

Ora le spie corrono su LinkedIn. Allarme lanciato dal MI5

Maria Cattini | 01/05/2021 | Open source intelligence

Bye bye Mata Hari, affascinante e inarrestabile 007 d'altri tempi. Oggi segreti e informazioni confidenziali degli altri si cercano su **LinkedIn**. O, almeno, questo è l'allarme lanciato dal MI5, il servizio segreto britannico.

La notizia [rimbalza dalla BBC](#) che riferisce di un rapporto dei servizi segreti di Sua Maestà, appunto, secondo i quali, negli ultimi cinque anni almeno dieci mila cittadini inglesi sarebbero stati bersaglio di operazioni di intelligence promosse da Governi stranieri nel tentativo di accaparrarsi segreti di Stato e informazioni confidenziali.

E, tutto, sarebbe avvenuto online.

In particolare, stando al MI5, gli spioni stranieri avrebbero creato una serie di profili LinkedIn fake, completamente fasulli, attraverso i quali persone ritenute in possesso di informazioni sensibili – o capaci di procurarsele – sarebbero state “avvicinate” via LinkedIn con la scusa di un invito a partecipare come speaker a convegni esclusivi a spese degli organizzatori o con irresistibili offerte di lavoro e, ottenuto il contatto via LinkedIn, le avrebbero indotte a fidarsi dei loro interlocutori e, magari – ma nulla il rapporto dice circa il successo di queste operazioni – a fornire informazioni preziose per l'intelligence di Paesi stranieri.

A prescindere dalla vicenda specifica, dai suoi effetti e dalle eventuali conseguenze e a prescindere dal fatto che se i servizi inglesi hanno lanciato un allarme e segnalato un rischio tanto diffuso ed elevato sia in termini quantitativi che qualitativi, non c'è ragione per ritenere che altrettanto non sia avvenuto o non stia avvenendo anche a casa nostra, la notizia conferma una circostanza che tendiamo, forse, troppo spesso a sottovalutare.

Nella dimensione digitale, spesso ma spesso davvero, l'anello debole della catena non sono i software, gli algoritmi, le password, la sicurezza informatica ma, più semplicemente siamo noi.

L'ingegneria sociale, i raggiri, i “camuffamenti” digitali sono strumenti di intrusione di massa nei nostri segreti, in quelli dei Governi e delle società private più potenti e difficili da neutralizzare di tanti altri dei quali, pure, si parla più di frequente.

Serve più educazione, più attenzione, più approccio critico alle relazioni che allacciamo – in tempo di pandemia più che in qualsiasi altro momento in passato – online, attraverso i social network tutti e, naturalmente, non solo attraverso LinkedIn.

È difficile sapere per davvero chi sta dall'altra parte di un dispositivo, chi è la persona dietro un account che, pure, ci si presenta inoffensivo, amico e, talvolta, più che amico.

Chi ci offre, online, la più grande occasione della nostra vita, talvolta, potrebbe provare a rifilarci la più grande fregatura della nostra vita.

E questo non vale solo nel mondo dello spionaggio internazionale ma in tutti gli ambiti della nostra vita nella dimensione digitale.

Le stesse tecniche di ingegneria sociale - o loro varianti messe a punto per l'occasione - possono, evidentemente, essere usate, per le ragioni più diverse, nei siti d'incontri, nei social frequentati anche dai più piccoli, nelle bacheche di annunci di lavoro o di vendita di ogni genere di prodotto.

Guai, naturalmente, a fare d'ogni erba un fascio e guai a trarre la conclusione che online tutto quello che sembra vero non lo è ma, al tempo stesso, guai a fidarci a cuor leggero che tutto quello che ci si dice lo sia e, soprattutto, che dietro Paolo, Francesco, Laura o Lucia ci siano davvero Paolo, Francesco, Laura o Lucia e, soprattutto, che nell'avvicinarsi a noi, magari nel cercarci siano animati per davvero dalle intenzioni che ci rappresentano.

Spesso, purtroppo, non è così e le conseguenze possono essere gravi per i più piccoli, innanzitutto, che corrono il rischio di essere adescati da adulti senza scrupoli ma anche per gli adulti.

Non esistono soluzioni salvifiche né ricette miracolose ma la prudenza e un briciolo di costruttiva diffidenza critica prima di costruire una relazione tra persone distanti e mediata da strumenti digitali sono risorse preziose, anzi, risorse irrinunciabili.

