Internet Intrusion: Indonesian Characteristics

by
Bisyron Wahyudi
Muhammad Salahuddien
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
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?
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
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
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

Monthly Scan Count Top 1-10

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

![Graph showing Monthly Scan Count Top 1-10]

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

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Counter</th>
<th>Cumulative Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>61.235.46.146</td>
<td>1136787</td>
<td>0.127079841</td>
</tr>
<tr>
<td>124.239.195.131</td>
<td>497699</td>
<td>0.182716922</td>
</tr>
<tr>
<td>218.75.49.242</td>
<td>485758</td>
<td>0.237019134</td>
</tr>
<tr>
<td>211.141.86.248</td>
<td>315837</td>
<td>0.272326114</td>
</tr>
<tr>
<td>202.155.14.117</td>
<td>241850</td>
<td>0.29936219</td>
</tr>
<tr>
<td>119.235.24.210</td>
<td>214618</td>
<td>0.323354038</td>
</tr>
<tr>
<td>60.190.118.153</td>
<td>148839</td>
<td>0.339992544</td>
</tr>
<tr>
<td>61.128.110.96</td>
<td>145968</td>
<td>0.356310104</td>
</tr>
<tr>
<td>117.102.102.34</td>
<td>124868</td>
<td>0.370268924</td>
</tr>
</tbody>
</table>
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
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)

\[ P(K) \] vs. \( k \)

\[ \gamma = 1.38 \]
All \((y(t))\)
All (DFA)

\[ F(l) \]

\[ \alpha = 0.51 \]

\[ \alpha = 1.20 \]
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

Monthly Scan Count Top 1-10

- Start Date: 2012-01-01 00:00:00
- End Date: 2012-01-31 23:59:59
Targeted Ports Distribution

Monthly Scan Count Top 1-10

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

Monthly Scan Count Top 1-10

Scan Count Per Day

Start Date: 2012-03-01 00:00:00
End Date: 2012-03-31 23:59:59
Cumulative Distribution Function (CDF) of Targeted Ports

Cumulative Distribution

Cumulative Distribution
## Distribution of Targeted Port

<table>
<thead>
<tr>
<th>Destination Port</th>
<th>Counter</th>
<th>Cumulative Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1434 (ms-sql-m)/udp</td>
<td>4129135</td>
<td>0.46774675</td>
</tr>
<tr>
<td>53 (domain)/udp</td>
<td>1900826</td>
<td>0.683071554</td>
</tr>
<tr>
<td>1433 (ms-sql-s)/tcp</td>
<td>891009</td>
<td>0.784004694</td>
</tr>
<tr>
<td>445 (microsoft_ds)/tcp</td>
<td>304656</td>
<td>0.818516003</td>
</tr>
<tr>
<td>3306/tcp</td>
<td>98583</td>
<td>0.829683446</td>
</tr>
<tr>
<td>80 (http)/tcp</td>
<td>78690</td>
<td>0.838597417</td>
</tr>
<tr>
<td>80 (http)/udp</td>
<td>65922</td>
<td>0.846065035</td>
</tr>
<tr>
<td>34354/tcp</td>
<td>62865</td>
<td>0.853186357</td>
</tr>
<tr>
<td>32115/udp</td>
<td>46580</td>
<td>0.85846292</td>
</tr>
</tbody>
</table>

- 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

Cumulative Distribution

Cumulative Distribution
## Distribution of Attack Types

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

![Graph showing the profile of y(t) over time]
Power Spectrum

\[ \gamma = 1.22 \]
DFA

\[ F(l) \]

\[ \alpha = 0.56 \]

\[ \alpha = 1.09 \]
Remarks

- The attacks behavior on port 1434 is random.
- The result of DFA seems to be divided into two regions 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 ($y(t)$)
DFA

\[ F(l) \]

\[ \alpha = 0.53 \]

\[ \alpha = 1.31 \]

\[ l = 2730 \]
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
DFA

\[ \alpha = 0.74937 \]
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 seem 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