CICIDS 2017

Alex jimenez, Victor Perez, Leonel Kachie, Landen Chambers, David Hernandez

Introduction

In this project, we explore the **CICIDS 2017** dataset, a widely-used, open-source dataset for cybersecurity research. Created by the **Canadian Institute for Cybersecurity (UNB).** Each network flow is labeled with its traffic type — like BENIGN, DDoS, PortScan, or Web Attack – Brute Force. These labels were added by the CICIDS team during controlled simulations, meaning we have ground truth for every entry. By analyzing the frequency of each label, we determine the dominant activity (e.g., normal traffic, or an ongoing attack).

What we know is in the data set

- 1. Friday Afternoon – DDoS Attack- What happened: There was a Distributed Denial of Service (DDoS) attack.
- How we know: Out of about 225,000 network flows, over 128,000 are labeled “DDoS”. That’s more than half the traffic during that session, meaning a massive attack was flooding the network with requests to overwhelm it.

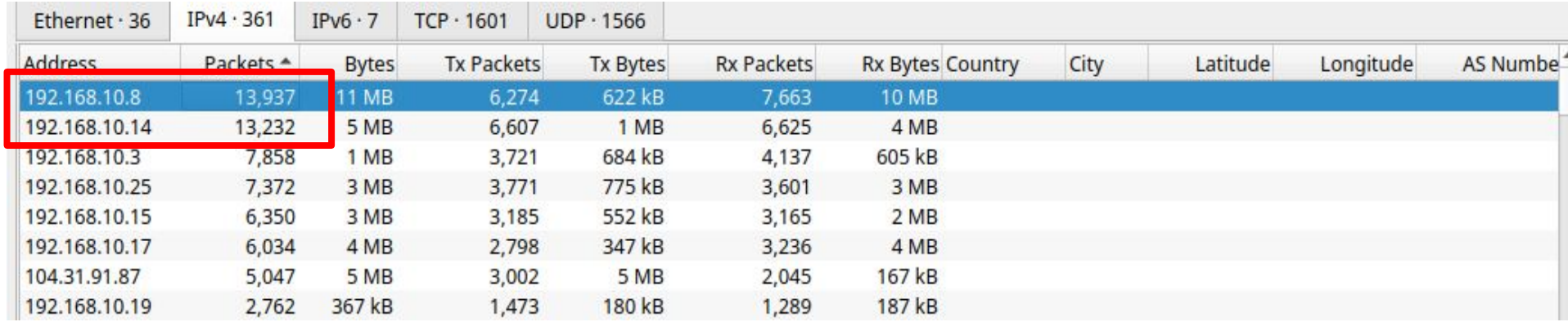
- 3. Friday Afternoon – Port Scanning
- What happened: Someone was scanning the network for open ports — a common way to look for weaknesses before an attack. How I know: The file has over 158,000 “PortScan” labeled flows, meaning a system was methodically checking different ports to see which ones were open and exploitable

- 5. Thursday Afternoon – Infiltration Attempt: A rare but serious infiltration attempt occurred.
- Although there were only 36 flows labeled “Infiltration”, they stand out because this type of label indicates a more advanced attack — possibly involving malware or lateral movement inside the network.

- 2. Thursday Morning – Web-Based Attacks: The system experienced multiple types of web attacks.
- The dataset includes flows labeled as: Brute Force: 1,507 times (trying to guess passwords), XSS: 652 times (injecting malicious scripts), SQL Injection: 21 times (targeting the database).

- 4. Tuesday Working Hours – Brute Force on Services: Attackers were trying to break into FTP and SSH services. The flows are labeled “FTP-Patator” (7,938) and “SSH-Patator” (5,897) — both of which are brute-force tools used to guess login credentials repeatedly.

