



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](http://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 Chakrawarthy 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 Assessment 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\_\_\_\_

# 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	Chakrawarthy 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

<b>Introduction .....</b>	<b>1</b>
<b>Methodology and Results .....</b>	<b>2</b>
<b>1. Methodology .....</b>	<b>2</b>
<b>2. Results .....</b>	<b>3</b>
<b>2.1. capturednetwork2024.pcap .....</b>	<b>3</b>
2.1.1. Wireshark Dashboard .....	3
2.1.2. Scan ip.addr == 10.0.90.215 .....	3
2.1.3. Scan ip.addr == 209.141.34.8 .....	3
2.1.4. Scan http .....	4
2.1.5. Scan tcp.port == 443 .....	4
<b>2.1.6. Suspicious Files/IPs .....</b>	<b>4</b>
2.1.6.1. Suspicious Ips .....	4
2.1.6.2. Suspicious Files .....	5
<b>2.2. alerts2024.txt .....</b>	<b>6</b>
2.2.1. High Priority .....	6
2.2.2. Medium Priority .....	6
2.2.3. Low Priority .....	6
<b>2.3. Alerts2024.jpg .....</b>	<b>7</b>
2.3.1. alerts2024.jpg .....	7
2.3.2. Key Findings .....	7
<b>Long-Term Plans for Detecting and Responding to Intruders .....</b>	<b>9</b>
<b>Conclusion .....</b>	<b>10</b>
<b>Reference .....</b>	<b>11</b>

## 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.

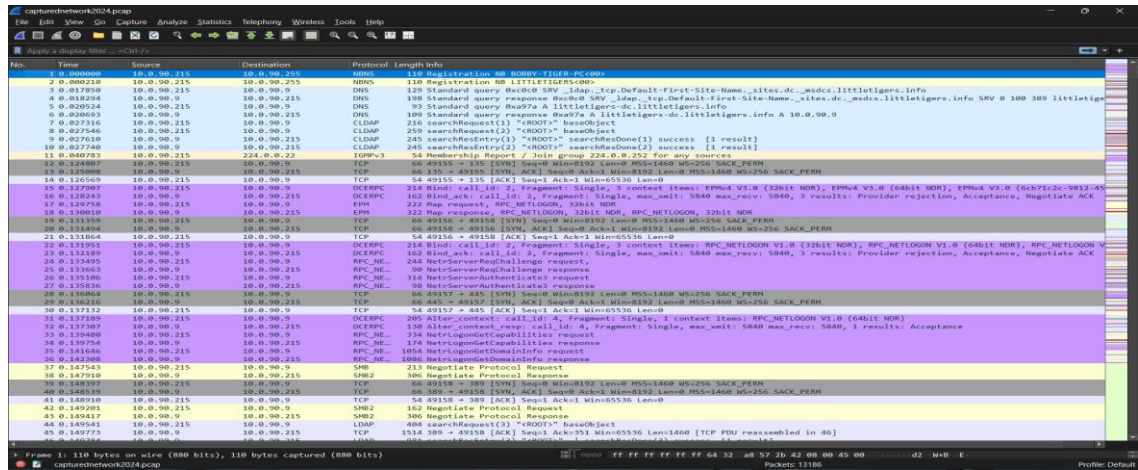
###### 1.2.6.Documentation with Screenshots

