Malicious Activity and Risky Behavior in Residential Networks

Gregor Maier[1], Anja Feldmann[1], Vern Paxson[2,3], Robin Sommer[2,4], Matthias Vallentin[3]

[1] TU Berlin / Deutsche Telekom Laboratories
[2] International Computer Science Institute (ICSI)
[3] University of California, Berkeley
[4] Lawrence Berkeley National Laboratories (LBNL)

Introduction

- Common perception: Residential users responsible for much of insecurity
- Even worse in developing regions
- But: Few systematic studies to date
- We undertake such a study
- Also important: What influences security?
  - Anti-virus
  - Software updates
  - Risky behavior (requesting blacklistes URLs)

Outline

- Data sets and vantage points
- Methodology
- Security awareness and risky behavior
- Malicious activity
- Discussion & Conclusion

Outline

- Data sets and vantage points
  - European ISP
  - AirJaldi network in India
  - Lawrence Berkeley Lab
  - Data annotations
- Methodology
- Security awareness and risky behavior
- Malicious activity
- Discussion & Conclusion

Data sets: European ISP

- Major ISP in Europe
- Observations from 20,000 DSL customers
- All data immediately **anonymized**
- 14 day observation period
- No traffic shaping or port filters
- Traffic makeup:
  - More than 50% HTTP
  - Peer-to-Peer around 15%
  - NNTP also significant

Data sets: AirJaldi in India

- Community network in rural India
- 10,000 users; several 1,000 machines
- All share 10Mbps uplink
- 400 wireless routers, spread over 80km radius
- Use "layered NAT" approach => Cannot identify individual hosts
- 3 traces, 34-40hrs each
- Traffic makeup:
  - 56—72% HTTP
  - Quite some VoIP and instant messenger traffic
  - Almost no Peer-to-Peer or NNTP

Data sets: LBNL

- Lawrence Berkeley National Lab, CA, USA
- 12,000 hosts
- 4 day observation period; 7,000 hosts active
- Open network policy but
- Security staff:
  - Uses Bro IDS
  - Infected machines are taken offline immediately
- We do not expect any/much malicious activity

Data annotation

- Want to know more about DSL-lines
- Identify influences on security
- Is NAT used? How many hosts are connected
- How active are they?
  - Group by number of HTTP request
  - Classify into high/medium/low activity
- Operating systems
  - Are Macs more secure?
  - Identify by HTTP user-agent string
  - Check DSL lines with **only Macs** (and no Windows)

