SOPHOS

# Intrusion attacks

2024-01-01 00:00:00 - 2024-05-31 23:59:59

Appliance:
XGS3100

Appliance key:
X310179B68D9C38

Firmware version:
SFOS 19.5.4 MR-4-Build718

Filter(s) applied while generating this report:
None

Reports:

1.Attack categories

2.Attacked platforms

3.Attack targets

4.Severity-wise attacks

5.Intrusion attacks

6.Attacks detected and allowed

7.Intrusion source

8.Intrusion destination

9.Users

10.Applications used for attacks

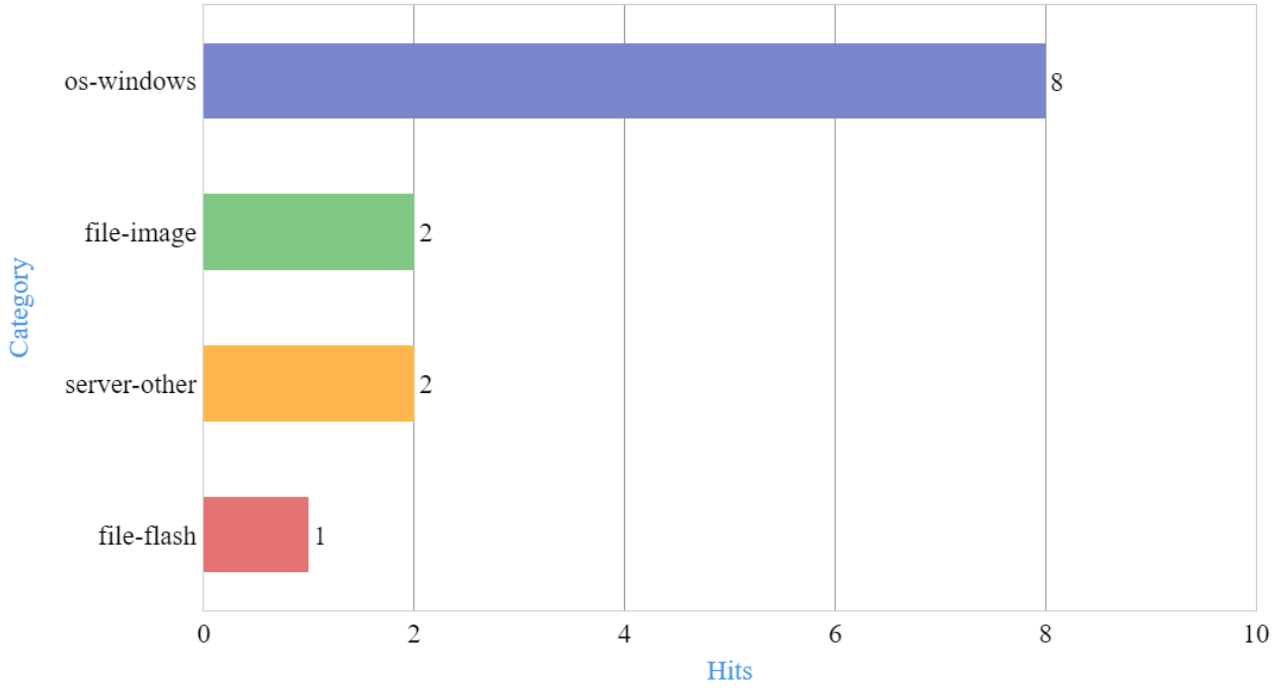
11.Lateral movement detection

12.Source countries

13.Trend - intrusion attacks

SOPHOS

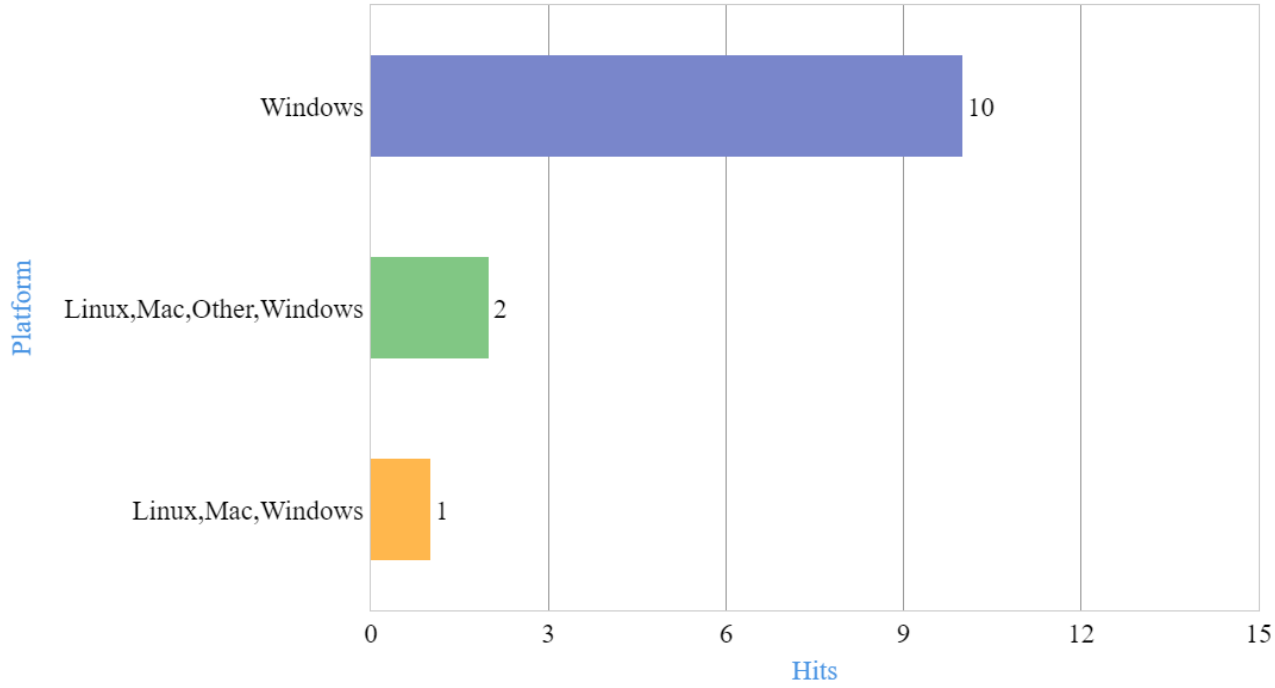
# 1.Attack categories




| CATEGORY | HITS |
|---|---|
| os-windows | 8 |
| file-image | 2 |
| server-other | 2 |
| file-flash | 1 |

