Individual Contribution Report

Name: RIZAL NANDANA ARYA GUNA
Student ID: 225150207111039
Group: Kelompok 3 nasibubu_fordig
Case: CASE BASE 2 MALWARE ANALYSIS
Date: 29/11/2025

---

1. My Role in the Team

Primary Role: Technical Analyst

Responsibilities:

Static Analysis

---

2. Tasks Completed

Week 1: Setup & Initial Analysis

- ☐ Task 1:Menyiapkan lingkungan analisis (VM Windows + isolasi jaringan) serta mengimpor sampel malware `c91267…68027.exe`.

    - Time spent: 3 jam
    - Output: Lingkungan analisis siap digunakan dan sampel malware berhasil diverifikasi integritasnya melalui hashing SHA-256.

- ☐ Task 2: Mengidentifikasi tipe file dan struktur PE menggunakan tool statis.

    - Time spent: 2 jam
    - Output: File terklasifikasi sebagai PE32 Executable (.NET) dan karakteristik dasar file terdokumentasi pada bagian Static Analysis Report.

Week 2: Deep Analysis

- ☐ Task 3: Melakukan deteksi packer dan obfuscation pada file sample.

- Time spent: 1 jam
- Output: Terdeteksi penggunaan UPX packer, indikasi teknik penyembunyian kode, serta terdokumentasi dalam tabel anomali.

☐ Task 4:Pemeriksaan timestamp metadata dan threat intelligence lookup (VirusTotal).

- Time spent: 1 jam
- Output: Teridentifikasi manipulasi timestamp (tahun 2061) serta hasil VirusTotal menunjukkan klasifikasi Malware/Trojan/Stealer dengan tingkat deteksi tinggi.

Week 3: Report & Presentation

☐ Task 5: Penyusunan bagian hasil *static analysis* untuk laporan akhir forensik digital.

- Time spent: 1 jam
- Output:Bab *Static Analysis Result* selesai beserta dokumentasi screenshot & tabel anomali.

Total Time Invested: [Total Hours] hours

---

3. Tools & Techniques Used

Tools

1. **PEStudio**

- Purpose:Mengidentifikasi tipe file, header, import API, dan timestamp.
- Key commands/features:Scanning otomatis melalui *Indicators* dan *Properties*.
- Output: Info PE32 .NET, metadata file, timestamp 2061, indikasi packer.

2. **VirusTotal**

- Purpose:Threat intelligence lookup]
- Key commands/features:Upload hash SHA-256
- Output:File terklasifikasi sebagai **Malware/Trojan/Stealer**

Analysis Techniques

- [Technique 1]: Static Binary Inspection:Pemeriksaan struktur file executable tanpa eksekusi untuk menemukan informasi teknis awal.

- [Technique 2]: Threat Intelligence Correlation:Membandingkan hash sampel dengan database AV untuk mengonfirmasi jenis ancaman dan keluarga malware.

---

4. My Key Findings

Finding 1: File Terdeteksi Menggunakan UPX

- **Description:**Malware dikompresi/di-pack menggunakan UPX untuk menyembunyikan kode internal.
- **Evidence:** Hasil DIE menunjukkan *Packer: UPX detected*.
- **Significance:**UPX menandakan upaya anti-analisis dan sering digunakan malware untuk menghindari deteksi.
- **My contribution:** Melakukan pemindaian packer dan mendokumentasikan hasil pada tabel anomaly findings.

Finding 2: Manipulasi Timestamp

- **Description:** Metadata PE memperlihatkan tanggal tahun **2061**, tidak realistis untuk executable saat ini.
- **Evidence:** PEStudio → *TimeDateStamp: Sat May 25 2061*.
- **Significance:**Timestomping umum digunakan untuk mengaburkan waktu pembuatan sehingga menyulitkan investigasi forensik
- **My contribution:**Menganalisis header PE dan mengidentifikasi anomali timestamp sebagai indikator anti-forensic.

Finding 3: Klasifikasi Malware: Trojan / Stealer (AgentTesla)

- **Description:**VirusTotal menunjukkan tingkat deteksi tinggi dengan klasifikasi Malware/Trojan/Stealer.
- **Evidence:**VirusTotal detection ratio tinggi dan label keluarga ancaman *AgentTesla* pada beberapa mesin AV.
- **Significance:** Memperkuat bahwa file merupakan malware infostealer yang berpotensi mencuri kredensial pengguna.
- **My contribution:**Melakukan lookup hash pada VirusTotal dan memasukkan hasil klasifikasi ke laporan.

