentati dalla disinformazione e dalle false notizie, per distribuire malware tramite le applicazioni **Google Play**, link

e allegati dannosi ed eseguire attacchi ransomware.

Nuovo tema, vecchi pericoli

Ogni Paese del mondo ha visto almeno un attacco a tema COVID-19 realizzato ex novo. Questi attacchi rappresentano tuttavia meno del 2% di tutti i Cyber incident solitamente tracciati, secondo un recente studio di **Microsoft**.

I dati raccolti, infatti, mostrano che queste minacce a tema COVID-19 sono una ricostruzione di attacchi esistenti che sono stati leggermente modificati per legarsi a questa pandemia. Ciò significa che stiamo assistendo a un cambiamento delle esche, non ad un'impennata di nuovi strumenti del Cyber Crime.

Ma quali sono i metodi più in voga al momento?

Mobile Malware

I Criminal Hacker stanno sfruttando le paure e i timori delle persone riguardo ai coronavirus per diffondere malware mobile, compresi i Mobile Remote Access Trojans (MRAT), i banker trojans e i dialer premium, tramite app che affermano di offrire informazioni relative al Coronavirus e aiuto per gli utenti.

Solo per citare un esempio, un team di ricerca statunitense, ha recentemente scoperto almeno 16 diverse applicazioni mobili, che sostenevano di offrire informazioni relative all'epidemia ma che invece contenevano malware, tra cui adware (Hiddad) e banker Trojans (Cerberus), che rubavano i dati personali degli utenti o generavano entrate fraudolente da servizi a tariffa premium.

Tutte le 16 app in questione sono state scoperte su domini correlati al coronavirus di nuova creazione, che hanno visto

un enorme aumento nelle ultime settimane.

Phishing

Sempre in voga, adesso più che mai, questo metodo ha trovato un forte alleato nella propagazione delle botnet. La maggior parte delle e-mail di phishing relative a COVOD-19 sono, tra l'altro, unite a malware come AgentTesla (45%), NetWire (30%) e LokiBot (8%) incorporati come allegati, permettendo così all'aggressore di rubare dati personali e finanziari delle vittime.

Le e-mail, molto spesso, sono state mascherate da avvisi dell'Organizzazione Mondiale della Sanità, dell'UNICEF e di altre agenzie e società internazionali come Maersk e CISCO.

Malware as a Service con scontistica dedicata

Contestualmente all'aumento dell'infezione c'è stata anche un'impennata di post su forum underground dove gli utenti offrivano sconti sui malware e codici promozionali su DDoS, spamming e altri servizi malware. Una sorta di solidarietà perversa tra Criminal Hacker

Smishing

È stata anche rilevata un'impennata di falsi messaggi SMS di mittenti come "COVID" e "UKGOV" che contengono un link a siti di phishing. Oltre agli SMS, i canali possibili includono WhatsApp e altri servizi di messaggistica.

Software dannoso

Mentre le persone lavorano sempre più spesso da casa e le piattaforme di comunicazione online come Zoom e Microsoft Teams diventano cruciali, i Criminal Hacker inviano e-mail di phishing che includono file dannosi con nomi come "zoom-us-us-zoom_##############.exe" e "microsoft-teams_V#mu#mu#D_##############.exe" nel tentativo di ingannare le persone a scaricare malware sui loro dispositivi.

Ransomware

I criminali informatici stanno cercando di colpire i principali ospedali e altre istituzioni in prima linea nella lotta contro COVID-19 con attacchi Ransomware.

I criminali informatici stanno usando il ransomware per tenere in ostaggio gli ospedali e i servizi medici in modo digitale, impedendo loro di accedere a file e sistemi vitali fino a quando il riscatto non sarà pagato. Alcuni casi hanno compreso Paesi come Regno Unito e Repubblica Ceca.

Come difendersi

I Criminal Hacker adattano continuamente le loro tattiche per trarre vantaggio da nuove situazioni, e la pandemia COVID-19 non fa eccezione. Stanno usando l'elevato appetito per le informazioni relative a COVID-19 come un'opportunità per fornire malware e ransomware e per rubare le credenziali degli utenti.