SOPHOS

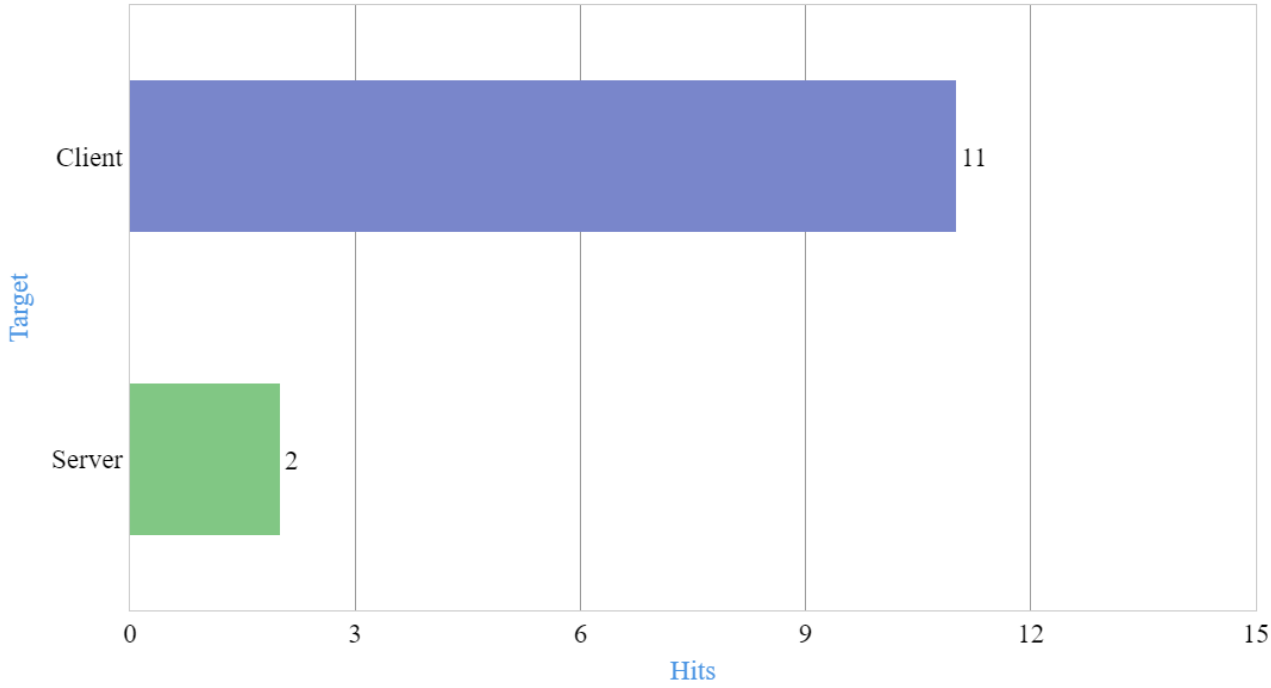
## 2.Attacked platforms




| PLATFORM | HITS |
|---|---|
| Windows | 10 |
| Linux,Mac,Other,Windows | 2 |
| Linux,Mac,Windows | 1 |

