PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4930 di Lunedì 10 maggio 2021

La protezione dati personali presenti nei file PDF

Il formato di file PDF è uno dei più diffusi al mondo e viene utilizzato per lo scambio di comunicazioni di varia natura. Un recente studio ha messo in evidenza come in questi file siano presenti dati personali di cui spesso gli utenti non sono coscienti.

Oggi il formato PDF è uno di quelli più diffusi, per lo scambio e la distribuzione di documenti elettronici. Purtroppo, molte organizzazioni non sono al corrente del fatto che questi documenti possono rivelare dati personali, anche particolari, ad insaputa degli autori del documento.

Ad esempio, il nome dell'autore del documento, informazioni sull'architettura informatica con la quale documento è stato prodotto ed altre notizie possono essere estratte dal documento e utilizzate per perpetrare attacchi informatici.

Due ricercatori dell'Università di Grenoble hanno raccolto poco meno di 40.000 file PDF, pubblicati da sette enti di sicurezza, situati in 47 paesi, e li hanno analizzati.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0330] ?#>

I ricercatori hanno estratto e misurato la quantità e la qualità di informazioni, che erano presenti in questi file. Molte di queste informazioni potevano essere usate per individuare dei punti deboli nell'architettura informatica, utilizzabili per un attacco.

I ricercatori inoltre hanno verificato quanti enti adottavano delle tecniche di pulizia dei file PDF. Solo alcuni enti utilizzavano queste tecniche e non le applicavano neanche a tutti i documenti, che venivano pubblicati.

Inoltre, l'efficienza dei processi di pulizia era lungi dall'essere soddisfacente, perché nel 65% dei file puliti sono stati comunque recuperati dei dati significativi.

La ragione di questo fatto è da imputare all'utilizzo di sistemi di pulizia, che non entrano sufficientemente in profondità nell'analisi del documento.

Per sottolineare l'importanza di questi interventi, i ricercatori hanno ricordato un evento, verificatosi nel febbraio 2003, quando il governo britannico ha pubblicato su un sito Web un dossier sulla organizzazione della sicurezza e la intelligence dell'Iraq. Il dossier era un file di Word trasformato in PDF. Un ricercatore analizzò attentamente questo documento e poté identificare gli autori del documento, la loro posizione nel governo britannico e le varie date di revisione del documento. La diffusione di queste informazioni creò grande imbarazzo per il governo britannico.

Nel 2005, vi fu uno scontro accidentale fra i soldati americani e agenti del servizio segreto italiano, vicino all'aeroporto di Bagdad. Andrea Nicola Calipari, funzionario e agente segreto italiano, fu ucciso da soldati statunitensi (nel contesto della guerra d'Iraq) il 4 marzo del 2005, mentre si recava in macchina all'aeroporto di Baghdad, nelle fasi immediatamente successive alla liberazione della giornalista Giuliana Sgrena.

Sono certo che tutti i lettori si ricordano perfettamente questo tragico evento. Le forze multinazionali dell'Iraq pubblicarono un rapporto sulle indagini su questo incidente. Il rapporto venne pubblicato come file PDF con alcuni dati sensibili, presenti nel testo, oscurati. Fu assai facile, per chi aveva una minima esperienza informatica, provvedere alla analisi del documento e ad eliminare la mascheratura applicata su alcune parole del testo.

La National Security Agency americana poco dopo questi due eventi provvide a diffondere un documento, nel quale metteva in guardia tutti gli enti federali americani sul fatto che, se non venivano effettuate accurate procedure di bonifica di questi dati, essi potevano essere accessibili anche a soggetti non autorizzati.

A questo punto concludo questa informazione, ponendo due domande ai lettori:

- tutti coloro che compilano e diffondono documenti in formato PDF sono al corrente del fatto che da essi potrebbero essere recuperate informazioni riservate?
- quando vengono diffusi documenti aziendali in formato PDF, gli stessi sono stati sottoposti a procedure di bonifica?

Adalberto Biasiotti

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

www.puntosicuro.it