

HOW **MALWARE ANALYSIS** CAN GUIDE THREAT HUNTING & DETECTION ENGINEERING

*Kyle Cucci
Team Lead, Malware Response & Research
Finance and Banking Sector*

ABOUT ME


- ▶ Leading the malware research team @ German bank.
- ▶ Daily focus on researching malware threats affecting Finance, and dabbling in threat intelligence and hunting.
- ▶ Hobbies: Writing/blogging, playing with security tools, spending time with my wife and kid, sometimes running but mostly sitting.

○ Twitter:
@d4rksystem

○ LinkedIn:
<https://de.linkedin.com/in/kylecucci>

A series of three parallel white lines of varying lengths and orientations, starting from the right edge and extending towards the center of the slide, creating a dynamic, abstract graphic element.

AGENDA

1. Common Issues in Developing Hunt & Detection Use-Cases
 2. What is/isn't Malware Analysis?
 3. Developing Malware Analysis-Driven Use-Cases
 4. IoC Abstraction
- 
- A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.

DESIGNING USE-CASES*

THE PROBLEM(S)

- ▶ Difficult to build *quality* and *relevant* use-cases.
- ▶ Difficult to gather specific, technical data points and intelligence.
- ▶ Tools like MITRE ATT&CK help – but have their own sets of problems:
 - ▶ Very generalized, and little guidance. Where to focus?
 - ▶ Leading to: Poor (or no) prioritization!
- ▶ **Proposal:** Use Malware Analysis to help guide hunting and detection!

***Use-Case** = My generic term for a threat hunt or a detection rule.

WHAT IS (AND ISN'T) MALWARE ANALYSIS?

- ▶ Goals of Malware Analysis:
 - ▶ Understand malware's key behaviors.
 - ▶ Assess the impact of an infection/attack.
 - ▶ Identify containment/remediation measures.
 - ▶ **Extract IoC's, techniques, and intelligence.**
- ▶ All that is initially required is a dedicated analysts and a sandbox.
- ▶ Remember that malware analysis has its limits..😞


When you use CTRL + C instead of copying using right click



Source: Memebase

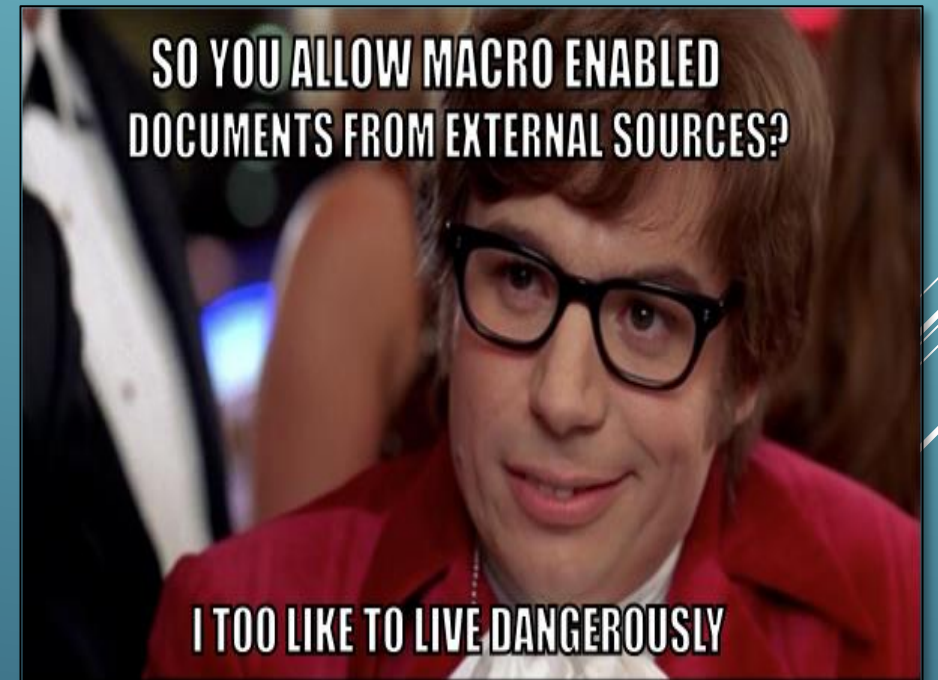
DESIGNING USE-CASES

USING MALWARE ANALYSIS

- ▶ Malware contains **concrete** indicators and techniques to guide hunting and detection engineering
 - ▶ These techniques often cover many areas of MITRE ATT&CK and can compliment MITRE ATT&CK.
 - ▶ If your malware sources are good, malware is **inherently relevant** to your organization! (More on this later.)
- 

