18/01/2011 - Social network senza difese

Da Milano - Nella recente edizione del **ToorCon**, una convention di e per hacker dedicata alla sicurezza informatica svoltasi a San Diego, c'è stato un interessante intervento di Eric Butler. Eric ha infatti dimostrato concretamente come grazie a un hijacking via Wi-Fi un attaccante sia in grado di prendere il controllo della sessione di un utente dopo che questi abbia effettuato il login o si sia autenticato su un server, fino ad arrivare a conoscere la sua password. Eric in particolare si è concentrato sulle sessioni generate dai principali siti "social" del momento tra cui Facebook e Twitter, risultati tutti vulnerabili all'attacco. Non a caso quindi il talk aveva il provocatorio titolo "Hey Web 2.0: Start protecting user privacy instead of pretending to" (Hey Web 2.0: inizia a proteggere davvero la privacy dell'utente invece di far finta).Vediamo come è possibile che ciò accada.

La falla

Il cuore del problema è costituito, come spesso accade, dalla concomitanza di diversi aspetti che impattano sulla sicurezza. Il primo di questi fattori è costituito da una rete wireless non protetta, attraverso cui la vittima decide di collegarsi a internet e da lì (secondo fattore) decide di accedere a uno dei social network vulnerabili. Essi infatti non applicano una protezione sulle comunicazioni successive all'autenticazione, prestando il fianco quindi a possibili attacchi.

Per rendersi conto di cosa stiamo parlando non è necessario essere

particolarmente abili, perché grazie a un plugin per **Firefox chiamato Firesheep** (open-source e disponibile per Windows, Linux e MacOSX) abbiamo sostanzialmente armato già il nostro browser a intercettare dati che non dovrebbero esserci resi disponibili, ma che al contrario sono trasmessi in chiaro.

Firesheep agisce in pratica da sniffer, dato che è in grado di intercettare i cookie dell'utente vittima che si trovi nello stesso network wireless cui è collegato l'attaccante, rendendo disponibili tutte le connessioni Http e Https associate. Il vero problema infatti è che la falla persiste anche con le connessioni Https, perché solo il login è cifrato mentre il resto della comunicazione resta non criptata.

Simulazione di attacco

Per fare un test abbiamo bisogno di poche cose:
- una rete Wi-Fi nella quale fare i test
- Winpcap (winpcap.org)
- Firesheep (Http://github.com/downloads/codebutler/firesheep/firesheep-0.1-1.xpi)

e ovviamente Firefox.

Prima di tutto installiamo Winpcap. Poi installiamo Firesheep e dopo aver riavviato Firefox possiamo avviarlo dal menu View -> Sidebar -> Firesheep (tasti scorciatoia SHIFT+CTRL+S).
Clicchiamo nella parte bassa sul pulsante delle preferenze e nel primo foglio del menu che ci si apre, impostiamo la scheda di rete Wi-Fi da utilizzare in modalità promiscua.

CED s.r.l. - Cod.Fisc., *P.IVA, n.iscrizione Reg.Imprese CCIAA Venezia: 03529610275 - R.E.A.:* 316199
Sede Legale: *via Po, 3 - frazione Mellaredo - 30030 Pianiga (Venezia) - Tel.041.868.5150 - Fax 041.964.1109*
Sede Operativa: *via Ruffilli, 2 - 65016 Montesilvano Spiaggia (Pescara) - Tel.085.868.1020 - Fax 085.868.1029*
http://www.ced.it/ - E-Mail: amministrazione@ced.it

Il pulsante in basso permette di selezionare la scheda di rete Wi-Fi da utilizzare per lo sniffing.

Colleghiamoci alla rete Wi-Fi e poi clicchiamo sul pulsante "Start capturing" aspettando che i dati comincino ad arrivare.

Selezionata la scheda Wi-Fi e connessi alla rete di test siamo pronti per partire con l'intercettazione dei cookie.

CED s.r.l. *- Cod.Fisc., P.IVA, n.iscrizione Reg.Imprese CCIAA Venezia: 03529610275 - R.E.A.: 316199*
Sede Legale: *via Po, 3 - frazione Mellaredo - 30030 Pianiga (Venezia) - Tel.041.868.5150 - Fax 041.964.1109*
Sede Operativa: *via Ruffilli, 2 - 65016 Montesilvano Spiaggia (Pescara) - Tel.085.868.1020 - Fax 085.868.1029*
http://www.ced.it/ - E-Mail: amministrazione@ced.it

Dopo un po' avremo i dati di sessioni pre-autenticate: cliccandoci sopra saranno aperte direttamente nel nostro browser. Immaginiamo quindi cosa può succedere in un aeroporto o internet caffè...

