So you wanna be a Malware Researcher

Suggestions from the field

Yevgeny Kulakov
@p_h_0_e_n_i_x

October 23, 2017

Content

Introduction
About Myself

- I'm Yevgeny Kulakov, nice to meet you!
- SW engineer and TL in image processing team
- At some point, I started to think about what to do next
- Cyber was associated with Terminator then (2011) & I didn't think about it
- I created a list of important things in a job and started the search
- Surprisingly, software security poped up with most bullets checked
- As complete n00b (on half cut salary) with big ambitions I started as MR @ Trusteer

Malware Research

What it has to offer - Cons & Pros are up to you

Constant technological challenge

- Cat & mouse game - you are reacting in most cases
- You need to learn constantly to be relevant
- Hours of wall hitting - too often there are no shortcuts

Malware Research

What it has to offer - Cons & Pros are up to you (cont.)

Financial compensation relatively high
as there is a shortage of skilled personnel.

Community

- It is relatively small - your reputation, help, connections
- In most cases if you need help, community is there for you
- Full of creative people - tons of activity in tooling creation & idea generation

Malware Research

What it has to offer - Cons & Pros are up to you (cont.)

Shifting horizontally in malware research field

- Vulnerability research
- Exploit development
- HW Research
- Security oriented SW engineering - if there is a developer in you

Shifting horizontally in malware research field

- Vulnerability research
- Exploit development
- HW Research
- Security oriented SW engineering - if there is a developer in you

In most cases you will need a significant resource investment to shift and become professional.

Malware Research
What to expect from day to day job

Job Titles

- Threat Analyst - mostly high level analysis (SOCs, tier I staff in security companies)
- Threat Hunter - intelligence gathering (company's self protection)
- AV/Malware Analyst/Researcher - more technical role

Common duties - depending on the company

- Network communication info - FW rules, net-based detection, CnC servers & etc.
- Packers/Evasion info - AV emulators, sandbox dev, signature generation & etc.
- Malware internals - prevention, detection implementation in security product.
- Evaluation of company's product against malicious code

Eventually, you'll need to use extracted info to enhance company's product.

Incident Response

- Understanding of sample purpose for damage assessment
- Forensic data gathering and analysis - memory dumps, network logs, disk images
- Finding the hole to close
- On-Call job - if you like action

More likely to be found in consulting companies.

Advanced Research - mostly in big companies

- Doing research for blog publishing
- Conducting big scale campaign analysis (APTs). Can span years.
- Research tools development - mostly voluntarily.

Example groups: GReAT (Kaspersky), FLARE (FireEye), Unit42 (Palo Alto)

Skill set
Computer Architecture

- Understand it on lower level - CPU, memory, peripherals
- Start with x86/x64 - the most common one
- Next is ARM
- Best source is architecture manuals
- You will master it over time

Skill set
Programming

- Assembly - you will know it one way or another
- How compiler works - improves your reversing skills
- C, C++ - most malware written in it, so you should know it too
- Python - a lot of tooling is developed with it

Skill set
Programming

You need to try to develop

- Code injector
- PE parser
- Kernel driver
- Shellcode "Hello World"

Skill set
(unusual) OS internals

- Invest in understanding of general OS architecture
- Memory management, User mode VS Kernel mode, Processes, Library concepts
- OS specific file formats - PE, ELF
- OS network implementation
- Code injections, hiding techniques
- Prepare for a lot of undocumented and low-level stuff (at least in Windows realm)
- Start with Windows

Skill set
Networking & Crypto

- Protocols - HTTP, TCP/IP
- At least general (practical) understanding of packet analysis and capturing
- Be familiar with implementation of crypto algos (RC4, AES, Hashing and etc)
- PKI - theory and implementation

Skill set
Reverse Engineering

- It’s not only staring on Assembly
- It’s hard and complex skill to develop
- It needs a lot of practice, ability to self learning, discipline
- Persistence and patience are the key
- Always clearly understand what is it you are looking for
- RE is based on knowledge we talked about, tools and your **BRAIN**
- … but once mustered - it’s like turning on a GOD mode

Tools of the trade

None exhaustive list

Debuggers

WinDbg - OllyDbg - x64dbg - GDB

Disassemblers

IDA Pro

Sandboxes

- Cuckoobox - open source, excellent for the start/home lab

File format editors

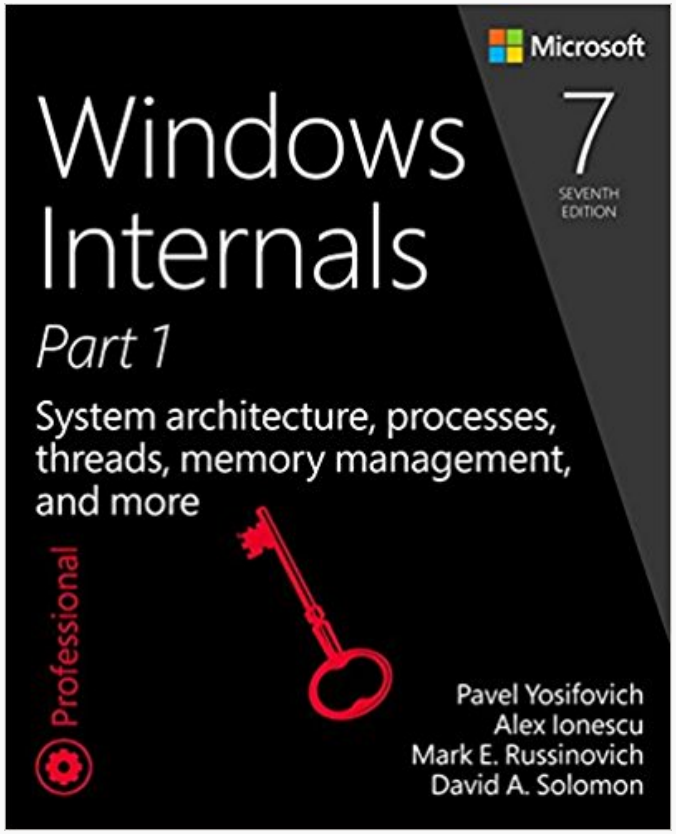
CFF Explorer - PEiD - LordPE - DiE

Memory analysis frameworks

Volatility - Rekall

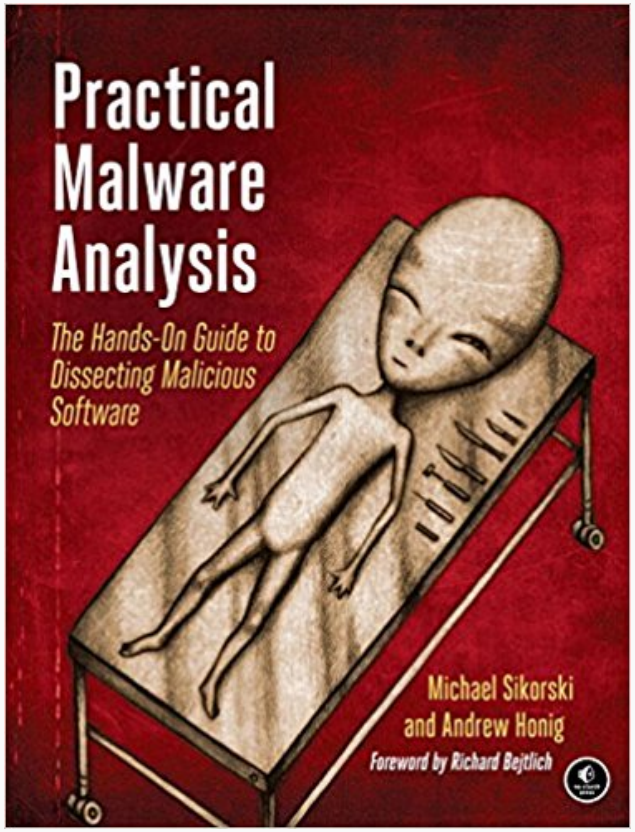
Book
on OS

This book is a bible on how Windows works. Keep it at your hand over the course of your career.



