Antivirus Software

Software-urile antivirus (uneori scris ca Anti-Virus sau anti-virus) sunt programe de computer care incearca sa identifice,neutralizeze sau sa elimine software-ul rau. Termenul “antivirus” este folosit pentru ca cele mai recente exemple construite exclusiv pentru a lupta impotriva virusilor de computer; totusi marea majoritate a software-ului antivirus modern este facut pentru a combate gama larga de amenintari, incluzand viermi,atacuri phishing,rootkits, si Troieni, adesea sunt colectiv descrisi ca malware.

Scannere virus

Software-ul de scanare antivirus, sau un scanner de virusi, este un program care examineaza toate fisierele din locatii specificate, continuturile de memorie, sistemul de operare, registrii, comportamentul imprevizibil al programelor si oriunde este relevant cu intentia de a identifica si inlatura orice malware.

In mod obisnuit sunt folosite doua abordari diferite pentru a identifica malware,deseori in combinative, chiar daca le scoate in evidenta din punctual de vedere al dictionarului de virusi.

- Examinarea(scanarea) fisierelor, etc.,de virusi cunoscuti care se potrivesc cu evidentele dintr-un dictionar de virusi si identificarea comportamentului suspicios din partea oricarui program care ar putea indica infectie. Aceasta abordare este numita analiza *heuristic*, si poate include capture de date, monitorizarea porturilor si alte metode.

Dictionar

In abordarea dictionarului de virusi, cand un software antivirus se uita la un fisier, se refera la dictionarul virusilor cunoscuti pe care autorii softului de antivirus i-au identificat. Daca o bucata dintr-un cod intr-un fisier cu orice virus identificat intr-un dictionary atunci antivirusl poate lua una din urmatoarele actiuni:

1. Incearca sa repare fisierul inlaturand insusi virusul din fisier,
2. Punerea in carantina a fisierului(in asa fel in cat disierul sa raman inaccesibil celorlalte programe si virusul sau sa nu se poate raspandi), sau
3. Stergerea fisierului infectat.

Pentru atinge success consistent pe termen mediu si lung,abordarea dictionarului de virusi necesita frecvent(online in general) descarcarea de intrari actualizate in dicionarul

de virusi. Utilizatori cu spirit civic si cu inclinatii tehnice, si aceia care vor sa ajute la gasirea virusilor care nu sunt detecatati de software, pot sa-si trimita fisierele infectate catre autorii softului de antivirus care le analizeaza si includ caracteristici si informatii de eliminare in dictionarele lor.

Softwareul antivirus bazat pe dictionary examineaza in mod obisnuit fisierele cand sistemul de operare al computerului creaza,deschide, inchide, sau el trimite prin e-mail. In acest fel poate detecta un virus cunoscut imediat ce-l primeste. Administratorii de system pot programa software-ul antivirus sa examineze(scaneze) toate fisierele din harddiscul computerului dupa un anumit principiu.

Cu toate ca abordarea dictioanrului poate efectiv sa contina descopriri de virusi in circumstantele potrivite, autori de virusi au incercat sa fie cu un pas ianintea acelor software-uri scriind virusi “oligomorphic”,”polymorphic” si mai nou “metamorphic”, care encripteaza parti a lor insusi sau pe de alta parte se modifica, ca o metoda de a se deghiza, in asa fel incat sa nu se potriveasca cu semnaturile din dicrtionarul de virusi.

O tehnica inovatoare pentru neutraliza malware in general is whitelisting. In loc sa caute doar malware cunoscut, acesta tehnica previne executarea a tuturor codurilor de computer cu exceptia a celora care au fost inainte identificate ca fiind de incredere de catre administratorul de system. Urmand acesta abordare,”negarea de la sine”, limitarile inascute in pastrarea actualizarii semnaturilor virusilor este evitata. Adtional, aplicatiile de computer care nu sunt dorite de adminstratorul de system sunt impiedicate sa pornesca din moment ce ele nu se afla pa “whitelist”. Din moment ce organizatiile intreprinderilor modern au cantitati mari de aplicatii de incredere, limitarile in adoptarea acestei tehnici stau in abiliatea administratorului de system pentru a inventaira si a intretine “whitelist-ul” aplicatiilor de incredere. Implementari viabile ale acestei tehnici include unelte pentru automatizarea inventarului si intretinerea procesului de “whitelist”.

