

Bugi - ja miten se debuggataan

4.10.2007 09:13 — Antti Kirves

Entistä useampi haittaohjelma käyttää jonkinlaisia menetelmiä, joilla tunnistaa virustutkijoiden debuggerit ja monitorointiohjelmat.

Bugi on ohjelmassa oleva virhe, jonka takia ohjelma ei toimi toivotulla tavalla. Virheiden etsiminen ja poistaminen on debuggausta, ohjelman tarkkaa seuranta, joka auttaa näkemään, toimiiko ohjelma niin kuin pitääkin.

Pääasiallisesti debuggausta käytetään vieläkin ohjelmistojen virheiden etsimiseen, mutta se käy myös haittaohjelmien tutkimiseen.

Miksei tehdä alun perin bugittomia ohjelmia, järjestelmiä ja palveluja?

- Debuggausta tarvitaan, koska erehtyminen on inhimillistä. Ihmiset eivät pysty luomaan luotettavasti bugittomia ohjelmistoja. Tästä syystä debuggauksen tarve ei koskaan katoa, sanoo tietoturva-asiantuntija **Toni Koivunen** Viestintäviraston CERT-FI-yksiköstä.

Debuggerien tunnistamisominaisuus tekee haittaohjelmista entistä tehokkaampia. Haittaohjelmat pysyvät jossain tapauksissa hieman kauemmin pimennossa tunnistajien suhteen, jos ne onnistuvat hyvin tunnistamaan debuggerin tai jonkin muun analysoinnissa yleisesti käytetyn ohjelmiston.

- Suurimmassa osassa haittaohjelmista on nykyään jonninäköistä "antikoodia", jolla pyritään tunnistamaan mahdolliset virtuaalikoneet, debuggerit sekä analysointi- tai sandbox-ohjelmistot. Myös haittaohjelmien pakkaamiseen ja suojaamiseen käytetyissä ohjelmissa on entistä enemmän tällaista koodia.

Debuggaus tehdään yleensä tarkoitukseen tehdyllä ohjelmistolla, joita on saatavilla ilmaiseksi. Monitorointiohjelma-termillä tarkoitetaan haittaohjelmatutkimuksessa yleisimmin käytettyjä ohjelmistotyökaluja.

Haittaohjelmien tekijät pyrkivät estämään debuggereiden käytön virustutkimuksessa, koska debuggerin avulla haittaohjelman koodia voidaan suorittaa hallitusti ja samalla tarkastella, miten se toimii. Tämä taas johtaa haittaohjelman nopeampaan tunnistumiseen ja torjuntakeinojen leviämiseen, ja sitä virusmaakarit eivät halua.

Debuggereiden tunnistamiseen haittaohjelmien tekijöillä on Koivusen mukaan kymmeniä erilaisia tapoja. Osa tunnistustavoista liittyy debuggerin aiheuttamaan koodin suorituksen hidastumiseen, osa taas siihen, millä tavoin aktiivisena oleva debuggeri käyttäytyy ja miten se muuttaa haittaohjelman muistiympäristöä.

Haittaohjelmien toimintaa tutkivan työtä voidaan hankaloittaa monin tavoin. Yleisimmin haittaohjelma, joka tunnistaa debuggerin, tyytyy vain sammuttamaan itsensä.

Tutkijan kannalta on kuitenkin hankalampaa, jos haittaohjelma muokkaa käytöstään sen sijaan, että se vain tyytyisi sammuttamaan itsensä. Jos haittaohjelma muokkaa käyttäytymistään riittävän hienovaraisesti, voi tutkijalta jäädä huomaamatta tärkeä osa sen toiminnasta.

Tutkijan työtä hankaloittavia menetelmiä voidaan kiertää. Parhaiten se onnistuu tunnistamalla ennalta haittaohjelmasta ne koodinpätkät, jotka etsivät debuggereita.

- Kun koodin sijainti on selvillä, sen muokkaaminen tai ohittaminen on hyvin nopeaa ja yksinkertaista, Koivunen sanoo.

ITviikko 4.10.2007

<http://www.digitoday.fi/tietoturva/2007/10/04/bugi---ja-miten-se-debuggataan/200724491/66>