



CIS:3345

Intrusion to Investigation

Part II

Chavez | Turner | Ponce

User Story

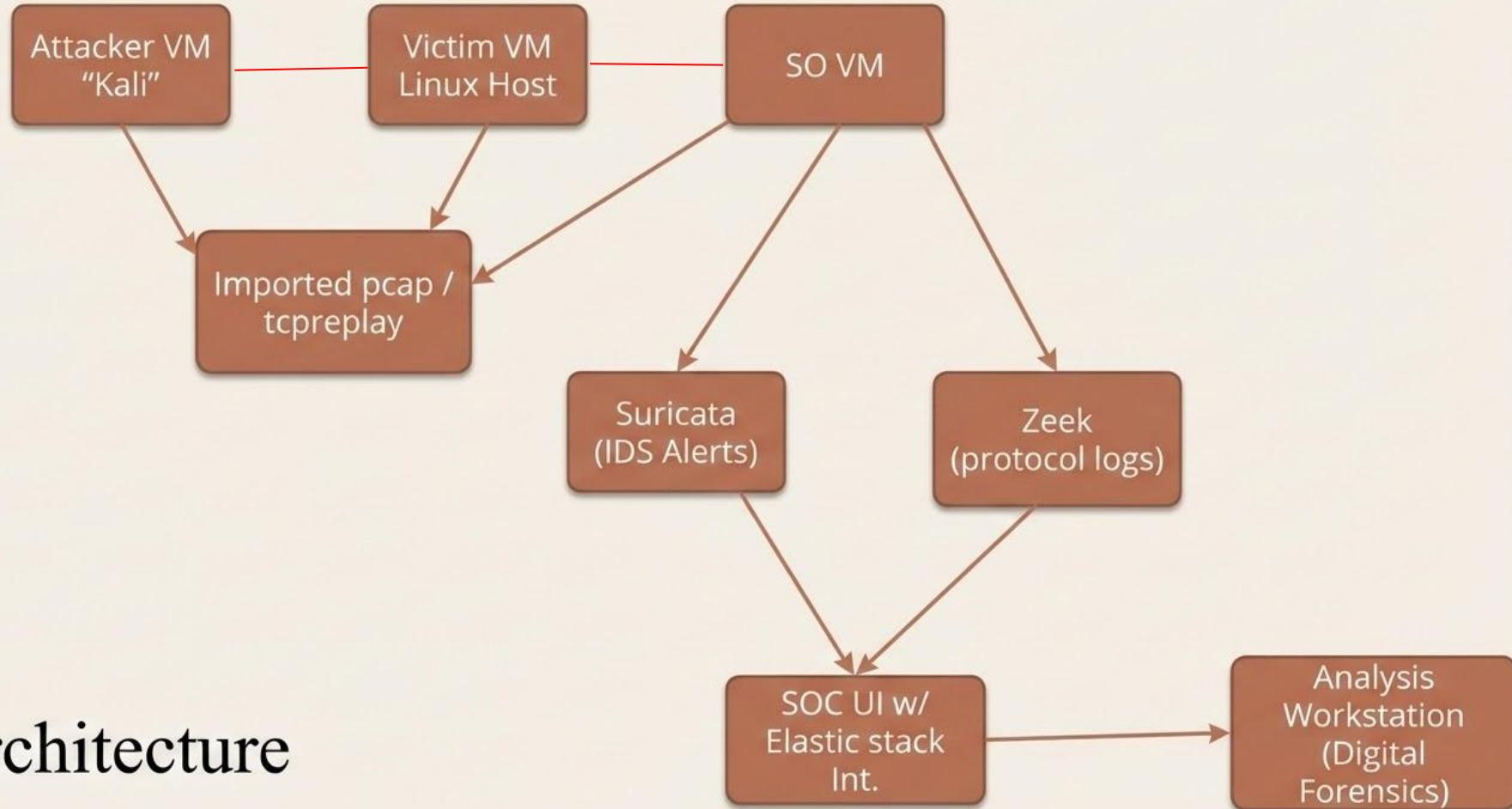
On May 14, 2021, our team was alerted to an intrusion within our system, we as the digital forensics team, and we as the intrusion detection team, were requested to study the case, documented in the GitHub is our findings (Digital Forensics) and our solutions to prevent this from happening in the future (Intrusion Detection). The email was first sent to an employee on May 3rd, which was an excel sheet with the macros for URSNIF. On May 14th another email was sent, that was similar in nature. URSNIF is more commonly referred to as a banking trojan. Originally identified in 2006, there was a GitHub leak of the source code for this trojan. Due to the recent event we, as the IDS team, will be working with the digital forensics team, not only find the root of the problem but also come together and create a solution so that this will not happen again.

