

MyDoom

Executive Summary

MyDoom, a notorious virus/worm first identified in 2004, spreads via email attachments and peer-to-peer networks like Kazaa, leveraging social engineering to infect over 500,000 computers in a single week, causing an estimated \$38.5 billion in damages. Originating possibly from Russia (though unconfirmed), it creates zombie networks for distributed denial-of-service (DDoS) attacks, initially targeting the SCO Group and later Microsoft, blocking access to 65 antivirus websites to hinder cleanup. Its payloads include a backdoor on TCP port 3127 for remote attacker access and coordinated DDoS attacks, with later variants disrupting major internet companies like Google and government organizations in the United States and South Korea. Despite speculation of motives tied to SCO's Linux litigation, no evidence supports this, and attribution remains unclear, potentially linked to organized cybercrime or, with low confidence, North Korean actors. As of 2025, MyDoom's threat level is negligible due to Microsoft's signature-based detection patches, widespread antivirus gateways blocking malicious attachments, evolved Windows architectures rendering the malware obsolete, and ISP-level controls like blacklisting and spam filtering. Mitigation strategies include gateway-level antivirus, updated endpoint detection, and user security training, while remediation involves quarantining executables, cleaning registry entries, disabling P2P software, and applying security patches.

Threat Profile

MyDoom, aka Novarg, was first discovered in the wild in 2004 and is a virus/worm that spreads through email attachments and the Kazaa peer-to-peer network. It is one of, if not the first, instances of social engineering creating massive fallout. Its intent is to create zombies out of each computer it infects in order to execute DDoS attacks. There is suspicion that it is Russian due to its similarity to other worms but this has never been verified. It is notorious for having infected over 500,000 computers worldwide in one week and caused an estimated \$38.5B in damages. The first version used infected computers to DDoS the SCO Group with homepage requests to crash the site. After an hour the company changed their homepage website to get back online. The second version of the worm targeted Microsoft's website and then prevented access to 65 antivirus websites to prevent the ability for people to cleanup their machines. Eventually, other variations of MyDoom were created and spread that affected Google, AltaVista, Lycos and other companies and government organizations in the United States and South Korea.

Technical Analysis

MyDoom has two main payloads:

- 1) A backdoor on TCP port 3127 granting remote access for attackers.
- 2) The DDoS attack orchestrated across the zombie machines it infects.
- 3) (Second version) added the blocking of antivirus websites to hinder cleanup.

The payload is delivered via phishing, posing as a transmission error email with attachment. After a victim opens the email attachment, the code moves into the Windows environment by creating a "taskmon.exe" in the Windows System folder, a registry event to launch at every startup (persistence) and a mutex to make sure only one instance runs per computer. Only Windows was susceptible to this. The code finds stored contacts and creates a new virus for each contact in the form of an email attachment which it then sends out to each contact through an SMTP engine. On a set date, infected computers launch DDoS.

Target Analysis

There were two main targets of the initial MyDoom campaigns:

- 1) SCO Group
- 2) Microsoft

Beyond those, other major internet companies and government organizations in the United States and Korea were targeted with similar worms that disrupted operations. Despite rumors that the initial attack on SCO was due to their litigation against Linux, no evidence was found to corroborate the allegation and that motivation was ultimately dismissed. The rest of the targets are simply large internet businesses and government websites that heavily rely on their web properties where DDoS attacks can have a major impact.

Attribution

The initial MyDoom attacks were unattributed although some people believed it was Linux users who were upset with SCO Group for their litigation against Linux. These accusations were proven to be unfounded. Ultimately, there has been no true attribution of the original MyDoom, likely done by organized cybercrime groups seeking disruption or extortion leverage. The attacks on the United States and South Korea point to possible North Korean aggression but that is a low confidence assumption.

Current Threat Level

Current threat level is very low to non-existent. The last sighting of MyDoom is from 2019 making it most likely inactive as of 2025. There are several reasons it poses virtually no risk now:

- 1) After the first attack in 2004, Microsoft issued signature-based detection updates and system patches to combat it.
- 2) Because MyDoom relied on unaware email users opening attachments, the deployment of gateway-level antivirus and firewalls by email clients also stopped MyDoom-style attacks before they could gain a foothold from an unsuspecting user.
- 3) It required manual execution, companies and email services began warning users about executing email attachments and warning them of the risks.
- 4) It was developed for early 2000s Windows and the Windows architecture is now much different rendering the malware non-functional on the majority of machines.

5) By mid-2004, ISPs began blacklisting infected IP ranges and blocking mass-mailing worms by detecting unusual SMTP volume from across consumer networks. Coupled with rate-limiting and spam filtering algos, MyDoom couldn't propagate the way it was designed to.

Mitigation and Remediations

There are several industry-level mitigations that were deployed and remediations that were done to combat MyDoom.

Mitigations:

- 1) Email providers applying antivirus to the gateway level to stop malicious executable attachments before they reach an unsuspecting user.
 - a) These blocked .exe, .zip and .scr attachments.
- 2) Updating EDRs and Antivirus/malware protection software to the most recent patch to ensure proper protection from malicious signatures.
- 3) Security awareness training for users and businesses

Remediations:

- 1) Quarantine infected executables
- 2) Clean up registry entries and startup events
- 3) Disable P2P software
- 4) Ensure machines have latest security patches