IN PARTNERSHIP WITH PLYMOUTH UNIVERSITY

| Name: Gusthingna de silva |
| --- |
| Student Reference Number: 10817966 |

| Module Code: PUSL3131 | Module Name: Security Operations & Incident Management |
| --- | --- |
| Coursework Title: Incident Prevention, Detection and Response | |
| Deadline Date: 16 January 2025 | Member of staff responsible for coursework: Hai-Van Dang |
| Programme: | |

Please note that University Academic Regulations are available under Rules and Regulations on the University website www.plymouth.ac.uk/studenthandbook.

Group work: please list all names of all participants formally associated with this work and state whether the work was undertaken alone or as part of a team. Please note you may be required to identify individual responsibility for component parts.

10899343 Ranasinghe Priyantha
10899273 Rajakaruna Gunawardhana
10817967 Chakrawarthi fernando
10817966 Gusthingna de silva
10899245 Deshitha Bandara
10899307 Hewawasam Hansana

***We confirm that we have read and understood the Plymouth University regulations relating to Assessment Offences and that we are aware of the possible penalties for any breach of these regulations. We confirm that this is the independent work of the group.***

Signed on behalf of the group:

Individual assignment: ***I confirm that I have read and understood the Plymouth University regulations relating to Assessmen Offences and that I am aware of the possible penalties for any breach of these regulations. I confirm that this is my own independent work.***

Signed:

Use of translation software: failure to declare that translation software or a similar writing aid has been used will be treated as an assessment offence.

I *have used/not used translation software.

If used, please state name of software……

**Overall mark _____%** **Assessors Initials _____** **Date_____**

*Please delete as appropriate

# PUSL3131
# Security Operations & Incident Management

## Group 01

### 20 CREDIT MODULE

### ASSESSMENT: 50% Coursework

## Members who have contributed to the group work

| Student ID | Student name | Summary of each student's contribution | Confirming if the student has been enrolled into the group on DLE (yes/no)? |
|---|---|---|---|
| 10899343 | Ranasinghe Priyantha | Section 4 | yes |
| 10899273 | Rajakaruna Gunawardhana | Section 3 | yes |
| 10817967 | Chakrawarthi fernando | Section 2 | yes |
| 10817966 | Gusthingna de silva | Documentation | yes |
| 10899245 | Deshitha Bandara | Section 2 | yes |
| 10899307 | Hewawasam Hansana | Section 1 | yes |

## Members who have not contributed to the group work

| Student ID | Student name | Confirming if the student has been enrolled into the group on DLE (yes/no)? |
|---|---|---|
| | | |
| | | |

# Contents

# Section 01

## Introduction

In today’s increasingly connected world, the threat landscape for organizations continues to evolve, and ensuring the security of internal systems and data has become a critical challenge. This report focuses on the intrusion analysis of suspected infection in DevonCinema, which provides cinematic entertainment.

The company has experienced unusual network traffic patterns, which prompted its IT team to investigate further. The analysis of network traffic logs, along with a set of security alerts, has led to the discovery of a potential infection within the company's network. The primary goal of this report is to conduct an in-depth intrusion analysis on the provided network traffic log file (capturednetwork2024.pcap) and alert files (alert2024.jpg, alert2024.txt) to detect the infected system’s information, identify how the system was compromised, and determine the nature of the infection.

By analyzing this data, the report will provide insight into the techniques and methods the attackers might have used to infiltrate the system, offering a roadmap for addressing the vulnerabilities that led to the breach. In addition to the immediate analysis, this report will outline a long-term strategy for improving the company's cybersecurity defenses. This includes recommendations on how DevonCinema can better detect, respond to, and prevent similar incidents in the future, leveraging techniques such as Intrusion Detection Systems (IDS), honeypots, and Security Information and Event Management (SIEM) systems.

Moreover, the likelihood of detecting future intrusions and tracing the source of these threats will also be evaluated. The analysis begins with an in-depth examination of the provided network capture file and alert logs. Using specialized forensic tools, the methodology will uncover details such as the infected system's IP address, indicators of compromise, and the infection vector. Screenshots and results will support the findings. In the longer term, this report will outline strategies to prevent similar incidents including implementing Intrusion Detection Systems, honeypots, and Security Information and Event Management solutions. These recommendations will include a critical analysis of their applicability, advantages, and limitations in the context of DevonCinema's infrastructure. By investigating the infection and proposing strong countermeasures this report aims to support DevonCinema in safeguarding its systems and maintaining a secure operational environment.

# Section 02

## Methodology and Results

## 1. Methodology

### 1.1. Tools Used

- Wireshark: For detailed packet analysis and identifying suspicious network activities.
- VirusTotal: This is used to scan suspicious files or URLs extracted from traffic data.
- Suricata/Snort: For applying signature-based detection on network traffic.

### 1.2. Step-by-Step Analysis

#### 1.2.1. Loading the PCAP File in Wireshark

- Open the capturednetwork2024.pcap file in Wireshark.
- Apply filters to detect anomalies, e.g., http, dns, tcp.stream, or known malicious indicators.
- Identify unusual traffic patterns, connections to suspicious IP addresses, or anomalous protocols.

