Internet Background Radiation: Monitoring the Packet Plague

WAND group, Friday 18 Jun 10

Nevil Brownlee
### Unsolicited Packets: Source Taxonomy

<table>
<thead>
<tr>
<th>Description</th>
<th>Source Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP only, many addrs, same port</td>
<td><strong>TCP port probe</strong></td>
</tr>
<tr>
<td>TCP only, single packet per destination</td>
<td>TCP only, &gt;1 pkt/addr</td>
</tr>
<tr>
<td>TCP only, single packet per destination</td>
<td>TCP only, 1 pkt/addr</td>
</tr>
<tr>
<td>UDP only, many addrs, same port</td>
<td><strong>UDP port probe</strong></td>
</tr>
<tr>
<td>UDP only, more than one packet per destination</td>
<td>UDP only, &gt;1 pkt/addr</td>
</tr>
<tr>
<td>UDP only, single packet per destination</td>
<td>UDP only, 1 pkt/addr</td>
</tr>
<tr>
<td>Mixed TCP and UDP packets</td>
<td><strong>Both TCP and UDP</strong></td>
</tr>
<tr>
<td>Only other protocols</td>
<td>Other protocols</td>
</tr>
<tr>
<td>TCP only, ACK flag set</td>
<td>Backscatter</td>
</tr>
<tr>
<td>All packets Conficker C p2p</td>
<td><strong>Only Conficker p2p</strong></td>
</tr>
<tr>
<td>TCP+UDP only, some Conficker C packets</td>
<td>Mixed Conficker p2p</td>
</tr>
<tr>
<td>Source sent less than 20 (10 at trace end) packets</td>
<td><strong>Unclassified</strong></td>
</tr>
</tbody>
</table>
Aggregated Source Groups, kS/h

(a) Stacked-bar Time Series: Sources by Group, Jan - Apr 2010 (UTC)

- Conficker P2P
- Other
- TCP and UDP
- TCP
- Unclassified
Packet Counts, % by Source Group

(d) Stacked-bar Time Series: Packet % by Source Group, Jan - Apr 2010 (UTC)
Aggregated Sources, % by Group

(b) Stacked-bar Time Series: Source % by Group, Jan - Apr 2010 (UTC)

16 Jan 30 Jan 13 Feb 27 Feb 13 Mar 27 Mar 10 Apr

Conficker P2P
Other
TCP and UDP
TCP
Unclassified
Lifetime of *TCP Probe* sources

![Heatmap of TCP Probe source lifetimes](image-url)
Packet Count of *TCP Probe* sources

The diagram shows the packet count of TCP probe sources over a period of time. The x-axis represents days of the week from Saturday to Saturday, while the y-axis represents the number of packets in thousands (kS). The color scale indicates the number of packets, with darker shades representing higher counts.
Lifetime of *Only Conficker P2P* sources
Packet Count of *Only Conficker P2P* sources

![Packet Count Graph]

IBR-IMC, WAND, 18 Jun 10 – p. 10/14
What happened after April 2010 ...

Source Types: kSource/hour, stacked bar plot, Apr - Jun 2010 (UTC)

Packet Counts, Mp, stacked bar plot, Apr - Jun 2010 (UTC)

Source Types, hourly percentage, stacked bar plot, Apr - Jun 2010 (UTC)

Packet Counts, hourly percentage, stacked bar plot, Apr - Jun 2010 (UTC)
Monitoring IBR at U Auckland

- I’ve extended owtmon to watch one-way traffic
  - Ignore streams that have packets both in and out of UA
  - It can take 40 or more packets in before we see one out!
  - Hard work to get data structure locking between threads correct!

- Has now run for nine days to Thursday 17 June

- Not enough data collected yet to really comment on
  - Making plots for this talk revealed more bugs
  - i.e. packet counters not being reset each hour

- Two plots of Auckland data follow . . .
  - Size of groups at Auckland clearly different to that at UCSD
Source Types: kSource/hour, stacked bar plot, 8 - 17 Jun 2010 (UTC)
U Auckland Packet Counts, Mp/h

Packet Counts, Mp, stacked bar plot, 8 - 17 Jun 2010 (UTC)

Conficker mixed
Conficker P2P
Backscatter
No TCP or UDP
TCP and UDP
UDP, 1p/a
UDP, > 1p/a
UDP port probe
TCP, 1p/a
TCP, > 1p/a
TCP port probe
Unclassified