Laboratory #5

Security Operations Centre (SOC)

Operation ShadowNet: *Rapid Response*

Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

This page is intentionally blank

Operation ShadowNet: Rapid Response

1 Scenario

A mid-sized e-commerce company, "*GlobalGadgets*," has detected a ransomware attack. A critical web server is showing signs of encryption, and a single, suspicious outbound network connection has been identified.

2 Objectives

- Rapidly identify the scope of the ransomware attack.
- Isolate the affected server.
- Identify the malicious network connection.
- Document key findings and actions.

3 Roles and Responsibilities

- **Incident Commander**
  - Directs the response and makes key decisions.
  - Tracks progress and time.
- **Network/Log Analyst**
  - Analyse provided logs and network data.
  - Identify the malicious IP and the affected server.
- **Endpoint/Forensics Analyst**
  - Focus on the webserver, and quickly identify the processes encrypting files.
  - Isolate the infected webserver.

4 Communication/Documentation

- Log key findings.
- Document isolation steps.
- Communicate findings to the Incident commander.

5 Exercise Materials (Simplified):

5.1 A short, focused log file (e.g., web server access logs)

```
Timestamp,Source IP,Destination IP,Port,Protocol,Action,User Agent,URI 2025-03-25
10:00:01,192.168.1.10,192.168.1.50,80,TCP,ALLOW,Mozilla/5.0, /index.html 2025-03-25
10:00:05,192.168.1.10,192.168.1.50,80,TCP,ALLOW,Mozilla/5.0, /products.html 2025-03-
25 10:01:12,192.168.1.10,192.168.1.50,80,TCP,ALLOW,Mozilla/5.0, /order.php 2025-03-25
10:02:30,192.168.1.10,192.168.1.50,80,TCP,ALLOW,Mozilla/5.0, /image.jpg 2025-03-25
10:03:45,192.168.1.10,192.168.1.50,80,TCP,ALLOW,Mozilla/5.0, /admin/login.php 2025-
03-25 10:04:15,192.168.1.10,192.168.1.50,80,TCP,ALLOW,Mozilla/5.0,
/admin/dashboard.php 2025-03-25
10:05:22,192.168.1.10,192.168.1.50,443,TCP,ALLOW,Mozilla/5.0, /api/upload.php 2025-
03-25 10:06:00,192.168.1.10,192.168.1.50,443,TCP,ALLOW,Mozilla/5.0, /api/process.php
2025-03-25 10:07:18,192.168.1.10,192.168.1.50,443,TCP,ALLOW,Mozilla/5.0,
/api/download.php 2025-03-25
10:08:35,192.168.1.10,192.168.1.50,443,TCP,ALLOW,Mozilla/5.0, /api/encrypt.php 2025-
03-25 10:09:10,192.168.1.10,192.168.1.50,443,TCP,ALLOW,Mozilla/5.0, /api/encrypt.php
2025-03-25 10:09:45,192.168.1.10,192.168.1.50,443,TCP,ALLOW,Mozilla/5.0,
/api/encrypt.php 2025-03-25
10:10:00,192.168.1.10,192.168.1.50,443,TCP,ALLOW,Mozilla/5.0, /api/encrypt.php 2025-
03-25 10:10:15,192.168.1.10,192.168.1.50,443,TCP,ALLOW,Mozilla/5.0, /api/encrypt.php
2025-03-25 10:10:30,192.168.1.10,192.168.1.50,443,TCP,ALLOW,Mozilla/5.0,
/api/encrypt.php 2025-03-25
10:11:00,192.168.1.50,198.51.100.10,5555,TCP,ALLOW,Unknown, -
```

Explanation and Points of Interest:

- **192.168.1.50:** This is the web server.
- **192.168.1.10:** This is a client accessing the web server.
- **198.51.100.10:** This is the malicious external IP.
- **Port 443:** HTTPS traffic, potentially hiding malicious activity.
- **/api/encrypt.php:** This URI is highly suspicious, indicating a possible encryption routine.
- **5555:** An unusual high port, potentially used for command-and-control.
- **"Unknown" User Agent and "-":** This is unusual, and could be an indicator of malicious traffic.
- The repetitive nature of the encrypt.php calls is a huge red flag.

How to Use It:

- This log file provides a clear timeline of events.
- Students should quickly identify the suspicious `/api/encrypt.php` calls and the unusual outbound connection to `198.51.100.10:5555`.
- This quickly shows the webserver (192.168.1.50) is compromised, and is reaching out to a suspicious external IP.
- This log is short and focused, allowing for rapid analysis in the limited time.

