OVERVIEW OF FORENSIC METODOLOGHY

FOR APPROACHING FORENSICS

tes
texto.texto@proton.me
July 2024

AGENDA | 3 SESSIONS

Pre-assessment:

1. Core key questions
2. Contextual assessment, Vetting & Consent collection
3. Documentation
4. Preparation (lab, tools)

Assessment:

1. Data Acquisition
2. Forensics Analysis

Post-assessment:

1. Communication
2. Output of analysis (Report)
3. Follow-up (recommended actions and support)
4. Lessons learned

REFERENCES

Built on top of other organizations/individuals efforts:

Trainings:

- Digital Forensics Fellowship from Amnesty International
- Digital Defenders workshop on Forensics (Jacobo Najera & Marla)

Online resources:

- Guide to forensics Security Without borders | Garnieri & Etienne (https://github.com/securitywithoutborders)

Tools development:

- MVT project (https://github.com/mvt-project)

& personal perspective of field work

DEFINITIONS

Forensics:

The use of methods and techniques to investigate and analyze data for a variety of purposes such as legal, humanitarian, and accountability.

Analysis of indicators left behind, looking for signs of compromise.

Investigating events that occur in a digital environment (...) you look for artifacts that suspected software or users might have introduced into the digital environment and try to determine how the digital environment changed in response to those artifacts.

Source: The Art of Memory Forensics by Hale.

APPROACH

Forensics from a Civic Society Organizations perspective

- consensual
- respectful
- specific objectives

Constrains to consensual forensics

- lack of literature, body of knowledge, specific tools
- technical limitations
- do not harm
- state of device

APPROACH

Exploratory approach

- Ongoing field of research
  - Literature review
  - Specific tools
- Each case has own caveats
- Very specific use case, technology dependent
- Technology changes rapidly
- The importance of understanding how "expected behavior" looks like

BEFORE THE ASSESSMENT

CORE QUESTIONS

Who are we?

- Are we part of a helpline in the front line?
- Are the initial triaging team of a multi-layer assessment?
- Are we a technical team aiming to conduct a more in depth-research?
- Are we the ones taking the samples and talking with a trusted partner that will conduct the technical analysis?
- Are we part of an internal team to check organization phones? Or wiling to learn how to conduct forensics for creating a threat lab?
- Are we self-learning with peers analyzing own phones?

BEFORE THE ASSESSMENT

CORE QUESTIONS

Why are we conducting this analysis/research/taking case? What is our aim?

- to identify if device is infected with spyware/stalkerware?
- to identify a known malicious indicator or any suspicious activity?
- to conduct technical/techno-political research?
- to gather evidence to be used in court?
- to do an initial triage just to clean a device?

* May change in the middle ...

BEFORE THE ASSESSMENT

CORE QUESTIONS

What is the expected outcome of our assessment?

- a yes/no/maybe answer regarding device being infected?
- an attributed attack by a malicious identifiable actor?
- a set of good practices surrounding device & accounts security?
- a report? a technical report? a threat intelligence report?
- a regional landscape of spyware?
- a policy to demand accountability?
- a set of evidence to be presented at court?
- a clean device?
- to build documentation, new tools, new approaches

* Expected for whom? Expectations need to be addressed

BEFORE THE ASSESSMENT

CORE QUESTIONS

What are our resources?

- How much time can we allocate?
- Do we need an interdisciplinary team? Do we need technologist? Do we have those peers in the team? Are we working with trusted partners?
- What are our time constrains? Can we allocate time for learning?
- What are our budget constrains? Can we "afford" tools/training/HW?

BEFORE THE ASSESSMENT

CORE QUESTIONS

What types of cases we will be receiving?

- Advanced attacks (0-click):
  a. no interaction
  b. several stages
     Remote Code Execution (RCE) ->
     Memory disclosure ->
     Elevation of privilege (sandbox escape) ->
     (Persistence)

BEFORE THE ASSESSMENT

CORE QUESTIONS

What types of cases we will be receiving?

- "1-click" attacks
  a. clicking on a link that infects device
  b. execute malicious program
  c. install malicious app
  d. enabling macros on malicious document

BEFORE THE ASSESSMENT

CORE QUESTIONS

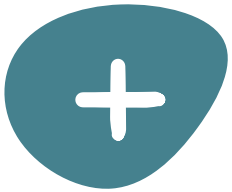
What types of cases we will be receiving?

Different threat scenarios:

- Targeted vs Non-targeted (cybercrime)
- Physical access (stalkerware, seizure) vs Remote
- Different by region

For each type of attack we need to look for different artifacts

- Advance attacks -> File traces, kernel panics ...?
- 1-clicks attacks
  -> Navigation. URLs in SMS.
  -> Malicious apps: source of installation, permissions, behavior
  -> Malicious programs / documents



BEFORE THE ASSESSMENT

CORE QUESTIONS

When we receive a case, what do we have in front of us?

- A (possibly) targeted mobile phone? Android/iOS?
- A (possibly) infected machine? MacO$, GNU/Linux or Window$?
- A (possibly) malicious email?
- A (possibly) malicious document?
- A (possibly) malicious binary?
- A (possibly) malicious infrastructure?

Plan accordingly:

- Methodology & lab (tools/cables/space)
- Documentation strategy (reproducible/peer review)
- Know to what trusted partners you can reach out

BEFORE THE ASSESSMENT

INITIAL TRIAGE

a. Contextual assessment

b. Vetting

c. Gather contextual facts

- what raised suspicious
- timeframe

d. Risk analysis

BEFORE THE ASSESSMENT

INITIAL TRIAGE

d. Explain the process

- with no technicalities
- open the door to opt-out anytime
- be clear on private information being gathered
- data/device handling policies. Destruction policies
- manage expectations

e. Consent collection

f. Understand future intentions (trial evidence / media outreach)