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

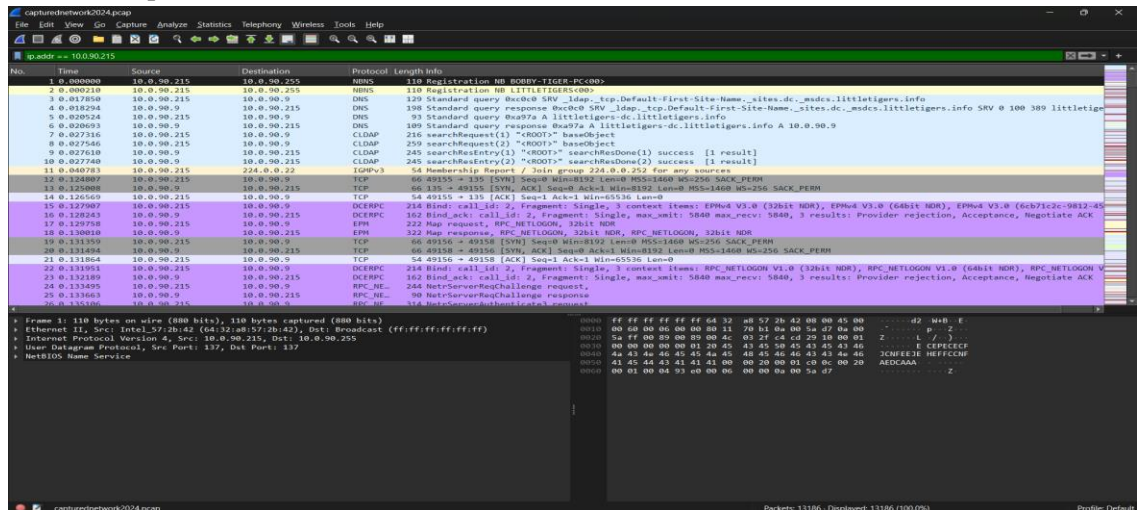
## 2. Results

### 2.1. capturednetwork2024.pcap

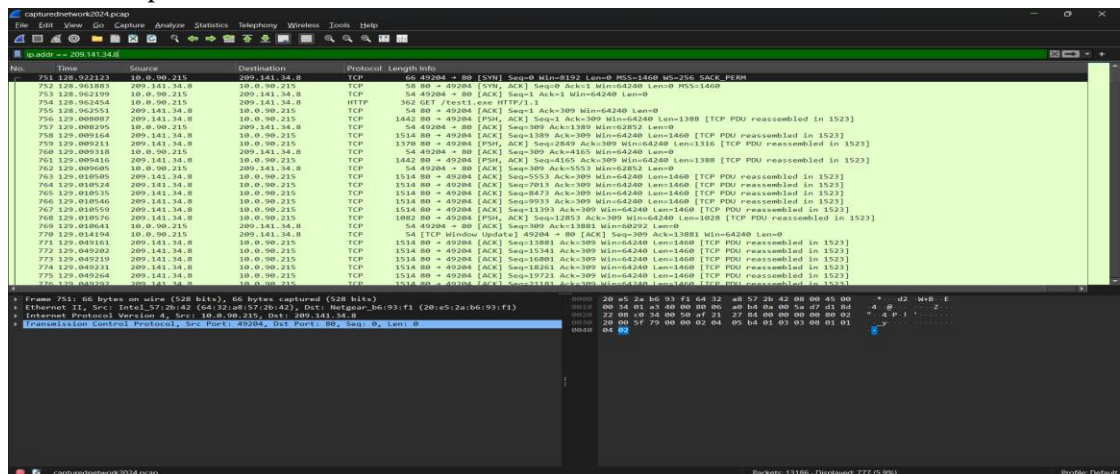
#### 2.1.1. Wireshark Dashboard



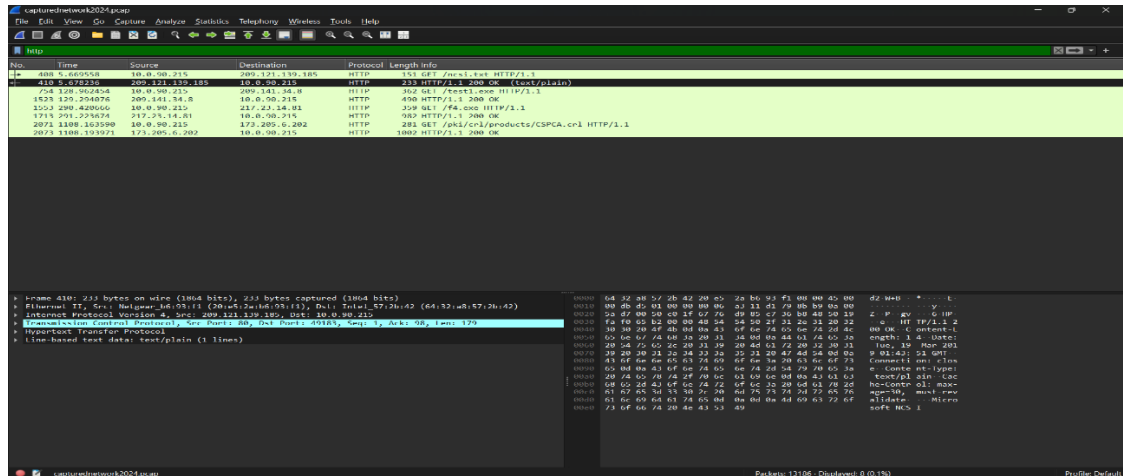
#### 2.1.2. Scan ip.addr == 10.0.90.215



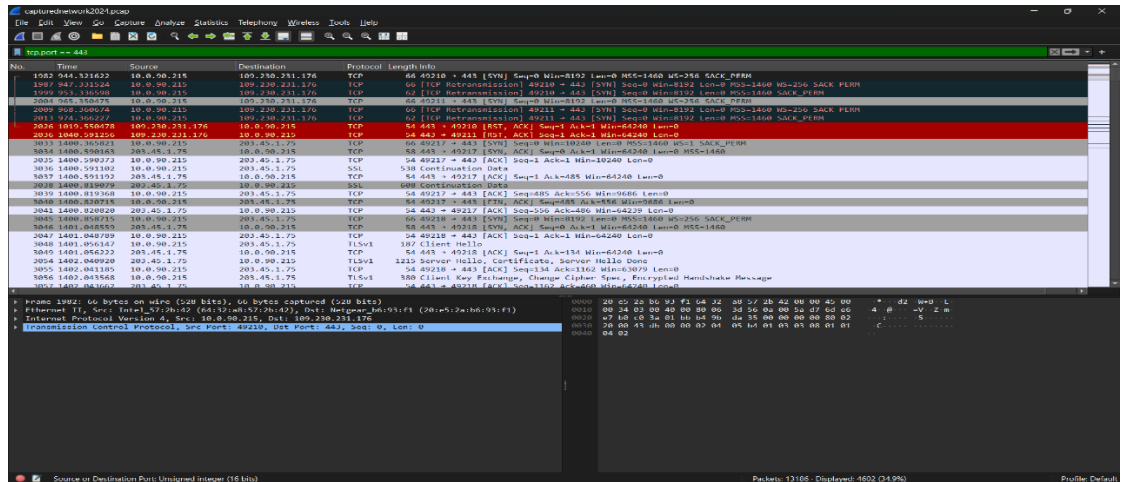
#### 2.1.3. Scan ip.addr == 209.141.34.8



## 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

0 / 94

Community Score

private

1 detected file communicating with this IP address

Reanalyze Similar Graph API

Last Analysis Date 20 days ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

0xSI_f33d	? Unrated	Abusix	? Unrated
Acronis	? Unrated	ADMINUSLabs	? Unrated
AILabs (MONITORAPP)	? Unrated	AlienVault	? Unrated

▪ 209.141.34.8

4 / 94  
Community Score

209.141.34.8 (217.23.0.0/20)  
AS 49981 (WorldStream B.V.)

4/94 security vendors flagged this IP address as malicious

Reanalyze Similar Graph API

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Vendor	Detection	Vendor	Detection
alphaMountain.ai	Malicious	CyRadar	Malicious
Fortinet	Malware	Webroot	Malicious
ESET	Suspicious	Abusix	Clean

▪ 217.23.14.81

9 / 94  
Community Score

209.141.34.8 (209.141.32.0/19)  
AS 53667 (PONYNET)

9/94 security vendors flagged this IP address as malicious

Reanalyze Similar Graph API

DETECTION DETAILS RELATIONS COMMUNITY 2

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Vendor	Detection	Vendor	Detection
alphaMountain.ai	Malicious	Antiy-AVL	Malicious
BitDefender	Malware	CyRadar	Malicious
Forcepoint ThreatSeeker	Malicious	G-Dat	Malware
Kaspersky	Malware	Lionix	Malicious
Webroot	Malicious	ESET	Suspicious