SOPHOS

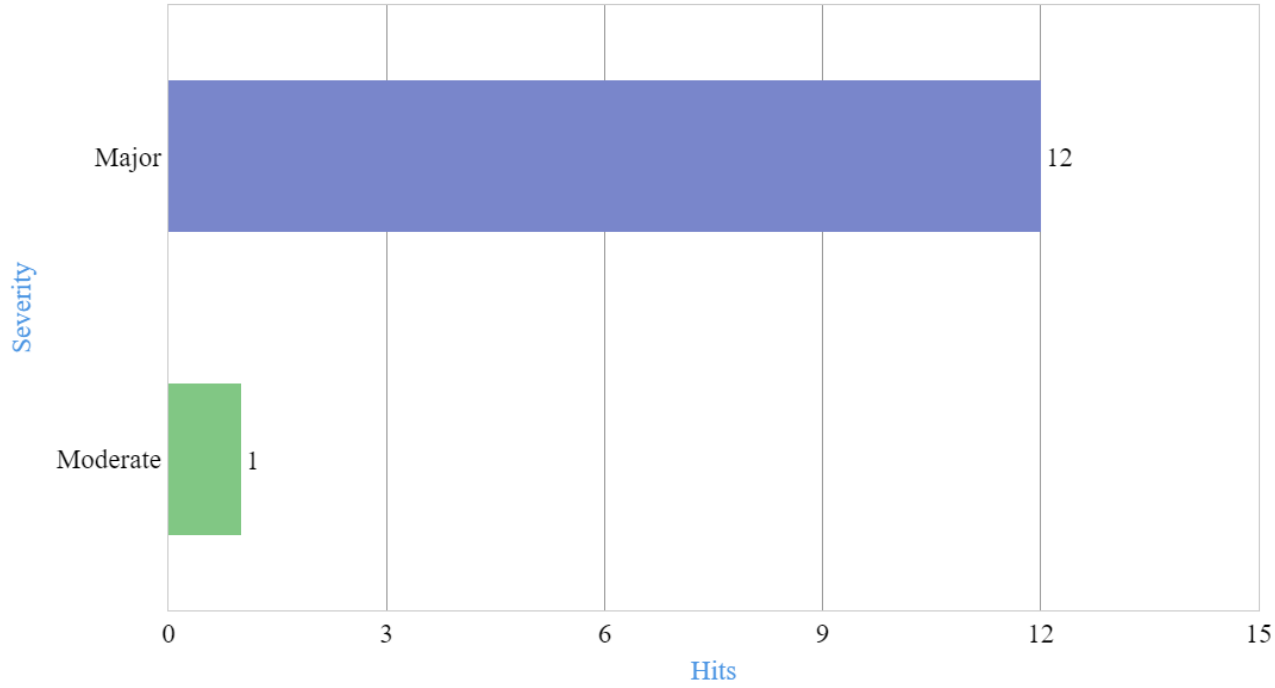
## 3.Attack targets




| TARGET | HITS |
|---|---|
| Client | 11 |
| Server | 2 |

SOPHOS

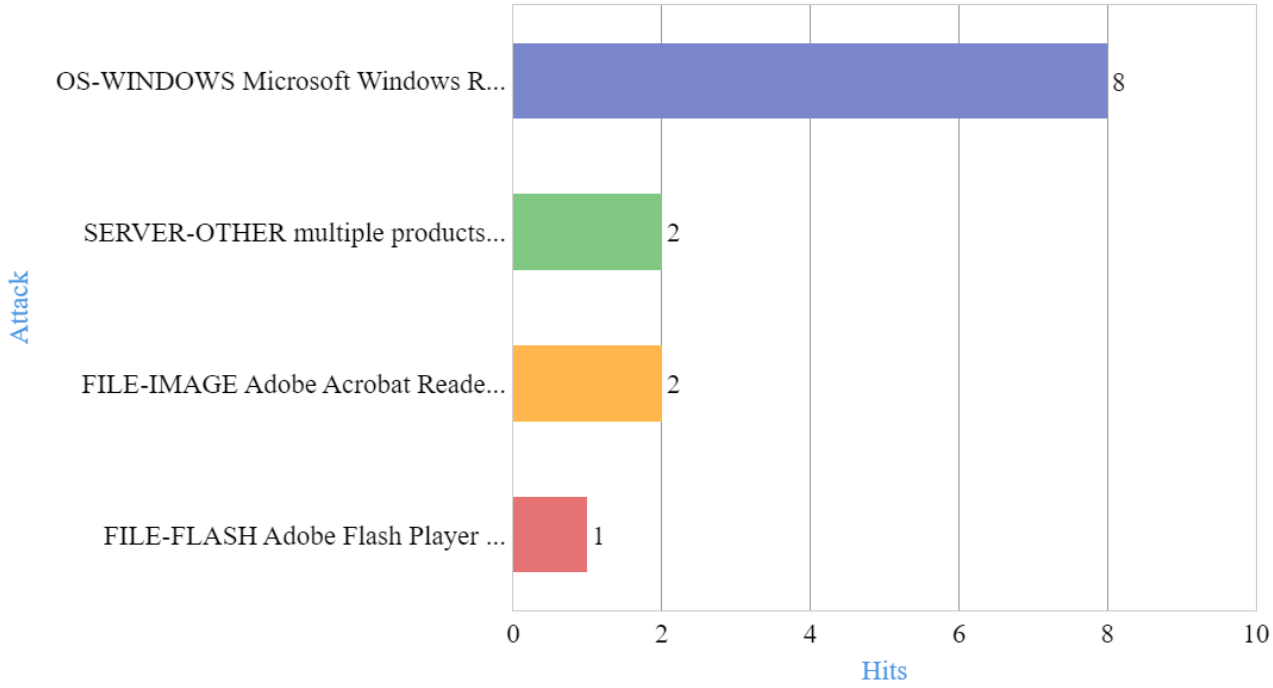
## 4.Severity-wise attacks




| SEVERITY | HITS |
|---|---|
| Major | 12 |
| Moderate | 1 |

SOPHOS

# 5.Intrusion attacks




| ATTACK | HITS |
|---|---|
| OS-WINDOWS Microsoft Windows Remote Procedure Call Runtime ProcessBindAckOrNak CVE-2022-26809 Integer Overflow | 8 |
| SERVER-OTHER multiple products blacknurse ICMP denial of service attempt | 2 |
| FILE-IMAGE Adobe Acrobat Reader JPEG 2000 tile memory corruption attempt | 2 |
| FILE-FLASH Adobe Flash Player domain security bypass attempt | 1 |

