BAHRIA UNIVERSITY
Discovering Knowledge

Denial / Distributed Denial of Service Attacks (DoS / DDoS)

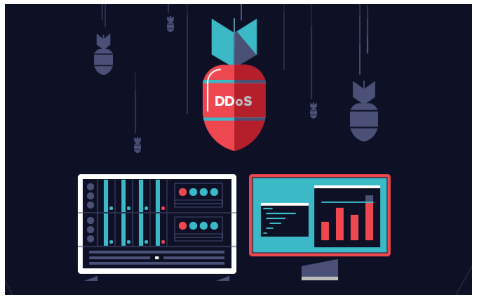
Information Security (CSC-407)

Fall 2024 (BSE-7A & 7B)

Availability of Service & Denial of Service

- **Availability** relates to a system being accessible and usable on-demand by authorized users.
- **Denial-of-service (DoS)** attack attempts to compromise the availability by **hindering** or **completely** blocking the provision of some service.
- The attack attempts to **exhaust** some critical **"resource(s)"** associated with the service.
- First known DoS/DDoS attack occurred in **1996** when **Panix ISP** was knocked offline for several days by a **SYN flood** attack.

DoS and DDoS



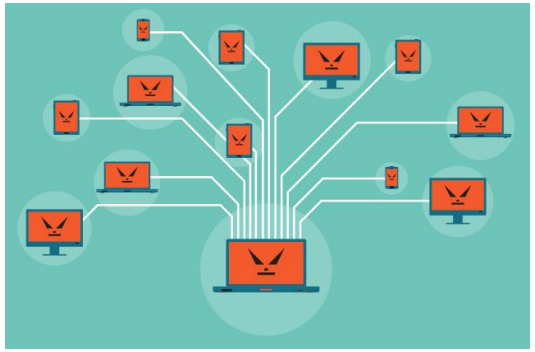
- **Denial-of-service (DoS) attack:** is an action that prevents or impairs the authorized use of ***networks, systems or applications*** by **exhausting resources** such as central processing units (CPU), memory, bandwidth and disk space.

OR

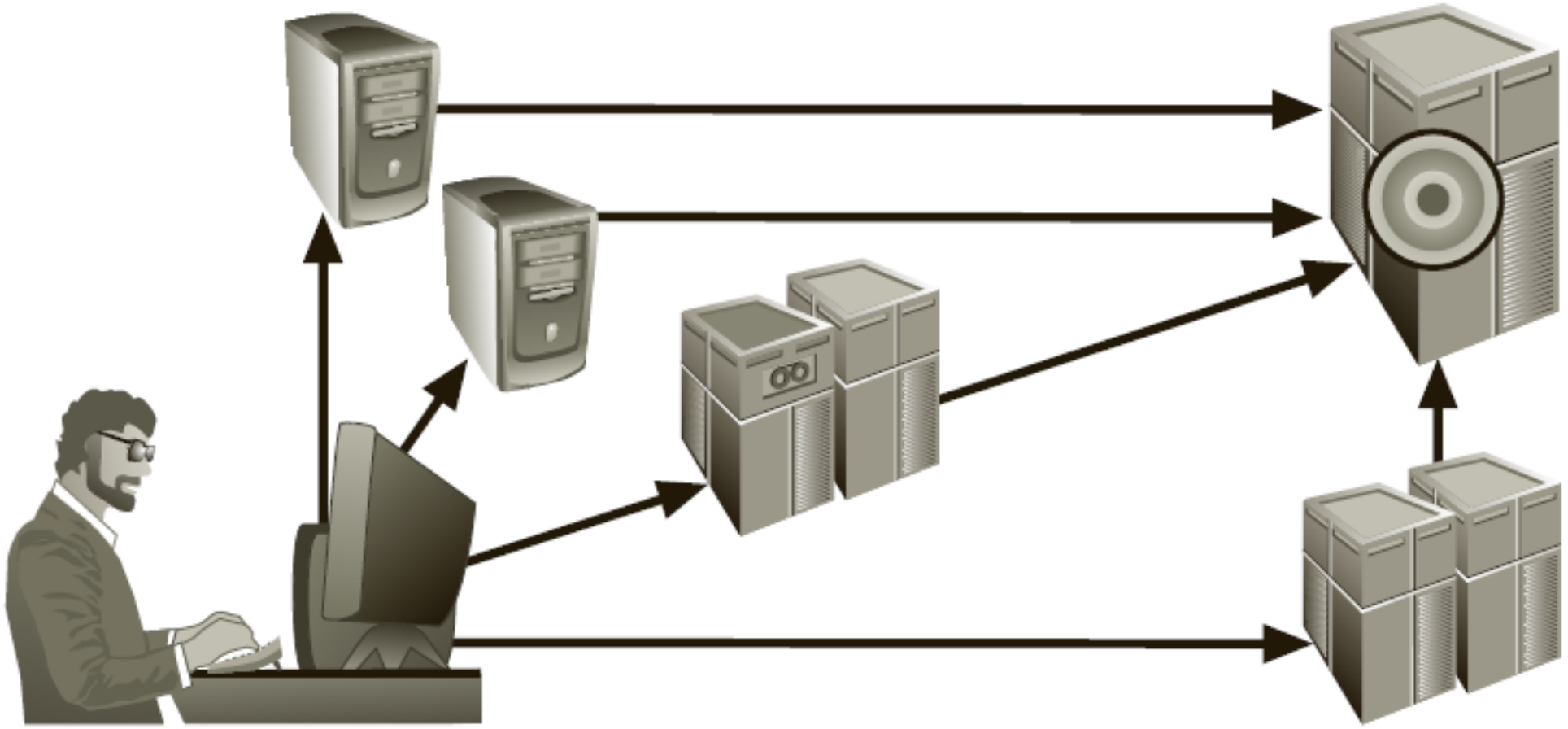
- **Denial-of-service (DoS) attack:** An attack that attempts to **overwhelm** a computer's ability to handle incoming communications, prohibiting legitimate users from accessing those systems.

DoS and DDoS (Cont.)

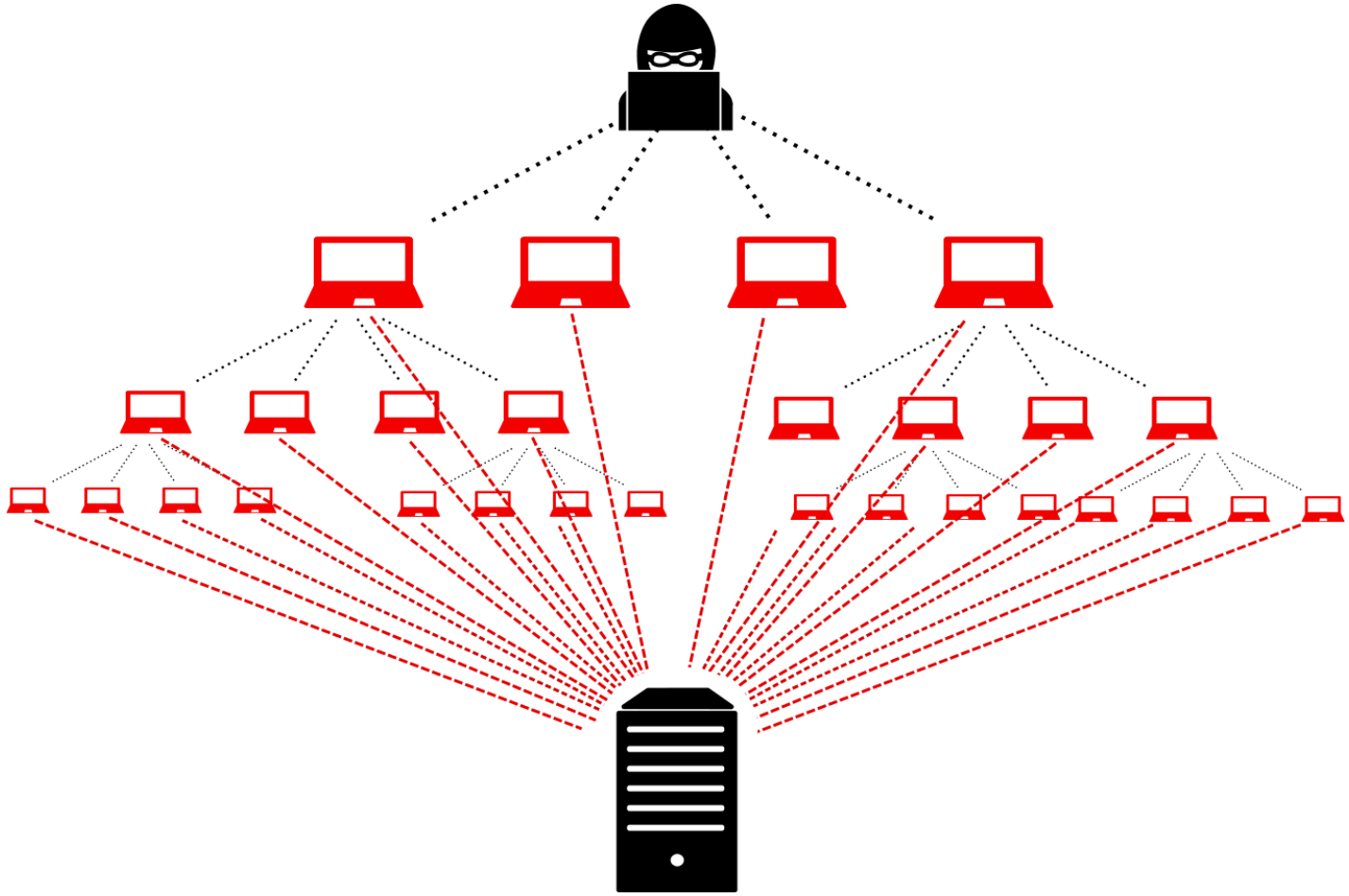
- **Distributed DoS (DDoS) attack:** A form of DoS attack in which a **coordinated** stream of requests is launched against a target from many locations simultaneously using **bots** or **zombies**.
- **Bot** (also referred as **botnet** or **zombie**): an abbreviation of robot, which is an **automated software program** that executes certain commands when it receives a specific input.



