



# ***Information System Security Operation***

## **Defending the Enterprise from Worms**

### **Detecting and Responding To Enterprise Level Worm Behavior**

#### **Overview**

The United States' critical infrastructures are extremely vulnerable to widespread attacks by new worms. Worms are malicious programs that use network connections to spread rapidly, with or without human intervention. A well-funded adversary could develop and unleash worms that would be orders of magnitude more devastating than anything we have seen to date. If released during warfare, a worm could nullify a great deal of the United States' information advantage. During a crisis, they could cause significant collateral damage by hampering relief efforts or crippling communication. Even our closed military and intelligence networks consist of tens of thousands of homogeneous, vulnerable systems—an attacker need only trick or coerce a single insider to breach the perimeter defenses of these networks and expose them to compromise.

Today the most prevalent defense against worms is anti-virus software. However, the anti-virus model is inadequate for dealing with both current and future worms. Anti-virus software is focused on defending individual hosts, whereas worms attack the enterprise's computing resources as a whole. The anti-virus model is primarily reactive, meaning a fast-moving worm can spread and cause tremendous damage before the anti-virus vendors have a chance to respond. Recent worms such as Nimda and Code Red have demonstrated that even when anti-virus defenses are updated within a day, millions of hosts can be compromised.

The Defending the Enterprise from Worms, or DE-Worm project is an approach that is radically different from traditional anti-virus defenses. Our key innovations are based on the significant observation that our goal is to defend the

enterprise network, not any specific host. With this shift in paradigm, new anti-worm detection and response strategies become possible. Specifically, it is acceptable to lose, or even sacrifice, a few hosts as long as the worm can be discovered and the damage can be contained.

#### **Research Contributions**

This research resulted in the following major research contributions:

- A greater understanding of worms that identifies dynamic behavioral traits as opposed to analyzing for individual file characteristics. This will help advance worm research by providing researchers with hard data, insights gleaned from that data, and a generic worm profile based on patterns of worm behavior.
- A method for discovering previously unknown worms that identifies spreading of behaviors from machine to machine. Even innocuous behaviors, when observed propagating across the network, could indicate the presence of a worm. This will significantly advance the state of the art in worm detection, using a macroscopic view of the enterprise network to observe worms to which our current microscopic level (i.e., individual host) views are blind.
- A strategy for constructing enterprise networks that can contain and survive a worm attack by restricting communication and dynamically quarantining arbitrary segments of the network. This will provide several orders of magnitude improvement in response capability over the manual approaches upon which system administrators must rely today.

**Solution**

Our solution can be distinguished from other existing approaches to defending against worms by the following features and advantages:

- Most expert analyses of worms focus on the mechanics of worm operation, gleaned from manual observation. The DE-Worm project will instead collect dynamic information in a controlled manner. The collection of real behavioural data will allow experts to profile existing worms and predict future worms more accurately.
- Signature-based intrusion detection systems (IDS) detect known attacks on network service. Our DE-Worm approach will be able to detect the spread of worm behaviors, without needing any prior knowledge of their attack mechanisms.
- Anomaly-based intrusion detection systems require extensive training periods to establish baseline behavior within a system. Even after this process, they often generate many false positives. Our DE-Worm

approach works without a training period and is less likely to generate false positives, because alarms are raised only in cases of suspicious behavior that match the profile of a worm.

- Response to worms is typically ad hoc: system administrators and users disconnect machines from the network in an attempt to protect their systems. The DE-Worm response strategy focuses on containment, using existing network mechanisms to restrict inter-system communication during an outbreak, and offers a significant improvement over manual, ad hoc responses.

We propose to replace the traditional anti-virus strategy of protecting the host with DE-Worm strategies that protect the enterprise network instead. Rather than detecting tainted files, we will focus on detecting tainted systems. From this perspective, it is acceptable to lose, or even sacrifice, a few hosts as long as the damage can be contained. With this paradigm shift, new anti-worm detection and containment mechanisms become possible.

