

اهب وظائف تحت يديتلا داعبتسالال ةمئاق تارييغت ةنمالال ةياهنلال ةطقن مكحت ةدحول Cisco

تايوتحملال

[ةمدقملا](#)

[ةيساسالالتابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ثيذحتلال دنع تاعقوتلا](#)

[تارييغتلا](#)

[2019 - س طسغأ 28](#)

[Microsoft Windows](#) ليضارتفالال ليغشتلال ماظن

[ذفاونلا - ةيسمشلال جايلا N-Able](#)

[Docker - Mac](#)

[ةديج مي: اوق عاشنلا م](#)

[2019 - ربم تبس 18](#)

[Apple MacOS](#) ليغشتلال ماظن ليضارتفالال عضولا

[McAfee - Mac](#)

[Cisco Jabber - Mac](#)

[Crashplan - Mac](#)

[JAMF Casper - Mac](#)

[VMWare Fusion - Mac](#)

[XCODE - Mac](#)

[Windows](#) - دجاو صارقأ كرحم

[Citrix ICA](#) - Windows لي مع

[ةديج مي: اوق عاشنلا م](#)

[2019 - ربم سي د 11](#)

[Windows](#) - دجاو صارقأ كرحم

[Splunk - Windows](#)

[Splunk - Linux](#)

[ةديج مي: اوق عاشنلا م](#)

[2020 - ري ارب ف 12](#)

[Windows](#) ليغشتلال ماظن - [Microsoft Windows](#) ليضارتفالال ليغشتلال ماظن

[WebSense - Windows](#)

[Microsoft SQL Server - Windows](#)

[2020 - وي ن وي 10](#)

[Malwarebytes - Windows](#)

[Microsoft Office - Windows](#)

[IIS - Windows](#)

[Symantec](#) - Windows ةطس اوب Altiris

[McAfee - Windows](#)

[ةديج مي: اوق عاشنلا م](#)

[2020 - وي ل وي 15](#)

[Windows](#) - لاجملاب مكحتلال تادجو

[Microsoft Teams - Windows](#)

[ةديج ةمئاق عاشنلا م](#)

[26 - س طس غأ 2020](#)

[Microsoft SQL Server - Windows](#)

[30 - ربم تبس 2020](#)

[Malwarebytes - Windows](#)

[Digital Guardian - Mac](#)

[قدیدج می: اوق عاش، نأ مت](#)

[3 - س رام 2021](#)

[Kaspersky - Windows](#)

[SCCM - Windows](#)

[Symantec - Windows](#)

[قدیدج می: اوق عاش، نأ مت](#)

[30 - وی، نو ی 2021](#)

[Microsoft Windows ل یض، ارت ف ال ا ل ی غ ش ت ل ا م اظن](#)

[Citrix ICA ل ی مع](#)

[Citrix دادم ا مداخ](#)

[قدیدج می: اوق عاش، نأ مت](#)

[29 - ربم تبس 2021](#)

[Cisco Webex - Windows](#)

[Crashplan - Windows](#)

[Crashplan - Mac](#)

[VMware - Windows](#)

[23 - س رام 2022](#)

[Microsoft Windows ل یض، ارت ف ال ا ل ی غ ش ت ل ا م اظن](#)

[Hyper-V - Windows](#)

[Microsoft Windows Defender - Windows](#)

[29 - وی، نو ی 2022](#)

[Microsoft Windows ل یض، ارت ف ال ا ل ی غ ش ت ل ا م اظن](#)

[Cisco AnyConnect VPN نم](#)

[Cisco Webex](#)

[Microsoft OneDrive \(اقتباس دحاو ص ارقأ ك حرم\)](#)

[Windows - موی، نات](#)

[Citrix دادم ا مداخ](#)

[قدیدج می: اوق عاش، نأ مت](#)

[14 - ربم تبس 2022](#)

[Microsoft Windows ل یض، ارت ف ال ا ل ی غ ش ت ل ا م اظن](#)

[Microsoft SQL Server](#)

[نوس ك ی ب أ / ورك ی ام دن یرت](#)

[قدیدج می: اوق عاش، نأ مت](#)

[2022 ربوت ك أ](#)

[14 - ربم س ی د 2022](#)

[Microsoft Windows ل یض، ارت ف ال ا ل ی غ ش ت ل ا م اظن](#)

[Windows - قی ف ل خ ل ا ت اری ی غ ت](#)

[قدیدج می: اوق عاش، نأ مت](#)

[12 - ل ی ربأ 2023](#)

[Microsoft Windows ل یض، ارت ف ال ا ل ی غ ش ت ل ا م اظن](#)

[Microsoft Intune](#)

[McAfee Trellix SolidCore](#)

[Cisco Webex](#)

[Microsoft Defender ل MacOS](#)

[Microsoft Defender ل Linux](#)

[31 - وی ام 2023](#)

[ميف](#)

