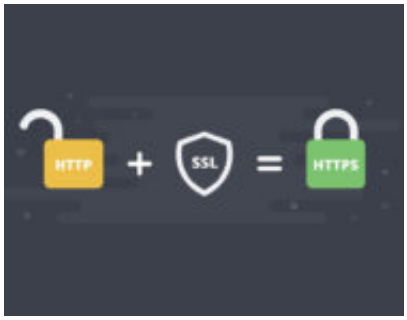
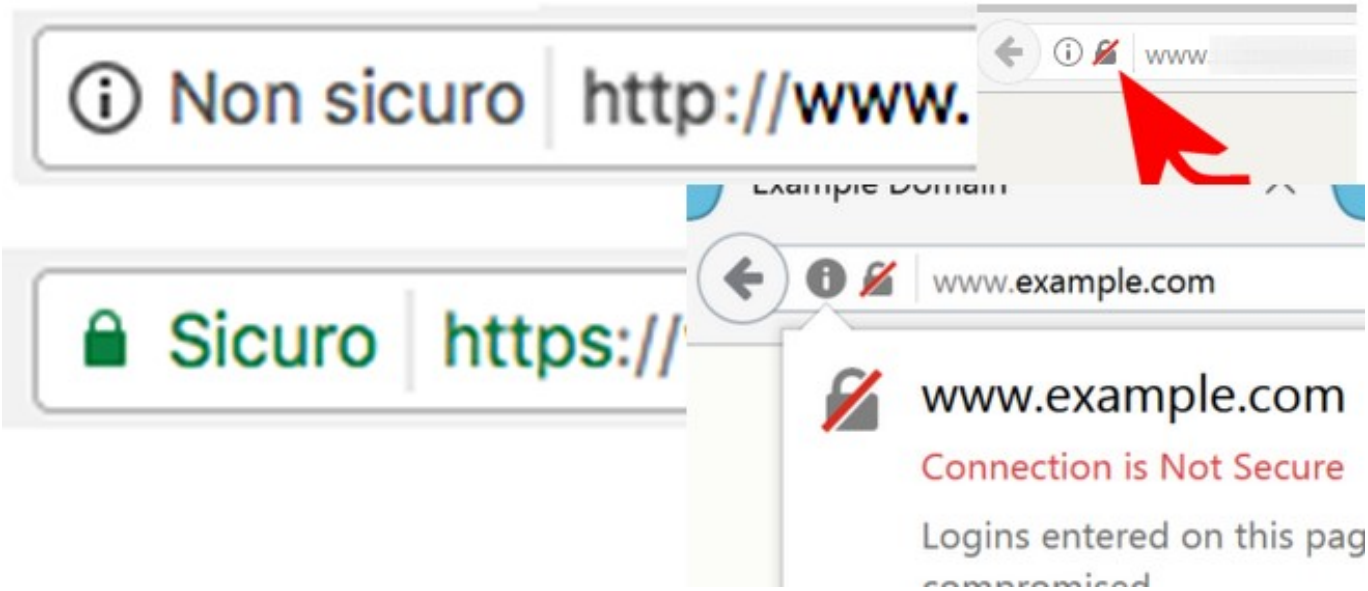
HTTPS è ancora sicuro?

Author : Daniele Rigitano

Date : 30 novembre 2018



Durante i primi mesi del 2017 gli utenti di internet potevano ritenersi un pizzico più sicuri in seguito all'uscita delle nuove versioni di Chrome e Firefox[1]. Google e Mozilla ebbero l'ottima idea di introdurre una funzionalità in grado di segnalare tutte i siti HTTP che contenessero al loro interno moduli da riempire: le pagine contenenti campi quali username, password, carta di credito o similari, iniziarono ad essere contrassegnate come "non sicure"[2].



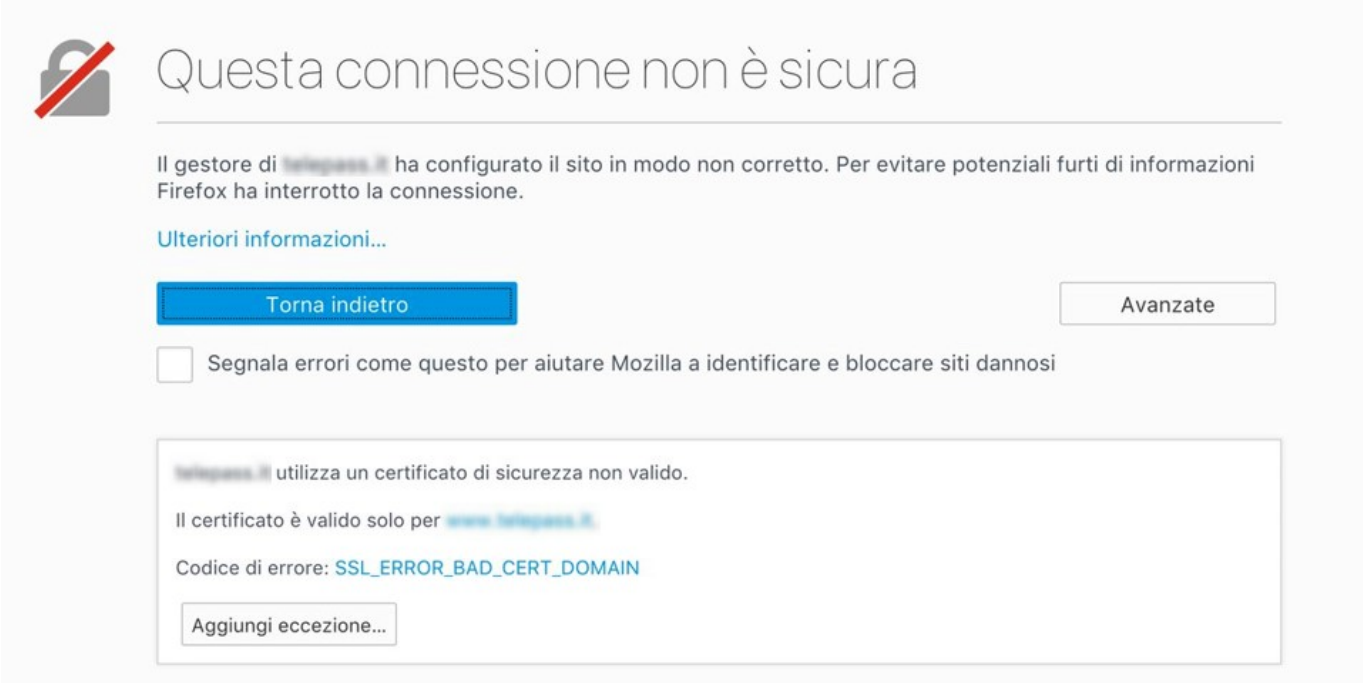
In questo modo è stato **indirettamente imposto** ai creatori di contenuti web l'utilizzo del protocollo HTTPS.

L'HTTPS consente la comunicazione sicura mediante il protocollo HTTP all'interno di una connessione criptata, SSL o TLS. Il principio alla base dell'HTTPS è quello di avere:

- un’autenticazione del sito web visitato;
- protezione della privacy;
- integrità dei dati scambiati tra le parti comunicanti.

Questa misura di sicurezza implica che se un utente ha intenzione di creare un proprio sito internet si trova nella condizione di dover acquistare un certificato SSL[3].

In caso contrario vi è l’opportunità di auto-generare il proprio certificato, ottenendo però uno sgradevole avviso come quello riportato nella figura sottostante, poiché non vi è alcuna Certification Autority (CA) in grado di garantire i punti precedentemente descritti.



Non tutti sanno però che già da prima dell’introduzione di queste restrizioni, è presente sul mercato un servizio totalmente gratuito che consente di generare certificati SSL in pochi semplici passaggi.

I VANTAGGI DI LET’S ENCRYPT

Let’s Encrypt è una Certification Authority che gratuitamente automatizza la creazione, la validazione, il rilascio ed il rinnovo di certificati X.509 per il protocollo TLS.

Il protocollo utilizzato da Let’s Encrypt per l’autenticazione e il rilascio dei certificati si chiama *Automated Certificate Management Environment* (ACME), ed è un protocollo di tipo *challenge-response*. Il server (Let’s Encrypt) presenta al client (il web server da certificare) un insieme di challenge che il proprietario del dominio deve risolvere per provare di essere il responsabile del dominio.

