**Ιoί Υπολογιστή**

Ένας **ιός υπολογιστή**είναι ένας τύπος [προγράμματος υπολογιστή](https://en.m.wikipedia.org/wiki/Computer_program) που, όταν εκτελείται, αναπαράγει τον εαυτό του τροποποιώντας άλλα προγράμματα υπολογιστή και [εισάγοντας](https://en.m.wikipedia.org/wiki/Code_injection) τον δικό του [κώδικα](https://en.m.wikipedia.org/wiki/Computer_language)

Εάν αυτή η αναπαραγωγή πετύχει, οι πληγείσες περιοχές λέγεται ότι έχουν «μολυνθεί» με έναν ιό υπολογιστή, μια μεταφορά που προέρχεται από βιολογικούς [ιούς](https://en.m.wikipedia.org/wiki/Virus) .



[Hex dump](https://en.m.wikipedia.org/wiki/Hex_dump) of the [Brain](https://en.m.wikipedia.org/wiki/Brain_%28computer_virus%29) virus, που γενικά θεωρείται ως ο πρώτος ιός υπολογιστή για τον προσωπικό υπολογιστή IBM (IBM PC) και συμβατά

Οι ιοί υπολογιστών απαιτούν γενικά ένα [πρόγραμμα υποδοχής](https://en.m.wikipedia.org/wiki/Computer_program) .  Ο ιός γράφει τον δικό του κώδικα στο κεντρικό πρόγραμμα. Όταν εκτελείται το πρόγραμμα, εκτελείται πρώτα το γραπτό πρόγραμμα ιών, προκαλώντας μόλυνση και ζημιά. Ένα [σκουλήκι υπολογιστή](https://en.m.wikipedia.org/wiki/Computer_worm) δεν χρειάζεται πρόγραμμα υποδοχής, καθώς είναι ένα ανεξάρτητο πρόγραμμα ή κομμάτι κώδικα. Επομένως, δεν περιορίζεται από το [πρόγραμμα υποδοχής](https://en.m.wikipedia.org/wiki/Computer_program) , αλλά μπορεί να εκτελεστεί ανεξάρτητα και να εκτελεί ενεργά επιθέσεις.

Οι συντάκτες ιών χρησιμοποιούν [απάτες](https://en.m.wikipedia.org/wiki/Deception)[κοινωνικής μηχανικής](https://en.m.wikipedia.org/wiki/Social_engineering_%28security%29) και εκμεταλλεύονται τη λεπτομερή γνώση των [τρωτών σημείων ασφαλείας](https://en.m.wikipedia.org/wiki/Vulnerability_%28computing%29) για να μολύνουν αρχικά συστήματα και να διαδώσουν τον ιό. Οι ιοί χρησιμοποιούν πολύπλοκες στρατηγικές κατά της ανίχνευσης/ μυστικότητας για να αποφύγουν [το λογισμικό προστασίας από ιούς](https://en.m.wikipedia.org/wiki/Antivirus_software) .  Τα κίνητρα για τη δημιουργία ιών μπορεί να περιλαμβάνουν την αναζήτηση [κέρδους](https://en.m.wikipedia.org/wiki/Income) (π.χ. με [ransomware](https://en.m.wikipedia.org/wiki/Ransomware%22%20%5Co%20%22Ransomware) ), την επιθυμία αποστολής πολιτικού μηνύματος, την προσωπική διασκέδαση, την απόδειξη ότι υπάρχει ευπάθεια στο λογισμικό, για [δολιοφθορά](https://en.m.wikipedia.org/wiki/Sabotage) και [άρνηση υπηρεσίας](https://en.m.wikipedia.org/wiki/Denial-of-service_attack) ή απλώς επειδή θέλουν να εξερευνήστε θέματα [κυβερνοασφάλειας](https://en.m.wikipedia.org/wiki/Cybersecurity%22%20%5Co%20%22Cybersecurity) , [τεχνητής ζωής](https://en.m.wikipedia.org/wiki/Artificial_life) και[εξελικτικοί αλγόριθμοι](https://en.m.wikipedia.org/wiki/Evolutionary_algorithm) .

Οι ιοί υπολογιστών προκαλούν οικονομική ζημιά δισεκατομμυρίων δολαρίων κάθε χρόνο.

Σε απάντηση, μια βιομηχανία [λογισμικού προστασίας](https://en.m.wikipedia.org/wiki/Antivirus_software) από ιούς έχει εμφανιστεί, πουλά ή διανέμει ελεύθερα προστασία από ιούς σε χρήστες διαφόρων [λειτουργικών συστημάτων](https://en.m.wikipedia.org/wiki/Operating_system) .

Η πρώτη ακαδημαϊκή εργασία για τη θεωρία των αυτοαναπαραγόμενων προγραμμάτων υπολογιστών έγινε το 1949 από τον [John von Neumann](https://en.m.wikipedia.org/wiki/John_von_Neumann) ο οποίος έδωσε διαλέξεις στο [Πανεπιστήμιο του Ιλινόις](https://en.m.wikipedia.org/wiki/University_of_Illinois) σχετικά με τη «Θεωρία και οργάνωση των περίπλοκων [αυτομάτων](https://en.m.wikipedia.org/wiki/Automata) ». Το έργο του φον Νόιμαν δημοσιεύτηκε αργότερα ως «Θεωρία αυτοαναπαραγόμενων αυτομάτων». Στο δοκίμιό του ο von Neumann περιέγραψε πώς ένα πρόγραμμα υπολογιστή θα μπορούσε να σχεδιαστεί για να αναπαραχθεί.  Ο σχεδιασμός του Von Neumann για ένα αυτοαναπαραγόμενο πρόγραμμα υπολογιστή θεωρείται ο πρώτος ιός υπολογιστή στον κόσμο και θεωρείται ο θεωρητικός «πατέρας» της ιολογίας υπολογιστών.

 Το 1972, ο Veith Risak βασίστηκε απευθείας στο έργο του von Neumann για[αυτοαναπαραγωγή](https://en.m.wikipedia.org/wiki/Self-replication) , δημοσίευσε το άρθρο του "Selbstreproduzierende Automaten mit minimaler Informationsübertragung" (Αυτοαναπαραγόμενα αυτόματα με ελάχιστη ανταλλαγή πληροφοριών).  Το άρθρο περιγράφει έναν πλήρως λειτουργικό ιό γραμμένο σε γλώσσα προγραμματισμού [assembler](https://en.m.wikipedia.org/wiki/Assembler_%28computer_programming%29) για ένα σύστημα υπολογιστή SIEMENS 4004/35. Το 1980 ο Jürgen Kraus έγραψε τη [διπλωματική](https://en.m.wikipedia.org/wiki/Diplom) του διατριβή "Selbstreproduktion bei Programmen" (Αυτοαναπαραγωγή προγραμμάτων) στο [Πανεπιστήμιο του Ντόρτμουντ](https://en.m.wikipedia.org/wiki/University_of_Dortmund) .  Στο έργο του ο Kraus υπέθεσε ότι τα προγράμματα υπολογιστών μπορούν να συμπεριφέρονται με τρόπο παρόμοιο με τους βιολογικούς ιούς.



Ο ιός [MacMag](https://en.m.wikipedia.org/wiki/MacMag%22%20%5Co%20%22MacMag) «Universal Peace», όπως εμφανίζεται σε Mac τον Μάρτιο του 1988

Ο [ιός Creeper](https://en.m.wikipedia.org/wiki/Creeper_%28program%29) εντοπίστηκε για πρώτη φορά στο [ARPANET](https://en.m.wikipedia.org/wiki/ARPANET) , τον πρόδρομο του [Διαδικτύου](https://en.m.wikipedia.org/wiki/Internet) , στις αρχές της δεκαετίας του 1970. Το Creeper ήταν ένα πειραματικό αυτοαναπαραγόμενο πρόγραμμα που γράφτηκε από τον Bob Thomas στην [BBN Technologies](https://en.m.wikipedia.org/wiki/BBN_Technologies) το 1971.

 Ο Creeper χρησιμοποίησε το ARPANET για να μολύνει υπολογιστές [DEC](https://en.m.wikipedia.org/wiki/Digital_Equipment_Corporation)[PDP-10](https://en.m.wikipedia.org/wiki/PDP-10) που εκτελούσαν το λειτουργικό σύστημα [TENEX](https://en.m.wikipedia.org/wiki/TENEX_%28operating_system%29) .  Το Creeper απέκτησε πρόσβαση μέσω του ARPANET και αντιγράφηκε στο απομακρυσμένο σύστημα όπου το μήνυμα, "I'm THE CREEPER. CATCH ME ΑΝ ΜΠΟΡΕΙΣ!" εμφανιζόταν. Το πρόγραμμα *Reaper* δημιουργήθηκε για να διαγράψει το Creeper.

Το 1982, ένα πρόγραμμα που ονομαζόταν « [Elk Cloner](https://en.m.wikipedia.org/wiki/Elk_Cloner) » ήταν ο πρώτος ιός προσωπικού υπολογιστή που εμφανίστηκε «στη φύση»—δηλαδή έξω από τον μοναδικό υπολογιστή ή το εργαστήριο υπολογιστών όπου δημιουργήθηκε.  Γράφτηκε το 1981 από τον [Richard Skrenta](https://en.m.wikipedia.org/wiki/Richard_Skrenta%22%20%5Co%20%22%CE%A1%CE%AF%CF%84%CF%83%CE%B1%CF%81%CE%BD%CF%84%20%CE%A3%CE%BA%CF%81%CE%AD%CE%BD%CF%84%CE%B1) , μαθητή της ένατης τάξης στο [Mount Lebanon High School](https://en.m.wikipedia.org/wiki/Mount_Lebanon_High_School) κοντά στο [Πίτσμπουργκ](https://en.m.wikipedia.org/wiki/Pittsburgh) , προσαρτήθηκε στο λειτουργικό σύστημα [Apple DOS](https://en.m.wikipedia.org/wiki/Apple_DOS) 3.3 και διαδόθηκε μέσω [δισκέτας](https://en.m.wikipedia.org/wiki/Floppy_disk) .

Κατά την 50ή χρήση του , ο ιός [Elk Cloner](https://en.m.wikipedia.org/wiki/Elk_Cloner) θα ενεργοποιηθεί, μολύνοντας τον προσωπικό υπολογιστή και εμφανίζοντας ένα σύντομο ποίημα που ξεκινά "Elk Cloner: Το πρόγραμμα με μια προσωπικότητα".