[VMWare](#)

[2023 - ريبم تيب س. 27](#)

[Cisco Webex](#)

[Microsoft OneNote](#)

[Microsoft SQL Server](#)

[Microsoft Teams](#)

[Microsoft Windows ل. يضا رت فال. ل. ي غ ش ت ل. ا م اظن](#)

[قيظش](#)

[Symantec Endpoint Protection جمان رب](#)

[قديج مئاوق عاشن ا م ت](#)

[2023 - ريبم فون. 22](#)

[Microsoft Windows ل. يضا رت فال. ل. ي غ ش ت ل. ا م اظن](#)

[Citrix ICA ل. ي م ع](#)

[قديج مئاوق عاشن ا م ت](#)

[2024 - ريب ا ني. 24](#)

[قديج مئاوق عاشن ا م ت](#)

ةم دق م ل ا

نم اهت نا ي ص م ت ي ت ل ا تاءان ثت س ا ل ا ل ا اهت فاض ا م ت ي ت ل ا تاري ي غ ت ل ا دن ت س م ل ا اذه فص ي Cisco.

ري فوت ل Cisco ط س ا و ب اهت نا ي ص و Cisco نم اهت نا ي ص م ت ي ت ل ا تاءان ثت س ا ل ا عاشن ا م ت ي ة ي ا ه ن ل ا طاقن ل ص و م ل (AMP) "ةراض ل ا جمار ب ل ا نم ةم دق ت م ل ا ة ي ا م ح ل ا" ن ي ب ل ص ف ا ق ف ا و ت ل ا تاءان ثت س ا ل ا هذ ه ة فاض ا ن ك م ي و ، ي ر خ ا ل ا جمار ب ل ا و ا نام ا ل ا و ا تاس و ر ي ف ل ا ة ح ف ا ك م جمان رب و ق ي ب ط ت ل ا نم ة د ي ج ل ا تارا د ص ل ا

ة ي س ا س ا ل ا ت ا ب ل ط ت م ل ا

ت ا ب ل ط ت م ل ا

ة ي ل ا ت ل ا ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل نو ك ت ن ا ب Cisco ي ص و ت :

- ة ي ا ه ن ل ا طاقن ل AMP ي ف تاءان ثت س ا ل ا
- AMP م ك ح ت ل ا ة د ح و

ة م د خ ت س م ل ا ت ا ن و ك م ل ا

ة ي ل ا ت ل ا ة ي د ا م ل ا ت ا ن و ك م ل ا و جمار ب ل ا تارا د ص ا ل ا ل ا دن ت س م ل ا اذه ي ف ة درا و ل ا تام و ل ع م ل ا دن ت س ت :

- AMP 5.4.20190820 راد ص ل ا ، ة ي ا ه ن ل ا طاقن م ك ح ت ة د ح و ل AMP

ة ص ا خ ة ي ل م ع م ة ئ ي ب ي ف ة د و ج و م ل ا ة ز ه ج ا ل ا نم دن ت س م ل ا اذه ي ف ة درا و ل ا تام و ل ع م ل ا عاشن ا م ت ت ن ا ك ا ذ ا . (ي ض ا ر ت ف ا) ح و س م م ن ي و ك ت ب دن ت س م ل ا اذه ي ف ة م د خ ت س م ل ا ة ز ه ج ا ل ا ع ي م ج ت ا د ب ر م ا ي ا ل ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف نم د ك ا ت ف ، ل ي غ ش ت ل ا د ي ق ك ت ك ب ش

ث ي د ح ت ل ا د ن ع ت ا ع ق و ت ل ا

Exclusions

Show Custom Exclusions Cisco-Maintained Exclusions ?

Search by exclusion set, path, extension, threat name, or SHA-256

All Products Windows Mac Linux

Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the AMP for Endpoints Connector and antivirus, security, or other software. These exclusions may be updated with improvements and new exclusions may be added for new versions of an application.

ريغيغتل كلذسكعيل يففلخل فرطال ىلع جهن ثيذحت ثذحي، Cisco نم اهتناي ص متي يتل مئاوقل ريغيغتن دنع ال. ةثدحملا ةسايسلا نوبحسي مهف، مهبلق تاقد نم ققحت ةمئاقلا كلت مدختست ةياهن ةطقن لك نأ امب ةمئاق يف اريغيغت ةينفلا ةيخانلا نم لثمت اهنأل قيقيدتل لاجس يف هذه ةسايسلا تاريغيغت سكعنتن قيقيدتل لاجس يف Cisco اب ظفتحت يتل داعبتسال مئاوق دجوت الو، اهسفن ةسايسلا سيلو، داعبتسال تاثيردحت نم ضيف هئاكو اذه ودبي، مچجال ةريكبلا تائيبلل ةبسنلابو. ةيدرفلا مكحتل تادحو يف يداعل ةياهنلا طاقن نم ةطقن لك ىلع ءادأل نيسحت يه ةيئاهنلا ةجيتنل نوكتسو، تاسايسلا

يف تاثيردحتلا متتس ف، تنرتنلاب ةلصتم ةزهجال عيجم تناك اذا. ةياهن ةطقن لك ىلع ثيذحتلا ةرتف دمتمت تنرتنل ربع ةزهجال لوخد عم ثودحل يف تاثيردحتلا رمتست، ةيمومع ةئيب هذه تناك اذا. ببلق ةضبن 1-2 قاطن، طاقتحال متي يتل ةمئاقلا عفد نم ةعاس 48 ىل 24 دعب ةسايسلل ةيفاضا تاثيردحت ةيؤر نم شهذنت ال اذل اب.