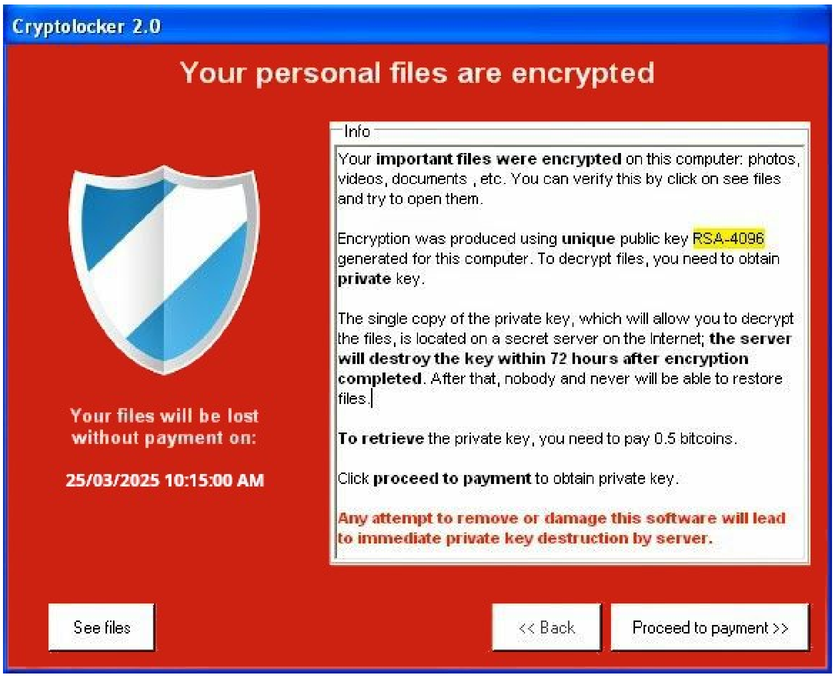
5.2 A single network connection log showing the malicious outbound connection.

```
Timestamp,Source IP,Source Port,Destination IP,Destination Port,Protocol,Bytes
Sent,Bytes Received,Connection State 2025-03-25
09:55:00,192.168.1.100,54321,192.168.1.1,80,TCP,1024,512,ESTABLISHED 2025-03-25
09:56:15,192.168.1.101,55678,192.168.1.10,22,TCP,256,128,ESTABLISHED 2025-03-25
09:57:30,192.168.1.102,56789,192.168.1.20,53,UDP,64,64,ESTABLISHED 2025-03-25
09:58:45,192.168.1.103,57890,192.168.1.30,80,TCP,2048,1024,ESTABLISHED 2025-03-25
09:59:00,192.168.1.104,58901,192.168.1.40,443,TCP,4096,2048,ESTABLISHED 2025-03-25
10:00:00,192.168.1.105,59012,192.168.1.50,80,TCP,512,256,ESTABLISHED 2025-03-25
10:01:15,192.168.1.106,60123,192.168.1.60,22,TCP,128,64,ESTABLISHED 2025-03-25
10:02:30,192.168.1.107,61234,192.168.1.70,53,UDP,64,64,ESTABLISHED 2025-03-25
10:03:45,192.168.1.108,62345,192.168.1.80,80,TCP,1024,512,ESTABLISHED 2025-03-25
10:04:00,192.168.1.109,63456,192.168.1.90,443,TCP,2048,1024,ESTABLISHED 2025-03-25
10:05:15,192.168.1.110,64567,192.168.1.100,80,TCP,512,256,ESTABLISHED 2025-03-25
10:06:30,192.168.1.111,65678,192.168.1.110,22,TCP,128,64,ESTABLISHED 2025-03-25
10:07:45,192.168.1.112,66789,192.168.1.120,53,UDP,64,64,ESTABLISHED 2025-03-25
10:08:00,192.168.1.113,67890,192.168.1.130,80,TCP,1024,512,ESTABLISHED 2025-03-25
10:09:15,192.168.1.114,68901,192.168.1.140,443,TCP,2048,1024,ESTABLISHED 2025-03-25
10:10:30,192.168.1.115,69012,192.168.1.150,80,TCP,512,256,ESTABLISHED 2025-03-25
10:11:00,192.168.1.50,49512,198.51.100.10,5555,TCP,1280,64,ESTABLISHED 2025-03-25
10:12:15,192.168.1.116,70123,192.168.1.160,22,TCP,128,64,ESTABLISHED 2025-03-25
10:13:30,192.168.1.117,71234,192.168.1.170,53,UDP,64,64,ESTABLISHED 2025-03-25
10:14:45,192.168.1.118,72345,192.168.1.180,80,TCP,1024,512,ESTABLISHED
```

