# Antivirus

Autor:
Data de publicació: 26-06-2021

Software antivirus (abreujat al software AV),també conegut com a software antimalware, és un programa informàtic que s'utilitza per prevenir, detectar i eliminar software maliciós.

El software antivirus es va desenvolupar originalment per detectar i eliminar virus informàtics,d'aquí el nom. No obstant això, amb la proliferació d'altres tipus de software maliciós,el software antivirus va començar a proporcionar protecció contra altres amenaces informàtiques. En particular, el software antivirus modern pot protegir els usuaris de: objectes d'ajuda del navegador maliciosos (BHOs), segrestadors del
navegador, ransomware, keyloggers, backdoors, rootkits, cavalls de troia, cucs, LSPsmaliciosos
, marcadors, fraudtools, adware i spyware. [1] Alguns productes també inclouen protecció d'altres amenaces informàtiques,com ara URL infectades i malicioses, spam,atacs d'estafa i pesca de credencials, identitat en línia (privacitat), atacs de banca en línia, tècniques d'enginyeria social, amenaces persistents avançades (APT) i atacs DDoS de botnet. [2]

contingut

història
Més informació: Història dels virus informàtics

Vegeu també: Cronologia de virus i cucs informàtics notables

Període 1949-1980 (dies pre-antivirus)
Tot i que les arrels del virus informàtic es remunten a principis de 1949, quan el científic hongarès John von Neumann va publicar la "Teoria de l'autoproducció d'autòmats",[3] el primer virus informàtic conegut va aparèixer el 1971 i va ser anomenat el"virus Creeper". [4] Aquest virus informàtic va infectar ordinadors centrals PDP-10 que executava el sistema operatiu TENEX. [5][6]

El virus Creeper va ser finalment eliminat per un programa creat per Ray Tomlinson i conegut com"The Reaper". [7] Algunes persones consideren "El Semental" el primer software antivirus mai escrit - pot ser que sigui així, però és important tenir en compte que el Se carregador era en realitat un virus dissenyat específicament per eliminar el virus Creeper. [7]

El virus Creeper va ser seguit per altres virus. El primer conegut que va aparèixer "en estat salvatge" va ser"Elk Cloner",el 1981, que va infectar els ordinadors Apple II. [9][10][11]

El 1983, fred Cohen va encunyar el terme "virus informàtic" en un dels primers articles acadèmics publicats sobre virus informàtics. [12] Cohen va utilitzar el terme "virus informàtic" per descriure un programa que: "afectar altres programes informàtics modificant-los de manera que inclogués una còpia (possiblement evolucionada) de si mateixa." [13] (tingueu en compte que una definició més recent i precisa del virus informàtic ha estat donada per l'investigador de seguretat hongarès Péter Sz?r: "un codi que replica recursivament una còpia possiblement evolucionada de si mateix"). [14]

El primer PC d'IBM compatible amb el virus informàtic "en estat salvatge", i una de les primeres infeccions reals generalitzades, va ser"Brain"el 1986. Des de llavors, el nombre de virus ha crescut exponencialment. [16] La majoria

dels virus informàtics escrits a principis i mitjans de la dècada de 1980 es limitaven a l'auto-reproducció i no tenien cap rutina específica de danys incorporada al codi. Això va canviar quan cada vegada més programadors es van familiaritzar amb la programació de virus informàtics i van crear virus que manipulaven o fins i tot destruïen dades en ordinadors infectats. [18]

Abans que la connectivitat a Internet fos generalitzada, els virus informàtics normalment es propagaven per disquets infectats. El software antivirus va entrar en ús, però es va actualitzar relativament poc freqüentment. Durant aquest temps, els verificadors de virus essencialment van haver de comprovar els fitxers executables i els sectors d'arrencada de disquets i discs durs. No obstant això, a mesura que l'ús d'Internet es va fer comú, els virus van començar a estendre's en línia. [19]

Període 1980-1990 (primers dies)
Hi ha reclamacions de competidors per haver estat el creador del primer producte antivirus. Possiblement, la primera eliminació documentada públicament d'un virus informàtic "en estat salvatge" (és a dir, el "virus de Viena") va ser realitzada per Bernd Fix el 1987. [20][21]

El 1987, Andreas Lüning i Kai Figge, que van fundar G Data Software el 1985, van llançar el seu primer producte antivirus per a la plataforma Atari ST. [22] El 1987 també es va publicar l'assassí del virus final (UVK). [23] Aquest va ser l'assassí estàndard de virus de la indústria de facto per a l'Atari ST i Atari Falcon,l'última versió del qual (versió 9.0) va ser llançat a l'abril de 2004. El 1987, als Estats Units, John McAfee va fundar l'empresa McAfee (formava part d'Intel Security)i, a finals d'aquest any, va llançar la primera versió de VirusScan. [25] També el 1987 (a Txecoslovàquia),Peter Paško, Rudolf Hrubý i Miroslav Trnka van crear la primera versió de l'antivirus NOD. [26]

El 1987, Fred Cohen va escriure que no hi ha cap algoritme que pugui detectar perfectament tots els virus informàtics possibles. [28]

Finalment, a finals de 1987, es van publicar les dues primeres utilitats antivirus heurístiques: Flushot Plus de Ross Greenberg[30] i Anti4us d'Erwin Lanting. [32] En el seu llibre O'Reilly, Malicious Mobile Code: Virus Protection for Windows, Roger Grimes va descriure Flushot Plus com "el primer programa holístic per lluitar contra el codi mòbil maliciós (MMC)." [33]

No obstant això, el tipus d'heurística utilitzada pels primers motors AV era totalment diferent dels utilitzats avui en dia. El primer producte amb un motor heurístic semblant als moderns va ser F-PROT el 1991. [34] Els primers motors heurístics es basaven en dividir el binari en diferents seccions: secció de dades, secció de codi (en un binari legítim, normalment comença sempre des de la mateixa ubicació). De fet, els virus inicials van reorganitzar la disposició de les seccions, o van sobreescriure la part inicial de la secció per saltar al final del fitxer on es trobava el codi maliciós, només tornant a reprendre l'execució del codi original. Aquest era un patró molt específic, no utilitzat en el seu moment per cap software legítim, que representava un elegant heurístic per atrapar codi sospitós. Més tard es van afegir altres tipus d'heurística més avançada, com ara noms de seccions sospitoses, mida de capçalera incorrecta, expressions regulars i coincidències parcials de patrons a la memòria.

El 1988, el creixement de les empreses antivirus va continuar. A Alemanya, Tjark Auerbach va fundar Avira (H+BEDV en aquell moment) i va llançar la primera versió d'AntiVir (anomenada "Luke Filewalker" en aquell moment). A Bulgària,Vesselin Bontchev va llançar el seu primer programa antivirus de software lliure (més tard es va unir a FRISK Software). També Frans Veldman va llançar la primera versió de ThunderByte Antivirus,també coneguda com a TBAV (va vendre la seva empresa a Norman Safeground el 1998). A Txecoslovàquia, Pavel Baudiš i Eduard Ku?era van començar a avast! (en aquell moment ALWIL Software) i van llançar la seva primera versió d'avast! antivirus. Al juny de 1988, a Corea del Sud, Ahn Cheol-soo va llançar el seu primer software antivirus, anomenat V1 (va fundar AhnLab més tard el 1995). Finalment, a la tardor de 1988, al Regne Unit, Alan Solomon va fundar S&S International i va crear el seu Dr. Solomon's Anti-Virus Toolkit (tot i que el va llançar comercialment només el 1991 – el 1998 l'empresa de Salomó va ser adquirida per McAfee). Al novembre de 1988, un professor de la Universitat Panamericana de Ciutat de Mèxic anomenat Alejandro E. Carriles va obtenir el primer software antivirus a Mèxic sota el nom de "Byte Matabichos" (Byte Bugkiller) per ajudar a resoldre la infestació de virus desenfrenada entre els estudiants. [35]

També el 1988, es va iniciar una llista de correu anomenada VIRUS-L[36] a la xarxa BITNET/EARN on es van discutir nous virus i les possibilitats de detectar i eliminar virus. Alguns membres d'aquesta llista de correu van ser: Alan Solomon, Eugene Kaspersky (Kaspersky Lab), Friðrik Skúlason (FRISK Software), John McAfee (McAfee),Luis Corrons(Panda Security), Mikko Hyppönen (F-Secure), Péter Sz?r, Tjark Auerbach(Avira) i Vesselintch Bonev(FRISK Software). [36]

El 1989, a Islàndia, Friðrik Skúlason va crear la primera versió de F-PROT Anti-Virus (va fundar FRISK Software només el 1993). Mentrestant, als Estats Units, Symantec (fundada per Gary Hendrix el 1982) va llançar el seu primer antivirus Symantec per a Macintosh (SAM). [37]SAM2.0, llançat el març de 1990, va incorporar la tecnologia que permetia als usuaris actualitzar fàcilment SAM per interceptar i eliminar nous virus, inclosos molts que no existien en el moment del llançament del programa. [39]

A finals de la dècada de 1980, al Regne Unit, Jan Hruska i Peter Lammer van fundar l'empresa de seguretat Sophos i van començar a produir els seus primers productes antivirus i xifrats. En el mateix període, a Hongria, també es va fundar VirusBuster (que recentment ha estat incorporat per Sophos).