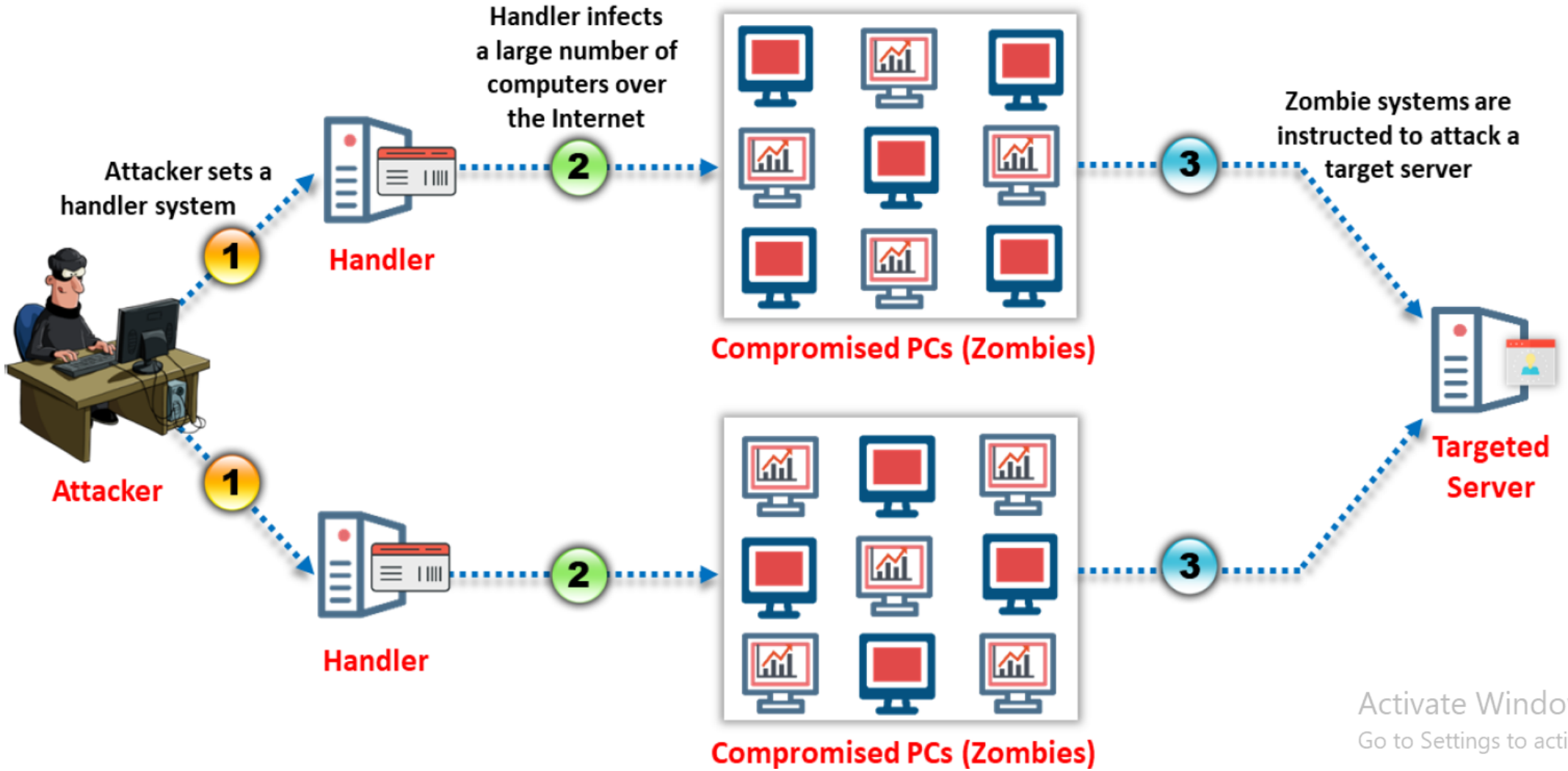
DDoS Attack Diagram



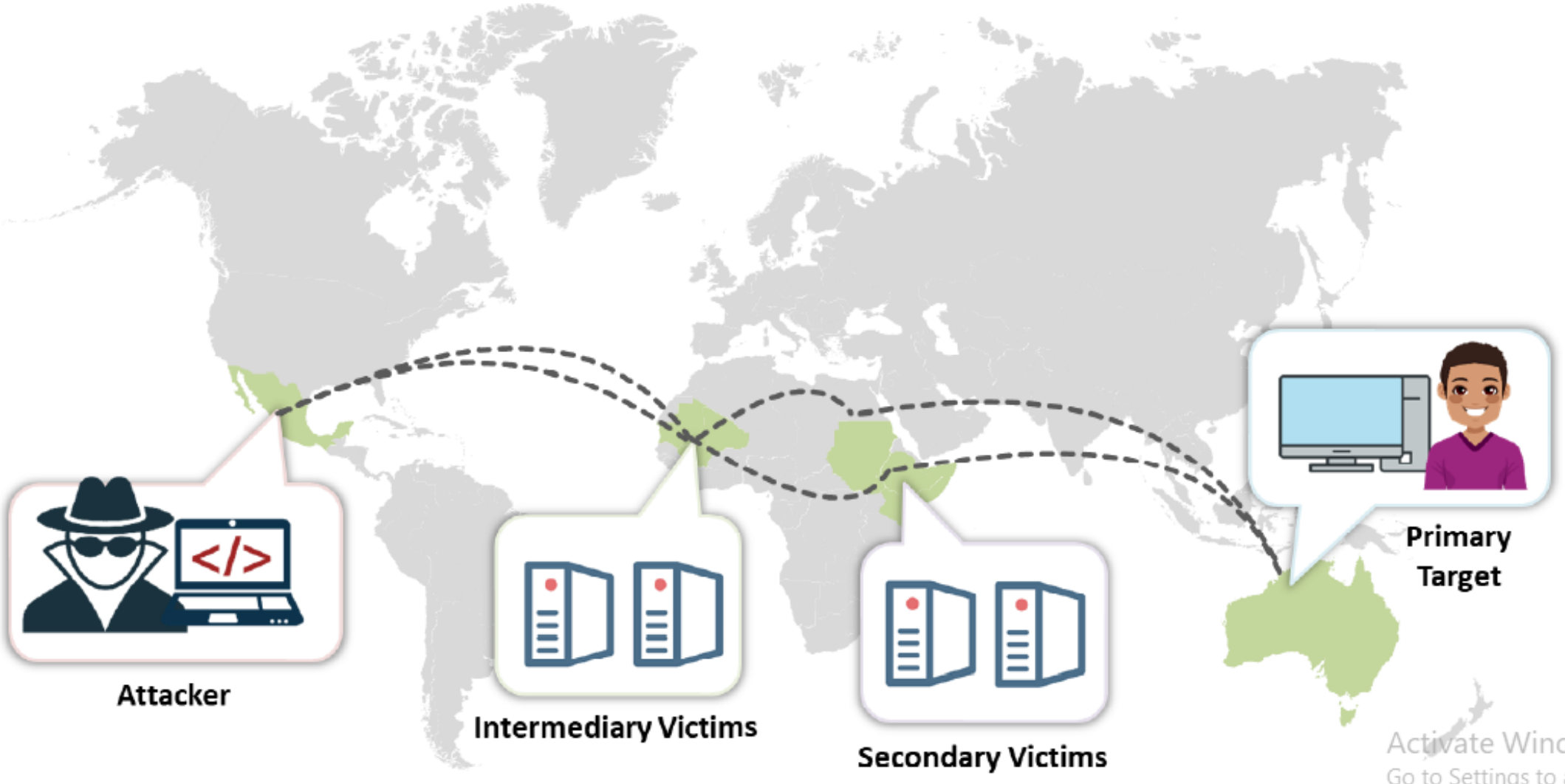
Use of Reflectors



Use of Reflectors (Cont.)



Distributed Reflection DoS (DRDoS) Attack



Not Defendable Attacks

- DDoS attacks are difficult to defend against, and currently there are **no controls** that any single organization can apply! ***WHY?***
- Any system connected to the Internet and providing TCP-based network services ***(such as a Web server, FTP server, mail server, routers)*** is vulnerable to DoS/DDoS attacks.
- One can not stop a given device from launching a DDoS attack as its **ownership** might be of someone else. Billions of devices exists that can launch DDoS attacks if compromised.

Increasing DDoS Attacks

DDoS attacks are expected to increase, Why?

1. With passage of time, there is a general trend in increasing the **network bandwidth** per user. Several new technologies are on the edge of being introduced that can provide **large bandwidth** and **easy accessibility** to such services. E.g. through **5G (Avg. 100 Mbps)** and **6G** cellular technologies.

Increasing DDoS Attacks

DDoS attacks are expected to increase (Cont.):

2. The introduction of **5G** technologies has accelerated the spread of **Internet of Things (IoT)** around the world. Hence, creating a huge pool of **"under protected"** new recruits for **botnet** armies used to launch DDoS attacks on **massive scales**.

Increasing DDoS Attacks (Cont.)

