Nietypowe narzędzia do debugowania kodu

Dominik Czarnota (disconnect3d)

O mnie


EVERYBODY'S OUT PARTYING
AND I'M SITTING HERE REVERSE ENGINEERING
memegenerator.net

Linux tracers

- Strace – śledzenie wywołań systemowych oraz sygnałów
- Ltrace – śledzenie wywołań funkcji z bibliotek współdzielonych (.so)
  - Przykłady: 0_tracers
    - „Unix WildCards Gone Wild” http://www.defensecode.com/public/DefenseCode_Unix_WildCards_Gone_Wild.txt

Valgrind

- Zestaw narzędzi do debugowania i profilowania:
  - Memcheck – detektor wycieków pamięci
  - Cachegrind – cache profiler
  - Callgrind – profiler, rozszerzenie Cachegrinda
  - Massif – heap profiler
  - Helgrind, DRD – debugowanie wątków, wykrywanie race condition
  - Other Tools – data flow tracer, bounds checker, IOgrind

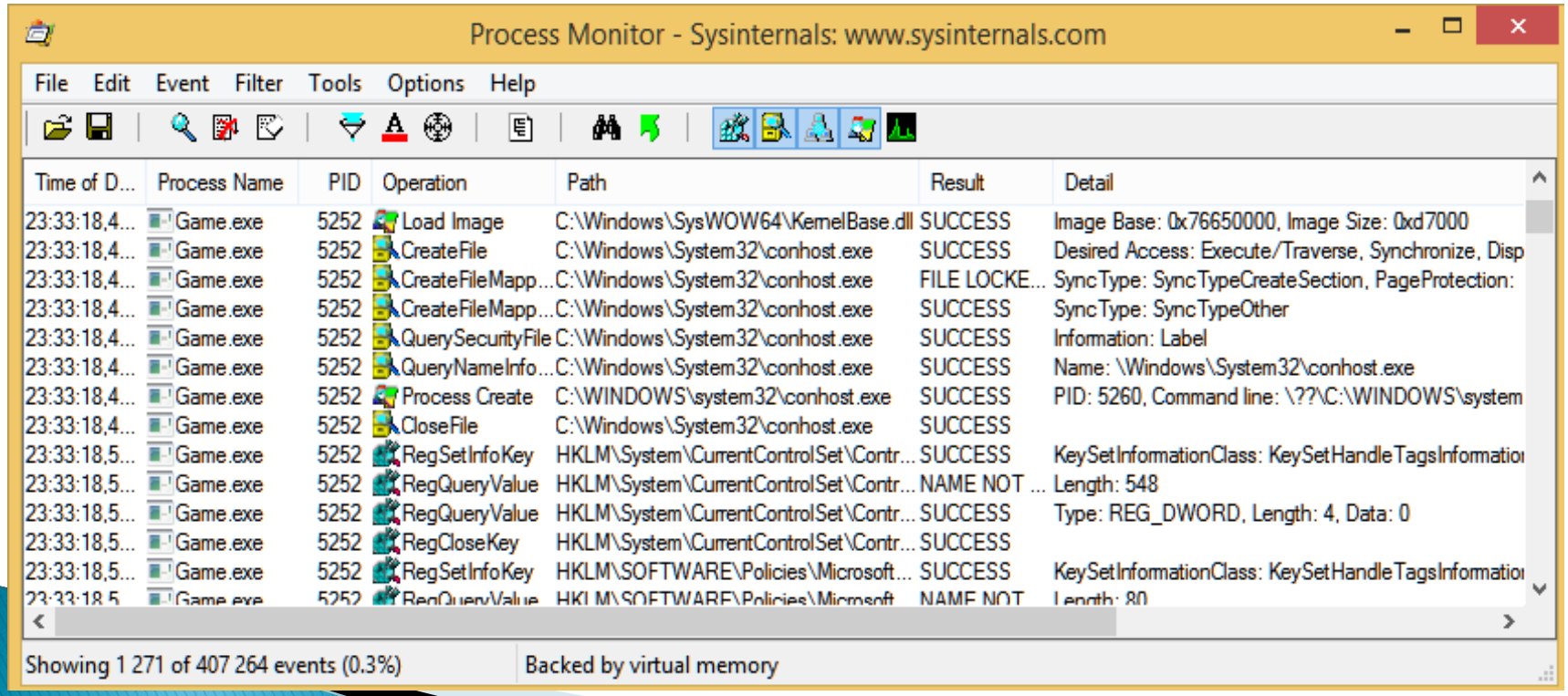
Sanitizery w gcc/clang

- Gcc/g++
  - Przykład: 2_sanitizers/ → make gcc-<sanitizer>
  - (leak, undefined, thread)

- Clang/clang++
  - Przykład: 2_sanitizers/ → make clang-<sanitizer>
  - (pass leak, undefined or thread as <sanitizer>)