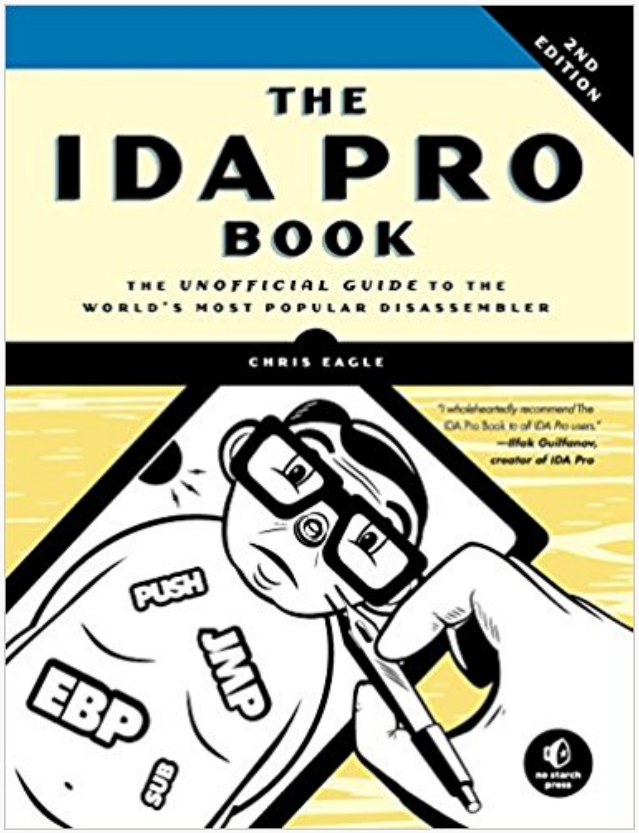
Book
on Malware Analysis

De-facto book that can train you as Malware Researcher.



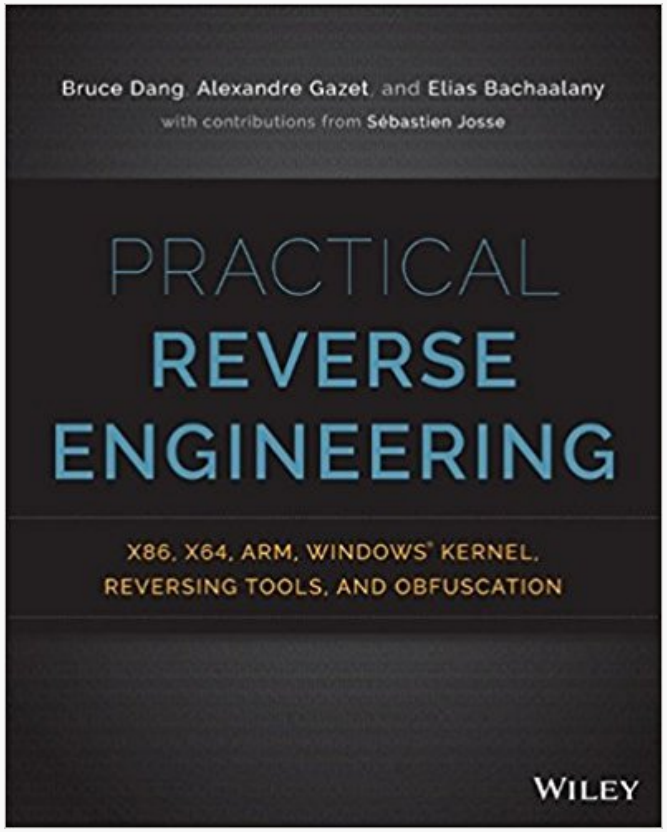
Book
on Disassembling

De-facto book for learning static analysis.



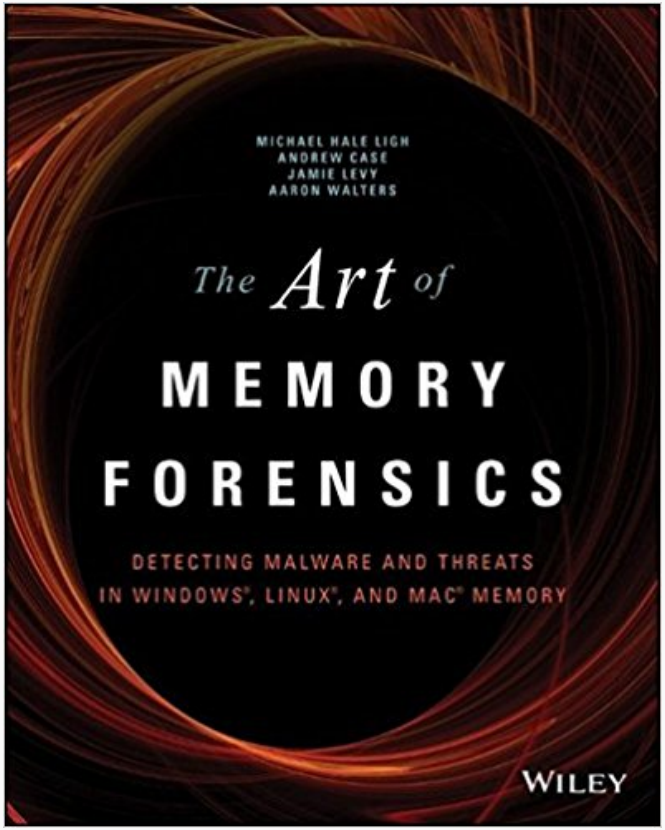
Book
on Reversing

More advanced chapters on RE.



