# I Data Breach degli account aziendali: le raccomandazioni per non sottovalutare il rischio

**Date :** 28 settembre 2017


## Scenario

Ogni giorno assistiamo ad un numero crescente di furto di dati (e-mail, password, carte di credito, documenti confidenziali, etc) sui sistemi aziendali o personali, perpetrati principalmente da gruppi di cyber criminali, comunemente chiamati in gergo “Bad Actors”. I Bad Actors realizzano cyber attacchi per diverse finalità, come: l’estorsione, spionaggio o danneggiamento degli asset critici Nazionali o Aziendali. Negli ultimi anni i Bad Actors si stanno evolvendo sia dal punto di vista dell’organizzazione interna, reclutando nuove persone all’interno dei diversi forum sparsi nel Deep e Dark Web, sia dal punto di vista della complessità degli attacchi.

Basti pensare che esistono gruppi specializzati per diversi settori come ad esempio Lazarus (finanziario e governativo), APT 28 (governativo), OilRig (energetico), FIN7 (finanziario), etc, con un raggio di azione che ha come obiettivo gli asset critici delle singole Nazioni, grandi corporate, piccole aziende (SME), organizzazioni sanitarie e istituti finanziari.

Un esempio recente è rappresentato dal Data Breach di una delle più grandi agenzie di credito americana (Equifax), la quale ha annunciato di avere subito un Breach con un potenziale effetto su oltre 143 Milioni di clienti sparsi tra gli Stati Uniti, Canada e Regno Unito. I dati rubati in questo caso contenevano nomi, numeri di previdenza sociale, date di nascita, indirizzi, numero della patente di guida e 209.000 numeri di carte di credito di clienti US (https://www.equifaxsecurity2017.com/).

La possibilità che i dati rubati non vengano utilizzati è decisamente scarsa, mentre è molto probabile che i dati saranno poi utilizzati per attività di Phishing, Spear Phishing o per attacchi di ingegneria sociale, e quindi utilizzati per compromettere il proprio PC o l’infrastruttura di un azienda, rendendola magari parte di una bot-net da usare in un secondo momento per un cyber attacco più complesso o come vittima di un attacco Ramsonware (es. WannaCry o notPetya).

La compromissione, come si deduce dall’ultimo caso è pressoché inevitabile, pertanto bisogna cercare di spostare l’attenzione dei decisori, verso forme di prevenzione e detection delle cyber minacce, riducendo così la possibilità di essere oggetto di Data Breach.

Esiste però una buona notizia, in quanto il Breach di una rete o sistema non è immediatamente uguagliabile alla perdita di un dato o alla distruzione di un servizio. Ogni attaccante segue delle precise fasi “Cyberattack Lifecycle” con precisi step operativi prima di perpetrare un attacco e raggiungere il suo obiettivo, in cui la parte di *Gather Intelligence* rappresentata dalle attività di *Reconnaissance*, risulta essere fondamentale per la buona riuscita dell’attacco, in cui i dati presenti in eventuali Data Breach pubblici possono essere utilizzati per le attività di *Initial Compromise* o addirittura nella fase di *Lateral Movement* (Dopo la creazione di un accesso remoto al sistema all’interno di una rete aziendale, l’attaccante può fare leva sulle informazioni ricavate o già in suo possesso per spostare la compromissione verso altri asset aziendali).