## 2.1.6.2. Suspicious Files

52 / 70  
Community Score

2a9b0ed40f1f0bc0c13f35cd30468e9cad633781cbcad1c2d2b52ced3f1c85  
WEXTRACT.EXE\_MUI

52/70 security vendors flagged this file as malicious

Reanalyze Similar More

DETECTION DETAILS RELATIONS ASSOCIATIONS BEHAVIOR COMMUNITY 11

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label Trojan.vbkryptor/bape

Threat categories Trojan

Family labels vbkryptor bape

Security vendors' analysis

Vendor	Detection	Vendor	Detection
Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan.Win32.Generic.C3113109
Alibaba	Trojan.Win32/VBKryptor.5263373d	AliCloud	Trojan.Win/Injector.EAVP
ALYac	Trojan.VBKrypt.gen	Arcabit	Trojan.Generic.D430061B
Avast	Win32:Evo-gen [Trj]	AVG	Win32:Evo-gen [Trj]
Avira (no cloud)	TR/Injector.prior	BitDefender	Trojan.Generic.KD.70256667
Bkav Pro	W32.AIDetect/Malware	ClamAV	Win.Malware.VBKryptor-6902159-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Evo.trojan.vbkryptor
Cylance	Unsafe	Cynet	Malicious (score: 99)
DeepInSight	MALICIOUS	DrWeb	Trojan.SiggenB.18466
Elastic	Malicious (High Confidence)	Emsisoft	Trojan.Generic.KD.70256667 (B)

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	Dest IP	DPort	Pr	Event Message	
ET	2	2019-03-19...	10.0.90.215	49204	209.141.34.8	80	6	ET POLICY exe download via HTTP - Informational	
ET	2	2019-03-19...	10.0.90.215	49204	209.141.34.8	80	6	ET INFO Executable Download from dotted-quad Host	
ET	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	
ET	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	
ET	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	
ET	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	
ET	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	
ET	5	2019-03-19...	10.0.90.215	49205	103.1.184.108	2404	6	ET TROJAN Remcos RAT Checkin Z3	
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	
ET	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	
ET	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	
ET	3	2019-03-19...	217.23.14.81	80	10.0.90.215	49206	6	ET POLICY Terse Named Filename EXE Download - Possibly Hostile	
ET	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	
ET	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 webservice	
ET	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	
ET	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)	
ET	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)	
ET	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

0 / 94

Community Score

1 detected file communicating with this IP address

10.0.90.215

private

Last Analysis Date  
21 days ago

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join our Community and enjoy additional community insights and crowd-sourced detections, plus an API key to automate checks.

Passive DNS Replication (13)

Date resolved	Detections	Resolver	Domain
2022-10-08	0 / 94	VirusTotal	vpcw-010d32c8b63b4d40e-tpcd2zy.s3.us-east-1.vpcw.amazonaws.com
2022-10-08	0 / 94	VirusTotal	bucket.vpcw-010d32c8b63b4d40e-tpcd2zy.s3.us-east-1.vpcw.amazonaws.com
2022-10-08	0 / 94	VirusTotal	control.vpcw-010d32c8b63b4d40e-tpcd2zy.s3.us-east-1.vpcw.amazonaws.com
2022-10-08	0 / 94	VirusTotal	vpcw-010d32c8b63b4d40e-tpcd2zy-us-east-1.s3.us-east-1.vpcw.amazonaws.com
2022-10-08	0 / 94	VirusTotal	amazon.vpcw-010d32c8b63b4d40e-tpcd2zy.s3.us-east-1.vpcw.amazonaws.com
2022-10-08	0 / 94	VirusTotal	control.vpcw-010d32c8b63b4d40e-tpcd2zy-us-east-1.s3.us-east-1.vpcw.amazonaws.com
2022-10-08	0 / 94	VirusTotal	bucket.vpcw-010d32c8b63b4d40e-tpcd2zy-us-east-1.s3.us-east-1.vpcw.amazonaws.com
2022-10-08	0 / 94	VirusTotal	ec2.vpcw-010d32c8b63b4d40e-tpcd2zy-us-east-1.s3.us-east-1.vpcw.amazonaws.com
2022-09-20	0 / 94	VirusTotal	infocenter.kuba.1ntrivc.116.kuba.us-east-1.amazonaws.com
2022-07-05	0 / 94	VirusTotal	chs-102-capi-update-falls.mubestaging.com.br
2022-07-05	0 / 94	VirusTotal	chs-102-capi-update-falls.mubestaging.com
2022-07-05	0 / 94	VirusTotal	chs-102-capi-update-falls.mubestaging.com.mn
2020-06-15	0 / 94	VirusTotal	MicrosoftEdgeUpdateService-1.quickstart1.amazonaws.com

