

Cisco في اهترادو تاءانثتسالا نيوكت Secure Endpoint Connector

تايوتحمل

[عمدقمل](#)

[قيساسالا تابلطتمل](#)

[تابلطتمل](#)

[عمدختسمل تانوكمل](#)

[قنمألا قياهنلا عطقن لمع ريس](#)

[تاداعبتسالا لعل Cisco تظفاح](#)

[قصصخم تاداعبتسالا](#)

[قنمألا قياهنلا عطقن كرحم](#)

[راسمل اعنثتسالا](#)

[Wildcard اعنثتسالا](#)

[فللمل اقحلم اعنثتسالا](#)

[تافللمل احسم اعنثتسالا: قيلمعلا](#)

[\(SPP\) ماظنلا قيلمع قيامح](#)

[SPP اعنثتسالا](#)

[\(MAP\) قراضلا عطش نألا قيامح](#)

[عطيرخل اعنثتسالا](#)

[\(EXPREV\) لالغتسالا اعنم](#)

[\(BP\) قيكولسالا قيامحلا](#)

[قلمص تاذت امولعم](#)

عمدقمل

عطقن مكحت ةدحو لعل ةفلتخملا تاكرحملا داعبتسالا اعشنإ قيفيك دنتمسالا اذه فصق
Cisco نم قنمألا قياهنلا

قيساسالا تابلطتمل

تابلطتمل

ةيلالل عيضاوملاب ةفرعم كيدل نوكت نأ Cisco قيصوت:

- قنمألا قياهنلا عطقن مكحت ةدحو قيسايس لعل اهقبيبطتو داعبتسالا عمئاق ليدعت
- Windows CSIDL قيقافتا

عمدختسمل تانوكمل

ةيلالل قيدامل تانوكمل او جماربلل تارادصا لىل دنتمسالا اذه قف ةدراولل تامولعمل دنتمست

- Cisco نم 5.4.20211013 ةنمآلا ةياهنلا ةطقن مكحت ةدحو
- 2021 ربوتكأ 15 ةنمآلا ةياهنلا ةطقن مدختسم ليلد ةعجارم

ةصاخ ةيلعم ةئيب يف ةدوجوملا ةزهجالا نم دنتسملا اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا. (يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجالا عيمج تادب رمأ يال لمحتملا ريثاتلل كمهف نم دكأتف، ليغشتلا ديقتك تش

ةنمآلا ةياهنلا ةطقن لمع ريس

ةيمزراوخ ةجلعم يل Cisco نم ةنمآلا ةياهنلا ةطقن لمعت، تايلعمل نم ليع يوتسم يف لصلول ةيسيلل تانوكملا لالخنم بيترتلا اذبه (SHA) تافللمل ةنمآلا ةئجتل

- تاداعبتسالا
- ارتت كرحم
- (رظحلا ةمئاق / حامسلا ةمئاق) قيبطتلا يف مكحتلا
- SHA كرحم
- كرحم / ماظنلا ةيلعم ةيماح / (MAP) راضلا طاشنلا ةيماح / (ExPrev) لالغتسالا عنم (زاهجلا قفدت طبر) ةكبشلا



فشتك يذلا كرحملا يلع ةمئاقلا رظح/حامسالا وأ داعبتسالا عاشنإ دمتعي: ةظالم فللم.

تاداعبتسالا يلع Cisco تظفاح

ريفوتل Cisco ةطساوب اهتنايصو Cisco نم اهتنايص متي يتلا تاءانثتسالا عاشنإ متي وأ نامألا تاجتنمو تاسوريفل ةحفاكمو ةنمآلا ةياهنلا ةطقن لصلوم نيب لصفأ قفاوت يرخألا جماربلا.

ليغشتلا نامضل تاداعبتسالا نم ةفلتخم عاونأ يلع هذه داعبتسالا تاعومجم يوتحت ميلسلا.

[تاريخيغت](#) ةلاقملا يف تاءانثتسالا هذه يلع اهؤارج متي يتلا تاريخيغتلا بقعت كنكمي [Cisco J Cisco Secure Endpoint Console](#) نم اهتنايص متي يتلا داعبتسالا ةمئاق.

ةصصخم تاداعبتسا

ةنمآلا ةياهنلا ةطقن كرحم

كرحم ةطساوب (تافللملا فاشتك / (CPU) ةيزكرملا ةجلعمل ةدحو مادختسا) تافللملا صحف Tetra و SHA:


[ةدحو نيماأ فيفختل](#) وأ فلم لزع/فاشتك بئجتل تاداعبتسالا نم عاونألا هذه مدختسا [ةياهنلا ةطقنل \(CPU\) ةيزكرملا ةجلعمل](#).

