



Debugging.TV

Frame 0x26

Presenter: Dmitry Vostokov

SOFTWARE DIAGNOSTICS SERVICES

www.DumpAnalysis.com

Including Memory Dump and Software Trace Analysis Audit, Seminars,
Certification and Training

Sponsors

OPENTASK

Iterative and Incremental Publishing

Topics

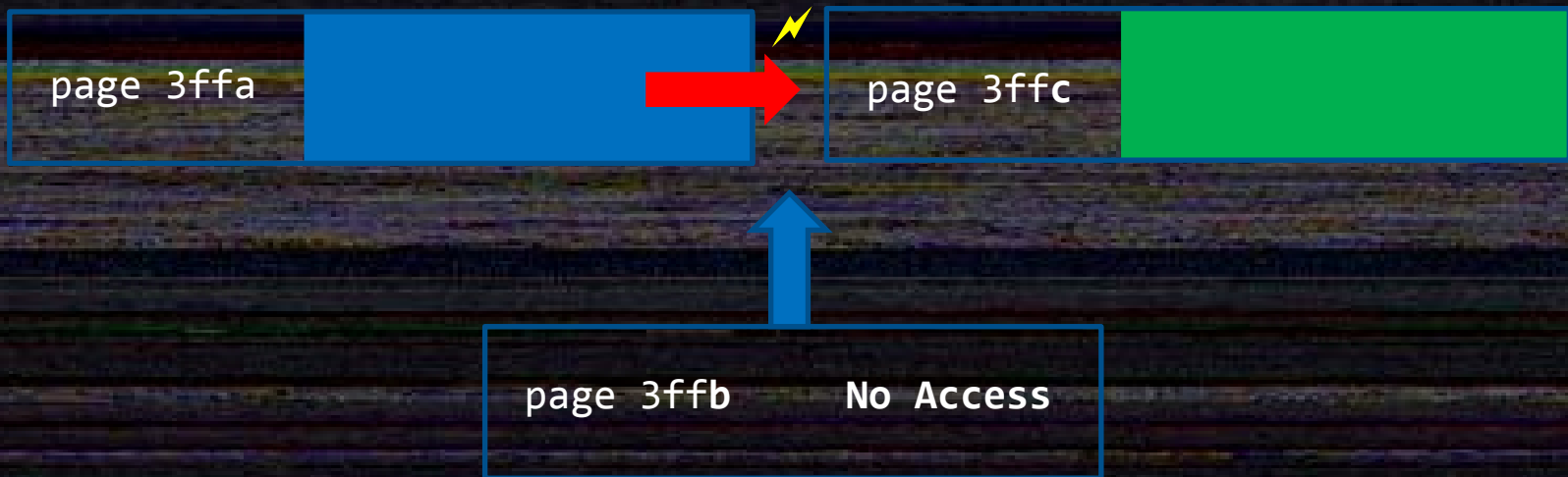
- Windows process heap corruption
- Buffer overwrite / overflow
- Buffer underwrite / underflow
- Gflags.exe

