PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

Ferhat Abbas University Setif 1

Faculty of Sciences

IT Department

Cyber Security

Module: DMSS

Title

MyDoom Malware

realized by:

- ***Bouzidi Aymene***
- ***Yessad Djaafar***

Supervised by:

Mme. ALIOUAT

Academic year: 2023/2024

Table of Contents

Table of Figures

Introduction

Some people call MyDoom a virus. Some people call it a worm. Some people spell the term My Doom. Others just call it the Doom Virus.

No matter what you call it or how you spell it, MyDoom is serious. This tiny bit of code spreads over a million computers. If you get these messages and open their files, the program sits on your computer. Soon, everyone in your address book gets a message from your computer.

People became aware of MyDoom in 2004, and the attacks launched then have long since passed. But plenty of infected computers remain. So, it’s wise to know how this worm works and how you can rid your computer of the code.

Definitions

1. Malware Definition

Before delving into MyDoom, it's crucial to grasp the concept of malware, which encompasses various types of software designed to damage, disrupt, or gain unauthorized access to computer systems. MyDoom falls under the category of a computer worm.

2. Worm Definition

A worm is a self-replicating computer program that can spread across computer networks and systems without needing to attach itself to other files or programs. Worms can cause harm, transmit themselves to other devices, and often carry out malicious actions on the computers they infect.

3. MyDoom Definition

MyDoom is a computer worm affecting Windows devices. It’s considered to be one of the fastest-spreading malicious types of software in history and has infected millions of computers worldwide since its launch in 2004. Several security firms expressed their belief that the worm originated from a programmer in Russia. The actual author of the worm is unknown.

Propagation

The user spot a unique email amongst the typical spam, or family member, the emails message generally varies on "Message could not be displayed, check the attachment for your message" and, of course, the attachment is an .exe file or a .tiff or .bat or a .scr which contains the email worm.

Most people don't open the email and assume it's a spam. However a few handful of people do open the email, and download the attached file, then run it that's all it will take to unleash the most successful computer worm in history, the worm immediately drops two files into system32 directory the first one is "shimgapi.dll" which acts as a backdoor which allows unauthorized access while the other is "taskmon.exe" which is the worm itself, then scans the address book of the infected machine then the worm emails itself to every single contact in the user's address book this generates a new wave of infected emails only this time coming from familiar and safe email addresses to hundreds of people, those hundreds open their infected emails from a trusted source, immediately infecting their own computers once more MyDoom scans their address books and emails itself to every contact on it within the span of an hour a single infected user has successfully spread the infection to thousands of other users.

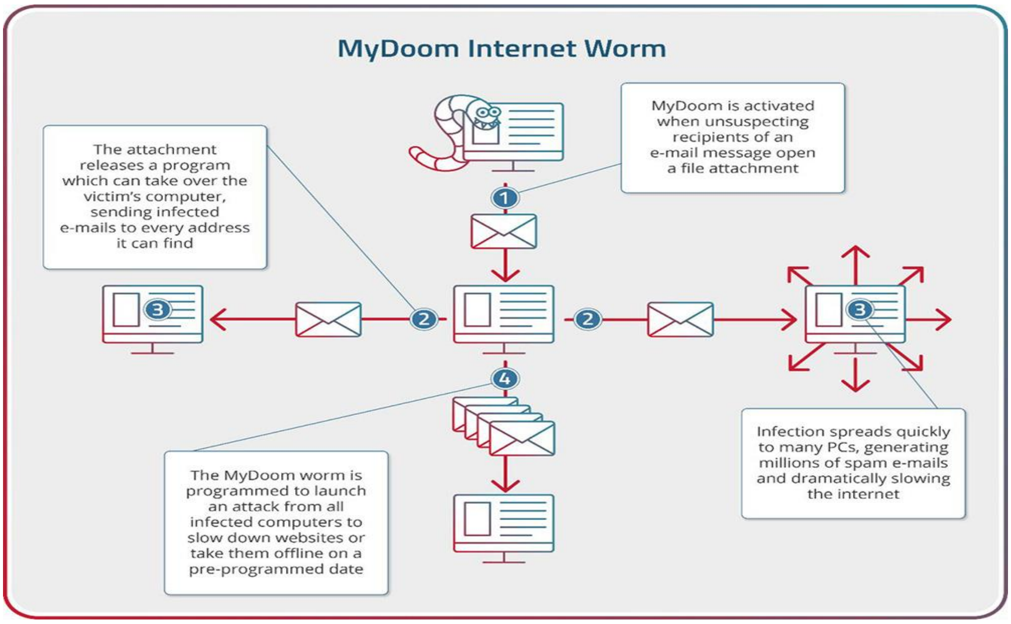

MyDoom Internet Worm
MyDoom is activated when unsuspecting recipients of an e-mail message open a file attachment
The attachment releases a program which can take over the victim's computer, sending infected e-mails to every address it can find
1
2
2
3
3
4
Infection spreads quickly to many PCs, generating millions of spam e-mails and dramatically slowing the internet
The MyDoom worm is programmed to launch an attack from all infected computers to slow down websites or take them offline on a pre-programmed date

image 1 MyDoom propagation

Targets & Damages

MyDoom is a very effective worm made to create zombies out of hundreds of thousands of Windows computers. Hackers could then use each hijacked terminal to wage a Denial of Service (DoS) attack toward a company they identified.

