Petya (malware)

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Petya_(malware)#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Petya_(malware)#searchInput)

|  |  |
| --- | --- |
| **Petya** | |
| [ASCII art](https://en.wikipedia.org/wiki/ASCII_art) of a [skull and crossbones](https://en.wikipedia.org/wiki/Skull_and_crossbones_(symbol)) is displayed as part of the payload on the original version of Petya.[[1]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-cp-petya-1) | |
| **Aliases** | GoldenEye NotPetya |
| **Classification** | [Trojan horse](https://en.wikipedia.org/wiki/Trojan_horse_(computing)) |
| **Type** | [Malware](https://en.wikipedia.org/wiki/Malware) |
| **Subtype** | [Cryptovirus](https://en.wikipedia.org/wiki/Cryptovirology) |
| [**Operating system(s)**](https://en.wikipedia.org/wiki/Operating_system)**affected** | [Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) |

**Petya** is a family of encrypting [malware](https://en.wikipedia.org/wiki/Malware) that was first discovered in 2016.[[2]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-:0-2) The malware targets [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows)–based systems, infecting the [master boot record](https://en.wikipedia.org/wiki/Master_boot_record) to execute a [payload](https://en.wikipedia.org/wiki/Payload_(computing)) that encrypts a hard drive's [file system](https://en.wikipedia.org/wiki/File_system) table and prevents Windows from booting. It subsequently demands that the user make a payment in [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) in order to regain access to the system. The Petya malware had infected millions of people during its first year of its release. The maker of the Petya malware was fined and arrested.

Variants of Petya were first seen in March 2016, which propagated via infected [e-mail attachments](https://en.wikipedia.org/wiki/E-mail_attachment). In June 2017, a new variant of Petya was used for a [global cyberattack](https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine), primarily targeting [Ukraine](https://en.wikipedia.org/wiki/Ukraine). The new variant propagates via the [EternalBlue](https://en.wikipedia.org/wiki/EternalBlue) exploit, which is generally believed to have been developed by the [U.S](https://en.wikipedia.org/wiki/United_States). [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (NSA), and was used earlier in the year by the [WannaCry](https://en.wikipedia.org/wiki/WannaCry) ransomware. [Kaspersky Lab](https://en.wikipedia.org/wiki/Kaspersky_Lab) referred to this new version as **NotPetya** to distinguish it from the 2016 variants, due to these differences in operation. In addition, although it purports to be ransomware, this variant was modified so that it is unable to actually revert its own changes. The NotPetya attacks have been blamed on the Russian government, specifically the [Sandworm](https://en.wikipedia.org/w/index.php?title=Sandworm_(hacker_group)&action=edit&redlink=1) hacking group within the [GRU](https://en.wikipedia.org/wiki/GRU_(G.U.)) Russian military intelligence organization, by security researchers, Google, and several governments.[[2]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-:0-2)[[3]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-3)[[4]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-4)[[5]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-5)



**Contents**

* [1History](https://en.wikipedia.org/wiki/Petya_(malware)#History)
* [22017 cyberattack](https://en.wikipedia.org/wiki/Petya_(malware)#2017_cyberattack)
* [3Operation](https://en.wikipedia.org/wiki/Petya_(malware)#Operation)
* [4Mitigation](https://en.wikipedia.org/wiki/Petya_(malware)#Mitigation)
* [5Impact](https://en.wikipedia.org/wiki/Petya_(malware)#Impact)
* [6Reaction](https://en.wikipedia.org/wiki/Petya_(malware)#Reaction)
* [7Other Notable Low-Level Malware](https://en.wikipedia.org/wiki/Petya_(malware)#Other_Notable_Low-Level_Malware)
* [8See also](https://en.wikipedia.org/wiki/Petya_(malware)#See_also)
* [9References](https://en.wikipedia.org/wiki/Petya_(malware)#References)
* [10Further reading](https://en.wikipedia.org/wiki/Petya_(malware)#Further_reading)

History[[edit](https://en.wikipedia.org/w/index.php?title=Petya_(malware)&action=edit&section=1)]

