Response to DDoS Attacks

FITCE INTERNATIONAL CONGRESS

26-28 September 2024, Kraków, Poland

PLAY | iliad GROUP

Agenda

- Incident

  (incident management process, communication, reporting, recommendations)
- Visibility
- Technology
- Service
- Collaboration
- Trust

Tomasz Kędziora

Director of the IT Infrastructure and Security Department, CISO

P4 Sp. z o.o.

Incident

Let's assume that a **DDoS attack was reported** at 8:40 a.m. and its target was one of the provided telecommunications services

Ready…

Cyber-attack

…start

Detection and Analysis

Incident:

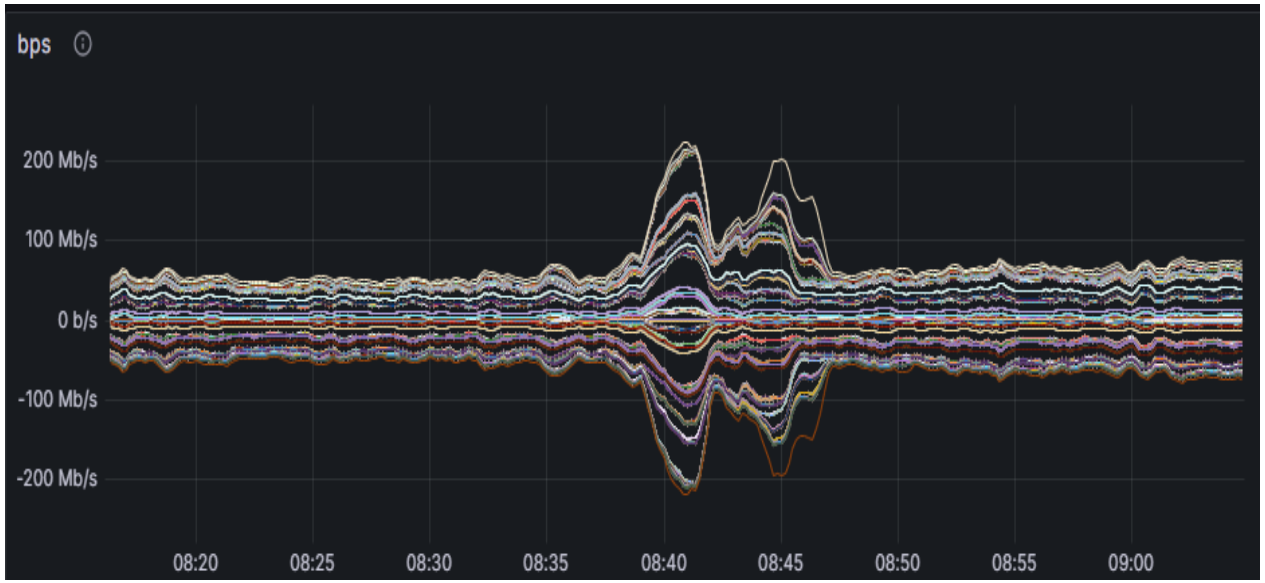
- Initial analysis and **classification of the incident**
- Context and **area of impact**

PLAY | iliad GROUP

Launching the incident management process

Preliminary analysis results:

- DDoS attack of **230 Mb/s** observed
- Anti-DDoS systems **activated automatically**



Main tasks:

- Determining the exact moment **when** the incident started
- **Neutralizing** the incident and its effects

PLAY | iliad GROUP

Obtaining information and communicating

Background of the incident:

- DDoS attacks are common
- Poland's support for Ukraine

What needs to be determined:

- **Are monitoring and collaboration services operational?**
- **Are experts and specialists available?**
- What services or assets were attacked?
- Are all services and assets operational and working?
- Are Anti-DDoS mechanisms operational?
- Is the IP layer overloaded/Are links saturated?
- Which IP traffic exchange points are being used for the attack?

