ALDIBOT

trendmicro.com/vinfo/us/threat-encyclopedia/malware/aldibot

OVERVIEW

ALDIBOT first appeared in late August 2012 in relevant forums. Variants can steal passwords from the browser Mozilla Firefox, instant messenger client Pidgin, and the download manager jDownloader. ALDIBOT variants send the gathered information to their command-and-control (C&C) servers.

This malware family can also launch Distributed Denial of Service (DDoS) attacks using different protocols such as HTTP, TCP, UDP, and SYN. It can also perform flood attacks via Slowloris and Layer 7.

This bot can also be set up as a SOCKS proxy to abuse the infected machine as a proxy for any protocols.

This malware family can download and execute arbitrary files, and update itself. Variants can steal information, gathering the infected machine's hardware identification (HWID), host name, local IP address, and OS version.

This backdoor executes commands from a remote malicious user, effectively compromising the affected system.

TECHNICAL DETAILS

Installation

This backdoor drops the following copies of itself into the affected system:

- %Application Data%\AudioTreiber_x64.exe
- %Application Data%\hklm.exe
- %Application Data%\nvsvc32.exe
- %Application Data%\Windowsie.exe

(Note: *%Application Data%* is the current user's Application Data folder, which is usually C:\Documents and Settings\{user name}\Application Data on Windows 2000, XP, and Server 2003, or C:\Users\{user name}\AppData\Roaming on Windows Vista and 7.)

Other System Modifications

This backdoor adds the following registry keys:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Active Setup\Installed Components\{random}

It adds the following registry entries:

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
Audio Treiber x64 = "%Application Data%\AudioTreiber_x64.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run
Audio Treiber x64 = "%Application Data%\AudioTreiber_x64.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Active Setup\Installed Components\{random}
Audio Treiber x64 = ""%Application Data%\AudioTreiber_x64.exe /ActiveX""

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\AuthorizedApplications\
List
%Application Data%\AudioTreiber_x64.exe = "%Application
Data%\AudioTreiber_x64.exe:*:Enabled:"

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
c0xG3w0pwDWmTic = "%Application Data%\hklm.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run
c0xG3w0pwDWmTic = "%Application Data%\hklm.exe"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\AuthorizedApplications\
List
%Application Data%\hklm.exe = "%Application Data%\hklm.exe:*:Enabled:"

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
NVidia Physx Service = "%Application Data%\nvsvc32.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run
NVidia Physx Service = "%Application Data%\nvsvc32.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Active Setup\Installed Components\{random}
NVidia Physx Service = ""%Application Data%\nvsvc32.exe /ActiveX""

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
KyKEJSLY1Nb07ie = "%Application Data%\Windowsie.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run
KyKEJSLY1Nb07ie = "%Application Data%\Windowsie.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Active Setup\Installed Components\{random}
KyKEJSLY1Nb07ie = ""%Application Data%\Windowsie.exe /ActiveX""

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Run
sw9YAYyV3loUuvj = "%Application Data%\AudioTreiber_x64.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run
sw9YAYyV3loUuvj = "%Application Data%\AudioTreiber_x64.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Active Setup\Installed Components\{random}
sw9YAYyV3loUuvj = ""%Application Data%\AudioTreiber_x64.exe /ActiveX""

Backdoor Routine

This backdoor executes the following commands from a remote malicious user:

- StartHTTP - starts an HTTP DDoS attack
- StartSlowloris - starts a Slowloris DDoS attack
- StartTCP - starts a TCP DDoS attack
- StartSSYN - starts SYN DDoS attack
- StartLayer7 - starts Layer 7 DDoS attack
- StopHTTPDDoS - stops an HTTP DDoS attack
- StopTCPDDoS - stops a TCP DDoS attack
- StopDDoS - stops all DDoS attack
- DownloadEx - downloads and executes file
- startUDP - starts a UDP DDoS attack
- OpenWebSite - visits sites
- CreateSocks - creates SOCKS5 proxy
- StealData - performs password stealing capability

- Update - updates itself

Other Details

This backdoor connects to the following possibly malicious URL:

- http://{BLOCKED}i.{BLOCKED}t.w2c.ru/gate.php?hwid={HWID}&pc={Host Name}&localip={Local IP Address}&winver={OS Version}
- http://{BLOCKED}1.ba.{BLOCKED}c.de/aldi/gate.php?hwid={HWID}&pc={Host Name}&localip={Local IP Address}&winver={OS Version}
- http://{BLOCKED}e.{BLOCKED}b.com/tt/gate.php?hwid={HWID}&pc={Host Name}&localip={Local IP Address}&winver={OS Version}
- http://{BLOCKED}lnoe.{BLOCKED}ke.com/musice/gate.php?hwid={HWID}&pc={Host Name}&localip={Local IP Address}&winver={OS Version}
- http://www.{BLOCKED}ued.de/aldi/gate.php?hwid={HWID}&pc={Host Name}&localip={Local IP Address}&winver={OS Version}

NOTES:

It attempts to get stored information such as user names, passwords, and host names from the following browsers:

> Mozilla Firefox

It steals information such as user names and passwords from the following application:

- Pidgin
- jDownloader

It also uses the following as its User-Agent:

> Aldi Bot FTW :D