Outline

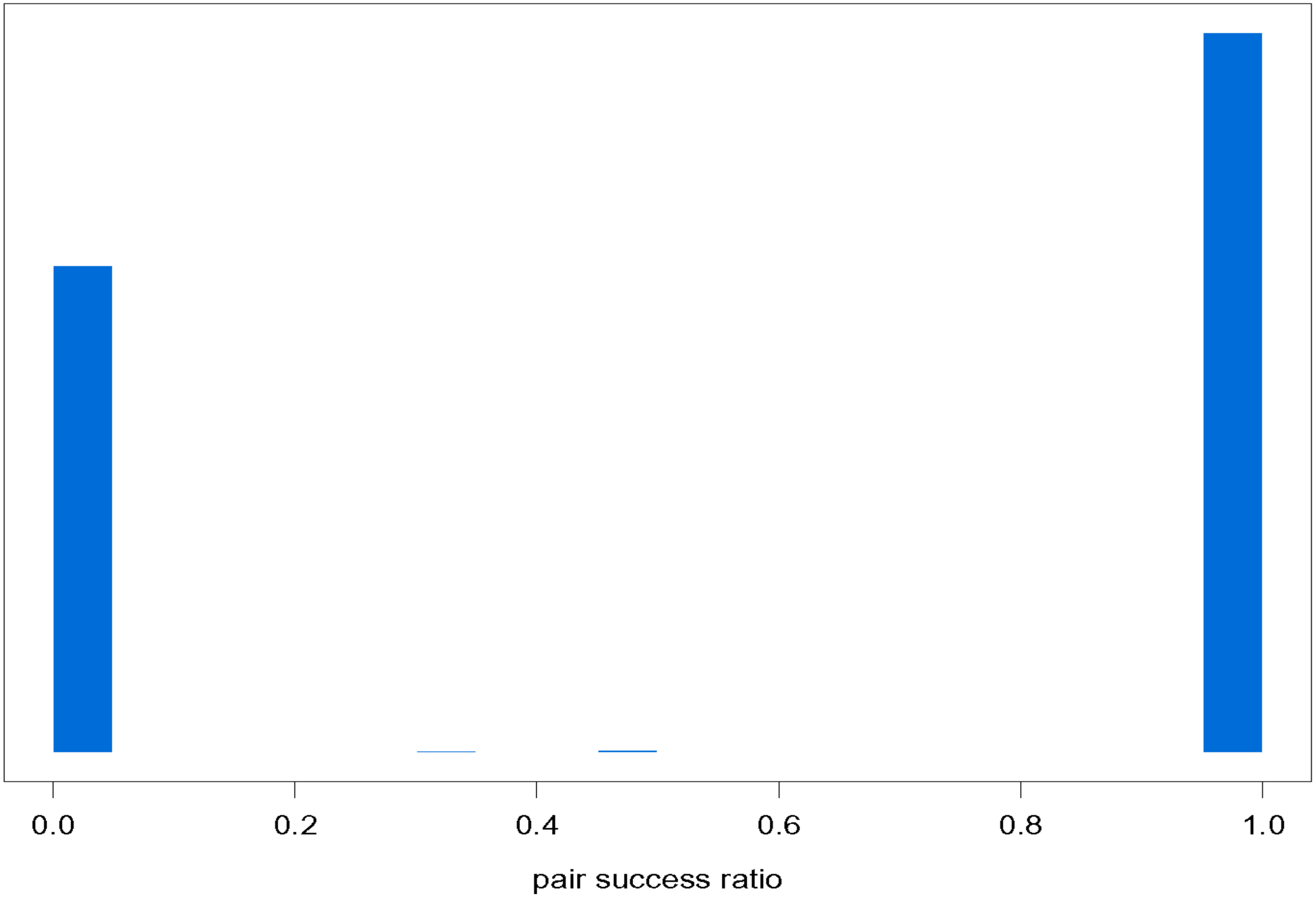
- Data sets and vantage points
- Methodology
  - Scanning
  - Spamming
  - Known malware families
  - Generic NIDS
  - Security awareness and risky behavior
- Security awareness and risky behavior
- Malicious activity
- Discussion & Conclusion

Finding Scanners (I)

- Problem: NIDS are tuned to find incoming scans
  - Often use threshold of unsuccessful connections per source
- We want outgoing scans but
  - Scan traffic embedded in benign activity
  - Cannot use simple threshold
- Idea (borrowed from TRW scan detector)
  - Ratio of successful connections / all connections per <DSL-line, remote-IP> pair
  - Does it work?

