



Worm-Proofing Your Network

QualysGuard On Demand Web Service

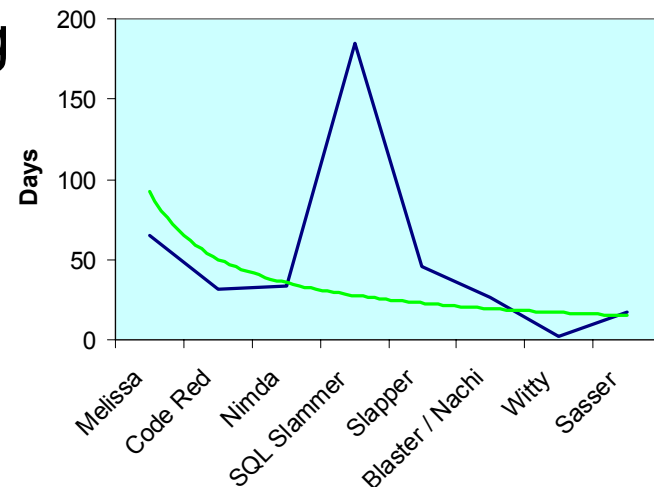


Agenda

1. Today's Worms vs. Yesterday's Worms
2. Why Worms Bypass Today's Defenses
3. Strategy: Focus on the Vulnerability; *NOT* the Worm
4. 4 Steps to Worm-Proofing Your Network
5. How QualysGuard Works: A DEMO
6. A QualysGuard Success Story: DuPont
7. The QualysGuard Difference

Today's Worms vs. Yesterday's Worms

- Time from vulnerability announcement & patch to worm creation & execution is shrinking
 - Slammer: Months
 - Blaster & Sasser: Weeks
 - Witty: Days
- Each new worm is appearing faster and with an increasing number of variants
- Worms are carrying increasingly more deceptive and “heavier” payloads



Why Worms Bypass Today's Defenses

- Weakening & expanding network perimeters
- Inefficient or incomplete assessment processes
- Information overload
- Lack of resources (people and funds)
- Lack of knowledge / expertise

Yesterday's Security Solutions Will Not Protect You From Today's Worms

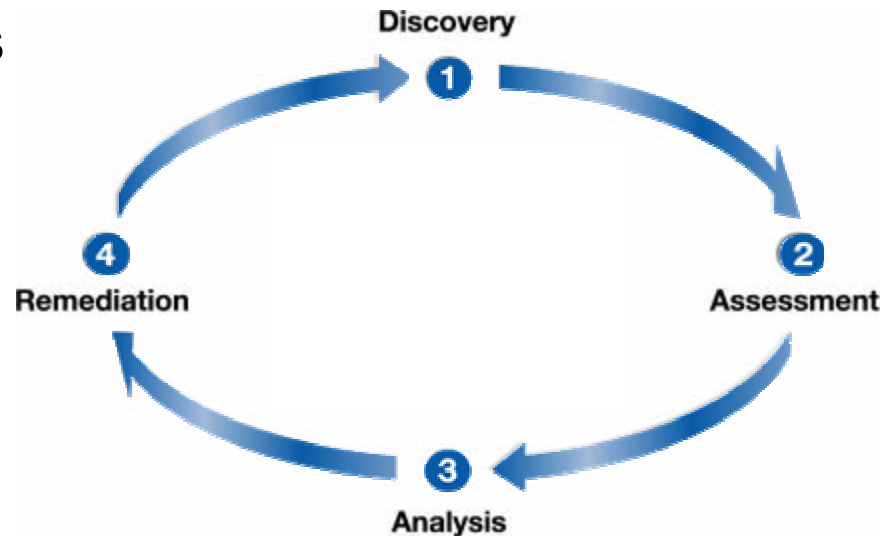
- Antivirus, IDS, and Firewalls are not enough
 - AV agents must be installed and active on every host
 - Problem: Worms can disable AV services
 - Problem: Rogue devices & non-company devices
 - Problem: Devices not in compliance with standards
 - IDS requires manual 'care & feeding'
 - IDS signatures will only find the worm after it is too late
 - Failure to update IDS signatures ⇒ IDS won't find worm at all
 - Worms are permeating network and host FWs
 - Worms often come as email attachments, not stopped by FWs
 - FW configurations are not audited frequently enough

Strategy: Fight the Vulnerability, NOT the Worm

- Worms can only infect vulnerable systems
- Most organizations react to worms 'after the fact'
- Instead – fix the vulnerability before the problem arises. Be proactive, not reactive.
 - How?
 - Know your resources
 - Manage your processes
 - Identify vulnerable systems before they become infected
 - AUTOMATE

4 Steps to “Worm-proofing” Your Network

- Worm-proofing your network can be as easy as:
 1. Proactively discover devices on your networks
 2. Regularly scan / assess your devices
 3. Analyze the results & prioritize mitigation activities
 4. Manage the vulnerability remediation process



QualysGuard® Demo

QUALYS GUARD

Home Download Quick Help

Technical Report

Summary of Vulnerabilities 10/06/2003

Vulnerabilities Total		Overall Trend:		Security Risk	
156		+ 14		5.0	

by Status	Vulnerabilities	by Severity			5 Biggest Categories		
		Severity	Vulnerabilities	Trend	Category	Vulnerabilities	Trend
New	7	8	36	+6	Web server	27	+4
Active	145	4	23	+1	General remote services	28	+4
Re-Opened	8	3	40	+2	RFC	25	+1
Fixed	5	2	30	+2	Information gathering	24	+1
Changed	8	1	60	+3	TCP/IP	22	-3

Vulnerabilities

- MS-SQL 8.0 UDP Stammer Worm Buffer Overflow Vulnerability (1)

QID: 10010 Category: Database CVE ID: CVE-2002-0606

DESCRIPTION
 Your MS-SQL 8.0 server is NOT patched for the stammer worm buffer overflow vulnerability. This vulnerability allows for the execution of arbitrary code on the SQL Server computer due to a stack buffer overflow. Once the worm compromises a machine, it will try to propagate itself. The worm will craft packets of 276 bytes and send them to randomly chosen IP addresses on port 1434/tcp. If the packet is sent to a vulnerable machine, this machine will become infected and will also begin to propagate. Previous the scanning activity for new hosts, the correct value of this worm has no other packet.

