VírusHíradó

Lopják a dokumentumainkat

A KLEZ nevű féreg új változata kezdett terjedni az Interneten. Az új változatot, melyet I-Worm.Klez.h névvel jelölnek, már több országban is észlelték, többek közt Japánban, Kínában, Ausztriában, Csehországban és az USA-ban. Az utóbbi napokban pedig már Magyarországon is tömegesen kapnak a felhasználók ilyen leveleket.

I-Worm.Klez.H
Névváltozatok: I-Worm.Klez.H, W32/Klez.H, Klez.K (Messagelabs), Klez.G (Trend)

A KLEZ nevű féreg új változata kezdett terjedni az Interneten. Az új változatot, melyet I-Worm.Klez.h névvel jelölnek, már több országban is észlelték, többek közt Japánban, Kínában, Ausztriában, Csehországban és az USA-ban. Az utóbbi napokban pedig már magyarországon is tömegesen kapnak a felhasználók ilyen leveleket. A napi statisztikát megjelenítő lapon láthatjuk, hogy a cikk írásakor (2002. április 26-án) a Klez.H vírus elképesztő értékkel vezeti a fertőzési listát.

Sor.	Előfordulás	Vírusnév
1.	(15477)	I-Worm.Klez.a-h (Klez Family)
2.	(750)	Win32.Elkern.c
3.	(604)	Exploit.IFrame.FileDownload
4.	(447)	JS.Trojan.Seeker
5.	(412)	I-Worm.Sircam
6.	(404)	Exploit.IFrame
7.	(359)	I-Worm.Nimda
8.	(340)	I-Worm.Hybris
9.	(328)	I-Worm.Magistr.b
10.	(241)	I-Worm.Badtransll
11.	(231)	I-Worm.Magistr
12.	(199)	April
13.	(190)	I-Worm.Badtrans
14.	(186)	Win32.FunLove (a.k.a. Fun Loving Criminals)
15.	(179)	Joke.Buttons
16.	(166)	Win95.CIH-Killer
17.	(161)	Trojan.PSW.GIP
18.	(146)	Riot Family
19.	(143)	I-Worm.MTX
20.	(141)	BigMouse Family

Ez a féreg-vírus az Internet segítségével terjed, fertőzött email üzenetek mellékleteként. A dolog érdekessége, hogy magát Klez.E elleni irtóprogramnak állítja be, pedig mentesítő program helyett egy új vírus verziót tartalmaz. A levélszövegben a furfangos vírusíró még azt is írja, hogy ne

törődjünk vele, ha a víruskeresők riasztanak a mellékelt programra, ez így helyes.

A fertőzött üzenet az alábbiak szerint néz ki:

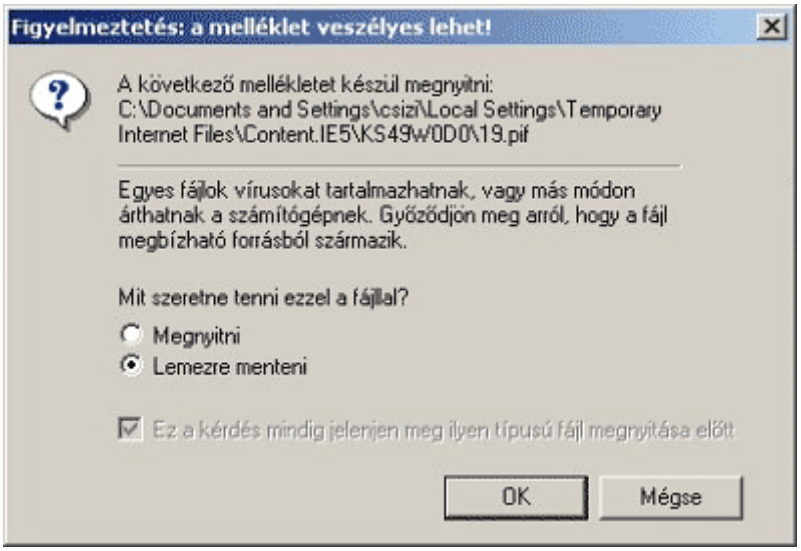
Tárgy: (Subject)
Worm Klez.E immunity

Levélszöveg: (Body)
Klez.E is the most common world-wide spreading worm.It's very
dangerous by corrupting your files.
Because of its very smart stealth and anti-anti-virus technic,most common AV software can't detect or clean it.
We developed this free immunity tool to defeat the malicious virus.
You only need to run this tool once,and then Klez will never come into your PC.
NOTE: Because this tool acts as a fake Klez to fool the real worm,some AV monitor maybe cry when you run it.
If so, Ignore the warning,and select 'continue'.
If you have any question,please mail to me.

A levél mellékletében a víruson kívül egy, a helyi gépen megtalálható állomány is szerepel, amelyet véletlenszerűen választ ki az alábbi kiterjesztésű fájlok közül: .TXT .HTM .HTML .WAB .ASP .DOC .RTF .XLS .JPG .CPP .C .PAS .MPG .MPEG .BAK .MP3 .PDF

Ez a módszer igen veszélyes (korábban a Sircam vírusnál tapasztalhattunk hasonlót), hiszen így személyes és bizalmas dokumentumaink kerülhetnek közkézre.

A féreg a lefuttatásához az IFRAME biztonsági rést használja ki (ugyanazt, melyet a Nimda és Aliz féreg is használt). Így a féreg már akkor aktiválódni tud, ha csak olvassuk vagy a Preview ablakban megjelenítjük a fertőzött üzenetet (ehhez hasonló volt a KAK.worm, ahol szintén a fertőzött melléklet megnyitása nélkül tudott aktiválódni a vírus).



A féreg ezenkívül megpóbálja megkeresni az adott gépen az ismertebb víruskereső programokat és megpróbálja azokat hatástalanítani. Az alábbi listán feltüntetett folyamatokat a "TerminateProcess" utasításal kísérli meg leállítani:

_AVP32, _AVPCC, _AVPM, ALERTSVC, AMON, AVP32, AVPCC, AVPM, N32SCANW, NAVAPSVC, NAVAPW32, NAVLU32, NAVRUNR, NAVW32, NAVWNT, NOD32, NPSSVC, NRESQ32, NSCHED32, NSCHEDNT, NSPLUGIN, SCAN, SMSS

A Klez.H elleni védekezéshez javasolt azonnal vírusismereti adatbázis frissítést végrehajtani. A fertőzés további megelőzéséhez érdemes lefuttatni a megfelelő javító patch állományokat is, a Microsoft Outlook Express biztonsági lyukainak befoltozására.

Ezeket az alábbi helyről lehet letölteni: http://www.microsoft.com/windows/ie/downloads/critical/Q319182/default.asp

Mentesítéshez a következő, Klez.H ellen is alkalmas CLRAV utility célprogramot ajánljuk a Kaspersky Labs cégtől: CLRAV gyorsmentesítő.

Az F-Secure és Kaspersky Anti-Virus programok a 2002. április 17. délutáni adatállományokkal már képesek detektálni ezt az új változatot is.

Csizmazia István