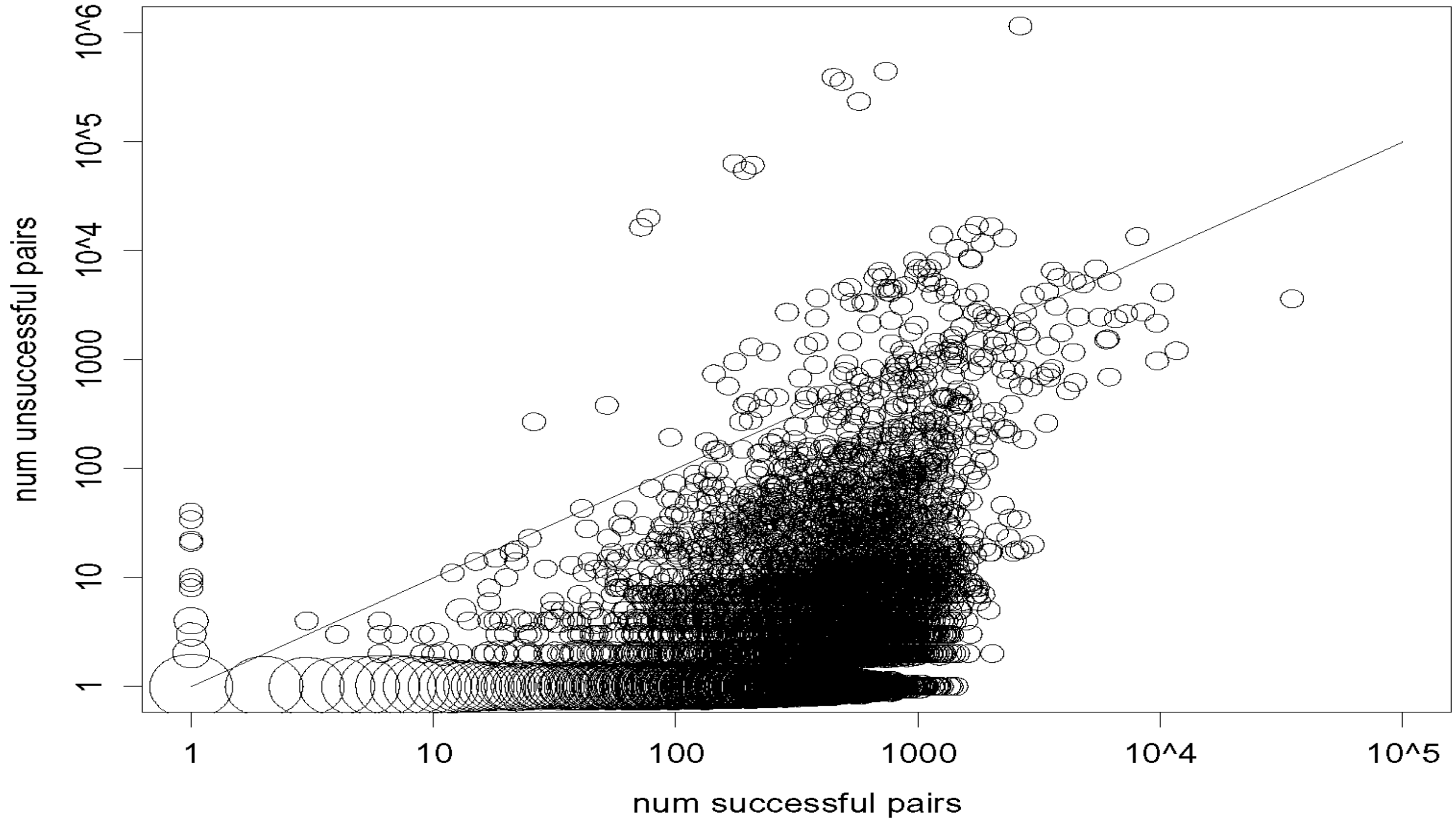
Finding Scanners (2)

- Histogram: Success ratio per pair



Finding Scanners (3)

- Next step: classify pair as successful or unsuccessful
- Count #successful VS. #unsuccessful pairs per DSL-line