DDoS attacks are expected to increase (Cont.):

3. The increase of free DDoS attack tools or inexpensive **DDoS-as-a-service** platforms.

- **DDoS-as-a-service:** a service providing DDoS attacks for money, usually offered by **botnet owners** using special website in a **darknet**.
- **Darknet:** an **"overlay network"** within the Internet that can only be accessed with *specific software, configurations* or *authorization*, and often uses a *unique customized communication protocol*.

Increasing DDoS Attacks (Cont.)

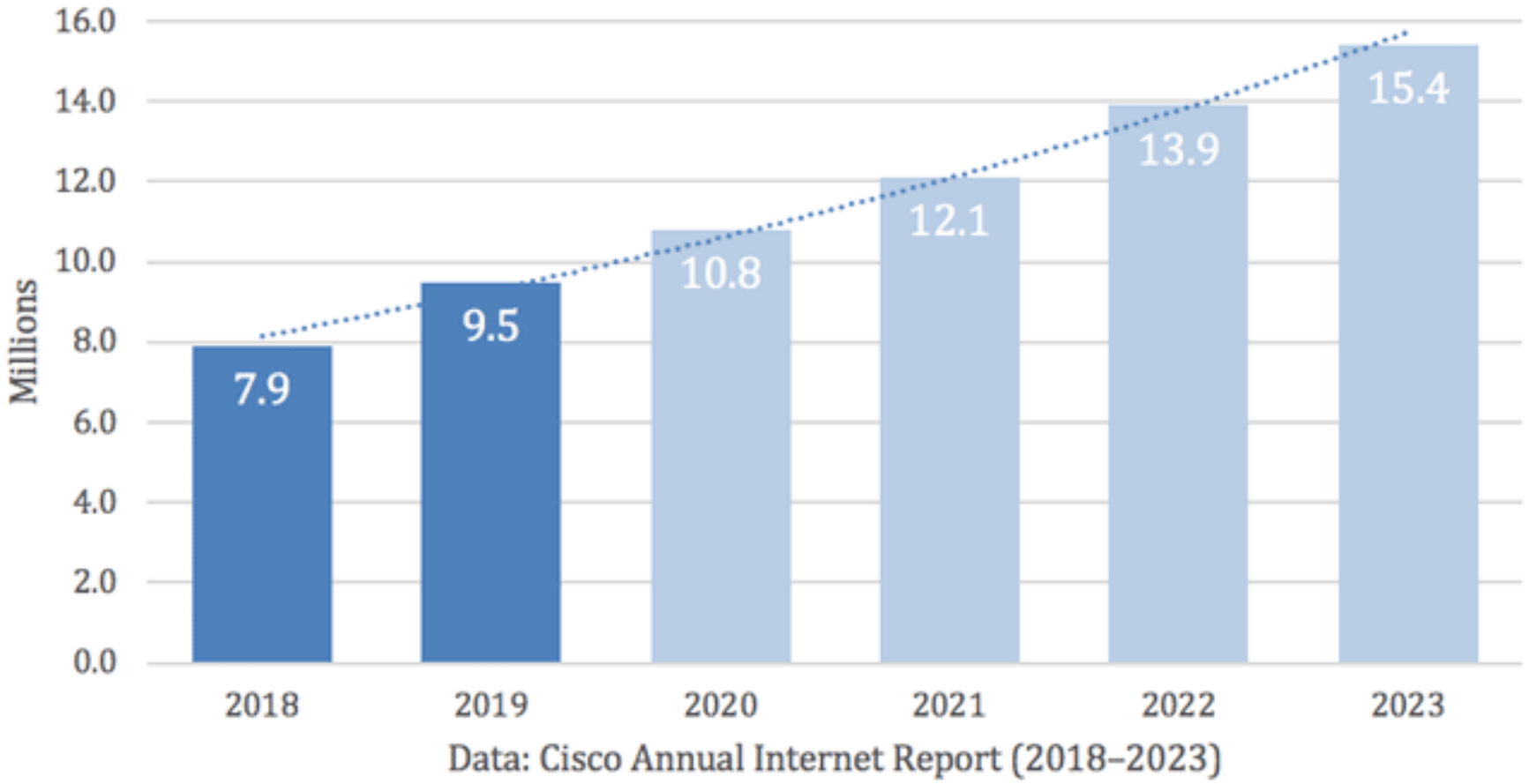
- **Examples of Free DDoS tools:**
  - **Hping3:** *http://www.hping.org*
  - **HULK:** *https://sibernianlaika.ru*
  - **High Orbit Ion Cannon (HOIC):** *https://sourceforge.net*

Increasing DDoS Attacks (Cont.)

Increasing DDoS Attacks (Cont.)

- In-terms of attack volume, DDoS attacks have increased from ***400 Mbps in 2002***, to ***100 Gbps in 2010***, to ***300 Gbps in 2013*** and to ***600 Gbps in 2015***.
- The above phenomenon is mainly due to the growth in the **Internet bandwidth**!
- In-terms of attack numbers, Cisco predicts that DDoS attacks will double from the ***7.9 million (2018)*** to ***15.4 million (2023)***.

Increasing DDoS Attacks (Cont.)



Cisco's analysis of DDoS total attacks: history & predictions.

Increasing DDoS Attacks (Cont.)

- During the *pandemic*, there was a rapid increase in **DDoS weapons**, widespread **botnet** activity and **largest DDoS attacks** ever recorded.

1. **Amazon Inc.** reports that in ***February 2020***, they defended against a **2.3 Tbps** DDoS attack.
2. In ***November 2021***, **Microsoft** mitigated a DDoS attack targeting an **Azure customer** with a throughput of **3.45 Tbps**. This is believed to be the ***largest in History (so far)***.

Increasing DDoS Attacks (Cont.)

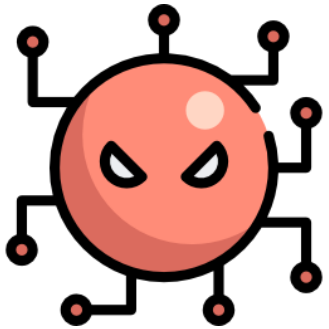
- Massive DDoS attacks in **50 Gbps** range are powerful enough to exceed the bandwidth capacity of almost any intended target, including **core Internet Exchanges** or **critical DNS servers**.
- However, a DDoS attack of **1 Gbps** is enough to knock most organizations off the internet.

Cost of DDoS Attacks

- Given that **IT services downtime** costs companies anywhere from ***$300,000 to over $1,000,000 per hour***, we can imagine the financial hit from DDoS attacks.
- DDoS attack can damage brand reputation and revenue.
- DDoS attacks are sometimes used to distract cybersecurity operations while other criminal activity, such as ***data theft or network infiltration*** is underway.

DDoS Attack: Mirai Malware

Mirai Malware



- **Mirai** is the name of a malicious software that infected **IoT** devices in **August of 2016**.
- Till date, **Mirai** is considered to be the most damaging **DDoS** attack in history that spawned from insecure **IoT** devices in remote areas.
- The attack came in form of **botnets (zombie agent)** that generated massive **DDoS** storm.
- The **botnet** devices comprised ***IP cameras, DVRs, consumer routers, VOIP phones and printers***.

Mirai Malware (Cont.)

- In total, **600,000 IoT** devices were infected as part of the **botnet**.
- Targets included *"Krebs on Security", Dyn, Lonestar cell, Italian political sites, Minecraft servers, Russian auction sites*.
- **Dyn** had secondary effects on other extremely large providers that used their services, such as *Sony Playstation servers, Amazon, GitHub, Netflix, PayPal, Reddit and Twitter*.
- Mirai source code was released on **hackforums.net** *(a hacker blog site)*.

Mirai Malware (Cont.)

Mirai attack working mechanism:

1. **Scan for victims:** perform a rapid scan using **TCP SYN** packets to probe random IPv4 addresses. It specifically looked for **SSH/Telnet** TCP port **23** and **2323**.

2. **Brute Force Telnet:** Mirai attempted to establish a functional Telnet session with a victim by sending **10 username and password** pairs randomly using a dictionary attack of **62 pairs**. If a login was successful, Mirai logged the host to a central **C2 server**.

Mirai Malware (Cont.)

Mirai attack working mechanism:

3. **Infect:** a **loader program** ***(device specific malware)*** was sent to potential victim from **server C2**. The program searches for other **competing processes** using **port 23** and kills them ***(along with other malware that could already be present on the device)***. The **loader binary** was deleted and the process name was **"obfuscated"** to hide its presence. The malware did not reside in persistent storage and didn't survive a **reboot**. The bot stayed **dormant** until it received an attack command.

