TROJ_FAKEAV.GZD - Threat Encyclopedia | Trend Micro (US)

By Analysis by: Sabrina Lei Sioting

Archived: 2026-04-06 00:23:12 UTC

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

It employs registry shell spawning by adding certain registry entries. This allows this malware to execute even when other applications are opened.

It modifies registry entries to disable the Windows Firewall settings. This action allows this malware to perform its routines without being deteted by the Windows Firewall. It creates certain registry entries to disable applications related to security.

It deletes itself after execution.

It displays fake alerts that warn users of infection. It also displays fake scanning results of the affected system. It then asks for users to purchase it once scanning is completed. If users decide to purchase the rogue product, users are directed to a certain website asking for sensitive information, such as credit card numbers.

Arrival Details

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

Installation

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

- %User Profile%\Local Settings\Application Data\{random 3 letters}.exe

(Note: *%User Profile%* is the current user's profile folder, which is usually C:\Windows\Profiles\{user name} on Windows 98 and ME, C:\WINNT\Profiles\{user name} on Windows NT, and C:\Documents and Settings\{user name} on Windows 2000, XP, and Server 2003.)

Autostart Technique

This Trojan employs registry shell spawning to ensure its execution when certain file types are accessed by adding the following entries:

HKEY_CLASSES_ROOT\.exe\shell\
open\command
(Default) = ""%User Profile%\Local Settings\Application Data\{random 3 letters}.exe" -a "%1" %*"

HKEY_CLASSES_ROOT\.exe\shell\
open\command
IsolatedCommand = ""%1" %*"

HKEY_CLASSES_ROOT\.exe\shell\
runas\command
(Default) = ""%1" %*"

HKEY_CLASSES_ROOT\.exe\shell\
runas\command
IsolatedCommand = ""%1" %*"

HKEY_CLASSES_ROOT\exefile\shell\
open\command
IsolatedCommand = ""%1" %*"

HKEY_CLASSES_ROOT\exefile\shell\
runas\command
IsolatedCommand = ""%1" %*"

HKEY_CURRENT_USER\Software\Classes\
.exe\shell\open\
command
(Default) = ""%User Profile%\Local Settings\Application Data\{random 3 letters}.exe" -a "%1" %*"

HKEY_CURRENT_USER\Software\Classes\
.exe\shell\open\
command
IsolatedCommand = ""%1" %*"

HKEY_CURRENT_USER\Software\Classes\
.exe\shell\runas\
command
(Default) = ""%1" %*"

HKEY_CURRENT_USER\Software\Classes\
.exe\shell\runas\
command
IsolatedCommand = ""%1" %*"

HKEY_CURRENT_USER\Software\Classes\
exefile\shell\open\
command
(Default) = ""%User Profile%\Local Settings\Application Data\{random 3 letters}.exe" -a "%1" %*"

HKEY_CURRENT_USER\Software\Classes\
exefile\shell\open\
command
IsolatedCommand = ""%1" %*"

HKEY_CURRENT_USER\Software\Classes\
exefile\shell\runas\
command
(Default) = ""%1" %*"

HKEY_CURRENT_USER\Software\Classes\
exefile\shell\runas\
command
IsolatedCommand = ""%1" %*"

Other System Modifications

This Trojan adds the following registry keys:

HKEY_CLASSES_ROOT\.exe\shell

HKEY_CLASSES_ROOT\.exe\shell\
open

HKEY_CLASSES_ROOT\.exe\shell\
open\command

HKEY_CLASSES_ROOT\.exe\shell\
runas

HKEY_CLASSES_ROOT\.exe\shell\
runas\command

HKEY_CURRENT_USER\Software\Classes\
.exe\shell

HKEY_CURRENT_USER\Software\Classes\
.exe\shell\open

HKEY_CURRENT_USER\Software\Classes\
.exe\shell\open\
command

HKEY_CURRENT_USER\Software\Classes\
.exe\shell\runas

HKEY_CURRENT_USER\Software\Classes\
.exe\shell\runas\
command

HKEY_CURRENT_USER\Software\Classes\
exefile\shell

HKEY_CURRENT_USER\Software\Classes\
exefile\shell\open

HKEY_CURRENT_USER\Software\Classes\
exefile\shell\open\
command

HKEY_CURRENT_USER\Software\Classes\
exefile\shell\runas

HKEY_CURRENT_USER\Software\Classes\
exefile\shell\runas\
command

HKEY_CURRENT_USER\Software\Microsoft\
Internet Connection Wizard

It adds the following registry entries as part of its installation routine:

HKEY_CURRENT_USER\Software\Microsoft\
Internet Connection Wizard
ShellNext = "http://{BLOCKED}qag.com/10170004131137353284"

It modifies the following registry key(s)/entry(ies) as part of its installation routine:

HKEY_CLASSES_ROOT\exefile\shell\
open\command
(Default) = ""%User Profile%\Local Settings\Application Data\{random 3 letters}.exe" -a "%1" %*"

(Note: The default value data of the said registry entry is *"%1" %**.)

HKEY_LOCAL_MACHINE\SOFTWARE\Clients\
StartMenuInternet\FIREFOX.EXE\shell\
open\command
(Default) = ""%User Profile%\Local Settings\Application Data\{random three letter}.exe" -a "%Program Files%\Mozilla Firefox\firefox.exe""

(Note: The default value data of the said registry entry is *%Program Files%\Mozilla Firefox\firefox.exe*.)

HKEY_LOCAL_MACHINE\SOFTWARE\Clients\
StartMenuInternet\FIREFOX.EXE\shell\
safemode\command
(Default) = ""%User Profile%\Local Settings\Application Data\{random three letter}.exe" -a "%Program Files%\Mozilla Firefox\firefox.exe" -safe-mode"

(Note: The default value data of the said registry entry is *"%Program Files%\Mozilla Firefox\firefox.exe" -safe-mode*.)

HKEY_LOCAL_MACHINE\SOFTWARE\Clients\
StartMenuInternet\IEXPLORE.EXE\shell\
open\command
(Default) = ""%User Profile%\Local Settings\Application Data\{random three letter}.exe" -a "%Program Files%\Internet Explorer\iexplore.exe""

(Note: The default value data of the said registry entry is *"%Program Files%\Internet Explorer\iexplore.exe"*.)

It modifies the following registry entries to disable the Windows Firewall settings:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile
EnableFirewall = "0"

(Note: The default value data of the said registry entry is *1*.)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SharedAccess\Parameters\

FirewallPolicy\StandardProfile
DisableNotifications = "1"

(Note: The default value data of the said registry entry is *0*.)

It creates the following registry entry(ies) to bypass Windows Firewall:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile
EnableFirewall = "0"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile
DoNotAllowExceptions = "0"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile
DisableNotifications = "1"

It creates the following registry entries to disable applications related to security:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Security Center
AntiVirusDisableNotify = "1"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Security Center
AntiVirusOverride = "1"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Security Center
FirewallDisableNotify = "1"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Security Center
FirewallOverride = "1"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Security Center
UpdatesDisableNotify = "1"

Dropping Routine

This Trojan drops the following files:

- %System Root%\Documents and Settings\All Users\Application Data\2335886254
- %User Profile%\Local Settings\Application Data\2335886254
- %User Temp%\2335886254
- %User Profile%\Templates\2335886254

(Note: *%System Root%* is the root folder, which is usually C:\. It is also where the operating system is located.. *%User Profile%* is the current user's profile folder, which is usually C:\Windows\Profiles\{user name} on Windows 98 and ME, C:\WINNT\Profiles\{user name} on Windows NT, and C:\Documents and Settings\{user name} on Windows 2000, XP, and Server 2003.. *%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 Trojan connects to the following possibly malicious URL:

- http://{BLOCKED}qag.com/10170004131137353284

It deletes itself after execution.

Rogue Antivirus Routine

This Trojan displays fake alerts that warn users of infection. It also displays fake scanning results of the affected system. It then asks for users to purchase it once scanning is completed. If users decide to purchase the rogue product, users are directed to a certain website asking for sensitive information, such as credit card numbers.

Step 2

Identify and terminate files detected as TROJ_FAKEAV.GZD

[Learn More]

a. If the detected file is displayed in either Windows Task Manager or Process Explorer but you cannot delete it, restart your computer in safe mode. To do this, refer to this linkopen on a new tab for the complete steps.
b. If the detected file is *not* displayed in either Windows Task Manager or Process Explorer, continue doing the next steps.