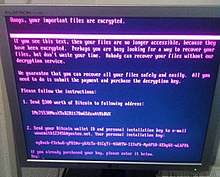
Petya was discovered in March 2016;[[6]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-nw-petyadouble-6) [Check Point](https://en.wikipedia.org/wiki/Check_Point) noted that while it had achieved fewer infections than other ransomware active in early 2016, such as [CryptoWall](https://en.wikipedia.org/wiki/CryptoWall), it contained notable differences in operation that caused it to be "immediately flagged as the next step in ransomware evolution".[[1]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-cp-petya-1) Another variant of Petya discovered in May 2016 contained a secondary payload used if the malware cannot achieve [administrator](https://en.wikipedia.org/wiki/Superuser)-level access.[[6]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-nw-petyadouble-6)

The name "Petya" is a reference to the 1995 [*James Bond*](https://en.wikipedia.org/wiki/James_Bond_in_film) film [*GoldenEye*](https://en.wikipedia.org/wiki/GoldenEye), wherein *Petya* is one of the two Soviet weapon satellites which carry a "Goldeneye"—an atomic bomb detonated in low Earth orbit to produce an [electromagnetic pulse](https://en.wikipedia.org/wiki/Electromagnetic_pulse). A [Twitter](https://en.wikipedia.org/wiki/Twitter) account that [*Heise*](https://en.wikipedia.org/wiki/Heise_Online) suggested may have belonged to the author of the malware, named "Janus Cybercrime Solutions" after [Alec Trevelyan](https://en.wikipedia.org/wiki/Alec_Trevelyan)'s crime group in *GoldenEye*, had an avatar with an image of *GoldenEye* character Boris Grishenko, a Russian hacker and antagonist in the film played by Scottish actor [Alan Cumming](https://en.wikipedia.org/wiki/Alan_Cumming).[[7]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-7)

On 30 August 2018, a regional court in [Nikopol](https://en.wikipedia.org/wiki/Nikopol,_Ukraine) in the [Dnipropetrovsk Oblast](https://en.wikipedia.org/wiki/Dnipropetrovsk_Oblast) of Ukraine convicted an unnamed Ukrainian citizen to one year in prison after pleading guilty to having spread a version of Petya online.[[8]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-8)[[9]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-9)[[10]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-10)

2017 cyberattack[[edit](https://en.wikipedia.org/w/index.php?title=Petya_(malware)&action=edit&section=2)]

*Main article:*[*2017 cyberattacks on Ukraine*](https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine)

[](https://en.wikipedia.org/wiki/File:PetyaA.jpg)

NotPetya's ransom note displayed on a compromised system

On 27 June 2017, a major global [cyberattack](https://en.wikipedia.org/wiki/Cyberattack) began (Ukrainian companies were among the first to state they were being attacked[[11]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-BBCGlobalR-11)), utilizing a new variant of Petya. On that day, [Kaspersky Lab](https://en.wikipedia.org/wiki/Kaspersky_Lab) reported infections in France, Germany, Italy, Poland, the United Kingdom, and the United States, but that the majority of infections targeted Russia and Ukraine, where more than 80 companies were initially attacked, including the [National Bank of Ukraine](https://en.wikipedia.org/wiki/National_Bank_of_Ukraine).[[11]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-BBCGlobalR-11)[[12]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-BloombergUkrRus-12) [ESET](https://en.wikipedia.org/wiki/ESET) estimated on 28 June 2017 that 80% of all infections were in Ukraine, with Germany second hardest hit with about 9%.[[13]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-BBCUkr80-13) Russian president [Vladimir Putin](https://en.wikipedia.org/wiki/Vladimir_Putin)'s press secretary, [Dmitry Peskov](https://en.wikipedia.org/wiki/Dmitry_Peskov), stated that the attack had caused no serious damage in Russia.[[13]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-BBCUkr80-13) Experts believed this was a politically-motivated attack against Ukraine, since it occurred on the eve of the Ukrainian holiday [Constitution Day](https://en.wikipedia.org/wiki/Constitution_Day_(Ukraine)).[[14]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-NYTcfU-14)[[15]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-BBCUkraineR-15)

Kaspersky dubbed this variant "NotPetya", as it has major differences in its operations in comparison to earlier variants.[[11]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-BBCGlobalR-11) [McAfee](https://en.wikipedia.org/wiki/McAfee) engineer Christiaan Beek stated that this variant was designed to spread quickly, and that it had been targeting "complete energy companies, the [power grid](https://en.wikipedia.org/wiki/Power_grid), bus stations, gas stations, the airport, and banks".[[11]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-BBCGlobalR-11)[[16]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-16)

