Insecurities at the Edge

IAB Plenary

IETF 58

Minneapolis, MN

http://www.drizzle.com/~aboba/IAB/

November 12, 2003

Acknowledgments

- Thanks to Dave Crocker, Vern Paxson, and Mark Handley for providing data and presentation materials.
- Thanks to members of the ASRG for suggestions and discussion.

Disclaimer

- The IAB does not claim authoritative knowledge in this area.
- Our goal is to ask questions and stimulate discussion about the implications for the Internet Architecture.
  - What should the IETF be doing, if anything?
  - What additional questions need to be asked?
- There are many aspects to these problems that are outside the technical realm (e.g. legal, economic…).
  - Let's keep focused on technical issues the IETF can help solve, such as new work.
- Since the session is about questions and time is limited, **please abstain from presenting solutions.**

A Recent Headline

(London Financial Times, 11/11/2003)

http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1066565805264&p=1012571727088

Home US

Print article | Email

Crime gangs extort money with hacking threat

By Chris Nuttall in London

Published: November 11 2003 21:57 | Last Updated: November 11 2003 23:23

Evidence of a new type of international extortion racket emerged on Tuesday with revelations that blackmailers have been exploiting computer hacking techniques to threaten the ability of companies to conduct business online.

Gangs based in Eastern Europe have been found to have been launching waves of attacks on corporate networks, costing the companies millions of dollars in lost business and exposing them to blackmail.

Some Data

- This data is all anecdotal.
- It's here to frame the problem, not to be discussed in great detail.
- Key points
  - Today's Internet provides an ideal environment for the spread of epidemics
    - Large host population
    - Global connectivity
    - Substantial fraction of unprotected hosts
    - Rising infectivity
  - The virus & spam problems are growing at a daunting rate, and to some degree appear interlinked.
  - There is a reservoir of unmanaged systems that serve as a host population