Període 1990-2000 (aparició de la indústria antivirus)
El 1990, a Espanya, Mikel Urizarbarrena va fundar Panda Security (Panda Software en aquell moment). [40] A Hongria, l'investigador de seguretat Péter Sz?r va publicar la primera versió de Pasteur antivirus. A Itàlia, Gianfranco Tonello va crear la primera versió de l'antivirus VirIT eXplorer, i un any més tard va fundar TG Soft. [41]

El 1990 es va fundar l'Organització d'Investigació Antivirus per Ordinador (CARO). El 1991, CARO va llançar el "Virus Naming Scheme",escrit originalment per Friðrik Skúlason i Vesselin Bontchev. [42] Tot i que aquest esquema de nomenclatura ara està obsolet, continua sent l'únic estàndard existent que la majoria d'empreses i investigadors de seguretat informàtica han intentat adoptar. Els membres del CARO inclouen: Alan Solomon, Costin Raiu, Dmitri Gryaznov, Eugene Kaspersky, Friðrik Skúlason, Igor Muttik, Mikko Hyppönen, Morton Swimmer, Nick FitzGerald, Padgett Peterson, Peter Ferrie, Righard Zwienenberg i Vesselin Bontchev. [43]

El 1991, als Estats Units, Symantec va llançar la primera versió de Norton AntiVirus. El mateix any, a la República Txeca,Jan Gritzbach i Tomáš Hofer van fundar AVG Technologies (Grisoft en aquell moment), tot i que van llançar la primera versió de la seva Guàrdia Antivirus (AVG) només el 1992. D'altra banda, a Finlàndia, F-Secure (fundada el 1988 per Petri Allas i Risto Siilasmaa – amb el nom de Data Fellows) va publicar la primera versió del seu producte antivirus. F-Secure afirma ser la primera empresa antivirus a establir presència a la World Wide Web. [45]

El 1991, l'Institut Europeu de Recerca en Antivirus per Ordinador (EICAR) va ser fundat per continuar investigant antivirus i millorar el desenvolupament de software antivirus. [46]

El 1992, a Rússia, Igor Danilov va llançar la primera versió de SpiderWeb, que més tard es va convertir en dr. Web. [48]

El 1994, AV-TEST va informar que hi havia 28.613 mostres úniques de malware (basades en MD5) a la seva base de dades. [49]

Amb el temps es van fundar altres empreses. El 1996, a Romania, Bitdefender va ser fundada i llançada la primera versió d'Anti-Virus eXpert (AVX). El 1997, a Rússia, Eugene Kaspersky i Natalya Kaspersky van cofundar l'empresa de seguretat Kaspersky Lab. [51]

El 1996, també hi va haver el primer virus Linux "en estat salvatge", conegut com a "Staog". [52]

El 1999, AV-TEST va informar que hi havia 98.428 mostres de malware úniques (basades en MD5) a la seva base de dades. [49]

Període 2000-2005
El 2000, Rainer Link i Howard Fuhs van iniciar el primer motor antivirus de codi obert, anomenat OpenAntivirus Project. [53]

El 2001, Tomasz Kojm va llançar la primera versió de ClamAV,el primer motor antivirus de codi obert que es va comercialitzar. El 2007, ClamAV va ser comprada per Sourcefire , que al seu torn va ser adquirida per Cisco Systems el 2013. [55]

El 2002, al Regne Unit, Morten Lund i Theis Søndergaard van cofundar l'empresa antivirus BullGuard. [56]

El 2005, AV-TEST va informar que hi havia 333.425 mostres úniques de malware (basades en MD5) a la seva base de dades. [49]

2005–2014 period
El 2007, AV-TEST va informar d'un nombre de 5.490.960 noves mostres de malware úniques (basades en MD5) només

per a aquest any. [49] El 2012 i el 2013, les empreses antivirus van informar que les noves mostres de malware oscil·len entre 300.000 i més de 500.000 al dia. [55]

Al llarg dels anys s'ha fet necessari que el software antivirus utilitzi diverses estratègies diferents (per exemple, mòduls específics de protecció de correu electrònic i xarxa o de baix nivell) i algoritmes de detecció, així com per comprovar una varietat creixent d'arxius, en lloc de només executables, per diverses raons:

Les macros potents utilitzades en aplicacions de processador de text, com ara el Microsoft Word,presentaven un risc. Els escriptors de virus podrien utilitzar les macros per escriure virus incrustats als documents. Això significava que els ordinadors ara també podien estar en risc d'infecció obrint documents amb macros adjuntes ocultes. [59]
La possibilitat d'incrustar objectes executables dins de formats de fitxer no executables pot fer que l'obertura d'aquests fitxers sigui un risc. [60]
Els programes de correu electrònic posteriors, en particular l'Outlook Express i l'Outlookde Microsoft, eren vulnerables als virus incrustats en el propi cos del correu electrònic. L'ordinador d'un usuari es pot infectar només obrint o previsualitzant un missatge. [61]

El 2005, F-Secure va ser la primera empresa de seguretat que va desenvolupar una tecnologia Anti-Rootkit, anomenada BlackLight.

Com que la majoria dels usuaris solen estar connectats a Internet de manera continuada, Jon Oberheide va proposar per primera vegada un disseny antivirus basat en el núvol el 2008. [62]

Al febrer de 2008 McAfee Labs va afegir la primera funcionalitat antimalware basada en el núvol de la indústria a VirusScan sota el nom d'Artemis. Va ser provat per AV-Comparatives el febrer de 2008[63] i es va donar a conèixer oficialment a l'agost de 2008 a McAfee VirusScan. [64]

Cloud AV va crear problemes per a proves comparatives de software de seguretat: part de les definicions AV estava fora del control dels verificadors (en servidors de l'empresa AV constantment actualitzats) fent que els resultats no es repetisquessin. Com a resultat, Anti-Malware Testing Standards Organization (AMTSO) va començar a treballar en el mètode de proves de productes en el núvol que va ser adoptat el 7 de maig de 2009. [65]

El 2011, AVG va introduir un servei similar en el núvol, anomenat Protective Cloud Technology. [66]

2014-actualitat (ascens del següent gen)
Després del llançament de 2013 de l'informe APT 1 de Mandiant,la indústria ha vist un canvi cap a enfocaments menys de signatura al problema capaç de detectar i mitigar atacs de dia zero. [66] Han aparegut nombrosos enfocaments per abordar aquestes noves formes d'amenaces, incloent la detecció de comportament, intel·ligència artificial, aprenentatge automàtic i detonació d'arxius basada en el núvol. Segons Gartner, s'espera que l'auge de nous participants, com Carbon Black, Cylance i Crowdstrike, obliguin els titulars de l'EPP a una nova fase d'innovació i adquisició. [66] Un mètode de Bromium implica la micro-virtualització per protegir els escriptoris de l'execució de codi maliciós iniciada per l'usuari final. Un altre enfocament de SentinelOne i Carbon Black se centra en la detecció de comportament mitjançant la construcció d'un context complet al voltant de cada camí d'execució de processos en temps real,mentre que Cylance aprofita un model d'intel·ligència artificial basat en l'aprenentatge automàtic. [71] Cada vegada més, aquests enfocaments sense signatura han estat definits pels mitjans de comunicació i les empreses d'analistes com a antivirus de "propera generació"[72] i estan veient l'adopció ràpida del mercat com a tecnologies certificades de reemplaçament d'antivirus per part d'empreses com Coalfire i DirectDefense. [73] En resposta, els venedors tradicionals d'antivirus com Trend Micro,[74] Symantec i Sophos[75] han respost incorporant ofertes "de pròxim gènere" a les seves carteres, ja que empreses d'analistes com Forrester i Gartner han qualificat l'antivirus tradicional basat en la signatura "ineficaç" i "obsolet". [76]

Mètodes d'identificació
Un dels pocs resultats teòrics sòlids en l'estudi dels virus informàtics és la demostració de Frederick B. Cohen de 1987 que no hi ha cap algoritme que pugui detectar perfectament tots els virus possibles. [28] No obstant això, utilitzant diferents capes de defensa, es pot aconseguir una bona taxa de detecció.

