**Viruses and Antiviruses Team Research Project**

Ryan Nkansah, William Fan, Sidnye King, Danielle Santos Almeida

Montgomery College

NWIT 245 - Defending The Network

Prof. Lemma

8/9/25

**Introduction**

As we rely more on technology, the risks to our digital security increase. Out of the countless ways one can be hacked, a computer virus is one of the most harmful. In this project, we summarize possibly the three most infamous viruses in history: Blaster, Slammer, and MyDoom, as well as provide a comparison of two of the most popular antiviruses, Malwarebytes and Panda Antivirus. By looking into these viruses of how they operated, how they were neutralized, and their impact, it's easier for future cyber professionals to understand how to prevent future cyber attacks. We will also compare two antivirus tools, Malwarebytes and Panda Antivirus, to evaluate their attributes and effectiveness.

**Blaster**

First detected in August 2003, the Blaster virus, also known as Lovsan or MSBlast, was a fast-spreading worm that wreaked havoc on Windows XP and 2000 systems. It took advantage of a flaw in Microsoft’s Remote Procedure Call (RPC) service, allowing the virus to infiltrate systems without any user interaction (CERT Coordination Center). Once inside, Blaster caused computers to crash or reboot repeatedly and even attempted a denial-of-service attack on Microsoft’s own update servers. It spread by scanning networks for machines with the same unpatched vulnerability, exploiting the flaw to install itself, and then using each new victim to find more targets. Blaster became infamous not just for the damage it caused, which is estimated in the hundreds of millions of dollars, but also for its taunting message aimed at Bill Gates, suggesting the hacker’s grudge against Microsoft (Lemos). The exploited vulnerability was later documented as CVE-2003-0352. Defending against Blaster involved installing Microsoft’s patch, enabling firewalls to block malicious traffic, disabling unnecessary services, and keeping antivirus tools updated to detect and remove the worm (Symantec Security Response).

**Slammer** The SQL Slammer worm, also known as Sapphire, was a significant incident that lasted primarily from January 25th to 27th, 2003, with some lingering effects until 2017. It exploited a known buffer overflow vulnerability in Microsoft SQL Servers. The worm was initially scripted by researcher David Litchfield in 2002 and later self-replicated accidentally six months later. It primarily affected Windows XP and SQL Server systems. The worm, a 376-byte packet spreading via UDP port 1434, doubled every 8.5 seconds, performed 55 million scans per second, and infected 75,000 SQL servers worldwide, making it the fastest-spreading worm in recorded history. It significantly slowed global internet traffic and overwhelmed stateful firewalls (NetScout). Its mechanism involved: 1) posing as a harmless UDP packet, requesting an online database with a name containing run-on bytes to cause a memory leak; 2) reprogramming the infected machine to send UDP requests by overwriting its stack with new instructions; 3) randomly selecting victims by generating random IP addresses; 4) replicating by copying the packet; and 5) repeating the process to infect other computers. This allowed it to spread uncontrollably within minutes, especially across unpatched servers directly connected to the internet. Corporate data centers were heavily impacted due to their powerful machines launching tens of thousands of copies per second. The response was swift, with Arbor Sightline quickly identifying the harmful traffic and filtering UDP port 1434 to mitigate the spread (SecureWorks). This process was later documented in CVE-2002-0649. Another solution was simply blocking port 1434, as the worm relied solely on this port. Additional defense measures included applying Microsoft’s security patch released six months before the outbreak, segmenting networks to limit exposure, and using intrusion detection systems to spot abnormal scanning patterns. The worm’s impact lasted hours, with stability restored as filters were deployed. In conclusion, SQL Slammer exposed critical weaknesses in patch management and network security, prompting improved practices. Though its activity has faded, its legacy underscores the need for robust cybersecurity.

**MyDoom**

MyDoom, discovered in January 2004, is known as one of the fastest spreading email worms ever discovered. It mainly spread to victims through emails by disguising itself as a harmless attachment, like the viral “Rick Roll” meme. MyDoom infected computers by tricking users into opening an attachment, and then it would send itself to contacts in the victim's email, secretly open a backdoor in the infected computer, and finally it would use the infected computer to launch DDOS attacks (Okta). Once installed, it replicated rapidly by harvesting email addresses from the infected system and sending itself out, which allowed it to spread globally in just hours. This virus caused an estimated $38 billion in damage, through its slow downs in internet traffic, productivity loss, and more (“What Is…”). In order to prevent and mitigate this attack, be wary of unknown email attachments, keep your antivirus updated, block affected ports, such as 3127 on your machine, and lastly use email filters and firewalls ("MyDoom…”). Additional defenses include user awareness training to avoid phishing tactics and disabling unnecessary services that could be exploited by the worm’s backdoor. Interestingly, there is no CVE for this attack, because MyDoom relied on social engineering, not exploiting a vulnerability in the computer.

**Malwarebytes vs Panda Antivirus**

Antivirus is often the first line of defense against viruses, offering malware detection and basic firewalls at the very least. There are a multitude of antivirus solutions available to casual internet users and enterprises alike. This table compares two well-known antivirus solutions, Malwarebytes and Panda Antivirus.

