VírusHíradó

## Hamisított levelek és egyéb álhírek

**Célkeresztben a Microsoft - hamisított levelek vírusos melléklettel. Számos alkalommal fordul elő, hogy a vírusírók ismert cégek nevében írt levélben terjesztik magát a vírust, kihasználva ezzel a gyanútlan felhasználók hiszékenységét. Ezek a levelek lehetnek egyszerű tájékoztató jellegűek, vagy akár vírusellenes figyelmeztetésnek tűnő írások formájában is feltűnhetnek.**

### HardHead/VBS/Hard.A@MM

A vírusfigyelmeztetésnek álcázott féreg terjedésekor az Outlook Express címjegyzékéből vett összes névre elküldi magát. A levélben az alábbiakat lehet olvasni:

> Symantec vírus ellenes figyelmeztetés
> Helló! Megjelent egy új féreg a Neten. Ez a féreg nagyon gyorsan terjed és nagyon veszélyes! A Symantec észlelte először 2001. április 4-én. A mellékelt állományban van a leírása a féregnek és hogy hogyan tud terjedni. Üdvözlettel:
> F. Jones, Symantec vezető fejlesztő.
> Mellékelve: www.symantec.com.vbs

A Hard.A büntetőrutint is tartalmaz, ez november 24-én aktivizálódik. Ekkor a féreg egy üzenetablakot mutat az alábbi címmel és szöveggel:

> Some shocking news. Don't look surprised! It is only a warning about your stupidity Take care!

Magyarul:

> Megdöbbentő hír: Ne légy meglepve! Most a hülyeségedre figyelmeztetünk. Vigyázz!

**A víruskeresőket fejlesztő cégeket is igyekeznek befeketíteni!**

### I-Worm.Unis

Ha a féreg levélmellékletként érkező EXE állományát

lefuttatják, először elindít egy rejtett alkalmazást rendszer szervizként, bemásolja magát a Windows system könyvtárába MSVBVM60.EXE néven (nem keverendő össze a MSVBVM60.DLL nevű, tényleg létező VisualBasic DLL könyvtárral), és bejegyzi magát a Windows regisztrációs adatbázisába: SOFTWARE\Microsoft\Windows \CurrentVersion\Run

Több más ténykedése mellett itt is levélhamisítást láthatunk, de a hitelesség látszatát keltve több vírusvédelmi cég nevét is belekeverték:

From: "Microsoft Support" [support (a) microsoft.com]
Reply-To: "Peter Szor" [pszor (a) symantec.com]
To: "Mikko Hypponen" [mikko.hypponen (a) f-secure.com]
Subject: Virus Alert
Attached file name: uniclean.zip

"Kedves felhasználó
Az F-Secure, a Symantec és a Microsoft, az informatika területén vezető cégek, egy nagyon veszélyes vadon élő Internet-férget fedeztek fel (I-Worm.Universe). A féreg szerzője a "Benny" becenevű jól ismert európai "hacker" a 29A nevű vírusíró csoportból.

A Univers egy gyorsan terjedő féreg, ami egész számítógéprendszereket tett már tönkre az FBI-nál és a Microsoft-nál. A féreg erős titkosítást használ, és nagyon bonyolult. Nagyon sok független részből (úgynevezett modulból) áll, melyek nagyon sokfélék: minden második órában egy új modul jön létre, ami teljesen megváltoztatja a féreg viselkedését, beleértve a felismerést nehezítő trükköket is.

Ajánlatos ellenőrizni a rendszert a mi anti-vírus programunkkal, amelyet csatoltunk a levélhez. A jelentéseket kérjük, hogy a következő címek valamelyikére postázzák: universe (a) microsoft.com vagy universe (a) f-secure.com

üdvözlettel,
F-Secure, Symantec és Microsoft, az informatika területén vezető cégek. "

**Érdemes vigyázni, mert a büntetés akár a winchester formázása is lehet!**

**I-Worm.Redesi**

Új, magát Microsoft termékekhez kapcsolódó biztonsági javító állománynak álcázó, e-mailben terjedő Internetes féreg felbukkanását észlelték, melynek neve: "Redesi". Eddig két változatát fedezték fel:

**Redesi.a**
Az üzenet tárgya véletlenszerűen választódik ki az alábbi listából:

FW: Microsoft security update.
FW: Security Update by Microsoft.
FW: IT departments on state of HIGH ALERT.
FW: Important news from Microsoft.
FW: Stop terrorists computer viruses reign.
FW: Terrorists release computer virus.
FW: Emergency response from Microsoft Corp.
FW: Terrorist Emergency. Latest virus can wipe disk in minutes.
FW: Microsoft Update. Final Release Candidate.
FW: New computer virus.

-----Original Message-----
From: Microsoft Support Desk [mailto:Support (a) microsoft.com]
Sent: 17 October 2001 15:21
Subject: Security Update

Az üzenet szövegében egy biztonsági patchről esik szó, amelyet állítólag a Microsoft Corp. küldött, azonban ehelyett maga a vírus várakozik a levél mellékletében.

A féreg első indításakor egy üzenetet jelenít meg:

Cím: Microsoft Windows Update
Üzenet: Your Windows Update has been successful.

A másik variáns, az úgynevezett "**Redesi.b**" változatnál az üzenet tárgya véletlenszerűen választódik ki egy másik listából, és a következő üzenetet jeleníti meg:

Cím: %file path%\%filename% is not a valid Win32 application.
Üzenet: %file path%\%filename% is not a valid Win32 application.

Mindkét változat esetén a csatolt állomány nevét a féreg a következő listáról választja:

Si.exe, ReDe.exe, Disk.exe, Common.exe, UserConf.exe

Ha a mellékletet lefuttatjuk, a féreg először bemásolja magát a C meghajtóra a fenti nevek mindegyikén, majd elküldi magát

a Microsoft Outlook címjegyzékében található összes címre. Ha a Microsoft Outlook program nincs telepítve a gépen, a féreg nem képes továbbterjedni. 2001. november 11-én, ha a Windows rövid dátumformátuma "dd/mm/yy" vagy "mm/dd/yy", a "Redesi" aktiválja a büntető eljárását, melynek keretében az AUTOEXEC.BAT fájlba olyan parancsokat helyez el, hogy a gép következő indításakor a C lemezt megformázza.

**Hoax-ok, azaz álhírek - ezúttal vírusmentesen**

Igen sok esetben maga az e-mail útján érkező kéretlen levél a támadás eszköze, melyben arra kérnek minket, hogy legyünk szívesek azt minden ismerősünknek elküldeni. Azt hiszem, ez az a pont, ahol érdemes gyanakvóvá válni, hiszen értelmes és hiteles levélben ilyen kitétel szinte sosem szerepel. Azonban minden ilyen levél kapcsán bebizonyítja az élet, hogy akadnak, akik kellő gyanakvás vagy gondolkodás nélkül beteljesítik az álhír készítőjének akaratát, és újra meg újra útra kelnek a "jóindulatú" figyelmeztetések. Remek példa erre a már több éve keringő, a Budweiser nevű képernyőkímélő alkalmazás állítólagos fertőzöttségére figyelmeztető levél. Az ilyen álhírek küldözgetése felesleges riadalmat és szükségtelen forgalmat idéz elő, valamint sok esetben lelassítja az értelmes adatok átviteli sebességét.

Akiket bővebben is érdekelnek a hoax-ok, vagy gyanús levél érkezésekor szeretné azokat az álhírek adatbázisában leellenőrizni, azok az alábbi címen tudnak keresni: www.f-secure.com/hoaxes/hoax_index.shtml

Csizmazia István