

# Winning the War on Worms

**Pete Lindstrom, CISSP**  
Research Director

**Spire Security, LLC**  
[www.spiresecurity.com](http://www.spiresecurity.com)  
[petelind@spiresecurity.com](mailto:petelind@spiresecurity.com)

# Worm / IPS panel

## ● **Business impact**

- **Why do I care?**
- **How do I measure the impact/significance of worms?**
- **How do worms compare as a threat to other types – viruses, spyware, targeted hacks, etc?**

## Worm / IPS panel

### ● General threat questions

- **With no large worm outbreaks recently, what is the threat?**
- **What is “wormability”?**
- **What techniques are used for worm propagation?**
- **How long could “the Internet” be down for?**

# Worm / IPS panel

## ● Features

- Performance
- Ease of use
- Manageability
- Suitability to task

## Worm / IPS panel

### ● **Intrusion revention techniques**

- **What detection methods are there?**
- **Which ones are the most useful?**
- **How are worms evading detection?**
- **How can we get smarter about worm detection? (or, are we smart enough?)**

# Worm / IPS panel

## ● IPS Architecture

- **What are the performance constraints?**
- **How does IPS fit in at the perimeter?**
- **Where else should I put IPS?**
- **How does it integrate with network devices?**
- **Should we be thinking about multifunction security gateways?**

# *Agree? Disagree?*

**Pete Lindstrom**

**[petelind@spiresecurity.com](mailto:petelind@spiresecurity.com)**

**[www.spiresecurity.com](http://www.spiresecurity.com)**