#### 1.2.2. Identifying the Infected System

1.2.2.1. Extract the following information from the packet data:

- IP Address: Filter traffic to find the source of suspicious activity.
- MAC Address: Analyze ARP packets to associate the IP with a MAC address.
- Hostname: Look for NetBIOS or DNS queries revealing device hostnames.
- User Account Name: Check for SMB traffic or other authentication protocols revealing usernames.

#### 1.2.3. Detecting Indicators of Compromise (IOCs)

- Analyze payloads for signatures of malware.
- Cross-reference IPs, domains, and file hashes with threat intelligence sources like VirusTotal.

#### 1.2.4. Tracing the Infection Vector

1.2.4.1. Identify the origin of the infection by:

- Reviewing outbound connections to external servers.
- Checking for downloaded executables or scripts.
- Analyzing phishing attempts or malicious email traffic.

#### 1.2.5. Alert Analysis

- Review alert2024.txt for triggered IDS/IPS alerts.
- Analyze alert2024.jpg for visual indicators of compromise.

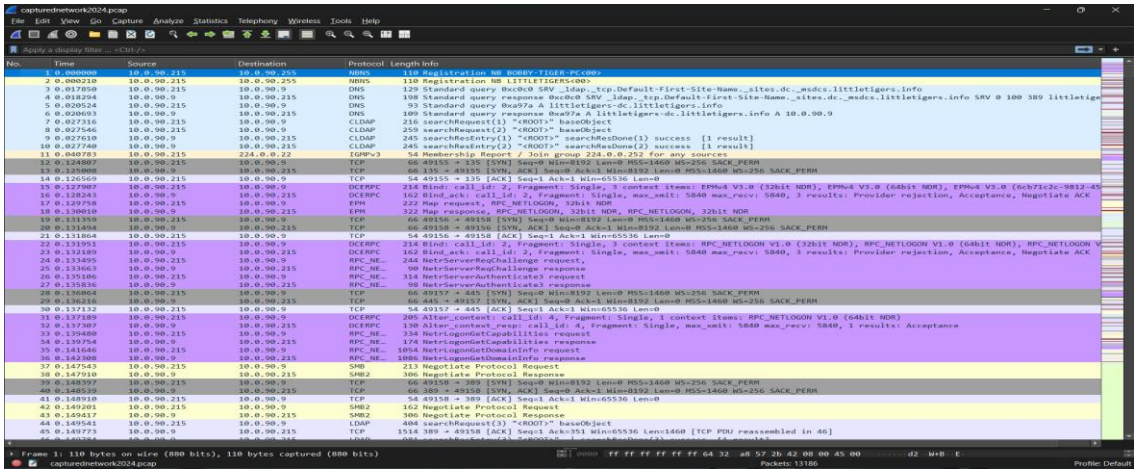
#### 1.2.6. Documentation with Screenshots

- Capture and document all relevant findings with screenshots from Wireshark, Zeek logs, and VirusTotal results.

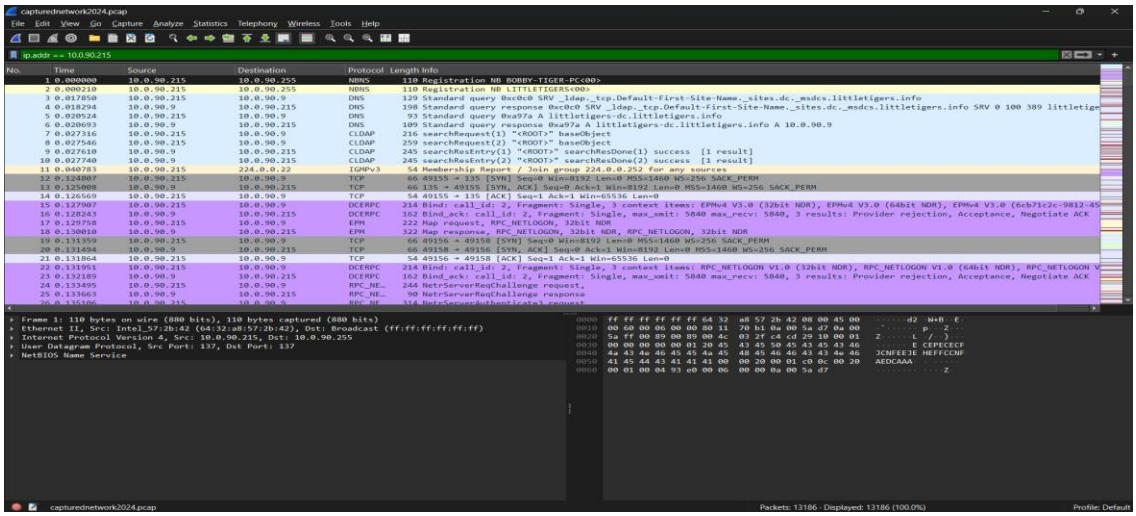
## 2. Results

### 2.1. capturednetwork2024.pcap

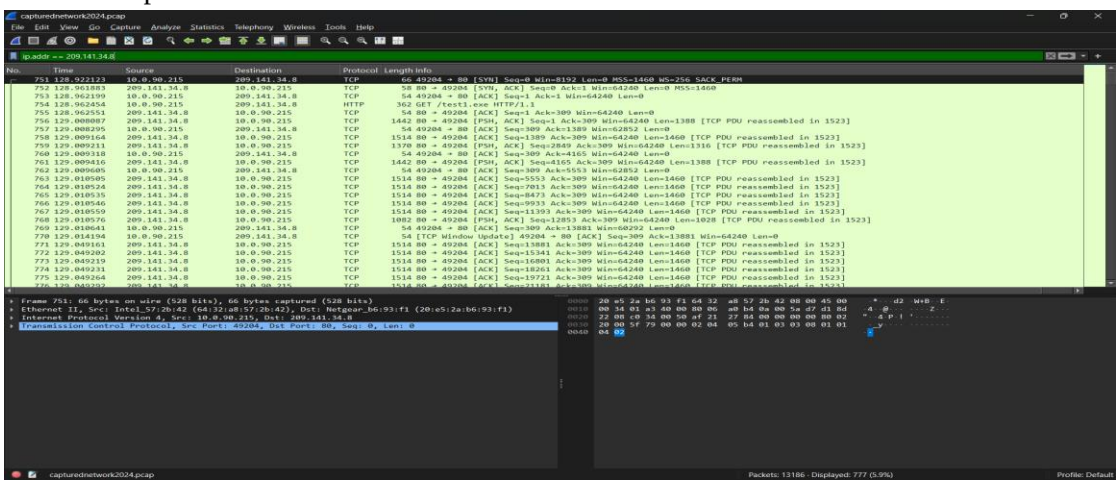
#### 2.1.1.Wireshark Dashboard



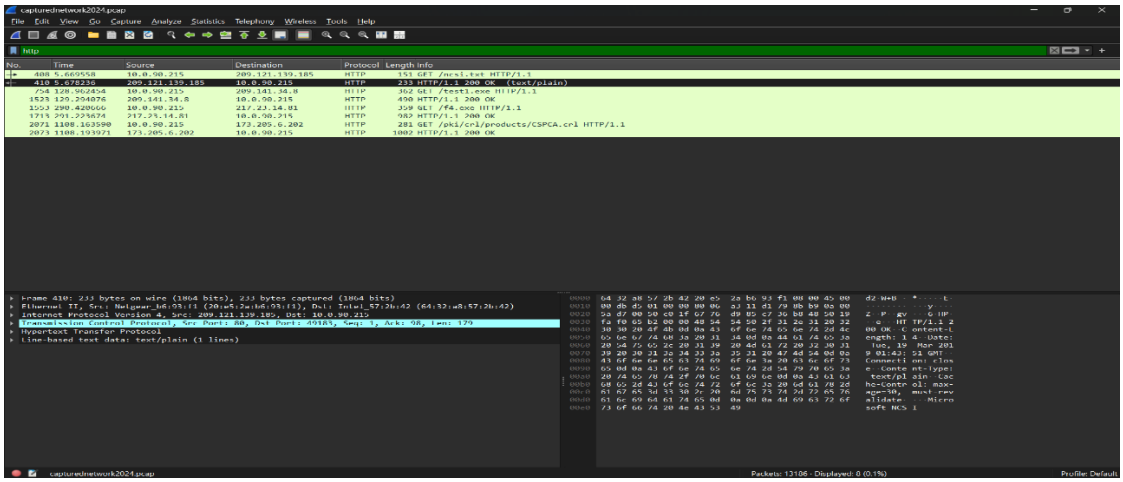
#### 2.1.2.Scan ip.addr = = 10.0.90.215



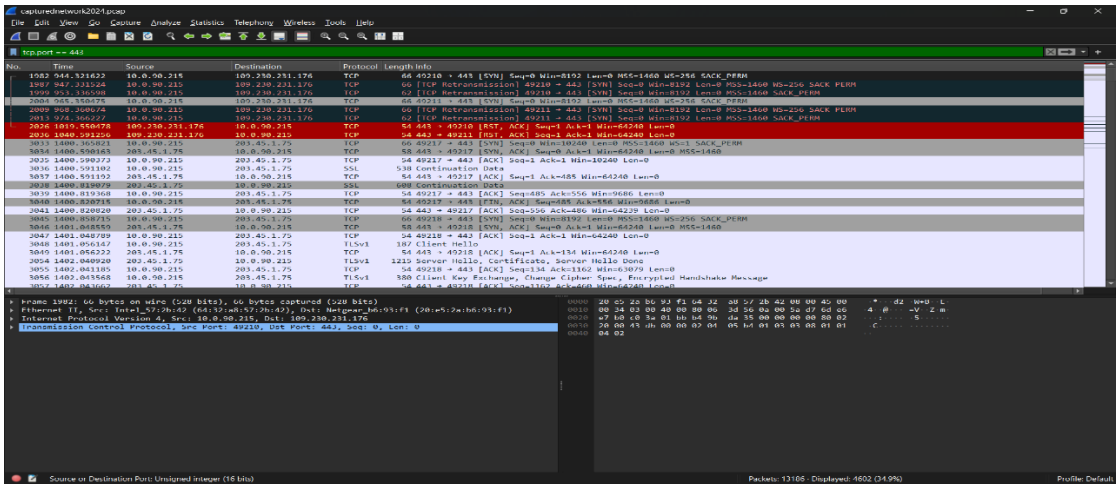
#### 2.1.3.Scan ip.addr = = 209.141.34.8



