

# The Data Dig

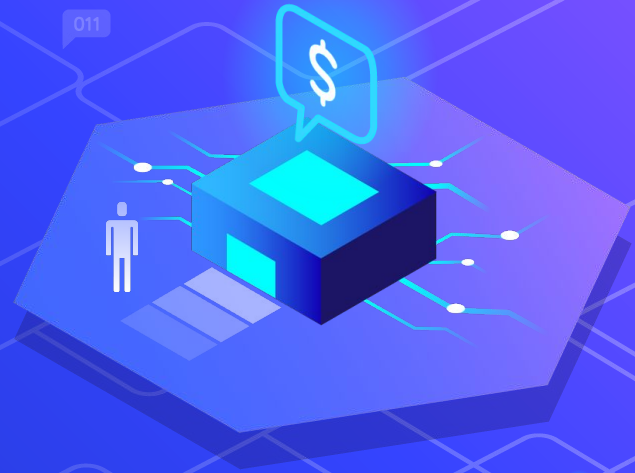
CodePath CYB102 Pod 32



# “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

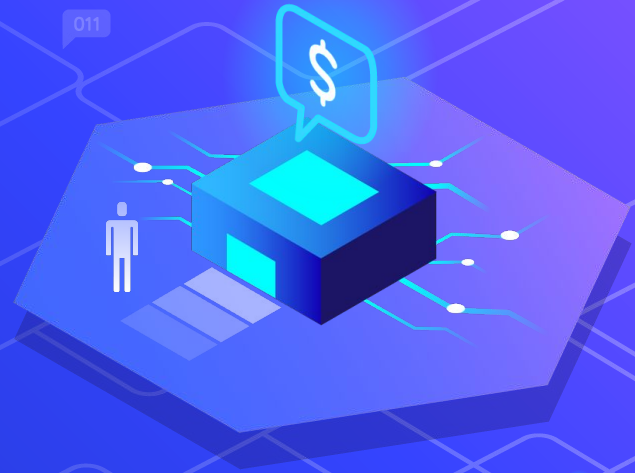


Ajitpal Singh  
He/Him/His



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

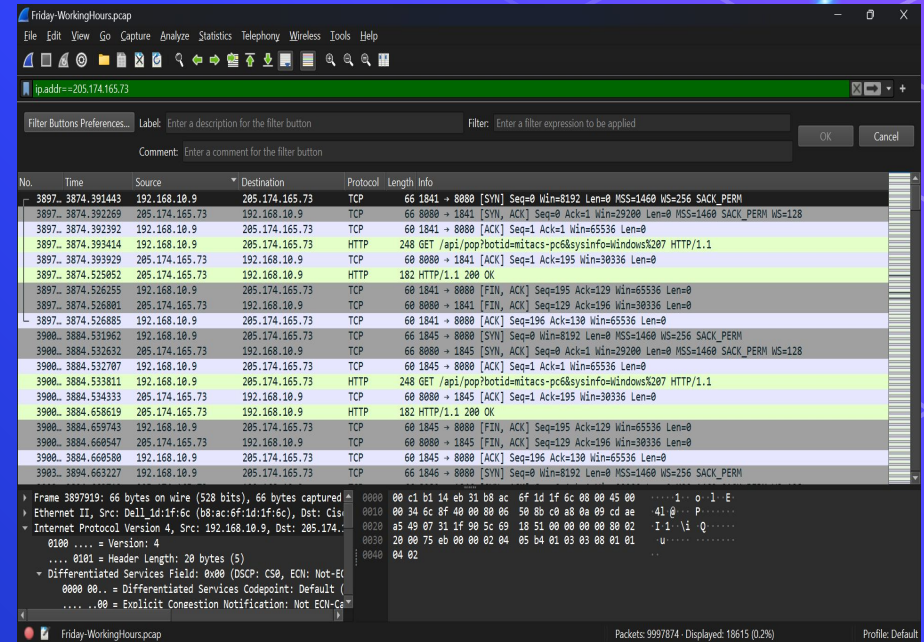
- ⬡ Incident documentation, response coordination
- ⬡ Analysis of incident data
- ⬡ Remediation strategies



# 3. Findings



- 14





# Botnet ARES Attack

Friday-WorkingHours.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==205.174.165.73