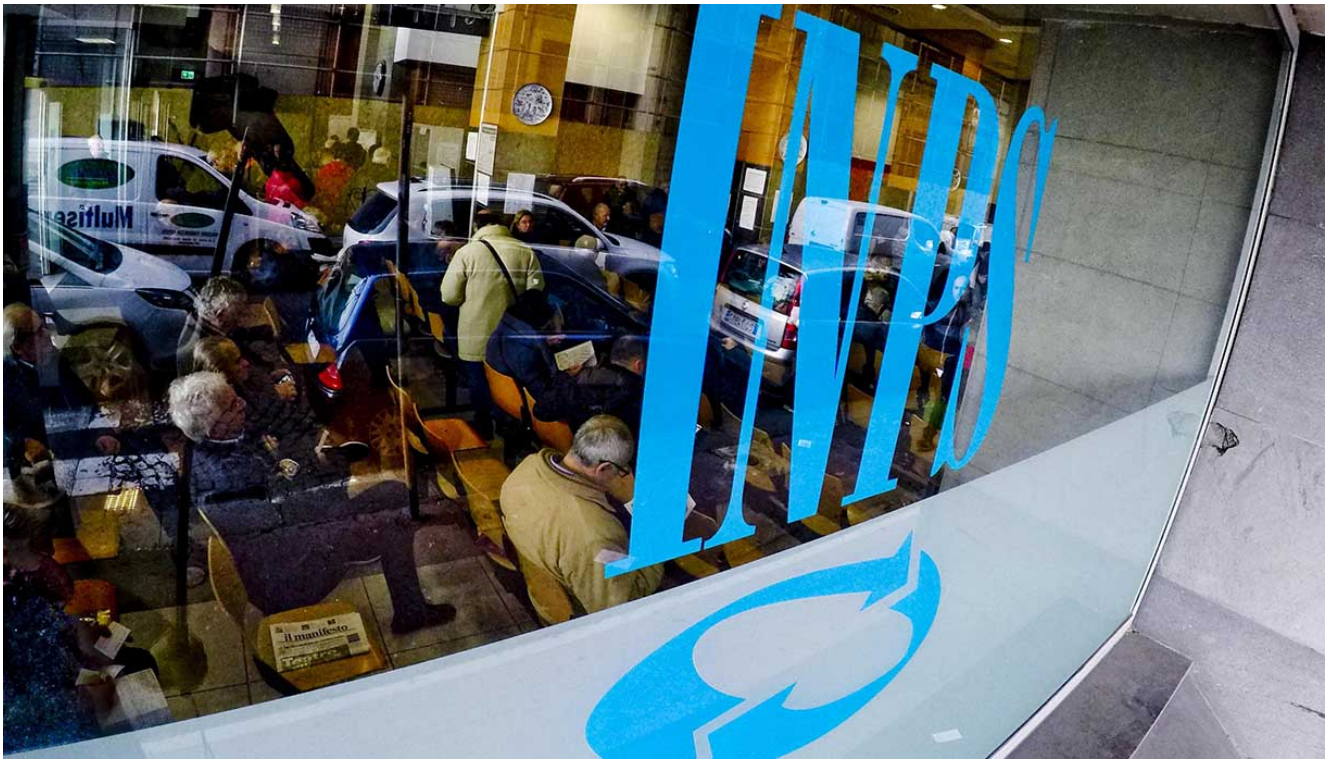
Il consiglio è sempre lo stesso, non abbassare mai la guardia di fronte a tutto ciò che riceviamo via mail o che decidiamo di scaricare.

In generale, evitare di cliccare sui link nelle e-mail non richieste e diffidare degli allegati di posta elettronica, non rendere pubbliche le riunioni e assicurarsi che siano protette da password per evitare il dirottamento delle videoconferenze.

