White Paper

Proteggere la tua azienda dai pericoli del Dark Web

IL GRANDE FRATELLO ORWELLIANO? UN PRINCIPIANTE

Cinquecento e passa milioni. Quasi dieci volte la popolazione italiana, più di un decimo di tutti gli utenti Internet del mondo.

È questa la **dimensione di una raccolta illecita di dati personali emersa nella primavera 2021 che ha reso facilmente reperibili in rete le informazioni private di profili personali Facebook** come numeri di telefono, date di nascita, indirizzi e via discorrendo.

Un "furto di dati" che in realtà non ha richiesto particolari competenze tecniche: probabilmente è stato sufficiente sfruttare la funzione "cerca amici" di Facebook usando una rubrica contatti personale contenente tutti i numeri di telefono possibili, generati algoritmicamente a partire da 000000 fino a 999999999 per tutti i prefissi esistenti. Un trucco che Facebook ha neutralizzato nel 2019, ma che non è escluso possa essere usato anche con altri social e sistemi di messaggistica dotati di una funzione simile.

La raccolta e la vendita di informazioni personali su Internet è talmente cresciuta nell'ultimo decennio da diventare un'industria a sé stante. Il caso di Facebook, eclatante per dimensioni e per la notorietà dell'azienda colpita, segue sulla scia di numerosi altri. **Ricordiamone alcuni**, solo per restare in Italia:

- 2.500.000 di profili di clienti di Ho Mobile, operatore telefonico di Vodafone Italia, nel 2020
- 165.000 account del portale del trasporto pubblico locale Unico Campania nel 2020
- 42.000 profili dell'Ordine degli Avvocati di Roma con relativi messaggi email nel 2019
- 14.600 profili sottratti alla SIAE nel 2018

Non che nel resto del mondo le cose siano andate diversamente: ricordiamo brevemente

- 5.000.000 di record personali sottratti al fisco bulgaro nel 2019
- 780.000 record di clienti sottratti a Sephora nel 2017
- 164.000.000 account LinkedIn violati nel 2012 e messi in vendita nel 2016
- 4.500.000 account sottratti a Snapchat nel 2014
- 152.000.000 di account Adobe violati nel 2013
- 68.000.000 di account Dropbox violati nel 2012

e l'elenco potrebbe proseguire a lungo.

Tutte queste informazioni non sono ovviamente destinate a restare chiuse nel computer di chi le ha raccolte, ma **prima o poi finiscono in vendita sul mercato nero del cybercrimine che si trova all'interno del famigerato Dark Web**: un vero e proprio web alternativo a quello che sei abituato a navigare, basato su tecnologie orientate alla privacy e inaccessibile ai browser tradizionali come Google Chrome o Mozilla Firefox.

FACCIAMO UN PO' DI LUCE

Non che entrare nel Dark Web sia particolarmente complicato: è sufficiente un browser apposito come ad esempio Tor per essere immediatamente in grado di consultare uno dei diversi motori di ricerca disponibili (a differenza del Web "ufficiale", i siti del Dark Web tendono a cambiare frequentemente indirizzo, quindi il motore di ricerca è ancora più fondamentale del solito) e andare alla scoperta di un mondo a se stante.

Va sottolineato comunque che il Dark Web non è solo cybercriminalità, essendo utilizzato anche da attivisti e cittadini di regimi autoritari che ne sfruttano la tecnologia per aggirare censure e repressione – il che, peraltro, è lo scopo per cui è nato.

Sul Dark Web si trova davvero di tutto, e qualche anno fa sui giornali aveva fatto scalpore la storia di un marketplace chiamato Silk Road, una sorta di Amazon illegale sul quale approdavano venditori di qualsiasi cosa: stupefacenti, armi, documenti falsi, killer a pagamento e, ovviamente, dati e informazioni. Il gestore di Silk Road è stato identificato e arrestato nel 2013 per essere condannato all'ergastolo l'anno successivo, ma questo non ha evitato che altri abbiano preso il suo posto fondando altri marketplace piccoli e grandi che aprono e chiudono con una certa frequenza.

