Internet Intrusion:
Indonesian Characteristics

by
Bisyron Wahyudi
Muhammad Salahuddien

Background

- Amount of malicious traffic circulating on the Internet is increasing significantly.
- Increasing complexity and rapid change in hosts and networks technology suggests that there will be new vulnerabilities.
- Attackers have interest in identifying networks and hosts to expose vulnerabilities :
  - Network scans
  - Worms
  - Trojans
  - Botnet

Background (2)

- Complicated methods of attacks make difficult to identify the real attacks : It is not simple as filtering out the traffic from some sources
- Security is implemented like an “add on” module for the Internet.

Objectives

- Understanding nature behavior of malicious sources and targeted ports is important to minimize the damage by build strong specific security rules and counter measures
- Help the cyber security policy-making process, and to raise public awareness
- Questions :
  - Do malicious sources generate the attacks uniformly ?
  - Is there any pattern specific i.e. recurrence event ?
  - Is there any correlation between the number of some attacks over specific time ?

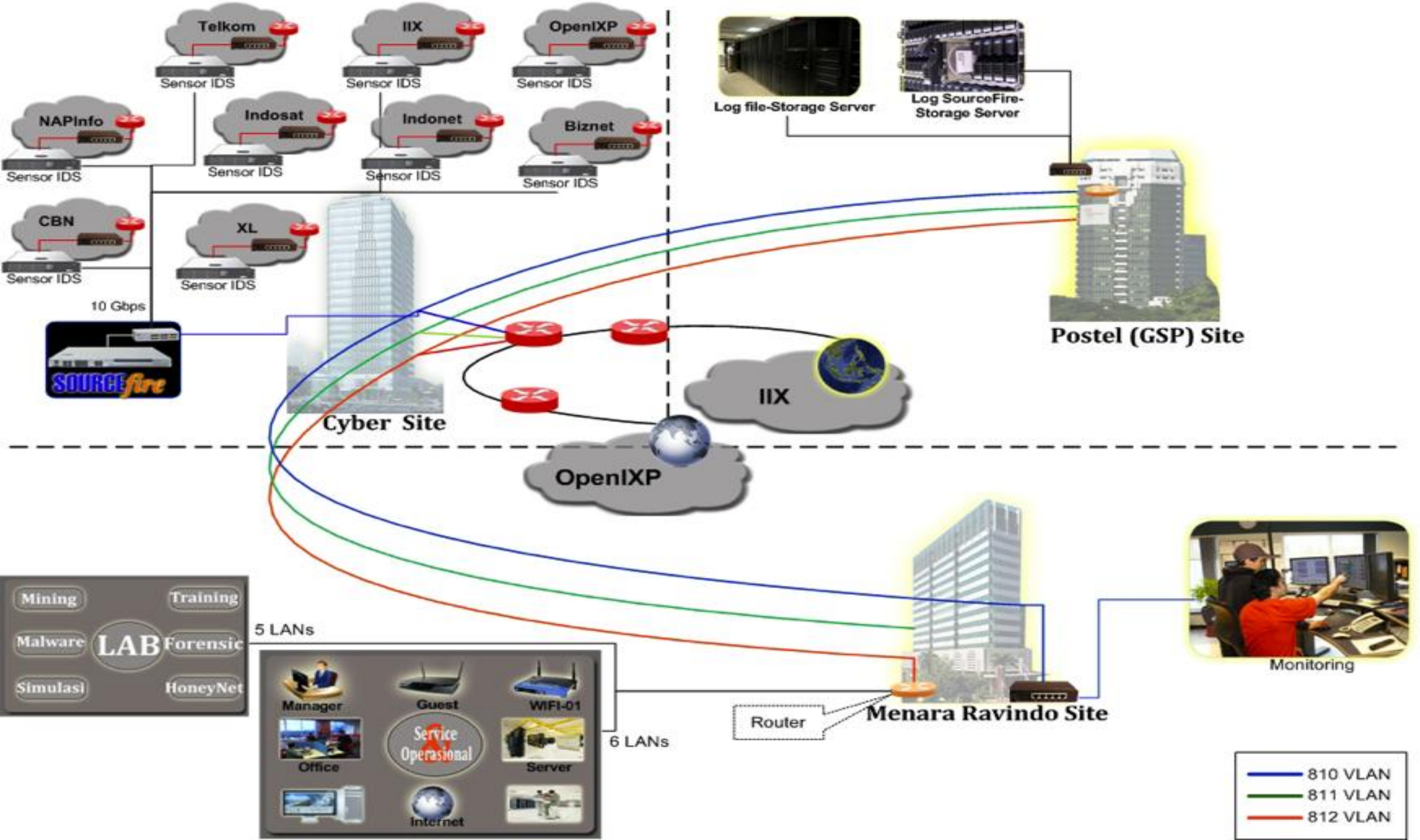
Motivation

- Many systems and phenomena (events) are distributed according to a "power law"
- When one quantity (say *y*) *depends on another (say x) raised to some power, we say that y is described by a **power law***
- A power law applies to a system when:
  - **large is rare and**
  - **small is common**

Sample Data

- Collection of System logs from Networked Intrusion Detection System (IDS)
- The NIDS contains 11 sensors installed in different core networks in Indonesian ISP (NAP)
- Period : January, 2012 - September, 2012
  - Available fields :
    - Event Message, Timestamp, Dest. IP, Source IP, Attacks Classification, Priority, Protocol, Dest. Port/ICMP code, Source Port/ICMP type, Sensors ID

System Architecture



Power Laws

- Two quantities x and y are related by a *power law* if y is proportional to $x^{(-c)}$ for a constant c

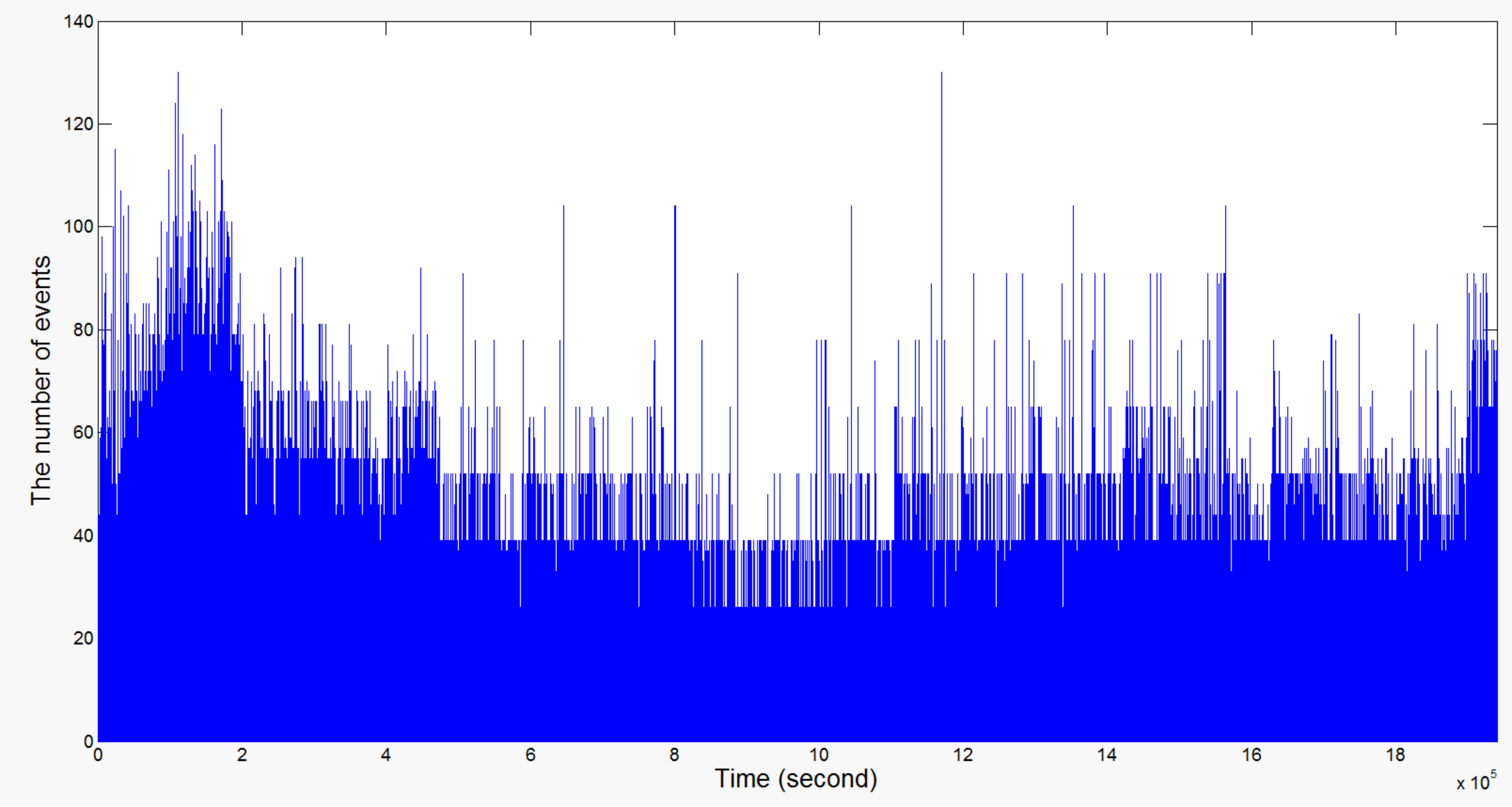
$$y = \alpha . x^{(-c)}$$

- If x and y are related by a power law, then the graph of $\log(y)$ versus $\log(x)$ is a straight line

$$\log(y) = -c . \log(x) + \log(\alpha)$$

- The slope of the log-log plot is the *power exponent* c

Time Series
The plot of the number of event vs. time



Intrusion Characteristics

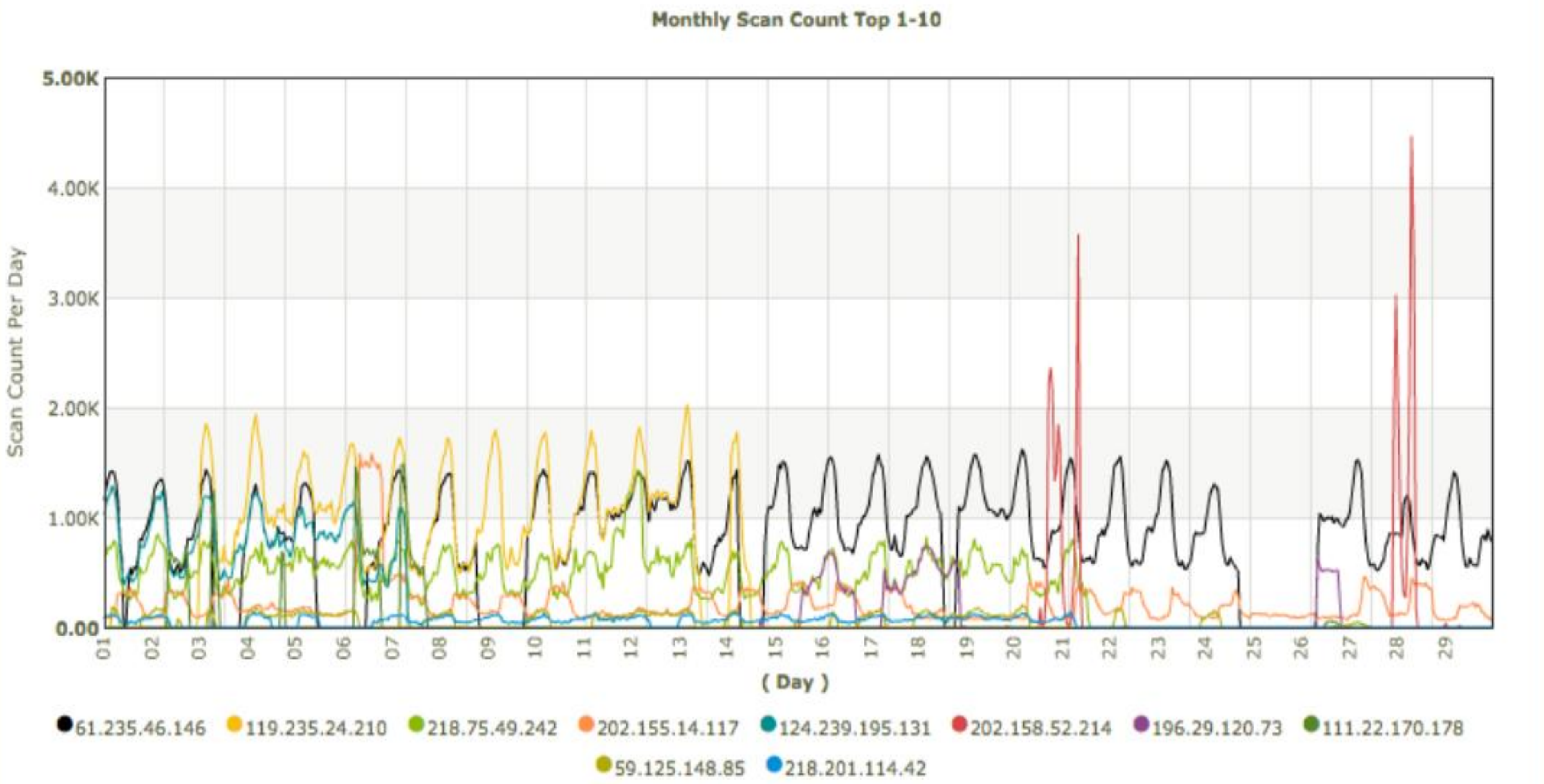
- Destination Port Distribution
  - Monitor destination port for intrusion attempts
- Source IP's Distribution
  - Look for trends in the source address associated with intrusions events
  - Group intrusions into port 1434, 1433, 53, and 445