2.1.4.Scan http



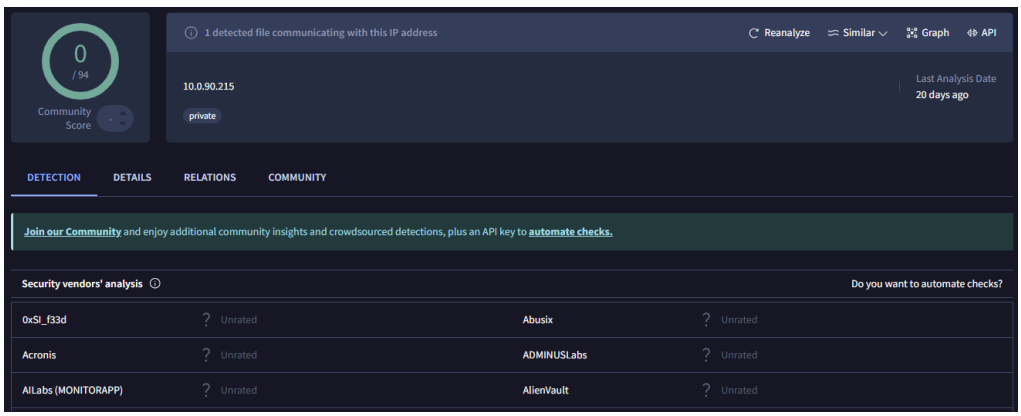
2.1.5.Scan tcp.port = = 443



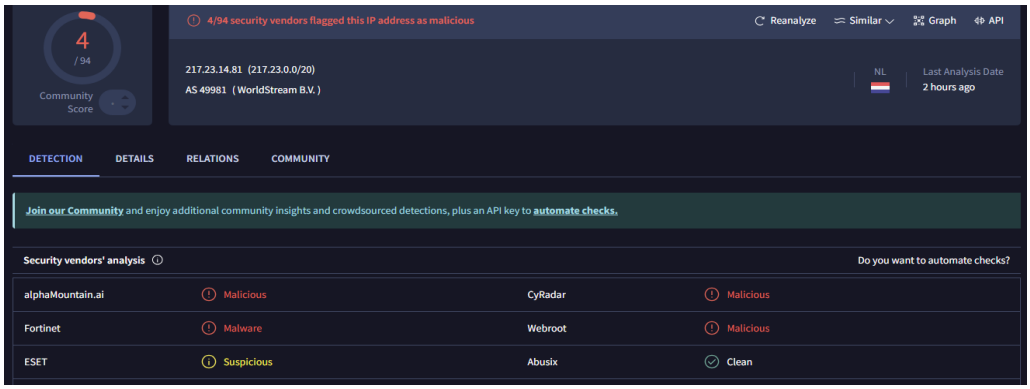
## 2.1.6.Suspicious Files/IPs

2.1.6.1. Suspicious Ips

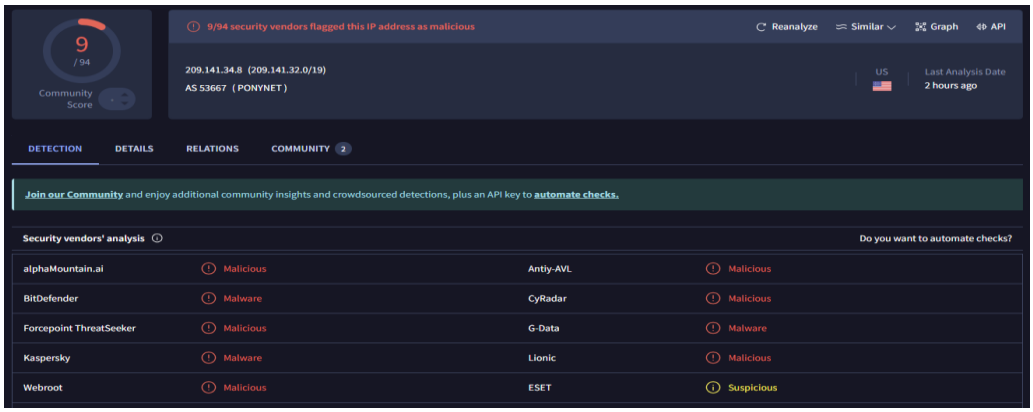
- 10.0.90.215



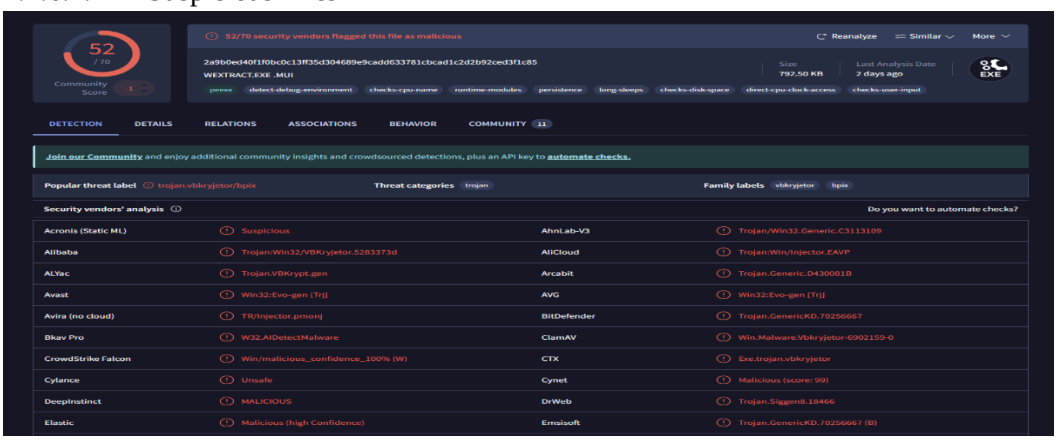
- 209.141.34.8




- 217.23.14.81




### 2.1.6.2. Suspicious Files




| IP Address | Activity |
|---|---|
| 10.0.90.215 | Internal devices used in suspicious actions. There is a possibility of compromise. |
| 209.141.34.8 | External IP address supplying potentially malicious payloads (such as.exe files). |
| 217.23.14.81 | Repeated connection attempts suggest possible command and control. |

### 2.2. alerts2024.txt

2.2.1. High Priority

| Source IP | Event Description | Destination IP |
|---|---|---|
| 10.0.90.215 | ET TROJAN Remcos RAT Checkin 23 | 103.1.184.108 |
| 10.0.90.215 | ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex) | 31.22.4.176 |
