# L'insicurezza del Web: dai Trojan alle frodi online

Sommario:
Il grande successo dell'utilizzo di Internet per le transazioni economiche ha portato all'interesse di gruppi criminali dediti a furti e truffe. Sfruttando principalmente le vulnerabilità degli applicativi ed il basso livello di sicurezza intrinseca di Internet, tramite codice maligno installato sui PC o SmartPhone degli utenti finali, è possibile realizzare frodi e furti quasi senza essere individuati.

Negli ultimi anni, Internet ed in particolare l'interfaccia web alla comunicazione, è diventato uno strumento ormai indispensabile nella vita di tutti i giorni. Internet non è solo utilizzato per piacere, informazione o mantenere i contatti con amici, conoscenti e colleghi, ma è diventato forse la piattaforma più pervasiva utilizzata negli scambi commerciali. Acquisti grandi e piccoli, ricerche, contrattazioni, gestione dei patrimoni e del proprio conto in banca, dallo stipendio alla rata del mutuo ed al pagamento delle bollette, vengono effettuati online. Negli ultimi anni l'aumento del valore economico delle transazioni online effettuate dal cliente finale è stato enorme.
Inevitabilmente l'interesse di malfattori alle transazioni online è aumentato di pari passo e nell'arco degli ultimi 10 anni siamo passati da attacchi informatici fatti per lo più per '*divertimento*' o '*disturbo*' e per questo molto evidenti, ad organizzazioni criminali di tipo mafioso che cercano il più possibile di agire in incognito e di non essere individuati.
Anche il mito degli attacchi stranieri provenienti da paesi dell'est o estremo oriente è parzialmente da sfatare. Se è vero che le più grandi organizzazioni criminali che agiscono in Internet sono dei paesi dell'est o estremo oriente, è anche vero che la maggior parte delle frodi online effettuate in Italia è fatta da Italiani che nel caso utilizzano strumenti sviluppati principalmente all'estero.

Ci si potrebbe aspettare che le frodi oggi siano perpetrate tramite o i messaggi di posta elettronica di finte vincite alle lotterie e di eredità più o meno convincenti, oppure tramite attacchi diretti ai server di istituti finanziari ed aziende. Se è vero che un attacco ad un server ad esempio di un istituto finanziario potrebbe procurare un bottino molto ingente con una unica azione, è anche vero che questi servizi sono gestiti da professionisti è che non è facile né effettuare la frode né riuscire a non lasciare tracce. E' molto più semplice invece attaccare l'anello più debole della catena, ovvero il

cliente finale, in modo quasi totalmente invisibile.

## La frode all'utilizzatore finale

Descriviamo brevemente le principali caratteristiche di una frode online fatta direttamente all'utilizzatore finale tramite gli strumenti più recenti raccontando un fittizio ma possibile evento.

1. Il toolkit

Un Italiano decide di perpetrare una frode in Internet ai danni di clienti di un Istituto di Credito di cui conosce abbastanza bene il sistema di Internet Banking. Per questo acquista online uno dei toolkit disponibile, da Zeus,[1] forse il più famoso e diffuso, a SpyEye,[2] più recente e per alcuni aspetti più innovativo, ed altri quali Phoenix, Darkness, BlackEnergy, Eleonore. I costi di un toolkit vanno da 500 USD sino a 20.000USD per le versioni con gli add-on più costosi. Nuove versioni dei toolkit sono prodotte tipicamente con cadenza settimanale principalmente per evitare l'identificazione da parte degli anti-virus.

2. Lo sviluppo

Il frodatore sviluppa una versione del Trojan specializzata per la frode che intende compiere. Le principali e più comuni caratteristiche di questi Trojan sono:

a) sfruttando vulnerabilità dei sistemi, si installano a livello amministrativo ed hanno accesso a tutti i dati e funzionalità del sistema
b) hanno molteplici procedure di re-installazione in caso di cancellazione da parte ad esempio di un anti-virus, sono modulari e varie funzionalità sono attivabili da remoto
c) sono in grado di intercettare sia quanto visualizzato sullo schermo che quanto digitato dall'utente (key-logger) che i dati in transito verso Internet (in modo non cifrato) oltre ovviamente a tutti i dati presenti sulle memorie di massa di qualunque tipo
d) sono in grado, tramite modifiche delle librerie di sistema, di modificare i dati inviati o ricevuti dai browser internet
e) inviano ad un centro di Comando e Controllo (C&C) i dati intercettati, possono installare nuove componenti o aggiornamenti e (dis-) attivare funzionalità su richiesta del C&C
f) permettono l'esecuzione di sessioni in terminale remoto come amministratore del sistema o utente del sistema da parte del frodatore tramite una interfaccia web sul C&C.

