KASPERSKY lab

Anatomy of Duqu exploit

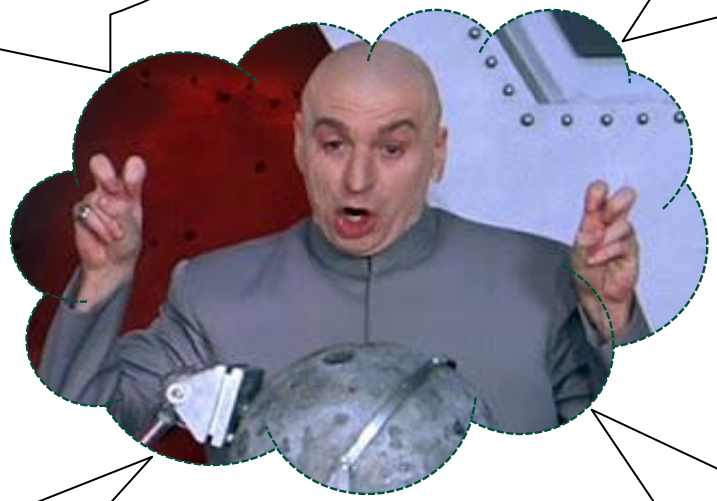
Ivan Teblin, Head of Hosted & Streaming Technologies Research

Virus Bulletin, Dallas, 05 October 2012

OpenType: evil opportunities

Complex format
8 - 30 cross-referenced sub-tables!

Rendering VM
> 120 instructions!