Scan Computer started on 08/07/03 19:36:36

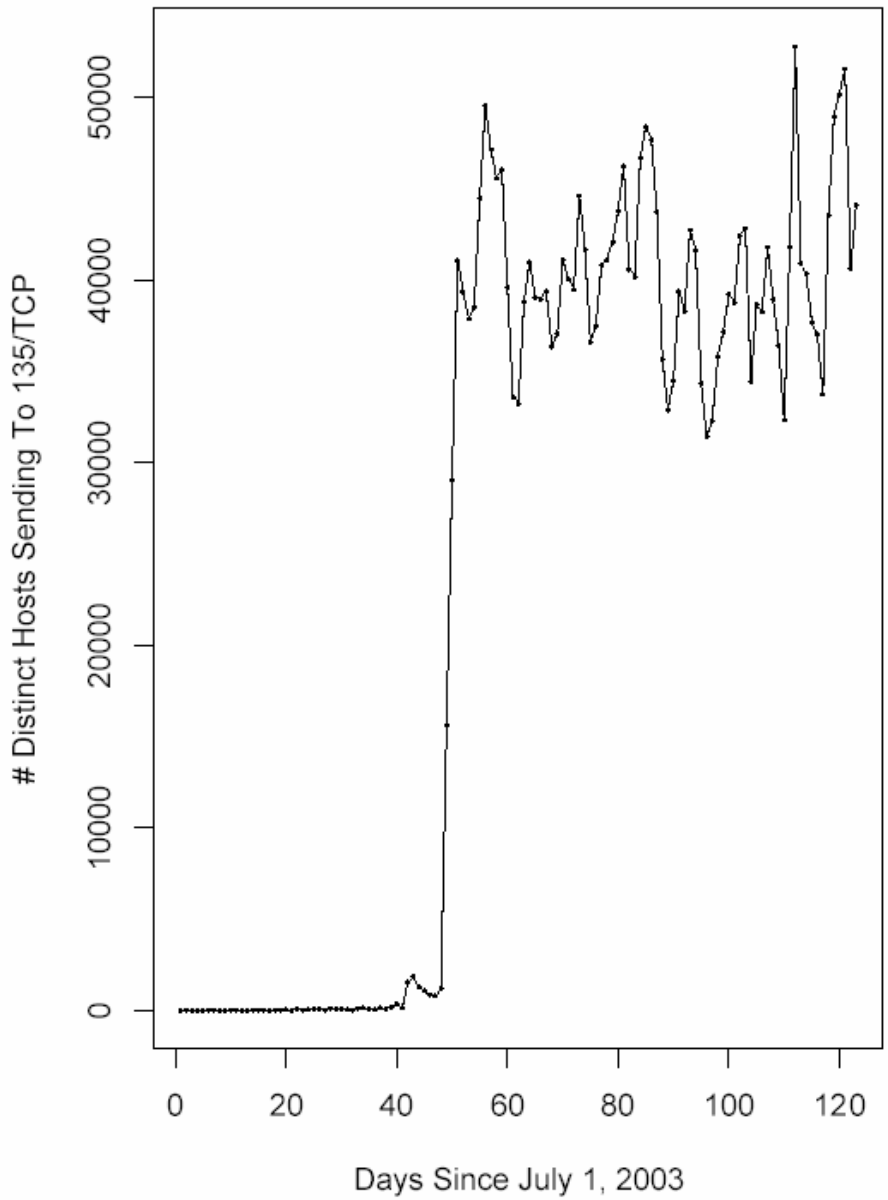
ENPartitionMagic7Demo.exe

C:₩Program Files₩WS_FTP

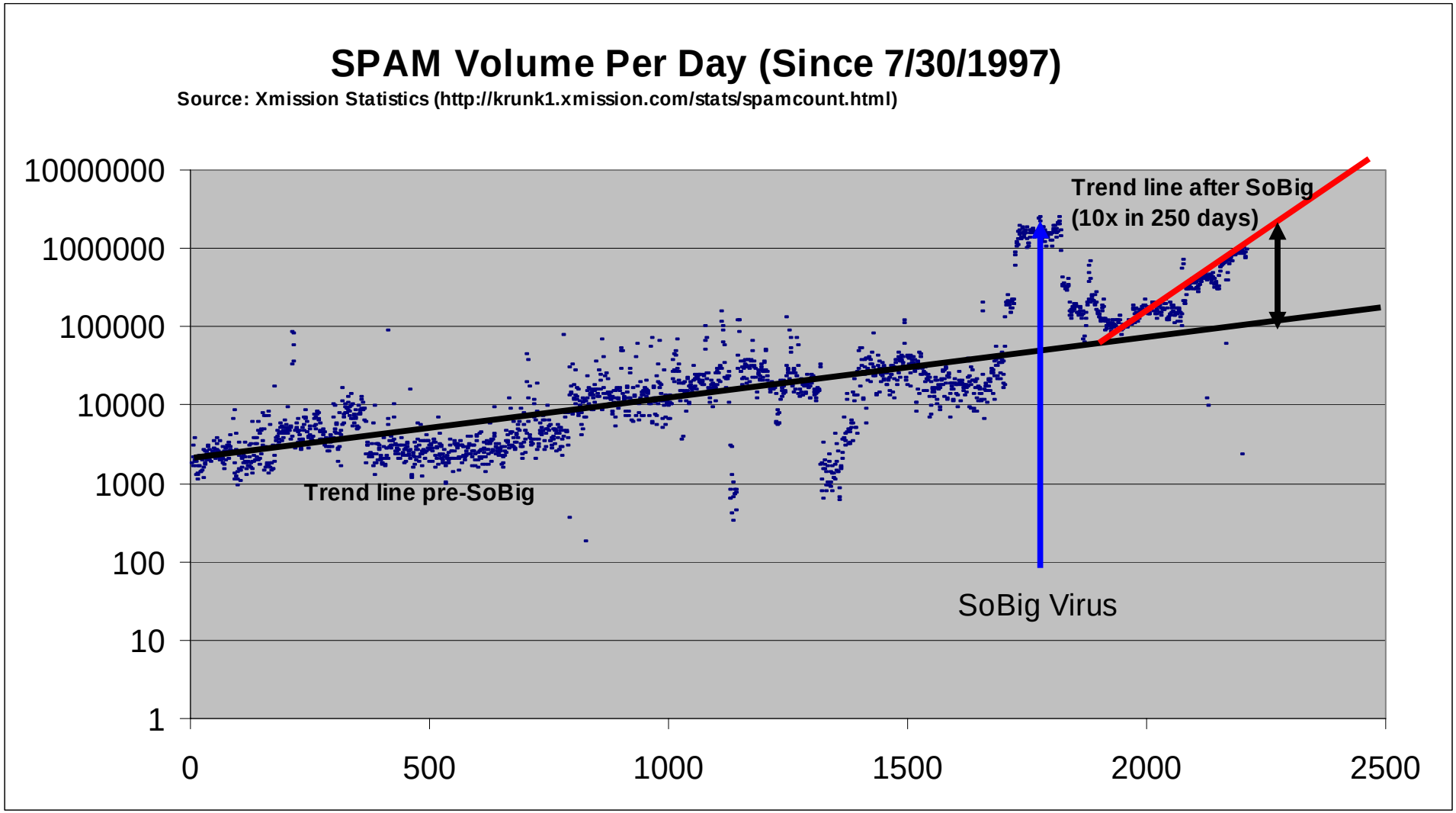
Date	Filename	Virus Name	Virus Type	Action T...	Computer	User
2003-08-07 오후 7:37:12	DAINST.EXE		Compressed...	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:19	XVPLL.HLP	Backdoor.IRC.Flood	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:17	dll32NT.hlp	IRC Trojan	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:40:03	gg.bat	Trojan.IrcBounce	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:40:34	mdm.scr	Trojan.IrcBounce	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:38:31	zoxj.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:39:53	winnet.exe	W32.Spybot.Worm	File	Left alone	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:40:19	ghp32.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:19	cachedll.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:22	Unreal2_bloodpatch.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:22	Battlefield1942_bloodpatch.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:22	Porn.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:21	AVP_Crack.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:21	zoneallarm_pro_crack.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:23	FIFA2003 crack.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:23	NBA2003_crack.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:23	AquaNox2 Crack.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:22	UT2003_bloodpatch.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:24	Half Life Counter Strike Full.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:23	Half Life Full.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:23	C&C Generals_crack.exe	W32.Spybot.Worm	File	Quaranti...	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:41:31	tpibktzn.exe	W32.Spybot.Worm	File	Left alone	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:36:49	xjby.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:36:49	lvsl.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:36:49	dhqx.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:36:49	jybj.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:36:50	szvv.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:36:56	MERGE.EXE	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:36:58	gswin32.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:37:04	uninstgs.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:37:11	DAINST.EXE	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:37:12	PREINSTL.EXE	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator
2003-08-07 오후 7:37:13	Setup.exe	W32.Weird	File	Cleaned	PHYSICS-NZ...	Administrator