| 10.0.90.215 | ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex) | 203.45.1.75 |
| 10.0.90.215 | ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex) | 115.112.43.81 |
| 10.0.90.215 | ET POLICY Binary Download Smaller than 1 MB Likely Hostile | 209.141.34.8 |
| 10.0.90.215 | ET CURRENT_EVENTS DRIVEBY Likely Evil EXE with no referer from HFS webserver | 217.23.14.81 |

2.2.2. Medium Priority

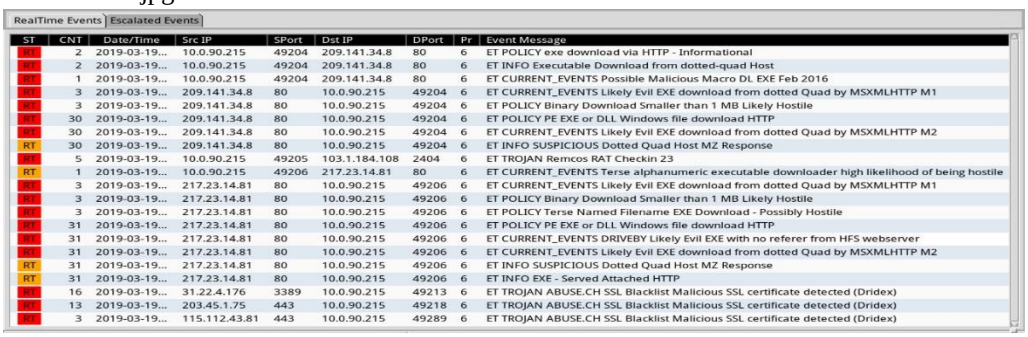
| Source IP | Event Description | Destination IP |
|---|---|---|
| 10.0.90.215 | ET POLICY PE EXE or DLL Windows file download HTTP | 209.141.34.8 |
| 10.0.90.215 | ET POLICY PE EXE or DLL Windows file download HTTP | 217.23.14.81 |
| 10.0.90.215 | ET POLICY Binary Download Smaller than 1 MB Likely Hostile | 217.23.14.81 |

2.2.3. Low Priority

| Source IP | Event Description | Destination IP |
|---|---|---|
| 10.0.90.215 | ET INFO Executable Download from dotted-quad Host | 209.141.34.8 |
| 10.0.90.215 | ET CURRENT_EVENTS Possible Malicious Macro DL EXE Feb 2016 | 209.141.34.8 |