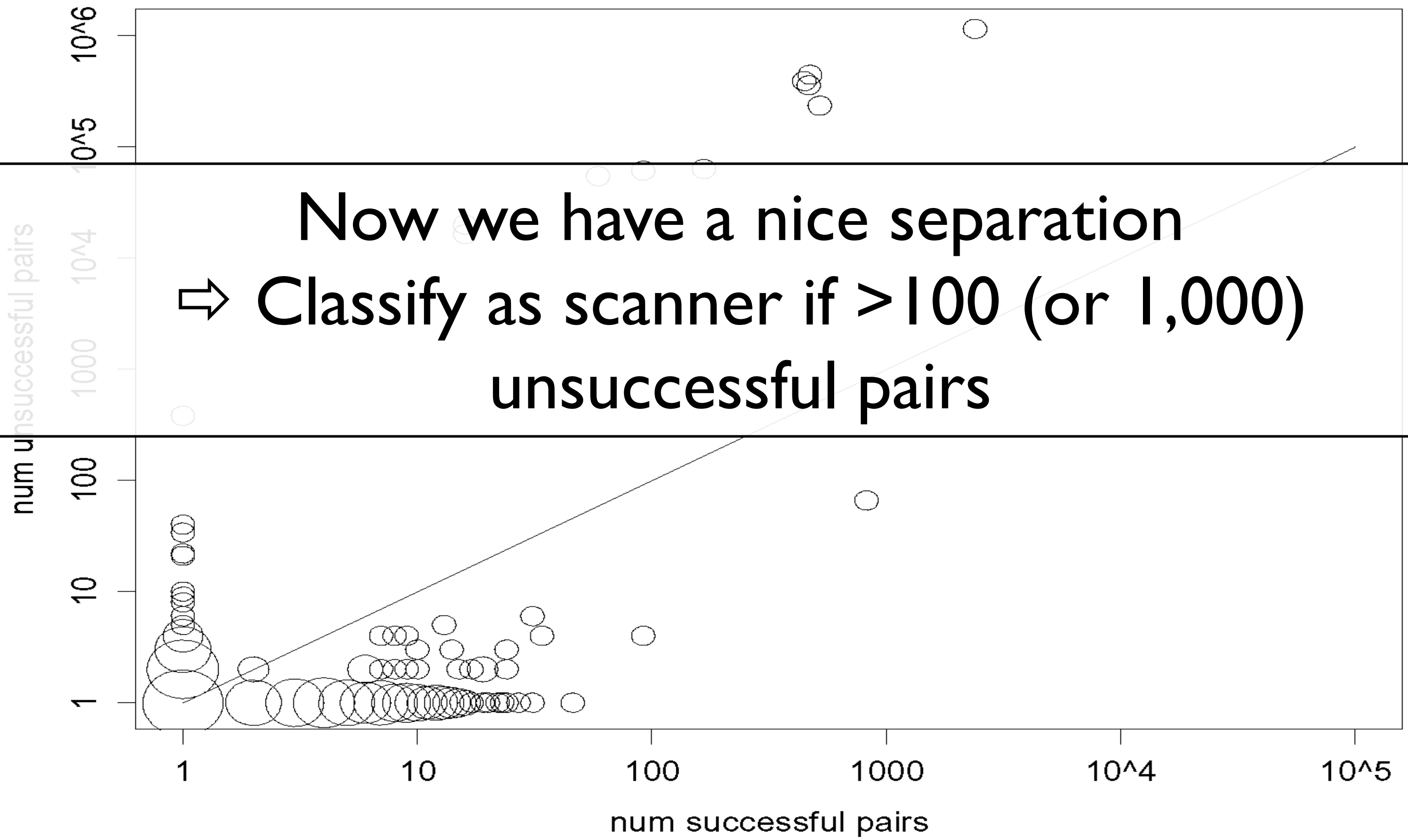


Finding Scanners (4)

- Where's the problem?
- ➢ Peer-to-Peer (P2P) protocols
  - Peer tries to contact peers' IPs
  - But peer might be offline now or moved to other IP
  - ➢ Many unsuccessful connections
  - But not only filesharing, WoW also uses P2P protocol for maps
- Solution: Look only for suspicious / dangerous ports
  - E.g., windows SMB, databases, VNC, remote desktop

Finding Scanners (5)

- #successful VS. #unsuccessful for suspicious ports



Now we have a nice separation

⇨ Classify as scanner if >100 (or 1,000) unsuccessful pairs

Finding Spammers

- We omit the details for brevity
- Similar idea to scanning:
  - Count number of contacted SMTP servers
- DSL lines contact <<25 or >> 100 SMTP servers
  - Use cutoff of 100 for spam classification

Malware families

- Use network signatures of known malware
- Conficker
  - Tries to resolve known DNS names
- Zlob
  - Changes DNS resolvers
  - Targets Macs and Windows
- Zeus
  - Tries to resolve DNS names of C&C servers
    Domain names from blacklist

Generic NIDS

- Use Snort with Emerging Threads rulesets
- 3,500 rules (but undocumented)
- 1million alarms per day, 90% of DSL lines
    - Unuseable
- Includes everything
    - Adware: users might have installed them on purpose
    - "Spyware": includes Alexa toolbar, but Alexa clearly states what it does
    - etc.
    - Excluded those

Generic NIDS (2)

- Still too many hits :-(
- Lack of documentation ⇨ Cannot tell:
  - How bad traffic triggering a specific rule is
  - False positives
- E.g., signatures for botnet command & control:
  - Check for single or double-letter URL parameters (b=...., tm=...)
  - Many benign websites use them too
- Conclusion
  - Emerging threads might be useful for small networks with strict policies but for our case
  - **Document rules!!!!**

Security awareness & risky behavior

- Security awareness
  - Do user use/update anti-virus software?
  - Do user update operating systems?
  - Detecting by inspecting HTTP user-agents
- Risky behavior
  - Do users request URLs blacklisted by Google Safe Browsing?
  - We update our blacklist copy every 25 minutes
- Again: this helps to find factors **influencing** security problems