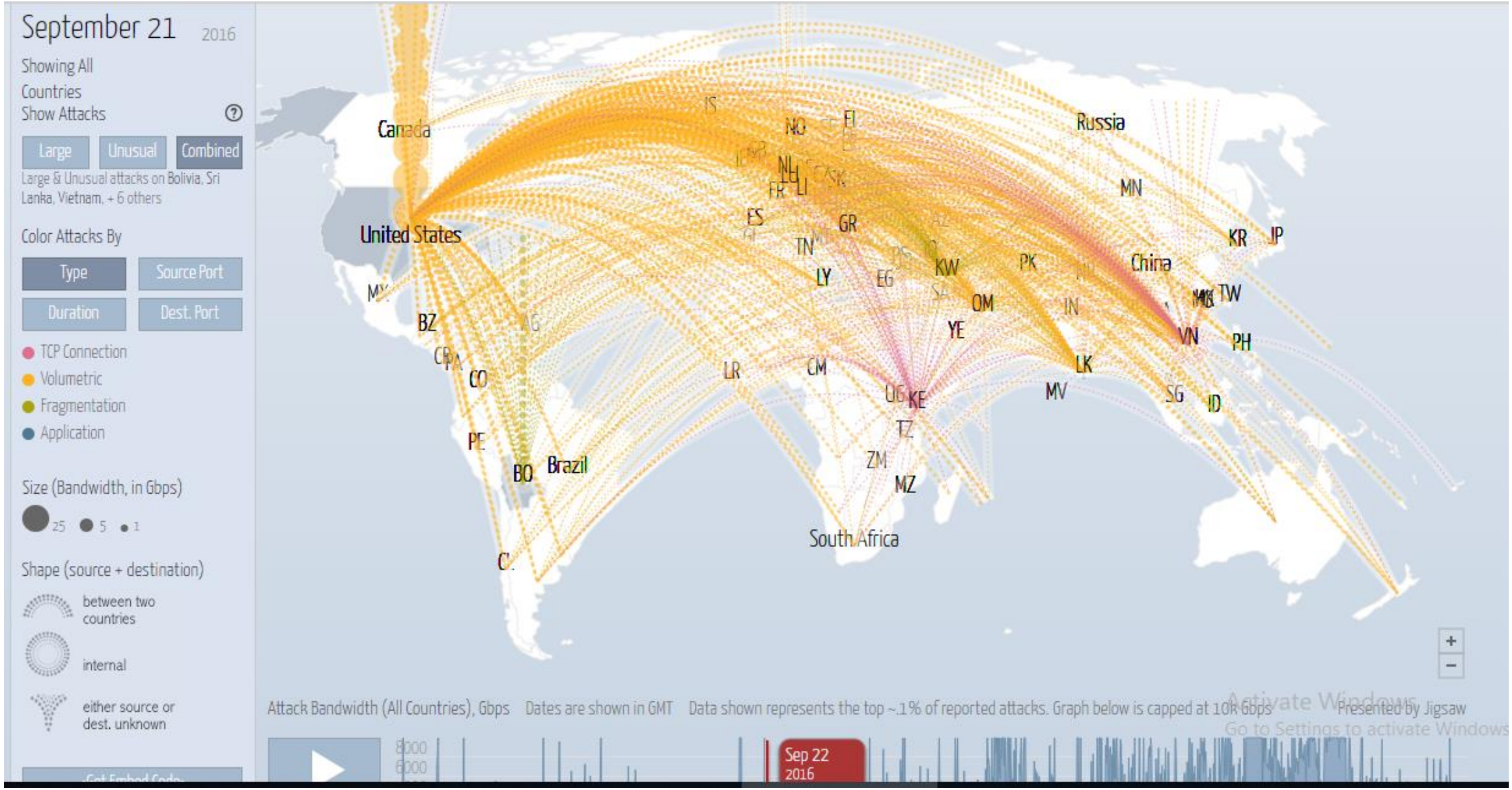
Mirai Malware (Cont.)

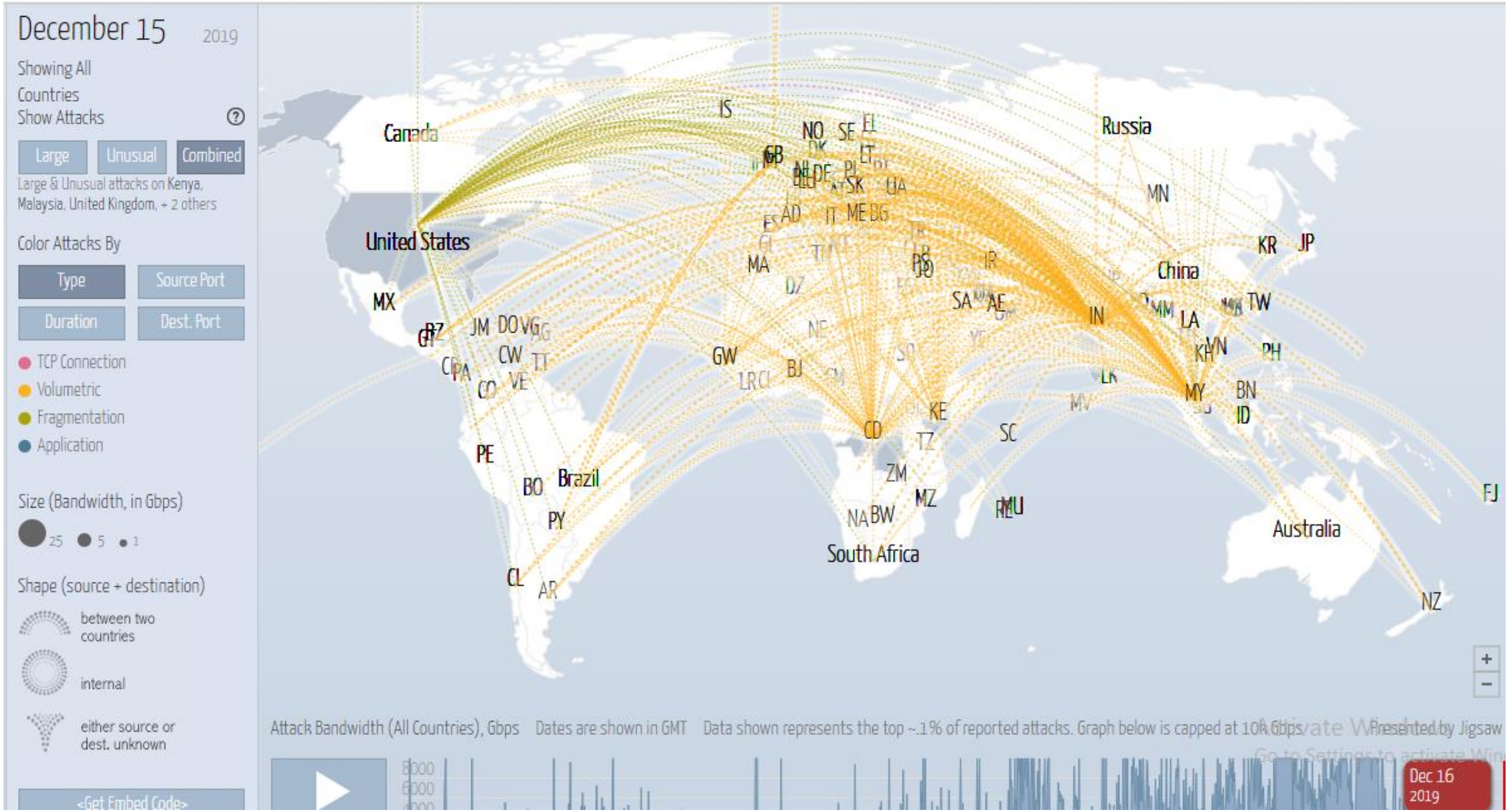
- First **scan** ***(reconnaissance attack)*** occurred on **August 1, 2016**.
- The scan took **120 minutes** before it found a host with an open port and password in the dictionary.
- After one additional minute, **834 other devices** were infected.
- Within 20 hours, 64,500 devices were infected.
- Most of infected devices that turned into **botnets** were located in **Brazil (15.0%)**, **Columbia (14.0%)** and **Vietnam (12.5%)**.

Mirai Malware (Cont.)

- **September 21, 2016**, the Mirai botnet unleashed a massive DDoS attack on the ***Krebs on Security*** blogging site and generated **623 Gbps** of traffic. ***It accounted for the single worst IoT-based DDoS attack of all time.***
- Over a span of five months, 15,194 individual attack commands were issued by the **C2 servers** and hit 5,042 internet sites.
- Global DDoS attack map:

https://www.digitalattackmap.com/


September 21 2016
Showing All Countries
Show Attacks
Large
Unusual
Combined
Large & Unusual attacks on Bolivia, Sri Lanka, Vietnam, + 6 others
Color Attacks By
Type
Source Port
Duration
Dest. Port
TCP Connection
Volumetric
Fragmentation
Application
Size (Bandwidth, in Gbps)
25
5
1
Shape (source + destination)
between two countries
internal
either source or dest. unknown
Canada
United States
Russia
China
Brazil
South Africa
Attack Bandwidth (All Countries), Gbps
Dates are shown in GMT
Data shown represents the top ~1% of reported attacks. Graph below is capped at 10k Gbps
Presented by Jigsaw
Sep 22 2016