Overwrite / Overflow

Normal heap



Full page heap

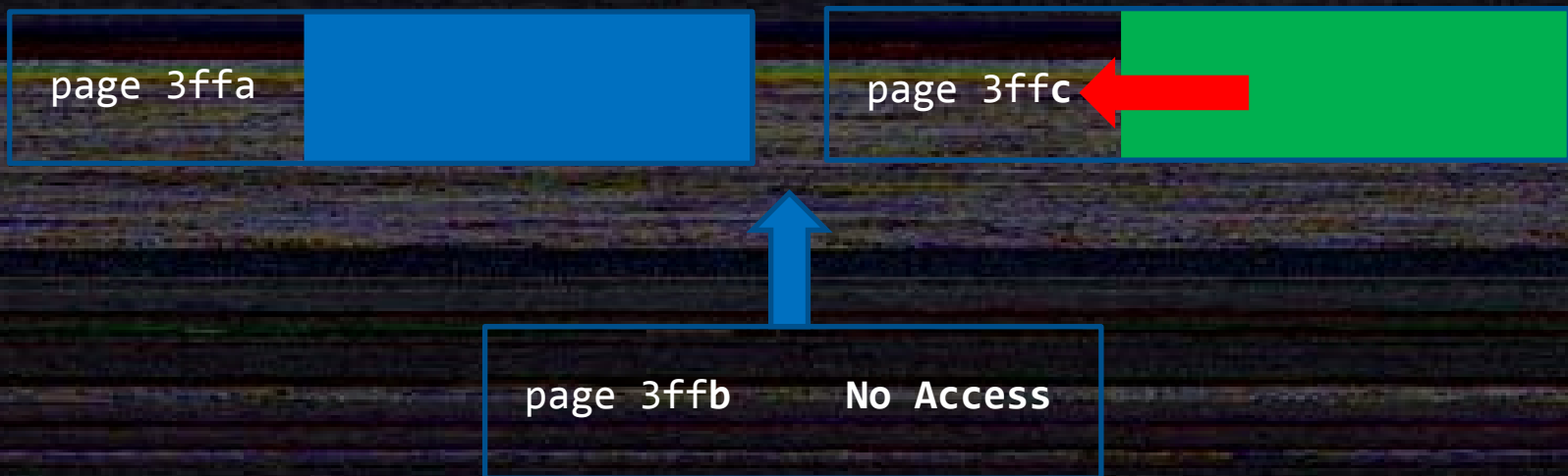


Underwrite / Underflow

Normal heap



Full page heap

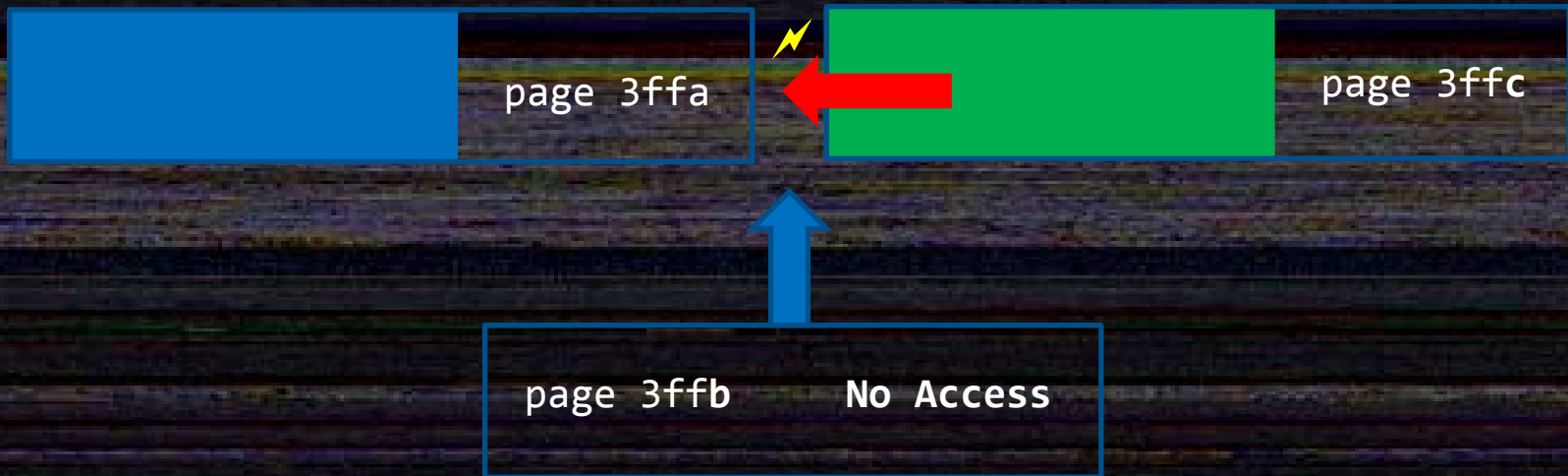


Underwrite / Underflow

Normal heap



Full page heap (backwards)



Gflags

Overflow / Overwrite

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

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

(Default)	REG_SZ	(value not set)
GlobalFlag	REG_SZ	0x02000000
PageHeapFlags	REG_SZ	0x3
VerifierFlags	REG_DWORD	0x00000001 (1)

Underflow / Underwrite

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

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

(Default)	REG_SZ	(value not set)
GlobalFlag	REG_SZ	0x02000000
PageHeapFlags	REG_SZ	0x13
VerifierFlags	REG_DWORD	0x00000001 (1)

!Ad Hardcore Software Diagnostics Training

June 24, 2013	<u>Pattern-Oriented Network Trace Analysis</u> (FREE)
July, 19-22, 2013	<u>Accelerated Windows Debugging³</u>
July 24-29, 2013	<u>Accelerated Windows Memory Dump Analysis</u>
July 30-31, 2013	<u>Accelerated .NET Memory Dump Analysis</u>
2013	The New Old Debugging
2013	Accelerated Network Trace Analysis

Debugging³

Now Available for Booking

Debugging.TV

Now on YouTube!

<http://www.youtube.com/DebuggingTV>