[1] D. R. Ellis, J. G. Aiken, K. S. Attwood, and S. D. Tenaglia. A behavioral approach to worm detection. In *Proceedings of the 2004 ACM Workshop on Rapid Malcode (WORM)*, pages 43-53, 2004. [bib | DOI]

> This paper presents a new approach to the automatic detection of worms using behavioral signatures. A behavioral signature describes aspects of any particular worm's behavior that are common across the manifestations of a given worm and that span its nodes in temporal order. Characteristic patterns of worm behaviors in network traffic include 1) sending similar data from one machine to the next, 2) tree-like propagation and reconnaissance, and 3) changing a server into a client. These behavioral signatures are presented within the context of a general worm propagation model. Taken together, they have the potential to detect entire classes of worms including those which have yet to be observed.

[2] D. M. Kienzle and M. C. Elder. Recent worms: a survey and trends. In *Proceedings of the 2003 ACM Workshop on Rapid Malcode (WORM)*, pages 1-10, 2003. [bib | DOI]

> In this paper, we present a broad overview of recent worm activity. Virus information repositories, such as the Network Associates' Virus Information Library, contain over 4500 different entries (through the first quarter of 2003). While many of these entries are interesting, a great number of them are now simply historical and a large percentage of them are completely derivative in nature. However, these virus information repositories are the best source of material on the breadth of malicious code, including worms.This paper is meant to provide worm researchers with a high-level roadmap to the vast body of virus and worm information. After sifting through hundreds of entries, we present only those that we considered breakthrough or novel, primarily from a technical perspective. As a result, we found ourselves omitting some of the most notorious worms simply because they lacked any original aspects. It is our hope that others in the community who need to get up to speed in the worm literature can benefit from this survey. While this study does not contain any original research, it provides an overview of worms using a truly breadth-first approach, which has been lacking in the existing worm literature.From this raw data, we have also extracted a number of broad quantitative and qualitative trends that we have found to be interesting. We believe that a workshop discussion of these, and other thoughts, will be engaging and informative.

[3] OSX.Leap.A worm, 16 February 2006. [bib | .html]

[4] D. Stutzbach and R. Rejaie. Capturing accurate snapshots of the gnutella network. In *Proceedings of 8th IEEE Global Internet Symposium*, pages 127-132, March 2005. [bib | .pdf]

[5] D. Stutzbach, R. Rejaie, and S. Sen. Characterizing unstructured overlay topologies in modern P2P file-sharing systems. In *Proceedings of the ACM SIGCOMM Internet Measurement Conference*, October 2005. [bib | .pdf]

> During recent years, peer-to-peer (P2P) file-sharing systems have evolved in many ways to accommodate growing numbers of participating peers. In particular, new features have changed the properties of the unstructured overlay topology formed by these peers. Despite their importance, little is known about the characteristics of these topologies and their dynamics in modern file-sharing applications.
>
> This paper presents a detailed characterization of P2P overlay topologies and their dynamics, focusing on the modern Gnutella network. Using our fast and accurate P2P crawler, we capture a complete snapshot of the Gnutella network with more than one million peers in just a few minutes. Leveraging more than 18,000 recent overlay snapshots, we characterize the graph-related properties of individual overlay snapshots and overlay dynamics across hundreds of back-to-back snapshots. We show how inaccuracy in snapshots can lead to erroneous conclusions-such as a power-law degree distribution. Our results reveal that while the Gnutella network has dramatically grown and changed in many ways, it still exhibits the clustering and short path lengths of a small world network. Furthermore, its overlay topology is highly resilient to random peer departure and even systematic attacks. More interestingly, overlay dynamics lead to an “onion-like” biased connectivity among peers where each peer is more likely connected to peers with higher uptime. Therefore, long-lived peers form a stable core that ensures reachability among peers despite overlay dynamics.

[6] VBS.Gnutella worm, 30 May 2000. [bib | .html]

[7] W32.Gnuman worm, 26 February 2001. [bib | .html]

[8] R. Wouhaybi and A. Campbell. Phenix: supporting resilient low-diameter peer-to-peer topologies. In *Proceedings of INFOCOM 2004*, volume 1, pages -119, March 2004. [bib | DOI]

> Peer-to-peer networks are mainly unstructured, where no specific topology is imposed on the network during its operations. These networks offer a high degree of resilience against network dynamics disrupting the network's operation. Unstructured networks, based on random connections are limited, however, in the performance and node reachability they can offer to applications. In contrast, structured networks impose predetermined connectivity relationships between nodes in order to offer a guarantee on the diameter between requesting nodes and the requested objects. We observe that neither structured nor unstructured networks can simultaneously offer both good performance and resilience in a single algorithm. To address this challenge, we propose Phenix, a peer-to-peer algorithm that can construct low-diameter resilient topologies. Phenix supports low diameter operations by creating a topology of nodes whose degree distribution follows a power-law, while the implementation of the underlying algorithm is fully distributed requiring no central server, thus, eliminating the possibility of a single point of failure in the system. We present the design and evaluation of the algorithm and show through analysis, simulation, and experimental results obtained from an implementation on the PlanetLab testbed that Phenix is robust to network dynamics such as joins/leaves, node failure and large-scale network attacks, while maintaining low overhead when implemented in an experimental network.

[9] W. Yu. Analyze the worm-based attack in large scale P2P. In *8th IEEE International Symposium on High-Assurance Systems Engineering (HASE)*, pages 308-309, March 2004. [bib | DOI]

> Peer-to-Peer (P2P) computing has become an interesting research topic during recent years. In this paper, we address issue related to analyzing the worm-based attack in P2P systems. Particularly, our technologies include: 1) generic mathematical models for attacker/defender and different P2P systems; 2) practical and effective attack prevention schemes. We find that our proposed defense strategy can efficiently improve the performance of worm detection and system recovery.

[10] L. Zhou, L. Zhang, F. McSherry, N. Immorlica, M. Costa, and S. Chien. A first look at peer-to-peer worms: Threats and defenses. In *Proceedings of Peer-to-Peer Systems IV, 4th International Workshop (IPTPS)*, pages 24-35, February 2005. [bib | DOI]

> Peer-to-peer (P2P) worms exploit common vulnerabilities in member hosts of a P2P network and spread topologically in the P2P network, a potentially more effective strategy than random scanning for locating victims. This paper describes the danger posed by P2P worms and initiates the study of possible mitigation mechanisms. In particular, the paper explores the feasibility of a self-defense infrastructure inside a P2P network, outlines the challenges, evaluates how well this defense mechanism contains P2P worms, and reveals correlations between containment and the overlay topology of a P2P network. Our experiments suggest a number of design directions to improve the resilience of P2P networks to worm attacks.

This file was generated by bibtex2html 1.96.