Το 1984 [ο Fred Cohen](https://en.m.wikipedia.org/wiki/Fred_Cohen) από το [Πανεπιστήμιο της Νότιας Καλιφόρνια](https://en.m.wikipedia.org/wiki/University_of_Southern_California) έγραψε την εργασία του "Computer Viruses – Theory and Experiments".  Ήταν η πρώτη δημοσίευση που αποκάλεσε ρητά ένα πρόγραμμα αυτο-αναπαραγωγής «ιό», έναν όρο που εισήγαγε ο μέντορας του Κοέν, [Λέοναρντ Άντλεμαν](https://en.m.wikipedia.org/wiki/Leonard_Adleman%22%20%5Co%20%22%CE%9B%CE%AD%CE%BF%CE%BD%CE%B1%CF%81%CE%BD%CF%84%20%CE%86%CE%BD%CF%84%CE%BB%CE%B5%CE%BC%CE%B1%CE%BD) . Το 1987, ο Fred Cohen δημοσίευσε μια επίδειξη ότι δεν υπάρχει [αλγόριθμος](https://en.m.wikipedia.org/wiki/Algorithm) που να μπορεί να ανιχνεύσει τέλεια όλους τους πιθανούς ιούς.

[Ο θεωρητικός ιός συμπίεσης](https://en.m.wikipedia.org/wiki/Compression_virus) του Fred Cohen ήταν ένα παράδειγμα ιού που δεν ήταν κακόβουλο λογισμικό ( [malware](https://en.m.wikipedia.org/wiki/Malware)), αλλά ήταν υποθετικά καλοπροαίρετος (καλοπροαίρετος). Ωστόσο, οι επαγγελματίες προστασίας από ιούς δεν αποδέχονται την έννοια των "καλοπροαίρετων ιών", καθώς οποιαδήποτε επιθυμητή λειτουργία μπορεί να υλοποιηθεί χωρίς τη συμμετοχή ιών (η αυτόματη συμπίεση, για παράδειγμα, είναι διαθέσιμη στα [Windows](https://en.m.wikipedia.org/wiki/Windows_%28operating_system%29) κατόπιν επιλογής του χρήστη). Οποιοσδήποτε ιός εξ ορισμού θα κάνει μη εξουσιοδοτημένες αλλαγές σε έναν υπολογιστή, κάτι που δεν είναι επιθυμητό, ​​ακόμη κι αν δεν έχει προκληθεί ή προοριστεί καμία ζημιά. Η πρώτη σελίδα της *Εγκυκλοπαίδειας του Dr Solomon's Virus* εξηγεί την ανεπιθύμητη χρήση των ιών, ακόμη και εκείνων που δεν κάνουν τίποτα άλλο από την αναπαραγωγή.

Ένα άρθρο που περιγράφει «χρήσιμες λειτουργίες ιών» δημοσιεύτηκε από τον [JB Gunn](https://en.m.wikipedia.org/wiki/J._B._Gunn) με τον τίτλο «Use of virus functions to provide a virtual interpreter [APL](https://en.m.wikipedia.org/wiki/APL_%28programming_language%29) under user control» το 1984.  Ο πρώτος ιός [PC της IBM](https://en.m.wikipedia.org/wiki/IBM_PC_compatible) στο «wild» ήταν Ο ιός του [τομέα εκκίνησης με τίτλο](https://en.m.wikipedia.org/wiki/Boot_sector)[(c)Brain](https://en.m.wikipedia.org/wiki/Brain_%28computer_virus%29) ,  δημιουργήθηκε το 1986 από τους Amjad Farooq Alvi και Basit Farooq Alvi στη [Λαχόρη του Πακιστάν](https://en.m.wikipedia.org/wiki/Lahore%22%20%5Co%20%22%CE%9B%CE%B1%CF%87%CF%8C%CF%81%CE%B7) , σύμφωνα με αναφορές για να αποτρέψει την μη εξουσιοδοτημένη αντιγραφή του λογισμικού που είχαν γράψει.

 Ο πρώτος ιός που στόχευσε ειδικά τα [Microsoft Windows](https://en.m.wikipedia.org/wiki/Microsoft_Windows) , [το WinVir](https://en.m.wikipedia.org/w/index.php?title=WinVir&action=edit&redlink=1)ανακαλύφθηκε τον Απρίλιο του 1992, δύο χρόνια μετά την κυκλοφορία των [Windows 3.0](https://en.m.wikipedia.org/wiki/Windows_3.0) .  Ο ιός δεν περιείχε [κλήσεις](https://en.m.wikipedia.org/wiki/Subroutine)[API των Windows](https://en.m.wikipedia.org/wiki/Windows_API) , αντίθετα βασιζόταν σε [διακοπές DOS](https://en.m.wikipedia.org/wiki/DOS_API) . Λίγα χρόνια αργότερα, τον Φεβρουάριο του 1996, Αυστραλοί χάκερ από το συνεργείο συγγραφής ιών VLAD δημιούργησαν τον ιό Bizatch (γνωστός και ως ιός "Boza"), ο οποίος ήταν ο πρώτος γνωστός ιός που στόχευε [τα Windows 95](https://en.m.wikipedia.org/wiki/Windows_95) . Στα τέλη του 1997 κυκλοφόρησε ο κρυπτογραφημένος, μόνιμος ιός κρυφής μνήμης [Win32.Cabanas](https://en.m.wikipedia.org/w/index.php?title=Win32.Cabanas&action=edit&redlink=1) — ο πρώτος γνωστός ιός που στόχευε [τα Windows NT](https://en.m.wikipedia.org/wiki/Windows_NT) (ήταν επίσης σε θέση να μολύνει κεντρικούς υπολογιστές Windows 3.0 και Windows 9x).

Ακόμη και [οι υπολογιστές του σπιτιού](https://en.m.wikipedia.org/wiki/Home_computer) επηρεάστηκαν από ιούς. Ο πρώτος που εμφανίστηκε στο [Commodore Amiga](https://en.m.wikipedia.org/wiki/Commodore_Amiga) ήταν ένας ιός τομέα εκκίνησης που ονομάζεται [SCA virus](https://en.m.wikipedia.org/wiki/SCA_%28computer_virus%29) , ο οποίος εντοπίστηκε τον Νοέμβριο του 1987

Ένας ιός υπολογιστή περιλαμβάνει γενικά τρία μέρη: τον μηχανισμό μόλυνσης, ο οποίος βρίσκει και μολύνει νέα αρχεία, τον έναυσμα, που καθορίζει πότε θα ενεργοποιηθεί το ωφέλιμο φορτίο και το ωφέλιμο φορτίο, που είναι ο κακόβουλος κώδικας που πρέπει να εκτελεστεί.

**Μηχανισμός μόλυνσης**

Ονομάζεται επίσης φορέας μόλυνσης, έτσι εξαπλώνεται ο ιός. Ορισμένοι ιοί έχουν μια [ρουτίνα αναζήτησης](https://en.m.wikipedia.org/wiki/Search_algorithm) , η οποία εντοπίζει και μολύνει αρχεία στο δίσκο. [[34]](https://en.m.wikipedia.org/wiki/Computer_virus#cite_note-Stallings_2012_p.183-34) Άλλοι ιοί μολύνουν τα αρχεία καθώς εκτελούνται, όπως ο [ιός DOS της Ιερουσαλήμ](https://en.m.wikipedia.org/wiki/Jerusalem_%28computer_virus%29) .

**Θα Δώσει το έναυσμα για**

Γνωστό και ως [λογική βόμβα](https://en.m.wikipedia.org/wiki/Logic_bomb) , αυτό είναι το μέρος του ιού που καθορίζει την κατάσταση για την οποία ενεργοποιείται το

Αυτή η συνθήκη μπορεί να είναι μια συγκεκριμένη ημερομηνία, ώρα, παρουσία άλλου προγράμματος, μέγεθος στο [δίσκο](https://en.m.wikipedia.org/wiki/Disk_storage) που υπερβαίνει ένα όριο,

 ή άνοιγμα ενός συγκεκριμένου αρχείου.

**Φορτίο επί πληρωμή**

Το ωφέλιμο φορτίο είναι το σώμα του ιού που εκτελεί την κακόβουλη δραστηριότητα. Παραδείγματα κακόβουλων δραστηριοτήτων περιλαμβάνουν την καταστροφή αρχείων, την κλοπή εμπιστευτικών πληροφοριών ή την κατασκοπεία του μολυσμένου συστήματος.

 Η δραστηριότητα ωφέλιμου φορτίου είναι μερικές φορές αισθητή καθώς μπορεί να προκαλέσει επιβράδυνση ή «παγώσει» του συστήματος

Μερικές φορές τα ωφέλιμα φορτία είναι μη καταστροφικά και ο κύριος σκοπός τους είναι να διαδώσουν ένα μήνυμα σε όσο το δυνατόν περισσότερους ανθρώπους. Αυτό ονομάζεται [φάρσα από ιούς](https://en.m.wikipedia.org/wiki/Virus_hoax) .

**Φάσεις**

Οι φάσεις του ιού είναι ο [κύκλος ζωής](https://en.m.wikipedia.org/wiki/Object_lifetime) του ιού υπολογιστή, που περιγράφεται χρησιμοποιώντας μια αναλογία με τη [βιολογία](https://en.m.wikipedia.org/wiki/Biology) . Αυτός ο κύκλος ζωής μπορεί να χωριστεί σε τέσσερις φάσεις:

1. **Αδρανής φάση**

Το πρόγραμμα ιών είναι αδρανές σε αυτό το στάδιο. Το πρόγραμμα ιών κατάφερε να αποκτήσει πρόσβαση στον υπολογιστή ή το λογισμικό του χρήστη-στόχου, αλλά σε αυτό το στάδιο, ο ιός δεν προβαίνει σε καμία ενέργεια. Ο ιός τελικά θα ενεργοποιηθεί από το "trigger" που δηλώνει ποιο συμβάν θα εκτελέσει τον ιό. Δεν έχουν όλοι οι ιοί αυτό το στάδιο.

1. **Φάση πολλαπλασιασμού**

Ο ιός αρχίζει να διαδίδεται, ο οποίος πολλαπλασιάζεται και πολλαπλασιάζεται. Ο ιός τοποθετεί ένα αντίγραφο του εαυτού του σε άλλα προγράμματα ή σε ορισμένες περιοχές συστήματος στο δίσκο. Το αντίγραφο μπορεί να μην είναι πανομοιότυπο με την έκδοση που διαδίδεται. Οι ιοί συχνά «μορφώνονται» ή αλλάζουν για να αποφύγουν τον εντοπισμό από επαγγελματίες πληροφορικής και λογισμικό προστασίας από ιούς. Κάθε μολυσμένο πρόγραμμα θα περιέχει τώρα έναν [κλώνο](https://en.m.wikipedia.org/wiki/Clone_%28computing%29) του ιού, ο οποίος θα εισέλθει σε φάση διάδοσης.

**3.Φάση ενεργοποίησης**

Ένας αδρανής ιός μετακινείται σε αυτή τη φάση όταν ενεργοποιηθεί και θα εκτελέσει τώρα τη λειτουργία για την οποία προοριζόταν. Η φάση ενεργοποίησης μπορεί να προκληθεί από μια ποικιλία συμβάντων συστήματος, συμπεριλαμβανομένου του αριθμού των φορών που αυτό το αντίγραφο του ιού έχει δημιουργήσει αντίγραφα του εαυτού του.  Το έναυσμα μπορεί να προκύψει όταν ένας εργαζόμενος τερματιστεί από την απασχόλησή του ή μετά την πάροδο καθορισμένης χρονικής περιόδου, προκειμένου να μειωθεί η υποψία.

**4.Φάση εκτέλεσης**

Αυτό είναι το πραγματικό έργο του ιού, όπου θα απελευθερωθεί το «ωφέλιμο φορτίο». Μπορεί να είναι καταστροφικό, όπως η διαγραφή αρχείων στο δίσκο, η κατάρρευση του συστήματος ή η καταστροφή αρχείων ή σχετικά ακίνδυνο, όπως η εμφάνιση χιουμοριστικών ή πολιτικών μηνυμάτων στην οθόνη.

**Στόχοι και αναπαραγωγή**

Οι ιοί υπολογιστών μολύνουν μια ποικιλία διαφορετικών υποσυστημάτων στους κεντρικούς υπολογιστές και το λογισμικό τους.  Ένας τρόπος ταξινόμησης των ιών είναι να αναλυθεί εάν βρίσκονται σε [δυαδικά εκτελέσιμα αρχεία](https://en.m.wikipedia.org/wiki/Binary_executables) (όπως αρχεία [.EXE](https://en.m.wikipedia.org/wiki/.EXE) ή [.COM](https://en.m.wikipedia.org/wiki/.COM_files) ), αρχεία δεδομένων (όπως έγγραφα [Microsoft Word](https://en.m.wikipedia.org/wiki/Microsoft_Word) ή [αρχεία PDF](https://en.m.wikipedia.org/wiki/PDF_files) ) ή στον [τομέα εκκίνησης](https://en.m.wikipedia.org/wiki/Boot_sector) του [σκληρού υπολογιστή του κεντρικού υπολογιστή drive](https://en.m.wikipedia.org/wiki/Hard_drive) (ή κάποιος συνδυασμός όλων αυτών).

Ένας *ιός που κατοικεί στη μνήμη* (ή απλώς "μόνιμος ιός") εγκαθίσταται ως μέρος του λειτουργικού συστήματος όταν εκτελείται, μετά την οποία παραμένει στη [μνήμη RAM](https://en.m.wikipedia.org/wiki/RAM) από την εκκίνηση του υπολογιστή μέχρι τον τερματισμό της λειτουργίας του. Οι μόνιμοι ιοί αντικαθιστούν τον κώδικα [χειρισμού διακοπής ή άλλες](https://en.m.wikipedia.org/wiki/Interrupt_handling)[λειτουργίες](https://en.m.wikipedia.org/wiki/Function_%28programming%29) και όταν το λειτουργικό σύστημα επιχειρεί να αποκτήσει πρόσβαση στο αρχείο προορισμού ή στον τομέα του δίσκου, ο κώδικας ιών παρεμποδίζει το αίτημα και ανακατευθύνει τη [ροή ελέγχου](https://en.m.wikipedia.org/wiki/Control_flow) στη μονάδα αναπαραγωγής, μολύνοντας τον στόχο.

Αντίθετα, ένας ιός που δεν *κατοικεί στη μνήμη* (ή "ιός μη μόνιμος"), όταν εκτελείται, σαρώνει το δίσκο για στόχους, τους μολύνει και μετά εξέρχεται (δηλαδή δεν παραμένει στη μνήμη αφού ολοκληρωθεί η εκτέλεση).

Πολλές κοινές εφαρμογές, όπως το [Microsoft Outlook](https://en.m.wikipedia.org/wiki/Microsoft_Outlook) και [το Microsoft Word](https://en.m.wikipedia.org/wiki/Microsoft_Word) , επιτρέπουν την ενσωμάτωση προγραμμάτων [μακροεντολών](https://en.m.wikipedia.org/wiki/Macro_%28computer_science%29%22%20%5Co%20%22%CE%9C%CE%B1%CE%BA%CF%81%CE%BF%CE%B5%CE%BD%CF%84%CE%BF%CE%BB%CE%AE%20%28%CE%B5%CF%80%CE%B9%CF%83%CF%84%CE%AE%CE%BC%CE%B7%20%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD%29) σε έγγραφα ή μηνύματα ηλεκτρονικού ταχυδρομείου, έτσι ώστε τα προγράμματα να εκτελούνται αυτόματα όταν ανοίγει το έγγραφο.

 Ένας *ιός μακροεντολής* (ή "ιός εγγράφων") είναι ένας ιός που είναι γραμμένος σε [γλώσσα μακροεντολής](https://en.m.wikipedia.org/wiki/Macro_language) και ενσωματωμένος σε αυτά τα έγγραφα, έτσι ώστε όταν οι χρήστες ανοίγουν το αρχείο, εκτελείται ο κώδικας ιού και μπορεί να μολύνει τον υπολογιστή του χρήστη. Αυτός είναι ένας από τους λόγους που είναι επικίνδυνο να ανοίγετε απροσδόκητα ή ύποπτα [συνημμένα](https://en.m.wikipedia.org/wiki/E-mail_attachment) σε [μηνύματα ηλεκτρονικού ταχυδρομείου](https://en.m.wikipedia.org/wiki/E-mail) .

Αν και το να μην ανοίγετε συνημμένα σε μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστα άτομα ή οργανισμούς μπορεί να βοηθήσει στη μείωση της πιθανότητας μόλυνσης από ιό, σε ορισμένες περιπτώσεις, ο ιός έχει σχεδιαστεί έτσι ώστε το e-mail να φαίνεται ότι προέρχεται από έναν αξιόπιστο οργανισμό (π.χ. τράπεζα ή εταιρεία πιστωτικών καρτών).

*Οι ιοί του τομέα εκκίνησης* στοχεύουν ειδικά τον [τομέα εκκίνησης](https://en.m.wikipedia.org/wiki/Boot_sector) ή/και την [κύρια εγγραφή εκκίνησης](https://en.m.wikipedia.org/wiki/Master_Boot_Record) (MBR) της [μονάδας σκληρού δίσκου](https://en.m.wikipedia.org/wiki/Hard_disk_drive) του κεντρικού υπολογιστή , της μονάδας [στερεάς κατάστασης](https://en.m.wikipedia.org/wiki/Solid-state_drive) ή των αφαιρούμενων μέσων αποθήκευσης ( [μονάδες flash](https://en.m.wikipedia.org/wiki/Flash_drives) , [δισκέτες](https://en.m.wikipedia.org/wiki/Floppy_disks) κ.λπ.).

Ο πιο συνηθισμένος τρόπος μετάδοσης ιών υπολογιστών στον τομέα εκκίνησης είναι τα φυσικά μέσα. Κατά την ανάγνωση του VBR της μονάδας δίσκου, η μολυσμένη δισκέτα ή η μονάδα flash USB που είναι συνδεδεμένη στον υπολογιστή θα μεταφέρει δεδομένα και στη συνέχεια θα τροποποιήσει ή θα αντικαταστήσει τον υπάρχοντα κωδικό εκκίνησης. Την επόμενη φορά που ένας χρήστης θα προσπαθήσει να ξεκινήσει την επιφάνεια εργασίας, ο ιός θα φορτωθεί και θα εκτελεστεί αμέσως ως μέρος της κύριας εγγραφής εκκίνησης.

Οι ιοί ηλεκτρονικού ταχυδρομείου είναι ιοί που σκοπίμως, αντί κατά λάθος, χρησιμοποιούν το σύστημα ηλεκτρονικού ταχυδρομείου για να διαδοθούν. Ενώ τα αρχεία που έχουν μολυνθεί από ιούς μπορεί να σταλούν κατά λάθος ως [συνημμένα](https://en.m.wikipedia.org/wiki/Email_attachment) email, οι ιοί email γνωρίζουν τις λειτουργίες του συστήματος email. Γενικά στοχεύουν έναν συγκεκριμένο τύπο συστήματος ηλεκτρονικού ταχυδρομείου ( [το Microsoft Outlook](https://en.m.wikipedia.org/wiki/Microsoft_Outlook) είναι το πιο συχνά χρησιμοποιούμενο), συλλέγουν διευθύνσεις email από διάφορες πηγές και ενδέχεται να προσαρτούν αντίγραφα του εαυτού τους σε όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται ή ενδέχεται να δημιουργούν μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν αντίγραφα του εαυτού τους ως συνημμένα.

**Ανίχνευση**

Για να αποφευχθεί ο εντοπισμός από τους χρήστες, ορισμένοι ιοί χρησιμοποιούν διαφορετικά είδη [εξαπάτησης](https://en.m.wikipedia.org/wiki/Deception) . Ορισμένοι παλιοί ιοί, ειδικά στην πλατφόρμα [DOS](https://en.m.wikipedia.org/wiki/DOS) , διασφαλίζουν ότι η ημερομηνία "τελευταίας τροποποίησης" ενός αρχείου κεντρικού υπολογιστή παραμένει ίδια όταν το αρχείο έχει μολυνθεί από τον ιό. Ωστόσο, αυτή η προσέγγιση δεν ξεγελά το [λογισμικό](https://en.m.wikipedia.org/wiki/Software) προστασίας από ιούς , ειδικά εκείνα που διατηρούν και χρονολογούν [κυκλικούς ελέγχους πλεονασμού](https://en.m.wikipedia.org/wiki/Cyclic_redundancy_check) στις αλλαγές αρχείων.

 Ορισμένοι ιοί μπορούν να μολύνουν αρχεία χωρίς να αυξήσουν το μέγεθός τους ή να καταστρέψουν τα αρχεία. Αυτό το επιτυγχάνουν αντικαθιστώντας τις αχρησιμοποίητες περιοχές των εκτελέσιμων αρχείων. Αυτοί ονομάζονται *ιοί κοιλότητας* . Για παράδειγμα, ο [ιός CIH](https://en.m.wikipedia.org/wiki/CIH_virus) , ή ο ιός του Τσερνομπίλ, μολύνει το [Portable Executable](https://en.m.wikipedia.org/wiki/Portable_Executable) αρχεία. Επειδή αυτά τα αρχεία έχουν πολλά κενά κενά, ο ιός, που είχε μήκος 1 [KB](https://en.m.wikipedia.org/wiki/Kilobyte) , δεν προστέθηκε στο μέγεθος του αρχείου.

 Ορισμένοι ιοί προσπαθούν να αποφύγουν τον εντοπισμό σκοτώνοντας τις εργασίες που σχετίζονται με το λογισμικό προστασίας από ιούς προτού μπορέσει να τις εντοπίσει (για παράδειγμα, [Conficker](https://en.m.wikipedia.org/wiki/Conficker%22%20%5Cl%20%22Self-defense%22%20%5Co%20%22Conficker) ). Ένας ιός μπορεί επίσης να κρύψει την παρουσία του χρησιμοποιώντας ένα [rootkit](https://en.m.wikipedia.org/wiki/Rootkit%22%20%5Co%20%22Rootkit) μη εμφανιζόμενος στη λίστα των [διεργασιών](https://en.m.wikipedia.org/wiki/Process_%28computing%29) του συστήματος ή μεταμφιεσμένος σε μια αξιόπιστη διαδικασία.