Temporal Analysis

- Understanding the behavior of malicious sources over the time

- Is there any correlation between the number of attacks over time ?
  - Time series analysis : Power spectrum analysis and Detrended Fluctuation Analysis (DFA)

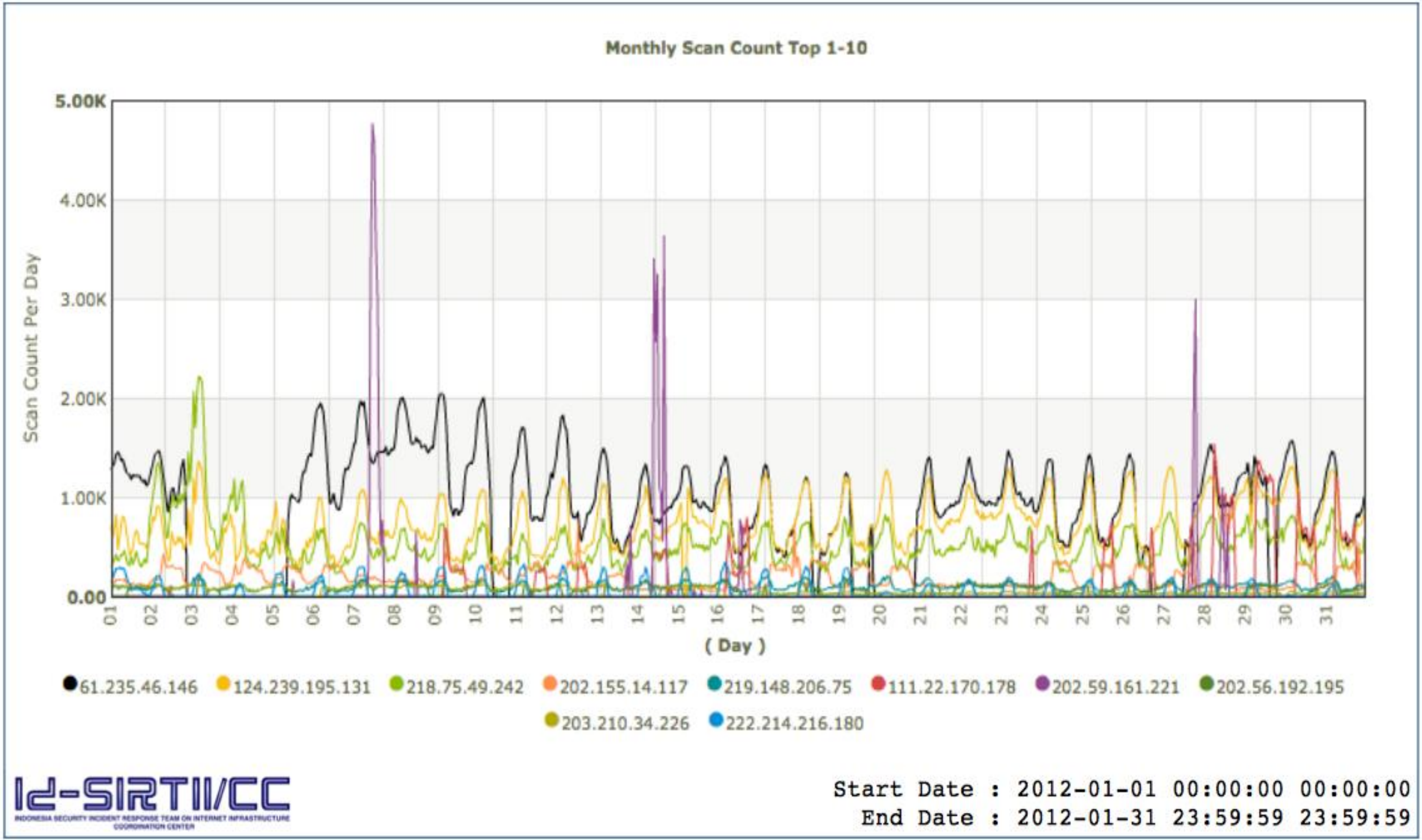
Malicious Sources Distribution



Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

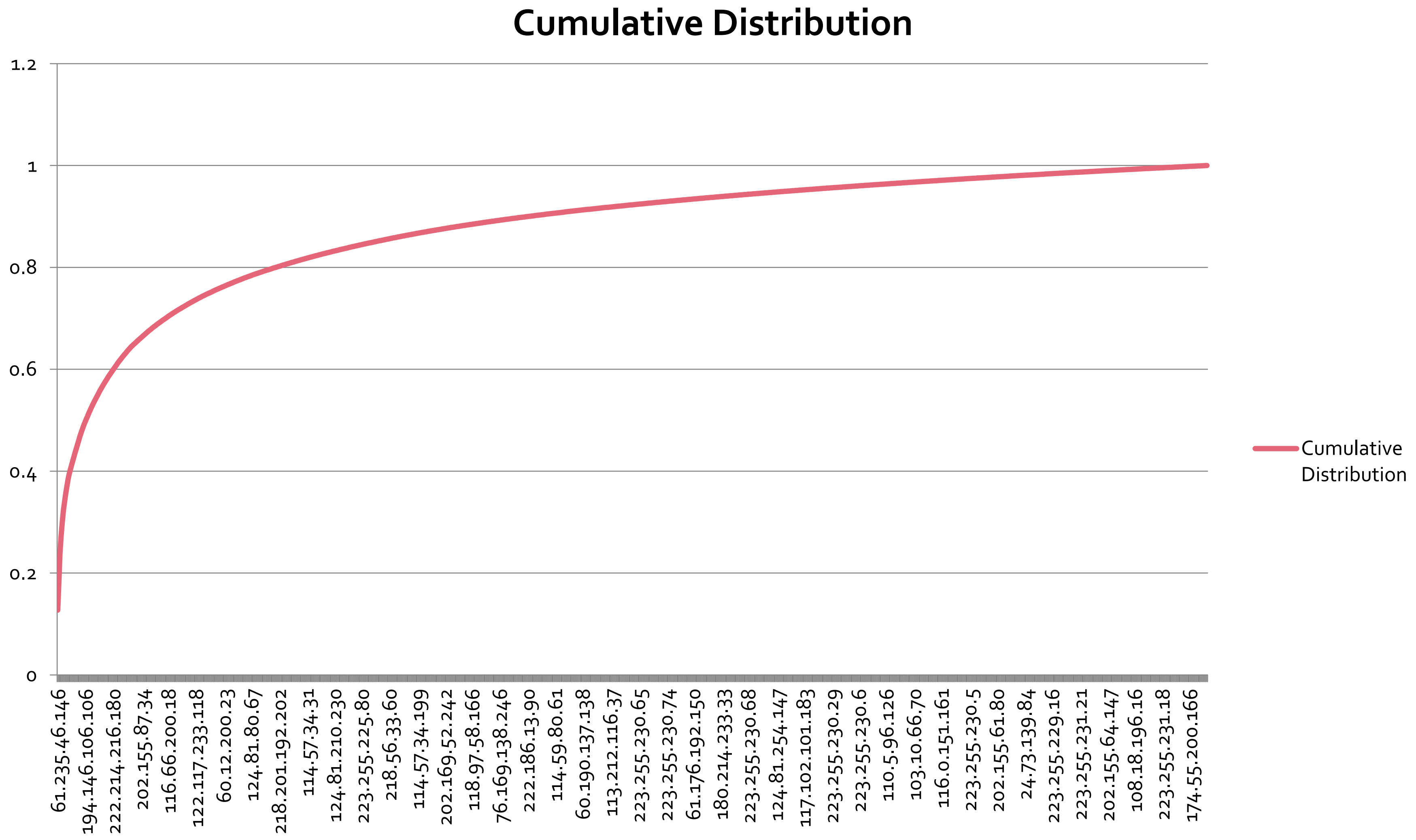
```
Start Date : 2012-02-01 00:00:00 00:00:00
  End Date : 2012-02-29 23:59:59 23:59:59
```

Malicious Sources Distribution



```
Start Date : 2012-01-01 00:00:00 00:00:00
  End Date : 2012-01-31 23:59:59 23:59:59
```

Cumulative Distribution Function (CDF) of Malicious Sources



Malicious IP Sources Remarks

Source IP	Counter	Cumulative Distribution
61.235.46.146	1136787	0.127079841
124.239.195.131	497699	0.182716922
218.75.49.242	485758	0.237019134
211.141.86.248	315837	0.272326114
202.155.14.117	241850	0.29936219
119.235.24.210	214618	0.323354038
60.190.118.153	148839	0.339992544
61.128.110.96	145968	0.356310104
117.102.102.34	124868	0.370268924

Do malicious sources generate the attacks uniformly ?

- Only a few sources are responsible for many generating malicious traffics
  - These sources attacks on ports 1434 (MS SQL-M), 53 (DNS), 445 (Microsoft DS), 1433(MS SQL-S)
- Argument for a blacklist
- Most of sources are generating 1 attack
  - It is not efficient to filtering out these type of sources

