Most Prominent Pandemics of Cyber Viruses

Ujjwal Sharma[1], Samruddhi Mangesh Kalekar[2]

[1]Cyber Security Architect, Production Technology, SLB
[2]Technical Business Analyst, SAP, SLB

Abstract

This paper delves into the potential devastation that can be wrought when a virus is executed on a target machine. We provide a brief overview of the topic, backed by statistical data on viruses' impact. Our analysis, based on data from various sources, reveals the profound effects of some of the most notorious viruses. We underscore the evolving nature of technology and the critical role of security within the system model. Users and organizations must remain vigilant about the diverse security threats of viruses.

Keywords: Virus, Malware, ILOVEYOU, Stuxnet, Shamoon, Heartbleed, Nimda

1. Introduction

The global cyber security market is on the brink of a significant expansion, with a projected value of USD 345.4 billion by 2026, a substantial increase from USD 217.7 billion in 2021. This growth is expected to be propelled by a Compound Annual Growth Rate (CAGR) of 9.7%. India's forecast for the next three years (2019 – 2022) is even more promising, with a projected CAGR of 15.3%. This thriving industry underscores the paramount importance of data, which is valuable and the very lifeblood of this sector. With the advent of big data and various modern technologies, trends and patterns can be discerned, providing actionable intelligence.

In the contemporary world, organizations are spread across various geographical locations, and applications are more centrally located. An organization’s data is its most prized resource and must be treated as such. While technological advancements have undoubtedly improved human life, there have been instances of technology misuse. The Internet, a global information-sharing platform, has also become a gateway for computer viruses. Sophisticated, engineered viruses can wreak havoc on organizations and individuals worldwide. This underscores the need for constant vigilance and our critical role in maintaining cyber security.

2. What is a Computer Virus?

Any program that is programmed to spread itself from one computer system to another and change how the computer works. A computer virus typically performs one or more of the following malicious activities:

- It can change programs that assist macros and insert its code.
- It has the potential to corrupt the system software completely.
- It could even destroy any data.

A virus is typically a type of malware.

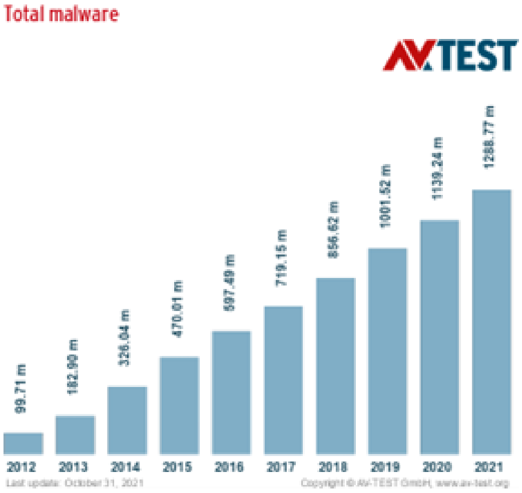
3. What Does a Computer Virus Do?

A computer virus depends on how exactly it has been coded. Sometimes, the impact could be as simple as a hoax that might not cause damage. In other cases, it could lead to advanced and adverse effects, potentially being considered fraud or criminal activity. Most viruses affect local hosts, but some spread through a network to find other vulnerable hosts.

4. Malware Statistics

The number of malware infections worldwide has increased tenfold in the last ten years and has been exponential yearly. Figure 1 is a statistical graph for AV-TEST showing the rise in malware infections.