---

5. Report Sections I Contributed To

Section	My Contribution	Percentage
Executive Summary	Memberikan ringkasan singkat mengenai hasil identifikasi malware berdasarkan analisis statis, termasuk risiko dan dampaknya.	[%]
Technical Analysis	Menyusun hasil analisis statis secara detail,	[%]
Evidence Collection	Mengumpulkan artefak berupa hash, screenshot hasil VirusTotal sebagai bukti teknis.	[%]
Timeline	Menyusun urutan tahapan analisis statis dari tahap inisiasi hingga finalisasi.	[%]
IoC List	Menyediakan IoC berbasis hash SHA-256 dan signature packer untuk AgentTesla.	[%]
Recommendations	Memberikan rekomendasi keamanan terkait mitigasi ancaman dari malware infostealer berbasis .NET.	[%]
Presentation Slides	menjelaskan bagian Hasil Analisis Statis dalam presentasi.	[%]

6. Collaboration Activities

Team Meetings Attended

- Meeting 1 ([Date]): Pembagian tugas per anggota. Berkontribusi memberi masukan metode analisis statis vs dinamis.
- Meeting 2 ([Date]):Update perkembangan analisis dan integrasi hasil tim. Memberikan update temuan packer dan timestamp abnormal.
- Meeting 3 ([Date]): Finalisasi laporan dan pembagian tugas presentasi. Menyampaikan hasil temuan statis dan revisi bagian laporan.

Communication

- **Primary channel:**WhatsApp
- **Response rate:** Within 2 hours typically
- **Proactive communication:** menemukan anomali timestamp dan packer untuk sinkronisasi dengan tim analisis dinamis.

Helping Team Members

- Helped [Member name] with: [Description]
- Shared knowledge about: [Topic]
- Peer reviewed: [What I reviewed]

---

7. Challenges & Solutions

Challenge 1: [Description]

- **Problem:**Kesulitan mengidentifikasi packer secara akurat pada tahap awal.
- **Impact:**Analisis terhambat karena sulit membuka struktur internal.
- **My solution:** Menggunakan DIE dan membandingkan signature packer UPX.
- **Outcome:**Packer UPX berhasil teridentifikasi sebagai indikasi anti-analysis.

---

8. Skills Developed

Technical Skills

- [Skill 1]Static Malware Analysis:Analisis struktur PE, packer, metadata, IoC,Intermediate
- [Skill 2]Threat Intelligence Lookup: Penggunaan VirusTotal dan hash-based lookup,Intermediate

Soft Skills

- [Skill 1]Technical writing:Menyusun sebagian laporan teknis statis secara terstruktur

---

9. What I Learned

Technical Knowledge

1. Pembelajaran mengenai struktur **PE32 .NET** dan atribut header yang digunakan malware.
2. Teknik **packer & obfuscation**, khususnya implementasi UPX pada malware.
3. Pentingnya **Threat Intelligence** (VirusTotal) untuk konfirmasi keluarga malware.

Forensic Methodology

1. Pentingnya tahapan **analisis statis sebelum analisis dinamis** untuk meminimalkan risiko.
2. Dokumentasi bukti digital menjadi bagian penting untuk **chain of evidence**.

Team Collaboration

1. Pembagian peran yang jelas mempercepat penyelesaian investigasi.
2. Komunikasi terbuka membuat hasil tiap anggota saling melengkapi.

---

10. Self-Evaluation

Strengths in This Project

- Konsisten menyelesaikan tugas tepat waktu.
- Teliti dalam dokumentasi bukti teknis.
- Aktif membantu integrasi hasil analisis antar anggota.

Areas for Improvement

- Bisa meningkatkan pemahaman mengenai analisis dinamis.
- Manajemen waktu dapat lebih optimal pada minggu kedua.
- Perlu meningkatkan kemampuan scripting untuk otomasi analisis.

Overall Self-Assessment

Contribution Level: Medium**Effort Level:** [1-10]
Quality of Work:8

Brief Justification: Kontribusi berfokus pada analisis statis sebagai fondasi identifikasi malware. Hasil analisis memberikan bukti teknis yang menjadi acuan anggota lain dalam analisis dinamis, IoC, dan rekomendasi.