Un qualunque truffatore anche non particolarmente esperto di informatica può trovare qui tutto ciò che gli occorre per portare a termine operazioni di sottrazione dell'identità, furti con carte di credito, campagne di spam e phishing, spionaggio industriale e personale, ricatto e così via, tutto comodamente pagabile in Bitcoin.

E per chi si preoccupa giustamente della tracciabilità delle compravendite in criptovaluta, esistono anche servizi di anonimizzazione che spezzettano la moneta digitale in piccolissimi importi in una lunga serie di transazioni: una sorta di "frullatore" il cui scopo è quello di far perdere le tracce del denaro. Servizi, ovviamente, acquistabili sul Dark Web.

Negli ultimi tempi si sta assistendo alla diffusione di un ulteriore canale per l'e-commerce cybercriminale, ed è quello dei gruppi Telegram.

In questo servizio di messaggistica sono presenti persino dei *bot*, software automatici che sbrigano l'intero ciclo ordine - pagamento - fornitura senza alcun bisogno di intervento umano. Uno di questi, per tornare a Facebook, permette di conoscere i numeri di telefono di tutti gli utenti che hanno concesso il loro *like* a una determinata pagina: un servizio di un certo interesse per chi si occupa di telemarketing, oltretutto basato su informazioni che sembrano essere più aggiornate di quelle del file da 500 milioni di utenti di cui parlavamo all'inizio.

Si tratta di un segnale che suggerisce come il traffico sotterraneo di informazioni stia allargando la propria platea di utilizzatori, il che dovrebbe aumentare la preoccupazione di tutti noi e l'attenzione con la quale trattiamo i nostri dati e ci comportiamo nella dimensione digitale della nostra vita personale e lavorativa.

UN TUFFO NEL PROFONDO WEB

Anche perché non c'è solo l'ambiente opaco del Dark Web: basti ricordare come la stragrande maggioranza delle informazioni presenti nel Web "normale" non sia rastrellata dai motori di ricerca come Google – si tratta per esempio di contenuti audio o video, database o siti dinamici – e che sia anzi in costante crescita grazie all'avvento dell'IoT o Internet of Things (la rete dei dispositivi automatici, macchinari e sensori che ci circonda sempre più in ogni aspetto pratico della nostra quotidianità).

Potremmo dunque definire il **Deep Web come quella parte del Web "normale" che resta al di sotto dell'orizzonte stabilito dai motori di ricerca, e come tale può infondere nei suoi autori un falso senso di sicurezza con un conseguente abbassamento dei normali livelli di difesa informatica** che viene prontamente sfruttato dai malintenzionati che carpiscono così informazioni rivendibili nel Dark Web. Ecco qualche casistica di diffusione di dati riservati, giusto per restare tra quelle venute alla luce nel 2020:

- 500.000 documenti di natura bancaria e legale (compresi documenti di identità personali) legati alla app di due finanziarie americane;
- 845 gigabyte di informazioni provenienti da almeno otto app per la ricerca dell'anima gemella realizzate dal medesimo sviluppatore e installate da centinaia di migliaia di utenti in tutto il mondo;
- 10 anni di informazioni personali e bancarie su viaggiatori raccolte da un fornitore di servizi software utilizzati dalle più diffuse piattaforme online per la prenotazione di voli e hotel.

Come vedi, sono lontanissimi i tempi in cui potevi concederti il lusso di ignorare le questioni legate a sicurezza informatica e disseminazione delle informazioni personali "perché tanto sono problemi che riguardano le aziende grandi, ricche e famose".

Il rischio è ormai comune a tutti, anche perché il cybercrimine si avvale in gran parte di processi automatizzati che non guardano in faccia nessuno: dalla multinazionale al pensionato, oggi siamo tutti potenziali bersagli.

Se non ci credi, riguarda gli esempi di furti di dati citati prima; dopodiché **capirai bene come non sia difficile sfruttare le informazioni sottratte a un operatore telefonico per portare a termine un'azione di *SIM swapping***, ovvero lo spostamento illecito di un numero di telefono su una SIM in possesso dell'attaccante che potrà quindi ricevere tutti i codici di verifica per l'autenticazione a due fattori (2FA) destinati al proprietario originale del numero. Numero che viene quindi facilmente incrociato con i vari database circolanti nel Dark Web per scoprire gli indirizzi email ad esso associati e, tramite questi ultimi, risalire agli account aperti su social media e altri servizi online.