Figure 1: Rise in Malware (Source: AV-TEST)

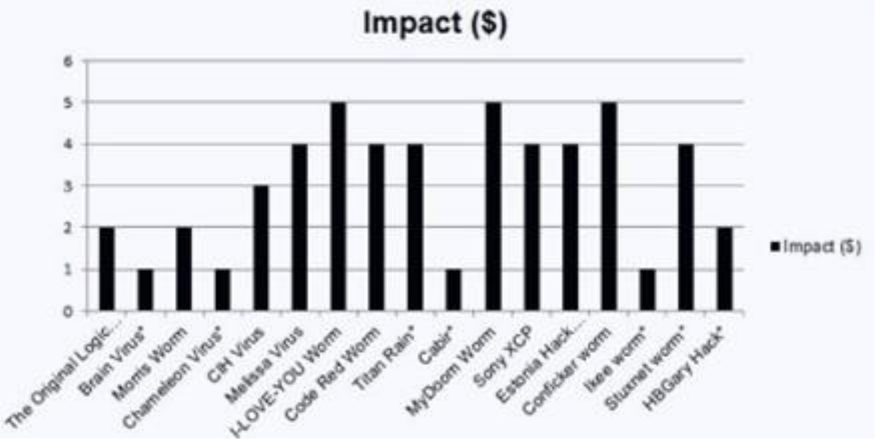


According to Legaljobs, malware has increased by an astonishing 87%. The United States of America has the most attacks, nearly 37% more than any other country. As a result, a cost of USD 5 trillion has been projected for the malware effects as of 2021.

5. Most Prominent Cyber Viruses

As more businesses go online worldwide, a massive surge in cyber-attacks will also occur. In the latest article published by the topbrandscompare website, there was a comparison of the most dangerous computer viruses of all. Below is the impact of computer virus in terms of USD dollars(millions):

Figure 2: Impact of the most vicious computer viruses (Source-topbrandscompare)



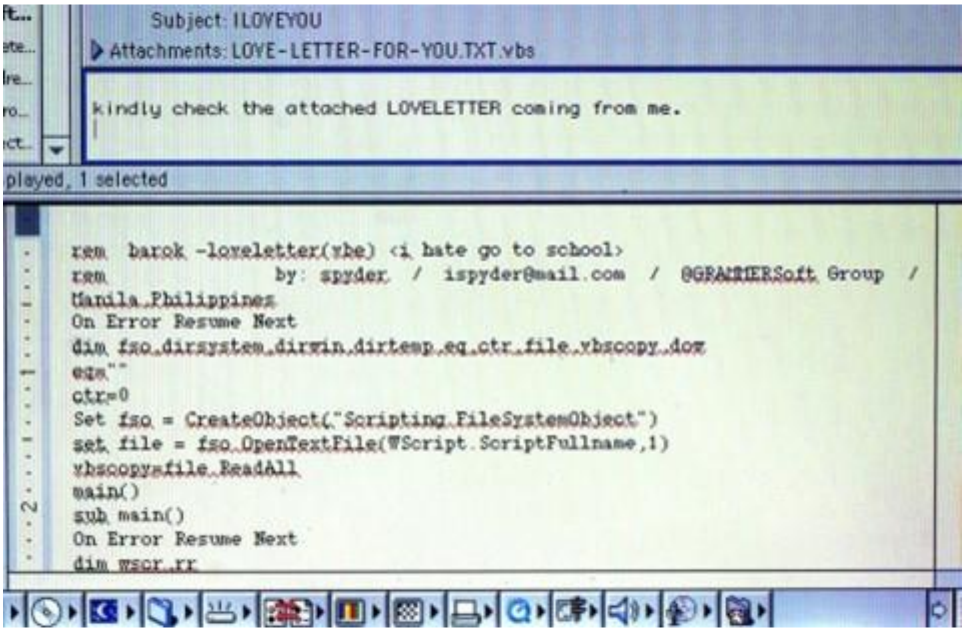
Based on the impact of computer viruses, the ILOVEYOU virus is believed to be one of the deadliest viruses ever created. We will dive deeper into the different types of destructive viruses in the coming sections.

6. ILOVEYOU

Famously called the Love Letter for You or Love Bug, it is a computer worm. It is one of the most destructive viruses, affecting nearly 55 million Windows machines. It started spreading an email with the message “kindly check the attached LOVELETTER coming from me” and an attachment of a VBs file extension, usually hidden by default in Windows machines, thus ensuring that users would think it was a regular file.

