McDonald's Wi-Fi Login System by BT Italia S.p.A.

Multiple Vulnerabilities Report

Sommario

Introduzione

Il caso McDonald's, è un classico caso di cattiva programmazione e gestione della sicurezza delle reti.

Analizzando il portale di login per gli ospiti del sistema Wi-Fi abbiamo identificato un errore, relativamente banale, nel processo di generazione dell'autenticazione a doppio fattore dell'account utente. In pratica era possibile registrare account fittizi saltando il passaggio obbligatorio di verifica dell'identità a mezzo della ricezione di un sms sul cellulare; tramite una analisi del traffico dati siamo stati inoltre in grado di recuperare i dati necessari all'automatismo della registrazione tramite bot.

Questa vulnerabilità permetteva pertanto di utilizzare la rete del McDonald's come scudo e proxy per poter non solo navigare anonimamente in rete ma anche per portare attacchi ad altri sistemi in totale sicurezza.

Inoltre sulla rete pubblica abbiamo identificato la presenza di alcuni servizi di back-end quali una vpn privata, il sistema di gestione wi-fi e il POS (gestione pagamenti bancomat e carte di credito).

Lista delle Vulnerabilità

- XSS non persistente
- Captcha bypass
- Login bypass
- McDonald's VPN login bruteforce

Descrizione delle vulnerabilità

Le vulnerabilità riscontrate ad eccezione dell'attacco alla VPN sono presenti in tutti i McDonald's d'Italia con sistemi Wi-Fi pubblici

XSS

Cross-site scripting non persistente su alcuni parametri degli URL del sistema di login Wi-Fi per gli ospiti, permettendo di inserire ed eseguire codice lato client al fine di attuare un insieme variegato di attacchi quali ad esempio:

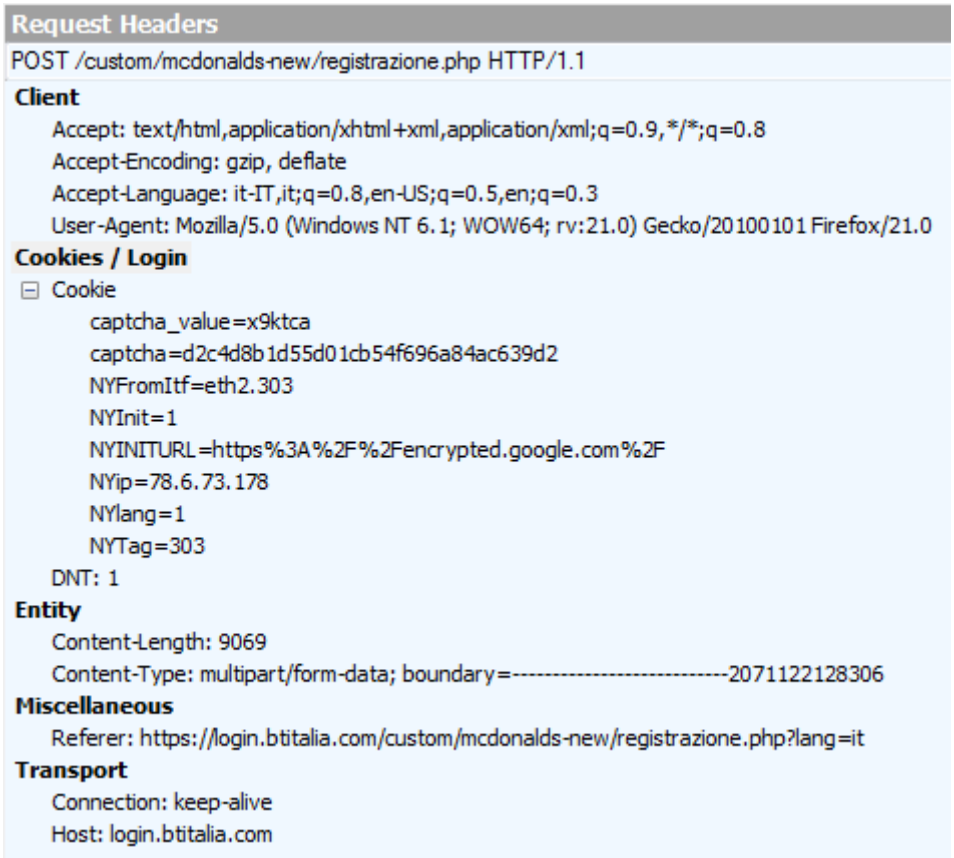
- Raccolta, manipolazione e reindirizzamento d'informazioni riservate
- Visualizzazione e modifica di dati presenti sui server
- Alterazione del comportamento dinamico delle pagine web

Nell'ultimo caso è possibile iniettare codice HTML attuando un "deface" non persistente dell'home page, un redirect o a un tentativo di phishing.

