TSPY_TRICKLOAD.N - Threat Encyclopedia | Trend Micro (US)

By Analysis by: Francis Xavier Antazo

Archived: 2026-04-06 01:07:14 UTC

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

It uses the Windows Task Scheduler to add a scheduled task that executes the copies it drops.

It connects to certain websites to send and receive information. It deletes the initially executed copy of itself.

Arrival Details

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

It may be dropped by the following malware:

- TROJ_UPATRE.YYSTV

Installation

This spyware drops the following copies of itself into the affected system and executes them:

- %Application Data%\{malware file name}.exe

(Note: *%Application Data%* is the Application Data folder, where it usually is C:\Documents and Settings\{user name}\Application Data on Windows 2000, Windows Server 2003, and Windows XP (32- and 64-bit); C:\Users\{user name}\AppData\Roaming on Windows Vista (32- and 64-bit), Windows 7 (32- and 64-bit), Windows 8 (32- and 64-bit), Windows 8.1 (32- and 64-bit), Windows Server 2008, and Windows Server 2012.)

It drops the following files:

- %Application Data%\client_id
- %Application Data%\group_tag

(Note: *%Application Data%* is the Application Data folder, where it usually is C:\Documents and Settings\{user name}\Application Data on Windows 2000, Windows Server 2003, and Windows XP (32- and 64-bit); C:\Users\{user name}\AppData\Roaming on Windows Vista (32- and 64-bit), Windows 7 (32- and 64-bit), Windows 8 (32- and 64-bit), Windows 8.1 (32- and 64-bit), Windows Server 2008, and Windows Server 2012.)

It uses the Windows Task Scheduler to add a scheduled task that executes the copies it drops.

It adds the following processes:

- svchost.exe

It creates the following folders:

- %Application Data%\Modules\
- %Application Data%\Modules\injectDll32_configs

(Note: *%Application Data%* is the Application Data folder, where it usually is C:\Documents and Settings\{user name}\Application Data on Windows 2000, Windows Server 2003, and Windows XP (32- and 64-bit); C:\Users\{user name}\AppData\Roaming on Windows Vista (32- and 64-bit), Windows 7 (32- and 64-bit), Windows 8 (32- and 64-bit), Windows 8.1 (32- and 64-bit), Windows Server 2008, and Windows Server 2012.)

It adds the following mutexes to ensure that only one of its copies runs at any one time:

- Global\TrickBot

It injects codes into the following process(es):

- added svchost.exe

Autostart Technique

The scheduled task executes the malware every:

- minute

Download Routine

This spyware saves the files it downloads using the following names:

- %Application Data%\Modules\injectDll32
- %Application Data%\Modules\systeminfo32
- %Application Data%\Modules\config.conf (updated config file)
- %Application Data%\Modules\injectDll32_configs\dinj
- %Application Data%\Modules\injectDll32_configs\dpost
- %Application Data%\Modules\injectDll32_configs\sinj

(Note: *%Application Data%* is the Application Data folder, where it usually is C:\Documents and Settings\{user name}\Application Data on Windows 2000, Windows Server 2003, and Windows XP (32- and 64-bit); C:\Users\{user name}\AppData\Roaming on Windows Vista (32- and 64-bit), Windows 7 (32- and 64-bit), Windows 8 (32- and 64-bit), Windows 8.1 (32- and 64-bit), Windows Server 2008, and Windows Server 2012.)