According to McAfee, it also included a wide range of attacks. It could add new files to the victim’s registry keys and replace several kinds of files with copies of itself. It also downloaded a file called “WIN—BUGSFIX.EXE” and executed it. According to reports, nearly 10% of computers worldwide were affected ten days after the virus's breakout. Financially, it caused a loss of approximately $5 to $9 billion. Thus, it ranks among the top devastating viruses ever.

Figure 3: Sample Email of ILOVEYOU virus (Source: cnn.com)



Subject: ILOVEYOU

Attachments: LOVE-LETTER-FOR-YOU.TXT.vbs

kindly check the attached LOVELETTER coming from me.

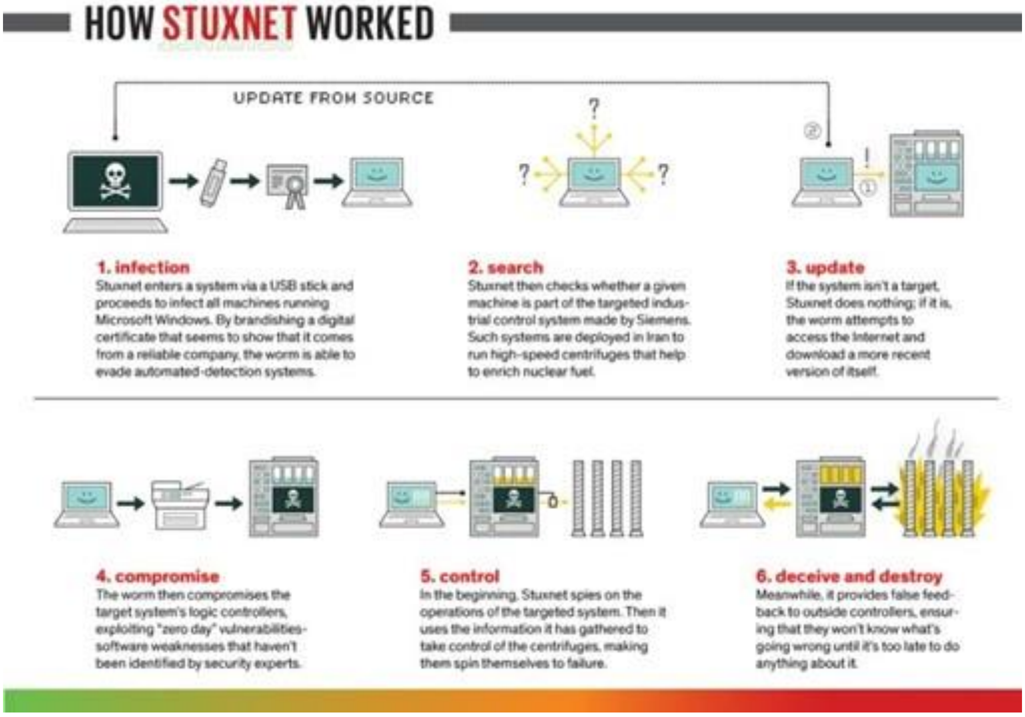
```
rem  barok -loveletter(vbe) <i hate go to school>
rem                 by: spyder  /  ispyder@mail.com  /  @GRAMMERSoft Group  /
Manila,Philippines
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullname,1)
vbscopy=file.ReadAll
main()
sub main()
On Error Resume Next
dim wscr,rr
```

7. STUXNET

Stuxnet was a malicious malware worm discovered in July 2010 by VirusBlokAda in Belarus. It had been widely reported that this cyberweapon was joint work of the United States and Israel under a covert operation – the Olympic Games. Stuxnet was highly selective in targeting the most common industrial control systems (ICS) types, such as supervisory control and data acquisition (SCADA) systems of an Iranian nuclear facility in Natanz.

