

# ةي صننلا جماربلا ةيامح عاطخأ فاشكتسا ةياهنلا طاقنل AMP في اهالصال

## تاوت حمل

[ةمدقملا](#)

[ةيساسألا تابلطتلا](#)

[تابلطتلا](#)

[ةمدختسلا تانوكملا](#)

[ةيساسألا تامولعم](#)

[نيوكتلا](#)

[فاشكتسا](#)

[اهالصال عاطخألا فاشكتسا](#)

[فشكتلا في قيقتلا](#)

[بذالكلا يباچيالا فشكتلا](#)

[ةلص تاذا تامولعم](#)

## ةمدقملا

جماربلا نم ةمدقتلا ةيامحلا في يصننلا جماربلا ةيامح كرحم نيوكت دننتسلا اذه فصلي  
ةياهنلا طاقنل (AMP) ةراضلا.

## ةيساسألا تابلطتلا

### تابلطتلا

ةيلاتلا عيضاوملاب ةفرعم كيديل نيوكت ناب Cisco في صوت:

- AMP مكحت ةدحو لىل لوؤسلا لوصو.

### ةمدختسلا تانوكملا

ةيلاتلا ةيداملا تانوكملا وجماربلا تارادصلا لىل دننتسلا اذه في ةدراولا تامولعملا دننتست:

- شحأ رادصا وأ 7.2.1 رادصالا لوصوملا
- 1709 رادصالا Windows Server 2016 وأ شحألا تارادصالا او 1709 رادصالا Windows 10 شحألا تارادصالا او

ةصاخ ةيلمعم ةئيبي في ةدوجوملا ةزهجالا نم دننتسلا اذه في ةدراولا تامولعملا عاشنلا مت  
تلك اذا. (فيضارتفا). حوسمم نيوكتب دننتسلا اذه في ةمدختسلا ةزهجالا عيمج تادب  
رما يال لمحتحملا ريثاتلل كمهف نم دكاتف، ليغشتلا ديقتك تكبش.

## ةيساسألا تامولعم

م تي يتلا ةيصننلا جماربلا فاشكتسا لىل ةردقلا ةيصننلا جماربلا ةيامح كرحم رفوي

ةمئاقلا تامجهلا نم ةيماحللا ىلع دعاسي امك ،اهرظحو كب ةصاخلا ةياهنلا طاقن ىلع اهذيفنت راسم "جمانرب رفوي .ماع لكشب ةراضلا جماربلا اهمدختست يتلا ةيصنلا جماربلا ىلع تاقببطللا ةبقارم كنكمي اذهو ،ةلسلسلا ذيفنت ءانثأ ةقئاف ةيؤر ةيناكم! "زاهجلا كتزهجا ىلع ةيصنلا جماربلا ذيفنتب موقت يتلا

ةيلالاتلا يصنلا جمانربلا تافلما ءاونأ حسمب لصوملل كرحملا حمسي

قبيطتلا	فلملا قحلم
HTML قبيطت	اته
ةيصنلا جماربلا	JS و VB و VBS و CMD و BAT
رفشم يصن جمانرب	ي   س   ف ، ي   س   ج
Windows Script	WS و WASF و SWC و WSH
لش رواب	PS1، PS1XML، PSC1، PSC2، MSH، MSH1، MSH2، MSHXML، MSH1XML، MSH2XML
راصتخالا	SCF
طبار	LNK
دادعإ	INF و INX
لجسلا	جير
ةملك	DOCX و dotx و DOCM و DOTM
Excel	XLS و XLSX و XLTX و XLSM و XLTM و XLAM
تنيوب رواب	PPT و PPTX و POTX و POTM و PPTM و PPAM و PPSM و SLDM

نيلالاتلا يصنلا جمانربلا يمجرتم عم يصنلا جمانربلا ةيماح لمعت

- PowerShell (ثدخال تارادصإ او ثلاثلا رادصإ)
- Windows Script Host (wscript.exe و cscript.exe)
- JavaScript (حفصتم ريغ)
- VBScript
- Office VBA وركام تادحو