Experts agreed that MyDoom was dangerous. Reporters said the code was:

- **Fast.** No other virus had spread so quickly.
- **Effective.** MyDoom infected more than 500,000 machines in just one week.
- **Expensive.** Damage estimates reached $38.5 billion or more.

The worm infected many computers, and most discussions were about removing it. However, two companies suffered the most.

The first version (MyDoom.A) of the worm used infected computers to bombard SCO Group with homepage requests. The company couldn't handle that kind of traffic, and the site crashed. After an hour of constant attack, the company changed website addresses altogether.

The second version (MyDoom.B) of the worm did two things:

- **Attack:** Infected computers bombarded Microsoft's website.
- **Protect:** After the infection, computers couldn't access 65 antivirus websites. In essence, the worm kept people from cleaning up their computers.

Before hackers released MyDoom, experts knew that an attack like this was possible. But they had no idea what it would look like, how it would work, or how users could clean up their computers. They would learn all about these attacks in the coming months.

Tech industry leaders like Microsoft offered a $250,000 bounty to anyone who could track down the attackers. When the culprits remained elusive, Microsoft doubled the reward to $500,000.

The spread of Mydoom continued and finally hit its peak on 28th January 2004, when it was apparently responsible **one in ten** emails containing the virus *on the planet* that day.

As time went on following the first outbreak of the Mydoom, several more attacks took place – all using variations of the original Mydoom worm such as C, F, G/H, U, V, W, X were spotted in the wild later, but none achieved the notoriety of the A variant.

In July 2004, a variant targeted Google, Lycos, and AltaVista and it was largely successful. Though early days for the search engine, Mydoom managed to take down Google for almost an entire day, something that would be unthinkable today.

As for where Mydoom is today, interestingly, there is still a level of circulation of those same infected emails from back in 2004. In 2019, analysis by Unit 42 showed that 1.1% of all email traffic with malware attachments were still Mydoom related. For such an old virus, that’s actually somewhat impressive but it also means there are some people out there still falling for the oldest trick in the email malware book.

The end of the beginning

Of course, nothing lasts forever, so how did the initial spread of Mydoom actually end?

Well, in a way, Mydoom was the architect of its own downfall or, at least, the B-variant was. You see, MydoomB had certain coding errors within it which prevented it from spreading as quickly as the initial version had done. This meant that, when it attempted the DDoS attack on Microsoft on 3rd February 2004, the botnet wasn't actually big enough to take down their sites once this attack had failed, it seemed that the Mydoom incident was essentially over. In fact, it was *programmed* to be over.

On 12th February 2004, Mydoom.A stopped spreading.
On 1st March 2004, Mydoom.B stopped spreading.

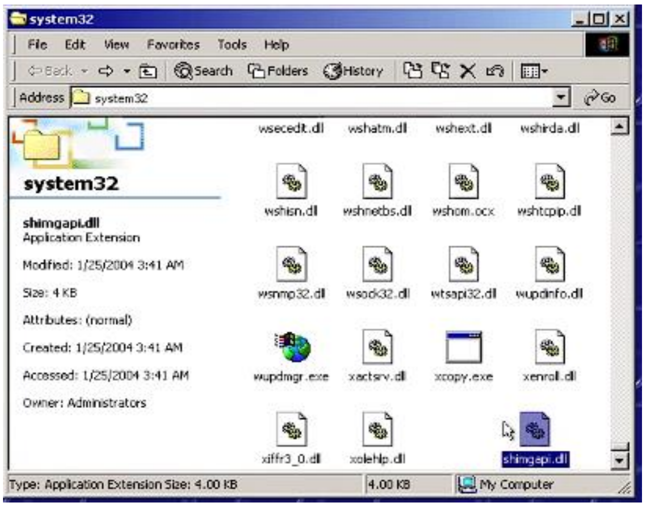
Importantly, any computer which had been infected was *still* infected, meaning any backdoors created by this malware were essentially still wide open.

It wouldn't take much for others to pick up the mantle of Mydoom and continue its nefarious strategy, and around this time Microsoft suffered *another* DDoS attack powered by the same botnet and referred to as "Doomjuice". Luckily, once again, this attack failed to penetrate Microsoft's cyber defenses.

