Network Worm Spread Visualization Tool

Protecting Our Digital World

What is a Network Worm ?

Definition: A standalone, malicious software program that self replicates and spreads autonomously across networks.

Core Function: It exploits security vulnerabilities in one computer, then uses that host to scan for and infect other vulnerable systems.

Key Attribute: Its primary purpose is to propagate itself, often as a payload carrier for other malware (like ransomware, bots).

Worm vs. Virus vs. Trojan Horse

	Worm	Virus	Trojan Horse
Propagation	Self-propagating via networks	Attaches itself to a legitimate program/file	Disguised a s legitimate, useful software
Human Action	Requires **NO** human interaction to spread	Requires a user to **execute the host file** to activate and spread	Requires a user to download **and install/run it**
Target	Exploits system/software vulnerabilities	Infects file on a system	Creates a backdoor, doesn't self-replicate

Real-World Impact

Financial Cost: Billions of dollars in damages annually from:

- Data loss and theft
- Disruption of business operations
- Cost of IT remediation (cleaning systems, patching)
- Lost productivity

Operational Cost: Congestion and collapse of networks (e.g., **SQL Slammer(2003)** brought global banking and airline systems to a halt).

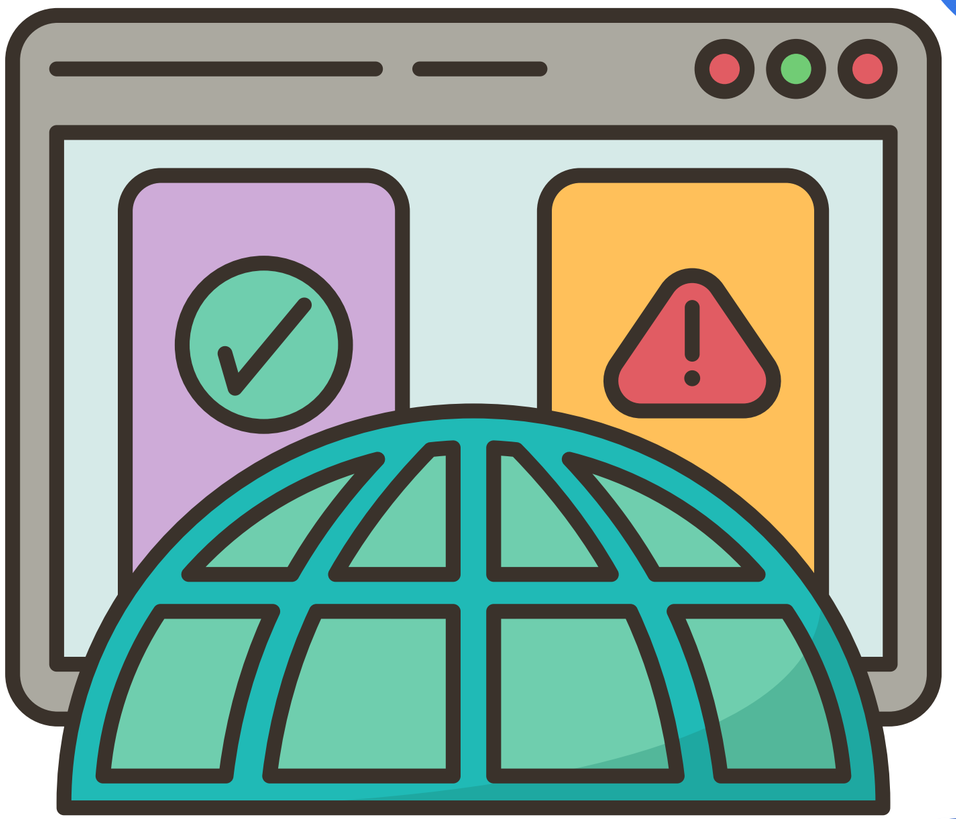
Threat to Critical Infrastructure

Worms do not discriminate—they attack any vulnerable system.

High-Risk Targets:

- **Healthcare Systems:** (e.g., WannaCry(2017) disrupted UK's NHS, canceling surgeries).
- **Energy Grids & Utilities:** Potential for widespread blackouts.
- **Financial Networks:** Trading floors, ATM networks, banking.
- **Transportation Systems:** Air traffic control, railway networks.