According to Symantec, it was a highly sophisticated malware that exploited four zero-day vulnerabilities in the Microsoft Windows operating system, Siemens’ Simatic WinCC/Step-7 industrial software, and one or more programmable logic controllers. After infection, the worm is used to update itself and send information. The attack was then launched by abruptly altering the rotational speed of the motors such that the obsolete and fragile IR-1 centrifuges could be rendered unusable. Reports claimed that more than 1000 (one-fifth) centrifuges of Iran's uranium enrichment plant were damaged. It is interesting to note that the Natanz nuclear plant is placed in an air-gapped network physically isolated from the public internet. It would be fair to conclude that a person infecting the closed network delivered Stuxnet using a removable USB drive. Considering the effort level, resources, and sophistication involved, it is not difficult to attribute this to a state-sponsored attack that had severe social, political, economic, technological, and international effects on Iran and the entire globe. Vanity Fair called it " One of the greatest technical blockbusters in malware history."

Figure 4: How Stuxnet worked, David Kushner, Source – spectrum.ieee.org



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

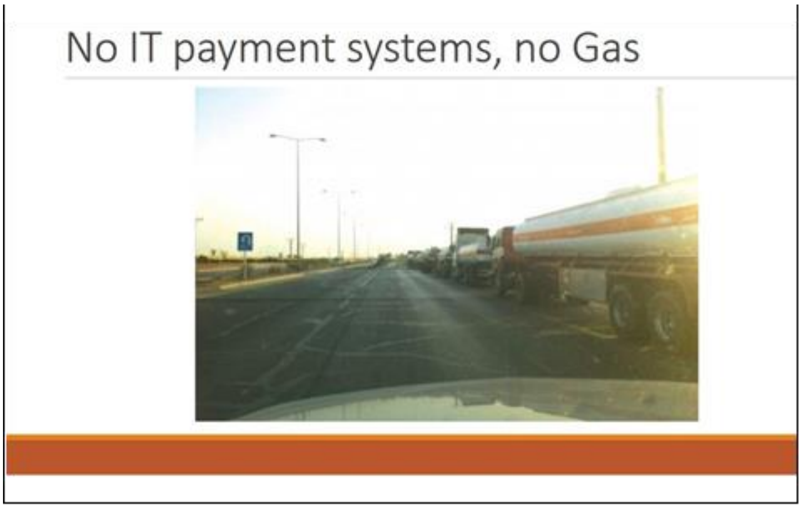
6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

8. SHAMOON

The W32.DistTrack virus was a self-replicating computer virus used for cyberwarfare against the world's largest oil producer1 – Saudi Arabian Oil Company (Saudi Aramco). It is also named Shamoon by the malware community due to a folder name in the executable's directory structure. The attack began on August 15, 2012, at 11:08 am Saudi Arabian time, where more than 30,000 Windows-based computer systems were overwritten, and data was deleted from the hard drives. It corrupted workstations and overwrote the Master Boot Record (MBR) to make them unusable. According to Symantec, the virus consists of three components. The Dropper module was responsible for the infection, the Wiper was accountable for erasing data, and the Reporter returned the information to the attacker. It was also reported that some files on the infected computers were replaced with the image of a burning American flag.

According to Kaspersky Labs, Shamoon could be loosely related to Wiper, which was used against Iran's oil ministry in April 2012. It was also commented that delivery of the malware required physical access to Saudi Aramco's network, raising questions about physical security & cyber awareness. Further, it was very well timed during the holiday month of Ramadan to maximize the damage and minimize the chance of discovery. The company went offline for almost two weeks until an official statement was issued on August 25, 2012, that they had restored their network services. However, a Middle Eastern journalist proved the statement wrong by publishing a photograph of tanker trucks unable to be loaded with gasoline. Jose Pagliery described it as "the biggest hack in history."

Figure 5: Weeks after the initial attack on 15 August, petrol trucks could not be loaded due to business system outages, contrary to a company statement by 25 August 2012. A Middle Eastern journalist leaked a photo proving the statement wrong.

