Debugging.TV

Frame 0x26

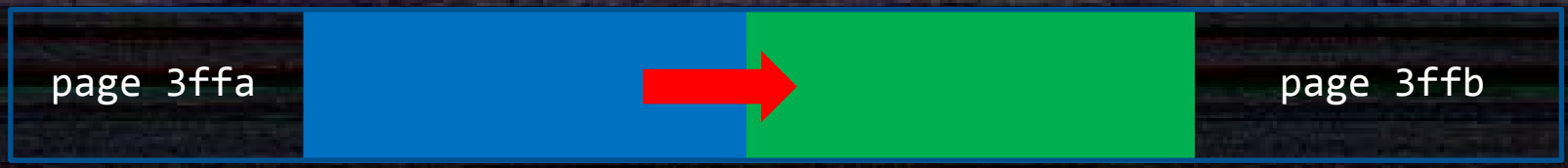
Presenter: Dmitry Vostokov

Topics

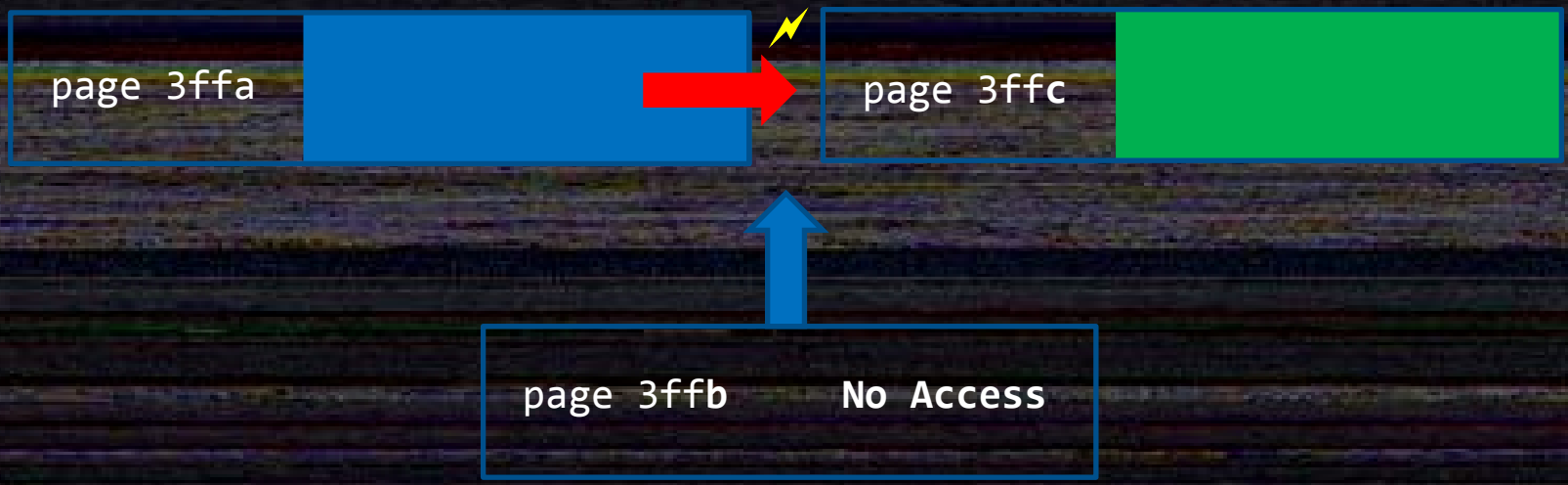
- Windows process heap corruption
- Buffer overwrite / overflow
- Buffer underwrite / underflow
- Gflags.exe