Summary of the Project

Our digital forensics project treats the provided pcap as real-world evidence from a suspected malware incident. We define the case scope, document chain-of-custody, and hash the evidence to show it hasn't been altered. Using Wireshark, we reconstruct the attack timeline and extract key artifacts like malicious IPs, domains, and payloads. Finally, we turn those findings into a concise case report with an IOC list and practical recommendations that a blue team could actually deploy.

Materials

- A system with Wireshark
 - VMware
 - Security Onion
 - Kali system run through the VM
 - <https://www.malware-traffic-analysis.net/index.html>
 - Private network, to be able to utilize security onion and its resources without anything blocking or interfering
-



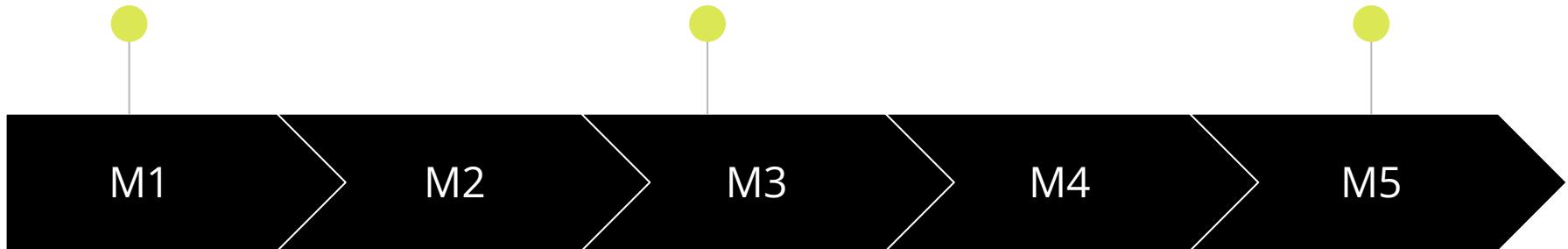
Architecture

MILESTONES

Case scope,
chain-of-custody.

(Optional) Memory/Disk
triage and correlation to
PCAP.

Future work

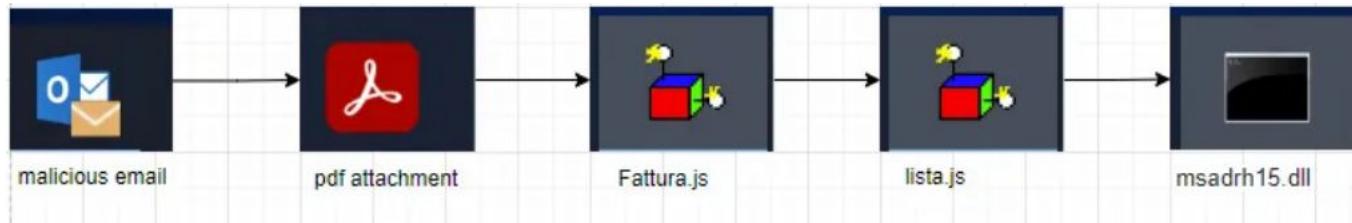


Wireshark
reconstruction +
artifact extraction.

Final case report + IOC
list + recommendations +
demo.