Files scanned: 37653 | Viruses found: 173 | Elapsed time: 17:43

Blaster Prevalence



Source: Vern Paxson

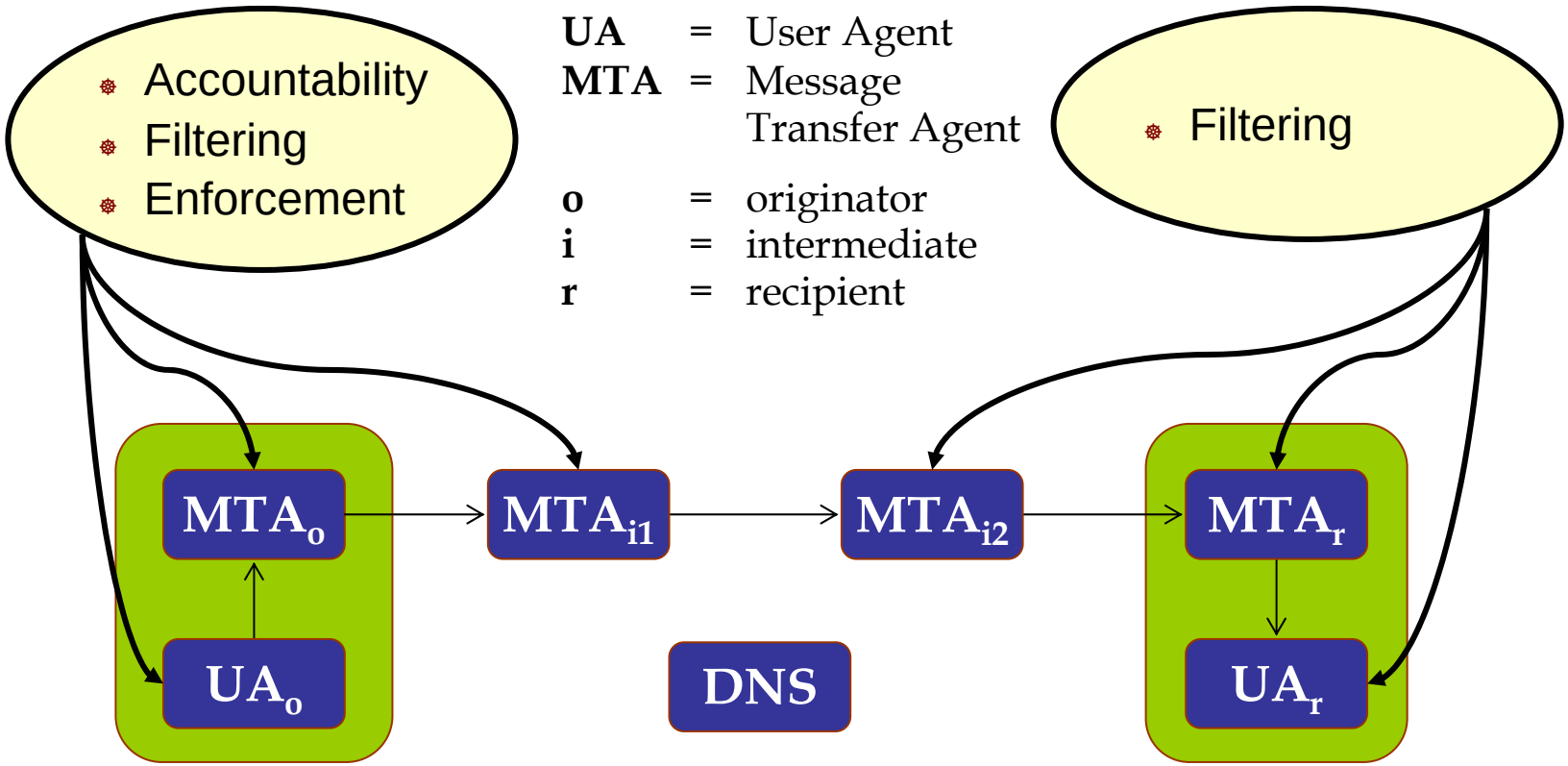


Source: Xmission Statistics Web Site

What Are the Implications for the Internet Architecture?

- The end isn't necessarily trustable
- Authentication helpful but not sufficient
  - "What you know"/"What you have" -> "What you are"
  - Composition of mechanisms valuable (authentication + whitelisting)
  - Weaker (but more efficient) authentication may be more useful than strong (but expensive)
- Sometimes the middle may have to take action to protect the ends & middle
- Interactions with legal & economic forces need to be considered

Points of Control



Source: Dave Crocker, Brandenburg Consulting

What New Work is Needed?

- Is it time to think about one or more IETF WGs?
  - Are there existing technologies sufficiently mature to enter the IETF process?
  - Are there other technologies that could help support legal, economic or forensic activities?
- Are there research activities we should be considering?
- Is there something we should be doing *other* than chartering IETF or IRTF WGs

Potential IETF Activities

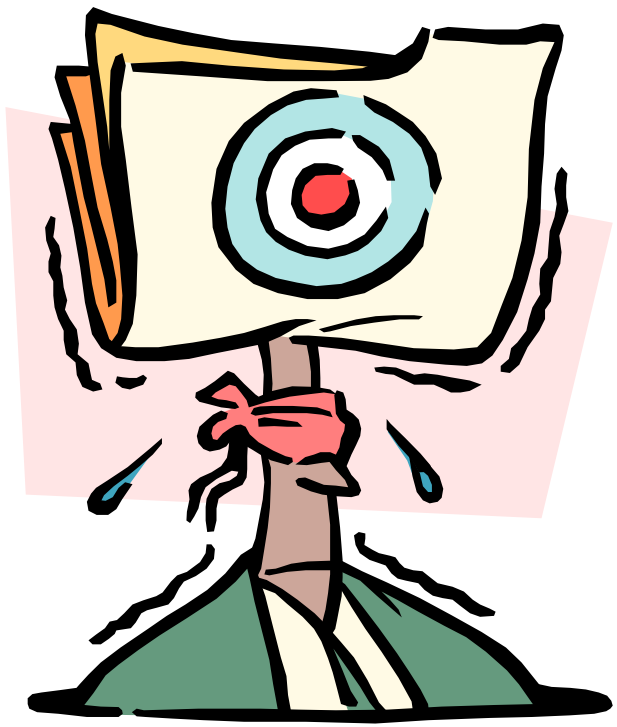
- Studies
  - Problem characterization
- Accountability
  - Authentication
  - Tracking
  - Non-repudiation
- Detection
  - Whitelist
    - Challenge/Response
    - Domain signatures
    - Consent tokens
  - Blacklist
    - RBLs
- Epidemiology (Post Hoc)
  - DDoS community of attackers -> community of responders
  - Standardized abuse reporting
  - Whitelist/blacklist interchange

