Windows Kernel & Driver Development

Marcus Botacin[1]

[1]Informatics - Federal University of Parana (UFPR) - Brazil
mfbotacin@inf.ufpr.br

November 2018

Agenda

Agenda

About Me

- Malware Analyst (2012)
- BsC. Computer Engineer @ UNICAMP (2015)
  - **Sandbox Development**
- MsC. Computer Science @ UNICAMP (2017)
  - Hardware-Assisted Malware Analysis
- PhD. Computer Science @ UFPR (Present)
  - Hardware-Assisted Malware Detection
  - AntiVirus Evaluation
  - Future Threats
  - Contextual and Social Malware effects

Windows Model: Kernel Entering

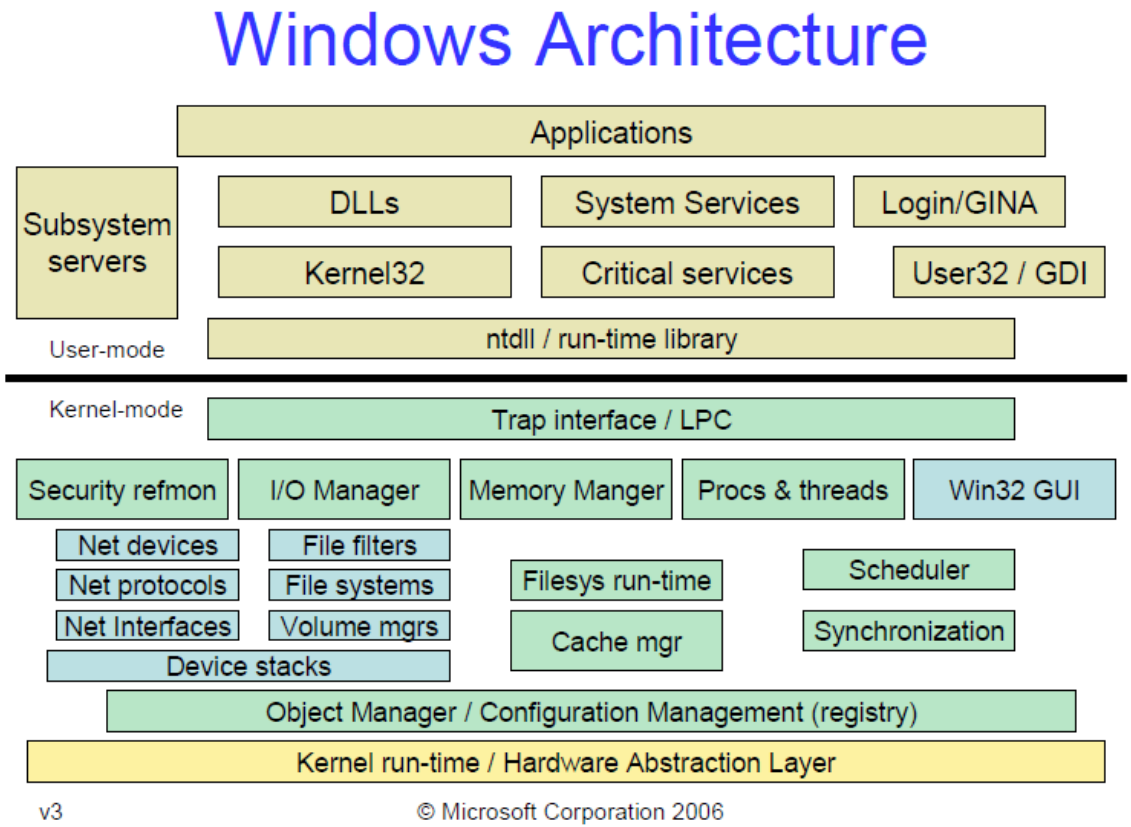

Figure: https://blogs.msdn.microsoft.com/hanybarakat/2007/02/25/deeper-into-windows-architecture/

Function Prototypes: Multiple Contexts

Wrapper

```
1 HANDLE OpenProcess(
2   DWORD dwDesiredAccess,
3   BOOL  bInheritHandle,
4   DWORD dwProcessId);
```

Complete Version

```
1 _kernel_entry NTSYSCALLAPI NTSTATUS NtOpenProcess(
2   PHANDLE            ProcessHandle,
3   ACCESS_MASK        DesiredAccess,
4   POBJECT_ATTRIBUTES ObjectAttributes,
5   PCLIENT_ID         ClientId);
```

Functions: Undocumented things

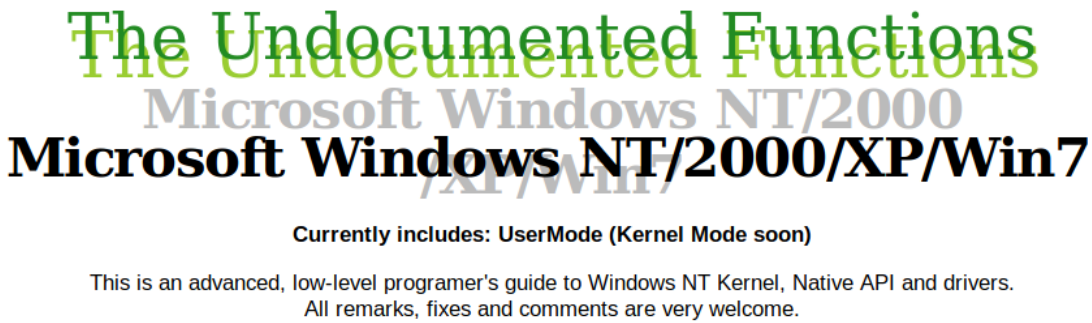

Figure: `http://undocumented.ntinternals.net/`

64-bit Windows

- Kernel Patch Protection (KPP).
- Driver Signing.
- Session Isolation.
- API Changes (`Ex` versions)

Agenda

Requirements

- VCC + WDK
- You don't need Visual Studio **but** You need Visual Studio
- SysInternals (DebugView)

Basics

- **Driver Models**: FileFilter, WDK & NDIS.
- **Basics**: Loading and Unloading.
- **Debugging**: Printing debug messages.

Userland Interaction

- Loading Driver Object as a file.
- Writing IO routines.

First Time Low Level

- Privileged instructions with intrinsics.

Monitoring

- My First Process Callback.

Agenda

References: Books

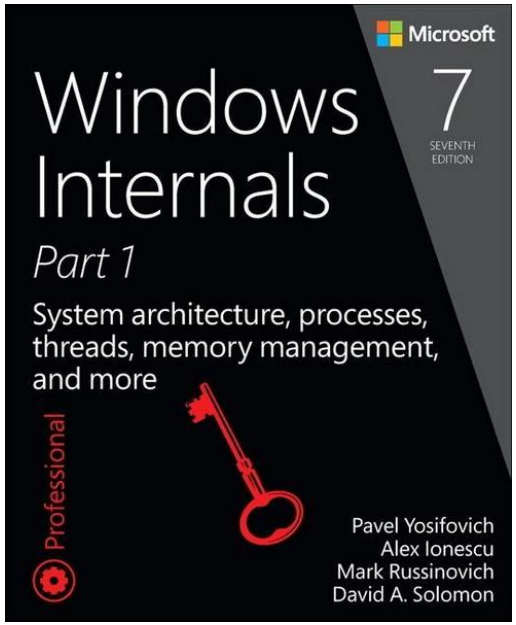

Figure:
https://blogs.msdn.microsoft.com/microsoft_press/2017/05/09/new-book-windows-internals-seventh-edition-part-1/

References: Books

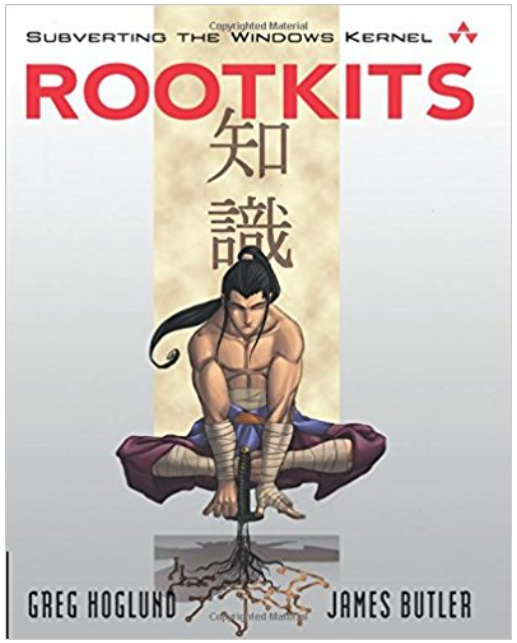

Figure: `https://www.amazon.com/Rootkits-Subverting-Windows-Greg-Hoglund/dp/0321294319`

References: Papers

- *Who watches the watchmen: A security-focused review on current state-of-the-art techniques, tools and methods for systems and binary analysis on modern platforms*—ACM Computing Surveys.
- *Enhancing Branch Monitoring for Security Purposes: From Control Flow Integrity to Malware Analysis and Debugging*—ACM Transactions on Privacy and Security.
- **Windows Sandbox** $\rightarrow$ *The other guys: automated analysis of marginalized malware*—Journal of Computer Virology and Hacking techniques.

Conclusions

Thanks

- Thanks Tilo for hosting me.
- Thanks CTF guys for inviting me.
- Open to hear your questions.

Contact

- `mfbotacin@inf.ufpr.br`
- `https://github.com/marcusbotacin`