NTNU

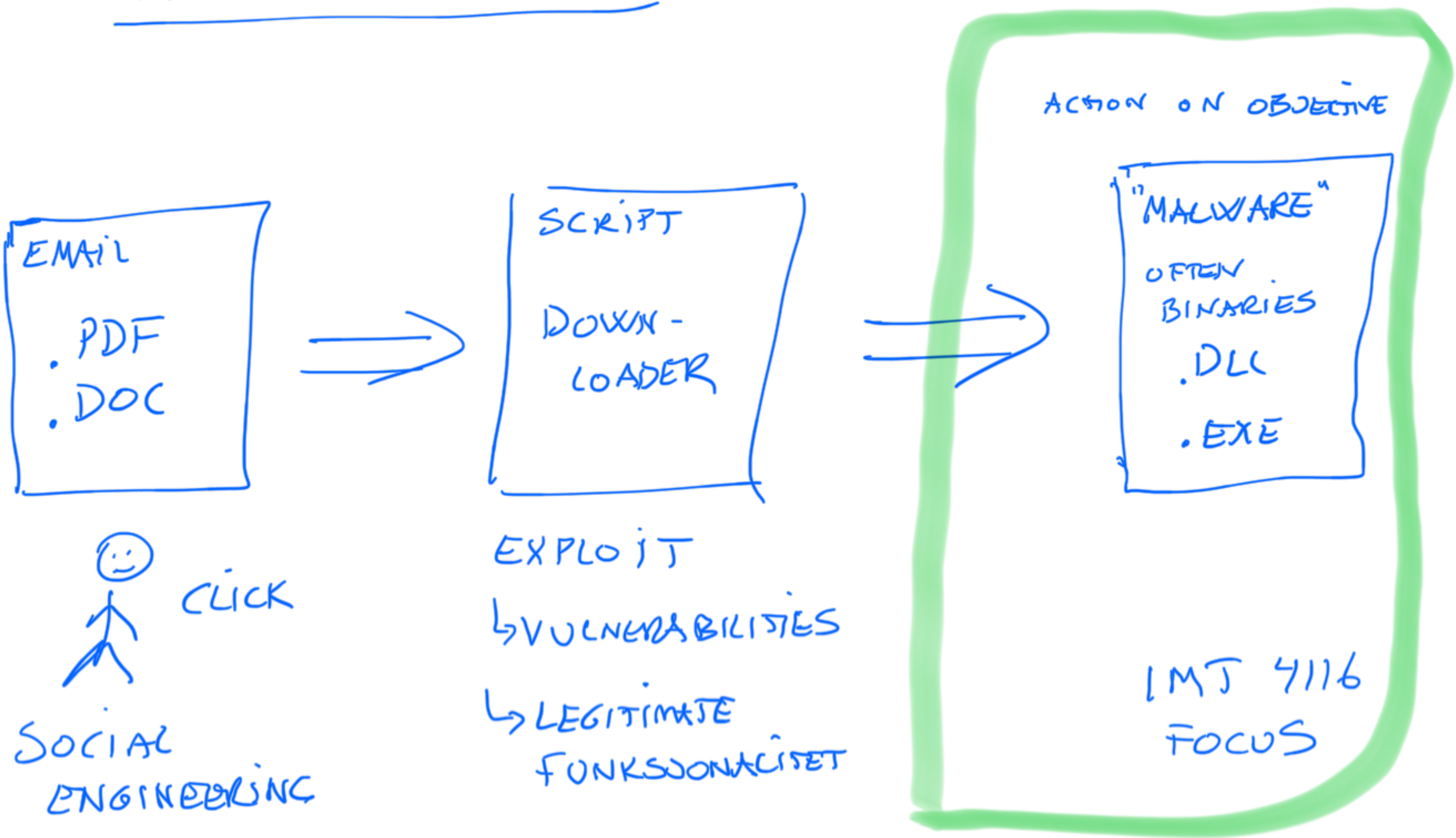
DFRWS 2019
MALWARE ANALYSIS WORKSHOP

Associate Professor Geir Olav Dyrkolbotn

PhD Candidate Sergii Banin

DISSECTING A KEY LOGGER

TYPICAL ATTACK



In this tutorial

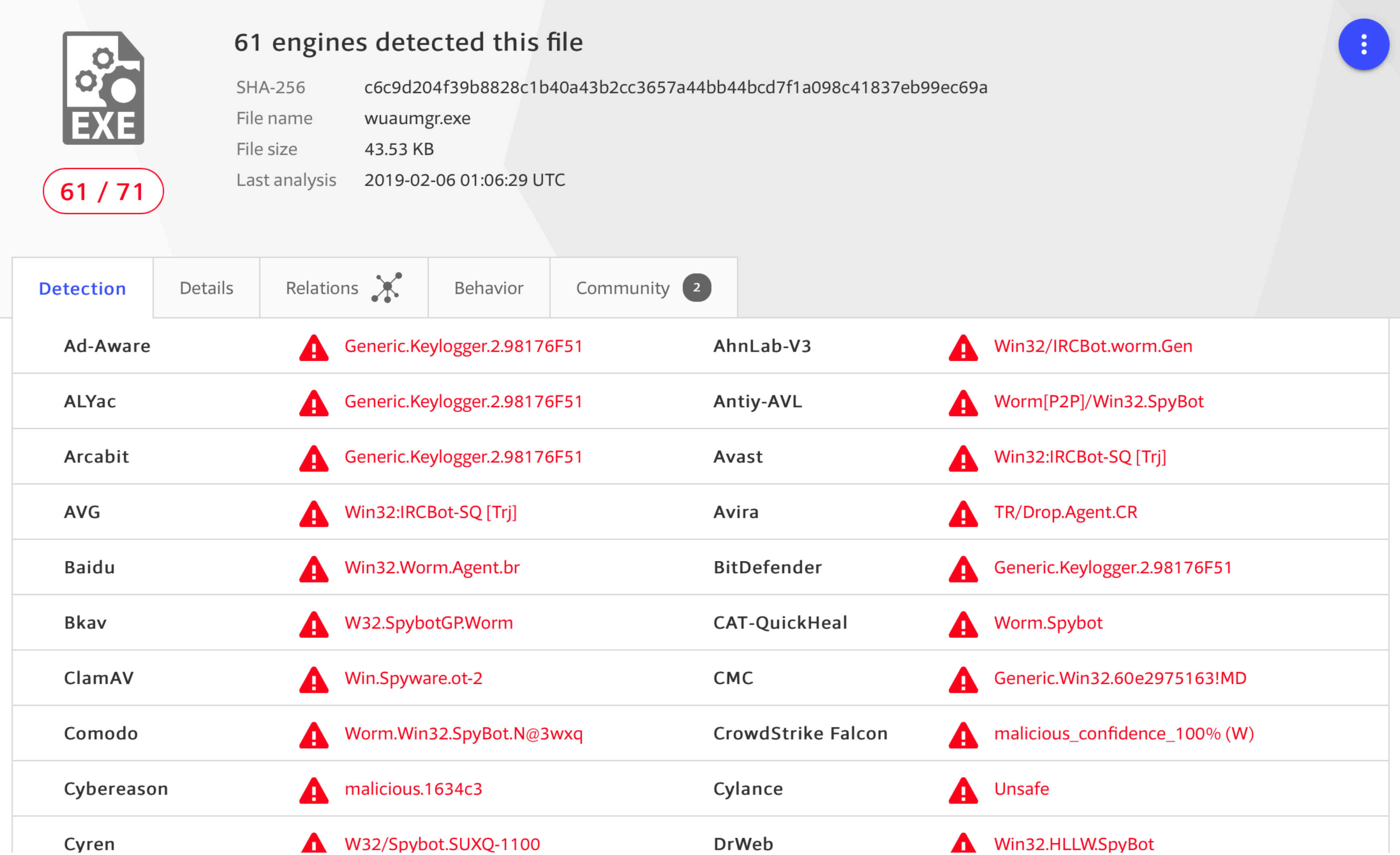
Look at one sample in detail

1. **Basic static analysis**
   How to retrieve information without executing the malware and form a quick hypothesis about what it is doing
2. **Basic Dynamic analysis**
   What happens to our file system and registry if we run the malware. Can we detect any network traffic?
3. **Advanced Static Analysis**
   How can we use a disassembler (IDA Pro free) to learn more about the malware’s functionality?
4. **Advanced Dynamic Analysis**
   How can a controlled execution of the malware in a debugger (OllyDbg) increase your understanding?