Initial Attack

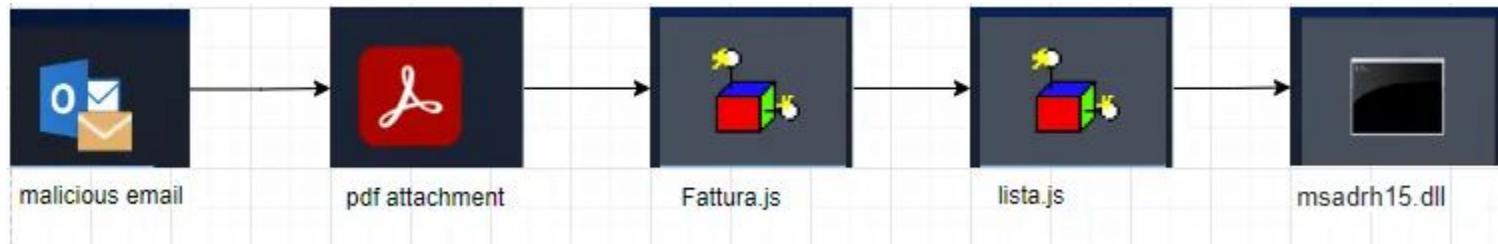
The email was first sent to an employee on May 3rd, which was an excel sheet with the macros for URSNIF. On May 14th another email was sent, that was similar in nature. URSNIF is more commonly referred to as a banking trojan. Originally identified in 2006, there was a GitHub leak of the source code for this trojan. Trojan Path is as follows:



Ursnif, the banking trojan

Ursnif is a variant of the GOZI malware, usually disguises itself as a part of an invoice, was first seen in 2006, but had its script leaked in 2015, making it more accessible to other. So now it has a github:

- <https://github.com/MBCProject/mbc-markdown/blob/main/xample-malware/ursnif.md>



Milestone 1 - Case scope, chain-of-custody, evidence hashing.

- Brief overview of the case
 - Identify evidence
 - Chain of Custody
 - Scope
-

CASE FILE:

First documented on May 3rd a suspicious email was sent to an employee, this email contained an excel sheet with the macros for URSNIF. On May 14th another email was sent, that was similar in nature. URSNIF is more commonly referred to as a banking trojan. Originally identified in 2006, there was a GitHub leak of the source code for this trojan.

Evidence on hand

- Original Email file sent, See Figure 1.
- Pcaps that were sent, See Figure 2.
- Excel sheet attached, See Figure 3.

Original Phishing email (Figure 1)

The screenshot shows an Outlook email window with the following details:

- Subject:** Re: Your [information removed] Application
- To:** "[removed]"@[removed].eu
- From:** "[removed]"@[removed].uk
- Date:** Mon 5/3/2021 9:40 AM
- Attachment:** i8m7XluZbbj10J53.xlsb (94 KB)
- Email Body:**

Here is an update of the project.

Dear [name removed]

>Thank you for submitting your [information removed] application online.

>

>Your payment has been accepted.

>

>Your [information removed] application has been submitted for validation checks. The [information removed] should arrive in the post within 2 weeks.

>

>Please print this page or make a note of the application reference number in case you have a query. You can use your application reference number to check the progress of your application at [information removed].

>

>Application details

>-----

>Name: [name removed]

>Application Reference Number: [information removed]

>

>[information removed]

>-----

>

>[paragraphs removed]