The Stakes: This moves the threat beyond financial loss to potential **catastrophic societal disruption and risk to human life.**



Famous Worm Attacks - A Timeline of Disruption

Morris Worm (1988):

The wake-up call. First major worm to gain mainstream attention.

Code Red (2001):

Demonstrated speed and scale on the modern web.

SQL Slammer (2003):

Showcased breathtaking propagation speed.

WannaCry (2017):

A modern, global crisis with tangible human impact.

Morris Worm (1988)

What it did: Exploited vulnerabilities in Unix systems. Not intended to be malicious, but a coding error caused it to overload and crash infected machines.

Impact: Infected ~10% of the early internet (6,000 computers). Led to the creation of the first CERT (Computer Emergency Response Team).

Lesson: Even "experimental" code can cause widespread harm.

Code Red (2001)

What it did: Targeted Microsoft IIS web servers. Defaced websites with "HELLO! Welcome to http://www.worm.com! Hacked By Chinese!".

Impact: Infected over 350,000 servers in days. Caused ~$2.6 billion in damage. Slowed down overall internet traffic.

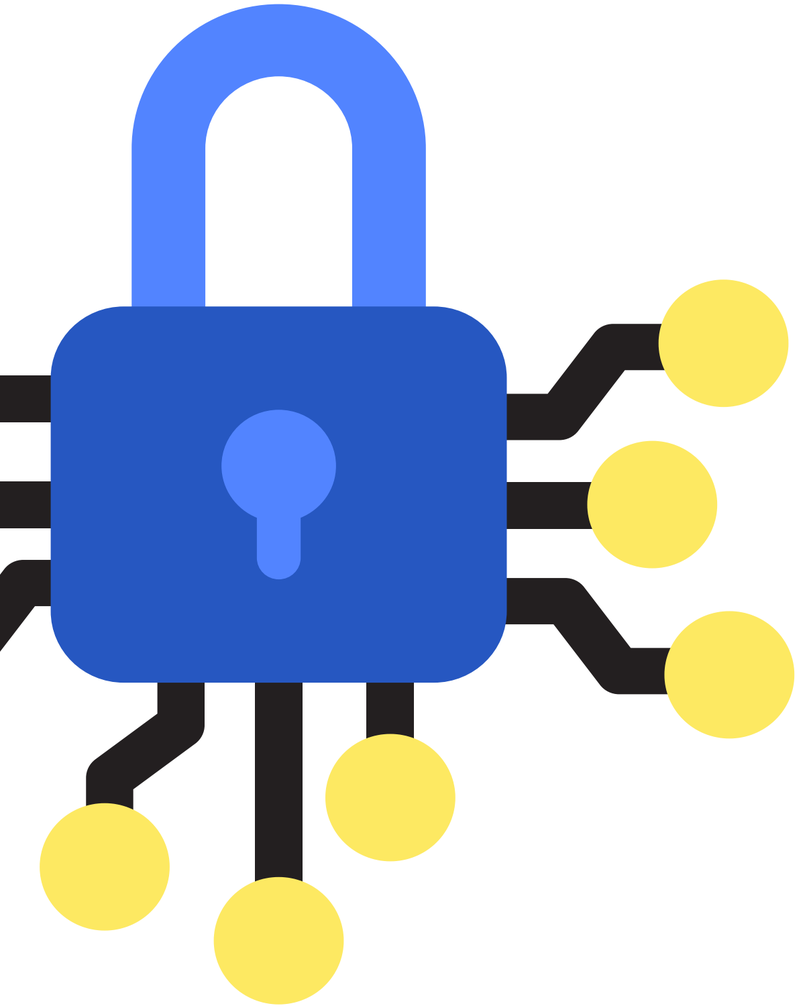
Lesson: Highlighted the speed at which a worm could spread globally.

SQL Slammer (2003)

What it did: Exploited a buffer overflow in Microsoft SQL Server. Its entire code fit in a single 376-byte packet, making it incredibly fast.

Impact: Doubled internet traffic within 10 minutes. Crashed bank ATMs, 911 call centers, and airline check-in systems. Peak infection reached in ~10 minutes.

Lesson: Demonstrated the potential for a "flash worm" to cause near-instant, global infrastructure failure.



WannaCry (2017)

What it was: A **worm** carrying a **ransomware** payload. Used the "EternalBlue" exploit, allegedly developed by the NSA and leaked.

