traduzione dell'articolo - in lingua inglese - raggiungibile QUI

Cara NSA, la **privacy** e' un **diritto**, non un *ragionevole* motivo di sospetto.
Apprendere qualcosa su Linux non e' un crimine - ma non ditelo alla NSA!!
Una storia , pubblicata in Germania, e seguita da un articolo in inglese, rivela come l'NSA sta indagando attentamente sulle persone che visitano determinate pagine web, tra i quali Tor Project o Linux Journal. Cio' e' allarmante in molti modi, in maniera particolare perche' l'NSA identifica il lettore con un codice (
fingerprint
), che ricalca molto fedelmente quello che in altri tempi sarebbe stato chiamato un
marchio d'infamia
o una
lettera scarlatta
. E' una grave minaccia alla liberta' d'espressione che sta alla base dei diritti moderni di cui tutti noi godiamo.

Cosa sappiamo

L'articolo, basato su una dettagliata opera di investigazione, rivela il codice di **Xkeyscore** e dimostra come funziona questo metodo di tracciamento. Xkeyscore e' lo strumento con cui l'NSA setaccia una
enorme
mole di dati. Questo codice puo' essere utilizzato in qualunque punto all'interno del processo di collezione e analisi dei dati, in modo da mettere in evidenza certe attivita' dell'utente. Secondo Il Guardian
, il software di controllo pacchetti di Xkeyscore gira su una vasta collezione di siti web sparsi in tutto il mondo, fagocitando qualcosa come 2 bilioni di record al giorno.

Il codice contiene le definizioni usate per determinare se piazzare il *marchio* ('**fingerprint**') su una comunicazione ragionevolmente sospetta. Per esempio l'NSA marchia come sospette le ricerche online su strumenti per la sicurezza tra le comunicazioni (es.: Tails)

Come si vede dal codice:

> This fingerprint identifies users searching for the TAILs (The Amnesic Incognito Live System) software program, viewing documents relating to TAILs, or viewing websites that detail TAILs.

Tails e' un sistema operativo live, che puo' essere eseguito da vari supporti (dvd, usb, schede sd), e permette ad un utente di non lasciar traccia su computer su cui gira. Questo e' particolarmente utile per persone che si trovano a comunicare da computer di cui non si fidano (es: internet cafe'). E' allarmante come cio' possa allarmare l'NSA tanto da schedare gli utento che si interessano a TAILs

Altra notizia sconcertante e' che Xkeyscore etichetti come "*meritevoli di sospetto*" tutti i lettori di **Linux Journal**
- una rivista mensile per tutti gli appassionati di free e open software - come se fossero tutti membro di un forum di estremisti!! E' risaputo che l'unica guerra di religione in corso su Linux Journal e' quella tra i devoti di Vi e Emacs :D

La nostra sicurezza non e' fonte di sospetto

Da quanto abbiamo visto sul codice di Xkeyscore, e' implicita l'idea che sia da considerarsi sospetta qualsiasi l'installazione di - o il semplice informarsi su - strumenti che aiutino l'utente a difendere il proprio diritto alla sicurezza e la privacy dei proprio dati. Evidentemente per l'NSA questo e' Il Problema.
Ma tutti noi desideriamo e abbiamo necessita' di conservare i nostri dati in modo sicuro e celarli sotto il diritto alla privacy, cosi' come non puo' essere considerato "sospetto" montare tende alle finestre e chiudere a chiave la porta di casa, vi pare? Dunque non e' ammissibile che dotarsi di certi strumenti di protezione, o il semplice informarsi a riguardo, possa qualificarvi come merivetoli di essere sospettati e scrutinati in quello che fate.

Anche la **FISA** (U.S. Foreign Intelligence Surveillance Court) riconosce questo diritto e proibisce qualsiasi attivita' di indagine basata solo sulla libera espressione (il famoso primo emendamento della Costituzione U.S.A.). Che l'NSA necessiti o meno dell'autorizzazione della FISA per spiare comunicazioni oltreconfine, lo spionaggio condotto dall'NSA costitusce un problema. La costituzione USA protegge i proprii cittadini anche al di fuori dei confini nazionali, e tale protezione si estende anche ai non cittadini USA (PDF)

In piu', il **diritto** alla privacy e' stato ufficialmente riconosciuto dagli USA con la sigla del documento **International Covenant on Civil and Political Rights** . Xkeyscore dimostra ampiamente quanto sia ingiusta l'azione della NSA.

Tor e' utilizzato per eludere la censura su internet

Xkeyscore sembra puntualizzare molto sul progetto Tor e i software di anonimato. Tor e' uno strumento essenziale per eludere quella censura su internet, che governi come la cina e iran adottano per controllare la fuoriuscita di informazioni e mantenere una certa leva di potere sulla popolazione. Tor su sviluppato con l'aviuto della U.S. Navy, e correntemente acquisisce fondi da varie fonti governative americane (u.s.a.). Il segretario di stato Hilary Clinton supporta gli strumenti anti-censura come elemento chiave della sua politica a proprosito di intenert: "**The freedom to connect is like the freedom of assembly in cyberspace**
."
(la liberta' di connettersi e' l'equivalente, nello spazio virtuale, della liberta' di riunione)

Puoi ancora usare Tor e Tails

Visto l'operato della NSA, ci si potrebbe chiedere se, per evitare il Marchio e mantenere l'anonimato, non sia il caso di unon utilizzare Tor e Tails. Ecco quanto: se utilizzate Tor e Tails c'e' la possibilita' di essere scrutinati dalla NSA, ma noi crediamo che i benefici superino i disagi. Infatti, piu' persone utilizzano Tor, piu' sicure esse sono. Il frequente utilizzo di questi strumenti di protezione e' la nostra migliore speranza per proteggere persone che davvero necessitano di protezione. **Piu' persone comuni utilizzano Tor e Tails, piu' arduo e' il compito della NSA nel dire che l'utilizzo di questi strumenti sia "sospetto"**