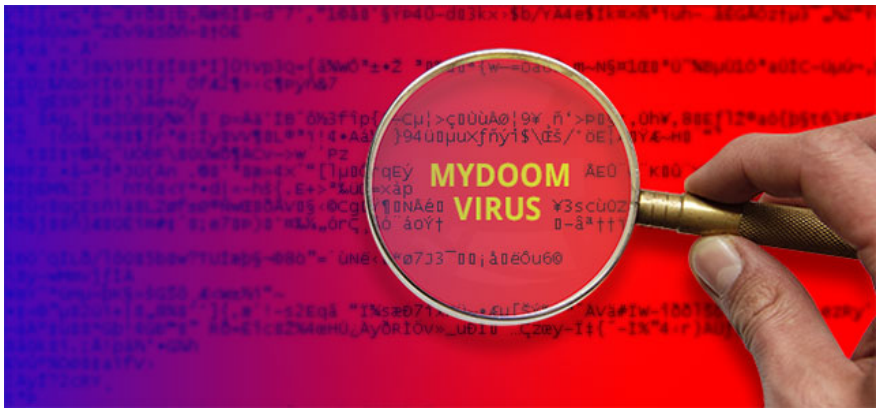
After 15 years, the notorious MyDoom poison worm still exists and threatens email users worldwide

MyDoom (also known as Novarg, Mimail and Shimg) is a family of malicious software that is believed to have been at least active since 2004 until now.

MyDoom, the once notorious poisonous worm, has once shattered millions of email users around the world and is considered one of the most serious types of malware ever recorded in the calendar. Security industry, network security - still lurking in a few corners of the Internet, operating with automatic mode and actively targeting email users around the world.

MyDoom (also known as Novarg, Mimail and Shimg) is a family of malicious software that is believed to have been at least active since 2004 until now. This malicious code targets primarily users of online mailing services. They are designed to spread quickly across a wide range of products through mass email (email spam). In addition, some of the harmful variants of MyDoom are also able to infect targets through peer-to-peer networks.

1. Warning: Appeared fake FaceApp application to install malicious code on users' devices

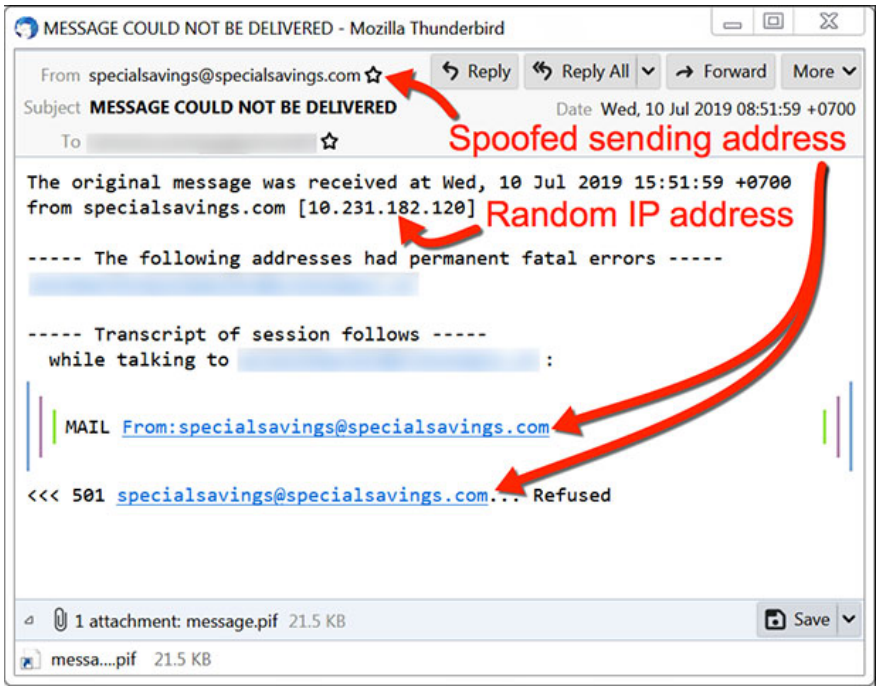


MyDoom has been operating since 2004 until now

After successful infection on the victim computer, MyDoom poison worm will silently set up a backdoor on TCP ports from 3127 to 3198, thereby allowing an attacker to have remote access to compromised systems. Added to distribute other malicious payloads. In some special cases, MyDoom variants also allow hackers to launch a denial of service (DoS) attack, causing paralysis of the target system.

As mentioned, email is the main spreading tool of MyDoom. This worm can collect many email addresses from different files on the compromised system, then automatically send an email with a malicious copy attached to itself to all the addresses it finds. , while the owner of the compromised system is completely unaware.

1. Ransomware (ransomware) is showing signs of explosion worldwide, paying is no longer the most effective option.



Email form containing malicious code MyDoom

Here are some noteworthy statistics, citing an in-depth analysis of MyDoom conducted by The Cylance Threat Research Team, a security research team:

MyDoom has been holding the record for the world's fastest-spreading email worm since it was first discovered in 2004 so far.