It was believed that the [software update mechanism](https://en.wikipedia.org/wiki/Patch_(computing)#Software_update_systems) of [M.E.Doc](https://en.wikipedia.org/w/index.php?title=M.E.Doc&action=edit&redlink=1) [[uk](https://uk.wikipedia.org/wiki/M.E.Doc)]—a Ukrainian tax preparation program that, according to [F-Secure](https://en.wikipedia.org/wiki/F-Secure) analyst [Mikko Hyppönen](https://en.wikipedia.org/wiki/Mikko_Hypp%C3%B6nen), "appears to be de facto" among companies doing business in the country—had been compromised to spread the malware.[[13]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-BBCUkr80-13)[[17]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-bloomberg-medoc-17)[[18]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-reuters-20170703-18) Analysis by [ESET](https://en.wikipedia.org/wiki/ESET) found that a [backdoor](https://en.wikipedia.org/wiki/Backdoor_(computing)) had been present in the update system for at least six weeks prior to the attack, describing it as a "thoroughly well-planned and well-executed operation".[[19]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-ars-backdoormedoc-19) The developers of M.E.Doc denied that they were entirely responsible for the cyberattack, stating that they too were victims.[[17]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-bloomberg-medoc-17)[[20]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-ars-medoc-20)[[21]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-21)[[22]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-abcau-medocseized-22)

On 4 July 2017, Ukraine's cybercrime unit seized the company's servers after detecting "new activity" that it believed would result in "uncontrolled proliferation" of malware. Ukraine police advised M.E.Doc users to stop using the software, as it presumed that the backdoor was still present.[[19]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-ars-backdoormedoc-19)[[23]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-23) Analysis of the seized servers showed that software updates had not been applied since 2013, there was evidence of Russian presence, and an employee's account on the servers had been compromised; the head of the units warned that M.E.Doc could be found criminally responsible for enabling the attack because of its negligence in maintaining the security of their servers.[[19]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-ars-backdoormedoc-19)[[22]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-abcau-medocseized-22)[[24]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-reuters-20170705-24)

Operation[[edit](https://en.wikipedia.org/w/index.php?title=Petya_(malware)&action=edit&section=3)]

Petya's payload infects the computer's [master boot record](https://en.wikipedia.org/wiki/Master_boot_record) (MBR), overwrites the Windows [bootloader](https://en.wikipedia.org/wiki/Bootloader), and triggers a restart. Upon startup, the payload encrypts the [Master File Table](https://en.wikipedia.org/wiki/Master_File_Table) of the [NTFS](https://en.wikipedia.org/wiki/NTFS) [file system](https://en.wikipedia.org/wiki/File_system), and then displays the ransom message demanding a payment made in [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin).[[6]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-nw-petyadouble-6)[[25]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-25)[[26]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-verge-notpetya-26) Meanwhile, the computer's screen displays text purportedly output by [chkdsk](https://en.wikipedia.org/wiki/Chkdsk), Windows' file system scanner, suggesting that the hard drive's sectors are being repaired.[[1]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-cp-petya-1)

The original payload required the user to grant it administrative privileges; one variant of Petya was bundled with a second payload, Mischa, which activated if Petya failed to install. Mischa is a more conventional ransomware payload that encrypts user documents, as well as executable files, and does not require administrative privileges to execute.[[6]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-nw-petyadouble-6) The earlier versions of Petya disguised their payload as a [PDF](https://en.wikipedia.org/wiki/PDF) file, attached to an e-mail.[[6]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-nw-petyadouble-6) United States Computer Emergency Response Team (US-CERT) and National Cybersecurity and Communications Integration Center (NCCIC) released Malware Initial Findings Report (MIFR) about Petya on 30 June 2017.[[27]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-27)

