Active Botnet Probing to Identify Obscure Command and Control Channels

Guofei Gu[1], Vinod Yegneswaran[2], Phillip Porras[2], Jennifer Stoll[3], Wenke Lee[3]

[1]Texas A&M University
[2]SRI International
[3]Georgia Institute of Technology

Roadmap

- Introduction
- BotProbe
- Evaluation
- Summary & Future Work

TEXAS A&M UNIVERSITY

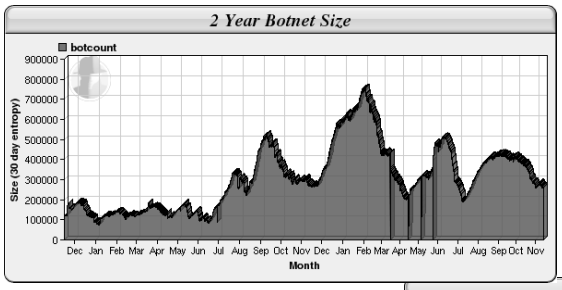
Bots and Botnets

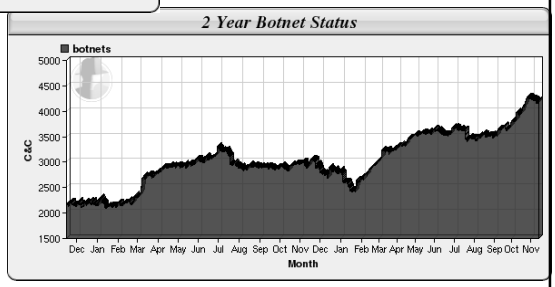
- Computers on the Internet used to be *mere targets*
  - For fun and fame
- Now they are *Resources/Platforms*
  - For profit

- Bots (Zombies)
  - Compromised computers controlled by botcode (malware) without owner consent/knowledge
- Botnets (Bot Armies)
  - Networks of bots controlled by criminals

TEXAS A&M UNIVERSITY

Increasing Number of Bots/Botnets



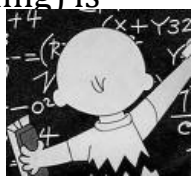


Source: shadowserver.org, Nov. 2009

TEXAS A&M UNIVERSITY

Detecting Botnet C&C

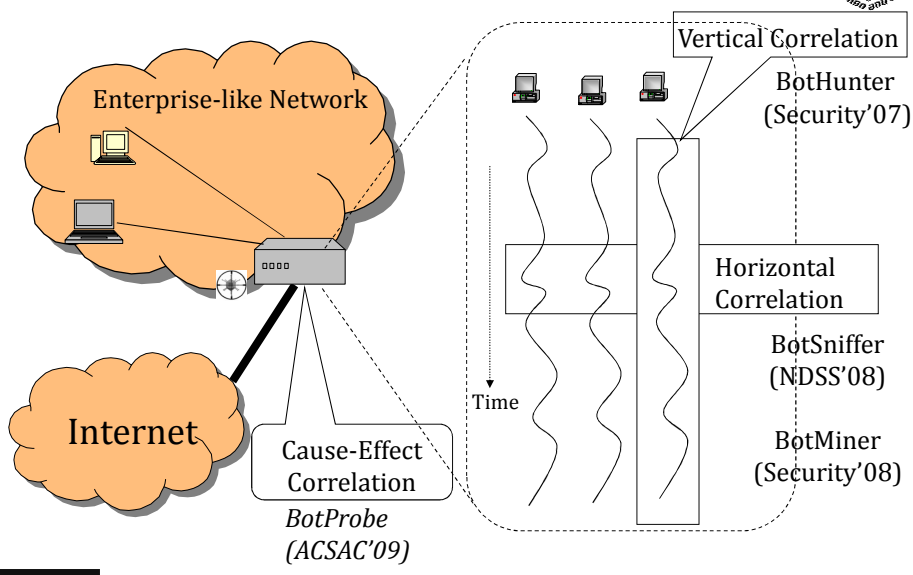
- Botnet C&C can be considered as an *overlay command-response protocol* (over well-known protocols such as IRC)
- C&C obfuscation/obscurity (custom dialect/foreign language, naïve encryption like XOR/hashing) is easy
  - Spybot, Mocbot, Rustock, Nugache, Peacomm
  - "Aloha" → Can this mean "scan"?