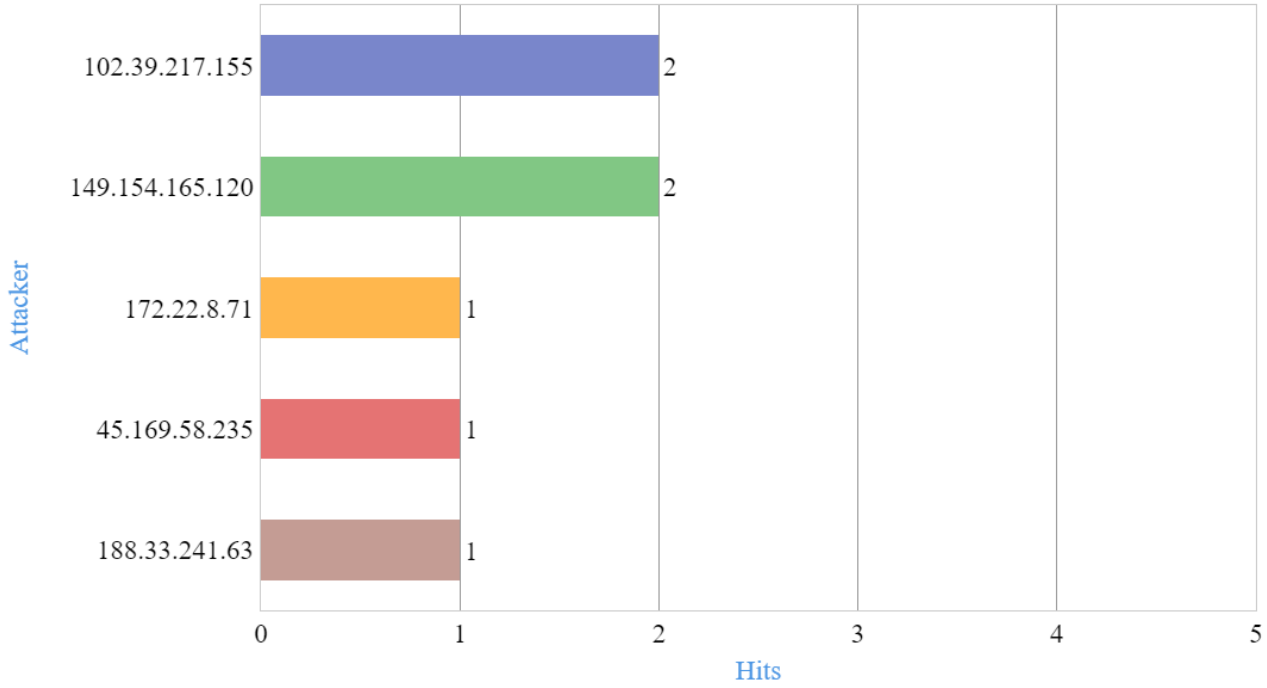
SOPHOS

## 6.Attacks detected and allowed

| ATTACK | HITS |
| --- | --- |
| No record found | |

SOPHOS

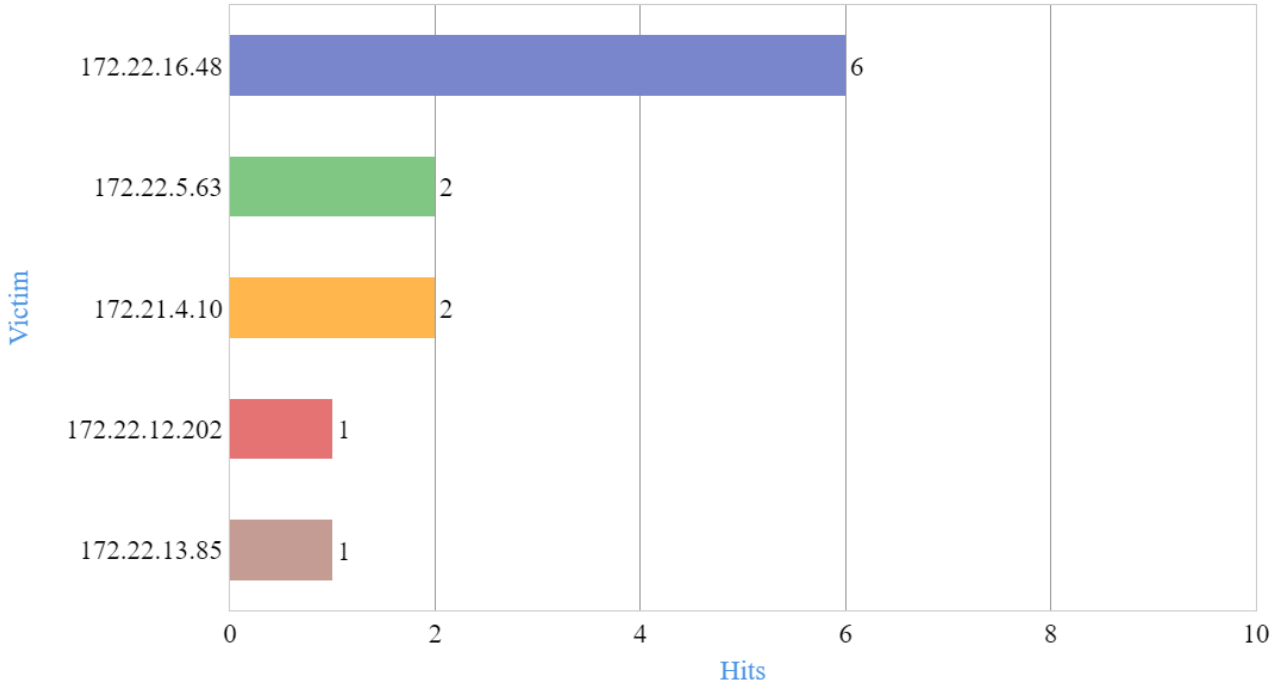
## 7.Intrusion source




| ATTACKER | HITS |
|---|---|
| 102.39.217.155 | 2 |
| 149.154.165.120 | 2 |
| 172.22.8.71 | 1 |
| 45.169.58.235 | 1 |
| 188.33.241.63 | 1 |

