Debugging.TV

Frame 0x31

Presenter: Dmitry Vostokov

Topics

- Heap Leaks: explicit and implicit
- Parameter reconstruction
- Example

Varieties of Leaks

- Explicit
  - alloc / missing free
- Implicit
  - API call / missing matching “free” call
  - API call with wrong parameter

Modeling

```
void bar(HWND hWnd)
{
    LPCTSTR lpString = L"Hello Weird!";
    int size = 0xFFFFFFF; // "uninitialized" or corrupt

    HDC hDC = GetWindowDC(hWnd);

    if (!TextOut(hDC, 0, 0, lpString, size))
    {
        ReportError(GetLastError());
    }

    ReleaseDC(hWnd, hDC);
}
```

WinDbg session…

!Ad Hardcore Software Diagnostics Training

August 19-20, 2013	Accelerated Windows Malware Analysis
August 27, 2013	Mobile Software Diagnostics (FREE)
September 3, 2013	Psychology of Software Diagnostics (FREE)
September 6, 2013	Semiotics of Debugging (FREE)
September 13, 2013	Generative Software Narratology (FREE)
October 25-28, 2013	Accelerated Disassembly, Reconstruction and Reversing

Debugging.TV

Now on YouTube!

http://www.youtube.com/DebuggingTV