Temporal Analysis

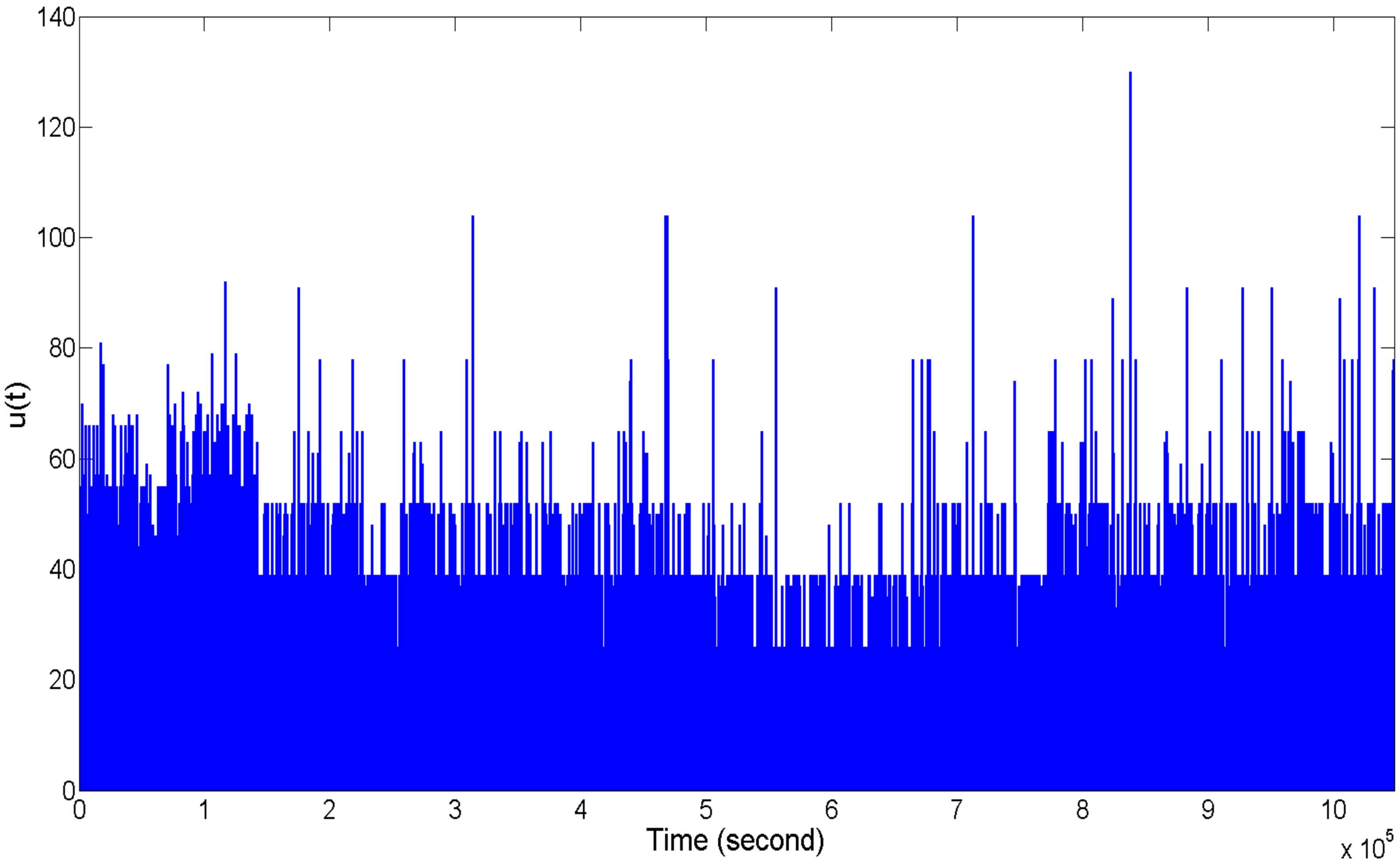
- Understanding the behavior of malicious sources over the time

- Is there any correlation between the number of attacks over time ?
  - Time series analysis : Power spectrum analysis and DFA

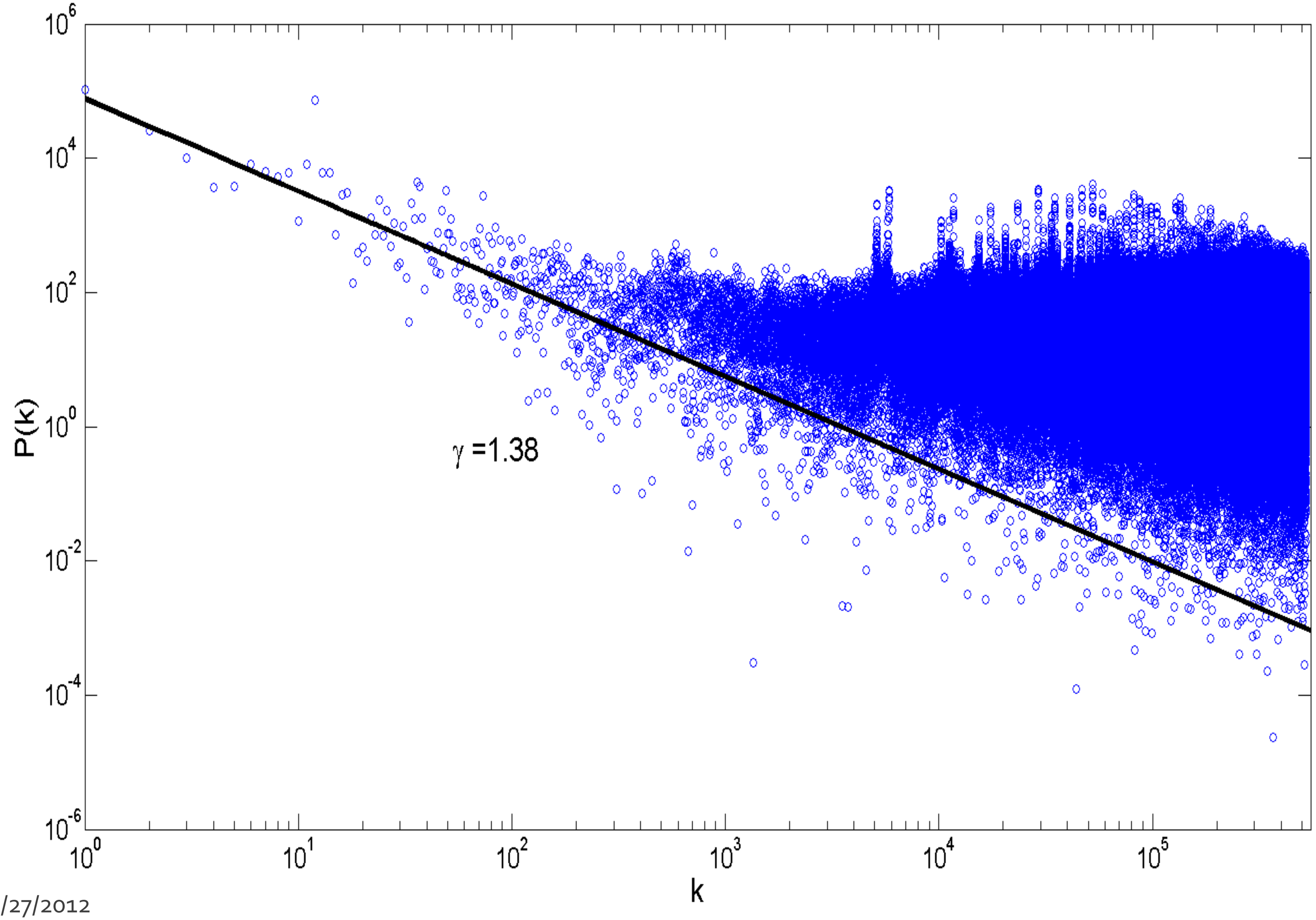
Temporal Analysis

- If we analyze the total time series from all sensors: there are no strong correlation between the number of attacks and time
- Analyzing the time series from each sensor is preferred. The statistical properties for each sensor is not the same.

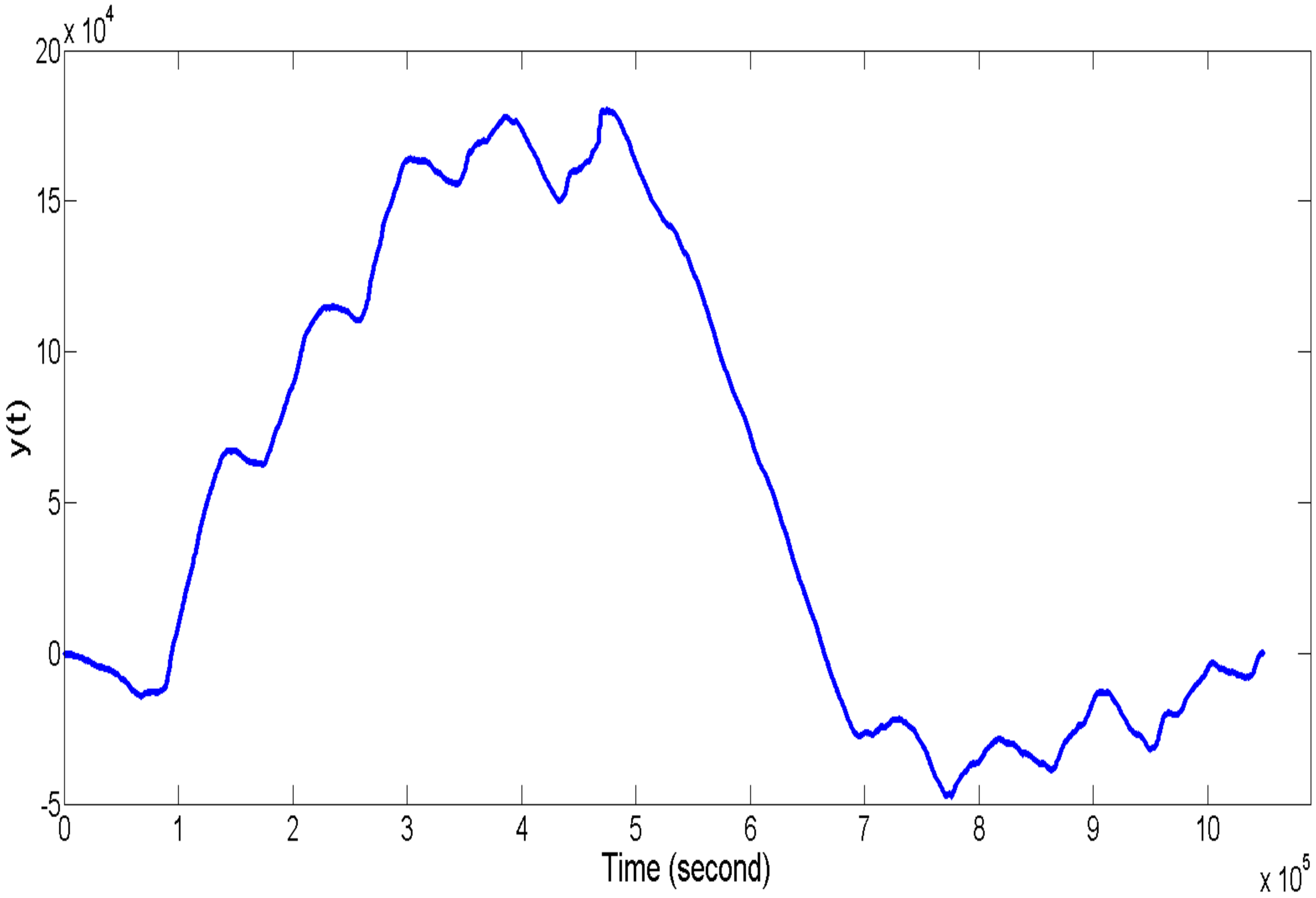
All (u(t))



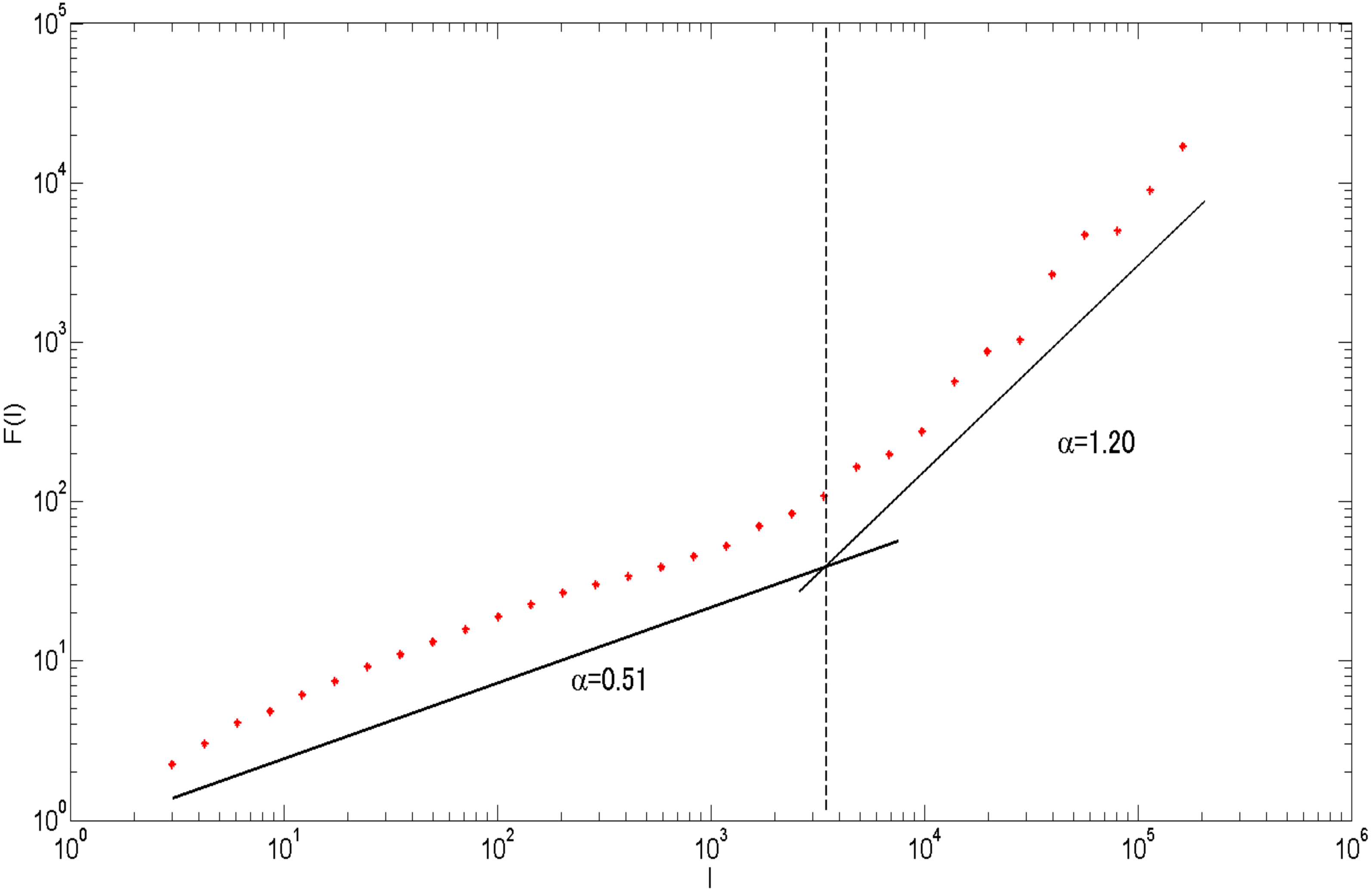
All (Power Spectrum)