Communication and cooperation:

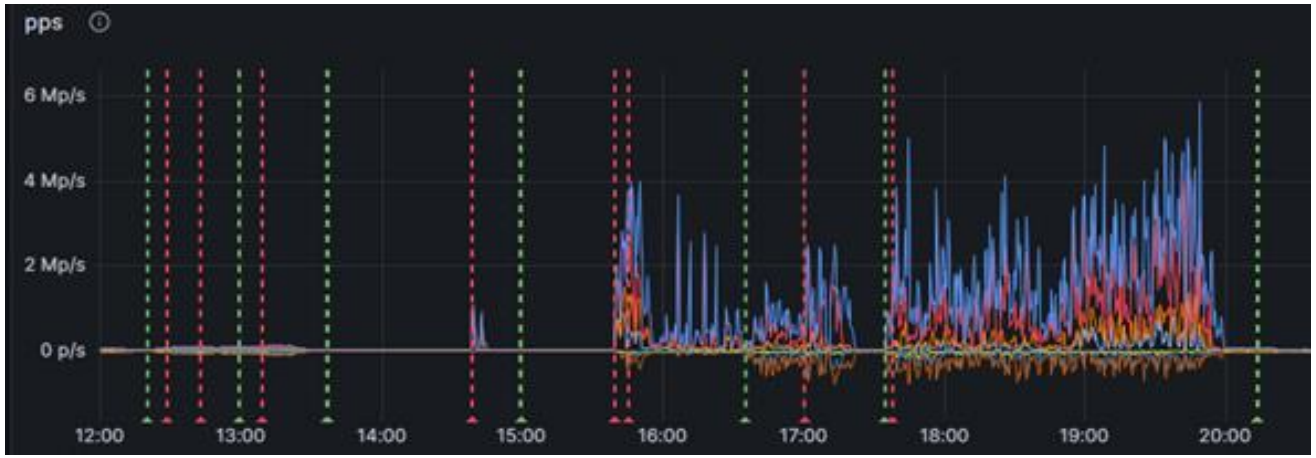
- Between Teams in the organization
- To the Management Board, if necessary
- With the relevant authorities

PLAY | iliad GROUP

Details and observations

Details:

- Duration **~20 hours**
- At peak over **500 Gb/s**, average **~200 Gb/s**
- Methods used: **IP Fragmentation, TCP SYN, UDP, DNS Amplification, WSD Amplification, TCP RST, SSDP Amplification, TCP ACK**



Observation:

- Continuous querying of **one URL**
- A sequence of **several hundred** related attacks
- Incorrect and valid requests to an existing URL **using a botnet**

PLAY | iliad GROUP

Report and recommend

Report:

- Incident details
- Actions taken during incident handling
- Unavailability of resources or services, if any
- What worked and what didn't

Examples:

- Routers **capacity should be increased**
- It is necessary to change the approach and **block all suspicious IP addresses**, not just those already involved in the attack
- Some services/resources were **temporarily unavailable** because they did not have Anti-DDoS protection
- It is necessary **to plan the architecture and implement a new** Anti-DDoS solution (for all services/assets)

Recommend:

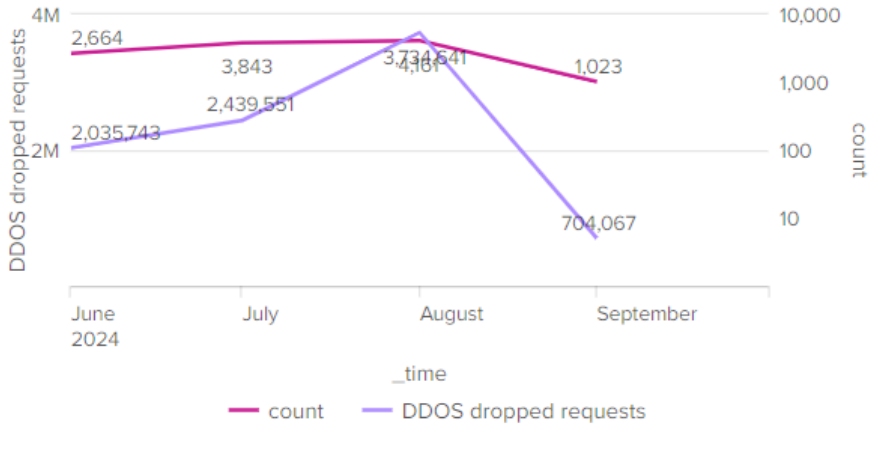
- Necessary changes in the incident management process
- Necessary changes in the solutions used or services provided