ةيصنلا جماربلا نم ةيماحللا وأ ةيؤرلا ةيناكم | ةيصنلا جماربلا ةيماح رفوت ال :ريذحت Ruby و PHP و Perl و Python لثم Microsoft ل ةعباتلا ريغ ةرسفملا

لثم مدختسملا تاقببطل ىلع يحيصل روجللا ءن اذإ عضو رثوي نأ لمحتحملا نم :ريذحت Word و Excel و PowerPoint. راض يصن VBA جمانرب ذيفنت تاقببطللا هذه تلواح اذإ . قبيطتلا فاقبي متيس

ىلع لمعتو ،ذيفنتلا دنع ليغشتلا عضو مارتحإ ىلع يصنلا جمانربلا ةيماح لمعت نم ةيصنلا جماربلا عنم متي ،طشنلا عضولا ي ف .Active و Passive: نيلفلتخم ني عضو ي ف .ةلهم ىلا لوصولا مت وأ اثببخ ناك اذإ امع تامولعم لصوملا ملتسي يتح ذيفنتلا يصنلا جمانربلا نع ثحبلا ءانثأ ةيصنلا جماربلا ذيفنتب حامسلا متي ،لماخلا عضولا ال ما اثببخ ناك اذإ ام ديذحتل

## نيوكتلا

دح "تاكرحملاو اعاضوالا" تحت مث ،جهنلا تادادعإ ىلا لقتنا ،ةيصنلا جماربلا ةيماح نيكممتل ةروصلا ي ف حضوم وه امك ،لليطعتلا وأ لزعللا وأ قيقدتلل ءنادإل عضو

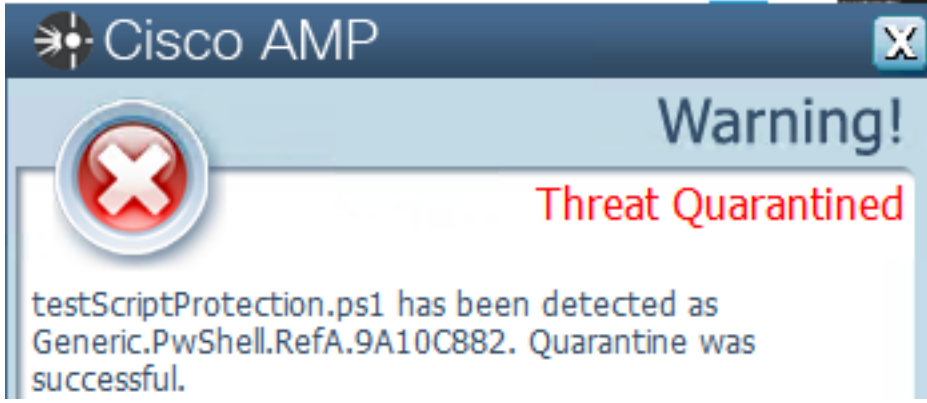
### Script Protection

Quarantine	Audit	Disabled
------------	-------	----------

TETRA نيكمت مت اذا نكلو TETRA ىلع ةيصننلا جماربلا ةيامح دمتعت ال: ةطخال م ةيفاضا ةيامح ري فوتل اهمدختست اهناف.

## فاشكا

يف حضورم وه امك، ةياهنلا ةطقن ىلع قثبنم مالعإ ضرع متي، فاشكال ليغشت درجم ب ةروصلال.



ةروصلال ي ف حضورم وه امك، "ديدهت نع فاشكال مت" ثدح مكحتلال ةدحو ضرعت.

leisanch detected testScriptProtection.ps1 as Generic.PwShell.RefA.9A10C882		Medium	Threat Detected	2021-04-13 20:30:12 UTC
File Detection	Detection	Generic.PwShell.RefA.9A10C882		
Connector Details	Fingerprint (SHA-256)	df5b2781...e83e15cc		
Comments	File Name	testScriptProtection.ps1		
	File Path	C:\Users\mex-amp\Downloads\testScriptProtection.ps1		
	File Size	2.1 MB		
	Parent Fingerprint (SHA-256)	7d37bc10...9a9aed11		
	Parent Filename	notepad.exe		
Analyze		Restore File	All Computers	View Upload Status
		Add to Allowed Applications	File Trajectory	

ال هناف، كلذ عمو، راض ي صنن جمانرب ذي فننت دنع اثدح قيقدتلل عضو قلخي: ةطخال م ه لزع متي.