SOPHOS

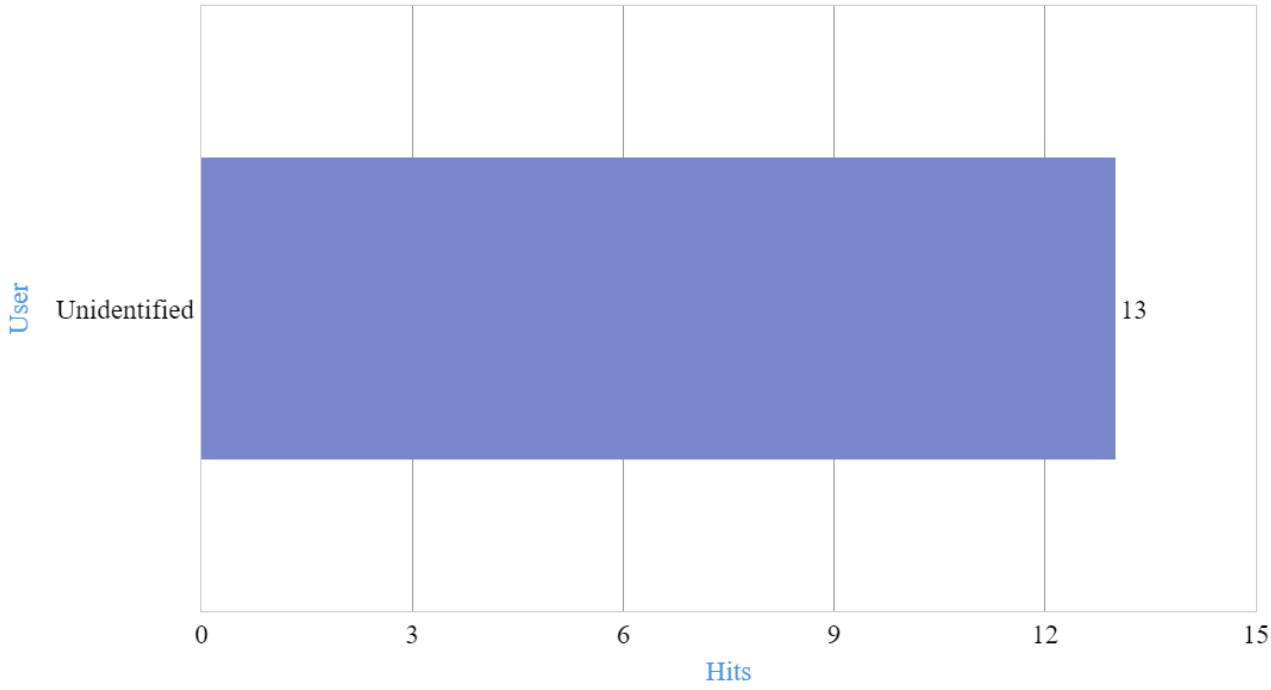
## 8.Intrusion destination




| VICTIM | HITS |
|---|---|
| 172.22.16.48 | 6 |
| 172.22.5.63 | 2 |
| 172.21.4.10 | 2 |
| 172.22.12.202 | 1 |
| 172.22.13.85 | 1 |