 Στη δεκαετία του 2010, καθώς οι υπολογιστές και τα λειτουργικά συστήματα μεγαλώνουν και γίνονται πιο περίπλοκα, οι παλιές τεχνικές απόκρυψης πρέπει να ενημερωθούν ή να αντικατασταθούν. Η υπεράσπιση ενός υπολογιστή από ιούς μπορεί να απαιτεί τη μετεγκατάσταση ενός συστήματος αρχείων προς λεπτομερή και ρητή άδεια για κάθε είδους πρόσβαση σε αρχεία.

**Yποκλοπές Aιτημάτων**

Ενώ ορισμένα είδη λογισμικού προστασίας από ιούς χρησιμοποιούν διάφορες τεχνικές για την αντιμετώπιση μυστικών μηχανισμών, όταν συμβεί η μόλυνση, οποιαδήποτε προσφυγή για «καθαρισμό» του συστήματος είναι αναξιόπιστη. Στα λειτουργικά συστήματα Microsoft Windows, το [σύστημα αρχείων NTFS](https://en.m.wikipedia.org/wiki/NTFS_file_system) είναι αποκλειστικό. Αυτό αφήνει το λογισμικό προστασίας από ιούς ελάχιστη εναλλακτική από το να στείλει ένα αίτημα "ανάγνωσης" στα αρχεία των Windows που χειρίζονται τέτοια αιτήματα. Ορισμένοι ιοί ξεγελούν το λογισμικό προστασίας από ιούς παρεμποδίζοντας τα αιτήματά του προς το λειτουργικό σύστημα. Ένας ιός μπορεί να κρυφτεί παρεμποδίζοντας το αίτημα για ανάγνωση του μολυσμένου αρχείου, χειριζόμενο το ίδιο το αίτημα και επιστρέφοντας μια μη μολυσμένη έκδοση του αρχείου στο λογισμικό προστασίας από ιούς. Η υποκλοπή μπορεί να συμβεί με [ένεση κωδικού](https://en.m.wikipedia.org/wiki/Code_injection) των πραγματικών αρχείων του λειτουργικού συστήματος που θα χειρίζονταν το αίτημα ανάγνωσης. Έτσι, ένα λογισμικό προστασίας από ιούς που επιχειρεί να ανιχνεύσει τον ιό είτε δεν θα επιτρέπεται να διαβάσει το μολυσμένο αρχείο είτε το αίτημα "ανάγνωσης" θα εξυπηρετηθεί με την μη μολυσμένη έκδοση του ίδιου αρχείου.

Η μόνη αξιόπιστη μέθοδος για την αποφυγή ιών "κρυφής" είναι η εκκίνηση από ένα μέσο που είναι γνωστό ότι είναι "καθαρό". Το λογισμικό ασφαλείας μπορεί στη συνέχεια να χρησιμοποιηθεί για τον έλεγχο των αδρανών αρχείων του λειτουργικού συστήματος. Τα περισσότερα λογισμικά ασφαλείας βασίζονται σε υπογραφές ιών ή χρησιμοποιούν [ευρετικές](https://en.m.wikipedia.org/wiki/Heuristic_analysis%22%20%5Co%20%22%CE%95%CF%85%CF%81%CE%B5%CF%84%CE%B9%CE%BA%CE%AE%20%CE%B1%CE%BD%CE%AC%CE%BB%CF%85%CF%83%CE%B7) μεθόδους .

 Το λογισμικό ασφαλείας μπορεί επίσης να χρησιμοποιεί μια βάση δεδομένων αρχείων " [κατακερματισμού](https://en.m.wikipedia.org/wiki/Hash_%28computing%29) " για αρχεία λειτουργικού συστήματος Windows, ώστε το λογισμικό ασφαλείας να μπορεί να αναγνωρίσει τα τροποποιημένα αρχεία και να ζητήσει από τα μέσα εγκατάστασης των Windows να τα αντικαταστήσουν με αυθεντικές εκδόσεις. Σε παλαιότερες εκδόσεις των Windows, [οι κρυπτογραφικές συναρτήσεις κατακερματισμού](https://en.m.wikipedia.org/wiki/Cryptographic_hash_function) αρχείων των αρχείων του λειτουργικού συστήματος Windows που είναι αποθηκευμένα στα Windows—για να επιτρέπεται ο έλεγχος της ακεραιότητας/αυθεντικότητας των αρχείων—θα μπορούσαν να αντικατασταθούν έτσι ώστε ο [Έλεγχος αρχείων συστήματος](https://en.m.wikipedia.org/wiki/System_File_Checker)θα ανέφερε ότι τα τροποποιημένα αρχεία συστήματος είναι αυθεντικά, επομένως η χρήση κατακερματισμών αρχείων για σάρωση για τροποποιημένα αρχεία δεν εγγυάται πάντα την εύρεση μόλυνσης.

**Αυτοτροποποίηση**

Τα περισσότερα σύγχρονα προγράμματα προστασίας από ιούς προσπαθούν να βρουν μοτίβα ιών μέσα σε συνηθισμένα προγράμματα σαρώνοντάς τα για τις λεγόμενες *υπογραφές ιών* .  Διαφορετικά προγράμματα προστασίας από ιούς θα χρησιμοποιούν διαφορετικές μεθόδους αναζήτησης κατά τον εντοπισμό ιών. Εάν ένας ανιχνευτής ιών βρει ένα τέτοιο μοτίβο σε ένα αρχείο, θα εκτελέσει άλλους ελέγχους για να βεβαιωθεί ότι έχει βρει τον ιό, και όχι απλώς μια συμπτωματική ακολουθία σε ένα αθώο αρχείο, προτού ειδοποιήσει τον χρήστη ότι το αρχείο έχει μολυνθεί. Ο χρήστης μπορεί στη συνέχεια να διαγράψει ή (σε ορισμένες περιπτώσεις) να "καθαρίσει" ή να "θεραπεύσει" το μολυσμένο αρχείο. Ορισμένοι ιοί χρησιμοποιούν τεχνικές που καθιστούν την ανίχνευση μέσω υπογραφών δύσκολη αλλά μάλλον όχι αδύνατη. Αυτοί οι ιοί τροποποιούν τον κώδικά τους σε κάθε μόλυνση. Δηλαδή, κάθε μολυσμένο αρχείο περιέχει μια διαφορετική παραλλαγή του ιού.]

Μια μέθοδος αποφυγής ανίχνευσης υπογραφής είναι η χρήση απλής [κρυπτογράφησης](https://en.m.wikipedia.org/wiki/Encryption) για την κρυπτογράφηση (κωδικοποίηση) του σώματος του ιού, αφήνοντας μόνο τη μονάδα κρυπτογράφησης και ένα στατικό [κρυπτογραφικό κλειδί](https://en.m.wikipedia.org/wiki/Cryptographic_key) σε [καθαρό κείμενο](https://en.m.wikipedia.org/wiki/Cleartext) που δεν αλλάζει από τη μία μόλυνση στην άλλη.

 Σε αυτήν την περίπτωση, ο ιός αποτελείται από μια μικρή μονάδα αποκρυπτογράφησης και ένα κρυπτογραφημένο αντίγραφο του κώδικα του ιού. Εάν ο ιός είναι κρυπτογραφημένος με διαφορετικό κλειδί για κάθε μολυσμένο αρχείο, το μόνο μέρος του ιού που παραμένει σταθερό είναι η μονάδα αποκρυπτογράφησης, η οποία (για παράδειγμα) θα προσαρτηθεί στο τέλος. Σε αυτήν την περίπτωση, ένας ανιχνευτής ιών δεν μπορεί να εντοπίσει απευθείας τον ιό χρησιμοποιώντας υπογραφές, αλλά εξακολουθεί να μπορεί να ανιχνεύσει τη μονάδα αποκρυπτογράφησης, η οποία εξακολουθεί να καθιστά δυνατή την έμμεση ανίχνευση του ιού. Δεδομένου ότι αυτά θα ήταν συμμετρικά κλειδιά, αποθηκευμένα στον μολυσμένο κεντρικό υπολογιστή, είναι απολύτως δυνατό να αποκρυπτογραφηθεί ο τελικός ιός, αλλά αυτό μάλλον δεν απαιτείται, καθώς [η αυτοτροποποίηση κώδικα](https://en.m.wikipedia.org/wiki/Self-modifying_code) είναι τόσο σπάνια που η εύρεση ορισμένων μπορεί να είναι επαρκής λόγος για τους σαρωτές ιών να τουλάχιστον "σημαία" του αρχείου ως ύποπτο.

 Ένας παλιός αλλά συμπαγής τρόπος θα είναι η χρήση αριθμητικής πράξης όπως η πρόσθεση ή η αφαίρεση και η χρήση λογικών συνθηκών όπως το[XORing](https://en.m.wikipedia.org/wiki/Exclusive_or),

 όπου κάθε byte σε έναν ιό είναι με μια σταθερά, έτσι ώστε η πράξη αποκλειστικότητα ή μόνο να επαναληφθεί για αποκρυπτογράφηση. Είναι ύποπτο να τροποποιηθεί ένας κώδικας, επομένως ο κώδικας για την κρυπτογράφηση/αποκρυπτογράφηση μπορεί να είναι μέρος της υπογραφής σε πολλούς ορισμούς ιών. []Μια απλούστερη παλαιότερη προσέγγιση δεν χρησιμοποιούσε κλειδί, όπου η κρυπτογράφηση αποτελούνταν μόνο από πράξεις χωρίς παραμέτρους, όπως αύξηση και μείωση, περιστροφή bitwise, αριθμητική άρνηση και λογικό ΟΧΙ.

 Ορισμένοι ιοί, που ονομάζονται πολυμορφικοί ιοί, θα χρησιμοποιήσουν ένα μέσο κρυπτογράφησης μέσα σε ένα εκτελέσιμο αρχείο στο οποίο ο ιός κρυπτογραφείται κάτω από ορισμένα συμβάντα, όπως η απενεργοποίηση του σαρωτή ιών για ενημερώσεις ή η [επανεκκίνηση](https://en.m.wikipedia.org/wiki/Reboot_%28computing%29) του υπολογιστή .

Αυτό ονομάζεται [κρυπτοϊολογία](https://en.m.wikipedia.org/wiki/Cryptovirology%22%20%5Co%20%22%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CF%8A%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1) .

