Incident Response Lab

Participant Guide — AlertOverload Security Labs

Scenario

An employee at Bajiri Corp has logged into their computer and found that none of their files can open and that there is a ransom note on the desktop. The IT team was able to scope out the incident to the device and has taken a memory capture, used KAPE to gather evidence, and has also provided the Elastic logs for what they believe is the incident scope.

Bajiri Corp has hired the AlertOverload incident response team to work this incident and determine the full scope and impact. They have provided a list of questions that they would like answered about the incident.

Engagement Rules

- **Stay in scope.** Only analyze the provided artifacts. Do not attempt to reach out to, connect to, or interact with any external infrastructure referenced in the logs or artifacts. Most of it will be disabled anyway.
- **Document your methodology.** For open-ended questions, the *how* matters as much as the *what*. Record your steps as you go. The best reference is your own experience, documented in real time.
- **If you find malware, do not attempt to analyze it without using a VM.** These are real payloads that take destructive actions. *I will be unable to assist you if you ransom your device.*
- **Ask questions.** I'll be available to help throughout the lab. Working with your peers is also encouraged — incident response is a team effort.

Environment

Victim Devices

Hostname	Role
DESKTOP-V924VDR	Victimized endpoint — Windows 10, domain-joined
WIN-64NSQJJ63B8	Domain controller

Victim User

User	Notes
sgonk@corp.bajiri.com	The compromised user account

Ransom Note

```
You've been hacked!

MESS WITH THE BEST,
DIE LIKE THE REST

Bajiri
```

Artifacts

You have been provided with the following artifacts. Access details will be provided by the instructor.

Artifact	Description	Access
ELK Logs	Elastic logs covering the incident scope from both victim devices	Kibana — credentials on whiteboard
KAPE Output	Triage collection from DESKTOP-V924VDR, parsed with EZParser	Download link provided
Memory Capture	Full physical memory image captured from DESKTOP-V924VDR post-incident	Download link provided

> *Note: The Kibana time filter has been pre-scoped to the incident window. If you are seeing no results, verify the time range before assuming data is missing.*

Recommended Tools

You may use any tools you are comfortable with. The following are recommended based on the artifacts provided.

Memory Analysis

- **Volatility** — primary tool for memory analysis. Plugins of interest include `pslist`, `cmdline`, `netscan`, `malfind`, and `dumpfiles`.

Artifact Parsing & Review

- **Eric Zimmerman's Tools (EZ Tools)** — strongly recommended for parsing KAPE output.
  - **Timeline Explorer** — navigate EZParser CSV output, MFT, and UsnJrnl
  - **PECmd** — prefetch analysis and execution artifacts
  - **AmcacheParser** — binary execution evidence
  - **AppCompatCacheParser** — ShimCache execution entries
  - **EvtxECmd** — event log parsing
  - **MFTECmd** — Master File Table analysis
  - **RECmd** — registry analysis

Note: Eric Zimmerman's tools are Windows-only. Linux and Mac users can use Volatility for memory analysis but will need a Windows VM or alternative tools for artifact parsing.

Note: Use the .NET 6 versions of EZ Tools where available. They are faster and more actively maintained.

Log Analysis

- **Kibana** — pre-configured with the incident log data. Familiarity with KQL is helpful but not required.

Deliverables

Answer each question below as thoroughly as you can. For open-ended and short-answer questions:

- Describe the artifact or evidence you found
- Explain how you found it — what tool, what query, what process
- Provide the relevant file path, timestamp, log entry, or value where applicable

Some questions will be short answer, some will require longer answers with log excerpts. The questions are designed around real incident response reports, processes, and procedures. While not equivalent to a full incident response report, the questions are designed in a way that enables a functional report to be written.

Questions

Section 1: Scoping the Incident

1. What is the hostname of the victim device?

2. What is the full username and domain of the compromised user?

3. What is the operating system version of the victimized endpoint?

4. What are the IP addresses of the impacted systems?

5. What is the Security Identifier (SID) of the compromised account? How is tracking the SID useful during an investigation?