## اهحالص او ءاطخال فاشكسا

مكحتلال ةدحو ي ف فاشكال ليغشت دنع ددحم ثدح عون ىلع ةيصننلا جماربلا ةيامح يوتحت ال متي ني او فلملال عون ىل اذانتسا راضال فلملال فاشككي نم ىلع فرعتلل ةقيرط ي هو هليغشت.

لبي بس ىلع، فلملال قحلم فيرعتب مق، ةم و ءدملا ةيصننلا جماربلا عم حضورم وه امل اقفو. 1. ps1. ل ي صنن جمانرب وه، لاثملا.

نم ديزملا ضرع متي مسقلا اذ ه ي ف، ثدحلال ليصافت > زاوجل راسم ىل ا لقتنا. 2. دي دحت ه ي ف مت راسم وهو، SHA256 لثم، هنع فاشكال مت يذلا فلملاب ةقلعتملا ليصافتلا يذلا كرحملاو، AMP لصوصم ةطساوب هذاختا مت يذلا ءارجالو، ديدهتلا مساو، فلملال عقوم لبي بس ىلع، SHA Engine ضرورملا كرحملا نوكي، TETRA نيكمت مدع ءلاحي ي ف. ه فاشككي ي صننلا جمانربلا ةيامح عم لمعي، TETRA نيكمت دنع ه نأ شيح TETRA ضرع متي، لاثملا ةروصلال ي ف حضورم وه امك، ةيفاضا ةيامح ري فوتل.

Event Details

Medium

2021-04-13 20:30:12 UTC

Detected **testScriptProtection.ps1** (df5b2781...e83e15cc) as **Generic.PwShell.RefA.9A10C882**.

Created by **notepad.exe**, Microsoft® Windows® Operating System [7d37bc10...9a9aed11][PE\_Executable] executing as mex-amp@LEISANCH.

The file was **quarantined**.

File full path: C:\Users\mex-amp\Downloads\testScriptProtection.ps1

File size: 2206875 bytes.

Parent file SHA-1: e8ee95e69c9c8ba5046016d47f140f43b76c2b20.

Parent file MD5: 4093249b1156c08762d198ba5ef8bddb.

Parent file size: 181248 bytes.

Parent process id: 9708.

Parent process SID: S-1-5-21-525038272-3878948191-2405044030-1001.

Detected by the Tetra engines.

## فشكلا في قيقحتلا

رېفوتل "زاهجال راسم" مادختسا كنكمي، ال مأل فللاب اراض فشكلا ناك اذا ام ديدحتلا، لصلالا تايلمعال لثم يصنلا جم انربلا ليغشت اناثا تثدح يتلا اذحلال ةيؤرة ناكم، لبق نم اهليزنت نكمي يتلا ةفورعلم ريغ تافلماو، دعب نع ني فيضملاب تالاصتالاو ةراضلا جماربالا.

## بذاكلا يباحيالا فشكلا

ةئيبلا لبق نم افورعمو هب اقووم يصنلا جم انربلا ناك اذاو فشكلا يلع فرعتلا درجمب اناثتسا عاشن كنكمي، هحسم نم لصلومال عنمل. بذاك بجوم هتيمست نكمي، كب ةصاخلا ةروصلال في حضورم وه امك، يصنلا جم انربلا كذل.

Path C:\Pathlocation\ScriptName.ps1

لصلومال يلع ةقبطملا ةسايسلا لىل داعبتسالا ةومجم ةفاضل نم دكأت: ةظحالم رثاتملا.

## ةلص تاذا تامولعم

- [AMP مدختسم ليلد](#)
- [تادن تسم لاول ينقت لامل عدلا - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةففارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل