Backdoor - porta del darrera

Autor:
Data de publicació: 07-01-2019

En el món de la informàtica, una porta del darrere (o en anglès backdoor) és una seqüència especial dintre del codi de programació, mitjançant la qual es poden evitar els sistemes de seguretat de l'algorisme (autenticació) per accedir al sistema. Tot i que aquestes portes poden ser utilitzades per a fins maliciosos i espionatge no sempre són un error, ja que poden haver estat dissenyades amb la intenció de tenir una entrada secreta.

En essència una Backdoor (també anomenada trapdoor o backdoor) és una peça de programari (sovint creada per l'autor) que permet als usuaris accedir a l'ordinador o la funció protegida d'un programa informàtic, evitant la funció d' accés normal. [1]

Portes del darrere més conegudes

Un exemple són les contrasenyes universals per a un BIOS [2] o un programari especial (en general secretat per un troià), que permet un accés remot corresponent a l'ordinador.

Els més coneguts són Back Orifice i NetBus , dues de les primeres portes del darrere, que fins als nostres dies segueixen vigents encara que en menor quantitat atès que la majoria dels programes antivirus els detecten. Un altre molt conegut és el SubSeven , que també va ser introduït en milions d'ordinadors al món.

Diferència entre Backdoor i Troià

Troijan Horse o Troià, és un programa informàtic o script que es disfressa com una aplicació útil, però realitza una funció diferent en segon pla sense el coneixement de l'usuari. [3] L'exemple més senzill d'això és un programa maliciós que elimina els fitxers de l'usuari, però el nom del fitxer implica una altra funció, com ara funny_screen_schoner.exe . No importa si el "salvapantalles divertit" realment mostra un estalvi de pantalla mentre destrueix les dades o simplement destrueix les dades. L'ús del nom del fitxer enganyós és suficient per classificar el programa com un cavall de Troia.

Els troians també es poden utilitzar per instal·lar programes de backdoor, però no els inclouen necessàriament. Si un troià alberga i instal·la un programa de backdoor independent, l'intrús accedeix al programa de porta del darrere instal·lat, no al troià. El troià només va servir en aquest cas com a utilitat per a la instal·lació secreta. El troià es pot esborrar en qualsevol moment, sense que això tingui un efecte en la funció addicional del programa de la porta del darrere.

Tanmateix, ningú impedeix que el desenvolupador d'un programa de backdoor utilitzi la tecnologia d'un troià. Un programa de backdoor que es disfressa com una aplicació útil (per exemple, un rellotge d'escriptori que permet, de forma secreta, l'accés remot a l'ordinador) és un híbrid entre una porta del darrere i un troià. Si aquest tipus de programa està acabat o fins i tot esborra, la funció de porta tancada secreta ja no està disponible.

Exemples
Una variant consisteix a incorporar en un sistema contrasenyes fixes conegudes només pel creador del sistema o altres funcions ocultes que permeten l'accés sense l' autenticació habitual. [1] Un exemple conegut d'això és el codi hash emès per Award Programari durant diversos anys, que funciona amb la contrasenya universal BIOS "lkwpeter" [2] .

El programari que permet l'accés remot a l'ordinador, z. Per exemple, programes com Sub Seven i Back Orifice .

L'any 1999 es va trobar una variable anomenada NSAKEY a Windows i també una sospita de porta del darrere.

Els enrutadors de Cisco Systems que gestionen grans parts del trànsit d'Internet també es proporcionen amb porta a terra per als serveis d'intel·ligència nord-americans [4] .

S'ha demostrat l'ús d'una porta del darrere en pel·lícules com WarGames - War Games i Jurassic Park .

Protecció contra una backdoor mitjançant verificabilitat del text original
Per als productes de programari, tenir una mirada gratuïta al seu codi font és un aspecte de seguretat informàtica. Entre altres coses, és important minimitzar el risc que un producte pugui contenir funcionalitats que l'usuari no hauria de saber, com ara la funció secreta d'una porta del darrere.

El programari de codi obert pot ser verificat pel públic i, a més, es pot examinar amb mitjans legalment inobjables per a vulnerabilitats que es puguin tancar amb més rapidesa d'aquesta manera.

Borders
Tot i que el programari de codi obert pot ser examinat per qualsevol que tingui coneixements adequats, fins i tot en funcions i vulnerabilitats secretes, però això no vol dir que la simple disponibilitat del codi font sigui una garantia que els usuaris d'ordinadors hagin verificat adequadament. Les vulnerabilitats del programari de codi obert durant un llarg període de temps apunten a aquest fet. [5] [6] A més, una porta d'entrada intel·ligentment construïda és difícil de reconèixer, fins i tot amb coneixements especialitzats ben fonamentats. El temps necessari per a l'anàlisi és sovint considerable en programes complexos.