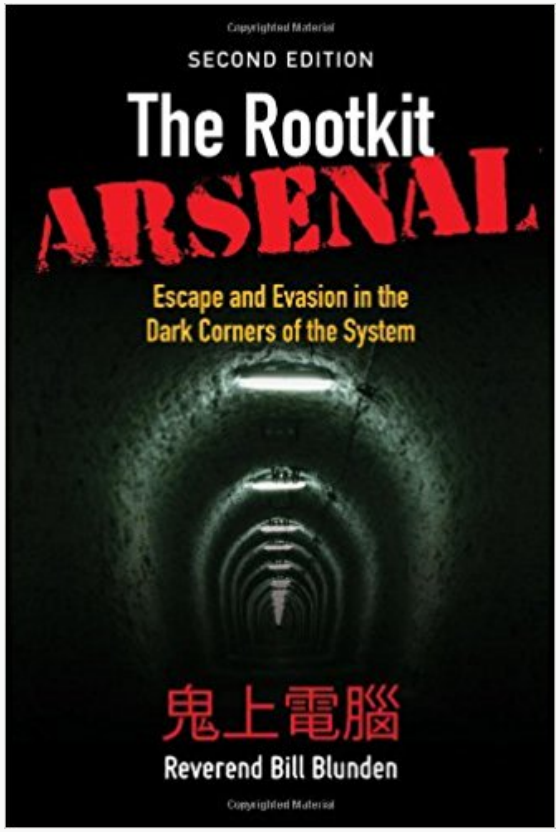
Book
on Memory Analysis bonus

Covers you on memory dumps analysis.



Book
on Dark side (bonus)

Dark side of the trade but very insightful - know your enemy.



Examples of malware research results

- Kaspersky
- ESET
- Virus Bulletin
- CitizenLab
- Alex Ionescu - world class expert on Windows internals
- Tuts4you - excellent place for everything RE

Real sources of malware families

- Carberp
- Tinba - pure asm
- Rovnix - kernel rootkit

Excellent sources of bootstrapping information

- Open Security Training
- Get yourself started with your first lab
- Lena51 - get you into RE fast (kidding)
- Coursera - Malicious Software and its Underground Economy

Experienced Malware Researcher - AV Company

Main Duties

- Lead research efforts within a particular threat research area
- Conduct analysis of a variety of different malware families and threats
- Produce high-quality proactive protection against Windows malware and applications
- Consult with development teams to enhance protection capabilities in Sophos products
- Publish articles and/or white-papers on research
- Help with complex malware detection issues escalated by customers
- Develop tools, work flow and/or systems improvements

Experience and Skills

- 5+ years in computer security field, 2+ years direct anti-malware industry experience
- Advanced reverse engineering using IDA Pro
- Expert-level debugging, OllyDbg or WinDbg
- Detailed knowledge of Windows internals and kernel-level analysis
- Proven ability to prioritize and organize assigned tasks
- Ability to work both independently and as part of a team
- Good written and verbal communication skills
- Bachelor degree in Computer Software (or equivalent)

Jonior Malware Researcher - Security Company

Company has an exciting opportunity to join our Anti-Virus Analyst team in Burnaby. You have an appetite for learning botnets, viruses, and other malicious software analysis techniques to make the world a safer place. Build your malware knowledge and reverse engineer different types of malware – file infectors, network worms, Trojans, backdoors, rootkits, etc. *Company* **has a training program for all Anti-Virus Analysts where you will learn with your peers**, how to analyze viruses and help our customers detect and understand the behavior of malware. As a new grad, this extensive training will help you excel in your role to become an expert in this field and prepare you for a range of internal growth opportunities, as *Company* is recognized as a company that continually promotes from within.

Job Responsibilities:

- Virus/malware replication and analysis
- Analyze customers' inquiries and submissions of virus/malware
- Develop virus/malware detection algorithms in proprietary description language
- Write descriptions of virus/malware for publication on *Company*'s website
- Develop programs/scripts for virus/malware analysis and replication

Job Skills Required:

- Experience and understanding of software programming (C/C++)
- Experience and understanding of Intel x86 assembly language is an asset
- Experience with scripting languages (Python, Perl, JavaScript, VBS, Linux Shell) is an asset
- Fast learner with a good attitude
- Team player
- Proven analytical and problem solving skills
- Empowered to make a difference in network security


Thank you!