- Traditional pure signature based detection approaches may not work

TEXAS A&M UNIVERSITY

Our Correlation-based Framework



TEXAS A&M UNIVERSITY

Why BotProbe?

- Problem with previous passive behavior-based approaches: relatively slow detection, because it requires observing
  - Multiple different infection stages (BotHunter)
  - Multiple instances/rounds of communications/activities (BotSniffer)
  - A long time of communication/activity (BotMiner)
- New *active* approach from BotProbe
  - Requires at most one round of actual C&C
  - Works for a large portion of present real-world IRC botnets

TEXAS A&M UNIVERSITY

Active C&C Detection?

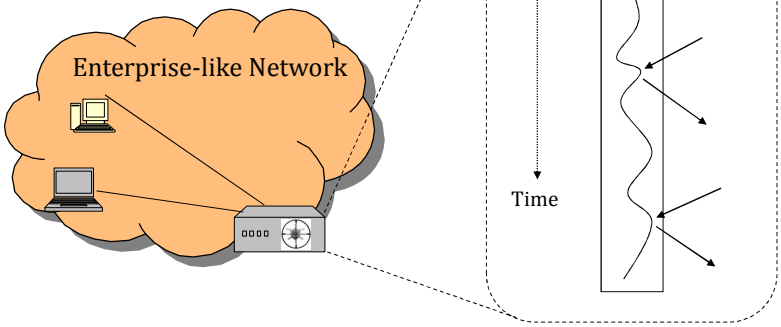
- Why only passively sniff the traffic?
- Can we be more aggressive, and *active*?
- Suppose given a suspicious chat session, how to further verify bot C&C communication or human chatting?
- Now let's think active!
  - Active bot probing for fun (and not profit)

TEXAS A&M UNIVERSITY

BotProbe

Cause-Effect Correlation

- *Bots are non-human*
- *Deterministic command-response pattern*



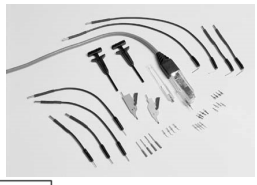
TEXAS A&M UNIVERSITY

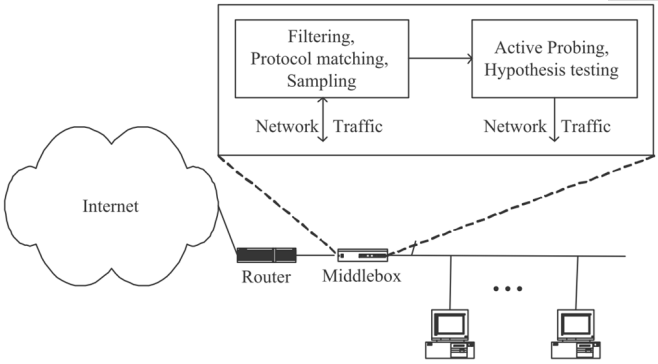
Intuition and Assumptions

- Intuition
  - Bots are *pre-programmed* to respond some command
  - Bots behave almost *deterministically* on given command
  - Bots have lower tolerance for *typographical* errors
- Assumptions
  - *Command-Response* pattern (→ *cause-effect correlation*)
    - Message response
      - E.g., IRC PRIVMSG
    - Activity response
      - E.g., scan, spam,3rd party access (visit a website, downloading)
  - Chat protocol awareness