[Ο πολυμορφικός κώδικας](https://en.m.wikipedia.org/wiki/Polymorphic_code) ήταν η πρώτη τεχνική που αποτελούσε σοβαρή [απειλή](https://en.m.wikipedia.org/wiki/Threat_%28computer%29) για τους σαρωτές ιών. Ακριβώς όπως οι κανονικοί κρυπτογραφημένοι ιοί, ένας πολυμορφικός ιός μολύνει αρχεία με ένα κρυπτογραφημένο αντίγραφο του εαυτού του, το οποίο αποκωδικοποιείται από μια μονάδα [αποκρυπτογράφησης](https://en.m.wikipedia.org/wiki/Decryption) . Στην περίπτωση των πολυμορφικών ιών, ωστόσο, αυτή η ενότητα αποκρυπτογράφησης τροποποιείται επίσης σε κάθε μόλυνση. Επομένως, ένας καλογραμμένος πολυμορφικός ιός δεν έχει μέρη που να παραμένουν πανομοιότυπα μεταξύ των λοιμώξεων, γεγονός που καθιστά πολύ δύσκολο τον απευθείας εντοπισμό με χρήση «υπογραφών».

 Το λογισμικό προστασίας από ιούς μπορεί να το εντοπίσει αποκρυπτογραφώντας τους ιούς χρησιμοποιώντας έναν [εξομοιωτή](https://en.m.wikipedia.org/wiki/Emulator) ή με [στατιστική ανάλυση προτύπων](https://en.m.wikipedia.org/w/index.php?title=Statistical_pattern_analysis&action=edit&redlink=1)του κρυπτογραφημένου σώματος του ιού. Για να ενεργοποιηθεί ο πολυμορφικός κώδικας, ο ιός πρέπει να έχει μια [πολυμορφική μηχανή](https://en.m.wikipedia.org/wiki/Polymorphic_engine) (που ονομάζεται επίσης "μηχανή μετάλλαξης" ή " μηχανή [μετάλλαξης](https://en.m.wikipedia.org/wiki/Mutation) ") κάπου στο κρυπτογραφημένο σώμα του. Δείτε τον [πολυμορφικό κώδικα](https://en.m.wikipedia.org/wiki/Polymorphic_code) για τεχνικές λεπτομέρειες σχετικά με τον τρόπο λειτουργίας αυτών των κινητήρων.

Ορισμένοι ιοί χρησιμοποιούν πολυμορφικό κώδικα με τρόπο που περιορίζει σημαντικά τον ρυθμό μετάλλαξης του ιού. Για παράδειγμα, ένας ιός μπορεί να προγραμματιστεί να μεταλλάσσεται ελάχιστα με την πάροδο του χρόνου ή μπορεί να προγραμματιστεί ώστε να αποφεύγει τη μετάλλαξη όταν μολύνει ένα αρχείο σε έναν υπολογιστή που περιέχει ήδη αντίγραφα του ιού. Το πλεονέκτημα της χρήσης τόσο αργού πολυμορφικού κώδικα είναι ότι καθιστά πιο δύσκολο για τους επαγγελματίες προστασίας από ιούς και τους ερευνητές να αποκτήσουν αντιπροσωπευτικά δείγματα του ιού, επειδή τα αρχεία "δόλωμα" που μολύνονται σε μία εκτέλεση θα περιέχουν συνήθως πανομοιότυπα ή παρόμοια δείγματα του ιού. Αυτό θα καταστήσει πιο πιθανό ότι η ανίχνευση από το σαρωτή ιών θα είναι αναξιόπιστη και ότι ορισμένες περιπτώσεις του ιού μπορεί να αποφύγουν τον εντοπισμό.

Για να αποφευχθεί ο εντοπισμός τους από την εξομοίωση, ορισμένοι ιοί ξαναγράφουν τον εαυτό τους εντελώς κάθε φορά που πρόκειται να μολύνουν νέα εκτελέσιμα. Οι ιοί που χρησιμοποιούν αυτή την τεχνική λέγεται ότι είναι σε [μεταμορφικό κώδικα](https://en.m.wikipedia.org/wiki/Metamorphic_code) . Για να ενεργοποιηθεί η μεταμόρφωση, χρειάζεται μια «μεταμορφική μηχανή». Ένας μεταμορφωμένος ιός είναι συνήθως πολύ μεγάλος και πολύπλοκος. Για παράδειγμα, το [W32/Simile](https://en.m.wikipedia.org/wiki/W32/Simile) αποτελούνταν από περισσότερες από 14.000 γραμμές κώδικα [γλώσσας συναρμολόγησης](https://en.m.wikipedia.org/wiki/Assembly_language) , το 90% των οποίων είναι μέρος της μεταμορφικής μηχανής.

**Υπάρχοντα**

Η ζημιά οφείλεται στην πρόκληση βλάβης του συστήματος, στην καταστροφή δεδομένων, στη σπατάλη πόρων υπολογιστή, στην αύξηση του κόστους συντήρησης ή στην κλοπή προσωπικών πληροφοριών.

Παρόλο που κανένα λογισμικό προστασίας από ιούς δεν μπορεί να αποκαλύψει όλους τους ιούς υπολογιστών (ειδικά τους νέους), οι ερευνητές ασφάλειας υπολογιστών αναζητούν ενεργά νέους τρόπους για να επιτρέψουν στις λύσεις προστασίας από ιούς να εντοπίζουν αποτελεσματικότερα τους αναδυόμενους ιούς, προτού διαδοθούν ευρέως.

Ένας *ιός ισχύος* είναι ένα πρόγραμμα υπολογιστή που εκτελεί συγκεκριμένο κώδικα μηχανής για να φτάσει τη μέγιστη [απαγωγή ισχύος της CPU](https://en.m.wikipedia.org/wiki/CPU_power_dissipation) ( [θερμική ενέργεια](https://en.m.wikipedia.org/wiki/Thermal_energy) εξόδου για τις [κεντρικές μονάδες ς](https://en.m.wikipedia.org/wiki/Central_processing_unit) ). Οι συσκευές ψύξης υπολογιστών έχουν σχεδιαστεί για να διαχέουν την ισχύ μέχρι τη [θερμική ισχύ σχεδιασμού](https://en.m.wikipedia.org/wiki/Thermal_design_power) , αντί για τη μέγιστη ισχύ, και ένας ιός ισχύος θα μπορούσε να προκαλέσει υπερθέρμανση του συστήματος εάν δεν έχει λογική να σταματήσει τον επεξεργαστή. Αυτό μπορεί να προκαλέσει μόνιμη σωματική βλάβη. Οι ιοί ισχύος μπορεί να είναι κακόβουλοι, αλλά είναι συχνά σειρές λογισμικού δοκιμής που χρησιμοποιούνται για [δοκιμές ενοποίησης](https://en.m.wikipedia.org/wiki/Integration_testing) και θερμικές δοκιμές εξαρτημάτων υπολογιστή κατά τη φάση σχεδιασμού ενός προϊόντος ή για [συγκριτική αξιολόγηση](https://en.m.wikipedia.org/wiki/Benchmark_%28computing%29) προϊόντων .

[Οι εφαρμογές δοκιμής σταθερότητας](https://en.m.wikipedia.org/wiki/Software_testing) είναι παρόμοια προγράμματα που έχουν το ίδιο αποτέλεσμα με τους ιούς ισχύος (υψηλή χρήση CPU) αλλά παραμένουν υπό τον έλεγχο του χρήστη. Χρησιμοποιούνται για τη δοκιμή των CPU, για παράδειγμα, κατά το [overclocking](https://en.m.wikipedia.org/wiki/Overclocking%22%20%5Co%20%22Overclocking) . [Το Spinlock](https://en.m.wikipedia.org/wiki/Spinlock) σε ένα κακογραμμένο πρόγραμμα μπορεί να προκαλέσει παρόμοια συμπτώματα, εάν διαρκέσει αρκετά.

Διαφορετικές μικροαρχιτεκτονικές απαιτούν συνήθως διαφορετικό κώδικα μηχανής για να πετύχουν τη μέγιστη ισχύ τους. Παραδείγματα τέτοιου κώδικα μηχανής δεν φαίνεται να διανέμονται σε υλικά αναφοράς CPU.

**Φορείς μόλυνσης**

Καθώς το λογισμικό συχνά σχεδιάζεται με χαρακτηριστικά ασφαλείας για την πρόληψη της μη εξουσιοδοτημένης χρήσης πόρων συστήματος, πολλοί ιοί πρέπει να εκμεταλλεύονται και να χειρίζονται [σφάλματα ασφαλείας](https://en.m.wikipedia.org/wiki/Security_bug) , τα οποία είναι [ελαττώματα ασφαλείας](https://en.m.wikipedia.org/wiki/Malware#Security_defect) σε ένα σύστημα ή λογισμικό εφαρμογής, για να εξαπλωθούν και να μολύνουν άλλους υπολογιστές. [Οι στρατηγικές ανάπτυξης λογισμικού](https://en.m.wikipedia.org/wiki/Software_engineering) που παράγουν μεγάλους αριθμούς "σφαλμάτων" θα δημιουργήσουν γενικά επίσης πιθανές [εκμεταλλεύσιμες](https://en.m.wikipedia.org/wiki/Exploit_%28computer_security%29) "τρύπες" ή "εισόδους" για τον ιό.

Για να αναπαραχθεί, πρέπει να επιτρέπεται σε έναν ιό να εκτελεί κώδικα και να γράφει στη μνήμη. Για αυτόν τον λόγο, πολλοί ιοί συνδέονται με [εκτελέσιμα αρχεία](https://en.m.wikipedia.org/wiki/Executable_files) που μπορεί να αποτελούν μέρος νόμιμων προγραμμάτων (δείτε την [εισαγωγή κώδικα](https://en.m.wikipedia.org/wiki/Code_injection) ). Εάν ένας χρήστης επιχειρήσει να εκκινήσει ένα μολυσμένο πρόγραμμα, ο κώδικας του ιού μπορεί να εκτελεστεί ταυτόχρονα.

 Σε λειτουργικά συστήματα που χρησιμοποιούν [επεκτάσεις αρχείων](https://en.m.wikipedia.org/wiki/File_extension) για τον προσδιορισμό συσχετίσεων προγραμμάτων (όπως τα Microsoft Windows), οι επεκτάσεις ενδέχεται να είναι κρυφές από τον χρήστη από προεπιλογή. Αυτό καθιστά δυνατή τη δημιουργία ενός αρχείου διαφορετικού τύπου από αυτό που φαίνεται στον χρήστη. Για παράδειγμα, ένα εκτελέσιμο αρχείο μπορεί να δημιουργηθεί και να ονομάζεται "picture.png.exe", στο οποίο ο χρήστης βλέπει μόνο το "picture.png" και επομένως υποθέτει ότι αυτό το αρχείο είναι [ψηφιακή εικόνα](https://en.m.wikipedia.org/wiki/Digital_image) και πιθανότατα είναι ασφαλής, αλλά όταν ανοιχτεί, εκτελεί το εκτελέσιμο αρχείο στον υπολογιστή-πελάτη.