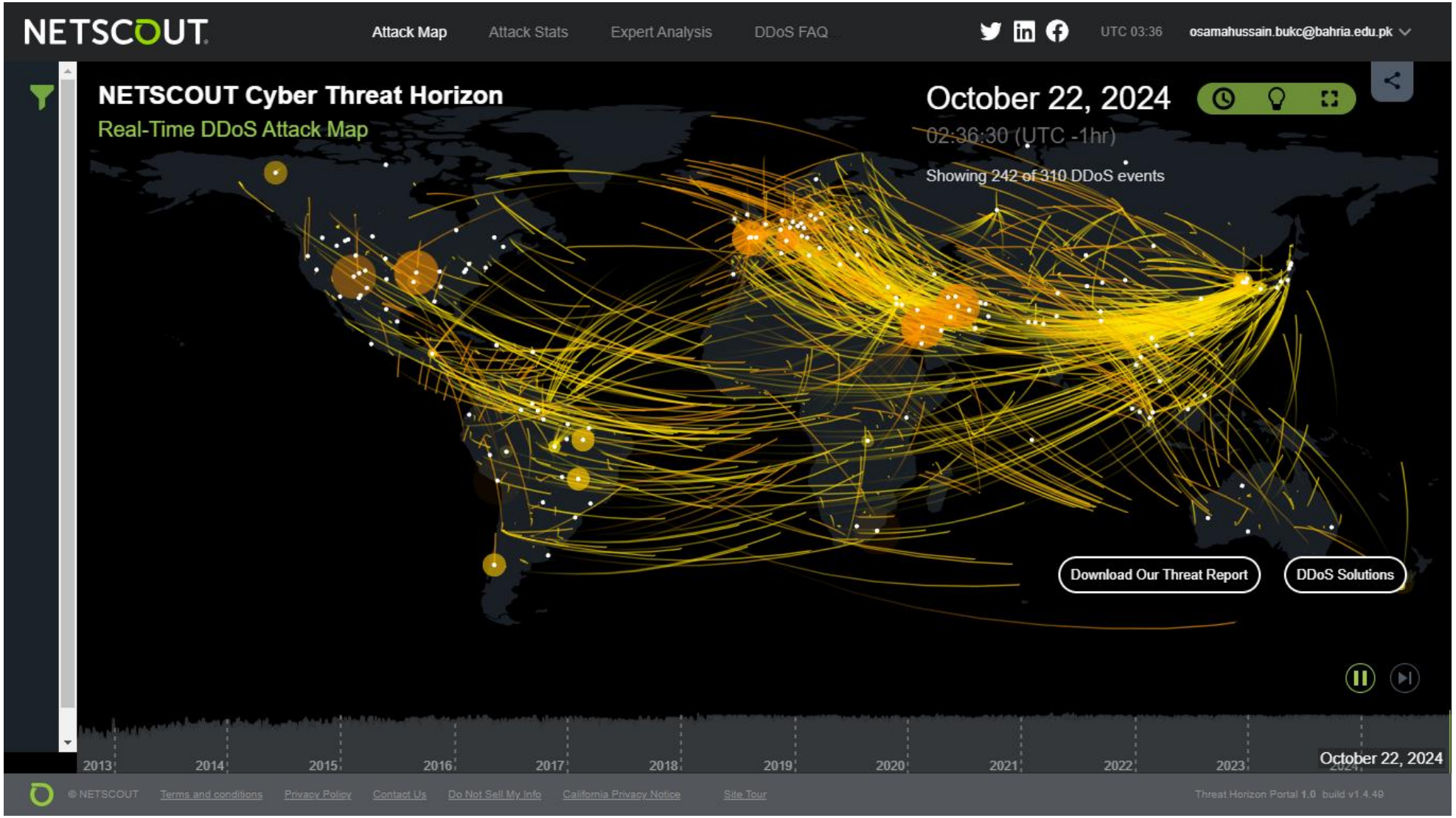

December 15
2019
Showing All
Countries
Show Attacks
Large
Unusual
Combined
Large & Unusual attacks on Kenya, Malaysia, United Kingdom, + 2 others
Color Attacks By
Type
Source Port
Duration
Dest. Port
TCP Connection
Volumetric
Fragmentation
Application
Size (Bandwidth, in Gbps)
25
5
1
Shape (source + destination)
between two countries
internal
either source or dest. unknown
<Get Embed Code>
Canada
United States
MX
Brazil
PE
BO
PY
CL
AR
Russia
China
India
Australia
South Africa
NZ
FJ
Attack Bandwidth (All Countries), Gbps
Dates are shown in GMT
Data shown represents the top ~.1% of reported attacks. Graph below is capped at 10k Gbps
Presented by Jigsaw
Dec 16
2019

https://www.netscout.com/ddos-attack-map

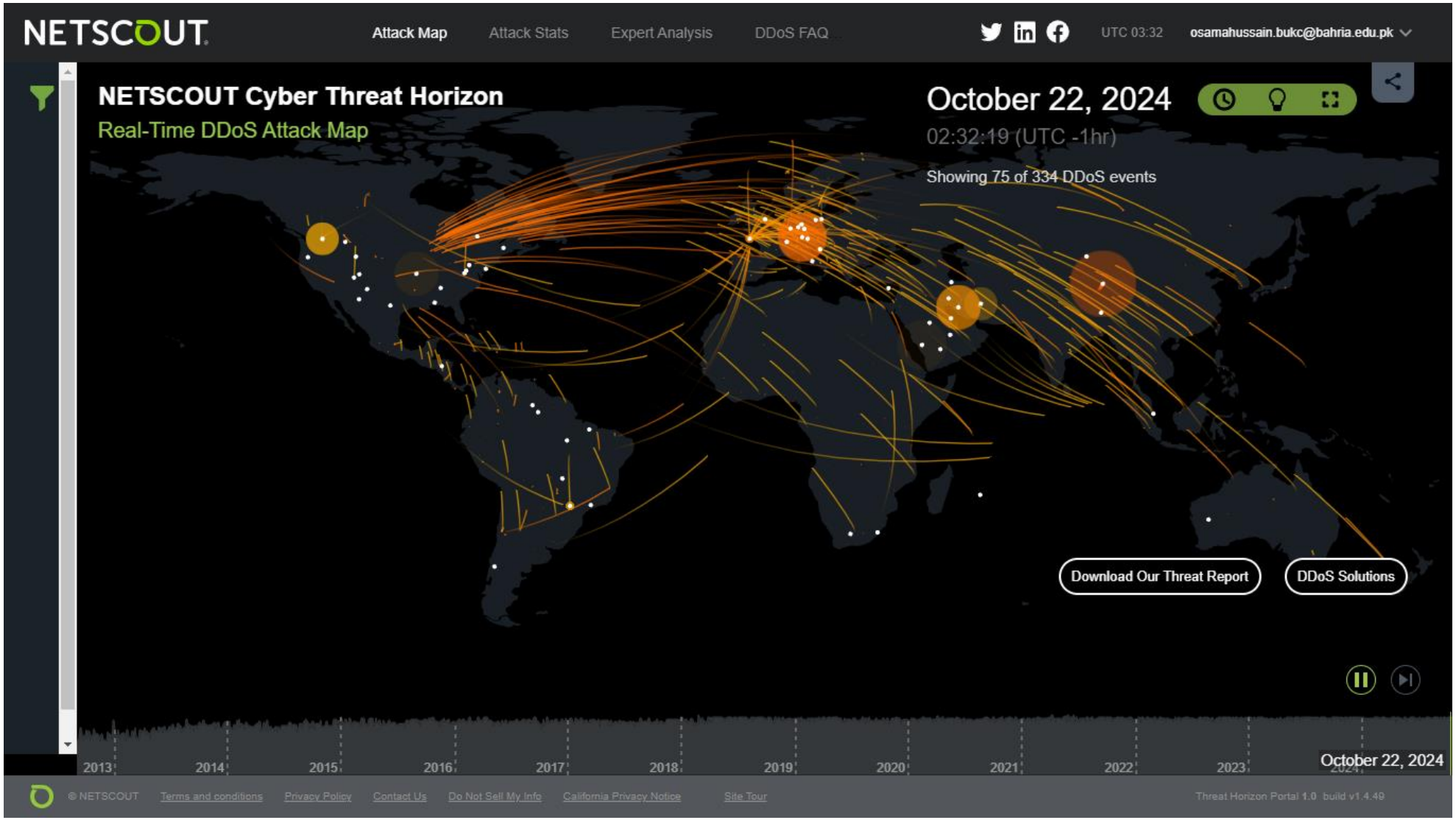
@ ALL


NETSCOUT
Attack Map
Attack Stats
Expert Analysis
DDoS FAQ
UTC 03:30
osamahussain.bukc@bahria.edu.pk
NETSCOUT Cyber Threat Horizon
Real-Time DDoS Attack Map
October 22, 2024
02:30:09 (UTC -1hr)
Showing 268 of 349 DDoS events
Download Our Threat Report
DDoS Solutions
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
October 22, 2024
© NETSCOUT
Terms and conditions
Privacy Policy
Contact Us
Do Not Sell My Info
California Privacy Notice
Site Tour
Threat Horizon Portal 1.0 build v1.4.49