تاريغتل

2019 - س طسغأ 28

Microsoft Windows ل يضارثفالا ليغشثلا ماظن:

ةلارا:

- CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\edb*.log
- CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log
- CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log

ءانثتسال اذه يطغي ةيساسالا ةومجملا يف رخآ ءانثتسا كانه. راركتلا: ببسال

ةفاضل:

- C:\\$WINDOWS~BT\Sources\SetupHost.exe

ةيلمعلل تي رجا يتل صحتل ايلممع ببسب عطقتم لك شب Windows 10 تاثيردحت تلشف: ببسال

ذفاونلا - ةيسمشلا حايرلا N-Able:

ةفاضل:

- C:\Program Files (x86)\N-able Technologies\Windows Agent\bin\agent.exe
- C:\Program Files (x86)\BeAnywhere Express\GetSupportService_N-Central\BASupSvc.exe
- C:\Program Files (x86)\N-able Technologies\PatchManagement\ThirdPartyPatch\ThirdPartyPatch.exe

Docker - Mac:

ذلازا:

- /users/*/Library/Containers/com.docker.docker/Data/vms/*/Docker.*
- /usr/local/bin/docker

لضفأ تاداعبتسا ةيمنتلا تدح كذل ،نمألا نأشب لغاوش عم ةيفاضلا ابراجتلا انتكرت دقو: ببس

إفاض:

- /Applications/Docker.app/Contents/MacOS/Docker
- /Applications/Docker.app/Contents/Resources/bin/docker

ةديج مئاوق عاشنإ مت:

سك وني:

- Docker - لصوملا 1.10.2
- 1.11+ لصوملا - مداخل
- سكيباز

كام:

- يرهاظلا قودنصلا
- يمقرلا سراجلا

2019 - ربمتبس 18

Apple MacOS: ليغشتلا ماظنل يضارتفالا عضولا

إفاض:

- /Applications/Time Machine.app/Contents/MacOS/Time Machine
- /System/Library/CoreServices/Spotlight.app/Contents/MacOS/Spotlight

McAfee - Mac

إفاض:

- /Library/McAfee/Agent/bin/CmdAgent

Cisco Jabber - Mac

تلاز:

- /usr/bing/grep
- /bin/ps

تيلمغلا ىلع عمئاقلا تاداعبتس الل ةيفاضل فئاظوو لصفأ نام: ببسلا

ةفاضل:

- /Applications/Cisco Jabber.app/Contents/MacOS/Cisco Jabber

Crashplan - Mac

ةفاضل:

- /Applications/CrashPlan.app/Contents/Library/LaunchServices/CrashPlanService.app/Contents/MacOS/CrashPlanService

JAMF Casper - Mac

تلاز:

- /usr/bin/sw_vers

تيلمغلا ىلع عمئاقلا تاداعبتس الل ةيفاضل فئاظوو لصفأ نام: ببسلا

ةفاضل:

- /library/application Support/JAMF/Jamf.app/Contents/MacOS/JamfDaemon.app/contents/MacOS/JamfDaemon
- /usr/local/jamf/bin/jamfAgent
- /usr/local/jamf/bin/jamf
- /library/application Support/JAMF/Jamf.app/Contents/MacOS/JamfAgent.app/contents/MacOS/jamfAgent

VMWare Fusion - Mac

ةفاضل:

- /Applications/VMware Fusion.app/Contents/MacOS/VMware Fusion

XCODE - Mac

ةفاضل:

- /Applications/Xcode.app/Contents/SharedFrameworks/XCBuild.framework/Versions/A/PlugIns/XCBuildService.bundle/Co
- /Applications/Xcode.app/Contents/Developer/usr/bin/xcodebuild

Windows - دحاو صارقأ كرحم

فئاط ربيغت:

- C:*Users\OneDrive\ (لضف أ ناماً إلى لوصحلل ةيسكع ةلئام ةطرش فاضاً)

ICA - Windows ليمع سكرتيس

ةفاض:

- Csidl_PROGRAM_FILES\Citrix\User Profile Manager\UserProfileManager.exe
- csidl_program_files\Citrix\Virtual Desktop Agent\BrokerAgent.exe
- CSIDL_PROGRAM_FILES\Citrix\ICAService\picaSvc2.exe
- CSIDL_PROGRAM_FILES\Citrix\ICAService\CpSvc.exe

