Welcome to

5. Malware and Incident Response

Introduction to Incident Response Elective, KEA

Henrik Kramselund he/him han/ham xhek@kea.dk @kramse

Slides are available as PDF, kramse@Codeberg https://codeberg.org/kramse/
5-Malware-and-Incident-Response.tex in the repo security-courses

Goals for today

- Finish part II of the book
  F3EAD process: Find, Fix Finish, Exploit, Analyze, Disseminate.
- Continue building your knowledge of basic and popular tools
- Talk about exam – so you know what to expect

Photo by Thomas Galler on Unsplash

Plan for today

- Look at a few more cases
- Find tools for helping during incident response
- Malware and Incident Response
- Go over chapters 8 and 9 from the book

Exercise theme:

- Loki - Simple IOC and YARA Scanner
  https://github.com/Neo23x0/Loki

Time schedule

- 1) Going over a few cases and Tool Loki scanner – 45min
- Break 15min
- 2) IDIR Chapter 8+9 – 2x45min
- 3) Plan your incident response, the mission and tools – 45min
- 4) Plan your incident response, processes 45min

So today we will go through the chapters 8 and 9

Time schedule

This day we will be doing a larger project, get started planning incident response

- 1) Going over a few cases – first 45min
- 2) Plan your incident response, the mission – 45 min
- Break 15min
- 3) Plan your incident response, tools – 45min
- 4) Plan your incident response, processes 45min

Times are suggested, in real life this process would take months!

Part 1: Cases

Goal is to find descriptions of specific malware

Search for IoCs and/or YARA rules

- Hashes
- Filenames specific for malware
- Yara rules for process memory
- C2 Back Connections – endpoints, IPs, domain names, host names, URLs

Part 2: Tools

We have talked about IoCs a few times, but lets dive deeper

There are many tools for different purposes, but they all have prerequisites, and very often you will need to modify the tools!

You can find lots of information about tools from books, and lists on the internet.

Many things are marked with forensics – and can be used during incident response.

- Awesome lists, like: https://github.com/meirwah/awesome-incident-response
- Sigma is another popular format: for more information see *Generic Signature Format for SIEM Systems* https://github.com/SigmaHQ/sigma

Exercise

Now lets do the exercise

⚠ Scan using Loki Simple IOC and YARA Scanner 45 min

which is number 23 in the exercise PDF.

Part 3: Reading Summary – IDIR chapter 8

Intelligence-Driven Incident Response (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781098120689

> The Analyze phase is where we take data and information and process it into intelligence. This chapter covers the basic principles of analysis, models such as target-centric and structured analysis, and processes to assign confidence levels and address cognitive biases.

- Chapter 8: Analyze

Analyze phase of F3EAD

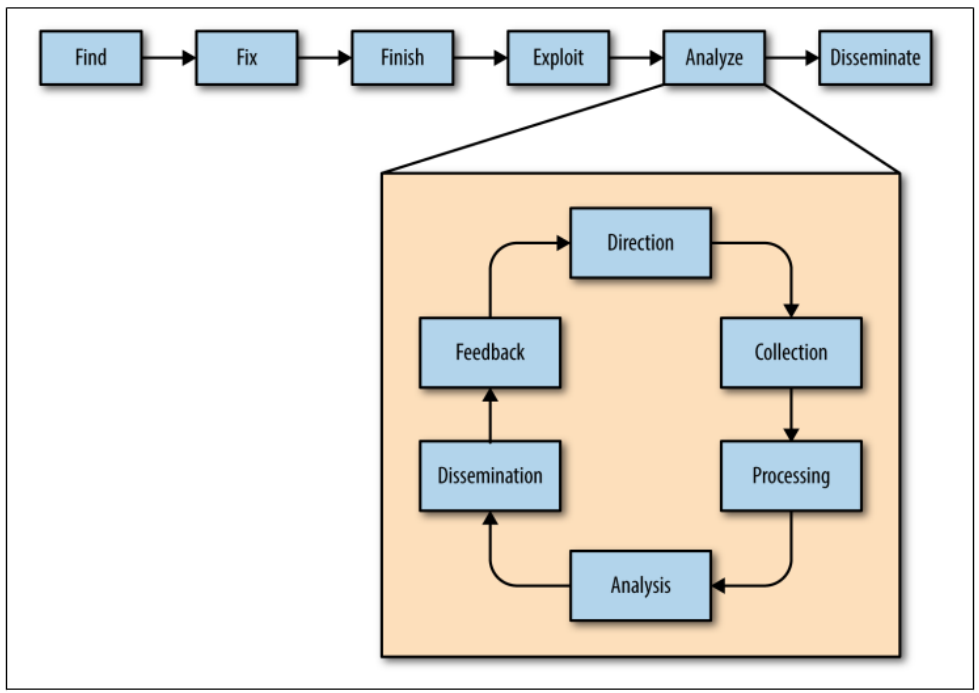


Figure 8-1. Analysis within F3EAD

Source: *Intelligence-Driven Incident Response* (IDIR)

Identify, analyze, predict

Rather than **only identifying** the technical details of the attack in order to respond and remediate, we can **analyze** those same domains and IPs to identify patterns that can be used to better **understand the attacker's tactics**. That involves gathering additional information about the domains and IPs, including who they were registered to and how the attacker used them, in order to determine whether **patterns** can be used to **identify or predict future behaviors**. This new information is then analyzed, intelligence gaps (critical pieces of information that are needed to conduct analysis) are identified, and more information is gathered as needed.