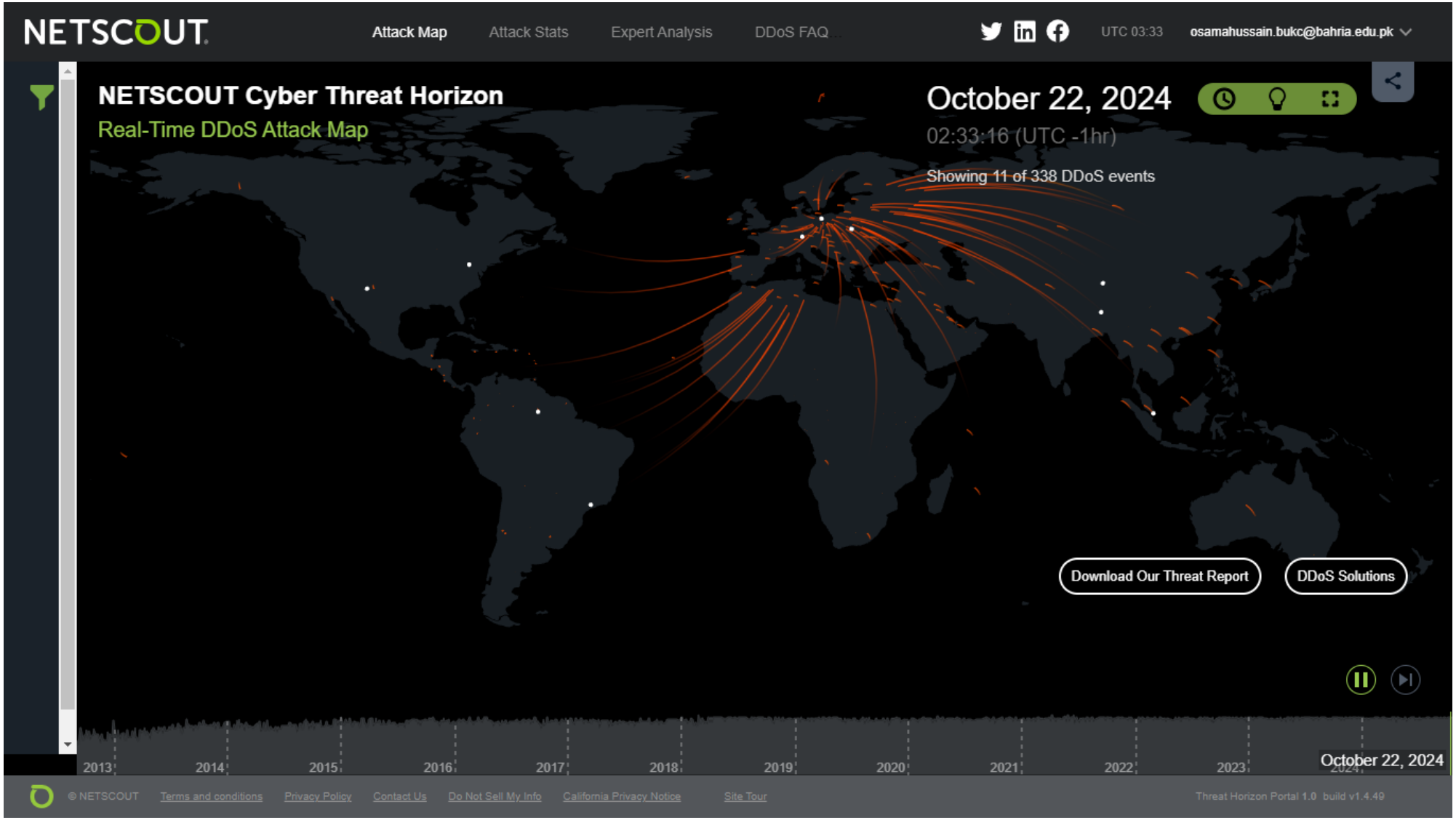
@ 10 MB


NETSCOUT
Attack Map
Attack Stats
Expert Analysis
DDoS FAQ
UTC 03:36
osamahussain.bukc@bahria.edu.pk
NETSCOUT Cyber Threat Horizon
Real-Time DDoS Attack Map
October 22, 2024
02:36:30 (UTC -1hr)
Showing 242 of 310 DDoS events
Download Our Threat Report
DDoS Solutions
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
October 22, 2024
© NETSCOUT
Terms and conditions
Privacy Policy
Contact Us
Do Not Sell My Info
California Privacy Notice
Site Tour
Threat Horizon Portal 1.0 build v1.4.49