In un attimo è dunque possibile infiltrarsi:

- nella posta elettronica;
- nei social media;
- nei servizi bancari e finanziari

di una qualunque persona modificando le password proprio grazie al controllo del telefono e, quindi, del meccanismo 2FA che è ormai il sistema consolidato per comprovare a distanza l'identità di titolari di conti correnti o utenti di servizi pubblici o piattaforme online.

E se quel numero di telefono fosse proprio il tuo?

LE MOTIVAZIONI NON MANCANO

Uno degli aspetti più temibili della violazione del profilo digitale di una persona è che questa non si limita in genere a un unico malintenzionato.

L'underground informatico è popolato da numerosi individui, spesso organizzati in gruppi, che agiscono indipendentemente l'uno dall'altro attingendo in gran parte alle medesime risorse. **Ne consegue che la presenza dei tuoi dati in qualche angolo del Dark Web potrà essere sfruttata da più di un criminale**, ciascuno per i propri scopi.

Come nella vita reale, anche qui la varietà di truffe che possono essere perpetrate online è davvero vastissima e in costante evoluzione. In genere però lo schema sottostante tende a essere sempre lo stesso: **acquisire le informazioni digitali relative a una persona e assumerne l'identità per colpirla direttamente oppure per risultare convincenti agli occhi di una terza vittima**.

Quest'ultimo caso è molto in auge negli ultimi tempi grazie alla diffusione del cosiddetto **spear phishing**, una tecnica che si avvale di **messaggi email accuratamente personalizzati per spingere qualcuno a compiere una determinata azione**. In genere si tratta di fare click su un allegato o un link, un'azione che scatena l'installazione di codice pericoloso (il famigerato malware) sul computer o dispositivo del malcapitato.

Lo spear phishing registra percentuali di successo maggiori quando il messaggio che lo accompagna appare legittimo agli occhi del destinatario. **Le informazioni contenute devono essere realistiche o credibili**, e la mail deve preferibilmente provenire da un indirizzo conosciuto ed essere firmata da una conoscenza effettiva. **Per questo le informazioni disponibili nel Dark Web risultano utilissime**, se non addirittura fondamentali.

Senza il phishing non avremmo probabilmente assistito alla capillare diffusione del **fenomeno del ransomware**, un particolare tipo di malware che crittografa dati e documenti presenti sul computer colpito (a volte, sfruttando le reti interne, su tutti i computer di un'organizzazione) rendendoli di fatto inutilizzabili fintanto che non venga pagato un riscatto, generalmente in Bitcoin.

Avrai letto molte volte sui giornali i casi di **aziende**, scuole o enti pubblici **le cui attività sono state fermate da non meglio precisati "attacchi informatici"**.

Ebbene, nella maggior parte dei casi **si tratta esattamente di attacchi ransomware**, che tra l'altro hanno spesso un carattere definitivo dal momento che non sempre i cybercriminali forniscono la chiave di decifrazione una volta versato il riscatto – senza contare che agli enti pubblici e a molte aziende è proibito per legge o per policy interna pagare alcuna somma in casi come questi.

Una variante maggiormente sofisticata del phishing, realizzata su misura della vittima specifica, è poi la cosiddetta "email del boss" **o BEC, Business Email Compromise**: in questo caso si prende di mira una persona che ricopre un determinato ruolo all'interno di un'azienda per convincerla a effettuare un bonifico a un fornitore fasullo oppure a modificare l'IBAN di un beneficiario legittimo.

Una truffa del genere, che richiede una preparazione degna di un servizio di intelligence, si articola in un periodo di tempo sufficiente per imparare le abitudini della vittima, risalire alla sua rete di contatti e frequentazioni, e magari assumere anche il controllo dei profili social o delle caselle email degli interlocutori ritenuti maggiormente funzionali al successo dell'iniziativa allo scopo di rendere più credibile la storia che viene propinata.

Tanto lavoro viene fatto pagare a caro prezzo: gli importi sottratti sono solitamente elevati (nel 2019 il gruppo italiano Maire Tecnimont è stato truffato di 17 milioni di euro, per fare un esempio), quando addirittura non venga dato corso ad azioni di spionaggio industriale o di sabotaggio una tantum o ripetute nel tempo.

IL RUOLO ATTIVO DELLE VITTIME

L'enorme incremento dei casi di cybertruffe al quale si sta assistendo negli ultimi tempi non rimane incontrastato.

Anzi, a ben vedere l'aumento del ricorso ad azioni di ingegneria sociale è proprio la conseguenza del rafforzamento contro virus e attacchi algoritmici cui sono state generalmente sottoposte in questi anni le infrastrutture IT. In altre parole, abbiamo oggi un'informatica più solida e affidabile dal punto di vista tecnico, il che **ha costretto i criminali a trovare un nuovo anello debole della catena – l'utente**.

Banche, enti pubblici, operatori telefonici e grandi organizzazioni in genere stanno già modificando i propri processi operativi in modo da rendere più difficile che la disattenzione di un dipendente possa creare una vulnerabilità interna o nei confronti di un cliente. **Le piccole aziende e i privati sono invece ancora in grande ritardo in termini sia di sensibilizzazione che di contrasto al problema**.

È qui che tu stesso puoi iniziare a fare la differenza, innanzitutto informandoti (e il fatto che tu stia leggendo questo white paper è già un passo utile al riguardo) e quindi **responsabilizzando le persone che ti sono vicine sia nella vita personale che in quella lavorativa**.

Segui e fai **seguire queste semplici regolette**:

- non fidarti mai di email, SMS, messaggi WhatsApp e simili: non sempre chi ti contatta è davvero chi pretende di essere. Lo stesso vale per i numeri telefonici di chi ti chiama, che possono essere facilmente falsificati;
- non aprire mai allegati né seguire link che ti vengono proposti in un messaggio se non ne hai prima verificato la legittimità;
- chiedi sempre conferma usando un canale diverso da quello del contatto iniziale: per esempio, manda una email per verificare un SMS o un messaggio WhatsApp. Se ti contattano da un numero mobile, richiama al numero fisso;
- sospetta in modo particolare in caso di richieste di denaro, di dati personali (tuoi o di altri), di numeri di carte di credito o di qualunque richiesta diversa dal consueto;
- mai, mai, mai fornire password e credenziali a chicchessia, qualunque sia il motivo;
- non esistono sconosciuti che fanno regali. Se ti contattano perché vogliono donarti soldi, perché hai vinto a concorsi a cui non hai mai partecipato, perché sei il fortunato milionesimo visitatore di un sito o perché c'è un superpremio che ti aspetta per aver risposto esattamente a tre domande stupide, ebbene, sei libero di crederci a tuo rischio e pericolo (poi non dire che non ti avevamo avvisato) ;
- infine, la regola d'oro: se è troppo bello per essere vero, quasi certamente non lo è.

I PASSI SUCCESSIVI

Stabilita una prima base di comportamenti fondamentali per la sicurezza tua, della tua azienda e delle persone che ti sono vicine, **arriva il momento di attrezzarsi in maniera un po' più strutturata** per erigere difese maggiormente efficaci.

Passo #1 - Consapevolezza della situazione

Per prima cosa dovresti andare a **controllare se i tuoi dati** – ed eventualmente quali – **stiano già circolando nel Dark Web**. A questo scopo ti consigliamo un sito verificato, Have I Been Pwned (https://haveibeenpwned.com), che tiene traccia di tutti gli indirizzi email coinvolti in casi pubblici di sottrazione di informazioni. Si tratta di un servizio legittimo del tutto simile a Mozilla Monitor (https://monitor.firefox.com), sul quale è possibile lasciare la propria email per essere avvisati nel caso dovesse improvvisamente comparire in qualche database di violazioni.