The "NotPetya" variant used in the 2017 attack uses [EternalBlue](https://en.wikipedia.org/wiki/EternalBlue), an [exploit](https://en.wikipedia.org/wiki/Exploit_(computer_security)) that takes advantage of a [vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing)) in Windows' [Server Message Block](https://en.wikipedia.org/wiki/Server_Message_Block) (SMB) protocol. EternalBlue is generally believed to have been developed by the U.S. [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (NSA);[[26]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-verge-notpetya-26) it was leaked in April 2017 and was also used by [WannaCry](https://en.wikipedia.org/wiki/WannaCry).[[26]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-verge-notpetya-26)[[28]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-ars-eternalblue-28) The malware harvests passwords (using tweaked build of open-source Mimikatz[[29]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-29)) and uses other techniques [to spread](https://en.wikipedia.org/wiki/Vector_(malware)) to other computers on the same network, and uses those passwords in conjunction with PSExec to run code on other local computers.[[30]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-ecot-30)[[31]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-31)[[32]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-techc-32) Additionally, although it still purports to be ransomware, the encryption routine was modified so that the malware could not technically revert its changes.[[33]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-33) This characteristic, along with other unusual signs in comparison to WannaCry (including the relatively low unlock fee of US$300, and using a single, fixed Bitcoin wallet to collect ransom payments rather than generating a unique ID for each specific infection for tracking purposes),[[34]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-verge-toolate-34) prompted researchers to speculate that this attack was not intended to be a profit-generating venture, but to damage devices quickly, and [ride off](https://en.wikipedia.org/wiki/Copycat_crime) the media attention WannaCry received by claiming to be ransomware.[[35]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-ars-wiper-35)[[36]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-BBCPMdc-36)

Mitigation[[edit](https://en.wikipedia.org/w/index.php?title=Petya_(malware)&action=edit&section=4)]

*See also:*[*Ransomware § Mitigation*](https://en.wikipedia.org/wiki/Ransomware#Mitigation)*,*[*Infection control*](https://en.wikipedia.org/wiki/Infection_control)*,*[*Disaster recovery*](https://en.wikipedia.org/wiki/Disaster_recovery)*,*[*Emergency management*](https://en.wikipedia.org/wiki/Emergency_management)*, and*[*Proactive cyber defence*](https://en.wikipedia.org/wiki/Proactive_cyber_defence)

It was found that it may be possible to stop the encryption process if an infected computer is immediately shut down when the fictitious chkdsk screen appears,[[37]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-37) and a security analyst proposed that creating [read-only](https://en.wikipedia.org/wiki/File_system_permissions) files named perf.c and/or perfc.dat in the Windows installation directory could prevent the payload of the current strain from executing.[[38]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-38)[[39]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-39)[[40]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-40)[[41]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-41) The email address listed on the ransom screen was suspended by its provider, [Posteo](https://en.wikipedia.org/wiki/Posteo), for being a violation of its [terms of use](https://en.wikipedia.org/wiki/Terms_of_use). As a result, infected users could not actually send the required payment confirmation to the perpetrator.[[34]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-verge-toolate-34)[[42]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-42)Additionally, if the computer's filesystem was FAT based, the MFT encryption sequence was skipped, and only the ransomware's message was displayed, allowing data to be recovered trivially.[[43]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-43)

Microsoft had already released patches for supported versions of [Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) in March 2017 to address the EternalBlue vulnerability. This was followed by patches for unsupported versions of Windows (such as [Windows XP](https://en.wikipedia.org/wiki/Windows_XP)) in May 2017, in the direct wake of WannaCry.[[44]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-6facts-44)[[45]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-verge-unsupported-45) *Wired* believed that "based on the extent of damage Petya has caused so far, though, it appears that many companies have put off patching, despite the clear and potentially devastating threat of a similar ransomware spread."[[46]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-46) Some enterprises may consider it too disruptive to install updates on certain systems, either due to possible downtime or compatibility concerns, which can be problematic in some environments.[[44]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-6facts-44)

Impact[[edit](https://en.wikipedia.org/w/index.php?title=Petya_(malware)&action=edit&section=5)]

In a report published by *Wired*, a White House assessment pegged the total damages brought about by NotPetya to more than $10 billion. This was confirmed by former Homeland Security adviser Tom Bossert, who at the time of the attack was the most senior cybersecurity focused official in the US government.[[47]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-Wired_2018-47)

During the attack initiated on 27 June 2017, the radiation monitoring system at Ukraine's [Chernobyl Nuclear Power Plant](https://en.wikipedia.org/wiki/Chernobyl_Nuclear_Power_Plant) went offline.[[48]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-48) Several Ukrainian ministries, banks and metro systems were also affected.[[49]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-NYTRan-49) It is said to have been the most destructive cyberattack ever.[[50]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-50)