Evaluating Proposals

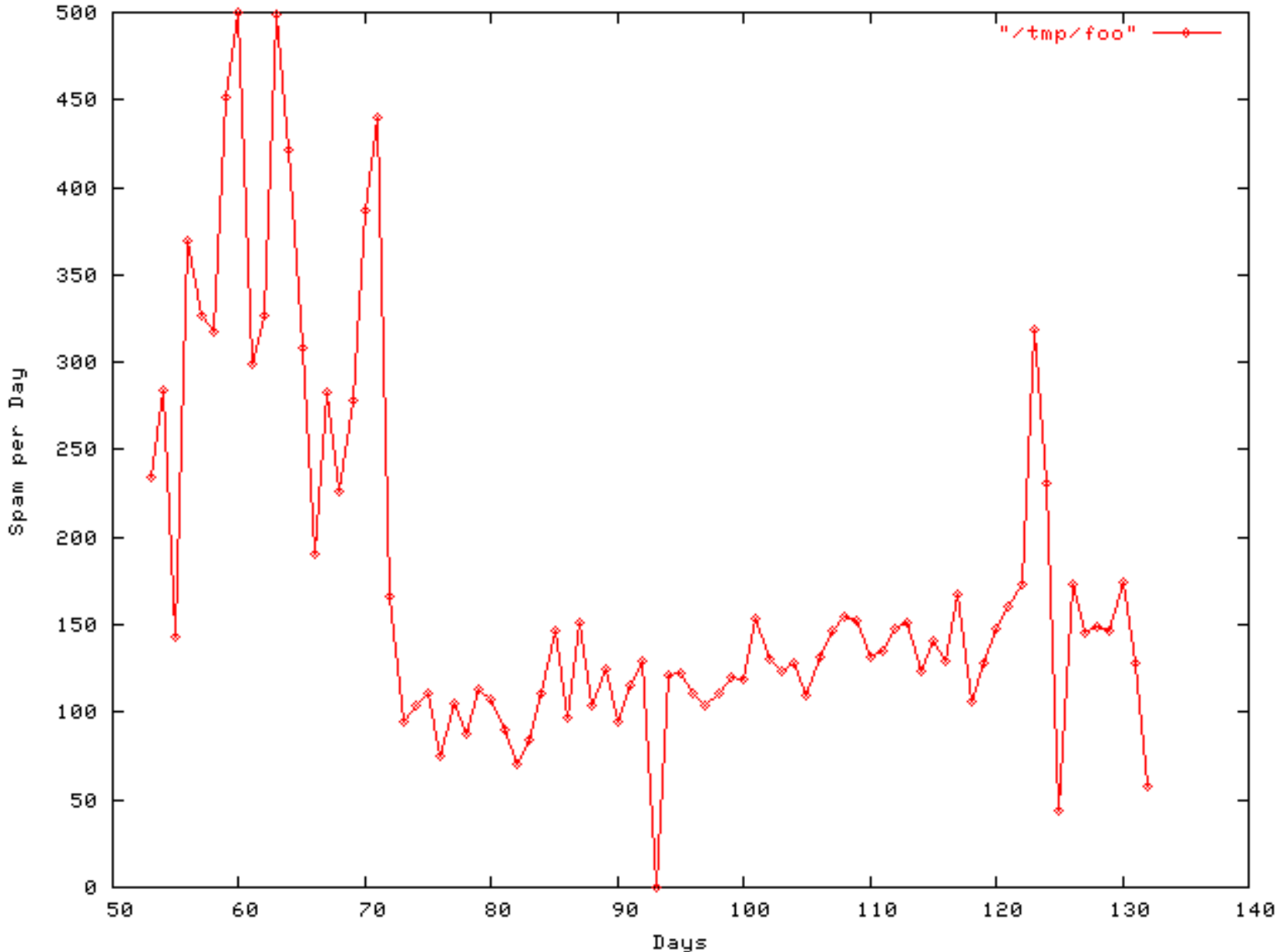
- Adoption
  - Effort to adopt proposal
  - Effort for ongoing use
  - Balance among participants
  - Threshold to benefit
- Operations impact on
  - Adopters of proposal
  - Others
- Internet scaling – What if…
  - Use by everyone
  - Much bigger Internet
- Robustness
  - How easily circumvented
- System metrics
  - Cost
  - Efficiency
  - Reliability
- Impact
  - Amount of Net affected
  - Amount of spam affected
- Test scenarios
  - Personal post/Reply
  - Mailing List
  - Inter-Enterprise