Nel 2017, l’organizzazione ha annunciato di aver emesso oltre 100 milioni di certificati di sicurezza, diventando in breve tempo una delle più grandi CA per numero di certificati emessi.

Lo scopo principale del progetto è quello di riuscire a cifrare tutte le comunicazioni sul World Wide Web. Let’s Encrypt si prefigge di raggiungere questo obiettivo azzerando il costo dei certificati ed andando ad automatizzare il processo di configurazione del web server, della verifica tramite email e del rinnovo del certificato. In questo modo la complessità di gestione e manutenzione di una cifratura TLS si riduce drasticamente[4].

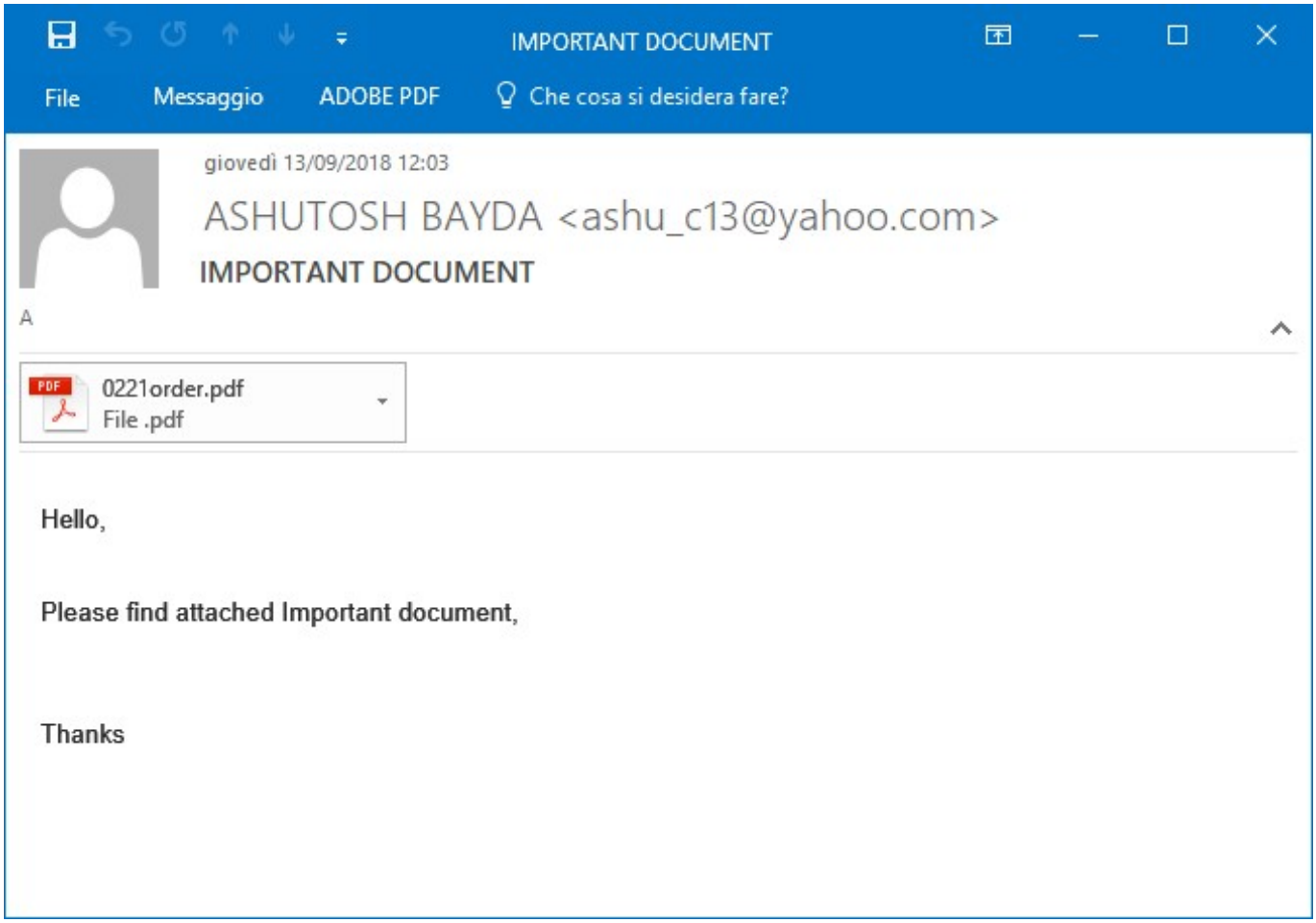
LET’S ENCRIPT È SICURO?