TEXAS A&M UNIVERSITY

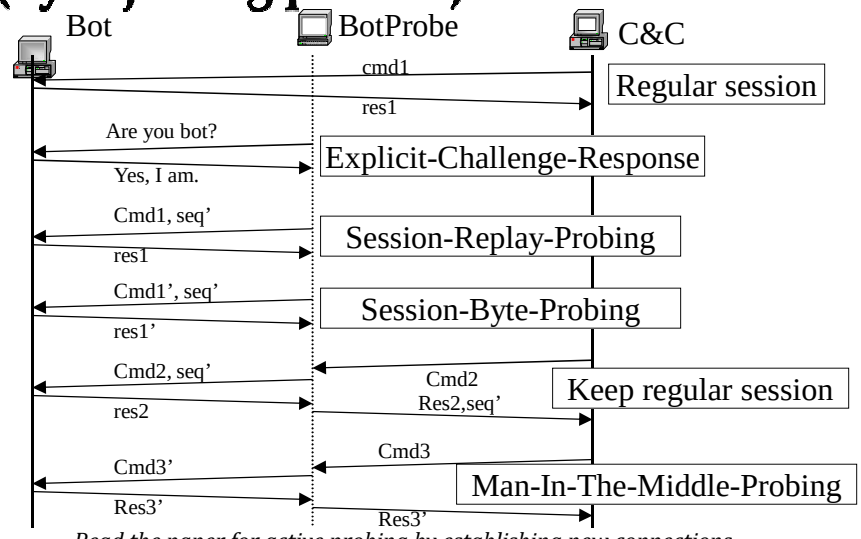
BotProbe: Architecture





TEXAS A&M UNIVERSITY

Active Botnet Probing (by injecting packets)

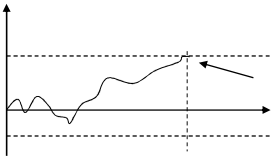


Read the paper for active probing by establishing new connections

TEXAS A&M UNIVERSITY

Hypothesis Testing Algorithm

- Each round, perform some active probing
- Observe some response (D)
  - Hypothesis
    - Pr(D=1|H1) high (for botnet C&C)
    - Pr(D=1|H0) low (for normal user)



- Make a random walk according to the observation D
- After several rounds, we may reach a decision (which hypothesis is more likely, H1 or H0)

- SPRT (Sequential Probability Ratio Testing), or also called TRW (Threshold Random Walk)
- Bounded false positive and false negative rate (as desired), and usually needs only a few rounds

TEXAS A&M UNIVERSITY

Example Algorithm 1: Single-Binary-Response-Hypothesis

- Algorithm 1a: each round is a Explicit-Challenge-Response Probing
  - Observation: D=1 if the answer is not correct
  - Hypothesis
    - Pr(D=1|H1) very high (for botnet C&C)
    - Pr(D=1|H0) very low (for normal user)

- Algorithm 1b: each round is a Session-Replay-Probing
  - Observation: D=1 if there is (PRIVMSG and/or scan) response (and/or within a short time window)
  - Hypothesis
    - Pr(D=1|H1) high (for botnet C&C)
    - Pr(D=1|H0) low (for normal user)

TEXAS A&M UNIVERSITY

Example Algorithm 2: Correlation-Response-Hypothesis

- Each round is a Session-Replay-Probing
- Observation: D=1 if current response is correlated with previous ones (e.g., similar content, length)
- Hypothesis
  - Pr(D=1|H1) very high (for botnet C&C)
  - Pr(D=1|H0) low (for normal user)

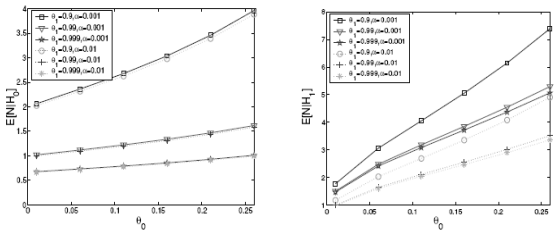
Example Algorithm 3: Interleave-Binary-Response-Hypothesis

- Each round: Interleave Session-Replay-Probing and Session-Byte-Probing
  - Replay original command: response?
  - Replay modified command: response?
- Observation D=1 if answer order is YES & NO
- Hypothesis
  - Pr(D=1|H1) very high (for botnet C&C)
  - Pr(D=1|H0) low (for normal user)

