Scenari di attacchi all'online banking

Che tipo di attacco?

- Del denaro viene trasferito al di fuori della disponibilità della vittima…
- …senza che la vittima ne sia consapevole
- Trasmettere ai sistemi informativi della banca una richiesta che appare legittimamente formulata dall'utente, ma non lo è

Come impersonare l'utente?

- Impossessandosi delle sue credenziali d'accesso

- Impossessandosi delle credenziali che il suo computer usa per comunicare con i sistemi della banca dopo che l'accesso è stato effettuato (*session riding, session hijacking)*

Il Phishing

- Inviare all'utente una comunicazione (ad es. tramite la posta elettronica) che sembri provenire dalla banca
- La comunicazione richiede un'azione da parte dell'utente
- L'azione si svolge selezionando un link, che però non porta al sito della banca

Il Phishing

- Il sito di destinazione assomiglia a quello della banca e chiede di fornire delle informazioni riservate (le credenziali d'accesso, gli estremi di una carta di credito…)

- *"Vishing"* e *"Smishing"*

Alcuni rimedi

- Autenticazione out-of-band (ad es. SMS)
- Credenziali che scadono, o che comunque non possono essere riutilizzate
  - One-time passwords, su carta o con token

Man-in-the-middle

- Un malintenzionato intercetta le comunicazioni che l'utente vorrebbe svolgere con la banca, e le modifica prima di presentarle al destinatario

- Spesso svolto agendo sul servizio DNS (*pharming*)

- SSL potrebbe essere d'aiuto a patto che sia implementato correttamente (e che lo sia la PKI!)

Malware

- Software dannoso, perlopiù installato senza la consapevolezza dell'utente
- Veicolato spacciandolo per altro tipo di software
- Veicolato tramite le vulnerabilità dei sistemi operativi, dei browser o degli altri programmi usati per fruire delle informazioni reperite su Internet

Malware

- Varia per modalità di installazione (*drive-by download*, phishing, vulnerabilità…) e compiti svolti

- Il malware più importante in questo caso è generalmente catalogato come *Trojan horse*

Keyloggers

- Registrano i tasti premuti dall'utente, e possibilmente anche altre azioni
- Possono rivelarle tramite vari canali
- Usati per impossessarsi delle credenziali di accesso e di altri dati sensibili
- Versione più sofisticata: *form grabbers*

Sistemi batch

- L'uso di malware permette di attaccare sistemi che dispongono transazioni bancarie in modalità batch, senza l'intervento dell'utente

Man-in-the-Browser

- Malware capace di intervenire sul comportamento del browser
- Invia delle informazioni che non corrispondono necessariamente a quelle immesse dall'utente
- Mostra all'utente informazioni che non corrispondono necessariamente a quelle comunicate dal server

Man-in-the-Browser: esempio

- L'utente chiede alla banca di disporre un bonifico di 400 euro ad un professionista
- Il browser invia alla banca la richiesta di un bonifico di 5.000 euro verso un intermediario
- La banca risponde con una pagina che chiede di confermare il bonifico di 5.000 euro
- Il browser visualizza la richiesta di confermare il bonifico di 400 euro

Man-in-the-browser

- Locale: le informazioni da modificare sono già note al malware, che provvede in modo autonomo
- Remoto: appena l'utente accede al servizio di online banking, l'attacco è pilotato dall'esterno
- MitMo: agisce sui dispositivi mobili

Alcuni altri rimedi

- Risk-based authentication
  - Autorizzare le transazioni anche in base al comportamento passato dell'utente
- Transaction signatures
  - Un dispositivo esterno richiede i dati della transazione (ad es. importo, destinatario) e fornisce un codice di autorizzazione