## 2.3. Alerts2024.jpg

### 2.3.1. alerts2024.jpg



RealTime Events | Escalated Events

| ST | CNT | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|---|---|---|---|---|---|---|---|---|
| RT | 2 | 2019-03-19... | 10.0.90.215 | 49204 | 209.141.34.8 | 80 | 6 | ET POLICY exe download via HTTP - Informational |
| RT | 2 | 2019-03-19... | 10.0.90.215 | 49204 | 209.141.34.8 | 80 | 6 | ET INFO Executable Download from dotted-quad Host |
| RT | 1 | 2019-03-19... | 10.0.90.215 | 49204 | 209.141.34.8 | 80 | 6 | ET CURRENT_EVENTS Possible Malicious Macro DL EXE Feb 2016 |
| RT | 3 | 2019-03-19... | 209.141.34.8 | 80 | 10.0.90.215 | 49204 | 6 | ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP M1 |
| RT | 3 | 2019-03-19... | 209.141.34.8 | 80 | 10.0.90.215 | 49204 | 6 | ET POLICY Binary Download Smaller than 1 MB Likely Hostile |
| RT | 30 | 2019-03-19... | 209.141.34.8 | 80 | 10.0.90.215 | 49204 | 6 | ET POLICY PE EXE or DLL Windows file download HTTP |
| RT | 30 | 2019-03-19... | 209.141.34.8 | 80 | 10.0.90.215 | 49204 | 6 | ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP M2 |
| RT | 30 | 2019-03-19... | 209.141.34.8 | 80 | 10.0.90.215 | 49204 | 6 | ET INFO SUSPICIOUS Dotted Quad Host MZ Response |
| RT | 5 | 2019-03-19... | 10.0.90.215 | 49205 | 103.1.184.108 | 2404 | 6 | ET TROJAN Remcos RAT Checkin 23 |
| RT | 1 | 2019-03-19... | 10.0.90.215 | 49206 | 217.23.14.81 | 80 | 6 | ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile |
| RT | 3 | 2019-03-19... | 217.23.14.81 | 80 | 10.0.90.215 | 49206 | 6 | ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP M1 |
| RT | 3 | 2019-03-19... | 217.23.14.81 | 80 | 10.0.90.215 | 49206 | 6 | ET POLICY Binary Download Smaller than 1 MB Likely Hostile |
| RT | 3 | 2019-03-19... | 217.23.14.81 | 80 | 10.0.90.215 | 49206 | 6 | ET POLICY Terse Named Filename EXE Download - Possibly Hostile |
| RT | 31 | 2019-03-19... | 217.23.14.81 | 80 | 10.0.90.215 | 49206 | 6 | ET POLICY PE EXE or DLL Windows file download HTTP |
| RT | 31 | 2019-03-19... | 217.23.14.81 | 80 | 10.0.90.215 | 49206 | 6 | ET CURRENT_EVENTS DRIVEBY Likely Evil EXE with no referer from HFS webserver |
| RT | 31 | 2019-03-19... | 217.23.14.81 | 80 | 10.0.90.215 | 49206 | 6 | ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP M2 |
| RT | 31 | 2019-03-19... | 217.23.14.81 | 80 | 10.0.90.215 | 49206 | 6 | ET INFO SUSPICIOUS Dotted Quad Host MZ Response |
| RT | 31 | 2019-03-19... | 217.23.14.81 | 80 | 10.0.90.215 | 49206 | 6 | ET INFO EXE - Served Attached HTTP |
| RT | 16 | 2019-03-19... | 31.22.4.176 | 3389 | 10.0.90.215 | 49213 | 6 | ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex) |
| RT | 13 | 2019-03-19... | 203.45.1.75 | 443 | 10.0.90.215 | 49218 | 6 | ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex) |
| RT | 3 | 2019-03-19... | 115.112.43.81 | 443 | 10.0.90.215 | 49289 | 6 | ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex) |

- Trojan Activity: Several instances of Trojan-related behavior were discovered, suggesting a potential compromise.
- Malicious Downloads: Downloads of executable (EXE) files were classified as hostile.
- Suspicious IPs: Several IP addresses were reported for unusual or potentially malicious activities.

### 2.3.2. Key Findings

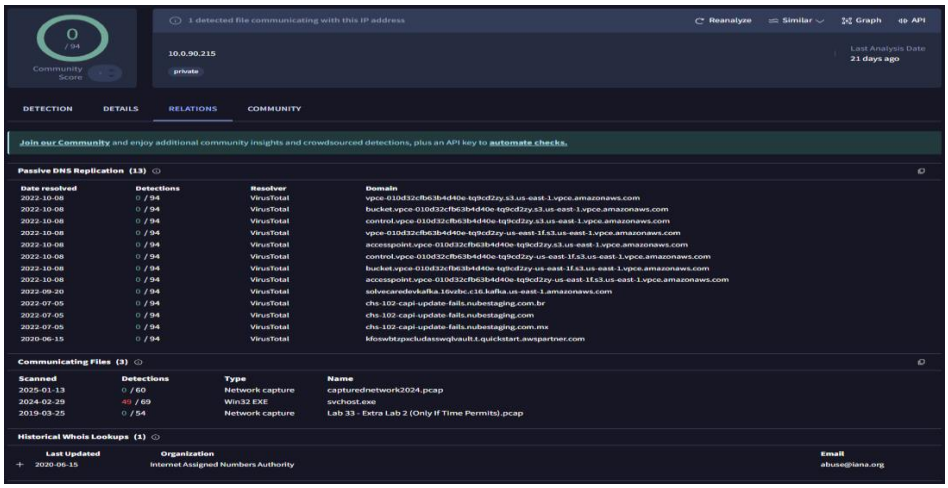
- Malicious Ips (Source Ips)

| Rank | IP Address | Alert Count | Notes |
|---|---|---|---|
| 1 | 10.0.90.215 | 45 | Likely infected the internal host |
| 2 | 209.141.34.8 | 30 | Dotted-quad malicious host |
| 3 | 217.23.14.81 | 31 | Repeated connection attempts |
| 4 | 115.112.43.81 | 3 | SSL Blacklist (Dridex Trojan) |
| 5 | 203.45.1.75 | 1 | Potential SSL abuse |