 Οι ιοί μπορούν να εγκατασταθούν σε αφαιρούμενα μέσα, όπως [μονάδες flash](https://en.m.wikipedia.org/wiki/Flash_drives) . Οι μονάδες δίσκου μπορεί να μείνουν σε χώρο στάθμευσης κυβερνητικού κτιρίου ή άλλου στόχου, με την ελπίδα ότι οι περίεργοι χρήστες θα τοποθετήσουν τη μονάδα σε έναν υπολογιστή. Σε ένα πείραμα του 2015, ερευνητές στο Πανεπιστήμιο του Μίσιγκαν διαπίστωσαν ότι το 45-98 τοις εκατό των χρηστών θα έβαζαν μια μονάδα flash άγνωστης προέλευσης.

Η συντριπτική πλειοψηφία των ιών στοχεύει συστήματα που εκτελούν [Microsoft Windows](https://en.m.wikipedia.org/wiki/Microsoft_Windows) . Αυτό οφείλεται στο μεγάλο μερίδιο αγοράς της Microsoft σε χρήστες [επιτραπέζιων υπολογιστών .](https://en.m.wikipedia.org/wiki/Desktop_computer)

 Η ποικιλία των συστημάτων λογισμικού σε ένα δίκτυο περιορίζει τις καταστροφικές δυνατότητες των ιών και του κακόβουλου λογισμικού.

[Λειτουργικά συστήματα ανοιχτού κώδικα](https://en.m.wikipedia.org/wiki/Open-source_software) όπως το [Linux](https://en.m.wikipedia.org/wiki/Linux) επιτρέπουν στους χρήστες να επιλέξουν από μια ποικιλία [περιβαλλόντων επιφάνειας εργασίας](https://en.m.wikipedia.org/wiki/Desktop_environments) , εργαλείων συσκευασίας κ.λπ., πράγμα που σημαίνει ότι κακόβουλος κώδικας που στοχεύει οποιοδήποτε από αυτά τα συστήματα θα επηρεάσει μόνο ένα υποσύνολο όλων των χρηστών. Πολλοί χρήστες των Windows εκτελούν το ίδιο σύνολο εφαρμογών, επιτρέποντας στους ιούς να εξαπλωθούν γρήγορα μεταξύ των συστημάτων Microsoft Windows στοχεύοντας τα ίδια exploit σε μεγάλο αριθμό κεντρικών υπολογιστών.

Ενώ το Linux και το Unix γενικά πάντα εμπόδιζαν εγγενώς τους κανονικούς χρήστες από το να κάνουν αλλαγές στο περιβάλλον του [λειτουργικού συστήματος](https://en.m.wikipedia.org/wiki/Operating_system) χωρίς άδεια, οι χρήστες Windows γενικά δεν εμποδίζονται να κάνουν αυτές τις αλλαγές, πράγμα που σημαίνει ότι οι ιοί μπορούν εύκολα να αποκτήσουν τον έλεγχο ολόκληρου του συστήματος στους κεντρικούς υπολογιστές των Windows. Αυτή η διαφορά συνεχίστηκε εν μέρει λόγω της ευρείας χρήσης λογαριασμών [διαχειριστή](https://en.m.wikipedia.org/wiki/System_administrator) σε σύγχρονες εκδόσεις όπως [τα Windows XP](https://en.m.wikipedia.org/wiki/Windows_XP) . Το 1997, οι ερευνητές δημιούργησαν και κυκλοφόρησαν έναν ιό για Linux — γνωστό ως " [Bliss](https://en.m.wikipedia.org/wiki/Bliss_%28virus%29) ".  Το Bliss, ωστόσο, απαιτεί από τον χρήστη να το εκτελεί ρητά και μπορεί να μολύνει μόνο προγράμματα που ο χρήστης έχει την πρόσβαση να τροποποιήσει. Σε αντίθεση με τους χρήστες των Windows, οι περισσότεροι χρήστες Unix δεν [συνδέονται](https://en.m.wikipedia.org/wiki/Login%22%20%5Co%20%22%CE%A3%CF%8D%CE%BD%CE%B4%CE%B5%CF%83%CE%B7)ως διαχειριστής ή ["root user"](https://en.m.wikipedia.org/wiki/Superuser) , εκτός από την εγκατάσταση ή τη διαμόρφωση λογισμικού. ως αποτέλεσμα, ακόμα κι αν ένας χρήστης διέτρεχε τον ιό, δεν θα μπορούσε να βλάψει το λειτουργικό του σύστημα. Ο ιός Bliss δεν έγινε ποτέ ευρέως διαδεδομένος και παραμένει κυρίως ένα ερευνητικό ενδιαφέρον. Ο δημιουργός του αργότερα δημοσίευσε τον πηγαίο κώδικα στο [Usenet](https://en.m.wikipedia.org/wiki/Usenet) , επιτρέποντας στους ερευνητές να δουν πώς λειτουργούσε.

Πριν διαδοθούν ευρέως τα δίκτυα υπολογιστών, οι περισσότεροι ιοί εξαπλώθηκαν σε [αφαιρούμενα μέσα](https://en.m.wikipedia.org/wiki/Removable_media) , ιδιαίτερα σε [δισκέτες](https://en.m.wikipedia.org/wiki/Floppy_disk) . Στις πρώτες μέρες του [προσωπικού υπολογιστή](https://en.m.wikipedia.org/wiki/Personal_computer) , πολλοί χρήστες αντάλλασσαν τακτικά πληροφορίες και προγράμματα σε δισκέτες. Ορισμένοι ιοί εξαπλώνονται μολύνοντας προγράμματα που είναι αποθηκευμένα σε αυτούς τους δίσκους, ενώ άλλοι εγκαταστάθηκαν στον [τομέα εκκίνησης του δίσκου](https://en.m.wikipedia.org/wiki/Boot_sector), διασφαλίζοντας ότι θα εκτελούνταν όταν ο χρήστης εκκινούσε τον υπολογιστή από το δίσκο, συνήθως κατά λάθος.

Οι προσωπικοί υπολογιστές της εποχής θα προσπαθούσαν να εκκινήσουν πρώτα από μια δισκέτα, αν είχαν μείνει στη μονάδα δίσκου. Μέχρι να βγουν εκτός χρήσης οι δισκέτες, αυτή ήταν η πιο επιτυχημένη στρατηγική μόλυνσης και οι ιοί του τομέα εκκίνησης ήταν οι πιο συνηθισμένοι στην «άγρια» για πολλά χρόνια.

Οι παραδοσιακοί ιοί υπολογιστών εμφανίστηκαν τη δεκαετία του 1980, λόγω της εξάπλωσης των προσωπικών υπολογιστών και της επακόλουθης αύξησης του [συστήματος πινάκων ανακοινώσεων](https://en.m.wikipedia.org/wiki/Bulletin_board_system) (BBS), της χρήσης [μόντεμ](https://en.m.wikipedia.org/wiki/Modem) και της κοινής χρήσης λογισμικού. [Η κοινή χρήση λογισμικού που βασίζεται σε πίνακες](https://en.m.wikipedia.org/wiki/Bulletin_board) ανακοινώσεων συνέβαλε άμεσα στην εξάπλωση των προγραμμάτων [Δούρειου ίππου](https://en.m.wikipedia.org/wiki/Trojan_horse_%28computing%29) και οι ιοί γράφτηκαν για να μολύνουν το δημοφιλές λογισμικό. [Shareware](https://en.m.wikipedia.org/wiki/Shareware)και το λογισμικό [bootleg](https://en.m.wikipedia.org/wiki/Copyright_infringement) ήταν εξίσου συνηθισμένοι [φορείς](https://en.m.wikipedia.org/wiki/Vector_%28malware%29) για ιούς σε BBS.

 Οι ιοί μπορούν να αυξήσουν τις πιθανότητές τους να εξαπλωθούν σε άλλους υπολογιστές μολύνοντας αρχεία σε ένα [σύστημα αρχείων δικτύου](https://en.m.wikipedia.org/wiki/Clustered_file_system#Distributed_file_systems) ή σε ένα σύστημα αρχείων στο οποίο έχουν πρόσβαση άλλοι υπολογιστές.

[Οι μακροϊοί](https://en.m.wikipedia.org/wiki/Macro_virus) έχουν γίνει κοινοί από τα μέσα της δεκαετίας του 1990. Οι περισσότεροι από αυτούς τους ιούς είναι γραμμένοι στις γλώσσες δέσμης ενεργειών για προγράμματα της Microsoft όπως το [Microsoft Word](https://en.m.wikipedia.org/wiki/Microsoft_Word) και [το Microsoft Excel](https://en.m.wikipedia.org/wiki/Microsoft_Excel) και εξαπλώνονται σε όλο [το Microsoft Office](https://en.m.wikipedia.org/wiki/Microsoft_Office) μολύνοντας έγγραφα και [υπολογιστικά φύλλα](https://en.m.wikipedia.org/wiki/Spreadsheet) . Δεδομένου ότι το Word και το Excel ήταν επίσης διαθέσιμα για [Mac OS](https://en.m.wikipedia.org/wiki/Mac_OS) , τα περισσότερα μπορούσαν να εξαπλωθούν και σε [υπολογιστές Macintosh](https://en.m.wikipedia.org/wiki/Macintosh) . Αν και οι περισσότεροι από αυτούς τους ιούς δεν είχαν τη δυνατότητα αποστολής μολυσμένων [μηνυμάτων ηλεκτρονικού ταχυδρομείου](https://en.m.wikipedia.org/wiki/Email) , αυτοί οι ιοί που εκμεταλλεύονταν τη διεπαφή του [Microsoft Outlook](https://en.m.wikipedia.org/wiki/Microsoft_Outlook)[Component Object Model](https://en.m.wikipedia.org/wiki/Component_Object_Model) (COM).

 Ορισμένες παλιές εκδόσεις του Microsoft Word επιτρέπουν στις μακροεντολές να αναπαράγονται με πρόσθετες κενές γραμμές. Εάν δύο μακροϊοί μολύνουν ταυτόχρονα ένα έγγραφο, ο συνδυασμός των δύο, αν και αυτοαναπαράγεται, μπορεί να εμφανιστεί ως "ζευγάρωμα" των δύο και πιθανότατα θα ανιχνευθεί ως ένας μοναδικός ιός από τους "γονείς".

Ένας ιός μπορεί επίσης να στείλει έναν [σύνδεσμο διεύθυνσης web](https://en.m.wikipedia.org/wiki/Uniform_Resource_Locator) ως [άμεσο μήνυμα](https://en.m.wikipedia.org/wiki/Instant_messaging) σε όλες τις επαφές (π.χ. διευθύνσεις ηλεκτρονικού ταχυδρομείου φίλων και συναδέλφων) που είναι αποθηκευμένες σε ένα μολυσμένο μηχάνημα. Εάν ο παραλήπτης, νομίζοντας ότι ο σύνδεσμος προέρχεται από έναν φίλο (μια αξιόπιστη πηγή) ακολουθήσει τον σύνδεσμο προς τον ιστότοπο, ο ιός που φιλοξενείται στον ιστότοπο ενδέχεται να μπορέσει να μολύνει αυτόν τον νέο υπολογιστή και να συνεχίσει να διαδίδεται.