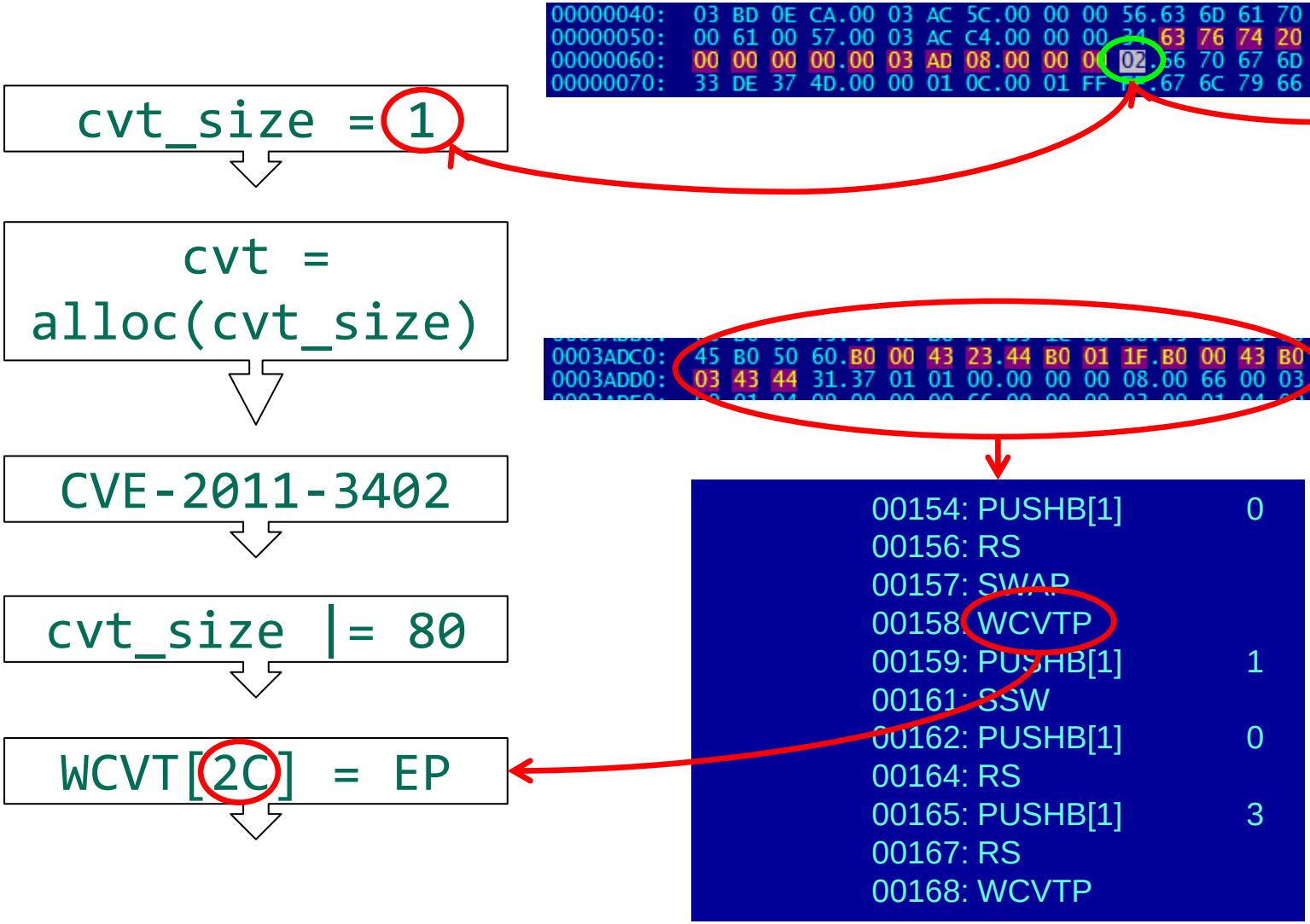


'Sbit' bitmaps
9 + 3 sub-formats!

