Review of Ecology of Malware Article

TP #10 Peer Reviewed by: _____

Alex Laird
CS 3310-01
Date: November 7, 2009
Operating Systems
Fall 2009
Computer Science, (319) 360-8771
alexdlaird@cedarville.edu

Grading Rubric	Max	Earn
On Time/Format	1	
Correct	5	
Clear	2	
Concise	2	
TOTAL	10	

ABSTRACT

This paper is a review of the scholarly journal article The Ecology of Malware[1].

Keywords

Scholarly, Review, Ecology, Malware

1. INTRODUCTION

Malware, the sneaky and frequently sinister cousin to viruses, has become the dreaded nemesis of operating systems today. As malware developers continue to investigate sneakier and more abrasive methods of attacking a users system, protection against such intrusions grows better as well. A new study considers that malware follows certain ecological principles and that interactions between malware and humans and malware with other malware is unpredictable for malware developers but predictable for malware defense specialists.

2. THEORY

Ecology is the biological study of how one living organism deals with another. Ecology involves testing certain specimens in controlled environments, seeing how they react in ideal situations, then introducing a new species to see how the original organism reacts to that new species.

The theory is that malware presents similar characteristics to living organisms. It grows, it latches on to certain other "organisms" on a system, and for all intensive purposes it seems alive. If malware can be tested in clean environment to see how it reacts, the root causes and defenses needed to protect against these threats can be discovered.

3. TESTING

Analysts must sift through tens of thousands of unique pieces of malware in a single day, only a few of which will be captured to perform further tests on. Specimens are only captured if they can be easily reproduced and if the symptoms the malware causes can be duplicated on a clean, freshly installed copy of the vulnerable system.

Of course, not all malware captured can be viewed as a single instance or specimen. Some types of malware contain multiple parts, essentially creating an ecological system that all must be captured and duplicated in order to fully test it. These systems can contain multiple different types of malware in their various parts.

4. PRESENCE/ABSENCE MATRIX

Ecologists have developed a presence/absence binary matrix that has species as its rows and sites as its columns, one which indicates the presence of a specimen with a "1" in the row or column it exists in. If there is a probe on a particular port from an IP address, it means that IP address is infected. For instance, if an SYN package is observed on the IP address w.x.y.z on port 135 in a network, it means that the w.x.y.z is infected with the species corresponding to port 135.

Once the matrix is established, tests can be run to detect concurrence patterns in the malware. Hypothesis can then be made in an attempt to come to the null hypothesis (that the malware has not effected the system). The null hypothesis can be used to generate a null model, one which the test results want to cling toward. If a null hypothesis is not established, test results are considered inconclusive.

5. PRESENCE OF SPECIES

The presence of a particular species in a system would likely make the presence of another species less likely. Pieces of malware, just like living organisms, fight with each other and the stronger piece will win. The other species does not necessarily leave, the impact of it may simply be significantly thwarted by the dominant species.

Competition diminishes the presence of the same or similar species, facilitation encourages such a presence. For instance, if an SQL server worm is present on an SQL server, other such worms are likely to come join the worm on the server. Competition was noticed largely between ports 135 and 445, probably due to the Blaster worm and its variants. The Blaster worm and its variants frequently leave a trace of themselves, making the infected port an easy target for future inhabitants, thus re-inhabitation is common for this malware type.

.

6. CONCLUSIONS

Malware prevention studies investigate the organizational structure and component interactions between malware and the environment it is placed on. Researchers use solutions found from biological environment studies to help control and prevent malware in its ecological system. These techniques can then be implemented into malware prevention software, increasing the likeliness for such software to stop the malware before it infects your system and improving the reliability of killing such ailments after they have infected a computer.

7. REFERENCES

[1] J. R. Crandall, R. Ensaf, S. Forrest, J. Ladau, and B. Shebaro. The ecology of malware, 2009.