Troj/Binanen-B

sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Binanen-B/detailed-analysis.aspx

Examples of Troj/Binanen-B include:

Example 1

File Information

Size
56K

SHA-1
849bfe083318883d21a22d3c0e60c3ca299eb207

MD5
36fafb384871eb1709b529a429f8bb7e

CRC-32
200e631d

File type
Windows executable

First seen
2012-08-30

Example 2

File Information

Size
56K

SHA-1
0dde72f98a5d0fd673cd6e6935979f2eed6fb624

MD5
cd7e2ba8c978dfe7d897818324b1ade2

CRC-32
e2dbaef0

File type
Windows executable

First seen
2012-08-08

Runtime Analysis

Processes Created

c:\windows\system32\ipconfig.exe

HTTP Requests

- http://webmail.onlinelibraryus.org/3449/dldlfgfeej/cSem/dddpfmlfqddq/SF/
- http://webmail.onlinelibraryus.org/4153/z7z7121115/yo08/zzzB1871CzzC/ob/
- http://webmail.onlinelibraryus.org/4509/jrjrlmllmm/iYks/jjjvlsrlwjjw/YL/
- http://webmail.onlinelibraryus.org/5187/fnfnhihgio/eUgo/fffrhonhsffs/UH/
- http://webmail.onlinelibraryus.org/7499/x5x5z0zy26/wmy6/xxx9z65zAxxA/mZ/

DNS Requests

webmail.onlinelibraryus.org

Example 3

File Information

Size
56K

SHA-1
209cd7cdf5e9feaac88c80d19e40f56c25278fcf

MD5
338df7ec071b3487b1c015787dfe97a6

CRC-32
83cdffe9

File type
Windows executable

First seen
2011-06-28