Trojan-Dropper.Win32.Agent.albv

This is a malicious trojan. It adds its executable file to the list of trusted applications in Windows firewall ...

Detection date: March 29, 2009

Technical details

This is a malicious trojan. It is a Windows PE EXE file, its size is 23552 bytes.

Setting

This Trojan automatically copies its executable file as follows:

% Windir% systemsvhost.exe

To make sure that the trojan is started automatically when the system restarts, it adds a link to its executable file in the registry system as follows:

[HKLMSOFTWAREMicrosoftWindowsCurrentVersionRun]
"WSVCHO" = "% WinDir% systemsvhost.exe"

Work

It adds its executable file to the list of trusted applications in Windows firewall. It then starts the " ***iexplore.exe*** " process and injects its code into this process.

It also tries to end the following processes:

avesvc.exe
ashdisp.exe
avgrsx.exe
bdss.exe
spider.exe
avp.exe
nod32krn.exe
cclaw.exe
dvpapi.exe
ewidoctrl.exe

mcshield.exe
pavfires.exe
almon.exe
ccapp.exe
pccntmon.exe
fssm32.exe
issvc.exe
vsmon.exe
cpf.exe
ca.exe
tnbutil.exe
avp.exe
mpfservice.exe
npfmsg.exe
outpost.exe
psrv.exe
pavfires.exe
kpf4ss.exe
persfw.exe
vsserv.exe
smc.exe

It also attempts to disable the following services in conjunction with antivirus and firewall programs:

AntiVir
Avast Antivirus
AVG Antivirus
BitDefender
Dr.Web
Kaspersky Antivirus
Nod32
Norman
Authentium Antivirus
Ewido Security Suite
McAfee VirusScan
Panda Antivirus / Firewall
Sophos
Symantec / Norton
PC-cillin Antivirus
F-Secure
Norton Personal Firewall
ZoneAlarm
Comodo Firewall
eTrust EZ Firewall
F-Secure Internet Security
Kaspersky Antihacker
McAfee Personal Firewall

Norman Personal Firewall
Outpost Personal Firewall
Panda Internet Seciruty Suite
Panda Anti-Virus / Firewall
Kerio Personal Firewall
Tiny Personal Firewall
BitDefender / Bull Guard Antivirus
Sygate Personal Firewall

The Trojan also collects passwords to websites cached by the following browsers:

Mozilla Firefox
Internet Explorer

It also collects data about the accounts and passwords of the following chat programs:

Trillian
Miranda
Yahoo Messenger
MySpace IM
Gaim

The Trojan has the features of a keylogger and can create screenshots of the user's desktop. These screenshots are saved to the *Temporary* directory as with a decimal.

The collected data will be sent to the operator's server:

212.158.160. *

Spread through mobile storage devices

The Trojan copies its executable file to the root of each removable drive under the following name:

: wlan.exe with X is a drive

Along with the executable file, it also replaces the following file in the root of each drive:

: autorun.inf

This file will launch the executable file of the trojan every time a user opens an infected drive by double clicking on the drive.

Instructions for deleting

If your computer does not have an updated antivirus program, or does not have an effective antivirus solution,

follow these instructions to delete this malicious program:

1. Use Task Manager to determine the progress of this malicious program and turn it off.

2. Delete the original trojan file (the path will depend on how the original program infects the victim's system)

3. Delete the following keys in the registry system:

[HKLMSOFTWAREMicrosoftWindowsCurrentVersionRun]
"WSVCHO" = "% WinDir% systemsvhost.exe"

4. Delete the following files:

% WinDir% systemsvhost.exe

5. Wipe temporary folders (***% Temp%***)

6. Delete the following files from all drives:

: autorun.inf
: wlan.exe , with X being a drive

7. Update the antivirus program database and perform a "full scan" scan for your computer.