Among those affected elsewhere included British advertising company [WPP](https://en.wikipedia.org/wiki/WPP_plc),[[49]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-NYTRan-49) [Maersk Line](https://en.wikipedia.org/wiki/Maersk),[[51]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-NPRCyber-51) American pharmaceutical company [Merck & Co.](https://en.wikipedia.org/wiki/Merck_%26_Co.), Russian oil company [Rosneft](https://en.wikipedia.org/wiki/Rosneft) (its oil production was unaffected[[52]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-52)), multinational law firm [DLA Piper](https://en.wikipedia.org/wiki/DLA_Piper),[[49]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-NYTRan-49) French construction company [Saint-Gobain](https://en.wikipedia.org/wiki/Saint-Gobain) and its retail and subsidiary outlets in Estonia,[[53]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-Postimees-53) British consumer goods company [Reckitt Benckiser](https://en.wikipedia.org/wiki/Reckitt_Benckiser),[[54]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-54) German personal care company [Beiersdorf](https://en.wikipedia.org/wiki/Beiersdorf), German logistics company [DHL](https://en.wikipedia.org/wiki/DHL_Express),[[55]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-55) United States food company [Mondelez International](https://en.wikipedia.org/wiki/Mondelez_International), and American hospital operator Heritage Valley Health System.[[11]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-BBCGlobalR-11)[[56]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-56) The [Cadbury's Chocolate Factory](https://en.wikipedia.org/wiki/Cadbury%27s_Chocolate_Factory,_Tasmania) in [Hobart](https://en.wikipedia.org/wiki/Hobart), Tasmania, is the first company in Australia to be affected by Petya.[[57]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-57) On 28 June 2017, [JNPT](https://en.wikipedia.org/wiki/Jawaharlal_Nehru_Port#Jawaharlal_Nehru_Port_Trust), India's largest container port, had reportedly been affected, with all operations coming to a standstill.[[58]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-58) Princeton Community Hospital in rural West Virginia will scrap and replace its entire computer network on its path to recovery.[[59]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-59)

The business interruption to Maersk, the world's largest container ship and supply vessel operator, was estimated between $200m and $300m in lost revenues.[[60]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-60)

The business impact on FedEx is estimated to be $400m in 2018, according to the company's 2019 annual report.[[61]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-61)

[Jens Stoltenberg](https://en.wikipedia.org/wiki/Jens_Stoltenberg), [NATO](https://en.wikipedia.org/wiki/NATO) Secretary-General, pressed the alliance to strengthen its cyber defenses, saying that a cyberattack could trigger the Article 5 principle of collective defense.[[62]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-62)[[63]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-63)

Mondelez International's insurance carrier, [Zurich American Insurance Company](https://en.wikipedia.org/wiki/Zurich_American_Insurance_Company), has refused to pay out a claim for cleaning up damage from a Notpetya infection, on the grounds that Notpetya is an "act of war" that is not covered by the policy. Mondelez is suing Zurich American for $100 million.[[64]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-64)

Reaction[[edit](https://en.wikipedia.org/w/index.php?title=Petya_(malware)&action=edit&section=6)]

[Europol](https://en.wikipedia.org/wiki/Europol) said it was aware of and urgently responding to reports of a cyber attack in member states of the [European Union](https://en.wikipedia.org/wiki/European_Union).[[12]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-BloombergUkrRus-12) The [United States Department of Homeland Security](https://en.wikipedia.org/wiki/United_States_Department_of_Homeland_Security) was involved and coordinating with its international and local partners.[[51]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-NPRCyber-51) In a letter to the NSA,[[65]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-65) Democratic Congressman [Ted Lieu](https://en.wikipedia.org/wiki/Ted_Lieu) asked the agency to collaborate more actively with technology companies to notify them of software vulnerabilities and help them prevent future attacks based on malware created by the NSA.[[32]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-techc-32)[[66]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-66) On 15 February 2018, the Trump administration blamed Russia for the attack and warned that there would be "international consequences".[[67]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-67) The United Kingdom and the Australian government also issued similar statements.[[68]](https://en.wikipedia.org/wiki/Petya_(malware)#cite_note-68)