



Of high Stakes and Stacks An Observability war story

Or Weis,
CEO, Rookout

Lt. IDF Intl. corps



Diving into the deeps



- Problem space: Gigabytes of remote Haystacks ...

Partition Boot Record (PBR)

Partitioning type:	MBR															
Filename	Ext.	Size	Created	Modified	Accs											
Partition 3	FAT32	495 MB														
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3A1B208A00	EB	58	90	4D	53	44	4F	53	35	2E	30	00	02	08	26	00
3A1B208A10	02	00	00	00	00	F8	00	00	3F	00	FF	00	45	90	0D	1D
3A1B208A20	BA	37	0E	00	8D	03	00	00	00	00	00	00	02	00	00	00
3A1B208A30	01	00	06	00	00	00	00	00	00	00	00	00	00	00	00	00
3A1B208A40	80	00	29	95	AB	76	6C	4E	4F	20	4E	41	4D	45	20	20
3A1B208A50	20	20	46	41	54	33	32	20	20	20	33	C9	8E	D1	BC	F4
3A1B208A60	7B	8E	C1	8E	D9	BD	00	7C	88	4E	02	8A	56	40	B4	08
3A1B208A70	CD	13	73	05	B9	FF	FF	8A	F1	66	0F	B6	C6	40	66	0F
3A1B208A80	B6	D1	80	E2	3F	F7	E2	86	CD	C0	ED	06	41	66	0F	B7
3A1B208A90	C9	66	F7	E1	66	89	46	F8	83	7E	16	00	75	38	83	7E
3A1B208AA0	2A	00	77	32	66	8B	46	1C	66	83	C0	0C	BB	00	80	B9
3A1B208AB0	01	00	E8	2B	00	E9	48	03	A0	FA	7D	B4	7D	8B	F0	AC
3A1B208AC0	84	C0	74	17	3C	FF	74	09	B4	0E	BB	07	00	CD	10	EB
3A1B208AD0	EE	A0	FB	7D	EB	E5	A0	F9	7D	EB	E0	98	CD	16	CD	19
3A1B208AE0	66	60	66	3B	46	F8	0F	82	4A	00	66	6A	00	66	5D	06
3A1B208AF0	53	66	68	10	00	01	00	80	7E	02	00	0F	85	20	00	0F
3A1B208B00	41	BB	AA	55	8A	56	40	CD	13	0F	82	1C	00	61	FB	55
3A1B208B10	AA	0F	85	14	00	F6	C1	01	0F	84	00	FE	46	02	B4	
3A1B208B20	42	8A	56	40	8B	F4	CD	13	B0	F9	66	58	66	58	66	58
3A1B208B30	66	58	EB	2A	66	33	D2	66	0F	B7	4E	18	66	F7	F1	FE
3A1B208B40	C2	8A	CA	66	8B	D0	66	C1	EA	10	F7	76	1A	86	D6	8A
3A1B208B50	56	40	8A	E8	C0	E4	06	0A	CC	B8	01	02	CD	13	66	61
3A1B208B60	0F	82	54	FF	81	C3	00	02	66	40	49	0F	85	71	FF	C3
3A1B208B70	4E	54	4C	44	52	20	20	20	20	20	20	00	00	00	00	00
3A1B208B80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
3A1B208B90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
3A1B208BA0	00	00	00	00	00	00	00	00	00	00	00	00	00	0A	52	65
3A1B208BB0	6D	6F	76	65	20	64	69	73	6B	73	20	6F	72	20	6F	74
3A1B208BC0	68	65	72	20	6D	65	64	69	61	2E	FF	0D	0A	44	69	73
3A1B208BD0	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	20
3A1B208BE0	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	61
3A1B208BF0	72	74	0D	0A	00	00	00	00	00	AC	CB	D8	00	00	55	AA

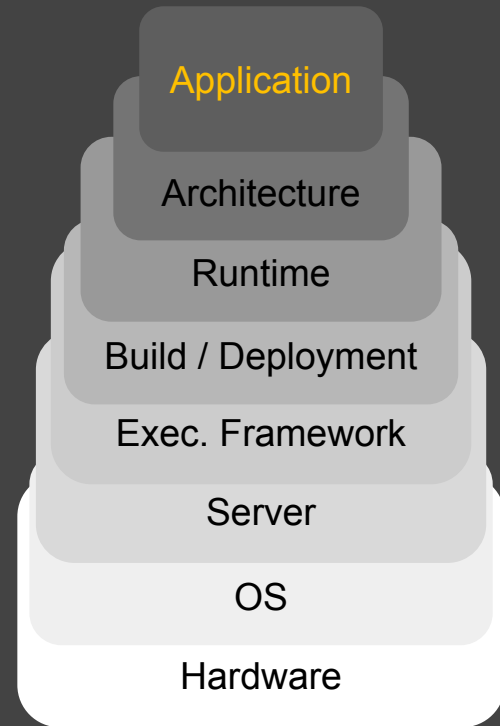
BIOS Parameter Block (points to offset 0x00000000)