Navigante avvisato è mezzo salvato.

di Guido Scorza (Fonte: The Huffington Post)

Bye bye Mata Hari, affascinante e inarrestabile 007 d'altri tempi. Oggi segreti e informazioni confidenziali degli altri si cercano su **LinkedIn**. O, almeno, questo è l'allarme lanciato dal MI5, il servizio segreto britannico.

La notizia [rimbalza dalla BBC](#) che riferisce di un rapporto dei servizi segreti di Sua Maestà, appunto, secondo i quali, negli ultimi cinque anni almeno dieci mila cittadini inglesi sarebbero stati bersaglio di operazioni di intelligence promosse da Governi stranieri nel tentativo di accaparrarsi segreti di Stato e informazioni confidenziali.

E, tutto, sarebbe avvenuto online.

In particolare, stando al MI5, gli spioni stranieri avrebbero creato una serie di profili LinkedIn fake, completamente fasulli, attraverso i quali persone ritenute in possesso di informazioni sensibili - o capaci di procurarsele - sarebbero state "avvicinate" via LinkedIn con la scusa di un invito a partecipare come speaker a convegni esclusivi a spese degli organizzatori o con irresistibili offerte di lavoro e, ottenuto il contatto via LinkedIn, le avrebbero indotte a fidarsi dei loro interlocutori e, magari - ma nulla il rapporto dice circa il successo di queste operazioni - a fornire informazioni preziose per l'intelligence di Paesi stranieri.

A prescindere dalla vicenda specifica, dai suoi effetti e dalle eventuali conseguenze e a prescindere dal fatto che se i servizi inglesi hanno lanciato un allarme e segnalato un rischio tanto diffuso ed elevato sia in termini quantitativi che qualitativi, non c'è ragione per ritenere che altrettanto non sia avvenuto o non stia avvenendo anche a casa nostra, la notizia conferma una circostanza che tendiamo, forse, troppo spesso a sottovalutare.

Nella dimensione digitale, spesso ma spesso davvero, l'anello debole della catena non sono i software, gli algoritmi, le password, la sicurezza informatica ma, più semplicemente siamo noi.

L'ingegneria sociale, i raggiri, i "camuffamenti" digitali sono strumenti di intrusione di massa nei nostri segreti, in quelli dei Governi e delle società private più potenti e difficili da neutralizzare di tanti altri dei quali, pure, si parla più di frequente.

Serve più educazione, più attenzione, più approccio critico alle relazioni che allacciamo - in tempo di pandemia più che in qualsiasi altro momento in passato - online, attraverso i social network tutti e, naturalmente, non solo attraverso LinkedIn.

È difficile sapere per davvero chi sta dall'altra parte di un dispositivo, chi è la persona dietro un account che, pure, ci si presenta inoffensivo, amico e, talvolta, più che amico.

Chi ci offre, online, la più grande occasione della nostra vita, talvolta, potrebbe provare a rifilarci la più grande fregatura della nostra vita.

E questo non vale solo nel mondo dello spionaggio internazionale ma in tutti gli ambiti della nostra vita nella dimensione digitale.

Le stesse tecniche di ingegneria sociale - o loro varianti messe a punto per l'occasione - possono, evidentemente, essere usate, per le ragioni più diverse, nei siti d'incontri, nei social frequentati anche dai più piccoli, nelle bacheche di annunci di lavoro o di vendita di ogni genere di prodotto.

Guai, naturalmente, a fare d'ogni erba un fascio e guai a trarre la conclusione che online tutto quello che sembra vero non lo è ma, al tempo stesso, guai a fidarci a cuor leggero che tutto quello che ci si dice lo sia e, soprattutto, che dietro Paolo, Francesco, Laura o Lucia ci siano davvero Paolo, Francesco, Laura o Lucia e, soprattutto, che nell'avvicinarsi a noi, magari nel cercarci siano animati per davvero dalle intenzioni che ci rappresentano.

Spesso, purtroppo, non è così e le conseguenze possono essere gravi per i più piccoli, innanzitutto, che corrono il rischio di essere adescati da adulti senza scrupoli ma anche per gli adulti.

Non esistono soluzioni salvifiche né ricette miracolose ma la prudenza e un briciolo di costruttiva diffidenza critica prima di costruire una relazione tra persone distanti e mediata da strumenti digitali sono risorse preziose, anzi, risorse irrinunciabili.

Navigante avvisato è mezzo salvato.

di Guido Scorza (Fonte: The Huffington Post)