Source: Dave Crocker, Brandenburg Consulting

Discussion?

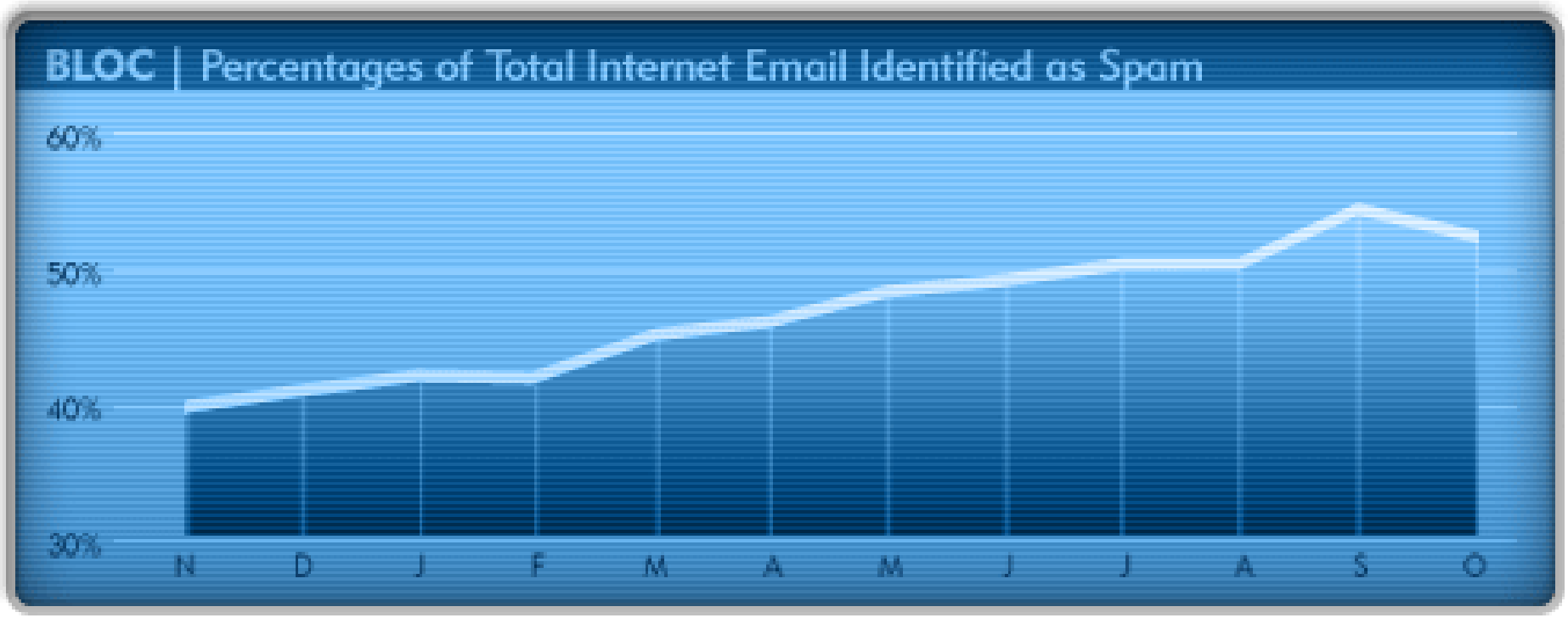


Mark Handley's Data



Percent of Total Email Identified as Spam

http://www.brightmail.com/spamstats.html



SOURCE: Brightmail Logistics and Operations Center (BLOC)