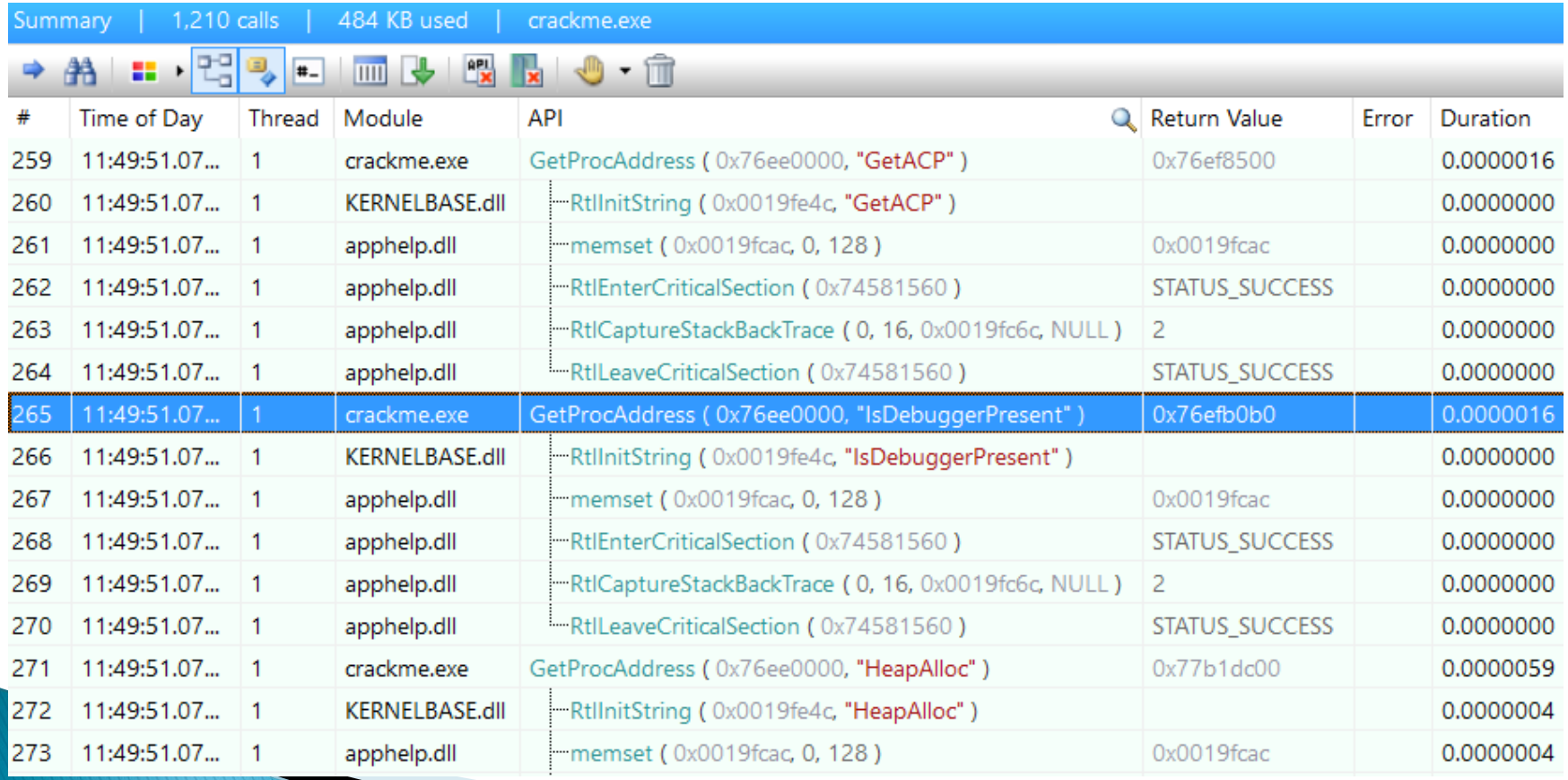
Process Monitor (SysInternals)

Narzędzie do monitorowania aktywności procesów w systemie Windows (odwołań do plików i rejestru).



API Monitor

Monitor odwołań do API Win32.



#	Time of Day	Thread	Module	API	Return Value	Error	Duration
259	11:49:51.07...	1	crackme.exe	GetProcAddress (0x76ee0000, "GetACP")	0x76ef8500		0.0000016
260	11:49:51.07...	1	KERNELBASE.dll	RtlInitString (0x0019fe4c, "GetACP")			0.0000000
261	11:49:51.07...	1	apphelp.dll	memset (0x0019fcac, 0, 128)	0x0019fcac		0.0000000
262	11:49:51.07...	1	apphelp.dll	RtlEnterCriticalSection (0x74581560)	STATUS_SUCCESS		0.0000000
263	11:49:51.07...	1	apphelp.dll	RtlCaptureStackBackTrace (0, 16, 0x0019fc6c, NULL)	2		0.0000000
264	11:49:51.07...	1	apphelp.dll	RtlLeaveCriticalSection (0x74581560)	STATUS_SUCCESS		0.0000000
265	11:49:51.07...	1	crackme.exe	GetProcAddress (0x76ee0000, "IsDebuggerPresent")	0x76efb0b0		0.0000016
266	11:49:51.07...	1	KERNELBASE.dll	RtlInitString (0x0019fe4c, "IsDebuggerPresent")			0.0000000
267	11:49:51.07...	1	apphelp.dll	memset (0x0019fcac, 0, 128)	0x0019fcac		0.0000000
268	11:49:51.07...	1	apphelp.dll	RtlEnterCriticalSection (0x74581560)	STATUS_SUCCESS		0.0000000
269	11:49:51.07...	1	apphelp.dll	RtlCaptureStackBackTrace (0, 16, 0x0019fc6c, NULL)	2		0.0000000
270	11:49:51.07...	1	apphelp.dll	RtlLeaveCriticalSection (0x74581560)	STATUS_SUCCESS		0.0000000
271	11:49:51.07...	1	crackme.exe	GetProcAddress (0x76ee0000, "HeapAlloc")	0x77b1dc00		0.0000059
272	11:49:51.07...	1	KERNELBASE.dll	RtlInitString (0x0019fe4c, "HeapAlloc")			0.0000004
273	11:49:51.07...	1	apphelp.dll	memset (0x0019fcac, 0, 128)	0x0019fcac		0.0000004

Dziękuję za uwagę

Pytania?

https://github.com/disconnect3d/unusual_dbg_presentation