6. What is the time range of the ELK collection? What does this tell you about the incident?

Section 2: Initial Access

1. Where on the filesystem is the PowerShell console history file stored? Under which user profile was it found?

2. What was the exact command the victim executed that initiated the compromise? Provide the full command line.

3. What domain was referenced in that command, and what does it tell you about the lure technique used?

4. What was the remote access tool found running on the compromised endpoint?

5. Which version of the remote access tool was used?

6. Where on the filesystem was the remote access tool installed?

7. How was the remote access tool installed, and what technique was used to install it?

8. What external IP did the tool connect to? What port was used?

9. When was the first observed network connection from the remote access tool? Provide the timestamp.

10. What Windows Security event code is associated with logon activity? Were there events with that ID associated with the remote access tool?

Section 3: Discovery and Enumeration

1. What command was most commonly used to enumerate the machine? Is this a CMD or PowerShell command? What is it used for?

2. Which process spawned the command execution? List the process name and ID.

3. How many times was the command executed within the incident time range?

4. Were any other user accounts accessed or browsed to during the incident? What artifact revealed this?

5. Which Sysmon event ID corresponds to process creation events? Which fields in the Sysmon log are most useful when examining process activity?

6. What was the process ID of the remote access tool? How does tracking the process ID help you reconstruct threat activity across an incident?

Section 4: Remote Control and Lateral Movement

1. A second remote access-related process was observed. What is the name of the tool, and why do you think it was deployed?

2. Which version of this tool was used? How many times was the installer executed, and what does that tell you about the deployment process?

3. A network logon event was recorded for the compromised user on the domain controller. Provide the timestamp and event ID.

4. Based on the combination of the remote access tools and the domain controller logon activity, construct a hypothesis about the attacker's goals during this phase of the incident.

Section 5: Filesystem and Artifact Analysis

1. What is the MFT, and what does it tell you about the filesystem?

2. What is the UsnJrnl ($J), and what can be identified from it?

3. Where on the filesystem was the ransomware deployed? When was it placed there?

4. What was the exact time range of the ransomware execution based on the filesystem artifacts?

5. What were the contents of the compromised user's Recent Items? Which entries are significant to the investigation and why?

6. Retrieve each stage of the loader from the available artifacts. How does the staging chain work?

Section 6: Impact

1. The victim reported they could not open their files and found a ransom note on the desktop. Based on your artifact review, what is the name and full path of the ransom note?

2. Identify the ransomware executable name. What artifact source confirmed this?

3. Is it possible to extract the ransomware payload from the memory capture? What information can you recover without executing it?

Section 7: Analysis and Synthesis

1. What Sysmon event ID corresponds to network connection events? Which ID corresponds to DNS events? How were these events useful during your analysis?

2. Construct a timeline of events from the first observed activity to the last. Include timestamps for each significant event.

3. What misconfigurations or actions taken before or during the incident allowed the malware to run undetected? Who was responsible for each?

4. How do the KAPE artifacts compare to the ELK logs in terms of what each source reveals? Where do they overlap, and where does each fill a gap the other cannot?

5. Was there any evidence of file exfiltration? What artifact sources did you use to assess this, and what was your conclusion?

6. What was the dwell time of the attacker in this incident?

7. Which log source was the most useful during your analysis, and why?

8. One of the remote access tools used in this incident is a legitimate remote administration tool. What challenges does this present for defenders, and why would an attacker choose to use legitimate software in a compromise?

9. Identify at least three detection opportunities present in the artifacts that, if alerted on, could have shortened the attacker's dwell time. For each, describe the artifact, the alert logic, and the phase of the attack it would have interrupted.

10. Write a brief incident summary using your timeline as a foundation. Write for an executive audience — no technical jargon.

Schedule

Refer to the whiteboard for today's schedule. Times are approximate and subject to adjustment.