Captcha

Osservando le richieste lato client e le risposte date dal server si nota che la soluzione del captcha viene passata in chiaro al client tramite i cookie, rendendo inutile un intervento manuale; qualsiasi bot o software automatizzato è in grado di recuperare il valore dal cookie e successivamente registrare con successo innumerevoli account.

In dettaglio, tra i cookie dell'URL (registrazione.php) è presente un campo captcha_value con un valore alfanumerico corrispondente alla soluzione dell'immagine mostrata nella pagina della registrazione.



Login

La seguente vulnerabilità è da considerarsi la più importante poiché permette a un qualsiasi utente non identificato di registrarsi con dati fittizi e in seguito utilizzare il collegamento Wi-Fi per navigare in modo anonimo in rete e/o utilizzare l'hotspot come proxy per attaccare altre infrastrutture.

In seguito alla registrazione ogni utente utilizzatore del servizio è identificato dai dati anagrafici inseriti e dal numero di telefono cellulare utilizzato. Normalmente anche se un malintenzionato inserisse dati anagrafici fittizi, la tracciabilità sarebbe garantita dal numero di cellulare fornito; come mostrato in seguito, la password di autenticazione inviata per sms al telefono è erroneamente generata dal client, rendendo impossibile l'identificazione dell'utilizzatore nel caso si usi un numero di cellulare falso.

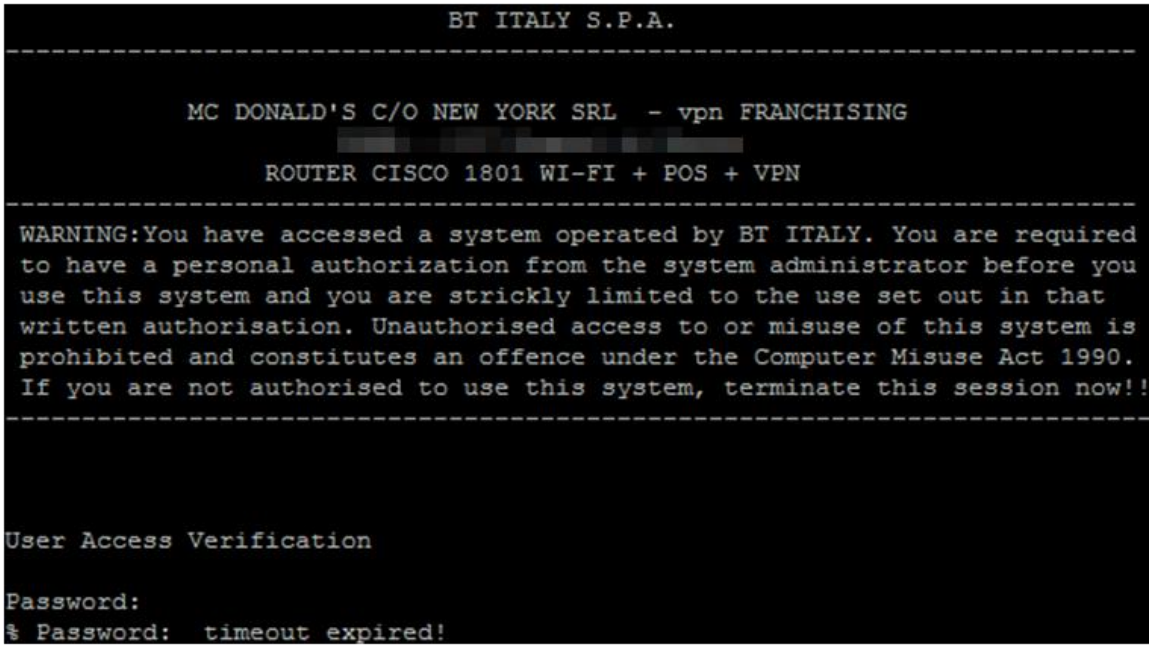
Analisi di un POST DATA fittizio:

Chiave	Valore
captcha	x9ktca
Consenso1	NO
Consenso2	NO
Consenso3	NO
email	mail@gmail.com
FirstName	Nome
Info1	YES
lang	1
Language	it
LastName	Cognome
operazione	
password	1Cccc11c
PhoneNumber1	3333333333
PrefixPhoneNumber1	+39
textarea	Art. 13 D.Lgs. n. 196 del 30 giugno 2003.
username	MCD_003_Utente
x	63
y	14

Da cui si ricavano username e password, rispettivamente *MCD_003_Utente* e *1Cccc11c*.