All (y(t))



All (DFA)

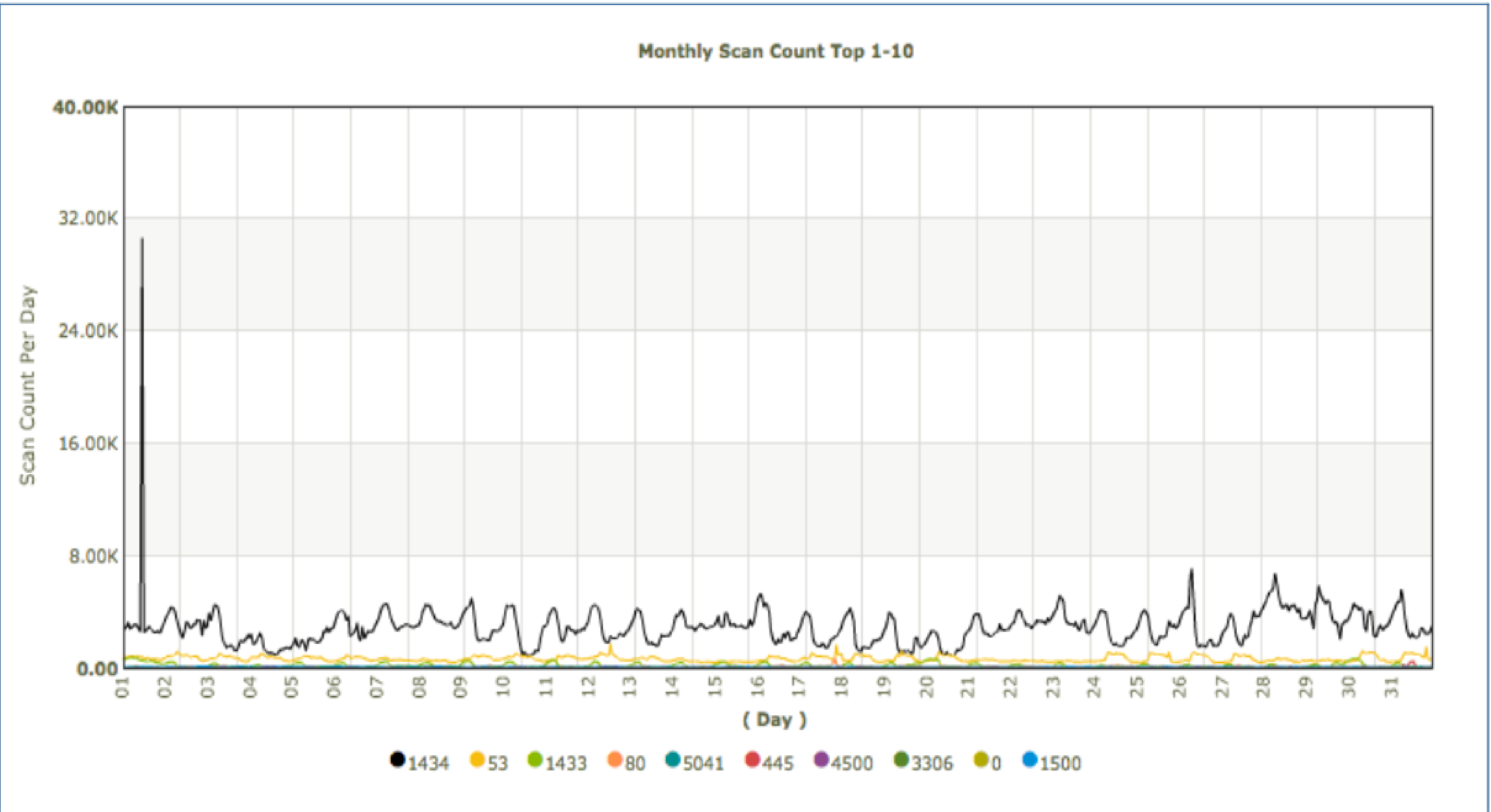


10^5
10^4
10^3
10^2
10^1
10^0
F(l)
α=1.20
α=0.51
10^0
10^1
10^2
10^3
10^4
10^5
10^6
l

Remarks

- The number of attacks behavior over the time is random
- The result of DFA seems to be divided into two region of different exponents of Power Law fluctuation.
- There is a bending point, need more investigation.

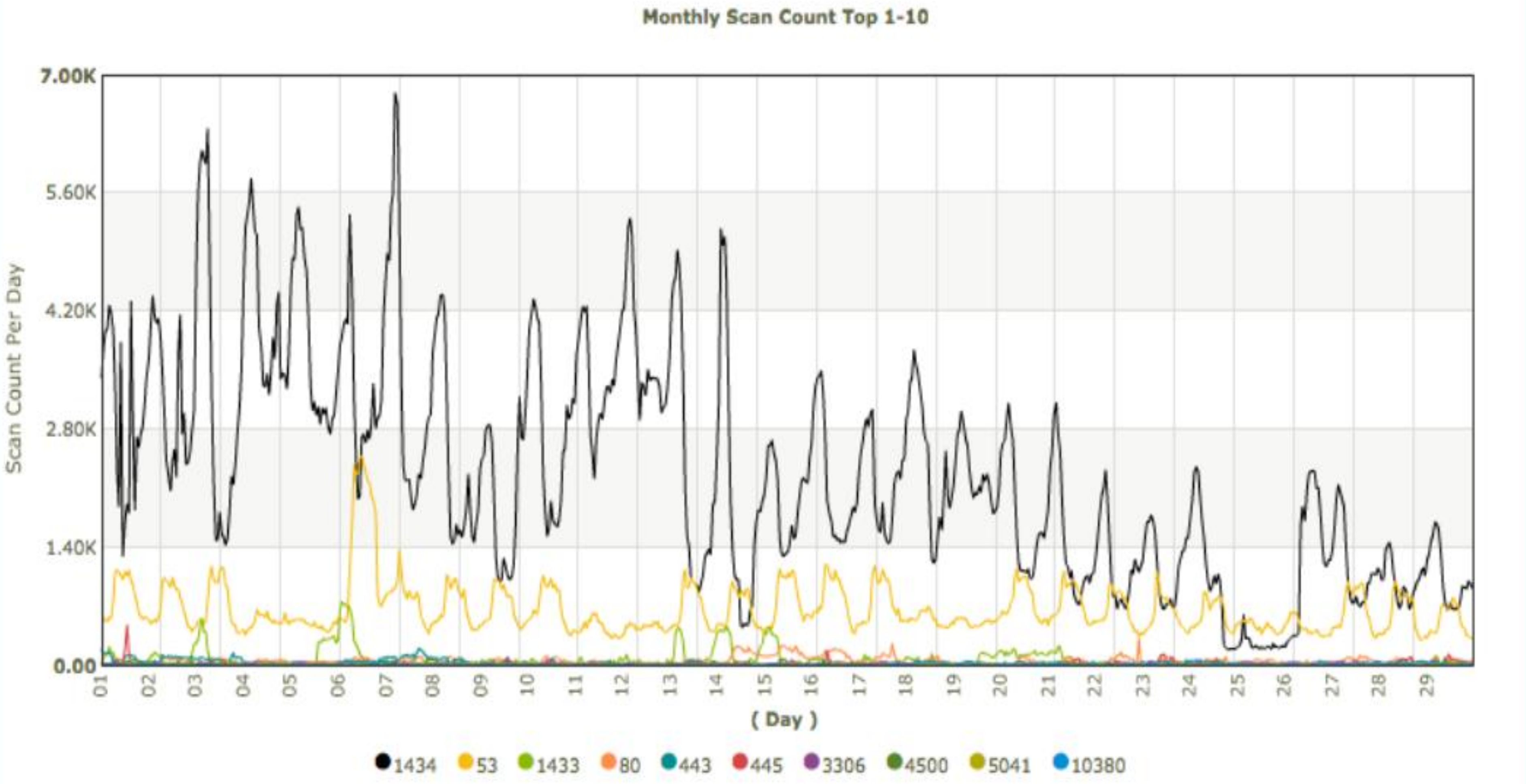
Targeted Ports Distribution



ID-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

```
Start Date : 2012-01-01 00:00:00 00:00:00
  End Date : 2012-01-31 23:59:59 23:59:59
```