Source: *Intelligence-Driven Incident Response* (IDIR)

OPM

One of the most significant breaches in recent history is the breach of the United State's **Office of Personnel Management (OPM)**, which resulted in the loss of **personal, highly sensitive** information about more than **20 million individuals** who had undergone a **background investigation for a security clearance**. In addition to the size and sensitivity of the information that was stolen, the OPM breach is notable because of the **multiple, missed opportunities** for the attack to be **identified and prevented**. The intrusion was a complex campaign that spanned years and included the theft of IT manuals and network maps, the compromise of two contractors with access to OPM's networks, as well as OPM directly. Even when the individual intrusions were identified, no one connected the dots to identify that a larger threat needed to be addressed.

Source: *Intelligence-Driven Incident Response* (IDIR)

What to Analyze?

- Why were we targeted?
- Who attacked us?
- How could this have been prevented?
- How can this be detected?
- Are there any patterns or trends that can be identified?

  The **output of the analysis** that you conduct in this phase should **enable action**, whether that action is **updating a threat profile, patching systems, or creating rules for detection**.

Source: *Intelligence-Driven Incident Response* (IDIR)

Conducting the Analysis

Enriching Your Data

- Internet WHOIS information given as example
- DNS – passive DNS provides historical data
- Malware information – often Virus Total is mentioned
- Sharing groups – also add public blogs and sites like SANS Internet Storm Center https://isc.sans.edu/

Structured Analysis

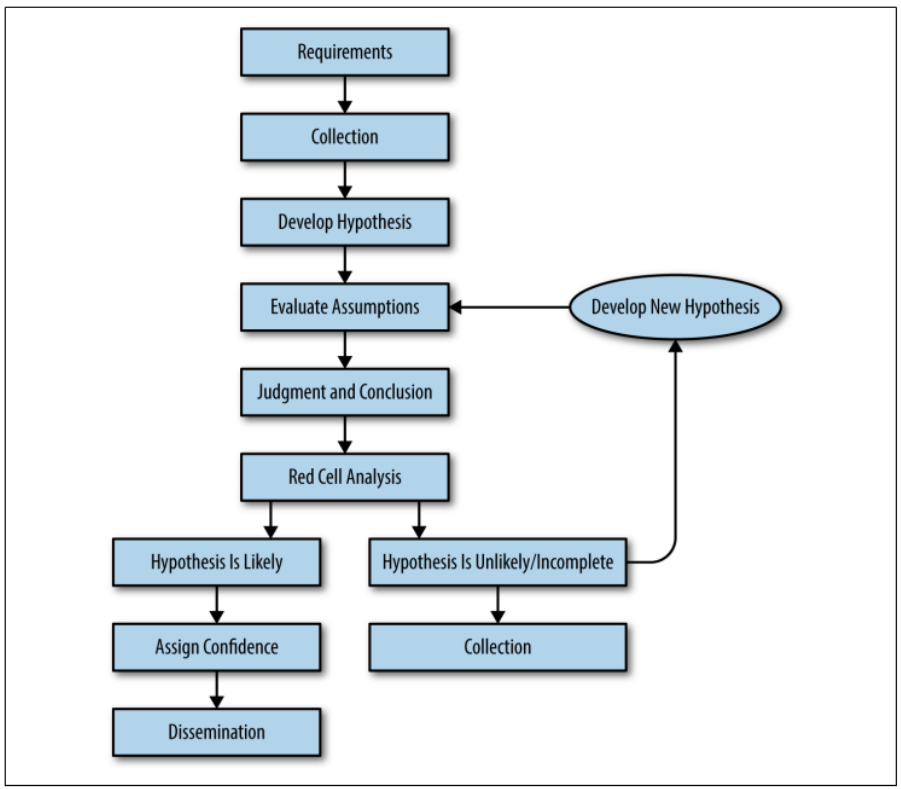
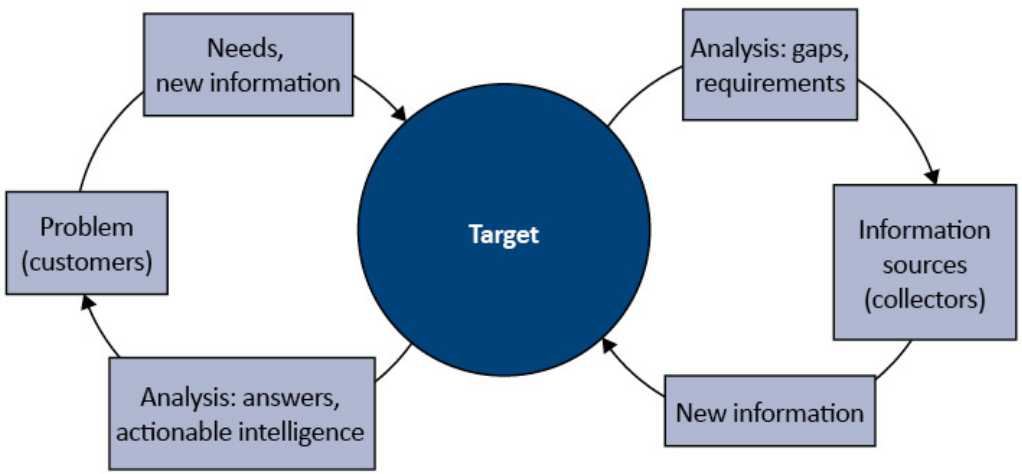