ةروصللا يف حضورم وه امك ةنمآلا ةياهنلا ةطقن مكحت ةدحو يلع دوجوملا شحل ضرع متي

luivelaz detected CCC.ps1 as Generic.PwShell.RefA.E40F0C1F Medium [Share] [Comment] [Quarantine: Successful] 2020-03-19 23:19:11 UTC

File Detection	Detection	Generic.PwShell.RefA.E40F0C1F
Connector Info	Fingerprint (SHA-256)	943fdc5f...6cf70fc1
Comments	File Name	CCC.ps1
	File Path	C:\Users\luivelaz\Desktop\CCC.ps1
	File Size	2.1 MB
	Parent Fingerprint (SHA-256)	e5d90bee...a7f914f7
	Parent Filename	notepad.exe

[Analyze](#)
[Restore File](#)
[All Computers](#)
[View Upload Status](#)
[Add to Allowed Applications](#)
[File Trajectory](#)


 **اذه Microsoft دنتسم** ىلا عوجرلا ىجري ، تاداعبتس لال CSIDL مادختسا نكمي :ةظحالم CSIDL لوح تامولعمل نم ديزم ىلع لوصحلل

راسملا ءانثتسا

Path	C:\Users\luivelaz\Desktop\CCC.ps1	
------	-----------------------------------	---


Wildcard ءانثتسا

Wildcard	C:\Users*\Desktop\CCC.ps1	
	<input type="checkbox"/> Apply to all drive letters	


 قىبطتل "صارقالا كرحم فرحأ عي مج ىلع قىبطت" رايخالا مادختسا متي :ةظحالم م.ماظنلاب ةلصت مالا [ىلى A نىم] صارقالا تاكرحم ىلع اضيا ءانثتسا لال

فللملا قحلم ءانثتسا

File Extension	.ps1	
----------------	------	---

 تافللملا عي مج دعبتسي هنأل رذحلا ىخوت عم داعبتس لال نم عونلا اذه مدختسا :ريذحت راسملا عقوم نع رظنلا ضغب صحفلا تايلمع نم فللملا قحلم اذا

تافللملا حسم ءانثتسا :ةيلمعلا

Process	Path	C:\Path\to\executable.exe	
File Scan	SHA		
	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.		
	<input checked="" type="checkbox"/> Apply to child processes		

(SPP) ماظنلا ةيلمع ةيماح

Windows تايلمع ةيماح موقيو و 6.0.5 رادصلا لصوملا نم ماظنلا تايلمع ةيماح كرحم رفوتي ةيلات:

- لملعلا ةسلج ريدمل يعرفلا ماظنلا (smss.exe)
- مداخلال/اليعملال ليغشت تقول يعرفلا ماظنلا (csrss.exe)
- ةلحمل نمألا ةطلسل يعرفلا ماظنلا (lsass.exe)
- Windows (winlogon.exe) لولخلد ليحست قيبطت
- Windows (wininit.exe) ليغشت ادب قيبطت

SPP ةروصلال هذه ضرعت

▼ UMONTERO-Y36YQ.cisco.com prevented unexpected access to lsass.exe by TestAMPprotect.exe. Low [P] [P] [P] System Process Protection 2020-03-09 21:03:11 UTC

Event Details	Fingerprint (SHA-256)	aa52b2d3...acee8d21
Connector Info	File Name	lsass.exe
Comments	File Path	C:\Windows\System32\lsass.exe
	File Size	56.73 KB
	Reason	Process module is not clean and not signed
	Parent Fingerprint (SHA-256)	f3c7b460...fd3b16dd
	Parent Filename	TestAMPprotect.exe
	Parent File Size (bytes)	1608704

[Analyze](#)

SPP ءانثتسا

Process	Path	Path\to\the\executable.exe
System Process	SHA	
<p>You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.</p> <p><input checked="" type="checkbox"/> Apply to child processes</p>		

Process	Path	
System Process	SHA	SHA-256 of the file (From the Parent Filename field)
<p>not a valid SHA-256</p> <p>You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.</p> <p><input checked="" type="checkbox"/> Apply to child processes</p>		

(MAP) ةراضلا ةطشنألا ةيامح

جمانرب موجه نم كب ةصاخلا ةياهنلا ةطقن نع عفاذي، (MAP) ةراضلا ةطشنألا ةيامح كرحم ريفشتلا نم كئانايب يمحيو، اهذيفنت دنع ةراضلا تايلمعل وأ تاءارجال ددحي وهو. ةيدفلا