 Οι ιοί που εξαπλώθηκαν χρησιμοποιώντας [δέσμες ενεργειών μεταξύ τοποθεσιών](https://en.m.wikipedia.org/wiki/Cross-site_scripting) αναφέρθηκαν για πρώτη φορά το 2002,  και αποδείχθηκαν ακαδημαϊκά το 2005.  Υπήρξαν πολλές περιπτώσεις ιών δέσμης ενεργειών μεταξύ τοποθεσιών στην "άγρια", που εκμεταλλεύονται ιστότοπους όπως το [MySpace](https://en.m.wikipedia.org/wiki/Samy_%28computer_worm%29%22%20%5Co%20%22Samy%20%28%CF%83%CE%BA%CE%BF%CF%85%CE%BB%CE%AE%CE%BA%CE%B9%20%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE%29) (με το σκουλήκι Samy) και το [Yahoo!](https://en.m.wikipedia.org/wiki/Yahoo%21%22%20%5Co%20%22Yahoo%21).

**Αντίμετρα**



Στιγμιότυπο οθόνης του [λογισμικού προστασίας από ιούς](https://en.m.wikipedia.org/wiki/Antivirus_software)[ClamWin](https://en.m.wikipedia.org/wiki/ClamWin)[ανοιχτού κώδικα](https://en.m.wikipedia.org/wiki/Open-source_software) που εκτελείται στο [Wine](https://en.m.wikipedia.org/wiki/Wine_%28software%29%22%20%5Co%20%22Wine%20%28software%29) στο [Ubuntu Linux](https://en.m.wikipedia.org/wiki/Ubuntu_Linux%22%20%5Co%20%22Ubuntu%20Linux)

Το 1989 η Διεύθυνση *Βιομηχανίας Λογισμικού*[*ADAPSO*](https://en.m.wikipedia.org/wiki/ADAPSO) δημοσίευσε το *Dealing With Electronic Vandalism* στο οποίο ακολούθησαν τον κίνδυνο απώλειας δεδομένων με «τον πρόσθετο κίνδυνο απώλειας της εμπιστοσύνης των πελατών».

Πολλοί χρήστες εγκαθιστούν [λογισμικό προστασίας από ιούς](https://en.m.wikipedia.org/wiki/Antivirus_software) που μπορεί να εντοπίσει και να εξαλείψει γνωστούς ιούς όταν ο υπολογιστής επιχειρεί να πραγματοποιήσει [λήψη](https://en.m.wikipedia.org/wiki/Downloading) ή εκτέλεση του εκτελέσιμου αρχείου (το οποίο μπορεί να διανεμηθεί ως συνημμένο email ή σε [μονάδες flash USB](https://en.m.wikipedia.org/wiki/USB_flash_drive_security#Malware_Infections) , για παράδειγμα). Ορισμένο λογισμικό προστασίας από ιούς αποκλείει γνωστούς κακόβουλους ιστότοπους που επιχειρούν να εγκαταστήσουν κακόβουλο λογισμικό. Το λογισμικό προστασίας από ιούς δεν αλλάζει την υποκείμενη ικανότητα των κεντρικών υπολογιστών να μεταδίδουν ιούς. Οι χρήστες πρέπει να ενημερώνουν τακτικά το λογισμικό τους για να [επιδιορθώνουν](https://en.m.wikipedia.org/wiki/Patch_%28computing%29)[τα τρωτά σημεία ασφαλείας](https://en.m.wikipedia.org/wiki/Malware#Vulnerability) ("τρύπες"). Το λογισμικό προστασίας από ιούς πρέπει επίσης να ενημερώνεται τακτικά για να αναγνωρίζει τις πιο πρόσφατες [απειλές](https://en.m.wikipedia.org/wiki/Threat_%28computer%29) . Αυτό συμβαίνει επειδή κακόβουλοι [χάκερ](https://en.m.wikipedia.org/wiki/Hacker%22%20%5Co%20%22%CE%A7%CE%AC%CE%BA%CE%B5%CF%81)και άλλα άτομα δημιουργούν πάντα νέους ιούς.

 Το Γερμανικό Ινστιτούτο [AV-TEST](https://en.m.wikipedia.org/wiki/AV-TEST) δημοσιεύει αξιολογήσεις λογισμικού προστασίας από ιούς για Windows και Android.

Παραδείγματα λογισμικού [προστασίας από ιούς](https://en.m.wikipedia.org/wiki/Antivirus) και κακόβουλου λογισμικού Microsoft Windows περιλαμβάνουν το προαιρετικό [Microsoft Security Essentials](https://en.m.wikipedia.org/wiki/Microsoft_Security_Essentials) (για Windows XP, Vista και Windows 7) για προστασία σε πραγματικό χρόνο, το [Εργαλείο κατάργησης κακόβουλου λογισμικού των Windows](https://en.m.wikipedia.org/wiki/Windows_Malicious_Software_Removal_Tool) (τώρα περιλαμβάνεται στα [Windows (Ασφάλεια) Ενημερώσεις](https://en.m.wikipedia.org/wiki/Windows_Update) για το " [Patch Tuesday](https://en.m.wikipedia.org/wiki/Patch_Tuesday) ", τη δεύτερη Τρίτη κάθε μήνα) και [το Windows Defender](https://en.m.wikipedia.org/wiki/Windows_Defender) (προαιρετική λήψη στην περίπτωση των Windows XP).

 Επιπλέον, αρκετά ικανά προγράμματα λογισμικού προστασίας από ιούς είναι διαθέσιμα για δωρεάν λήψη από το Διαδίκτυο (συνήθως περιορίζονται σε μη εμπορική χρήση).  Μερικά τέτοια δωρεάν προγράμματα είναι σχεδόν εξίσου καλά με τους εμπορικούς ανταγωνιστές.

Οι κοινές [ευπάθειες ασφαλείας](https://en.m.wikipedia.org/wiki/Malware#Vulnerability) έχουν εκχωρηθεί [αναγνωριστικά CVE](https://en.m.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures) και παρατίθενται στην [Εθνική βάση δεδομένων ευπάθειας](https://en.m.wikipedia.org/wiki/National_Vulnerability_Database) των ΗΠΑ . [Το Secunia PSI](https://en.m.wikipedia.org/wiki/Secunia#PSI)είναι ένα παράδειγμα λογισμικού, δωρεάν για προσωπική χρήση, που θα ελέγξει έναν υπολογιστή για ευάλωτο μη ενημερωμένο λογισμικό και θα προσπαθήσει να το ενημερώσει. [Οι ειδοποιήσεις για απάτη](https://en.m.wikipedia.org/wiki/Scam)[ransomware](https://en.m.wikipedia.org/wiki/Ransomware_%28malware%29) και [phishing](https://en.m.wikipedia.org/wiki/Phishing%22%20%5Co%20%22Phishing) εμφανίζονται ως δελτία τύπου στον πίνακα ανακοινώσεων του [Κέντρου καταγγελιών για εγκλήματα στο Διαδίκτυο](https://en.m.wikipedia.org/wiki/Internet_Crime_Complaint_Center#External_links) . Το Ransomware είναι ένας ιός που δημοσιεύει ένα μήνυμα στην οθόνη του χρήστη λέγοντας ότι η οθόνη ή το σύστημα θα παραμείνει κλειδωμένο ή άχρηστο έως ότου γίνει [λύτρα](https://en.m.wikipedia.org/wiki/Ransom%22%20%5Co%20%22%CE%9B%CF%8D%CF%84%CF%81%CE%B1)η πληρωμή γίνεται. [Το ηλεκτρονικό "ψάρεμα"](https://en.m.wikipedia.org/wiki/Phishing) είναι μια εξαπάτηση κατά την οποία το κακόβουλο άτομο προσποιείται ότι είναι φίλος, ειδικός σε θέματα ασφάλειας υπολογιστών ή άλλο καλοπροαίρετο άτομο, με στόχο να πείσει το στοχευόμενο άτομο να αποκαλύψει [κωδικούς πρόσβασης](https://en.m.wikipedia.org/wiki/Password) ή άλλες προσωπικές πληροφορίες.

Άλλα προληπτικά μέτρα που χρησιμοποιούνται συνήθως περιλαμβάνουν έγκαιρες ενημερώσεις λειτουργικού συστήματος, ενημερώσεις λογισμικού, προσεκτική περιήγηση στο Διαδίκτυο (αποφυγή σκιερών ιστοτόπων) και εγκατάσταση μόνο αξιόπιστου λογισμικού.

 Ορισμένα προγράμματα περιήγησης επισημαίνουν ιστότοπους που έχουν αναφερθεί στην Google και οι οποίοι έχουν επιβεβαιωθεί ότι φιλοξενούν κακόβουλο λογισμικό από την Google.

Υπάρχουν δύο συνήθεις μέθοδοι που χρησιμοποιεί μια εφαρμογή λογισμικού προστασίας από ιούς για τον εντοπισμό ιών, όπως περιγράφεται στο άρθρο του [λογισμικού προστασίας από ιούς](https://en.m.wikipedia.org/wiki/Antivirus_software#Identification_methods) . Η πρώτη και μακράν η πιο κοινή μέθοδος ανίχνευσης ιών είναι η χρήση μιας λίστας ορισμών [υπογραφής ιών .](https://en.m.wikipedia.org/wiki/Virus_signature)Αυτό λειτουργεί εξετάζοντας το περιεχόμενο της μνήμης του υπολογιστή (τη μνήμη [τυχαίας πρόσβασης](https://en.m.wikipedia.org/wiki/Random_Access_Memory) (RAM) και τους [τομείς εκκίνησης](https://en.m.wikipedia.org/wiki/Boot_sector) ) και τα αρχεία που είναι αποθηκευμένα σε σταθερές ή αφαιρούμενες μονάδες (σκληροί δίσκοι, μονάδες δισκέτας ή μονάδες flash USB) και συγκρίνοντας αυτά τα αρχεία με μια [βάση δεδομένων](https://en.m.wikipedia.org/wiki/Database)γνωστών «υπογραφών» ιών. Οι υπογραφές ιών είναι απλώς σειρές κώδικα που χρησιμοποιούνται για την αναγνώριση μεμονωμένων ιών. για κάθε ιό, ο σχεδιαστής προστασίας από ιούς προσπαθεί να επιλέξει μια μοναδική συμβολοσειρά υπογραφής που δεν θα βρεθεί σε ένα νόμιμο πρόγραμμα. Διαφορετικά προγράμματα προστασίας από ιούς χρησιμοποιούν διαφορετικές "υπογραφές" για την αναγνώριση ιών. Το μειονέκτημα αυτής της μεθόδου ανίχνευσης είναι ότι οι χρήστες προστατεύονται μόνο από ιούς που εντοπίζονται από υπογραφές στην πιο πρόσφατη ενημέρωση ορισμού ιών και δεν προστατεύονται από νέους ιούς (βλ. " [Επίθεση μηδενικής ημέρας](https://en.m.wikipedia.org/wiki/Zero-day_attack) ").

