WORM_EMUDBOT.JP

trendmicro.com/vinfo/us/threat-encyclopedia/malware/worm_emudbot.jp

- 
  Threat Type: Worm
- 
  Destructiveness: No
- 
  Encrypted:
- 
  In the wild: Yes

OVERVIEW

This worm arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

TECHNICAL DETAILS

Arrival Details

This worm arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

Other System Modifications

This worm deletes the following files:

- A:\autorun.inf
- A:\autorun.bat
- A:\autorun.vbs

Dropping Routine

This worm drops the following files:

- %User Temp%\tzscd.exe

- A:\recycle.exe

(Note: *%User Temp%* is the current user's Temp folder, which is usually C:\Documents and Settings\{user name}\Local Settings\Temp on Windows 2000, XP, and Server 2003.)

Other Details

This worm connects to the following possibly malicious URL:

- http://network.{BLOCKED}d.com/webyx/iLog.php?dl=5.1&log=Loader: 501~EXP
- http://absbh.{BLOCKED}tedya.com/webyx/remote.php?{random characters}
- http://ccy.{BLOCKED}tedya.com/webyx/settings.cfg?build=501&os=XP
- http://jgfx.{BLOCKED}ntedya.com/webyx/remote.php?{random characters}
- http://meya.{BLOCKED}ntedya.com/webyx/settings.cfg?build=501&os=XP
- http://asgsaq.{BLOCKED}ctya.com/webyx/remote.php?{random characters}
- http://abmnab.{BLOCKED}ctya.com/webyx/settings.cfg?build=501&os=XP
- http://kla.{BLOCKED}fying.com/webyx/remote.php?{random characters}
- http://wfayhg.{BLOCKED}fying.com/webyx/settings.cfg?build=501&os=XP
- http://txnkft.{BLOCKED}orked.com/webyx/remote.php?{random characters}
- http://vtwupbp.{BLOCKED}orked.com/webyx/settings.cfg?build=501&os=XP
- http://yvwsqa.{BLOCKED}tedya.com/webyx/remote.php?{random characters}
- http://kawi.{BLOCKED}tedya.com/webyx/settings.cfg?build=501&os=XP

This report is generated via an automated analysis system.

SOLUTION

Step 1

For Windows XP and Windows Server 2003 users, before doing any scans, please make sure you disable *System Restore* to allow full scanning of your computer.

Step 2

Search and delete these files

[Learn More]

There may be some component files that are hidden. Please make sure you check the *Search Hidden Files and Folders* checkbox in the "More advanced options" option to include all hidden files and folders in the search result.

- %User Temp%\tzscd.exe
- A:\recycle.exe

Step 3

Scan your computer with your Trend Micro product to delete files detected as WORM_EMUDBOT.JP. If the detected files have already been cleaned, deleted, or quarantined by your Trend Micro product, no further step is required. You may opt to simply delete the quarantined files. Please check this Knowledge Base page for more information.

Step 4

Restore this file from backup only Microsoft-related files will be restored. If this malware/grayware also deleted files related to programs that are not from Microsoft, please reinstall those programs on you computer again.

- A:\autorun.inf
- A:\autorun.bat
- A:\autorun.vbs

Did this description help? Tell us how we did.