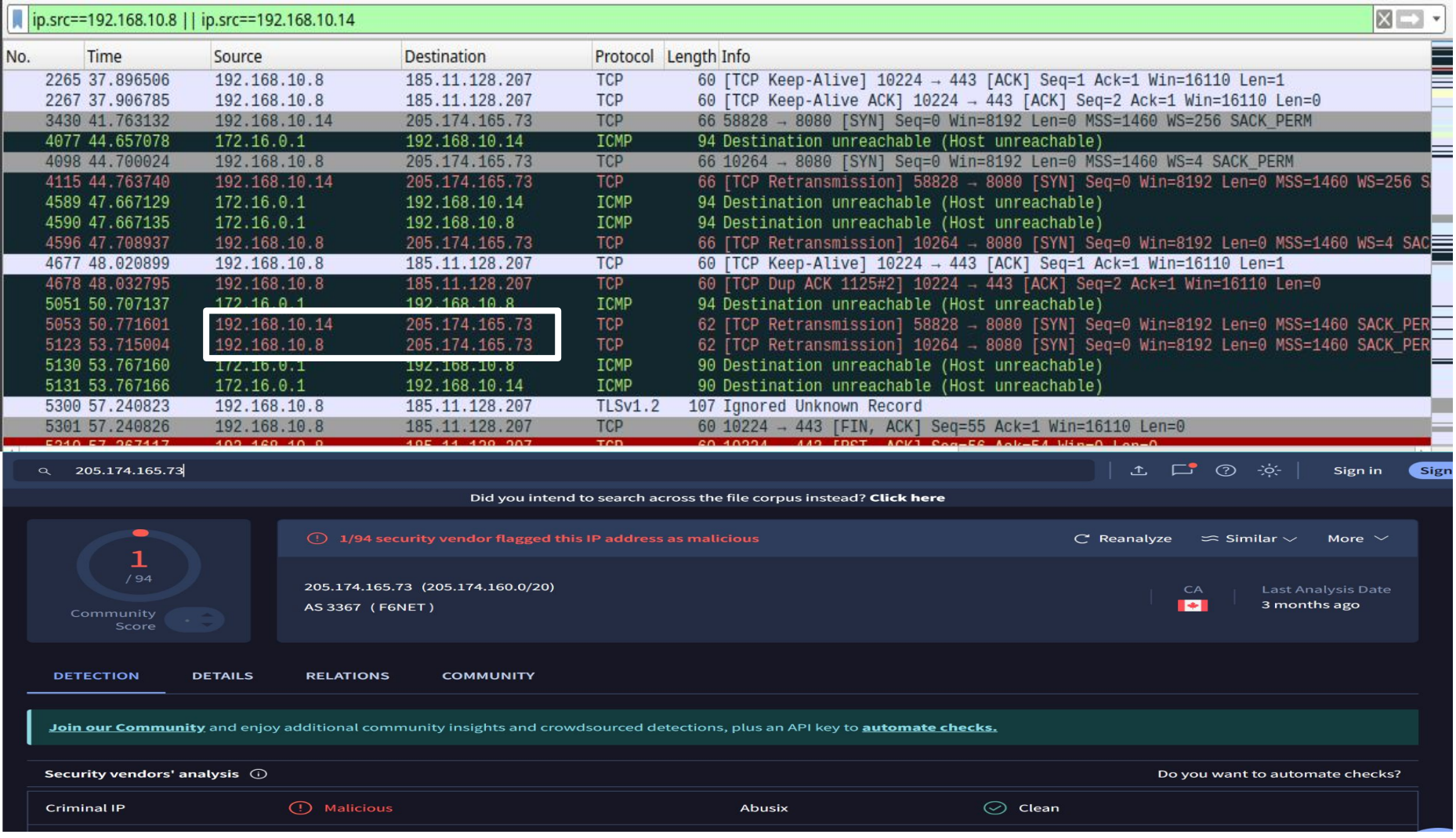
Phase 1: Detection



Ethernet · 36 | IPv4 · 361 | IPv6 · 7 | TCP · 1601 | UDP · 1566

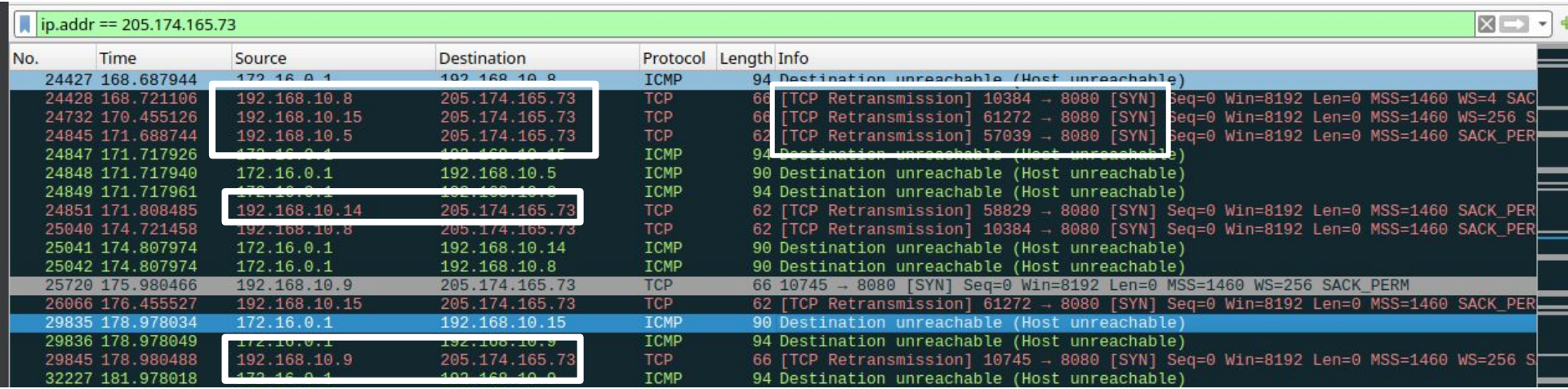
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Numbe
192.168.10.8	13,937	11 MB	6,274	622 kB	7,663	10 MB					
192.168.10.14	13,232	5 MB	6,607	1 MB	6,625	4 MB					
192.168.10.3	7,858	1 MB	3,721	684 kB	4,137	605 kB					
192.168.10.25	7,372	3 MB	3,771	775 kB	3,601	3 MB					
192.168.10.15	6,350	3 MB	3,185	552 kB	3,165	2 MB					
192.168.10.17	6,034	4 MB	2,798	347 kB	3,236	4 MB					
104.31.91.87	5,047	5 MB	3,002	5 MB	2,045	167 kB					
192.168.10.19	2,762	367 kB	1,473	180 kB	1,289	187 kB					

WireShark: Statistics -> endpoints
we see there is 2 ip addresses associated with high amounts of packets


ip.src==192.168.10.8 || ip.src==192.168.10.14
No. Time Source Destination Protocol Length Info
2265 37.896506 192.168.10.8 185.11.128.207 TCP 60 [TCP Keep-Alive] 10224 → 443 [ACK] Seq=1 Ack=1 Win=16110 Len=1
2267 37.906785 192.168.10.8 185.11.128.207 TCP 60 [TCP Keep-Alive ACK] 10224 → 443 [ACK] Seq=2 Ack=1 Win=16110 Len=0
3430 41.763132 192.168.10.14 205.174.165.73 TCP 66 58828 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4077 44.657078 172.16.0.1 192.168.10.14 ICMP 94 Destination unreachable (Host unreachable)
4098 44.700024 192.168.10.8 205.174.165.73 TCP 66 10264 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
4115 44.763740 192.168.10.14 205.174.165.73 TCP 66 [TCP Retransmission] 58828 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 S
4589 47.667129 172.16.0.1 192.168.10.14 ICMP 94 Destination unreachable (Host unreachable)