Overwrite / Overflow

Normal heap



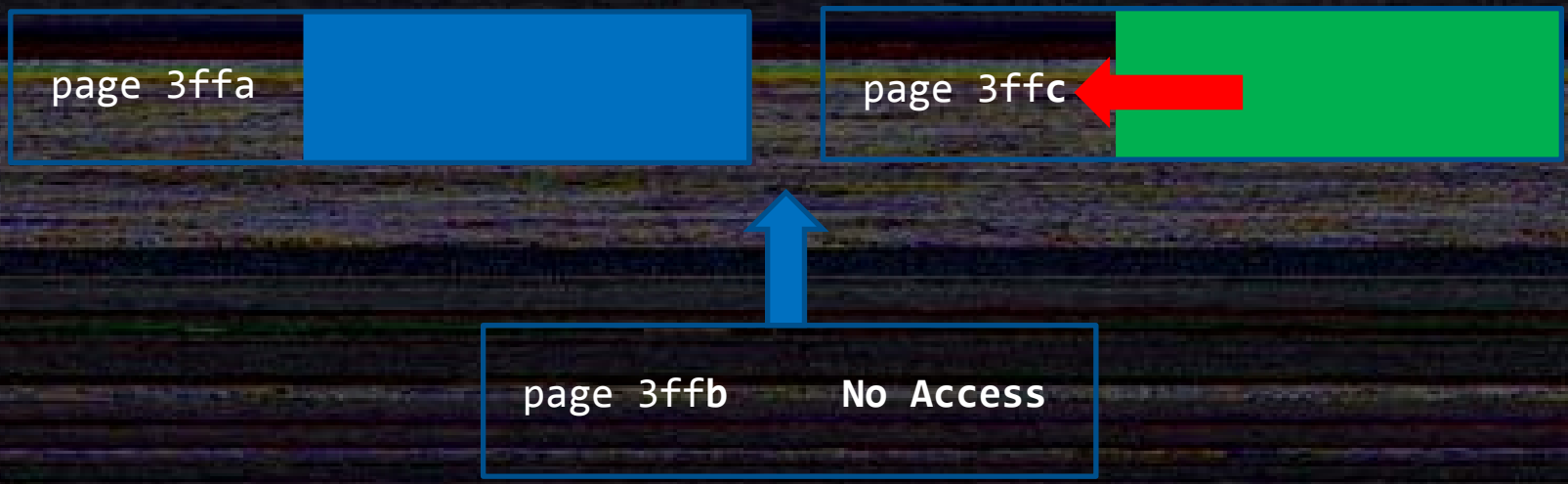
Full page heap



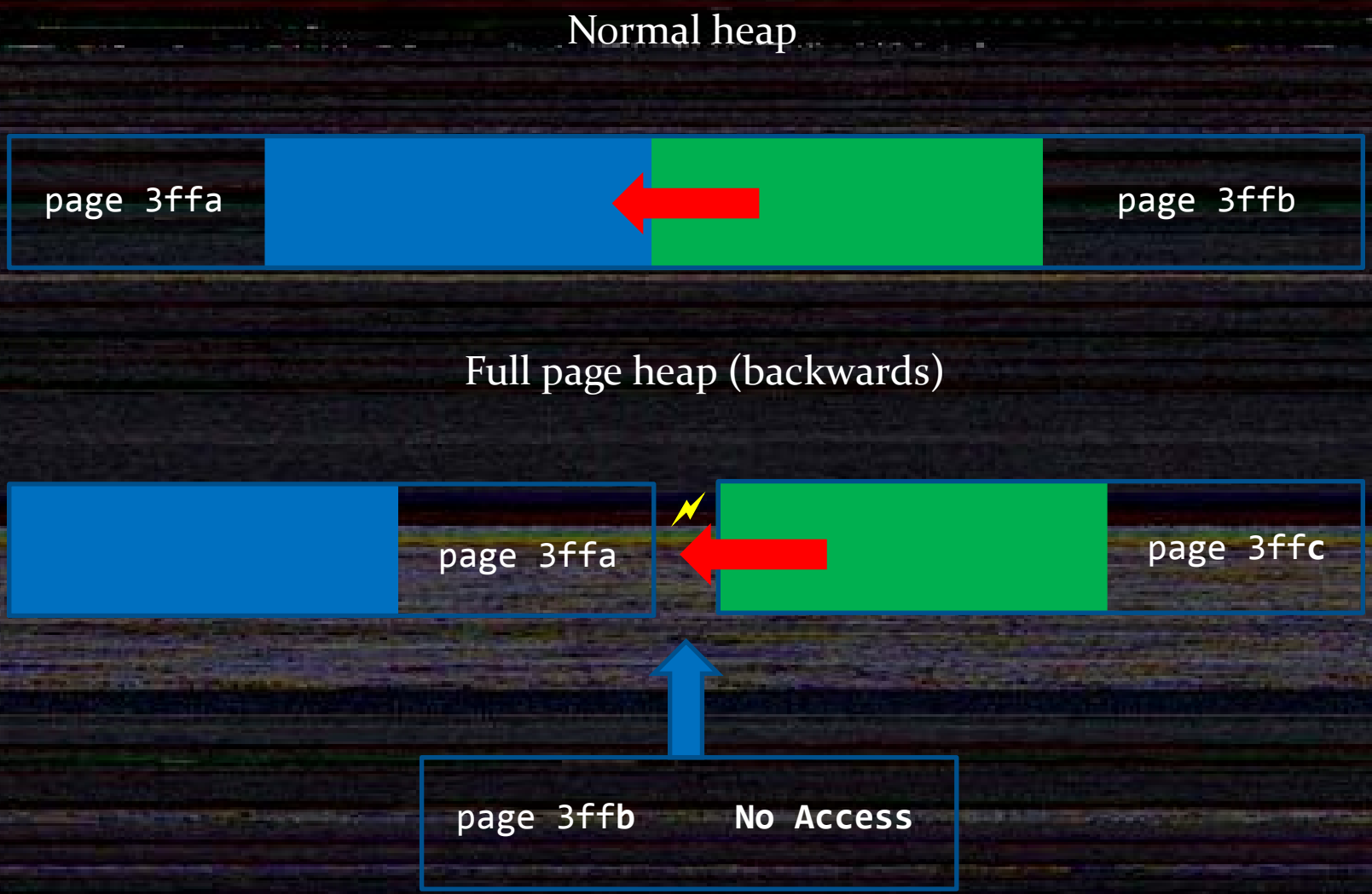
Underwrite / Underflow

Normal heap

Full page heap



Underwrite / Underflow

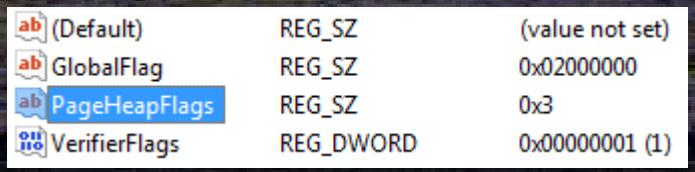


Gflags

Overflow / Overwrite

```
gflags /p /enable notepad.exe /full
```

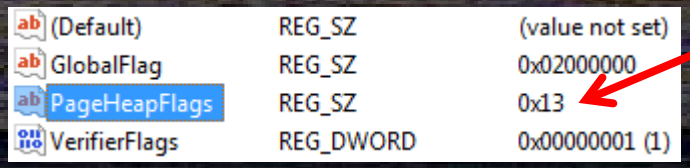
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe



Underflow / Underwrite

```
gflags /p /enable notepad.exe /full /backwards
```

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe



!Ad Hardcore Software Diagnostics Training

June 24, 2013	Pattern-Oriented Network Trace Analysis (FREE)
July, 19-22, 2013	Accelerated Windows Debugging^3
July 24-29, 2013	Accelerated Windows Memory Dump Analysis
July 30-31, 2013	Accelerated .NET Memory Dump Analysis
2013	The New Old Debugging
2013	Accelerated Network Trace Analysis

Debugging^3

Now Available for Booking

Debugging.TV

Now on YouTube!

http://www.youtube.com/DebuggingTV