Comportament suspicios-euristice

Comportamentul suspicios abordeaza, prin contrast, nu incearca sa identifice virusi cunoscuti, dar in schimb monitorizeaza comportamentul tuturor programelor. Daca un program incearca sa scrie date catre un program executabil, de exemplu software-ul antivirus poate semnala acest comportament suspicos , alerta utilizatorul si a-l intreba ce sa faca.

Spre deosebire de abordarea dictionarului, abordarea comportamentului suspicios, prin urmare ofera protective impotriva noilor virusi care nu exsita inca in dictionarele de virusi. Pe de alta parte , poate de asemenea sa semnaleze un numar mare de positive false, si utilizatorii probabil devin dezinteresati la toate avertismentele.

Daca utilizatorul da click pe “accept”pe fiecare dintre avertismente, atunci desigur antivirusul nu-I da nici un beneficu utilizatorului. Acesta problema s-a inrautatit din 1997 de cand mult mai multe proiectari de programe nemalitioaseau aparut pentru a modifica

alte fisiere .exe fara a privy aceasta problema falsa pozitiva. Prin urmare, cele mai modern software-uri de antivirus folosesc din ce in ce mai putin acesta tehnica .

Emulatiea fisierelor-euristice

Unele softuri antivirus folosesc alte tipuri de analiza euristica. De exemplu, ar putea incerca sa emuleze inceputul codului fiecarui exacutabil pe care il invoca sistemul inante de a transfera controlul acelui executabil. Daca program pare sa foloseasca un cod automodificator sau altfel apare ca un virus(daca incerca imediat sa gaseasca alte executabile,de exemplu), se poate presupune ca un virus a infectat executabilul de altfel aceasta metoda ar putea rezulta in multe false positive.

Sandbox

Inca o metoda de detectare include folosirea unui sandbox. Un sandbox emuleaza sistemul de operare si ruleaza executabile in acesta simulare. Dup ace programul a terminat software-ul analizeaza sandboxul pentru orice schimbari care ar putea indica un virus. Din cauza problemelor de performanta, acest tip de detectare are loc in mod normal in timpul scnarii la cerere. Deasemenea acesta metoda ar putea esua din moment ce un virus poate fi nondeterministic sis a faca lucruri diferite,incluzand a nu face nimic, de fiecare data este rulat-deci va fi imposibil sa-l detecteze de la o singura rulare. Unele scanere de virusi pot avertiza utilizatorul daca un fisier este predispus la un virus pe baza tipului de fisier.

Alte metode de prevenire a infectiilor.

In afara de softul de antivirus prevenirea infectiei poate fi realizata de alte metode cum ar fi implemntarea unui firewall, sau virtualizarea sistemului. Pe de alta parte numai softurile de antivirus sunt facute special pentru prevenirea infectiilor cu virusi cunoscuti.

Network Firewall

Firewall-urile nu lasa programele cunoscute si procesele de internet sa aiba acces la sistemul protejat; Nu sunt sisteme antivirus si nu fac nici o incercare in a identifica sau a inlatura ceva, dar protejaza impotriva infectiei si limiteaza activitatea oricarui soft malicious care e prezent prin blocarea cererilor care vin si pleaca inr-un anumit TCP/IP port. De altfel este facut sa se ocupe de amenintarile mari din system care vin din retea in sistem.