4590 47.667135 172.16.0.1 192.168.10.8 ICMP 94 Destination unreachable (Host unreachable)
4596 47.708937 192.168.10.8 205.174.165.73 TCP 66 [TCP Retransmission] 10264 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SAC
4677 48.020899 192.168.10.8 185.11.128.207 TCP 60 [TCP Keep-Alive] 10224 → 443 [ACK] Seq=1 Ack=1 Win=16110 Len=1
4678 48.032795 192.168.10.8 185.11.128.207 TCP 60 [TCP Dup ACK 1125#2] 10224 → 443 [ACK] Seq=2 Ack=1 Win=16110 Len=0
5051 50.707137 172.16.0.1 192.168.10.8 ICMP 94 Destination unreachable (Host unreachable)
5053 50.771601 192.168.10.14 205.174.165.73 TCP 62 [TCP Retransmission] 58828 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PER
5123 53.715004 192.168.10.8 205.174.165.73 TCP 62 [TCP Retransmission] 10264 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PER
5130 53.767160 172.16.0.1 192.168.10.8 ICMP 90 Destination unreachable (Host unreachable)
5131 53.767166 172.16.0.1 192.168.10.14 ICMP 90 Destination unreachable (Host unreachable)
5300 57.240823 192.168.10.8 185.11.128.207 TLSv1.2 107 Ignored Unknown Record
5301 57.240826 192.168.10.8 185.11.128.207 TCP 60 10224 → 443 [FIN, ACK] Seq=55 Ack=1 Win=16110 Len=0
205.174.165.73
Sign in
Sign
Did you intend to search across the file corpus instead? Click here
1
/ 94
Community Score
1/94 security vendor flagged this IP address as malicious
Reanalyze
Similar
More
205.174.165.73 (205.174.160.0/20)
AS 3367 (F6NET)
CA
Last Analysis Date
3 months 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?
Criminal IP
Malicious
Abusix
Clean