تاءانثتس إ حرتقي Citrix ةكرشل شيدحت ثدجاً: ببسلا

ةديج مئوق عاشنإ مت

زودنيو

- Citrix دادمإ مداخل
- Citrix ةباحس لصوم

2019 - ربمسي د 11

Windows - دجاو صارقأ كرحم

ةفاض:

- CSIDL_LOCAL_APPDATA\Microsoft\OneDrive\OneDrive.exe

Splunk - Windows

ةفاض:

- CSIDL_PROGRAM_FILE\splunkforwarder\bin\splunk-winevtlog.exe
- CSIDL_PROGRAM_FILE\splunkforwarder\bin\splunkd.exe

Splunk - Linux

ةفاض:

- /opt/splunkforwarder/bin/splunk
- /opt/splunk/bin/splunk

ةديج مئوق عاشنإ مت

Azure - Linux

Mac - درشتملا

رياربف 12 - 2020

Windows لڤيغشتللا ماطن - Microsoft Windows لڤيغشتللا ماطن

إفاضة:

- C:\Program Files\Cisco\Orbital\osqueryd.exe
- C:\Program Files\Cisco\Orbital\orbital-ampwin.exe

WebSense - Windows

إفاضة:

- [ةددعت م صارقاً تاركح م]:\Program Files*\WebSense\
- C:\Program Files (x86)\WebSense\WebSense Endpoint\dserui.exe
- C:\Program Files\WebSense\WebSense Endpoint\dserui.exe
- C:\Program Files (x86)\WebSense\WebSense Endpoint\EndPointClassifier.exe
- C:\Program Files (x86)\WebSense\WebSense Endpoint\FilterSDK\kvoop.exe
- C:\Program Files (x86)\WebSense\WebSense Endpoint\wepsvc.exe

Microsoft SQL Server - Windows

إفاضة:

- csidl_program_files\Microsoft SQL Server\MSSQL\FTDATA\
- .sql

وينوي 10 - 2020

Malwarebytes - Windows

فيفط ريغت:

- C:\ProgramData\Malwarebytes Endpoint Agent\
- C:\ProgramData\Malwarebytes\MBAMService\

Microsoft Office - Windows

إفاضة:

- C:\Program Files\Common Files\Microsoft shared\ClickToRun\OfficeClickToRun.exe

IIS - Windows

إفاضة:

- C:\Windows\SysWOW64\inetsrv\w3wp.exe

- C:\Windows\System32\inetsrv\w3wp.exe

Altiris ةطس اوب Symantec - Windows

ةفاضل:

- C:\Program Files\Altiris\AltirisAgent\AeXNSAgent.exe

McAfee - Windows

ةفاضل:

- C:\Program Files\McAfee\Endpoint security\Adaptive Threat Protection\mfeature.exe

ةديج ةمئ اوق ءاشن ا مت

NetScout - Windows

IBM - Windows

2020 - وي لوي 15

Windows - لاجم ل اب م كحت ل ا تادحو

ةفاضل:

- csidl_windows\System32\dfs.exe
- csidl_windows\System32\dfsrs.exe
- csidl_windows\System32\dns.exe
- csidl_windows\System32\ntfrs.exe

Microsoft Teams - Windows

ةفاضل:

- CSIDL_LOCAL_APPDATA\Microsoft\Teams\current\teams.exe
- CSIDL_LOCAL_APPDATA\Microsoft\Teams\update.exe

ةديج ةمئ ا ق ءاشن ا مت

م كحت ل ا

2020 - س طس غ ا 26

ن ي رش ع ل ا و س داس ل ا ل ا رش ع س ا ت ل ا ن م ي ل ص ا ل ا ر ا د ص ا ل ا خ ي ر ا ت د ي د م ت م ت ، ر ا ب ت خ ا ل ا ن م د ي ز م ل ا ر ط ن **

Microsoft SQL Server - Windows

لادبتسالا:

- csidl_program_files\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\SQLServr.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.2\OLAP\Bin\MSMDSrv.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.3\Reporting Services\ReportServer\Bin\ReportingServicesService.exe

ةفاضل:

- csidl_program_files\Microsoft SQL Server\MSSQL.11\MSSQL\Binn\SQLServr.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.12\MSSQL\Binn\SQLServr.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.13\MSSQL\Binn\SQLServr.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.11\OLAP\Bin\MSMDSrv.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.12\OLAP\Bin\MSMDSrv.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.13\OLAP\Bin\MSMDSrv.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.11\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.12\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.13\Reporting Services\ReportServer\Bin\ReportingServicesService.exe

30 ربم تبس 2020

Malwarebytes - Windows

ةفاضل:

- Csidl_PROGRAM_FILES\Malwarebytes' AntiWare\mbam.exe
- Csidl_PROGRAM_FILESX86\Malwarebytes' AntiWare\mbam.exe

Digital Guardian - Mac

ةفاضل:

- /usr/local/dgagent
- /dgagent

ةديج ةمئاق عاشنل مت

Digital Guardian - Windows

3 س رام 2021

Kaspersky - Windows

ةفاضل:

- Cisco_PROGRAM_FILESX86\Kaspersky Lab\Kaspersky Endpoint Security J Windows\avp.exe
- csidl_program_filesx86\Kaspersky Lab\NetworkAgent\klnagent.exe

SCCM - Windows

إزالة:

- Windows\CCM\ServiceData - راسم لة فعضم
- Microsoft\EasySetupPayload - رركم راسم - ةرادا اج ارب ل ات اف ل م

Symantec - Windows

إضافة:

- csidl_program_files\Symantec\Endpoint Agent\edpa.exe
- csidl_program_filesx86\Symantec\Symantec Endpoint Protection\12.1.4013.4013.105\Bin64\SMC.exe
- Csidl_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.6608.6300.105\Bin\ccSvcHst.exe
- Cisco_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.7061.6600.105\Bin\ccSvcHst.exe
- Csidl_PROGRAM_FILESX86\Symantec\Symantec Endpoint Protection\12.1.7385.6902.105\Bin\ccSvcHst.exe
- csidl_program_filesx86\Symantec\Symantec Endpoint Protection\
- csidl_program_files\Symantec\Endpoint Agent\brkrprcs64.exe

ة ديدج مئاوق عاشن ا مت

Cisco AnyConnect - Windows

Microsoft Defender ATP - Windows

30 - وينوي 2021

Microsoft Windows ل يضا رت فالال لي غش التال ماظن

إضافة:

- CSIDL_WINDOWS\System32\GroupPolicy\User\registry.pol
- CSIDL_WINDOWS\System32\GroupPolicy\Machine\registry.pol

لي مع Citrix ICA

إضافة:

- CSIDL_PROGRAM_FILES\Citrix\Broker\Service\BrokerService.exe
- CSIDL_PROGRAM_FILES\Citrix\Broker\Service\HighAvailabilityService.exe
- CSIDL_PROGRAM_FILES\Citrix\ConfigSync\ConfigSyncService.exe
- csidl_program_filesx86\Citrix\ICA Client\

Citrix دادم | مداخ

ةلأنا:

- C:\System32\drivers\CfsDep2.sys
- C:\System32\drivers\CvhdBusP6.sys
- C:\System32\drivers\CVhdMp.sys

ةفاضل:

- CSIDL_WINDOWS\System32\drivers\CfsDep2.sys
- CSIDL_WINDOWS\System32\drivers\CvhdBusP6.sys
- CSIDL_WINDOWS\System32\drivers\CVhdMp.sys
- csidl_program_files\Citrix\Provisioning Services\BNTFTP.EXE
- csidl_program_files\Citrix\Provisioning Services\PVSTSB.exe
- csidl_program_files\Citrix\Provisioning Services\StreamService.exe
- Csidl_Program_Files\Citrix\Provisioning Services\StreamProcess.exe
- csidl_program_files\Citrix\Provisioning Services\soapserver.exe
- csidl_program_files\Citrix\Provisioning Services\Inventory.exe
- csidl_program_files\Citrix\Provisioning Services\Notifier.exe
- csidl_program_files\Citrix\Provisioning Services\MgmtDaemon.exe
- csidl_program_files\Citrix\Provisioning Services\BNPXE.exe
- csidl_program_files\Citrix\Provisioning Services\BndEvice.exe

ةديج مئوق عاشن | مت

CommVault - Windows جمانرب

Citrix - Windows لمرع تاسلج ليحست

2021 - ربمتبس 29

Cisco Webex - Windows

ةفاضل:

- Csidl_LOCAL_APPDATA\CiscoSparkLauncher\CiscoCollabHost.exe
- csidl_local_appdata\CiscoSparkLauncher\
- CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_01\atmgr.exe
- CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_02\atmgr.exe
- CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_03\atmgr.exe
- CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_04\atmgr.exe
- CSIDL_LOCAL_APPDATA\WebEx\WebEx\Meetings_*

Crashplan - Windows

ةفاضل:

- Cisco_PROGRAM_FILES\Code42\Code42Service.exe

Crashplan - Mac

إفاضة:

- /Applications/Code42.app/Contents/Library/LaunchServices/Code42Service.app/Contents/MacOS/C

VMware - Windows

إفاضة:

- csidl_program_filesx86\VMware\VMware DaaS Agent\service\DaaSAgent.exe

23 سرام - 2022

Microsoft Windows ل يضا رت فالال لي غشت لال ماظن

إفاضة:

- C:\Windows\System32\SearchIndexer.exe

Hyper-V - Windows

إفاضة:

- CSIDL_COMMON_APPDATA\Microsoft\Windows\Hyper-V\
- CSIDL_COMMON_DOCUMENTS\Hyper-V\الصارقأل\ةتباثلال صا رة اظلالا

Microsoft Windows Defender - Windows

إفاضة:

- *\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataCollection\

29 وينوي - 2022

Microsoft Windows ل يضا رت فالال لي غشت لال ماظن

إفاضة:

- *.applocker

AnyConnect VPN ن Cisco

إفاضة:

- Cisco_PROGRAM_FILESX86\Cisco\Cisco AnyConnect Secure Mobility Client\acwebhelper.exe

Cisco Webex

إضافة:

- C:\Users*\AppData\Local\WebEx\WebEx\Meetings\atmgr.exe

Microsoft OneDrive (اقباس دجاو صارقاً كرحم)

إضافة:

- C:\Users*\AppData\Local\Microsoft\OneDrive\OneDrive.exe

Windows - مويينات

إضافة:

- C:\Program Files (x86)\Tanium\Tanium End User Notification Tools\bin\End-user-notifications.exe

Citrix دادم| مداخ

إضافة:

- csidl_program_files\Citrix\Provisioning Services\MgmtDaemon.com

إزالة:

- csidl_program_files\Citrix\Provisioning Services\MgmtDaemon.com

ةديج مئاوق عاشن| مت

X1 - Windows ثحب

Microsoft Intune - Windows

2022 - ربمتبس 14

Microsoft Windows ل يضارتفالا ليغشتلا ماطن

إضافة:

- Cisco_PROGRAM_FILESX86\Cisco\Cisco Secure Client\
- Cisco_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\Acumbrellaagent.exe
- Cisco_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\Acumbrellaagent.exencrypt-proxy.exe
- Cisco_PROGRAM_FILESX86\Cisco\Cisco Secure Client\NVM\acnvmagent.exe
- Cisco_PROGRAM_FILESX86\Cisco\Cisco Secure Client\vpnagent.exe
- Cisco_PROGRAM_FILESX86\Cisco\Cisco Secure Client\acnamlogonagent.exe
- Cisco_PROGRAM_FILESX86\Cisco\Cisco Secure Client\acnamagent.exe
- Cisco_PROGRAM_FILESX86\Cisco\Cisco Secure Client\UI\csc_ui.exe

- Cisco_PROGRAM_FILES\Cisco\Cisco Secure Client\CM*\CMID*\csc_cmdid.exe
- Cisco_PROGRAM_FILES\Cisco\Cisco Secure Client\CM*\CMPM*\csc_pm.exe
- Cisco_PROGRAM_FILES\Cisco\Cisco Secure Client\CM*\Service*\csc_cms.exe
- csidl_system\appidpolicyConverter.exe

Microsoft SQL Server

2019 رادصإلا لمشييل هعيسوت مت

إفاضا:

- csidl_program_files\Microsoft SQL Server*\MSSQL\Binn\SQLServr.exe
- csidl_program_files\Microsoft SQL Server*\OLAP\Bin\MSMDSrv.exe
- csidl_program_files\Microsoft SQL Server*\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- Csidl_PROGRAM_FILES\Microsoft SQL Server*\Shared\SQLDumper.exe
- CSIDL_PROGRAM_FILES\Microsoft SQL Server\MS*.*
- csidl_program_files\Microsoft SQL Server*\com\
- csidl_program_files\Microsoft SQL Server*\DTS\
- CSIDL_PROGRAM_FILES\Microsoft SQL Server*\Shared\

نوسكيبأ / وركيام دنيرت

إفاضا:

- csidl_program_filesx86\Trend Micro\Security Agent\CCSF\TMCCSF.exe
- csidl_program_filesx86\Trend Micro\Security Agent\TmPfw.exe
- Csidl_PROGRAM_FILESX86\Trend Micro\Security Agent\TmListen.exe
- csidl_program_filesx86\Trend Micro\Security Agent\Ntrtscan.exe
- csidl_program_filesx86\Trend Micro\iService\iATAS\ATASAgent.exe
- csidl_program_filesx86\Trend Micro\iService\iAC\ac_bin\TMiACAgentSvc.exe
- csidl_program_filesx86\Trend Micro\iService\iES\ESE\ESEServiceShell.exe
- csidl_program_filesx86\Trend Micro\iService\iES\ESE\ESClient.exe
- csidl_program_filesx86\Trend Micro\BM\TMBMSRV.exe
- csidl_program_filesx86\Trend Micro\Security Agent\TMBMSRV.exe
- csidl_program_filesx86\Trend Micro\iService\iVP\iVPAgent.exe
- csidl_program_filesx86\Trend Micro\Security Agent\TmSSClient.exe
- csidl_program_filesx86\Trend Micro\Security Agent\LogServer.exe
- csidl_program_filesx86\Trend Micro\Security Agent\Temp\LogServer\LogServer.exe
- csidl_program_filesx86\Trend Micro\Security Agent\CCSF\module\BES\TmsalInstance64.exe
- Csidl_PROGRAM_FILESX86\Trend Micro\Security Agent\CNTAoSMgr.exe
- Csidl_PROGRAM_FILESX86\Trend Micro\Security Agent\PccNTMon.exe
- csidl_program_filesx86\Trend Micro\iService\iES\ESE\ESEFrameworkHost.exe
- csidl_system\showMsg.exe
- csidl_system\dsagent.exe
- .bkf