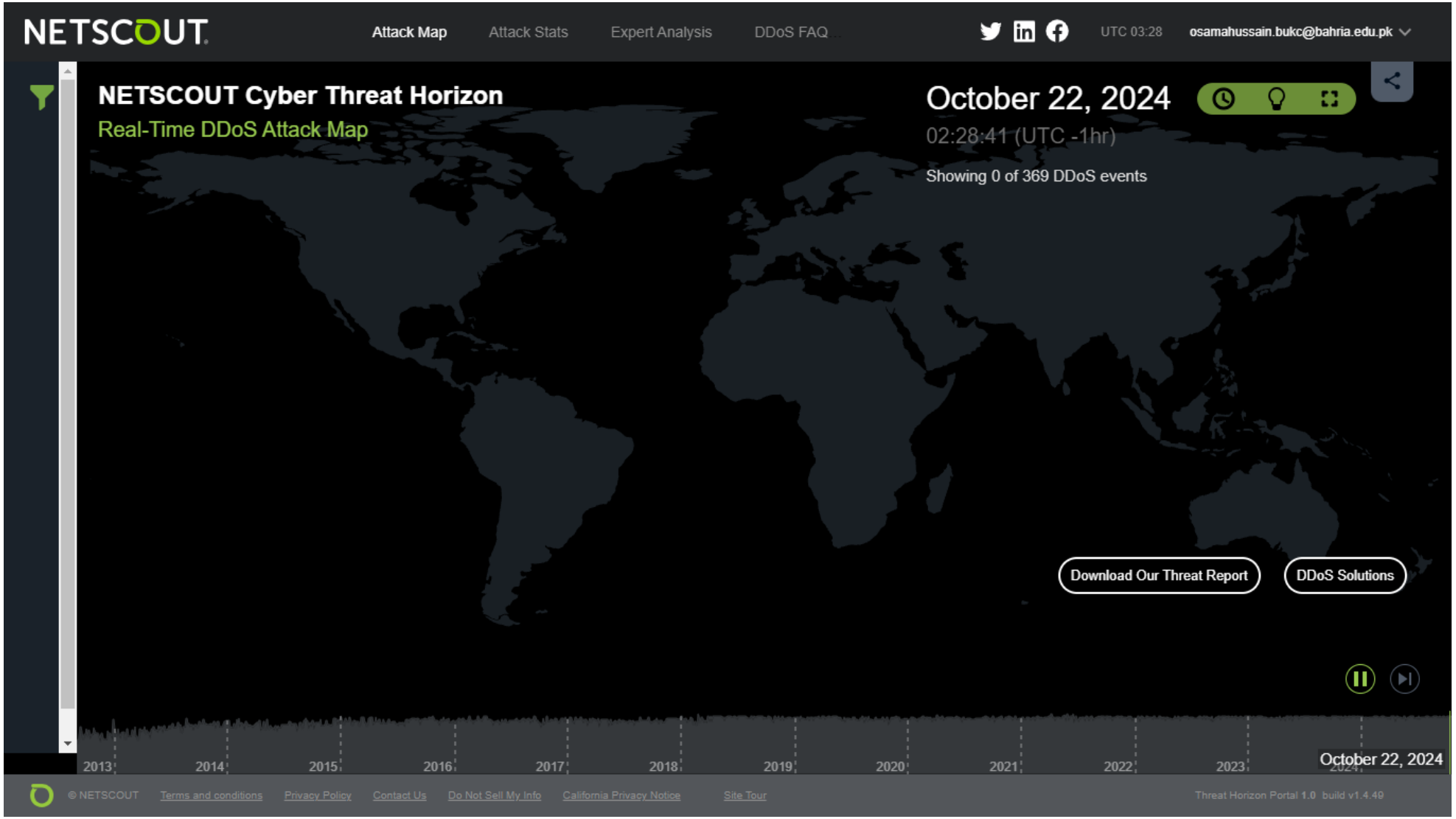
@1 GB

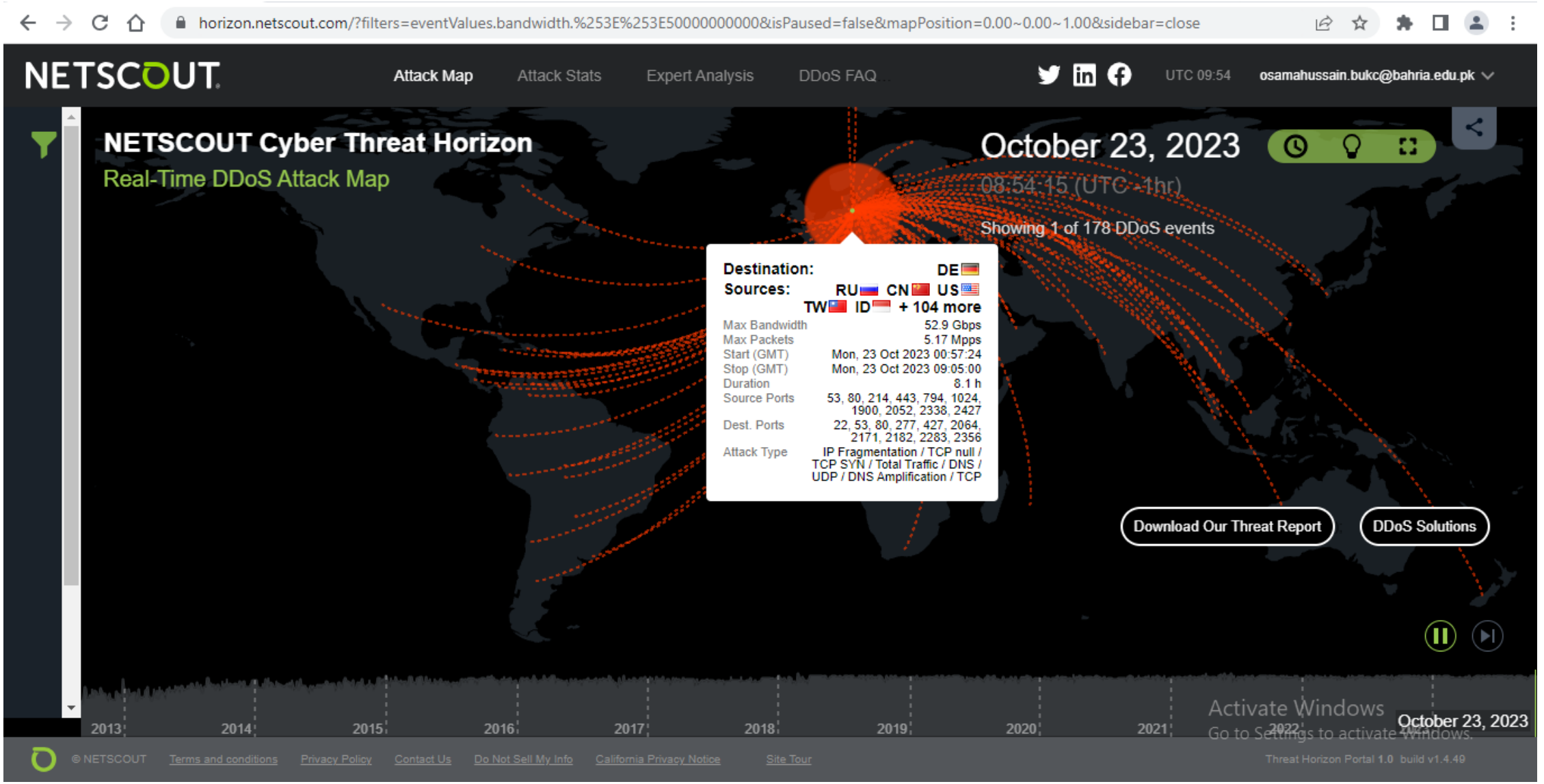

NETSCOUT
Attack Map
Attack Stats
Expert Analysis
DDoS FAQ
UTC 03:32
osamahussain.bukc@bahria.edu.pk
NETSCOUT Cyber Threat Horizon
Real-Time DDoS Attack Map
October 22, 2024
02:32:19 (UTC -1hr)
Showing 75 of 334 DDoS events
Download Our Threat Report
DDoS Solutions
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
October 22, 2024
© NETSCOUT
Terms and conditions
Privacy Policy
Contact Us
Do Not Sell My Info
California Privacy Notice
Site Tour
Threat Horizon Portal 1.0 build v1.4.49

@ 10 GB


NETSCOUT
Attack Map
Attack Stats
Expert Analysis
DDoS FAQ
UTC 03:33
osamahussain.bukc@bahria.edu.pk
NETSCOUT Cyber Threat Horizon
Real-Time DDoS Attack Map
October 22, 2024
02:33:16 (UTC -1hr)
Showing 11 of 338 DDoS events
Download Our Threat Report
DDoS Solutions
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
October 22, 2024
© NETSCOUT
Terms and conditions
Privacy Policy
Contact Us
Do Not Sell My Info
California Privacy Notice
Site Tour
Threat Horizon Portal 1.0 build v1.4.49

@ 50 GB


NETSCOUT
Attack Map
Attack Stats
Expert Analysis
DDoS FAQ
UTC 03:28
osamahussain.bukc@bahria.edu.pk
NETSCOUT Cyber Threat Horizon
Real-Time DDoS Attack Map
October 22, 2024
02:28:41 (UTC -1hr)
Showing 0 of 369 DDoS events
Download Our Threat Report
DDoS Solutions
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
October 22, 2024
© NETSCOUT
Terms and conditions
Privacy Policy
Contact Us
Do Not Sell My Info
California Privacy Notice
Site Tour
Threat Horizon Portal 1.0 build v1.4.49


horizon.netscout.com/?filters=eventValues.bandwidth.%253E%253E50000000000&isPaused=false&mapPosition=0.00~0.00~1.00&sidebar=close
NETSCOUT
Attack Map
Attack Stats
Expert Analysis
DDoS FAQ
UTC 09:54
osamahussain.bukc@bahria.edu.pk
NETSCOUT Cyber Threat Horizon
Real-Time DDoS Attack Map
October 23, 2023
08:54:15 (UTC -1hr)
Showing 1 of 178 DDoS events
Destination: DE
Sources: RU CN US TW ID + 104 more
Max Bandwidth 52.9 Gbps
Max Packets 5.17 Mpps
Start (GMT) Mon, 23 Oct 2023 00:57:24
Stop (GMT) Mon, 23 Oct 2023 09:05:00
Duration 8.1 h
Source Ports 53, 80, 214, 443, 794, 1024, 1900, 2052, 2338, 2427
Dest. Ports 22, 53, 80, 277, 427, 2064, 2171, 2182, 2283, 2356
Attack Type IP Fragmentation / TCP null / TCP SYN / Total Traffic / DNS / UDP / DNS Amplification / TCP
Download Our Threat Report
DDoS Solutions
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
October 23, 2023
Activate Windows
Go to Settings to activate Windows.
© NETSCOUT
Terms and conditions
Privacy Policy
Contact Us
Do Not Sell My Info
California Privacy Notice
Site Tour
Threat Horizon Portal 1.0 build v1.4.49

Types of DDoS Attacks

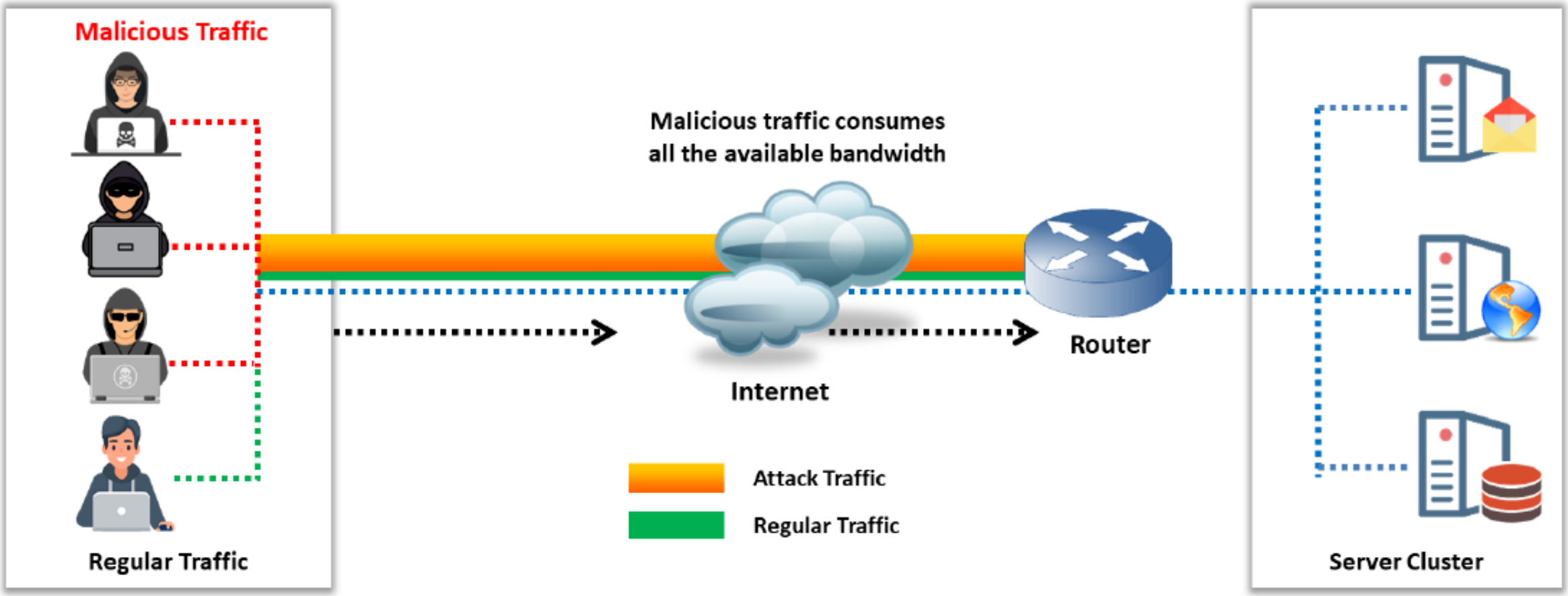
Types of DDoS

- Several categories of resources could be attacked in DDoS:
  1. ***Network bandwidth***
  2. ***Open Connections***
  3. ***System resources***
  4. ***Application resources***

Network Bandwidth Attack

- Network bandwidth relates to the **network's link capacity** connecting a **server** to the **Internet** through **ISP**.
- In **network bandwidth attack**, the attackers **floods** the victim's system with more traffic than it can handle.
- Majority of traffic directed at the target **server** is **malicious** which **overwhelms** the **server**, hence denying **legitimate users** access to the server.

Network Bandwidth Attack (Cont.)

