Attacco alle WebMail basate su Memova:

tampering dei parametri di inoltro automatico

Rosario Valotta

Matteo Carli

Indice

Overview

Attraverso le vulnerabilità di seguito descritte un attacker può modificare le configurazioni delle caselle di posta elettronica delle vittime, impostando l'inoltro automatico di tutte le mail in arrivo verso un account e-mail da egli controllato.
In tal modo è possibile violare la riservatezza delle comunicazioni delle vittime senza ricorrere ai comuni metodi di identity stealing (cookie stealing, credential stealing) attualmente sfruttati dai malware circolanti sul web, ma semplicemente inviando una particolare e-mail alle vittime.

La pericolosità di questa tecnica è resa critica grazie a tre fattori:

1. semplicità di exploiting (cross-browser)
2. scarsa awareness della vittima (nessuna interazione richiesta)
3. diffusione sul web (ampia diffusione della piattaforma Memova e possibilità di propagazione virale)

Segue un flow chart che riassume un ipotetico utilizzo delle vulnerabilità scoperte.
Riassumendo per passi:

1. L'attaccante invia una e-mail preparata ad arte alla casella e-mail della vittima
2. La vittima legge l'e-mail e inconsapevolmente imposta l'inoltro automatico di tutte le e-mail in ingresso
3. Conoscenti, colleghi ed amici della vittima scrivono e-mail alla vittima stessa
4. Tutte le e-mail in ingresso nella casella della vittima vengono inoltrate all'attaccante in maniera trasparente.