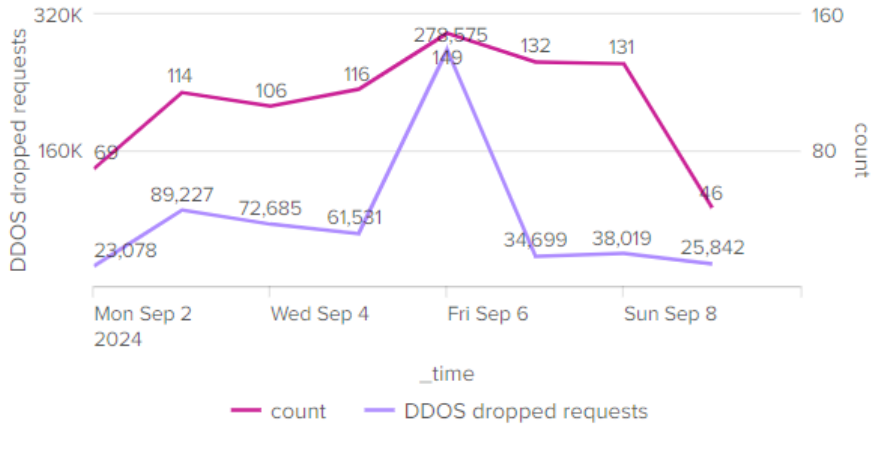
PLAY | iliad GROUP

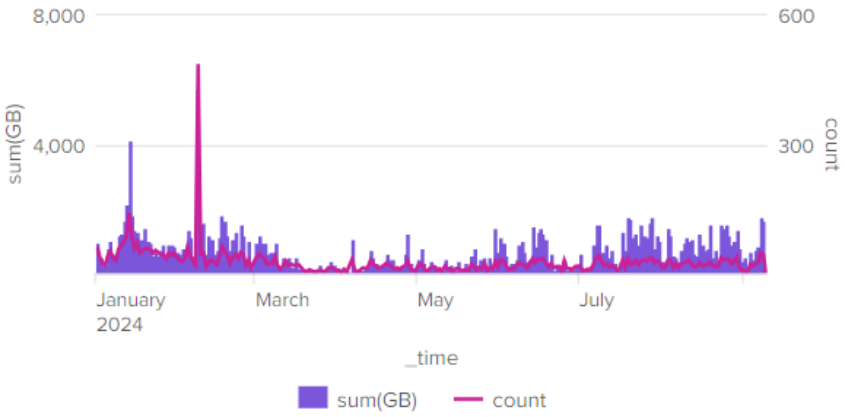
Visibility (*monitoring*)

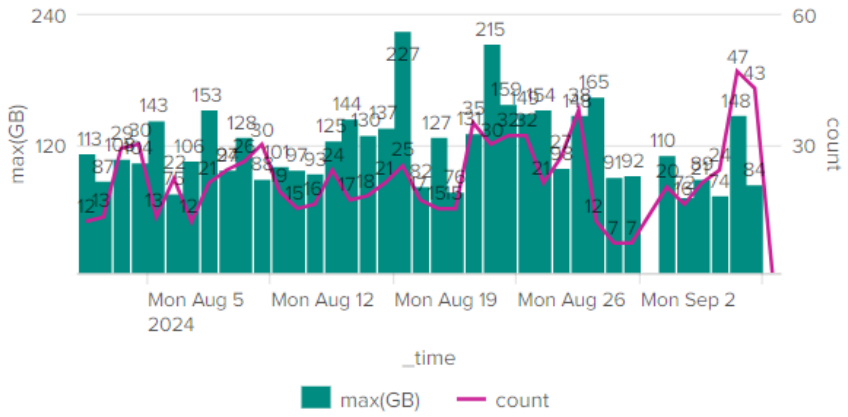
Follow:

- Trends
- Details
- Changes/deviations









CIDR	IP	misuse_types	max(GB)
5.173.0.0	5.173.0.0	Total Traffic	110
188.33.0.0	188.33.0.0	Total Traffic	148
94.254.0.0	94.254.0.0	Total Traffic	77
109.243.0.0	109.243.0.0	Total Traffic	54
164.127.0.0	164.127.0.0	Total Traffic	70
46.113.0.0	46.113.0.0	Total Traffic	78

PLAY | iliad GROUP

Technology (*and understanding its limitations*)

One in a series of attacks:

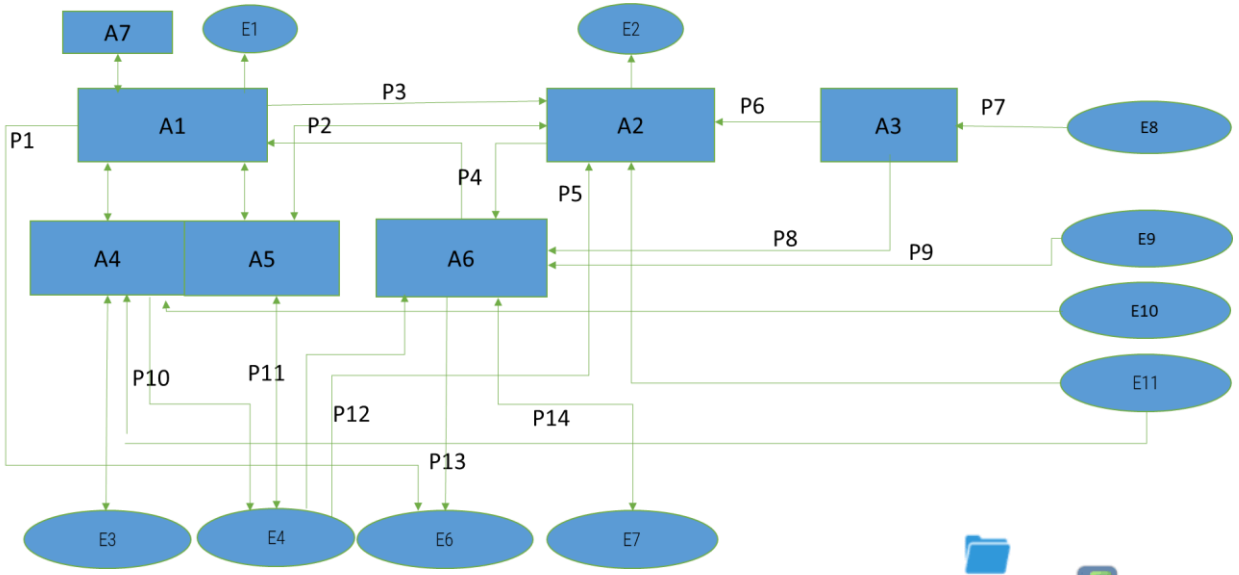
1) Attack begins
2) Anti-DDoS starts working
3) Attack is ending
4) Business as usual

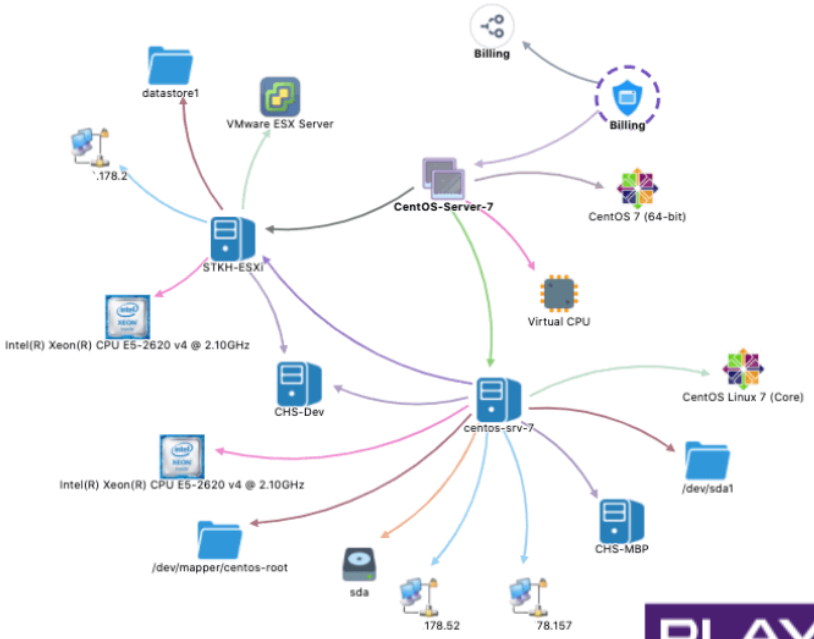
PLAY | iliad GROUP

Service (*and its dependence on assets*)

Think about…before going live:

1) Cyber Threats
2) Major Suppliers
3) Third-Party Dependencies
4) Safeguards/Cyber Resilience
5) Operations/Change Management
6) Client devices
7) Customers' personal data





Collaboration (*across Teams and with CISO/CSO*)

Hints:

- Knowledge about assets, processes and services is "scattered" between Teams
- Not all data is relevant and has been thoroughly checked
- The focus should not be on "who is to blame", but on the causes and solutions to the problem
- The Management "does not like" to be scared, but facts should not be hidden from it
- And…Monitoring and Collaboration Tools may not function properly - "Plan B" is welcome

PLAY | iliad GROUP

Trust (*in closing, but very important*)

The CISO/CSO **is perceived by the organization** in terms of what he/she believes in, how he/she works, his/her competence and ability to connect…not what he/she is responsible for

And something to think about: **what can CISO/CSO do** to improve the way the Security and IT Teams perceive each other…before the next incident happens

PLAY | iliad GROUP