The Data Dig

CodePath CYB102 Pod 32

Agenda:

1. Introductions
2. Dataset/Playbook/Tools
3. Findings
4. Impact of Incident
5. Lessons Learned

1. Introduction

Who We Are

Laith Darras
He/Him/His

Cara Failer
She/Her/Hers

Esha Sidhu
She/Her/Hers

Ajitpal Singh
He/Him/His

Rudy Cazares
He/Him/His

2. Dataset

Exploring CICIDS2017 Dataset

- Source: Canadian Institute for Cybersecurity (CIC) at the University of New Brunswick
- Creators: Iman Sharafaldin, Arash Habibi Lashkari, Ali A. Ghorbani

- Content:
  - Network traffic captures in PCAP format
  - CSV files optimized for machine learning

- Attack Types: DDoS, brute-force, and botnet attacks
- Servers, Laptops, Cell Phones are all affected

Exploring CICIDS2017 Dataset

Hypotheses:

- DDoS attacks show unique patterns vs others
- Most attacks exploit HTTP, HTTPS, FTP packet transfers
- All listed attacks will have corresponding CVEs

Playbook

Incident Response Consortium

- Diversity of Scenarios
  - Different types of attacks
- Clear Guidelines
  - Each phase of incident response is detailed well
- Industry Recognition
  - Reputable source in cybersecurity, enhancing the credibility of our response strategy

Tools

Wireshark

- Detailed packet analysis
- Assess severity of attacks

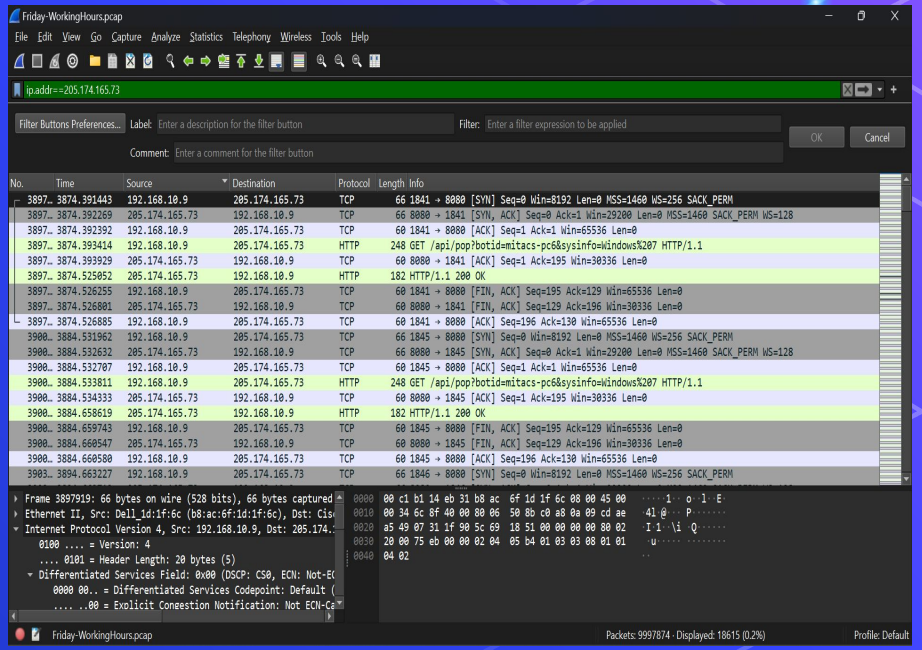
Catalyst

- Incident documentation, response coordination
- Analysis of incident data
- Remediation strategies