Figure 8-4. The structured analysis process.png

Target-centric intelligence analysis



In the book Intelligence Analysis, a Target-Centric Approach (CQ Press, 2003), Robert Clark describes the traditional intelligence cycle as an attempt to give a linear struc- ture to a decidedly nonlinear process, and introduces target-centric analysis as an alternative approach.

Part 4: Reading Summary – IDIR chapter 9

Intelligence-Driven Incident Response (IDIR) Scott Roberts. Rebekah Brown, ISBN: 9781098120689

> At some point, the investigation **needs to end, or at least pause**, long enough to create outputs useful to other teams or organizations. We call the process of organizing, publishing, and sharing developed **intelligence dissemination**. This is a skill set unto itself and, just like any other skill, has processes and takes time to develop. Good intelligence can be ruined by poor dissemination. Although writing up something after hours of analysis may seem unimportant, it's worth the time for any intelligence team to focus and build their skills disseminating information.

- Chapter 9: Disseminate

Focus on Writing and Disseminate

Dissemination is such an important skill that in larger intelligence teams, resources may be dedicated just to the dissemination phase. These dissemination-focused ana- lysts need the following:

A strong understanding of the overall process and importance of the information they're sharing.
A firm grasp of the types and needs of stakeholders that the intelligence will be going to.
A disciplined and clear writing style. (Intelligence writing is a little different from typical narrative writing; we'll get into that later in this chapter.)
An eye toward operational security to protect the valuable intelligence products and materials.

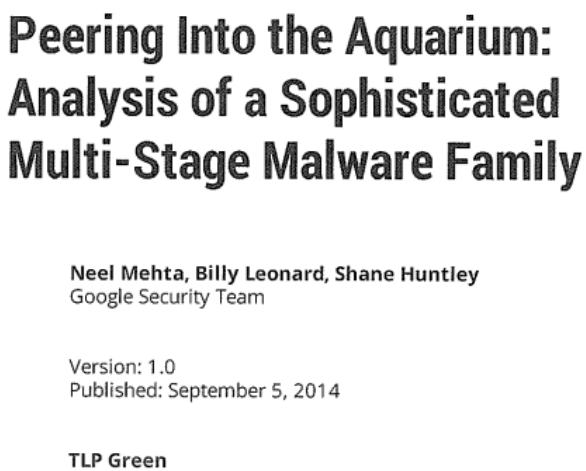
- Similarly an exploit without a *write-up* can seldomly be changed or added to

Intelligence Consumer Goals

Also known as consumers, the audience is tied directly into the goal of any intelligence product. The execution of the goal is intrinsically tied to the stakeholders you're writing a product for. Every intelligence writer and team must develop an understanding of the audience they're writing for, as this understanding leads directly to creating useful and actionable products. This is never a one-time exercise, as teams you're writing for change, evolve, and learn.

- Audience – stakeholders, CEO, board of directors, your boss?
- Internal Technical Consumers – SOC analysts, incident responders, cyber threat intelligence analysts, etc.
- External Technical Consumers – book PDF links to article about Google's *Looking into the Aquarium report*
  https://www.vice.com/en/article/3djn9y/a-glimpse-into-how-much-google-knows-about-russian-government-hackers
  https://s3.documentcloud.org/documents/3461560/Google-Aquarium-Clean.pdf

Pause – lets browse this report



Peering Into the Aquarium:
Analysis of a Sophisticated
Multi-Stage Malware Family

Neel Mehta, Billy Leonard, Shane Huntley
Google Security Team

Version: 1.0
Published: September 5, 2014

TLP Green

https://s3.documentcloud.org/documents/3461560/Google-Aquarium-Clean.pdf

- You would not be expected to produce this kind of report immediately, but use it for inspiration
- Book also spend some time discussing *report writing* and have examples

Disseminate Conclusion

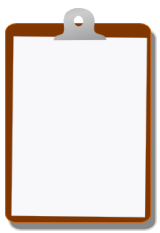
Great intelligence products generally have the following characteristics:

- Accuracy
- Audience focused
- Actionable

In addition, analysts should ask themselves the following five questions during the writing process to ensure that the intelligence products that they develop will be well received and will meet the needs of their intelligence customers:

- What is the goal?
- Who is the audience?
- What is the proper length of product?
- What level of intelligence? (Tactical, operational, strategic?)
- What tone and type of language can you use? (Technical or nontechnical?)

For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools

Read the books! Play with tools