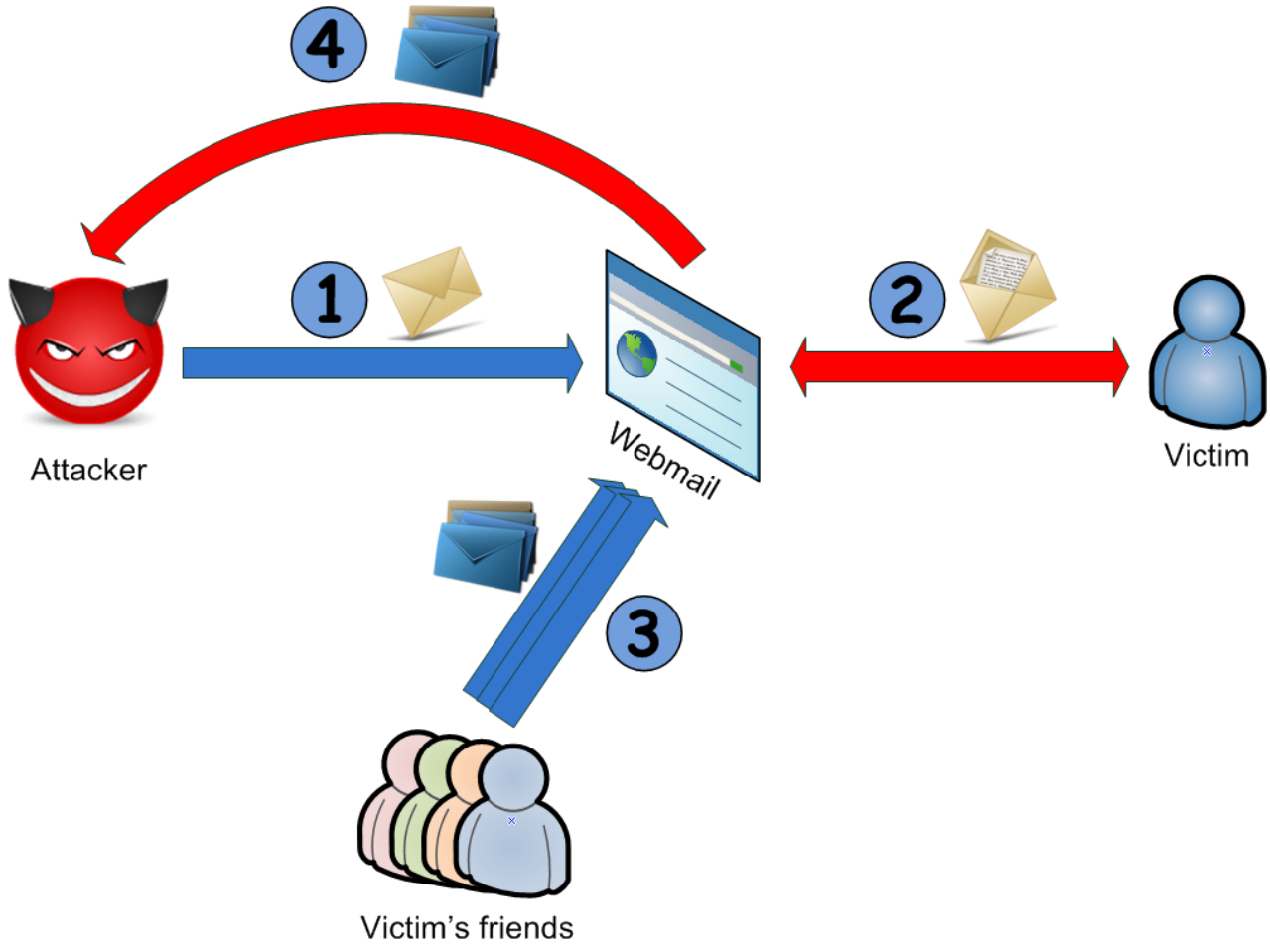

Figura 1 - Esempio possibile utilizzo delle vulnerabilità

Exploit della vulnerabilità

L'attacker deve semplicemente inviare una mail costruita ad-hoc alla vittima; è sufficiente che la vittima si limiti ad aprire la mail (nessuna ulteriore interazione richiesta) perché la modifica delle impostazioni di inoltro automatico vengano modificate in modo totalmente trasparente.

Awareness delle vittime

L'impostazione dell'inoltro automatico è solitamente disponibile all'utente sotto le voci "Impostazioni" o "Opzioni" della WebMail. Questa opzioni non viene tuttavia consultata e modificata di frequente (tipicamente una sola volta, durante il setup della WebMail), per cui un'eventuale modifica silente di queste configurazioni passerebbe verosimilmente inosservata per parecchio tempo.
In alcune web mail, interessate dalle vulnerabilità, non viene neppure concessa all'utente finale la possibilità di impostare l'inoltro automatico tramite il menù delle opzioni; in tale scenario è praticamente impossibile per la vittima disabilitare le opzioni di inoltro senza il supporto dell'assistenza tecnica dell'ISP.
La possibilità, da parte dell'attaccante, di impostare il parametro di inoltro è completamente indipendentemente dalla disponibilità di questa opzione nel menù della WebMail.

Diffusione sul Web

Le WebMail interessate dalle vulnerabilità sono quelle basate sul framework di messaggistica "Memova" sviluppato da Critical Path (http://www.criticalpath.net). Si tratta di una soluzione per la gestione della posta elettronica enormemente diffusa sul web: uno snapshot dei principali clienti è disponibile alla url http://www.criticalpath.net/About/Customers.html.

Giusto per riportarne qualcuno:

- Tiscali IT/UK/NL
- Wind
- Telecom
- Vodafone
- Swisscom
- Telefonica
- Virgin
- Sonera
- Terra.es
- Telia
- T-Mobile
- FastwebNet
- Ono
- Regione Puglia
- Regione Sicilia
- Diversi domini gov.uk

Si tratta di ISP diffusi **worldwide** con una enorme base di utenti, ciascuno dei quali ha sul proprio portale un servizio di WebMail basato sulla piattaforma Memova.
Ovviamente su ciascuna installazione, la soluzione Memova è stata opportunamente personalizzata, sia nel look&feel che nelle funzionalità per venire incontro alle necessità del cliente, ma le caratteristiche di base sono comuni e, purtroppo, **comuni sono anche le vulnerabilità**.
E' per questo motivo che un attacker con una sola mail può "spiare" le comunicazioni di milioni di account esattamente come se fosse in Cc (Copia Carbone) su ciascuno dei messaggi inoltrati.
Per avere un'idea delle installazioni "live" di questo prodotto, vi invitiamo ad effettuare una semplice ricerca sul Web:

http://www.google.it/search?hl=it&q=inurl%3Acp%2Fps%2FMail&btnG=Cerca&meta=

dove "cp/ps/Mail" è un prefisso comune alle installazioni di Critical Path Memova.