Contromisure

Il protocollo Https non può essere la soluzione del problema e nei casi menzionati ci si deve rivolgere necessariamente a servizi VPN quando si accede a dati sensibili tramite rete di accesso pubblico Wi-Fi. Cercando su google si possono trovare diversi servizi gratuiti e anche a pagamento.

Se vogliamo risolvere in economia, è possibile installare un proprio server SSH, anche su Windows tramite Cygwin e utilizzare un client SSH come Putty per accedervi, mentre il browser può essere configurato per utilizzare la connessione socket del proxy e da lì accedere al sito web desiderato.

Ecco un esempio di come si presenta il pannello di Firesheep dopo che ha intercettato diversi cookie, tra cui Google, Facebook, Twitter e Flickr e si è aperto il link verso Facebook.

Parlando poi dell'accesso Wi-Fi, è chiaro che vanno prese delle minime precauzioni anche da chi ne gestisce l'accesso: se anche si stabilisce che il servizio deve poter essere libero per tutti i fruitori, è bene comunque aggiungere una password di connessione per gli utenti autorizzati. L'ideale sarebbe poi che fosse utilizzata una protezione più forte, come WPA2.

CED s.r.l. *- Cod.Fisc., P.IVA, n.iscrizione Reg.Imprese CCIAA Venezia: 03529610275 - R.E.A.: 316199*
Sede Legale: *via Po, 3 - frazione Mellaredo - 30030 Pianiga (Venezia) - Tel.041.868.5150 - Fax 041.964.1109*
Sede Operativa: *via Ruffilli, 2 - 65016 Montesilvano Spiaggia (Pescara) - Tel.085.868.1020 - Fax 085.868.1029*
http://www.ced.it/ - E-Mail: amministrazione@ced.it

Lato client, per gli utenti di Firefox è già disponibile un plugin che sembra possa rappresentare una possibile risposta al pericolo di essere "dirottati" da attaccanti dotati di Firesheep: si chiama Force-TLS (Http://forcetls.sidstamm.com) e forza il client ad accettare solo connessioni sicure verso i server cui ci stiamo collegando. E' disponibile anche una modalità debug che ci permette di visualizzare tutte le comunicazioni che intercorrono durante l'autenticazione e le successive transazioni. Per abilitarla è sufficiente seguire questi step:

1. apriamo about:config
2. impostiamo la preferenza extensions.forcetls@sid.stamm.debug al valore "true"
3. riavviamo Firefox

Ho scritto "sembra" dato che alcuni utilizzatori hanno rilevato comunque dei problemi.
Un'altra possibile soluzione potrebbe essere rappresentata da HTTPS Everywhere (https://www.eff.org/https-everywhere) che però è tuttora in beta e non offre ancora garanzie certe nei confronti di Firesheep.

Nell'attesa che sia quindi ufficializzata una adeguata contromisura all'hijacking possibile con Firesheep è bene evitare di connettersi a social network da posti di accesso pubblico Wi-Fi.

In generale la rete cui ci connettiamo va comunque considerata insicura e dopo Firesheep sono comparsi altri tool realizzati al solo scopo di ricordarcelo, come Idiocy (https://github.com/Jonty/Idiocy/blob/master/idiocy.py) che in neanche 130 linee in Python realizza il dirottamento di un account Twitter scrivendo un twit al posto nostro.

CED s.r.l. - Cod.Fisc., *P.IVA, n.iscrizione Reg.Imprese CCIAA Venezia: 03529610275 - R.E.A.:* 316199
Sede Legale: *via Po, 3 - frazione Mellaredo - 30030 Pianiga (Venezia) - Tel.041.868.5150 - Fax 041.964.1109*
Sede Operativa: *via Ruffilli, 2 - 65016 Montesilvano Spiaggia (Pescara) - Tel.085.868.1020 - Fax 085.868.1029*
http://www.ced.it/ - E-Mail: amministrazione@ced.it