Read the paper for more complex situations

Trade-Off Between Disturbance & Accuracy

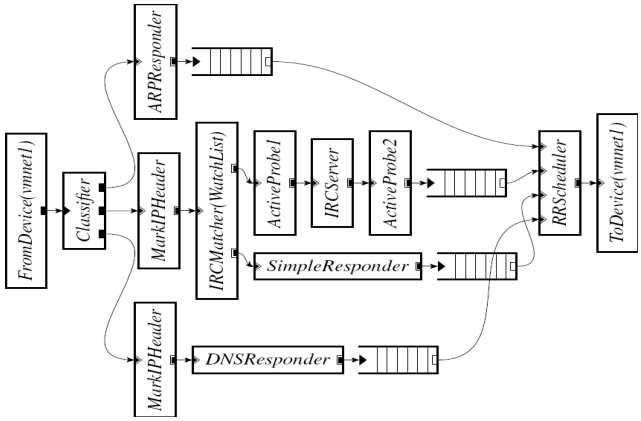
- By probing, you may disturb normal IRC client?
  - Measured by number of rounds
- You also want a desired detection rate and false positive rate, right?
- How to make a trade-Off? (choosing maximum number of probing rounds)



- More discussion
  - Whitelist
  - act as one threat indicator for further examination (e.g., BotHunter)…

TEXAS A&M UNIVERSITY

BotProbe: Click Implementation



- Can be used as a middle box (similar to software router) for given network
- Can also be used as a black box testing environment for a given bot binary

TEXAS A&M UNIVERSITY

Experiment with Real IRC Bots

- Rbot: clear text commands
  - .id -> [MAIN]: Bot ID: rx01.
  - .sysinfo -> [SYSINFO]: [CPU]: ...
  - .scan 192... -> [SCAN]: Port scan started...
- Spybot: obfuscated commands
  - otlu (info) -> Version:... cpu:...
  - vgyy}uxjy (passwords) -> Error operation failed
  - yigt&7?847<>477<4<&79?&7 (scan 192...) -> Portscanner startip:...
  - ju}trugj&nzzv@55oxi... (download http:...) -> download http:...
- It takes 2 or 4 rounds to detect bot C&C (depending on the response type) [using Interleave-Binary-Response-Hypothesis]

TEXAS A&M UNIVERSITY

Experiment with Real IRC Bots (cont.)

- Wargbot (captured in SRI honeynet in the wild)
  - 2 rounds to detect
  - We crack the encryption scheme with the assistance of BotProbe…
    - !Q ;\\|!Q <W:Z<Z=B=B=>;P;E;E<[=;<Y=>=:<S<U<W;D<U===;;E<V<[=@<W<U=B===@=G;E<V<[=@;I;O;N;O;E;G;G;N;G;J;H;L;G;O;H<Q;M;J;F;K;D<\\=><Y
    - " F |" e http://img2.freeimagehosting.net/uploads/03bd27490b.jpg
- More examples in the paper

TEXAS A&M UNIVERSITY

User Study

- About a hundred online users at meebo and IRC chatting channels
- Turing-Test-Hypothesis is not very effective
- Interleave-Binary-Response-Hypothesis result:

	meebo chats	IRC chats	Total
Detected in 2 rounds	63 (75%)	10 (77%)	73 (75.3%)
Detected in 3 rounds	8 (9.5%)	1 (7.7%)	9 (9.3%)
Pending after 3 rounds	13 (15.5%)	2 (15.3%)	15 (15.4%)
Total	84	13	97

TEXAS A&M UNIVERSITY

Summary & Future Work

- Summary
  - Explore the feasibility of using active technique to enhance botnet C&C detection, especially for chat-like protocols
  - Design a simple effective hypothesis testing algorithmic framework
  - Implement a prototype system and validate on real world IRC bots
- Future work
  - More robust, practical, and less controversial extensions of active techniques
  - Apply to a more general class of botnet C&C detection (e.g., HTTP- and P2Pbased botnets)
  - Server-side probing

TEXAS A&M UNIVERSITY

Discussion

- Policy concern
- Evasion
  - Strong encryption
  - Timer-based evasion
  - Stateful C&C