ةديج مئوق عاشنإ مت

2022 ربوتكأ

ةئيب لىل اهلاخدا مت يتلاوحيحص ريغ لكشب اهنيوكت مت يتلا تاداعبتسالال ةلازا متتس ،ربوتكأ رهش لالخ لىل عالطال انكميو .ةصصخملا داعبتسالال مئوق نم جتنم لل ةقباسلا تاراركتلا ءانثأ ةنمآلا ةياهنلا ةطقن [.انه](#) ةردابملا هذبه ةقلعتملا تامولعملا نم ديزم

2022 - ربمسي د 14

Microsoft Windows ل يضارتفالال ليغششال ماظن

إفاضة:

- C:\Windows\System32\omadmclient.exe
- .autoDestination-ms

Windows - ةيفلخلال تارييغت

- csc_ui.exe لىل فاضت Exploit Prevention Excludes Global Excludes ل V5 و Script Control.

[تاداعبتسالال لىل ع رثؤي ءادأ](#): ةلازا

ةديج مئوق ءاشنإ مت

Linux و Mac و Windows - رورم ةم لك 1

McAfee Trellix SolidCore - Windows

2023 - ليربأ 12

Microsoft Windows ل يضارتفالال ليغششال ماظن

إفاضة:

- .pf
- Cisco_PROGRAM_FILESX86\Cisco\Cisco Secure Client\acumbrellaagent.exe

ةلازا:

- CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs*.log
- CSIDL_SYSTEM\CatRoot2\
- CSIDL_WINDOWS\Prefetch\

Microsoft Intune

إضافة:

- csidl_program_filesx86\Microsoft Intune Management Extension\Microsoft.Management.Services.IntuneWindowsAgent.exe

McAfee Trellix SolidCore

في ملف ربيغ:

- csidl_PROGRAM_FILESX86\McAfee\Policy Audit Agent\engineMain.exe

Cisco Webex

إضافة:

- C:\Users*\AppData\WebEx\WebexHost.exe

Microsoft Defender ل MacOS

إضافة:

- /تاق يبط ل ل /ة بت ك م ل ا م ع د /Microsoft/Defender/

Microsoft Defender ل Linux

إضافة:

- /opt/microsoft/mdatp/sbin/wdavdaemon
- /opt/microsoft/mdatp/

31 ويام - 2023

ميف

إضافة:

- Csidl_PROGRAM_FILES\Common Files\Veeam\Backup and Replication\Explorer Recovery Service\Veeam.StandBy.Service.exe
- Csidl_PROGRAM_FILES\Common Files\Veeam\Backup and Replication\Mount Service\Veeam.Backup.MountService.exe
- Csidl_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.BrokerService.exe
- csidl_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.CloudService.exe
- Csidl_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.ExternalInfrastructure.DbProvider.exe
- csidl_program_filesx86\Veeam\Backup

- Transport\GuestInteraction\VSS\VeeamGuestHelperCtrl.exe
- csidl_program_files\Veeam\البرنامج\Backup\Veeam.Backup.Service.exe
- Csidl_PROGRAM_FILES\Veeam\Backup and Replication\Backup Catalog\Veeam.Backup.CatalogDataService.exe
- Csidl_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.ManagerGCServer.exe
- csidl_PROGRAM_FILES\Veeam\Backup and Replication\Backup\Veeam.Backup.cdp.Service.exe
- csidl_PROGRAM_FILES\Veeam\Backup and Replication\Console\veeam.backup.shell.exe
- csidl_PROGRAM_FILESX86\Veeam\Backup Transport\x64\VeeamAgent.exe
- csidl_program_files\Veeam\البرنامج\Backup\Veeam.Backup.Manager.exe
- CSIDL_WINDOWS\Veeam\Backup\VeeamDeploymentSvc.exe
- .vbm.temp
- حطس م.

