
TERENA – May 23, 2007
Colleen Shannon
cshannon@caida.org
Outline

• UCSD Network Telescope
• Denial-of-Service Attacks
• Viruses and Worms
• Botnets
Network Telescope

• Chunk of (globally) routed IP address space
  – 16 million IP addresses
• Little or no legitimate traffic (or easily filtered)
• Unexpected traffic arriving at the network telescope can imply remote network/security events
• Generally good for seeing explosions, not small events
• Depends on random component in spread
Network Telescope: Denial-of-Service Attacks

- Attacker floods the victim with requests using random spoofed source IP addresses
- Victim believes requests are legitimate and responds to each spoofed address
- We observe 1/256th of all victim responses to spoofed addresses
Denial-of-Service Attacks
DoS Attacks over time
Network Telescope Observation Station

- http://www.caida.org/data/realtime/telescope/

- Prevalence and trends in spoofed-source denial-of-service attacks

- (live demo)
What is a Network Worm?

• Self-propagating self-replicating network program
  – Exploits some vulnerability to infect remote machines
    • No human intervention necessary
  – Infected machines continue propagating infection
Network Telescope: Worm Attacks

- Infected host scans for other vulnerable hosts by randomly generating IP addresses
- We monitor 1/256\textsuperscript{th} of all IPv4 addresses
- We see 1/256\textsuperscript{th} of all worm traffic of worms with no bias and no bugs
Witty Worm Background
March 19, 2004

• ISS Vulnerability
  – A buffer overflow in a PAM (Protocol Analysis Module) in a Internet Security Systems firewall products
    • Version 3.6.16 of iss-pam1.dll
  – Analyzes ICQ traffic (inbound port 4000)
  – Discovered by eEye on March 8, 2004
  – Jointly announced March 18, 2004 when “patch” available
    • Upgrade to the next version at customer cost…

• By far the closest to a zero-day exploit
  – Instead of 2-4 weeks after bug release, Witty appeared after 36 hours
Witty Worm Structure
March 19, 2004

- Infects a host running an ISS firewall product
- Sends 20,000 UDP packets as quickly as possible:
  - to random source IP addresses
  - to random destination port
  - with random size between 796 and 1307 bytes
- Damage Victim:
  - select random physical device
  - seek to random point on that device
  - attempt to write over 65k of data with a copy of the beginning of the vulnerable dll
- Repeat until machine is rebooted or machine crashes irreparably
Typical (Code-Red) Host Infection Rate
Early Growth of Witty (5 minutes)
Witty Worm Spread
March 19, 2004

- Sharp rise via initial coordinated activity
- Peaked after approximately 45 minutes
  - Approximately 30 minutes later than the fastest worm we’ve seen so far (SQL Slammer)
  - Still far faster than any human response
  - At peak, Witty generated:
    - 90 GB/sec of network traffic
    - 11 million packets per second
Early Growth of Witty (2 hours)
Early Growth of Witty (3 days)
Witty Worm Victims

• Consistent with past worms:
  – Globally distributed
  – Majority high-bandwidth home/small business users

• Unique victim characteristics
  – 100% taking proactive security measures
  – Infected via software they ran purposefully
## Witty Worm Victims

<table>
<thead>
<tr>
<th>Country</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>26.28</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>7.27</td>
</tr>
<tr>
<td>Canada</td>
<td>3.46</td>
</tr>
<tr>
<td>China</td>
<td>3.36</td>
</tr>
<tr>
<td>France</td>
<td>2.94</td>
</tr>
<tr>
<td>Japan</td>
<td>2.17</td>
</tr>
<tr>
<td>Australia</td>
<td>1.83</td>
</tr>
<tr>
<td>Germany</td>
<td>1.82</td>
</tr>
<tr>
<td>Netherlands</td>
<td>1.36</td>
</tr>
<tr>
<td>Korea</td>
<td>1.21</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TLD</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>com</td>
<td>33</td>
</tr>
<tr>
<td>net</td>
<td>20</td>
</tr>
<tr>
<td>no-DNS</td>
<td>15</td>
</tr>
<tr>
<td>fr</td>
<td>3</td>
</tr>
<tr>
<td>ca</td>
<td>2</td>
</tr>
<tr>
<td>jp</td>
<td>2</td>
</tr>
<tr>
<td>au</td>
<td>2</td>
</tr>
<tr>
<td>edu</td>
<td>1</td>
</tr>
<tr>
<td>nl</td>
<td>1</td>
</tr>
<tr>
<td>ar</td>
<td>1</td>
</tr>
</tbody>
</table>

Cooperative Association for Internet Data Analysis
Geographic Spread of Witty

![Graph showing the geographic spread of Witty](image)

Cooperative Association for Internet Data Analysis
Witty Summary

Before 9:30PM (PST)  After 9:45PM (PST)

- ~12,000 hosts infected in **30 minutes**
- Averaged more than 11 million probes per second world-wide
- Unstoppable
- Irreparably destroyed a significant number of infected computers
Conclusions (1)

Witty incorporates a number of novel and disturbing features:

- Next day exploit for publicized bug
- Wide-scale deployment
- Successful exploit of small population (no more security through obscurity)
- Future worms will continue to emulate botnets – increasing levels of stealth and flexibility
- Infected a security product
Conclusions (2)

• Witty demonstrates conclusively that the patch model of networked device security has failed
  – You can’t encourage people to sign on to the ‘net with one click and then also expect them to be security experts
  – Running commercial firewall software at their own expense is the gold standard for end user behavior
    • Recognition that security is important
    • Recognition that they can’t do it themselves
Conclusions (3)

- End-user behavior cannot solve current software security problems
- End-user behavior cannot effectively mitigate current software security problems
- We must:
  - Actively address prevention of software vulnerabilities
  - Turn our attention to developing large-scale, robust, reliable infrastructure that can mitigate current security problems without end-user intervention
About Blackworm

• Began to spread January 15, 2006
• 95k Visual Basic executable email attachment run by users
• Also spread to attached network shares
• Malicious: on the 3rd day of every month:
  – searches for files with 12 common file extensions (.doc, .xls, .mdb, .mde, .ppt, .pps, .zip, .rar, .pdf, .psd, and .dmp)
  – replaces those files with the text string "DATA Error [47 0F 94 93 F4 K5]"
So who cares?