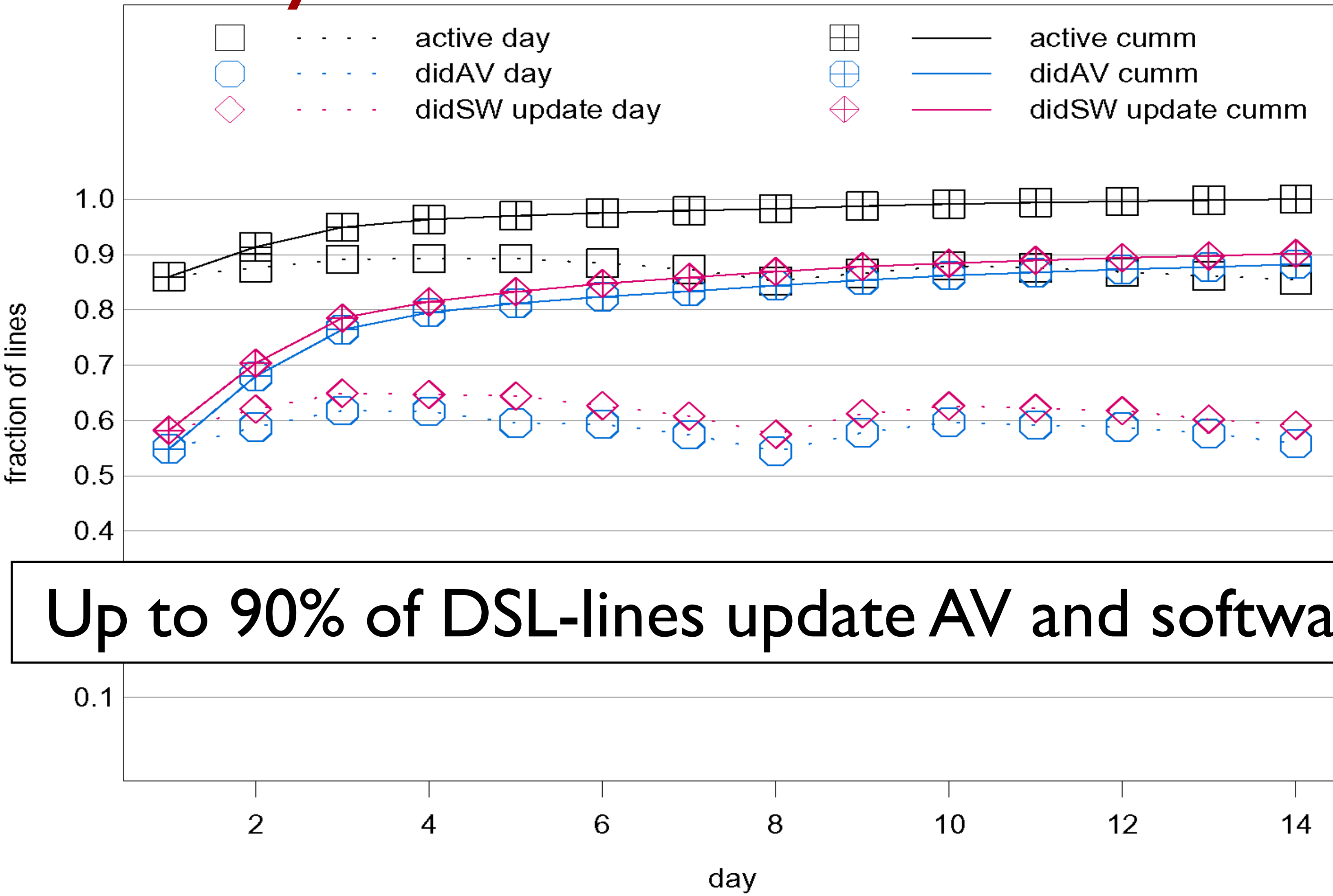
Methodology summary

- Behaviroal metrics
  - Scanning
  - Spamming
- Malware families
  - Conficker
  - Zlob
  - Zeus
- Generic NIDS (Snort with Emerging Threads)
  - Unuseable
- Security awareness and risky behavior

Outline

- Data sets and vantage points
- Methodology
- Security awareness and risky behavior
  - Security awareness
  - Google blacklist
  - Comparision with AirJaldi and LBNL
- Malicious activity
- Discussion & Conclusion