Hi ha diversos mètodes que els motors antivirus poden utilitzar per identificar software maliciós:

Detecció sandbox:una determinada tècnica de detecció basada en el comportament que, en lloc de detectar l'empremta

dactilar conductual en temps d'execució, executa els programes en un entorn virtual,registrant quines accions realitza el programa. Depenent de les accions registrades, el motor antivirus pot determinar si el programa és maliciós o no. Tot i que aquesta tècnica ha demostrat ser bastant efectiva, donada la seva pesadesa i lentitud, rarament s'utilitza en solucions antivirus d'usuari final. [78]
Tècniques de mineria de dades: un dels últims enfocaments aplicats en la detecció de malware. La mineria de dades i els algoritmes d'aprenentatge automàtic s'utilitzen per intentar classificar el comportament d'un fitxer (ja sigui maliciós o benigne) donat una sèrie de característiques d'arxiu, que s'extreuen del propi fitxer. [79][80][81][82][83][84][85][86][87][88][89][90][91][92]

Detecció basada en signatura
El software antivirus tradicional es basa en gran manera en les signatures per identificar software maliciós. [93]

Substancialment, quan un malware arriba a les mans d'una empresa antivirus, és analitzat per investigadors de malware o per sistemes d'anàlisi dinàmics. Després, un cop determinat que és un software maliciós, s'extreu una signatura adequada del fitxer i s'afegeix a la base de dades de signatures del software antivirus. [94]

Tot i que l'enfocament basat en la signatura pot contenir eficaçment brots de malware, els autors de malware han intentat mantenir-se un pas per davant d'aquest software escrivint"oligomorf","polimòrfic"i, més recentment,"virus metamòrfics",que xifren parts d'ells mateixos o es modifiquen com un mètode de disfressa, per no coincidir amb les signatures de virus al diccionari. [95]

Heurística
Molts virus comencen com una sola infecció i a través de mutacions o refinaments per part d'altres atacants, poden créixer en dotzenes de soques lleugerament diferents, anomenades variants. La detecció genèrica es refereix a la detecció i eliminació de múltiples amenaces mitjançant una única definició de virus. [96]

Per exemple, el troià Vundo té diversos membres de la família, depenent de la classificació del venedor antivirus. Symantec classifica els membres de la família Vundo en dues categories diferents, Trojan.Vundo i Trojan.Vundo.B. [97]

Tot i que pot ser avantatjós identificar un virus específic, pot ser més ràpid detectar una família de virus mitjançant una signatura genèrica o mitjançant una coincidència inexacta amb una signatura existent. Els investigadors del virus troben àrees comunes que tots els virus d'una família comparteixen de manera única i, per tant, poden crear una única signatura genèrica. Aquestes signatures sovint contenen codi no contigu, utilitzant caràcters comodí on hi ha diferències. Aquests comodins permeten a l'escàner detectar virus encara que estiguin embuatats amb codi addicional i sense sentit. [99] Es diu que una detecció que utilitza aquest mètode és "detecció heurística".

Detecció de Rootkit
Article principal: Rootkit

El software antivirus pot intentar cercar rootkits. Un rootkit és un tipus de software maliciós dissenyat per obtenir control a nivell administratiu sobre un sistema informàtic sense ser detectat. Rootkits pot canviar el funcionament del sistema operatiu i en alguns casos pot manipular el programa antivirus i fer-lo ineficaç. Els rootkits també són difícils d'eliminar, en alguns casos requereixen una reinstal·lació completa del sistema operatiu. [100]

Protecció en temps real
La protecció en temps real, l'escaneig en accés, la guàrdia de fons, l'escut resident, l'autoprotecció i altres sinònims fan referència a la protecció automàtica proporcionada per la majoria de programes antivirus, antiespia i altres programes antimalware. Això supervisa els sistemes informàtics per a activitats sospitoses, com ara virus informàtics, software espia, adware i altres objectes maliciosos. La protecció en temps real detecta amenaces en fitxers oberts i escaneja aplicacions en temps real a mesura que s'instal·len al dispositiu. [101] En inserir un CD, obrir un correu electrònic o navegar per la web, o quan s'obre o executa un fitxer que ja està a l'ordinador. [102]

Temes de preocupació
Costos de renovació inesperats
Alguns contractes comercials de llicència d'usuari final de software antivirus inclouen una clàusula que la subscripció es renovarà automàticament i la targeta de crèdit del comprador es facturarà automàticament, en el moment de la renovació sense l'aprovació explícita. Per exemple, McAfee requereix que els usuaris cancel·lin la subscripció almenys 60 dies abans de la caducitat de la subscripció actual[103] mentre que BitDefender envia notificacions per cancel·lar la subscripció 30 dies abans de la renovació. [104] Norton AntiVirus també renova les subscripcions automàticament per

defecte. [105]

Aplicacions de seguretat rogue
Article principal: Software de seguretat rogue

Alguns programes antivirus aparents són en realitat software maliciós que es disfressa de software legítim, com WinFixer, MS Antivirusi Mac Defender. [106]

Problemes causats per falsos positius
Un "fals positiu" o "falsa alarma" és quan el software antivirus identifica un fitxer no maliciós com a software maliciós. Quan això passa, pot causar problemes greus. Per exemple, si un programa antivirus està configurat per suprimir o posar en quarantena immediatament els fitxers infectats, com és habitual en aplicacions antivirus de Microsoft Windows, un fals positiu en un fitxer essencial pot fer que el sistema operatiu Windows o algunes aplicacions no es puguin utilitzar. [107] Recuperar-se d'aquests danys en infraestructures de software crític comporta costos de suport tècnic i les empreses es poden veure obligades a tancar mentre es duen a terme accions de remei. [108][109]

Exemples de falsos positius greus:

Maig de 2007: una signatura de virus defectuosa emesa per Symantec va eliminar erròniament els fitxers essencials del sistema operatiu, deixant milers de PC incapaços d'arrencar. [110]
Maig de 2007: El fitxer executable requerit per Pegasus Mail a Windows va ser detectat falsament per Norton AntiVirus com un troià i va ser eliminat automàticament, impedint que Pegasus Mail s'executi. Norton AntiVirus havia identificat falsament tres llançaments de Pegasus Mail com a software maliciós, i eliminaria el fitxer d'instal·lador de Pegasus Mail quan això passés. [111] En resposta a aquest Pegasus Mail va declarar:

Sobre la base que Norton /Symantec ha fet això per a cada un dels tres últims llançaments de Pegasus Mail, només podem condemnar aquest producte com massa defectuós a utilitzar, i recomanar en els termes més forts que els nostres usuaris deixen d'utilitzar-lo a favor de paquets antivirus alternatius i menys buggy. [111]

Abril de 2010: McAfee VirusScan va detectar svchost.exe, un binari normal de Windows, com un virus en màquines que executen Windows XP amb Service Pack 3, causant un bucle de reinici i pèrdua de tot l'accés a la xarxa. [112][113]
Desembre 2010: una actualització defectuosa de la suite antivirus AVG va danyar les versions de 64 bits de Windows 7, fent que no pogués arrencar, a causa d'un bucle d'arrencada interminable creat. [114]
Octubre de 2011: Microsoft Security Essentials (MSE) ha suprimit el navegador web Google Chrome, rival al propi Internet Explorerde Microsoft. MSE va marcar Chrome com un troià bancari Zbot. [115]
Setembre 2012: La suite antivirus de Sophosva identificar diversos mecanismes d'actualització, inclosos els seus, com a software maliciós. Si estava configurat per eliminar automàticament els fitxers detectats, Sophos Antivirus podria no poder actualitzar- se, requeria una intervenció manual per solucionar el problema. [116][117]
Setembre de 2017: l'antivirus Google Play Protect va començar a identificar l'aplicació Bluetooth de Moto G4 de Motorolacom a software maliciós, fent que la funcionalitat de Bluetooth es desactivés. [118]

Problemes relacionats amb el sistema i la interoperabilitat
Executar (la protecció en temps real de) diversos programes antivirus simultàniament pot degradar el rendiment i crear conflictes. [119] No obstant això, utilitzant un concepte anomenat multiscanning,diverses empreses (incloent G Data Software[120] i Microsoft[121]) han creat aplicacions que poden executar múltiples motors simultàniament.

De vegades és necessari inhabilitar temporalment la protecció contra virus en instal·lar actualitzacions importants, com ara els paquets de serveis del Windows o l'actualització dels controladors de targetes gràfiques. [122] La protecció antivirus activa pot impedir parcial o totalment la instal·lació d'una actualització important. El software antivirus pot causar problemes durant la instal·lació d'una actualització del sistema operatiu, per exemple, quan s'actualitza a una versió més recent del Windows "in situ" sense esborrar la versió anterior del Windows. Microsoft recomana que s'inhabiliti el software antivirus per evitar conflictes amb el procés d'instal·lació de l'actualització. [123][124]El software antivirus actiu també pot interferir amb un procés d'actualització de microsoftware. [126]

La funcionalitat d'alguns programes informàtics es pot veure obstaculitzada pel software antivirus actiu. Per exemple, TrueCrypt, un programa d'encriptació de disc, afirma a la seva pàgina de resolució de problemes que els programes antivirus poden entrar en conflicte amb TrueCrypt i fer que funcioni malament o funcioni molt lentament. [127] El software antivirus pot perjudicar el rendiment i l'estabilitat dels jocs que s'executen a la plataforma Steam. [128]

També hi ha problemes de suport al voltant de la interoperabilitat d'aplicacions antivirus amb solucions comunes com l'accés remot SSL VPN i els productes de control d'accés a la xarxa. [129] Aquestes solucions tecnològiques sovint tenen aplicacions d'avaluació de polítiques que requereixen un antivirus actualitzat per instal·lar-se i executar-se. Si l'aplicació antivirus no és reconeguda per l'avaluació de la norma, ja sigui perquè l'aplicació antivirus s'ha actualitzat o perquè no forma part de la biblioteca d'avaluació de polítiques, l'usuari no es podrà connectar.

efectivitat
Estudis al desembre de 2007 van demostrar que l'eficàcia del software antivirus havia disminuït l'any anterior, particularment contra atacs desconeguts o de dia zero. La revista informàtica no va trobar que les taxes de detecció d'aquestes amenaces havien baixat del 40 al 50% el 2006 al 20-30% el 2007. En aquell moment, l'única excepció era l'antivirus NOD32, que gestionava una taxa de detecció del 68%. [130] Segons el lloc web de seguiment ZeuS, la taxa mitjana de detecció de totes les variants del conegut troià ZeuS és tan baixa com el 40%. [131]

El problema es magnifica amb la intenció canviant dels autors del virus. Fa uns anys era evident quan hi havia una infecció per virus. En aquell moment, els virus eren escrits per aficionats i exhibien comportaments destructius o finestres emergents. Els virus moderns sovint són escrits per professionals, finançats per organitzacions criminals. [132]

El 2008, Eva Chen, CEO de Trend Micro, va declarar que la indústria antivirus ha sobreescrit l'efectivitat dels seus productes , i així ha estat enganyant els clients durant anys. [133]

Les proves independents en tots els principals escàners de virus mostren consistentment que cap proporciona una detecció 100% del virus. Els millors van proporcionar fins a un 99,9% de detecció per a situacions simulades del món real, mentre que els més baixos van proporcionar el 91,1% en proves realitzades a l'agost de 2013. Molts antivirus també produeixen resultats falsos positius, identificant fitxers benignes com a software maliciós. [134]

Encara que els mètodes poden variar, algunes agències de proves de qualitat independents notables inclouen AV-Comparatives, ICSA Labs,West Coast Labs, Virus Bulletin, AV-TEST i altres membres de l'Organització d'Estàndards de Proves Anti-Malware. [135][136]

Nous virus
Els programes antivirus no sempre són eficaços contra nous virus, fins i tot aquells que utilitzen mètodes no basats en la signatura que haurien de detectar nous virus. La raó d'això és que els dissenyadors de virus proven els seus nous virus en les principals aplicacions antivirus per assegurar-se que no es detecten abans d'alliberar-los en llibertat. [137]

Alguns virus nous, particularment el ransomware,utilitzen codi polimòrfic per evitar la detecció per antivirus. Jerome Segura, analista de seguretat de ParetoLogic, va explicar:[138]

És una cosa que troben a faltar molt de temps perquè aquest tipus de [virus del ransomware] prové de llocs que utilitzen un polimorfisme, el que significa que bàsicament aleatoritzen el fitxer que us envien i obté per productes antivirus coneguts molt fàcilment. He vist gent de primera mà infectant-se, tenint totes les finestres emergents i, no obstant això, tenen software antivirus en execució i no està detectant res. En realitat pot ser bastant difícil desfer-se'n, i mai no estàs segur de si realment ha desaparegut. Quan veiem alguna cosa així normalment aconsellem tornar a instal·lar el sistema operatiu o tornar a instal·lar còpies de seguretat. [138]

Una prova de concepte virus ha utilitzat la Unitat de Processament de Gràfics (GPU) per evitar la detecció de software antivirus. L'èxit potencial d'això implica eludir la CPU per dificultar molt que els investigadors de seguretat analitzin el funcionament intern d'aquest software maliciós. [139]

Rootkits
La detecció de rootkits és un repte important per als programes antivirus. Els Rootkits tenen accés administratiu complet a l'ordinador i són invisibles per als usuaris i amagats de la llista de processos en execució del gestor de

tasques. Rootkits pot modificar el funcionament intern del sistema operatiu i manipular programes antivirus. [140]

Fitxers danyats
Si un fitxer ha estat infectat per un virus informàtic, el software antivirus intentarà eliminar el codi virus del fitxer durant la desinfecció, però no sempre és capaç de restaurar el fitxer al seu estat indemnat. [141] En aquestes circumstàncies, els fitxers danyats només es poden restaurar a partir de còpies de seguretat existents o còpies instantànies (això també és cert per al ransomware[143]); el software instal·lat que està danyat requereix tornar a instal·lar[144] (tanmateix, vegeu Verificador de fitxers de sistema).

Infeccions de microsoftware
Qualsevol microsoftware que es pugui escriure a l'ordinador pot estar infectat per codi maliciós. [145] Aquesta és una preocupació important, ja que una BIOS infectada podria requerir la substitució del xip de la BIOS real per assegurar-se que el codi maliciós s'elimina completament. [146] El software antivirus no és eficaç per protegir el microsoftware i la BIOS de la placa base de la infecció. [147] El 2014, els investigadors de seguretat van descobrir que els dispositius USB contenen microsoftware enregistrable que es pot modificar amb codi maliciós (anomenat"BadUSB"),que el software antivirus no pot detectar ni prevenir. El codi maliciós pot funcionar sense ser detectat a l'ordinador i fins i tot podria infectar el sistema operatiu abans d'arrencar-lo. [148]

Rendiment i altres inconvenients
El software antivirus té alguns inconvenients, primer dels quals pot afectar el rendiment d'un ordinador. [150]

A més, els usuaris sense experiència es poden portar a una falsa sensació de seguretat quan utilitzen l'ordinador, considerant que els seus ordinadors són invulnerables, i poden tenir problemes per entendre les sol·licituds i decisions amb què els presenta el software antivirus. Una decisió incorrecta pot provocar una bretxa de seguretat. Si el software antivirus utilitza detecció heurística, s'ha d'afinar per minimitzar software inofensiu malintencionat com a maliciós(fals positiu). [151]

El software antivirus en si sol funcionar a nivell de nucli de gran confiança del sistema operatiu per permetre-li accedir a tot el procés i arxius maliciosos potencials, creant una possible via d'atac. [152] L'Agència de Seguretat Nacional dels Estats Units (NSA) i les agències d'intel·ligència de la Seu de Comunicacions del Govern del Regne Unit (GCHQ), respectivament, han estat explotant software antivirus per espiar els usuaris. [153] El software antivirus té un accés altament privilegiat i de confiança al sistema operatiu subjacent, cosa que el converteix en un objectiu molt més atractiu per als atacs remots. [154] A més, el software antivirus està "anys darrere d'aplicacions del costat del client conscients de la seguretat, com navegadors o lectors de documents. Significa que Acrobat Reader, Microsoft Word o Google Chrome són més difícils d'explotar que el 90 per cent dels productes antivirus que hi ha", segons Joxean Koret, investigador de Coseinc, una consultora de seguretat de la informació amb seu a Singapur. [154]

Solucions alternatives

L'escàner de virus de la línia d'ordres de clam AV 0.95.2 executant una actualització de la definició de la signatura de virus, escanejant un fitxer i identificant un troià.

El software antivirus que s'executa en ordinadors individuals és el mètode més comú utilitzat per protegir-se contra el software maliciós, però no és l'única solució. Altres solucions també poden ser emprades pels usuaris, incloent-hi La gestió d'amenaces unificades (UTM),tallafocs de maquinari i xarxa, antivirus basats en el núvol i escàners en línia.

Tallafocs de maquinari i xarxa
Els tallafocs de xarxa impedeixen que programes i processos desconeguts accedeixin al sistema. No obstant això, no són sistemes antivirus i no intenten identificar ni eliminar res. Poden protegir contra la infecció des de fora de l'ordinador o la xarxaprotegits, i limitar l'activitat de qualsevol software maliciós que estigui present bloquejant sol·licituds entrants o sortints en determinats ports TCP/IP. Un tallafocs està dissenyat per fer front a amenaces més àmplies del sistema que provenen de connexions de xarxa al sistema i no és una alternativa a un sistema de protecció contra virus.

Antivirus en núvol
L'antivirus en el núvol és una tecnologia que utilitza software d'agents lleugers a l'ordinador protegit, alhora que descarrega la majoria de l'anàlisi de dades a la infraestructura del proveïdor. [155]

Una aproximació a la implementació de l'antivirus en el núvol consisteix a escanejar fitxers sospitosos mitjançant múltiples motors antivirus. Aquest enfocament va ser proposat per una implementació primerenca del concepte antivirus en el núvol anomenat CloudAV. CloudAV va ser dissenyat per enviar programes o documents a un núvol de xarxa on s'utilitzen múltiples programes antivirus i de detecció de comportament simultàniament per millorar les taxes de detecció. L'escaneig paral·lel de fitxers utilitzant escàners antivirus potencialment incompatibles s'aconsegueix generant una màquina virtual per motor de detecció i, per tant, eliminant qualsevol possible problema. CloudAV també pot realitzar "detecció retrospectiva", mitjançant la qual el motor de detecció en el núvol reassori tots els fitxers del seu historial d'accés a arxius quan s'identifica una nova amenaça millorant així la nova velocitat de detecció d'amenaces. Finalment, CloudAV és una solució per a l'escaneig eficaç de virus en dispositius que no tenen la potència informàtica per realitzar les pròpies exploracions. [156]

Alguns exemples de productes antivirus en núvol són Panda Cloud Antivirus i Immunet. Comodo Group també ha produït antivirus basats en el núvol. [157]

Escaneig en línia
Alguns proveïdors d'antivirus mantenen llocs web amb capacitat d'escaneig en línia gratuïta de tot l'ordinador, àrees crítiques només, discos locals, carpetes o fitxers. L'escaneig periòdic en línia és una bona idea per a aquells que executen aplicacions antivirus als seus ordinadors perquè aquestes aplicacions sovint són lentes per atrapar amenaces. Una de les primeres coses que fa el software maliciós en un atac és desactivar qualsevol software antivirus existent i de vegades l'única manera de saber d'un atac és recorrent a un recurs en línia que no està instal·lat a l'ordinador infectat. [159]

Eines especialitzades

L'escàner rkhunter de la línia d'ordres, un motor per escanejar els rootkits de Linux que s'executen a Ubuntu.

Hi ha eines d'eliminació de virus disponibles per ajudar a eliminar infeccions tossudes o certs tipus d'infecció. Alguns exemples són Avast Free Anti- Malware,[160] Eines d'eliminació de malware gratuïtes AVG ,[161] i l'eina d'eliminació antivir d'Avira. [162] També val la pena assenyalar que de vegades el software antivirus pot produir un resultat positiu fals, indicant una infecció on no n'hi ha. [163]

Un disc de rescat que és arrencable, com ara un CD o un dispositiu d'emmagatzematge USB, es pot utilitzar per executar software antivirus fora del sistema operatiu instal·lat, per tal d'eliminar infeccions mentre estan inactius. Un disc antivirus d'arrencada pot ser útil quan, per exemple, el sistema operatiu instal·lat ja no és arrencable o té software maliciós que es resisteix a tots els intents de ser eliminat pel software antivirus instal·lat. Exemples d'alguns d'aquests discos d'arrencada inclouen el Bitdefender Rescue CD,[164] Kaspersky Rescue Disk 2018,[165] i Windows Defender Offline[166] (integrat a Windows 10 des de l'actualització d'aniversari). La majoria del software de CD de rescat també es pot instal·lar en un dispositiu d'emmagatzematge USB, que es pot arrencar en ordinadors més nous.

Ús i riscos
Segons una enquesta de l'FBI, les principals empreses perden 12 milions de dòlars anuals per fer front als incidents del virus. [167] Una enquesta de Symantec el 2009 va trobar que un terç de les petites i mitjanes empreses no utilitzaven protecció antivirus en aquell moment, mentre que més del 80% dels usuaris domèstics tenien algun tipus d'antivirus instal·lat. [168] Segons una enquesta sociològica realitzada per G Data Software el 2010, el 49% de les dones no van utilitzar cap programa antivirus. [169]

Vegeu també

Software antivirus i antimalware
CARO, l'Organització de Recerca En Antivirus informàtic
Comparació de software antivirus
Comparació de virus informàtics
EICAR, l'Institut Europeu d'Investigació Antivirus per Computador
Software tallafocs
Seguretat a Internet
Software maliciós de Linux
Quarantena (informàtica)
Sandbox (seguretat informàtica)
Cronologia de virus informàtics i cucs
Engany del virus

Referències

^ Henry, Alan. "La diferència entre antivirus i antimalware (i quins utilitzar)". Arxivat de l'original el 22 de novembre de 2013.
^ "Què és el software antivirus?". Microsoft. Arxivat de l'original l'11 d'abril de 2011.
^ von Neumann, John (1966) Teoria de l'autoproducció d'autòmats Arxivats el 13 de juny de 2010, al Wayback Machine. Premsa de la Universitat d'Illinois.
^ Thomas Chen, Jean-Marc Robert (2004). "L'evolució de virus i cucs". Arxivat de l'original el 17 de maig de 2009. Consultat el 16 de febrer de 2009.
^ Des del primer correu electrònic al primer vídeo de YouTube: una història definitiva d'Internet Arxivada el 31 de desembre de 2016, al Wayback Machine. Tom Meltzer i Sarah Phillips. El Guardià. 23 d'octubre de 2009
^ IEEE Annals de la Història de la Informàtica, Volums 27–28. IEEE Computer Society, 2005. 74 Arxivat el 13 de maig de 2016, a la Wayback Machine: "[...] d'una màquina a una altra va conduir a l'experimentació amb el programa Creeper, que es va convertir en el primer cuc informàtic del món: un càlcul que utilitzava la xarxa per recrear-se en un altre node i estendre's de node a node."
^ Jump up to:un grup sanguini John Metcalf (2014). "Guerra Central: Creeper &Segador". Arxivat de l'original el 2 de maig de 2014. Consultat l'1 de maig de 2014.
^ "Creeper – L'Enciclopèdia del Virus". Arxivat de l'original el 20 de setembre de 2015.
^ "Elk Cloner". Arxivat de l'original el 7 de gener de 2011. Consultat el 10 de desembre de 2010.
^ "Top 10 virus informàtics: núm. 10 – Clonador de uapití". Arxivat de l'original el 7 de febrer de 2011. Consultat el 10 de desembre de 2010.
^ "Llista de virus informàtics desenvolupats en la dècada de 1980". Arxivat de l'original el 24 de juliol de 2011. Consultat el 10 de desembre de 2010.
^ Fred Cohen: "Computer Viruses – Theory and Experiments" (1983) Arxivat el 8 de juny de 2011 a la Wayback Machine. Eecs.umich.edu (3 de novembre de 1983). Consultat en 2017-01-03.
^ Cohen, Fred (1 d'abril de 1988). "Ponència convidada: Sobre les implicacions dels virus informàtics i els mètodes de defensa". Informàtica i Seguretat. 7 (2): 167–184. doi:10.1016/0167-4048(88)90334-3.
^ Szor 2005, p. [pàgina necessària].
^ "Butlletí de virus :: In memoriam: Péter Ször 1970–2013". Arxivat de l'original el 26 d'agost de 2014.
^ "Història dels virus". Octubre de 1992. Arxivat de l'original el 23 d'abril de 2011.
^ ? Leyden, John (19 de gener de 2006). "El virus del PC celebra el 20è aniversari". El Registre. Arxivat de l'original el 6 de setembre de 2010. Consultat març 21, 2011.
^ "La història dels virus informàtics".
^ Seguretat panda (abril de 2004). "(II) Evolució de virus informàtics". Arxivat de l'original el 2 d'agost de 2009. Consultat el 20 de juny de 2009.
^ Llista de virus del laboratori Kaspersky. viruslist.com
^ Wells, Joe (30 d'agost de 1996). "Cronologia del virus". IBM. Arxivat de l'original el 4 de juny de 2008. Consultat el 6 de juny de 2008.
^ G Data Software AG (2017). "G Data presenta la primera solució Antivirus el 1987". Arxivat de l'original el 15 de març de 2017. Consultat el 13 de desembre de 2017.
^ Karsmakers, Richard (gener 2010). "El llibre i software d'assassins de virus definitius". Arxivat de l'original el 29 de juliol de 2016. Consultat el 6 de juliol de 2016.
^ "McAfee es converteix en Seguretat Intel". McAfee Inc. Consultat el 15 de gener de2014.
^ Cavendish, Marshall (2007). Inventors i Invencions, Volum 4. Pau Bernabéu. p. 1033. ISBN 978-0761477679.
^ "Sobre l'empresa ESET". Arxivat de l'original el 28 d'octubre de 2016.
^ "ESET NOD32 Antivirus". Plaça de la Visió. 16 de Febrer de 2016. Arxivat de l'original el 24 de febrer de 2016.
^ Jump up to:un grup sanguini Cohen, Fred, Un virus informàtic indetectable (Arxivat), 1987, IBM

