VírusHíradó

Nimda

2001. szeptember 18-án az F-Secure Corporation új, világszerte rendkívül gyorsan terjedő e-mail féregre hívta fel a számítógép-használók figyelmét. A "Nimda" néven ismert féreg e-mail mellékleteken keresztül, weblapokon és lokális hálózaton található fájlok fertőzésével terjed.

2001. szeptember 18-án az F-Secure Corporation új, világszerte rendkívül gyorsan terjedő e-mail féregre hívta fel a számítógép-használók figyelmét. A "Nimda" néven ismert féreg e-mail mellékleteken keresztül, weblapokon és lokális hálózaton található fájlok fertőzésével terjed. A féreg a "Copyright 2001 R.P.China" szöveget tartalmazza.

A végfelhasználók megfertőződhetnek a README.EXE kiterjesztésű e-mail mellékletek megnyitásától, vagy olyan, már fertőzött weblapok látogatásától, melyek README.EXE fájlok letöltését ajánlják fel. A program lefutását követően a féreg két módon terjedhet tovább. Elküldi magát a felhasználó e-mail címlistájában található összes címre, és szúrópróba-szerűen védtelen, megfertőzhető IIS webszervereket keres, amelyeket azután meg is fertőz. A Nimda a levelek és a weblapok mellett az IRC-n és az FTP-szervereken keresztül is terjedhet.

A féreg néhány ismert biztonsági rést kihasználva terjed tovább. Ilyen például néhány levelező program azon hibája, hogy automatikusan megnyitja a levelekhez csatolt fájlokat. A Nimda az Outlook Express levelezőprogram hibáját használja ki, továbbá a Microsoft IIS webszerver 4-es és 5-ös változatának 16 ismert biztonsági résést próbálja végig, behatolási pontot keresve. Ezek között van az a lyuk is, amelyet a korábban nagy károkat okozó Code Red hagyott maga után - írja a CNN.

"Igen veszélyes és nagyon gyorsan terjedő féreggel állunk szemben, mert a "Nimda" ötvözi számos elődjének tulajdonságát" - mondta Mikko Hypponen, az F-Secure Corporation Anti-Vírus kutató részlegének vezetője.

Képes a helyi hálózatok megosztott könyvtáraiban is terjedni, ezen felül a "Nimda" még jelentős mennyiségű Internet-forgalmat is generál. Az FBI véleménye szerint a Nimda nagyobb kárt okozhat, mint a CodeRed.

A "Nimda" az első olyan vírus, amely úgy módosít létező internetes oldalakat, hogy azok fertőzött állományokat kínáljanak fel letöltésre. Szintén ez az első féreg, amely végfelhasználói gépeket használ sebezhető webhelyek felkutatására. Ez a technika - amely az eddigi férgekben, például a Code Redben még nem volt jelen - lehetővé teszi a "Nimda" számára, hogy elérjen tűzfalak mögött elhelyezkedő intranet weblapokat.

A féreg az alábbiakat teszi:

- megosztja a C: meghajtót, így az kívülről is hozzáférhetővé, védtelenné válik.
- a lokális meghajtókon .ASP, .HTM és .HTML állományokat keres, amelyek nevében szerepel a DEFAULT, INDEX, MAIN vagy README részlet, ha a gép web szerver is egyben, akkor megfertőzze a rajta levő weblapokat. Ha talál ilyet, akkor ezek végére illeszt egy rövid Javascript kódot, ami a weblap megtekintésekor egy, az Internet Explorer 5.0 és 5.01 verzióiban levő biztonsági hiba miatt, automatikusan letölti és megnyitja a README.EML állományt, aminek hatására a vírus aktivizálódik.
- az Internetről letöltött ideiglenes állományok könyvtárában végignézi az összes .HTM* állományt, és ezekből kigyűjti az e-mail címeket, melyekre elküldi magát. Ezek küldésekor az SMTP protokollt használja.

A Microsoft Outlook és IIS webszerverek legutolsó javító állományai befoltozzák azokat a biztonsági réseket, amelyeket a féreg kihasznál.

Az F-Secure Anti-Virus képes felismerni és eltávolítani a "Nimda"-t, a vírusdefiníciós állományokban szeptember 18-a óta szerepel.

Az FBI szakmai szervezetek bevonásával már nyomozásba kezdett az ügyben. A kutatás jelenlegi állása szerint az új vírust szeptember 18-án észlelték először, Norvégiában. A nyomozók szerint semmi jele annak, hogy a vírus kapcsolatban lenne az amerikai szeptember 11-i terrortámadásokkal, ugyanakkor azt is hozzátették, hogy egyelőre korai lenne bármit is mondani arról, hogy ki és miért bocsátotta útjára a vírust.

Csizmazia István