SOPHOS

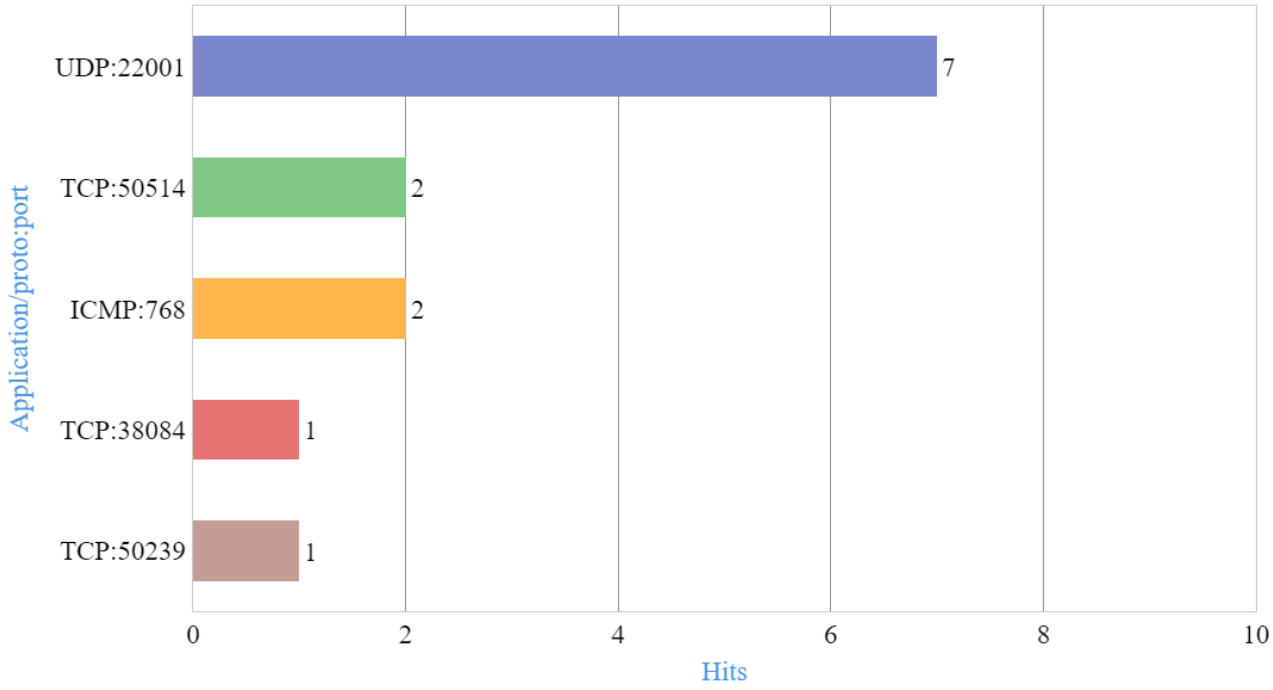
# 9.Users




| USER | HITS |
|---|---|
| Unidentified | 13 |

SOPHOS

# 10.Applications used for attacks



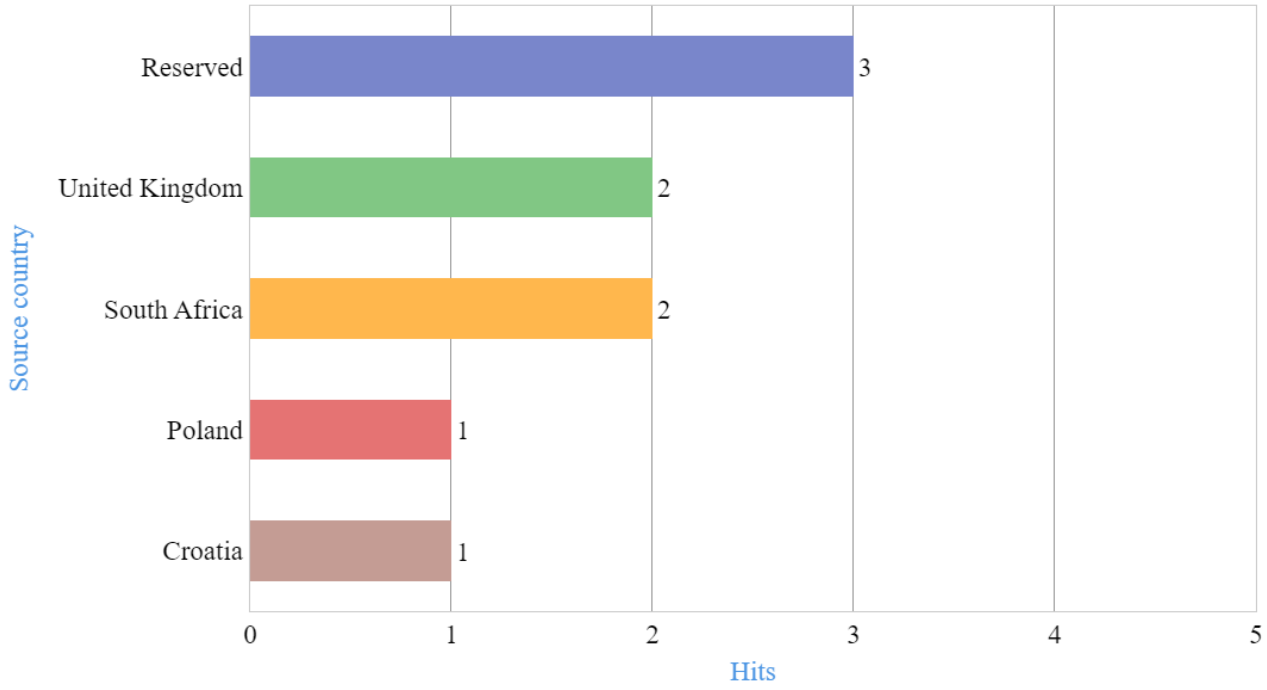

| APPLICATION/PROTO:PORT | HITS |
|---|---|
| UDP:22001 | 7 |
| TCP:50514 | 2 |
| ICMP:768 | 2 |
| TCP:38084 | 1 |
| TCP:50239 | 1 |