ةروصلال هذه يف MAP ةروصلال ضرعت متي

Malicious Activity Protection	Fingerprint (SHA-256)	9967f55a...2956d820
Connector Info	Affected Files Count	5
Comments	Affected Files	C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\1.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\0.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\4.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\2.txt.new C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite_data\3.txt.new
	File Name	rewrite.exe
	File Path	C:\Users\umontero\Desktop\Test files\AMP4E-8120-SPP-MAP-EXPREV-test_files\Map\rewrite.exe
	File Size	4.37 MB
	Parent Fingerprint (SHA-256)	9967f55a...2956d820
	Parent Filename	rewrite.exe
	<input type="button" value="Analyze"/> <input type="button" value="Restore File"/> <input type="button" value="All Computers"/>	

ةطيرخلاءانثتسإ

Process	Path	Path\to\the\executable.exe
Malicious Activity	SHA	
You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.		
<input checked="" type="checkbox"/> Apply to child processes		

سېل فشكلا نأ نم دكأتلادعبو رذخلال يخوت عم داعبتسالا نم عونلا اذه مدختسأ: ريذحت لعلاب اراض.

لالغتسالا عنم (EXPREV)

ةركاذلا نقح تامجه نم كب ةصاخلا ةياهنلا طاقن نع عافدلابلالغتسالا عنم كرحم موقري متي يتلا ىرخألا تامجه لاول ةراضلال جماربلا لبق نم عئاش لكشب اهم ادختسإ متي يتلا اهححصت متي مل يتلا جماربلا لىل ع رفض موي يف اهذيفنت نل نكل، اذح دلويو عنم متيس، ةيمحم ةيلمع دض موجه فشتكى ام دنع. فعضلا نم كم يحص رجح كانه نوكي.

ةروصلال هذه يف Exprev ثدح ضرع متي.

Testing.machine1.amp.com prevented an exploit in CUDL.LOS.exe process.		
Exploit Prevention	Fingerprint (SHA-256)	ab6b87b8...3e70e087
Connector Details	Attacked Module	c:\program files (x86)\adobe\acrobat dc\acrobat\bib.dll
Comments	Application	CUDL.LOS.exe
	Base Address	0x7C700000
	File Name	CUDL.LOS.exe
	File Path	C:\Users\mabat\AppData\Local\Apps\2.0\E9781GXN.CJV\80XQ3X5B.94H\lend...app_1d4e2229d1ba886_07e5.0402_a608579ft
	File Size	5.82 MB
	Parent Fingerprint (SHA-256)	375a7501...e8624659
	Parent Filename	dfsvc.exe
	Parent File Size	24.27 KB
	<input type="button" value="Analyze"/>	

لالغتسالا Exprev

Executable	Name	CUDL.LOS.exe	
Exploit Prevention	Provide an executable name to be excluded from protection by the Exploit Prevention engine (Example: ValidExecutable.exe).		

+ Add Exclusion + Add Multiple Exclusions... Save

⚠ دحوال ىلع طاشننلا يف قثت تنك املك داعبتسال اذم مدختسأ: ريذحت رثأت ملاقىب طتل/ةي طمنلا

ةي كولسللا ةيامحل (BP)

قمعتو. ايكولس اهف اقي او تاديدهتلا فاشتك ىلع ةردقلا ةي كولسللا ةيامحل كرحم ززي رفوتو "يضارال جراح متت يتلا" تامحل فاشتك ىلع ةردقلا عيقوتلا شيذحت لالخنم ديدهتلا ةئيبي يف تاريغتلل عرسأ ةباحسإ

ةروصللا هذه يف BP شح ضرع متي

Testing.machine2.amp detected Scheduled Task Containing Suspicious Target Tactics Medium Threat Detection 2022-10-20 17:07:41 UTC

Event Overview	Description	A suspicious scheduled task was created. This particular task stands out because it references a shortcut (.lnk) or a VB script file (.vba or .vbs). The schtasks command can create one-time only tasks, recurring tasks, and tasks that run based on specific system events, such as logon and startup. Malware can use scheduled tasks to establish persistence.	
Connector Details	Occurred At	2022-10-20 17:07:40 UTC	
Comments	Tactics	TA0002: Execution TA0003: Persistence	
	Techniques	T1053.005: Scheduled Task/Job: Scheduled Task	

MITRE | ATT&CK

Observables

File: schtasks.exe 013c013e...b0ad28ef

Analyze

BP ءانثتسإ

Process	Path	Path/to/the/executable/executable.exe	
Behavioral Protection	SHA	You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.	
<input type="checkbox"/> Apply to child processes			

+ Add Exclusion + Add Multiple Exclusions... Save

ةلص تاذ تامولعم

- [مدختس ملاقىلد ىلا لقتنا، جهنلا نيوكت لوح تامولعملا نم ديزم](#)
- [Cisco Secure Endpoint Connector ويدي في تاءانثتسإ ءاشنلا](#)
- [Cisco Systems - تادنتس ملاقىل وينقتلا معدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة يرش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ل أ مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا