Virus informàtic

Autor:
Data de publicació: 26-06-2021

Un virus informàtic[1] és un tipus de programa informàtic que, quan s'executa, es replica modificant altres programes informàtics i inserint el seu propi codi. [2] Si aquesta replicació té èxit, es diu que les àrees afectades estan "infectades" amb un virus informàtic. [4][5]

Els virus informàtics generalment requereixen un programa amfitrió. [2] El virus escriu el seu propi codi al programa host. Quan el programa s'executa, el programa de virus escrit s'executa primer, causant infecció i danys. Un cuc de l'ordinador no necessita un programa d'amfitrió, ja que és un programa independent o un fragment de codi. Per tant, no està restringit pel programa d'amfitrió,però pot executar-se de manera independent i activa dur a terme atacs. [6]

Els virus informàtics causen milers de milions de dòlars de danys econòmics cada any. [8]

El 1989, la divisió de la indústria del software ADAPSO va publicar Dealing With Electronic Vandalism,[9] en la qual seguien el risc de pèrdua de dades pel "risc afegit de perdre la confiança dels clients". [10][11][12]

Com a resposta, s'han desenvolupat eines antivirus de codi obert gratuïtes i una indústria de software antivirus ha crescut, venent o distribuint lliurement la protecció antivirus als usuaris de diversos sistemes operatius. [13]

Visió general
Els escriptors de virus utilitzen enganys d'enginyeria social i exploten un coneixement detallat de les vulnerabilitats de seguretat per infectar inicialment els sistemes i propagar el virus. La gran majoria de virus dirigeixen sistemes que executen Microsoft Windows,[14][15] [16]utilitzant una varietat de mecanismes per infectar nous hostes,[17] i sovint utilitzant estratègies complexes anti-detecció / sigil per eludir el software antivirus. [18][19][20]Els motius per crear virus poden incloure la recerca de beneficis (per exemple, amb ransomware),el desig d'enviar un missatge polític, la diversió personal, per demostrar que existeix una vulnerabilitat en el software, per sabotatge i negació del servei,o simplement perquè volen explorar problemes de ciberseguretat, vida artificial i algoritmes evolutius. [22]

Els danys[8] es deuen a causar fallades del sistema, malmetre dades, malgastar recursos informàtics, augmentar els costos de manteniment o robar informació personal. Tot i que cap software antivirus pot descobrir tots els virus informàtics (especialment els nous), els investigadors de seguretat informàtica busquen activament noves maneres de permetre que les solucions antivirus detectin de manera més efectiva virus emergents, abans que es distribueixin àmpliament. [23]

Altres programes maliciosos
Article principal: software maliciós

El terme "virus" també s'utilitza malament per extensió per referir-se a altres tipus de software maliciós. "Malware" engloba virus informàtics juntament amb moltes altres formes de software maliciós, com ara "cucs" informàtics, ransomware, software espia, adware, cavalls de troia, keyloggers, rootkits, bootkits, objecte d'ajuda del navegador maliciós (BHOs), i altres programes maliciosos. La majoria de les amenaces actives de malware són programes de cavalls troians o cucs d'ordinador en lloc de virus informàtics. El terme virus informàtic, encunyat per Fred Cohen el 1985, és un error. [24] Els virus sovint realitzen algun tipus d'activitat nociva en ordinadors host infectats, com ara

l'adquisició d'espai de disc dur o el temps de la unitat central de processament (CPU), l'accés i el robatori d'informació privada (per exemple, números de targetes de crèdit, números de targeta de dèbit, números de telèfon, noms, adreces de correu electrònic, contrasenyes, informació bancària, adreces de la casa, etc.), la corrupció de les dades, la visualització de missatges polítics, humorísticso amenaçadors a la pantalla de l'usuari, l'emmagatzematge dels seus contactes de correu electrònic, el registre de les seves claus o, fins i tot, l'ús de l'ordinador. No obstant això, no tots els virus porten una"càrrega útil"destructiva i intenten amagar-se, la característica definidora dels virus és que són programes informàtics auto-replicants que modifiquen un altre software sense el consentiment de l'usuari injectant-se en aquests programes, similar a un virus biològic que es replica dins de les cèl·lules vives.

Desenvolupament històric
Vegeu també: Història del software antivirus, Història del ransomware, i Història del software maliciós

Més informació: Cronologia de virus i cucs informàtics notables

Primers treballs acadèmics en programes d'auto-replicació
Més informació: Recerca en malware

El primer treball acadèmic sobre la teoria dels programes informàtics auto-replicants[25] va ser realitzat el 1949 per John von Neumann que va donar conferències a la Universitat d'Illinois sobre la "Teoria i Organització d'Autòmats Complicats". El treball de von Neumann va ser publicat més tard com la "Teoria de l'autoproducció d'autòmats". En el seu assaig, von Neumann va descriure com un programa informàtic podria ser dissenyat per reproduir-se. [26] El disseny de Von Neumann per a un programa informàtic que s'autoprodueix es considera el primer virus informàtic del món, i és considerat el "pare" teòric de la virologia informàtica. [27] El 1972, Veith Risak va basar-se directament en el treball de von Neumann sobre l'auto-replicació, va publicar el seu article "Selbstreproduzierende Automaten mit minimaler Informationsübertragung" (Autoproducció d'autòmats amb un mínim intercanvi d'informació). [28] L'article descriu un virus totalment funcional escrit en llenguatge de programació assemblador per a un sistema informàtic SIEMENS 4004/35. El 1980 Jürgen Kraus va escriure la seva tesi "Selbstreproduktion bei Programmen" (Auto-reproducció de programes) a la Universitat de Dortmund. [29] En el seu treball, Kraus va postular que els programes informàtics es poden comportar d'una manera similar als virus biològics.

ciència-ficció
La primera descripció coneguda d'un programa d'autoproducció en ficció és en el relat curt de 1970 The Scarred Man de Gregory Benford que descriu un programa informàtic anomenat VIRUS que, quan s'instal·la en un ordinador amb capacitat de marcatge de mòdem telefònic, marca aleatòriament els números de telèfon fins que colpeja un mòdem que és respost per un altre ordinador, i després intenta programar l'ordinador de resposta amb el seu propi programa, de manera que el segon ordinador també començarà a marcar números aleatoris, a la recerca d'un altre ordinador a programar. El programa s'estén ràpidament exponencialment a través d'ordinadors susceptibles i només pot ser contrarestat per un segon programa anomenat VACCINE. [30]

La idea va ser explorada encara més en dues novel·les de 1972, When HARLIE Was One de David Gerrold i The Terminal Man de Michael Crichton, i es va convertir en un tema important de la novel·la de 1975 The Shockwave Rider de John Brunner. [31]

La pel·lícula de ciència-ficció westworld de Michael Crichton de 1973 va fer una menció primerenca al concepte de virus informàtic, sent un tema central de trama que fa que els androides executin amok. [32] El personatge d'Alan Oppenheimerresumeix el problema afirmant que "... aquí hi ha un patró clar que suggereix una analogia a un procés de malalties infeccioses, que s'estén des d'un ... zona a la següent." A la qual cosa s'afirma les respostes: "Potser hi ha similituds superficials amb la malaltia" i, "he de confessar que em costa creure en una malaltia de maquinària". [33]

Primers exemples

El virus MacMag 'Pau Universal', tal com es mostra en un Mac el març de 1988

El virus Creeper va ser detectat per primera vegada a ARPANET, el precursor d'Internet, a principis de la dècada de1970. [35] Creeper va utilitzar l'ARPANET per infectar ordinadors PDP-10 de DEC que executaven el sistema operatiu TENEX. [36] Creeper va accedir a través de l'ARPANET i es va copiar al sistema remot on es mostrava el missatge " Sóc l'esgarrifós, agafa'm si pots!". El programa Reaper s'ha creat per suprimir Creeper. [37]

El 1982, un programa anomenat"Elk Cloner"va ser el primer virus informàtic personal que va aparèixer "en estat salvatge", és a dir, fora de l'ordinador únic o laboratori d'ordinadors on es va crear. Escrit el 1981 per Richard Skrenta, un estudiant de novè grau a la Mount Lebanon High School prop de Pittsburgh,es va unir al sistema operatiu Apple DOS 3.3 i es va estendre a través del disquet. [38] En el seu 50è ús s'activaria el virus Elk Cloner, infectant l'ordinador personal i mostrant un poema curt que començava "Elk Cloner: El programa amb una personalitat".

El 1984 Fred Cohen de la Universitat del Sud de Califòrnia va escriure el seu article "Computer Viruses – Theory and Experiments". [39] Va ser el primer article que va anomenar explícitament un programa d'autoproducció d'un "virus", un terme introduït pel mentor de Cohen, Leonard Adleman. El 1987, Fred Cohen va publicar una demostració que no hi ha cap algoritme que pugui detectar perfectament tots els virus possibles. [40] El virus teòric de compressióde Fred Cohen[41] era un exemple d'un virus que no era software maliciós(software maliciós),sinó que era putativament benèvol (ben intencionat). No obstant això, els professionals de l'antivirus no accepten el concepte de "virus benèvols", ja que qualsevol funció desitjada es pot implementar sense implicar un virus (la compressió automàtica, per exemple, està disponible a Windows a elecció de l'usuari). Qualsevol virus, per definició, farà canvis no autoritzats en un ordinador, cosa que no és desitjable encara que no es faci o es pretengui cap dany. La primera pàgina de l'Enciclopèdia del Virus del Dr. Solomon explica la indesitjabilitat dels virus, fins i tot aquells que no fan res més que reproduir-se. [42][5]

J.B. Gunn va publicar un article que descriu "funcionalitats útils del virus" sota el títol "Ús de funcions de virus per proporcionar un intèrpret virtual DAPL sota control d'usuari" el 1984. [43] El primer virus IBM PC en el "salvatge" va ser un virus del sector d'arrencada anomenat (c)Brain,creat el 1986 per Amjad Farooq Alvi i Basit Farooq Alvi a Lahore, Pakistan ,segons es diu per dissuadir la còpia no autoritzada del software que havien escrit. [45] El primer virus dirigit específicament a Microsoft Windows, WinVir va ser descobert a l'abril de 1992, dos anys després del llançament de Windows 3.0. [46] El virus no contenia cap crida de l'API delWindows, sinó que es basava en interrupcions del DOS. Uns anys més tard, al febrer de 1996, els hackers australians de la tripulació que escrivia el virus VLAD van crear el virus Bizatch (també conegut com a virus "Boza"), que va ser el primer virus conegut dirigit a Windows 95. A finals de 1997 es va llançar el virus xifrat i resident a la memòria Win32.Cabanas, el primer virus conegut que es va dirigir a Windows NT (també va poder infectar windows 3.0 i Windows 9x hosts). [47]

Fins i tot els ordinadors domèstics es van veure afectats per virus. El primer que va aparèixer al Commodore Amiga va ser un virus del sector d'arrencada anomenat virus SCA,que es va detectar el novembre de 1987. [48]

Operacions i funcions

Parts

Un virus informàtic viable ha de contenir una rutina de cerca,que localitza nous fitxers o nous discos que valen la pena dianes per a la infecció. En segon lloc, cada virus informàtic ha de contenir una rutina per copiar-se al programa que la rutina de cerca localitza. [49] Les tres parts principals del virus són:

Mecanisme d'infecció (també anomenat 'vector infecció'): Així és com el virus es propaga o es propaga. Un virus normalment té una rutina de cerca, que localitza fitxers nous o nous discos per a la infecció. [50]
Disparador: També conegut com a bomba lògica, aquesta és la versió compilada que es podria activar en qualsevol moment dins d'un fitxer executable quan s'executa el virus que determina l'esdeveniment o condició perquè la"càrrega útil"maliciosa " s'activi o es lliuri[51] com una data concreta, una hora concreta, presència particular d'un altre programa, capacitat del disc que excedeixi algun límit,[52] o un doble clic que obri un arxiu en particular. [53]
Càrrega útil:La "càrrega útil" és el cos o dades reals que duu a terme la finalitat maliciosa del virus. L'activitat de càrrega útil pot ser notable (per exemple, perquè provoca que el sistema s'alenteixi o es "congeli"), ja que la majoria de les vegades la "càrrega útil" en si és l'activitat nociva,[50] o algunes vegades no destructiva però distributiva, que s'anomena virus engany . [54]

Fases

Les fases del virus són el cicle de vida del virus informàtic, descrit mitjançant l'ús d'una analogia a la biologia. Aquest cicle de vida es pot dividir en quatre fases:

Fase adormida:El programa de virus està inactiu durant aquesta etapa. El programa virus ha aconseguit accedir a

l'ordinador o al software de l'usuari objectiu, però durant aquesta etapa, el virus no fa cap acció. El virus s'activarà eventualment pel "desencadenant" que estableix quin esdeveniment executarà el virus. No tots els virus tenen aquesta etapa. [50]
Fase de propagació:El virus comença a propagar-se, que es multiplica i es replica. El virus col·loca una còpia de si mateixa en altres programes o en determinades àrees del sistema del disc. Pot ser que la còpia no sigui idèntica a la versió de propagació; virus sovint "morph" o canvi per eludir la detecció per professionals de TI i software antivirus. Cada programa infectat ara contindrà un clon del virus, que entrarà en una fase de propagació. [50]
Fase de desencadenament:Un virus adormit es mou en aquesta fase quan s'activa, i ara realitzarà la funció per a la qual estava destinat. La fase de desencadenament pot ser causada per una varietat d'esdeveniments del sistema, incloent un recompte de les vegades que aquesta còpia del virus ha fet còpies de si mateix. [50] El detonant pot ocórrer quan un empleat és cessat de la seva feina o després d'un període de temps determinat, per tal de reduir la sospita.
Fase d'execució: Aquest és el treball real del virus, on s'alliberarà la "càrrega útil". Pot ser destructiu, com ara suprimir fitxers del disc, bloquejar el sistema o corrompre fitxers o relativament inofensius, com ara aparèixer missatges humorístics o polítics a la pantalla. [50]

Dianes d'infecció i tècniques de replicació
Els virus informàtics infecten una varietat de subsistemes diferents en els seus ordinadors i software d'amfitrió. [55] Una manera de classificar els virus és analitzar si resideixen en executables binaris (com ara . EXE o .COM fitxers),fitxers de dades (com ara documents de Microsoft Word o fitxers PDF),o en el sector d'arrencada del disc dur de l'amfitrió (o alguna combinació de tots aquests). [56][57]

Residents vs virus no residents
Un virus resident a la memòria (o simplement "virus resident") s'instal·la com a part del sistema operatiu quan s'executa, després del qual roman en RAM des del moment en què l'ordinador s'arrenca fins que s'apaga. Els virus residents sobreescriu el codi de manipulació o altres funcions,i quan el sistema operatiu intenta accedir al sector del fitxer o disc de destinació, el codi virus intercepta la sol·licitud i redirigeix el flux de control al mòdul de replicació, infectant l'objectiu. En canvi, un virus no resident a la memòria (o "virus no resident"), quan s'executa, escaneja el disc per als objectius, els infecta i surt (és a dir, no roman a la memòria després d'executar-lo). [58][59][60]

Virus de macro
Moltes aplicacions habituals, com ara el Microsoft Outlook i el Microsoft Word,permeten incrustar programes de macro en documents o correus electrònics, de manera que els programes es poden executar automàticament quan s'obre el document. Un virus de macro (o "virus del document") és un virus que s'escriu en un idioma de macro i s'incrusta en aquests documents de manera que quan els usuaris obren el fitxer, el codi virus s'executa i pot infectar l'ordinador de l'usuari. Aquesta és una de les raons per les quals és perillós obrir fitxers adjunts inesperats o sospitosos als correus electrònics. [61] Tot i que no obrir fitxers adjunts en correus electrònics de persones o organitzacions desconegudes pot ajudar a reduir la probabilitat de contraure un virus, en alguns casos, el virus està dissenyat perquè el correu electrònic sembli d'una organització de bona reputació (per exemple, una empresa bancària o de targeta de crèdit important).

Virus del sector d'arrencada
Els virus del sector d'arrencada s'adrecen específicament al sector d'arrencada i/o al Registre d'arrencada mestre[63] (MBR) de la unitat de disc durde la màquina, unitat d'estat sòlido suport d'emmagatzematge extraïble(unitats flaix, disquets,etc.). [56][64][65]

La forma més comuna de transmissió de virus informàtics en el sector d'arrencada són els mitjans físics. En llegir el VBR de la unitat, el disquet infectat o la unitat flaix USB connectada a l'ordinador transferiran dades i, a continuació, modificaran o substituiran el codi d'arrencada existent. La propera vegada que un usuari intenti iniciar l'escriptori, el virus es carregarà i s'executarà immediatament com a part del registre d'arrencada mestre. [66]

Virus del correu electrònic
Els virus de correu electrònic són virus que intencionadament, en lloc de accidentalment, utilitzen el sistema de correu electrònic per difondre's. Tot i que els fitxers infectats per virus es poden enviar accidentalment com a fitxers adjunts de correu electrònic,els virus de correu electrònic són conscients de les funcions del sistema de correu electrònic. Generalment s'adrecen a un tipus específic de sistema de correu electrònic(Microsoft Outlook és el més utilitzat), recullen adreces de correu electrònic de diverses fonts, i poden afegir còpies d'ells mateixos a tots els correus electrònics enviats, o poden generar missatges de correu electrònic que continguin còpies d'ells mateixos com a fitxers adjunts. [66]

Tècniques de sigil·li
Per evitar la detecció per part dels usuaris, alguns virus utilitzen diferents tipus d'enganys. Alguns virus antics,

especialment a la plataforma DOS, assegureu-vos que la data "última modificació" d'un fitxer host es manté igual quan el fitxer està infectat pel virus. Aquest enfocament no enganya el softwareantivirus, però, especialment aquells que mantenen i daten controls cíclics de redundància en els canvis de fitxer. [66] Alguns virus poden infectar fitxers sense augmentar les seves mides ni danyar els fitxers. Ho aconsegueixen sobreescrivint les àrees no aprofitades dels fitxers executables. Aquests s'anomenen virus de cavitat. Per exemple, el virus CIH, o el virus de Txernòbil, infecta fitxers executables portàtils. Com que aquests fitxers tenen molts espais buits, el virus, que tenia 1 KB de longitud, no s'ha afegit a la mida del fitxer. [66] Alguns virus intenten evitar la detecció matant les tasques associades al software antivirus abans de detectar-los (per exemple, Conficker). A la dècada de 2010, a mesura que els ordinadors i els sistemes operatius creixen més i més complexos, cal actualitzar o substituir tècniques d'amagatall antigues. La defensa d'un ordinador contra virus pot exigir que un sistema de fitxers migri cap a permisos detallats i explícits per a tot tipus d'accés a fitxers. [cal citació]

Interceptacions de sol·licitud de lectura
Mentre que alguns tipus de software antivirus utilitzen diverses tècniques per contrarestar els mecanismes de sigil, un cop es produeix la infecció qualsevol recurs per "netejar" el sistema és poc fiable. Als sistemes operatius Microsoft Windows, el sistema de fitxers NTFS és propietari. Això deixa un software antivirus una mica alternatiu, però per enviar una sol·licitud "llegida" als fitxers de Windows que gestionen aquestes sol·licituds. Alguns virus enganyen el software antivirus interceptant les seves sol·licituds al sistema operatiu. Un virus es pot amagar interceptant la sol·licitud de lectura del fitxer infectat, manejant la pròpia sol·licitud i retornant una versió no infectada del fitxer al software antivirus. La intercepció es pot produir per injecció de codi dels fitxers reals del sistema operatiu que gestionarien la sol·licitud de lectura. Per tant, un software antivirus que intenti detectar el virus no podrà llegir el fitxer infectat o, la sol·licitud "llegir" se servirà amb la versió no infectada del mateix fitxer. [70]

L'únic mètode fiable per evitar virus "sigil·loses" és "reiniciar" des d'un mitjà que se sap que és "clar". A continuació, es pot utilitzar software de seguretat per comprovar els fitxers del sistema operatiu adormits. La majoria del software de seguretat es basa en signatures de virus, o utilitzen heurística. [71]El software de seguretat també pot utilitzar una base de dades de fitxers"hashes"per a arxius del sistema operatiu Windows, de manera que el software de seguretat pugui identificar arxius alterats, i sol·licitar suports d'instal·lació de Windows per reemplaçar-los per versions autèntiques. En versions anteriors del Windows, les funcions hash criptogràfiques de fitxers del sistema operatiu Windows emmagatzemades al Windows —per permetre comprovar la integritat/autenticitat dels fitxers— es podrien sobreescriure de manera que el Verificador de fitxers de sistema informés que els fitxers del sistema alterats són autèntics, de manera que l'ús de hashs de fitxers per escanejar fitxers alterats no sempre garantiria trobar una infecció. [73]

Autoavaluació
Vegeu també: Codi d'automodifiquen

La majoria dels programes antivirus moderns intenten trobar patrons de virus dins dels programes ordinaris escanejant-los per a les anomenades signatures de virus. [74] Malauradament, el terme és enganyós, ja que els virus no tenen signatures úniques de la manera que fan els éssers humans. Aquesta "signatura" de virus és només una seqüència de bytes que busca un programa antivirus perquè se sap que forma part del virus. Un terme millor seria "cadenes decerca". Diferents programes antivirus empraran diferents cadenes de cerca, i de fet diferents mètodes de cerca, a l'hora d'identificar virus. Si un antivirus troba aquest patró en un fitxer, realitzarà altres comprovacions per assegurar-se que ha trobat el virus, i no només una seqüència coincident en un fitxer innocent, abans de notificar a l'usuari que el fitxer està infectat. A continuació, l'usuari pot eliminar, o (en alguns casos) "netejar" o "curar" el fitxer infectat. Alguns virus utilitzen tècniques que dificulten la detecció mitjançant signatures, però probablement no impossibles. Aquests virus modifiquen el seu codi sobre cada infecció. És a dir, cada fitxer infectat conté una variant diferent del virus. [cal citació]

Virus xifrats
Un mètode per eludir la detecció de signatura és utilitzar el xifrat simple per xifrar (codificar) el cos del virus, deixant només el mòdul de xifrat i una clau criptogràfica estàtica en text clar que no canvia d'una infecció a una altra. [75] En aquest cas, el virus consisteix en un petit mòdul de desencriptatge i una còpia xifrada del codi del virus. Si el virus s'encripta amb una clau diferent per a cada fitxer infectat, l'única part del virus que roman constant és el mòdul de desencriptatge, que (per exemple) s'afegiria al final. En aquest cas, un antivirus no pot detectar directament el virus mitjançant signatures, però encara pot detectar el mòdul de desencriptatge, que encara fa possible la detecció indirecta del virus. Atès que aquestes serien claus simètrics, emmagatzemades a l'host infectat, és totalment possible desxifrar el virus final, però probablement no és necessari, ja que el codi automodificador és una raresa que trobar alguns pot ser motiu suficient perquè els escàners de virus almenys "marquin" el fitxer com a sospitós. [cal citació] Una manera antiga però compacta serà l'ús d'operacions aritmètiques com l'addició o resta i l'ús de condicions lògiques com XORing,[76] on cada byte d'un virus és amb una constant de manera que l'operació exclusiva només s'havia de repetir per al desencriptació. És sospitós que un codi es modifiqui, de manera que el codi per fer el xifrat/desencriptació pot formar

part de la signatura en moltes definicions de virus. [cal citació] Un enfocament més senzill i antic no va utilitzar una clau, on el xifrat consistia només en operacions sense paràmetres, com ara increment i disminució, rotació a bits, negació aritmètica i lògica NOT.[76] Alguns virus, anomenats virus polimòrfics, empraran un mitjà d'encriptació dins d'un executable en el qual el virus està xifrat sota certs esdeveniments, com ara que l'escàner de virus estigui desactivat. [77] Això s'anomena criptomoneda.