Servizi di questo tipo **non possono escludere al 100% che i tuoi dati non siano stati sottratti**, ma costituiscono comunque un buon punto di partenza per approfondire eventuali segnalazioni che dovessero emergere. **A volte le violazioni comportano anche la sottrazione di password**: questo permette ai malintenzionati non solo di entrare facilmente nell'account violato, ma anche di sfruttare le medesime credenziali per tentare l'accesso ad altri servizi nella certezza che ancora molte persone tendono a riutilizzare più e più volte la stessa coppia username/password. Ecco perché tutti gli esperti raccomandano sempre di usare sempre password differenti.

Ci sono poi dei sistemi, più “intelligenti”, in grado di **monitorare costantemente cosa accade nel Dark Web** e di avvertirti prontamente nel caso in cui le tue credenziali dovessero comparirvi in qualche modo.

Questi possono essere molto utili per scongiurare un disastro, intercettando il losco traffico di dati prima che possa arrecare dei danni alla tua azienda.

Puoi chiedere al tuo fornitore IT maggiori informazioni su questo tema.

Passo #2 - Aggiornamento e formazione

Come abbiamo detto, il cybercrimine non si siede sugli allori ed è sempre all'opera per trovare nuove strade e nuove vittime.

Per questo **è importante che tu e chi lavora nella tua organizzazione siate sempre informati sulle tecniche più recenti e sulle tipologie di attacchi in atto**. Tieni alta l'attenzione di chi ti circonda, magari invitando degli esperti a tenere degli incontri periodici di aggiornamento: il tema si presta bene a conversazioni vivaci costellate di interessanti aneddoti ed esempi concreti. Il tuo consulente IT potrà darti una mano al riguardo.

Prendi anche in considerazione l'opportunità di organizzare delle campagne di spear phishing simulato.

Si tratta di **ideare e diffondere all'interno della tua azienda delle finte mail di phishing**. Quanti ci sono cascati? Quanti hanno ignorato il messaggio? Quanti lo hanno segnalato al reparto IT e ai colleghi? Mettere alla prova l'organizzazione è il modo migliore per verificarne concretamente l'effettiva preparazione e, nel caso, adottare le opportune contromisure. Puoi chiedere aiuto al tuo fornitore di servizi IT per preparare una campagna di questo tipo.

Passo #3 - Un po' di procedura

Restare aggiornati sulle tendenze cybercriminali ti aiuterà anche a capire quali siano i punti deboli sui quali spingono i truffatori. Per rendere più solida e resistente la tua organizzazione puoi approntare qualche semplice procedura allo scopo di evitare che la disattenzione di un singolo possa mettere a repentaglio l'azienda e i suoi asset.

Considera per esempio la **variazione degli IBAN**, una situazione che accade legittimamente quando un'azienda cambia banca o quando avviene una fusione tra istituti di credito – ma che **viene cavalcata a fini illeciti dagli specialisti in truffe BEC**. In questo caso **puoi definire due procedure**:

- *protezione degli incassi*: aggiungi nelle tue comunicazioni formali ai clienti (fatture comprese) una dicitura standard che li inviti a contattarti telefonicamente qualora ricevessero mai una richiesta di modificare il tuo IBAN;
- *protezione degli esborsi*: stabilisci la prassi di verificare telefonicamente o di persona le richieste di modifica dell'IBAN che ricevi dai tuoi fornitori. Tieni traccia delle persone coinvolte dalle verifiche (sia dal tuo lato che da quello del fornitore).

Ancora, predisponi degli accorgimenti formali per gestire richieste insolite o sensibili provenienti da dirigenti o dipendenti che si trovano in viaggio per una trasferta di lavoro o una vacanza.

I cybercriminali sono soliti seguire i profili social dei loro potenziali obiettivi per conoscerne gli spostamenti e approfittare della distanza fisica per allentare le verifiche interne delle aziende: questo ha favorito la diffusione di richieste illecite di denaro conosciute come le truffe "del capo in vacanza".