MyDoom holds the record for the most devastating virus in the history of security - cyber security, with the estimated damage of 38.5 billion USD worldwide.

At its peak, MyDoom created malicious email accounts for 16-25% of all emails sent every day worldwide.

The problem here is that after 15 years of being discovered, MyDoom still exists on the internet and is showing signs of strong growth again. Reports of MyDoom from many research groups and security service providers are still appearing every year and are on the rise in the past few months, with tens of thousands of cases of MyDoom infected emails being discovered. every month.

1. What is email encryption? Why does it play an important role in email security?

"Although it is no longer a strong development, creating large-scale attacks like other modern malware families, MyDoom's strength lies in the fact that this malicious code is still able to maintain. Relatively stable presence on the internet despite being discovered 15 years ago and increasingly faced with more advanced email security tools, on average, about 1.1% of the total number of emails gets us found the attachment of the malware, "said Brad Duncan, head of Unit 42 security research group at Palo Alto Networks.

Tens of thousands of malicious emails distributed by MyDoom worldwide every month target a variety of industries ranging from high technology, wholesale and retail, to health care, education, as well as as production in general.

1. Malicious Code EvilGnome attacks Linux systems with many rare tricks

Year	MyDoom emails	Total emails with malware	% of MyDoom emails	MyDoom samples	Total malware samples	% of MyDoom samples
2015	574,674	27,599,631	2.1%	87,119	615,386	14.2%
2016	589,107	77,575,376	0.8%	142,659	960,517	14.9%
2017	309,978	79,599,864	0.4%	95,115	340,433	27.9%
2018	663,212	64,919,295	1.0%	150,075	528,306	28.4%

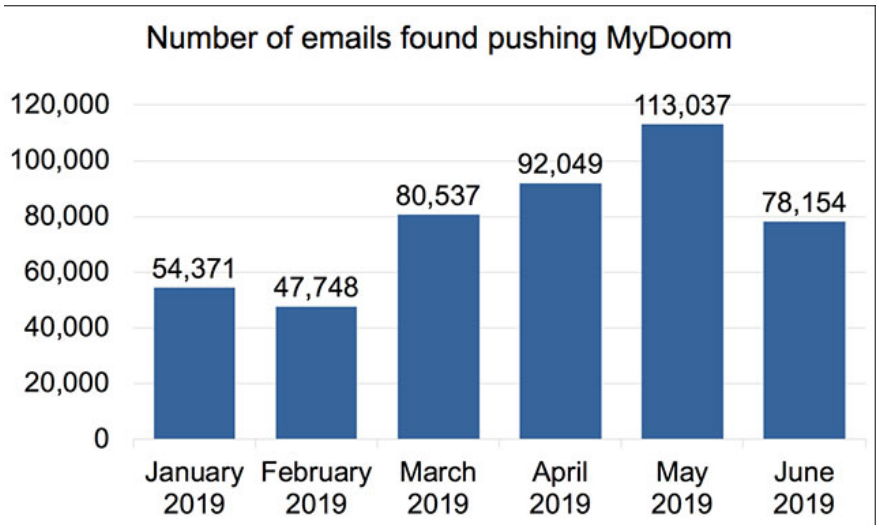
Data about MyDoom between 2015 and 2018

From 2015 to 2018, MyDoom was found in 1.1% of all malicious emails discovered by Palo Alto Networks security team, reaching "an average of 21.4% for all malicious software attachments. Harm is recorded spread through spam emails ".

The difference in the number of attachments and emails MyDoom is due to the polymorphic nature of this worm, which leads to a higher number of malware-related statistics, thus significantly increasing the number of samples. detected.

In the first half of 2019, Palo Alto Networks recorded a slight increase in the number of detected MyDoom-related malware samples, as well as a significant increase in the number of malicious emails sent to and away from the victims (the system has been infected with malicious code).

1. Shade ransomware, the nightmare of 5 years ago is showing signs of returning



MyDoom's activity in 2019 is based on Palo Alto Networks statistics

Since the first case of infection was recorded in 2004, MyDoom has been working hard for many years and infecting a large enough number of computers to help the malware stay active. and its presence on the internet

for many years, despite the growing number of more advanced email security systems being created, as well as no longer maintaining the same danger as in the beginning.

"Both China and the United States are the largest 'MyDoom' outbreaks in the world. The email containing the worm is mainly sent to and from these two countries, although basically, the process of distributing malicious code "It's still global and targets many different countries," added Brad Duncan.

1. Tracking email and privacy infringement - old problems that are not old

For more detailed information as well as statistics regarding how MyDoom spreads between servers, and the IOC index list containing hash values ??for MyDoom EXE patterns found in July of the year. 2019, please consult an in-depth analysis of Palo Alto Networks' MyDoom activity at: https://blog.talosintelligence.com/2019/07/rats-and-stealers-rush-through-heavens.html