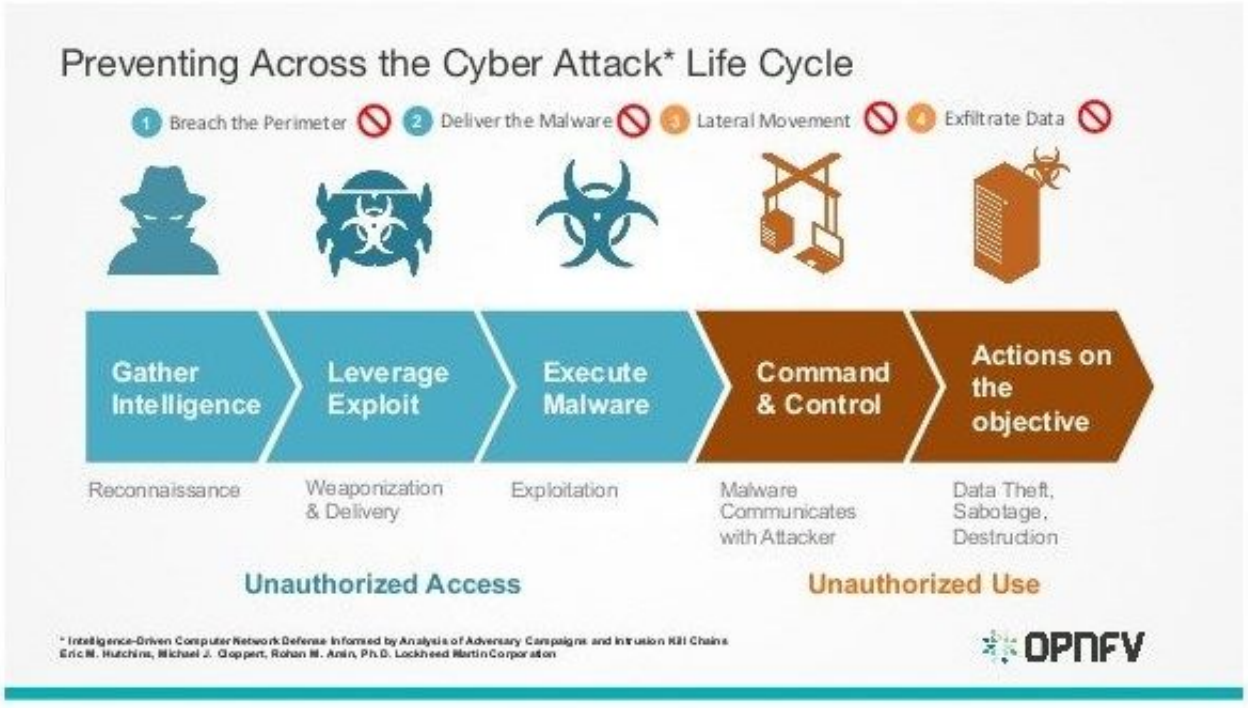


Figura 1 - Cyberattack Lifecycle fonte OPNFV

L’attività di *Reconnaissance*, rappresenta lo step iniziale in cui l’attaccante sceglie l’obiettivo, rappresentato da una possibile vittima (persona fisica), l’infrastruttura critica da distruggere o a chi inviare un messaggio di minaccia. Successivamente sceglie i sistemi o il sistema che può essere attaccato su cui l’attacco può avere maggiore successo, magari anche in base alle informazioni già in possesso.  Infine procede nella scrittura di exploite code, customizzazione di mail di spearphishing associate ad un dominio fasullo, o sopralluoghi del sito fisico.

Esistono diversi modi di verifica se una persona o un’azienda è stata oggetto o se è soggetta ad un Data Breach.  Il modo più facile per una persona è attraverso la verifica della propria mail (personale o aziendale)  attraverso portali come ad esempio *( https://haveibeenpwned.com; https://hacked-emails.com/; https://Breachalarm.com/ )*

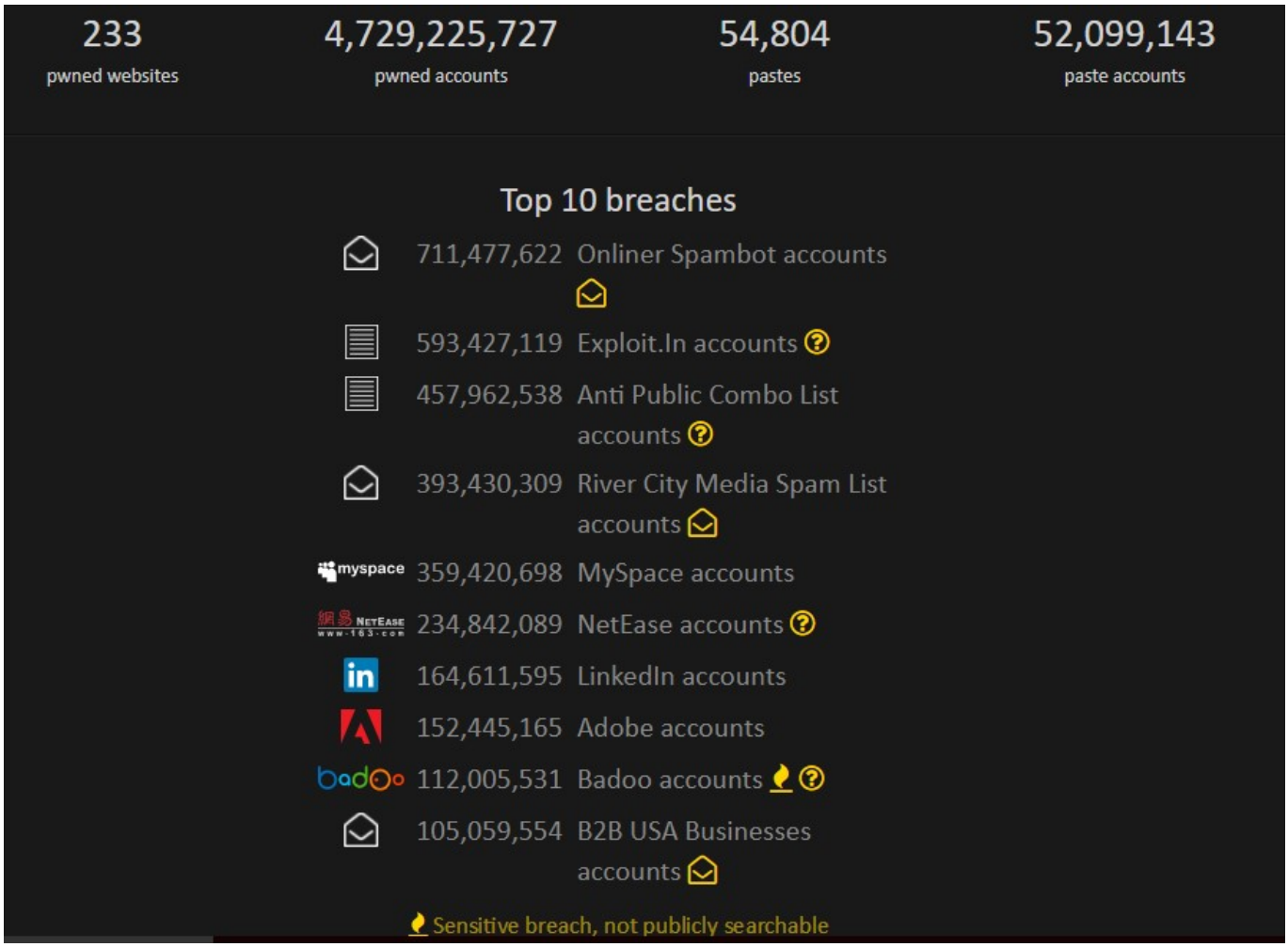


Figura 2 - Lista dei TOP Breaches segnalati da haveibeenpwned.com

Nel caso in cui la propria e-mail sia presente all'interno del Database, non significa che i sistemi o le applicazioni gestite dalla singola persona (es. Smartphone, Home banking, Gmail, Facebook, Tweeter, etc) siano già oggetto di attacco, ma bensì i dati presenti nel Data Breach, potrebbero essere utilizzati da un cyber criminale per un futuro cyber attacco.

Cosa diversa se una azienda vuole sapere se i propri dati, sono presenti in alcuni Data Breach resi pubblici, come ad esempio siti di dump (es. Pastbin (https://pastebin.com/), ricercabili attraverso ricerche nel surface, deep/dark web, segnalate da soggetti che effettuano investigazioni "in-the-wild" o presenti in qualche Trusted Circle. La soluzione migliore è di dotarsi di servizi di Feed ad hoc (a pagamento), da includere all'interno dei propri sistemi di sicurezza, in modo da far scattare immediatamente un alert in caso di Breach ed attivare successivamente le procedure di contenimento.