Phase 2: Analysis

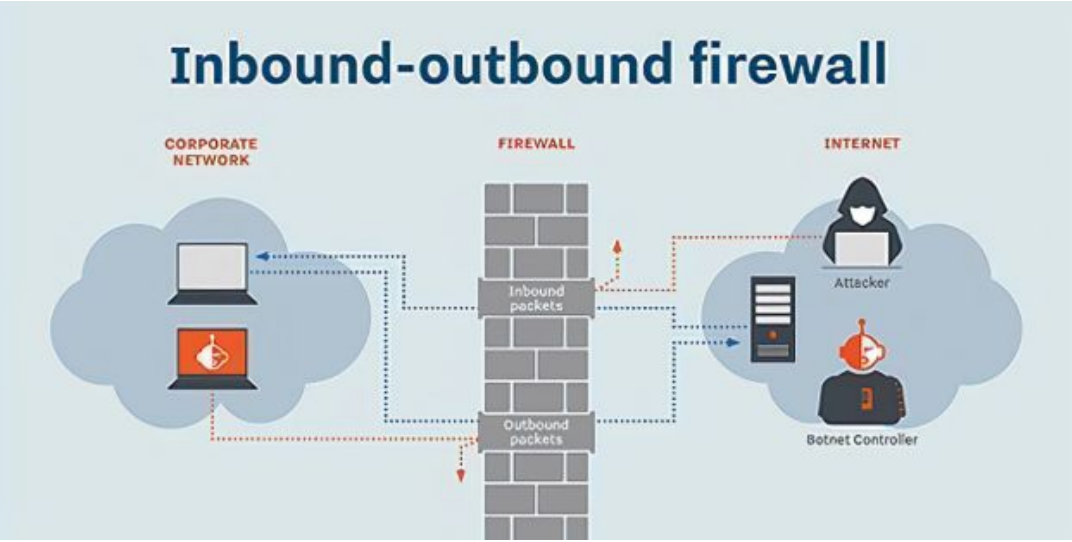
- **TCP Retransmission** (handshake not completed) is being sent multiple times to 5 different victims
- Going through **port 8080**
- **Victims IP:** 192.168.10.5, .8, .9, .15, .14
- **Attacker:** 205.174.165.73



Phase 3: Preventing the attack

- Block outbound access from the **victim IP** addresses to **205.174.165.73** on the company firewall or proxy