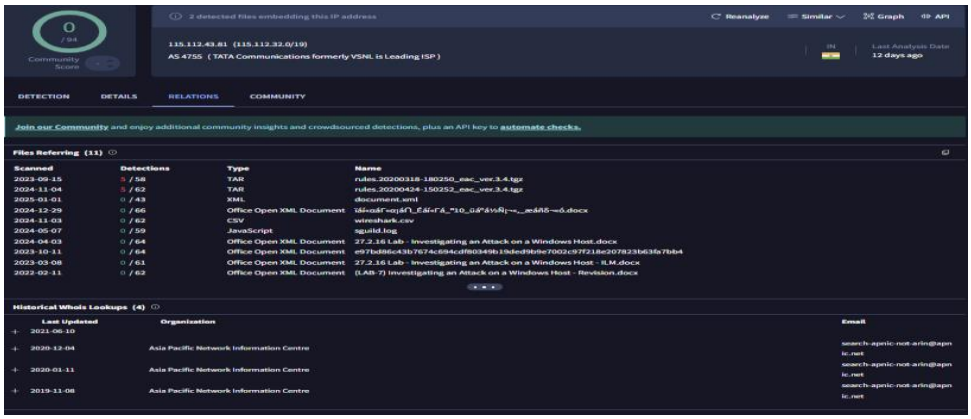
- Most Frequent Alerts

| Alert Type | Count |
|---|---|
| Likely Evil EXE download | 45 |
| Trojan detection (e.g., Remcos RAT) | 5 |
| SSL Blacklist (Dridex) | 10 |
| Executable download flagged as hostile | 25 |

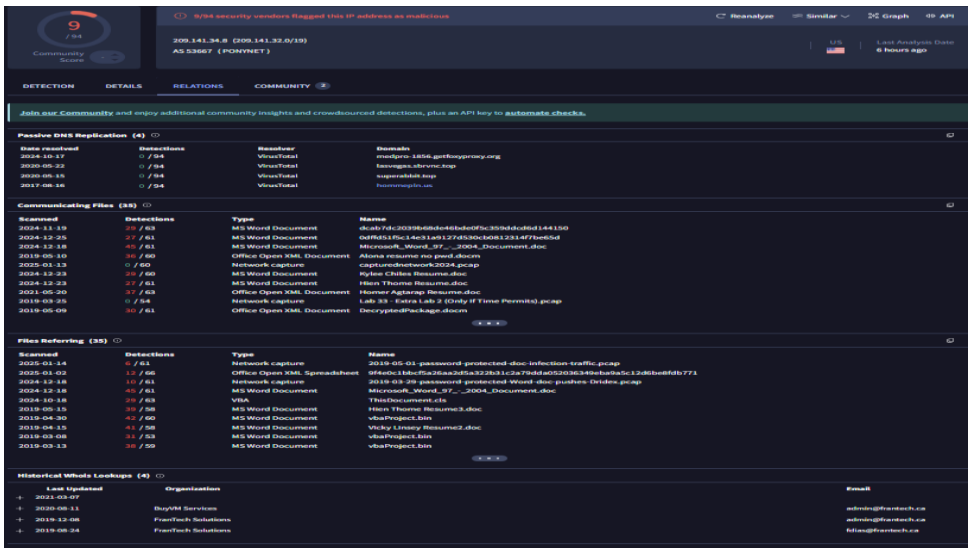
- 10.0.90.215



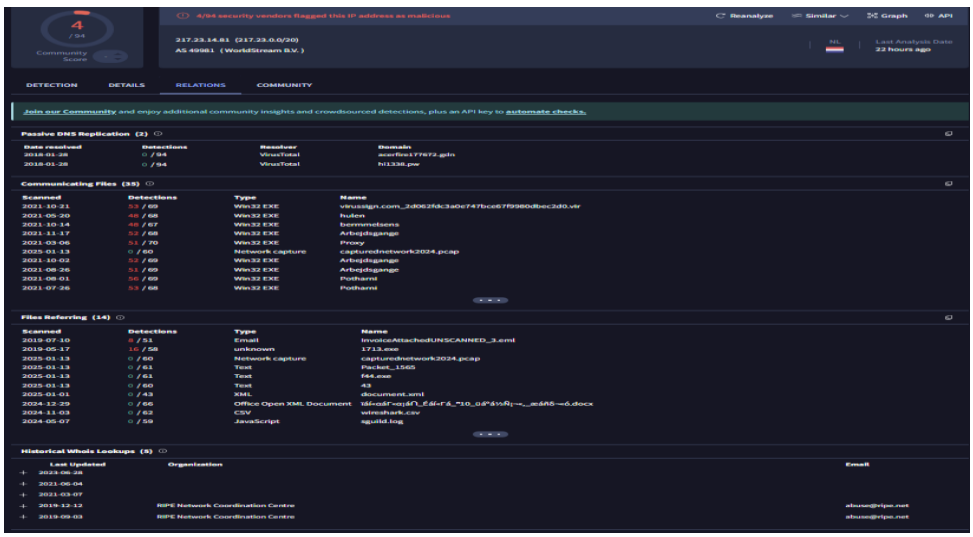
- 115.112.43.81




- 209.141.34.8




- 217.23.14.81



# Section 03

## Long-Term Plans for Detecting and Responding to Intruders

1. Deploy Endpoint Detection and Response (EDR) Tools:
    - Tools such as CrowdStrike and Microsoft Defender for Endpoints continually monitor endpoint activity. They detect and quarantine harmful files, processes, and behaviors in real-time, enabling incident responders to act fast. These technologies also create detailed reports on discovered dangers, which help in further research.

