LAPORAN SERANGAN

REKAP SERANGAN
BULAN FEBRUARI & MARET

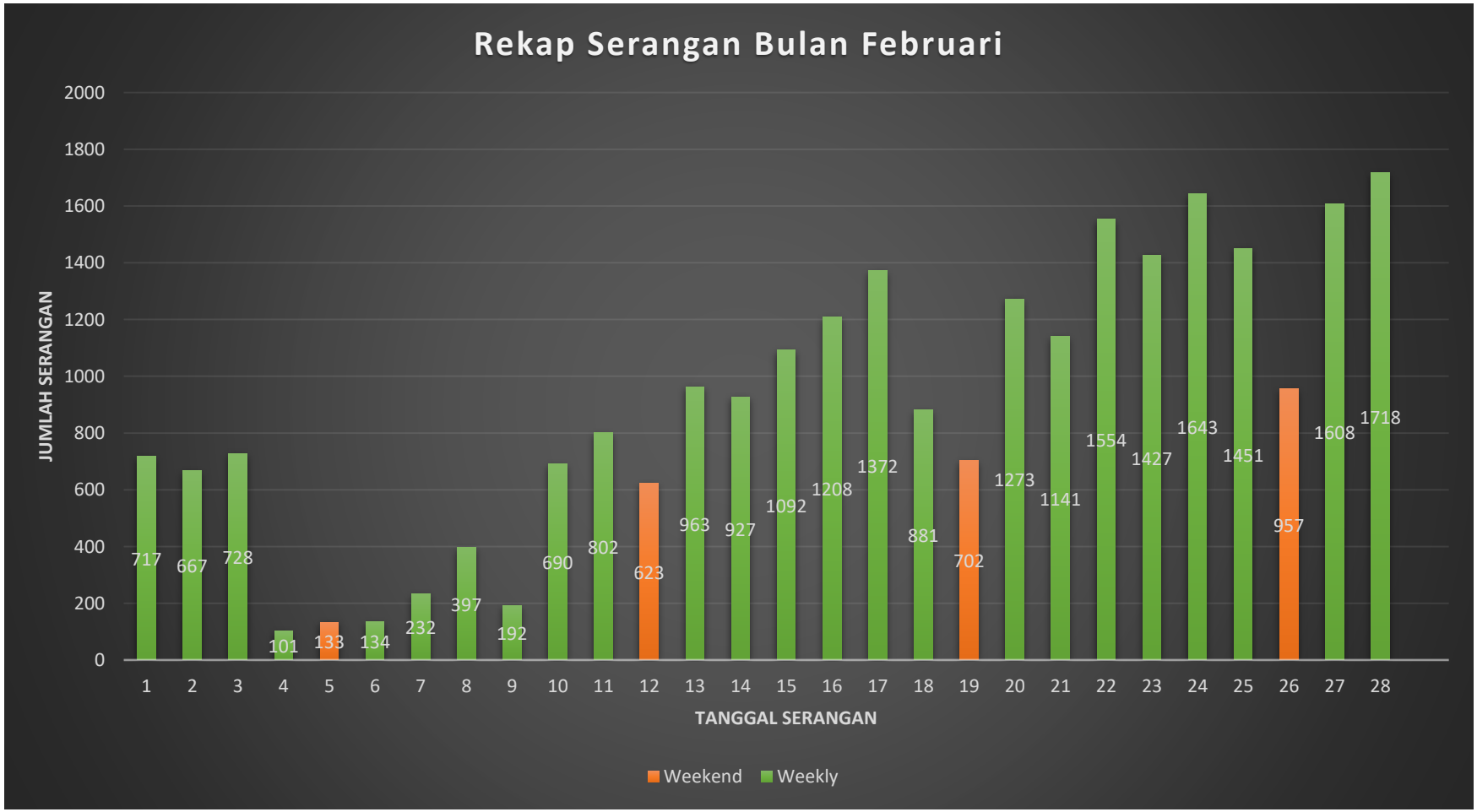
DINAS KOMUNIKASI INFORMATIKA DAN PERSANDIAN ACEH
BANDA ACEH
PEMPROV ACEH
2023/1444