Explanation:

- **Timestamp:** 2025-03-25 10:11:00 - Correlates with the suspicious activity in the web server logs.
- **Source IP:** 192.168.1.50 - The compromised web server.
- **Source Port:** 49512 - A high, ephemeral port.
- **Destination IP:** 198.51.100.10 - The malicious external IP.
- **Destination Port:** 5555 - An unusual high port, often used for custom applications or malicious traffic.
- **Protocol:** TCP - A reliable connection protocol.
- **Bytes Sent/Received:** Indicates data transfer, confirming communication.
- **Connection State:** ESTABLISHED - Confirms an active connection.

5.3 A screenshot of the affected web server showing encrypted files.



Your personal files are encrypted

Your files will be lost without payment on:

25/03/2025 10:15:00 AM

Info

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

Figure 1: Screenshot of Affected Server

- **File extensions:** Encrypted files often have extensions appended by the ransomware (e.g., ".locked", ".encrypted", ".[ransomware name]").
- **File icons:** Encrypted files might have different icons than normal files.
- **File sizes:** Encrypted files might have unexpected sizes.
- **Ransom note:** A text file might be present with instructions from the attackers.

5.4 A simplified network diagram showing the webserver

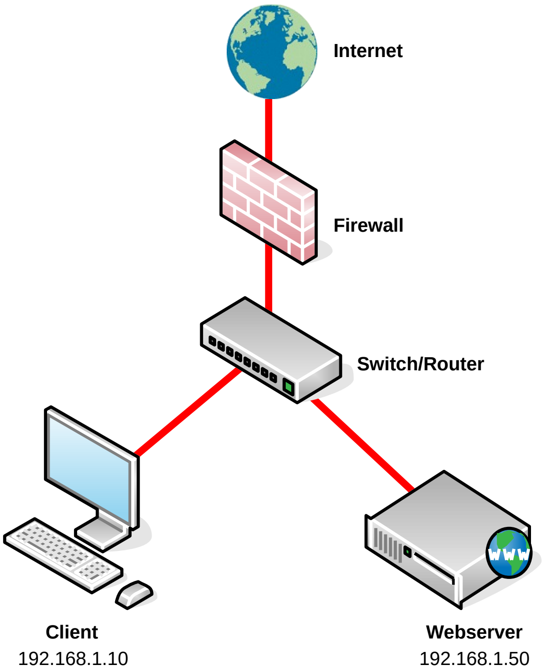


Figure 2: Network Diagram

Explanation:

- **Internet:** Represents the external network.
- **Firewall:** The security boundary between the internal and external networks.
- **Switch/Router:** The network device that connects the internal devices.
- **Client (192.168.1.10):** A typical user on the internal network.
- **Web Server (192.168.1.50):** The target of the ransomware attack.

5.5 A simple incident log template

Incident Log

Incident ID: SHADOWNET-20231027-001

Date: 2025-03-25

Time: 10:15 UTC

Reported By: Automated Alert System

1. **Initial Report**
   - **10:15 UTC:** Automated alert triggered by unusual network traffic and file system modifications on web server 192.168.1.50.
   - **Alert details:** High CPU utilisation, encrypted file extensions detected, outbound connection to 198.51.100.10:5555.

2. **Triage and Analysis (10:15 - 10:30 UTC)**
   - **10:16 UTC:** Incident Commander assigned roles to Network/Log Analysts, Endpoint/Forensics Analysts, and Communication/Documentation team.
   - **10:20 UTC:** Network/Log Analysts confirmed outbound connection to 198.51.100.10:5555, TCP, established state.
   - **10:25 UTC:** Endpoint/Forensics Analysts confirmed file encryption on 192.168.1.50, /api/encrypt.php identified in web server logs as source of encryption.
   - **10:28 UTC:** Network/Log Analysts confirmed malicious IP address is not within internal network range.

