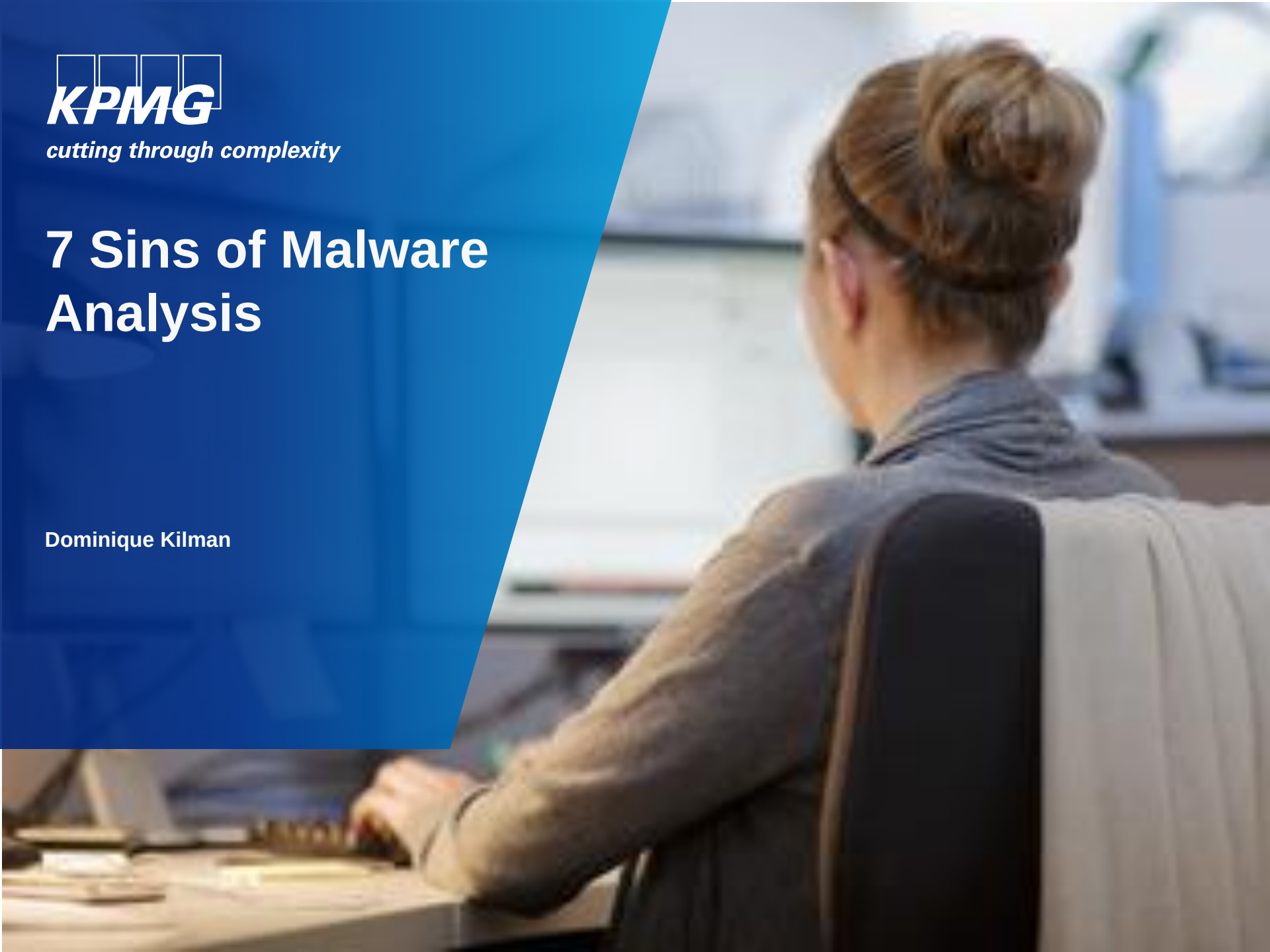
KPMG

cutting through complexity

7 Sins of Malware Analysis

Dominique Kilman



Dominique Kilman

Programmer and software tester

Security geek for over 10 years

- Incident response
- Red teaming
- Modeling and simulation of security protocols
- Forensics

CISSP, CISM, GCIH, GREM, GAWN … a few more ☺

Why we are here…

- Discuss the common mistakes that analysts make when performing malware analysis
- Give new analysts some of the “gotchas” to avoid
- Provide tips for experienced analysts to help them get better