^ Yevics, Patricia A. "Trets de grip per a virus informàtics". americanbar.org. Arxivat de l'original el 26 d'agost de 2014.
^ Strom, David (1 d'abril de 2010). "Com els amics ajuden els amics a Internet: La història de Ross Greenberg". wordpress.com. Arxivat de l'original el 26 d'agost de 2014.
^ "L'antivirus té 30 anys". spgedwards.com. d'abril de 2012. Arxivat de l'original el 27 d'abril de 2015.
^ "Una breu història del software antivirus". techlineinfo.com. Arxivat de l'original el 26 d'agost de 2014.
^ Grimes, Roger A. (1 de juny de 2001). Codi mòbil maliciós: protecció antivirus per al Windows. O'Reilly Media, Inc. pàg. ISBN 9781565926820. Arxivat de l'original el 21 de març de 2017.
^ ? «Friðrik Skúlason ehf» (islandès). Arxivat de l'original el 17 de juny de 2006.
^ Dirección General del Derecho de Autor, SEP, Registre de la D.F. Mèxic 20709/88 Llibre 8, full 40, de 24 de novembre de 1988.
^ Jump up to:un grup sanguini "The 'Security Digest' Archives (TM) : www.phreak.org-virus_l". Arxivatde l'original el 5 de gener de 2010.
^ "Softwares Symantec i seguretat a Internet a PCM". Arxivat de l'original l'1 de juliol de 2014.
^ SAM identifica fitxers infectats per virus, aplicacions de reparació, InfoWorld, 22 de maig de 1989
^ SAM Update permet als usuaris programar per a nous virus, InfoWorld, 19 de febrer de 1990
^ Naveen, Sharanya. "Seguretat Panda". Arxivat de l'original el 30 de juny de 2016.Consultat el 31 de maig de 2016.
^ "Qui som – TG Soft Software House". www.tgsoft.it. Arxivat de l'original el 13 d'octubre de 2014.
^ "Una nova Convenció de Nomenclatura de Virus (1991) – CARO – Computer Antivirus Research Organization". Arxivat de l'original el 13 d'agost de 2011.
^ "MEMBRES CARO". Caro. Arxivat de l'original el 18 de juliol de 2011. Consultat el 6 de juny de 2011.
^ CAROids, Hamburg 2003 Arxivat el 7 de novembre de 2014, a la Wayback Machine
^ "F-Secure Weblog : Notícies del Laboratori". F-secure.com. Arxivat de l'original el 23 de setembre de 2012. Consultat setembre 23, 2012.
^ "Sobre EICAR". Lloc web oficial d'EICAR. Arxivat de l'original el 14 de juny de 2018.Consultat el 28 d'octubre de 2013.
^ David Harley, Lysa Myers & Eddy Willems. "Fitxers de prova i avaluació de productes: el cas a i contra la simulació de malware" (PDF). AVAR2010 13a Associació d'Investigadors antiVirus d'Àsia Conferència Internacional. Arxivat de l'original (PDF) el 29 de setembre de 2011. Consultat el 30 de juny de 2011.
^ "Dr. Web LTD Doctor Web / Dr. Web Reviews, Millors ressenyes de software antiVirus, Centre de revisió". Reviewcentre.com. Arxivat de l'original el 23 de febrer de 2014.Consultat el 17 de febrer de 2014.
^ Jump up to:un b c d [El 1994, AV-Test.org va informar de 28.613 mostres úniques de malware (basades en MD5). "Una breu història del malware; Els primers 25 anys"]
^ "Historial de productes bitDefender". Arxivat de l'original el 17 de març de 2012.
^ "InfoWatch Management". InformacióWatch. Arxivat de l'original el 21 d'agost de 2013. Consultat agost 12, 2013.
^ «Linuxvirus – Ajuda de la comunitat Wiki». Arxivat de l'original el 24 de març de 2017.
^ "Sorry – recovering..." Arxivat de l'original el 26 d'agost de 2014.
^ "Sourcefire adquireix ClamAV". ClamAV. 17 d'agost de 2007. Arxivat de l'original el 15 de desembre de 2007. Consultat el 12 de febrer de 2008.
^ "Cisco Completa Adquisició de Sourcefire". cisco.com7 d'octubre de 2013. Arxivat de l'original el 13 de gener de 2015. Consultat el 18 de juny de 2014.
^ Der Unternehmer – marca eins online Arxivat el 22 de novembre de 2012, a la Wayback Machine. Brandeins.de (juliol 2009). Consultat el 3 de gener de 2017.
^ ? Williams, Greg (abril 2012). "El detectiu digital: la guerra contra el software maliciós de Mikko Hypponen està augmentant". Cablejat. Arxivat de l'original el 15 de març de 2016.
^ "Ciberdelinqüència quotidiana i què pots fer al respecte". Arxivat de l'original el 20 de febrer de 2014.
^ Szor 2005, pp. 66–67.
^ "El nou virus viatja en arxius PDF". 7 d'agost de 2001. Arxivat de l'original el 16 de juny de 2011. Consultat el 29 d'octubre de 2011.
^ Sistemes Slipstick (febrer de 2009). "Protecció del Microsoft Outlook contra virus".Arxivat de l'original el 2 de juny de 2009. Consultat el 18 de juny de 2009.
^ "CloudAV: N-Version Antivirus en el Núvol de Xarxa". usenix.org. Arxivat de l'original el 26 d'agost de 2014.
^ Informe de previsualització McAfee Artemis Arxivat el 3 d'abril de 2016, a la Wayback Machine. av-comparatives.org
^ McAfee Tercer Trimestre 2008 Arxivat el 3 d'abril de 2016, a la Wayback Machine. corporate-ir.net
^ "Bones pràctiques d'AMTSO per provar productes de seguretat en el núvol » AMTSO". Arxivat de l'original el 14 d'abril de 2016. Consultat març 21, 2016.
^ "VISIÓ GENERAL DE LA TECNOLOGIA". Seguretat AVG. Arxivat de l'original el 2 de juny de 2015. Consultat el 16 de febrer de 2015.
^ "El misteriós retorn del malware xinès d'anys d'antiguitat". 18 d'octubre de 2018. Consultat el 16 de juny de 2019 – via www.wired.com.
^ "Plataformes màgiques de protecció de punts finals quadrants 2016". Gartner Research.
^ Messmer, Ellen (20 d'agost de 2014). "L'start-up ofereix detecció i resposta de punts finals per a la detecció de