Nonostante l’obiettivo prefissato dai creatori di Let’s Encrypt sia quello di migliorare la sicurezza e la privacy per tutti gli utenti, ciò non significa che non vi siano modi per utilizzare i certificati generati in modo improprio. Difatti, nel marzo 2017, l’esperto di crittografia *Vincent Lynch* ha rivelato che in un periodo di 12 mesi Let’s Encrypt ha emesso circa 15.000 certificati di sicurezza contenenti il ??termine PayPal riconducibile a siti utilizzati per attività di phishing[5].

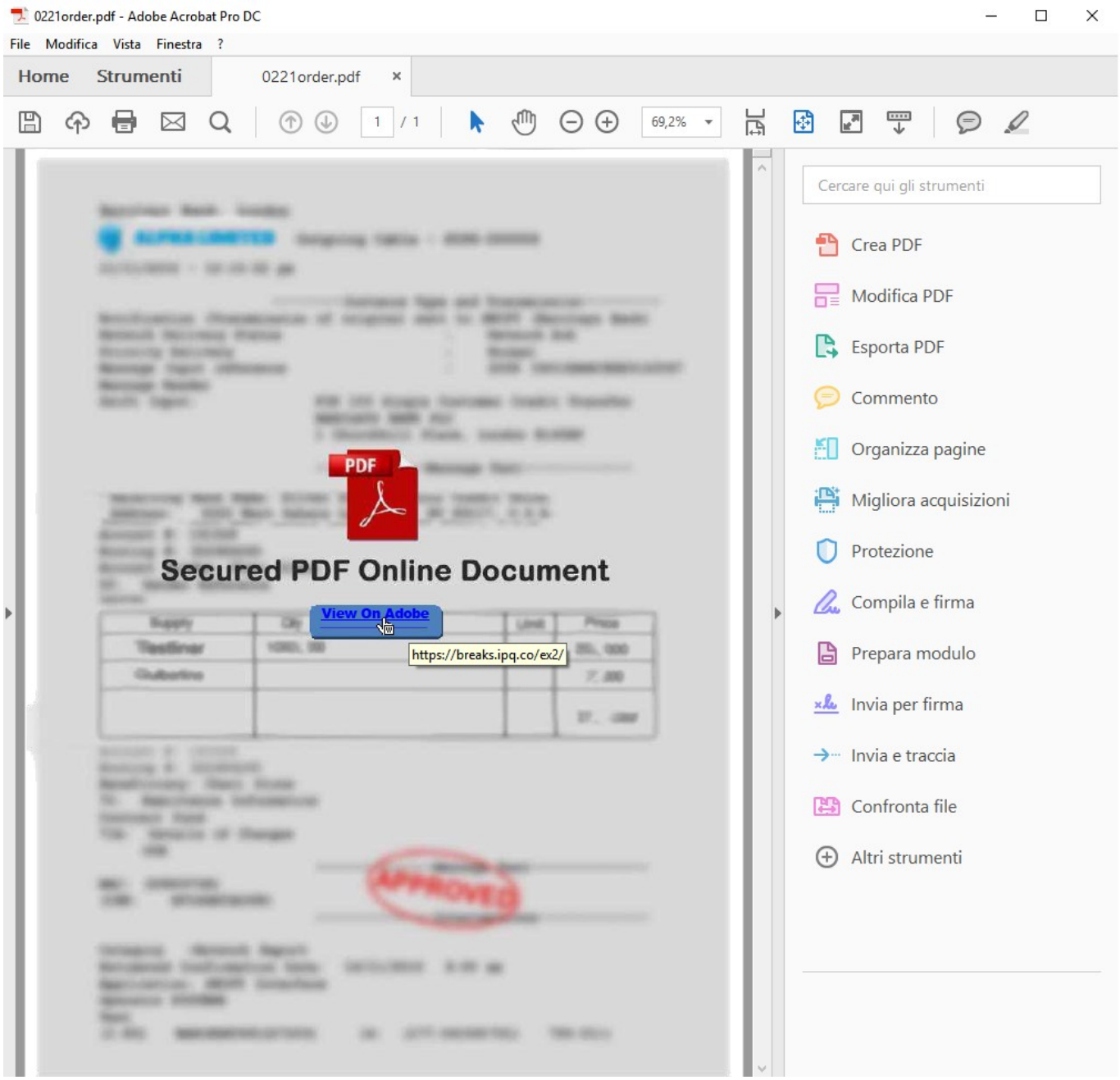
Allo stato dell’arte, questo tipo di attacchi si è palesato anche in Italia.