Da un'analisi effettuata dai dati disponibili sul web (referenze Critical Path e informazioni sulla base dati degli ISP) il bacino di **account worldwide vulnerabili a questo attacco si aggira intorno ai 40 milioni di account e-mail.**

Proof of Concept

Per il Proof of Concept delle vulnerabilità sono state analizzate le tre più popolari WebMail italiane (almeno in termini di account registrati) che tra l'altro fanno uso tutte e tre del framework Memova:

- Tiscali
- Libero (Wind)
- Virgilio (Telecom)

Tramite l'invio di una mail contenente un unico vettore di attacco (una stringa testuale in grado di "sfuggire" ai controlli di sicurezza delle WebMail), è possibile infettare gli account di tutte e tre le WebMail, impostando le opzioni di inoltro automatico verso un account di posta elettronica controllato dalla vittima.
Sulla base di una scelta "etica" e per rispetto nei confronti di tutte le parti coinvolte (la privacy degli utenti da una parte, il rispetto del lavoro di professionisti dall'altra) il codice sorgente e le specifiche tecniche alla base del PoC non verranno divulgate. Lo scopo del PoC è unicamente quello di documentare le vulnerabilità esistenti e di informare Critical Path del lacunoso stato di sicurezza del prodotto, che rischia di compromettere la privacy di milioni di utenti nel mondo (il prodotto è largamente usato anche fuori dall'Italia).

Elementi di base

L'attacco si basa sull'utilizzo incrociato di due differenti vulnerabilità presenti sulle WebMail delle vittime:

- Cross site scripting – XSS
- Cross site request forgery – CSRF

Per un approfondimento delle tematiche legate a queste due vulnerabilità rimando alle numerose fonti disponibili sul web; in sintesi l'XSS (Cross-site Scripting) è legato alla possibilità, per un attacker, di veicolare del codice JavaScript "malicous" verso una vittima sfruttando un errore di validazione di una applicazione web. Il CSRF (Cross-Site Request Forgery) è invece legato alla possibilità, per un attacker, di generare delle richieste "nascoste" alla vittima, ma riconoscibili come autentiche dall'applicazione Web.

Fase 1 – invio della mail

Per l'invio della mail l'attacker ha la necessità di creare un testo ad-hoc in modo da sfruttare le vulnerabilità presente sui filtri di validazione dell'input presenti nelle WebMail coinvolte.
Il vettore riportato sopra è studiato ad hoc per evadere i filtri anti XSS di tutte le WebMail testate, sia nella loro vecchia versione, sia nella loro nuova versione 2.0 (basata su tecnologia Ajax).
Nonostante il PoC sia stato testato solo sulle 3 WebMail sopra descritte, è verosimile attendersi che anche nelle installazioni presso altri clienti, il software di filtering di Memova sia vulnerabile a questo XSS.

Fase 2 – lettura della mail

All'apertura della mail, il vettore inviato viene posizionato nel codice HTML di un iframe preposto alla visualizzazione del testo di ciascuna e-mail.
Il codice del vettore richiama un file JavaScript ospitato su un server Web in possesso all'attaccante che viene eseguito nel contesto dell'iframe (es: mioisp.it)
In alcune delle implementazioni testate esiste un meccanismo di "protezione" per limitare i danni provocati da XSS abbinati a CSRF: il dominio dell'iframe in cui viene letta la mail (e quindi eseguito il JavaScript) è differente dal dominio della WebMail (es. mail.mioisp.it).

Questo meccanismo, sfruttando i vincoli nativi del browser (Same Origin Policy) impedisce di fatto:

1. di recuperare il token di sessione (necessario per ogni tipo operazione sull'applicazione) presente nella document.location della WebMail
2. di effettuare richieste XmlHttp verso il dominio della WebMail

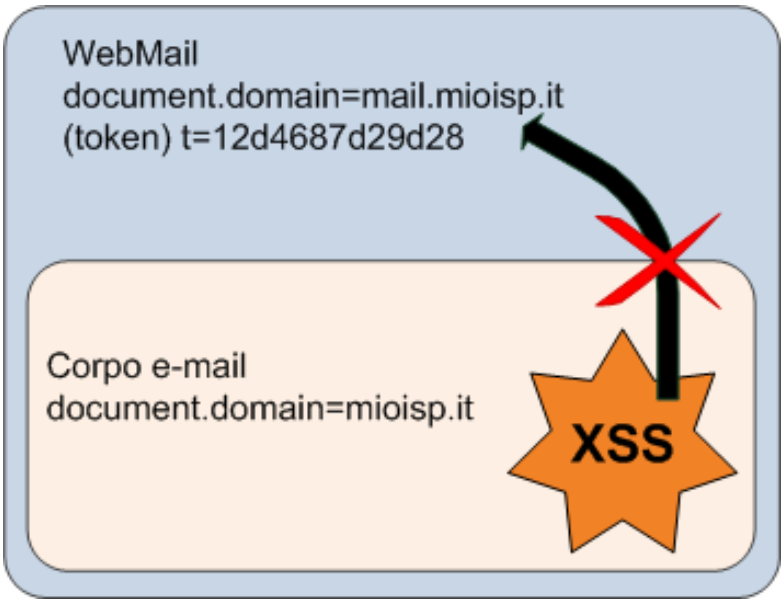

Figura 2: La Same Origin Policy blocca l'accesso di uno script al di fuori del suo dominio di esecuzione