Targeted Ports Distribution

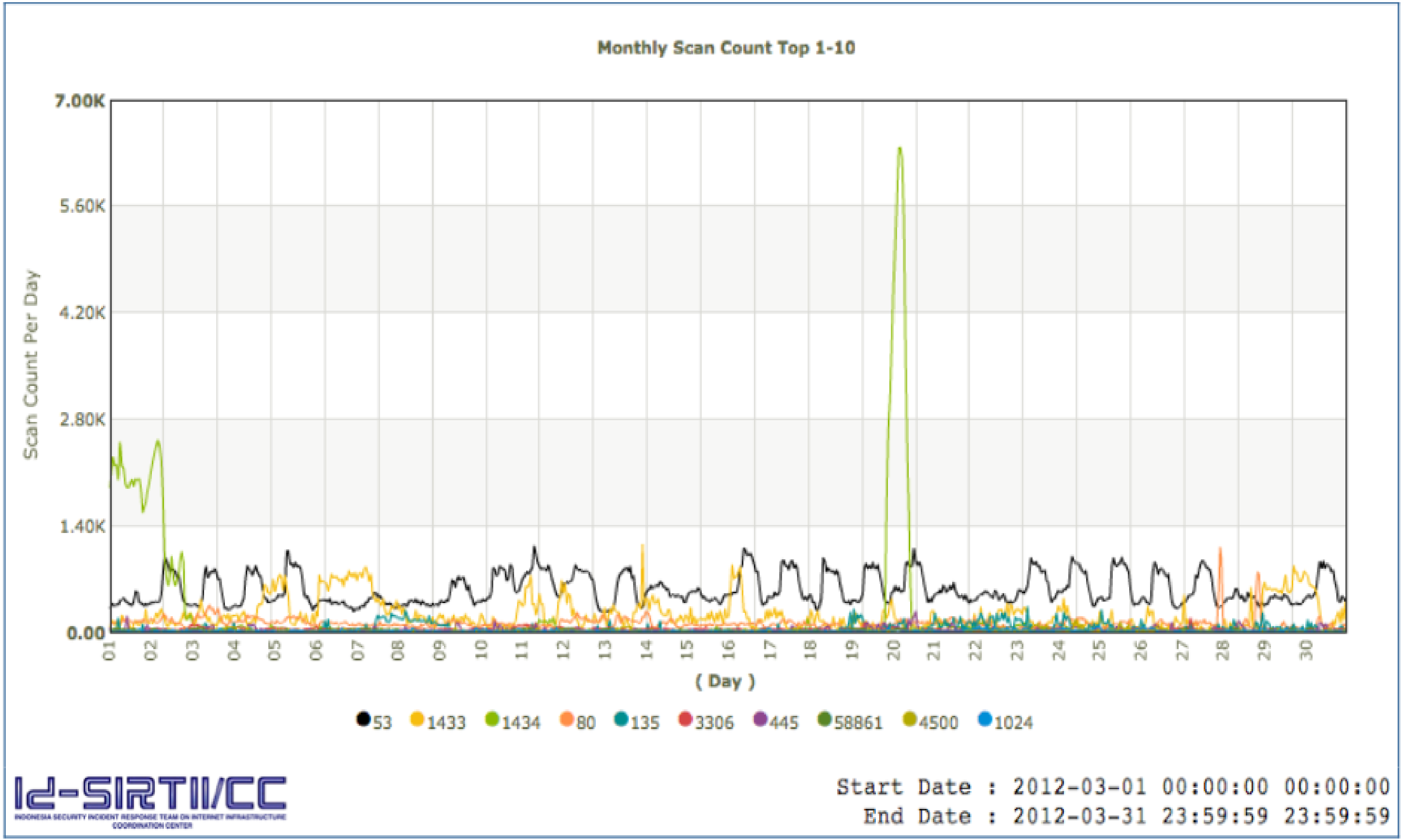


Id-SIRTII/CC

INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

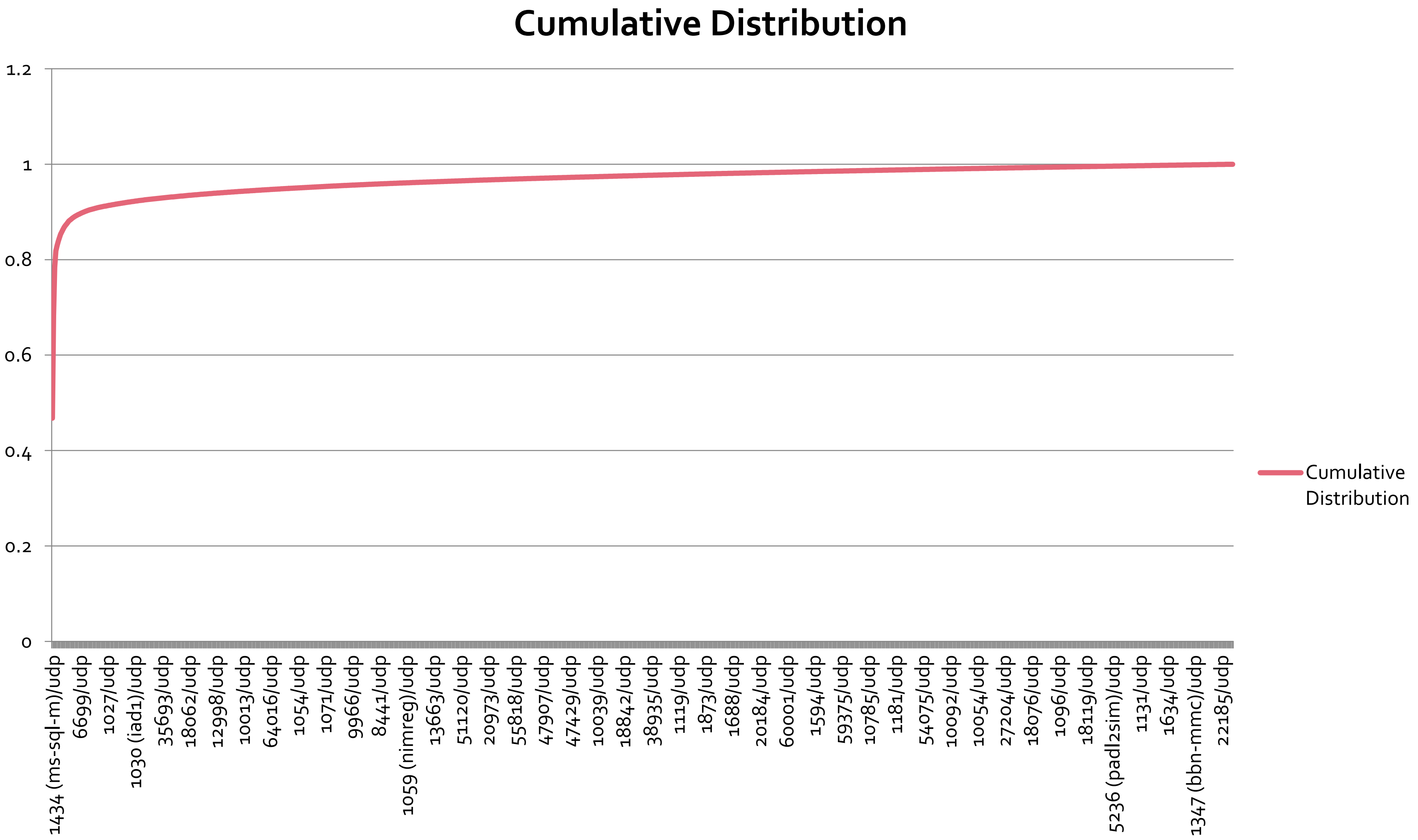
Start Date : 2012-02-01 00:00:00 00:00:00
End Date : 2012-02-29 23:59:59 23:59:59

Targeted Ports Distribution



Start Date : 2012-03-01 00:00:00 00:00:00
End Date : 2012-03-31 23:59:59 23:59:59

Cumulative Distribution Function (CDF) of Targeted Ports

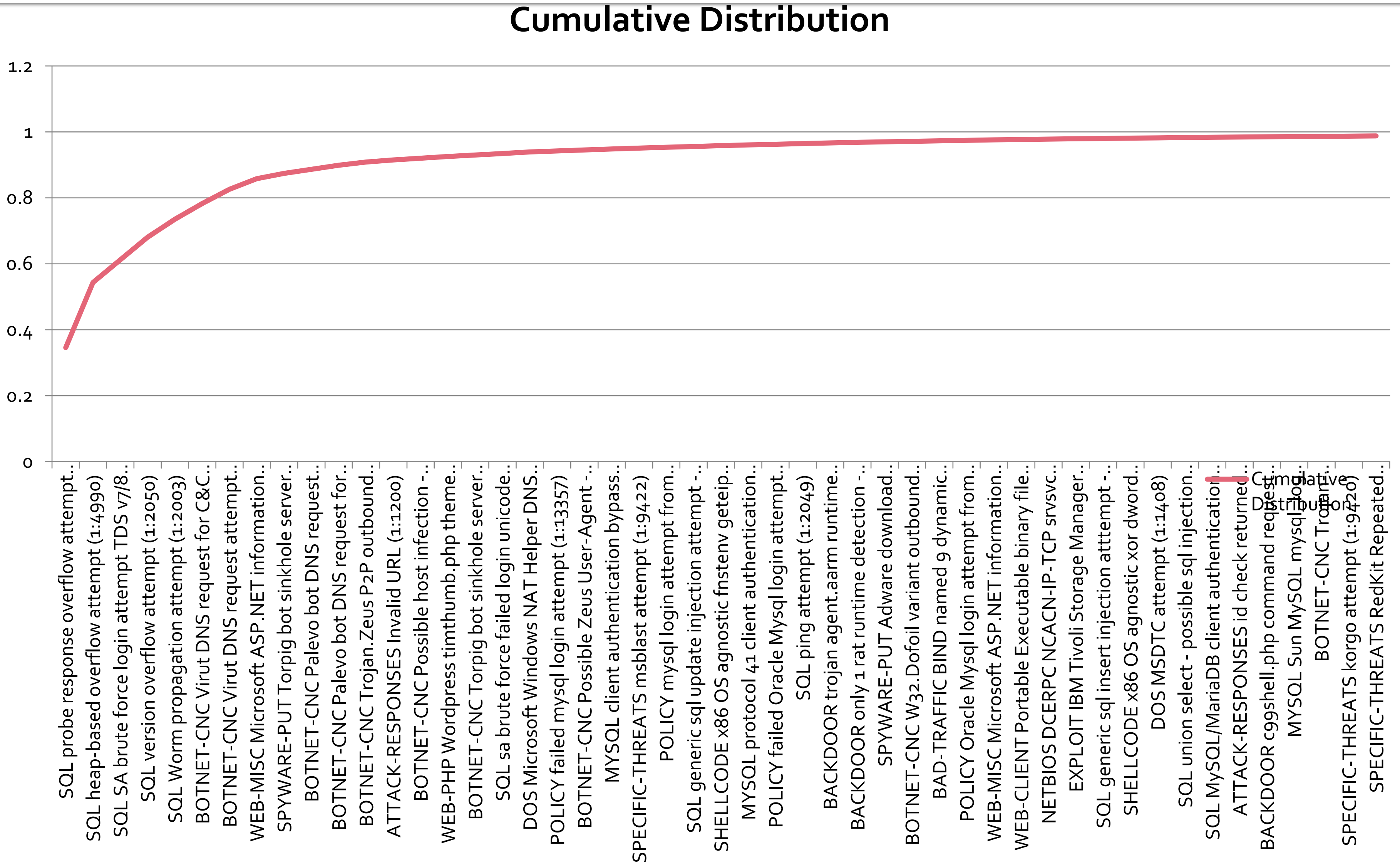


Distribution of Targeted Port

Destination Port	Counter	Cumulative Distribution
1434 (ms-sql-m)/udp	4129135	0.46774675
53 (domain)/udp	1900826	0.683071554
1433 (ms-sql-s)/tcp	891009	0.784004694
445 (microsoft-ds)/tcp	304656	0.818516003
3306/tcp	98583	0.829683446
80 (http)/tcp	78690	0.838597417
80 (http)/udp	65922	0.846065035
34354/tcp	62865	0.853186357
32115/udp	46580	0.85846292

- Only a few ports become target of most attacks
- Port 1434 (MS SQL-M), 53 (DNS), 1433 (MS SQL-S), 445 (microsoft-ds)