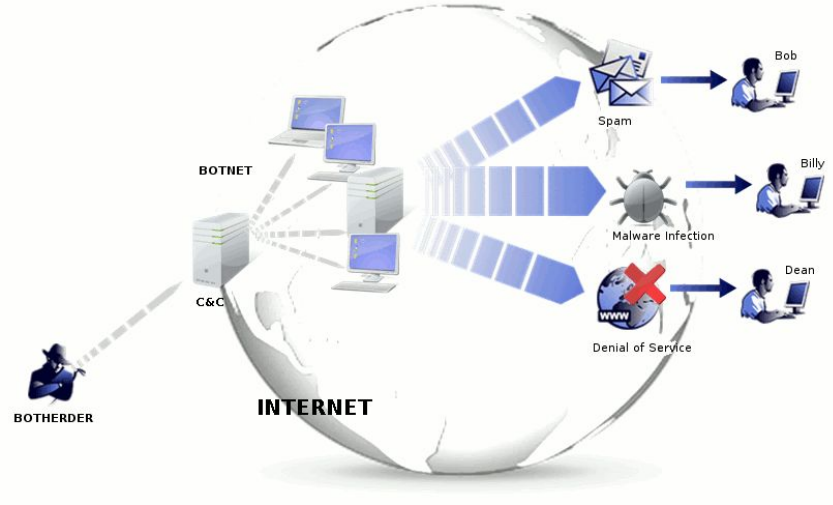
- Add the malicious IP to a blocklist or threat intel feed



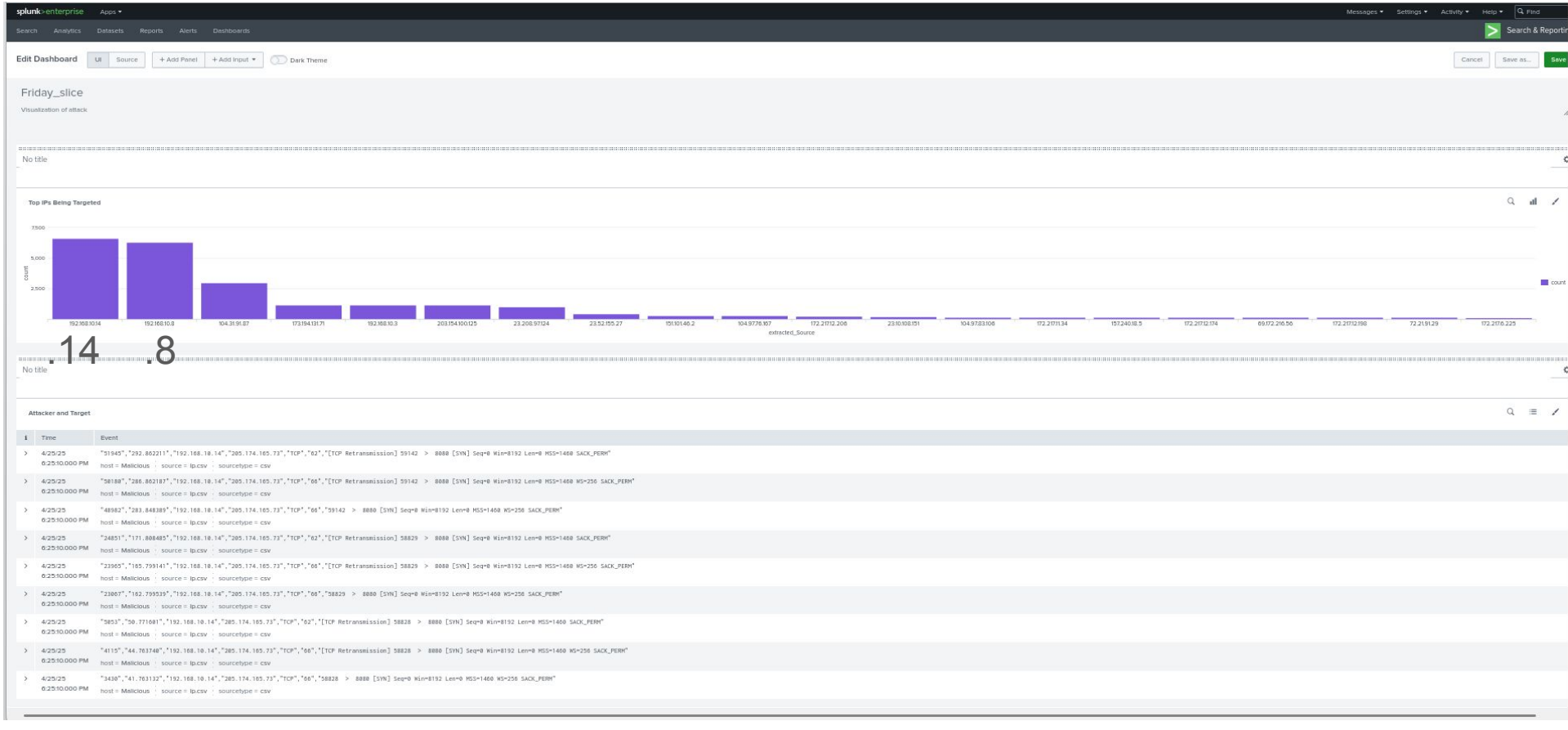
Enterprise Cybersecurity Solutions | Comcast Business

Phase 4: Eradication / Recovery

- Check for stealthy ways an attacker can stay on the machines (scripts set on autoruns scheduled tasks)
- Scan the systems for botnet malware
- possible created or compromised accounts
- Kill C2 connections (prevent remote access)
-
- Allow traffic from affected systems slowly and monitor in Wireshark
- Ensure systems no longer reach out to C2 IPs (205.174.165.73)



Phase 6: Lessons Learned / Reporting



Catalyst Report

Incident #10092: CICIDS 2017 - DDos, Brute Force, and Infiltration Events

Open · 2025-04-25 11:16:33 · 2025-04-26 12:26:23

Details CHANGE TEMPLATE

Severity: High

TLP

Description

The CICIDS 2017 dataset revealed multiple simulated attack events across different days. On a friday afternoon, a DDoS attack, brute force attacks targeting FTP and SSH services, port scanning, web-based attacks (Brute Force, XSS, SQLi), and an infiltration attempt were recorded. During analysis, a significant volume of packet flows was observed between two IP adresses. Further investigation revealed repeated TCP retransmissions associated with IP address 205.174.165.73 communicating over port 8080. The presence of multiple retransmissions indicates a high likelihood of botnet activity or SYN flood attack.

- IP Address, 205.174.165.73, Attacker IP Adress — Unknown — 0
- IP Address, 192.168.19.5, Victim IP Adress — Unknown — 0
- IP Address, 192.168.19.8, Victim IP Adress — Unknown — 0
- IP Address, 192.168.19.9, Victim IP Adress — Unknown — 0
- IP Address, 192.168.19.14, Victim IP Adress — Unknown — 0
- IP Address, 192.168.19.15, Victim IP Adress — Unknown — 0
- Port, 192.168.19.15, TCP Malicious Traffic Port — Unknown — 0

admin today, 12:03 AM
No C2 connections observed after blocking attacker IP

admin today, 12:03 AM
Scanning systems for malware persistence (botnet indicators)

admin today, 12:03 AM
Recommending blocking outbound connections to 205.174.165.73

admin today, 12:02 AM
Confirmed attacker IP= 205.174.165.73 and victim IP= 192.168.10.5,.8,.9,.14,.15

admin today, 12:01 AM
Reviewed Wireshark capture, identified multiple TCP SYN retransmissions from 205.174.165.73 targeting victims

CreateTicket · **admin** · today, 11:16 PM

References

Canadian Institute for Cybersecurity. *Index of /CICDataset/CIC-IDS-2017/Dataset*. University of New Brunswick. Accessed 25 Apr. 2025. http://205.174.165.80/CICDataset/CIC-IDS-2017/Dataset/.

Canadian Institute for Cybersecurity. *IDS 2017* | *Datasets* | *Research*. University of New Brunswick, 2017. Accessed 25 Apr. 2025. https://www.unb.ca/cic/datasets/ids-2017.html.

DDoS Incident Response Workflow. IncidentResponse.com. Accessed 25 Apr. 2025. https://incidentresponse.com/mini-sites/workflows/download/DDoS.pdf.

VirusTotal. *IP Address Report: 205.174.165.73*. VirusTotal, Google, Accessed 25 Apr. 2025. https://www.virustotal.com/gui/ip-address/205.174.165.73.