malware basada en el comportament". networkworld.com. Arxivatde l'original el 5 de febrer de 2015.
^ "Seguretat pàtria avui: Bromium Research revela la inseguretat en els desplegaments existents de protecció contra malware de punts finals". Arxivat de l'original el 24 de setembre de 2015.
^ "Duelling Unicorns: CrowdStrike Vs. Cylance en una batalla brutal per colpejar els hackers fora". Forbes. 6 de juliol de 2016. Arxivat de l'original l'11 de setembre de 2016.
^ Potter, Davitt (9 de juny de 2016). "L'antivirus és mort? El desplaçament cap als punts finals del següent gen". Arxivat de l'original el 20 de desembre de 2016.
^ "CylancePROTECT® aconsegueix la certificació de compliment de normes de seguretat HIPAA". En Cylance. Arxivat de l'original el 22 d'octubre de 2016. Consultat el 21 d'octubre de 2016.
^ "Tendència Micro-XGen". Tendència Micro. 18 d'octubre de 2016. Arxivat de l'original el 21 de desembre de 2016.
^ "Punt final del següent gen". Sophos. Arxivat de l'original el 6 de novembre de 2016.
^ The Forrester Wave™: Endpoint Security Suites, Q4 2016 Arxivat el 22 d'octubre de 2016, al Wayback Machine. Forrester.com (19 d'octubre de 2016). Consultat en 2017-01-03.
^ L'espai aïllat protegeix els punts finals | Queda't per davant de zero amenaces diaarxivades el 2 d'abril de 2015, a la Wayback Machine. Enterprise.comodo.com (20 de juny de 2014). Consultat en 2017-01-03.
^ Szor 2005, pp. 474–481.
^ Kiem, Hoang; Thuy, Nguyen Yhanh i Quang, Truong Minh Nhat (desembre de 2004) "Un enfocament d'aprenentatge automàtic al sistema antivirus", Taller conjunt de la Societat Vietnamita d'IA, SIGKBS-JSAI, ICS-IPSJ i IEICE-SIGAI sobre Mineria Activa; Sessió 3: Intel·ligència Artificial, Vol. 67, pàg.
^ Mètodes de mineria de dades per a la detecció de malware. 2008. pàg. ISBN 978-0-549-88885-7. Arxivat de l'original el 20 de març de 2017.
^ Dua, Sumeet; Du, Xian (19 d'abril de 2016). Mineria de Dades i Aprenentatge Automàtic en Ciberseguretat. Premsa CRC. pàg. ISBN 978-1-4398-3943-0. Arxivat de l'original el 20 de març de 2017.
^ Firdausi, Ivan; Lim, Charles; Erwin, Alva; Nugroho, Anto Satriyo (2010). "Anàlisi de tècniques d'aprenentatge automàtic utilitzades en la detecció de malware basat en el comportament". II Conferència Internacional sobre Avenços en Tecnologies de Computació, Control i Telecomunicació 2010. p. 201. doi:10.1109/ACT.2010.33. ISBN 978-1-4244-8746-2. S2CID 18522498.
^ Siddiqui, Muazzam; Wang, Morgan C.; Lee, Joohan (2008). "Una enquesta de tècniques de mineria de dades per a la detecció de malware mitjançant característiques de fitxers". Actes de la 46a Conferència Regional Anual del Sud-est sobre XX – ACM-SE 46. p. 509. doi:10.1145/1593105.1593239. ISBN 9781605581057. S2CID 729418.
^ Deng, P.S.; Jau-Hwang Wang; Wen-Gong Shieh; Chih-Pin Yen; Cheng-Tan Tung (2003). "Extracció intel·ligent automàtica de signatures de codi maliciós". IEEE 37a Conferència Internacional de Carnahan 2003 sobre Tecnologia de seguretat, 2003. Procediments. p. 600. doi:10.1109/CCST.2003.1297626. ISBN 978-0-7803-7882-7. S2CID 56533298.
^ Komashinskiy, Dmitriy; Kotenko, Igor (2010). "Detecció de malware mitjançant tècniques de mineria de dades basades en característiques posicionalment dependents". 2010 18a Conferència Euromicro sobre Processament Paral·lel, Distribuït i Basat en Xarxa. p. 617. doi:10.1109/PDP.2010.30. ISBN 978-1-4244-5672-7. S2CID 314909.
^ Schultz, M.G.; Eskin, E.; Zadok, F.; Stolfo, S.J. (2001). "Mètodes de mineria de dades per a la detecció de nous executables maliciosos". Procediments 2001 Simposi IEEE sobre Seguretat i Privacitat. S&P 2001. p. 38. CiteSeerX 10.1.1.408.5676. doi:10.1109/SECPRI.2001.924286. ISBN 978-0-7695-1046-0. S2CID 21791.
^ Sí, Yanfang; Wang, Dingding; Li, Tao; Ye, Dongyi (2007). ? «IMDS». Actes de la 13a conferència internacional de l'ACM SIGKDD sobre descobriment de coneixements i mineria de dades – KDD '07. p. 1043. doi:10.1145/1281192.1281308. ISBN 9781595936097. S2CID 8142630.
^ Kolter, J. Zico; Maloof, Marc A. (1 de desembre de 2006). "Aprendre a detectar i classificar executables maliciosos en llibertat". J. Mach. Aprèn. Res. 7: 2721–2744.
^ Tabish, S. Momina; Shafiq, M. Zubair; Farooq, Muddassar (2009). "Detecció de malware mitjançant anàlisi estadística del contingut de fitxers a nivell de byte". Actes del Taller de Ciberseguretat de l'ACM SIGKDD Informàtica de Seguretat i Intel·ligència – CSI-KDD '09. p. 23. CiteSeerX 10.1.1.466.5074. doi:10.1145/1599272.1599278. ISBN 9781605586694. S2CID 10661197.
^ Sí, Yanfang; Wang, Dingding; Li, Tao; Sí, Dongyi; Jiang, Qingshan (2008). "Un sistema intel·ligent de detecció de malware PE basat en la mineria d'associacions". Revista en Virologia informàtica. 4 (4): 323. CiteSeerX 10.1.1.172.4316. doi:10.1007/s11416-008-0082-4. S2CID 207288887.
^ Sami, Ashkan; Yadegari, Babak; Peiravian, Naser; Hashemi, Sattar; Hamze, Ali (2010). "Detecció de malware basada en trucades d'API mineres". Actes del Simposi de l'ACM 2010 sobre Computació Aplicada – SAC '10. p. 1020. doi:10.1145/1774088.1774303. ISBN9781605586397. S2CID 9330550.
^ Shabtai, Asaf; Kanonov, Uri; Elovici, Yuval; Glezer, Chanan; Weiss, Yael (2011). "Andromaly": Un marc de detecció de malware conductual per a dispositius Android". Revista de Sistemes Intel·ligents d'Informació. 38: 161. doi:10.1007/s10844-010-0148-x. S2CID 6993130.
^ Fox-Brewster, Thomas. "Netflix està abocant antivirus, presagia la mort d'una indústria". Forbes. Arxivat de l'original el 6 de setembre de 2015. Consultat setembre 4, 2015.
^ Generació automàtica de signatura de malware arxivada el 24 de gener de 2021, a la Wayback Machine. (PDF) .

Consultat el 3 de gener de 2017.
^ Vegades 2005, pàg.
^ "Detecció genèrica". Kaspersky. Arxivat de l'original el 3 de desembre de 2013.Consultat l'11 de juliol de 2013.
^ Symantec Corporation (febrer de 2009). "Trojan.Vundo". Arxivat de l'original el 9 d'abril de 2009. Consultat el 14 d'abril de 2009.
^ Symantec Corporation (febrer de 2007). "Trojan.Vundo.B". Arxivat de l'original el 27 d'abril de 2009. Consultat el 14 d'abril de 2009.
^ "Tècniques d'Investigació i Detecció Antivirus". ExtremeTech. Arxivat de l'original el 27 de febrer de 2009. Consultat el 24 de febrer de 2009.
^ "Terminologia – F-Secure Labs". Arxivat de l'original el 24 d'agost de 2010.
^ "Protecció en temps real". support.kaspersky.com. Consultat el 9 d'abril de 2021.
^ "Solucions de seguretat cibernètica Kaspersky per a la llar i | de negocis Kaspersky". usa.kaspersky.com. Arxivat de l'original el 14 de febrer de 2011.
^ Kelly, Michael (octubre de 2006). "Comprant perillosament". Arxivat de l'original el 15 de juliol de 2010. Consultat el 29 de novembre de 2009.
^ Bitdefender (2009). "Renovació automàtica". Arxivat de l'original el 6 d'octubre de 2009. Consultat el 29 de novembre de 2009.
^ Symantec (2014). "Preguntes freqüents sobre el servei de renovació automàtica de Norton". Arxivat de l'original el 13 d'abril de 2014. Consultat el 9 d'abril de 2014.
^ SpywareWarrior (2007). "Productes i llocs web antiespia sospitosos / sospitosos".Consultat el 29 de novembre de 2009.
^ Protalinski, Emil (11 de novembre de 2008). "AVG marca incorrectament l'usuari32.dll al Windows XP SP2/SP3". Ars Technica. Arxivat de l'original el 30 d'abril de 2011.Consultat el 24 de febrer de 2011.
^ "McAfee per compensar les empreses per l'actualització de buggy". Arxivat de l'original el 4 de setembre de 2010. Consultat el 2 de desembre de 2010.
^ "Buggy McAfee actualitzar whacks Windows XP PCs". Arxivat de l'original el 13 de gener de 2011. Consultat el 2 de desembre de 2010.
^ Tan, Aaron (24 de maig de 2007). "L'actualització de Symantec defectuosa desbarata els ordinadors xinesos". Xarxes CNET. Arxivat de l'original el 26 d'abril de 2011. Consultat el 5 d'abril de 2009.
^ Jump up to:un grup sanguini Harris, David (29 de juny de 2009). "Gener 2010 – Pegasus Mail v4.52 Release". Correu Pegasus. Arxivat de l'original el 28 de maig de 2010. Consultat el 21 de maig de 2010.
^ "McAfee DAT 5958 Problemes d'actualització". 21 d'abril de 2010. Arxivat de l'original el 24 d'abril de 2010. Consultat el 22 d'abril de 2010.
^ "Actualització de McAfee botched tancant màquines XP corporatives a tot el món". 21 d'abril de 2010. Arxivat de l'original el 22 d'abril de 2010. Consultat el 22 d'abril de 2010.
^ ? Leyden, John (2 de desembre de 2010). "Horror AVG actualització de maons de boles Windows 7". El Registre. Arxivat de l'original el 5 de desembre de 2010. Consultat el 2 de desembre de 2010.
^ La detecció falsa de positius de MSE obliga Google a actualitzar Chrome,3 d'octubre de 2011, arxivat de l'original el 4 d'octubre de 2011, recuperat el 3 d'octubre de 2011
^ Sophos Antivirus es detecta com malware, elimina binaris de claus, La propera web, 20 de setembre de 2012, arxivat de l'original el 17 de gener de 2014, recuperat el 5 de març de 2014
^ Shh/Updater-B fals positiu per productes antivirus de Sophos, Sophos, Setembre 19, 2012, arxivat de l'original el 21 d'abril de 2014 , recuperat el 5 demarç de 2014 , recuperat el 5 de març de 2014
^ Si Google Play Protect trenca bluetooth a Moto G4 Plus, no et preocupis perquè hi ha una solució, Policia d'Android, 11 de setembre de 2017, arxivat de l'original el 7 de novembre de 2017 , recuperat l'1 de novembre de2017
^ "Plus! 98: Com eliminar McAfee VirusScan". Microsoft. Gener de 2007. Arxivat de l'original el 8 d'abril de 2010. Consultat setembre 27, 2014.
^ Vamosi, Robert (28 de maig de 2009). "G-Data Internet Security 2010". Món de PC. Arxivat de l'original l'11 de febrer de 2011. Consultat el 24 de febrer de 2011.
^ Higgins, Kelly Jackson (5 de maig de 2010). "El nou software d'avantguarda de Microsoft executa cinc motors de proveïdors antivirus". Enfosquiment. Arxivat de l'original el 12 de maig de 2010. Consultat el 24 de febrer de 2011.
^ "Passos a seguir abans d'instal·lar el Windows XP Service Pack 3". Microsoft. Abril de 2009. Arxivat de l'original el 8 de desembre de 2009. Consultat el 29 de novembre de2009.
^ "Actualització de Windows Vista a Windows 7". Arxivat de l'original el 30 de novembre de 2011. Consultat març 24, 2012. Mencionat dins de "Abans de començar".
^ "Actualització als passos recomanats del Microsoft Windows Vista". Arxivat de l'original el 8 de març de 2012. Consultat març 24, 2012.
^ "Com solucionar problemes durant la instal·lació quan actualitzeu des del Windows 98 o el Windows Millennium Edition al Windows XP". 7 de maig de 2007. Arxivat de l'original el 9 de març de 2012. Consultat març 24, 2012. S'esmenta dins de "Solució general de problemes".