VPN

Sulla rete accessibile agli ospiti abbiamo rilevato, grazie a quello che crediamo essere una configurazione non corretta, un host che permetteva l'accesso alla VPN interna, al Wi-Fi e al POS.



La nostra etica ci ha impedito di "forzare" il sistema di login, è però importante segnalare come con un attacco bruteforce sia possibile tentare di superare questa protezione.

Fix

XSS

Validare e filtrare ulteriormente i parametri in input che l'utente può manipolare.

Il metodo più sicuro per un programmatore, è quello di usare una delle funzioni che permettono l'escape dei caratteri html inserite in una stringa. Dette funzioni sono: htmlspecialchars(), htmlentities(), strip_tags.

Captcha

Non restituire mai il valore in chiaro del capctha. Solitamente per ogni immagine è presente l'hash del suo valore nel database in modo da poter ricevere in input il valore dell'utente, eseguirne l'hash e successivamente confrontarlo con quello memorizzato nel database per l'autenticazione.

Login

Generare la password e l'username, per autenticare un ospite sulla rete, solo lato server e inviare il tutto al numero di telefono acquisito in input in modo da poter così rendere tracciabile e identificabile l'utente.

VPN

Ammesso che la tipologia di rete lo permetta, inserire l'host con accesso alla VPN in una sottorete non accessibile dagli ospiti di McDonald's.

Conclusioni:

Data l'architettura di rete che abbiamo "incontrato", compromettere il servizio di back-end avrebbe comportato l'accesso al gateway principale d'interscambio dei dati sulla rete, pertanto, sicuramente sarebbe stato possibile rubare i dati di navigazione degli ospiti del McDonald's e i dati in transito sulla VPN.

Data la presenza in rete del sistema di pagamento tramite POS si potrebbe pensare di attaccare questo servizio al fine di rubare del denaro; per fare delle valutazioni sarebbe necessario conoscere la struttura della rete, riteniamo comunque l'attacco poco probabile data la struttura stessa dei POS. Sottolineiamo che negli ultimi tempi si stanno sviluppando malware per attaccare queste strutture. Precisiamo che la nostra etica ci ha impedito di violare e di conseguenza, di portare attacchi diretti a questo sistema.

Quantificando il rischio dell'azienda, sarebbe stato possibile rubare i dati di navigazione, potenzialmente recuperare i dati di registrazione degli ospiti, redirigire il traffico web su un altro sistema ed eventualmente compromettere i computer dei visitatori e i dispositivi di rete.

Il contatto con McDonald's è stato più facile del previsto, non avendo a disposizione nessun contatto di un reparto tecnico competente, abbiamo semplicemente notificato il desiderio di riportare una vulnerabilità, siamo stati (tempestivamente) ricontattati da un operatore, molto disponibile al dialogo, con cui abbiamo instaurato una collaborazione.

Informazioni Generali

Reporter	VoidSec Security Team
Autori	Paolo Stagno, Luca Poletti
Contatto	08-08-13
Risposta del Vendor	09-08-13
Ultima risposta del Vendor	29-08-13 *
Data di disclosure pubblica	24-11-13

*Il Vendor è diventato inattivo dopo questa data non rispondendo ai due successivi contatti.

Common Vulnerability Scoring System 2.0 (CVSS)

Parametro	Punteggio
CVSS Base Score	3.3
CVSS Temporal Score	3.3
CVSS Environmental Score	3.3
Overall CVSS Score	**3.3**

Full CVSS v2 VECTOR:

(AV:A/AC:L/AU:N/C:N/I:N/A:P/E:H/RL:U/RC:C/CDP:N/TD:H/CR:M/IR:L/AR:M)

Informazioni aggiuntive:

Guida CVSS v2

NIST Calculator

Contatti

VoidSec Security Team | security@voidsec.com | http://voidsec.com | Vulnerability Disclosure Policy