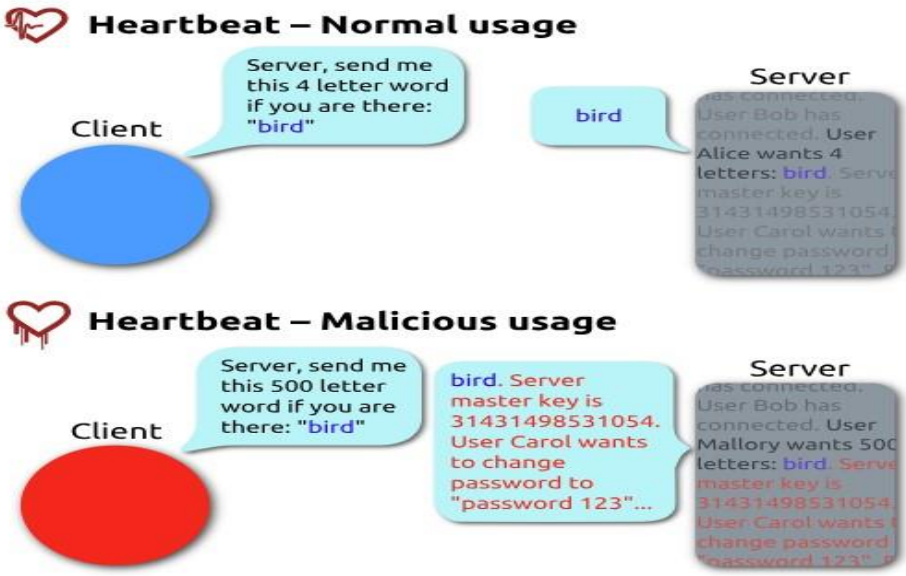


No IT payment systems, no Gas

9. HEARTBLEED

Unlike common malware that is induced by viruses/worms, Heartbleed, on the other hand, is a bug that compromises the cryptographic library. This bug intercepts SSL/TLS, a widely used norm for encryption in the World Wide Web. If a system has a weak open SSL suite installed, it becomes vulnerable as these weak suits become an entry point for a hacker to eavesdrop on the internet traffic to steal information. All internet applications like email, web browsers, VPN, and instant messaging are prone to this bug.

Figure 6: A depiction of Heartbleed.


Heartbeat – Normal usage
Client
Server, send me this 4 letter word if you are there: "bird"
bird
Server
has connected. User Bob has connected. User Alice wants 4 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P
Heartbeat – Malicious usage
Client
Server, send me this 500 letter word if you are there: "bird"
bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...
Server
has connected. User Bob has connected. User Mallory wants 500 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". P

10. NIMDA

Nimda was first created in 2001 to stop internet traffic when the WWW culture was blooming. This virus works like a daemon process that creates multiple replicas of itself, which causes the network to clog. Clogging of the network ultimately slows down internet traffic, eventually leading to a DENIAL OF SERVICE. Windows 95 is a classic example of a victim of this virus.

Admin spelled backward gives us the virus title, “NIMDA.” It was predominantly located in the Windows directory and was part of the “system.ini” file. It could download pages when the web server was infected and execute JavaScript automatically, thus sending the virus to other computers.

In addition to the ones mentioned above, other notable viruses include Shlayer, Tinba, Welchia, Morris Worm, and SQL Slammer.

11. Conclusion

Statistically, computer viruses cost an estimated loss of USD 55 billion annually in repair and cleanup. To tackle this threat, it is essential that users employ due care and thought before opening emails from unidentified sources. Also, what is equally important is that the infrastructure is protected and has vital anti-virus programs installed. While one cannot be sure that such countermeasures will eradicate the cyber-attack problem, they can be propitious in reducing the impact.