^ "BT Home Hub Procediment d'actualització de microsoftware". Arxivat de l'original el 12 de maig de 2011. Consultat març 6, 2011.
^ "Detecció d'errors". Consultat el 17 de febrer de 2011.
^ "Software espia, adware i virus que interfereixen amb el vapor". Arxivat de l'original l'1 de juliol de 2013. Consultat l'11 d'abril de 2013. Pàgina de suport de vapor.
^ "Avís de camp: FN – 63204 – Cisco Clean Access té un problema d'interoperabilitat amb Symantec Antivirus - retarda la posada en marxa de l'agent". Arxivat de l'original el 24 de setembre de 2009.
^ Goodin, Dan (21 de desembre de 2007). "La protecció antivirus empitjora". Registre de canals. Arxivat de l'original l'11 de maig de 2011. Consultat el 24 de febrer de 2011.
^ "Rastrejador ZeuS :: Inici". Arxivat de l'original el 3 de novembre de 2010.
^ Illett, Dan (13 de juliol de 2007). "La pirateria planteja amenaces als negocis". Ordinador setmanal. Arxivat de l'original el 12 de gener de 2010. Consultat el 15 de novembre de 2009.
^ Espiner, Tom (30 de juny de 2008). "Trend Micro: La indústria antivirus va mentir durant 20 anys". ZDNet. Arxivat de l'original el 6 d'octubre de 2014. Consultat setembre 27,2014.
^ Comparatives AV (desembre 2013). Test de producció "Whole Product Dynamic "Real World" (PDF). Arxivat (PDF) de l'original el 2 de gener de 2014. Consultat el 2 gener2014.
^ Kirk, Jeremy (14 de juny de 2010). "Directrius publicades per a proves de software antivirus". Arxivat de l'original el 22 d'abril de 2011.
^ Harley, David (2011). Guia de defensa de malware AVIEN per a l'empresa. Més pesat.p. 487. ISBN 9780080558660. Arxivat de l'original el 3 de gener de 2014.
^ Kotadia, Munir (juliol 2006). "Per què les aplicacions antivirus populars "no funcionen". Arxivat de l'original el 30 d'abril de 2011. Consultat el 14 d'abril de 2010.
^ Jump up to:un grup sanguini La premsa canadenca (abril de 2010). "L'estafa a Internet utilitza el joc adult per extorsionar els diners". Notícies CBC. Arxivat de l'original el 18 d'abril de 2010. Consultat el 17 d'abril de 2010.
^ Explotar codi; Robatori de dades; Seguretat de la informació; Privacitat; Hackers; sistema, els mandats de seguretat tenen com a objectiu apuntalar la SSL destrossada; Reader, Adobe mata dos errors explotats activament; assetjador, el jutge desestima els càrrecs contra l'acusat Twitter. "Els investigadors aixequen el mal ante amb malware assistit per GPU". Arxivat de l'original el 10 d'agost de 2017.
^ Iresh, Gina (10 d'abril de 2010). "Revisió de Bitdefender Antivirus Security Software edició 2017". www.digitalgrog.com.au. Digital Grog. Arxivat de l'original el 21 de novembre de 2016. Consultat el 20 de novembre de 2016.
^ "Per què F-PROT Antivirus no desinfecta el virus al meu ordinador?". Arxivat de l'original el 17 de setembre de 2015. Consultat agost 20, 2015.
^ "Accions a realitzar sobre objectes infectats". Arxivat de l'original el 9 d'agost de 2015. Consultat agost 20, 2015.
^ "Ransomware criptogràfic: el que necessites saber". 8 d'octubre de 2013. Arxivat de l'original el 9 de febrer de 2014. Consultat març 28, 2014.
^ "Com funciona el software antivirus". Arxivat de l'original el 2 de març de 2011.Consultat el 16 de febrer de 2011.
^ "Les 10 cares del software maliciós de l'ordinador". 17 de juliol de 2009. Arxivat de l'original el 9 de febrer de 2011. Consultat març 6, 2011.
^ "El nou virus de la BIOS suporta les tovalloletes HDD". 27 de març de 2009. Arxivatde l'original l'1 d'abril de 2011. Consultat març 6, 2011.
^ "Phrack Inc. Infecció persistent de la BIOS". 1 de juny de 2009. Arxivat de l'original el30 d'abril de 2011. Consultat març 6, 2011.
^ "Convertir perifèrics USB en BadUSB". Arxivat de l'original el 18 d'abril de 2016.Consultat l'11 d'octubre de 2014.
^ "Per què la seguretat d'USB està fonamentalment trencada". Cablejat. 31 de Juliol de 2014. Arxivat de l'original el 3 d'agost de 2014. Consultat l'11 d'octubre de 2014.
^ "Com el software antivirus pot alentir l'ordinador". bloc Support.com. Arxivat de l'original el 29 de setembre de 2012. Consultat el 26 de juliol de 2010.
^ "Softpedia Entrevista exclusiva: Avira 10". Ionut Ilascu. Softpedia. 14 d'abril de 2010. Arxivat de l'original el 26 d'agost de 2011. Consultat setembre 11, 2011.
^ "Norton AntiVirus ignora les instruccions malicioses de WMI". Munir Kotadia. CBS Interactiu. 21 d'octubre de 2004. Arxivat de l'original el 12 de setembre de 2009.Consultat el 5 d'abril de 2009.
^ "LA NSA i GCHQ van atacar el software antivirus perquè poguessin espiar les persones, les fuites indiquen". 24 de Juny de 2015. Consultat el 30 d'octubre de 2016.
^ Jump up to:un grup sanguini "El software de seguretat popular va ser sotmès a atacs implacables de la NSA i GCHQ". Andrew Fishman, Morgan Marquès-Boire. 22 de Juny de 2015. Arxivat de l'original el 31 d'octubre de 2016. Consultat el 30 d'octubre de 2016.
^ Zeltser, Lenny (octubre 2010). "Què és l'antivirus en el núvol i com funciona?". Arxivatde l'original el 10 d'octubre de 2010. Consultat el 26 d'octubre de 2010.
^ Erickson, Jon (6 d'agost de 2008). "Caps de software antivirus per als núvols". Setmana de la informació. Arxivat de

l'original el 26 d'abril de 2011. Consultat el 24 de febrer de 2010.
^ "Comodo Cloud Antivirus llançat". wikipost.org. Arxivat de l'original el 17 de maig de 2016. Consultat el 30 de maig de 2016.
^ "Comodo Cloud Antivirus Guia d'usuari PDF" (PDF). help.comodo.com. Arxivat(PDF) de l'original el 4 de juny de 2016. Consultat el 30 de maig de 2016.
^ Krebs, Brian (9 de març de 2007). "Exploracions en línia antivirus: una segona opinió gratuïta". El Washington Post. Consultat el 24 de febrer de 2011.
^ "Avast Lliure antimalware". Software AVAST. Consultat l'1 de maig de 2018.
^ "Escàner de virus gratuït i eines d'eliminació de malware". Tecnologies AVG. Consultat l'1 de maig de 2018.
^ "Descarrega l'eina d'eliminació d'antiVir d'Avira". Operacions Avira GmbH &. Co. KG. Consultat l'1 de maig de 2018.
^ "Com saber si un virus és realment un fals positiu". Com fer geek. Consultat el 2 d'octubre de 2018.
^ "Com crear un CD de rescat bitdefender". Mossegadors. Consultat l'1 de juny de 2018.
^ "Desinfectar el sistema operatiu". Laboratori Kaspersky. Consultat l'1 de juny de 2018.
^ "Ajuda a protegir l'ordinador amb el Windows Defender fora de línia". Corporació Microsoft. Consultat l'1 de juny de 2018.
^ "L'FBI estima que les principals empreses perden 12 milions de dòlars anuals per virus". 30 de gener de 2007. Arxivat de l'original el 24 de juliol de 2012. Consultat el 20 de febrer de 2011.
^ Kaiser, Michael (17 d'abril de 2009). "Les petites i mitjanes empreses són vulnerables".Aliança Nacional de Ciberseguretat. Arxivat de l'original el 22 d'abril de 2011. Consultat el 24 de febrer de 2011.
^ Gairebé el 50% de les dones no utilitzen software antivirus arxivat el 13 de maig de 2013, a la Wayback Machine. Spamfighter.com (2 de setembre de 2010). Consultat el 3 de gener de 2017.

bibliografia

Szor, Peter (2005), L'art de la investigació i defensa de virus informàtics, Addison-Wesley, ISBN 978-0-321-30454-4