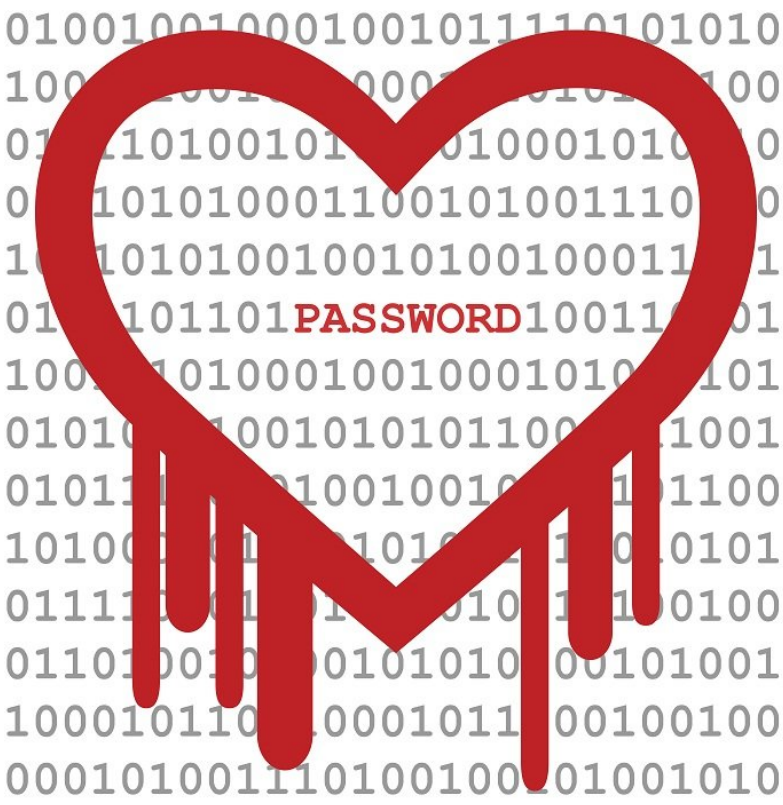
Cure e primi arresti per Heartbleed

Data: Invalid Date | Autore: Luca Tiriolo



E’ stato arrestato uno dei primi hacker ad aver sfruttato il bug Heartbleed, tramite il quale in Canada sono stati rubati i numeri di previdenza sociale di circa 900 contribuenti. Non è stato lui quello che ha creato la falla che ha minato la sicurezza di due terzi del traffico Internet globale, ma ha colto l'occasione per usarlo, anche se non sono resi noti, ancora, i suoi fini.
Secondo quanto riferito dal Wall Street Journal, il ragazzo arrestato dalla polizia canadese avrebbe solo 19 anni e si chiamerebbe Stephen Arthuro Solis-Reyes: si tratterebbe di uno studente modello dell'Ontario e figlio di un docente, guarda caso, di Computer Science della Western University. Le accuse sono utilizzo non autorizzato di computer e uso di dati altrui per scopi illeciti. [MORE]

La prima prova di furti informatici a causa del bug "Heartbleed" è emersa con la scoperta di password e messaggi privati rubati dal sito Mumsnet, il secondo più grande sito web del Regno Unito per i genitori.
Il Canada Revenue Agency ha detto che i cyber criminali hanno rubato i numeri di previdenza sociale di circa 900 contribuenti, utilizzando la vulnerabilità di un software di sicurezza che ha interessato circa i due terzi di tutti i siti web.
A tale scopo la compagnia Codenomicon ha creato il nome Heartbleed, letteralmente sanguinare il cuore, per diffondere la conoscenza del problema: l’origine del nome risiede dal fatto che il bug ha origine nell’estensione heartbeat del protocollo TLS, che è uno dei più usati protocolli crittografici che permettono una comunicazione sicura dal sorgente al destinatario (end-to-end) su reti TCP/IP (come ad esempio Internet) fornendo autenticazione, integrità dei dati e cifratura operando al di sopra del livello di trasporto.

Una versione corretta di OpenSSL è stata rilasciata il 7 Aprile 2014, mentre la notizia della vulnerabilità veniva diffusa. Prima del 7 Aprile, si stima che circa il 17% ovvero mezzo milione di server web sicuri, certificati da autorità fidate, siano stati vulnerabili all'attacco, permettendo il furto delle chiavi private del server, delle password e cookie degli utenti.

Le grandi aziende tecnologiche , tra cui Google e Facebook si sono precipitate a proteggere i loro siti, ma molte piccole imprese e organizzazioni potrebbero essere ancora vulnerabili.
Mumsnet non è un obiettivo dirette, perché non si tratta di informazioni finanziarie o riservate , ma, solo di consigli sull'essere mamma e papà: gli hacker, però, sono a conoscenza del fatto che la maggior parte delle persone spesso utilizza le stesse password per siti anche completamente diversi, da Facebook ad Instagram, dal forum sui genitori a le proprie carte di credito e così gli hacker potrebbe aver ottenuto le informazioni da utilizzare su altri siti .
Heartbleed è una delle più grandi falle mai trovate, perché risiede in un software di sicurezza molto comunemente usato: la notizia peggiore è che questa falla è rimasta aperta da almeno due anni.

Per spiegare in cosa consiste tecnicamente questo bug abbiamo scelto un fumetto creato per l'occasione da Randall Monroe e riportato nelle sue comic strip online http://xkcd.com/1354/