Cumulative Distribution Function (CDF) of Attack Types



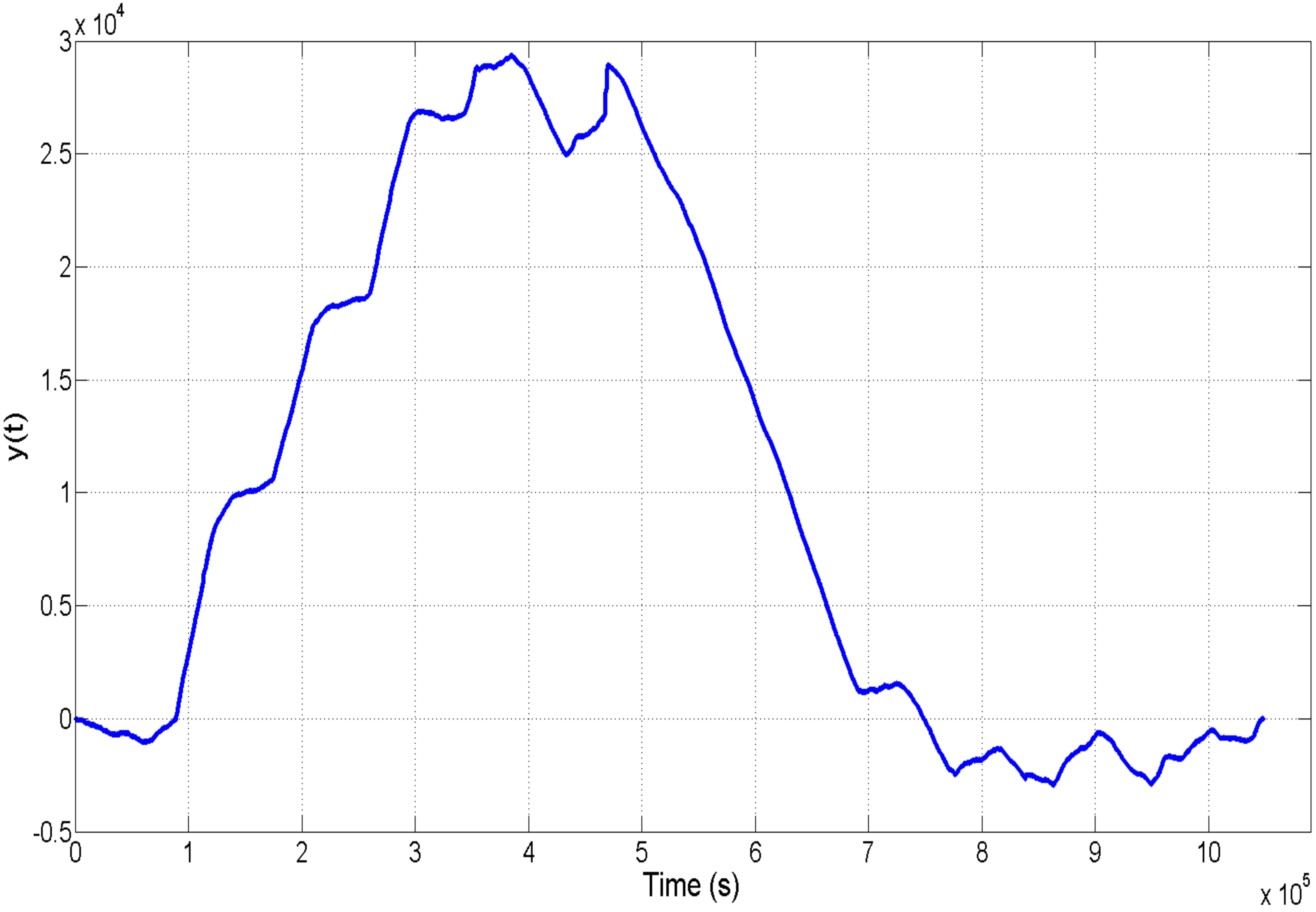
Distribution of Attack Types

Event Message	Counter	Cumulative Distribution
SQL probe response overflow attempt (1:2329)	4436014	0.34605762
SQL heap-based overflow attempt (1:4990)	2526867	0.543180888
SQL SA brute force login attempt TDS v7/8 (1:3543)	884743	0.612200521
SQL version overflow attempt (1:2050)	878459	0.680729933
SQL Worm propagation attempt (1:2003)	696421	0.735058389
BOTNET-CNC Virut DNS request for C&C attempt (1:16302)	609160	0.782579533
BOTNET-CNC Virut DNS request attempt (1:16304)	554635	0.825847131
WEB-MISC Microsoft ASP.NET information disclosure attempt (3:17429)	413011	0.858066507
SPYWARE-PUT Torpig bot sinkhole server DNS lookup attempt (1:16693)	208301	0.874316263

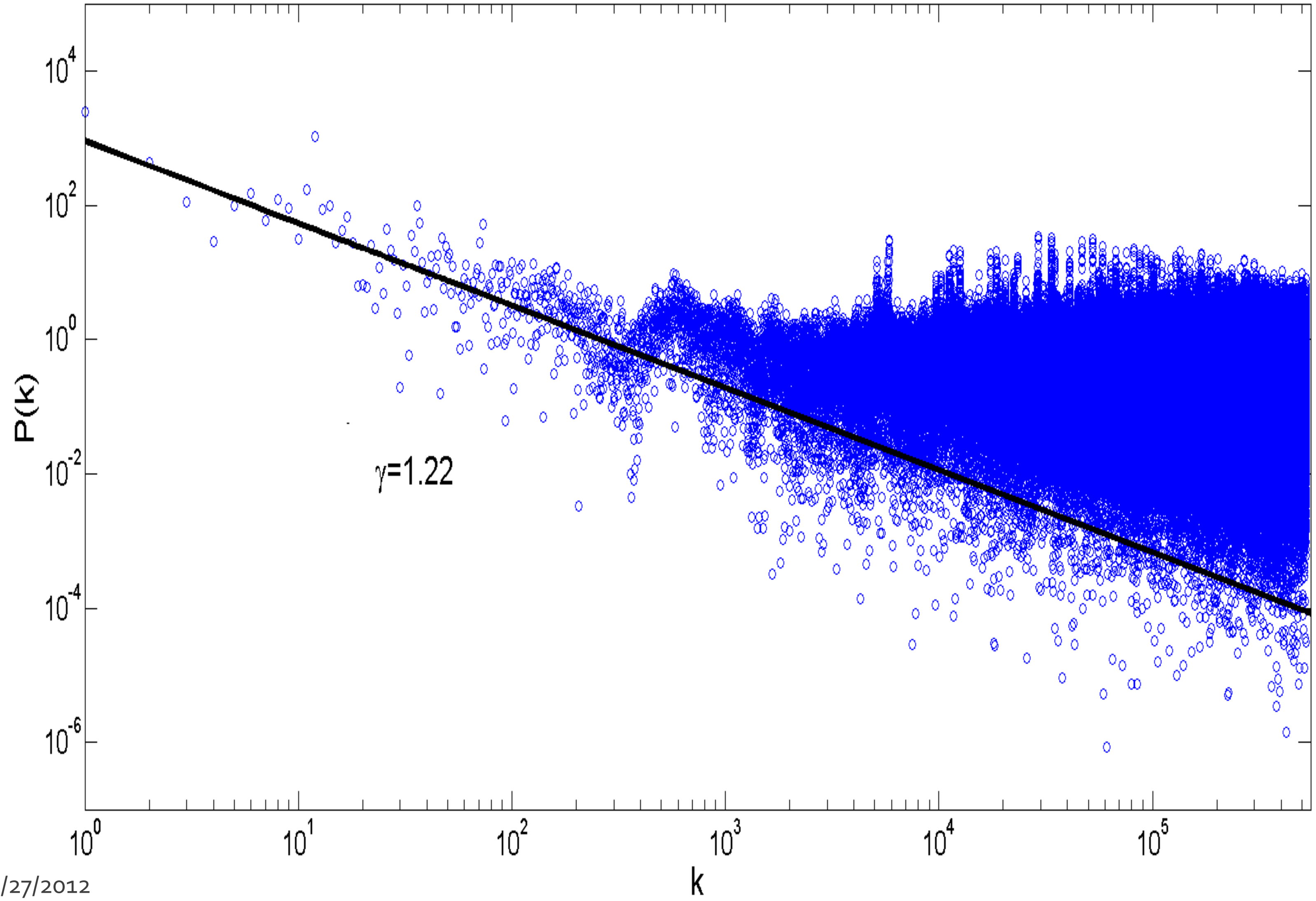
Incident data targeted to port 1434 (udp)

- Exploit for the SQL Server 2000 resolution service buffer overflow
- The SQL Slammer or Sapphire worm used a classic Buffer Overflow in the Microsoft SQL Resolution Service that was provided with SQL Server 2000 and MSDE
- It used only a single UDP packet aimed at port 1434 to spread, causing it to be fast and nearly unstoppable

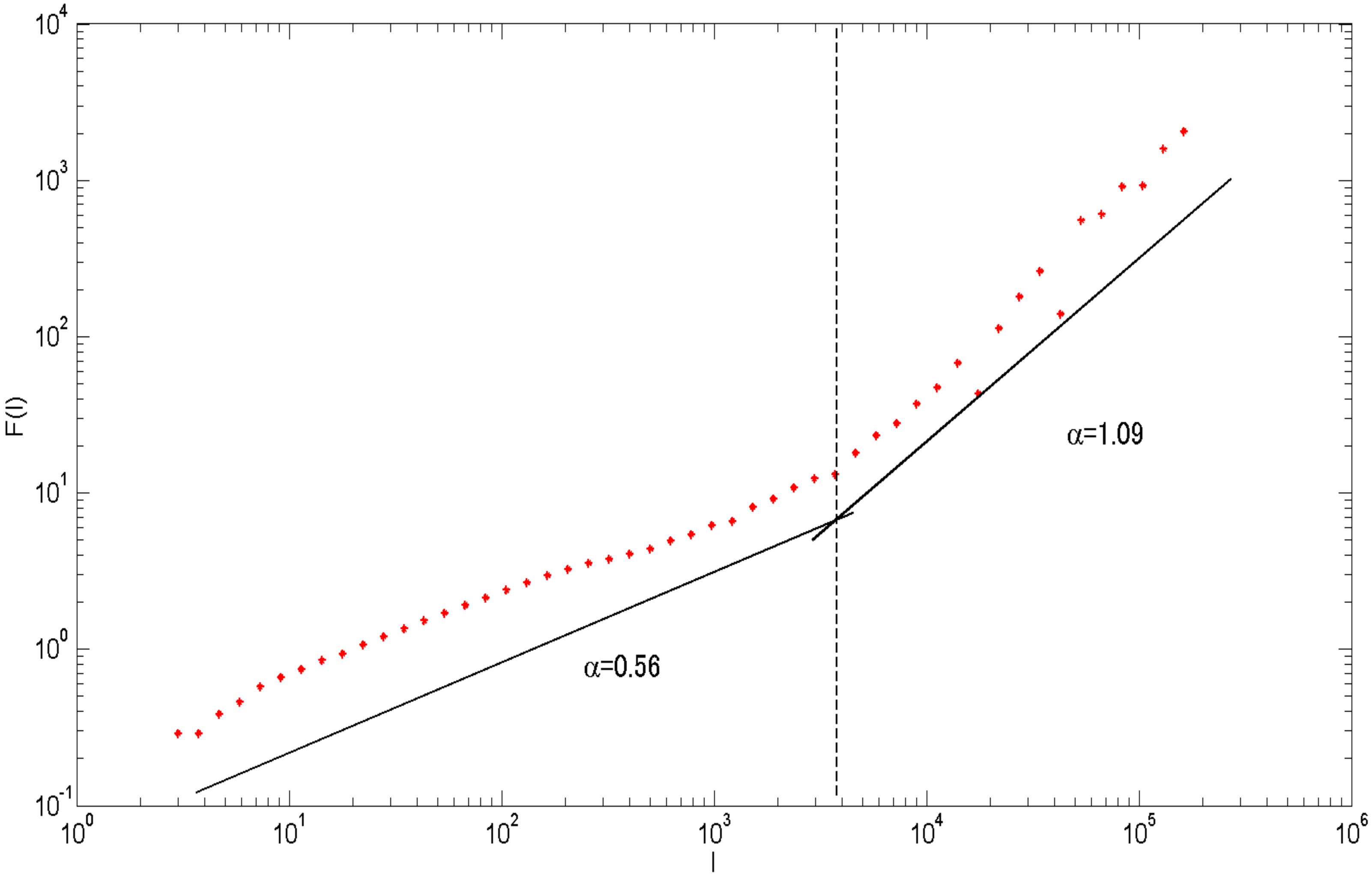
Profile (y(t))



Power Spectrum



DFA



10^4
10^3
10^2
10^1
10^0
10^{-1}
F(l)
10^0
10^1
10^2
10^3
10^4
10^5
10^6
l
α=1.09
α=0.56

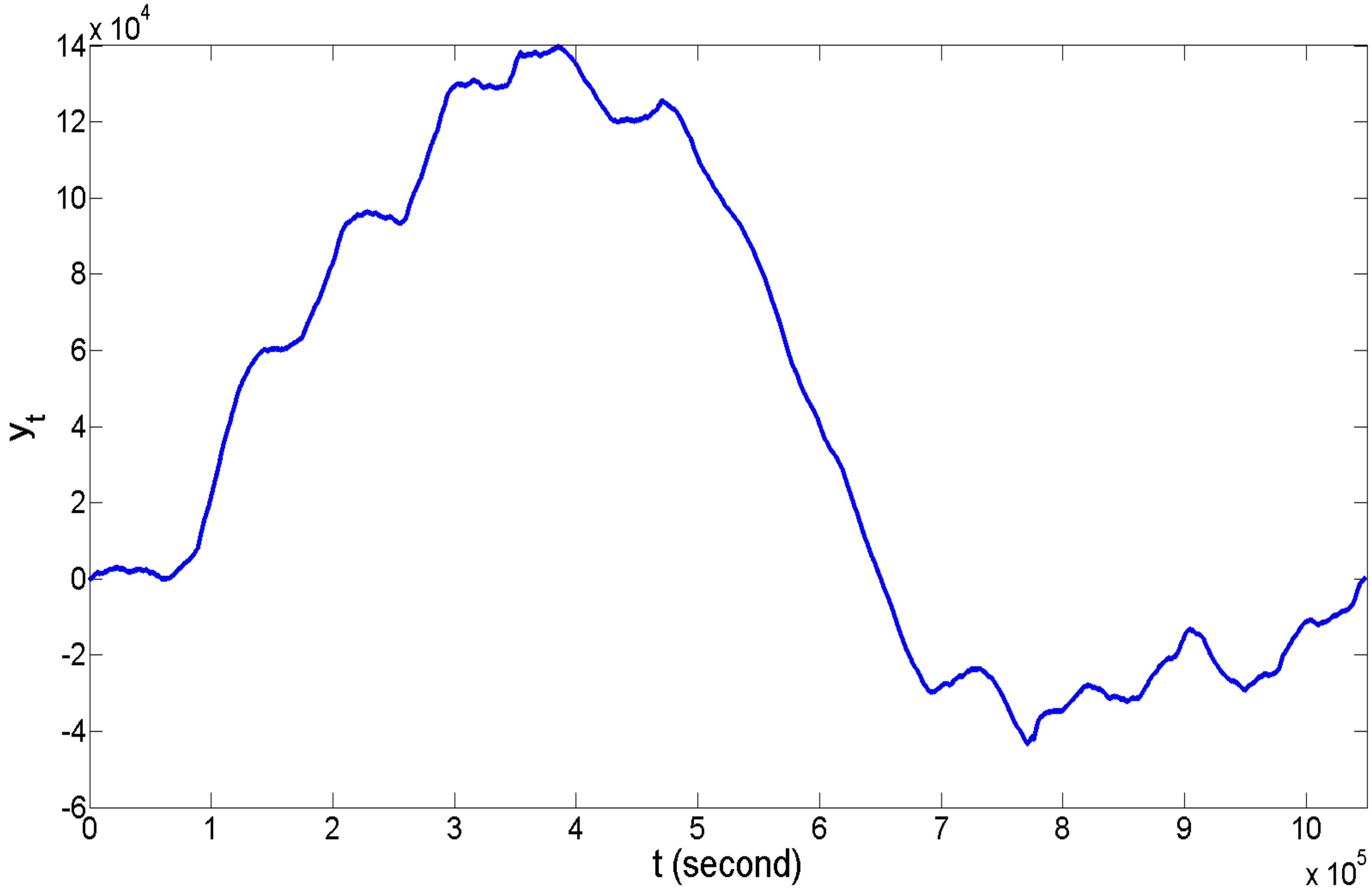
Remarks

- The attacks behavior on port 1434 is random
- The result of DFA seems to be divided into two region of different exponents of Power Law fluctuation
- There is a bending point– further analysis needed, is there any specific real activities (social, user behavior, etc.) related to this different exponents

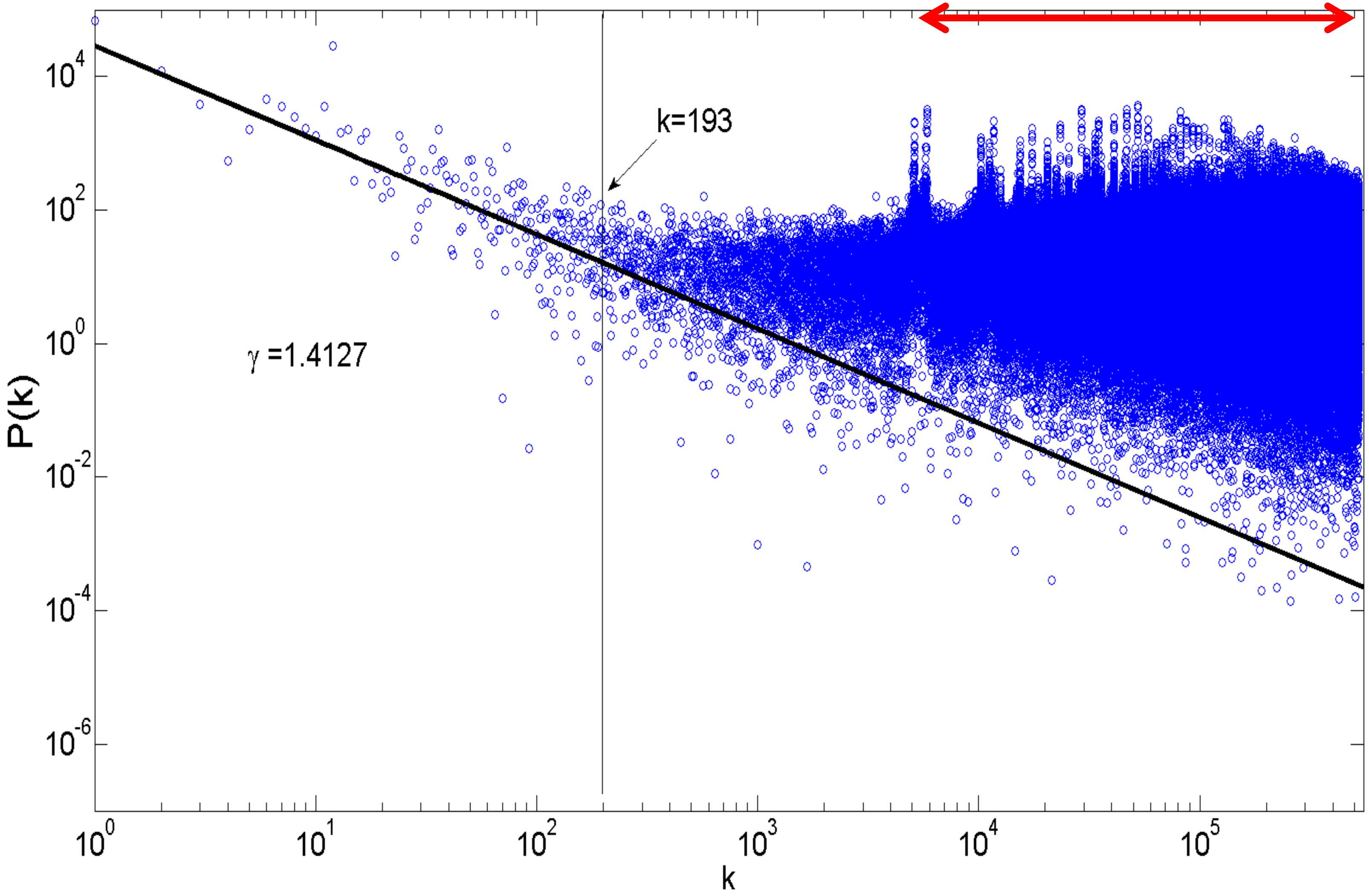
Incident data targeted to port 53 (udp/tcp)

- Blocking adultery sites address (Admin policy)
- Authors of viruses, Trojan horses and other malware may interfere with user DNS for a variety of reasons, including:
  - attempting to block access to remediation resources (such as system patches, AV updates, malware cleanup tools)
  - attempting to redirect users from legitimate sensitive sites (such as online banks and brokerages) to rogue web sites run by phishers
  - attempting to redirect users from legitimate sites to malware-tainted sites where the user can become (further) infected
  - attempting to redirect users to pay-per-view or pay-per-click websites in an effort to garner advertising revenues
  - attempting to resolve the target for spreading malware

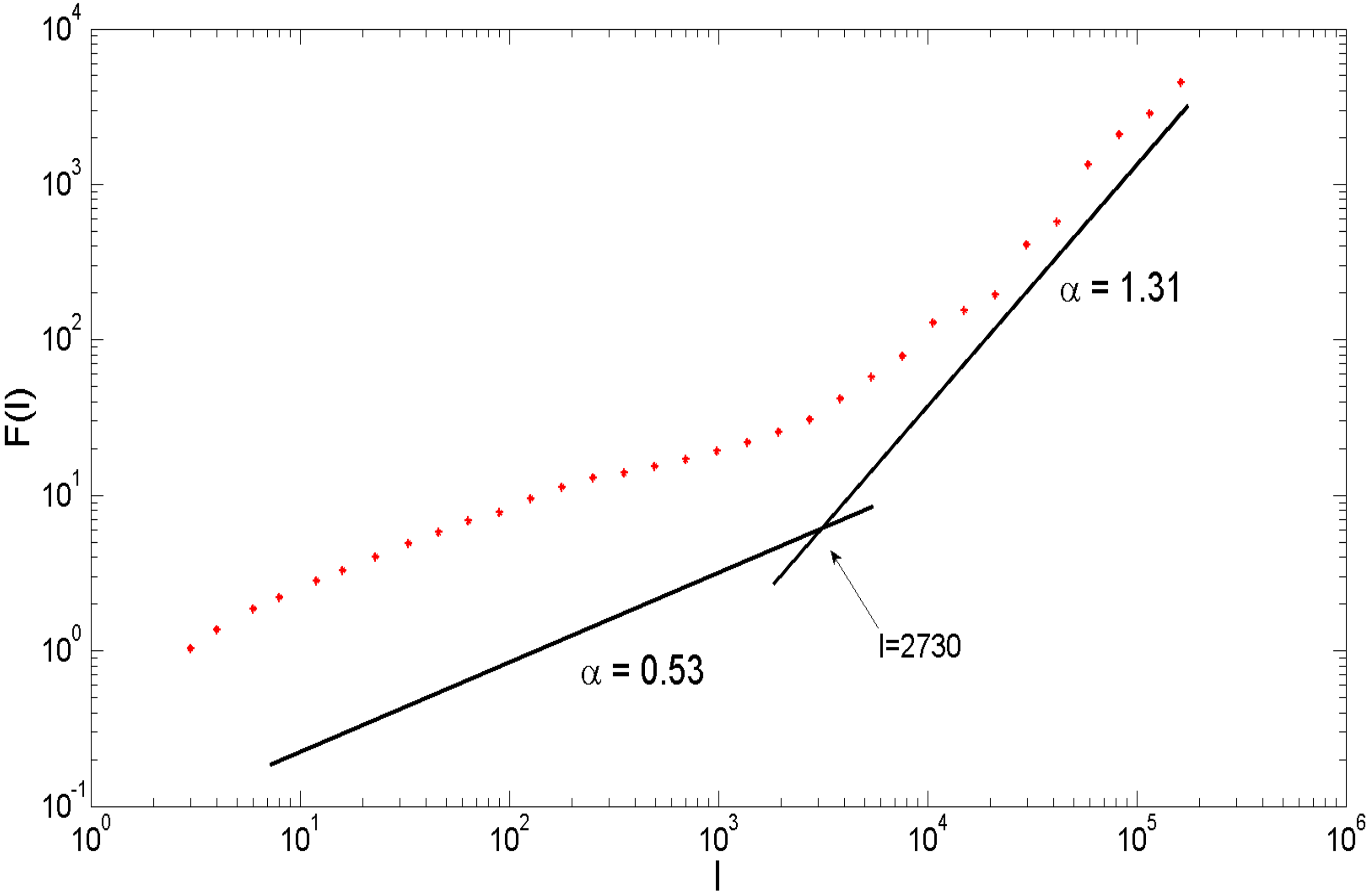
Profile (y(t))



Power Spectrum



DFA



10^4
10^3
10^2
10^1
10^0
10^{-1}
F(l)
α = 1.31
α = 0.53
l=2730
10^0
10^1
10^2
10^3
10^4
10^5
10^6
l