3. **Containment (10:30 - 10:50 UTC)**
   - **10:32 UTC:** Endpoint/Forensics Analysts initiated isolation of web server 192.168.1.50 from the network.
   - **10:35 UTC:** Firewall rules updated to block all traffic to/from 198.51.100.10.
   - **10:40 UTC:** Communication/Documentation team began compiling incident report and communication log.
   - **10:45 UTC:** Verified network isolation of web server 192.168.1.50.

4. **Key Findings (10:50 - 11:00 UTC)**
   - Ransomware infection confirmed on web server 192.168.1.50.
   - Malicious external IP: 198.51.100.10, port 5555.
   - Encryption initiated via /api/encrypt.php script.

- Webserver network traffic was reaching out to the malicious external IP.

5. **Actions Taken**

- Web server 192.168.1.50 isolated from the network.
- Firewall rules implemented to block malicious IP 198.51.100.10.
- Incident documentation initiated.

6. **Next Steps**

- Forensic analysis of affected web server.
- Ransomware identification and analysis.
- Data recovery planning.
- Post-incident review and lessons learned.

7. **Communication Log**

- **10:20 UTC:** Internal SOC channel: "Suspicious outbound connection detected from web server."
- **10:35 UTC:** Internal SOC channel: "Firewall rules updated to block malicious IP."
- **10:55 UTC:** Incident Commander to SOC Team: "Incident summary being compiled."

8. **Attachments**

- Web server access logs (excerpt).
- Network connection logs (excerpt).
- Screenshot of encrypted files.
- Network diagram.

6 Key Points for the Exercise

- This diagram clearly shows the web server's position in the network.
- Students can quickly understand the potential impact of a compromise on the web server.
- The diagram is simple, and easily understood, which is important for the time constraints of the exercise.
- The diagram shows the clear path that the malicious traffic took, from the internet, through the firewall, to the webserver.

7 Who/what generates the Incident Log in the SOC

The incident log is typically a combination of both human input and machine-generated data. It's not exclusively one or the other. Here's a breakdown:

1. Human Input:

- **Analyst Notes:** SOC analysts are responsible for documenting their observations, actions, and decisions. This includes:
  - Timelines of events.
  - Analysis findings.
  - Communication logs.
  - Rationale for actions taken.
  - Lessons learned.
- **Manual Data Entry:** Some information might need to be manually entered into the incident management system, such as:
  - Contact information for affected parties.
  - Descriptions of unusual behaviour.
  - Summaries of conversations.

2. Machine-Generated Data:

- **Security Information and Event Management (SIEM) Systems:** These systems automatically collect and aggregate logs from various sources (firewalls, IDS/IPS, servers, etc.). They can:
  - Generate alerts based on predefined rules.
  - Record timestamps and source/destination IPs.
  - Correlate events and identify patterns.
- **Endpoint Detection and Response (EDR) Tools:** These tools provide detailed information about endpoint activity, including:
  - Process execution.
  - File modifications.
  - Network connections.
- **Automated Logging:** Many systems and applications automatically generate logs that are captured by the incident management system.
- **Ticketing Systems:** These systems often automatically record actions performed on tickets, and time stamps.

In Summary:

- A modern SOC uses a blend of both. Machines provide the raw data, and humans provide the context, analysis, and decision-making.
- It is very important that a human reviews the machine data, to avoid false positives, and to add context.
- Incident management systems are designed to facilitate this combination, allowing analysts to easily add their notes and annotations to machine-generated logs.

In essence, machines provide the raw material, and humans craft the narrative.

8 Exercise Phases

8.1 Rapid Triage and Identification

- Incident Commander distributes materials and assigns roles.
- Teams quickly analyse the provided data.
- Identify the affected web server and the malicious IP address.

8.2 Immediate Containment

- Endpoint/Forensics Analysts isolate the affected web server (simulated).
- Network/Log Analysts confirm the malicious IP address.
- Communication/Documentation team logs all actions.

8.3 Key Findings and Documentation

- Teams consolidate their findings.
- Communication/Documentation team prepares a brief incident summary.
- Incident Commander reports on the key findings and containment steps.

9 Exercise Execution

9.1 Briefing

- Quickly introduce the scenario and objectives.
- Assign roles and distribute materials.

9.2 Execution

- Students work rapidly to analyse data and take action.
- Facilitator provides minimal guidance, emphasising speed.

9.3 Debriefing

- Briefly review the team's actions and findings.
- Discuss the importance of rapid response.