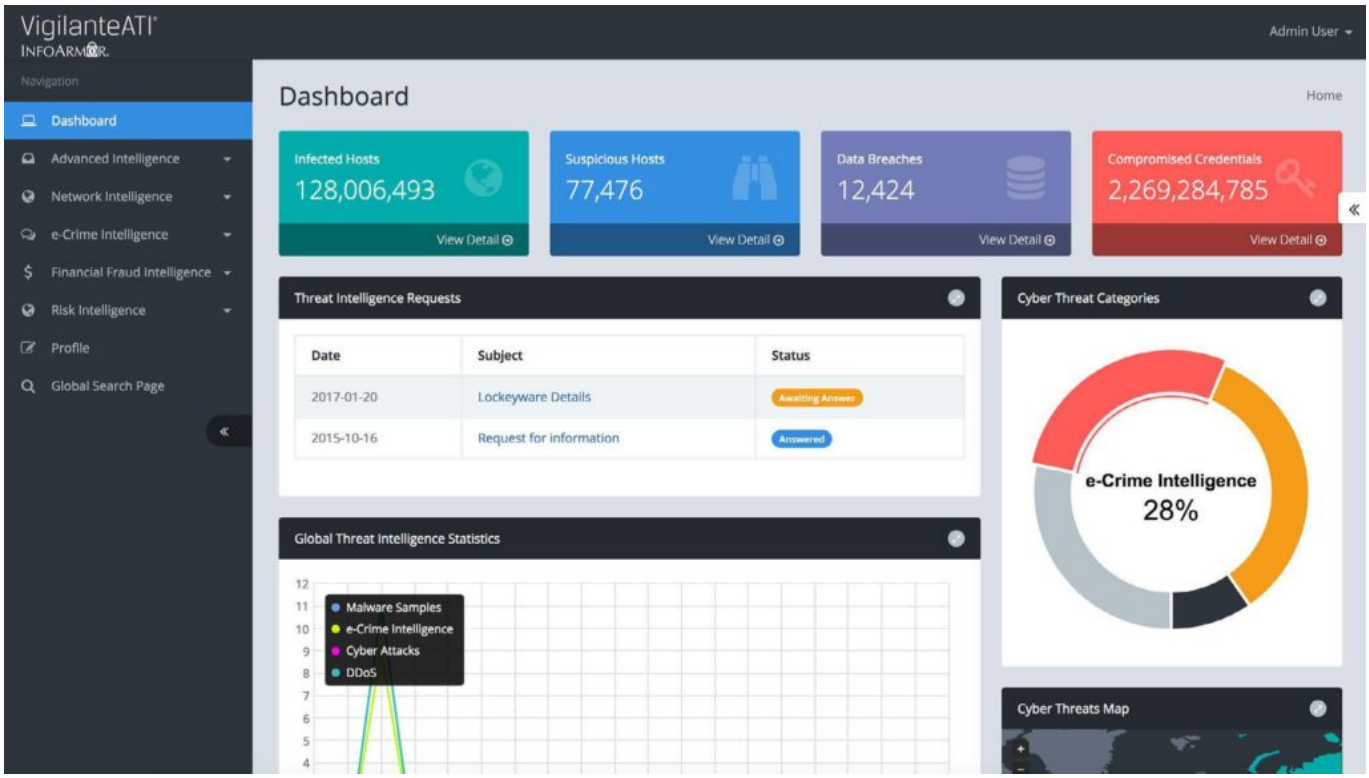


Figura 3 - Esempio di Dashboard di un Feed Provider

Anche se molto spesso parte delle password indicate all'interno dei Data Breach, possono essere datate e non corrispondenti alle attuali, ciò comporta comunque un rischio di futura compromissione sia per la persona sia per l'azienda.  Molto spesso l'"algoritmo" (*rectius* metodo) utilizzato per costruire la password rimane lo stesso che si utilizzi una e-mail privata o un'e-mail aziendale e quindi facilmente decifrabile da parte di un algoritmo automatico es. tramite attacchi a dizionario.

I consigli di base per gestire eventuali furti di dati sia per le aziende sia per le singole persone sono:

- **Utilizzare sempre per ciascuno servizio una password diversa**. La cosa migliore è crearsi una regola memonica non banale per costruire password preferibilmente di almeno 12 caratteri o parti di una frase;
- **Cambiare con una certa regolarità la password** come la mail, servizi di home banking o social network;
- **Verificare con regolarità sui portali di cui sopra l'eventuale furto delle credenziali**.
- **Attivare le notifiche di login nei vari servizi**come la posta elettronica, home banking, etc;
- **Utilizzare autenticazione multi-fattore** (es. token, SMS sul telefono, etc).

Al momento, il consiglio più importante per le organizzazioni resta quello implementare una Cybersecurity Strategy che combini gli aspetti di Cyber Threat Intelligence, Continuous

Monitoring, Advanced Analytics e Incident Response, al fine di identificare, rispondere e neutralizzare la minaccia prima che si trasformi in un incidente.

A cura di: **Ing. Mattia Siciliano**