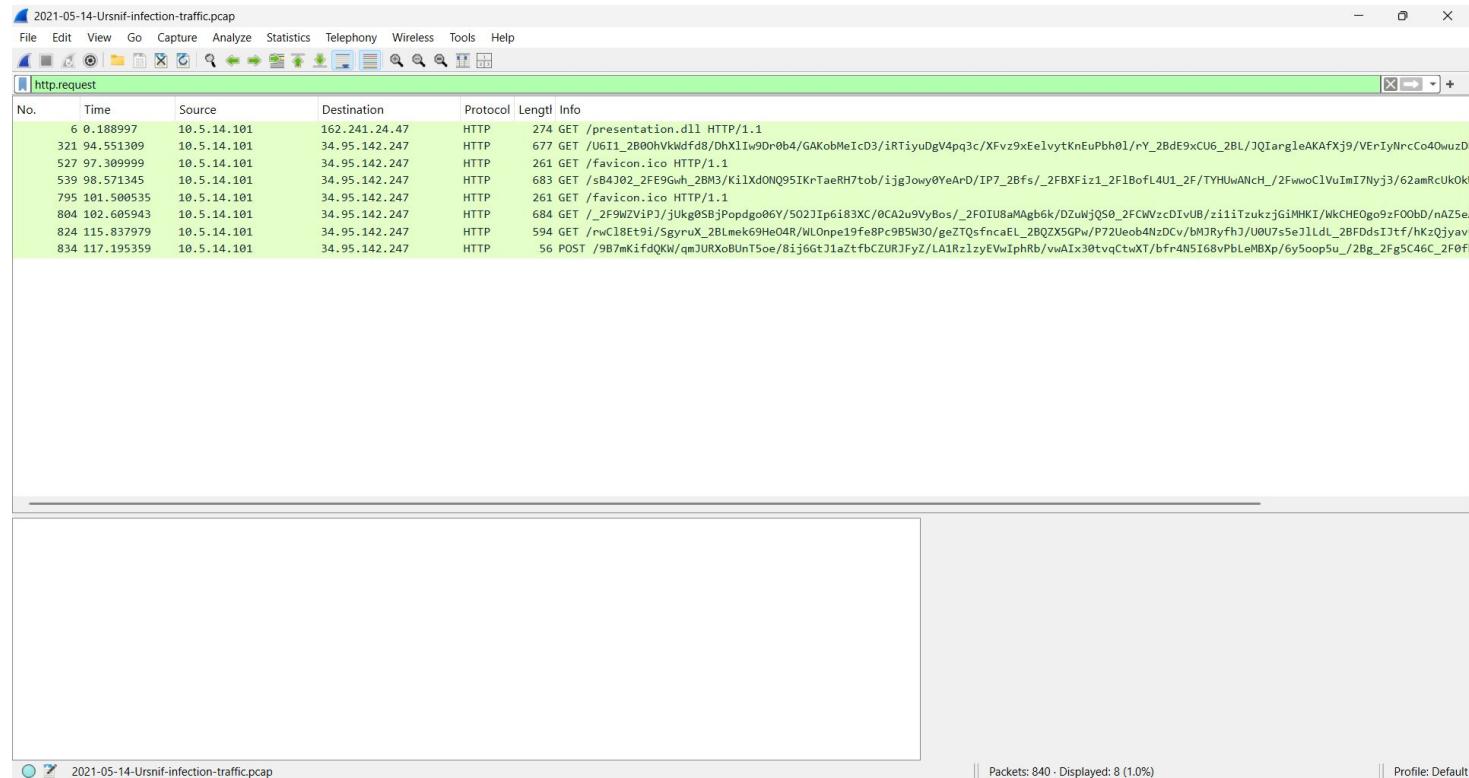
>

>Please do not respond directly to this e-mail address. The originating e-mail account is not monitored

>

>

Wireshark Analysis of Pcap file (Figure 2)



Excel Sheet (Figure 3)

The screenshot shows an Excel spreadsheet window with the following details:

- File Tab:** i8m7XluZbj10I53 • Saved to this PC
- Clipboard Bar:** Cut, Copy, Paste, Format Painter
- Font Group:** Calibri, Size 11, Bold, Italic, Underline, Font Color, Font Style, Alignment, Wrap Text, Merge & Center
- Number Group:** \$, %, , 0.00
- Styles Group:** Conditional Formatting, Format as Table, Cell Styles
- Cells Group:** Insert, Delete, Format, AutoSum, Fill, Clear
- Editing Group:** Sort & Filter, Find & Select, Add-ins

SECURITY RISK: Microsoft has blocked macros from running because the source of this file is untrusted. [Learn More](#)

SIGN IN TO OFFICE: It looks like your stored credentials are out of date. Please sign in as miturner@student.uiwtx.edu so we can verify your subscription. [Sign In](#)

Cell A1: DocuSign® THIS DOCUMENT IS ENCRYPTED BY DOCUSIGN® PROTECT SERVICE
PERFORM THE FOLLOWING STEPS TO PERFORM DECRYPTION

- If this document was downloaded from Email, please click **Enable Editing** from the yellow bar above
- Once You have Enable Editing , please click **Enable Content** from the yellow bar above

WHY I CANNOT OPEN THIS DOCUMENT?

