SUMMARY OF Ph.D. DISSERTATION

SURNAME, First name

School School of Science for Open and Environment Systems	Student Identification Number	Terada Masato

Title

A study on incident operation for combatting network worm infection

Abstract

Network infection through worms such as Code Red, Slammer and Blaster has caused much damage. Most previous works have focused on incident response, i.e., what to do after being affected. This has led to insufficiency in information sharing environments, damage prediction of critical incidents and minimization of network worm's infection damage.

We focus on incident operation which predicts and prevents the damage caused by network worm infection incidents, and minimizes the damage in case of an occurrence of an incident. We examine how we can provide and construct the parts of incident operation for combatting network worm infection. We propose three systems: JVN (JP Vendor Status Notes) as a security information sharing system, an experimental environment for network worm infection and Web mapper, a Web server port/host mapping system.

First, we take the position that sharing information is important and necessary to eliminate security incidents. JVN accomplishes this by including two service components - “Vendor Status Notes (VN)” and “Status Tracking Notes (TRnotes)”. The former is a service providing countermeasure information concerning vulnerability, and the latter is a service providing event information of incidents, specifically worm activities, exploit code releases and countermeasures of security incidents.

Second, an organization should not rely solely on outside information and should have some information gathering method of its own, such as experimental environments to evaluate network worm infection, to plan countermeasures and to predict damage. We thus propose two types of experimental environment - an experimental environment for search behavior and an experimental environment for infection behavior. These environments do not need any special devices, and are small-scale and readily-available system on conventional hardware/software.

The third system, Web mapper, provides a continuous service to users for reducing the damage of a targeted HTTP port worm propagation. Web mapper shifts the Web network service port number to an alternative port number to suppress the targeted HTTP port worm propagation. The web server operation does not stop by having a port / host conversion component on a proxy server hide the URL change accompanied by the shift to the alternative port number.

An evaluation of our systems showed the validity of our approach.