Communicating Files (3)

Scanned	Detections	Type	Name
2025-01-11	0 / 60	Network capture	capturednetwork3024.pcap
2024-02-29	0 / 69	Win32 EXE	sechost.exe
2019-03-25	0 / 54	Network capture	Lab 33 - Extra Lab 2 (Only if Time Permits).pcap

Historical Whois Lookups (1)

Last Updated	Organization	Email
2020-06-15	Internet Assigned Numbers Authority	abuse@iana.org

■ 115.112.43.81

0 / 94  
Community Score

2 detected files embedding this IP address

115.112.43.81 (115.112.32.0/19)  
AS 4755 (TATA Communications formerly VSNL is Leading ISP)

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

**Files Referring (11)**

Scanned	Detections	Type	Name
2023-08-15	3 / 58	TAR	rules.20200318-180350_mac_vse-3.4.tgz
2024-11-04	0 / 63	TAR	rules.20200424-150352_mac_vse-3.4.tgz
2023-01-01	0 / 43	XML	document.xml
2024-12-29	0 / 66	Office Open XML Document	libredfcpdf_E6nfA_710_0P4nu8y~_~_e685~d.docx
2024-11-03	0 / 63	CSV	winshark.csv
2024-05-07	0 / 59	JavaScript	sguild.log
2024-04-03	0 / 64	Office Open XML Document	27.2.14 Lab - Investigating an Attack on a Windows Host.docx
2023-10-11	0 / 64	Office Open XML Document	e97b86c43b7674c694c4f8034961b0d9b0e7002c97218e207823b63b67b04
2023-03-08	0 / 61	Office Open XML Document	27.2.14 Lab - Investigating an Attack on a Windows Host - LM.docx
2023-02-11	0 / 63	Office Open XML Document	1 Lab 7) Investigating an Attack on a Windows Host - Revision.docx

**Historical Whois Lookups (4)**

Last Updated	Organization	Email
2021-06-10		
2020-05-04	Asia Pacific Network Information Centre	search.apnic-net.arin@apnic.net
2020-01-11	Asia Pacific Network Information Centre	search.apnic-net.arin@apnic.net
2019-11-08	Asia Pacific Network Information Centre	search.apnic-net.arin@apnic.net

■ 209.141.34.8

9 / 94  
Community Score

1094 security vendors flagged this IP address as malicious

209.141.34.8 (209.141.32.0/19)  
AS 53667 (POWNET)

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

**Passive DNS Replication (4)**

Date received	Detections	Resolver	Domain
2024-09-17	0 / 84	ViewTotal	modano-1556-gettingpony.org
2020-05-22	0 / 84	ViewTotal	tasvagas.sbrunc.mpg
2020-06-16	0 / 84	ViewTotal	superdaddy.mpg
2017-08-16	0 / 54	ViewTotal	homeraplanet.us