Detection and Elimination

If you believe that you have been infected by MyDoom, seek out the problem and remove it by:

- **Deleting the two files (shimgapi.dll, taskmon.exe):** that are typically stored in: C:\windows\system32 for Windows XP, C:\winnt\system32 for NT/2000, or C:\windows\system for Windows 9x/Me.



system32

shimgapi.dll
Application Extension

Modified: 1/25/2004 3:41 AM

Size: 4 KB

Attributes: (normal)

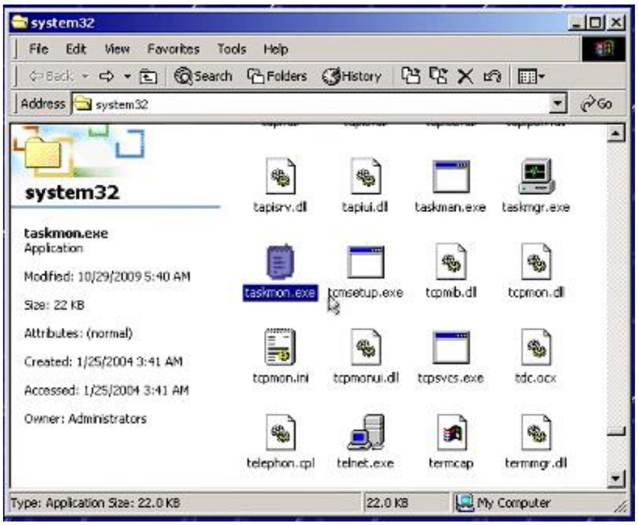
Created: 1/25/2004 3:41 AM

Accessed: 1/25/2004 3:41 AM

Owner: Administrators

Type: Application Extension Size: 4.00 KB | 4.00 KB

image 3 shimgapi.dll



system32

taskmon.exe
Application

Modified: 10/29/2009 5:40 AM

Size: 22 KB

Attributes: (normal)

Created: 1/25/2004 3:41 AM

Accessed: 1/25/2004 3:41 AM

Owner: Administrators

Type: Application Size: 22.0 KB | 22.0 KB

image 2 taskmon.exe

- **Updating Windows:** The worm can only infect computers running Windows, if you're not running the last version of Windows, amend that now.
- **Running antivirus software:** Download the latest patch so your antivirus software works against the latest threats. Then, run a complete clean of your system.
- **Checking:** Reach out to people in your contacts, and ask them if you're sending them suspicious notes. Then, head to common antivirus websites and see if you can load the page.

Prevention

- **Don’t open malicious attachments:** Always closely inspect every email you receive, and never open an attachment unless you are 100% sure it’s legitimate. If you can’t tell if an email is safe, verify it with the sender.
- **Update your Windows:** Running your computer on outdated windows is a bad idea, so always update your software on time. This will keep viruses away and mitigate the risk of your computer getting infected.
- **Install antivirus:** While Windows machines have a native antivirus installed, you can also get third-party software to enhance your security.
- **Block ports:** Since MyDoom targets specific TCP ports, you can block them and avoid trouble.

If you work on security for a large company, ensure that all of your employees know these same rules. Encourage them to send you anything they think is suspicious, so you can check it for them.

MyDoom timeline

Here's how it went down from then on.

- **January 26, 2004.** MyDoom is spotted. By lunchtime in America, the virus has spread globally, with **one in ten emails containing the virus**. Global Internet speeds slow down by **10 percent**.
- **January 27.** The FBI and Secret Service begin to investigate the origins of the worm. A **$250,000 reward** is offered for info leading to the arrest of MyDoom's developer.
- **January 28.** The second version of the worm, **MyDoom.B**, begins to spread. **Half of all email traffic in the world contains the virus**. The virus blocks access to over sixty Internet security companies. The financial impact climbs, both from lost revenue and increased technical assistance for users.
- **January 29.** Microsoft raises a previous bounty and offers **$500,000** for catching MyDoom's creators.
- **February 1.** A massive distributed denial-of-service (DDoS) attack against the SCO Group is launched. Over 1 million computers are unleashed in a botnet built by MyDoom.
- **February 3.** A DDoS attack against Microsoft is launched, but unsuccessfully.
- **February 9, 2004**. Doomjuice is unleashed it spreads only to infected computers, using the backdoor created by MyDoom.B to gain access. A new DDoS attack against Microsoft is launched. The bounty skyrockets to **$650,000**.
- **February 12**. The first version of MyDoom is programed to stop spreading. But the perpetrators continue to have access to over half a million computers.
- **March 1.** MyDoom.B self-terminates.
- **July 26, 2004**. Another MyDoom variant brings down search engines, like Google, AltaVista and Lycos.
- **Early 2005.** MyDoom has been largely neutralized.

- **July 2009.** MyDoom’s code targets government and financial networks in South Korea and the US. The overall impact was low.
- **2009 — now.** Traces of the virus continue to infect unwary Internet users around the world.