Impact: Infected over 200,000 computers across 150 countries. Crippled the UK's National Health Service (NHS), forcing hospitals to turn away patients. Caused billions in losses.

Lesson: Showed the devastating combo of worm-like propagation with a destructive payload. A stark reminder of the critical importance of patching.

The Worm Lifecycle

Step 1

Propagation

Scans the network for vulnerable targets (random or targeted IPs)

Step 2

Exploitation

Uses a specific vulnerability (in an OS, app, or protocol) to gain access

Step 3

Infection

Transfers its code to the new host.

Step 4

Execution

The worm code runs on the new host

Step 5

Repetition

The new host begins Scanning for its next targets, repeating the cycle

Defense Strategies - The Multi-Layered Approach

Patching & Updates: THE MOST CRITICAL DEFENSE. Fixing vulnerabilities removes the worm's weapon

Network Segmentation: Limits how far a worm can spread internally (e.g., separating guest Wi-Fi from core servers)

Intrusion Detection/Prevention Systems (IDS/IPS): Monitor network traffic for known worm-like scanning patterns or exploit attempts

Firewalls: Block unauthorized access and can restrict unnecessary internal network communication

User Awareness: While worms don't need user action, awareness prevents other malware that might pave the way for worms

The Need for Visualization

- **The Problem:** Worm spread happens in milliseconds across complex networks. Logs and alerts are numerical and abstract.

- **The Solution:** A Network Worm Spread Visualization Tool.

- **What It Does:**

-Maps the propagation in real-time or simulated time.
-Shows infection epicenters and propagation paths.
-Visualizes scan traffic and network congestion.
-Transforms abstract data into an intuitive, spatial understanding of the attack.

- **Value:** Helps researchers understand worm behavior, allows IT teams to see the scope of an outbreak instantly, and is a powerful tool for education and defense planning.

Introducing Our Visualization Tool

- **Objective:** To simulate and visually demonstrate the spread of worms and how it differs when mitigation measures are applied across a network map. This simulation integrates cost modeling at every phase, quantifying the financial impact of both the outbreak and the defensive measures deployed.

- **Key Features:**

-Customizable network topologies.
-Models for different worms, trojan horses, or viruses threats.
-Control over infection and mitigation parameters.
-Visual output showing healthy vs. infected vs. recovered nodes, traffic spikes, and infection timelines.

- **Educational Goal:** To make the invisible threat of a worm outbreak visible, understandable, and memorable.

Network Topologies

Topology	Spread Speed	Infected Pattern	Detection Diffcuty
Ring	Slow	Travels node-by-node in circular path	Easy
Star	Instant	All nodes infected simultaneously through central hub/switch	Easy
Mesh	Very Fast	Explodes through multiple redundant paths simultaneously	Hard
Tree	Fast	Spreads up hierarchy, then cascades down to all branches	Medium

Simulation Performance & Cost Grading

How Did Your Defenses Hold Up? The Bottom Line.

Our tool doesn't just show infection spread; it scores your mitigation strategy based on financial resilience.

Key Takeaway: Effective cybersecurity isn't just about stopping the attack—it's about doing so in a way that is operationally and economically sustainable. This grade reflects that real-world balance.

The Grading Metric: Percentage of Initial Capital Preserved

Grade	Financial Outcome	What It Means for Your Network
A Excellent	>80% Capital Retained	Your defenses were highly efficient. You stopped the worm quickly with minimal disruption and cost-effective measures.
B Good Job	>50% Capital Retained	Your response was effective overall. You contained the outbreak, but some losses from infection or expensive countermeasures were incurred.
C Survived	>0% Capital Retained	You avoided total bankruptcy, but just barely. The worm caused severe damage or your response was extremely costly. A pyrrhic victory.
F Disaster	$0 (Bankruptcy)	The worm propagated unchecked or your mitigation efforts crippled operations. Total financial failure.

Conclusion &Takeaways

- Network worms are a unique, high-speed, high-impact threat.
- Their history shows a trend towards greater speed and more destructive payloads.
- Defense is possible but requires diligence (patching!) and layered security.
- Visualization is a critical tool for comprehension, preparedness, and response, turning complex attack data into actionable insight.

Github Repo

View GitHub Repository

Thank You

Any Questions?