3. La diffusione

Una volta preparato il Trojan, il frodatore deve caricarlo su un C&C (servizio tipicamente a pagamento) e contattare una organizzazione quale ad esempio AV-profit,[3] che si occupi (sempre a pagamento) della diffusione del Trojan alle vittime. La diffusione avviene oggi principalmente in due modi:

a) tramite l'invio di email che convincono l'utente a connettersi tramite URL fraudolente a siti web che inviano al browser l'Installer del Trojan e poi ridirigono l'utente al vero sito web: in questo modo l'utente non nota nulla di particolare, se non al più un rallentamento nel caricamento del vero sito web
b) inserendo ad esempio con tecniche di XSS/SQL-Injection, il richiamo all'Installer del Trojan direttamente in siti web molto famosi e ritenuti generalmente sicuri (si noti che anche siti di Microsoft, Google ecc. sono stati brevemente utilizzati a questo scopo[4]).

Il secondo è al momento il metodo preferito e che fornisce i migliori risultati per la diffusione dei Trojan.

Si noti che la diffusione del Trojan è generica e non mirata, la maggior parte di coloro sui cui PC o SamrtPhone[5] è installato il Trojan non sono clienti del sistema di Internet Banking per cui è stato sviluppato e pertanto non subiscono direttamente danni. Il frodatore però può sempre rivendere l'utilizzo del proprio Trojan ad altri a cui può interessare per altri scopi, dall'invio di email di Spam, ad attacchi di Denial of Service al carpire per poi rivendere numeri di carte di credito o credenziali di accesso a siti di interesse.

4. La truffa

Il truffatore riceve costantemente dal Trojan informazioni sulle attività dei PC o SmartPhone su cui è installato. Quando viene segnalato al frodatore che un particolare utente ha a disposizione una ingente somma sul proprio conto corrente, avendo già intercettato le credenziali di accesso al sistema di Internet Banking, questi si collega al sistema di Internet Banking ed effettua un trasferimento economico a proprio favore. Si noti che la transazione può essere effettuata anche direttamente dal PC dell'utente mentre questi è connesso al sistema di Internet Banking, utilizzando la funzionalità di sessione remota del Trojan. In caso di utilizzo di credenziali di tipo OTP (One Time Password) tipicamente generate da chiavette hardware in possesso del cliente, il frodatore configura il Trojan ad intercettare in tempo reale ad esempio un bonifico effettuato dall'utente e cambiarne cifra e destinatario in modo che all'utente venga sempre mostrata la cifra ed il destinatario che ha inserito, mentre al sistema di Internet Banking dell'Istituto di Credito vengano mostrati i dati inseriti dal frodatore.

## Possibili difese

E' chiaro che l'aggiornamento dei sistemi operativi e degli applicativi è il primo livello di difesa in quanto l'Installer sfrutta vulnerabilità (note e no) per poter installare il Trojan. Un anti-virus aggiornato è anche utile ma generalmente non garantisce di individuare questi tipi di Trojan. Infatti le più recenti statistiche indicano che la probabilità che un qualunque anti-virus identifichi questi Trojan è solamente del 30%. Questo è dovuto sia al fatto che vi sono moltissime versione di ogni Trojan ed anche al fatto che è difficile individuarle in quanto questi Trojan sono veramente poco visibili ed anzi vi sono stati casi in cui la presenza del Trojan migliorava le prestazione del PC in quanto spesso essi rimuovono altri virus che potrebbero interferire con le proprie attività o rendere sospetto l'utente.

Questi Trojan sono facilmente individuabili via rete, in quanto si connettono una o due volte al minuto ai C&C, e questo tipo di traffico è ad esempio facilmente individuabile da un sistema di Intrusion Detection (IDS/IPS). Ovviamente, se gli utenti aziendali possono sperare di avere qualche protezione da parte dei sistemi di sicurezza dell'azienda, gli utenti privati non hanno questa possibilità ne ce l'hanno gli utenti aziendali quando utilizzano il proprio PC portatile o SmartPhone al di fuori della rete aziendale.