DAFTAR ISI

Rekap serangan

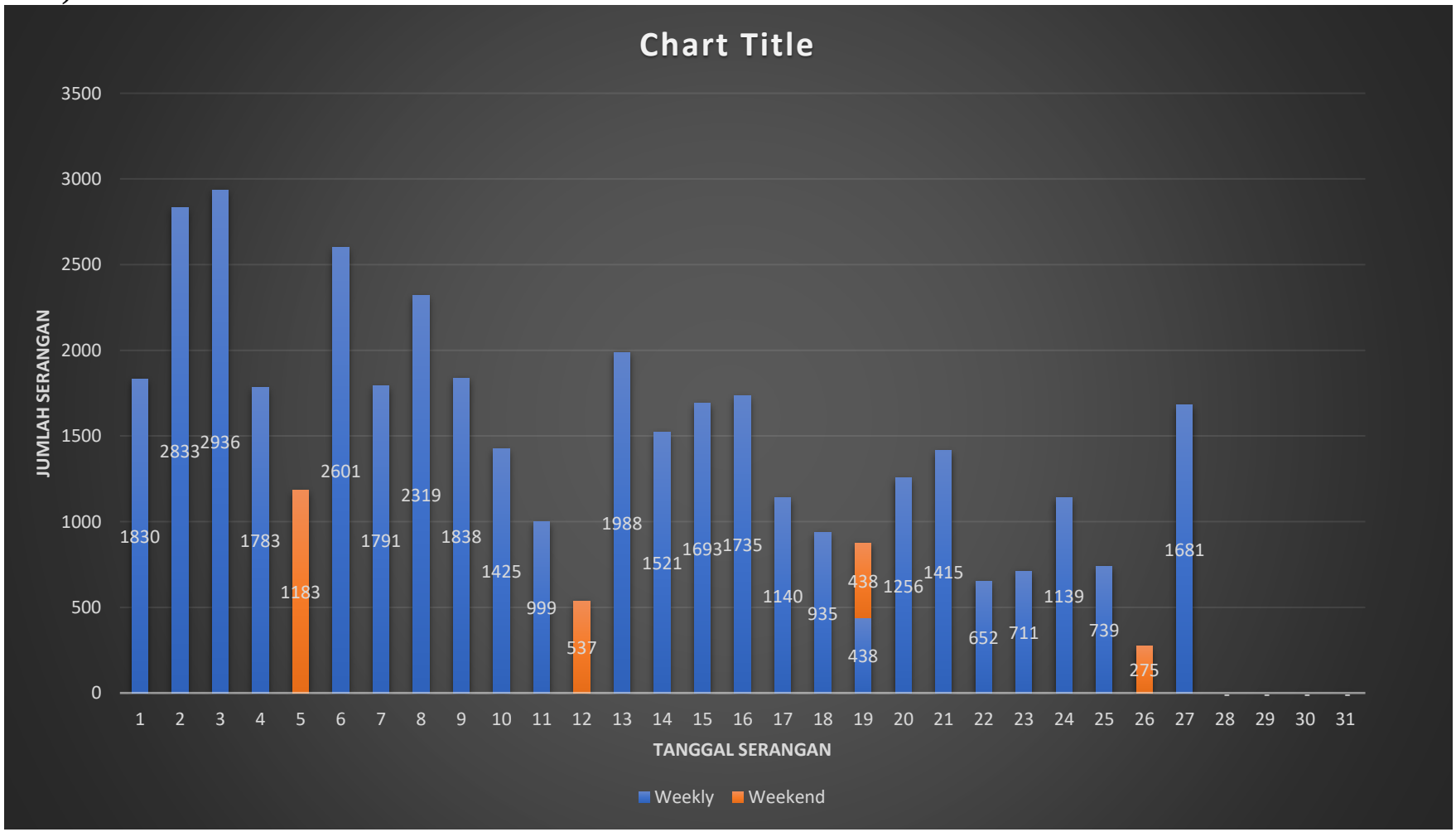
A.Serangan Pada IP Address

a) Bulan Februari



***Total serangan pada bulan februari sebanyak 25.333 serangan, umumnya serangan menjadi lebih masif terjadi pada hari kerja dan pada akhir bulan serangan sangat meningkat tinggi dibandingkan awal bulan.**

b) Bulan Maret



***Total serangan pada bulan maret sebanyak 39.393 serangan, serangan pada bulan Maret umumnya sangat masif pada hari kerja dan pada awal bulan serangan sangat meningkat tinggi, namun pada akhir bulan serangan beransur lebih menurun.**

B. Serangan Pada *PORT*

1. Bulan Februari

Pada bulan Februari terdapat serangan pada beberapa *Port*, serangan yang terjadi pada bulan ini sebanyak 25.333 serangan yang dilakukan dan *port* 445 menjadi target serangan yang terbanyak pada bulan februari.

