The State of the Net in India

From 2012 to 2014…
What have we learned in 2014?
Executive Summary

- The top malware infection in India is still Botnet related
  - Hackers own your PC’s and use them for spamming, DDOS or other malicious activity to make $$
- Banking related malware has been consistently topping the chart in India
  - Ramnit malware steals bank user names and passwords
  - Spreads through – USB removable drives
- PC’s in India are moving away from Windows XP
  - We have also observed the decline in Downadup/Conficker infection over the past 3 years in India
Timeline 2014: total count of detections in India
Top 5 Family Detections (% of total detections in India) 2014

- Sality: 14%
- All other detections: 70%
- Trojan.Script: 4%
- Trojan.LNK.Gen: 4%
- Ramnit: 5%
- Virtob...
Malware Trends in India 2012-2014
Top 5 malware types over 2012-2014

- **2012**
  - Downadup/conficker: 16%
  - Ramnit: 8%
  - Autorun worms: 4%
  - Trojan.Script: 3%
  - Sality: 3%

- **2013**
  - Ramnit: 18%
  - Sality: 14%
  - Virtob: 5%
  - Downadup/conficker: 4%
  - Exploit:w32/wormlink: 2%

- **2014**
  - Sality: 14%
  - Ramnit: 5%
  - Trojan.LNK: 4%
  - Trojan.Script: 4%
  - Virtob: 3%
Cities breakdown in India
Top 5 Cities in India, by % of total detections (2014)

- Delhi: 20%
- Hyderabad: 9%
- Chennai: 7%
- Chandigarh: 9%
- All other cities (536): 55%
Top 5 Families in Top 5 Cities, by % of total detections per city

- **New Delhi**
  - Sality
  - Trojan.Script
  - Trojan.LNK.Gen
  - Ramnit
  - Win32.Virtob.Gen

- **Hyderabad**
  - Sality
  - Ramnit
  - Trojan.Script
  - Win32.Virtob.Gen
  - Trojan.LNK.Gen

- **Delhi**
  - Sality
  - Trojan.Script
  - Ramnit
  - Trojan.LNK.Gen
  - JS:Exploit.BlackHole.QY

- **Chennai**
  - Sality
  - Trojan.LNK.Gen
  - Trojan.Script
  - Ramnit
  - Trojan-Spy:W32/Zbot.AVTF

- **Chandigarh**
  - Sality
  - Ramnit
  - Trojan.LNK.Gen
  - Win32.Virtob.Gen
  - Stealth_file
Highlights

- Cities of interest topping the chart
  - Delhi (20%)
  - Hyderabad (9%)
  - Chandigarh (9%)
  - Chennai (7%)
The Mobile Threat Landscape
Top 10 Android Detection Families in India 2014

- Top 10 Trojan: Android/Smssend, 17%
- Top 10 Riskware: Android/Smsreg, 11%
- Top 10 Riskware: Android/Minimob, 8%
- Top 10 Spyware: Android/Counterclank, 8%
- Top 10 Trojan: Android/Fakeinst, 6%
- Top 10 Trojan: Android/Downloader, 6%
- Top 10 Riskware: Android/Seicap, 5%
- Top 10 Trojan: Android/SmsSpy, 4%
- Top 10 Trojan: Android/Qtplugin, 3%

Total, All other families, 4759, 26%
Main motivation for hacking your mobile devices in India:

Android/SMSSend & Android/FakeInst

- Premium rate SMS is still the No.1 reason behind a high number of SMS-related malware in the Android platform in India
- In line with what the CERT-In (Computer Emergency Response Team of India) found in December of 2014

"Once infected, it sends text messages (typically with a link to itself or a different threat) to a specific number, typically to numbers on the contact list and is also capable to send SMS to premium rate numbers," the Computer Emergency Response Team of India (CERT-In) said in its latest advisory to Android phone users in the country.
Android/SMSreg

The application also collects the following information:

- API key
- Application ID
- Carrier
- Device manufacturer
- Device model
- GPS location
- International Mobile Equipment Identity (IMEI) number
- Network operator
- Package name
- SDK version
Cities in India breakdown in mobile infection
Top 10 Cities in India 2014, by total count of detections

- **Top 10 Cities Mumbai**, 22%
- **Top 10 Cities Chandra**, 10%
- **Top 10 Cities Delhi**, 9%
- **Top 10 Cities Chennai**, 8%
- **Top 10 Cities Gurgaon**, 8%
- **Top 10 Cities New Delhi**, 7%
- **Top 10 Cities Hyderabad**, 7%
- **Top 10 Cities Bangalore**, 7%
- **Top 10 Cities Pune**, 4%
- **Top 10 Cities Kolkata**, 2%

**Total, All other cities (308)**, 16%

Other, 84%
### Top 5 Families in Top 5 Cities, by % of total detections per city

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mumbai</td>
<td>32%</td>
<td>25%</td>
<td>20%</td>
<td>15%</td>
<td>10%</td>
</tr>
<tr>
<td>Delhi</td>
<td>35%</td>
<td>26%</td>
<td>18%</td>
<td>13%</td>
<td>8%</td>
</tr>
<tr>
<td>Chandra</td>
<td>33%</td>
<td>23%</td>
<td>17%</td>
<td>12%</td>
<td>8%</td>
</tr>
<tr>
<td>Chennai</td>
<td>24%</td>
<td>19%</td>
<td>14%</td>
<td>13%</td>
<td>10%</td>
</tr>
<tr>
<td>Gurgaon</td>
<td>27%</td>
<td>21%</td>
<td>17%</td>
<td>14%</td>
<td>11%</td>
</tr>
</tbody>
</table>
Public Wi-Fi Demo
SWITCH ON FREEDOM