

# Virus Attacks and Mitigation ISP Review and Action Process

Suresh Ramasamy  
Time dotNet Bhd

ansuresh@net

## Agenda

- Virii History
- Patterns and Trends
- How do we do it?
- Lesson learnt
- Moving forward

ansuresh@net

## Agenda

- **Virii History?**
- Patterns and Trends
- How do we do it?
- Lesson learnt
- Moving forward

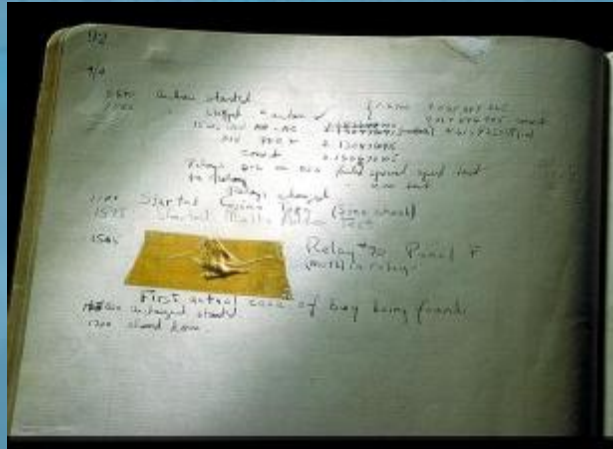
ansuresh.net

## Evolution of Viruses

- Started off as a glitch
- The term bug comes from a moth stuck in the motherboard

ansuresh.net

## Evolution of Viruses – Computer Bug



विकासशील

## Evolution of Viruses

- Good ol' days
  - Simple assembly codes that perform system routines
  - E.g. format hard drive
  - TSR – terminate & stay resident (days of DOS)
  - Marijuana, PingPong
  - Manual propagation

विकासशील

## Evolution of Viruses

- **Viruses attach to executables**
  - Opcode as part of the program, attached to files with .com, .exe
- **Propagation**
  - Infected diskettes
- **Intention?**
  - Malicious
  - Data Corruption

ansuresh.net

## Agenda

- Virii History
- **Patterns and Trends**
- How do we do it?
- Lesson learnt
- Moving forward

ansuresh.net

## Patterns and Trends Current day threat

- **Exploit based viruses**
  - OS vulnerabilities
  - Services vulnerabilities
- **Purpose**
  - Botnet
  - Open Relays
  - Free Distributed Computing based on user gullibility

ansuresh.net

## Patterns and Trends Current day threat

- **Propogation Method**
  - Email
    - Open Relays
    - Address Book harvesting
    - Email sender address spoofing
  - Network (Internet/LAN)
  - Open Network Share

MycERT SIG - July 2004

ansuresh.net

## Patterns and Trends Future?

- Lead time to release is reducing
- 0-day attacks are imminent
- No environment is safe
- Mobility viruses to emerge by the dozens

ansuresh.net

## Patterns and Trends Future?

- Propagation
  - Wifi Peer to peer for insecure clients
  - Bluetooth - bluesnarfing
  - Mobile application viruses
- Vulnerabilities
  - Zero Day viruses
  - Multiple vulnerability viruses
  - Full services suite payloads