Step 3

Delete this registry key

[Learn More]

Important: Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this step only if you know how or you can ask assistance from your system administrator. Else, check this Microsoft articleopen on a new tab first before modifying your computer's registry.

- In *HKEY_CLASSES_ROOT\.exe\shell*
  - **runas**
- In *HKEY_CURRENT_USER\Software\Classes\.exe*
  - **shell**
- In *HKEY_CURRENT_USER\Software\Classes\exefile*
  - **shell**
- In *HKEY_CURRENT_USER\Software\Microsoft*
  - **Internet Connection Wizard**

Step 4

Delete this registry value

[Learn More]

Important: Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this step only if you know how or you can ask assistance from your system administrator. Else, check this Microsoft articleopen on a new tab first before modifying your computer's registry.

- In *HKEY_CLASSES_ROOT\exefile\shell\open\command*
  - **IsolatedCommand = "%1 %*"**
- In *HKEY_CLASSES_ROOT\exefile\shell\runas\command*
  - **IsolatedCommand = "%1 %*"**
- In *HKEY_CURRENT_USER\Software\Classes\exefile\shell\open\command*
  - **(Default) = "%User Profile%\Local Settings\Application Data\{random 3 letters}.exe -a %1 %*"**
- In *HKEY_CURRENT_USER\Software\Classes\exefile\shell\open\command*
  - **IsolatedCommand = "%1 %*"**
- In *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfil*
  - **EnableFirewall = "0"**
- In *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfil*
  - **DoNotAllowExceptions = "0"**
- In *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfil*
  - **DisableNotifications = "1"**
- In *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center*
  - **AntiVirusDisableNotify = "1"**
- In *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center*
  - **AntiVirusOverride = "1"**
- In *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center*
  - **FirewallDisableNotify = "1"**
- In *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center*
  - **FirewallOverride = "1"**
- In *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center*
  - **UpdatesDisableNotify = "1"**

Step 5

Restore this modified registry value

[Learn More]

Important: Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this step only if you know how or you can ask assistance from your system administrator. Else, check this Microsoft articleopen on a new tab first before modifying your computer"s registry.

- In *HKEY_CLASSES_ROOT\exefile\shell\open\command*
  - From: **(Default) = "%User Profile%\Local Settings\Application Data\{random 3 letters}.exe -a %1 %*"**
    To: **(Default) = "%1 %*"**
- In *HKEY_LOCAL_MACHINE\SOFTWARE\Clients\StartMenuInternet\FIREFOX.EXE\shell\open\command*
  - From: **(Default) = "%User Profile%\Local Settings\Application Data\{random 3 letters}.exe -a %Program Files%\Mozilla Firefox\firefox.exe"**

To: **(Default) = "%Program Files%\Mozilla Firefox\firefox.exe"**

- In *HKEY_LOCAL_MACHINE\SOFTWARE\Clients\StartMenuInternet\FIREFOX.EXE\shell\safemode\command*
  - From: **(Default) = %User Profile%\Local Settings\Application Data\{random 3 letters}.exe -a %Program Files%\Mozilla Firefox\firefox.exe -safe-mode**
    To: **(Default) = %Program Files%\Mozilla Firefox\firefox.exe -safe-mode**
- In *HKEY_LOCAL_MACHINE\SOFTWARE\Clients\StartMenuInternet\IEXPLORE.EXE\shell\open\command*
  - From: **(Default) = "%User Profile%\Local Settings\Application Data\{random 3 letters}.exe -a %Program Files%\Internet Explorer\iexplore.exe"**
    To: **(Default) = "%Program Files%\Internet Explorer\iexplore.exe"**
- In *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfi*
  - From: **EnableFirewall = "0"**
    To: **EnableFirewall = "1"**
- In *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfi*
  - From: **DisableNotifications = "1"**
    To: **DisableNotifications = "0"**

Step 6

Search and delete this file

[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.

- %System Root%\Documents and Settings\All Users\Application Data\2335886254
- %User Profile%\Local Settings\Application Data\2335886254
- %User Temp%\2335886254
- %User Profile%\Templates\2335886254

Step 7

Scan your computer with your Trend Micro product to delete files detected as TROJ_FAKEAV.GZD. 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 pageopen on a new tab for more information.

Did this description help? Tell us how we did.open on a new tab

---