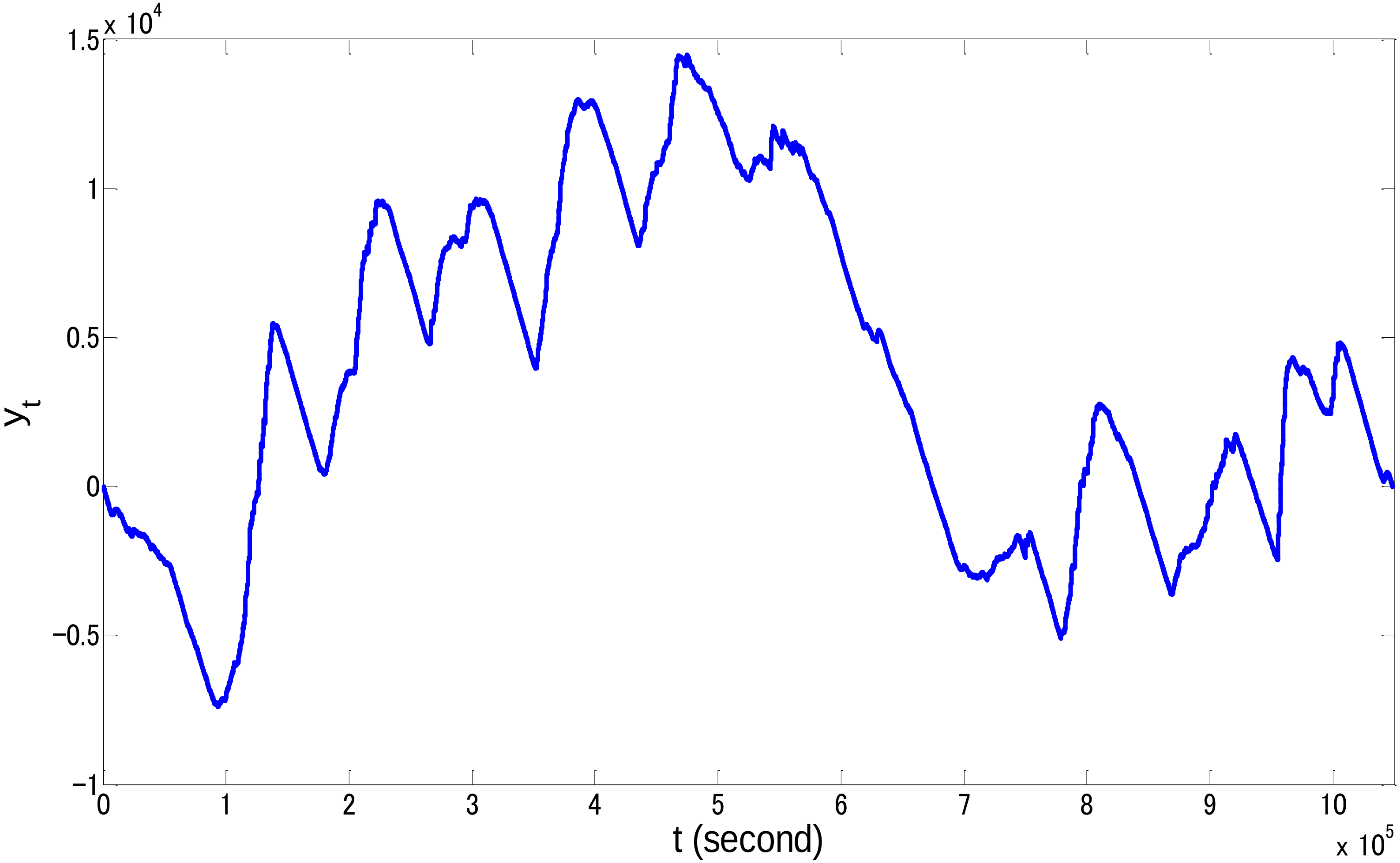
Remarks

- The attacks behavior on port 53 is random
- The result of DFA seems to be divided into two region of different exponents of Power Law fluctuation
- There is a bending point – further analysis needed, is there any specific real occasion (social, user behavior, etc.) related to this different exponents
- Peaks appears several times in the short time scales
  - Suggestion :
    - DNS poisoning
    - Network scans running by hosts infected by malware or hosts part of bot-net

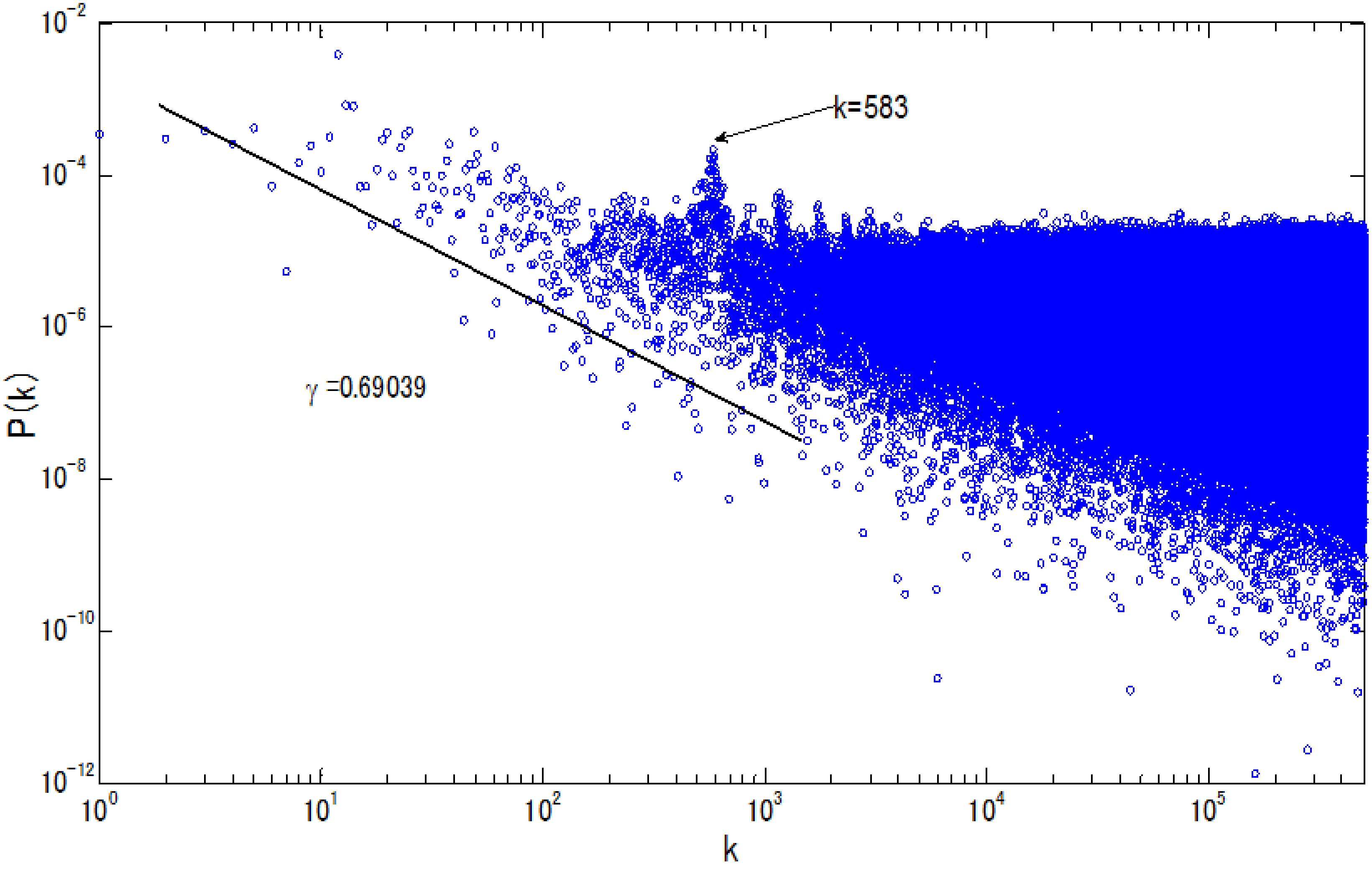
Incident data targeted to port 445

- Microsoft-DS Service is used for resource sharing on Windows 2000, XP, 2003, and other samba based connections
- This is the port that is used to connect file shares for example

Profile

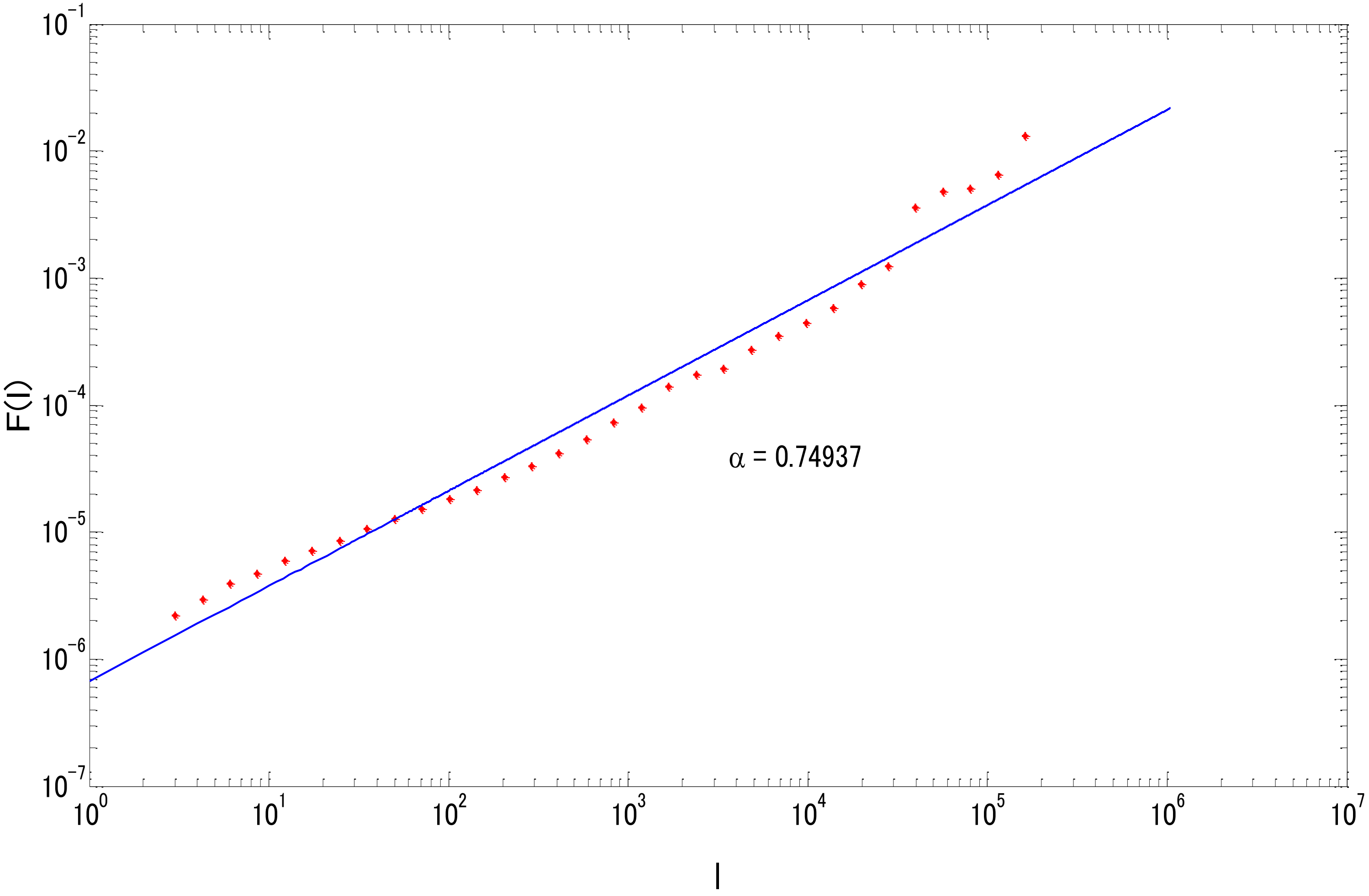


PSA



10^{-2}
10^{-4}
10^{-6}
10^{-8}
10^{-10}
10^{-12}
P(k)
10^{0}
10^{1}
10^{2}
10^{3}
10^{4}
10^{5}
k
k=583
γ =0.69039

DFA



10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
F(l)
α = 0.74937
10^{0}
10^{1}
10^{2}
10^{3}
10^{4}
10^{5}
10^{6}
10^{7}
l

Remarks

- The data shows clear Power Law fluctuations
- The exponents of the fluctuation for attacks targeted port 445 are almost unity
- The attacks on the port 445 seems to have correlation (possible recurrence event)
- This finding agrees with previous research done by Uli Harder, “Observing Internet Worm and Virus Attacks with a Small Network Telescope”

Thank You

- Ravindo Tower 17th Floor
- Kebon Sirih Raya, Kav. 75
- Central Jakarta, 10340
- Phone +62 21 3192 5551
- Fax +62 21 3193 5556
- office@idsirtii.or.id ; www.idsirtii.or.id