Virtualizarea sistemului

Acesta metoda de avertizare este realizata de fapt de virtualizarea sistemului in lucru facand asta , actualul system se protejeaza de a fi alterat de orice infectie incercata de un virus. De fapt previne orice incercare de alterare al intregului system sub virtualizare. Dupa cum este virtualizarea facuta, fara orice soft de antivirus sistemul virtual poate fi infectat si in consecinta avaria sau malicia actiuni pe care virusul este facut sa le cauzeze, dra cand sistemul se va inchide si restarta, toate schimbarile si avariile facute anterior sistemului virtual vor fi resetate. IN acest fel, sistemul este protejat si virusul inlaturat.

Cu toate acestea orice avarie a datei neprotejata (sau nevirtualizata) va ramane. La fel si efectele malicioase au cauzat acest furt de date.

Instrumente de inlaturare a viruslui.

Un instrument de inalturare a virusului este softul pentru inlaturarea anumitor virusi din computerele infectate. Spre deosebire de scopul general al scanerelor de virusi, nu este facut sa detecteze sau sa inlature toti virusii cunoscuti;este conceput sa inlature anumiti virusi mult mai efficient si mai complet decat un program cu scop general .

Multe instrumented oar pentru virusi pot fi gasite cautand www pentru “unelte de inlaturarea a virusului”; altele , cum ar fi McAfee,Stinger si Microsoft malicious software removal tool ruleaza automat din windows update , sunt facute pentru a in latura un nr limitat de virusi. Multe dintre aceste unelte pot descarcate gratuit. Daca un virus este identificat de catre un scanner cu scop general nu poate fi inalturat de tot; odata ce virusul a fost identificat, rularea unie unelte facute special pentru acesta poate sa faca o treaba mai buna de curatare.

Motive de ingrijorare

- Aparitia regulate de noi malware este cu siguranta in interesul financiar al vanzatorilor de software de antivirus desi nu este evident de acesta coliziune.
- Unele softuri de antivirus pot reduce considerabil performanta. Utilizatorii pot dezactiva protectia antivirusului pentru a compensa pierderea performantei, astfel crescand riscul de infectie. Pentru o maxima protective, antiviruslu treb sa fie active tot timpul, desori la costul performantei reduse.
- Programele antivirus pot avea un risc de securitate din moment ce deseori ruleaza la nivelul sistemului de privilegii si pot afecta miezul

-Ambele acestea sunt necesare pentru ca software-ul sa-si faca treaba efficient, dar are si o parte proasta. Asta poate insemna exploatarea antiviruslui , poate duce la estinderea privilegilor si crea o severa amenintare de securitate.Folosirea unui soft de antivirus in comparative cu principiul celui mai mic privilegiu, este foarte inefficient cand ramificatiile softului adaugat sunt trecute in cont.

- Este important de tinut minte ca nu trebuie sa ia mai mult de un antivirus resident in memorie, instalat intr-un singur comp la orice timp. Altfel,computeurl poate fi afectat.
- Este cateodata necesara dezactivarea protectiei impotriva virusilor cand instalam actualizari importante cum ar fi Windows service Packs, sau actualizariel driverelor placilor video. Protectia active a antiviruslui poate preveni partial sua comlet instalarea unei actualizari majore.
- Cand cumparam un antivirus acordul poate include o clauza cum ca licenta poate fi reinoita automat si cardul cumparatorului va fi automat taxat, la timpul de reinoire fara aprobare explicita. De exemplu , McAfee cere o dezabonare cu cel putin 60 de zile inainte de expirarea prezentului abonament. Norton antivirus de asemenea reinoieste licente automat.
- Unele programe antivirus sunt defapt spyware mascandu-se ca antivirus. Este cel mai bines a verifici de 2 ori ca antiviruslul pe care-l ldescarci este chiar un antivirus.
- Unele programe de antivirus commercial contin adware. Cele mai acceptate antivirusuri desori nu detecteaza virusi noi create.
- Producatorii de antivirusi au fost criticati pentru vanzarea de frica, exagerand despre ce poate face un virus concumatorilor.
- Daca un program antivirus este econfigurat la stergere imediata sua punerea in carantina a fisierelor infectate(sau o face implicit), positive false in fisiere esentiale poate ingreuna sistemul de operare sau alte apliactii nefolosite.