Trojan:Win32/Barkiofork.A

Article URL
malware.php?mal_id=15325204304f55b81313d570.37593033

Author
SecurityHome.eu

Published: 06 March 2012

Aliases :

Trojan:Win32/Barkiofork.A

is also known as *Trojan.ADH.2 (Symantec)*

.

Explanation :

Trojan:Win32/Barkiofork.A is a trojan that steals information from an infected computer, and sends it to a remote host. It may also download and execute arbitrary files.

Top

Trojan:Win32/Barkiofork.A is a trojan that steals information from an infected computer, and sends it to a remote host. It may also download and execute arbitrary files.

Installation

As part of its installation, Trojan:Win32/Barkiofork.A creates the following files:

* %Documents and Settings%ntshrui.dll
* %temp%update.exe
* %windir%ntshrui.dll
* %windir%ntshrui.dll1

* <startup folder>Adobe_u.exe
* <startup folder>adobeup.exe

Note: <startup folder> refers to a variable location that is determined by the malware by querying the operating system. The default installation location for the Startup folder for Windows 9x, Me, NT, 2000, XP and 2003 is '%USERPROFILE%Start MenuProgramsStartup'. For Windows Vista and 7, the default location is '%USERPROFILE%AppDataRoamingMicrosoftWindowsStart MenuProgramsStartup'.

Payload

Steals sensitive information

Trojan:Win32/Barkiofork.A collects the following information from the affected computer which it may later send to a remote host:

* Current user name
* Current process IDs
* How long it has been running
* Processor type
* CPU Speed
* Windows version
* Windows build
* Memory usage and amount available
* Disk information for each disk
* Disk brand
* Disk total size
* Disk used size
* Disk serial number
* Disk model number
* Disk controller information

* Drive information
* Drive type
* Drive model
* Drive serial number
* Drive controller
* Drive revision number
* Drive controller information
* Drive bus type
* Whether the drive is removable or not
* Drive vendor

Contacts remote hosts

Trojan:Win32/Barkiofork.A contacts one of the following remote hosts to send the stolen information it collects:

* tian.mymom.info:8000
* www2.update.ns1.name:80
* hal.vircheck.com:443
* cisco.ns01.info:80
* hlagl.vircheck.com:443
* cisco.ns01.info:80
* tian.mymom.info:8000
* up.msdn.ns01.us:80
* mast.zyns.com:8086

Downloads arbitrary files

Trojan:Win32/Barkiofork.A may download %temp%update.exe from the following locations:

* vircheck.com/a.bin
* 152.160.131.83/1216.bin
* ftp.update.acmetoy.com/update/a.bin
* update.itsAOL.com/0902.bin

Analysis by Michael Johnson

Last update 06 March 2012