Modeling and Detection of Camouflaging Worm

Abstract:-

Active worms pose major security threats to the Internet. This is due to the ability of active worms to propagate in an automated fashion as they continuously compromise computers on the Internet. Active worms evolve during their propagation and thus pose great challenges to defend against them. In this paper, we investigate a new class of active worms, referred to as Camouflaging Worm (C-Worm in short). The C-Worm is different from traditional worms because of its ability to intelligently manipulate its scan traffic volume over time. Thereby, the C-Worm camouflages its propagation from existing worm detection systems based on analyzing the propagation traffic generated by worms. We analyze characteristics of the C-Worm and conduct a comprehensive comparison between its traffic and non-worm traffic (background traffic). We observe that these two types of traffic are barely distinguishable in the time domain. However, their distinction is clear in the frequency domain, due to the recurring manipulative nature of the C-Worm. Motivated by our observations, we design a novel spectrum-based scheme to detect the C-Worm. Our scheme uses the Power Spectral Density (PSD) distribution of the scan traffic volume and its corresponding Spectral Flatness Measure (SFM) to distinguish the C-Worm traffic from background traffic. Using a comprehensive set of detection metrics and real-world traces as background traffic, we conduct extensive performance evaluations on our proposed spectrum-based detection scheme. The performance data clearly demonstrates that our scheme can effectively detect the C-Worm propagation. Furthermore, we show the generality of our spectrum-based scheme in effectively detecting not only the C-Worm, but traditional worms as well.

Existing System:

Existing worm detection schemes will not be able to detect such scan traffic patterns, it is very important to understand such smart-worms and develop new countermeasures to defend against them.

Existing detection schemes are based on a tacit assumption that each worm-infected computer keeps scanning the Internet and propagates itself at the highest possible speed. Furthermore, it has been shown that the worm scan traffic volume and the number of worm-infected computers exhibit exponentially increasing patterns. Nevertheless, the attackers are crafting attack strategies that intend to defeat existing worm detection systems. In particular, 'stealth' is one attack strategy used by a recently-discovered active worm called "Attack" worm and the "self-stopping" worm circumvent detection by hibernating (i.e., stop propagating) with a pre-determined period. Worm might also use the evasive scan and traffic morphing technique to hide the detection

Disadvantages:

- **Creation of replica folder in system**
- **Worm makes the computer performance low**
- **Wastage of memory becomes maximum**
- **Detecting a C-worm is a complicated issue**
- **Killing a worm is not much easy**

Proposed System:

Proposed Worm detection schemes that are based on the global scan traffic monitor by detecting traffic anomalous behavior, there are other worm detection and defense schemes such as sequential hypothesis testing for detecting worm-infected computers, payload-based worm signature detection. . In presented both theoretical modeling and experimental results on a collaborative worm signature generation system that employs distributed fingerprint filtering and aggregation and multiple edge networks... In presented a state-space feedback control model that detects and control the spread of these viruses or worms by measuring the velocity of the number of new connections an infected computer makes. Despite the different approaches described above, we believe that detecting widely scanning anomaly behavior continues to be a useful weapon against worms, and that in practice multifaceted defense has advantages

Advantages:

- **This scheme easily finds C-worm**
- **Not only detecting but also deletes C-worm**
- **Saving of memory**
- **Making the CPU performance high**
- **Maintaining the system in a safe manner**

Modules:

1. **Creating C-worms Module**
2. **Loading Antivirus Module**
3. **Detecting C-worms Module**
4. **Removing C-worms module**
5. **Log Viewer Module**

SOFTWARE REQUIREMENTS:

- Operating System :Windows
- Technology : JDK 1.6
- Front End : Java Swing

HARDWARE REQUIREMENTS:

- Processor : Any Processor above 500 MHz
- RAM : 512 MB
- Hard Disk : 10 GB
- Input Device : Standard Keyboard & Mouse
- Output Device : VGA & High Resolution Monitor