Di seguito è presentato un semplicissimo esempio (reale) di come può essere utilizzato questo servizio per far sembrale lecito un sito che non lo è.

Il vettore iniziale è la solita **email di phishing** che invita ad aprire un allegato.



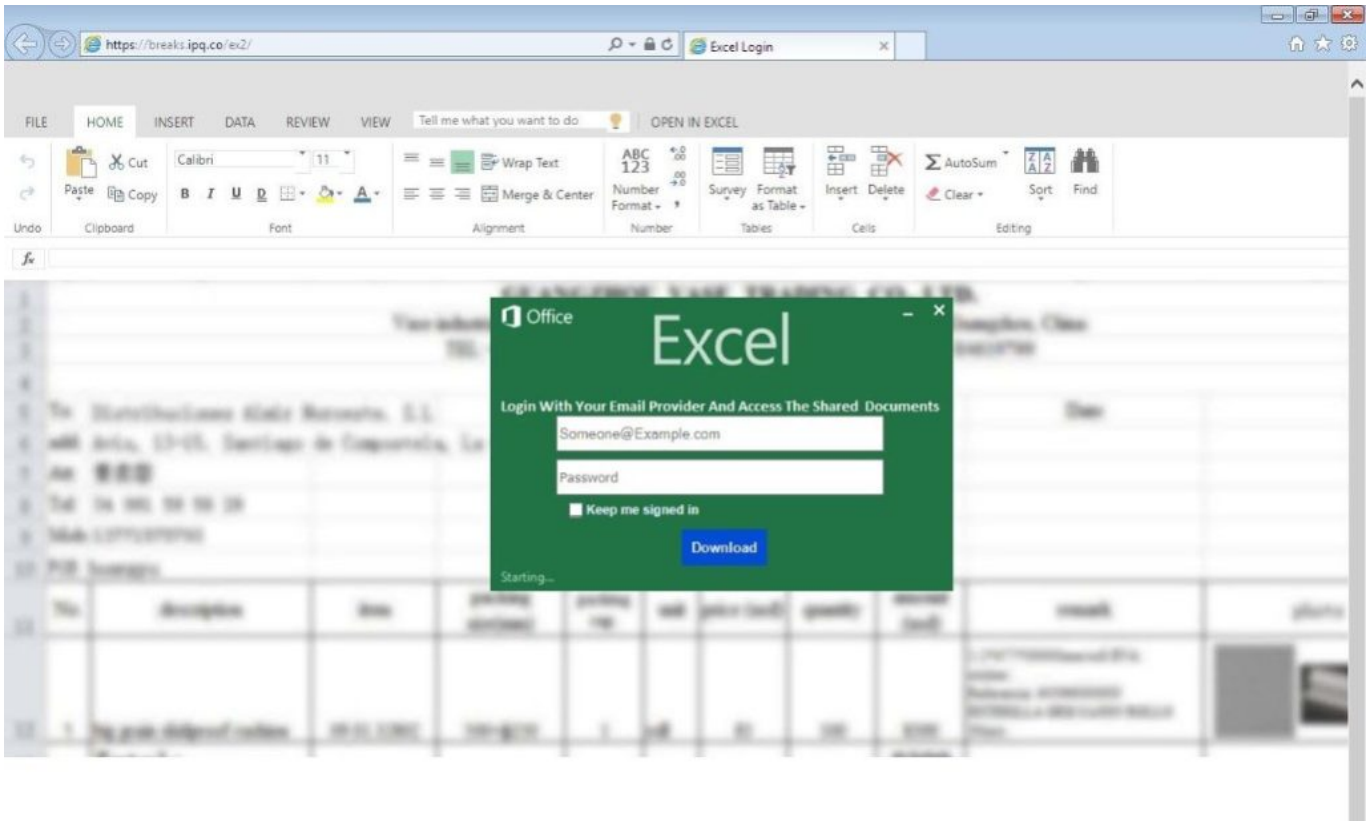
Aprendo l’allegato pdf, non virato, ci troviamo di fronte alla seguente schermata:



Come si può notare, il documento tenta di ingannare l'utente inesperto simulando un documento "secretato", accessibile cliccando su un bottone posto in evidenza al centro della pagina.

Il bottone in questione non è altro che un link che punta al sito https://breaks.ipq.co/ex2/ (oggi bonificato e non più raggiungibile).

Un click su tale link permetterà l'apertura di una pagina internet che invita l'utente ad autenticarsi, in modo da poter "finalmente" effettuare il download del documento secretato inviatoci dal mittente della email:



Ovviamente lo scopo ultimo dell'attaccante è quello di estorcere malevolmente i dati sensibili dell'utente vittima. Infatti, inserendo anche credenziali a caso e cliccando su download, verrà prelevato un documento pubblico relativo ad un'analisi economica americana, totalmente privo di senso per l'utente vittima.

Ad ogni modo, quest'ultimo potrebbe non essersi reso conto di essere stato raggirato, poiché nella sequenza di passaggi effettuata non è stato presentato all'utenza alcun messaggio di allerta.

Questo perché il sito di destinazione è stato certificato dall'attaccante proprio con il servizio messo a disposizione da Let's Encrypt.

DIFFERENZE TRA LET'S ENCRYPT E GLI ALTRI CERTIFICATI SSL

Nonostante gli svantaggi derivanti da un utilizzo fraudolento di Let's Encrypt, è da sottolineare che vi sono ben altri motivi per i quali ogni giorno continuano ad essere venduti, dalle CA commerciali, un gran numero di certificati SSL a pagamento.

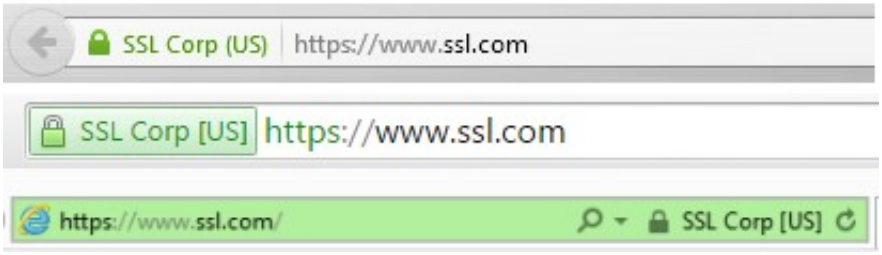
Quello di maggior interesse in termini di sicurezza, riguarda il fatto che Let's Encrypt fornisce solo certificati di tipo Domain Validated (DV); non offre certificati Organizazion Validated (OV) né tantomeno Extended Validated (EV).

Nel dettaglio con il DV di Let's Encrypt è possibile **validare esclusivamente la proprietà del dominio**, ovvero la CA conferma esclusivamente che il dominio è controllato dalla parte che

richiede il certificato, qualunque essa sia (benevola o malevola). Semplificando, chi si connette ad un sito certificato con Let's Encrypt può star certo che il proprietario del dominio ha il pieno controllo su di esso, e che la trasmissione tra host e server è sicura. Quanto detto è chiaramente un ossimoro: basti pensare a tutti i casi di utilizzo fraudolento simili a quello descritto in precedenza.

Viceversa, un certificato di tipo OV[6], contiene al suo interno il nome dell'organizzazione. Ciò permette di garantire un grado di fiducia superiore verso il sito che si sta visitando e l'azienda che esso rappresenta.