**Communicating Files (38)**

Scanned	Detections	Type	Name
2024-11-19	28 / 63	MS Word Document	dcab7fd20398b6d48b0ef07c30b0d4d144150
2024-12-20	17 / 61	MS Word Document	6af6f31b6c43d31a12743bcb4812314f7b0d4
2024-12-18	40 / 61	MS Word Document	Microsoft_Word_97_..._2004_Document.doc
2019-06-18	0 / 60	Office Open XML Document	Alena resume no post.docm
2025-01-13	0 / 60	Network capture	captureNetwork2024.pcap
2024-12-23	20 / 60	MS Word Document	Ruben Chiles Resume.doc
2024-12-23	17 / 61	MS Word Document	Helen Thomas Resume.doc
2021-05-20	32 / 63	Office Open XML Document	Homer Aghajani Resume.doc
2019-05-20	0 / 54	Network capture	Lab 3.1 - Extra Lab 3 (Only IP Trace Permitted).pcap
2019-05-09	30 / 61	Office Open XML Document	DecryptedPackage.docm

**Files Referring (35)**

Scanned	Detections	Type	Name
2025-01-14	0 / 61	Network capture	2019-05-01 password protected doc infection traffic.pcap
2025-01-03	12 / 65	Office Open XML Spreadsheet	6f4ebc1b6c43d31a12743bcb4812314f7b0d4
2024-12-18	17 / 61	Network capture	2019-03-08 password protected Word doc pushes Outbox.pcap
2024-12-18	40 / 61	MS Word Document	Microsoft_Word_97_..._2004_Document.doc
2019-02-18	0 / 58	VBA	ThelDocument.doc
2019-06-15	20 / 58	MS Word Document	Helen Thomas Resume3.doc
2019-04-30	42 / 60	MS Word Document	vbaProject.bin
2019-04-15	17 / 58	MS Word Document	Vicky Limmy Resume3.doc
2019-03-08	32 / 63	MS Word Document	vbaProject.bin
2019-03-15	40 / 59	MS Word Document	vbaProject.bin

**Historical Whois Lookups (4)**

Last Updated	Organization	Email
2024-08-07		
2020-08-11	BuyVM Services	admin@frantech.co
2019-12-08	Frantech Solutions	admin@frantech.co
2019-08-24	Frantech Solutions	admin@frantech.co

■ 217.23.14.81

4 / 94  
Community Score

4/94 security vendors flagged this IP address as malicious

217.23.14.81 (217.23.0.0/20)  
AS 49981 (Worldstream B.V.)

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

**Passive DNS Replication (2)**

Date received	Detections	Resolver	Domain
2018-01-28	0 / 84	ViewTotal	h11336.pw

**Communicating Files (35)**

Scanned	Detections	Type	Name
2021-10-21	53 / 68	Win32 EXE	virusign.com_2d062fd3abe747bc0d7f9500bdec2d0.vir
2021-06-20	40 / 68	Win32 EXE	hulen
2021-10-14	40 / 67	Win32 EXE	kennethelena
2021-11-17	52 / 65	Win32 EXE	Arbteggang
2021-03-06	51 / 70	Win32 EXE	Proxy
2025-01-13	0 / 60	Network capture	captureNetwork2024.pcap
2021-10-03	52 / 68	Win32 EXE	Arbteggang
2021-06-26	51 / 69	Win32 EXE	Arbteggang
2021-06-01	50 / 69	Win32 EXE	Pothares
2021-07-26	53 / 68	Win32 EXE	Pothares

**Files Referring (14)**

Scanned	Detections	Type	Name
2019-07-10	0 / 51	Email	hookeAttachedUNSCANNED_3.eml
2019-05-17	14 / 58	unknown	1713.exe
2025-01-13	0 / 60	Network capture	captureNetwork2024.pcap
2025-01-13	0 / 61	Text	Packet_1565
2025-01-13	0 / 61	Text	file.exe
2025-01-13	0 / 60	Text	43
2025-01-01	0 / 48	XML	document.xml
2024-12-29	0 / 66	Office Open XML Document	libredfcpdf_E6nfA_710_0P4nu8y~_~_e685~d.docx
2024-11-03	0 / 63	CSV	winshark.csv
2024-05-07	0 / 59	JavaScript	sguild.log

**Historical Whois Lookups (5)**

Last Updated	Organization	Email
2023-06-04		
2021-06-04		
2021-03-07		
2019-02-12	RIPE Network Coordination Centre	abuse@ripe.net
2019-09-03	RIPE Network Coordination Centre	abuse@ripe.net

## 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](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).