Metric design for botnet mitigation

Santiago Aragn, *Member, IEEE,* John Doe, *Fellow, OSA,* and Jane Doe, *Life Fellow, IEEE*

***Abstract*—Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.**

***Keywords*—IEEEtran, journal, LaTeX, paper, template.**

I. What security issue does the data speak to?

+ Botnet attack ++ RCE Vulnerability ++ Exploiting Java reflexion ++ Bypassing White and Blacklisting

II. What would be the ideal metrics for security decision makers?

What would be the ideal metrics for security decision makers?

The security issue defined in section **??** have distinct effects depending on the issued party. We identify several parties that might be aimed by the security issue and we arrange them in three groups which are affected in similar ways by the security issue. For each group, we identify how the botnet (BN) is negatively influencing their interests, as well as a set of ideal metrics which could help each party to derive better decisions to mitigate their problem while maximizing the return on security investment.

a) Internet Service Provider (ISP) & Botnet's victim: For this parties it is of main interest to avoid misuse of resources i.e. the ISP would like to block not legitim incoming traffic to its network while the botnet's victim would like to maintain availability of its resources.

b) Metrics:

- Attack prediction
- BN identity detection
- Resources (un)availability cost

c) Botnet's zombie machine: Even when this party might not be directly interested in avoiding being a tool of the botnet, it should be interested in not misusing its computational resources as part of the botnet.

d) Metrics:

- Rootkit detection
- Resources misuse cost

e) Regulator authority & Law enforcement agencies: The parties interested in prevent, prosecute and punish the ones behind a security issue, i.e., For the regulator authority is of main interest to transfer the risk to the ISP, to encourage the zombies machines to increase their security protection, while for a law enforcement agency is to have mechanisms to hunt down the attacker

f) Metrics:

- BN location detection

III. What are the metrics that exist in practice?

IV. A definition of the metrics you can design from the dataset

BN Location (geo time ip) Attack prediction/probability (Flow anaylis)

V. An evaluation of the the metrics you have defined. This should include graphical representations of the metrics (e.g., histograms, scatter plots, time series, bar charts).

VI. Conclusion

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Appendix A
Proof of the First Zonklar Equation

Some text for the appendix.

Acknowledgment

The authors would like to thank...

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.

M. Shell is with the Department of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, 30332 USA e-mail: (see http://www.michaelshell.org/contact.html).

J. Doe and J. Doe are with Anonymous University.

Manuscript received April 19, 2005; revised January 11, 2007.

John Doe Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.