



Working Group #8

Internet Service Provider (ISP) Network Protection Practices

Presented by

John Morris, Co-Chair

Richard Lynch, Co-Chair

Jason Livingood, WG Member

Problems to Address

- Security flaws in hardware and software, plus poor home computer and network administration practices, have resulted in an epidemic of compromised computers.
- Most of the compromised computers can be remotely controlled in “bot networks.”
- Users are then at risk:
 - Personal and financial information, communications can be monitored;
 - Their PCs and Internet access can be exploited;
 - Armies of these compromised PCs are also used to send spam, store and transfer illegal content, and to launch massive DDoS attacks.



Expected Deliverables

- Capture Best Practices that address ISP user botnet compromises and mitigate the potential network impact on ISPs.
- Investigate and assess any related privacy concerns.
- Identify technical references for each issue or best practice, to educate ISPs and others.
- Make recommendations for any related future work.

Participation

- We had a range of participants from leading ISPs, security companies, content providers, U.S. Government agencies, and public interest groups.
- The group met bi-weekly starting in March, and weekly as we wrapped up our work, with two face-to-face meetings.
- The best practices documented are a snap-shot in time; they will necessarily change in the future as threats and technology evolves.



Working Group Participants

Co-Chairs:

John Morris - Center for Democracy &
Technology

Richard Lynch - Verizon

WG Members/Participants:

William Salusky - AOL

Mike Recchia - AT&T

Tim Battles - AT&T

Neil Schwartzman - Coalition Against Unsolicited
Commercial Email (CAUCE)

Jason Livingood - Comcast

Doug Davis - Comptel / HyperCube Telecom

Brian Moir - E-Commerce, Telecommunications
Users Group (e-TUG)

Pete Fonash - Federal Reserve

Richard Hovey - FCC

Vern Mosley - FCC

Eric Davis - Google

Lead Best Practice Editors:

Robert Thornberry - Bell Labs, Alcatel-Lucent

Paul Diamond - Qwest

Jeff Williams - Microsoft

Kevin McGuire - NTCA

Michael Fiumano - Sprint – Nextel

Damon Dowdall - Sprint – Nextel

Vince Weafer - Symantec

Nick Lordi - Telcordia Technologies

Barry Harp - U.S. Department of Health and
Human Services

Delano Marshall - U.S. Department of Health and
Human Services

David Young - Verizon

Marcus Sachs - Verizon



Expert Consultation

- In addition to our direct WG members, we consulted with a range of experts in various areas for detailed briefings on the problems and/or feedback on our best practices.
- This included:
 - Coalition Against Unsolicited Commercial Email (CAUCE)
 - Damballa
 - Messaging Anti-Abuse Working Group
 - National Cyber Security Alliance
 - Neustar
 - The Spamhaus Project



Understanding Bots

- End-user PCs are infected with malware.
- Bots connect to a network (a “botnet”) and can be remotely controlled.
- Once active, bots can download software and instructions, and pose a range of threats.
- Threats faced by the end user, the ISP, and other end users:
 - Key logging and credential theft;
 - Theft of files on PC and LAN;
 - Hosting / distributing illegal content;
 - Sending spam;
 - DDoS attacks.

Bot Trends & Solutions

- Overall, the threat is worsening and the infected number of PCs continue to grow – this is not getting better.
- Catch rates of preventative tools, such as A/V, are low.
- Remediation tools are relatively immature.
- Thus, the level of technical expertise needed to remediate is relatively high.
- The Working Group concluded Best Practices should take this into account and try to guard against and mitigate the threat in four different ways...

Best Practice Areas

The Working Group directed its focus to four critical areas.

- **Prevention** – Preventing infections before they occur.
- **Detection** – ISP detection of infections & attacks.
- **Notification** – Notifying end users of possible infection.
- **Mitigation** – Mitigating end user device botnet infections and network impacts.
- Also: **Privacy Considerations** – Addressing concerns.



Recommendations

- Industry needs to stay one step ahead of the bad guys, who have huge economic and other incentives.
 - If industry does not join this battle, end user trust in Internet computing could be affected over time and network costs could increase.
- Government has a leadership role to play, ensuring government networks are kept safe.
- Best Practices should be reviewed every two years.
 - It is hoped that remediation tools will improve, which may change Mitigation practices, as well as evolve Notification practices.



Recommendations

- Methods for sharing information with end users and among ISPs can be better defined.
 - End user awareness, and behaviors, can be improved.
 - There may be an opportunity for cross-industry coordination.
- Protection of customer information is an important issue that warrants continued attention.
- Implementation of the botnet Best Practices should be evaluated over time to get a better idea how effective these practices are in dealing with the botnet problem.