- You are using iOS or Android, please use Desktop PC
- You are trying to view this document using Online Viewer

Bottom navigation bar: SafeForm, +, Ready, 100%

Chain of Custody Chart



CHAIN OF CUSTODY

Submitter Name:	Chavez, Turner, Ponce			Bill to:		
Company:	DF Investigations			Address:	{REDACTED}	
Address:	400 Army Blvd,			City/State:	Zip: _____	
City/State:	San Antonio, Texas	Zip:	78215	PO #:		
Project Information						
Project Name: Phishing Email/ Ursnif			Project Manager: Marissa Turner			
Project #:			Telephone – Office/Cell 210 ### ####			
Reports - Email Address: marissaleighturner@gmail.com						
Invoice - Email Address: DFinvestigation@gmail.com			Notification By: Email: <input type="checkbox"/> Verbal: <input checked="" type="checkbox"/>			
Special Instructions:						
Turnaround Times – Please Select One						
Emergency* <input type="checkbox"/>	1 Day <input type="checkbox"/>	2 Day <input checked="" type="checkbox"/>	3 Day <input type="checkbox"/>	5 Day <input type="checkbox"/>		

Scope

This project designs, implements, and documents an end-to-end workflow that uses Security Onion (Suricata + Zeek) and Wireshark-based digital forensics to detect, reconstruct, and analyze a malware infection in captured network traffic, then produce actionable IOCs, a case report, and a short live demo that shows how detection and investigation work together.

Milestone 2 - Wireshark Reconstruction & Artifact Extraction

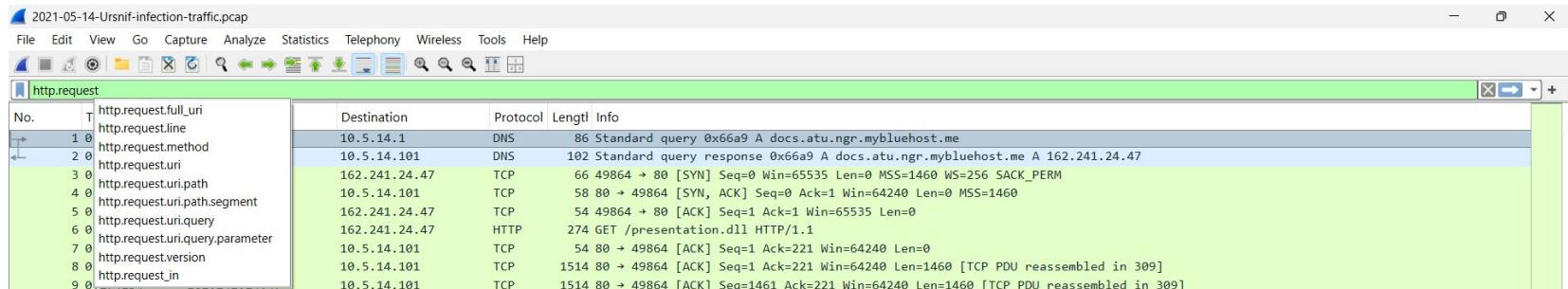
- Configure Wireshark
- Pass Malicious PCAPs
- Draw connections
between entries

M2 - Wireshark Reconstruction



- Disabling noisy traffic
- Customizing columns
- TCP stream

CUSTOM FILTERS



M2 – Malware PCAPs



- Extract the PCAP evidence
 - Identify Top Talkers & Key Protocols
 - Marked suspicious IP addresses
-