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

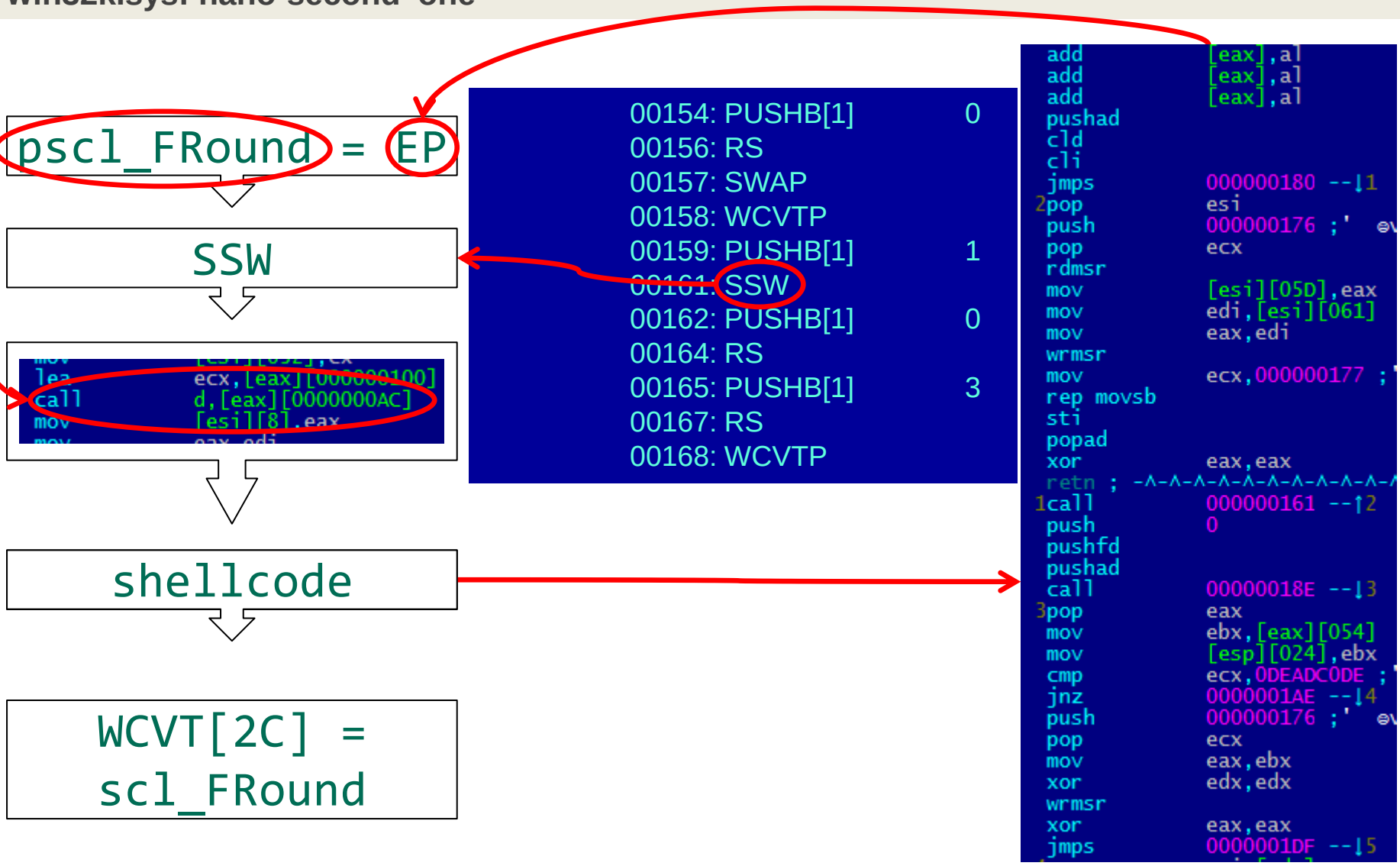
Duqu exploit

win32k.sys: nano-second 'zero'



Duqu exploit

win32k.sys: nano-second 'one'

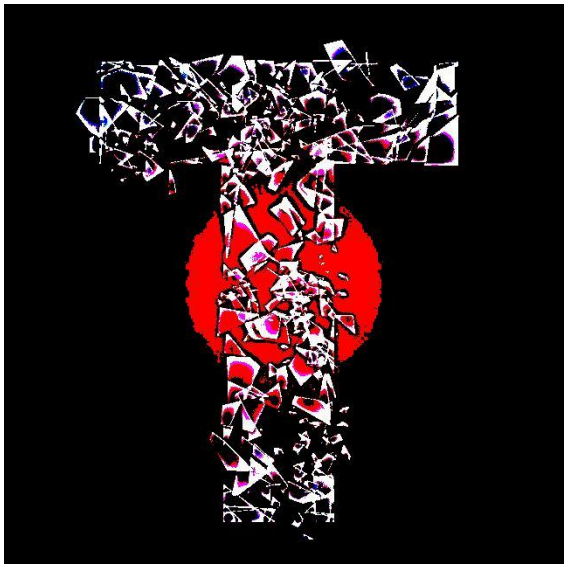


KASPERSKY

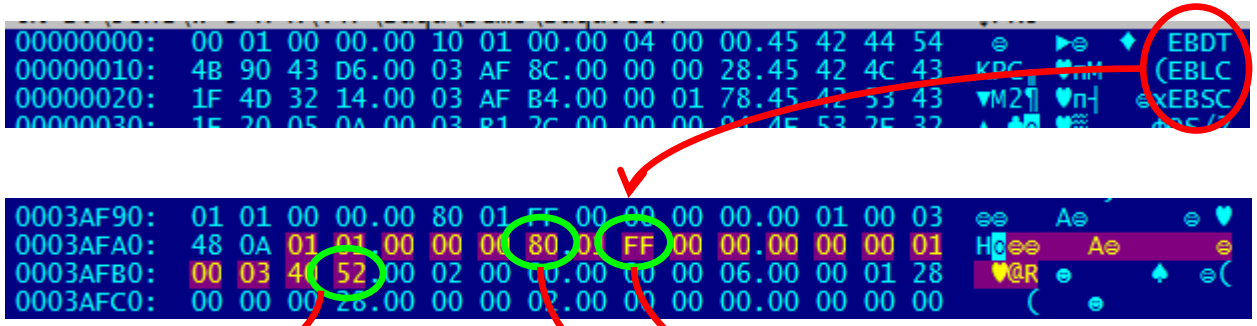
CVE-2011-3402

win32k.sys

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



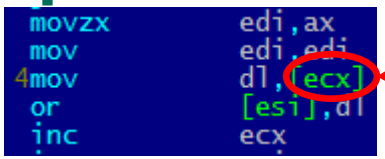
CVE-2011-3402



Calculate *WorkSize*: 200

Calculate *WorkOffs*: A40

Tamper *cvt_size*:



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

KASPERSKY lab