1. *Port* 445 (*https*)

Pada *port* 445 terdapat 6.091 serangan yang terjadi pada bulan ini, berikut adalah beberapa ip yang melakukan penyerangan pada *port* 445 dan jumlah serangan yang dituju.

IP	Negara	Jumlah Serangan
101.255.118.129	Indonesia	3
101.255.122.68	Indonesia	18
101.255.126.210	Indonesia	9
101.255.150.126	Indonesia	3
101.255.157.214	Indonesia	2
101.255.162.126	Indonesia	1
101.255.162.43	Indonesia	21
101.255.164.138	Indonesia	3
101.255.171.203	Indonesia	3
101.255.200.10	Indonesia	3

2. *Port* 3306 (MySQL)

Pada *port* 3306 terdapat sebanyak 5.999 serangan yang dilancarkan, berikut adalah beberapa ip yang melakukan penyerangan pada *port* 3306 dan jumlah serangan yang dituju.

IP	Negara	Jumlah Serangan
101.255.118.129	Indonesia	3
101.255.122.68	Indonesia	18
101.255.126.210	Indonesia	9
101.255.150.126	Indonesia	3
101.255.157.214	Indonesia	2
101.255.162.126	Indonesia	1
101.255.162.43	Indonesia	21
101.255.164.138	Indonesia	3
101.255.171.203	Indonesia	3
101.255.200.10	Indonesia	3

3. *Port* 21 (FTP)

Pada *port* 21 terdapat sebanyak 60 serangan, berikut adalah beberapa ip yang melakukan penyerangan pada *port* 21 dan jumlah serangan yang dituju.

IP	Negara	Jumlah Serangan
36.71.142.157	Indonesia	56
36.71.143.126	Indonesia	4

4. *Port* 135 (RPC)

Pada *port* 135 terdapat sebanyak 4 serangan, berikut adalah beberapa ip yang melakukan penyerangan pada *port* 135 dan jumlah serangan yang dituju.

IP	Negara	Jumlah Serangan
36.71.142.157	Indonesia	3
36.71.143.126	Indonesia	1

5. *Port* 5060 (Non-encrypted traffic)

Pada *port* 5060 terdapat sebanyak 60 serangan, berikut adalah beberapa ip yang melakukan penyerangan pada *port* 4 dan jumlah serangan yang dituju.

IP	Negara	Jumlah Serangan
152.32.154.144	Indonesia	1
180.250.247.29	Indonesia	1
36.71.142.157	Indonesia	1
43.240.224.204	Indonesia	1

2. Bulan Maret

Pada bulan Maret serangan yang terjadi hanya pada 2 *port*, serangan pada bulan Maret sebanyak 39.393 serangan yang dilancarakan.

1. *Port* 445 (https)

Pada *port* 445 terdapat sebanyak 12.314 serangan yang terjadi pada bulan ini, berikut adalah beberapa ip yang melakukan penyerangan pada *port* 445 dan jumlah serangan yang dituju.

IP	Negara	Jumlah Serangan
101.255.115.242	Indonesia	5
101.255.117.225	Indonesia	3
101.255.120.193	Indonesia	6
101.255.120.194	Indonesia	3
101.255.123.202	Indonesia	3
101.255.126.210	Indonesia	16
101.255.126.211	Indonesia	2
101.255.140.110	Indonesia	2
101.255.156.246	Indonesia	3
101.255.162.126	Indonesia	4

2. *Port* 3306 (MySQL)

Pada *port* 3306 terdapat sebanyak 16.931 serangan yang dilancarkan, berikut adalah beberapa ip yang melakukan penyerangan pada *port* 3306 dan jumlah serangan yang dituju.