Non dobbiamo mai e poi mai dimenticare: la cura per il COVID-19 non la troveremo mai online!

https://www.key4biz.it/coronavirus-come-difendersi-dai-principali-vettori-di-attacco-hacker/299703/

Come funziona Anubis, il malware che sfrutta l'INPS come esca



I Criminal Hacker stanno prendendo di mira l'**INPS**. Ma non riguarda il sito ufficiale dell'ente nazionale italiano, ma vere e proprie truffe utilizzando l'ente previdenziale italiano come esca.

La denuncia dell'INPS

Due giorni fa, l'Istituto guidato da **Pasquale Tridico**, ha comunicato ai propri utenti che si sono verificato sospetti **tentativi fraudolenti** di richiesta di **dati sensibili**.

In particolare, spiega l'INPS, sarebbe in atto una massiccia campagna malware attraverso l'invio di **SMS** che invitano a cliccare su un link per aggiornare la propria domanda **COVID-19** e inducono a installare una app malevola.

"Questi SMS, conferma l'ente previdenziale, ***non sono inviati***

dall'INPS. *Eventuali SMS che l'Istituto dovesse inviare non conterranno link a siti web, l'unico accesso ai servizi INPS è tramite il sito istituzionale*".

Il CERT-PA conferma la denuncia dell'INPS

La conferma della campagna malevola in atto arriva anche dal **CERT-PA**, la struttura che opera all'interno dell'**Agenzia per l'Italia Digitale** e preposta al trattamento degli incidenti di sicurezza informatica dei domini della pubblica amministrazione.

"*La campagna malevola denunciata dall'INPS si appoggia al dominio inps-informa.online, un dominio palesemente falso*, ha comunicato il Cert-PA. *La homepage contiene un link per il download di una fantomatica applicazione per richiedere un bonus in denaro, se installata l'applicazione è in grado di infettare il telefono. L'applicazione,* continua la struttura*, è diffusa anche tramite QR code che rimandano al link per il download.*

Il CERT-PA ha quindi analizzato l'applicazione e provveduto a diffonderne gli indicatori di compromissione alla constituency tramite il Canale Nazionale di Trasmissione IoC (CNTI).

Il malware Anubis

L'applicazione, spiega il CERT-PA, *è un derivato del* ***malware Anubis****. Il codice di Anubis è così riusato per l'infezione di dispositivi Android da essere stato impiegato anche in precedenti campagne FTCODE, con cui condivide buona parte delle funzionalità*".

Il malware Anubis è in grado di:

- di leggere gli SMS ed occultare gli SMS ricevuti;

- mutare tutti i volumi del cellulare e bloccare lo schermo come forma di riscatto;
- rubare informazioni come numero di telefono, operatore e modello di cellulare;
- disinstallare applicazioni, mostrare pagine di phishing all'apertura di determinate applicazioni (di home banking, IM e client e-mail);
- impedire la propria disinstallazione (chiudendo la finestra di sistema ogni volta che ci si prova)

Cosa difendersi

- Se ricevete sms dall'INPS NON aprite nessun link
- Non installate mai programmi scaricati fuori dagli store ufficiali
- Ignorate email, sms o altre comunicazioni che ci chiedono di compiere una qualsiasi azione (download allegato, clic su link)
- Se siete stati truffati denunciate subito l'accaduto alla polizia locale con più dettagli possibili
- Comunicate la frode alla vostra banca e tenete sotto controllo il vostro conto

https://www.key4biz.it/come-funziona-anubis-il-malware-che-sfrutta-linps-come-esca/299611/

Caso INPS. Intervista a Raoul Chiesa: "Una bugia che fa

capire perché la cybersecurity in Italia non funziona”



Sulla scia del caso **INPS** si sono sollevate polemiche senza fine sull’accaduto, sulle dichiarazioni del presidente dell’ente, **Pasquale Tridico**, e sui commenti che ne sono seguiti. Sul caso, come è noto, il **Garante per la protezione dei dati personali** ha già disposto un intervento ispettivo di cui aspetteremo gli esiti. Intanto sull’intera vicenda abbiamo voluto raccogliere il parere di **Raoul Chiesa**, uno dei massimi esperti nazionali in tema di sicurezza cibernetica.