SOPHOS

## 11.Lateral movement detection

| ATTACKER SOURCE IP | VICTIM DESTINATION IP | SEVERITY | SIGNATURE ID | SIGNATURE NAME | ACTION | LOGIN USER | PROCESS USER | EXECUTABLE | ATTACK LAST SEEN | HITS |
|---|---|---|---|---|---|---|---|---|---|---|
| No record found | | | | | | | | | | |

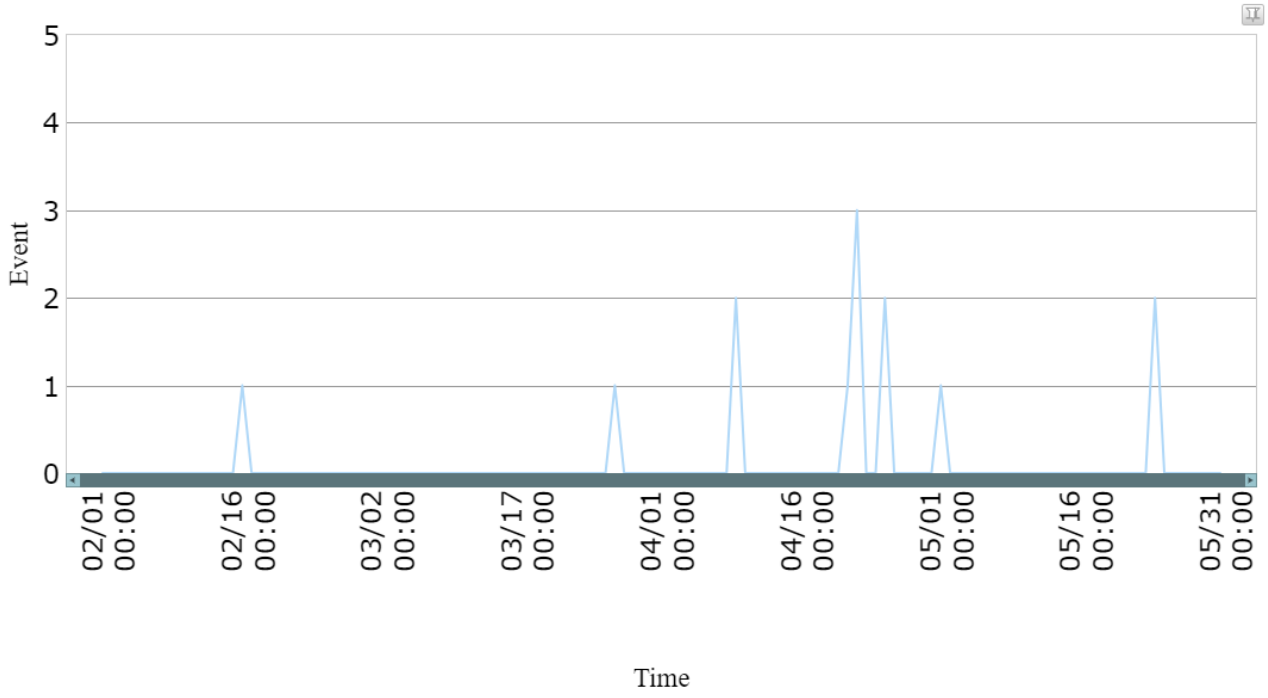
# 12.Source countries




| SOURCE COUNTRY | HITS |
|---|---|
| Reserved | 3 |
| United Kingdom | 2 |
| South Africa | 2 |
| Poland | 1 |
| Croatia | 1 |

SOPHOS

# 13.Trend - intrusion attacks




| TIME | EVENT TYPE | EVENT |
|---|---|---|
| 2024-02-01 00:00:00 | IPS Attack | 0 |
| 2024-02-02 00:00:00 | IPS Attack | 0 |
| 2024-02-03 00:00:00 | IPS Attack | 0 |
| 2024-02-04 00:00:00 | IPS Attack | 0 |
| 2024-02-05 00:00:00 | IPS Attack | 0 |