On the Limits of “On the Limits”

Towards Automated Detection of Peer-to-Peer Botnets: On the Limits of Local Approaches, Jelasity, M. and Bilicki, V., 2009, in proceedings of *2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET ’09)*, Berkeley, CA

Danver Braganza
4316790

8th October, 2009

Summary

In a nutshell

We would like to detect botnets automatically, but it could not be done with a local approach:

In a nutshell

We would like to detect botnets automatically, but it could not be done with a local approach:

1. describe how they created a (clever) virtual botnet on a AS-level simulation of the Internet

In a nutshell

We would like to detect botnets automatically, but it could not be done with a local approach:

1. describe how they created a (clever) virtual botnet on a AS-level simulation of the Internet
2. show that the local visibility of the botnet is dimished or destroyed

In a nutshell

We would like to detect botnets automatically, but it could not be done with a local approach:

1. describe how they created a (clever) virtual botnet on a AS-level simulation of the Internet
2. show that the local visibility of the botnet is dimished or destroyed
3. conclude that detection of botnets by a local approach is impossible

Appreciative Comments

In general, the paper

In general, the paper

- is forward-looking, aimed a problem which is important and likely to get worse

In general, the paper

- is forward-looking, aimed a problem which is important and likely to get worse
- identifies that P2P traffic, even botnet traffic, is not inherently malicious

In general, the paper

- is forward-looking, aimed a problem which is important and likely to get worse
- identifies that P2P traffic, even botnet traffic, is not inherently malicious
- suggests that automated detection is supplemented by knowledge about attack sources

More appreciation

The paper also shows some deep thinking in their robust justification of limitations.

> We are aware of the methodological problems with collecting AS-level links and simulating protocols over them. However, for the purposes of this study, the main goal was not to achieve perfect low level realism but to capture the important structural properties of the Internet as a complex network, a level that even a good topology generator could provide.

Critical Comments

Minor Annoyances

Minor Annoyances

- TDG (Traffic Dispersion Graph) is used before it is defined

Minor Annoyances

- TDG (Traffic Dispersion Graph) is used before it is defined
- They never *define* what AS means. There is not even one use of the word Autonomous in their paper

Minor Annoyances

- TDG (Traffic Dispersion Graph) is used before it is defined
- They never *define* what AS means. There is not even one use of the word Autonomous in their paper
- They get away with this:

> Finally, we state without proof that a much simpler stochastic approach in which we have no clustering at all, but where each node can use only one random long range link results in a similar routing complexity in expectation.

Critical hit

- Three ways to do automated detection

Critical hit

- Three ways to do automated detection

  1. Propagation

Critical hit

- Three ways to do automated detection

  1. Propagation
  2. Overlay traffic

Critical hit

- Three ways to do automated detection
  1. Propagation
  2. Overlay traffic
  3. Source of attacks

Critical hit

- Three ways to do automated detection
  1. Propagation
  2. Overlay traffic
  3. Source of attacks
- Argue weakly that overlay traffic is the most promising

Critical hit

- Three ways to do automated detection
  1. Propagation
  2. Overlay traffic
  3. Source of attacks
- Argue weakly that overlay traffic is the most promising
- Rest of paper goes on to show the weaknesses of overlay traffic inspection locally

Critical hit

- Three ways to do automated detection
  1. Propagation
  2. Overlay traffic
  3. Source of attacks
- Argue weakly that overlay traffic is the most promising
- Rest of paper goes on to show the weaknesses of overlay traffic inspection locally
- Practically, where else but locally?

Critical hit

- Three ways to do automated detection
  1. Propagation
  2. Overlay traffic
  3. Source of attacks
- Argue weakly that overlay traffic is the most promising
- Rest of paper goes on to show the weaknesses of overlay traffic inspection locally
- Practically, where else but locally?
- Exclude unstructured and superpeer networks (not clear why the former, weak why the latter)

Conclusion

- Experimented with simulated botnets

Conclusion

- Experimented with simulated botnets
- Attempted to get inside the mind of a botmaster who hopes to evade detection

Conclusion

- Experimented with simulated botnets
- Attempted to get inside the mind of a botmaster who hopes to evade detection
- Showed that it is possible to foil a local approach

Conclusion

- Experimented with simulated botnets
- Attempted to get inside the mind of a botmaster who hopes to evade detection
- Showed that it is possible to foil a local approach
- Suggested that a distributed anti-botnet system is needed

On the Limits of “On the Limits”

*Towards Automated Detection of Peer-to-Peer Botnets: On the Limits of Local Approaches***,** Jelasity, M. and Bilicki, V., 2009, in proceedings of *2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET ’09)***,** Berkeley, CA

Danver Braganza
4316790

8th October, 2009

*

Question

Who is responsible for combating the botnet?

- End User

Who is responsible for combating the botnet?

- End User
- ISP

Who is responsible for combating the botnet?

- End User
- ISP
- Goverment

Who is responsible for combating the botnet?

- End User
- ISP
- Goverment
- International Net Police