Si el programa executable derivat d'una font externa es creava realment utilitzant el codi font publicat, o si una porta del darrere no estava instal·lada prèviament o que qualsevol altra modificació que es fa sovint és difícil per a l'usuari reconèixer. De nou, amb una experiència adequada, almenys en teoria, és possible una revisió. Tanmateix, sovint això és difícil en la pràctica, ja que els fitxers binaris creats durant la compilació poden estar influïts per molts factors, especialment en el cas d'una base de codi més gran, i en general no hi ha cap manera confiable d'esbrinar en quines condicions es va crear un fitxer executable determinat.

Una forma de garantir aquest pas de compilació és crear " compilacions reproduïbles ". El programari es compila d'una manera reproduïble o determinista, de manera que qualsevol pot verificar mitjançant la compilació pròpia que la compilació es va crear a partir del codi font corresponent i que no es va inserir cap porta del darrer durant el procés de compilació.

El 1984, durant el seu discurs de Turing Award, el pioner de l'ordinador, Ken Thompson, va presentar un exemple d'una porta al darrere que seria difícil de seguir fins i tot si el codi font estava disponible. La xerrada era d'un programa d'inici de sessió per a Unix , que es canvia de manera que accepta una contrasenya general a més de la contrasenya normal. Segons Thompson, aquesta porta del darrere pot afegir automàticament un compilador C adequadament manipulat quan es tradueix el programa d'inici de sessió, el que significa que el codi font del programa d'inici de sessió no indica cap manipulació. El procediment es podria moure a una altra instància, que s'encarrega de traduir el propi compilador C en un fitxer executable, pel qual la manipulació no seria evident ni tan sols a partir del codi font del compilador C.

Vegeu també

malware
rootkit

Enllaços web
Wiktionary: porta del darrere - definicions de significats, origen de paraules, sinònims, traduccions

Proves individuals

? Hochspringen nach:a b Robert C. Newman: Seguretat informàtica: protecció de recursos digitals ; Febrer de 2009, ISBN 978-0-7637-5994-0 , extracte de la pàgina 49: "El programari de backdoor permet que un intrús accedeixi a una computadora mitjançant un mètode d'entrada alternatiu. Wheras legitima els usuaris a connectar-se a través de portes frontals utilitzant un usuari i contrasenya, els atacants utilitzen portes posteriors per evitar aquests controls d'accés normals ", Books.google.com (revisió completa en línia del fragment citat); Windows Vista Security ; O'Reilly Verlag, 2007, ISBN 978-3-89721-466-8 , extracte pàgina 105: "Una porta del darrere és una porta del darrere d'una aplicació, un accés ocult a una computadora o una abreviació a través d'un mecanisme d'autorització"; books.google.de

(informació completa en línia sobre el extracte citat).
? Hochspringen nach:a b Protecció de la privacitat i informàtica forense - segona edició . ISBN 1-58053-830-4 , 2004, extracte de la pàgina 250: "Contrasenyes del BIOS de CMOS: [...] lkwpeter [...]", books.google.de (extracte complet del citat text).
? Cavalls troians (Memento de l' original del 27 d' octubre de 2012 a l' Arxiu d'Internet) Informació: el vincle de l'arxiu s'ha inserit automàticament i encara no s'ha verificat.Comproveu l'enllaç segons les instruccions i, a continuació, elimineu aquesta informació. , una breu descripció del BSI
? Sönke Iwersen, Ina Karabasz, Jens Koenen, Susanne Metzger: molèstia per un amic . A: Handelsblatt . No. 109 , 11 de juny de 2013, ISSN 0017-7296 , p. 1, 4 .
? El servidor IRC de codi obert UnrealIRCd va executar una porta del darrere des de novembre de 2009 fins a juny de 2010 , permetent als estrangers executar ordres amb els privilegis de l'usuari de UnrealRCd en el servidor - seguretat de Heise , autor Reiko Kaps, 12 de juny de 2010.
? El 13 de maig de 2008 , el projecte Debian va anunciar que el paquet OpenSSL de distribucions havia estat vulnerable des del 17 de setembre de 2006 (versió 0.9.8c-1 a 0.9.8g-9).
? Ken Thompson: Reflexions sobre la confiança de confiança . Comunicacions de l'ACM, agost de 1984 (PDF, 225 kB).

Altres eines
Netcat és una de les eines de hacking i administració de xarxes que pot ser emprada per obrir portes posteriors així com emprar-la per protegir-se d'elles. Originalment desenvolupada per a sistemes Unix , en l'actualitat també està disponible per Microsoft Windows .