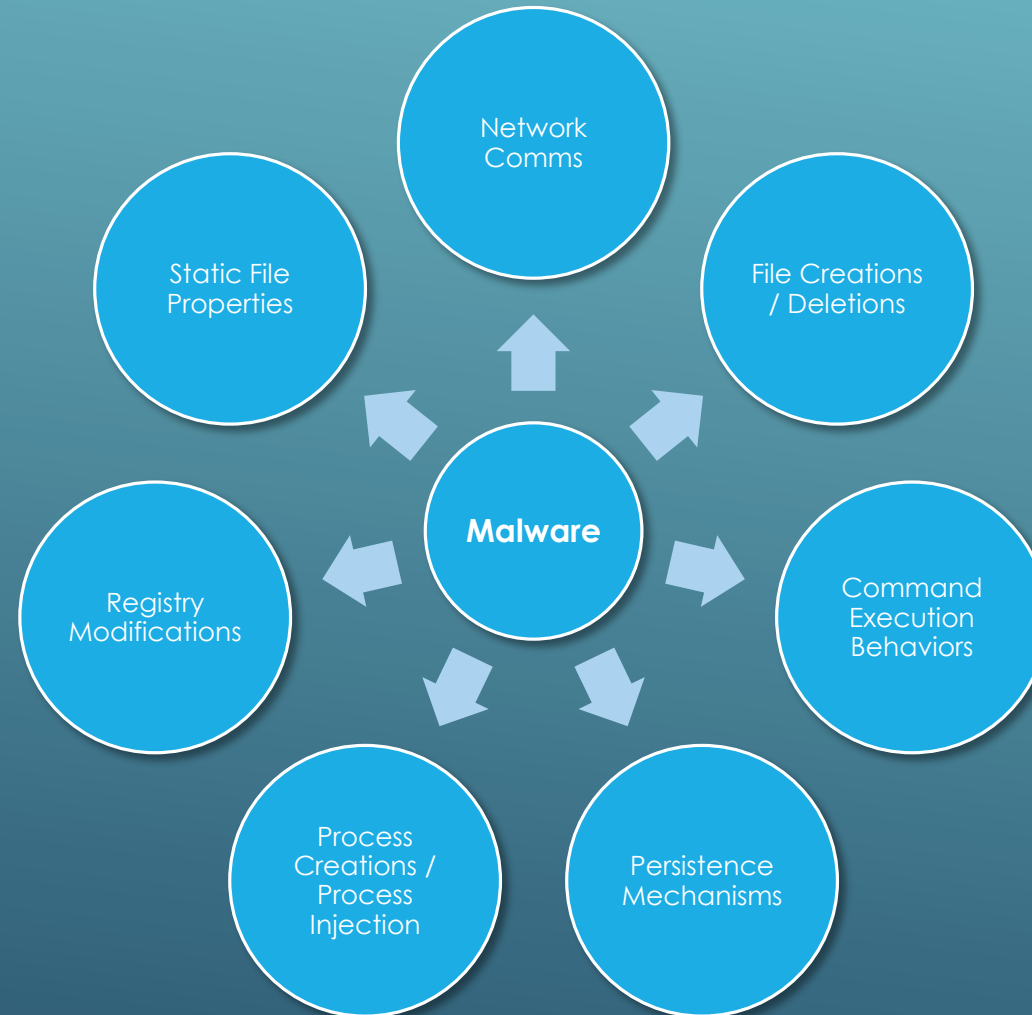
WHERE CAN I GET MALWARE?

- ▶ End-Users.
- ▶ Email gateway / email threat monitoring.
- ▶ Anti-virus.
- ▶ Endpoint detection & response (EDR).
- ▶ Network Threat Protection.
- ▶ External threat feeds and sharing partners.