Security awareness



Up to 90% of DSL-lines update AV and software

Google blacklists

- Up to 4.4% of DSL-lines request blacklisted URL per day
- **Over 14 days: 19% do so!!!**
- Google blacklist integrated in many browsers
  - Were users warned by browser and ignored it?
  - Google requires update every 30 min
  - Check whether same user-agent downloads blacklist and requests URL
  - Result: mixed. Some **were warned, but ignored it!!**

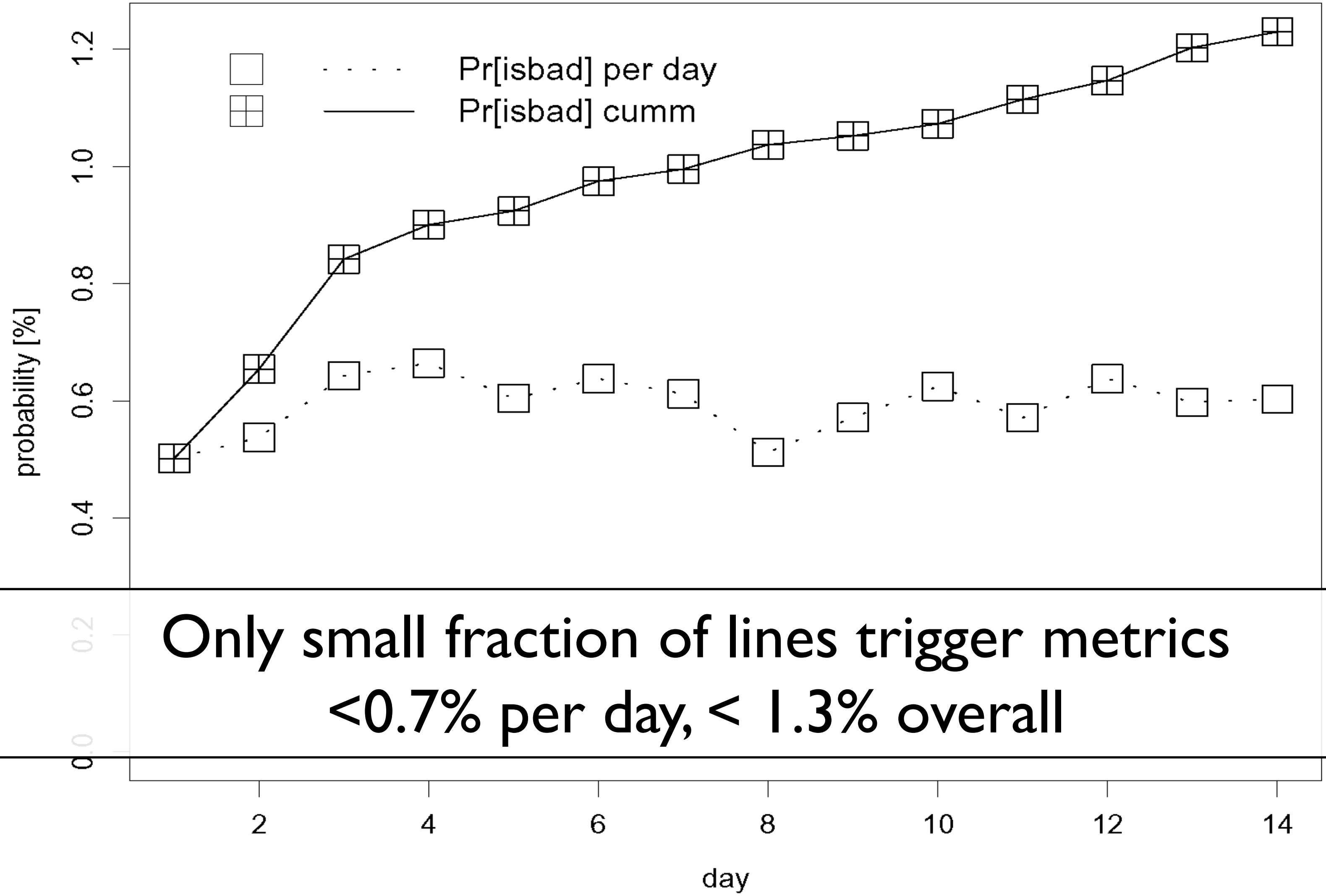
Compare to AirJaldi and LBNL

- AirJaldi
  - Cannot do per DSL-line or host (NAT hierachy)
  - Fraction of requests for anti-virus and software updates similar
  - Fraction of requests that are blacklisted similar
- LBNL:
  - Less anti-virus and software updates
    - But central update servers at LBNL
    - Other OS mix
  - Significantly less risky behavior

