Stormy Weather
A quantitative assessment of the Storm web threat in 2007

Raimund Genes, Anthony Arrott, and David Sancho
Trend Micro

VB2008 - Ottawa
October 2008
Storm activity by country of IP source
How does Storm infect computers?

- Users open executable email attachments (e.g. ‘Full Story.exe’)

or

- Users visit infected websites (e.g. ‘click_for_full_story’)

- Either way, user click results in becoming a remotely-controlled botnet zombie
What does Storm do to make money for its perpetrators?

- ‘Botnets for rent’ in underground economy
- Rented botnets used:
  - as spam engines
  - in denial of service attacks
- Sell mined zombie data (e.g. address book contents)
How does Storm protect itself from detection & removal?

- Infects host zombies with rootkits
- Provides periodic updates of malware code
- Botnets configured
  - decentralized control
  - rotating activation
  - enhanced encryption
  - frequent code replacement
Stormy Weather
A quantitative assessment of the Storm web threat in 2007

Storm outbreaks in 2007

- 17 Jan 07 - “European Storm” Spam
- 12 Apr 07 - “Worm Alert” Spam
- 27 Jun 07 - “E-card” (applet.exe)
- 4 July 07 - “231st B-day”
- 2 Sep 07 - “Labor Day” (labor.exe)
- 5 Sep 07 - “Tor Proxy”
- 10 Sep 07 - “NFL Tracker”
- 17 Sep 07 - “Arcade Games”

Adopted from: Porras, Saidi & Yagneswaran
Stormy Weather
A quantitative assessment of the Storm web threat in 2007

[Graph of daily global spam volume (millions) showing peaks in January, March, April, June, July, August, and September.]

- Original attack: Total volume: 40 million messages, Format: attachment
- Two attacks: Total volume: 1 billion messages, Format: e-mail and URL

Source: Postini
Stormy Weather
A quantitative assessment of the Storm web threat in 2007

Detects of Storm-related malware files

% computers infected

source: Trend Micro
Stormy Weather
A quantitative assessment of the Storm web threat in 2007
# Stormy Weather

A quantitative assessment of the Storm web threat in 2007

| Delay after 17-Jan-07 | January 2007 Storm Attacks  
("European Storm") |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>malware detection</td>
<td></td>
</tr>
<tr>
<td>trough</td>
<td>2 weeks</td>
</tr>
<tr>
<td>peak</td>
<td>3 weeks</td>
</tr>
<tr>
<td>peak spam</td>
<td>1 week</td>
</tr>
</tbody>
</table>

| Delay after 12-Apr-07  | April 2007 Storm Attacks    
("Worm Alert")       |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>malware detection</td>
<td></td>
</tr>
<tr>
<td>trough</td>
<td>1 week</td>
</tr>
<tr>
<td>peak</td>
<td>3 weeks</td>
</tr>
<tr>
<td>peak spam</td>
<td>3 weeks</td>
</tr>
</tbody>
</table>

| Delay after 27-Jun-07  | June/July 2007 Storm Attacks  
("E-card", "231st B-day") |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>malware detection</td>
<td></td>
</tr>
<tr>
<td>trough</td>
<td>1 week</td>
</tr>
<tr>
<td>peak</td>
<td>8 weeks</td>
</tr>
<tr>
<td>peak spam</td>
<td>7 weeks</td>
</tr>
</tbody>
</table>

| Delay after 2-Sep-07   | September 2007 Storm Attacks  
("Labor Day", "I0r Proxy",  
"NFL Tracker", "Arcade Games") |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>malware detection</td>
<td></td>
</tr>
<tr>
<td>trough</td>
<td>2 weeks</td>
</tr>
<tr>
<td>peak</td>
<td>12 weeks</td>
</tr>
<tr>
<td>peak spam</td>
<td>[not available]</td>
</tr>
</tbody>
</table>
Stormy Weather
A quantitative assessment of the Storm web threat in 2007

Storm activity - Apr 3 - Jul 1

Storm activity - Jul 2 - Sep 29
Thank you