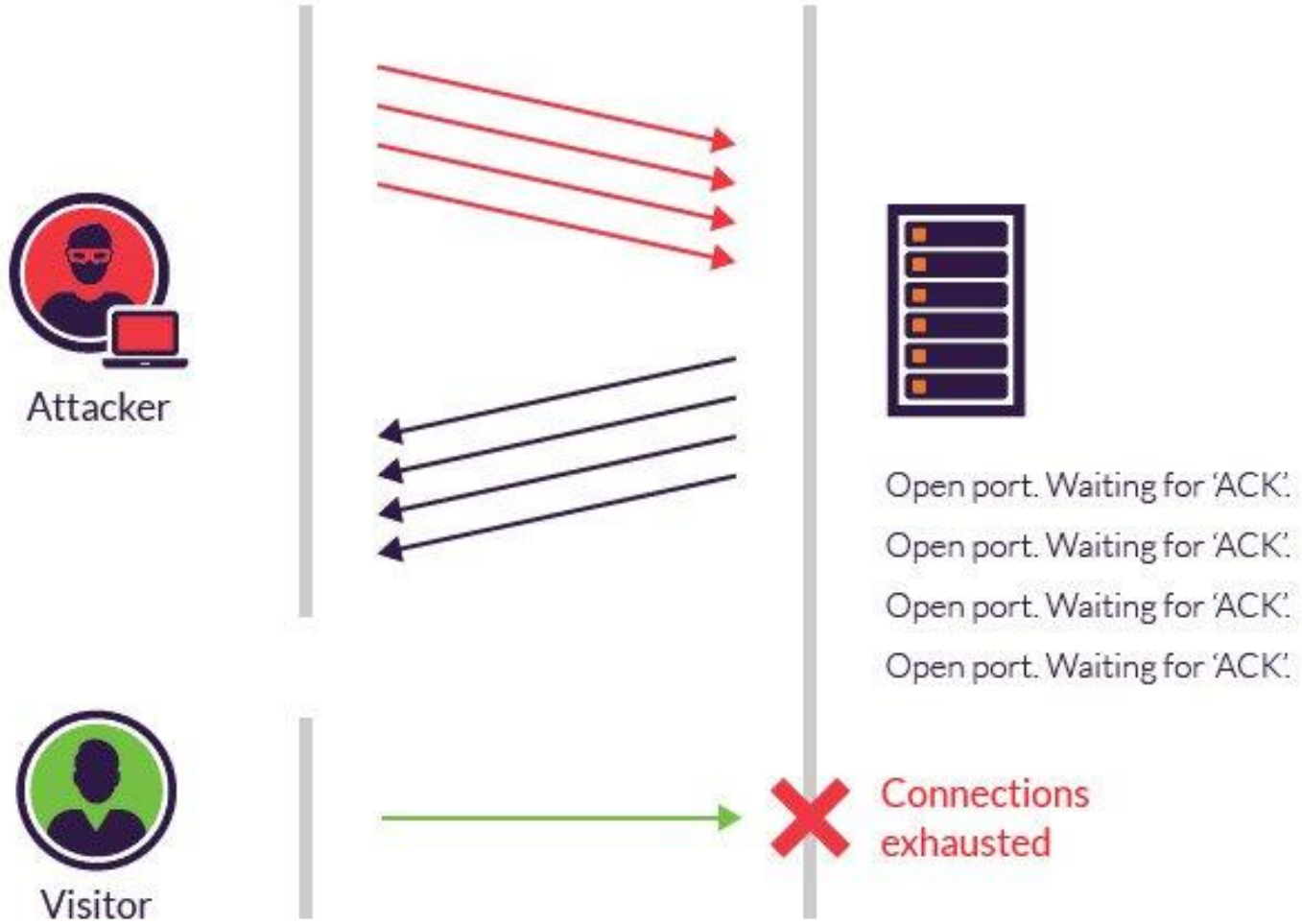


Open Connections

- The attacker overflow a system with a ***large number of connection requests***.
- Hence, consuming all available ***OS resources*** to prevent the system from processing legitimate user requests.
- **E.g.** food catering companies conducts much of its business over the phone. An attacker can disrupt services by finding ways to **block the company's phone lines** using DDoS by creating ***overwhelming amount of connections***.

Open Connections (Cont.)

- ***Tables of open connections attacks.***
- The **SYN spoofing attack** is of this type, which targets the table of **TCP connections** on the server.



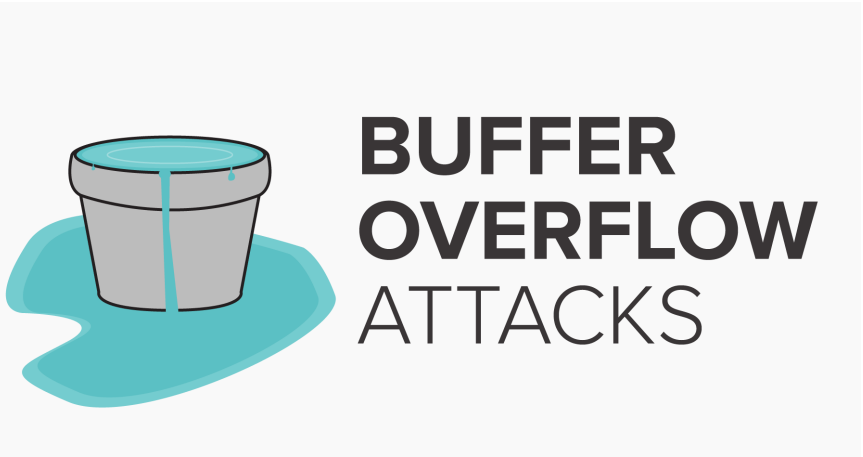
System Resources Attack

- A DoS attack targeting system resources typically aims at its **"network handling software"** to:

1. **Overload the system**
2. **Crash the system**

System Resources Attack: Overload

- Rather than consuming bandwidth with large volumes of traffic, ***specific types of packets are sent*** that **"consume"** the limited resources available on the system. These include:
  - **Temporary buffers** *(used to hold arriving packets)*
  - **Memory data structures**



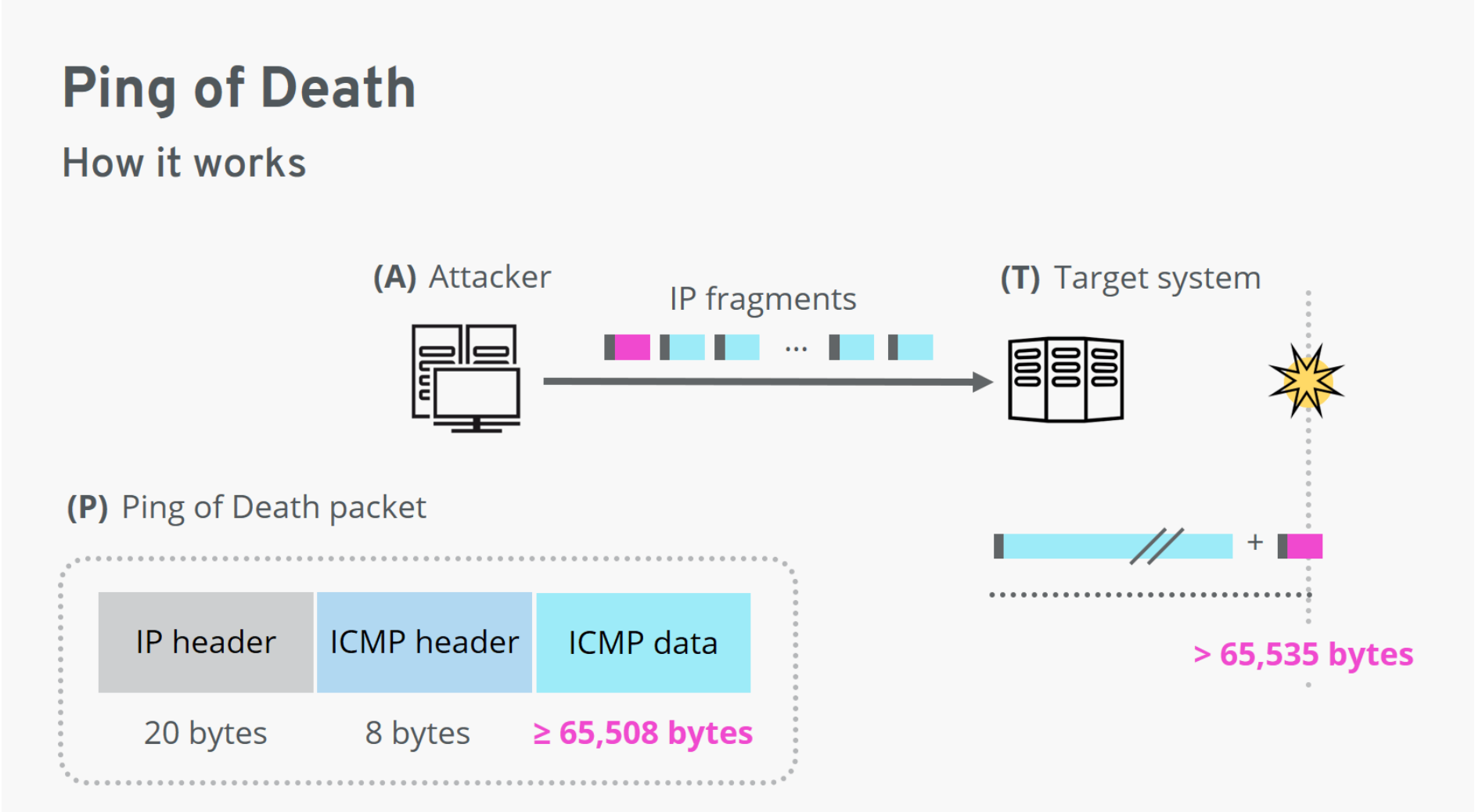
System Resources Attack: Crash

- Another form of system resource attack uses packets whose structure triggers a **bug** in the ***"system's network handling software"***, **causing it to crash.** This is known as a **poison packet,** which include:
  - **Ping of Death**: targets **ICMP echo** request packets.
  - **Teardrop**: targets **packet fragmentation**.
- After crashing, the system can no longer communicate over the network until this software is reloaded ***(generally by rebooting)***.

Ping of Death Attack

- In **Ping of Death (PoD)**, an attacker attempts to crash the target system by sending **oversized packets** using a simple **ping command**.
- **E.g.** an attacker sends a packet with a size of **65,538 bytes** to the target web server. This size exceeds the size limit which is **65,535 bytes**.
- The reassembly process might cause the system to crash. In such attacks, the attacker need no detailed knowledge of the target machine, except its **IP address**.

Ping of Death Attack (Cont.)



Application Resources Attack

- Similar to **System Resources Attack**, the **Application Resources Attack** can:

1. **Overload the application:** An attack on a **"specific application"**, such as a **Database server**. A Web server might handle **database queries.** If a ***large and costly query*** is received, then a server can be overloaded, hence limiting its ability to respond to valid requests from other users.
2. **Crash the application:** An attacker constructs a request that triggers a **bug** in the server program, causing it to **crash**.

Thank You!