Source: blackhillsinfosec.com

WHAT CAN I GET FROM MALWARE?



TYPICAL MALWARE ARCHITECTURE

Dropper

Responsible for downloading the next stages and payloads of the malware.

Payload

The “payload” is the malware’s main code and functionality. The payload is responsible for the primary behaviors and capabilities of the malware.

C&C

C&C (Command & Control) communication typically occurs after installation of the malware’s payload.

TYPICAL MALWARE ARCHITECTURE

Dropper

Droppers may utilize multiple techniques to download the next stages of the malware. (PowerShell, CMD.exe, WMI, WMIC, etc.)

Payload

The payload will likely attempt to establish persistence, escalate privileges, or a number of other actions.

C&C

The payload will likely attempt to establish contact to a C2.

HUNT & DETECTION USE-CASE (EXAMPLES)

Cobalt Strike Beacon (Example)

IcedID (Example)

Dropper

MS Office product **spawns rundll32.exe**, which attempts to **contact a domain** on the Internet.

MS Office document executes **Powershell** to invoke **mshta.exe** and download a file.

Payload

Once download, **payload is injected into rundll32.exe** process. Beacon establishes persistence via a **specific Scheduled Task**.

Payload is downloaded to "**C:\programfiles*.jpg**" and executed using **regsvr32.exe**.

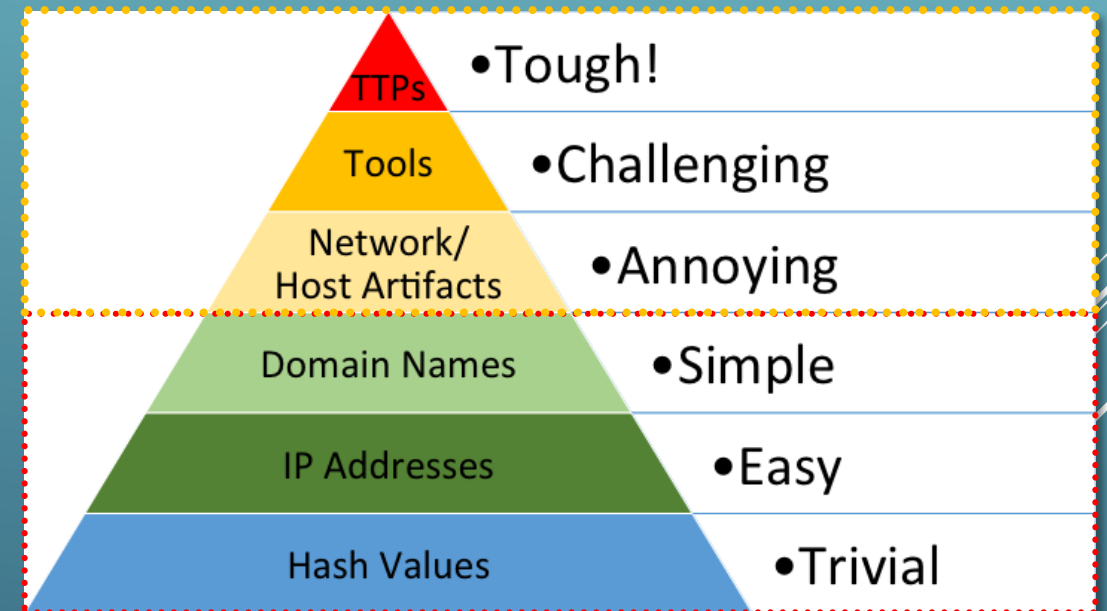
C&C

Payload attempts to **contact a specific domain** every **25 seconds**, using a specific **user agent**.