Key4biz. ***Chiesa, lei ha seguito in questi giorni la vicenda della presunta incursione hacker ai danni del sito dell’INPS, che idea si è fatto?***

Raoul Chiesa. Ho letto commenti ed opinioni di vario genere,

confronti, battute, disamine molto precise, piuttosto che post quasi "goliardici", ma ritengo che si tratti di un "incidente interno", e non certo di un attacco, di cui stiamo sottovalutando le conseguenze e che, secondo il mio parere, è solo la punta dell'iceberg di ciò che non funziona nel nostro Belpaese in ambito di sicurezza informatica e procedure nella Pubblica Amministrazione.

Key4biz. ***In che senso?***

Raoul Chiesa. Innanzitutto reputo estremamente grave che il Presidente di un ente come l'**INPS** affermi cose non fondate. Affermare di "*…essere stati oggetto di un attacco hacker…*", quando ciò non è vero, ma anzi nasconde (consapevolmente o meno) una chiara incompetenza dell'ente nella gestione di una emergenza (che era peraltro facilmente prevedibile) ed indica semmai delle problematiche a monte. E non sto parlando "solo" di *cybersecurity*, ma anche di comunicazione e della cosiddetta *"gestione di Cyber Crisis".* Ancora qualche giorno fa, su **Rai1** a "***Porta a Porta***", il conduttore **Bruno Vespa** chiede a **Pasquale Tridico**, presidente di INPS degli "*attacchi hacker*", e quest'ultimo conferma e ribadisce quella che è, a tutti gli effetti, una cosa non vera o, se si vuole,una "*Fake News*", come si usa definirle oggi.

Key4biz. ***E allora cosa è successo?***

Raoul Chiesa. Tornando a noi ed al giorno del down del sito INPS, immagino più o meno quello che deve essere successo. Vi è stato un prevedibile picco di richieste e non inaspettato (come qualcuno ha detto), dal momento che era stato previsto all'interno del DPCM "***Cura Italia***". Il problema è ovviamente andato subito in carico alla società che gestisce il sito, (che, non sappiamo, ma magari avrà subappaltato ad altre società le lavorazioni o parte di esse?), ma, come abbiamo visto, il problema è rimasto per ore ed ore.

Key4biz. ***Ma lei sostiene che il problema va anche oltre, in***

che senso?

Raoul Chiesa. Si, vorrei andare oltre, ad un livello superiore. Mi viene da pensare al bando di gara di assegnazione di quel sito così importante. Non lo conosco, ma mi chiedo, considerato quello che è successo, cosa avranno previsto per l'infrastruttura IT e di rete, nella progettazione e gestione dei server in caso di "picchi di rete" o di emergenze, per anche ciò che riguarda *Business continuity*, *Disaster recovery*, *Secure coding* e *Secure programming*. O molto più banalmente: hanno previsto dei servizi di outsourcing da attivare in caso di situazioni di questo tipo con provider che gestiscano gli improvvisi aumenti di carico banda e di richieste server-side? Ma mi viene anche da pensare che, forse, si è confusa la responsabilità sistemistica con quella di networking. Insomma si possono fare tante ipotesi tra negligenza e procedure di controllo discutibili

Key4biz. ***Quindi è stata sbagliata anche la comunicazione, cosa avrebbero potuto o dovuto fare?***

Raoul Chiesa. Beh, c'è da chiedersi se i responsabili della comunicazione non debbano studiare un po' cosa sia una "*crisi cyber*", che altro non è se non una crisi ordinaria come le altre, ma che a differenza di altre è causata però da un incidente di tipo cyber, il che potrebbe indurre ad una gestione diversa e più cauta.