Executable Code (points to offset 0x00000008)

- Machine Language Code
- Processor Specific
- Decodes BPB
- Searches for OS

PBR "Signature" (points to offset 0x00000055)

- 0x55AA



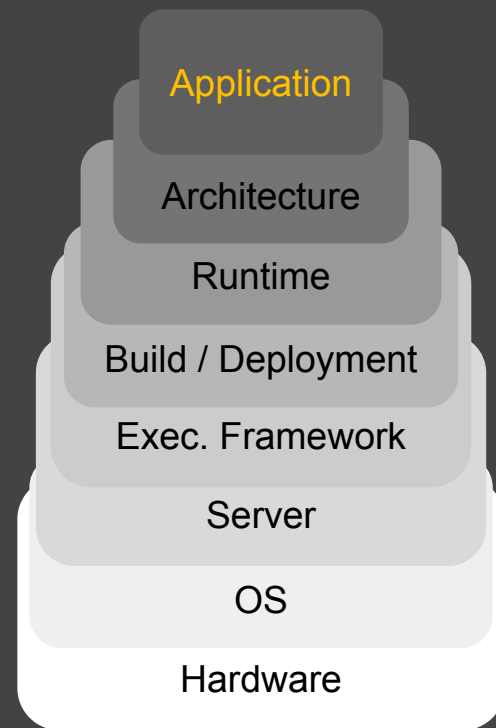
Diving into the deeps



- Reality doesn't care about our expectations
 - The challenge of the developer mindset
- Need to get creative in how we observe the problem
- Need to be able to iterate, and make each iteration count

- The bug: A Windows vulnerability, that become publicly known only 5 years later

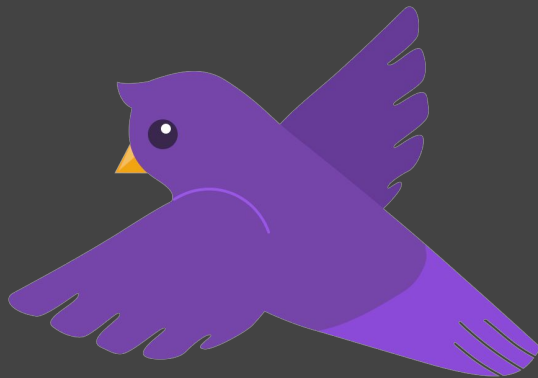
CVE-2014-4115



Production Observability and Debugging



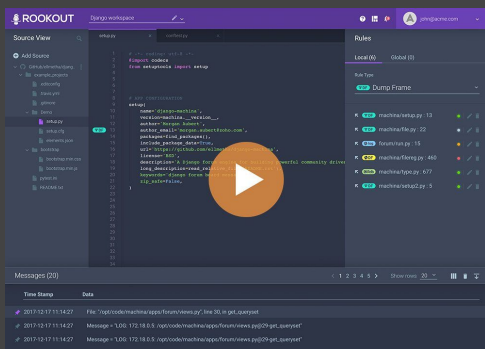
- You can't always simulate or replicate
 - Real data is needed to understand reality
 - Consider: scale, workloads, usage patterns, race conditions, ...
 - Modern technologies just make the problem worse
- Iteration is a must to hone-in on understanding
- Agility
 - Reduce risk
 - Reduce friction
 - Reduce dependency
 - Find the right data balance



Videos and links



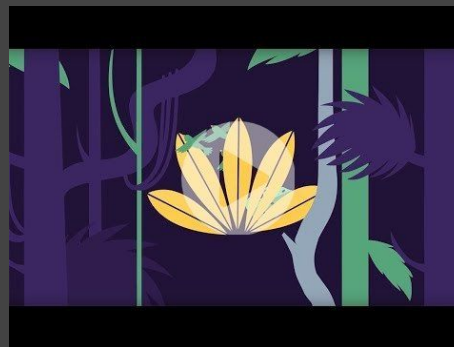
Basic demo



AWS Lambda Demo



“Your live code is a jungle” video



Select press coverage:

- [TechCrunch - Rookout fundraising](#)
- [TechCrunch - Rookout AWS Lambda Debugging](#)
- [ComputerWeekly - Production Debugging](#)
- [ComputerWeekly - Application Debugging \(ElectronJS\)](#)
- [Rookout CEO interview Sentry.io blog](#)

Links:

- [Rookout site](#)
- [Rookout Docs](#)
- [Brochure](#)

Serverless.com survey: Debugging is the biggest challenge