What sample? SpyBot

(SHA-256: c6c9d204f39b8828c1b40a43b2cc3657a44bb44bcd7f1a098c41837eb99ec69a)

spybot.zip password: infected



61 engines detected this file

SHA-256	c6c9d204f39b8828c1b40a43b2cc3657a44bb44bcd7f1a098c41837eb99ec69a
File name	wuaumgr.exe
File size	43.53 KB
Last analysis	2019-02-06 01:06:29 UTC

61 / 71

Ad-Aware	Generic.Keylogger.2.98176F51	AhnLab-V3	Win32/IRCBot.worm.Gen
ALYac	Generic.Keylogger.2.98176F51	Antiy-AVL	Worm[P2P]/Win32.SpyBot
Arcabit	Generic.Keylogger.2.98176F51	Avast	Win32:IRCBot-SQ [Trj]
AVG	Win32:IRCBot-SQ [Trj]	Avira	TR/Drop.Agent.CR
Baidu	Win32.Worm.Agent.br	BitDefender	Generic.Keylogger.2.98176F51
Bkav	W32.SpybotGP.Worm	CAT-QuickHeal	Worm.Spybot
ClamAV	Win.Spyware.ot-2	CMC	Generic.Win32.60e2975163!MD
Comodo	Worm.Win32.SpyBot.N@3wxq	CrowdStrike Falcon	malicious_confidence_100% (W)
Cybereason	malicious.1634c3	Cylance	Unsafe
Cyren	W32/Spybot.SUXQ-1100	DrWeb	Win32.HLLW.SpyBot

General comments

- I will show one or a few ways to analyze
- In malware analysis it is important to try many different approaches
- Sometimes one will work, other times another
- No tool is optimal in all cases.

- I will encourage you to
  - Try different approaches yourself
  - Share (malware forum in BlackBoard or ??)

- The slides I use, with screenshoots, will be provided after the workshop

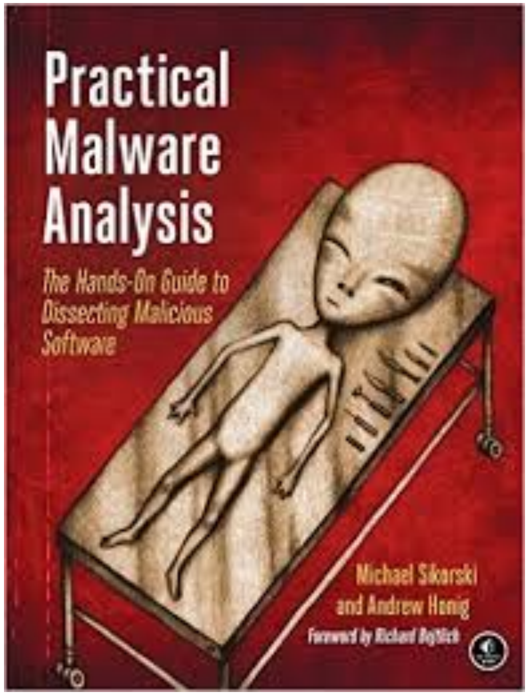
Moral and Ethics

- Malware analysis and reverse engineering can be used for good or evil
- Misuse of knowledge obtained can lead to criminal charges.
- By following this workshop you agree to take full responsibility for any misuse of knowledge obtained
- DFRWS, NTNU and the lecturer will not be responsible for any misuse of knowledge obtained during the workshop

Further Reading

- Pratical Malware Analysis
  A bit old, but still a very good introduction

- NTNU Malware Forum 2019
  - June 5th Oslo
  - Michael Sikorski will be there
  - https://www.nsm.stat.no/norcert/norcertforum2019/


Practical
Malware
Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski
and Andrew Honig
Foreword by Richard Bejtlich

M.Sikorski and A. Honig:
Practical Malware Analysis,
The hands on guide to dissecting Malicious Software
ISBN: 978-1-59327-290-6

Time Schedule (ish)

Session 1 - 09:30-11:00

- Introduction (15)
- Basic static (30)
- Basic Dynamic (45)

Break 11:00-11:15

Session 2 - 11:15-12:30

- Advanced Static (45)
- Advanced Dynamic (30)