No.	Time	Source	Destination	Protocol	Length	Info
4940...	7343.304608	192.168.10.8	205.174.165.73	TCP	60	3051 → 8080 [ACK] Seq=200 Ack=130 Win=65572 Len=0
4952...	7414.757465	192.168.10.15	205.174.165.73	TCP	66	53109 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4952...	7414.758770	205.174.165.73	192.168.10.15	TCP	60	8080 → 53109 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4952...	7415.270105	192.168.10.15	205.174.165.73	TCP	66	[TCP Port numbers reused] 53109 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4952...	7415.270677	205.174.165.73	192.168.10.15	TCP	60	8080 → 53109 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4952...	7415.785743	192.168.10.15	205.174.165.73	TCP	62	[TCP Port numbers reused] 53109 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM
4952...	7415.786311	205.174.165.73	192.168.10.15	TCP	60	8080 → 53109 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4952...	7417.513479	192.168.10.8	205.174.165.73	TCP	66	3067 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4952...	7417.514303	205.174.165.73	192.168.10.8	TCP	60	8080 → 3067 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4952...	7418.009929	192.168.10.8	205.174.165.73	TCP	66	[TCP Port numbers reused] 3067 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4952...	7418.010371	205.174.165.73	192.168.10.8	TCP	60	8080 → 3067 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4952...	7418.509095	192.168.10.8	205.174.165.73	TCP	62	[TCP Port numbers reused] 3067 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM
4952...	7418.509675	205.174.165.73	192.168.10.8	TCP	60	8080 → 3067 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4952...	7423.304498	192.168.10.14	205.174.165.73	TCP	66	51850 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4952...	7423.304915	205.174.165.73	192.168.10.14	TCP	60	8080 → 51850 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4952...	7423.818065	192.168.10.14	205.174.165.73	TCP	66	[TCP Port numbers reused] 51850 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4952...	7423.818461	205.174.165.73	192.168.10.14	TCP	60	8080 → 51850 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4952...	7424.045822	192.168.10.9	205.174.165.73	TCP	66	5071 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4952...	7424.046334	205.174.165.73	192.168.10.9	TCP	60	8080 → 5071 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4952...	7424.175100	192.168.10.5	205.174.165.73	TCP	66	50074 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4952...	7424.175711	205.174.165.73	192.168.10.5	TCP	60	8080 → 50074 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4952...	7424.319368	192.168.10.14	205.174.165.73	TCP	62	[TCP Port numbers reused] 51850 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM

Host: 205.174.165.73:8080\r\nConnection: keep-alive\r\nAccept-Encoding: gzip, deflate\r\nAccept: \*/\*\r\nUser-Agent: python-requests/2.14.2\r\n\r\n[Full request URI: http://205.174.165.73:8080/api/pop?botid=1]\r\n[HTTP request 1/1]\r\n[Response in frame: 4850859]

HTTP User-Agent header (http.user\_agent), 36 bytes

Packets: 9997874 · Displayed: 18615 (0.2%) Profile: Default

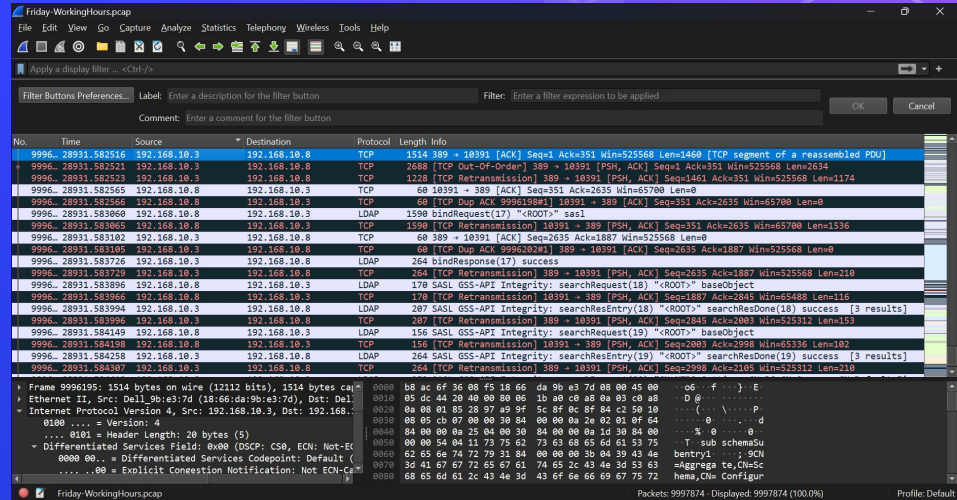


## 4. Impact of Incident



# 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!

