

Izpoved "white hat" hekerja: Kako sem dobil tisto dragoceno datoteko z vašega računalnika

Luka Treiber
Varnostni analitik
Acros d.o.o.
owasper@gmail.com

OWASP
27.01.2010

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>

Agenda

- Zakaj nas spletni brskalnik vara?
 - ▶ Zakaj ravno mi?
 - ▶ Varnostne napake
- Kako, kje in s čim?
 - ▶ Naše dobrine(dragocenosti)
 - ▶ Demo (primer zlorabe varnostne napake v brskalniku)
- Kako ga bomo spametovali?
 - ▶ Protiukrepi

Vaš brskalnik ima napako/je ranljiv, pa kaj?

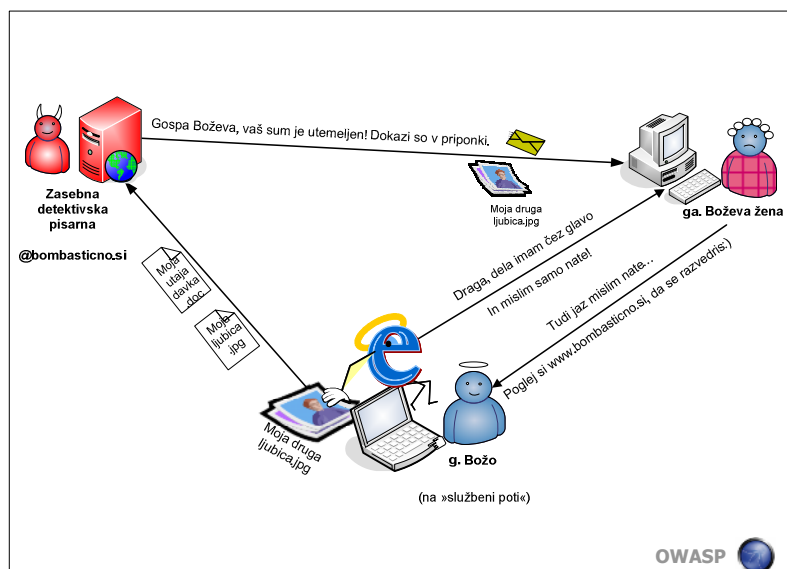
Mislimo, da smo varni, ker

- ni verjetno, da bi obiskali podtaknjeno stran
- ne vejo kje iskati
- ni dostopa do notranjega omrežja
- ne morejo pisati
- ni česa ukrasti
- ni prepričljivega scenarija

Kaj lahko izgubimo?

- IP naslov našega računalnika (123.123.123.123)
- seznam nameščenih windows posodobitev
- seznam nameščene programske opreme
- ...
- katero koli datoteko!?

Kdo koga vara?



Znane lokacije sočnih informacij

- mape brskalnikovega medpomnilnika
- datoteke z zgodovino
- Indexing Service, Help Indexing
- Poročila in dnevniki o napakah
 - ▶ Sistemski dnevnik
 - ▶ Dr Watson (C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dmp)
- Kontakti, sporočila in nastavitve IM odjemalcev
- Kontakti, sporočila in nastavitve E-Poštnih odjemalcev

Kako brskalnik/skripta ve, kje iskati?

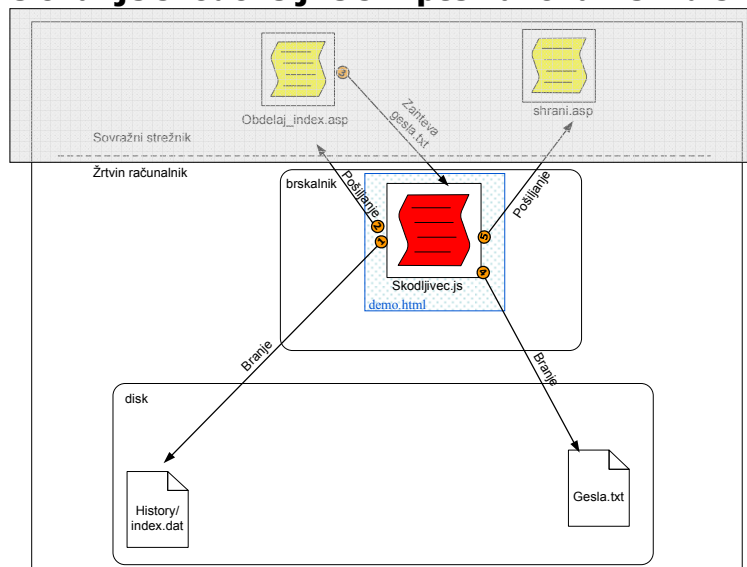
- **Temporary Internet Files**
 - ▶ XP:
 - C:\Documents and Settings\Username\Local Settings\Temporary Internet Files\Content.IE5\index.dat
 - ▶ Vista
 - C:\Users\Username\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
- **History**
 - ▶ XP:
 - C:\Documents and Settings\Username\Local Settings\History\History.ie5\index.dat
 - ▶ Vista
 - C:\Users\acros\AppData\Local\Microsoft\Windows\History\History.IE5
- **Indexing Service**
 - ▶ XP
 - C:\System Volume Information\catalog.wci\propstor.bk2
 - ▶ Vista
 - C:\ProgramData\Microsoft\Search
- **Drugo**
 - ▶ System Restore Point (C:\System Volume Information_restore~1)
 - ▶ Help Indexing (userprofile/.../help/hh.dat)
 - ▶ Office Recent (index.dat)
 - ▶ C:\WINDOWS\Debug\NetSetup.LOG (username, domain, workstation, domaincontroller)
 - ▶ C:\WINDOWS\Prefetch\Layout.ini (username, random folder names, recent links)
 - ▶ C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dmp

Demo

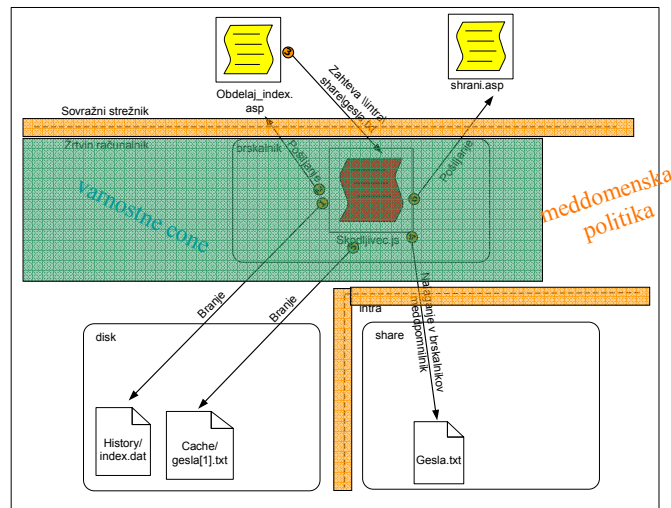
Pokazali bomo, da lahko sovražna koda, ki se izvaja lokalno znotraj spletnega brskalnika:

- bere datoteke z diska na katerem se izvaja
- bere datoteke, ki pripadajo drugi domeni (s pomočjo brskalnikovega medpomnjenja-cachiranja)
- nakaže pošiljanje datoteke na spletni strežnik (napadalec)

Delovanje škodoželjne skripte na lokalnem disku



Delovanje škodoželjne skripte izven lokalnega diska



Protiukrepi

Kaj je Božev greh?

Rešitve:

- ne-Administrator
 - UAC?
- protected mode/InPrivate Browsing?
- vklop "ne shranjuj kriptiranih strani"
- brisanje zgodovine
- SmartScreen Filter?
- ...

Nadaljnji razvoj tehnik branja in medpomnjenja

Alternative XMLHttpRequest (XHR) branju

- iframe tag
- object tag
- tdc
- ...

=> skrivno izvajanje zahtevkov v imenu žrtve
(Cross-Site Request Forgery)

CSRF+lokalni dostop+medpomnilnik=**intranet**

■ zasebna škoda

- ▶ osebni dokumenti
- ▶ skrivnosti, gesla, sporočila, računi, fotografije, navade/početje

■ poslovna škoda

- ▶ spletne bančne storitve
- ▶ telefonske storitve
- ▶ poslovna in privatna pošta
- ▶ notranje omrežje
- ▶ sistemske nastavitve
- ▶ topologija omrežja, programi, posodobitve, register, kriptografski ključi)
- ▶ poslovne skrivnosti, ponudbe, poročila, načrti
- ▶ podatki o strankah, knjigovodski podatki



Reference

- <http://www.coresecurity.com/content/ie-security-zone-bypass>
- [http://msdn.microsoft.com/en-us/library/ms537183\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms537183(VS.85).aspx)