Codi polimòrfic

El codi polimòrfic va ser la primera tècnica que va suposar una greu amenaça per als escàners de virus. Igual que els virus xifrats regulars, un virus polimòrfic infecta fitxers amb una còpia xifrada de si mateixa, que és descodificada per un mòdul de desxifrat. En el cas dels virus polimòrfics, però, aquest mòdul de desxifrat també es modifica en cada infecció. Per tant, un virus polimòrfic ben escrit no té parts que romanguin idèntiques entre infeccions, la qual cosa dificulta molt la detecció directa mitjançant "signatures". [78]El software antivirus pot detectar-lo desxifrant els virus utilitzant un emulador,o mitjançant l'anàlisi estadística de patrons del cos del virus xifrat. Per habilitar el codi polimòrfic, el virus ha de tenir un motor polimòrfic (també anomenat "motor mutant" o "motor demutació") en algun lloc del seu cos xifrat. Vegeu el codi polimòrfic per obtenir detalls tècnics sobre el funcionament d'aquests motors. [80]

Alguns virus utilitzen codi polimòrfic de manera que limita significativament la taxa de mutació del virus. Per exemple, es pot programar un virus per mutar només lleugerament amb el temps, o es pot programar per abstenir-se de mutar quan infecta un fitxer d'un ordinador que ja conté còpies del virus. L'avantatge d'utilitzar un codi polimòrfic tan lent és que dificulta que professionals i investigadors antivirus obtinguin mostres representatives del virus, ja que els fitxers "esquers" que s'infecten en una sola carrera solen contenir mostres idèntiques o similars del virus. Això farà més probable que la detecció per part de l'escàner del virus sigui poc fiable, i que alguns casos del virus puguin evitar la detecció.

Codi metamòrfic

Per evitar ser detectats per l'emulació, alguns virus es reescriuen completament cada vegada que han d'infectar nous executables. Es diu que els virus que utilitzen aquesta tècnica estan en codi metamòrfic. Per permetre el metamorfisme es necessita un "motor metamòrfic". Un virus metamòrfic sol ser molt gran i complex. Per exemple, W32/Símil consistia en més de 14.000 línies de codi de llenguatge assemblador, el 90% de les quals forma part del motor metamòrfic. [81]

Vulnerabilitats i vectors d'infecció

Errors de software

Com que el software sovint està dissenyat amb característiques de seguretat per evitar l'ús no autoritzat dels recursos del sistema, molts virus han d'explotar i manipular errors de seguretat,que són defectes de seguretat en un sistema o software d'aplicació, per difondre's i infectar altres ordinadors. Les estratègies de desenvolupament de software que produeixen un gran nombre d'"errors" generalment també produiran potencials "forats" o "entrades" explotables per al virus.

Enginyeria social i males pràctiques de seguretat

Per replicar-se, cal permetre que un virus executi codi i escrigui a la memòria. Per aquest motiu, molts virus s'adhereixen a fitxers executables que poden formar part de programes legítims (veure injecció de codi). Si un usuari intenta iniciar un programa infectat, el codi del virus es pot executar simultàniament. [83] En sistemes operatius que utilitzen extensions de fitxers per determinar associacions de programes (com microsoft Windows), les extensions poden estar ocultes a l'usuari per defecte. Això permet crear un fitxer d'un tipus diferent del que sembla a l'usuari. Per exemple, es pot crear un executable i anomenar-lo "imatge.png.exe", en el qual l'usuari només veu "imatge.png" i per tant assumeix que aquest fitxer és una imatge digital i molt probablement és segur, però quan s'obre, executa l'executable a la màquina client. [84] Els virus es poden instal·lar en suports extraïbles, com ara unitats flaix. Les unitats es poden deixar en un aparcament d'un edifici governamental o d'un altre objectiu, amb l'esperança que els usuaris curiosos insereixin la unitat en un ordinador. En un experiment de 2015, investigadors de la Universitat de Michigan van trobar que el 45-98 per cent dels usuaris connectarien una unitat flaix d'origen desconegut. [85]

Vulnerabilitat de diferents sistemes operatius

La gran majoria de virus dirigeixen sistemes que executen el Microsoft Windows. Això és degut a la gran quota de mercat de Microsoft d'usuaris d'ordinadors d'escriptori. [86] La diversitat de sistemes de software en una xarxa limita el potencial destructiu de virus i malware. [87] Els sistemes operatius de codi obert com Linux permeten als usuaris triar entre una varietat d'entorns d'escriptori,eines d'embalatge, etc., el que significa que el codi maliciós dirigit a qualsevol d'aquests sistemes només afectarà un subconjunt de tots els usuaris. Molts usuaris de Windows estan executant el mateix conjunt d'aplicacions, permetent que els virus es propaguin ràpidament entre els sistemes Microsoft Windows orientant-se a les mateixes gestes en un gran nombre d'amfitrions. [14][15][16][88]

Tot i que Linux i Unix en general sempre han impedit nativament als usuaris normals fer canvis a l'entorn del sistema operatiu sense permís, els usuaris de Windows generalment no poden fer aquests canvis, el que significa que els virus poden obtenir fàcilment el control de tot el sistema en màquines Windows. Aquesta diferència s'ha mantingut en part a causa de l'ús generalitzat de comptes d'administrador en versions contemporànies com Windows XP. El 1997, els investigadors van crear i alliberar un virus per a Linux, conegut com a"Bliss". [89] Tanmateix, Bliss requereix que l'usuari l'executi explícitament, i només pot infectar programes que l'usuari tingui accés a modificar. A diferència dels usuaris de Windows, la majoria dels usuaris d'Unix no inicien la sessió com a administrador, o "usuari arrel",excepte per instal·lar o configurar software; com a resultat, fins i tot si un usuari va córrer el virus, no va poder danyar el seu sistema operatiu. El virus de la Felicitat mai es va generalitzar, i continua sent principalment una curiositat investigadora. Més tard, el seu creador va publicar el codi font a Usenet,permetent als investigadors veure com funcionava. [90]

Contramesures
Vegeu també: Malware § Vulnerabilitat a software maliciós, Antimalwarei Seguretat del navegador § Enduriment del navegador

software antivirus

Captura de pantalla del software antivirus ClamWin de codi obert que s'executa a Wine on Ubuntu Linux

Molts usuaris instal·len software antivirus que pot detectar i eliminar virus coneguts quan l'ordinador intenta descarregar o executar el fitxer executable (que es pot distribuir com un fitxer adjunt de correu electrònic, o en unitats flaix USB,per exemple). Alguns blocs de software antivirus coneguts llocs web maliciosos que intenten instal·lar software maliciós. El software antivirus no canvia la capacitat subjacent dels amfitrions per transmetre virus. Els usuaris han d'actualitzar el seu software regularment per apedaçar vulnerabilitats de seguretat ("forats"). El software antivirus també s'ha d'actualitzar periòdicament per reconèixer les últimes amenaces. Això es deu al fet que els hackers maliciosos i altres individus sempre estan creant nous virus. L'Institut Alemany AV-TEST publica avaluacions de software antivirus per a Windows[91] i Android. [92]

Alguns exemples de Microsoft Windows antivirus i software antimalware inclouen l'opcional Microsoft Security Essentials[93] (per a Windows XP, Vista i Windows 7) per a la protecció en temps real, l'eina d'eliminació de software maliciósde Windows[94] (ara inclosa amb Windows (Security) Updates a"Patch Tuesday",el segon dimarts de cada mes), i Windows Defender (una descàrrega opcional en el cas de Windows XP). [95] A més, diversos programes antivirus capaços estan disponibles per a la descàrrega gratuïta des d'Internet (normalment restringit a ús no comercial). [96] Alguns d'aquests programes gratuïts són gairebé tan bons com els competidors comercials. [97] Les vulnerabilitats de seguretat comunes s'assignen als ID de CVE i s'enumeren a la Base de Dades Nacional de Vulnerabilitat delsEstats Units. Secunia PSI[98] és un exemple de software, gratuït per a ús personal, que comprovarà que un PC tingui software vulnerable no actualitzat i intentarà actualitzar-lo. Les alertes d'estafa de ransomware i phishing apareixen com a notes de premsa al tauler d'anuncis del Centre de Denúncies de Delictes d'Internet. El ransomware és un virus que publica un missatge a la pantalla de l'usuari dient que la pantalla o el sistema romandran bloquejats o inutilitzables fins que es faci un pagament de rescat. El phishing és un engany en el qual l'individu maliciós pretén ser amic, expert en seguretat informàtica o un altre individu benèvol, amb l'objectiu de convèncer l'individu objectiu de revelar contrasenyes o altra informació personal.

Altres mesures preventives d'ús comú inclouen actualitzacions oportunes del sistema operatiu, actualitzacions de software, navegació acurada per Internet (evitant llocs web ombrívols) i la instal·lació de només software de confiança. [99] Alguns navegadors marquen llocs web que han estat notificats a Google i que Google ha confirmat com a software maliciós d'allotjament. [100][101]

Hi ha dos mètodes comuns que una aplicació de software antivirus utilitza per detectar virus, tal com es descriu a l'article de software antivirus. El primer, i amb diferència, el mètode més comú de detecció de virus és l'ús d'una llista de definicions de signatura de virus. Això funciona examinant el contingut de la memòria de l'ordinador (la seva memòria d'accés aleatori (RAM) i els sectors d'arrencada)i els fitxers emmagatzemats en unitats fixes o extraïbles (discs durs,

disquets o unitats flaix USB), i comparant aquests fitxers amb una base de dades de "signatures" de virus coneguts. Les signatures de virus són només cadenes de codi que s'utilitzen per identificar virus individuals; per a cada virus, el dissenyador antivirus intenta triar una cadena de signatura única que no es trobarà en un programa legítim. Diferents programes antivirus utilitzen diferents "signatures" per identificar virus. L'inconvenient d'aquest mètode de detecció és que els usuaris només estan protegits de virus que es detecten mitjançant signatures en la seva última actualització de definició de virus, i no estan protegits de nous virus (vegeu"atac de dia zero"). [102]

Un segon mètode per trobar virus és utilitzar un algoritme heurístic basat en comportaments comuns del virus. Aquest mètode pot detectar nous virus per als quals les empreses de seguretat antivirus encara no han definit una "signatura", però també dóna lloc a més falsos positius que l'ús de signatures. Els falsos positius poden ser disruptius, sobretot en un entorn comercial, ja que pot provocar que una empresa indique al personal que no utilitzi el sistema informàtic de l'empresa fins que els serveis informàtics hagin comprovat el sistema per detectar virus. Això pot alentir la productivitat dels treballadors habituals.

Estratègies i mètodes de recuperació

Es pot reduir el dany causat pels virus fent còpies de seguretat periòdiques de les dades (i dels sistemes operatius) en diferents suports, que o bé es mantenen aliens al sistema (la majoria de les vegades, com en un disc dur), només de lectura o no accessibles per altres motius, com l'ús de diferents sistemes de fitxers. D'aquesta manera, si les dades es perden a través d'un virus, es pot tornar a començar utilitzant la còpia de seguretat (que esperem que sigui recent). [103] Si es tanca una sessió de còpia de seguretat en suports òptics com CD i DVD, esdevé només de lectura i ja no es pot veure afectada per un virus (sempre que un virus o un fitxer infectat no s'hagi copiat al CD/DVD). Així mateix, es pot utilitzar un sistema operatiu en un CD d'arrencada per iniciar l'ordinador si els sistemes operatius instal·lats es tornen inutilitzables. Les còpies de seguretat en suports extraïbles s'han d'inspeccionar acuradament abans de la restauració. El virus de Gammima, per exemple, es propaga a través d'unitats flaixextraïbles. [104][105]

Eliminació de virus

Molts llocs web gestionats per empreses de software antivirus proporcionen escaneig gratuït de virus en línia, amb instal·lacions limitades de "neteja" (al cap i a la fi, l'objectiu dels llocs web és vendre productes i serveis antivirus). Alguns llocs web, com ara la filial de Google VirusTotal.com, permeten als usuaris penjar un o més fitxers sospitosos per ser escanejats i comprovats per un o més programes antivirus en una sola operació. [106][107] A més, diversos programes antivirus capaços estan disponibles per a la descàrrega gratuïta des d'Internet (normalment restringit a ús no comercial). [108] Microsoft ofereix una utilitat antivirus gratuïta opcional anomenada Microsoft Security Essentials,una eina d'eliminació de software maliciós de Windows que s'actualitza com a part del règim d'actualització regular de Windows, i una eina opcional antimalware (eliminació de software maliciós) windows Defender que s'ha actualitzat a un producte antivirus a Windows 8.

Alguns virus inhabiliten Restaura el sistema i altres eines importants del Windows, com ara l'Administrador de tasques i el CMD. Un exemple d'un virus que fa això és CiaDoor. Molts d'aquests virus es poden suprimir reiniciant l'ordinador, introduint windows"mode segur"amb xarxa i després utilitzant eines del sistema o escàner de seguretat de Microsoft. [109] Restaura el sistema a Windows Me, Windows XP, Windows Vista i Windows 7 poden restaurar el registre i els fitxers crítics del sistema a un punt de control anterior. Sovint un virus farà que un sistema "pengi" o "es congeli", i un reinici dur posterior renderitzarà un punt de restauració del sistema des del mateix dia malmès. Els punts de restauració de dies anteriors haurien de funcionar, sempre que el virus no estigui dissenyat per corrompre els fitxers de restauració i no existeixi en punts de restauració anteriors. [110][111]

Reinstal·lació del sistema operatiu

El Verificador de fitxers de sistema de Microsoft (millorat al Windows 7 i posteriors) es pot utilitzar per comprovar i reparar fitxers del sistema malmesos. [112] Restaurar una còpia anterior "neta" (sense virus) de tota la partició d'un disc clonat, una imatge de disco una còpia de seguretat és una solució: restaurar una "imatge" anterior del disc de còpia de seguretat és relativament senzill de fer, normalment elimina qualsevol malware, i pot ser més ràpid que "desinfectar" l'ordinador - o reinstal·lar i reconfigurar el sistema operatiu i des de programes, com es descriu a continuació, les preferències de l'usuari. [103] Reinstal·lar el sistema operatiu és una altra aproximació a l'eliminació de virus. És possible recuperar còpies de dades essencials de l'usuari mitjançant l'arrencada des d'un CD en viu, o connectant el disc dur a un altre ordinador i arrencant des del sistema operatiu del segon ordinador, tenint molta cura de no infectar aquest ordinador executant qualsevol programa infectat a la unitat original. A continuació, es pot tornar a formatar el disc dur original i el sistema operatiu i tots els programes instal·lats des del suport original. Un cop restaurat el sistema, s'han de prendre precaucions per evitar la reinfecció dels fitxers executables restaurats. [113]

Virus i Internet

Potser vol dir: Cuc de l'ordinador

Abans que les xarxes informàtiques es generalitzin, la majoria de virus es van estendre en suports extraïbles,particularment disquets. En els primers dies de l'ordinador personal,molts usuaris intercanviaven regularment informació i programes sobre disquets. Alguns virus es propaguen infectant programes emmagatzemats en aquests discos, mentre que d'altres s'instal·len en el sector d'arrencadadel disc, assegurant-se que s'executarien quan l'usuari arrenqués l'ordinador des del disc, normalment sense voler. Els ordinadors personals de l'època intentarien arrencar primer des d'un disquet si se n'hagués deixat un a la unitat. Fins que els disquets van caure en desús, aquesta va ser l'estratègia d'infecció més reeixida i els virus del sector d'arrencada van ser els més comuns en el "salvatge" durant molts anys. Els virus informàtics tradicionals van sorgir en la dècada de 1980, impulsats per la propagació d'ordinadors personals i l'augment resultant del sistema de taulers d'anuncis (BBS), l'ús del mòdem i l'intercanvi de software. Tauler d'anuncis– l'intercanvi de software impulsat va contribuir directament a la propagació dels programes de cavalls de Troia, i els virus es van escriure per infectar software popularment comercialitzat. El software shareware i bootleg eren vectors igualment comuns per a virus en BBSs.[114]Els virus poden augmentar les seves possibilitats de propagació a altres ordinadors infectant fitxers en un sistema de fitxers de xarxa o un sistema de fitxers al qual accedeixen altres ordinadors. [116]

Els virus macro s'han tornat comuns des de mitjan anys noranta. La majoria d'aquests virus s'escriuen en les llengües de seqüències per a programes de Microsoft, com ara microsoft Word i Microsoft Excel, i es distribueixen per tot el Microsoft Office infectant documents i fulls de càlcul. Atès que Word i Excel també estaven disponibles per a Mac OS,la majoria també es podia estendre als ordinadors Macintosh. Tot i que la majoria d'aquests virus no tenien la capacitat d'enviar missatges de correu electrònicinfectats, aquells virus que sí que van aprofitar la interfície del Microsoft Outlook Component Object Model (COM). [117] Algunes versions antigues de Microsoft Word permeten a les macros replicar-se amb línies en blanc addicionals. Si dos virus macro infecten simultàniament un document, la combinació dels dos, si també s'auto-replica, pot aparèixer com un "aparellament" dels dos i probablement es detectaria com un virus únic dels "pares". [119]

Un virus també pot enviar un enllaç d'adreça web com a missatge instantani a tots els contactes (per exemple, les adreces electròniques d'amics i companys) emmagatzemats en una màquina infectada. Si el destinatari, pensant que l'enllaç prové d'un amic (una font de confiança) segueix l'enllaç al lloc web, el virus allotjat al lloc pot ser capaç d'infectar aquest nou ordinador i continuar propagant- se. [120] Els virus que es van estendre mitjançant scripts entre llocs es van informar per primera vegada el 2002,[121] i es van demostrar acadèmicament el 2005. [122] Hi ha hagut múltiples casos de virus de scripts entre llocs en els "salvatges", explotant llocs web com MySpace (amb el cuc Samy) i Yahoo!.

Vegeu també

Botnet
Comparació de virus informàtics
Llei de frau i abús informàtic
Inseguretat informàtica
software criminal
Core Wars: un joc d'ordinador primerenc amb competidors semblants a virus
Criptomoneda
Registre del tecleig
software maliciós
Correu brossa (electrònic)
Estafa de suport tècnic: trucades telefòniques no sol·licitades d'una persona falsa de "suport tècnic", al·legant que l'ordinador té un virus o altres problemes
Cavall de Troia (informàtica)
Engany del virus
Recuperació de fitxers del Windows 7
Centre de manteniment del Windows (Centre deseguretat)
Zombie (informàtica)

Referències

^ "Internet baixa amb un virus". The New York Times. 6 d'agost de 2014.
^ Jump up to:un grup sanguini "Cuc vs. Virus: Quina és la diferència i importa?". Acadèmia D'Avast.Avast Software s.r.o. Recuperat el 9 de març de 2021.
^ Stallings, William (2012). Seguretat informàtica : principis i pràctica. Boston: Pearson. p. 182. ISBN 978-0-13-277506-9.

^ ? Aycock, John (2006). Virus informàtics i software maliciós. Springer. p. 14. ISBN978-0-387-30236-2.
^ Jump up to:un grup sanguini Alan Salomó (2011-06-14). "Tot sobre virus". VX Cels. Arxivat de l'original el 2012-01-17. Recuperat el 2014-07-17.
^ Sí, Sang-soo. (2012). Informàtica i les seves aplicacions: CSA 2012, Jeju, Corea, 22-25.11.2012. Springer. p. 515. ISBN 978-94-007-5699-1. OCLC 897634290.
^ Yu, Wei; Zhang, Nan; Fu, Xinwen; Zhao, Wei (octubre 2010). "Cucs i Contramesures Autodisciplinàries: Modelització i Anàlisi". IEEE Operacions sobre Sistemes Paral·lels i Distribuïts. 21 (10): 1501–1514. doi:10.1109/tpds.2009.161. ISSN 1045-9219. S2CID2242419.
^ Jump up to:un grup sanguini "Virus que et poden costar". Arxivat de l'original el 2013-09-25.
^ Eugene H. Spafford; Kathleen A. Heaphy; David J. Ferbrache (1989). Tractar el vandalisme electrònic. ADAPSO Divisió de la Indústria del software.
^ ?Ka-Boom: Anatomia d'un virus informàtic". InformacióWeek. 3 de desembre de 1990. p. 60.
^ "Trove". trove.nla.gov.au.
^ "Reacció del mercat de capitals als productes de TI defectuosos". DL.acm.org (Biblioteca Digital de l'ACM) (Associació de Maquinària Informàtica).
^ Granneman, Scott. «Virus de Linux vs. Windows». El Registre. Arxivat de l'original el 7 de setembre de 2015. Consultat setembre 4, 2015.
^ Jump up to:un grup sanguini Mookhey, K.K.; et al. (2005). Linux: Característiques de seguretat, auditoria i control. ISACA. p. 128. ISBN 9781893209787. Arxivat de l'original el 2016-12-01.
^ Jump up to:un grup sanguini Toxen, Bob (2003). Seguretat Real World Linux: Prevenció, detecció i recuperació d'intrusions. Sala Prentice Professional. p. 365. ISBN 9780130464569. Arxivat de l'original el 2016-12-01.
^ Jump up to:un grup sanguini Noyes, Katherine (3 d'agost de 2010). «Per què Linux és més segur que Windows». PCWorld. Arxivat de l'original el 2013-09-01.
^ Skoudis, Eduard (2004). "Mecanismes i objectius d'infecció". Malware: Lluita contra el codi maliciós. Sala Prentice Professional. 31-48. ISBN 9780131014053. Arxivat de l'original el 2017-03-16.
^ ? Aycock, John (2006). Virus informàtics i software maliciós. Springer. p. 27. ISBN978-0-387-30236-2.
^ Ludwig, Mark A. (1996). El petit llibre negre de virus informàtics: Volum 1, Les Tecnologies Bàsiques. pàg. ISBN 0-929408-02-0.
^ Harley, David; et al. (2001). Virus revelats. McGraw-Hill. p. 6. ISBN 0-07-222818-0.
^ Filiol, Eric (2005). Virus informàtics: de la teoria a les aplicacions. Springer. p. 8. ISBN978-2-287-23939-7.
^ Bell, David J.; et al., eds. (2004). "Virus". Cibercultura: Els conceptes clau. Encaminament. p. 154. ISBN 9780203647059.
^ Kaspersky, Eugene (21 de novembre de 2005). "La indústria antivirus contemporània i els seus problemes". Llum segura. Arxivat de l'original el 5 d'octubre de 2013.
^ Ludwig, Mark (1998). El llibre negre gegant de virus informàtics. Espectacle Low, Ariz: Àguila americana. p. 13. ISBN 978-0-929408-23-1.
^ El terme "virus de l'ordinador" no es va utilitzar en aquell moment.
^ von Neumann, John (1966). "Teoria de l'Autoproducció d'Autòmats" (PDF). Assajos sobre autòmats cel·lulars. Premsa de la Universitat d'Illinois: 66-87. Arxivat (PDF) de l'original el 13 de juny de 2010. Consultat el 10 de juny de 2010.
^ Éric Filiol, Virus informàtics: de la teoria a les aplicacions, Volum 1 Arxivat 2017-01-14 a la Wayback Machine, Birkhäuser, 2005, pàg.
^ Risak, Veith (1972), "Selbstreproduzierende Automaten mit minimaler Informationsübertragung", Zeitschrift für Maschinenbau und Elektrotechnik, arxivat de l'original el 2010-10-05
^ Kraus, Jürgen (febrer 1980), Selbstreproduktion bei Programmen (PDF), arxivat des de l'original (PDF) el 2015-07-14, consultat el 2015-05-08
^ Benford, Gregory (maig de 1970). "L'home cicatritzat". Venture Ciència Ficció. Vol. 4 núm. pàg.
^ Clute, John. ?«Brunner, John». L'Enciclopèdia de Ciència Ficció. Grup de publicació d'Orion. Recuperat el 30 de gener de 2013.
^ Sinopsi de l'IMDB de Westworld. Consultat el 28 de novembre de 2015.
^ Michael Crichton (21 de novembre de 1973). Westworld (pel·lícula). 201 S. Kinney Road, Tucson, Arizona, Estats Units: Metro-Goldwyn-Mayer. L'esdeveniment té lloc als 32 minuts. I aquí hi ha un patró clar que suggereix una analogia a un procés de malalties infeccioses, que s'estén d'una zona d'estació a una altra." "Potser hi ha similituds superficials amb la malaltia." "He de confessar que em costa creure en una malaltia de maquinària.
^ "Llista de virus". Arxivat de l'original el 2006-10-16. Recuperat el 2008-02-07.
^ Thomas Chen; Jean-Marc Robert (2004). "L'evolució de virus i cucs". Arxivat de l'original el 2013-08-09. Recuperat el 2009-02-16.
^ ? Parikka, Jussi (2007). Contagis digitals: una arqueologia mediàtica de virus informàtics. Nova York: Peter Lang. p. 50. ISBN 978-0-8204-8837-0. Arxivat de l'original el 2017-03-16.
^ Russell, Deborah; Gangemi, G.T. (1991). Conceptes bàsics de seguretat informàtica.Reilly. p. 86. ISBN 0-937175-71-4.

^ Jump up to:un grup sanguini Anick Jesdanun (1 de setembre de 2007). "La broma de l'escola comença 25 anys de problemes de seguretat". CNBC. Arxivat de l'original el 20 de desembre de 2014. Consultat el 12 d'abril de 2013.
^ Cohen, Fred (1984), Virus informàtics – Teoria i Experiments, arxivat de l'original el 2007-02-18
^ Cohen, Fred, Un virus informàtic indetectable arxivat el 2014-05-25 a la Wayback Machine, 1987, IBM
^ Burger, Ralph, 1991. Virus informàtics i protecció de dades,pàg.
^ Alan Salomó; Dmitri O Gryaznov (1995). Enciclopèdia del Virus del Dr. Solomon.Aylesbury, Buckinghamshire, Regne Unit: S & S International PLC. ISBN 1-897661-00-2.
^ Gunn, J.B. (juny de 1984). "Ús de funcions de virus per proporcionar un intèrpret APL virtual sota control de l'usuari". ACM SIGAPL APL Cita Quad Archive. ACM Nova York, NY, Estats Units d'Amèrica. 14 (4): 163–168. doi:10.1145/384283.801093. ISSN 0163-6006.
^ "Reparació del virus del sector d'arrencada". Antivirus.about.com. 2010-06-10. Arxivat de l'original el 2011-01-12. Recuperat el 2010-08-27.
^ "Amjad Farooq Alvi Inventor del primer PC Virus post de Zagham". YouTube. Arxivatde l'original el 2013-07-06. Recuperat el 2010-08-27.
^ "virus winvir". Arxivat de l'original el 8 d'agost de 2016. Consultat el 10 de juny de2016.
^ Grimes, Roger (2001). Codi mòbil maliciós: protecció antivirus per al Windows. Reilly. pàg. ISBN 9781565926820.
^ "Virus SCA". Centre de Proves de Virus, Universitat d'Hamburg. 1990-06-05. Arxivatde l'original el 2012-02-08. Consultat el 2014-01-14.
^ Ludwig, Mark (1998). El llibre negre gegant de virus informàtics. Espectacle Low, Ariz: Àguila americana. p. 15. ISBN 978-0-929408-23-1.
^ Jump up to:un b c d e f Stallings, William (2012). Seguretat informàtica : principis i pràctica. Boston: Pearson. p. 183. ISBN 978-0-13-277506-9.
^ Ludwig, Mark (1998). El llibre negre gegant de virus informàtics. Espectacle Low, Ariz: Àguila americana. p. 292. ISBN 978-0-929408-23-1.
^ "Conceptes bàsics de malware" (PDF). cs.colostate.edu. Arxivat (PDF) de l'original el 2016-05-09. Consultat el 2016-04-25.
^ Gregori, Pere (2004). Virus informàtics per a maniquís. Hoboken, NJ: Wiley Pub. p. 210. ISBN 0-7645-7418-3.
^ Szor, Pere (2005). L'art de la investigació i defensa de virus informàtics. Riu Upper Saddle, NJ: Addison-Wesley. p. 43. ISBN 0-321-30454-3.
^ Serazzi, Giuseppe; Zanero, Stefano (2004). "Models de Propagació de Virus Informàtics" (PDF). A Calzarossa, Maria Carla; Gelenbe, Erol (eds.). Eines i aplicacions de rendiment a sistemes en xarxa. Notes de conferència en Informàtica. Vol. 2965. pàg. Arxivat (PDF) de l'original el 2013-08-18. |volume= has extra text (help)
^ Jump up to:un grup sanguini Avoine, Gildas; et al. (2007). Seguretat del sistema informàtic: conceptes bàsics i exercicis resolts. Premsa EPFL / Premsa CRC. 21-22. ISBN 9781420046205. Arxivat de l'original el 2017-03-16.
^ Cervell, Marshall; Fenton, Wesley (abril 2000). "Com funcionen els virus informàtics". HowStuffWorks.com. Arxivat de l'original el 29 de juny de 2013. Consultat el 16 de juny de 2013.
^ Grimes, Roger (2001). Codi mòbil maliciós: protecció antivirus per al Windows. Reilly. pàg. ISBN 9781565926820.
^ Salomon, David (2006). Fonaments de Seguretat Informàtica. Springer. 47-48. ISBN9781846283413. Arxivat de l'original el 2017-03-16.
^ Polk, William T. (1995). Eines i Tècniques Antivirus per a Sistemes Informàtics. William Andrew (Elsevier). p. 4. ISBN 9780815513643. Arxivat de l'original el 2017-03-16.
^ Grimes, Roger (2001). "Virus macro". Codi mòbil maliciós: protecció antivirus per al Windows. Reilly. ISBN 9781565926820.
^ ? Aycock, John (2006). Virus informàtics i software maliciós. Springer. p. 89. ISBN9780387341880. Arxivat de l'original el 2017-03-16.
^ "What is boot sector virus?". Archived from the original on 2015-11-18. Retrieved 2015-10-16.
^ Anonymous (2003). Maximum Security. Sams Publishing. pp. 331–333. ISBN 9780672324598. Archived from the original on 2014-07-06.
^ Skoudis, Edward (2004). "Infection mechanisms and targets". Malware: Fighting Malicious Code. Prentice Hall Professional. pp. 37–38. ISBN 9780131014053. Archivedfrom the original on 2017-03-16.
^ Mishra, Umakant (2012). "Detecting Boot Sector Viruses- Applying TRIZ to Improve Anti-Virus Programs". SSRN Electronic Journal. doi:10.2139/ssrn.1981886. ISSN 1556-5068. S2CID 109103460.
^ Dave Jones. 2001 (December 2001). "Building an e-mail virus detection system for your network. Linux J. 2001, 92, 2-". Cite journal requires (help|journal=)
^ Béla G. Lipták, ed. (2002). Instrument engineers' handbook (3rd ed.). Boca Raton: CRC Press. p. 874. ISBN 9781439863442. Retrieved September 4, 2015.
^ "Computer Virus Strategies and Detection Methods" (PDF). Archived (PDF) from the original on 23 October 2013. Retrieved 2 September 2008.
^ Szor, Peter (2005). The Art of Computer Virus Research and Defense. Boston: Addison-Wesley. p. 285. ISBN 0-321-30454-3. Archived from the original on 2017-03-16.

^ Fox-Brewster, Thomas. "Netflix Is Dumping Anti-Virus, Presages Death Of An Industry". Forbes. Archived from the original on September 6, 2015. Retrieved September 4, 2015.
^ "How Anti-Virus Software Works". Stanford University. Archived from the original on July 7, 2015. Retrieved September 4, 2015.
^ "www.sans.org". Archived from the original on 2016-04-25. Retrieved 2016-04-16.
^ Jacobs, Stuart (2015-12-01). Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance. John Wiley & Sons. ISBN 9781119104711.
^ Bishop, Matt (2003). Computer Security: Art and Science. Addison-Wesley Professional. p. 620. ISBN 9780201440997. Archived from the original on 2017-03-16.
^ Jump up to:un grup sanguini John Aycock (19 September 2006). Computer Viruses and Malware. Springer. pp. 35–36. ISBN 978-0-387-34188-0. Archived from the original on 16 March 2017.
^ "What is a polymorphic virus? - Definition from WhatIs.com". SearchSecurity. Retrieved 2018-08-07.
^ Kizza, Joseph M. (2009). Guide to Computer Network Security. Springer. p. 341. ISBN 9781848009165.
^ Eilam, Eldad (2011). Reversing: Secrets of Reverse Engineering. John Wiley & Sons. p. 216. ISBN 9781118079768. Archived from the original on 2017-03-16.
^ "Virus Bulletin : Glossary – Polymorphic virus". Virusbtn.com. 2009-10-01. Archivedfrom the original on 2010-10-01. Retrieved 2010-08-27.
^ Perriot, Fredrick; Peter Ferrie; Peter Szor (May 2002). "Striking Similarities" (PDF). Archived (PDF) from the original on September 27, 2007. Retrieved September 9, 2007.
^ "Virus Bulletin : Glossary — Metamorphic virus". Virusbtn.com. Archived from the original on 2010-07-22. Retrieved 2010-08-27.
^ "Virus Basics". US-CERT. Archived from the original on 2013-10-03.
^ "Virus Notice: Network Associates' AVERT Discovers First Virus That Can Infect JPEG Files, Assigns Low-Profiled Risk". Archived from the original on 2005-05-04. Retrieved 2002-06-13.
^ "Users Really Do Plug in USB Drives They Find" (PDF).
^ "Operating system market share". netmarketshare.com. Archived from the original on 2015-05-12. Retrieved 2015-05-16.
^ This is analogous to how genetic diversity in a population decreases the chance of a single disease wiping out a population in biology
^ Raggi, Emilio; et al. (2011). Començant Per Ubuntu Linux. Apress. p. 148. ISBN9781430236276. Arxivat de l'original el 2017-03-16.
^ "McAfee descobreix el primer virus linux" (Nota de premsa). McAfee, a través d'Axel Boldt. 5 de febrer de 1997. Arxivat de l'original el 17 de desembre de 2005.
^ Boldt, Axel (19 de gener de 2000). «Bliss, unvirus'de Linux ". Arxivat de l'original el 14 de desembre de 2005.
^ "Informes detallats de prova —(Windows) usuari domèstic". AV-Test.org. Arxivat de l'original el 2013-04-07. Consultat el 2013-04-08.
^ "Informes de prova detallats - Dispositius mòbils Android". AV-Test.org. 2019-10-22. Arxivat de l'original el 2013-04-07.
^ "Elements bàsics de seguretat de Microsoft". Arxivat de l'original el 21 de juny de 2012. Consultat el 21 de juny de 2012.
^ "Eina d'eliminació de software maliciós". Arxivat de l'original el 21 de juny de 2012.Consultat el 21 de juny de 2012.
^ "Windows Defender". Arxivat de l'original el 22 de juny de 2012. Consultat el 21 de juny de 2012.
^ Rubenking, Neil J. (17 de febrer de 2012). "El millor Antivirus Lliure per al 2012". pcmag.com. Arxivat de l'original el 2017-08-30.
^ Rubenking, Neil J. (10 de gener de 2013). "El millor Antivirus per al 2013". pcmag.com. Arxivat de l'original el 2016-04-25.
^ Rubenking, Neil J. "Secunia Personal Software Inspector 3.0 Revisió i qualificació". PCMag.com. Arxivat de l'original el 2013-01-16. Recuperat el 2013-01-19.
^ "Guia de 10 passos per protegir-se contra virus". GrnLight.net. Arxivat de l'original el 24 de maig de 2014. Consultat el 23 maig 2014.
^ "Navegació segura de Google". Arxivat de l'original el 2014-09-14.
^ "Informar de software maliciós (URL) a Google". Arxivat de l'original el 2014-09-12.
^ Zhang, Yu; et al. (2008). "Un nou enfocament basat en la immunitat per a la detecció del virus PE de Windows". A Tang, Changjie; et al. (eds.). Mineria i Aplicacions Avançades de Dades: 4a Conferència Internacional, ADMA 2008, Chengdu, Xina, 8-10 d'octubre de 2008, Actes. Springer. p. 250. ISBN 9783540881919. Arxivat de l'original el 2017-03-16.
^ Jump up to:un grup sanguini "Els bons hàbits de seguretat | US-CERT". Arxivat de l'original el 2016-04-20. Recuperat el 2016-04-16.
^ "W32. Gammima.AG". Symantec. Arxivat de l'original el 2014-07-13. Recuperat el 2014-07-17.
^ "Virus! dins! Espai!". GrnLight.net. Arxivat de l'original el 2014-05-24. Recuperat el 2014-07-17.

^ "VirusTotal.com (filial de Google)". Arxivat de l'original el 2012-06-16.
^ "VirScan.org". Arxivat de l'original el 2013-01-26.
^ Rubenking, Neil J. "El millor antivirus lliure per al 2014". pcmag.com. Arxivat de l'original el 2017-08-30.
^ "Escàner de seguretat de Microsoft". Arxivat de l'original el 2013-06-29.
^ "Eliminació de virus -Ajuda". Arxivat de l'original el 2015-01-31. Consultat el 2015-01-31.
^ "W32. Gammima.AG Supressió — Supressió de l'Ajuda". Symantec. 2007-08-27. Arxivat de l'original el 2014-08-04. Recuperat el 2014-07-17.
^ "support.microsoft.com". Arxivat de l'original el 2016-04-07. Recuperat el 2016-04-16.
^ "www.us-cert.gov" (PDF). Arxivat (PDF) de l'original el 2016-04-19. Recuperat el 2016-04-16.
^ David Kim; Michael G. Solomon (17 de novembre de 2010). Fonaments de Seguretat dels Sistemes d'Informació. Jones i Bartlett Publishers. pàg. ISBN 978-1-4496-7164-8. Arxivat de l'original el 16 de març de 2017.
^ "Dècada de 1980 – Kaspersky IT Encyclopedia". Recuperat el 2021-03-16.
^ "Què és un virus informàtic?". Actlab.utexas.edu. 1996-03-31. Arxivat de l'original el 2010-05-27. Recuperat el 2010-08-27.
^ La guia definitiva per controlar el malware, el software espia, el suplantació d'identitat i el correu brossa. Realtimepublishers.com. 1 de gener de 2005. pàg. ISBN 978-1-931491-44-0. Arxivat de l'original el 16 de març de 2017.
^ Eli B. Cohen (2011). Navegar pels reptes de la informació. Informar la ciència. pàg. ISBN 978-1-932886-47-4. Arxivat de l'original el 2017-12-19.
^ Vesselin Bontchev. "Problemes d'identificació de virus de macro". FRISK Software Internacional. Arxivat de l'original el 2012-08-05.
^ "Facebook 'virus fotogràfic' es difon per correu electrònic". 2012-07-19. Arxivat de l'original el 2014-05-29. Consultat el 2014-04-28.
^ Berend-Jan Wever. "Error XSS a la pàgina d'inici de sessió del hotmail". Arxivat de l'original el 2014-07-04. Recuperat el 2014-04-07.
^ Wade Alcorn. "El virus dels scripts entre llocs". bindshell.net. Arxivat de l'original el2014-08-23. Recuperat el 2015-10-13.

Lectura posterior

Burger, Ralf (16 de febrer de 2010) [1991]. Virus informàtics i protecció de dades. àbac. p. 353. ISBN 978-1-55755-123-8.
? Granneman, Scott (6 d'octubre de 2003). «Virus de Linux vs. Windows». El Registre.
Ludwig, Mark (1993). Virus informàtics, vida artificial i evolució. Tucson, Arizona 85717: American Eagle Publications, Inc. ISBN 0-929408-07-1. Arxivat de l'original el 4 de juliol de 2008.
Mark Russinovich (novembre de 2006). Vídeo avançat de neteja de malware (Web (WMV / MP4)). Corporació Microsoft. Consultat el 24 juliol 2011.
? Parikka, Jussi (2007). Contagis digitals. Una arqueologia mediàtica de virus informàtics. Formacions Digitals. Nova York: Peter Lang. ISBN 978-0-8204-8837-0.

Enllaços externs

A Wikimedia Commons hi ha contingut multimèdia relatiu a: Virus de l'ordinador

Virus a Curlie (DMOZ)
Portal de seguretat de Microsoft
Lloc US Govt CERT (Computer Emergency Readiness Team)
'Computer Viruses – Teoria i Experiments' – L'article original de Fred Cohen, 1984
Hacking Away at the Counterculture d'Andrew Ross (On hacking, 1990)