IP	Negara	Jumlah Serangan
101.0.6.217	Indonesia	6
101.0.6.233	Indonesia	4
101.128.109.56	Indonesia	6
101.128.66.249	Indonesia	6
101.128.68.207	Indonesia	4
101.128.75.179	Indonesia	1
101.128.85.116	Indonesia	6
101.128.85.178	Indonesia	15
101.128.92.254	Indonesia	3
101.128.99.192	Indonesia	2

C. Serangan Malware

Dalam beberapa bulan terakhir tidak ada terjadinya penyerangan malware yang tertuju ke sistem, serangan malware terakhir kali terjadi pada sistem yaitu di bulan Oktober tahun 2022 lalu, selama bulan Januari – April 2023 tidak ada serangan malware yang dilancarkan ke sistem.

D. Pantauan Serangan Siber

1. Pantauan serangan pada bulan Februari
    - IP 123.108.98.32 menjadi target serangan terbanyak pada bulan Maret dengan jumlah 1.230 serangan,
    - IP 123.108.98.114 memperoleh serangan sebanyak 543 serangan,
    - IP 123.108.98.32 memperoleh serangan sebanyak 304 serangan,
    - IP 180.250.33.131 memperoleh serangan sebanyak 73 serangan, ini adalah IP address PT TELKOM Indonesia, Jakarta,
    - IP 103.155.105.100 memperoleh serangan sebanyak 68 serangan, ini merupakan IP address PemKab Wonosobo, Jawa Tengah,
    - IP 103.111.190.50 memperoleh serangan sebanyak 68 serangan, ini adalah IP address dari PT. Maga Inti Solusi, Jakarta Selatan,
    - IP 139.255.85.114 memperoleh serangan sebanyak 64 serangan, ini adalah IP address dari PT. First Media Service, Jakarta,
    - IP 112.78.188.242 memperoleh serangan sebanyak 53 serangan, ini adalah IP address dari Biznet Network, Jakarta,
    - IP 103.94.0.66 memperoleh serangan sebanyak 53 serangan, ini adalah IP address dari PT Indonesia Comnets Plus, Depok.

2. Pantauan serangan pada bulan Maret
    - IP 123.108.98.11 menjadi target serangan terbanyak pada bulan Maret dengan jumlah 739 serangan secara total,
    - IP 123.108.98.114 memperoleh serangan sebanyak 351 serangan,
    - IP 14.102.153.194 memperoleh serangan sebanyak 140 serangan, ini adalah IP address dari PT Skyline Semesta, Bandung Jawa Barat,
    - IP 103.111.208.26 memperoleh serangan sebanyak 125 serangan, ini adalah IP address dari CV Bina Wahana Pusaka, Jakarta Timur,
    - IP 36.89.91.153 memperoleh serangan sebanyak 122 serangan, ini merupakan IP address dari PT Telekomunikasi Indonesia, Jakarta,
    - IP 36.71.150.118 memperoleh serangan sebanyak 121 serangan, ini merupakan IP address dari PT Telkom Indonesia, Jakarta,
    - IP 123.108.64.233 memperoleh serangan sebanyak 100 serangan, ini merupakan IP address dari PT. GOMEDS NETWORK, Gorontalo,
    - IP 43.252.238.94 memperoleh serangan sebanyak 76 serangan, ini adalah IP address PT. Usaha Adi Sanggoro, Bogor,
    - IP 103.126.173.54 memperoleh serangan sebanyak 53 serangan, ini adalah IP address dari PT Magarap Mitra Solusi, Bandar Lampung.

E. Kesimpulan

Serangan siber bisa terjadi kapan saja dan di mana saja tampat memandang waktu dan tempat dari target korbannya, semakin canggih alat modern maka semakin hebat para penyerang dalam melakukan serangannya. Dalam rekap serangan ini, serangan yang terjadi pada bulan bulan februari mencapai 25.333 ribu total serangan yang dilakukan oleh para *attacker*, pada bulan februari terdapat 5 target port yang dilancarkan dan port 445 (https) mejadi target terbanyak pada bulan februari.

Serangan siber pada bulan Maret mencapai 39.393 ribu serangan yang dilancarkan oleh penyerang, penyerangan pada bulan Maret lebih banyak dibandingankan dengan bulan Februari, pada bulan Maret terdapat 2 port target yang diserang oleh attacker yaitu port 445 (https) dan port 3306 (MySQL) pada bulan ini port yang terbanyak menjadi target ialah port 3306 (MySQL) dengan total sebanyak 16.931 ribu serangan. pada bulan April tidak ada informasi ataupun serngan yang terdapat pada portal Honeynet BSSN.