In most significant pandemics created by these viruses, the first line of defense, i.e., physical security, was compromised. Hence, organizations should put adequate emphasis on physical security measures as closed public networks are no longer safe to handle cyberattacks. The need of the hour is due diligence in implementing robust recovery strategies. As the level of malware sophistication is increasing, all enterprises must conduct timely audits, regular infrastructure penetration testing, and dedicated bug bounty programs to battle the critical zero-day exploits and security in general.

12. References

1. Tom Gerencer, “The Top 10 Worst Computer Viruses In History”, https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history
2. James Griffiths, “How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on” https://www.cnn.com/2020/05/01/tech/iloveyou-virus-computersecurityintlhnk/index.html#:~:text=Twenty%20years%20on%2C%20the%20ILOVEYOU,posed%20by%20malicious%20cyber%20actors.
3. Worst Virus Statistics https://www.topbrandscompare.com/antivirus/what-is-an-antivirus/
4. Malware Statistics https://www.av-test.org/en/statistics/malware/
5. N. Sönnichsen, “Selected oil companies worldwide ranked by daily crude oil production as of 2020*”, https://www.statista.com/statistics/280705/leading-oil-companies-worldwide-based-on-daily-oil- production-2012/
6. Shamoon, https://en.wikipedia.org/wiki/Shamoon
7. Nicole Perlroth, “Among Digital Crumbs from Saudi Aramco Cyberattack, Image of Burning U.S. Flag”, The New York Times, https://archive.nytimes.com/bits.blogs.nytimes.com/2012/08/24/among-digital-crumbs-from-saudi-aramco-cyberattack-image-of-burning-u-s-flag/
8. Jeffrey Carr, “Was Iran Responsible For Saudi Aramco's Network Attack?”, Digital Dao, https://jeffreycarr.blogspot.com/2012/08/was-iran-responsible-for-saudi-aramcos.html

9. Jose Pagliery, “The inside story of the biggest hack in history,” CNN Business, https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html
10. Gregg Keizer, “Is Stuxnet the 'best' malware ever?” InfoWorld, https://www.infoworld.com/article/2626009/is-stuxnet-the--best--malware-ever-.html
11. Nate Anderson, “Confirmed: US and Israel created Stuxnet, lost control of it,” arsTechnica, https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/
12. David Albright, Paul Brannan, and Christina Walrond, “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment”, ISIS, https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/
13. De Falco, “Stuxnet Facts Report. A Technical and Strategic Analysis”, CCDCOE, https://ccdcoe.org/library/publications/stuxnet-facts-report-a-technical-and-strategic-analysis-2/
14. Michael Joseph Gross,“A DECLARATION OF CYBER-WAR,” Vanity Fair, https://www.vanityfair.com/news/2011/03/stuxnet-201104
15. Chen, T.M., Abu-Nimeh, S., “Lessons from Stuxnet”, IEEE Computer Society
16. Christopher Bronk & Eneken Tikk-Ringas, “Hack or Attack? Shamoon and the Evolution of Cyber Conflict”, The James A. Baker III Institute for Public Policy of Rice University
17. David E. Sanger, “Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power” Baezner, Marie & Robin, Patrice, “Stuxnet,” The Center for Security Studies (CSS) at ETH Zurich
18. Wikipedia Contributors (2019). Heartbleed. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Heartbleed
19. Wikipedia. (2021). Nimda. [online] Available at: https://en.wikipedia.org/wiki/Nimda
20. Wikipedia. (2024). Shamoon. [online] Available at: https://en.wikipedia.org/wiki/Shamoon#/media/File:Petrol_truck_shipments_halted_during_Shamoon_attacks_on_1_September_2012.png [Accessed 30 May 2024] By Superboy 1989 - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=63824763
21. Wikipedia. (2024). Heartbleed. [online] Available at: https://en.wikipedia.org/wiki/Heartbleed#/media/File:Simplified_Heartbleed_explanation.svg [Accessed 30 May 2024] By FenixFeather - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=32276981