Complacency

- Not keeping up with new developments and tools in the field
- Focusing on a single tool to get answers
  - Olly may be your go-to for reversing, but don’t forget that Immunity or IDA may have features that will speed up your process (depends on the goal)

Sampling of malware analysis tools released/updated in last 6 months:

Procdot

Sampling of malware analysis tools released/updated in last 6 months (continued):

Procdot

HookAnalyser 2.4

Sampling of malware analysis tools released/updated in last 6 months (continued):

Procdot

HookAnalyser 2.4

PeStudio added VirusTotal support

Sampling of malware analysis tools released/updated in last 6 months (continued):

Procdot

HookAnalyser 2.4

PeStudio added VT support

REMnux v4: added ~ 15 new tools including:

- OfficeMalScanner
- ProcDot
- ExifTool

Sampling of malware analysis tools released/updated in last 6 months (continued):

Procdot

HookAnalyser 2.4

PeStudio added VT support

REMnux v4 added ~ 15 new tools

CrowdInspect

Isolation

- Working inside a bubble may help you focus and get tasks done, but learning from others and asking for help can make you a better analyst
- Everyone can use a different perspective when they hit a wall

Connection

- Running malware on a live network can lead to infections of the network
- Your now-infected analysis machine may start attacking others and spreading more malware
- You do not want to be the reason your company (or ISP) gets a call from the authorities!

Browsing

Clicking on links in phishing e-mails or connecting directly to IPs or URLs embedded in malware could infect your machine

- And the rest of the network depending on the nature of the malware

Malware sites may be monitoring their C2 sites

- They may be monitoring to see if their tool has been detected
- They may try to identify researchers
- They may provide different results for connections coming from unknown IP, domain or user agents

Infecting

Sending malware to other analysts or coworkers may be necessary - but infecting those people is a sin

- Use password-protected compressed files (this will also prevent mail systems from quarantining your messages)
- Make sure the recipient knows that the file may be malicious
- Changing the extension (eee vs. exe) can prevent accidental infections

Malware stored in regular compressed files or as executables can and does get cleaned as AV signatures update

- Getting the malware back from the AV company often does not work
- If the exe was in e-mail, likely the e-mail system has also removed the file

Exposure

Online sites that allow you to upload malware sample for quick analysis are nice, however:

- Attackers may be monitoring for just such information
- Organization may not want to disclose publicly that they have a specific infection (or any infection)

Always get permission before uploading samples to online scanning sites

Automation

Automated tools are a fast way to get results, but they may miss things.

It never hurts to manually analyze specimens, especially when automated tools give conflicting answers:

- One tool identifies a file as suspicious
- Another finds no suspicious indicators
- The third will not execute the file at all

Keep in mind

… many of the behaviors here are not BAD in and of themselves…

- The problem comes in when you stop planning what you are doing or do not think before you act
- Everything in moderation

The goal here is to get you to think before you do you analysis…

- Set up your analysis environment correctly
- Make sure you have an understanding of the goal (yours and the organization's)
- Most of all keep learning!

Are there any virtues?

of course!

Experiment

- Try out new tools
- Try new methods of analysis
  - New automation options (in moderation of course!)
  - New sites that provide information
- Attend conferences and training to learn new methods

Contribute

Be involved in the community

- Blog
- Tweet
- Develop tools

Try to make the state of the art better

Critique

- When you try out those new tools and methods - give **constructive** criticism
- Help developers make the tools better
- For those getting the critique - be receptive to the comments and try not to take them as a personal attack

Verify

- Just because you are paranoid…
- Checking that your environment is configured correctly before you start analysis
- Double check before you send files to others to make sure they are shared safely

Mentor

- Help others develop their skills
- The more knowledgeable, capable people out there - the better chance of winning

Share

When you can:

- Share indicators
- Share methodologies
- Share knowledge

This is the flip-side of exposure - sharing when appropriate and with permission

Final thoughts

- The theme of the virtues is about making the state of the art of malware analysis better
- The more we help each other, develop and enhance our TTP, the more we can focus on the “hard problems” (or as I call this, the fun stuff)
- We should think as a community where we are here to help, not as competitors who need to “beat” the other analyst

Questions?

Dominique Kilman
dkilman@kpmg.com

General Disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.