C2 communication:
<http://x.x.x.x/in.php/g=196A8&r=108..>

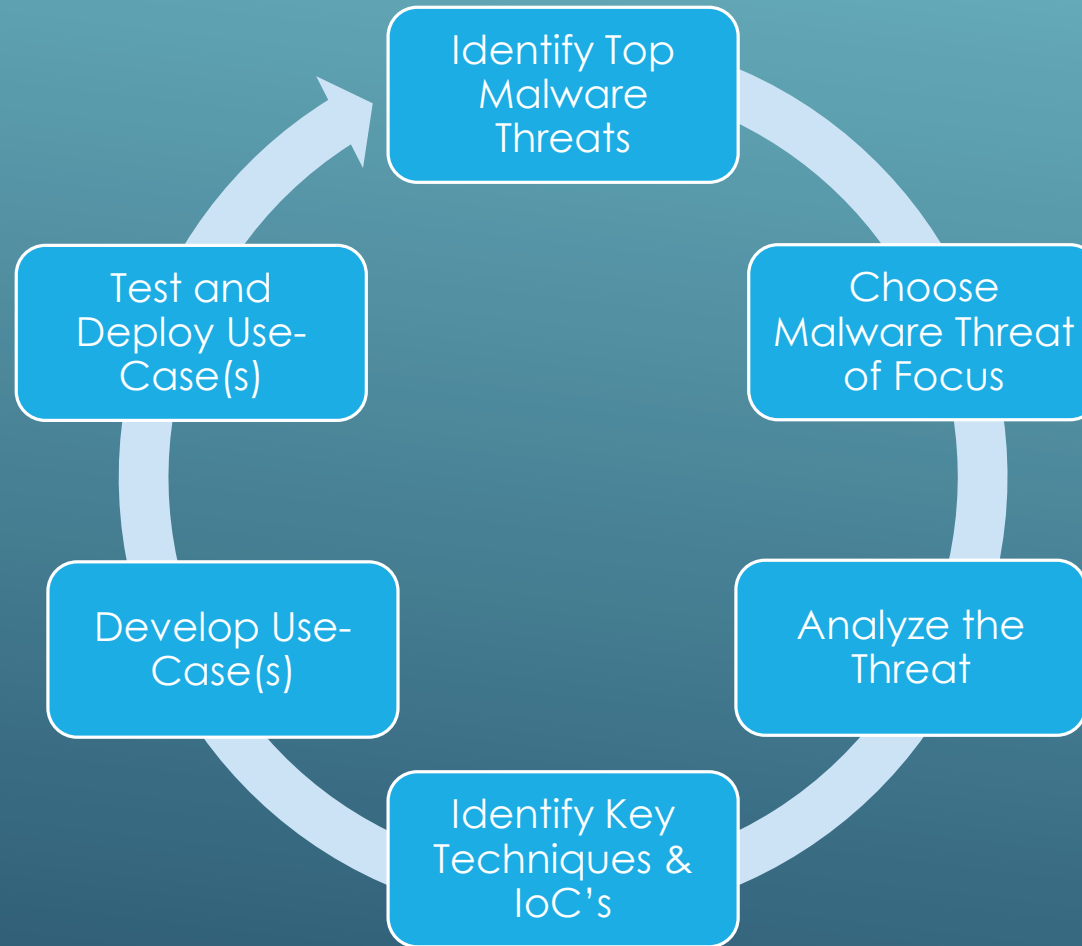
A NOTE ON IOC ABSTRACTION

- ▶ Focusing on concrete IOC's will likely result in high-accuracy, low FP's - but less findings.
- ▶ Focusing on abstract IoC's & techniques will likely result in more FP's - but more findings.
- ▶ Tip: Abstract your IoC's!
 - ▶ **Low Abstraction:**
„https://45.10.20.30/fre.php“
 - ▶ **Higher Abstraction:**
„*/fre.php“
 - ▶ **Even Higher Abstraction**
 - ▶ Beaconing intervals
 - ▶ PCAP data
 - ▶ User Agents...




Source: <https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

MALWARE ANALYSIS AND USE-CASE “LIFECYCLE”



CONCLUSION

1. Malware analysis can be a key input for your hunting and detection use-cases.
 2. Malware analysis can be used to help prioritize detection rules.
 3. Malware analysis should be used in conjunction with tools like MITRE ATT&CK.
 4. It does not take a full reverse-engineering team to start using malware analysis in your use-cases.
- 

QUESTIONS?



Contact: @d4rksystem <https://de.linkedin.com/in/kylecucci>