Wireshark Analysis of Pcap file

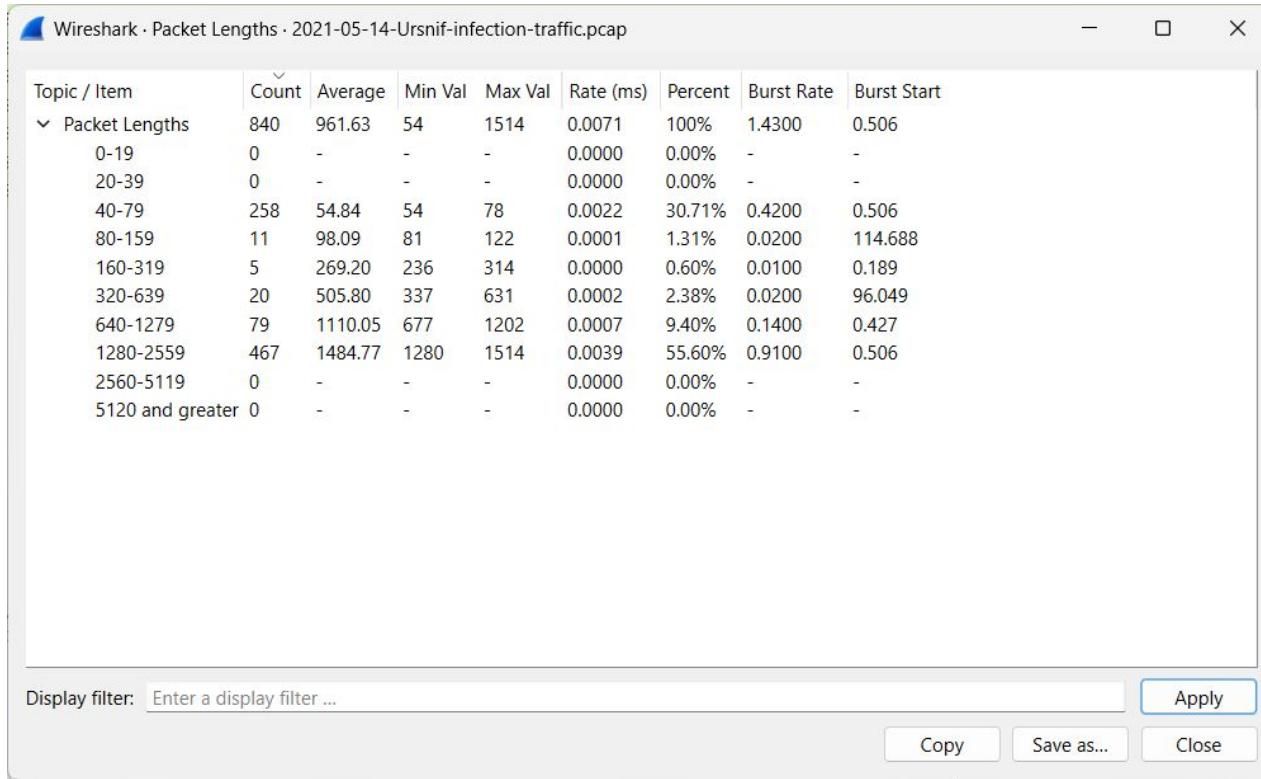
The screenshot shows the Wireshark interface with the following details:

- File Path:** 2021-05-14-Ursnif-infection-traffic.pcap
- Toolbar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Search Bar:** http.request
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info
- Table Data:** A list of 844 rows of network traffic. The first few rows are:

No.	Time	Source	Destination	Protocol	Length	Info
6	0.188997	10.5.14.101	162.241.24.47	HTTP	274	GET /presentation.dll HTTP/1.1
321	94.551309	10.5.14.101	34.95.142.247	HTTP	677	GET /J6II_2B0OhVkfdf8/DhXlIw9Dr0b4/GAKobMeIcD3/iRTiyuDgV4pq3c/XFvz9xEelvytKnEuPbh01/rY_2BdE9xCU6_2BL/JQIargleAKAfXj9/VErIyNrcCo40wuzDf
527	97.309999	10.5.14.101	34.95.142.247	HTTP	261	GET /favicon.ico HTTP/1.1
539	98.571345	10.5.14.101	34.95.142.247	HTTP	683	GET /sB4J02_2FE9Gwh_2BM3/KilXdONQ95IKrTaeRH7tob/ijgJowy0YeArD/IP7_2Bfs/_2FBXFiz1_2F1BofL4U1_2F/TYHuwAnCh_/2FwwoC1VuImI7Nyj3/62amRcUk0k
795	101.500535	10.5.14.101	34.95.142.247	HTTP	261	GET /favicon.ico HTTP/1.1
804	102.605943	10.5.14.101	34.95.142.247	HTTP	684	GET /_2F9WZViPj/jUkg0SBjPopdgo06Y/502JIp6i83XC/_0CA2u9vYBos/_2FOIU8aMgb6k/DzuWjQ50_2FCWVzcDiVUB/ziiiTzukzjGiMHKI/WkCHEOgo9zFOObD/nA25e
824	115.837979	10.5.14.101	34.95.142.247	HTTP	594	GET /rwC18Et9i/SgyruX_2BLmek69He04R/WlOnpe19fe8Pc9BSW30/geZTQsfncalEL_2BQZXSGPw/P72Uebd4NzDCv/bmJ Ryfhj/w0U7s5e1ldl_2BFdsIJtf/hkzQjyavf
834	117.195359	10.5.14.101	34.95.142.247	HTTP	56	POST /9B7mKifdQKw/qmJURXoBuNT5oe/8ij6GtJ1aZtfbCZURJFyZ/LA1RzlzyEVwIphRb/vwAIx30tvqCtwXT/bfr4N5168vPbLeNBXp/6y5oop5u/_2Bg_2Fg5C46C_2f0f

Bottom Status Bar: Packets: 840 · Displayed: 8 (1.0%) · Profile: Default

Wireshark Analysis of Pcap File



Wireshark Statistics (Filtered)

Wireshark - Capture File Properties - 2021-05-14-Ursnif-infection-traffic.pcap

Details

File

Name: C:\Users\maris\Downloads\2021-05-14-Ursnif-traffic-and-malware-and-IOCs\2021-05-14-Ursnif-traffic-and-malware-and-IOCs\2021-05-14-Ursnif-infection-traffic.pcap
Length: 821 kB
Hash (SHA256): d8121c60f63cbab4f04b466395ced4548591fc1b29de74637eeb5dae585fd7e
Hash (SHA1): 28d316f823c5d1247e4a468690cfa1b67055183
Format: Wireshark/tcpdump/... - pcap
Encapsulation: Ethernet
Snapshot length: 65535

Time

First packet: 2021-05-14 10:56:49
Last packet: 2021-05-14 10:58:47
Elapsed: 0:00:15

Capture

Hardware: Unknown
OS: Unknown
Application: Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	840	8 (1.0%)	—
Time span, s	118.317	117.006	—
Average pps	7.1	0.1	—
Average packet size, B	962	436	—
Bytes	807773	3490 (0.4%)	0
Average bytes/s	6827	29	—
Average bits/s	54 k	238	—

Refresh Edit Comments Close Copy To Clipboard Help

Milestone 4 – Final Case Report IOC list recommendations demo

- IOC List
- Practical Recommendations

M4 – IOC list

- Email IOCs
 - File IOCs
-

M4 – Practical Recommendations

- Strengthen web and email defenses
 - Harden endpoints and browsers
 - Improve logging, monitoring, and IOC use
 - Policies, training, and response
-

Key Takeaways

- Treated PCAP as real evidence
 - Case scope, chain of custody
- Wireshark Reconstruction
- Extracted concrete artifacts
- Findings directly tied with IDS side

GITHUB

https://github.com/mwchavez/IDS_DF_F2025_Project_MC_MT_DP

Future Status of the project

- Expand evidence sources
 - Automate IOC extraction
-

Resources used in gathering information

- <https://www.malware-traffic-analysis.net/2021/05/14/index.html>
- <https://github.com/MBCProject/mbc-markdown/blob/main/xample-malware/ursnif.md>
- <https://www.acronis.com/en/tru/posts/ursnif-the-banking-trojan/>
- <https://attack.mitre.org/software/S0386/>



Thank You!!