Μια δεύτερη μέθοδος για την εύρεση ιών είναι η χρήση ενός [ευρετικού](https://en.m.wikipedia.org/wiki/Heuristic_%28computer_science%29%22%20%5Co%20%22%CE%95%CF%85%CF%81%CE%B5%CF%84%CE%B9%CE%BA%CE%AE%20%28%CE%B5%CF%80%CE%B9%CF%83%CF%84%CE%AE%CE%BC%CE%B7%20%CF%84%CF%89%CE%BD%20%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CF%8E%CE%BD%29)[αλγόριθμου που](https://en.m.wikipedia.org/wiki/Algorithm) βασίζεται σε κοινές συμπεριφορές ιών. Αυτή η μέθοδος μπορεί να ανιχνεύσει νέους ιούς για τους οποίους οι εταιρείες ασφάλειας προστασίας από ιούς δεν έχουν ακόμη ορίσει μια "υπογραφή", αλλά επίσης οδηγεί σε περισσότερα [ψευδώς θετικά αποτελέσματα](https://en.m.wikipedia.org/wiki/Antivirus_software#Problems_caused_by_false_positives) από τη χρήση υπογραφών. Τα ψευδώς θετικά στοιχεία μπορεί να είναι ενοχλητικά, ειδικά σε ένα εμπορικό περιβάλλον, επειδή μπορεί να οδηγήσουν σε μια εταιρεία να δώσει εντολή στο προσωπικό να μην χρησιμοποιεί το σύστημα υπολογιστή της εταιρείας έως ότου οι υπηρεσίες IT ελέγξουν το σύστημα για ιούς. Αυτό μπορεί να επιβραδύνει την παραγωγικότητα των τακτικών εργαζομένων.

**Στρατηγικές και μέθοδοι αποκατάστασης**

Κάποιος μπορεί να μειώσει τη ζημιά που προκαλείται από ιούς κάνοντας τακτικά αντίγραφα ασφαλείας των δεδομένων (και των λειτουργικών συστημάτων) σε διαφορετικά μέσα, τα οποία είτε διατηρούνται ασύνδετα με το σύστημα (τις περισσότερες φορές, όπως σε σκληρό δίσκο), μόνο για ανάγνωση ή όχι είναι προσβάσιμο για άλλους λόγους, όπως η χρήση διαφορετικών συστημάτων αρχείων. Με αυτόν τον τρόπο, εάν χαθούν δεδομένα μέσω ενός ιού, μπορεί κανείς να ξαναρχίσει να χρησιμοποιεί το αντίγραφο ασφαλείας (το οποίο ελπίζουμε ότι θα είναι πρόσφατο).

 Εάν μια περίοδος λειτουργίας δημιουργίας αντιγράφων ασφαλείας σε οπτικά μέσα όπως CD και DVD είναι κλειστή, γίνεται μόνο για ανάγνωση και δεν μπορεί πλέον να επηρεαστεί από ιό (εφόσον ένας ιός ή ένα μολυσμένο αρχείο δεν αντιγράφηκε στο CD/DVD). Ομοίως, ένα λειτουργικό σύστημα σε ένα CD με δυνατότητα εκκίνησης μπορεί να χρησιμοποιηθεί για την εκκίνηση του υπολογιστή εάν τα εγκατεστημένα λειτουργικά συστήματα καταστούν άχρηστα. Τα αντίγραφα ασφαλείας σε αφαιρούμενα μέσα πρέπει να επιθεωρούνται προσεκτικά πριν από την αποκατάσταση. Ο ιός Gammima, για παράδειγμα, διαδίδεται μέσω αφαιρούμενων μονάδων flash.

Πολλές ιστοσελίδες που διαχειρίζονται εταιρείες λογισμικού προστασίας από ιούς παρέχουν δωρεάν online ανίχνευση ιών, με περιορισμένες δυνατότητες «καθαρισμού» (άλλωστε σκοπός των ιστοσελίδων είναι η πώληση προϊόντων και υπηρεσιών προστασίας από ιούς). Ορισμένοι ιστότοποι —όπως η θυγατρική της Google VirusTotal.com— επιτρέπουν στους χρήστες να ανεβάζουν ένα ή περισσότερα ύποπτα αρχεία για σάρωση και έλεγχο από ένα ή περισσότερα προγράμματα προστασίας από ιούς σε μία λειτουργία.

Επιπλέον, αρκετά ικανά προγράμματα λογισμικού προστασίας από ιούς είναι διαθέσιμα για δωρεάν λήψη από το Διαδίκτυο (συνήθως περιορίζονται σε μη εμπορική χρήση).

 Η Microsoft προσφέρει ένα προαιρετικό δωρεάν βοηθητικό πρόγραμμα προστασίας από ιούς που ονομάζεται Microsoft Security Essentials, ένα Εργαλείο κατάργησης κακόβουλου λογισμικού των Windows που ενημερώνεται ως μέρος του κανονικού καθεστώτος ενημέρωσης των Windows και ένα παλαιότερο προαιρετικό εργαλείο προστασίας από κακόβουλο λογισμικό (κατάργηση κακόβουλου λογισμικού) Windows Defender που έχει αναβαθμιστεί σε προϊόν προστασίας από ιούς στα Windows 8.

Ορισμένοι ιοί απενεργοποιούν την Επαναφορά Συστήματος και άλλα σημαντικά εργαλεία των Windows, όπως το Task Manager και το CMD. Ένα παράδειγμα ιού που το κάνει αυτό είναι το CiaDoor. Πολλοί τέτοιοι ιοί μπορούν να αφαιρεθούν με επανεκκίνηση του υπολογιστή, είσοδο στην "ασφαλή λειτουργία" των Windows με δικτύωση και, στη συνέχεια, χρησιμοποιώντας εργαλεία συστήματος ή το Microsoft Safety Scanner.

 Η Επαναφορά Συστήματος σε Windows Me, Windows XP, Windows Vista και Windows 7 μπορεί να επαναφέρει το μητρώο και τα κρίσιμα αρχεία συστήματος σε ένα προηγούμενο σημείο ελέγχου. Συχνά ένας ιός θα προκαλέσει το "κολλημένο" ή το "παγώσει" ενός συστήματος και μια επακόλουθη σκληρή επανεκκίνηση θα καταστρέψει ένα σημείο επαναφοράς συστήματος από την ίδια μέρα. Τα σημεία επαναφοράς από προηγούμενες ημέρες θα πρέπει να λειτουργούν, υπό την προϋπόθεση ότι ο ιός δεν έχει σχεδιαστεί για να καταστρέφει τα αρχεία επαναφοράς και δεν υπάρχει σε προηγούμενα σημεία επαναφοράς

Ο Έλεγχος αρχείων συστήματος της Microsoft (βελτιωμένος στα Windows 7 και νεότερες εκδόσεις) μπορεί να χρησιμοποιηθεί για τον έλεγχο και την επιδιόρθωση κατεστραμμένων αρχείων συστήματος

Η επαναφορά ενός παλαιότερου "καθαρού" (χωρίς ιούς) αντιγράφου ολόκληρου του διαμερίσματος από έναν κλωνοποιημένο δίσκο, μια εικόνα δίσκου ή ένα αντίγραφο ασφαλείας είναι μια λύση - η επαναφορά μιας προηγούμενης "εικόνας" αντιγράφου ασφαλείας δίσκου είναι σχετικά απλή, συνήθως αφαιρεί οποιαδήποτε κακόβουλο λογισμικό και μπορεί να είναι πιο γρήγορο από την «απολύμανση» του υπολογιστή—ή την επανεγκατάσταση και τη διαμόρφωση του λειτουργικού συστήματος και των προγραμμάτων από την αρχή, όπως περιγράφεται παρακάτω, και στη συνέχεια επαναφέροντας τις προτιμήσεις των χρηστών.[106] Η επανεγκατάσταση του λειτουργικού συστήματος είναι μια άλλη προσέγγιση για την αφαίρεση ιών. Ενδέχεται να είναι δυνατή η ανάκτηση αντιγράφων βασικών δεδομένων χρήστη με εκκίνηση από ένα ζωντανό CD ή σύνδεση του σκληρού δίσκου σε άλλον υπολογιστή και εκκίνηση από το λειτουργικό σύστημα του δεύτερου υπολογιστή, προσέχοντας πολύ να μην μολύνει αυτόν τον υπολογιστή εκτελώντας τυχόν μολυσμένα προγράμματα στο αρχική μονάδα δίσκου. Στη συνέχεια, ο αρχικός σκληρός δίσκος μπορεί να διαμορφωθεί ξανά και το λειτουργικό σύστημα και όλα τα προγράμματα να εγκατασταθούν από τα αρχικά μέσα. Μόλις αποκατασταθεί το σύστημα, πρέπει να ληφθούν προφυλάξεις για να αποφευχθεί η εκ νέου μόλυνση από τυχόν αποκαταστημένα εκτελέσιμα αρχεία.

**Λαϊκός πολιτισμός**

Η πρώτη γνωστή περιγραφή ενός αυτοαναπαραγόμενου προγράμματος στη μυθοπλασία είναι στο διήγημα του 1970 The Scarred Man του Gregory Benford, το οποίο περιγράφει ένα πρόγραμμα υπολογιστή που ονομάζεται VIRUS το οποίο, όταν εγκατασταθεί σε έναν υπολογιστή με δυνατότητα κλήσης μόντεμ τηλεφώνου, καλεί τυχαία αριθμούς τηλεφώνου μέχρι να χτυπά ένα μόντεμ που απαντά ένας άλλος υπολογιστής και, στη συνέχεια, επιχειρεί να προγραμματίσει τον τηλεφωνητή με το δικό του πρόγραμμα, έτσι ώστε ο δεύτερος υπολογιστής να αρχίσει επίσης να καλεί τυχαίους αριθμούς, αναζητώντας έναν άλλο υπολογιστή για προγραμματισμό. Το πρόγραμμα εξαπλώνεται γρήγορα εκθετικά μέσω ευαίσθητων υπολογιστών και μπορεί να αντιμετωπιστεί μόνο από ένα δεύτερο πρόγραμμα που ονομάζεται VACCINE

Η ιδέα εξερευνήθηκε περαιτέρω σε δύο μυθιστορήματα του 1972, When HARLIE Was One του David Gerrold και The Terminal Man του Michael Crichton, και έγινε κύριο θέμα του μυθιστορήματος του 1975 The Shockwave Rider του John Brunner

Η ταινία επιστημονικής φαντασίας του 1973 του Michael Crichton Westworld έκανε μια πρώιμη αναφορά στην έννοια του ιού υπολογιστή, που είναι ένα κεντρικό θέμα της πλοκής που κάνει τα android να λειτουργούν ακατάστατα.[119][απαιτείται καλύτερη πηγή] Ο χαρακτήρας του Alan Oppenheimer συνοψίζει το πρόβλημα δηλώνοντας ότι «...υπάρχει ένα σαφές μοτίβο εδώ που προτείνει μια αναλογία με μια διαδικασία μολυσματικής νόσου, που εξαπλώνεται από