Information Theft

This spyware s configuration file contains the following information:

- CnC
- Modules
- targeted banks (downloaded config file)

Other Details

This spyware connects to the following URL(s) to get the affected system's IP address:

- {BLOCKED}rnalip.com

It connects to the following website to send and receive information:

- {BLOCKED}.{BLOCKED}.138.194:443
- {BLOCKED}.{BLOCKED}.44.28:443
- {BLOCKED}.{BLOCKED}.23.98:443
- {BLOCKED}.{BLOCKED}.28.24:443
- {BLOCKED}.{BLOCKED}.176.6:443
- {BLOCKED}.{BLOCKED}.209.51:443
- {BLOCKED}.{BLOCKED}.52.75:443
- {BLOCKED}.{BLOCKED}.211.34:443
- {BLOCKED}.{BLOCKED}.28.0:443
- {BLOCKED}.{BLOCKED}.234.69:443
- {BLOCKED}.{BLOCKED}.251.0:443
- {BLOCKED}.{BLOCKED}.28.103/response.php
- {BLOCKED}.{BLOCKED}.28.77:443
- http://{BLOCKED}.{BLOCKED}.1.53:8082

It does the following:

- It monitors bank related site accesses in browsers using the following strings:
  - */onlineserv/CM*
  - *ibanking.stgeorge.com.au/ibank/loginPage.action*
  - *ib.nab.com.au/nabib/index.jsp*
  - *banking.westpac.com.au/wbc/banking/handler*
  - *anz.com/IBAU/BANKAWAYTRAN*
  - *anz.com/INETBANK/login.asp*
  - *cibconline.cibc.com/olbtxn/authentication/*.cibc*

It deletes the initially executed copy of itself

Step 2

Note that not all files, folders, and registry keys and entries are installed on your computer during this malware's/spyware's/grayware's execution. This may be due to incomplete installation or other operating system conditions. If you do not find the same files/folders/registry information, please proceed to the next step.

Step 3

Remove the malware/grayware file that dropped/downloaded TSPY_TRICKLOAD.N. (Note: Please skip this step if the threat(s) listed below have already been removed.)

- TROJ_UPATRE.YYSTV

Step 4

Restart in Safe Mode

[Learn More]

Step 5

Delete the Scheduled Tasks added by this malware/grayware

[Learn More]

To delete the added Scheduled Task file:

For Windows 2000, Windows XP, and Windows Server 2003:

1. Open the Windows Scheduled Tasks. To do this, click Start>Programs>Accessories>System Tools>Scheduled Tasks.
2. Double-click on a .JOB file.
3. Check if the malware path and file name exists in the .JOB file. To do this, check the value in the *Run* field.
4. If found, select the .JOB file then press SHIFT+DELETE to permanently delete the file.
5. Repeat the steps above for the remaining .JOB files.

For Windows Vista, Windows 7, Windows Server 2008, Windows 8, Windows 8.1, and Windows Server 2012:

1. Open the Windows Task Scheduler. To do this:
   • On *Windows Vista, Windows 7,* and *Windows Server 2008,* click *Start*, type *taskschd.msc* in the *Search* input field, then press *Enter*.
   • On *Windows 8, Windows 8.1*, and *Windows Server 2012*, right-click on the lower left corner of the screen, click *Run*, type *taskschd.msc*, then press *Enter*.
2. In the left panel of the Task Scheduler Window, click *Task Scheduler Library*.
3. In the upper-middle panel, click a Task.
4. In the lower middle panel, click the *Actions* tab
5. Check if the malware path and file name exists in the task. To do this, check the value in the *Details* column under the *Actions* tab.
6. If found, select the task and press DELETE and click Yes to delete the task.
7. Repeat the steps above for the remaining tasks.

Step 6

Search and delete these folders

[Learn More]

Please make sure you check the *Search Hidden Files and Folders* checkbox in the More advanced options option to include all hidden folders in the search result.

- %Application Data%\Modules\
- %Application Data%\Modules\injectDll32_configs

Step 7

Search and delete these files

[Learn More]

There may be some 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.

- %Application Data%\client_id
- %Application Data%\group_tag

Step 8

Restart in normal mode and scan your computer with your Trend Micro product for files detected as TSPY_TRICKLOAD.N. 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.

Step 9

Scan your computer with your Trend Micro product to delete files detected as TSPY_TRICKLOAD.N. 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

---