- Blackworm is not particularly different from many, many other email viruses, except…
- Every infected computer automatically generates an http request for a web page that displayed a hit count graph (self-documenting code?)
- Logs for the website were available before the first date of payload destruction
- Some victims could be notified before they lost data
Log Analysis

• Simple! Just take the logs and look at who connected and you’ll have the infected IP addresses!
• Except that the url was publicized…
• Many folks looked at the page to observe the spread of the virus
• Denial-of-service attacks added a large volume of spurious traffic
Log Filtering

• Why not just count IP addresses that were logged once?
• Web traffic aggregators (NAT, proxy servers) obscure victim IP addresses; multiple probes can represent multiple infections
• DHCP use allows two different computers to have the same IP at the time that they become infected
Log Filtering Process

- Remove referer/browser strings set by common DDoS tools (91.1% of all hits)
- Remove requests for pages different from the one accessed by the virus (0.2%)
- Remove any request with a referer string (virus did not use one in its probes) (0.8%)
- Remove requests from invulnerable Operating Systems: MacOS, Unix, cell phone, and PDA devices (0.03%)
Sources of Error and Uncertainty

• Infected computers that failed to send the probe
• Network firewalls or outages that prevented victims from reaching the web page
• Denial-of-Service attacks preventing infected computers from reaching the web page
• People who viewed the counter only once using a vulnerable browser, but were not infected
Estimating a Victim Count

- Lower bound: for each IP address, the number of unique, vulnerable browser types received from that IP address

- Upper bound: for each IP address, the total number of probes received from that IP address
• Blackworm victim estimate: between 469,507 and 946,835 (3.2%-6.4% of original log entries)
Blackworm by Continent

Cooperative Association for Internet Data Analysis
# Blackworm by Country (>2%)

<table>
<thead>
<tr>
<th>Country</th>
<th>Min. Count</th>
<th>Min %</th>
<th>Max Count</th>
<th>Max %</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>151341</td>
<td>32</td>
<td>273013</td>
<td>29</td>
</tr>
<tr>
<td>Peru</td>
<td>87599</td>
<td>19</td>
<td>150785</td>
<td>16</td>
</tr>
<tr>
<td>Italy</td>
<td>38216</td>
<td>8</td>
<td>58002</td>
<td>6</td>
</tr>
<tr>
<td>Turkey</td>
<td>28264</td>
<td>6</td>
<td>43437</td>
<td>5</td>
</tr>
<tr>
<td>USA</td>
<td>26315</td>
<td>6</td>
<td>58791</td>
<td>6</td>
</tr>
<tr>
<td>Egypt</td>
<td>12201</td>
<td>3</td>
<td>25104</td>
<td>3</td>
</tr>
<tr>
<td>Malaysia</td>
<td>11160</td>
<td>2</td>
<td>19942</td>
<td>2</td>
</tr>
</tbody>
</table>
Concurrent Infections

• 45,401 Blackworm victims (10%) had concurrent spyware and/or botnet infections advertised in their browser string

  - Mozilla/4.0 (compatible; MSIE 5.5; Windows 98; Sgrunt|V109|29|S493689067|dial; FunWebProducts; XBE|29|S04069679521143#398|isdn; snprtz|S04138822910124)
Cuttlefish Animation...
Conclusions

• Log analysis allows insight into email virus spread given sufficient data mining
• Email viruses spread in a slower and steadier pattern than Internet worms, which infect the vast majority of their victims in the first day
• Diurnal patterns are strongly apparent in spread data (people read their email when they are awake)
Conclusions (2)

• Country distribution of victims does not correlate with web infrastructure development
• Spread strongly influenced by geographic location (based on social and linguistic similarity)
• TLD distribution reflects geographic distribution rather than # of vulnerable hosts/TLD
• 10% of victims had concurrent botnet or spyware infection
Botnets

• Significant transition in motivation for widespread, non-specific malicious activity
  – From notoriety -> want to be noticed
  – To money -> want stealth to protect revenue stream

• So how do you make money?
  – Sending spam
  – DoS extortion
  – Active (phishing) and passive identity theft
Current Events

• Malicious software development is a business aimed at scalable, manageable distributed systems
• Coordinated activity makes current antivirus activities increasingly irrelevant
• Demise of signature-based security?
• High system complexity + naïve/uneducated = bad combination
Current Security Research

- Longitudinal study of Blackworm
- Spamsscatter
- Botnet Economics
- Worm Risk Analysis
- Anomaly Detection
CAIDA Security Datasets

• Freely available datasets (no IP addresses):
  – Code-Red Worm
  – Witty Worm
• Academic / Non-profit access datasets:
  – Denial-of-service attack backscatter
  – Witty Worm
  – OC48 peering point traces (many contain attacks; also provide real background traffic for testing detection/mitigation technology)
Internet Measurement Data Catalog

http://imdc.datcat.org