**Malwarebytes vs Panda Antivirus Table**

| **Vendor** | **Cost** | **Support** | **Features** | **Pros/Cons** | **Company Reputation** |
| --- | --- | --- | --- | --- | --- |
| MalwareBytes | Free (but offers paid tiers)   * Standard: $49.99/yr * Plus: $59.99/yr * Ultimate: $199.99/yr | * 24/7 AI Chatbot * Phone & Email | * Manual Scanning Tool for Windows, Android, Mac, and iOS devices * BrowserGuard Extension   Use Case: Secondary Scanner  Scanning Type: Signature-based | * Strong malware removal tool * Minimum system impact * Does not offer real-time protection | Strong |
| Panda Antivirus | Free (but offers paid tiers)   * Essential: $49.99/yr * Advanced: $59.99/yr * Complete: $89.99/yr * Premium: $139.99/yr | * 24/7 Tech Support * Community Forums | * Real-time Antivirus for Windows and Android Devices * VPN (150 MB/day)   Use Case: Primary Antivirus for Casual Users  Scanning Type: Behavioral-based (AI and ML) | * Offloads processing to the cloud * Frequent Ads and Pop-ups (Bloatware) * Customer Service is slow / unresponsive for the free tier | Mixed |

Source: Data from [Malwarebytes (“Free Antivirus")](https://www.malwarebytes.com/solutions/free-antivirus); [Malwarebytes (“Pricing and Plans")](http://www.malwarebytes.com/pricing); [Panda ("Download Panda Dome")](https://www.pandasecurity.com/en/homeusers/downloads/); [Panda ("Free Antivirus for...")](http://www.pandasecurity.com/en/homeusers/free-antivirus/)

Like most home-user antiviruses, MalwareBytes and Panda Antivirus are both affordable, contain user-friendly interfaces, and utilize strong virus scanning. Both vendors offer free versions with limited features, however, MalwareBytes is generally considered a better option due to its support and company reputation. Panda’s Free Antivirus is known for its aggressive advertising for its paid tiers, and has been scrutinized in the past for collecting user data. Users who value privacy should consider MalwareBytes over Panda Antivirus.

**Conclusion**

It is only inevitable that users on the internet will encounter malware at one point in time – the consequences will depend on one’s preparedness. Computer viruses like Blaster, Slammer, and MyDoom, the impact of which can range from trivial annoying pop-ups to billions of dollars in damage, are notable examples of why internet users must prioritize the security of their online devices. Security training such as regularly patching and hardening devices, as well as using antivirus software that offer virus scanning, virus removal, and browser protection, like Malwarebytes and Panda Antivirus, provide protection and defense against viruses. Ultimately, staying informed, practicing safe online habits, and using layered security measures is the most effective way to reduce risks and keep systems secure.

**Works Cited**

CERT Coordination Center. *CERT Advisory CA-2003-20 W32/Blaster Worm*. Carnegie Mellon University, 11 Aug. 2003, <https://www.cert.org/advisories/CA-2003-20.html>.

“Download Panda Dome.” Pandasecurity.com, 2025, [www.pandasecurity.com/en/homeusers/downloads/](http://www.pandasecurity.com/en/homeusers/downloads/).

“Free Antivirus.” *Malwarebytes*, 29 Jan. 2025, [www.malwarebytes.com/solutions/free-antivirus](http://www.malwarebytes.com/solutions/free-antivirus).

“Free Antivirus for Windows and Android.” Pandasecurity.com, 2025, [www.pandasecurity.com/en/homeusers/free-antivirus/](http://www.pandasecurity.com/en/homeusers/free-antivirus/).

Lemos, Robert. “Blaster Worm Begins Its Attack.” *CNET News*, 12 Aug. 2003, <https://www.cnet.com/news/security/blaster-worm-begins-its-attack/>.

“Pricing and Plans.” Malwarebytes, 31 July 2025, [www.malwarebytes.com/pricing](http://www.malwarebytes.com/pricing).

Symantec Security Response. “W32.Blaster.Worm.” *Symantec*, 11 Aug. 2003, <https://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html>.

NetScout. “The Sapphire Worm.” *NetScout Systems*, <https://www.netscout.com/blog/asert/sapphire-worm>.

“What Is the MyDoom Virus?” \*Corero Network Security\*, 18 Dec. 2024, <https://www.corero.com/what-is-mydoom-virus/>

Okta. “What Is MyDoom Malware? History, How It Works & Defense.” *Identity 101*, 21 Oct. 2024, Okta, [www.okta.com/identity-101/mydoom](http://www.okta.com/identity-101/mydoom/)/

"MyDoom — also known as 'Novarg'." \*DDoSPedia\*, Radware, n.d.,

<https://www.radware.com/security/ddos-knowledge-center/ddospedia/mydoom/>

Slammer - “SQL Slammer – 10 Years Later.” Secureworks, 2 Aug. 2013,

[www.secureworks.com/blog/general-sql-slammer-10-years-later](http://www.secureworks.com/blog/general-sql-slammer-10-years-later).

Slammer - “What Is SQL Slammer Virus?” GeeksforGeeks, 23 Jul. 2025, [www.geeksforgeeks.org/ethical-hacking/what-is-sql-slammer-virus/](http://www.geeksforgeeks.org/ethical-hacking/what-is-sql-slammer-virus/).

Slammer - “Remembering SQL Slammer.” NETSCOUT, 27 Jan. 2023, [www.netscout.com/blog/asert/remembering-sql-slammer](http://www.netscout.com/blog/asert/remembering-sql-slammer).‌