La giungla del Web

Quando pensi di essere al sicuro

Hello World

Alexandru Gherasim

- Sistemistica
- Linux
- Sicurezza Informatica
- Web Design

[Campo d’interesse]

1. **[Azione possibile]**

   [cosa accade]

- [cause]
- [cause]

[soluzione]

[soluzione]

Browser

Browser

1. **Accesso al PC**

   Trapelano informazioni

   Bypass delle contromisure dei browser

- Flash Player
- Java Drive-by (ora pure firmati - vedasi Realtek)
- Vulnerabilità del browser

Aggiornare il Browser

Flash e Java su “Chiedi per attivare”

Browser

2. **HSTS Bypass** [HTTP Strict Transport Security]
   Attacco MITM [Man-in-the-middle attack]
   Traffico in chiaro (“sslstrip”)

- Hardware di Rete
- Disattenzione al “lucchetto”

Firefox + HTTPSeverywhere (pro-privacy)
Chrome/Chromium integrato (Super Cookies -> meno privacy)

Browser

Open Source browser

Puoi sapere cosa e come viene eseguito sul PC

Aggiornamenti di performance e sicurezza frequenti

Supporto da parte di grosse ed attive comunita

Suggerisco *Firefox* (della Mozilla, un’azienda molto conosciuta in termini di privacy e sicurezza dei propri utenti)

o *Chromium* (versione completamente opensource di *Chrome*)

Cookie

Cosa sono i Cookie?

Una stringa testuale alfanumerica

- ➔ Sessione di Login
- ➔ Carrello della spesa
- ➔ Dati del volo aereo
- ➔ Ultima visita
- ➔ Siti visitati
- ➔ ID

Cookie

1. **Tracciamento (Social Network)**
   Tracciamento dei siti visitati (widget&pulsanti)
   Pubblicità mirate (ID)

- Volontà dei Social Network
- Widget
- Flash Cookie

Navigazione Anonima/Privata
Disconnect Plugin
Ghostery Plugin

Cookie

2. **Furto di Cookie**
   Possesso di account

- Nessuna verifica lato server
- (In)Sicurezza della Web App

HTTPSeverywhere Plugin(HTTPS://)

Cookie

3. **Compagnie Aeree**
   Prezzo aumentato ogni tot visite

- Profitti

Tab/Finestra Anonima/Privata

Cookie

4. **Spionaggio da privati (ex: Hacking Team)**
   Profilizzazione

- Cookie
- IP
- User Agent
- Ricerce Google

Combinare più soluzioni (Plugins,OpenVPN-NL)

Sistemi Operativi

Sistemi Operativi

Windows, Mac OS, Linux

- Remoto
- Locale
- Da chiavette
- Da cellulare
- ∞ metodi

è importante

Tempistività nel fixing

OpenSource

Reti

Reti

1. **Controllo totale della rete**
   MITM
   Controllo del traffico (richieste, risposte)
   ….incluse quelle dei Browser

- Vulnerabilità dei dispositivi di Routing
- Malconfigurazioni di rete

Modelli/Marche di router (o dispostivi) **NON** di nicchia

… altrimenti supporto ridotto o inesistente -> bug e vulnerabilità non patchate

ATM

ATM

1. **Clonazione**
    Copia della carta in formato digitale
    Acquisti e CashOut
- Skimmer
- Numpad
- IP-cam
- “USB-inside”

Occhio!

Skimmer


OTHER ATMs AVAILABLE AT
High Street Sliema Branch
St Julians Branch
OTHER ATMs AVAILABLE AT

Numpad

Webcam


STATEMENT
NCR
September 30, 2008, and be
TWO HYBRID CARS
OR ONE LUXURY HYBRID!

..a mali estremi

Skimmer

Barnaby Jack

Studiò il software e l’hardware di differenti ATM, alla ricerca di vulnerabilità, che trovo e ne mostro la loro efficacia durante una conferenza di Sicurezza Informatica (Blackhat USA 2010)

Perchè preoccuparsene?

La giungla

- Vendere
- Vendere
- Vendere
- Vendere
- Vendere
- Vendere
- $$$
- ~~€€€~~
- ….

La giungla

- Furto di Account Social (Facebook, Twitter, Instagram,ecc..)
  - Distribuzione di Malware
- Proxy Hijacker
  - MITM (file, sessioni, credenziali)
- Inviare CV a random
  - Creazione di documenti
  - Furto d’Identità (aka impersonificazione)
- Mail in chiaro
  - Spam
  - Phishing

La giungla

Contenuto digitale di un Bancomat:

Traccia #1 (+ Traccia #2 + Traccia #3)

B4888603170607238^Mario/Rossi^05051010000000000120319180519100000

Numero di conto, Nome, Cognome, scadenza e CVV

La giungla

Scrivere la stringa (tracce 1-2-3)

- CashOut senza PIN (in molti paesi)
- Acquisti online

Bye Bye

@ShinobiWPS http://shinobi.one