Esiste tuttavia un meccanismo per aggirare queste limitazioni:

1. occorre individuare un secondo XSS sullo stesso dominio della WebMail (es. mail.mioisp.it) e senza la presenza del token di sessione (che non abbiamo ancora a disposizione)
2. tale XSS (di tipo reflected) viene richiamato come source di un iframe creato all'interno del frame di lettura della mail
3. il Reflected XSS può avere accesso alla document.location della WebMail (steso dominio), riuscendo così a recuperare il token di sessione
4. Il reflected XSS può a sua volta lanciare attacchi CSRF verso pagine del dominio "mail.mioisp.it" riuscendo così a modificare i settagli dell'inoltro automatico

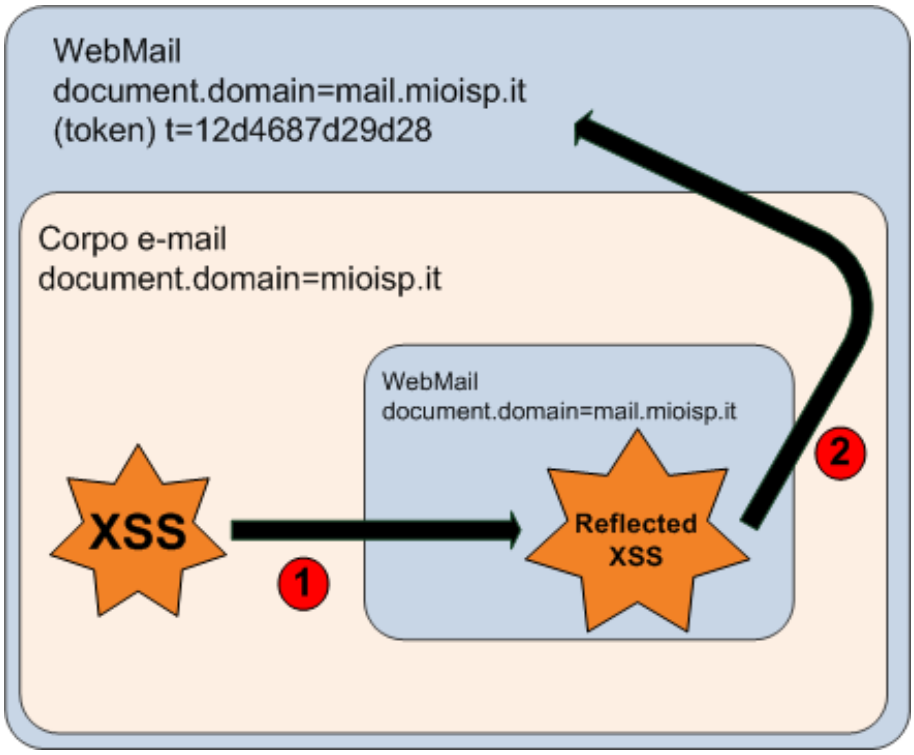

Figura 3 - Il Reflected XSS riesce ad aggirare i meccanismi di protezione della WebMail

Step 3 – Modifica delle impostazioni di inoltro automatico

Svincolato dalle restrizioni della Same Origin Policy, ed in possesso del token di sessione il codice del reflected XSS può effettuare chiamate XmlHttp verso qualunque risorsa presente sul dominio "mail.mioisp.it".
In particolare la URL da chiamare per impostare il forward automatico delle mail in arrivo è:

- POST /cp/ps/Mail/preferences/SetForward?

Questa pagina è sempre disponibile sulle installazioni testate di Memova, anche in quelle in cui l'opzione di inoltro automatico non è disponibile per gli utenti finali della WebMail.
In questi casi un attacco come quello descritto è praticamente invisibile e non disabilitabile senza il supporto tecnico del fornitore di servizi.