Activity of this worm is readily identifiable on a network by the presence of 276-byte UDP packets. These packets appear to be originating from seemingly random IP addresses and destined for port 1434/tcp.

CONSEQUENCES:
 Compromise by the worm confirms that a system is vulnerable to allowing a remote attacker to execute arbitrary code as the local SYSTEM user. Subsequently, it's possible for the attacker to leverage a local privilege escalation exploit in order to gain Administrator access to the vulnerable system.

The high volume of 1434/tcp traffic generated by hosts infected with the worm trying to find and compromise other SQL Server computers may itself lead to performance issues (including possible denial-of-service conditions) for Internet-connected hosts or for those computers on networks with compromised hosts.

SOLUTION:
 Microsoft has released patches to address this vulnerability. Check Microsoft's Security Site for updates.

- Microsoft IE 4.0SP 0 File Permission Canonicalization Vulnerability (1)
- Microsoft IE 4.0SP 0 Extended UNICODE Remote Execution Vulnerability (1)
- Microsoft IE 5.0SP 2 Directory Traversal and Remote Command Execution Vulnerability (1)
- Microsoft Windows 2000 IS WmiDav Buffer Overflow Vulnerability (1)
- Microsoft Windows Media Services NSISlog.dll Remote Buffer Overflow Vulnerability (1)
- SSL Server Has SSL2 Enabled Vulnerability (1)
- Remote Windows User List Disclosure Vulnerability (1)
- Microsoft IE Malformed HTTP Request Buffer Overflow Vulnerability (1)

QUALYS GUARD

Home Download Quick Help

Executive Report

Summary of Vulnerabilities 10/06/2003

Vulnerabilities Total		Overall Trend:		Security Risk	
68		- 2		4.0	

by Status	Vulnerabilities	by Severity			5 Biggest Categories		
		Severity	Vulnerabilities	Trend	Category	Vulnerabilities	Trend
New	0	5	10	0	General remote services	14	+1
Active	60	4	6	0	Web server	12	0
Re-Opened	0	3	27	-2	CGA	0	0
Fixed	4	3	56	0	RFC	7	0
Changed	4	1	9	0	TCP/IP	6	-2

Number of Vulnerabilities by Severity

Severity	Count
Severity 5	8
Severity 4	6
Severity 3	2
Severity 2	10
Severity 1	14

Your network had:

- 14 Severity 5 (Critical)
- 6 Severity 4 (Critical)
- 27 Severity 3 (Serious)
- 16 Severity 2 (Medium)
- 9 Severity 1 (Minor)

Total: 68

Vulnerabilities by Severity over Time

Severity:

- Severity 5 (Critical)
- Severity 4 (Critical)
- Severity 3 (Serious)
- Severity 2 (Medium)
- Severity 1 (Minor)

DuPont Case Study: The Need

- Implement a Vulnerability Management solution across a large enterprise that is globally dispersed
- Utilize the same solution across segmented, firewalled networks
- Provide “independently gathered” metric-rich detailed and management level reports
- Integrate the vulnerability management process
- The solution needs to be: comprehensive, accurate, auto-updating, non-harmful to systems and networks, deployed quickly, easy to use...

DuPont: The Objectives

Business objectives:

- Use a service versus build and run internally
- Don't buy software & hardware. Avoid capital expenditure
- Low TCO; avoid support, maintenance & misc costs.
- Proactively prevent worm exposures by eliminating vulnerabilities

Functional objectives:

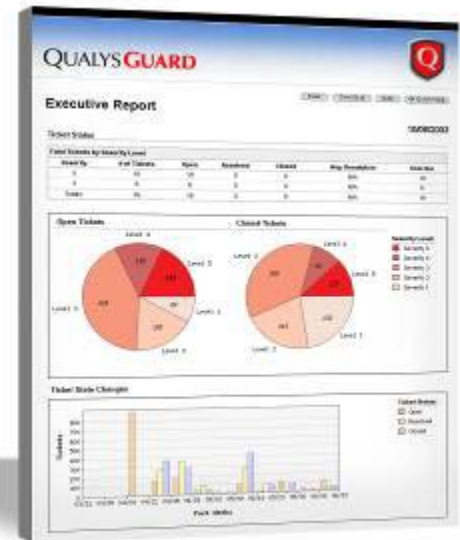
- Deploy a comprehensive VM solution across the enterprise
- Implement a “closed loop” approach (finding to fixing)
- Replace Security Team's tool kit

DuPont: The Results

- Globally deployed QualysGuard in weeks
 - Started scanning perimeter immediately
 - Installed 37 scanner appliances
- Initiated weekly and monthly scanning across the enterprise
- Built 75+ unique groups of assets for scanning, reporting and remediation
- First baseline scan ~60,000 devices
- Went from reacting to preventing worm outbreaks
 - Zero impact from Sasser

The QualysGuard[®] Difference

- Industry's most accurate & comprehensive solution
- On Demand & Always Up to Date
- Immediately deployable with no software to install
- 'Out of the box' interoperability
- Built in vulnerability remediation workflow



Next Steps

- Visit us on the web at <http://www.qualys.com/wormproof>
- Try it!...free full feature product trial
- Contact us at wormproof@qualys.com