2. Implement Network Segmentation:
    - Divide the network into discrete pieces depending on asset criticality, ensuring that unauthorized access is limited between them. Consider separating financial data servers from employee desktops.

3. Enhanced Threat Intelligence Integration:
    - Use feeds from reputable sources such as abuse.ch and VirusTotal to dynamically ban harmful IPs, domain names, and files. Integrating these feeds into firewalls and IDS/IPS systems provides proactive protection against known threats.

4. Regular Employee Training:
    - Implement cybersecurity awareness initiatives to educate staff on phishing assaults, social engineering strategies, and safe surfing behaviors. Use simulated phishing campaigns to assess and enhance staff preparedness.

5. Automated Log Analysis:
    - Use Security Information and Event Management (SIEM) systems like Splunk or Elastic Security to automatically correlate logs from many sources, discover abnormalities, and notify the security team.

6. Incident Response Plan (IRP):
    - Create and record a complete IRP that outlines methods for detection, containment, eradication, and recovery. Conduct frequent exercises to ensure that all stakeholders are properly prepared to respond to emergencies.

7. Regular Security Audits and Penetration Testing:
    - Engage third-party auditors or internal teams to do frequent vulnerability assessments and penetration testing. These audits aid in detecting flaws before attackers exploit them.

# Section 04

## Conclusion

This research discovered the affected system, 10.0.90.215 and conducted a thorough examination of the infection process. The investigation found significant evidence of malicious behavior, including the download and execution of damaging payloads, as well as subsequent contact with command-and-control (C2) servers. These findings identify flaws in the organization's present cybersecurity architecture and emphasize the significance of installing strong security measures.

To prevent similar events and improve the organization's overall cybersecurity posture, the study suggests the following important actions:

- Implementation of Intrusion Detection and Prevention Systems (IDPS): This will enable real-time monitoring and automatic reactions to detect and prevent malicious activity before it does substantial harm.

- Implementation of Security Information and Event Management (SIEM) solutions: SIEM systems will centralize log management, provide sophisticated threat correlation, and enable faster incident response by collecting data from across the IT ecosystem.

- Adoption of Endpoint Protection Tools: Modern endpoint protection solutions defend individual devices by detecting and mitigating malware, ransomware, and other endpoint-specific threats.

- Network segmentation will limit attackers' lateral movement, confine breaches to confined zones, and reduce the potential impact of a compromised system.

Implementing these procedures will greatly improve the organization's capacity to recognize, respond to, and avoid cyber-attacks. These proactive efforts will not only fix the vulnerabilities discovered during this research but will also establish a solid framework for managing future threats. Strengthening the cybersecurity infrastructure will result in a more robust IT environment that protects vital assets and ensures business continuity in the face of emerging cyber threats.

## Reference


I. (No date a) *SSLBL*. Available at: https://sslbl.abuse.ch/ (Accessed: 11 January 2025).

II. (No date b) *Snort rules and IDS software download*. Available at: https://www.snort.org/downloads (Accessed: 13 January 2025).

III. Admin, T. (2024) *Snort tutorial and practical examples, HackerTarget.com*. Available at: https://hackertarget.com/snort-tutorial-practical-examples/ (Accessed: 13 January 2025).

IV. CesarGBkR (no date) *CesarGBkR/snort_windows: How to install Snort on Windows 10 and 11, GitHub*. Available at: https://github.com/CesarGBkR/Snort_Windows (Accessed: 12 January 2025).

V. *Downloading nmap* (no date) *Download the Free Nmap Security Scanner for Linux/Mac/Windows*. Available at: https://nmap.org/download (Accessed: 13 January 2025).

VI. *How to install and configure Snort on Windows* (no date) *LetsDefend*. Available at: https://letsdefend.io/blog/how-to-install-and-configure-snort-on-windows (Accessed: 13 January 2025).

VII. Marketing, H. (2022) *Understanding the 5 types of intrusion detection systems, Helixstorm*. Available at: https://www.helixstorm.com/blog/types-of-intrusion-detection-systems/ (Accessed: 12 January 2025).

VIII. *Network intrusion detection* (no date) *network intrusion detection - an overview | ScienceDirect Topics*. Available at: https://www.sciencedirect.com/topics/computer-science/network-intrusion-detection (Accessed: 12 January 2025).

IX. *Snort explained: Understanding snort rules and use cases* (no date) *CrowdStrike*. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/snort-rules/ (Accessed: 13 January 2025).

X. *Wireshark · documentation* (no date) *Wireshark*. Available at: https://www.wireshark.org/docs/ (Accessed: 11 January 2025).

XI. *Intruder detection* (no date) *Intruder Detection - an overview | ScienceDirect Topics*. Available at: https://www.sciencedirect.com/topics/computer-science/intruder-detection (Accessed: 14 January 2025).

XII. Sweeney, P. (2024) *What is threat detection and response (TDR)? complete guide, Search Security*. Available at: https://www.techtarget.com/searchsecurity/definition/threat-detection-and-response-TDR (Accessed: 14 January 2025).

XIII. Underhill, E. (2024) *Intruder detection: A guide for businesses, Titan Security Europe*. Available at: https://www.titansecurityeurope.com/intruder-detection-a-guide-for-businesses/ (Accessed: 14 January 2025).