Key4biz. ***Di certo Pasquale Tridico presidente INPS avrà detto quello che i suoi tecnici gli avranno riferito o quantomeno immaginiamo che sia accaduto ciò…***

Raoul Chiesa. Naturalmente non rientra nelle competenze del presidente Tridico capire cosa sia accaduto nell'apparato IT dell'ente. Certo quando avrà chiesto cosa stesse accadendo e il responsabile del servizio avrebbe dovuto rispondere in modo cristallino, non ci sarebbe stato nulla di male ad ammettere

che non si era tecnicamente preparati a fronteggiare un picco di queste dimensioni (300-500 presentazioni di domande al minuto, che si sono rapidamente ammassate l'una sull'altra). E questo senza togliere nulla alla prevedibile generosità con cui immagino i dipendenti IT dell'INPS avranno lavorato in quei giorni per fronteggiare l'ondata di richieste annunciate dal premier Conte con il "Cura Italia".

Key4biz. ***Ma allora dove potrebbe essere l'errore nelle dichiarazioni del presidente dell'INPS o nei resoconti che i suoi sottoposti hanno riportato a lui?***

Raoul Chiesa. Innanzitutto vorrei ricordare che il malfunzionamento ha reso in chiaro le anagrafiche di contribuenti, dati che fanno molta gola al *cybercrime*. Cosa avrebbe dovuto fare Tridico? Non sta a me dirlo, ma mi faccio, come voi, qualche domanda. Prima di far perdere tempo alle competenti Autorità Giudiziare e alle Forze dell'Ordine, peraltrogià stracariche di lavoro e sotto forza; prima di gridare al mondo intero di essere stato vittima di un attacco hacker, peggiorando quindi la situazione e dichiarando magari cose non effettivamente verificatesi, avrei semplicemente chiesto prove, evidenze, per porre l'ente in condizione di sapere effettivamente cosa in dettaglio fosse accaduto e decidere quindi la comunicazione pubblica conseguente.

Key4biz. ***E gli hacker, quelli veri, che dicono?***

Raoul Chiesa. Siamo riusciti persino a fare ridere quelli di **Anonymous Italia**, che da sempre sono molto ironici e autoironici e non necessariamente "*cattivi sempre e per forza*". Non ho visto nessun hack di **LULZ** o di altri gruppi di **Hacktivism** in questo triste periodo che il nostro Paese ed il resto del mondo stanno attraversando. Il problema vero è e sarà il **Cybercrime** che sa essere sempre attivo ed approfittarsi di target indifesi, senza team tecnici presenti, di entità ed asset digitali abbandonati a sé stessi, in una nazione che sta affrontando una delle crisi più grandi degli

ultimi due secoli.

Key4biz. *E adesso cosa accadrà?*

Raoul Chiesa. Le conseguenze di questo "Al Lupo-Al lupo" saranno molto gravi.

E la cosa più grave è tutto quello che questo incidente cela, nasconde, tutto ciò che non viene detto e di cui nei prossimi giorni, settimane e mesi, probabilmente, verremo piano piano a conoscenza. È l'errore, sono gli errori che stanno alla base delle nostre falle di sistema. È il nostro Sistema-Paese che non è pronto a tutte quelle belle *buzzword* di cui leggiamo ogni giorno, su media e social, piuttosto che nei company profile di tante "*wanna-be*" aziende esperte di *trasformazione digitale, smartworking, cybersecurity, banda larga, big data, articial intelligence*…. il tutto applicato alla Pubblica Amministrazione Centrale e Locale del nostro Belpaese.

Key4biz. *Siamo vittime della fiumana delle tecnologie?*

Raoul Chiesa. No, qui non vince o perde la tecnologia, perché per usare le tecnologie bisogna partire dalle persone e dalle procedure e regole. Se la Pubblica Amministrazione appare, come in questa vicenda, abbandonata a sé stessa e senza le competenze adeguate, questo dipende in primis dai sistemi di assegnazione delle gare, tutte orientate al massimo ribasso, che vuol dire decadimento della qualità. Si usa questo sistema perché contribuisce ad immunizzare dalle corruttele, nel senso che ci sono margini minori, ma il risultato è che le corruttele continuano e la qualità tecnologica della PA è in molti casi non adeguata o in mani estere.

> *Caso INPS. Intervista a Raoul Chiesa: "Una bugia che fa capire perché la cybersecurity in Italia non funziona"*