Passo #4 - Sicurezza a strati

Poiché è oggettivamente difficile riuscire a tenere il ritmo forsennato delle tecniche sempre nuove che scaturiscono dagli ingegni cybercriminali, **una buona soluzione per te e per la tua azienda è quella di proteggerti con una serie di difese in grado di coordinarsi reciprocamente grazie a capacità di analisi e correlazione degli eventi**. L'obiettivo è quello di ottenere ciò che viene chiamata "visione olistica" della difesa informatica, ovvero la capacità di percepire l'insieme di segnali differenti che presi singolarmente non sarebbero fonte di preoccupazione ma che, messi in fila e inquadrati nel giusto contesto, possono far scattare tutti gli allarmi e le contromisure del caso salvaguardando i tuoi dati.

Il bello di una sicurezza a strati è che ogni suo elemento – da quello per la protezione degli endpoint a quello che tiene sotto controllo il traffico di rete – collabora con tutti gli altri rafforzando la protezione complessiva.

I malintenzionati si accorgono subito se una potenziale vittima dispone di adeguate contromisure o meno, e in genere **scelgono quella che offre la minor resistenza possibile**.

A parità di potenziale bottino, tra una villa circondata da alte mura con telecamere, sensori perimetrali, cani da guardia, allarmi volumetrici, porte e tapparelle blindate e invece un appartamento protetto solo da una semplice serratura a doppia mappa, a quale obiettivo credi che un ladro preferirà dedicarsi?

Anche nel crimine è sempre una questione di costo/risultato, e il tuo fornitore IT saprà certamente consigliarti anche in questo ambito.

Glossario

BEC Business Email Compromise – Una sofisticata truffa mirata che nella sua versione più diffusa assume l'aspetto di comunicazioni provenienti da un dirigente aziendale per convincere un altro dipendente a dare corso a pagamenti verso conti bancari riconducibili agli autori dell'illecito. Per dare credibilità alle richieste vengono spesso falsificati documenti ufficiali e creati domini Internet dal nome molto simile a quello delle aziende e degli enti coinvolti.

Dark web – Un vero e proprio web parallelo costituito da sistemi collegati a Internet attraverso software e configurazioni particolari, al cui interno si svolgono attività prevalentemente illegali di ogni genere. Il dark web rappresenta una componente del cosiddetto deep web, ovvero quella porzione del web che non è accessibile ai normali motori di ricerca.

Malware – Combinazione dei termini inglesi "malicious" (malevolo, pericoloso, illecito) e "software". Indica l'insieme degli strumenti software che i cybercriminali utilizzano per entrare nei computer delle loro vittime, assumerne il controllo in modo parziale o integrale, propagarsi all'interno della rete colpita ed effettuare attività illecite come la sottrazione di dati personali o sensibili, lo spionaggio, l'invio di messaggi di posta indesiderata o il blocco crittografico dei dati a scopo di riscatto. Ognuna di queste attività assume una propria denominazione, come spyware, spamware, ransomware ecc.

Phishing – Una truffa diffusa principalmente tramite messaggi di posta elettronica e SMS attraverso i quali si tenta di carpire informazioni sensibili alle vittime facendo credere che la richiesta provenga da un interlocutore affidabile. I messaggi solitamente rimandano a pagine web fraudolenti che replicano l'aspetto di quelle ufficiali invitando il destinatario a inserire le proprie credenziali o i codici delle carte di credito con le scuse più diverse. A differenza delle truffe BEC, concettualmente simili ma accuratamente personalizzate, il phishing si avvale di invii di messaggi in massa.

Ransomware – Un particolare tipo di malware che crittografa i file residenti sul computer colpito (e spesso anche su tutti gli altri dispositivi collegati alla stessa rete) che diventano così inaccessibili a meno di non pagare un riscatto per ottenere la chiave di decifrazione necessaria. Non sono rari i casi in cui anche la disponibilità di questa chiave non consenta il ripristino corretto dei sistemi, con gravi conseguenze per le aziende.

SMS Short Message Service – Servizio che permette l'invio di brevi messaggi di testo da 160 caratteri di lunghezza attraverso la rete telefonica. Reso possibile dalla definizione degli standard GSM del 1985, il servizio SMS ha dovuto attendere sette anni prima di essere implementato effettivamente, raggiungendo in breve un successo su scala planetaria che prosegue ancora oggi nonostante la concorrenza dei servizi di messaging basati su Internet come WhatsApp, Telegram, Viber, iMessage e Facebook Messenger.