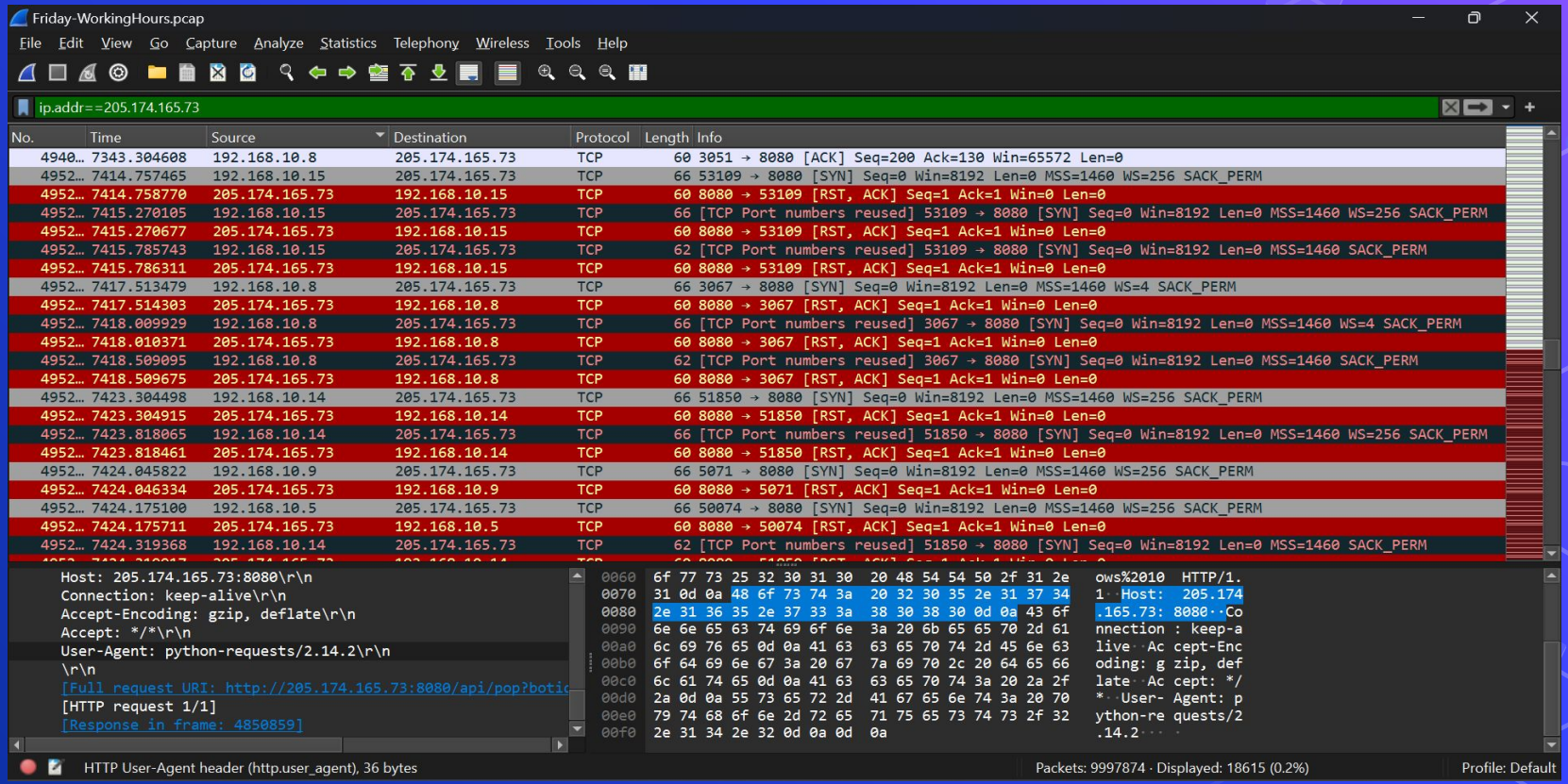
3. Findings

What Happened?

- The victim sent a packet to the malicious IP address using TCP protocol.
- Once the TCP 3-Way handshake was initiated, the malicious IP address sent a series of bots using a python script to the victim's IP address.
- Eventually the attack caused too much congestion, preventing SYN and ACK responses to go through.



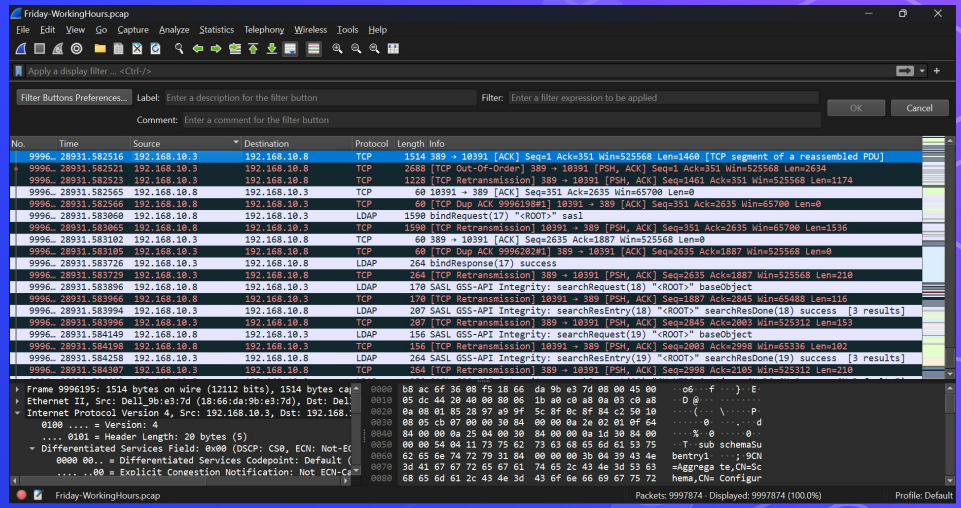
Botnet ARES Attack



4. Impact of Incident

Impact Analysis

- Threat actors:
  - Botnet ARES attack (IP 205.174.165.73) = High Severity
- Disruptions to network infrastructure and user interactions



Packet Above:

- Excessive TCP DUP ACKs
  - Indicates potential network congestion

Incident Response

What happened when we followed the playbook to “respond” to the incident?

- Identify and analyze threat actors and IoCs
- Ongoing surveillance against dynamic cyber threats

Relevant Data and Monitoring Sources on Identification

- Packet analysis data collection
- Useful for understanding attack strategies

5. Lessons Learned

Remediation

- **Response Effectiveness:** Our response was swift and coordinated, thanks in large part to the integration of our IDS with other security systems.
- **Improvement Areas:** We need to focus on reducing the time between threat detection and complete remediation. Improving our patch management process and updating our security configurations more frequently could prevent similar incidents.

Reflection

Was our hypothesis correct?

- The hypothesis about the Botnet ARES attack aligning with a DDoS pattern was correct.
- The attack formulated unique patterns, confirming the hypothesis

What was new or surprising to us?

- The usage of a python script to deploy bots was new to us
- The congestion causing a disruption to SYN and ACK responses were unexpected

Reflection

The role of playbooks in incident response?

- Playbooks provide comprehensive guides for structured incident response
- Automated and manual tasks specified in playbooks aid in mitigating attacks

The threat event dataset analysis?

- Thorough analysis using Wireshark discovering network patterns

Importance of documentation?

- VERY important for understanding the severity and impact of incidents
- Documented response strategies guide effective incident mitigation

Thanks!