In aggiunta il certificato di tipo EV[7], oltre a garantire gli stessi attributi del, mostra il nome dell'organizzazione direttamente nella barra degli indirizzi.



Infine, ulteriori motivi relativi alle modalità di "amministrazione" del dominio, sono i seguenti: Let's Encrypt…

- non offre alcuna garanzia, non c'è quindi alcuna assicurazione di protezione in caso, ad esempio, di data breach o di utilizzo non lecito da parte di terzi del certificato;
- non offre l'opzione Wildcard, quindi non copre i terzi livelli associati al dominio principale;
- in caso di problemi o quesiti, non è possibile ricevere assistenza via call center o altro; gli unici riscontri sono ottenibili unicamente accedendo ai pareri forniti dalla community online;
- scade dopo 90 giorni; occorre quindi attrezzarsi di frequente per rinnovarlo[8].

CONCLUSIONI

Indubbiamente Let's Encrypt è un prodotto estremamente valido, semplice ed utile a chi vuole pubblicare un proprio sito/servizio (anche per motivi ludici) senza dover forzatamente acquistare un certificato SSL (o doversi sorbire i noiosi avvisi presentati in caso di certificati autogenerati). È altresì vero che tale servizio non è adeguato nel caso in cui si voglia mettere in piedi un servizio di e-commerce, o una vetrina relativa ad un progetto importante.

Si potrebbe, nella pratica, affermare che l'obiettivo iniziale dei creatori di Let's Encript ha ottenuto i risultati (in termini di incremento della sicurezza del web) diametralmente opposti a quelli attesi. A conti fatti, gli hacker possono agevolmente mascherare siti fittizi e fraudolenti come portali sicuri.

Proprio per questo motivo si può affermare che i creatori di Let’s Encrypt hanno messo un po’ i bastoni tra le ruote sia agli sviluppatori di browser, sia ai tecnici che negli anni hanno ripetutamente esortato l’utente medio nel controllare che all’interno della barra degli indirizzi fosse presente la dicitura “HTTPS”, prima di “fidarsi” della bontà un sito internet.

Di fatto, ad oggi i controlli posti in essere volti ad arginare la navigazione erronea su siti fraudolenti e a salvaguardare l’utenza inesperta, risultano del tutto inefficaci.

L’unico rimedio, come nella maggior parte dei casi, risulta essere l’**awarness**. Sensibilizzare l’utenza poco esperta è l’unico modo per ovviare al problema.

Le uniche buone pratiche da seguire, per cercare di non incappare in siti malevoli sono, quelle di:

- verificare puntualmente l’indirizzo presente nella barra di navigazione;
- controllare nel dettaglio il tipo di certificato relativo ad un sito ogni qualvolta un sito possa risultarci di dubbia validità:
    - preferendo certificati di tipo OV/EV ai DV;
    - verificando la CA emettitrice dello stesso.

Note

- [1] Rispettivamente versione 56 e 51.
- [2] Quando apriamo un sito internet che usa il protocollo HTTP, un qualsiasi utente malintenzionato potrebbe facilmente leggere o modificare la pagina da noi visualizzata tramite la tecnica del “man in the middle”.
- [3] La spesa di un certificato SSL varia dalle decine alle centinaia di Euro l’anno, in base al tipo di certificato richiesto.
- [4] su un web server su un sistema unix-like sono sufficienti pochi secondi per configurare il supporto ad HTTPS, senza contare la possibilità di impostare job di rinnovo automatici.
- [5] https://www.thesslstore.com/blog/lets-encrypt-phishing/
- [6] https://www.ssl.com/faqs/ssl-ov-validation-requirements/
- [7] https://www.ssl.com/faqs/ssl-ev-validation-requirements/
- [8] problema facilmente risolvibile tramite meccanismi di rinnovo automatico basato su script, o job, auto eseguibili: uno tra tanti consiste nell’utilizzo del servizio **cron** sulle distribuzioni linux. In alteranativa, Let’s Encrypt stesso elenca qui i client compatibili per il rinnovo automatico dei suoi certificati.

Articolo a cura di **Daniele Rigitano**