In ogni caso, una volta accertato che sul proprio PC o SmartPhone è installato uno di questi Trojan, l'unico suggerimento che oggi si può dare è quello di re-installare completamente il sistema operativo e tutti gli applicativi.

A livello applicativo le difese adottabili sul PC o SmartPhone dell'utente sono anch'esse limitate. Visto che il frodatore ha completo accesso a tutte le risorse del PC o SmartPhone dell'utente in tempo reale e tramite una sessione di terminale remoto, c'è poco che possa essere fatto per limitarne l'attività. Ad esempio l'utilizzo di credenziali di accesso di tipo OTP su hardware indipendente, come già indicato, rendono la frode più difficile tecnicamente e quindi anche con minor successo, ma non la rendono impossibile. Si noti che è ormai da sconsigliare l'invio di codici tramite il canale telefonico, ad esempio SMS, questo sia perché vi sono Trojan per SmartPhone che intercettano questi SMS e li inviano ai C&C, sia perché gli SmartPhone più avanzati sono ormai dei piccoli PC e gli utenti accedono ai servizi di Internet Banking dalla stessa piattaforma sulla quale arriva anche il messaggio con il codice, rendendolo pertanto disponibile direttamente anche al truffatore.

D'altra parte il fornitore del servizio web può adottare tecniche e procedure che rendono la frode più complicata e costosa da implementare, e quindi meno redditizia, scoraggiando pertanto il frodatore. Inoltre usuali procedure anti-frode a livello di business, permettono nella maggior parte dei casi di

individuare la frode e bloccarla prima che il trasferimento di denaro sia completato.
Infatti se il successo nell'installazione del Trojan è notevole, in alcuni casi non altrettanto notevole è il successo delle frodi. Le ragioni sono molteplici:

- spesso vi sono errori nel codice per cui il Trojan non intercetta i dati che dovrebbe, o altre funzionalità non funzionano come dovrebbero incluso il fatto che l'Installer fallisce l'installazione o il Trojan è stato in alcuni casi facilmente individuabile o disattivabile
- la grande maggioranza di utenti sul cui PC o SmartPhone è installato il Trojan non sono clienti del sistema di Internet Banking a cui è indirizzata la frode o non hanno le disponibilità economiche per essere oggetto della frode
- i sistemi anti-frode e le indagini della polizia[6] riescono spesso ad individuare le frodi ed i frodatori, a bloccarle o tracciarle quanto basta per renderle non così redditizie per i frodatori.

## Conclusioni

Ove vi sono grandi numeri di transazioni economiche ed ingenti quantità di denaro, è inevitabile che vi siano anche tentativi di frodi e furti. Internet è una nuova piattaforma di comunicazione e scambi commerciali ed economici. Il suo enorme successo ha portato di pari passo allo sviluppo di organizzazioni criminali dedite a frodi e furti. Oggi l'anello più debole è l'utente finale il cui PC o SmartPhone può essere utilizzato direttamente (tramite un Trojan) da un malvivente per effettuare un furto o una frode. Difendere l'utente finale è molto difficile dato che non gli si può chiedere di diventare un esperto in sicurezza informatica. Le principali azioni da intraprendere sono il miglioramento della sicurezza e qualità del codice, l'aggiornamento automatico delle applicazioni e l'adattamento delle tradizionali procedure anti-frode implementate dalle aziende per adeguarsi alle nuove tecnologie.

Andrea Pasquinucci (PhD CISA CISSP) è un consulente freelance in sicurezza informatica. Si occupa prevalentemente di progetti di sicurezza ICT, audit, compliance, governance e formazione ICT per il management ed il personale tecnico. In particolare è esperto di sicurezza delle reti e dei servizi web, dei sistemi operativi e di crittografia.

1 https://zeustracker.abuse.ch/

2 https://zeustracker.abuse.ch/

3 http://voices.washingtonpost.com/securityfix/2009/06/web_fraud_20_franchising_cyber.html, http://krebsonsecurity.com/2010/03/avprofit-rogue-av-zeus/

4 http://www.theregister.co.uk/2010/12/13/doubleclick_msn_malware_attacks/

5 http://www.businesscomputingworld.co.uk/new-zeus-malware-attacks-smartphone-and-linkedin-users/

6 http://www.scmagazineus.com/fbi-announces-arrest-of-five-zeus-orchestrators/article/180213/