VMWare

إفاضة:

- csidl_program_files\common Files\VMware\ScannerRedirection\ftscanmgrhv.exe
- Cisco_PROGRAM_FILESX86\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe

27 - ربيع الثاني 2023

Cisco Webex

إفاضة:

- Cisco_LOCAL_APPDATA\Programs\Cisco Spark\Cisco CollabHost.exe

Microsoft OneNote

إفاضة:

- CSIDL_LOCAL_APPDATA\Microsoft\OneNote*\cache*.bin

Microsoft SQL Server

إفاضة:

- csidl_program_files\Microsoft SQL Server*\MSSQL\Binn\sqlagent.exe
- csidl_program_files\Microsoft SQL Server*\MSSQL\Binn\MsDtsSrvr.exe
- csidl_program_files\Microsoft SQL Server*\Shared\sqlbrowser.exe
- CSIDL_WINDOWCLUSTER\
- csidl_program_files\Microsoft SQL Server*\MSSQL\FTDATA\

- csidl_window\cluster\clussvc.exe
- csidl_window\cluster\rhs.exe
- .trc

إزالة:

- csidl_program_files\Microsoft SQL Server\MSSQL.11\MSSQL\Binn\SQLServr.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.11\OLAP\Bin\MSMDSrv.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.11\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.12\MSSQL\Binn\SQLServr.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.12\OLAP\Bin\MSMDSrv.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.12\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.13\MSSQL\Binn\SQLServr.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.13\OLAP\Bin\MSMDSrv.exe
- csidl_program_files\Microsoft SQL Server\MSSQL.13\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- csidl_program_files\Microsoft SQL Server\MSSQL*.MSSQLSERVER\MSSQL\Binn\SQLServr.exe
- csidl_program_files\Microsoft SQL Server\MSAS*.MSSQLSERVER\OLAP\Bin\MSMDSrv.exe
- csidl_program_files\Microsoft SQL Server\MSRS*.MSSQLSERVER\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- ف.أ
- .ctl
- .dbf
- .rdo

Microsoft Teams

إضافة:

- CSIDL_LOCAL_APPDATA\Microsoft\Teams\current\squirrel.exe
- csidl_local_appdata\Microsoft\TeamsMeetingAddin

Microsoft Windows لى ضارت فال لى غشت لى ماظن

إضافة:

- CSIDL_WINDOWS\WinSxS*\TiWorker.exe

ةيظاش

إضافة:

- CSIDL_PROGRAM_FILES\splunk\bin\splunk.exe

- CSIDL_PROGRAM_FILES\splunk\bin\splunk*.exe

جمانرب Symantec Endpoint Protection

إفاضة:

- Csidl_PROGRAM_FILES\Symantec\Symantec Endpoint Protection*\Bin64\ccSvcHst.exe
- CSIDL_COMMON_APPDATA\Symantec\Symantec Endpoint Protection\
- csidl_program_filesx86\Symantec\Symantec Endpoint Protection*\BIN64\SMC.exe

إفازة:

- Csidl_WINDOWS\Temp\TMP*.tmp
- CSIDL_WINDOWS\Temp\musdmys_*
- CSIDL_WINDOWS\Temp\content.zip.tmp\SymDeltaDecompressOptions.xml
- CSIDL_WINDOWS\Temp\content.zip.tmp*.diff
- CSIDL_WINDOWS\Temp\content.zip.tmp\cur.scr
- CSIDL_COMMON_APPDATA\Symantec\

ةديج مئوق عاشنإ مت

- Zscaler ليمع ل صوم
- ManageEngine Endpoint Central
- Symantec Data Loss Protection جمانرب

22 - ربمفون 2023

Microsoft Windows ل يضا رت فال ل ليغ شت ل ل ماظن

إفاضة:

- CSIDL_PROGRAM_FILES\Cisco\Orbital\python\python.exe

ليمع Citrix ICA

إفاضة:

- Csidl_PROGRAM_FILESX86\Citrix\ICA Client\SelfServicePlugin\SelfService.exe
- Csidl_PROGRAM_FILESX86\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe
- csidl_program_filesx86\Citrix\ICA Client\Receiver\FeatureFlag\CWAFeatureFlagUpdater.exe
- csidl_program_filesx86\Citrix\ICA Client\wfcrun32.exe
- csidl_program_filesx86\Citrix\ICA Client\Receiver\Receiver.exe

ةديج مئوق عاشنإ مت

- كسي دنال ي ت ن ا ف ي |
- ا ر ي ت ا ل ي ك و

2024 - ريانى 24

ف تاريخى غتلاب قلعتت ة في فط تاليدعت لى لى Microsoft SQL Server و Azure DevOps جاتحأ
تاءانثس إة فاضإ متت مل . Windows Endpoint 8.2.1+ ل داعبتسال ة لاعم

ة ديدج ةمئاق عاشنإ مت

- يل امشلا بطقلا بئذ

ةمچرتل هذه لوج

ةللأل تاي نقتلل نم ةومچم مادختساب دن تسملل اذه Cisco تچرت
ملاعلاء انءمچي في نيمدختسملل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مه تغلب
Cisco يلخت. فرتحم مچرت مامدقي يتلل ةيفارتحال ةمچرتلل عم لالحل وه
ىلإ أمئاد ةوچرلاب يصوت وتامچرتلل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزي لچنلإل دن تسملل