Outline

- Data sets and vantage points
- Methodology
- Security awareness and risky behavior
- Malicious activity
  - General results
  - Influences on malicious activity
  - Malicious activity and Macs
  - Comparison with AirJaldi and LBNL
- Discussion & Conclusion

Malicious activity



Only small fraction of lines trigger metrics
<0.7% per day, < 1.3% overall

Malicious activity (2)

- Malware families contribute most
  - Few DSL-lines scan or spam
- 44% of spammers active only single day
- 38% of Zeus lines only trigger single day
- Zlob active on 8.4 (10) days on average (median)
- Conficker active on 6.5 days mean, 6 median
- Most others around 4 days (mean) and 2-4 days median
- **92% of "bad" lines only trigger single metric**
- We likely underestimate total

Influences on malicious activity

- No strong influence of anti-virus and OS updates
  - Prob. only 1.26% if not using anti-virus
- No strong influence of NAT
- A l%ittle influence of activity
  - High activity: 4.08%
  - Medium activity: 1.94%
  - Low activity: 0.46%
- Only slight influence of blacklist hits
  - Prob. 3.19%. Less than high activity
  - **Risky behavior does not impact infections much!**

Malicious activity and Macs

- 2.7% of DSL-lines have only Macs
- Mac infections: 0.54% (compare to 1.23%)
- But only Zlob triggers
  - No scanning, spamming, Conficker, Zeus on Macs
- 0.54% of Macs have Zlob, only 0.24% overall
- Mac not better than Windows
- Malware that targets Macs is successful!

Comparison with AirJaldi and LBNL

- No malicious activity at LBNL
  - As we expected
  - Scan and spam metrics trigger on
    - Benign mail server
    - Penetration testing hosts that scan
- AirJaldi
  - 180—260 active IPs per trace
  - Each IP can have 1—1,000s of hosts
  - Cannot analyze per host (NAT)

AirJaldi malicious activity

	AirJaldi 1	AirJaldi 2	AirJaldi 3
IP 1	**ZeuS** Hi AV SW	**ZeuS** Med AV SW	**ZeuS** Hi AV SW
IP 2	**Conficker(3)** Med SW	**Conficker(1)** Med SW	**Spam** Med BLK AV SW
IP 3	Med BLK AV SW	Med AV SW	**Scan** Hi BLK AV SW
IP 4	X	X	**Spam** AV SW
IP 5	X	X	**Spam** Med BLK SW
IP 6	X	X	**Spam** Hi BLK AV
IP 7	Med BLK AV SW	**Scan** Hi BLK AV SW	Hi BLK AV SW
IP 8	Hi BLK SW	**Spam** Hi BLK AV SW	Hi BLK AV SW
IP 9	**Conficker(1)** Hi AV SW	Med AV SW	Med AV SW
IP 10	**Spam? Scan**	X	X
IP 11	**Scan** Med BLK AV SW	AV	AV

Not much malicious activity
Comparable to European ISP

Hi / Med = High / Medium Activity AV = anti-virus SW = software update BLK = Blacklist hit
Shaded background = malicious activity

Outline

- Data sets and vantage points
- Methodology
- Security awareness and risky behavior
- Malicious activity
- Discussion & Conclusion

Discussion & Conclusion (1)

- We use behavioral metrics and malware signatures
- Confident that metrics find what they should
- Cannot know how much we miss
  - Lower bound
  - Might be significant (e.g., most lines trigger 1 metric)
- Out approach mimics closely how security analysts work
  - Deploy toolbox of orthogonal strategies
- Snort with emerging threads problematic
  - Many blacklists have similar problems

Discussion & Conclusion (2)

- Residential users do not spam or scan
  - Likely not infected with such malware
- Users are risk aware
  - Anti-virus and software updates widespread
  - Does not lower infection risk
- Users exhibit risky behavior
  - Many request blacklisted URLs
  - Does not affect infection risk by as much as one may assume
- Comparing to rural community network in India
  - Very similar in terms of malicious activity and risky behavior
  - No infections at LBL and less risky behavior