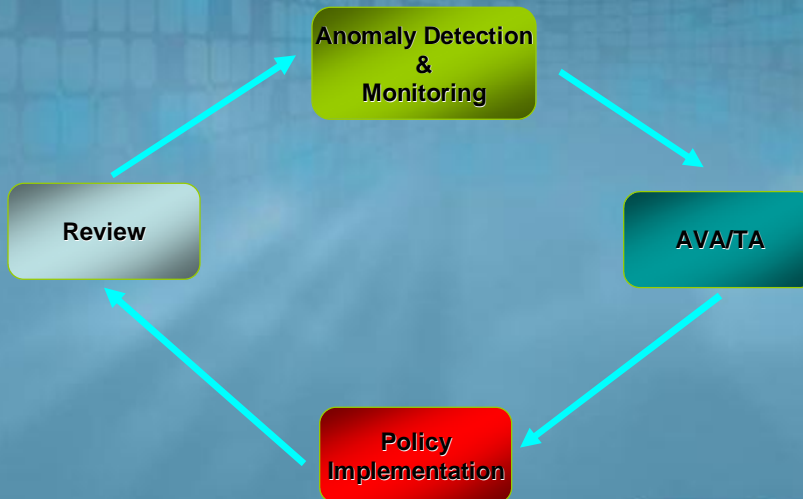
ansuresh.net

## Agenda

- Virii History
- Patterns and Trends
- **How do we do it?**
- Lesson learnt
- Moving forward

ansuresh.net

## General Process Flow



ansuresh.net

## Step 1. Anomaly Detection

- Security admin looks over intrusions
  - Common practice
- Security admin looks over type of traffic
- Determines traffic trends based on application
- Looks after suspicious traffic
  - Check for RFC conformity
  - Checks for unusual pattern

ansuresh.net

## Step 1. Anomaly Detection

- Tools
  - Sniffers
    - Tcpdump (free!)
    - Windump (free!)
  - Correlation
    - MRTG (?)
    - RRDTOol (?)
    - Commercial (I use SQL Server Analysis Services for data warehousing and correlation)

ansuresh.net

## Step 1. Anomaly Detection

- Is it easy?
  - NO!
- Is it automated
  - Not yet
- Is it tedious
  - YES!
- Future tools to support that

ansuresh.net

## Step 1. Monitoring

- Monitoring Security alerts
  - Look at possible traffic pattern
  - Monitor ports/services affected by the vulnerability
- Monitoring Virus Alerts
  - Look at possible traffic pattern
  - Monitor ports/services affected by the vulnerability

ansuresh.net

## Step 2: Attack Vector Analysis/Threat Analysis(AVA/TA)

- **Attack Vector Analysis/Threat Analysis**
  - Gives statistical view of current threats
  - Decision based on netblocks/network owners
  - Currently writing a whitepaper, to be published soon

ansuresh.net

## Step 2: AVA/TA

- **Variables in AVA/TA**
  - Source – where attack is coming from, a particular IP or netblock
  - Domain – Group of IPs belonging to the same owner (can be country or ISP)
  - Global – Your total network
  - Global Descriptor – How you segregate your total network

ansuresh.net

## Step 2: AVA/TA

- **Hostile Domain Percentage**
  - No of Source per domain/Total Clients per domain
- **Attack Percentage Per domain**
  - No attacks per domain/Total domains

ansuresh.net

## Step 2: AVA/TA

- **Sample Report**

ansuresh.net

## Step 3: Policy Implementation

- After AV/TA
  - Decide course of action
    - Notification
    - Warning
    - Blacklist
- Keep logs as proof in case of dispute
  - Document!!!
  - Keep track of cases (provide case number)

ansuresh.net

## Step 4: Review

- Check effectiveness of action taken
- If necessary, revert back to Step 3
- Document all steps for future reference
- Update Case if necessary
- Provide open channel of communications for issues resolution
  
- And it starts back from 1

ansuresh.net

## Agenda

- Virii History
- Patterns and Trends
- How do we do it?
- **Lesson learnt**
- Moving forward

ansuresh.net

## What did we learn?

- How ISPs tackle critical issues
- Same steps can be applied to organizations
- Domain/Global changes, but steps remain the same

ansuresh.net

## Agenda

- Virii History
- Patterns and Trends
- How do we do it?
- Lesson learnt
- **Moving forward**

ansuresh.net

## Moving Forward

- Effective tools are required to get information about network state
- Constant monitoring
- Security is a daily issue, not once in a while
- Proactive > Reactive
  
- Do you want your networks/services to go down?

ansuresh.net

# Questions?

- Offline : [suresh@drsuresh.net](mailto:suresh@drsuresh.net)

drsuresh.net