Scenario alternativo

In un ottica teorica, ma praticamente realizzabile e funzionante, potrebbe essere creato un "worm" che sfruttando le vulnerabilità riportate sia in grado di **autoreplicarsi** leggendo la rubrica o i mittenti e-mail presenti nella "inbox" della vittima. In questo modo si creerebbe un effetto a catena che comprometterebbe milioni di caselle e-mail interessate dal problema.
In più avendo il controllo completo della casella e-mail della vittima sarebbe possibile inviare e-mail a nome della vittima stessa (con gli header smtp orginali), come se fossero state effettivamente inviate dalla vittima.

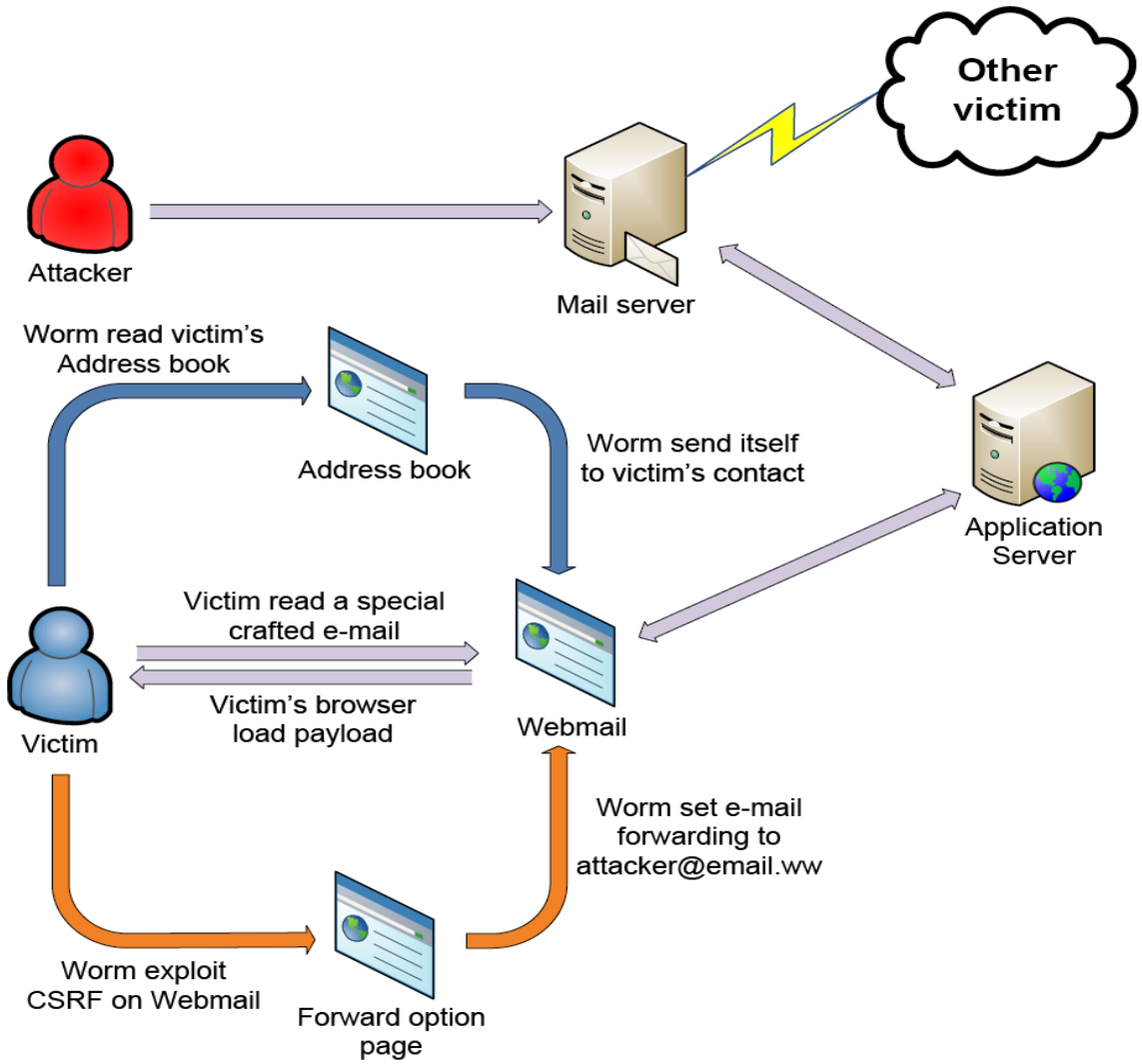

Figura 4 – Flusso di propagazione del worm